CA Enterprise Log Manager

Manuel d'administration

r12.1

La présente documentation ainsi que tout programme d'aide informatique y afférant (ci-après nommés "Documentation") vous sont exclusivement fournis à titre d'information et peuvent être à tout moment modifiés ou retirés par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si un autre accord de confidentialité entre vous et CA stipule le contraire.

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

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

SOUS RESERVE DES DISPOSITIONS PREVUES PAR LA LOI APPLICABLE, CA FOURNIT LA PRESENTE DOCUMENTATION "TELLE QUELLE" SANS AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, NOTAMMENT AUCUNE GARANTIE DE LA QUALITE MARCHANDE, D'UNE QUELCONQUE ADEQUATION A UN USAGE PARTICULIER OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ETRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RESULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITE, PERTE DE DONNEES OU DE CLIENTS, ET CE MEME DANS L'HYPOTHESE OU CA AURAIT ETE EXPRESSEMENT INFORME DE LA POSSIBILITE DE LA SURVENANCE DE TELS DOMMAGES OU PERTES.

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

CA est le fabricant de la présente Documentation.

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

Produits CA référencés

Ce document fait référence aux produits CA suivants :

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

Support technique

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

Modifications de la documentation

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

- Tâches associées aux rôles : cette section existante dans le chapitre Comptes d'utilisateur aborde les tâches prises en charge par chaque nouvelle fonctionnalité d'un point de vue basé sur les rôles.
- Stratégies d'accès prédéfinies : cette section existante dans le chapitre Stratégies contient des stratégies mises à jour prenant en charge l'accès aux nouvelles fonctionnalités.
- Configurations de services : cette section existante dans le chapitre Services et adaptateurs CA inclut de nouvelles rubriques sur les Remarques sur le serveur ODBC et sur le Service Etat du système.
- Tâches Etat du système : cette nouvelle section dans le chapitre Services et adaptateurs CA décrit la surveillance et la gestion du système CA Enterprise Log Manager.
- A propos des mises à jour à la demande : cette nouvelle section dans le chapitre Abonnement décrit la mise à jour des fichiers sur un serveur sélectionné en dehors du processus des mises à jour d'abonnement planifiées.
- Préparation à l'utilisation de rapports avec des listes à clés : cette section existante dans le chapitre Requêtes et rapports a été mise à jour afin de décrire un nouveau moyen de définir et de mettre à jour des valeurs de listes à clés : il s'agit de l'importation de valeurs mises à jour de manière dynamique par le processus CA IT PAM spécifié. Cette section identifie également de nouvelles clés prédéfinies et les rapports qui les utilisent.
- Personnalisation de requêtes pour les alertes d'action : cette nouvelle section a été ajoutée comme amélioration pour l'envoi d'alertes non seulement à des individus, mais également à des produits (CA NSM et CA Spectrum) et à des processus, plus précisément des processus de sortie de l'événement/de l'alerte CA IT PAM. Cette section est axée sur la création d'alertes pour les événements présentant une sévérité élevée.
- Utilisation de processus de sortie de l'événement/de l'alerte CA IT PAM : cette nouvelle section dans le chapitre Alertes d'action décrit l'intégration avec un produit CA IT PAM distant configuré avec un processus de sortie de l'événement/de l'alerte qui gère un produit tiers. Elle inclut des exemples d'exécution d'un processus de sortie de l'événement/de l'alerte à partir d'une ligne de résultat de requête sélectionnée, ainsi que des exemples d'exécution d'un tel processus par le biais d'une alerte planifiée avec des valeurs de paramètres sur mesure.

- Utilisation d'interruptions SNMP : cette nouvelle section dans le chapitre Alertes d'action décrit la configuration des serveurs de destination, CA Spectrum et CA NSM, pour recevoir des interruptions SNMP de CA Enterprise Log Manager, la configuration de la destination par défaut des interruptions SNMP et l'envoi d'alertes planifiées sous la forme d'interruptions SNMP vers des destinations spécifiées.
- Création d'une alerte d'action : cette section existante dans le chapitre Alertes d'action est mise à jour avec les nouvelles destinations de notification définies qui incluent des interruptions SNMP et CA IT PAM.
- Préparation à l'utilisation d'alertes avec des listes à clés : cette section existante dans le chapitre Alertes d'action est mise à jour avec des détails sur l'utilisation de nouvelles clés.
- Les alertes et rapports planifiés peuvent être activés, désactivés, modifiés ou supprimés comme indiqué par les nouvelles rubriques.
- Application de la suppression et de la récapitulation à des composants d'agents : cette nouvelle section dans le chapitre Suppression et récapitulation décrit l'utilisation de ce nouvel assistant.
- Création d'un filtre d'analyse : cette nouvelle section dans le chapitre Mappage et analyse décrit l'invocation du filtre d'analyse à partir de l'assistant d'analyse de message afin de définir comment le fichier XMP analyse des données d'événement.
- Création d'un fichier de mappage de données : cette section existante dans le chapitre Mappage et analyse a été mise à jour pour refléter l'assistant mis à jour.
- Tâches des règles de transfert d'événement : cette nouvelle section dans le chapitre Mappage et analyse décrit la gestion des règles de transfert d'événement.
- Création d'une intégration : cette section existante dans le chapitre Intégrations et connecteurs est mise à jour avec une explication sur la définition de nouvelles configurations.
- Configuration de sources de collecte : cette nouvelle section dans le chapitre Intégrations et connecteurs explique la configuration simultanée de plusieurs connecteurs et leur déploiement vers plusieurs agents.
- Affichage du tableau de bord des agents : cette nouvelle rubrique dans le chapitre Agents décrit la surveillance de l'état des agents.
- Accès à des événements collectés à l'aide d'ODBC/JDBC : cette nouvelle annexe décrit la création de rapports sur des données collectées par CA Enterprise Log Manager avec une application tierce de génération de rapports.
- Certificats personnalisés : désormais, ce chapitre contient une section supplémentaire, ainsi que d'autres mises à jour mineures.

Informations complémentaires :

Table des matières

Chapitre 1 : Introduction

Ce chapitre traite des sujets suivants :

A propos de ce manuel

Le présent *Manuel d'administration CA Enterprise Log Manager* s'intéresse aux tâches effectuées une fois l'installation de CA Enterprise Log Manager et la configuration initiale du serveur effectuées par l'administrateur. Certaines de ces tâches sont exécutées en réponse à des changements ponctuels sur le système ; d'autres sont des tâches de routine planifiées ; d'autres encore sont des tâches de surveillance réalisées de manière continue.

Ce manuel s'adresse à un public varié, notamment aux personnes ci-dessous.

- Les administrateurs, chargés de conserver la configuration du produit et de gérer le stockage des journaux et les mises à jour d'abonnement
- Les analystes, qui utilisent des rapports pour surveiller l'environnement, créer des rapports personnalisés et planifier la génération des alertes
- Les auditeurs, qui planifient des rapports, utilisent les requêtes et rapports pour vérifier la conformité aux normes et annotent des rapports.

Ce guide comprend un glossaire et un index. Le tableau ci-dessous résume son contenu.

Section	Description
Comptes d'utilisateur	Configurer les comptes d'utilisateur avec des rôles prédéfinis et auto-administrer les comptes d'utilisateur
Stratégies	Elaborer des rôles personnalisés et les stratégies associées en exploitant des stratégies et rôles prédéfinis
Stratégies et rôles personnalisés	Restreindre l'accès utilisateur à l'aide de rôles personnalisés, de stratégies personnalisées et de filtres d'accès
Services et adaptateurs CA	Configurer le magasin de journaux d'événements, le serveur de rapports, le module d'abonnement et certains adaptateurs d'événement
Stockage des journaux	Configurer l'archivage automatique et restaurer les bases de données archivées
Abonnement	Gérer la configuration d'abonnement, appliquer des mises à

Section	Description
	jour et restaurer une sauvegarde d'abonnement
Filtres et profils	Limiter les données affichées dans un rapport ou une requête, ou dans l'ensemble des rapports et requêtes à l'aide de filtres. Limiter la liste de balises, la liste de requêtes et la liste de rapports avec des profils.
Requêtes et rapports	Créer, modifier et importer ou exporter des requêtes et rapports pour afficher les journaux d'événements à jour et récents.
Alertes d'action	Créer une alerte d'action pour avertir les utilisateurs ou les destinations des interruptions SNMP ou encore pour exécuter un processus CA IT PAM lorsque des événements spécifiés se produisent.
Rapports planifiés	Planifier et conserver les jobs de rapports, afficher et annoter les rapports générés
Suppression et récapitulation	Créer et utiliser des règles de suppression et de récapitulation pour réduire la charge du serveur et empêcher la collecte ou le traitement d'événements indésirables
Mappage et analyse	Créer et utiliser des règles de mappage et d'analyse pour ajuster des événements bruts de divers formats en valeurs normalisées compatibles CEG, mais également pour créer des règles de transfert d'événement.
Intégrations et connecteurs	Créer des intégrations de produits qui, lorsqu'elles sont déployées en tant que connecteurs, vous permettent d'ajuster et de transmettre des événements, d'une seule source d'événement vers le serveur CA Enterprise Log Manager
Agents	Planifier l'usage des agents, préparer l'installation des agents, configurer les agents et les groupes d'agents, appliquer des mises à jour d'abonnement à des agents
Certificats personnalisés	Mettre en oeuvre des certificats personnalisés pour remplacer les certificats prédéfinis
Fonctions d'accessibilité	Utiliser les commandes d'accessibilité
Accès à des événements collectés à l'aide d'ODBC/JDBC	Configurer des rapports personnalisés avec un utilitaire de génération de rapport tiers ou extraire des informations de journaux sélectionnées avec des produits tiers

Remarque : Pour plus de détails sur la prise en charge des systèmes d'exploitation ou la configuration système requise, consultez les *Notes de parution*. Vous trouverez dans le *Manuel de présentation* un didacticiel vous expliquant comment faire fonctionner un système à un seul serveur pour pouvoir afficher les résultats des requêtes sur les événements Syslog et Windows collectés.Pour disposer de procédures pas à pas sur l'installation de CA Enterprise Log Manager et la configuration initiale, consultez le *Manuel d'implémentation* .Pour plus de détails sur l'installation des agents, consultez le *Manuel d'installation des agents*. Pour obtenir de l'aide quant à l'utilisation d'une page CA Enterprise Log Manager, consultez l'aide en ligne.

Chapitre 2 : Comptes d'utilisateur

Ce chapitre traite des sujets suivants :

Tâches d'auto-administration

Les utilisateurs avec un accès à CA Enterprise Log Manager peuvent modifier leurs propres mots de passe et déverrouiller un compte d'utilisateur verrouillé si le magasin d'utilisateurs configuré est celui par défaut, le magasin d'utilisateurs CA Enterprise Log Manager.

Lorsque l'administrateur crée un nouveau compte d'utilisateur, un nouveau mot de passe est affecté. Lors de la première connexion, l'utilisateur le remplace par un nouveau mot de passe conforme aux stratégies de mots de passe spécifiant si le mot de passe peut être identique au nom d'utilisateur, la longueur minimale et maximale, le nombre maximal de caractères répétés et le nombre minimal de caractères numériques. Il est de la responsabilité de l'utilisateur de modifier les mots de passe à la fréquence spécifiée par les stratégies fixant l'ancienneté minimale et maximale des mots de passe.

Chaque utilisateur administre son propre compte en effectuant les actions suivantes.

- Changer les mots de passe dans le respect des stratégies de mots de passe.
- Déverrouiller les comptes d'utilisateur qui ont été verrouillés, si cela est autorisé par la stratégie de mots de passe concernée

Déverrouillage d'un compte d'utilisateur

Vous pouvez déverrouiller un compte d'utilisateur verrouillé quel que soit votre rôle, si cela est permis par la stratégie de mots de passe. Lorsque votre compte se verrouille, un autre utilisateur doit le déverrouiller pour que vous ayez accès aux droits accordés à votre rôle.

Les verrouillages et déverrouillages sont contrôlés par les stratégies de mots de passe ci-dessous.

- Verrouiller le compte d'utilisateur après <n> échecs de connexion
- Permettre aux utilisateurs de déverrouiller les mots de passe

Les comptes d'utilisateurs peuvent se verrouiller si la stratégie de mots de passe est paramétrée pour verrouiller les comptes d'utilisateurs après un nombre défini d'échecs de connexion et au-delà d'un certain nombre de tentatives de connexion avec des informations d'identification incorrectes.

Tout utilisateur peut déverrouiller le compte d'un autre utilisateur si la stratégie de mots de passe permettant aux utilisateurs de déverrouiller les mots de passe est définie. Vous avez besoin du mot de passe de l'utilisateur pour déverrouiller ce compte d'utilisateur.

Pour déverrouiller un compte d'utilisateur

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Déverrouiller l'utilisateur dans le volet gauche.
3. Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur Déverrouiller.

   Le compte d'utilisateur est déverrouillé.

Modification de votre mot de passe

Vous pouvez modifier votre mot de passe, quel que soit votre rôle. Si la stratégie de mots de passe fixant l'ancienneté maximale des mots de passe est définie, vous devez changer votre mot de passe à la fréquence déterminée par cette stratégie.

Assurez-vous de changer votre mot de passe dès que possible dans les cas ci-dessous.

- Si vous communiquez votre mot de passe à autrui dans le but de déverrouiller votre compte
- Si vous oubliez votre mot de passe et que l'administrateur le réinitialise pour vous

Pour modifier votre mot de passe

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Changement de mot de passe dans le volet gauche.
3. Entrez votre ancien mot de passe.
4. Entrez votre nouveau mot de passe à deux reprises.
5. Cliquez sur OK.

Tâches associées aux rôles

Les administrateurs attribuent des rôles aux utilisateurs en fonction des tâches qu'ils doivent réaliser. Vous pouvez affecter aux utilisateurs les rôles prédéfinis Auditor, Analyst et Administrator, ou encore des rôles personnalisés, créés par vos soins. Pour évaluer l'impact de l'utilisation de rôles prédéfinis, examinez les tâches associées à chaque rôle.

Informations complémentaires :

Tâches du rôle Auditor (page 30)
Tâches du rôle Analyst (page 32)
Tâches du rôle Administrator (page 33)

Tâches du rôle Auditor

Les auditeurs internes peuvent réaliser les tâches ci-dessous.

- Rechercher et sélectionner une requête et en afficher les résultats
- Pour la ligne de résultats de requête sélectionnée, exécuter un processus de sortie de l'événement/de l'alerte configuré dans CA IT PAM
- Afficher les rapports en cours
- Planifier des rapports
- Afficher la liste des jobs de rapports planifiés
- Afficher la liste des rapports générés
- afficher et annoter les rapports générés.
- Définir des filtres et des profils

Vous pouvez affecter le rôle Auditor (peu de droits) lorsque vous créez des comptes d'utilisateur pour du personnel tiers. Par exemple, lorsqu'une alerte planifiée exécute un processus de sortie de l'événement/de l'alerte au niveau requête, l'alerte envoie une URL à CA Enterprise Log Manager, avec la description. Pour que les membres d'un personnel tiers puissent accéder à CA Enterprise Log Manager, ils doivent disposer de comptes d'utilisateur.

Remarque : Les analystes et les administrateurs peuvent effectuer toutes les tâches du rôle Auditor et les tâches propres à leur rôle.

Les auditeurs externes bénéficiant d'un accès temporaire à CA Enterprise Log Manager, pendant la période d'audit du site, peuvent contrôler la conformité des points suivants par rapport aux normes.

- Vérifier que les journaux sont collectés à partir des sources attendues.
- Vérifier que des procédures sont en place pour empêcher la perte de données ; par exemple, vérifier que les données sont sauvegardées suffisamment souvent pour éviter toute perte.
- Vérifier que les journaux sont examinés régulièrement pour détecter les brèches de sécurité.
- Vérifier que les journaux sont correctement stockés dans une archive sécurisée.
- Vérifier que l'ancienneté des données archivées est conforme aux normes de conservation des journaux.
- Vérifier que le contenu des journaux inclut le contenu à conserver impérativement.

Informations complémentaires :

Planification d'un job de rapport (page 508)
Affichage d'un rapport généré (page 505)
Annotation d'un rapport généré (page 507)
Affichage d'une requête (page 269)
Affichage d'un rapport (page 271)
Exemple : Exécution d'un processus de sortie de l'événement/de l'alerte avec les résultats de requête sélectionnés (page 416)
Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par requête (page 427)

Tâches du rôle Analyst

Les analystes système surveillent le réseau de collecte de journaux, puis collectent et distribuent les données des rapports.

Les administrateurs affectent le *rôle Analyst* aux utilisateurs responsables des tâches ci-après.

- Création et modification de requêtes et rapports personnalisés

  Un rapport est une représentation graphique ou tabulaire des données de journal d'événements qui est générée en exécutant des requêtes prédéfinies ou personnalisées à l'aide de filtres. Les données peuvent être issues de bases de données chaudes, tièdes et dégivrées dans le magasin de journaux d'événements du serveur sélectionné et, sur demande, de ses serveurs fédérés.

- Planifier des alertes d'action

  Une alerte d'action est un job de requête planifié qui peut être utilisé pour détecter les violations de stratégie, les tendances d'utilisation, les schémas de connexion et d'autres informations pouvant nécessiter une attention à court terme. Les données d'alerte peuvent être affichées dans l'interface utilisateur ou via un flux RSS. Vous pouvez envoyer une alerte planifiée à des destinataires de courriels, une destination d'interruption SNMP ou un processus de sortie de l'événement/de l'alerte CA IT PAM. Le processus est exécuté une fois par ligne ou une fois par requête.

- Création de balises

  Une *balise* est un terme ou une expression clé, qui permet d'identifier les requêtes ou rapports appartenant à la même catégorie. Pour ajouter un nouveau rapport à un job planifié et configuré pour sélectionner des rapports grâce à une balise spécifique, il vous suffit d'ajouter la balise commune au nouveau rapport. Une balise peut également être une expression clé associée à une requête, qui décrit ainsi le contenu de la requête et permet une classification et une recherche basées sur cette expression clé.

- Affichage de flux RSS (Rich Site Summary)

  Un *événement RSS* est un événement généré par CA Enterprise Log Manager pour transmettre une alerte d'action à des produits et utilisateurs tiers. L'événement est un récapitulatif de chaque résultat d'alerte d'action et un lien vers le fichier de résultat. La durée d'un flux RSS donné peut être configurée.

Les analystes peuvent procéder de la manière suivante pour se familiariser avec l'utilisation de CA Enterprise Log Manager.

1. Examiner les rapports prédéfinis disponibles (tâche également accessible aux auditeurs).
2. Planifier la génération régulière de rapports présentant un intérêt (tâche également accessible aux auditeurs).
3. Identifier les critères d'envoi d'une alerte, le format à utiliser et le destinataire. Ensuite, planifier l'alerte à générer lorsque ces critères sont remplis.
4. Eventuellement, concevoir des rapports personnalisés, créer des balises pour ces rapports, les planifier, les afficher et les annoter.
5. Vérifier les rapports générés et entrer des annotations de manière continue (tâche également accessible aux auditeurs).

Informations complémentaires :

Création d'un rapport (page 313)
Création d'une requête (page 295)
Tâches liées aux balises (page 269)

Tâches du rôle Administrator

Les utilisateurs détenant le rôle Administrator ont un accès illimité aux fonctionnalités disponibles dans tous les onglets de CA Enterprise Log Manager. Seuls les utilisateurs ayant le rôle Administrator disposent d'un plein accès à l'onglet Administration. Dans cet onglet, les administrateurs peuvent configurer et gérer tous les aspects de la collecte de journaux, de tous les services et de tous les accès utilisateur.

Informations complémentaires :

Personnalisation et configuration de la collecte de journaux (page 34)
Surveillance et configuration des services (page 36)
Gestion des utilisateurs et des accès (page 39)

Personnalisation et configuration de la collecte de journaux

Seuls les utilisateurs ayant le rôle Administrator peuvent configurer et gérer les fonctions relatives à la collecte de journaux. Pour ce faire, les administrateurs utilisent le sous-onglet Collecte de journaux de l'onglet Administration.

Ils utilisent l'explorateur de collecte de journaux pour configurer les connecteurs sur les agents, une tâche nécessaire pour la collecte de journaux. Ils appliquent également les mises à jour d'abonnement aux agents, le cas échéant.

L'utilisation de la bibliothèque d'ajustement d'événement est facultative. La fonctionnalité prête à l'emploi, qui est régulièrement mise à jour, a été conçue pour répondre aux besoins de la majorité des clients.

Les tâches d'administrateur impliquant la collecte des journaux incluent les tâches suivantes.

- Configurer et gérer les agents installés à partir d'un serveur CA Enterprise Log Manager dédié à la collecte.
- Interroger le catalogue d'archive sur un serveur de rapports CA Enterprise Log Manager.

  Le *catalogue d'archive* est l'enregistrement de toutes les bases de données qui ont déjà figuré sur le serveur CA Enterprise Log Manager. Cela inclut les bases de données récemment créées, celles qui ont été sauvegardées et déplacées, et celles qui ont été supprimées avant d'être sauvegardées, le cas échéant.
- Configurer les adaptateurs CA utilisés par CA Audit.
- Gérer la bibliothèque d'ajustement d'événement.
  - Travailler sur des intégrations prédéfinies et en créer de nouvelles, sans modèle ou sur la base d'une intégration prédéfinie.

    L'intégration est une méthode permettant de traiter les événements non classés en événements ajustés, pour pouvoir les afficher dans les requêtes et les rapports.
  - Créer un écouteur Syslog à partir de l'écouteur prédéfini.
  - Créer de nouveaux fichiers d'analyse, sans modèle ou sur la base d'un fichier prédéfini.

    Le fichier d'analyse de message (XMP), qui est associé à un type de source d'événement spécifique, applique les règles d'analyse qui permettent de décomposer l'événement brut en paires nom/valeur.

- Créer de nouveaux fichiers de mappage, sans modèle ou sur la base d'un fichier prédéfini.

  Les fichiers de mappage des données sont des fichiers XML utilisant la grammaire commune aux événements (CEG) de CA pour transformer des événements d'un format source en un format pouvant être stocké à des fins de rapport et d'analyse dans le magasin de journaux d'événements.

- Créer des règles de récapitulation, sans modèle ou sur la base d'une règle prédéfinie.

  Les règles de récapitulation sont des règles combinant certains événements natifs, d'un même type, en un seul événement ajusté.

- Créer des règles de suppression, sans modèle ou sur la base d'une règle prédéfinie.

  Les règles de suppression empêchent certains événements ajustés d'apparaître dans vos rapports.

- Créer des règles de transfert d'événement.

  Les règles de transfert d'événement stipulent que les événements sélectionnés sont transférés à des produits tiers, par exemple ceux qui mettent les événements en corrélation, après leur sauvegarde dans le magasin des journaux d'événements.

- Créer des profils.

  Un profil spécifie l'ensemble de balises et de filtres de données disponibles à la sélection. Les filtres de données restreignent les données affichées dans une requête ou un rapport ; les filtres de balise restreignent les balises affichées dans la liste des balises de requêtes et dans la liste de balises de rapports.

Informations complémentaires :

Création d'un groupe d'agents (page 665)
Configuration de la gestion des agents (page 668)
Application des mises à jour d'abonnement (page 675)

Surveillance et configuration des services

Seuls les utilisateurs ayant le rôle Administrator peuvent configurer et gérer les services accessibles dans le sous-onglet Services de l'onglet Administration. Configurez l'ensemble des services rapidement après l'installation de CA Enterprise Log Manager.

Les tâches d'administrateur impliquant des services incluent les tâches suivantes.

- Configurer les services globaux, notamment :
  - Intervalle de mise à jour
  - Délai d'expiration de la session
  - Authentification, requise ou non, pour l'affichage des alertes publiées dans les flux RSS
  - Balises à masquer
  - Profil par défaut
- Configurer le service de magasin de journaux d'événements.
  - Au niveau global, configurer les services s'appliquant à tous les serveurs CA Enterprise Log Manager.
  - Au niveau local, configurer l'archivage automatique.

    Le magasin de journaux d'événements sur le serveur CA Enterprise Log Manager de collecte héberge une base de données chaude des nouveaux journaux. Cette base de données est compressée lorsque le nombre maximum de lignes configuré est atteint.
    - Si l'archivage automatique est configuré entre le serveur de collecte et le serveur de rapports, la base de données tiède est copiée sur le serveur de rapports, puis supprimée du serveur de collecte.
    - Si l'archivage automatique est configuré entre le serveur de rapports et un serveur distant qui n'est pas un serveur CA Enterprise Log Manager, les bases de données tièdes sont copiées sur le serveur distant et supprimées du serveur de rapports chaque jour.
    - Si l'archivage automatique n'est pas configuré du serveur de rapports vers un serveur de stockage distant, créez manuellement une sauvegarde des bases de données tièdes et transférez-les sur le stockage à long terme. La base de données tiède est stockée dans le magasin de journaux d'événements d'un serveur de rapports (ou serveur de gestion/rapports dans un déploiement à deux serveurs) pendant le nombre de jours configuré en tant que Nbre max. de jours d'archivage, sauf si l'espace disponible descend en dessous du pourcentage défini par l'espace disque d'archivage. Dans ce cas, les bases de données tièdes sont supprimées, en commençant par la plus ancienne.

- Configurer le service Serveur de rapports.

  Le service Serveur de rapports gère les rapports et les alertes, y compris les stratégies de conservation, le format des rapports imprimés/envoyés par courriel et les valeurs à clés pour les rapports et les alertes. Il gère également les paramètres d'intégration des processus CA IT PAM, telles que les valeurs dynamiques et de sortie de l'événement/de l'alerte, et des destinations d'interruptions SNMP pour les alertes.

- Configurer les mises à jour d'abonnement.

  Les mises à jour d'abonnement font référence aux fichiers binaires et non binaires mis à disposition par le serveur d'abonnement CA pour les serveurs CA Enterprise Log Manager, le composant CA EEM du serveur de gestion et les agents.

- Gérer la fédération de serveurs CA Enterprise Log Manager.

  Au niveau du serveur de gestion, vous pouvez définir une requête d'extension aux enfants et pairs de la fédération. Les serveurs CA Enterprise Log Manager peuvent être fédérés aux deux fins ci-après.

  - Le serveur de collecte archive automatiquement chaque base de données chaude dans une base de données tiède, qu'il envoie au serveur de rapports lié. Créer une fédération entre le serveur de collecte et le serveur de rapports. Lorsque vous effectuez une requête sur le serveur de gestion avec la fédération sélectionnée, vous pouvez obtenir des résultats non seulement des bases de données tièdes locales, mais également de la base de données chaude du serveur de collecte.
  - Plusieurs serveurs de rapports peuvent être créés pour répartir le stockage des bases de données tièdes entre plusieurs magasins de journaux d'événements. Les serveurs de rapports peuvent être fédérés dans un maillage où chaque serveur de collecte fédéré est un enfant de son serveur de rapports. Toute requête fédérée issue de l'un des serveurs de rapports maillés renvoie des données de ses serveurs maillés (pairs) et de tous leurs serveurs enfants.

    Remarque : Si vous définissez CA Enterprise Log Manager de point de restauration dans le but de restaurer des bases de données archivées à partir d'un stockage à long terme, prévoyez de laisser ce serveur en dehors de la fédération.

- Surveiller et gérer l'état du système.

Informations complémentaires :

Modification de configurations globales (page 143)
Remarques sur le magasin de journaux d'événements (page 147)
Sauvegarde et restauration automatiques (page 180)
Configuration de l'authentification non interactive pour la restauration (page 181)
Requête dans le catalogue d'archive (page 183)
Restauration des fichiers archivés automatiquement (page 185)
Restauration : Script de restauration des bases de données archivées (page 186)
Remarques sur le serveur ODBC (page 151)
Remarques sur le serveur de rapports (page 152)
Modification de la configuration d'abonnement globale (page 207)
Modification de la configuration d'un proxy en ligne (page 208)
Modification de la configuration d'un proxy hors ligne (page 209)
Lancement d'une mise à jour à la demande (page 243)
Créez un fichier de diagnostic pour le support technique. (page 166)
Redémarrage d'un serveur hôte (page 167)
Redémarrage du service iGateway (page 167)
Vérification de l'état et de la version des services (page 168)
Vérification des événements d'autosurveillance de l'état d'un système (page 168)

Gestion des utilisateurs et des accès

Seuls les utilisateurs ayant le rôle Administrator peuvent configurer et gérer les comptes d'utilisateur, les stratégies et les autres objets d'application accessibles depuis le sous-onglet Gestion des utilisateurs et des accès de l'onglet Administration. Pour se connecter à CA Enterprise Log Manager, l'utilisateur doit disposer d'un compte d'utilisateur configuré avec un rôle et des informations d'identité dont il se sert pour ouvrir une session. Les stratégies et les rôles prédéfinis permettent aux administrateurs de configurer l'accès utilisateur en définissant des comptes d'utilisateur. Il n'est pas toujours nécessaire de créer des rôles et des stratégies personnalisés.

Les tâches d'administrateur impliquant les utilisateurs et les accès incluent les tâches suivantes.

- Définir de nouveaux utilisateurs globaux (si le magasin d'utilisateurs est le magasin d'utilisateurs CA Enterprise Log Manager par défaut).

  Lorsque vous ajoutez un nouvel utilisateur, vous créez un utilisateur global. Les détails tels que le nom, le lieu et le numéro de téléphone sont considérés comme des éléments globaux car ils peuvent être partagés. Un *utilisateur global* se compose des informations de compte d'utilisateur, à l'exclusion des données propres aux applications.

- Récupérer les utilisateurs référencés (s'il s'agit d'un magasin d'utilisateurs référencé).

  Les détails des utilisateurs globaux sont stockés dans le magasin d'utilisateurs configuré, qui peut être un répertoire externe.

- Affecter des groupes d'applications (rôles) prédéfinis ou personnalisés aux utilisateurs, nouveaux ou référencés.

  Les détails des applications sont toujours stockés dans le référentiel du serveur de gestion. Il s'agit des informations chargées au format lecture seule lorsque vous configurez un magasin d'utilisateurs externe.

- Modifier, supprimer et afficher des comptes d'utilisateur.

- Créer des groupes d'applications (rôles) personnalisés et les stratégies associées.

  La création de rôles d'utilisateurs commence par la définition d'un nouveau groupe d'utilisateurs d'applications, puis se poursuit par la création d'une stratégie définissant les actions autorisées sur les ressources spécifiées. Un rôle d'utilisateur peut être un groupe d'utilisateurs d'applications prédéfini ou un groupe d'applications défini par l'utilisateur. Des rôles d'utilisateur personnalisés sont nécessaires lorsque les groupes d'applications prédéfinis (Administrator, Analyst et Auditor) ne sont pas suffisamment affinés pour refléter les attributions de tâches. Les rôles d'utilisateur personnalisés nécessitent des stratégies d'accès personnalisées et une modification des stratégies prédéfinies pour inclure le nouveau rôle.

- Modifier, supprimer et afficher les groupes d'applications et les stratégies associées.
- Modifier la stratégie d'accès aux applications CALM.

  La stratégie d'accès aux applications CALM est une stratégie de portée de type Liste de contrôle d'accès, qui détermine qui peut accéder au serveur CA Enterprise Log Manager. Par défaut, l'accès est accordé aux rôles Administrator [Groupe], Analyst [Groupe] et Auditor [Groupe].
- Créer, modifier, supprimer et afficher les stratégies d'accès.

  Une stratégie d'accès est une règle qui accorde ou refuse à une identité (utilisateur ou groupe d'utilisateurs) des droits d'accès à une ressource d'application.
- Configurer, modifier, supprimer et afficher les filtres d'accès.

  Un filtre d'accès est un filtre que l'administrateur peut définir pour contrôler les données d'événement pouvant être consultées par les utilisateurs ou groupes ne détenant pas le rôle Administrator. Un filtre d'accès peut, par exemple, limiter les données que des identités spécifiées peuvent afficher dans un rapport. Les filtres d'accès sont automatiquement convertis en stratégies d'obligation.

Informations complémentaires :

Création d'un groupe global (page 42)
Création d'un utilisateur global (page 43)
Affectation d'un rôle à un utilisateur global (page 44)
Sauvegarde de toutes les stratégies d'accès (page 65)
Restauration des stratégies d'accès (page 69)
Configuration de rôles d'utilisateur et de stratégies d'accès personnalisés (page 88)
Ajout d'une identité à une stratégie existante (page 93)
Création d'une stratégie d'accès CALM (page 94)
Création d'une stratégie de groupe d'utilisateurs dynamique (page 103)
Création d'une stratégie basée sur une stratégie existante (page 101)
Création d'une stratégie de portée (page 97)
Création d'un filtre d'accès (page 105)
Création d'un groupe d'utilisateurs d'applications (rôle) (page 91)
Attribution d'un accès de rôle personnalisé à CA Enterprise Log Manager (page 92)
Test d'une nouvelle stratégie (page 102)
Création d'un calendrier (page 106)

Configuration des comptes avec des paramètres prêts à l'emploi

Lorsque vous élaborez un environnement de test temporaire, vous pouvez configurer la gestion des utilisateurs et des accès très rapidement en utilisant des paramètres prêts à l'emploi pour les comptes d'utilisateur et en remplissant uniquement les champs requis. Pour réaliser une configuration minimale à l'aide des paramètres prédéfinis, créez des comptes d'utilisateur pour les utilisateurs de CA Enterprise Log Manager comme suit.

- Si vous utilisez le magasin d'utilisateurs par défaut, créez un compte avec un nom d'utilisateur, puis affectez un groupe d'applications prédéfini (Administrator, Analyst, Auditor) ainsi qu'un mot de passe temporaire.
- Si vous faites référence à un magasin d'utilisateurs externe, recherchez l'utilisateur global par son nom, puis affectez un rôle prédéfini (Administrator, Analyst, Auditor) ainsi qu'un mot de passe temporaire.

Informations complémentaires :

Création d'un utilisateur global (page 43)
Affectation d'un rôle à un utilisateur global (page 44)
Gestion des comptes d'utilisateur référencés (page 46)

Création d'un groupe global

La capacité à créer un groupe dépend de la configuration du magasin d'utilisateurs. Tenez compte des éléments suivants.

- Si vous utilisez le magasin d'utilisateurs par défaut, la création de groupes globaux est une tâche facultative.
- Si vous utilisez comme référence un magasin d'utilisateurs externe, les groupes globaux et les comptes d'utilisateur sont automatiquement chargés dans le magasin d'utilisateurs par défaut. Vous pouvez, de manière facultative, créer des stratégies personnalisées pour ces groupes globaux, mais vous ne pouvez pas créer de nouveaux groupes.
- Si le magasin d'utilisateurs référencé est CA SiteMinder, vous pouvez utiliser tels quels les groupes globaux définis dans ce produit CA ou bien en créer de nouveaux à partir d'appartenances de groupe.

Pour créer un groupe global

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Groupes dans le volet gauche.

   Les volets Groupes de recherche et Groupes d'utilisateurs s'affichent.
3. Cliquez sur le bouton Nouveau groupe global, à côté du dossier Groupes globaux.

   Le volet Nouveau groupe global d'utilisateurs apparaît.
4. Saisissez un nom et, si vous le souhaitez, une description.
5. Si le groupe global doit contenir d'autres groupes globaux, procédez comme suit.
   a. Entrez des critères pour rechercher un groupe, puis cliquez sur Rechercher.
   b. Déplacez le groupe que vous souhaitez inclure dans la liste Groupes globaux d'utilisateurs sélectionnés.
   c. Répétez l'opération jusqu'à ce que la liste contienne tous les groupes souhaités.
6. Cliquez sur Enregistrer.

   Une boîte de dialogue de confirmation apparaît.

Informations complémentaires :

Planification des rôles d'utilisateur (page 87)

Création d'un utilisateur global

Vous pouvez créer de nouveaux utilisateurs uniquement si le magasin d'utilisateurs est configuré en tant que magasin d'utilisateurs CA Enterprise Log Manager, le magasin par défaut. Seuls les administrateurs peuvent créer de nouveaux comptes d'utilisateurs.

Si vous faites référence à un magasin d'utilisateurs externe, les comptes d'utilisateurs sont automatiquement chargés dans le magasin d'utilisateurs par défaut en tant qu'enregistrements en lecture seule. Si vous avez besoin de créer un nouvel utilisateur, vous devez le faire dans le magasin d'utilisateurs externe. Le nouvel enregistrement est automatiquement chargé.

Pour utiliser le produit CA Enterprise Log Manager, un utilisateur doit posséder un compte d'utilisateur global. Le compte doit être actif au moment de la connexion. Les comptes peuvent devenir inactifs s'ils sont suspendus par l'administrateur, verrouillés en raison d'une violation d'une stratégie de mots de passe ou désactivés suite à l'expiration de leur durée d'activation.

Pour créer un nouveau compte d'utilisateur global

1. Cliquez sur l'onglet Administration et sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur le bouton Utilisateurs.
3. Vérifiez que le compte que vous souhaitez créer n'existe pas déjà. Sélectionnez Utilisateurs globaux et cliquez sur OK. Si le nom n'apparaît pas dans les résultats, continuez.
4. Cliquez sur le bouton Nouvel utilisateur à gauche de l'arborescence Utilisateurs.

   La page Nouvel utilisateur s'affiche.
5. Entrez le nom de l'utilisateur dans le champ de saisie Nom.
6. Affectez un groupe d'utilisateurs d'applications (facultatif).
   a. Cliquez sur Ajouter les détails de l'utilisateur de l'application.
   b. Sélectionnez un ou plusieurs groupes d'utilisateurs disponibles et cliquez sur le bouton Déplacer pour déplacer la sélection dans la zone Groupes d'utilisateurs sélectionnés.

      Remarque : Si vous n'effectuez pas cette action maintenant, vous pouvez modifier le compte d'un utilisateur global ultérieurement et lui affecter un groupe d'utilisateurs d'applications.
7. Entrez les informations générales dans les détails de l'utilisateur global.
8. Affectez un groupe d'utilisateurs globaux (facultatif).

9. Remplissez les informations d'authentification.
    a. Entrez un chiffre dans Nombre de connexions incorrectes pour fixer un seuil concernant le nombre de connexions incorrectes autorisées avant le verrouillage du compte. Aucune limite n'est imposée avec la valeur 0.
    b. Laissez désélectionnée la case Ignorer la stratégie de mots de passe sauf si vous souhaitez autoriser l'utilisateur à définir des mots de passe non conformes à la stratégie de mots de passe.
    c. Répétez votre saisie dans la zone Confirmer le mot de passe.
    d. Sélectionnez Changer le mot de passe à la connexion suivante pour permettre à l'utilisateur de changer de mot de passe.
    e. Laissez l'option Suspendu vide lors de la création d'un compte.
    f. Entrez un mot de passe pour Nouveau mot de passe et Confirmer le mot de passe.
    g. Si cet utilisateur ne doit détenir qu'un accès temporaire, entrez une plage de dates pour l'activation et la désactivation du compte d'utilisateur.
    h. Pour reporter l'activation du compte d'utilisateur à une date ultérieure, entrez la date d'activation du compte.
10. Cliquez sur Enregistrer.
11. Cliquez sur Fermer.

Affectation d'un rôle à un utilisateur global

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

Seuls les administrateurs peuvent modifier des comptes d'utilisateurs.

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

1. Cliquez sur l'onglet Administration et sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Utilisateurs dans le volet gauche.

   Les volets Recherche d'utilisateurs et Utilisateurs apparaissent.
3. Sélectionnez Utilisateurs globaux, entrez des critères de recherche et cliquez sur OK.

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

   Important : Entrez toujours des critères lors des recherches pour éviter d'afficher toutes les entrées d'un magasin d'utilisateurs externe.
4. Sélectionnez un utilisateur global n'ayant aucune appartenance à un groupe d'applications CA Enterprise Log Manager.

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

   Le volet des détails de l'utilisateur "CAELM" se développe.
6. Sélectionnez le groupe souhaité dans la liste des groupes d'utilisateurs disponibles et cliquez sur la flèche de droite.

   Le groupe sélectionné apparaît dans la zone Groupes d'utilisateurs sélectionnés.
7. Cliquez sur Enregistrer.
8. Vérifiez l'ajout.
   a. Dans le volet Recherche d'utilisateurs, cliquez sur Détails de l'utilisateur de l'application, puis sur OK.
   b. Vérifiez que le nom du nouvel utilisateur de l'application apparaît bien dans les résultats affichés.
9. Cliquez sur Fermer.

Gestion des comptes d'utilisateur référencés

Vous pouvez utiliser les informations du compte d'utilisateur global lorsque vous référencez un magasin d'utilisateurs externe. Bien que vous ne puissiez pas mettre à jour l'enregistrement utilisateur du magasin externe à partir du système CA Enterprise Log Manager, vous pouvez attribuer des détails de niveau application.

Les approches suivantes sont recommandées dans la gestion de l'accès des utilisateurs disposant d'un compte stocké dans un magasin d'utilisateurs externe.

- Ajoutez au compte d'utilisateur un groupe d'utilisateurs, ou rôle, prédéfini.
- Ajoutez le groupe global aux stratégies prédéfinies, afin de fournir l'accès de votre choix à l'utilisateur.
- Créez des rôles personnalisés et les stratégies associées, puis ajoutez ces rôles au compte d'utilisateur.

Consignes d'activation d'un utilisateur

Observez les consignes suivantes lors de l'utilisation des fonctions d'activation d'un compte.

- Lorsque vous créez simultanément plusieurs comptes d'utilisateur, servez-vous du paramètre Date d'activation pour spécifier la date future à laquelle les comptes seront activés (tous les comptes ou une partie seulement). Cela vous permet de coordonner l'octroi des droits d'accès avec une éventuelle formation dispensée aux nouveaux utilisateurs.
- Lorsque vous créez des comptes temporaires pour des auditeurs externes, utilisez les paramètres Date d'activation et Date de désactivation pour définir l'intervalle de temps souhaité.
- En cas de comportement suspect de la part d'un utilisateur, vous pouvez immédiatement suspendre le compte et empêcher ainsi l'utilisateur de se connecter à un serveur CA Enterprise Log Manager.
- Lorsqu'un utilisateur quitte la société, vous pouvez supprimer l'ensemble de son dossier, suspendre son compte ou saisir une date d'expiration pour le placer en statut désactivé.

Informations complémentaires :

Création d'un utilisateur global (page 43)
Modification d'un compte d'utilisateur (page 47)
Suppression d'un compte d'utilisateur (page 50)

Modification d'un compte d'utilisateur

Seuls les administrateurs peuvent créer et modifier des comptes d'utilisateurs. Vous pouvez rechercher un utilisateur et afficher les informations du compte d'utilisateur sélectionné pour les raisons ci-dessous.

- Pour attribuer à un utilisateur global un rôle CA Enterprise Log Manager, c'est-à-dire une appartenance à un groupe d'applications, lorsque les informations de compte ont été chargées à partir d'un magasin d'utilisateurs référencé
- Pour mettre à jour les détails d'un utilisateur global pour un compte du magasin d'utilisateurs local
- Pour suspendre le compte d'utilisateur
- Pour réinitialiser le mot de passe d'un compte d'utilisateur suite à un oubli ou parce que le compte a été verrouillé et que la stratégie de mots de passe n'autorise pas les utilisateurs à déverrouiller des comptes d'utilisateurs
- Pour désactiver un compte d'utilisateur ou réinitialiser la durée d'activation du compte

Important : N'effectuez aucune saisie dans le champ Nombre de connexions incorrectes de la zone Authentification. La valeur affichée dans ce champ est mise à jour par le système.

Pour modifier un compte d'utilisateur

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Utilisateurs dans le volet gauche.

   Le volet Recherche d'utilisateurs s'affiche.
3. Spécifiez les critères de recherche dans le volet Recherche d'utilisateurs de l'une des manières suivantes.
   - Pour ajouter des détails d'application pour un utilisateur global, sélectionnez Utilisateurs globaux, entrez les critères de recherche et cliquez sur OK.
   - Pour modifier le compte d'un utilisateur avec un rôle CA Enterprise Log Manager existant, sélectionnez Détails de l'utilisateur de l'application, entrez les critères de recherche et cliquez sur OK.

Remarque : Pour les critères de recherche, utilisez l'opérateur LIKE lorsque vous spécifiez un caractère générique en tant que valeur et utilisez l'opérateur EQUAL lorsque vous spécifiez la chaîne complète. Vous trouverez plusieurs exemples ci-dessous.

- Group Membership LIKE Aud*
- Group Membership EQUALS Auditor

Les noms des utilisateurs correspondant aux critères de recherche apparaissent dans le volet Utilisateurs.

4. Cliquez sur le nom d'utilisateur du compte à modifier.

   Le compte sélectionné s'affiche dans le volet droit.

5. Pour ajouter un rôle, cliquez sur Ajouter les détails de l'utilisateur de l'application, sélectionnez le rôle approprié dans la liste des groupes d'utilisateurs disponibles et déplacez-le dans la liste des groupes d'utilisateurs sélectionnés.

6. Pour mettre à jour les détails de l'utilisateur global, remplacez les détails existants par les nouveaux détails dans la section des détails de l'utilisateur global.

   Remarque : Vous pouvez mettre à jour les détails uniquement si vous utilisez le magasin d'utilisateurs par défaut.

7. Pour mettre à jour la configuration d'authentification, procédez de l'une des manières ci-dessous.

   - Sélectionnez Ignorer la stratégie de mots de passe pour exclure cet utilisateur des contrôles effectués par toutes les stratégies de mots de passe.
   - Sélectionnez Suspendu pour empêcher cet utilisateur de se connecter à un serveur CA Enterprise Log Manager.
   - Désélectionnez Suspendu pour activer ce compte de telle sorte que l'utilisateur puisse se connecter.
   - Si votre stratégie de mots de passe n'autorise pas les utilisateurs à déverrouiller les mots de passe et que cet utilisateur dispose d'un mot de passe verrouillé, sélectionnez Réinitialiser le mot de passe, saisissez deux fois le nouveau mot de passe, puis sélectionnez Changer le mot de passe à la connexion suivante.

     Remarque : La valeur du champ Nombre de connexions incorrectes augmente automatiquement à chaque échec de tentative de connexion ; le champ est remis à zéro à chaque tentative de connexion réussie. Un compte d'utilisateur se verrouille lorsque la valeur du compteur atteint ou dépasse la valeur définie dans la stratégie de mots de passe (nombre d'échecs de connexion avant verrouillage du compte).

- Pour choisir la période d'activation du compte, cliquez sur Date d'activation pour définir la date de début et sur Date de désactivation pour définir la date de fin. Les utilisateurs ont accès au compte depuis le début de journée de la date d'activation jusqu'à la fin de journée de la date de désactivation. Pour autoriser l'accès au compte sur une journée uniquement, spécifiez la même date comme date d'activation et de désactivation.

8. Cliquez sur Enregistrer.

   Les mises à jour apportées au compte d'utilisateur sont enregistrées et appliquées.

Réinitialisation du mot de passe d'un utilisateur

Vous pouvez réinitialiser le mot de passe d'un utilisateur en cas d'oubli. Si un utilisateur ayant oublié son mot de passe voit son compte verrouillé suite au dépassement du nombre autorisé de tentatives de connexion, vous pouvez réinitialiser le mot de passe. L'utilisateur peut ensuite déverrouiller le compte, si la stratégie de mots de passe correspondante le lui permet.

Pour réinitialiser le mot de passe d'un utilisateur

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur le bouton Utilisateurs.
3. Recherchez le compte d'utilisateur à modifier.
   a. Sélectionnez Détails de l'utilisateur de l'application.
   b. Saisissez le nom d'utilisateur dans le champ Valeur, Attribut étant défini sur Nom d'utilisateur et Opérateur sur LIKE.
   c. Cliquez sur OK.
4. Cliquez sur le nom d'utilisateur dans l'arborescence Utilisateurs.

   Les détails du compte d'utilisateur sélectionné s'affichent.
5. Dans le volet Authentification, sélectionnez Réinitialiser le mot de passe.

   Les champs Nouveau mot de passe et Confirmer le mot de passe s'affichent.
6. Entrez le nouveau mot de passe dans les champs Nouveau mot de passe et Confirmer le mot de passe.
7. Cliquez sur Enregistrer, puis sur Fermer.

Suppression d'un compte d'utilisateur

Vous pouvez supprimer tout compte d'utilisateur global créé dans CA Enterprise Log Manager.

Vous pouvez désactiver un compte d'utilisateur sans le supprimer de l'une des manières ci-dessous.

- Vous pouvez définir une date à partir de laquelle désactiver un compte.
- Vous pouvez suspendre un compte de telle sorte que l'utilisateur associé ne puisse pas accéder à l'interface CA Enterprise Log Manager.

Pour supprimer un utilisateur global

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

   Les volets Recherche d'utilisateurs et Utilisateurs apparaissent.

2. Sélectionnez soit Utilisateurs globaux, soit Détails de l'utilisateur de l'application, spécifiez les critères de recherche et cliquez sur OK.

3. Sélectionnez l'utilisateur à supprimer de la liste des utilisateurs existants.

   L'enregistrement pour l'utilisateur sélectionné apparaît dans le volet droit.

4. Cliquez sur Supprimer.

   Un message vous demandant de confirmer la suppression de l'utilisateur s'affiche.

5. Cliquez sur OK.

   Le message de confirmation de suppression réussie de l'utilisateur global s'affiche.

   Remarque : Si vous cliquez une nouvelle fois sur OK dans le volet Recherche d'utilisateurs, la liste affichée ne contient pas le nom de l'utilisateur supprimé.

Chapitre 3 : Stratégies

La création de rôles personnalisés exige de modifier les stratégies prédéfinies pour créer des stratégies personnalisées. Avant de commencer ces tâches, il peut être utile d'étudier les stratégies prédéfinies associées à chaque rôle prédéfini. Il est également recommandé de sauvegarder les stratégies d'accès prédéfinies avant de commencer la modification.

Ce chapitre traite des sujets suivants :

Introduction aux stratégies

Une *stratégie d'accès* est une règle qui accorde ou refuse à une identité (utilisateur ou groupe d'utilisateurs) des droits d'accès à une ressource d'application ou à une ressource globale. CA Enterprise Log Manager détermine si les stratégies s'appliquent à l'utilisateur concerné en faisant correspondre les identités, les ressources, les classes de ressources et en évaluant les filtres. En d'autres termes, une stratégie autorise ou non des actions pour des identités spécifiques sur des ressources spécifiques. Les stratégies qui refusent l'accès à une ressource donnée ont priorité sur les stratégies qui accordent l'accès à cette même ressource.

CA Enterprise Log Manager prend en charge les types suivants de stratégies d'accès.

- Stratégies d'accès CALM
- Stratégies de délégation
- Stratégies de groupe d'utilisateurs dynamique (une approche alternative aux groupes d'applications personnalisés)
- Stratégies d'obligation (créées automatiquement lorsque vous créez un filtre d'accès)
- Stratégies de portée

CA Enterprise Log Manager est installé avec des stratégies d'accès CALM prédéfinies et des stratégies de portée pour trois groupes d'utilisateurs d'applications CA Enterprise Log Manager : Administrator, Analyst et Auditor. Ces stratégies sont suffisantes si vous envisagez d'affecter uniquement les groupes d'utilisateurs d'applications prêts à l'emploi aux utilisateurs endossant les différents rôles.

Important : Nous recommandons d'effectuer une sauvegarde des stratégies prédéfinies qui sont fournies avec CA Enterprise Log Manager. Si une stratégie d'accès CALM est supprimée accidentellement, les utilisateurs ne sont plus en mesure d'accéder à CA Enterprise Log Manager tant que cette stratégie n'est pas restaurée à partir d'une sauvegarde.

Stratégies d'accès prédéfinies

Si vous utilisez les fonctions prêtes à l'emploi en affectant un groupe d'applications prédéfini (Administrator, Analyst ou Auditor) comme rôle pour chaque utilisateur, vous n'avez pas besoin de créer de stratégie d'accès. Toutes les stratégies requises sont prédéfinies et prêtes à l'emploi.

Informations complémentaires :

Examen des stratégies pour tous les utilisateurs (page 53)
Examen des stratégies pour les auditeurs (page 57)
Examen des stratégies pour les analystes (page 59)
Examen des stratégies pour les administrateurs (page 62)
Ressources et actions (page 80)

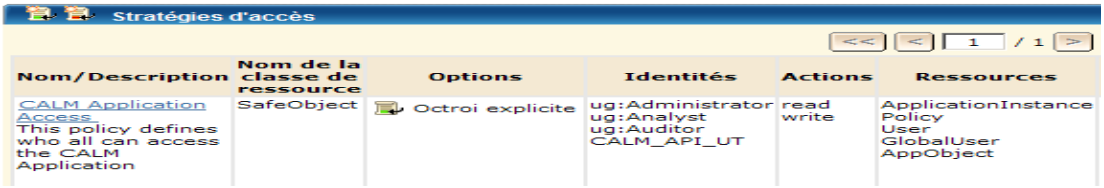
Examen des stratégies pour tous les utilisateurs

Vous pouvez examiner les stratégies pour tous les utilisateurs. Modifiez la stratégie d'accès aux applications CALM pour définir des rôles personnalisés. Tous les rôles personnalisés doivent être ajoutés en tant qu'identités à cette stratégie.

Pour examiner les stratégies pour tous les utilisateurs

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès dans le volet gauche.
3. Affichez la stratégie d'accès aux applications CALM en procédant comme suit.
   a. Sélectionnez Afficher les stratégies correspondant au nom.
   b. Entrez CALM*.
   c. Cliquez sur OK.
4. Examinez la stratégie d'accès aux applications CALM.

   Cette stratégie octroie un accès en lecture et en écriture aux ressources répertoriées pour tous les membres des groupes d'utilisateurs d'applications par défaut (Administrator, Analyst et Auditor) ainsi qu'à d'autres utilisant l'API CA Enterprise Log Manager.



Voici les ressources répertoriées.

- La ressource ApplicationInstance est CAELM, qui se réfère au produit CA Enterprise Log Manager.
- Le terme stratégie se réfère aux stratégies d'accès.
- Le terme utilisateur se réfère à tout utilisateur ajouté à un groupe d'utilisateurs d'applications CA Enterprise Log Manager.
- Le terme GlobalUser indique tout utilisateur défini dans le magasin d'utilisateurs au sein de CA Enterprise Log Manager ou référencé à partir de CA Enterprise Log Manager.
- AppObject, dont la valeur est pozFolder pour le dossier Profils, se réfère aux profils.
- AppObject, dont la valeur est pozFolder pour le dossier flex, désigne les données XML de plage de temps dynamique utilisées pour remplir la liste déroulante des plages de temps à l'étape Conditions de résultat des assistants basés sur la requête.

Le filtre d'accès aux applications CALM indique les limites d'action de chaque ressource.

Filtres				
WHERE	(req:resource	==	val:ApplicationInstance	
ET	req:action	{}	val:read	)
OU	(req:resource	==	val:Policy	
ET	req:action	{}	val:read	)
OU	(req:resource	==	val:User	
ET	req:action	{}	val:read,write	
ET	name:cn	==	req:identity	)
OU	(req:resource	==	val:GlobalUser	
ET	req:action	{}	val:read	
ET	name:cn	==	req:identity	)
OU	(req:resource	==	val:AppObject	
ET	req:action	==	val:read	
ET	name:pozFolder	*--*	val:/CALM_Configuration/Content/Profiles	)

5. Recherchez des stratégies pour tous les utilisateurs, en procédant comme suit.

   a. Cliquez sur Stratégies d'accès dans le volet gauche.

   b. Sélectionnez Afficher les stratégies correspondant à l'identité. Désélectionnez les autres options.

   c. Entrez [Toutes les identités] dans le champ Ajouter une identité.

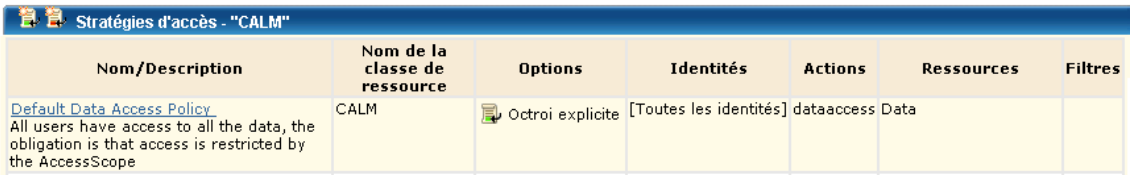
   d. Cliquez sur Ajouter.

   e. Cliquez sur OK.

   Quatre stratégies s'affichent, notamment la stratégie CEG et la stratégie d'accès aux données par défaut (si vous n'entrez pas précisément [Toutes les identités], de nombreuses autres stratégies s'affichent).

6. Examinez la stratégie d'accès aux données par défaut.

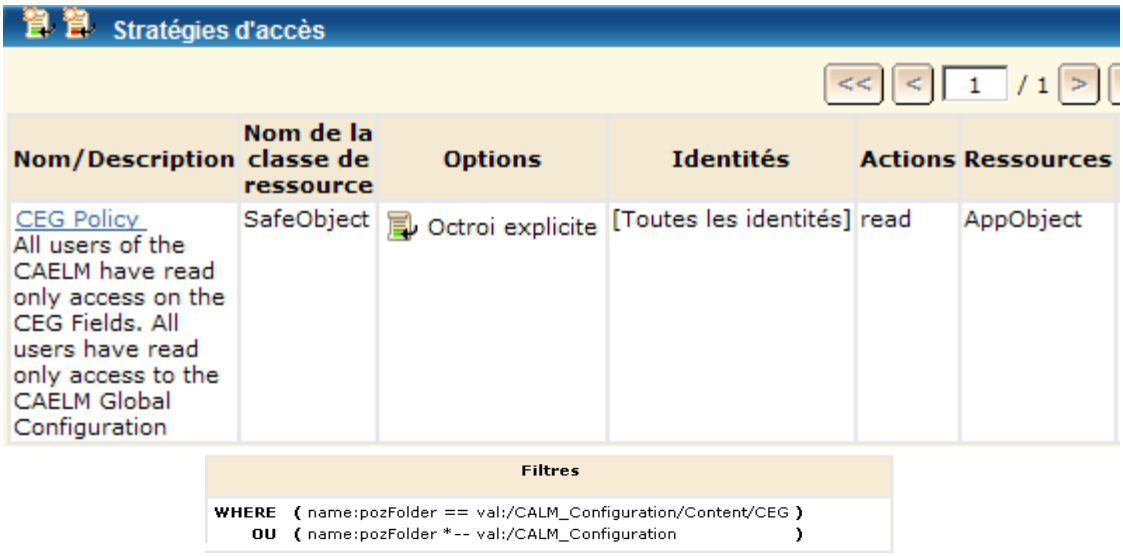
   La stratégie d'accès aux données par défaut prédéfinie pour la classe de ressource CALM autorise tous les utilisateurs à accéder aux données CA Enterprise Log Manager, dans les conditions fixées par un filtre d'accès. Un filtre d'accès se traduit en stratégie d'obligation avec l'action FulfillOnGrant définie sur dataaccess/CALM/Data.


Stratégies d'accès - "CALM"

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources	Filtres
Default Data Access Policy All users have access to all the data, the obligation is that access is restricted by the AccessScope	CALM	Octroi explicite	[Toutes les identités]	dataaccess	Data	

7. Examinez la stratégie de portée Stratégie CEG.

   La Stratégie CEG prédéfinie autorise tous les utilisateurs disposant d'un accès d'application CALM à afficher les champs de la grammaire commune aux événements. Par conséquent, les champs CEG s'affichent dans des listes déroulantes, afin de proposer des filtres simples et avancés pour tous les utilisateurs, étant donné que tous les utilisateurs peuvent définir des filtres globaux et locaux pour les requêtes qu'ils exécutent. Les utilisateurs autorisés à créer et à modifier des requêtes peuvent définir des filtres pour les requêtes qu'ils créent et modifient. Cette stratégie permet également de s'assurer que tous les utilisateurs peuvent consulter les paramètres de configuration globale.



Examen des stratégies pour les auditeurs

Vous pouvez examiner les stratégies prédéfinies pour les auditeurs, afin de savoir en quoi elles limitent l'accès aux applications pour les ressources nécessaires à la réalisation des tâches ci-dessous.

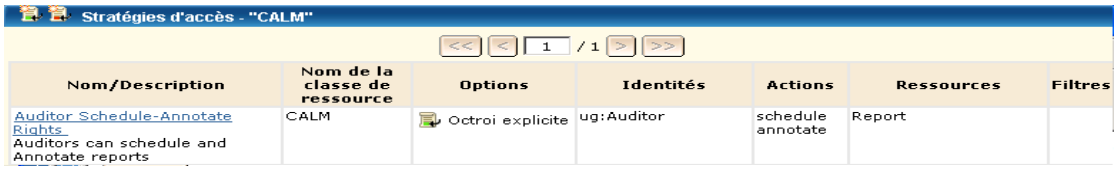
- Planification et annotation de rapports
- Affichage de rapports

Pour examiner les stratégies prédéfinies pour les auditeurs

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès dans le volet gauche.
3. Recherchez des stratégies pour les auditeurs, en procédant comme suit.
   a. Sélectionnez Afficher les stratégies correspondant à l'identité.
   b. Entrez ug:Auditor dans le champ Ajouter une identité.
   c. Cliquez sur Ajouter.
   d. Cliquez sur OK.

   Toutes les stratégies pour [Toutes les identités] et pour ug:Auditor s'affichent.
4. Examinez la stratégie des droits de planification et d'annotation de l'auditeur.

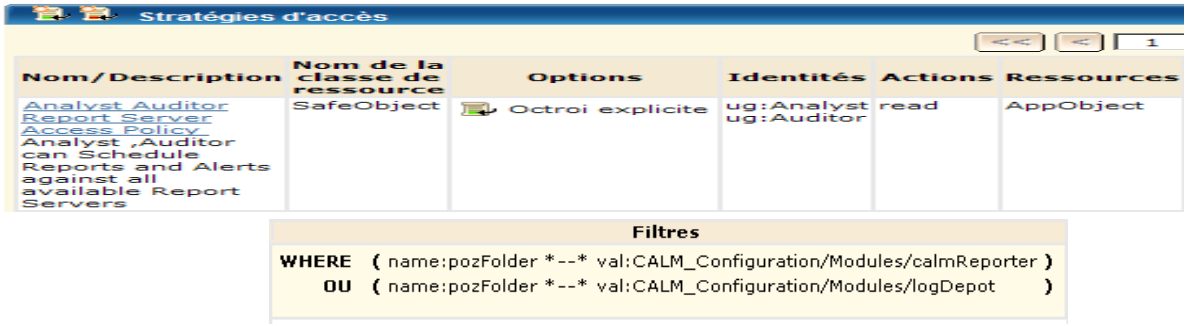
   Toutes les stratégies d'accès CALM définissent les actions pouvant être effectuées sur certaines ressources propres à l'application. Cette stratégie autorise les utilisateurs affectés au groupe d'utilisateurs d'applications Auditor à planifier et à annoter les rapports.



Comparez cette stratégie à la stratégie de création, de planification et d'annotation des analystes et à la stratégie de création des administrateurs.

5. Examinez la stratégie d'accès au serveur de rapports pour les auditeurs et les analystes.

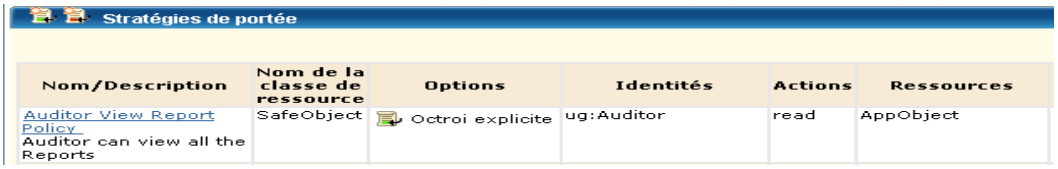
   Cette stratégie de portée permet aux auditeurs de définir comme destination du rapport n'importe quel serveur de rapports et de créer un rapport fédéré, qui requiert l'accès à un magasin de journaux d'événements. La ressource répertoriée dans cette stratégie est AppObject, pour laquelle les objets d'application sont les serveurs de rapports et les magasins de journaux d'événements.



   Remarque : Pour une stratégie d'accès CALM donnée, c'est-à-dire une stratégie pour la classe de ressource CALM, il existe généralement une stratégie de portée associée à la classe de ressource SafeObject.

6. Examinez la stratégie d'affichage de rapport pour un auditeur.

   Cette stratégie de portée octroie aux utilisateurs un accès en lecture aux rapports. La ressource répertoriée dans cette stratégie est AppObject.



   AppObject est limitée à une ressource d'application donnée, avec un filtre donnant le droit d'afficher les rapports. Le chemin d'accès est celui d'un dossier EEM, qui stocke le contenu de tous les rapports.

Examen des stratégies pour les analystes

Vous pouvez examiner les stratégies prédéfinies pour les analystes, afin de savoir en quoi elles limitent l'accès aux applications pour les ressources nécessaires à la réalisation des tâches ci-dessous.

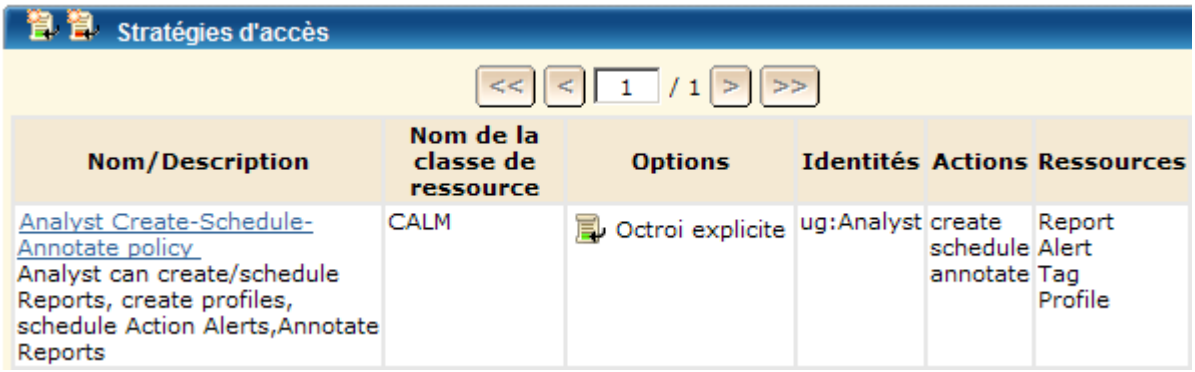
- Planification et annotation de rapports (tâches d'auditeur)
- Affichage de rapports (tâche d'auditeur)
- Création de rapports et de balises
- Création et planification d'alertes (requêtes)
- Modification de rapports, d'alertes et de balises

Pour examiner les stratégies prédéfinies pour les analystes

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès dans le volet gauche.
3. Recherchez des stratégies pour les analystes, en procédant comme suit.
   a. Désélectionnez la case à cocher Afficher les stratégies correspondant au nom.
   b. Sélectionnez Afficher les stratégies correspondant à l'identité.
   c. Entrez ug:Analyst dans le champ Ajouter une identité.
   d. Cliquez sur Ajouter.
   e. Cliquez sur OK.
4. Toutes les stratégies pour ug:Analyst s'affichent, y compris [Toutes les identités] qui incluent ce groupe d'utilisateurs.

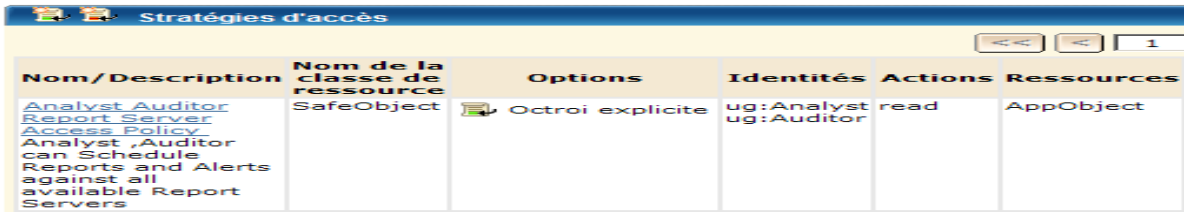
5. Examinez la stratégie de création, de planification et d'annotation des analystes.

   La stratégie d'accès CALM définit les actions pouvant être effectuées sur certaines ressources propres à l'application. Elle autorise les utilisateurs affectés au groupe d'utilisateurs d'applications CA Enterprise Log Manager Analyst à créer, planifier et annoter des rapports, à créer et planifier des alertes d'action et à créer des balises. Seuls les utilisateurs Auditor peuvent planifier et annoter des rapports.

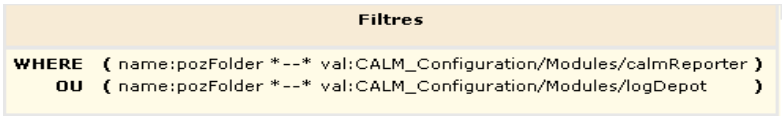


6. Examinez la stratégie d'accès au serveur de rapports pour les auditeurs et les analystes.

   Cette stratégie de portée autorise les analystes à planifier des actions sur n'importe quel serveur de rapports. La ressource répertoriée dans cette stratégie est AppObject.



   AppObject est limitée à des ressources d'application données, avec des filtres.

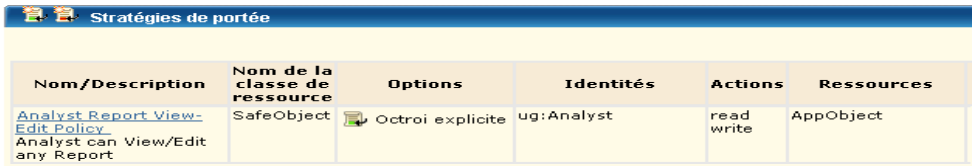


   - Le filtre se terminant par calmReporter autorise l'accès en lecture à tous les serveurs de rapports. Lorsqu'un rapport est planifié, vous spécifiez les serveurs de rapports de destination sur lesquels le rapport généré peut être affiché.

- Le filtre se terminant par logDepot autorise l'accès à tous les magasins de journaux d'événements. Lorsqu'un rapport est défini comme fédéré, les requêtes sont exécutées sur les données contenues dans l'ensemble des magasins de journaux d'événements éligibles. Leur éligibilité dépend de leur position dans la hiérarchie du serveur sur lequel le rapport est lancé, si la fédération est hiérarchique.

7. Examinez la stratégie de modification et d'affichage de rapports pour les analystes.

   Cette stratégie de portée autorise les utilisateurs affectés au rôle Analyst à afficher, modifier et supprimer n'importe quel rapport. La ressource spécifiée dans cette stratégie est AppObject.



Stratégies de portée

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	Octroi explicite	ug:Analyst	read write	AppObject

   AppObject se limite aux rapports désignés par le filtre suivant, qui donne le droit d'afficher les rapports générés sauvegardés dans le dossier EEM, situé dans /CALM_Configuration/Content/Reports.

Filtres
WHERE (name:pozFolder *--* val:/CALM_Configuration/Content/Reports)

   Remarque : L'autorisation de modification des rapports octroyée par cette stratégie est étendue par la stratégie CEG, qui permet d'ajouter des filtres aux rapports à l'aide des colonnes CEG.

Examen des stratégies pour les administrateurs

Les administrateurs attribuent le rôle Administrator aux utilisateurs devant accéder pleinement à l'application CA Enterprise Log Manager et à toutes ses fonctionnalités. Vous pouvez examiner les stratégies prédéfinies pour les administrateurs afin de savoir comment autoriser l'accès pour les utilisateurs devant effectuer les tâches ci-dessous.

- Créer une stratégie EventGrouping, c'est-à-dire créer des règles de suppression et de récapitulation à l'aide de la grammaire commune aux événements.
- Créer une stratégie Intégration, c'est-à-dire créer des fichiers de mappage des données et d'analyse de message à l'aide de la grammaire commune aux événements.
- Créer une stratégie EventForwarding, c'est-à-dire créer des règles pour transférer des événements à des systèmes tiers.
- Exécuter une stratégie Base de données, c'est-à-dire une requête de catalogue d'archive pour le nom des base de données sauvegardées ou déplacées vers un système d'archivage externe.
- Afficher ou modifier des stratégies.
- Afficher ou modifier des calendriers définis par l'utilisateur.
- Afficher ou modifier tout objet d'application. Les objets d'application sont les modèles de rapport, les modèles de requête, les jobs de rapport planifiés, les jobs d'alerte, les profils, les configurations de service, les fichiers de mappage des données (DM), les fichiers d'analyse de message (XMP), les règles de suppression et de récapitulation et les règles de transfert d'événement.
- Créer des filtres avec l'attribut iPoz pour AppObject.
- Afficher les dossiers répertoriés dans Administration, Gestion des utilisateurs et des accès, Dossiers EEM, et modifier les données définies par l'utilisateur et contenues dans ces dossiers.
- Afficher ou modifier les détails d'un utilisateur d'applications, d'un groupe d'utilisateurs d'applications ou d'un utilisateur global.
- Toute tâche des rôles Analyst ou Auditor.

Pour examiner les stratégies prédéfinies pour les administrateurs

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès dans le volet gauche.

3. Recherchez des stratégies pour les administrateurs, en procédant comme suit.

   a. Sélectionnez Afficher les stratégies correspondant à l'identité.

   b. Entrez ug:Administrator dans le champ Ajouter une identité.

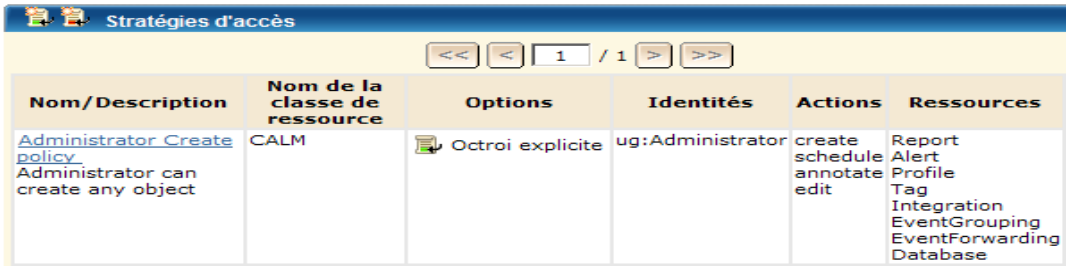
   c. Cliquez sur Ajouter.

   d. Cliquez sur OK.

   Toutes les stratégies pour [Toutes les identités] et pour ug:Administrator s'affichent.

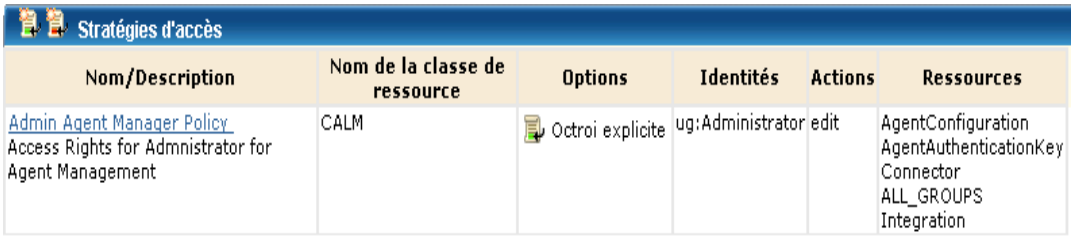
4. Examinez la stratégie d'accès de création d'administrateur CALM.

   Cette stratégie définit les actions pouvant être effectuées sur certaines ressources propres à l'application. Elle autorise les utilisateurs affectés au groupe d'utilisateurs d'applications Administrator à exécuter les actions spécifiées lorsqu'elles s'appliquent aux ressources précisées.



5. Examinez la stratégie d'accès du gestionnaire de l'agent d'administration CALM.

   Cette stratégie autorise les administrateurs à créer des groupes d'agents, modifier tous les groupes d'agents, configurer les connecteurs et créer des intégrations. Elle permet aux administrateurs de modifier la clé d'authentification d'agent pour l'instance d'application du serveur CA Enterprise Log Manager auquel l'agent transfère les événements collectés. Par défaut, la clé d'authentification d'agent configurée s'applique à tous les serveurs CA Enterprise Log Manager de l'ensemble des instances d'application, mais vous pouvez définir une clé unique pour une instance d'application donnée.



6. Examinez la stratégie de portée Stratégie d'administrateur par défaut.

   Cette stratégie autorise les administrateurs à afficher, modifier et supprimer les ressources répertoriées. Les ressources répertoriées ne sont pas spécifiques à CA Enterprise Log Manager et à AppObject. AppObject se réfère aux objets spécifiques à l'application, c'est-à-dire les ressources répertoriées dans les stratégies de création d'administrateur CALM et du gestionnaire de l'agent d'administration CALM.

Stratégies d'accès

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
Administrator Default Policy Administrators can view/modify/delete any Object	SafeObject	Octroi explicite	ug:Administrator	read write	Policy Calendar AppObject iPoz Folder User UserGroup GlobalUserGroup GlobalUser

Stratégies d'accès pour les produits enregistrés

Lorsqu'un produit est enregistré auprès de CA Enterprise Log Manager, un nouveau certificat est généré et certaines stratégies d'accès sont mises à jour pour permettre l'accès en lecture seule à l'ensemble des balises, requêtes et rapports. Plus spécifiquement, le nom du certificat utilisé pour authentifier le produit enregistré est ajouté en tant que Nom de certificat d'identité aux stratégies ci-dessous.

- Stratégie d'accès aux applications CALM
- Stratégie d'accès au serveur de rapports pour les auditeurs et les analystes
- Stratégie de modification et d'affichage des rapports pour les analystes

L'ajout du nom de certificat aux stratégies permet aux utilisateurs de tout produit CA, produit tiers ou client CA d'obtenir une liste des requêtes et des rapports par balise. Les utilisateurs peuvent afficher ces listes dans leur propre interface utilisateur et récupérer les données d'événements ajustés dont ils ont besoin.

Sauvegarde de toutes les stratégies d'accès

Il est recommandé d'exporter les stratégies d'accès prédéfinies, afin de conserver une copie de sauvegarde dans l'éventualité où ces stratégies seraient supprimées ou endommagées.

Important : Les stratégies pouvant être endommagées lors du redémarrage du système ou du service CA EEM, il est important de conserver une copie à jour à des fins de restauration. En outre, il est conseillé de sauvegarder régulièrement CA EEM, par exemple après l'installation d'un nouveau CA Enterprise Log Manager ou après la création de stratégies personnalisées.

Vous pouvez exporter toutes les stratégies pour chaque type de stratégie d'accès. Lorsque vous exportez des stratégies, un fichier XML est généré pour chaque stratégie du type sélectionné. Les fichiers XML ainsi obtenus sont ensuite compressés dans un fichier zip intitulé CAELM[1].xml.gz, qui contient le document CAELM[1].xml. Vous enregistrez ensuite le fichier zip exporté dans le répertoire de votre choix.

Pour pouvoir restaurer votre fichier de sauvegarde, vous devez le copier dans le répertoire CA Enterprise Log Manager suivant, avec le magasin d'utilisateurs interne : /opt/CA/LogManager/EEM. Vous pouvez effectuer cette copie juste après la sauvegarde dans votre répertoire local, ou attendre et effectuer la copie uniquement lorsqu'une restauration est nécessaire.

Le format d'exportation des stratégies dépend du nombre d'objets à exporter.

- Un fichier *nomfichier*.tar.gz est utilisé si le nombre d'objets exportés est très élevé.
- Un fichier *nomfichier*.xml.gz est utilisé si le nombre d'objets exportés est faible ou moyen.

Il est recommandé de renommer le fichier *nomfichier* (CAELM[n]) en choisissant un nom pertinent, lors de l'exportation. Par exemple, exportez les fichiers provenant des trois dossiers de stratégies et contenant des stratégies prédéfinies, telles que CAELM_CalmAccessPolicies, CAELM_EventPolicies et CAELM_ScopingPolicies.

Remarque : Conservez la même extension, xml.gz ou tar.gz.

Vous pouvez décompresser le fichier XML contenant la définition de stratégie d'accès et l'utiliser comme entrée pour le script SAFEX, qui sert à restaurer la stratégie d'accès.

Pour sauvegarder toutes les stratégies d'accès

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Sauvegardez les stratégies d'accès CALM prédéfinies, comme suit.
   a. Cliquez sur le bouton Stratégies d'accès.
   b. Cliquez sur CALM.

      La table Stratégies d'accès - "CALM" s'affiche.
   c. Cliquez sur le bouton Exporter.
   d. La boîte de dialogue Téléchargement de fichier s'affiche ; elle contient les options d'ouverture et d'enregistrement.
   e. Cliquez sur Ouvrir pour ouvrir le fichier zip CAELM[1].xml.gz (facultatif). Double-cliquez sur CAELM[1].xml pour examiner le fichier au format XML.
   f. Cliquez sur Enregistrer pour enregistrer le fichier.

      La boîte de dialogue Enregistrer sous s'affiche.
   g. Sélectionnez le dossier de destination de l'enregistrement, modifiez le nom du fichier si vous le souhaitez, puis cliquez sur Enregistrer.

      Si vous ne souhaitez pas modifier le nom du fichier, le fichier zip s'intitulera CAELM[1].xml.gz.
   h. Cliquez sur Fermer.

      La boîte de dialogue Téléchargement terminé se ferme. La liste des stratégies reste affichée dans le volet gauche.
3. Sauvegardez les stratégies d'événement prédéfinies, comme suit.
   a. Cliquez sur Stratégies d'événement.

      La table Stratégies d'événement s'affiche.
   b. Cliquez sur le bouton Exporter.
   c. La boîte de dialogue Téléchargement de fichier s'affiche ; elle contient les options d'ouverture et d'enregistrement.
   d. Cliquez sur Enregistrer pour enregistrer le fichier.

      Un message apparaît, vous demandant si vous souhaitez remplacer le fichier CAELM[1].xml.gz existant.

e. Cliquez sur Non.

f. Saisissez un nom unique dans le champ du nom de fichier, puis cliquez sur Enregistrer. Par exemple, modifiez l'entrée en CAELM[2].xml.gz ou saisissez le nom de votre choix pour le type de stratégie, tel que CAELM_EventPolicies.

g. Cliquez sur Fermer.

La boîte de dialogue Téléchargement terminé se ferme. La liste des stratégies reste affichée dans le volet gauche.

4. Sauvegardez les stratégies de portée prédéfinies, comme suit :

a. Cliquez sur Stratégies de portée.

La table Stratégies de portée s'affiche.

b. Cliquez sur le bouton Exporter. Il peut être nécessaire de faire défiler l'écran horizontalement pour afficher le bouton, situé en haut à droite.

c. La boîte de dialogue Téléchargement de fichier s'affiche ; elle contient les options d'ouverture et d'enregistrement.

d. Cliquez sur Enregistrer pour enregistrer le fichier.

Un message apparaît, vous demandant si vous souhaitez remplacer le fichier CAELM[1].xml.gz existant.

e. Cliquez sur Non.

f. Saisissez un nom unique dans le champ du nom de fichier, puis cliquez sur Enregistrer. Par exemple, modifiez l'entrée en CAELM[3].xml.gz ou saisissez le nom de votre choix pour le type de stratégie, tel que CAELM_ScopingPolicies.

g. Cliquez sur Fermer.

La boîte de dialogue Téléchargement terminé se ferme. La liste des stratégies reste affichée dans le volet gauche.

5. Cliquez sur Fermer.

La liste Stratégies d'accès se ferme.

Exemple --CAELM[1].xml pour les stratégies d'accès CALM

Voici une entrée de stratégie dans le fichier CAELM[1].xml.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <Safex>
    <Attach label="CAELM" />
    <Add />
  - <AddOrModify>
    - <Policy folder="/" name="Auditor Schedule-Annotate Rights">
        <Description>Auditors can schedule and Annotate reports</Description>
        <ResourceClassName>CALM</ResourceClassName>
        <PolicyType>policy</PolicyType>
        <Disabled>False</Disabled>
        <ExplicitDeny>False</ExplicitDeny>
        <PreDeployment>False</PreDeployment>
        <RegexCompare>False</RegexCompare>
        <Resource>Report</Resource>
        <Action>schedule</Action>
        <Action>annotate</Action>
        <Identity>ug:Auditor</Identity>
        <Attribute name="CreateTimestamp">20080926053329</Attribute>
      </Policy>
```

Informations complémentaires :

Sauvegarde manuelle des bases de données archivées (page 188)

Restauration des stratégies d'accès

Vous pouvez restaurer une stratégie d'accès qui a été supprimée ou modifiée de manière problématique. Lorsqu'une stratégie d'accès est accidentellement supprimée ou altérée, les utilisateurs référencés en tant qu'identités pour cette stratégie ne peuvent pas accéder à CA Enterprise Log Manager tant que la stratégie n'a pas été redéfinie ou restaurée.

La restauration des stratégies d'accès nécessite l'exécution du script SAFEX pour ces stratégies.

Observez l'une des deux procédures suivantes, selon si l'exportation a créé un fichier de sauvegarde avec l'extension xml.gz ou l'extension tar.gz.

Pour restaurer des stratégies d'accès à partir d'une sauvegarde nommée nom_fichier.xml.gz

1. Copiez vos fichiers de sauvegarde enregistrés dans le répertoire suivant du serveur de gestion CA Enterprise Log Manager, généralement le premier serveur installé.

   /opt/CA/LogManager/EEM

2. Exécutez la commande suivante pour récupérer le fichier XML.

   gunzip *nom_fichier*.xml.gz

   Vous créez ainsi le fichier *nom_fichier*.xml.

3. Si vous souhaitez restaurer une seule stratégie parmi celles du groupe sauvegardé, procédez comme suit (facultatif).

   a. Ouvrez le fichier XML.

   b. Pour les stratégies que vous ne souhaitez pas restaurer, supprimez les lignes XML commençant et se terminant par les balises ci-dessous. <Policy folder="/ name=*nom_stratégie*> et </Policy>

   c. Enregistrez le fichier.

4. Exécutez la commande suivante, où *nom_hôte_serveur_eem* représente le nom d'hôte du serveur de gestion CA Enterprise Log Manager.

   . /safex –h *nom_hôte_serveur_eem* –u EiamAdmin –p *mot_passe* –f *nom_fichier*.xml

   La ou les stratégies définies dans le fichier nom_fichier.xml à restaurer sont ajoutées au type de stratégie approprié et appliquées.

Pour restaurer des stratégies d'accès à partir d'une sauvegarde nommée nom_fichier.tar.gz

1. Copiez vos fichiers de sauvegarde enregistrés dans le répertoire suivant du serveur de gestion CA Enterprise Log Manager, généralement le premier serveur installé.

   /opt/CA/LogManager/EEM

2. Exécutez la commande suivante pour récupérer le fichier XML.

   gunzip *nom_fichier*.tar.gz

   Vous créez ainsi le fichier *nom_fichier*.tar.

3. Exécutez la commande ci-dessous.

   tar –xvf *nom_fichier*.tar

   Vous créez ainsi le fichier *nom_fichier*.xml.

4. Si vous souhaitez restaurer une seule stratégie parmi celles du groupe sauvegardé, procédez comme suit (facultatif).

   a. Ouvrez le fichier XML.

   b. Pour les stratégies que vous ne souhaitez pas restaurer, supprimez les lignes XML commençant et se terminant par les balises ci-dessous. <Policy folder="/ name=*nom_stratégie*> et </Policy>

   c. Enregistrez le fichier.

5. Exécutez la commande suivante, où *nom_hôte_serveur_eem* représente le nom d'hôte du serveur de gestion CA Enterprise Log Manager.

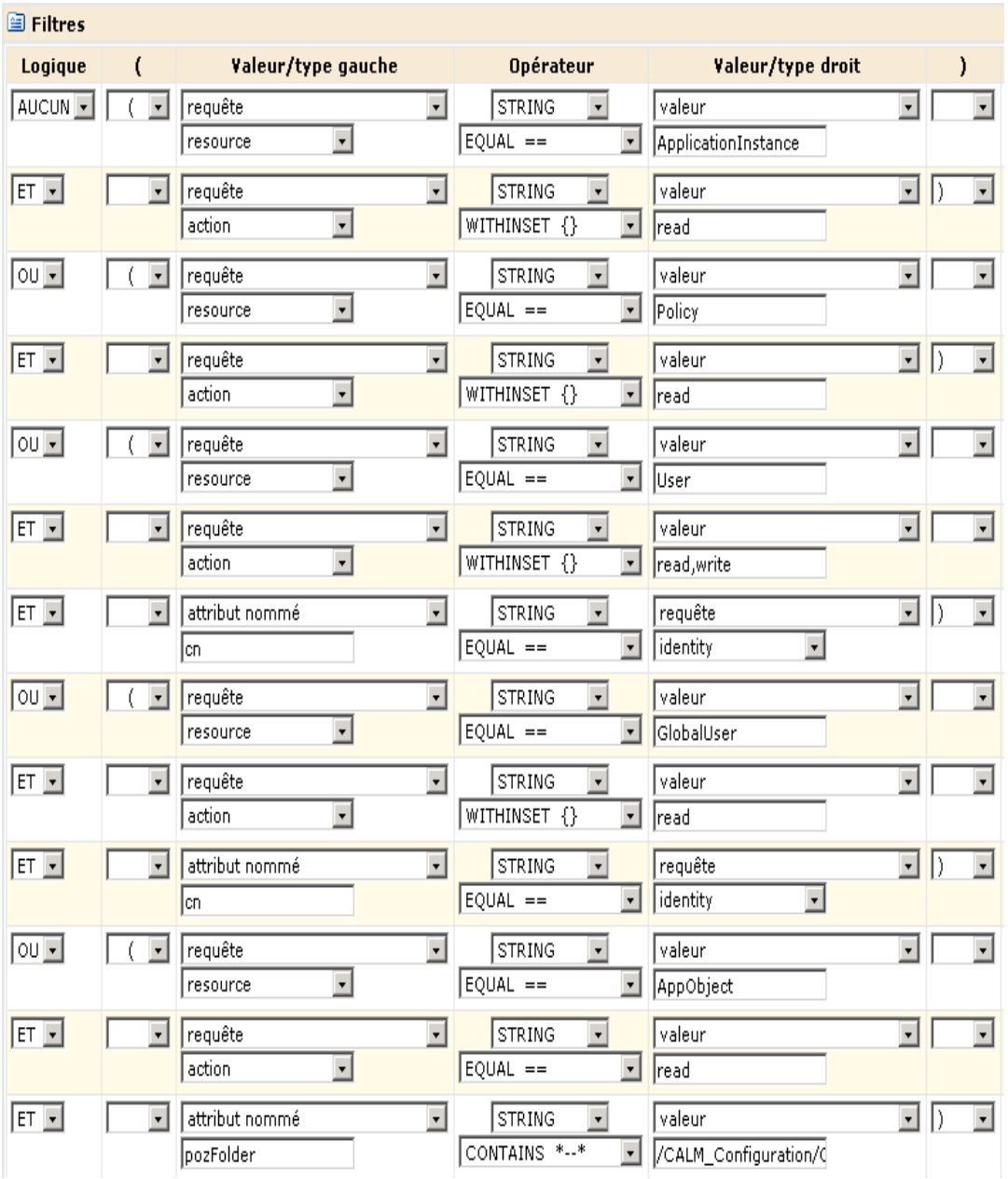
   . /safex –h *nom_hôte_serveur_eem* –u EiamAdmin –p *mot_passe* –f *nom_fichier*.xml

Pour recréer la stratégie d'accès CALM en l'absence de sauvegarde

Si vous n'avez pas effectué de sauvegarde, vous pouvez recréer la stratégie d'accès aux applications CALM.

1. Recréez la stratégie d'accès aux applications CALM. Consultez la section Stratégies prédéfinies.

2. Définissez les filtres comme indiqué dans l'illustration suivante. Les chemins d'accès partiels sont les suivants.
   - /CALM_Configuration/Content/Profiles
   - /CALM_Configuration/flex



Filtres

Logique	(	Valeur/type gauche	Opérateur	Valeur/type droit	)
AUCUN	(	requête resource	STRING EQUAL ==	valeur ApplicationInstance	
ET		requête action	STRING WITHINSET {}	valeur read	)
OU	(	requête resource	STRING EQUAL ==	valeur Policy	
ET		requête action	STRING WITHINSET {}	valeur read	)
OU	(	requête resource	STRING EQUAL ==	valeur User	
ET		requête action	STRING WITHINSET {}	valeur read,write	
ET		attribut nommé cn	STRING EQUAL ==	requête identity	)
OU	(	requête resource	STRING EQUAL ==	valeur GlobalUser	
ET		requête action	STRING WITHINSET {}	valeur read	
ET		attribut nommé cn	STRING EQUAL ==	requête identity	)
OU	(	requête resource	STRING EQUAL ==	valeur AppObject	
ET		requête action	STRING EQUAL ==	valeur read	
ET		attribut nommé pozFolder	STRING CONTAINS *--*	valeur /CALM_Configuration/C	)

La présence de cette stratégie permet à tous les administrateurs de se connecter et de créer les autres stratégies.

Chapitre 4 : Stratégies et rôles personnalisés

Ce chapitre traite des sujets suivants :

Instructions de création d'une stratégie

Toutes les stratégies de portées et d'accès CALM spécifient les actions autorisées ou interdites sur des ressources données, pour des identités données. Les stratégies pour la classe de ressource CALM autorisent ou interdisent à certaines identités d'effectuer des actions sur les ressources d'application, également appelées ressources CALM. Les stratégies de l'AppObject de la ressource SafeObject autorisent ou interdisent à des identités spécifiées les actions de lecture et d'écriture sur une ressource de niveau application, tel qu'indiqué dans les filtres. D'autres stratégies de la classe de ressource SafeObject autorisent ou interdisent à des identités spécifiées les actions de lecture et d'écriture sur des ressources globales.

Le type de stratégie que vous créez dépend de la ressource dont vous souhaitez limiter l'accès. Voici un récapitulatif des critères de chaque stratégie, en fonction de la ressource.

- Ressources exigeant une stratégie CALM et des stratégies de portée pour AppObject
  - Transfert d'événement
  - Regroupement d'événements
  - Intégration (hors agent)
  - Profil
  - Rapport

- Ressources exigeant uniquement une stratégie CALM
  - AgentAuthenticationKey
  - AgentConfiguration
  - Alerte
  - ALL_GROUPS
  - Connecteur
  - Base de données
  - Intégration (agent)
  - Balise
- Ressources exigeant uniquement des stratégies de portée pour la ressource globale
  - Calendar
  - Dossier
  - GlobalUser
  - GlobalUserGroup
  - iPoz
  - Policy
  - User
  - UserGroup

La section suivante met en relief les différences d'approche dans la création de stratégies, fondées sur les ressources que vous souhaitez contrôler.

Pour contrôler l'accès à EventForwarding, EventGrouping, Integration, Profile et Report

L'approche suivante s'applique uniquement aux stratégies des ressources CALM EventGrouping, Intégration, Profil et Rapport. Ces ressources d'application requièrent une stratégie CALM et deux stratégies de portée.

1. Créez une stratégie CALM pour une ou plusieurs ressources d'application, telles que Rapport ou Intégration. Spécifiez une ou plusieurs actions spécifiques à l'application, telles que la création, la planification ou l'annotation, valides pour les ressources spécifiées. Ajoutez les identités pour lesquelles les actions sont autorisées ou interdites.
2. Créez une stratégie de portée d'accompagnement pour la ressource AppObject, avec les actions de lecture et d'écriture. Spécifiez l'action d'écriture pour autoriser l'identité indiquée à modifier ou supprimer la ressource, mais pas à la créer. Spécifiez l'action de lecture pour autoriser l'identité à afficher ou consulter la ressource. Créez un filtre qui relie la ressource AppObject à la ressource d'application associée. Dans le filtre, indiquez le chemin d'accès au dossier EEM qui stocke le contenu de la ressource spécifiée ou qui correspond à un module dont l'accès est requis pour la ressource d'application associée. Ajoutez à la stratégie les mêmes identités que celles ajoutées à la stratégie CALM associée.
3. Créez une seconde stratégie de portée d'accompagnement pour la ressource AppObject, avec l'action de lecture. Spécifiez l'action de lecture pour autoriser l'identité à afficher ou consulter la ressource. Créez un filtre qui relie la ressource AppObject à la ressource d'application associée. Dans le filtre, indiquez le chemin d'accès au dossier EEM qui stocke le contenu de la ressource spécifiée ou qui correspond à un module dont l'accès est requis pour la ressource d'application associée. Ajoutez à cette stratégie des utilisateurs ou des groupes d'utilisateurs avec moins de droits en tant qu'Identités.

Pour contrôler l'accès aux ressources Alerte, Base de données, Balise et d'agent

L'approche suivante s'applique aux ressources d'application qui requièrent uniquement une stratégie CALM pour autoriser ou interdire un accès.

- Créez une stratégie d'accès CALM pour une ressource de type Connecteur ou Balise. Spécifiez l'action de modification pour permettre à l'identité de créer, modifier et supprimer la ressource et d'exécuter toute autre action valide. Ajoutez les identités pour lesquelles cette action est autorisée ou interdite.

  Remarque : L'accès aux ressources d'agent permet également d'utiliser les boutons du dossier Explorateur d'agent ou de ses sous-dossiers, dans le sous-onglet Collecte de journaux de l'onglet Administration. L'accès à la ressource Alerte permet à l'identité d'accéder à l'onglet Alertes. L'accès à la ressource Balise permet à l'identité de créer une balise pour une requête ou un rapport personnalisé. L'accès à la Base de données permet à l'identité d'exécuter une requête d'archivage.

Pour contrôler l'accès aux ressources globales utilisées dans l'application CAELM

L'approche suivante s'applique aux ressources globales, qui ne requièrent qu'une stratégie de portée pour limiter l'accès.

1. Créez une stratégie de portée pour une ou plusieurs ressources globales, telles que Utilisateur ou Stratégie. Spécifiez l'action d'écriture pour permettre à l'identité de créer, modifier ou supprimer la ressource. Ajoutez les identités pour lesquelles cette action est autorisée ou interdite.
2. Créez une stratégie de portée pour une ou plusieurs ressources globales, telles que Utilisateur ou Stratégie. Spécifiez l'action de lecture pour permettre à l'identité d'afficher la ressource globale. Ajoutez les identités pour lesquelles cette action est autorisée ou interdite.

   Remarque : Les ressources globales sont disponibles via les boutons du sous-onglet Gestion des utilisateurs et des accès de l'onglet Administration.

Informations complémentaires :

Types de stratégie d'accès CALM (page 77)
Ressources et actions (page 80)
Ressources CALM et dossiers EEM (page 83)
Ressources globales et fonctionnalité CA EEM (page 86)
Création d'une stratégie d'accès CALM (page 94)

Types de stratégie d'accès CALM

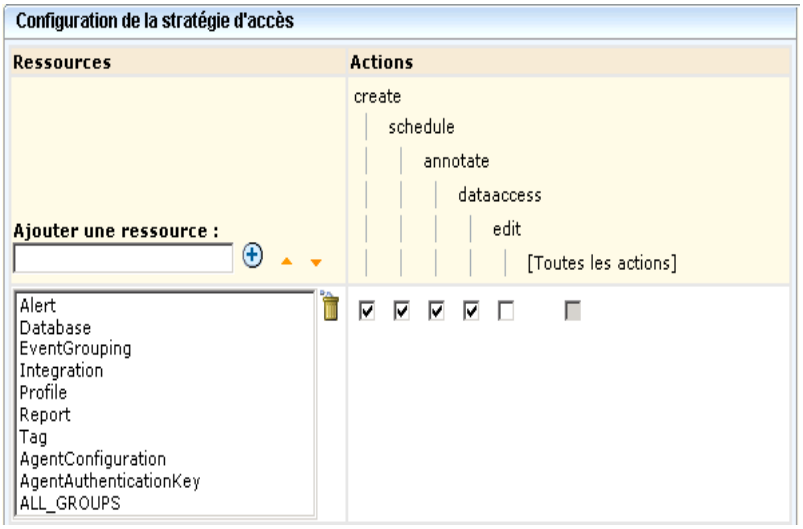
Lorsque vous créez une stratégie d'accès pour CALM ou pour une stratégie de portée, vous devez sélectionner l'un des trois types ci-dessous.

- Stratégie d'accès
- Liste de contrôle d'accès
- Liste de contrôle d'accès d'identité

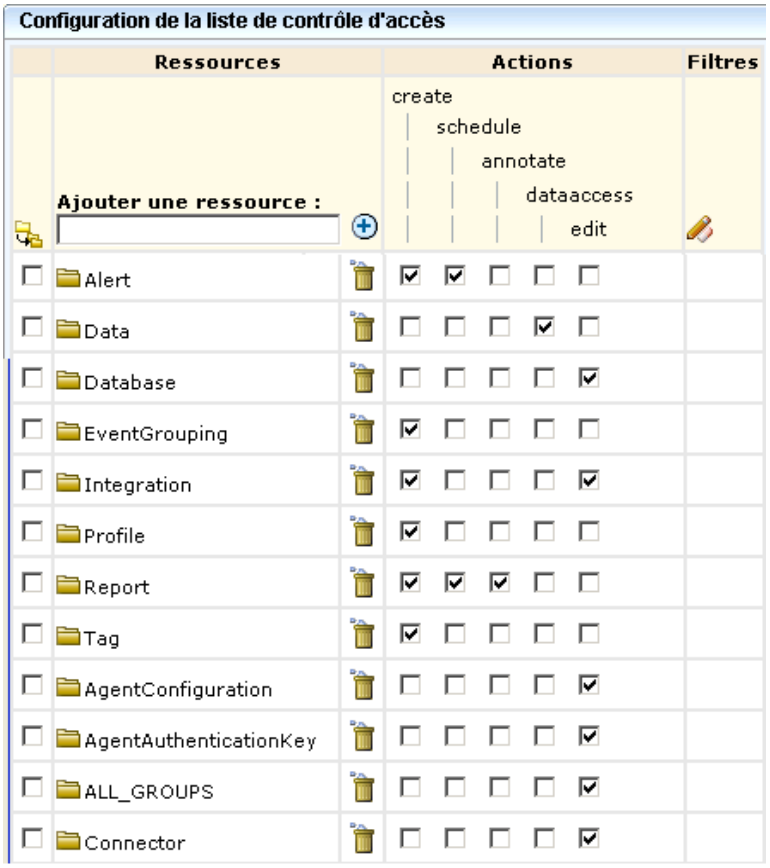
Ce choix influe sur le niveau de détail de la configuration des stratégies d'accès les plus larges.

Remarque : Les exemples présentés ici concernent des stratégies d'accès pour la classe de ressource CALM et incluent donc des actions et des ressources spécifiques à CA Enterprise Log Manager.

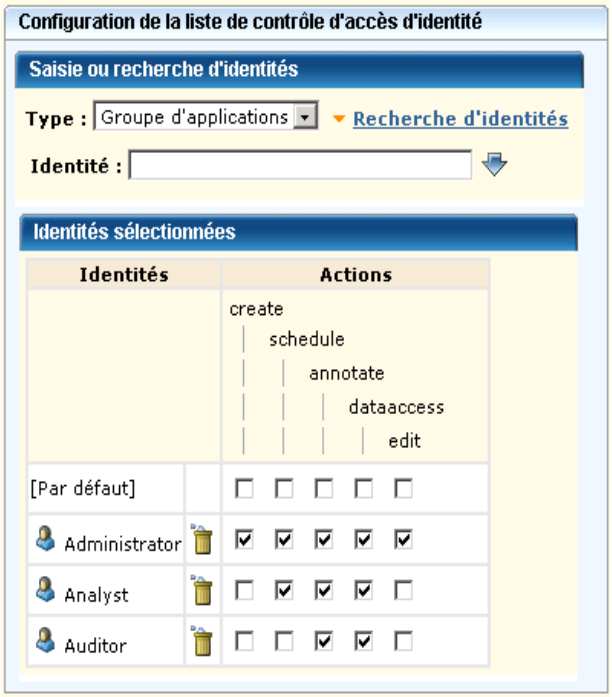
Une stratégie d'accès spécifie les actions valides pour les ressources sélectionnées, affectées à toutes les identités sélectionnées. Lorsque vous créez une stratégie générique pour CA Enterprise Log Manager, vous ajoutez des ressources appartenant à la classe de ressource CALM, puis vous sélectionnez les actions dans la liste qui s'affiche. Les actions choisies s'appliquent aux ressources sélectionnées, pour lesquelles elles sont valides. Dans cet exemple, la stratégie permet d'exécuter chaque action choisie sur toutes les ressources sélectionnées pour lesquelles l'action Création est valide.



Une liste de contrôle d'accès spécifie les actions valides pour chaque ressource individuellement, pour les identités sélectionnées. Lorsque vous créez une stratégie axée sur la ressource, vous devez spécifier les actions autorisées pour chaque ressource. Il n'est pas nécessaire de sélectionner des actions pour une ressource donnée simplement parce qu'elles sont valides. Par exemple, vous pouvez autoriser la création de rapports, mais pas la création d'alertes, même si l'action Création est valide pour les alertes. La liste de contrôle d'accès est la stratégie la plus affinée lorsqu'elle est mise en oeuvre pour chaque identité, individuellement.



Une liste de contrôle d'accès d'identité spécifie les actions autorisées pour les identités sélectionnées, pour toutes les ressources sélectionnées applicables. Lorsque vous créez une stratégie basée sur l'identité, spécifiez quelles actions chaque identité peut effectuer (Création, Planification, Annotation, Modification) sur toutes les ressources indiquées auxquelles chaque action s'applique. Si vous souhaitez empêcher les auditeurs de planifier des alertes, laissez le champ de planification vide. Mais cela empêche également l'auditeur de planifier des rapports.



Ressources et actions

Lors de la création de stratégies, configurez une stratégie d'accès pour laquelle un filtre d'accès est nécessaire. Un filtre d'accès est un filtre que l'administrateur peut définir pour contrôler les données d'événement pouvant être consultées par les utilisateurs ou groupes ne détenant pas le rôle Administrator. Par exemple, un filtre d'accès peut limiter les données figurant dans les rapports consultables par les groupes ou les utilisateurs spécifiés. Les filtres d'accès sont automatiquement convertis en stratégies d'obligation EEM. Ils sont souvent exprimés sous la forme du chemin d'accès relatif des objets dont l'accès utilisateur est limité. Vous pouvez afficher ces chemins d'accès relatifs dans la section Dossiers EEM de l'interface.

Généralement, les stratégies autorisant les actions telles que la création et la planification sont définies à l'aide de la classe de ressource CALM et des ressources CALM de type rapports, balises, fichiers de mappage de données et d'analyse de message, ainsi que règles de suppression et de récapitulation. Les stratégies autorisant les actions de lecture et d'écriture sont définies avec la classe de ressource SafeObject et la ressource AppObject. L'action Modifier est la seule action valide pour les ressources relatives aux agents dans la classe de ressource CALM.

Plus spécifiquement, les actions pouvant être autorisées pour les objets appartenant à la classe de ressource CALM sont répertoriées ci-dessous.

Action	Ressource	Description
Annotation	Rapport	Enregistrer des commentaires dans les rapports
Création	EventForwarding	Créer des règles pour transférer des événements spécifiques à des applications tierces
Création	EventGrouping	Créer des règles de suppression et de récapitulation à l'aide de la grammaire commune aux événements
Création	Intégration	Créer des fichiers de mappage des données et d'analyse de message à l'aide de la grammaire commune aux événements
Création	Profil	créer des profils.
Création	Rapport	Créer des rapports et des requêtes
Création	Balise	Créer des balises pour les rapports et les requêtes
Dataaccess	Données	Accéder aux données d'événements CALM, qui peuvent être limitées par des filtres d'accès aux données
Modification	AgentConfiguration	Créer des groupes d'agents. Configurer les agents installés avec les sources de collecte et la destination de

Action	Ressource	Description
		traitement
Modification	AgentAuthenticationKey	Créer et modifier la clé d'authentification de l'agent spécifiée durant l'installation de ce dernier
Modification	ALL_GROUPS	Modifier tous les groupes d'agents disponibles **Remarque :** L'accès peut être restreint à un groupe d'agents donné, en spécifiant le nom Groupe d'agents comme ressource
Modification	Connecteur	Configurer les connecteurs
Modification	Base de données	Déterminer les journaux qui correspondent aux critères de requête du catalogue d'archive et recataloguer la base de données
Modification	Intégration	Modifier les détails de l'intégration
Planification	Alerte	Planifier des alertes d'action
Planification	Rapport	Planifier les rapports et les requêtes

Les actions qui permettent aux utilisateurs d'afficher ou de modifier un objet appartenant à la classe de ressource SafeObject sont répertoriées ci-dessous.

Action	Ressource	Description
Lecture	AppObject	Afficher les modèles de rapport, les modèles de requête, les balises, les jobs de rapport planifié, les jobs d'alerte, les configurations de service, les fichiers de mappage des données, les fichiers d'analyse de message (XMP), les règles de suppression et de récapitulation, ainsi que les règles de transfert d'événement
Lecture	Calendar	Afficher les calendriers répertoriés dans Administration, Gestion des utilisateurs et des accès, Calendriers
Lecture	Dossier	Afficher les dossiers répertoriés dans Administration, Gestion des utilisateurs et des accès, Dossiers EEM
Lecture	GlobalUser	Visualiser les informations affichées pour les utilisateurs répertoriés lorsque vous effectuez une requête sur les Utilisateurs globaux dans Administration, Gestion des utilisateurs et des accès, Utilisateurs
Lecture	iPoz	Afficher les paramètres du magasin d'utilisateurs dans Administration, Gestion des utilisateurs et des accès, Magasin d'utilisateurs

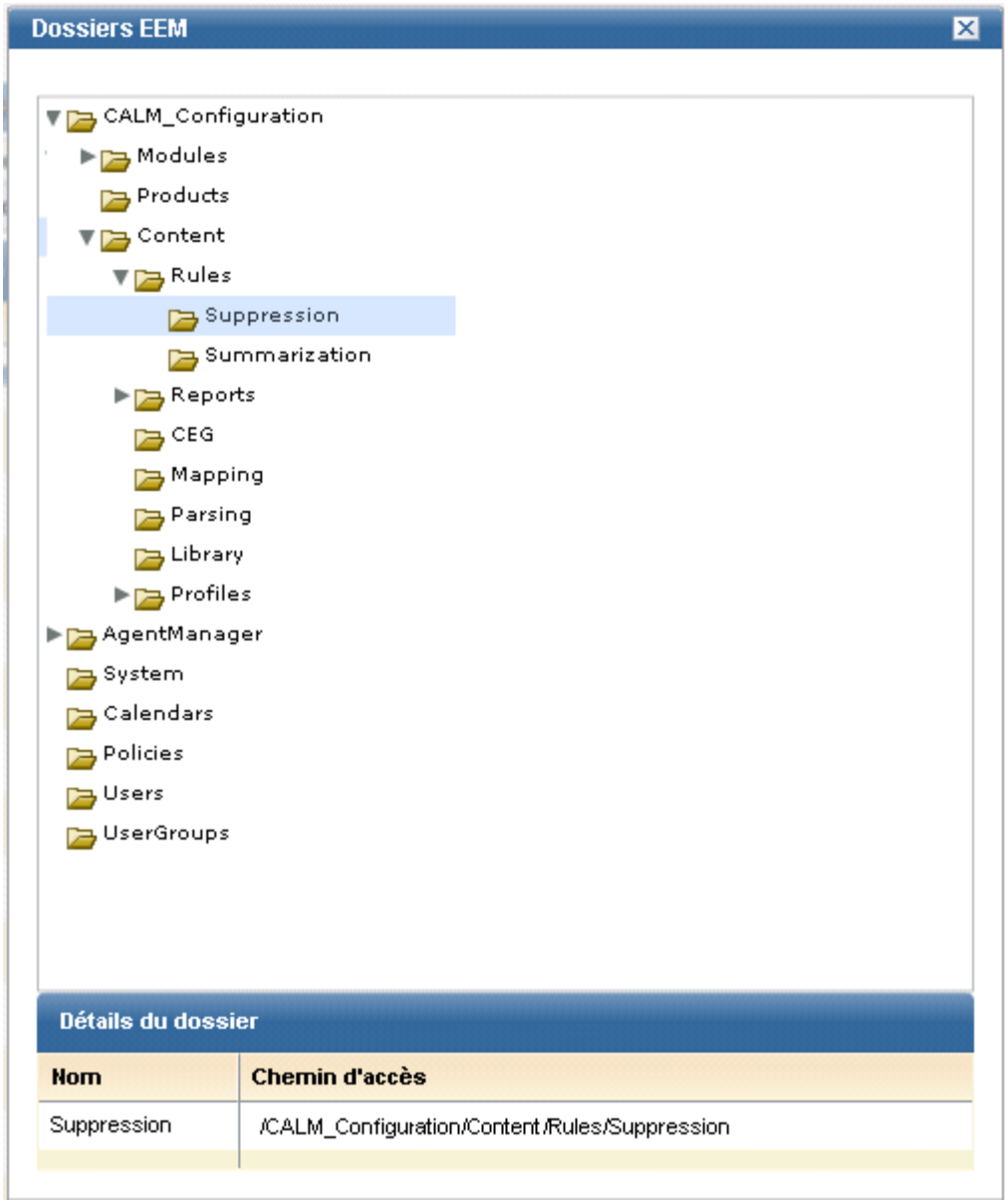
Action	Ressource	Description
		Afficher les paramètres de la stratégie de mots de passe dans Administration, Gestion des utilisateurs et des accès, Stratégies de mots de passe
Lecture	Policy	Afficher les stratégies répertoriées dans Administration, Gestion des utilisateurs et des accès, Stratégies d'accès
Lecture	User	Afficher les détails de l'utilisateur lorsque vous effectuez une requête sur les Détails de l'utilisateur de l'application, dans Administration, Gestion des utilisateurs et des accès, Utilisateurs
Lecture	UserGroup	Afficher l'appartenance au groupe d'applications pour les utilisateurs répertoriés lorsque vous effectuez une requête sur les Détails de l'utilisateur de l'application, dans Administration, Gestion des utilisateurs et des accès, Utilisateurs
Ecriture	AppObject	Modifier ou supprimer les modèles de rapport, les modèles de requête, les balises, les jobs de rapport planifiés, les jobs d'alerte, les configurations de service, les fichiers de mappage des données (DM), les fichiers d'analyse de message (XMP), les règles de suppression et de récapitulation et les règles de transfert d'événement
Ecriture	Calendar	Modifier les calendriers définis par l'utilisateur
Ecriture	Dossier	Modifier les données définies par l'utilisateur, ajoutées à la structure Dossiers EEM
Ecriture	GlobalUser	Modifier les informations de l'utilisateur global
Ecriture	iPoz	Configurer le magasin d'utilisateurs et les stratégies de mots de passe
Ecriture	Policy	Modifier les stratégies prédéfinies et définies par l'utilisateur
Ecriture	User	Modifier les détails de l'utilisateur de l'application
Ecriture	UserGroup	Créer, modifier ou supprimer un groupe d'utilisateurs d'applications

Ressources CALM et dossiers EEM

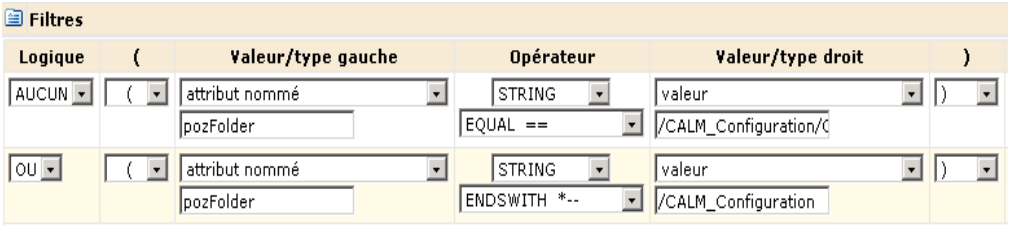
Pour chaque nouvelle stratégie CALM personnalisée de type EventForwarding, EventGrouping, Intégration, Profil ou Rapport, vous créez une stratégie de portée sur la base d'AppObject. Cette stratégie de portée dispose d'un accès en lecture/écriture qui filtre les chemins EEM pour chaque ressource CALM répertoriée dans la stratégie CALM correspondante. Les groupes d'utilisateurs correspondant aux Identités de la stratégie CALM sont affectés en tant qu'Identités à cette stratégie. Pour finaliser la configuration de la stratégie, créez une stratégie de portée supplémentaire en lecture seule, affectez-lui une Identité capable d'afficher uniquement la ressource, puis spécifiez un filtre avec un chemin d'accès au dossier EEM.

Remarque : La nécessité de créer une stratégie de portée pour la stratégie CALM dépend de la ressource que cette dernière utilise. Par exemple, les ressources Base de données, Balise et Alerte sont des ressources CALM pures, pour lesquelles aucune stratégie de portée n'est requise. Les stratégies de portée ne sont pas non plus requises pour les ressources relatives aux agents.

Vous pouvez afficher les dossiers EEM à partir du sous-onglet Gestion des utilisateurs et des accès, dans l'onglet Administration. Lorsque vous sélectionnez un dossier, comme le dossier Suppression, le chemin indiqué dans l'exemple suivant s'affiche.



Vous spécifiez le chemin d'accès au dossier EEM en tant que valeur d'une expression commençant par "pozFolder CONTAINS", tel qu'indiqué dans la section Filtres d'une définition de stratégie. Voici un exemple.



Les tableaux suivants contiennent des indications pour la valeur spécifiée dans le filtre d'une stratégie de portée associée à une stratégie CALM permettant d'octroyer, ou d'interdire, l'accès à des ressources CALM données.

Remarque : Il n'existe pas de correspondance unique entre les ressources CALM et les dossiers.

Lors de la création d'une stratégie de portée octroyant l'accès au contenu de cette ressource CALM	**Ajoutez un filtre spécifiant ce chemin d'accès de dossier EEM**
EventForwarding	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Forwarding
EventGrouping	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Summarization pozFolder CONTAINS /CALM_Configuration/Content/Rules/Suppression
Intégration (Serveur)	pozFolder CONTAINS /CALM_Configuration/Content/Mapping pozFolder CONTAINS /CALM_Configuration/Content/Parsing
Profil	pozFolder CONTAINS /CALM_Configuration/Content/Profiles
Rapport	pozFolder CONTAINS /CALM_Configuration/Content/CEG pozFolder CONTAINS /CALM_Configuration/Content/Reports

Lors de la création d'une stratégie de portée requérant l'accès à ce module CALM	**Ajoutez un filtre spécifiant ce chemin d'accès de dossier EEM**
Gestionnaire de l'agent	pozFolder CONTAINS /CALM_Configuration/Modules/AgentManager
Champ Magasin de journaux	pozFolder CONTAINS /CALM_Configuration/Modules/logDepot

Lors de la création d'une stratégie de portée requérant l'accès à ce module CALM	Ajoutez un filtre spécifiant ce chemin d'accès de dossier EEM
Serveur de rapports	pozFolder CONTAINS /CALM_Configuration/Modules/calmReporter
Module d'abonnement	pozFolder CONTAINS /CALM_Configuration/Modules/Subscription

Ressources globales et fonctionnalité CA EEM

Vous pouvez créer une stratégie de portée similaire, dans l'objectif, à une stratégie CALM, mais pour laquelle les ressources seront globales et non spécifiques au produit. Les ressources globales sont celles utilisées par plusieurs produits CA. Vous pouvez créer des stratégies afin d'autoriser ou d'interdire l'accès à des ressources globales spécifiques, accessibles via les boutons du sous-onglet Gestion des utilisateurs et des accès, dans l'onglet Administration.

Utilisez le tableau suivant pour créer une stratégie de portée destinée à autoriser ou interdire l'accès en lecture et en écriture, pour des identités données, aux ressources spécifiées comme globales.

Tâche	Action	Ressource globale
Afficher, créer, modifier ou supprimer un utilisateur global, un groupe d'utilisateurs globaux et un groupe d'utilisateurs d'applications (rôle) ; ajouter un groupe d'applications (rôle) à un utilisateur global ou créer un utilisateur global avec un rôle donné.	Lecture, écriture	User UserGroup GlobalUser GlobalUserGroup
Créer, modifier, copier, exporter, désactiver, tester, afficher ou supprimer une stratégie ; ajouter un calendrier à une stratégie	Lecture, écriture	Policy Calendar
Créer, modifier, copier, afficher ou supprimer un filtre d'accès ; afficher les dossiers EEM	Lecture, écriture	Policy
Créer un calendrier	Lecture, écriture	Calendar
Configurer le magasin d'utilisateurs ; créer, modifier ou afficher les stratégies de mots de passe	Lecture, écriture	iPoz

Lors de la création d'un filtre pour une ressource globale, référez-vous au filtre de la stratégie d'accès aux applications CALM comme guide. L'une des fonctions du filtre consiste à spécifier les actions associées à chaque ressource, Si vous cliquez sur Modifier dans une stratégie prédéfinie, vous pouvez examiner la source afin de savoir comment entrer la logique.

Planification des rôles d'utilisateur

Si les groupes d'utilisateurs d'applications prédéfinis (Administrator, Analyst et Auditor) ne suffisent pas à répondre à l'ensemble de vos besoins, vous pouvez créer des rôles personnalisés avec de nouveaux groupes d'utilisateurs d'applications. Par exemple, pour affecter un petit groupe d'individus à la gestion des comptes d'utilisateur (ces individus n'ayant aucun accès aux autres fonctions sur le serveur CA Enterprise Log Manager), vous pouvez définir un rôle UserAccountAdministrator, créer une stratégie de portée pour ce rôle, ajouter ce rôle à la stratégie d'accès aux applications de CALM et affecter ce rôle aux utilisateurs appelés à gérer les comptes d'utilisateur.

Le processus de planification des utilisateurs pour CA Enterprise Log Manager se compose des étapes suivantes.

- Déterminer le nombre d'utilisateurs nécessaires pour administrer, analyser et auditer CA Enterprise Log Manager.
- Identifier les utilisateurs auxquels accorder un accès à CA Enterprise Log Manager.

Si vous envisagez de créer des rôles personnalisés avec des stratégies d'accès associées, considérez l'approche suivante.

- Identifier le rôle à affecter à chaque utilisateur de CA Enterprise Log Manager.
- Identifier le type d'accès aux ressources de CA Enterprise Log Manager pour chaque rôle.

Vous pouvez également considérer les alternatives suivantes aux rôles définis par l'utilisateur (groupes d'applications).

- Configurer des stratégies de groupe d'utilisateurs dynamique qui créent des groupes d'utilisateurs dynamiques.
- Créer des groupes globaux et les traiter comme des groupes d'applications, c'est-à-dire les affecter à des utilisateurs et les affecter à des stratégies en tant qu'identités.

  Cette approche peut être utile si les stratégies sont créées dans le but de restreindre l'accès par zone géographique et si vous souhaitez que les mêmes utilisateurs détiennent le même niveau de droits sur plusieurs produits CA. Par exemple, un groupe global pour Location-A_Admin peut être affecté aux utilisateurs devant administrer plusieurs produits CA sur le site Location-A. Il est possible de créer des stratégies par produit CA qui accordent des droits administratifs pour les serveurs sur lesquels ce produit a été installé sur le site Location-A.

Informations complémentaires :

Création d'un groupe global (page 42)

Configuration de rôles d'utilisateur et de stratégies d'accès personnalisés

Un *rôle d'utilisateur* peut être un groupe d'utilisateurs d'applications prédéfini ou un groupe d'applications défini par l'utilisateur. Des rôles d'utilisateur personnalisés sont nécessaires lorsque les groupes d'applications prédéfinis (Administrator, Analyst et Auditor) ne sont pas suffisamment affinés pour refléter les attributions de tâches. Les rôles d'utilisateur personnalisés nécessitent des stratégies d'accès personnalisées et une modification des stratégies prédéfinies pour inclure le nouveau rôle.

Les administrateurs peuvent créer des rôles d'utilisateur et les stratégies correspondantes en suivant la procédure ci-dessous.

1. Pour chaque rôle endossé par les utilisateurs de CA Enterprise Log Manager
   - Identifiez les ressources auxquelles accorder l'accès.
   - Identifiez les actions autorisées sur chaque ressource.
   - Identifiez les identités (ou individus) auxquelles ce rôle s'applique.

     Remarque : Les identités peuvent être d'autres groupes d'applications appelés à constituer un "super groupe".

2. Si un groupe d'applications prédéfini est trop étendu pour vos besoins, créez un nouveau groupe d'applications et affectez-le aux individus que vous avez identifiés. Lorsque vous nommez un groupe d'applications défini par l'utilisateur, veillez à choisir un terme décrivant le rôle que doivent remplir les utilisateurs concernés.
3. Ajoutez le nouveau groupe d'applications à la stratégie d'accès aux applications CALM, qui est un type de liste de contrôle d'accès.
4. Si le nouveau rôle doit être en mesure d'entreprendre une action sur une ou plusieurs ressources (une action de création, par exemple), procédez comme suit.
    a. Configurez une stratégie CALM qui permet au nouveau groupe d'applications de créer ou d'entreprendre d'autres actions valides sur les ressources CA Enterprise Log Manager identifiées.
    b. Configurez une stratégie de portée qui accorde au nouveau groupe d'applications un accès en lecture et écriture à la ressource AppObject et spécifiez un filtre qui indique où la ressource identifiée est stockée dans les dossiers EEM. Pour chaque filtre, entrez l'attribut nommé, pozFolder, CONTAINS et une valeur, cette valeur étant le chemin d'accès au dossier EEM commençant par /CALM_Configuration.
5. Si le nouveau rôle doit pouvoir uniquement afficher une ressource CA Enterprise Log Manager spécifique, configurez une stratégie de portée qui autorise un accès en lecture à AppObject et spécifiez un filtre où l'attribut nommé, pozFolder, CONTAINS une valeur, cette valeur étant le chemin d'accès au dossier EEM (commençant par /CALM_Configuration) dans lequel cette ressource est stockée.
6. Testez les stratégies.
7. Affectez le nouveau rôle aux comptes d'utilisateur.

Les administrateurs peuvent également restreindre l'accès des utilisateurs à l'aide de filtres d'accès. Si un type particulier d'accès limité s'applique à un seul individu, vous pouvez omettre d'affecter à cette personne un groupe d'applications, ou un rôle. Pour limiter l'accès d'un utilisateur

1. Créez un utilisateur mais ne lui affectez aucun rôle.
2. Donnez-lui accès à l'application CA Enterprise Log Manager en ajoutant l'utilisateur à la stratégie d'accès CALM.
3. Créez une stratégie de portée qui accorde un accès en lecture ou en écriture à SafeObject, AppObject et spécifiez un filtre dans lequel l'attribut nommé pozFolder est égal à la valeur du dossier EEM pour cette la ressource. Par exemple, si la ressource est un ensemble de rapports, spécifiez que l'attribut nommé calmTag doit être égal à la valeur d'une balise de rapport.
4. Créez un filtre d'accès personnalisé.

Les administrateurs peuvent personnaliser l'accès utilisateur aux ressources CA Enterprise Log Manager. Etudiez les exemples ci-après.

- Créez des rôles pour affecter des responsabilités d'administration spécifiques à différents groupes d'administrateurs. Par exemple, créez un rôle UserAccountAdministrator. Créez une stratégie qui accorde aux utilisateurs détenant ce rôle un accès aux seules fonctions nécessaires aux opérations de maintenance des utilisateurs et groupes. Cette stratégie doit définir un accès en lecture et en écriture à la ressource GlobalUser comme aux ressources User et UserGroup.
- Créez des rôles pour distribuer des responsabilités d'analystes aux divers types de rapports et requêtes en fonction des balises. Par exemple, créez les rôles SystemAccessAnalyst et PCIAnalyst et affectez des analystes à un seul des rôles d'analystes à accès restreint. Créez ensuite des stratégies qui accordent un accès à un sous-ensemble de ces ressources en fonction des balises. Créez par exemple une stratégie qui accorde un accès propre au rôle SystemAccessAnalyst aux rapports et requêtes contenant la balise Accès au système et une autre qui accorde un accès propre au rôle PCIAnalyst aux rapports et requêtes contenant la balise PCI. Créez d'autres rôles et stratégies en fonction d'autres balises. Les stratégies qui limitent l'accès de cette manière utilisent des filtres d'accès.

Les administrateurs peuvent créer des stratégies basées sur des serveurs à l'aide de l'une des approches suivantes.

- Limiter les données

  Vous pouvez limiter l'accès à des journaux spécifiques en créant un filtre d'accès aux données, en le paramétrant sur le champ receiver_name et en spécifiant une valeur telle que systemstatus ou syslog.

- Limiter la configuration

  Vous pouvez limiter l'accès à un serveur CA Enterprise Log Manager en créant une stratégie sur la classe de ressources SafeObject avec AppObject en tant que ressource sélectionnée. Autrement dit, pour limiter l'accès à la seule configuration de serveur de rapports sur un hôte particulier, définissez un filtre du type suivant.

  pozFolder contains /CALM_Configuration/Modules/calmReporter/LogServer01

Informations complémentaires :

Exemples de stratégie pour les intégrations personnalisées (page 136)
Exemples de stratégie pour les règles de suppression et de récapitulation (page 137)
Création d'un filtre d'accès (page 105)
Restriction d'accès pour un utilisateur : scénario de l'administrateur Windows (page 116)
Restriction d'accès pour un rôle : scénario PCI-Analyst (page 129)

Création d'un groupe d'utilisateurs d'applications (rôle)

Vous pouvez créer un nouveau groupe d'utilisateurs d'applications pour accompagner les rôles dont vous avez besoin. Une fois un nouveau groupe d'utilisateurs d'applications créé, vous devez élaborer des stratégies d'accès pour ce groupe.

Il existe un cas dans lequel de nouvelles stratégies d'accès ne sont pas nécessaires pour un nouveau groupe : lorsque ce groupe possède des appartenances à des groupes existants. Imaginez que vous ayez besoin d'un rôle pour les individus devant créer des fichiers de mappage de données et d'analyse de message, un autre rôle pour les individus devant créer des règles de suppression et de récapitulation et un troisième rôle pour les utilisateurs qui peuvent effectuer l'une ou l'autre de ces deux tâches. Vous avez la possibilité de définir un groupe d'utilisateurs d'applications appelé AdminDMMP avec une stratégie qui accorde un accès en création à la ressource Integration et un autre groupe appelé AdminSS avec une stratégie qui accorde un accès en création à la ressource EventGrouping. Vous pouvez ensuite créer un troisième groupe AdminDMMPSS avec des appartenances au groupe AdminDMMP et au groupe AdminSS. Ce troisième groupe hériterait automatiquement des stratégies des deux groupes d'appartenance.

Plutôt que de créer de nouveaux groupes d'applications, ou rôles, vous pouvez étendre les rôles prédéfinis Analyst et Auditor. Par exemple, si vous souhaitez que les analystes soient en mesure de créer des règles de suppression et de récapitulation et que les auditeurs puissent afficher ces règles, vous pouvez créer une stratégie CALM qui donne la possibilité de créer des règles de récapitulation et de suppression ainsi qu'une stratégie de portée qui permette d'afficher ou de modifier des règles personnalisées, puis affecter le rôle Analyst à ces stratégies. Vous pouvez ensuite créer une stratégie de portée qui donne aux utilisateurs la possibilité d'afficher les règles de suppression et de récapitulation et affecter le groupe Auditor à cette stratégie.

Seuls les administrateurs peuvent créer de nouveaux rôles.

Pour créer un groupe d'utilisateurs d'applications (rôle)

1. Cliquez sur l'onglet Administration et sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Groupes.
3. Cliquez sur le bouton Nouveau groupe d'applications à gauche du dossier Groupes d'applications dans la liste Groupes d'utilisateurs.
4. Indiquez le nom du groupe et saisissez une description.
5. Si ce nouveau groupe d'utilisateurs doit avoir un accès que vous avez déjà défini pour au moins deux groupes d'applications définis par l'utilisateur, sélectionnez ces groupes d'applications pour appartenance. Sinon, n'effectuez aucune sélection.

Remarque : Si ce nouveau groupe est composé de groupes existants, leurs stratégies existantes s'appliquent à l'ensemble du groupe. Aucune autre stratégie n'est requise.

6. Cliquez sur Enregistrer.
7. Cliquez sur Fermer.

Informations complémentaires :

Etape 2 : création du rôle PCI-Analyst (page 131)
Exemples de stratégie pour les règles de suppression et de récapitulation (page 137)

Attribution d'un accès de rôle personnalisé à CA Enterprise Log Manager

Lorsque vous créez un groupe d'utilisateurs d'applications, ou rôle, assurez-vous de l'ajouter à la stratégie d'accès aux applications CALM prédéfinie. Seules les identités qui sont explicitement ajoutées à cette stratégie peuvent accéder à CA Enterprise Log Manager. Les identités peuvent être des utilisateurs individuels ou des membres d'un groupe d'utilisateurs.

Si vous rencontrez une situation dans laquelle des utilisateurs affectés à un nouveau groupe d'utilisateurs ne peuvent pas se connecter à CA Enterprise Log Manager, assurez-vous que les identités de la stratégie d'accès aux applications CALM incluent ce groupe.

Pour accorder un accès à CA Enterprise Log Manager à un groupe d'utilisateurs d'applications défini par l'utilisateur

1. Sélectionnez l'onglet Administration, cliquez sur Gestion des utilisateurs et des accès, puis sur Stratégies d'accès dans le volet gauche.
2. Cliquez sur Stratégies de portée et sélectionnez Accès aux applications CALM.
3. Sous Identités, recherchez le nouveau groupe d'applications comme suit.
   a. Pour Type, sélectionnez Groupe d'applications.
   b. Cliquez sur Recherche d'identités.
   c. Laissez Nom en tant qu'attribut et COMME en tant qu'opérateur. Cliquez sur Rechercher.

      Le nom du nouveau groupe d'applications apparaît dans la liste des identités qui s'affiche.
   d. Sélectionnez le nom du nouveau groupe d'applications et cliquez sur le bouton Déplacer pour déplacer le nom du groupe dans la zone Identités sélectionnées.
4. Cliquez sur Enregistrer.

Ajout d'une identité à une stratégie existante

Lors de sa création, vous pouvez ajouter un nouveau groupe d'utilisateurs d'applications à des stratégies existantes, le cas échéant. Lorsque vous créez un utilisateur qui ne possède aucun rôle mais détient un accès limité par un filtre d'accès, vous pouvez également l'ajouter à des stratégies existantes.

Important : Lorsque vous intervenez sur les stratégies d'accès installées, faites bien attention à ne pas les supprimer car elles ne sont ni verrouillées ni protégées.

Si une stratégie d'accès prédéfinie est supprimée par accident, les utilisateurs ne sont plus en mesure d'accéder au serveur CA Enterprise Log Manager jusqu'à sa restauration. Vous pouvez restaurer des stratégies en exécutant les scripts SAFEX pour les stratégies.

Pour ajouter une identité à une stratégie existante

1. Sélectionnez l'onglet Administration, cliquez sur Gestion des utilisateurs et des accès, puis sur Stratégies d'accès dans le volet gauche.
2. Cliquez sur le type de stratégie, puis sélectionnez la stratégie qui s'applique au nouveau groupe d'utilisateurs d'applications. Affichez le volet Identités.
3. Pour Type, sélectionnez Groupe d'applications.
4. Cliquez sur Recherche d'identités.
5. Laissez Nom en tant qu'attribut et COMME en tant qu'opérateur. Cliquez sur Rechercher.

   Le nom du nouveau groupe d'applications apparaît dans la liste des identités qui s'affiche.
6. Sélectionnez le nom du nouveau groupe d'applications et cliquez sur le bouton Déplacer pour déplacer le nom du groupe dans la zone Identités sélectionnées.
7. Cliquez sur Enregistrer.

Informations complémentaires :

Etape 4 : ajout du rôle PCI-Analyst aux stratégies existantes (page 132)

Création d'une stratégie d'accès CALM

Vous pouvez créer une stratégie d'accès CALM afin d'autoriser (ou d'interdire) une ou plusieurs actions valides pour une ou plusieurs ressources CALM.

Les ressources CALM suivantes sont spécifiques à une application, c'est-à-dire qu'elles sont utilisées uniquement par le produit CA Enterprise Log Manager.

- Alerte
- AgentConfiguration
- AgentAuthenticationKey
- ALL_GROUPS
- Connecteur
- Données
- Base de données
- EventGrouping
- Intégration
- Profil
- Rapport
- Balise

Pour créer une toute nouvelle stratégie CALM

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès.
3. Cliquez sur le bouton Nouvelle stratégie d'accès, situé à gauche du dossier CALM.
4. Entrez un nom pertinent pour la stratégie et, si vous le souhaitez, une courte description.
5. Si la stratégie est temporaire, sélectionnez le Calendrier contenant la plage de dates à laquelle la stratégie s'applique.
6. Acceptez CALM comme nom de classe de ressource.

7. Sélectionnez Type dans le panneau Général en fonction des critères suivants.
   - Sélectionnez Stratégie d'accès pour permettre ou non à toutes les identités sélectionnées d'effectuer toutes les actions sélectionnées sur toutes les ressources sélectionnées.
   - Sélectionnez Liste de contrôle d'accès pour permettre ou non à toutes les identités sélectionnées d'effectuer seulement les actions sélectionnées sur une ressource sélectionnée.

     Remarque : Il est impossible d'enregistrer des filtres pour plusieurs ressources. Pour contourner ce problème, créez des stratégies distinctes pour chaque combinaison ressource/filtres.
   - Sélectionnez Liste de contrôle d'accès des identités pour permettre ou non à chaque identité sélectionnée d'effectuer toutes les actions sélectionnées sur toutes les ressources sélectionnées auxquelles elle s'applique.
8. Dans la section Identités, sélectionnez les utilisateurs ou groupes auxquels cette stratégie va s'appliquer, en procédant comme suit.
   a. Sélectionnez Groupe d'applications dans le champ Type, ou l'une des autres options, cliquez sur Recherche d'identités, puis sur Rechercher.
   b. Sélectionnez des identités parmi celles disponibles, puis cliquez sur le bouton Déplacer pour les placer dans la zone Identités sélectionnées.
9. S'il s'agit d'une stratégie d'accès, finalisez la configuration de la stratégie comme suit.
   a. Entrez une ressource CALM dans le champ Ajouter une ressource, puis cliquez sur Ajouter.
   b. Sélectionnez chaque action que les identités sélectionnées doivent pouvoir exécuter sur une ressource donnée ; les actions valides incluent l'annotation, la création, l'accès aux données (dataaccess), la modification et la planification. Vous ne pouvez pas autoriser une action spécifique sur une ressource donnée uniquement, si celle-ci est valide également pour une autre ressource.

10. Si la stratégie est une liste de contrôle d'accès, renseignez les champs de configuration de la liste de contrôle d'accès comme suit.
    a. Entrez une ressource CALM dans le champ Ajouter une ressource, puis cliquez sur Ajouter.
    b. Sélectionnez chaque action que les identités sélectionnées doivent pouvoir exécuter sur cette ressource ; les actions valides incluent une ou plusieurs actions suivantes, à savoir l'annotation, la création, l'accès aux données (dataaccess), la modification et la planification.
    c. Répétez les deux dernières étapes pour chaque ressource soumise à cette stratégie.

       Ce type de stratégie vous permet d'autoriser une action (de type créer) pour une ressource et pas pour une autre.
11. Si la stratégie est une liste de contrôle d'accès des identités, renseignez les champs de configuration de la liste de contrôle d'accès des identités comme suit.
    a. Pour chaque identité sélectionnée, choisissez les actions à autoriser ou interdire sur toutes les ressources où ces actions sont valides.
    b. Pour chaque ressource à ajouter, entrez un nom de ressource CALM dans le champ Ajouter une ressource, puis cliquez sur Ajouter.
12. Etudiez les cases à cocher situées en haut de la fenêtre et sélectionnez celles qui s'appliquent.
    - Sélectionnez Refus explicite pour passer d'une stratégie qui autorise l'accès à une qui le refuse.
    - Sélectionnez Désactivé pour rendre temporairement inactive cette stratégie.
    - Sélectionnez Pré-déploiement, puis Affectation d'étiquettes et ajoutez les étiquettes si vous utilisez cette stratégie à des fins de test et si vous souhaitez classer les stratégies par étiquettes personnalisées.
13. Cliquez sur Enregistrer, puis sur Fermer dans le volet gauche.

Création d'une stratégie de portée

Vous pouvez créer une stratégie de portée sur n'importe quelle ressource globale. Les actions liées aux stratégies de portée se limitent à la lecture et l'écriture.

- Les ressources globales suivantes sont utilisées par de nombreux produits CA (applications).
  - Calendar
  - GlobalUser
  - GlobalUserGroup
  - iPoz
  - Policy
  - User
  - UserGroup
  - AppObject
- La ressource globale AppObject vous permet de créer des stratégies de portée sur des modules et des ressources spécifiques à une application. Pour ce faire, vous ajoutez un filtre désignant le dossier EEM concerné, où le module ou le contenu spécifique à l'application est stocké.
  - Vous trouverez ci-dessous les dossiers de contenu EEM utilisables dans les filtres avec la ressource AppObject.
    - EventGrouping
    - Intégration (Serveur)
    - Profil
    - Rapport
  - Vous trouverez ci-dessous les dossiers de module CA Enterprise Log Manager utilisables dans les filtres avec la ressource AppObject.
    - Champ Magasin de journaux
    - Serveur de rapports
    - Abonnement

Vous pouvez créer une stratégie en partant de zéro s'il n'en existe aucune dont vous pouvez tirer profit. Si vous créez une stratégie de portée associée à une stratégie CALM créée par vos soins, spécifiez les mêmes identités dans les deux stratégies.

Seuls les administrateurs peuvent créer, modifier, supprimer et afficher des stratégies d'accès.

Pour créer une nouvelle stratégie de portée avec accord explicite

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès.
3. Cliquez sur le bouton Nouvelle stratégie de portée, situé à gauche du dossier Stratégies de portée.
4. Donnez un nom évocateur à la stratégie. Par exemple, utilisez le ou les rôles auxquels elle s'applique et les tâches visées. Affichez les noms des stratégies prédéfinies pour voir des exemples.
5. Ajoutez une rapide description afin d'expliciter le nom crypté.
6. En général, vous acceptez SafeObject comme nom de classe de ressource.
7. Sélectionnez Type dans le panneau Général en fonction des critères suivants.
   - Sélectionnez Stratégie d'accès pour permettre ou non à toutes les identités sélectionnées d'effectuer toutes les actions sélectionnées sur toutes les ressources sélectionnées.
   - Sélectionnez Liste de contrôle d'accès pour permettre ou non à toutes les identités sélectionnées d'effectuer seulement les actions sélectionnées sur une ressource sélectionnée.

     Remarque : Il est impossible d'enregistrer des filtres pour plusieurs ressources. Pour contourner ce problème, créez des stratégies distinctes pour chaque combinaison ressource/filtres.
   - Sélectionnez Liste de contrôle d'accès des identités pour permettre ou non à chaque identité sélectionnée d'effectuer toutes les actions sélectionnées sur toutes les ressources sélectionnées auxquelles elle s'applique.
8. Si la stratégie est une stratégie d'accès ou une liste de contrôle d'accès, utilisez la zone Identités pour sélectionner les utilisateurs ou les groupes auxquels cette stratégie s'applique.
   a. Sélectionnez Groupe d'applications comme Type, cliquez sur Recherche d'identités, puis sur Rechercher.
   b. Sélectionnez des identités parmi celles disponibles, puis cliquez sur le bouton Déplacer pour les placer dans la zone Identités sélectionnées.

9. Si la stratégie est une stratégie d'accès, toutes les actions sont par défaut sélectionnées pour toutes les ressources. Pour la personnaliser, renseignez les champs de configuration de la stratégie d'accès comme suit.

   a. Sélectionnez une ressource dans la liste déroulante Ajouter une ressource, puis cliquez sur Ajouter.

      - Sélectionnez AppObject si les ressources dont l'accès en lecture ou en écriture doit être configuré sont des ressources CA Enterprise Log Manager.
      - Sélectionnez User et GlobalUser pour accéder aux boutons Utilisateurs du sous-onglet Gestion des utilisateurs et des accès, dans l'onglet Administration.
      - Sélectionnez UserGroup et GlobalUserGroup pour accéder aux boutons Groupes du sous-onglet Gestion des utilisateurs et des accès, dans l'onglet Administration.
      - Sélectionnez Policy pour accéder aux boutons Stratégies d'accès, Dossiers EEM et Stratégies de test du sous-onglet Gestion des utilisateurs et des accès, dans l'onglet Administration.
      - Sélectionnez Calendar pour accéder aux boutons Calendriers du sous-onglet Gestion des utilisateurs et des accès, dans l'onglet Administration.
      - Sélectionnez iPoz pour accéder aux boutons Stratégies de mots de passe et Magasin d'utilisateurs du sous-onglet Gestion des utilisateurs et des accès, dans l'onglet Administration.

   b. Sélectionnez lecture pour autoriser ou refuser l'accès en lecture et écriture pour autoriser ou refuser l'accès en écriture. Si vous ne sélectionnez rien, toutes les actions sont sélectionnées.

      Remarque : Pour autoriser ou refuser l'accès en création, vous devez définir une stratégie d'accès CALM et sélectionner les ressources CA Enterprise Log Manager individuellement.

   c. Si besoin, ajoutez un filtre générique qui s'applique aux ressources sélectionnées, le cas échéant.

10. Si la stratégie est une liste de contrôle d'accès, renseignez les champs de configuration de la liste de contrôle d'accès comme suit.
    a. Sélectionnez une ressource dans la liste déroulante Ajouter une ressource, puis cliquez sur le bouton Ajouter (+).
    b. Sélectionnez lecture, écriture ou les deux pour Actions.
    c. Cliquez sur le bouton Modifier les filtres pour ouvrir le formulaire de filtre. Créez un filtre pour la ressource associée en sélectionnant ou en saisissant des valeurs pour valeur/type de gauche, valeur/type d'opérateur et valeur/type de droite.
    d. Si le filtre possède un nom de ressource pour valeur, sélectionnez la case à cocher intitulée Traiter les noms de ressources comme des expressions régulières. Sinon, cette case à cocher doit rester désélectionnée.

    Important : Définissez une stratégie pour chaque combinaison ressource/filtres.

11. Si la stratégie est une liste de contrôle d'accès des identités, renseignez les champs de configuration de la liste de contrôle d'accès des identités comme suit.
    a. Pour Type, sélectionnez l'une des options affichées. Par exemple, sélectionnez Groupe d'applications, cliquez sur le lien Recherche d'identités, puis sur le bouton Rechercher afin d'afficher les membres du type sélectionné.
    b. Sélectionnez les identités, puis cliquez sur le bouton Déplacer afin de renseigner le volet Identités sélectionnées.
    c. Pour chaque identité sélectionnée, spécifiez lecture, écriture ou les deux.

       Les actions propres aux identités s'appliquent à toutes les ressources sélectionnées. Cela signifie qu'une identité donnée peut afficher, afficher et modifier ou seulement modifier l'ensemble des ressources sélectionnées.
    d. Ajoutez les ressources pour lesquelles les actions spécifiques aux identités doivent être autorisées ou refusées.
12. Vérifiez les cases à cocher et sélectionnez celles qui s'appliquent.
    - Sélectionnez Refus explicite pour passer d'une stratégie qui autorise l'accès à une qui le refuse.
    - Sélectionnez Désactivé pour rendre temporairement inactive cette stratégie.
    - Sélectionnez Pré-déploiement, puis Affectation d'étiquettes et ajoutez les étiquettes si vous utilisez cette stratégie à des fins de test et si vous souhaitez classer les stratégies par étiquettes personnalisées.
13. Cliquez sur Enregistrer, puis sur Fermer dans le volet gauche.

Informations complémentaires :

Etape 3 : création d'une stratégie d'accès au système Win-Admin (page 119)

Création d'une stratégie basée sur une stratégie existante

Vous pouvez créer une nouvelle stratégie d'accès en copiant une stratégie d'accès existante et en modifiant cette copie. Cette procédure peut vous faire économiser le temps nécessaire à la duplication manuelle des spécifications d'une stratégie existante qui ne requiert que des modifications mineures pour répondre à vos besoins actuels.

Seuls les administrateurs peuvent créer, modifier, supprimer ou afficher des stratégies d'accès.

Pour créer une stratégie basée sur une stratégie existante

1. Cliquez sur l'onglet Administration et sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès.
3. Sélectionnez le type de stratégie que vous souhaitez utiliser en tant que modèle, CALM ou de portée.
4. Cliquez sur le lien du nom pour ouvrir la stratégie à copier.
5. Cliquez sur Enregistrer sous.

   La boîte de dialogue d'exploration s'ouvre.
6. Entrez le nom de la nouvelle stratégie qui sera basée sur la stratégie ouverte et cliquez sur OK.
7. Effectuez les modifications nécessaires.

   Par exemple, remplacez l'identité copiée par le nom du rôle (groupe d'utilisateurs d'applications défini par l'utilisateur) auquel cette stratégie s'applique. Si vous le souhaitez, modifiez les actions autorisées sur les ressources copiées. Vous pouvez aussi cliquer sur Filtres et spécifier un filtre supplémentaire pour le nouveau rôle.
8. Cliquez sur Enregistrer, puis sur Fermer.
9. Vérifiez la nouvelle définition de stratégie.
   a. Sélectionnez de nouveau le type de stratégie pour afficher une vue de toutes les stratégies.
   b. Comparez la nouvelle stratégie avec celle d'origine et vérifiez que tous les changements prévus apparaissent bien dans la nouvelle stratégie.
   c. Cliquez sur Fermer.
10. Testez la stratégie.

Informations complémentaires :

Etape 5 : création d'une stratégie basée sur la stratégie de modification et d'affichage des rapports pour les analystes (page 133)

Test d'une nouvelle stratégie

La fonction Tester les stratégies vous permet de tester une nouvelle stratégie pour déterminer si sa syntaxe est correcte. Grâce à la fonction Tester les stratégies, vous pouvez exécuter des requêtes ad hoc sur les stratégies d'accès que vous définissez. Considérez une autorisation sous la forme de la demande suivante : "{Identité} peut-il effectuer {action} sur la ressource de type {classe de ressource} portant le nom {ressource} [avec les {attributs} suivants] [au {moment spécifié}] ?" Un résultat ALLOW signifie que l'identité saisie peut effectuer l'action spécifiée sur la ressource spécifiée avec les attributs spécifiés au moment spécifié.

Avant de commencer, gardez votre stratégie à disposition.

Pour tester une stratégie

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Tester les stratégies.

   La page Paramètres de contrôle d'autorisation s'affiche.
3. Si vous aviez sélectionné Pré-déploiement et ajouté des étiquettes pour la stratégie à vérifier, sélectionnez la case à cocher qui indique que vous souhaitez inclure des stratégies de pré-déploiement et ajoutez les étiquettes associées.
4. Remplissez les champs de saisie. Si votre stratégie inclut des filtres, spécifiez-les dans l'ordre de leur apparition dans la stratégie.
5. Cliquez sur Exécuter le contrôle d'autorisation.
6. Observez le résultat et procédez de l'une des manières indiquées ci-dessous.
   - Si le résultat est ALLOW, connectez-vous à CA Enterprise Log Manager en tant qu'utilisateur spécifié comme une identité dans cette nouvelle stratégie et testez l'efficacité, la portée et la couverture de la stratégie avant de l'utiliser en production.
   - Si le résultat est DENY, vérifiez vos saisies dans la requête. Si elles sont correctes, revenez à la stratégie et apportez les corrections nécessaires.

Création d'une stratégie de groupe d'utilisateurs dynamique

Un *groupe d'utilisateurs dynamique* est composé d'utilisateurs globaux qui partagent un ou plusieurs attributs communs. Un groupe d'utilisateurs dynamique est créé par le biais d'une stratégie de groupe d'utilisateurs dynamique particulière dans laquelle le nom de la ressource est le nom du groupe d'utilisateurs dynamique et l'appartenance repose sur un ensemble de filtres configurés sur les attributs d'utilisateur et de groupe.

Vous pouvez créer un groupe dynamique composé d'utilisateurs, de groupes d'applications, de groupes globaux ou de groupes dynamiques. Par exemple, vous pouvez créer un groupe dynamique de groupes globaux ou de groupes d'applications en fonction du nom, de la description ou de l'appartenance à un groupe. De même, vous pouvez créer un groupe dynamique d'utilisateurs avec différents rôles, fondé sur un attribut commun dans leur profil d'utilisateur global, par exemple :

- le poste ;
- le département ou bureau ;
- la ville, l'état ou le pays.

Seul l'administrateur peut créer des stratégies de groupes d'utilisateurs dynamique.

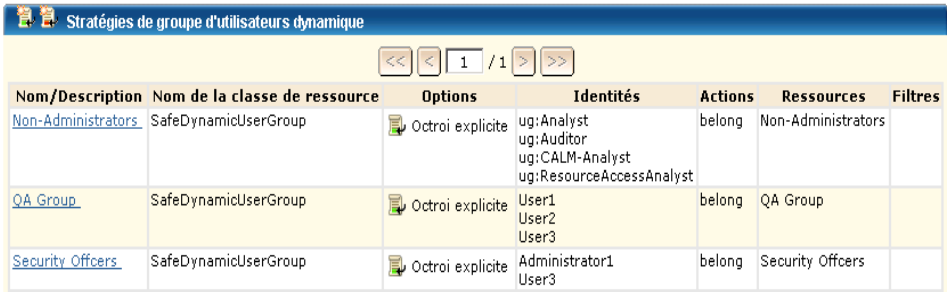
Pour créer une stratégie de groupe d'utilisateurs dynamique

1. Cliquez sur l'onglet Administration et sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès.
3. Cliquez sur Nouvelle stratégie de groupe dynamique.

   La page Nouvelle stratégie de groupe dynamique s'affiche.
4. Pour Nom, entrez un nom de groupe indiquant ce qu'il a en commun. Saisissez une description si vous le souhaitez.
5. Sélectionnez un type de stratégie. La valeur par défaut est Stratégie d'accès.

6. Sélectionnez les identités comme suit.
   a. Pour Type, sélectionnez Utilisateur, Groupe d'applications, Groupe global ou Groupe dynamique et cliquez sur Recherche d'identités.
   b. Pour Attribut, Opérateur et Valeur, saisissez l'expression qui définit les critères d'appartenance à ce groupe et cliquez sur Rechercher.

      Par exemple, si vous avez sélectionné Utilisateur, vous pouvez entrer l'expression Poste Like Manager et cliquer sur Rechercher pour trouver tous les utilisateurs occupant un poste de Manager.
   c. Dans les identités qui s'affichent, sélectionnez celles qui appartiennent à ce groupe dynamique et cliquez sur la flèche Déplacer pour déplacer vos sélections dans la zone Identités sélectionnées.
7. Pour les actions, sélectionnez "appartient".
8. Dans le champ Ajouter une ressource, entrez la valeur que vous avez saisie dans le champ Nom et cliquez sur le bouton Ajouter. Cela indique que les identités sélectionnées appartiennent à la ressource de groupe dynamique que vous venez de créer.
9. Ajoutez d'autres filtres si vous le souhaitez.
10. Cliquez sur Enregistrer.
11. Cliquez sur le lien Stratégies de groupe d'utilisateurs dynamique et vérifiez le nouveau groupe d'utilisateurs dynamique que vous avez créé. Par exemple :



Création d'un filtre d'accès

Vous pouvez créer un filtre d'accès afin de limiter l'accès aux données de journaux correspondant aux critères du filtre. Par défaut, tous les utilisateurs d'applications CA Enterprise Log Manager peuvent interroger les données de journaux d'événements des magasins de journaux d'événements du serveur CA Enterprise Log Manager actif, de serveurs pairs d'une fédération maillée ou de serveurs descendants d'une fédération hiérarchique.

Vous pouvez limiter l'accès au magasin de journaux d'événements d'un ou plusieurs serveurs CA Enterprise Log Manager spécifiques en créant un filtre d'accès aux données. Vous pouvez appliquer un filtre d'accès à un individu ou à un groupe.

Pour créer un filtre d'accès pour un rôle défini par l'utilisateur

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

   L'assistant de conception du filtre d'accès apparaît.
3. Pour Détails, entrez le nom et la description du filtre.
4. Cliquez sur Identités. Sélectionnez un type d'identité, cliquez sur Rechercher pour afficher les identités disponibles, puis utilisez le contrôle de déplacement pour sélectionner celles auxquelles s'applique ce filtre d'accès.

   Par exemple, sélectionnez le groupe d'applications que vous avez créé à cette fin.
5. Définissez les filtres d'accès.
   a. Cliquez sur Filtres d'accès.
   b. Cliquez sur le bouton Nouveau filtre d'événement.

   c. Ajoutez une ou plusieurs expressions définissant le filtre d'accès.
   d. Cliquez sur Enregistrer et fermer.

   Le filtre d'accès que vous avez créé apparaît.
6. Cliquez sur Fermer.

Informations complémentaires :

Etape 4 : création du filtre Accès aux données Win-Admin (page 123)
Création d'un groupe d'utilisateurs d'applications (rôle) (page 91)

Maintenance de comptes d'utilisateur et de stratégies d'accès

En tant qu'administrateur, vous pouvez réaliser les tâches de maintenance suivantes sur les comptes d'utilisateurs et stratégies d'accès.

- Verrouiller un compte d'utilisateur de sorte que l'utilisateur ne puisse pas se connecter à CA Enterprise Log Manager.
- Déverrouiller les comptes d'utilisateur qui ont été verrouillés, si la stratégie de mots de passe n'autorise aucun utilisateur à déverrouiller un compte d'utilisateur verrouillé.
- Ajouter de nouveaux comptes d'utilisateur.
- Modifier des comptes d'utilisateur existants.
- Verrouiller ou supprimer des comptes d'utilisateur qui appartiennent à des individus qui n'ont plus besoin d'un accès à CA Enterprise Log Manager.
- Modifier des stratégies d'accès existantes.
- Supprimer des stratégies d'accès qui ne sont plus nécessaires.
- Créer, modifier ou supprimer des stratégies de délégation.
- Créer, modifier ou supprimer des filtres d'accès avec leurs stratégies d'obligation automatiquement générées.
- Créer un "super rôle" à partir de rôles existants avec un accès limité.
- Ajouter un nouveau rôle personnalisé et les stratégies d'accès correspondantes.

Création d'un calendrier

Vous pouvez créer un nouveau calendrier pour restreindre l'accès des utilisateurs pendant certaines périodes. Les calendriers font partie intégrante des stratégies d'accès. Lorsque vous définissez un calendrier, vous pouvez inclure ou exclure des plages de temps en heures, en jours de la semaine ou par dates.

Pour créer un calendrier

1. Cliquez sur l'onglet Administration, cliquez sur Gestion des utilisateurs et des accès, puis cliquez sur le bouton Calendriers.

   La page Calendriers s'affiche.

2. Cliquez sur l'icône Nouveau calendrier, en haut à gauche de la liste des calendriers.

   Le volet des détails Nouveau calendrier s'affiche.

3. Entrez un nom spécifiant la stratégie cible et décrivez l'usage prévu.
4. Utilisez les icônes de calendrier pour définir des dates de début et de fin pour le calendrier.
5. Cliquez sur Ajouter une plage de temps à inclure ou Ajouter une plage de temps à exclure pour créer des périodes d'exception au sein de la période principale d'activité du calendrier.
6. Cliquez sur Enregistrer, puis sur Fermer.

Informations complémentaires

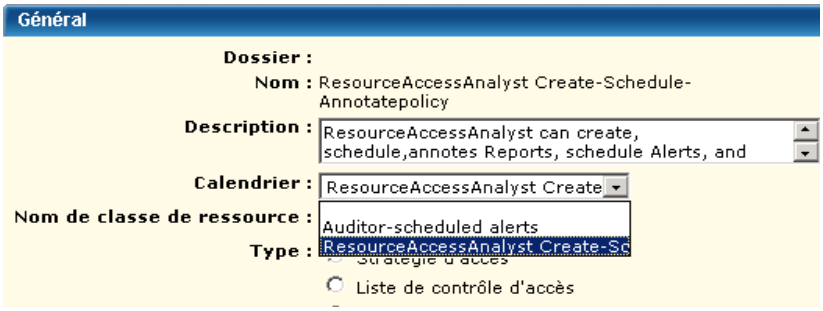
Ajout d'un calendrier à une stratégie (page 108)

Ajout d'un calendrier à une stratégie

Lors de la création d'une stratégie, vous pouvez sélectionner un calendrier existant qui indique à quel moment les identités spécifiées peuvent effectuer les actions sélectionnées sur les ressources spécifiées. Un calendrier peut définir des dates de début et de fin ainsi que des plages de temps en heures ou en jours de la semaine.

Pour ajouter un calendrier à une stratégie

1. Cliquez sur l'onglet Administration et sur le sous-onglet Gestion des utilisateurs et des accès.
2. Ouvrez la stratégie à laquelle ce calendrier s'applique.
   a. Cliquez sur Stratégies d'accès.
   b. Sélectionnez le type de stratégie.
   c. Sélectionnez la stratégie.
3. Ouvrez la liste déroulante Calendrier et sélectionnez le calendrier que vous avez créé pour cette stratégie.



4. Cliquez sur Enregistrer pour enregistrer l'ajout du calendrier à une stratégie existante.

Informations complémentaires :

Création d'un calendrier (page 106)

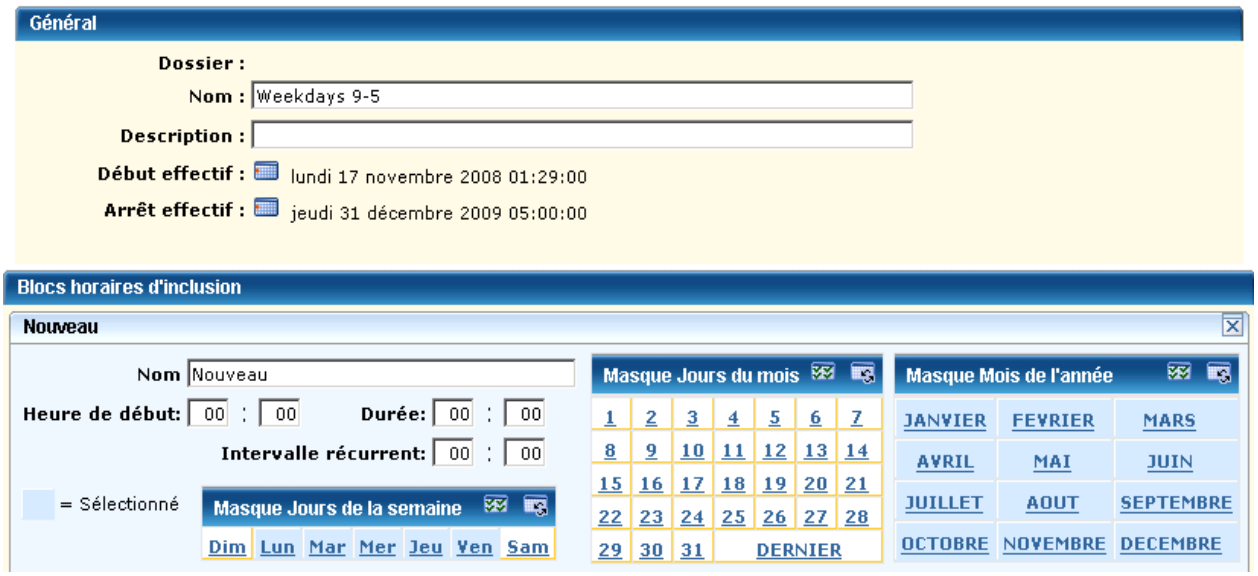
Exemple : Accès limité aux jours ouvrables

Vous pouvez limiter les plages d'accès à CA Enterprise Log Manager autorisées pour un groupe d'utilisateurs, par exemple à un horaire ou un jour donné, en créant un calendrier d'accès, un rôle personnalisé, une nouvelle stratégie basée sur la stratégie d'accès CA Enterprise Log Manager, puis en affectant le calendrier et le rôle personnalisé à cette stratégie.

Exemple : Accès CA Enterprise Log Manager limité aux jours ouvrés pour les auditeurs externes

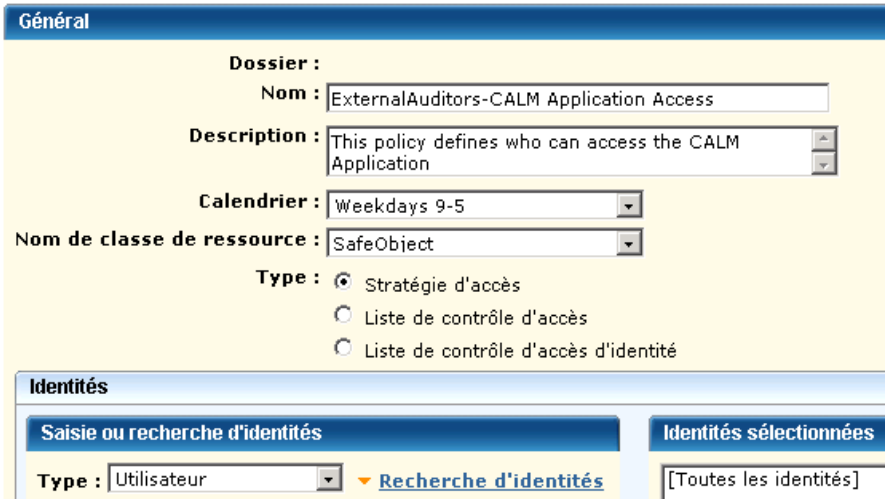
Pour limiter l'accès CA Enterprise Log Manager de certains groupes d'utilisateurs aux jours ouvrés, créez un calendrier pour les jours ouvrés et ajoutez-le aux stratégies d'accès spécifiques aux auditeurs.

Par exemple, si vous souhaitez que les auditeurs externes puissent accéder à CA Enterprise Log Manager uniquement durant les heures de bureau, créez un calendrier spécifiant les jours ouvrés, du lundi au vendredi, de 9 h 00 à 17 h 00, pour tous les mois de l'année.



Créez un rôle pour les auditeurs externes.

Ouvrez la stratégie de portée Accès aux applications CALM, puis enregistrez-la sous le nom AuditeursExternes-Accès aux applications CALM, sélectionnez le calendrier Jours ouvrés 9-5, puis sélectionnez le groupe d'utilisateurs Auditeurs externes comme identité.



Important : Utilisez la fonction Calendrier uniquement avec les stratégies d'octroi d'accès, mais pas avec les stratégies d'interdiction d'accès.

Informations complémentaires :

Création d'un calendrier (page 106)
Création d'un groupe d'utilisateurs d'applications (rôle) (page 91)
Création d'une stratégie basée sur une stratégie existante (page 101)
Ajout d'un calendrier à une stratégie (page 108)

Exportation de stratégies d'accès

Vous pouvez exporter toutes les stratégies d'un type sélectionné à tout moment, à la fois les stratégies prédéfinies et les stratégies personnalisées. L'exportation de stratégies est un bon moyen de maintenir à jour une sauvegarde.

Une exportation crée un fichier XML pour chaque stratégie sélectionnée, tous les fichiers XML étant compressés dans un fichier nommé CAELM[1].xml.gz.

Pour exporter des stratégies d'accès

1. Cliquez sur l'onglet Administration et sur le sous-onglet Gestion des utilisateurs et des accès.
2. Cliquez sur Stratégies d'accès.
3. Sélectionnez le type de stratégie d'accès à exporter et cliquez sur Exporter.

   La boîte de dialogue Téléchargement de fichier s'ouvre.
4. Cliquez sur Enregistrer et enregistrez le fichier sous un nom unique.
5. Cliquez sur Fermer.

Informations complémentaires :

Sauvegarde de toutes les stratégies d'accès (page 65)

Suppression d'une stratégie personnalisée

Vous pouvez supprimer une stratégie personnalisée pour l'une des raisons suivantes.

- Vous avez enregistré la stratégie sous un nom différent et ne prévoyez pas d'appliquer d'autres modifications ; vous pouvez donc supprimer la copie en double.
- Il n'existe plus d'appartenance active au sein des identités définies pour la stratégie ; celle-ci est donc inutile.

Important : Veillez à ne jamais supprimer une stratégie prédéfinie. Si cela se produit, vous ne pourrez la restaurer que si vous avez exporté une sauvegarde.

Pour supprimer une stratégie personnalisée

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

3. Sélectionnez le type de stratégie que vous souhaitez supprimer, CALM ou de portée.
4. Cliquez sur le nom de la stratégie à supprimer.
5. Cliquez sur Supprimer.
6. Cliquez sur OK pour confirmer la suppression.

Suppression d'un filtre d'accès et de sa stratégie d'obligation

Vous pouvez supprimer un filtre d'accès et la stratégie d'obligation générée par le filtre pour supprimer la restriction d'accès aux données.

Ne supprimez pas la stratégie d'obligation générée par le filtre des Stratégies d'accès.

Pour supprimer un filtre d'accès et sa stratégie d'obligation

1. Cliquez sur l'onglet Administration, puis sur Gestion des utilisateurs et des accès.

   La Liste des filtres d'accès apparaît en haut du volet gauche.

2. Sélectionnez le filtre à supprimer et cliquez sur le bouton Supprimer le filtre d'accès.

   Le message d'avertissement Confirmation de la suppression du filtre d'accès apparaît.

3. Cliquez sur Oui pour supprimer le filtre d'accès sélectionné et la stratégie d'obligation associée.

Exemple : Autorisation de gestion des archives par un non-administrateur

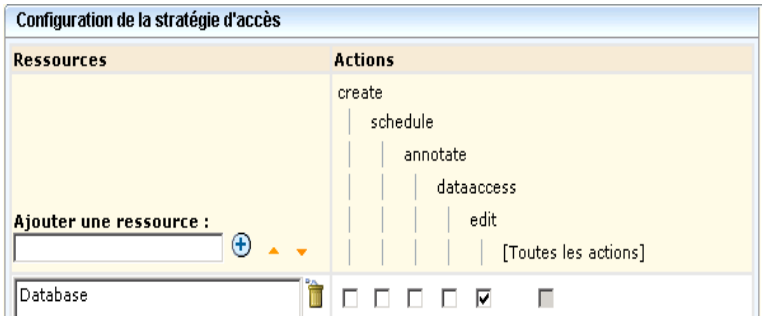
Imaginons que vous souhaitiez autoriser un groupe non administrateur à gérer l'archivage automatique. Vous pouvez créer un groupe appelé AdministrateurArchive et une stratégie CALM autorisant l'action de modification des ressources de base de données. Cela permet un accès en lecture au catalogue d'archive des bases de données à des fins de requête, un accès en écriture au catalogue d'archive à des fins de recatalogage et la capacité à faire appel à l'utilitaire LMArchive à des fins d'archivage manuel ou au script shell restore-ca-elm à des fins de restauration de bases de données archivées automatiquement.

Pour autoriser des non-administrateurs à gérer l'archivage

1. Créez un rôle appelé AdministrateurArchive.
    a. Sélectionnez l'onglet Administration, puis le sous-onglet Gestion des utilisateurs et des accès.
    b. Sélectionnez Groupes.
    c. Cliquez sur Nouveau groupe d'applications.
    d. Entrez AdministrateurArchive comme nom.
    e. Cliquez sur Enregistrer.

       Le groupe d'applications, ou rôle, AdministrateurArchive est créé.
    f. Cliquez sur Fermer.

2. Créez une stratégie CALM pour autoriser l'accès et la modification des ressources de base de données.
   a. Cliquez sur Stratégies d'accès.
   b. Cliquez sur Nouvelle stratégie d'accès pour créer une nouvelle stratégie CALM.
   c. Saisissez AdministrateurArchive dans le champ Nom.
   d. AdministrateurArchive peut exécuter l'utilitaire LMArchive et le script shell restore-ca-elm pour la description.
   e. Dans Identités, sélectionnez Groupe d'applications comme Type, cliquez sur Recherche d'identités, puis cliquez sur Rechercher.
   f. Sélectionnez AdministrateurArchive, puis cliquez sur la flèche de déplacement.
   g. Saisissez Base de données dans Ajouter une ressource, puis cliquez sur Ajouter.
   h. Sélectionnez Modifier comme Action.



   i. Cliquez sur Enregistrer. Cliquez sur Fermer.

3. Testez la stratégie et vérifiez que le résultat est bien ALLOW.

Résultat	Stratégie	Délégateur	Identité	Classe de ressource	Ressource	Action
AUTORISER	ArchiveAdministrator		ug:ArchiveAdministrator	CALM	Database	edit

4. Octroyez au rôle AdministrateurArchive le droit de se connecter à CA Enterprise Log Manager.
   a. Cliquez sur CALM sous Stratégies d'accès.
   b. Sélectionnez Accès aux applications CALM.
   c. Sous Identités, recherchez le groupe d'applications AdministrateurArchive et déplacez-le dans la zone Identités sélectionnées.

   d. Cliquez sur Enregistrer. Cliquez sur Fermer. Cliquez sur Fermer.

      L'onglet Gestion des utilisateurs et des accès s'affiche, les boutons dans le volet gauche.

5. Affectez le rôle AdministrateurArchive à un ou plusieurs utilisateurs.
   a. Cliquez sur Utilisateurs.
   b. Dans le champ Valeur sous Rechercher des utilisateurs, saisissez le nom d'une personne à laquelle vous souhaitez affecter ce rôle, puis cliquez sur OK.

      Le nom d'utilisateur sélectionné apparaît sous le dossier Utilisateurs.
   c. Sélectionnez le lien pour l'utilisateur sélectionné.
   d. Cliquez sur Ajouter les détails de l'utilisateur de l'application.
   e. Placez AdministrateurArchive dans la liste Groupes d'utilisateurs sélectionnés.

f. Cliquez sur Enregistrer. Cliquez sur Fermer.

g. Répétez la procédure pour chaque utilisateur auquel vous souhaitez affecter ce rôle.

h. Cliquez sur Fermer.

6. Passez en revue les résultats renvoyés par CA Enterprise Log Manager (facultatif).

   a. Cliquez sur Déconnexion pour vous déconnecter en tant qu'administrateur.

   b. Connectez-vous avec le nom d'utilisateur auquel vous avez affecté le rôle AdministrateurArchive.

   c. Cliquez sur l'onglet Administration, sous-onglet Collecte de journaux.

   d. Sélectionnez Requête de catalogue d'archive.

   e. Notez que vous utilisez les boutons Requête et Recataloguer.

7. Exécutez le script de restauration restore-ca-elm avec les informations d'identification de l'utilisateur défini sous le rôle AdministrateurArchive, afin de vérifier que la stratégie fonctionne comme prévu (facultatif).

Informations complémentaires :

Restauration des fichiers archivés automatiquement (page 185)

Restriction d'accès pour un utilisateur : scénario de l'administrateur Windows

Vous pouvez limiter les rapports que les utilisateurs peuvent afficher à ceux possédant une balise spécifiée. Vous pouvez limiter les données que les utilisateurs peuvent afficher dans ces rapports aux données générées à partir de sources d'événements spécifiées. La limitation de l'accès aux rapports associés à une balise donnée s'effectue par le biais d'une stratégie d'accès. La limitation de l'accès aux données pour des événements renvoyés à un serveur CA Enterprise Log Manager particulier s'effectue par le biais d'un filtre d'accès. Avec un filtre d'accès défini, l 'affectation d'un rôle est facultative. Vous pouvez donc créer un nouvel utilisateur, ne lui affecter aucun rôle et limiter son accès aux données à l'aide d'un filtre d'accès.

Prenons le cas de l'entreprise ABC avec ses quatre centres de données aux Etats-Unis. L'administrateur souhaite attribuer à l'administrateur Windows de la région de Houston un accès en lecture aux événements Windows traités par le contrôleur de domaine de la zone Houston. Les événements Windows traités par le serveur CA Enterprise Log Manager installé sur le contrôleur de domaine Houston sont envoyés depuis les sources sur lesquelles les noms d'hôtes commencent par la chaîne ABC-HOU-WDC.

Cet exemple vous guide dans la création d'un utilisateur appelé Win-Admin, qui ne doit pouvoir afficher que les rapports avec une balise Accès au système, les données de ces rapports étant limitées aux événements issus de sources d'événements portant des noms d'hôtes commençant par la convention d'attribution de nom connue.

L'exemple fourni détaille chacune des étapes ci-dessous.

1. Créez le nouvel utilisateur Win-Admin.
2. Attribuez au rôle Win-Admin un accès de base à CA Enterprise Log Manager. Ajoutez cette identité à la stratégie d'accès aux applications CALM.
3. Limitez l'accès de Win-Admin aux seuls rapports avec une balise Accès au système. Créez une stratégie de portée avec accès en lecture à AppObject grâce à des filtres qui spécifient le dossier EEM dans lequel les rapports sont stockés et qui exigent que calmTag soit égal à Accès au système. Testez la stratégie.
4. Limitez les données que Win-Admin peut afficher à celles générées par le contrôleur de domaine dans la région de Win-Admin. Créez un filtre d'accès, nommé Accès aux données Win-Admin, qui limite les données de requêtes et de rapports que Win-Admin peut afficher aux événements Windows issus de sources d'événements portant un nom d'hôte commençant par ABC-HOU-WDC.
5. Connectez-vous à CA Enterprise Log Manager en qualité d'utilisateur Win-Admin et évaluez l'accès accordé par les stratégies.
6. Si l'accès est trop limité pour permettre à l'utilisateur d'effectuer les tâches voulues, étendez-le à l'aide de stratégies supplémentaires.

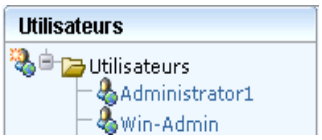
Etape 1 : création de l'utilisateur Win-Admin

Vous pouvez créer un utilisateur sans rôle (groupe d'applications) si vous spécifiez l'accès aux données à l'aide d'un filtre d'accès.

La première étape de la procédure complète visant à restreindre l'accès aux données de cette manière consiste à créer l'utilisateur.

Vous devez créer un utilisateur uniquement si le compte d'utilisateur global n'est pas disponible pour l'importation depuis un répertoire externe. Lors de la création de ce type de compte, n'ajoutez pas les détails de l'utilisateur de l'application. Dans notre scénario d'exemple, Win-Admin est le nom de l'utilisateur.

Si vous faites une recherche sur les utilisateurs, le nouveau nom apparaît dans la liste.



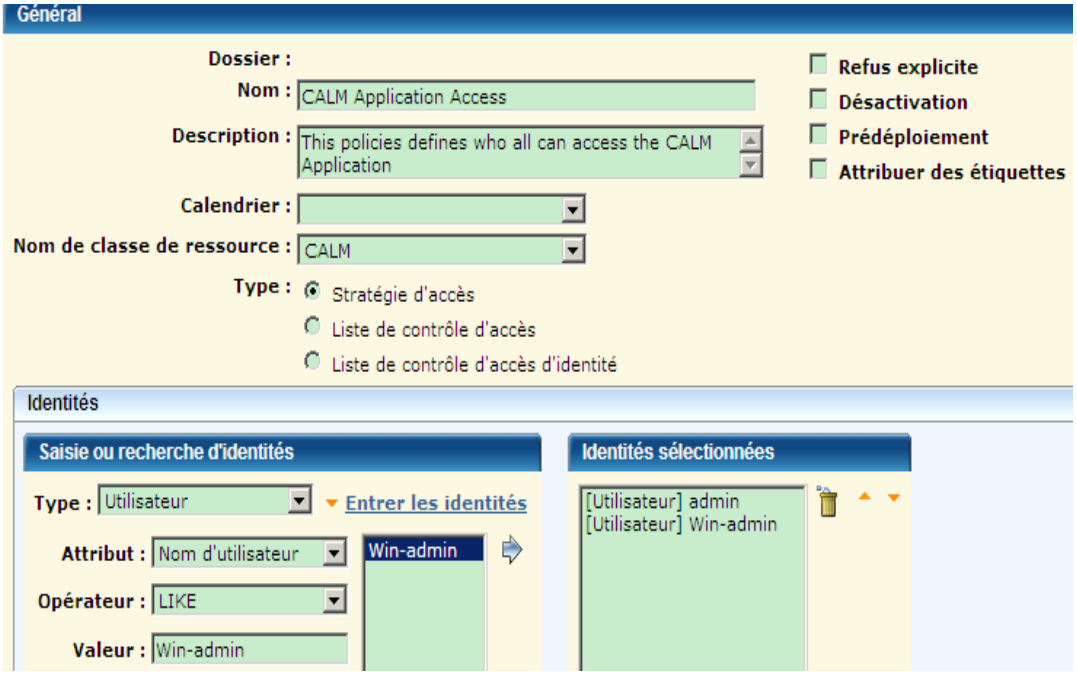
Informations complémentaires

Création d'un utilisateur global (page 43)

Etape 2 : ajout de Win-Admin à la stratégie d'accès aux applications CALM

La deuxième étape de la procédure visant à restreindre l'accès aux données d'un utilisateur nommé Win-Admin consiste à accorder à cette identité un accès à l'application CA Enterprise Log Manager.

Ajoutez le nouvel utilisateur à la stratégie d'accès aux applications CALM. Il s'agit de la même procédure que pour accorder un accès à CA Enterprise Log Manager à un nouveau rôle, à ceci près que la valeur Utilisateur doit être spécifiée pour le champ Type lors de la recherche d'identités.



Informations complémentaires :

Attribution d'un accès de rôle personnalisé à CA Enterprise Log Manager (page 92)

Etape 3 : création d'une stratégie d'accès au système Win-Admin

L'étape 2 accorde un accès pour se connecter à l'application CA Enterprise Log Manager.

L'étape 3 limite l'accès à l'application CA Enterprise Log Manager après la connexion. Au niveau le plus large, vous pouvez accorder un accès en lecture seule ou un accès en lecture et en écriture aux identités spécifiées.

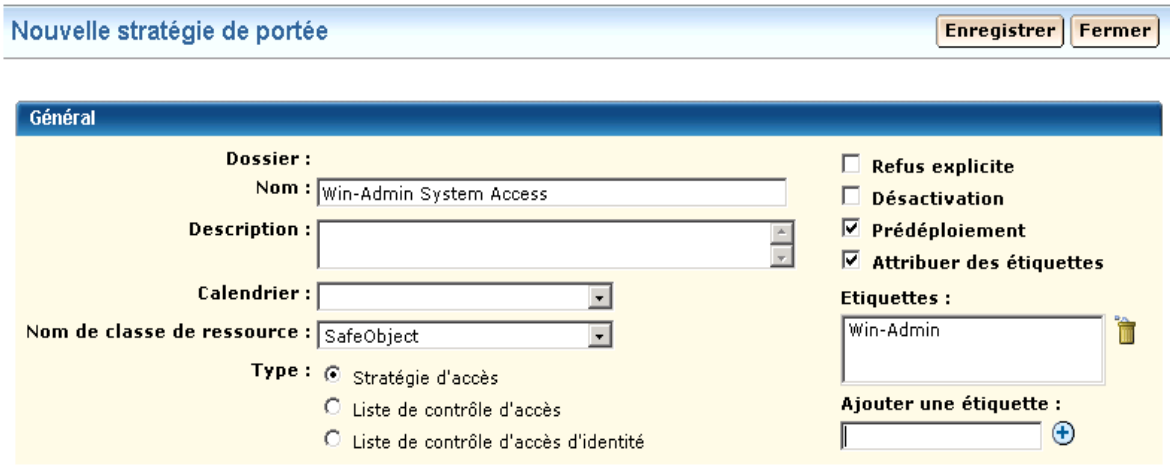
Le choix du type de stratégie détermine ensuite la granularité à laquelle vous pouvez spécifier les actions autorisées.

- Les stratégies d'accès autorisent les actions sélectionnées sur les ressources sélectionnées concernées.
- Les stratégies de type Liste de contrôle d'accès vous permettent de spécifier les actions autorisées sur chaque ressource ajoutée.
- Les stratégies du type Liste de contrôle d'accès des identités vous permettent de spécifier les actions qui sont autorisées sur les ressources concernées pour chaque identité.

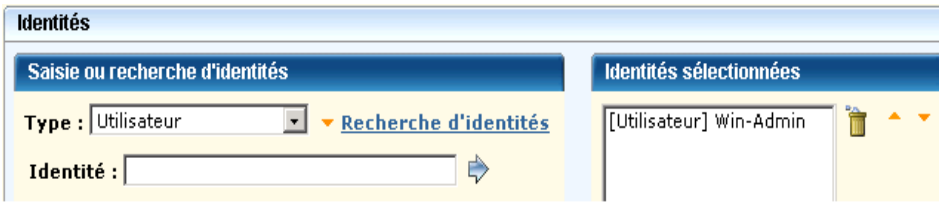
Vous pouvez autoriser un accès limité à une ressource en créant un filtre qui spécifie le dossier EEM pour cette ressource, puis en spécifiant des restrictions sur ce dossier.

L'exemple ci-dessous explique comment restreindre l'accès de manière générale aux seules opérations de lecture, avec des restrictions supplémentaires sur une fonction spécifique. Plus précisément, l'étape 3 limite l'accès de l'utilisateur Win-Admin à l'affichage des rapports d'accès au système. L'exemple suivant montre comment créer une stratégie de portée appelée Accès au système Win-Admin, qui accorde un accès en lecture à SafeObject, AppObject et spécifie des filtres qui limitent l'accès aux seuls rapports possédant la balise Accès au système. Il indique également comment tester la stratégie et, après cette vérification, comment supprimer le paramètre de pré-déploiement.

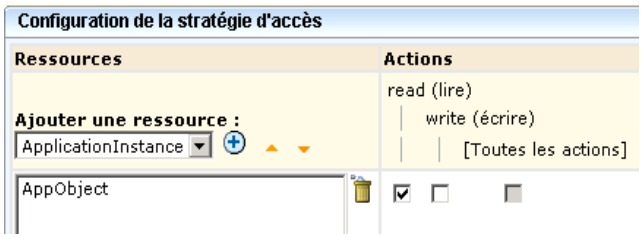
La zone Général d'une stratégie de portée conçue pour spécifier un accès en lecture seule ou en lecture/écriture aux applications spécifie SafeObject en tant que nom de classe de ressource. La stratégie de l'exemple qui suit porte le nom "Accès au système Win-Admin". Il est recommandé de sélectionner l'option Pré-déploiement pour une nouvelle stratégie tant que vous ne l'avez pas testée ou que vous n'en êtes pas suffisamment satisfait pour l'utiliser dans un environnement de production.



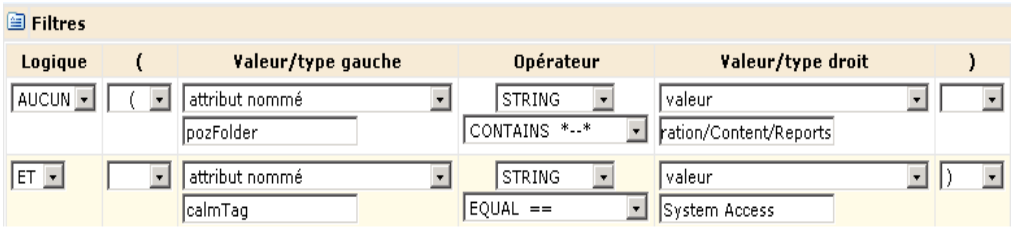
Vous pouvez accorder un accès à des utilisateurs ou à des groupes. Dans cet exemple, l'accès est accordé au nouvel utilisateur Win-Admin.



Le plus haut niveau de stratégie créé pour CA Enterprise Log Manager est la stratégie d'accès à CALM, CAELM étant l'instance de l'application. Cette stratégie de portée autorise un accès en lecture aux objets d'application, AppObject, faisant référence à l'ensemble des fonctions de l'application.

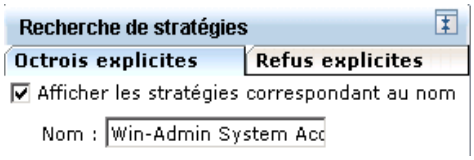


Vous pouvez ajouter des limites aux actions autorisées sur tous les objets en définissant des filtres. Les filtres sont souvent définis par paires, dans lesquelles le premier filtre spécifie le dossier CA EEM dans lequel les données liées à une fonction particulière sont stockées et le deuxième filtre fait porter une restriction sur les objets se trouvant à cet emplacement. Dans l'exemple suivant, le premier filtre limite l'accès du dossier CA EEM au dossier dans lequel la ressource rapports est stockée. Plus précisément, il spécifie que le dossier pozFolder contient /CALM_Configuration/Content/Reports. Le deuxième filtre limite l'accès aux rapports associés à la balise Accès au système en spécifiant que calmTag doit être égal à Accès au système.

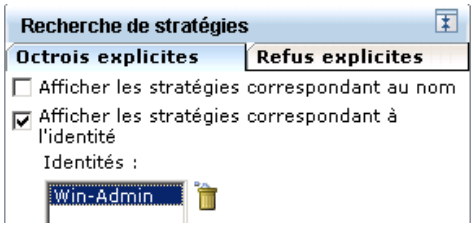


Une fois la stratégie enregistrée, vous pouvez la rechercher afin de la vérifier. Vous pouvez rechercher des stratégies par nom, identité ou ressource. Vous pouvez entrer une valeur partielle. Vous pouvez également entrer plusieurs critères. Des exemples sont fournis ci-après.

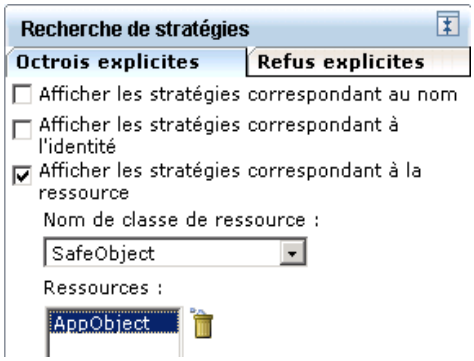
Une recherche sur le nom complet affiche la seule stratégie dont vous avez besoin.



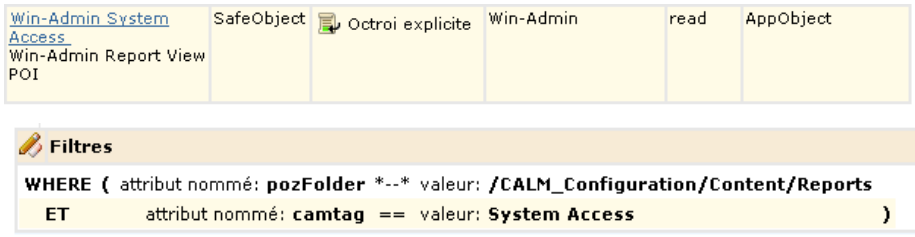
Une recherche par identité uniquement affiche toutes les stratégies qui s'appliquent à cette identité, y compris celles qui s'appliquent à toutes les identités.



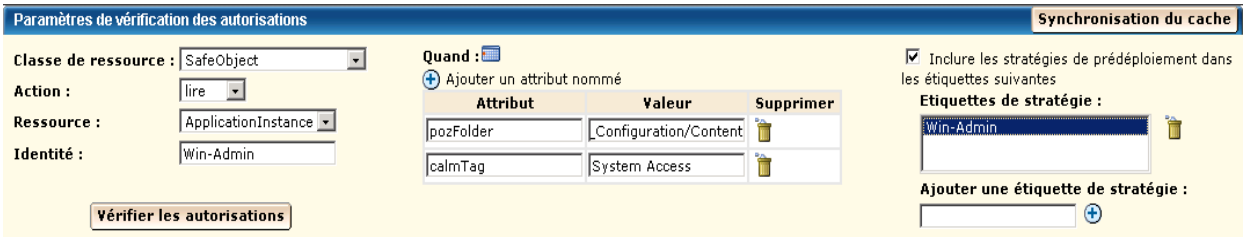
Une recherche par ressource uniquement, où la ressource est AppObject, affiche toutes les stratégies personnalisées et fournies par le système qui accordent un accès en lecture ou en lecture/écriture à toute identité.



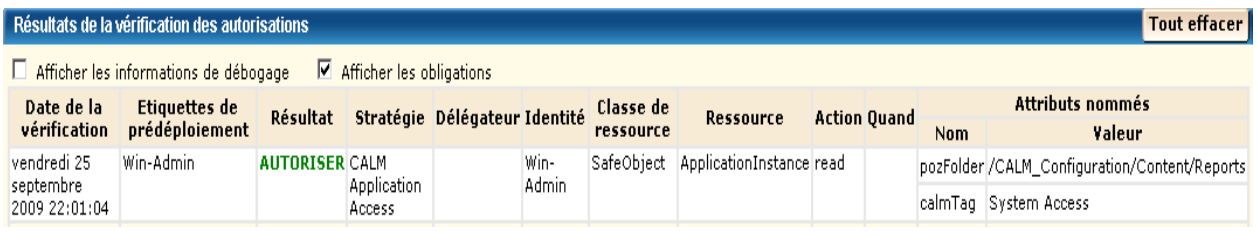
Lorsque la stratégie personnalisée que vous recherchez s'affiche dans le tableau des stratégies, examinez les valeurs, y compris les filtres. Si vous remarquez un élément à corriger, vous pouvez cliquer sur le lien du nom pour afficher la stratégie en mode d'édition.



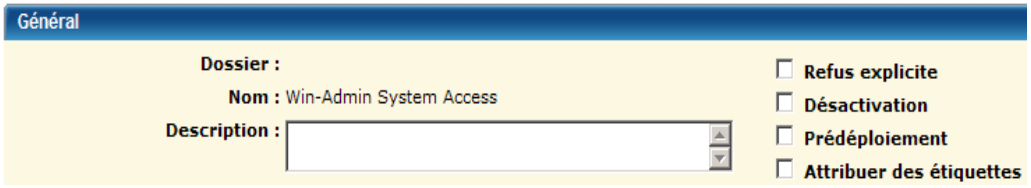
Il est recommandé de tester toute nouvelle stratégie. Assurez-vous d'entrer les paires attribut/valeur dans l'ordre de saisie des filtres, avec l'attribut du niveau le plus élevé en premier.



Vérifiez que le résultat est ALLOW.



Après avoir vérifié que le résultat est ALLOW, désélectionnez le paramètre Pré-déploiement de la stratégie. Dans le cas contraire, vous ne pourrez plus vous connecter sous l'identité Win-Admin pour évaluer les actions accessibles à cet utilisateur.



Informations complémentaires

Test d'une nouvelle stratégie (page 102)

Etape 4 : création du filtre Accès aux données Win-Admin

L'étape 3 limite l'accès de l'utilisateur Win-Admin à l'affichage des rapports d'accès au système. Ce niveau d'accès permet à l'utilisateur Win-Admin d'afficher les rapports d'accès au système pour les quatre zones géographiques de l'entreprise ABC.

L'étape 4 crée un filtre d'accès pour limiter les données que l'utilisateur Win-Admin peut afficher aux rapports d'accès au système pour le contrôleur de domaine Houston.

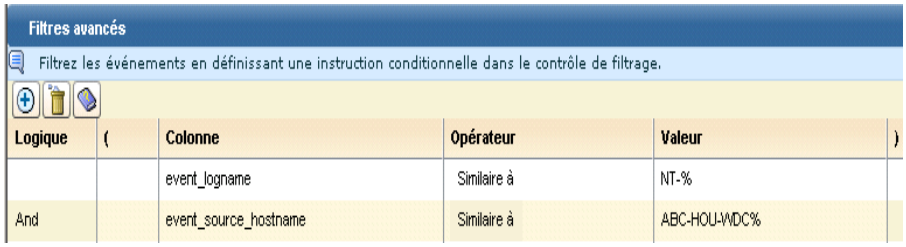
La création d'un filtre d'accès aux données commence par l'attribution d'un nom. Le nom utilisé dans ce scénario est Accès aux données Win-Admin.

Vous spécifiez les identités auxquelles le filtre d'accès s'applique dans la zone Identités. Un filtre peut s'appliquer à des utilisateurs ou groupes. Dans ce scénario, ce filtre d'accès s'applique uniquement à l'utilisateur Win-Admin.

Pour Filtres d'accès, chaque condition doit être définie en termes de valeur pour une colonne CEG. Les valeurs suivant l'opérateur LIKE peuvent contenir l'un des caractères génériques ci-après.

- _ (caractère de soulignement) : représente un seul caractère.
- % (symbole de pourcentage) : représente une chaîne contenant tout nombre de caractères.

Le premier filtre pour ce scénario tire parti du fait que tous les événements Windows portent le préfixe NT-. Pour limiter les données aux événements Windows, vous pouvez préciser que les données de la colonne CEG event_logname doivent inclure la chaîne NT-%. Pour limiter encore les événements Windows aux seuls événements d'un contrôleur de domaine spécifique, cet exemple précise que les données event_source_hostname doivent inclure une chaîne respectant les conventions locales. La valeur ABC-HOU-WDC% est basée sur la convention d'attribution de nom suivante : il s'agit d'un nom contenant des tirets et composé d'abréviations pour l'entreprise, la région et le préfixe du type de contrôleur de domaine.



Remarque : En l'absence de sources d'événements respectant une convention d'attribution de nom normalisée, vous pouvez créer une liste de valeurs à clés avec les noms d'hôtes event_source_hostname souhaités et utiliser le nom de cette liste de valeurs à clés en tant que valeur.

Avec seulement deux filtres et la logique AND, l'utilisation de parenthèses n'est pas obligatoire. Si vous entrez une expression complexe, comme celle qui suit, les parenthèses sont requises.

(event_logname like NT-%
And event_source_hostname=ABC-%)
Or (event_logname like CALM-%
And event_source_hostname=XYZ-%)

Lorsque vous enregistrez un filtre d'accès aux données, son nom s'affiche dans la liste des filtres d'accès.

Une recherche des stratégies correspondant au nom d'utilisateur Win-Admin affiche les trois stratégies pour toutes les identités plus trois autres : la stratégie d'accès aux applications CALM à laquelle Win-Admin a été ajouté, la stratégie d'accès au système Win-Admin créée en partant de zéro et la stratégie de données automatiquement ajoutée lorsque vous définissez un filtre d'accès. La stratégie de données est répertoriée en premier ci-dessous. Vous pouvez également l'afficher sous Stratégies d'obligation. Vous ne créez jamais des stratégies d'obligation directement avec CA Enterprise Log Manager.

Stratégies d'accès

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Octroi explicite	ug:Administrator ug:Analyst ug:Auditor Win-Admin	read write	ApplicationInstance AppObject Policy User GlobalUser
49aea1da-caelm54abaf7fc-8876c80-34 **Etiquettes :** DataPolicy	SafeObligation	Octroi explicite	Win-Admin	FulfillOnGrant	dataaccess/CALM/Data
Win-Admin System Access **Etiquettes :** Win-Admin	SafeObject	Octroi explicite Prédéploiement	Win-Admin	read	AppObject

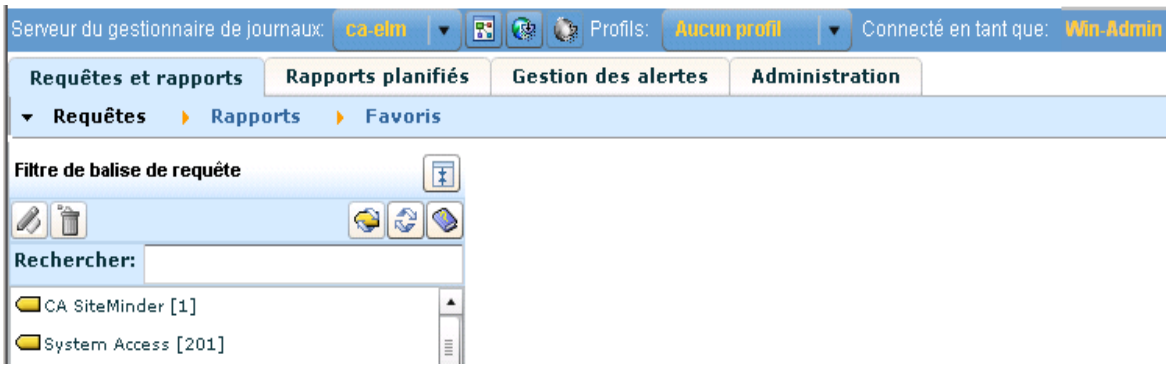
Informations complémentaires

Création d'un filtre d'accès (page 105)

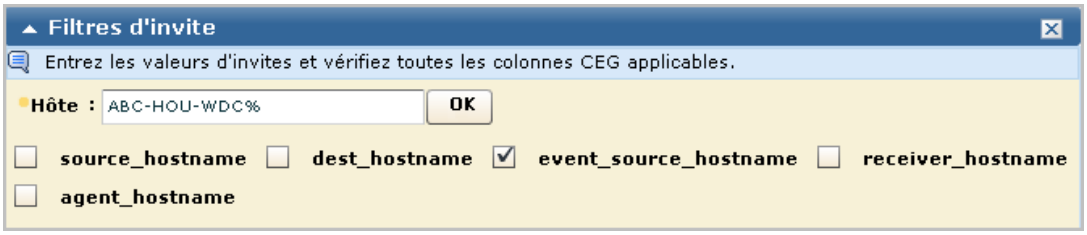
Etape 5 : connexion en tant qu'utilisateur Win-Admin

Avant de créer des stratégies pour un utilisateur ou un groupe d'utilisateurs d'applications donné, connectez-vous sous cette identité (utilisateur ou membre du groupe en question) pour déterminer ce que vous pouvez faire ou non. Premièrement, vérifiez que les restrictions attendues fonctionnent bien. Deuxièmement, assurez-vous que vous pouvez effectuer les tâches attribuées à ce type d'utilisateur.

Dans ce scénario, vous êtes censé pouvoir afficher uniquement les rapports ou alertes d'action associés à la balise Accès au système. Dans l'exemple, le seul filtre de balise de requête disponible est Accès au système. Vos attentes sont donc confirmées.



Une manière rapide de tester un filtre d'accès consiste à utiliser la fonction d'invites. Cette fonction n'est toutefois pas accessible à l'utilisateur Win-Admin. Toutes les requêtes d'invite possèdent la balise Visionneuse d'événements. L'accès aux filtres d'invite peut être accordé avec le filtre de stratégie calmTag=Visionneuse d'événements.



Le meilleur moyen de tester un filtre d'accès consiste à passer en revue les données affichées dans un rapport. Considérez le filtre d'accès suivant. La colonne CEG event_logname commence par NT- et la colonne CEG event_source_hostname commence par ABC-HOU-WDC, une abréviation de l'entreprise ABC, du site Houston et du contrôleur de domaine Windows.

event_logname Like NT-% AND event_source_hostname Like ABC-HOU-WDC%

L'exemple suivant affiche un rapport visible par l'utilisateur auquel ce filtre d'accès s'applique. Notez que les données de la colonne Nom du journal commencent par NT- et que les données de la colonne Source commencent par ABC-HOU-WDC.

System Access - All Events

Sévérité	Date	Source	Utilisateur	Action	Nom du journal	Catégorie
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informations	Mer. 21 oct. 2009 4:58:42	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management

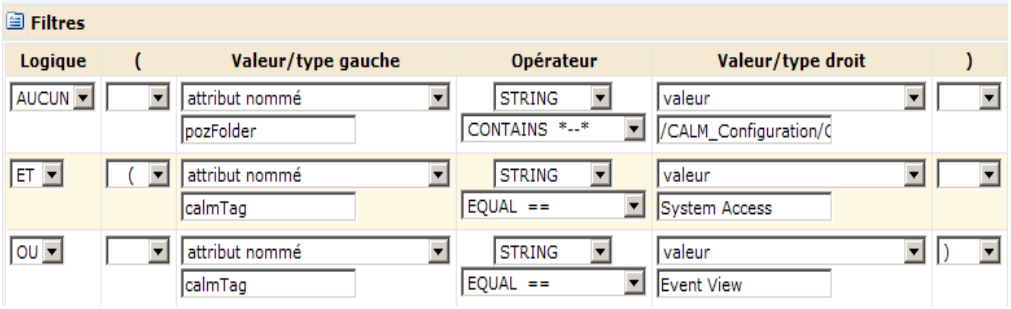
Etape 6 : extension des actions autorisées

Les stratégies et le filtre d'accès définis aux étapes 2, 3 et 4 de cet exemple permettent à l'utilisateur Win-Admin d'afficher les rapports associés à la balise Accès au système, avec certaines limites portant sur les données. Ce seul accès ne permet pas à l'utilisateur Win-Admin de planifier un rapport ou une alerte, ou encore d'annoter un rapport. Pour effectuer ces actions, ajoutez Win-Admin à la stratégie d'accès au serveur de rapports pour les auditeurs et les analystes et à la stratégie de création, de planification et d'annotation des analystes. Vous trouverez ci-dessous un exemple de ces stratégies après ajout de Win-Admin.

Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	Octroi explicite	ug:Analyst ug:Auditor Win-Admin	read	AppObject
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	Octroi explicite	ug:Analyst Win-Admin	create schedule annotate	Report Alert Tag Profile

Pour que Win-Admin puisse créer un rapport, un accès en écriture doit être préalablement ajouté à la stratégie Accès au système Win-Admin. Pour cela, il est nécessaire d'ouvrir la stratégie Accès au système Win-Admin en mode d'édition et d'ajouter des droits d'écriture pour les actions autorisées.

Pour que Win-Admin puisse utiliser les invites, le filtre de la stratégie Accès au système Win-Admin peut être modifié en spécifiant que l'attribut calmTag doit être égal soit à Accès au système, soit à Visionneuse d'événements.



Restriction d'accès pour un rôle : scénario PCI-Analyst

Vous pouvez créer un rôle similaire à un rôle prédéfini et élaborer rapidement des stratégies inspirées de stratégies prédéfinies. Le rôle défini par l'utilisateur peut être similaire au rôle prédéfini dans la mesure où il fournit un accès identique aux mêmes types de ressources, mais différent dans la mesure où il limite l'accès en fonction d'un filtre non présent dans le rôle prédéfini. Il peut exister plusieurs stratégies auxquelles ce rôle prédéfini a été ajouté en tant qu'identité. Si la configuration d'une stratégie est telle qu'elle s'applique à votre nouveau rôle, il vous suffit d'ajouter le nouveau rôle à la stratégie existante. Si la configuration est telle que vous devez modifier le type, les ressources, les actions ou les filtres, vous pouvez créer une nouvelle stratégie à partir d'une copie de celle existante.

L'exemple qui suit détaille la création d'un rôle pour un analyste qui doit intervenir uniquement sur les rapports associés à une balise PCI. La stratégie liée à ce rôle est créée à partir d'une copie d'une stratégie existante pour tous les analystes.

La procédure est énumérée ci-dessous.

1. Planifiez les stratégies dont vous avez besoin. Commencez par identifier les stratégies existantes à exploiter pour le nouveau rôle.
2. Créez le nouveau groupe d'utilisateurs (rôle) d'applications, PCI-Analyst.
3. Attribuez au rôle PCI-Analyst un accès de base à CA Enterprise Log Manager. Ajoutez cette identité à la stratégie d'accès aux applications CALM.
4. Attribuez au rôle PCI-Analyst le même accès aux serveurs de rapports et la même capacité de créer des rapports que possèdent les analystes. Ajoutez l'identité PCI-Analyst aux stratégies identifiées.
5. Limitez l'accès aux seuls rapports associés à la balise PCI calmTag. Utilisez la stratégie qui permet d'afficher et de modifier des rapports en tant que modèles à modifier.
6. Affectez le rôle PCI-Analyst à un utilisateur test à des fins d'évaluation.
7. Connectez-vous en tant qu'utilisateur test et évaluez l'accès.

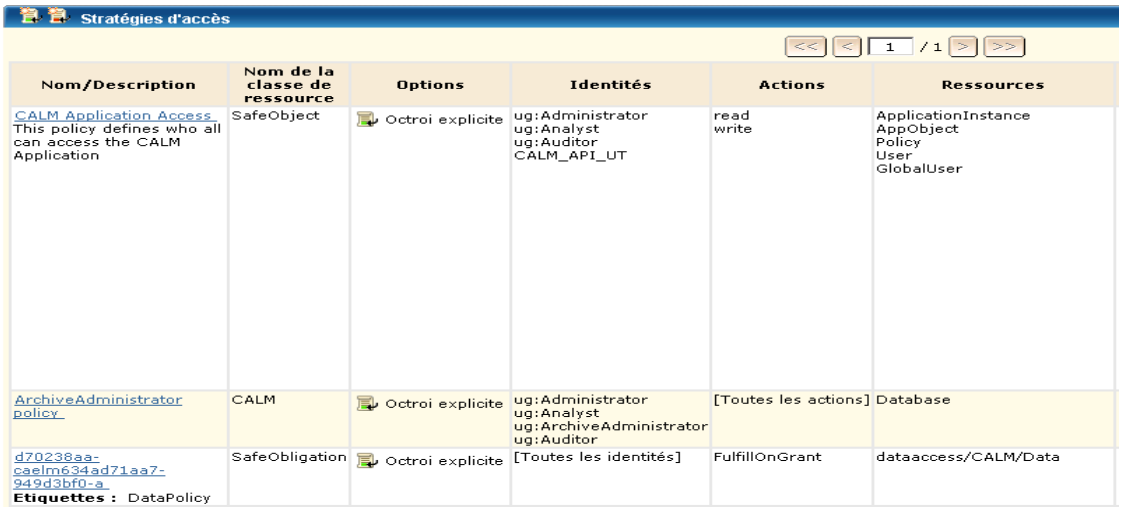
   Si l'accès autorisé par le rôle et les stratégies est conforme à vos attentes, affectez le rôle à tous les individus devant analyser les rapports PCI.

Etape 1 : planification du rôle et des stratégies à créer

Supposons que vous souhaitiez créer un rôle similaire au rôle Analyst, mais avec un accès limité aux seuls rapports et requêtes PCI. Recherchez un nom décrivant la fonction du rôle, "PCI-Analyst" par exemple.

Avant de commencer à créer de nouveaux rôles (ou groupes d'utilisateurs d'applications), réfléchissez aux stratégies devant compléter le nouveau rôle. Il est recommandé d'identifier les stratégies existantes susceptibles d'être utilisées en tant que modèles. Sous Identités, recherchez le rôle similaire à celui que vous souhaitez créer.

Dans notre exemple, il s'agit du rôle ug:Analyst. Sous Rechercher des stratégies, sélectionnez Afficher les stratégies correspondant à l'identité, entrez l'identité **ug:Analyst** et cliquez sur OK. Les stratégies affichées incluent celles concernant Toutes les identités ainsi que celles dans lesquelles ug:Analyst fait explicitement partie des identités nommées.



Stratégies d'accès

<< < 1 / 1 > >>

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Octroi explicite	ug:Administrator ug:Analyst ug:Auditor CALM_API_UT	read write	ApplicationInstance AppObject Policy User GlobalUser
ArchiveAdministrator policy	CALM	Octroi explicite	ug:Administrator ug:Analyst ug:ArchiveAdministrator ug:Auditor	[Toutes les actions]	Database
d70238aa-caelm634ad71aa7-949d3bf0-a **Etiquettes :** DataPolicy	SafeObligation	Octroi explicite	[Toutes les identités]	FulfillOnGrant	dataaccess/CALM/Data

Vous trouverez ci-dessous les noms des stratégies incluant ce rôle.

- Sous Portée, Accès aux applications CALM
- Sous Portée, Stratégie d'accès au serveur de rapports pour les auditeurs et les analystes
- Sous Portée, Stratégie de modification et d'affichage des rapports pour les analystes
- Sous CALM, Stratégie de création, de planification et d'annotation des analystes

Pour chacune des stratégies candidates, examinez la définition et déterminez quelles actions entreprendre dans la liste ci-dessous.

- Ajouter le nouveau rôle en tant qu'identité à laquelle cette stratégie s'applique. Il s'agit du choix le plus adapté si la stratégie s'applique au nouveau rôle sans aucune modification.

  Cette action convient aux stratégies ci-dessous dans notre exemple.

  - Accès aux applications CALM, qui définit toutes les identités pouvant accéder à CA Enterprise Log Manager.
  - Stratégie d'accès au serveur de rapports pour les auditeurs et les analystes, qui définit toutes les identités qui peuvent planifier des rapports et des alertes sur tous les serveurs de rapports disponibles. Ce rôle ne nécessite aucune limitation sur les serveurs de rapports.
  - Stratégie de création, de planification et d'annotation des analystes

- Enregistrer la stratégie sous un nouveau nom et modifier sa définition.

  Dans notre exemple, cette action convient à la stratégie suivante, la nouvelle copie incluant uniquement la nouvelle identité et possédant un filtre supplémentaire pour limiter l'accès en lecture/écriture aux seuls rapports associés à la balise PCI.

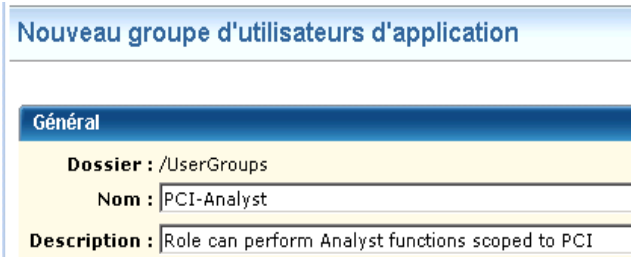
  - Stratégie de modification et d'affichage des rapports pour les analystes

Etape 2 : création du rôle PCI-Analyst

Vous pouvez créer un rôle personnalisé représentant une tâche que plusieurs utilisateurs effectuent avec l'application CA Enterprise Log Manager. Les termes "rôle" et "groupe d'utilisateurs d'applications" désignent exactement la même chose.

La première étape de la procédure visant à restreindre l'accès pour un rôle consiste à créer le rôle.

Lorsque vous créez un rôle personnalisé qui n'est pas un surensemble d'un rôle existant, n'effectuez aucune sélection dans la liste des groupes d'utilisateurs disponibles.



Informations complémentaires

Création d'un groupe d'utilisateurs d'applications (rôle) (page 91)

Etape 3 : ajout de PCI-Analyst à la stratégie d'accès aux applications CALM

L'étape suivant la création d'un nouveau rôle consiste à accorder à ce rôle une connexion de base à l'application CA Enterprise Log Manager. Par défaut, seuls les rôles prédéfinis possèdent un accès à la connexion. Ajoutez ce groupe d'applications à la stratégie d'accès aux applications CALM.

Informations complémentaires

Attribution d'un accès de rôle personnalisé à CA Enterprise Log Manager (page 92)

Etape 4 : ajout du rôle PCI-Analyst aux stratégies existantes

Après avoir identifié les stratégies qui s'appliquent à un groupe d'utilisateurs d'applications dont le nouveau rôle est un sous-ensemble, vous devez ajouter le nouveau rôle à la liste actuelle des identités.

Dans notre exemple, il nous faut ajouter le rôle PCI-Analyst aux stratégies existantes ci-dessous.

- Stratégie d'accès au serveur de rapports pour les auditeurs et les analystes
- Stratégie de création, de planification et d'annotation des analystes

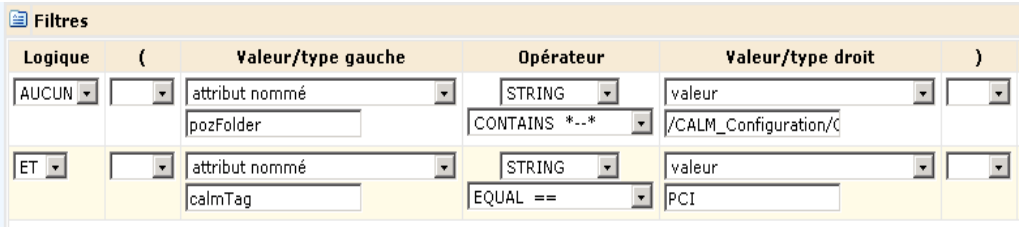
Informations complémentaires

Ajout d'une identité à une stratégie existante (page 93)

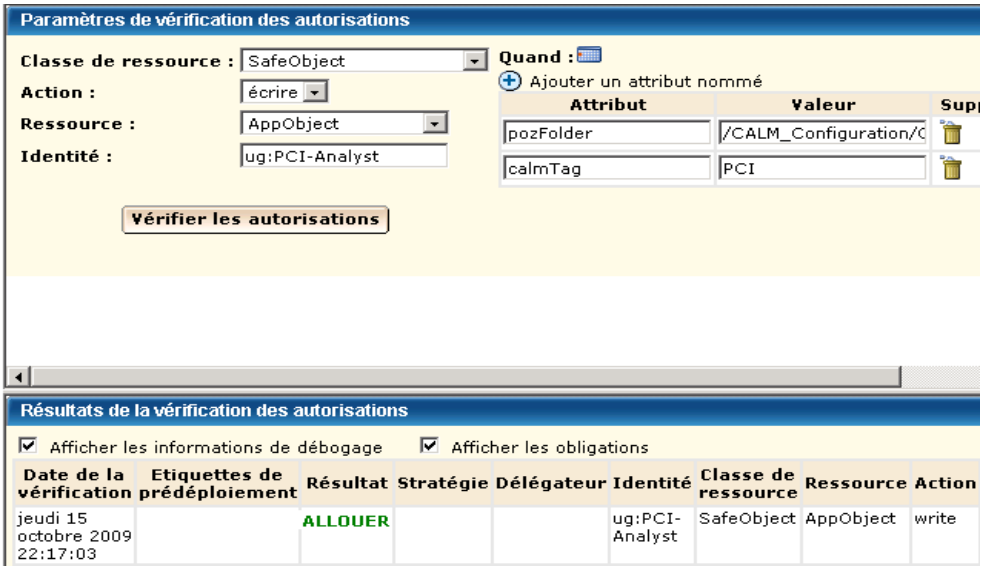
Etape 5 : création d'une stratégie basée sur la stratégie de modification et d'affichage des rapports pour les analystes

Pour créer une stratégie à partir d'une stratégie existante, vous devez copier la stratégie existante et l'enregistrer sous un nouveau nom. Puis vous devez la renommer, en modifier la description pour l'adapter au nouveau rôle et remplacer les identités existantes par votre nouvelle identité. Lorsque la stratégie que vous utilisez en tant que modèle offre un accès trop large pour votre nouveau rôle, vous devez créer des filtres afin de limiter cet accès.

Dans le scénario du rôle PCI-Analyst, copiez la stratégie de modification et d'affichage des rapports pour les analystes, enregistrez-la sous un nouveau nom, ouvrez la nouvelle stratégie, remplacez l'identité par le groupe PCI-Analyst et ajoutez un filtre pour limiter l'accès aux seuls rapports associés à la balise PCI calmTag.



Il est recommandé de tester une stratégie basée sur une stratégie existante de la même manière que vous testeriez une stratégie créée de toutes pièces. Lorsque vous testez une stratégie avec un filtre, assurez-vous d'entrer le filtre exactement comme il a été entré dans la stratégie. Lorsque vous entrez un nom de groupe pour une identité, assurez-vous de lui ajouter le préfixe ug:, par exemple ug:PCI-Analyst.



Informations complémentaires

Création d'une stratégie basée sur une stratégie existante (page 101)
Test d'une nouvelle stratégie (page 102)

Etape 6 : attribution du rôle PCI-Analyst à un utilisateur

Suite à la création d'un nouveau rôle et de ses stratégies associées, il est recommandé de vous connecter sous un nom d'utilisateur possédant uniquement ce rôle afin de déterminer si l'accès accordé correspond bien aux besoins. Une fois cette vérification effectuée, le nouveau rôle peut être ajouté aux comptes de tous les utilisateurs qui doivent effectuer les tâches pour lesquelles le rôle a été conçu.

Vous pouvez créer un compte d'utilisateur temporaire à des fins de test d'un nouveau rôle, puis supprimer ce compte à l'issue des tests. Vous pouvez également créer un utilisateur appelé Utilisateur-Test et lui affecter un rôle différent à chaque nouvelle utilisation.

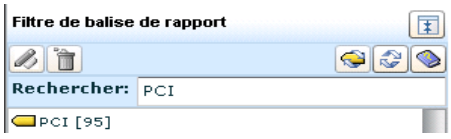
Informations complémentaires

Affectation d'un rôle à un utilisateur global (page 44)

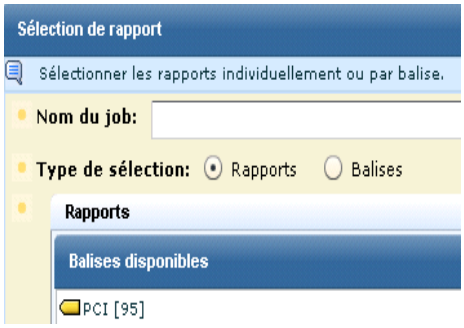
Etape 7 : connexion en tant que PCI-Analyst et évaluation de l'accès

Assurez-vous que les stratégies sont suffisantes pour limiter l'accès aux rapports et aux alertes associés à la balise PCI. Attribuez le rôle PCI-Analyst à un utilisateur et connectez-vous à CA Enterprise Log Manager sous l'identité de ce nouvel utilisateur.

Affichez les balises de rapports. Vérifiez que les rapports que vous pouvez afficher se limitent à ceux contenant la balise PCI.



Planifiez un rapport. Vérifiez que les rapports que vous pouvez planifier se limitent à ceux contenant la balise PCI.



Créez un rapport. Vérifiez que la seule balise disponible pour le nouveau rapport est PCI.

Exemples de stratégie pour les intégrations personnalisées

Vous pouvez autoriser des utilisateurs non administrateurs à créer des intégrations personnalisées, en créant un rôle personnalisé, une stratégie CALM et une stratégie de portée. D'autres utilisateurs non administrateurs pourront consulter ces intégrations personnalisées si vous créez un rôle personnalisé supplémentaire et la stratégie de portée associée. Vous devez ensuite ajouter les deux rôles personnalisés à la stratégie d'accès aux applications CALM et leur attribuer des utilisateurs.

L'exemple ci-dessous vous explique comment effectuer ces actions.

1. Créez un groupe d'utilisateurs d'applications appelé Créer-Fichiers-DM-XMP.
2. Créez un groupe d'utilisateurs d'applications appelé Afficher-Fichiers-DM-XMP.
3. Octroyez aux groupes Créer-Fichiers-DM-XMP et Afficher-Fichiers-DM-XMP l'accès au produit CA Enterprise Log Manager.

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Octroi explicite	ug:Administrator ug:Analyst ug:Auditor ug:Create-DM-XMP-Files ug:View-DM-XMP-Files	read write	ApplicationInstance Policy User GlobalUser

4. Créez une stratégie CALM pour octroyer au groupe Créer-Fichiers-DM-XMP le droit de créer des fichiers de mappage des données et des fichiers d'analyse de message à l'aide de la grammaire commune aux événements lorsque ce groupe est connecté à CA Enterprise Log Manager.

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
Integration-Create policy Can create data mapping anad message parsing files using common event grammar.	CALM	Octroi explicite	ug:Create-DM-XMP-Files	create	Integration

5. Créez une stratégie de portée pour octroyer au groupe Créer-Fichiers-DM-XMP le droit de modifier et d'afficher les fichiers DM personnalisés et le fichier XMP enregistrés dans le dossier EEM /CALM_Configuration/Content/Mapping ou /CALM_Configuration/Content/Parsing, à l'aide de la grammaire commune aux événements.

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
Edit-DM-XMP-Files with CEG Policy Can edit data mapping files and message parsing files using common event grammar saved to the EEM folders /CALM/Configuration/Content/...	SafeObject	Octroi explicite	ug:Create-DM-XMP-Files	read write	AppObject

Filtres	
WHERE	name:pozFolder *--* val:/CALMConfiguration/Content/Mapping
OU	name:pozFolder *-- val:/CALMConfiguration/Content/Parsing

6. Créez une stratégie de portée pour octroyer au groupe Afficher-Fichiers-DM-XMP le droit d'afficher les fichiers DM personnalisés et le fichier XMP enregistrés dans le dossier EEM /CALM_Configuration/Content/Mapping ou /CALM_Configuration/Content/Parsing.

   Remarque : La stratégie CEG octroie à toutes les identités le droit d'afficher la grammaire commune aux événements.

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
View-DM-XMP-Files Can View data mapping files and message parsing files.	SafeObject	Octroi explicite	ug:View-DM-XMP-Files	read	AppObject

Filtres
WHERE (name:pozFolder *--* val:/CALMConfiguration/Content/Mapping OU name:pozFolder *--* val:/CALM_Configuration/Content/Parsing)

7. Testez les stratégies.
8. Affectez les utilisateurs aux deux groupes, Créer-Fichiers-DM-XMP et Afficher-Fichiers-DM-XMP.

Exemples de stratégie pour les règles de suppression et de récapitulation

Vous pouvez autoriser des utilisateurs non administrateurs à créer des règles de suppression et de récapitulation personnalisées, en créant un rôle personnalisé, une stratégie CALM et une stratégie de portée. D'autres utilisateurs non administrateurs pourront consulter ces règles de suppression et de récapitulation personnalisées si vous créez un rôle personnalisé supplémentaire et la stratégie de portée associée. Vous devez ensuite ajouter les deux rôles personnalisés à la stratégie d'accès aux applications CALM et leur attribuer des utilisateurs.

L'exemple ci-dessous vous explique comment effectuer ces actions.

1. Créez un groupe d'utilisateurs d'applications appelé Créer-Règles-SUP-SUM.
2. Créez un groupe d'utilisateurs d'applications appelé Afficher-Règles-SUP-SUM.
3. Octroyez à ces deux groupes l'accès au produit CA Enterprise Log Manager.

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Octroi explicite	ug:Administrator ug:Analyst ug:Auditor ug:Create-Sup-Sum-Rules ug:View-Sup-Sum-Rules	read write	ApplicationInstance Policy User GlobalUser

4. Créez une stratégie CALM pour octroyer aux utilisateurs du groupe Créer-Règles-SUP-SUM le droit de créer des règles de suppression et de récapitulation ou d'en importer, lors de la connexion à CA Enterprise Log Manager.

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
EventGrouping-Create policy Can create custom summarization and suppression rules or import rules.	CALM	Octroi explicite	ug:Create-Sup-Sum-Rules	create	EventGrouping

5. Créez une stratégie de portée pour octroyer aux utilisateurs du groupe Créer-Règles-SUP-SUM le droit d'afficher et de modifier les règles de suppression ou de récapitulation personnalisées enregistrées dans le dossier EEM /CALM_Configuration/Content/Rules/Suppression ou /CALM_Configuration/Content/Rules/Summarization.

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
View-Edit-SUP-SUM-Rules Can view or edit suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	Octroi explicite	ug:Create-Sup-Sum-Rules	read write	AppObject

Filtres		
WHERE	name:pozFolder *--*	val:/CALMConfiguration/Content/Rules/Summarization
OU	val:pozFolder *--*	val:/CALMConfiguration/Content/Rules/Suppression

6. Créez une stratégie de portée pour octroyer aux utilisateurs du groupe Afficher-Règles-SUP-SUM le droit d'afficher les règles de suppression ou de récapitulation personnalisées.

Nom/Description	Nom de la classe de ressource	Options	Identités	Actions	Ressources
View-SUP-SUM-Rules Can view suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	Octroi explicite	ug:View-Sup-Sum-Rules	read	AppObject

Filtres		
WHERE	name:pozFolder *--*	val:/CALMConfiguration/Content/Rules/Summarization
OU	val:pozFolder *--*	val:/CALMConfiguration/Content/Rules/Suppression

7. Testez les stratégies.
8. Affectez les utilisateurs aux nouveaux rôles. Par exemple, les auditeurs externes peuvent souhaiter consulter vos règles de suppression et de récapitulation. Pour les y autoriser, vous pouvez affecter ces utilisateurs à un rôle de type Afficher-Règles-SUP-SUM.

Vous pouvez également, pour créer explicitement deux nouveaux rôles pour la tâche création/modification/affichage et la tâche affichage seul, développer les rôles prédéfinis Analyst et Auditor. Par exemple, vous pouvez ignorer les étapes 1, 2, 3 et 8 de la procédure précédente et, à la place, affecter Analyst comme identité pour la stratégie Créer-Regroupement-Evénement et Afficher-Modifier-Règles-SUP-SUM, et affecter le groupe d'utilisateurs Auditor comme identité pour Afficher-Règles-SUM-SUP.

Informations complémentaires :

Création d'un groupe d'utilisateurs d'applications (rôle) (page 91)
Attribution d'un accès de rôle personnalisé à CA Enterprise Log Manager (page 92)
Test d'une nouvelle stratégie (page 102)
Affectation d'un rôle à un utilisateur global (page 44)

Chapitre 5 : Services et adaptateurs CA

Ce chapitre traite des sujets suivants :

Tâches liées aux services

Vous pouvez définir des configurations globales qui s'appliquent à tous les serveurs CA Enterprise Log Manager. Vous pouvez afficher et modifier deux types de configuration de service : une configuration globale de service s'applique à toutes les instances d'un même service dans votre environnement et une configuration locale de service à un seul hôte de service sélectionné.

Remarque : Les configurations globales doivent être distinguées des configurations globales *de service* : les premières contrôlent le comportement de tous les serveurs CA Enterprise Log Manager, tandis que les deuxièmes contrôlent le comportement d'un service défini. Vous pouvez ainsi définir l'intervalle de mise à jour pour tous les services (configuration globale) ou des stratégies de conservation de rapport pour tous les serveurs de rapports (configuration globale de service).

Vous pouvez également afficher les événements d'autosurveillance à partir des zones de configuration de service.

Les services disponibles incluent les éléments suivants.

- Champ Magasin de journaux
- Serveur ODBC
- Serveur de rapports
- Module d'abonnement

Vous pouvez choisir d'afficher les services par nom de service ou par hôte.

Informations complémentaires :

Modification de configurations globales (page 143)
Modification d'une configuration globale de service (page 145)
Modification d'une configuration locale de service (page 146)
Affichage de l'état du magasin de journaux d'événements (page 151)
Configurations de services (page 147)
Suppression d'un hôte de service (page 142)

Suppression d'un hôte de service

Lorsque vous désinstallez un serveur CA Enterprise Log Manager, vous devez supprimer la configuration hôte du référentiel du serveur de gestion. La suppression de cette référence maintient le serveur à jour concernant la liste de ses serveurs CA Enterprise Log Manager enregistrés.

Pour supprimer un hôte de service

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.

   La Liste de services s'affiche.

2. Cliquez sur Hôte dans la boîte de dialogue Afficher les services par, en haut de la liste.

   Une liste extensible des hôtes de service apparaît sous la forme d'une arborescence.

3. Sélectionnez l'hôte que vous souhaitez supprimer, puis cliquez sur Supprimer.

   L'hôte est supprimé de la liste.

Important : Aucun avertissement ne s'affiche lors de la suppression d'un hôte. L'hôte est immédiatement supprimé si vous cliquez sur Supprimer. Par conséquent, vous devez être sûr de vouloir supprimer l'hôte.

Modification de configurations globales

Vous pouvez définir des configurations globales pour l'ensemble des services. Si vous essayez d'enregistrer des valeurs non comprises dans la plage autorisée, CA Enterprise Log Manager est défini par défaut sur la valeur minimale ou maximale, selon le cas. Plusieurs des paramètres sont interdépendants.

Pour modifier des paramètres globaux

1. Cliquez sur l'onglet Administration et le sous-onglet Services.

   La Liste de services s'affiche.

2. Cliquez sur Configuration globale dans la Liste de services.

   Le volet de détails Configuration globale du service s'ouvre.

3. Vous pouvez changer les paramètres de configuration suivants.

   Intervalle de mise à jour

   Spécifie la fréquence, en secondes, à laquelle les composants du serveur appliquent les mises à jour de configuration.

   Minimum : 30

   Maximum : 86 400

   Délai d'expiration de la session

   Spécifie la durée maximale d'une session inactive. Si l'actualisation automatique est activée, une session n'expire jamais.

   Minimum : 10

   Maximum : 60

   Permettre l'actualisation automatique

   Permet aux utilisateurs d'actualiser automatiquement les rapports ou les requêtes. Ce paramètre permet aux administrateurs de désactiver l'actualisation automatique de manière globale.

   Fréquence d'actualisation automatique

   Spécifie l'intervalle, en minutes, auquel les vues de rapport sont actualisées. Ce paramètre dépend de la sélection de Permettre l'actualisation automatique.

   Minimum : 1

   Maximum : 600

   Activer l'actualisation automatique

   Définit l'actualisation automatique dans l'ensemble des sessions. Par défaut, l'actualisation automatique n'est pas activée.

Pour afficher les alertes d'action, l'authentification est requise.

Empêche les auditeurs ou les produits tiers d'afficher les flux RSS des alertes d'action. Ce paramètre est activé par défaut.

Rapport par défaut

Spécifie le rapport par défaut.

Activer le lancement du rapport par défaut

Affiche le rapport par défaut lorsque vous cliquez sur l'onglet Rapports. Ce paramètre est activé par défaut.

4. Vous pouvez changer les paramètres de balise de rapport ou de requête suivants.

   Masquer les balises de rapport

   Empêche les balises spécifiées d'apparaître dans une liste de balises. Masquer les balises de rapport rationalise l'affichage des rapports disponibles.

   Masquer les balises de requête

   Vous permet de masquer les balises choisies. Les balises masquées n'apparaissent plus dans la liste de requêtes principale ou dans la liste de requêtes de planification d'alertes d'action. Masquer les balises de requête personnalise l'affichage des requêtes disponibles.

5. Vous pouvez changer les paramètres de profil suivants.

   Activer le profil par défaut

   Vous permet de définir le profil par défaut.

   Profil par défaut

   Spécifie le profil par défaut.

   Masquer les profils

   Vous permet de masquer les profils choisis. Lorsque l'interface s'actualise ou que l'intervalle de mise à jour expire, les profils masqués n'apparaissent plus. Masquer les profils personnalise l'affichage des profils disponibles.

   Remarque : Cliquez sur Réinitialiser pour restaurer les dernières valeurs enregistrées. Vous pouvez réinitialiser un ou plusieurs changements jusqu'à leur enregistrement. Une fois ces changements enregistrés, réinitialisez-les un par un.

6. Cliquez sur Enregistrer.

Modification d'une configuration globale de service

Vous pouvez modifier des configurations globales de service, qui sont des paramètres qui s'appliquent à toutes les instances d'un service donné dans votre environnement. Une configuration globale de service n'écrase *pas* les paramètres locaux de service qui sont différents des paramètres globaux.

Les valeurs de configuration maximales et minimales sont détaillées dans les sections sur les services. Si vous essayez d'enregistrer des valeurs non comprises dans la plage autorisée, CA Enterprise Log Manager est défini par défaut sur la valeur minimale ou maximale, selon le cas.

Pour modifier une configuration globale de service

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.

   La Liste de services s'affiche.

2. Sélectionnez le service dont vous souhaitez modifier la configuration.

   L'affichage Configuration globale du service s'ouvre dans le volet Détails.

3. Effectuez les changements de configuration souhaités.

   Remarque : Vous pouvez cliquez sur Réinitialiser pour restaurer la dernière valeur enregistrée des champs de saisie. Vous pouvez réinitialiser un seul ou plusieurs changements jusqu'au moment où vous avez cliqué sur Enregistrer. Une fois les changements enregistrés, vous devez les réinitialiser un par un.

4. Une fois les changements terminés, cliquez sur Enregistrer.

   Tous les changements de configuration que vous effectuez sont appliqués à tous les hôtes du service sélectionné, sauf s'ils ont des paramètres locaux différents.

Modification d'une configuration locale de service

Vous pouvez afficher ou modifier les configurations locales de service par service ou par serveur hôte. Les configurations locales de service vous permettent de contrôler les services ou les paramètres qui peuvent ne pas s'appliquer ou ne pas être requis pour l'ensemble de votre environnement, de manière à écraser les paramètres globaux pour certains hôtes uniquement. Par exemple, vous pouvez faire en sorte qu'un serveur CA Enterprise Log Manager conserve les alertes d'action plus longtemps que les autres. Une configuration locale peut vous permettre d'obtenir ce résultat.

Les valeurs de configuration maximales et minimales sont détaillées dans les sections sur les services. Si vous essayez d'enregistrer des valeurs non comprises dans la plage autorisée, CA Enterprise Log Manager est défini par défaut sur la valeur minimale ou maximale, selon le cas.

Pour modifier une configuration locale de service

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.

   La Liste de services s'affiche.

2. Cliquez sur la flèche en regard du service dont vous souhaitez modifier la configuration.

   La fenêtre du service se développe, affichant les différents hôtes de service.

3. Cliquez sur l'hôte de service de votre choix.

   La configuration du service que vous sélectionnez s'ouvre dans le volet Détails.

4. Effectuez les changements de configuration souhaités. Chaque champ de saisie, menu ou commande de la configuration locale comporte un bouton de configuration locale/globale qui permet de passer d'un état à l'autre.

   Configuration globale : 

   Configuration locale : 

   Chaque fois que vous cliquez sur le bouton, vous passez d'une configuration globale à locale, ou inversement, et la valeur associée devient utilisable. La valeur doit rester définie pour une configuration locale pour que ce paramètre prenne effet : si elle est définie pour une configuration globale, le paramètre global est effectif pour cet écouteur.

   Remarque : Lorsque vous cliquez sur Réinitialiser, les dernières valeurs de configuration enregistrées pour toutes les configurations disponibles s'affichent. Vous pouvez réinitialiser un seul ou plusieurs changements jusqu'au moment où vous avez cliqué sur Enregistrer. Une fois les changements enregistrés, vous devez les réinitialiser un par un.

5. Une fois les changements terminés, cliquez sur Enregistrer.

Tous les changements que vous effectuez s'appliquent uniquement à l'hôte de service sélectionné.

Configurations de services

Cette section inclut des détails et instructions sur les services à prendre en compte lorsque vous effectuez des changements de configuration sur les services CA Enterprise Log Manager suivants.

- Magasin de journaux d'événements : stocke tous les événements bruts ajustés et enregistrés.
- Serveur ODBC : permet d'accéder au magasin de journaux d'événements CA Enterprise Log Manager à partir d'une application externe telle que BusinessObjects Crystal Reports.
- Serveur de rapports : contrôle la distribution, le formatage et la conservation des rapports et alertes.
- Module d'abonnement : achemine les mises à jour de contenu et de configuration vers le serveur de gestion et les mises à jour des fichiers binaires vers les clients d'abonnement.

Informations complémentaires :

Abonnement (page 205)
Remarques sur le magasin de journaux d'événements (page 147)
Remarques sur l'abonnement (page 154)

Remarques sur le magasin de journaux d'événements

Le magasin de journaux d'événements utilise un système fédéré dans lequel chaque serveur hôte maintient son propre magasin de journaux d'événements local, avec la possibilité de contacter d'autres magasins de journaux d'événements dans votre environnement. Lorsque vous interrogez un serveur sur certaines informations d'événement, il peut lancer une recherche sur son propre magasin de journaux d'événements, ainsi que dans d'autres magasins connectés par le biais de la fédération. Cette organisation offre davantage de flexibilité pour le stockage et l'archivage des données d'événement.

Les paramètres d'archivage du magasin de journaux d'événements vous permettent d'indiquer à quelle fréquence les données sont archivées et à quel emplacement. Les magasins de journaux d'événements non compressés et les informations de journaux d'événements compressés sont tous interrogés. Les informations d'événement sauvegardées (distantes) ne sont pas interrogées.

Vous pouvez configurer les paramètres d'archivage et de magasin de journaux d'événements suivants.

Nombre maximum de lignes

Définit le nombre maximal d'événements contenus dans votre base de données chaude de magasin de journaux d'événements. Lorsque le nombre d'événements atteint cette valeur, le journal d'événements compresse toutes les informations d'événement de la base de données chaude et les déplacent dans la base de données tiède.

Minimum : 5 000

Maximum : 10 000 000

Nbre max. de jours d'archivage

Définit le nombre de jours pendant lequel les fichiers archivés sont conservés avant d'être supprimés.

Minimum : 1

Maximum : 28 000

Espace disque d'archivage

Définit le pourcentage d'espace disque restant qui déclenche la suppression automatique des fichiers d'archive les plus anciens. La valeur par défaut est 10, par exemple. Lorsque l'espace disponible du magasin de journaux d'événements passe en dessous de 5 %, le journal d'événements supprime les fichiers d'archive les plus anciens pour faire de la place.

Minimum : 10

Maximum : 90

Exporter la stratégie

Définit le nombre d'heures pendant lequel un fichier restauré dans l'archive depuis une source de sauvegarde extérieure (fichier dégivré) est conservé dans le magasin de journaux d'événements avant d'être supprimé.

Minimum : 0

Maximum : 168

Règles de récapitulation/suppression

Détermine les règles de récapitulation ou de suppression disponibles qui sont appliquées aux événements reçus. Les nouvelles règles de récapitulation ou de suppression doivent être appliquées par un administrateur avant de pouvoir ajuster des événements.

Enfants de fédération de serveurs

Détermine les magasins de journaux d'événements disponibles qui sont définis en tant qu'enfants du serveur actuel. Vous pouvez ainsi définir des arborescences de fédération distinctes et contrôler les niveaux d'accès aux requêtes. Cette option est uniquement disponible en tant que paramètre local.

Les paramètres de journalisation contrôlent la manière dont les différents modules CA Enterprise Log Manager enregistrent les messages internes. Ils sont uniquement disponibles en tant que paramètres locaux. Les paramètres de journalisation sont généralement utilisés à des fins de dépannage. Il n'est généralement pas nécessaire de modifier ces paramètres ; il est essentiel de bien comprendre le fonctionnement des fichiers journaux et de la journalisation avant d'effectuer tout changement.

Niveau de journal

Définit le type et le niveau de détail enregistrés dans le fichier journal. La liste déroulante est classée dans l'ordre croissant du niveau de détail.

Appliquer à tous les enregistreurs

Détermine si le paramètre Niveau de journal écrase tous les paramètres de journal issus du fichier des propriétés du journal. Ce réglage s'applique uniquement lorsque le paramètre Niveau de journal est inférieur (plus détaillé) au paramètre par défaut.

Les paramètres d'archivage automatique activent et contrôlent les jobs d'archivage de base de données planifiés, qui déplacent les bases de données tièdes vers un serveur distant. Vous pouvez définir les valeurs d'archivage automatique suivantes.

Activé(e)

Définit un job d'archivage automatique à exécuter. L'archivage automatique utilise l'utilitaire scp contrôlé par les autres paramètres.

Type de sauvegarde

Contrôle le type de sauvegarde : un archivage complet qui copie toutes les informations de base de données ou un archivage incrémentiel qui copie toutes les bases de données qui n'ont pas encore été sauvegardées.

Par défaut : Incrémentiel

Fréquence

Spécifie si le job d'archivage s'exécute tous les jours ou toutes les heures. Un job quotidien s'exécute à l'heure définie par la valeur Heure de début. Un job horaire s'exécute toutes les heures à chaque nouvelle heure de la journée.

Heure de début

Définit l'heure à laquelle un job d'archivage quotidien s'exécute (heures justes) en fonction de l'heure locale du serveur. La valeur est au format 24 heures.

Limites : 0-23, où 0 correspond à minuit et 23 à 23 h 00.

Utilisateur EEM

Spécifie l'utilisateur pouvant effectuer une requête d'archivage, recataloguer la base de données d'archivage, exécuter l'utilitaire LMArchive et exécuter le script de commandes shell restore-ca-elm pour restaurer les bases de données d'archivage en vue de leur examen. Cet utilisateur doit posséder le rôle prédéfini Administrator ou un rôle personnalisé associé à une stratégie personnalisée qui autorise l'action Modifier sur la ressource Base de données.

Par défaut : Utilisateur administrateur gestionnaire de journaux

Mot de passe EEM

Spécifie le mot de passe pour l'utilisateur possédant les droits définis dans le champ utilisateur EEM.

Serveur distant

Spécifie le nom d'hôte ou l'adresse IP du serveur distant sur lequel le job d'archivage automatique copie les informations de base de données.

Utilisateur distant

Spécifie le nom d'utilisateur utilisé par l'utilitaire scp pour se connecter au serveur distant.

Par défaut : caelmservice

Emplacement distant

Spécifie la destination du fichier d'archive sur le serveur distant.

Par défaut : /opt/CA/LogManager

Serveur ELM distant

Détermine si le serveur distant est un serveur de gestion ou non. Le cas échéant, le job d'archivage automatique supprime les bases de données de la machine locale lorsque le transfert est terminé et demande à la machine distante de se recataloguer.

Informations complémentaires :

Stockage des journaux (page 169)
Application d'une règle de suppression ou de récapitulation (page 543)
Exemple : Archivage automatique sur trois serveurs (page 174)

Affichage de l'état du magasin de journaux d'événements

Vous pouvez afficher les informations courantes sur le magasin de journaux d'événements, y compris les heures des requêtes, les insertions de données totales, les erreurs d'insertion et d'autres statistiques qui vous aident à surveiller les performances du magasin de journaux d'événements.

Pour afficher l'état du magasin de journaux d'événements

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.

   La Liste de services s'affiche.

2. Cliquez sur l'icône Magasin de journaux d'événements.

   L'arborescence du service se développe et affiche les hôtes du magasin de journaux d'événements.

3. Sélectionnez l'hôte dont vous souhaitez afficher l'état.

   La configuration locale de service de cet hôte apparaît dans le volet Détails.

4. Sélectionnez l'onglet Etat.

   Les informations d'état s'affichent.

   Remarque : Les informations d'état apparaissent uniquement dans le panneau de configuration locale.

Remarques sur le serveur ODBC

Vous pouvez installer un client ODBC ou un client JDBC pour accéder au magasin de journaux d'événements CA Enterprise Log Manager à partir d'une application externe telle que BusinessObjects Crystal Reports.

Le serveur ODBC contrôle les paramètres utilisés lors de l'accès aux données d'événement du serveur CA Enterprise Log Manager à partir d'une application externe utilisant un client ODBC ou JDBC. Vous pouvez effectuer les tâches suivantes depuis cette zone de configuration.

- Configurez le port de service utilisé pour les communications entre le client ODBC ou JDBC et le serveur CA Enterprise Log Manager.
- Spécifiez si les communications entre le client ODBC ou JDBC et le serveur CA Enterprise Log Manager sont cryptées.

Les descriptions des champs sont les suivantes.

Activer le service

Indique si les clients ODBC et JDBC peuvent accéder aux données dans le magasin de journaux d'événements. Sélectionnez cette case à cocher pour activer l'accès externe aux événements. Désélectionnez la case à cocher pour désactiver l'accès externe. La valeur par défaut de cette option *active* l'accès aux événements ODBC et JDBC.

Port d'écoute du serveur

Spécifie le numéro de port sur lequel une application cliente envoie des requêtes ODBC ou JDBC et reçoit des résultats du serveur CA Enterprise Log Manager. La valeur par défaut est 17002. Le serveur CA Enterprise Log Manager refuse les tentatives de connexion lorsqu'une valeur différente est spécifiée dans la source de données Windows ou dans la chaîne URL JDBC.

Chiffrement (SSL)

Indique si le chiffrement doit être utilisé pour les communications entre le client ODBC et le serveur CA Enterprise Log Manager. La valeur par défaut active le chiffrement SSL. Le serveur CA Enterprise Log Manager refuse les tentatives de connexion lorsque la valeur correspondante dans la source de données Windows ou dans l'URL JDBC est différente de ce paramètre.

Délai d'expiration de la session (en minutes)

Spécifie le nombre de minutes pendant lequel une session inactive reste ouverte avant d'être automatiquement fermée.

Niveau de journal

Définit le type et le niveau de détail enregistrés dans le fichier journal. La liste déroulante est classée dans l'ordre croissant du niveau de détail.

Appliquer à tous les enregistreurs

Détermine si le paramètre Niveau de journal écrase tous les paramètres de journal issus du fichier des propriétés du journal. Ce réglage s'applique uniquement lorsque le paramètre Niveau de journal est inférieur (plus détaillé) au paramètre par défaut.

Remarques sur le serveur de rapports

Le serveur de rapports contrôle l'administration des rapports diffusés de manière automatique, leur aspect au format PDF, ainsi que la conservation des alertes d'action et des rapports. Vous pouvez effectuer les tâches suivantes depuis la zone de configuration du serveur de rapports.

- Créer des listes définies par l'utilisateur.

  Listes définies par l'utilisateur (valeurs clés)

  Vous permet de créer des regroupements pertinents à utiliser dans les rapports et de contrôler les périodes de temps auxquelles ils s'appliquent.

- Définir le serveur de messagerie de rapports, le courriel de l'administrateur, le port SMTP et les informations d'authentification dans la zone Paramètres des courriels.
- Contrôler le nom et le logo de l'entreprise, les polices et d'autres paramètres des rapports au format PDF dans la zone Configurations des rapports.
- Définir le nombre total d'alertes d'action conservées et le nombre de jours pendant lequel elles sont conservées dans la zone Conservation d'alerte.

  Nombre maximum d'alertes d'action

  Définit le nombre maximal d'alertes d'action conservées par le serveur de rapports en vue de leur examen.

  Minimum : 50

  Maximum : 1 000

  Durée de conservation des alertes d'action

  Définit le nombre de jours maximal pendant lequel les alertes d'action sont conservées.

  Minimum : 1

  Maximum : 30
- Définir la stratégie de conservation pour chaque type de récurrence de rapport planifié dans la zone Conservation de rapport.
- Déterminer si l'utilitaire de conservation doit rechercher les rapports à supprimer automatiquement sur la base de ces stratégies, et si oui à quelle fréquence. Par exemple, si l'utilitaire de conservation de rapport fonctionne quotidiennement, il supprime chaque jour les rapports qui dépassent l'ancienneté spécifiée.
- Définition des paramètres du processus CA IT PAM
- Définition des paramètres des interruptions SNMP

Informations complémentaires :

Configuration de l'intégration de CA IT PAM pour la sortie de l'événement/de l'alerte (page 414)
Configuration de l'intégration avec une destination d'interruption SNMP (page 441)
Préparation à l'utilisation de rapports avec des listes à clés (page 329)
Ajout de clés pour les requêtes ou les rapports personnalisés (page 334)
Mise à jour manuelle d'une liste à clés (page 335)
Mise à jour d'une liste à clés avec Exporter/Importer (page 336)
Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)

Remarques sur l'abonnement

Un système de serveur proxy/client est utilisé pour la distribution des mises à jour. Le premier serveur installé est défini en tant que Proxy d'abonnement par défaut ; il contacte le serveur d'abonnement CA régulièrement pour vérifier la disponibilité de mises à jour. Les installations suivantes sont configurées en tant que clients de ce serveur proxy, qu'ils contactent pour obtenir les mises à jour.

Le système par défaut réduit le trafic réseau en éliminant la nécessité pour chaque serveur de contacter directement le serveur d'abonnement CA, tout en étant entièrement configurable. Vous pouvez ajouter autant de serveurs proxy que nécessaire.

Vous pouvez encore réduire le trafic Internet en créant des serveurs proxy hors ligne, qui stockent les informations de mise à jour au niveau local et les fournissent aux clients lorsqu'ils les contactent. Prenez en charge les serveurs proxy hors ligne en copiant manuellement l'intégralité du contenu à partir du chemin de téléchargement du proxy en ligne vers le chemin de téléchargement du proxy hors ligne. Des serveurs proxy hors ligne doivent être configurés dans les environnements contenant des serveurs CA Enterprise Log Manager qui ne peuvent pas accéder à Internet ou à un serveur connecté à Internet.

Lors de la configuration du service d'abonnement, tenez compte des éléments suivants concernant certains paramètres et leurs interactions.

Proxy d'abonnement par défaut

Définit le serveur proxy par défaut pour le service d'abonnement. Le proxy d'abonnement par défaut doit disposer d'un accès à Internet. Si aucun autre proxy d'abonnement n'est défini, ce serveur obtient les mises à jour d'abonnement du serveur d'abonnement CA, télécharge les mises à jour binaires sur tous les clients et distribue les mises à jour de contenu. Si d'autres proxies sont définis, les clients contactent ce serveur pour obtenir les mises à jour lorsqu'aucune liste de proxies d'abonnement n'est configurée ou lorsque la liste configurée est épuisée. La valeur par défaut est le premier serveur installé dans votre environnement. Cette valeur est uniquement disponible en tant que paramètre global.

Proxy d'abonnement

Détermine si le serveur local est un proxy d'abonnement. Un proxy d'abonnement en ligne utilise son accès à Internet pour obtenir les mises à jour d'abonnement du serveur d'abonnement CA. Les serveurs proxy d'abonnement en ligne peuvent être configurés pour télécharger les mises à jour binaires sur les clients et pour envoyer automatiquement les mises à jour de contenu au serveur de gestion. Un proxy en ligne peut également être utilisé en tant que source de copie des mises à jour vers les serveurs proxy d'abonnement hors ligne. Si elle est sélectionnée, la case Proxy d'abonnement hors ligne doit être désélectionnée. Cette valeur est uniquement disponible en tant que paramètre local.

Remarque : Si les deux cases de proxy d'abonnement sont désélectionnées, le serveur est un client d'abonnement.

Proxy d'abonnement hors ligne

Détermine si le serveur local est un proxy d'abonnement hors ligne. Un proxy d'abonnement hors ligne est un serveur qui obtient les mises à jour d'abonnement par une copie de répertoire manuelle (à l'aide de scp) à partir d'un proxy d'abonnement en ligne. Les serveurs proxy d'abonnement hors ligne peuvent être configurés pour télécharger les mises à jour des fichiers binaires sur les clients. Les proxies d'abonnement hors ligne n'ont pas besoin d'accès à Internet. Si elle est cochée, la case Proxy d'abonnement doit être désélectionnée. Cette valeur est uniquement disponible en tant que paramètre local.

Remarque : Si les deux cases à cocher de proxy d'abonnement sont désélectionnées, le serveur est un client d'abonnement.

Heure de début de la mise à jour

Applicable uniquement lorsque la fréquence de mise à jour est supérieure ou égale à 24.

Définit l'heure à laquelle commencer la première recherche de mises à jour (heures justes) en fonction de l'heure locale du serveur. La valeur est au format 24 heures. Cette valeur s'applique à la recherche initiale de mises à jour. L'option Fréquence de mise à jour contrôle la programmation de toutes les recherches de mises à jour suivantes. Ce paramètre s'applique uniquement au service de proxy d'abonnement.

Limites : 0-23, où 0 correspond à minuit et 23 à 23 h 00.

Fréquence de mise à jour

Définit la fréquence, en heures, à laquelle le proxy en ligne contacte le serveur d'abonnement CA, ainsi que la fréquence à laquelle le client d'abonnement contacte le proxy. Ce paramètre s'applique uniquement au service de proxy d'abonnement.

Exemples : .5 signifie toutes les 30 minutes ; 48 signifie un jour sur deux

Actualiser

Cliquez sur ce bouton pour démarrer immédiatement un cycle de mise à jour à la demande pour le serveur sélectionné. Vous pouvez effectuer une mise à jour à la demande pour un seul serveur à la fois. Mettez à jour le serveur proxy d'abonnement avant de mettre à jour un client d'abonnement.

URL du flux RSS

Définit l'URL du serveur d'abonnement CA. Les serveurs proxy d'abonnement en ligne utilisent cette URL pour accéder au serveur d'abonnement CA et télécharger les mises à jour d'abonnement. Cette valeur est uniquement disponible en tant que paramètre global.

Serveur proxy HTTP

Détermine si ce serveur contacte le serveur d'abonnement CA par l'intermédiaire d'un proxy HTTP pour obtenir les mises à jour, plutôt que directement.

Adresse proxy à utiliser

Spécifie l'adresse IP complète du proxy HTTP.

Port

Spécifie le numéro de port utilisé pour contacter le proxy HTTP.

ID d'utilisateur du proxy HTTP

Spécifie l'ID d'utilisateur utilisé pour contacter le proxy HTTP.

Mot de passe du proxy HTTP

Spécifie le mot de passe utilisé pour contacter le proxy HTTP.

Clé publique

Définit la clé utilisée pour tester et vérifier la signature utilisée pour signer les mises à jour. Ne mettez jamais cette valeur à jour manuellement. Lorsqu'une paire de clés publique-privée est mise à jour, le proxy télécharge la mise à jour de la valeur de clé publique et met ensuite à jour la clé publique. Cette valeur est uniquement disponible en tant que paramètre global.

Nettoyage des mises à jour antérieures à

Détermine le nombre de jours pendant lequel le serveur proxy conserve les packages de mises à jour. Cette valeur est uniquement disponible en tant que paramètre global.

Redémarrage automatique après mise à jour du SE

Détermine si CA Enterprise Log Manager redémarre automatiquement après une mise à jour du système d'exploitation. Cette valeur est uniquement disponible en tant que paramètre global.

Modules à télécharger

Vous permet de sélectionner les modules qui s'appliquent à votre environnement d'exploitation. Les modules sélectionnés pour les serveurs proxy déterminent les modules téléchargés à partir du serveur d'abonnement CA dans le cadre des mises à jour d'abonnement. Les modules sélectionnés pour les clients sont utilisés pour mettre à jour les modules correspondants installés sur le client. Vous pouvez sélectionner un module à télécharger pour un client qui n'est pas sélectionné pour son proxy. Le proxy le conserve pour le client, mais ne l'installe pas sur son propre système.

Remarque : Si ce champ n'est pas rempli, définissez l'URL du flux RSS. Ce paramètre permet au système de lire le flux RSS et, au prochain intervalle de mise à jour, d'afficher la liste des modules disponibles à télécharger.

Serveurs proxy d'abonnement pour le client

Vous permet de définir les proxies à contacter pour les mises à jour des produits et du système d'exploitation par l'ensemble des clients ou par le client sélectionné. Utilisez les flèches haut/bas pour définir l'ordre dans lequel le client contacte les serveurs proxy d'abonnement. Le client télécharge les mises à jour à partir du premier proxy auquel il parvient à accéder. Si aucun des serveurs proxy configurés n'est disponible, le client contacte le proxy d'abonnement par défaut.

Serveurs proxy d'abonnement pour les mises à jour de contenu

Vous permet de sélectionner les serveurs proxy utilisés pour distribuer les mises à jour de contenu au magasin d'utilisateurs. Vous pouvez sélectionner des serveurs proxy hors ligne ou en ligne. Cette valeur est uniquement disponible en tant que paramètre global.

Remarque : Nous vous recommandons de sélectionner plusieurs proxies à des fins de redondance.

Informations complémentaires

Modification de la configuration d'abonnement globale (page 207)
Modification de la configuration d'un proxy en ligne (page 208)
Modification de la configuration d'un proxy hors ligne (page 209)
Espace disque disponible pour les mises à jour (page 211)
A propos des modules à télécharger (page 211)
Sélection de nouveaux modules à télécharger (page 212)
Récupération manuelle des mises à jour d'abonnement (page 213)
Copie de mises à jour sur un proxy hors ligne (page 219)
A propos des clés publiques d'abonnement (page 221)
Evénements d'autosurveillance pour un abonnement (page 221)
Surveillance des événements d'abonnement (page 222)
Affichage des détails de l'événement d'abonnement (page 225)
Avertissements et échecs d'événements d'abonnement (page 226)

Service Etat du système

Vous pouvez utiliser le service Etat du système pour rassembler des informations sur un serveur CA Enterprise Log Manager et pour le contrôler. Vous pouvez afficher l'état du système uniquement pour les serveurs CA Enterprise Log Manager individuels. Tous les paramètres et options s'appliquent au niveau local.

Le service Etat du système présente les onglets suivants.

- Administration : permet de contrôler les services et les serveurs hôtes, ainsi que de créer un fichier de diagnostic de support
- Etat : permet de vérifier l'état et la version des processus et services du système
- Evénements d'autosurveillance : permet de vérifier les événements relatifs à l'état du système et des composants

Informations complémentaires :

Tâches Etat du système (page 165)
Créez un fichier de diagnostic pour le support technique. (page 166)
Redémarrage d'un serveur hôte (page 167)
Redémarrage du service iGateway (page 167)
Vérification de l'état et de la version des services (page 168)
Vérification des événements d'autosurveillance de l'état d'un système (page 168)

Tâches de configuration d'adaptateurs CA

Les écouteurs locaux reçoivent et collectent les événements natifs depuis certains types de sources à l'aide de divers types d'adaptateurs CA.

Vous pouvez afficher et modifier deux types de configurations d'adaptateur.

- Une configuration globale s'applique à toutes les instances d'un même adaptateur dans votre environnement, toutes les instances du collecteur SAPI, par exemple.
- Une configuration locale s'applique uniquement à un hôte d'adaptateur sélectionné, un seul collecteur SAPI, par exemple.

Vous pouvez également afficher les événements d'autosurveillance pour chaque service d'adaptateur ou hôte d'adaptateur depuis les zones de configuration globale ou locale de l'adaptateur en question.

Informations complémentaires

Modification d'une configuration globale d'adaptateur (page 159)
Modification d'une configuration locale d'adaptateur (page 160)
Affichage des événements d'autosurveillance d'adaptateur (page 161)
Affichage de l'état d'un adaptateur (page 162)
Remarques sur le service SAPI (page 163)
Remarques sur le service d'événement iTechnology (page 165)

Modification d'une configuration globale d'adaptateur

Vous pouvez modifier les configurations globales d'adaptateur, qui sont des paramètres qui s'appliquent à toutes les instances d'un adaptateur CA donné dans votre environnement. Par exemple, vous pouvez effectuer des changements de configuration qui s'appliquent à tous les collecteurs SAPI s'exécutant dans votre environnement. Une configuration globale d'adaptateur n'écrase *pas* les paramètres locaux d'adaptateur qui diffèrent des paramètres globaux.

Pour modifier une configuration globale d'adaptateur

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier Adaptateurs CA.

   Le dossier se développe et affiche les sous-dossiers pour chaque adaptateur.

3. Sélectionnez le dossier pour l'adaptateur dont vous souhaitez modifier la configuration.

   L'affichage Configuration globale du service s'ouvre dans le volet Détails.

4. Effectuez les changements de configuration souhaités.

   Remarque : Si vous cliquez sur Réinitialiser, les derniers états enregistrés sont restaurés en tant que valeurs de configuration. Vous pouvez réinitialiser un seul ou plusieurs changements jusqu'au moment où vous avez cliqué sur Enregistrer. Une fois les changements enregistrés, vous devez les réinitialiser un par un.

5. Cliquez sur Enregistrer lorsque les changements sont terminés.

   Tout changement de configuration effectué s'applique à tous les hôtes de l'adaptateur sélectionné, sauf s'ils ont des paramètres locaux différents.

Modification d'une configuration locale d'adaptateur

Vous pouvez afficher ou modifier les configurations locales d'adaptateur. Les configurations locales d'adaptateur vous permettent de contrôler les paramètres qui peuvent ne pas s'appliquer, ou être requis, dans l'ensemble de votre environnement. Ils remplacent les paramètres globaux de certains hôtes d'adaptateur uniquement. Par exemple, vous pouvez avoir besoin qu'un hôte d'adaptateur SAPI particulier utilise un autre port d'écoute. Vous pouvez définir ce comportement à l'aide d'une configuration locale.

Pour modifier une configuration locale d'adaptateur

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier Adaptateurs CA.

   Le dossier se développe et affiche les sous-dossiers pour chaque adaptateur.

3. Sélectionnez le dossier pour l'adaptateur dont vous souhaitez modifier la configuration.

   La fenêtre du service se développe, affichant les hôtes d'adaptateur.

4. Cliquez sur l'hôte d'adaptateur de votre choix.

   La configuration de l'hôte que vous sélectionnez s'ouvre dans le volet Détails.

5. Effectuez les changements de configuration souhaités. Chaque champ de saisie de valeur, menu ou commande de la configuration locale comporte un bouton de configuration locale/globale pouvant basculer d'un type de configuration à l'autre.

   Configuration globale : 

   Configuration locale : 

   Chaque fois que vous cliquez sur le bouton, vous passez d'un réglage global à un réglage local et le champ de saisie associé devient utilisable. Le champ de saisie doit rester défini en configuration locale pour que le paramètre prenne effet : en cas de réglage en configuration globale, le paramètre global pour cet adaptateur prend effet.

   Remarque : Lorsque vous cliquez sur Réinitialiser, les dernières valeurs de configuration enregistrées pour toutes les configurations disponibles s'affichent. Vous pouvez réinitialiser un seul ou plusieurs changements jusqu'au moment où vous avez cliqué sur Enregistrer. Une fois les changements enregistrés, vous devez les réinitialiser un par un.

6. Cliquez sur Enregistrer lorsque les changements sont terminés.

Tous les changements que vous effectuez s'appliquent uniquement à l'hôte d'adaptateur sélectionné.

Affichage des événements d'autosurveillance d'adaptateur

Vous pouvez surveiller l'activité des services d'adaptateur et dépanner les problèmes en consultant les événements d'autosurveillance pour chaque hôte de service d'adaptateur. Les événements prétriés sont accessibles dans les zones de configuration globale ou locale de chaque adaptateur.

Pour afficher les événements d'autosurveillance d'adaptateur

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier Adaptateurs CA.

   Le dossier se développe et affiche les sous-dossiers pour chaque service d'adaptateur.

3. Sélectionnez le dossier d'un service d'adaptateur pour afficher les événements d'autosurveillance le concernant ou développez les dossiers et choisissez un hôte d'adaptateur pour consulter uniquement les événements d'autosurveillance de cet hôte précis.

   La configuration de l'adaptateur s'affiche dans le volet Détails.

4. Cliquez sur l'onglet Evénements d'autosurveillance.

   La fenêtre de visionneuse d'événements qui s'affiche indique les événements correctement filtrés. Par exemple, en sélectionnant le dossier du module d'extension d'événements iTechnology à l'étape 3, vous affichez les événements d'autosurveillance de toutes les instances du module d'extension d'événements iTechnology. Si vous sélectionnez un hôte spécifique dans le dossier du module d'extension d'événements iTechnology, seuls les événements liés à cet hôte iTechnology s'affichent.

   Remarque : La structure de votre fédération détermine les événements visibles. Si aucune fédération n'est configurée, seuls les événements locaux apparaissent, quel que soit l'hôte sélectionné.

Informations complémentaires

Affichage de l'état d'un adaptateur (page 162)
Modification d'une configuration globale d'adaptateur (page 159)
Modification d'une configuration locale d'adaptateur (page 160)

Affichage de l'état d'un adaptateur

Vous pouvez consulter l'état actuel de certains services d'adaptateur CA, y compris l'heure de début, l'état d'exécution et des informations et statistiques de remise d'événement. En revanche, vous ne pouvez pas afficher l'état du service du module d'extension d'événements iTechnology.

Pour afficher l'état d'un adaptateur

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier Adaptateurs CA.

   Le dossier se développe et affiche les sous-dossiers pour chaque service d'adaptateur.

3. Sélectionnez le dossier pour l'adaptateur dont vous souhaitez afficher l'état.

   La fenêtre du service se développe, affichant les divers hôtes d'adaptateur.

4. Cliquez sur l'hôte d'adaptateur de votre choix.

   La configuration de l'hôte que vous sélectionnez s'ouvre dans le volet Détails.

5. Sélectionnez l'onglet Etat.

   Les informations d'état s'affichent.

   Remarque : Les informations d'état apparaissent uniquement dans le panneau de configuration locale.

Remarques sur le service SAPI

CA Enterprise Log Manager utilise deux instances d'un service SAPI (Submit Application Programming Interface) CA Audit, l'une installée en tant que collecteur SAPI, l'autre en tant que routeur SAPI. Les services SAPI sont généralement utilisés pour recevoir des événements de clients et produits intégrés CA Audit existants. Vous pouvez configurer les adaptateurs SAPI à l'aide des paramètres suivants.

Activer l'écouteur

Active le service sélectionné. Ce paramètre est activé par défaut.

Port SAPI

Définit un numéro de port spécifique pour le service sélectionné, s'il n'est pas enregistré avec le mappeur de ports. La valeur par défaut, 0, permet au service d'utiliser un port déterminé de manière aléatoire, si la case à cocher Enregistrer est sélectionnée.

Remarque : Le numéro de port doit être différent pour le collecteur SAPI et le routeur. Si les mêmes ports sont définis pour les deux services, le deuxième ne fonctionne pas.

Enregistrer

Détermine si le service enregistre avec le mappeur de ports du système. Si vous sélectionnez Enregistrer et saisissez 0 dans le champ Port SAPI, un port est sélectionné de manière aléatoire à chaque démarrage du service. Il s'agit du paramétrage par défaut pour les deux champs. Si Enregistrer n'est pas sélectionné, vous devez spécifier un port SAPI.

Clé de chiffrement

Définit la clé de chiffrement, si vous utilisez une clé de chiffrement non standard dans votre environnement CA Audit, que l'adaptateur SAPI utilise pour lire les événements SAPI entrants.

Classement des événements

S'assure que les événements sont envoyés au magasin de journaux d'événements dans l'ordre exact de réception. En cas de désactivation du classement des événements, l'ordre peut ne pas être respecté si certains événements sont analysés et transmis plus rapidement que d'autres. L'activation du classement des événements peut avoir un impact sur les performances de par l'augmentation de la taille de la file d'attente d'événements.

Régulation des événements

Définit le nombre maximal d'événements dans la file d'attente de traitement des événements, ce qui permet de contrôler les ressources de traitement. Aucune régulation n'est effectuée lorsque la valeur 0 est saisie dans ce champ. Les événements au-delà du seuil sont retardés à la source.

Nombre de threads par file d'attente

Définit le nombre de threads de traitement pour chaque protocole. L'utilisation de nombreux threads de traitement accélère le traitement si le classement des événements est désactivé. Si le classement des événements est activé, le nombre de threads n'a pas d'effet. L'utilisation d'un grand nombre de threads peut nuire aux performances.

Chiffre et mappage de données

- Le contrôle de déplacement Chiffres détermine celui des chiffres disponibles que le service utilise pour déchiffrer les messages entrants.
- Le contrôle de déplacement de fichier de mappage de données détermine celui des fichiers de mappage de données disponibles que le service utilise pour le mappage d'événements.

Les paramètres de journalisation contrôlent la manière dont les différents modules CA Enterprise Log Manager enregistrent les messages internes. Ils sont uniquement disponibles en tant que paramètres locaux. Les paramètres de journalisation sont généralement utilisés à des fins de dépannage. Il n'est généralement pas nécessaire de modifier ces paramètres ; il est essentiel de bien comprendre le fonctionnement des fichiers journaux et de la journalisation avant d'effectuer tout changement.

Niveau de journal

Définit le type et le niveau de détail enregistrés dans le fichier journal. La liste déroulante est classée dans l'ordre croissant du niveau de détail.

Appliquer à tous les enregistreurs

Détermine si le paramètre Niveau de journal écrase tous les paramètres de journal issus du fichier des propriétés du journal. Ce réglage s'applique uniquement lorsque le paramètre Niveau de journal est inférieur (plus détaillé) au paramètre par défaut.

Remarques sur le service d'événement iTechnology

Le service iTechnology contrôle les événements envoyés par le démon iGateway. Vous pouvez configurer le service en définissant le fichier de mappage de données que le service utilise pour le mappage d'événements, à l'aide du contrôle de déplacement de fichier de mappage de données.

Le service du module d'extension d'événements est préconfiguré pour inclure la plupart des principaux fichiers de mappage de données.

Les paramètres de journalisation contrôlent la manière dont les différents modules CA Enterprise Log Manager enregistrent les messages internes. Ils sont uniquement disponibles en tant que paramètres locaux. Les paramètres de journalisation sont généralement utilisés à des fins de dépannage. Il n'est généralement pas nécessaire de modifier ces paramètres ; il est essentiel de bien comprendre le fonctionnement des fichiers journaux et de la journalisation avant d'effectuer tout changement.

Niveau de journal

Définit le type et le niveau de détail enregistrés dans le fichier journal. La liste déroulante est classée dans l'ordre croissant du niveau de détail.

Appliquer à tous les enregistreurs

Détermine si le paramètre Niveau de journal écrase tous les paramètres de journal issus du fichier des propriétés du journal. Ce réglage s'applique uniquement lorsque le paramètre Niveau de journal est inférieur (plus détaillé) au paramètre par défaut.

Tâches Etat du système

Vous pouvez effectuer les opérations suivantes à partir du service Etat du système.

- Vérifier l'état et la version des services du système.
- Vérifier les événements d'autosurveillance relatifs à l'utilisation et aux composants du système.
- Créer un fichier de diagnostic de support.
- Redémarrez le service iGateway.
- Redémarrez le serveur hôte sur lequel fonctionne un serveur CA Enterprise Log Manager.

Informations complémentaires :

Créez un fichier de diagnostic pour le support technique. (page 166)
Redémarrage d'un serveur hôte (page 167)
Redémarrage du service iGateway (page 167)
Vérification de l'état et de la version des services (page 168)
Vérification des événements d'autosurveillance de l'état d'un système (page 168)

Créez un fichier de diagnostic pour le support technique.

Vous pouvez vérifier l'état et la version des services en cours d'exécution sur un serveur CA Enterprise Log Manager sélectionné. Cliquer sur Diagnostic de support exécute le script LmDiag.sh fourni avec CA Enterprise Log Manager.

Cet utilitaire rassemble les informations du système et les fichiers journaux en un fichier .tar compressé pour la transmission au personnel de support CA. Vous pouvez transférer ce fichier à l'aide de FTP ou d'une autre méthode de transfert de fichiers.

Remarque : Certaines informations dans le fichier obtenu peuvent être sensibles, notamment les adresses IP, les configurations de système, les journaux de matériel et les journaux de processus. Utilisez une méthode sécurisée pour le stockage et le transfert de ce fichier.

Pour créer un fichier de diagnostic

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

   La configuration du service Etat du système affiche l'onglet Administration.
4. Cliquez sur Diagnostic de support.
5. Sélectionnez un emplacement de fichier pour le téléchargement du fichier de diagnostic généré.

   L'utilitaire crée le fichier et le télécharge à l'emplacement spécifié. L'utilitaire se ferme automatiquement une fois le fichier copié.

Redémarrage d'un serveur hôte

Vous pouvez vérifier l'état et la version des services en cours d'exécution sur un serveur CA Enterprise Log Manager sélectionné.

Important : Utilisez cette fonctionnalité uniquement lorsque cela est nécessaire, ou lorsque le service de support de CA vous y invite. Le redémarrage d'un serveur CA Enterprise Log Manager l'empêche de recevoir, d'analyser et de stocker les journaux d'événements tant que le redémarrage n'est pas terminé. Si vous redémarrez le serveur de gestion, les sessions CA Enterprise Log Manager gérées sur d'autres serveurs ou sur des serveurs associés doivent se déconnecter et se reconnecter.

Pour redémarrer un serveur hôte

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

   La configuration du service Etat du système affiche l'onglet Administration.
4. Cliquez sur Redémarrer l'hôte.

Redémarrage du service iGateway

Vous pouvez redémarrer le service iGateway en cours d'exécution sur un serveur CA Enterprise Log Manager sélectionné.

Important : Utilisez cette fonctionnalité uniquement lorsque cela est nécessaire, ou lorsque le service de support de CA vous y invite. Lors du redémarrage du service iGateway, le serveur CA Enterprise Log Manager affecté ne peut plus recevoir, analyser, ni stocker de journaux d'événements tant que le redémarrage n'est pas achevé. Si vous redémarrez le serveur de gestion, la session actuelle et toutes les autres sessions CA Enterprise Log Manager sur les autres serveurs doivent se déconnecter et se reconnecter.

Pour redémarrer le service iGateway

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

   La configuration du service Etat du système affiche l'onglet Administration.
4. Cliquez sur Redémarrer iGateway.

Vérification de l'état et de la version des services

Vous pouvez vérifier l'état et la version des services en cours d'exécution sur un serveur CA Enterprise Log Manager sélectionné.

Pour vérifier l'état

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

Vérification des événements d'autosurveillance de l'état d'un système

Vous pouvez vérifier l'état et la version des services en cours d'exécution sur un serveur CA Enterprise Log Manager sélectionné. Les messages d'état incluent des événements relatifs à l'utilisation du processeur et de l'espace disque, aux moyennes de charge de l'UC, à l'utilisation de la mémoire, à l'utilisation et à l'accès au matériel, ainsi qu'à d'autres événements.

Pour vérifier les événements d'autosurveillance

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

Chapitre 6 : Stockage des journaux

Ce chapitre traite des sujets suivants :

A propos du stockage des journaux

Vous pouvez gérer deux aspects du stockage des journaux par le biais de CA Enterprise Log Manager.

- La sauvegarde des bases de données de fichiers journaux dans le répertoire d'archivage de chaque serveur de rapports vers un répertoire d'archivage que vous créez sur un serveur de stockage distant ; le serveur de stockage distant est un emplacement temporaire destiné à contenir les bases de données archivées jusqu'à ce qu'elles puissent être stockées hors site.
- La restauration des bases de données de fichiers journaux depuis un répertoire d'archivage sur un serveur de stockage distant vers le serveur de rapports d'origine ou un serveur CA Enterprise Log Manager défini en tant que point de restauration ; une fois les fichiers restaurés, vous pouvez en examiner le contenu à l'aide de requêtes et de rapports.

Vous pouvez gérer les sauvegardes des bases de données de journaux d'événements de l'une des manières ci-dessous.

- Configurez CA Enterprise Log Manager pour déplacer les bases de données tièdes vers un serveur de stockage distant par le biais d'un archivage automatique planifié (solution à privilégier). Le processus d'archivage automatique notifie le serveur CA Enterprise Log Manager que les bases de données ont été sauvegardées.

  Remarque : Consultez la section "A propos de l'archivage automatique" du *Manuel d'implémentation CA Enterprise Log Manager.*

- Sauvegardez manuellement les bases de données dans un emplacement de stockage sur site et utilisez l'utilitaire LMArchive pour indiquer au serveur CA Enterprise Log Manager de marquer ces bases de données comme étant sauvegardées.

  Le déplacement de fichiers sauvegardés vers un emplacement hors site est une tâche à effectuer en dehors de CA Enterprise Log Manager, de même que leur rapatriement sur le réseau, lorsque cela est nécessaire à la restauration.

Vous pouvez interroger le catalogue d'archive pour identifier les fichiers de bases de données à restaurer. Vous pouvez restaurer les bases de données selon l'évolution de vos besoins de l'une des manières suivantes.

- Vous pouvez les restaurer sur le serveur de rapports d'origine en utilisant l'une des méthodes ci-dessous.
  - Si vous avez configuré l'archivage automatique, exécutez le script restore-ca-elm.sh pour les restaurer depuis le serveur de stockage distant.

    Une fois les fichiers restaurés, effectuez une requête sur ces fichiers et générez les rapports les concernant pendant la période (en jours) configurée en tant que durée de vie des fichiers compressés.
  - Si vous avez sauvegardé manuellement les bases de données d'archive, recopiez les fichiers dans le même répertoire d'archive, puis notifiez ce serveur CA Enterprise Log Manager de la restauration. Vous utilisez une option de l'utilitaire de ligne de commande LMArchive pour informer CA Enterprise Log Manager des bases de données restaurées.

    Une fois les fichiers restaurés, effectuez une requête sur ces fichiers et générez les rapports les concernant pendant la période (en heures) configurée en tant que durée de vie des fichiers dégivrés.

- Vous pouvez les restaurer dans un autre magasin de journaux d'événements, à savoir un serveur de point de restauration dédié à l'examen des journaux d'événements restaurés, à l'aide de l'une des méthodes ci-après.
  - Si vous avez configuré le point de restauration en vue d'une authentification non interactive, vous pouvez exécuter le script restore-ca-elm.sh pour les restaurer depuis le serveur distant.
  - Si vous n'avez pas configuré le point de restauration en vue d'une authentification non interactive, copiez manuellement les bases de données d'archive dans le répertoire d'archive de ce serveur. Notifiez ensuite ce CA Enterprise Log Manager de la restauration avec un recatalogage à partir de la Requête de catalogue d'archive, dans l'Explorateur de collecte de journaux.

    Cette notification entraîne la reconstruction du catalogue, ce qui rend les fichiers de bases de données disponibles pour les requêtes et les rapports. Cette disponibilité repose sur le fait que la valeur configurée pour l'ancienneté (en jours) avant suppression des fichiers compressés soit supérieure à l'ancienneté des fichiers restaurés. Par conséquent, il est important que l'ancienneté maximale des fichiers compressés soit défini de manière appropriée sur tout point de restauration dédié.

Informations complémentaires

Exemple : Archivage automatique sur trois serveurs (page 174)
Configuration de l'authentification non interactive pour la restauration (page 181)
Restauration des fichiers archivés automatiquement (page 185)
Sauvegarde manuelle des bases de données archivées (page 188)
Configuration du nombre maximal de jours d'archivage pour les archives restaurées (page 201)
Restauration manuelle des archives dans le magasin de journaux d'événements d'origine (page 192)
Restauration manuelle des archives dans un nouveau magasin de journaux d'événements (page 199)
Remarques sur le magasin de journaux d'événements (page 147)
Restauration : Script de restauration des bases de données archivées (page 186)
LMArchive–Backup/Restore Tracking (page 203)

Etats des bases de données de journaux d'événements

Lorsque vous configurez l'archivage automatique sur trois serveurs (collecte, génération de rapports et stockage à distance), toutes les bases de données de journaux d'événements passent successivement par trois états : chaud, tiède et froid. Dans cette architecture, les bases de données de journaux chaudes sont uniquement présentes sur le serveur de collecte. Le serveur de rapports détient les bases de données tièdes. Enfin, le serveur de stockage distant stocke uniquement les bases de données froides. Lorsqu'une base de données froide est restaurée à l'aide du script de commandes de restauration shell, elle est restaurée à l'état tiède. Lorsqu'elle est restaurée manuellement à l'aide de l'utilitaire LMArchive, elle est restaurée à l'état dégivré.

Les quatre états de stockage des journaux d'événements sont décrits de manière plus détaillée ci-dessous.

Chaude

Une seule base de données se trouve à l'*état chaud* dans le magasin de journaux d'événements d'un serveur de collecte , c'est dans cette base de données que les événements nouvellement traités sont insérés. Vous pouvez configurer le nombre maximum de nouveaux enregistrements à stocker dans une base de données chaude (Nombre maximum de lignes) avant de la compresser. Vous pouvez planifier l'archivage automatique de sorte qu'il déplace les bases de données tièdes du serveur de collecte au serveur de rapports configuré toutes les heures. Notez qu'il existe également une base de données chaudes sur le serveur de rapports pour l'insertion des événements d'autosurveillance.

Tiède

Les bases de données conservées dans le magasin de journaux d'événements du serveur de rapports se trouvent à l'*état tiède*. Si vous configurez un archivage automatique quotidien entre le serveur de rapports et un serveur de stockage distant, les bases de données tièdes sont conservées jusqu'à ce qu'elles soient déplacées sur le serveur de stockage distant ; elles sont ensuite automatiquement supprimées du serveur de rapports. Si vous ne configurez pas l'archivage automatique entre le serveur de rapports et un serveur de stockage distant, les bases de données tièdes peuvent demeurer sur le serveur de rapports jusqu'à ce que leur nombre de jours d'existence atteigne la valeur configurée pour Nbre max. de jours d'archivage ou que le seuil Espace disque d'archivage configuré soit atteint (dès que l'une de ces deux conditions est remplie). Lorsque l'un de ces seuils est atteint, la base de données est supprimée et passe à l'état froid. Sans archivage automatique, vous devez sauvegarder manuellement les bases de données tièdes à l'aide d'un outil tiers avant qu'elles ne soient supprimées, puis exécuter l'utilitaire LMArchive pour notifier les noms des bases de données que vous avez sauvegardées et déplacées à CA Enterprise Log Manager. L'état tiède s'applique également lorsqu'un recatalogage est effectué à l'aide du script restore-ca-elm.sh ou du bouton Recataloguer après restauration d'une base de données froide.

Froid

Les bases de données stockées sur le serveur de stockage distant se trouvent à l'*état froid*. Un enregistrement d'une base de données froide est créé sur le serveur de rapports lorsque la base de données est archivée automatiquement sur le serveur de gestion distant et supprimée du serveur de rapports. En cas de gestion manuelle, un enregistrement de la base de données froide est créé lorsque l'utilitaire LMArchive est exécuté à l'aide de l'option -notify arch. Vous pouvez interroger le catalogue d'archive d'un serveur de rapports pour identifier les bases de données froides à restaurer.

Dégivré

L'*état dégivré* est l'état qualifiant une base de données froide physique qui a été restaurée dans le répertoire d'archivage après l'exécution de l'utilitaire LMArchive par l'administrateur à l'aide de l'option -notify rest pour indiquer à CA Enterprise Log Manager qu'elle a été restaurée. Les bases de données dégivrées sont conservées pendant le nombre d'heures configuré pour la stratégie d'exportation.

Vous pouvez interroger les bases de données dans chacun de ces états. Une requête normale renvoie les données d'événement issues des bases de données chaudes et tièdes sur le serveur de rapports ainsi que des bases de données dégivrées, si elles existent. Une requête fédérée renvoie les données d'événement de tous les serveurs de la fédération, y compris les serveurs de collecte fédérés qui incluent les bases de données chaudes. Une requête d'archivage renvoie la liste des bases de données qui n'existent plus sur le serveur de rapports, c'est-à-dire des bases de données à l'état froid. Des bases de données physiques représentées par une requête d'archivage peuvent exister sur le serveur de stockage distant utilisé pour le stockage sur site ou hors site.

Informations complémentaires :

Sauvegarde et restauration automatiques (page 180)
Sauvegarde manuelle des bases de données archivées (page 188)
Restauration manuelle des archives dans le magasin de journaux d'événements d'origine (page 192)
Restauration manuelle des archives dans un nouveau magasin de journaux d'événements (page 199)
Remarques sur le magasin de journaux d'événements (page 147)

Exemple : Archivage automatique sur trois serveurs

Dans une architecture collecte-génération de rapports, vous devez configurer l'archivage automatique entre le serveur de collecte et un serveur de rapports. Cette configuration automatise le déplacement d'une base de données tiède, contenant les données de journaux d'événements collectés et ajustés, vers le serveur de rapports sur lequel vous pouvez effectuer la génération de rapports. Il est recommandé de planifier cet archivage automatique toutes les heures, plutôt qu'une fois par jour, afin d'éviter de longs transferts quotidiens. Choisissez une planification basée sur votre charge et indiquez si vous souhaitez regrouper le traitement en une fois ou le répartir sur la journée. Lorsque la copie des bases de données s'effectue via un archivage automatique à partir d'un serveur de collecte vers son serveur de rapports, les bases sont supprimées du serveur de collecte.

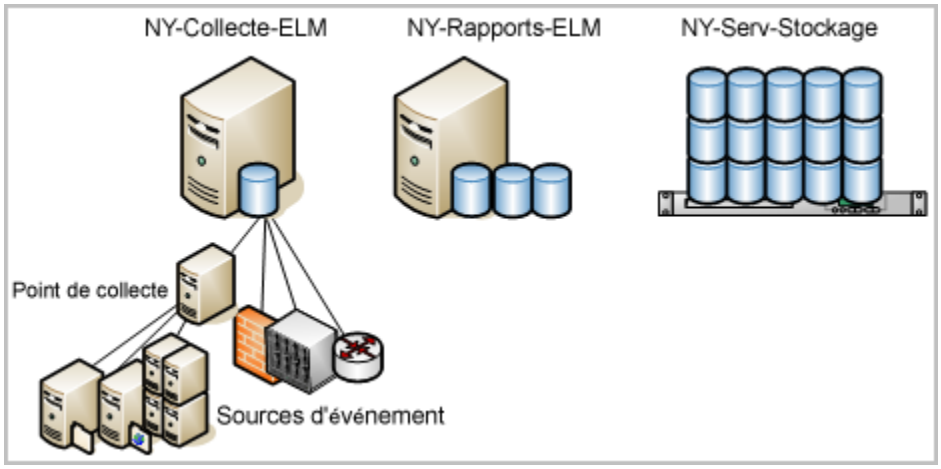
Après avoir identifié un serveur local disposant d'un espace de stockage suffisant, vous pouvez configurer l'archivage automatique du serveur de rapports vers ce serveur de stockage distant. Lorsque la copie des bases de données s'effectue via l'archivage automatique, à partir d'un serveur de rapports vers un serveur de stockage distant, les bases restent intactes sur le serveur de rapports jusqu'à ce que le délai défini par le paramètre Nbre max. de jours d'archivage soit écoulé. A ce moment seulement elles sont supprimées. L'avantage de cette phase d'archivage automatique est qu'elle évite la perte des bases de données archivées si celles-ci ne sont pas déplacées manuellement jusqu'à l'emplacement de stockage à long terme avant leur suppression automatique.

Remarque : Avant de configurer un serveur distant pour recevoir les bases de données archivées automatiquement, vous devez créer une structure de répertoires sur le serveur de destination, identique à celle existant sur le serveur CA Enterprise Log Manager source, puis affecter des droits de propriétés et des autorisations pour l'authentification. Pour plus de détails, consultez la section "Configuration d'une authentification non interactive", dans le *Manuel d'implémentation*. Veillez à bien suivre les instructions décrites dans la section "Définition de la propriété du fichier de clé sur un hôte distant".

Dans le cadre du présent scénario, imaginons que vous êtes administrateur CA Enterprise Log Manager d'un centre de données situé à New York et doté d'un réseau de serveurs CA Enterprise Log Manager, chacun possédant un rôle dédié, plus un serveur distant disposant d'une capacité de stockage importante. Les noms des serveurs utilisés pour l'archivage automatique sont les suivants.

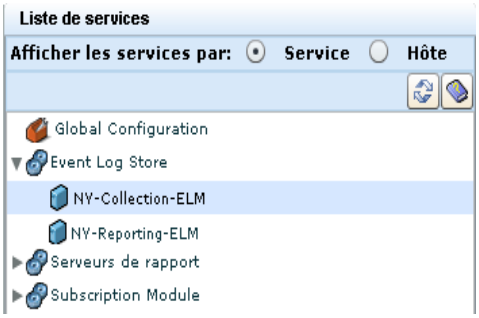
- NY-Collecte-ELM
- NY-Rapports-ELM
- NY-Serv-Stockage

Remarque : Cet exemple suppose l'existence d'un serveur de gestion dédié à l'administration du système de serveurs CA Enterprise Log Manager. Ce serveur n'est pas décrit ici car il n'a pas de fonction directe dans la procédure d'archivage automatique.



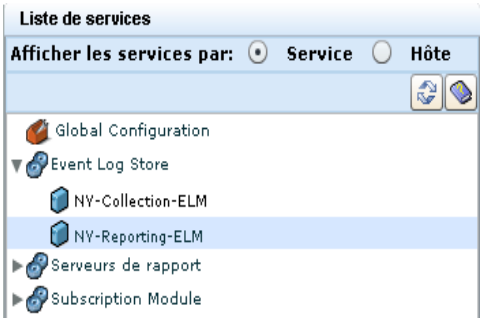
Pour configurer l'archivage automatique entre un serveur de collecte et un serveur de rapports, puis entre ce dernier et un serveur de stockage distant, basez-vous sur l'exemple suivant.

1. Sélectionnez l'onglet Administration, puis le sous-onglet Collecte de journaux.
2. Développez le dossier Magasin de journaux d'événements, puis sélectionnez un serveur de collecte.

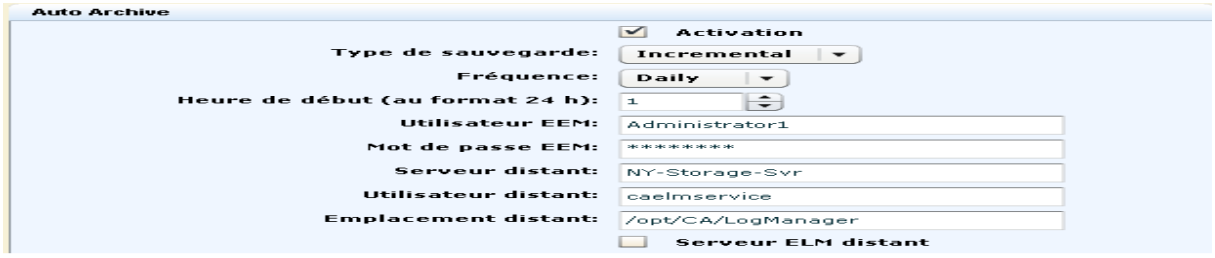


3. Indiquez une récurrence d'archivage automatique toutes les heures, avec le serveur de rapports comme destination. Entrez les informations d'identification d'un utilisateur CA Enterprise Log Manager doté d'un rôle d'administrateur. Si vous utilisez des stratégies personnalisées, cet utilisateur doit disposez de droits de modification sur les ressources de base de données, qui lui donnent la possibilité de supprimer la base de données archivée.

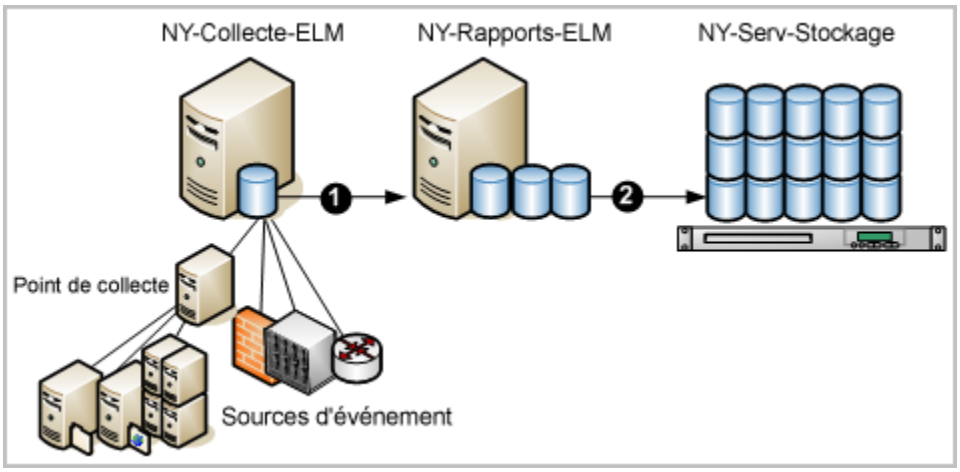
4. Dans la Liste de services, sélectionnez le serveur de rapports.



5. Indiquez une récurrence d'archivage automatique tous les jours, avec un serveur distant comme destination de stockage. Entrez les informations d'identification d'un compte d'utilisateur doté d'un rôle d'administrateur. Vous pouvez également créer une stratégie d'accès CALM avec l'action de modification sur les ressources de base de données et affecter un utilisateur comme identité. Dans ce cas, entrez les informations d'identification d'un utilisateur disposant de peu de droits.



Les numéros figurant sur le diagramme suivant représentent deux configurations d'archivage automatique : une entre le serveur de collecte et le serveur de rapports et une autre entre le serveur de rapports et un serveur distant du réseau.

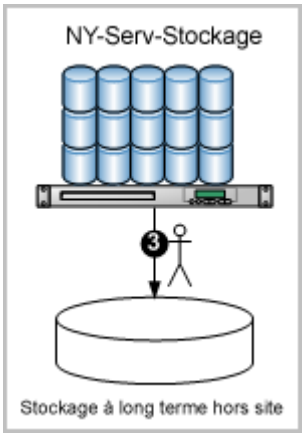


Dans une telle configuration, la procédure automatique fonctionne comme suit.

1. NY-Collecte-ELM, serveur de collecte CA Enterprise Log Manager, collecte et ajuste les événements et les intègre à la base de données chaude. Lorsque la base de données chaude atteint le nombre d'enregistrements configuré, elle est compressée. L'archivage automatique étant planifié toutes les heures, le système copie les bases de données tièdes une fois par heure et les transfère sur le serveur de rapports CA Enterprise Log Manager, NY-Rapports-ELM. Les bases de données tièdes sont supprimées du serveur NY-Collecte-ELM lors du déplacement.
2. NY-Rapports-ELM conserve les bases de données pouvant faire l'objet de requêtes tant que le délai défini par le paramètre Nbre max. de jours d'archivage n'est pas écoulé. L'archivage automatique étant planifié tous les jours, le système déplace quotidiennement les bases de données tièdes et les transfère sur NY-Serv-Stockage en tant que bases de données froides. Ces dernières peuvent être conservées sur le serveur de stockage pendant une longue période.

3. Pour conserver les bases de données froides pendant le nombre d'années requis, transférez-les depuis NY-Serv-Stockage sur le réseau jusqu'à un système de stockage à long terme hors site.

   La fonction de l'archivage est de garder les journaux d'événements à disposition à des fins de restauration. Les bases de données froides peuvent être restaurées si nécessaire, afin d'étudier des événements consignés dans les journaux. Le déplacement manuel des bases de données archivées, entre le serveur de stockage sur site et le système de stockage à long terme hors site, est illustré dans le schéma suivant.

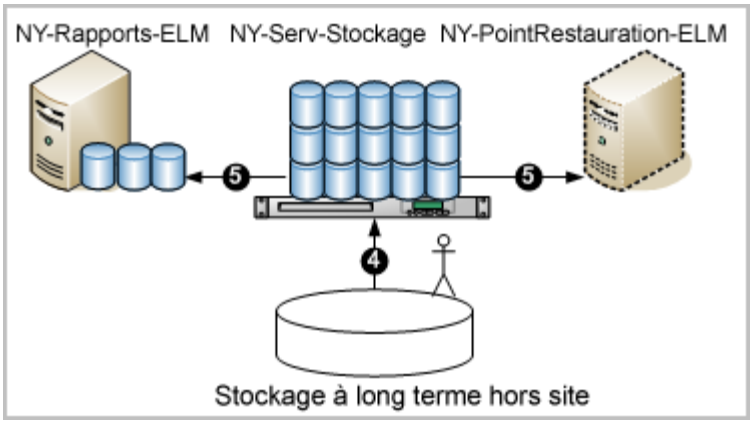


4. Imaginez une situation où il serait nécessaire d'étudier des journaux sauvegardés et stockés hors site. Pour identifier le nom de la base de données archivée à restaurer, faites une recherche dans le catalogue d'archive local sur NY-Rapports-ELM. Pour ce faire, cliquez sur l'onglet Administration, sélectionnez Requête de catalogue d'archive dans l'Explorateur de collecte de journaux, puis cliquez sur Requête.

5. Récupérez la base de données archivée identifiée dans le stockage hors site. Copiez-la dans le répertoire /opt/CA/LogManager/data/archive, sur le serveur de stockage NY-Serv-Stockage. Modifiez ensuite la propriété du répertoire d'archivage en sélectionnant l'utilisateur caelmservice.

6. Restaurez la base de données sur son serveur de rapports d'origine ou à un point de restauration dédié à l'étude des journaux contenus dans les bases de données restaurées, en procédant comme suit.

   - Si vous restaurez la base sur NY-Rapports-ELM, exécutez le script restore-ca-elm.sh à partir de NY-Rapports-ELM, en spécifiant NY-Serv-Stockage comme hôte distant.
   - Si vous restaurez la base sur NY-PointRestauration-ELM, exécutez le script restore-ca-elm.sh à partir de NY-PointRestauration-ELM en spécifiant NY-Serv-Stockage comme hôte distant.



   Remarque : Vous pouvez désormais créer des requêtes et des rapports sur les données restaurées.

Informations complémentaires :

Remarques sur le magasin de journaux d'événements (page 147)

Sauvegarde et restauration automatiques

La meilleure méthode pour sauvegarder des bases de données archivées est l'archivage automatique. L'archivage automatique est un transfert automatisé des bases de données archivées, qui s'effectue entre des paires de serveurs à la fréquence que vous avez spécifiée. Vous pouvez configurer l'archivage automatique :

- entre des serveurs de collecte et des serveurs de rapports ;
- entre des serveurs de rapports et un serveur de stockage distant.

L'archivage automatique entre un serveur de rapports et un serveur de stockage distant simplifie la procédure de restauration des bases de données archivées sur ce serveur distant vers le serveur de rapports d'origine. Pour réaliser cette procédure de restauration, vous utilisez le script restore-ca-elm.sh.

Tout comme le processus d'archivage automatique, le script restore-ca-elm.sh utilise une authentification non interactive, c'est-à-dire sans mot de passe, entre le serveur source et le serveur de destination. L'authentification sans mot de passe est une authentification par clé publique RSA, sans phrase de passe. Vous pouvez activer l'authentification sans mot de passe à des fins de restauration, dans les cas suivants.

- Entre le serveur de stockage distant et chaque serveur de rapports d'origine
- Entre le serveur de stockage distant et un serveur unique de point de restauration

Générez une paire de clés RSA sur le serveur de stockage distant et copiez le fichier de clé publique (id_rsa.pub) dans le répertoire /tmp/authorized_keys, sur le serveur de rapports de destination ou sur le serveur de point de restauration. Créez les comptes d'utilisateur caelmadmin et caelmservice. Créez le répertoire ssh avec caelmservice comme propriétaire, puis déplacez le fichier de clé dans ce nouveau répertoire.

Informations complémentaires :

Configuration de l'authentification non interactive pour la restauration (page 181)
Restauration des fichiers archivés automatiquement (page 185)
Exemple : Archivage automatique sur trois serveurs (page 174)
Remarques sur le magasin de journaux d'événements (page 147)

Configuration de l'authentification non interactive pour la restauration

Pour utiliser le script shell de restauration, vous devez d'abord configurer l'authentification non interactive *ssh* à l'aide de paires de clés RSA. Pour ce faire, vous devez faire appel à deux serveurs : le serveur distant, utilisé pour le stockage, et le serveur permettant la restauration des bases de données. *Non interactive* signifie qu'un serveur peut déplacer des fichiers vers un autre serveur sans nécessiter de mot de passe.

Cette procédure suppose que vous avez préalablement défini la propriété du fichier de clé sur l'hôte distant pour l'archivage automatique. Cette procédure crée les éléments suivants : l'utilisateur caelmadmin, le groupe caelmservice, l'utilisateur caelmservice, le répertoire /opt/CA/LogManager, comme répertoire de base pour caelmservice, et le répertoire .ssh, dont la propriété est définie sur le groupe et l'utilisateur caelmservice:caelmservice.

Remarque : Pour plus de détails, consultez la section "Définition de la propriété du fichier de clé sur un hôte distant" du *Manuel d'implémentation*.

Pour activer l'authentification non interactive du serveur distant vers le point de restauration

1. A partir du serveur distant, générez une paire de clés RSA en tant qu'utilisateur caelmservice, puis copiez la clé publique dans le répertoire /tmp/authorized_keys sur le serveur où vous souhaitez restaurer les bases de données.
   a. Connectez-vous, en tant qu'utilisateur caelmadmin et via ssh, au serveur distant utilisé pour le stockage.
   b. Basculez sur le compte d'utilisateur caelmservice.

      ```
      su – caelmservice
      ```

   c. Générez une paire de clés RSA en tant qu'utilisateur caelmservice.

      ```
      ssh-keygen –t rsa
      ```

   d. Acceptez toutes les valeurs par défaut et ne saisissez aucune phrase de passe.

e. Modifiez les autorisations du répertoire .ssh à l'aide de la commande ci-dessous.

```
chmod 755 .ssh
```

f. Naviguez jusqu'au répertoire .ssh.

```
cd .ssh
```

g. Copiez le fichier de clé publique, id_rsa.pub, dans le répertoire /tmp/authorized_keys situé sur le serveur où vous souhaitez restaurer les bases de données. Il peut s'agir de CA Enterprise Log Manager dédié, utilisé comme point de restauration, ou du serveur CA Enterprise Log Manager de gestion d'origine, à partir duquel cette base de données a été archivée automatiquement vers le serveur distant.

```
scp id_rsa.pub caelmadmin@<point_restauration>:/tmp/authorized_keys
```

2. Depuis le point de restauration, créez le répertoire .ssh en tant qu'utilisateur caelmadmin, copiez la clé publique dans ce répertoire et octroyez la propriété du fichier de clé à caelmservice.

a. Connectez-vous au point de restauration CA Enterprise Log Manager en tant que caelmadmin.

b. Basculez sur le compte d'utilisateur root.

```
su – root
```

c. Accédez au répertoire CA Enterprise Log Manager à l'aide de la commande ci-dessous.

```
cd /opt/CA/LogManager
```

d. Créez le répertoire .ssh.

```
mkdir .ssh
```

e. Octroyez la propriété du nouveau dossier au groupe et à l'utilisateur caelmservice, à l'aide de la commande ci-dessous.

```
chown caelmservice:caelmservice .ssh
```

f. Accédez au répertoire .ssh à l'aide de la commande ci-dessous.

```
cd .ssh
```

g. Copiez la clé publique du répertoire /tmp au répertoire .ssh.

```
cp /tmp/authorized_keys .
```

h. Octroyez la propriété du fichier de clé authorized_keys à caelmservice.

```
chown caelmservice:caelmservice authorized_keys
```

i. Modifiez les autorisations de ce fichier à l'aide de la commande ci-dessous.

```
chmod 644 authorized_keys
```

Requête dans le catalogue d'archive

Vous pouvez créer des requêtes pour rechercher le catalogue d'archive local des bases de données sauvegardées (stockées à distance), au moyen de filtres avancés ou rapides. Les résultats de la requête peuvent vous aider à identifier les fichiers de bases de données sauvegardées que vous devez restaurer pour examen.

Pour lancer une requête dans le catalogue d'archive

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

   La liste des dossiers de l'Explorateur de collecte de journaux s'affiche.

2. Cliquez sur le dossier Requête de catalogue d'archive.

   La boîte de dialogue de la requête d'archive s'affiche dans le volet Détails.

3. Sélectionnez ou saisissez la période de votre requête.

4. Cliquez sur Ajouter un filtre, sélectionnez une colonne, puis saisissez la valeur à rechercher. Vous pouvez ajouter plusieurs filtres.

5. Sélectionnez Exclure pour rechercher tous les journaux *excepté* ceux contenant la valeur saisie.

   Remarque : Si vous créez un filtre qui spécifie une colonne ne figurant *pas* dans le catalogue, CA Enterprise Log Manager renvoie toutes les bases de données correspondant à la période spécifiée, au lieu d'un champ vide. Cela signifie que vous n'avez pas besoin de connaître l'ensemble des colonnes du catalogue pour créer une requête d'archivage efficace.

6. Cliquez sur l'onglet Filtres avancés pour ajouter des filtres avancés (facultatif). Inclut les informations de l'événement si la colonne porte la relation appropriée à la valeur saisie. Sélectionnez une colonne, choisissez un opérateur, puis sélectionnez ou saisissez une valeur. Voici une description des différents opérateurs.

   Opérateurs relationnels

   Egal à, Différent de, Inférieur à, Supérieur à, Inférieur ou égal à, Supérieur ou égal à.

   Identique à

   Inclut les informations sur l'événement si la colonne contient un modèle correspondant à votre saisie de texte avec le caractère générique, %. L% inclut les valeurs commençant par L. %L% inclut les valeurs contenant L et excluant un L comme premier ou dernier caractère.

Distinct de

Inclut les informations de l'événement si la colonne ne contient pas le modèle spécifié.

Dans l'ensemble

Inclut les informations de l'événement si la colonne contient au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Hors ensemble

Inclut les informations de l'événement si la colonne contient au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Correspondance

Inclut toute information d'événement qui correspond au moins à un des caractères que vous avez saisis, ce qui vous permet de rechercher des mots clés.

A clés

Inclut toute information d'événement définie comme une valeur clé pendant la configuration du serveur de rapports. Utilisez les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Sans clé

Inclut toute information d'événement non définie comme une valeur clé pendant la configuration du serveur de rapports. Utilisez les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

7. Cliquez sur Requête.

Les résultats de la requête s'affichent.

Restauration des fichiers archivés automatiquement

Si vous copiez des fichiers d'archive provenant d'un stockage externe sur un serveur distant configuré pour l'archivage automatique, vous pouvez les restaurer à l'aide du script restore-ca-elm.sh. Cette alternative est préférable à l'utilisation manuelle de l'utilitaire LMArchive.

Pour restaurer des fichiers archivés automatiquement

1. Utilisez vos informations d'identification caelmadmin pour vous connecter au serveur CA Enterprise Log Manager qui héberge le magasin de journaux d'événements dans lequel vous souhaitez restaurer les bases de données.
2. A l'invite de commande, basculez sur le compte d'utilisateur root.

   su - root

3. Accédez au répertoire /opt/CA/SharedComponents/iTechnology à l'aide du raccourci suivant.

   cd $IGW_LOC

4. A l'invite de commande, basculez sur le compte d'utilisateur caelmservice.

   su - caelmservice

5. Exécutez la commande suivante, où *userid* et *pwd* sont les informations d'identification d'un compte d'utilisateur CA Enterprise Log Manager avec le rôle Administrator.

   restore-ca-elm.sh -euser *userid* -epasswd *pwd* -rhost *hostname* -ruser *userid* -rlocation *path* -files file1,file2,file3...

   Remarque : Pour autoriser un utilisateur non administrateur à exécuter le script shell restore-ca-elm, créez un rôle et une stratégie personnalisés. Les utilisateurs auxquels vous affectez ce rôle personnalisé pourront spécifier leurs informations d'identification pour "userid" et "pwd".

Informations complémentaires :

Restauration : Script de restauration des bases de données archivées (page 186)
Exemple : Autorisation de gestion des archives par un non-administrateur (page 113)
Sauvegarde et restauration automatiques (page 180)

Restauration : Script de restauration des bases de données archivées

Vous ne pouvez pas effectuer de requête ni générer de rapport sur des données qui se trouvent dans une base de données froide sur un serveur de stockage distant. Pour effectuer des requêtes et générer des rapports sur des données de ce type, ces données doivent se trouver dans un état tiède sur un serveur CA Enterprise Log Manager. Le script shell de restauration, restore-ca-elf.sh, est un utilitaire de ligne de commande qui déplace une base de données froide vers un serveur CA Enterprise Log Manager et la restaure à l'état tiède. Vous pouvez utiliser l'utilitaire de restauration pour déplacer une base de données vers le serveur de rapports d'origine ou vers un point de restauration dédié.

Vous devez exécuter le script de restauration à partir du serveur CA Enterprise Log Manager sur lequel vous souhaitez restaurer les fichiers. L'hôte distant que vous identifiez dans la commande désigne le serveur de stockage distant. Les bases de données froides se trouvent dans le répertoire d'archivage du serveur de stockage distant.

Voici les conditions requises pour la restauration de fichiers de bases de données vers le serveur de rapports d'origine ou vers un serveur de point de restauration.

- La propriété du fichier de clé RSA a été définie sur le serveur distant.
- L'autorisation pour le dossier /opt/CA/LogManager a été accordée à caelmservice sur le serveur distant.

Si vous restaurez des fichiers vers un serveur de point de restauration, effectuez les actions suivantes.

1. Copiez la clé RSA du serveur de stockage distant vers le serveur de point de restauration.
2. Définissez la propriété du fichier de clé RSA sur le serveur de point de restauration.

La commande présente le format suivant

restore-ca-elm.sh -euser *userid* -epasswd *pwd* -rhost *hostname* -ruser *userid* -rlocation *path* -files *file1,file2,file3...*

-euser *username*

Spécifie le nom d'utilisateur d'un compte CA Enterprise Log Manager avec le rôle Administrator.

-epasswd *pwd*

Spécifie le mot de passe CA Enterprise Log Manager associé au nom d'utilisateur.

-rhost *host*

Spécifie le nom d'hôte ou l'adresse IP de l'hôte distant où se trouvent les fichiers de bases de données froides dans le répertoire d'archivage. L'hôte distant n'est pas un serveur CA Enterprise Log Manager.

-ruser *remote user*

Spécifie le compte d'utilisateur disposant d'autorisations pour l'emplacement /opt/CA/LogManager et la propriété du dossier .ssh contenant le fichier de clés autorisées. En général, ce compte d'utilisateur est le compte caelmservice.

-rlocation *path*

Spécifie le chemin d'accès aux fichiers de bases de données sur le serveur de stockage distant. S'il s'agit d'un serveur UNIX, le chemin d'accès est /opt/CA/LogManager/data/archive.

files *file1,file2,file3...*

Spécifie une liste séparée par des virgules, sans espaces, répertoriant les fichiers de bases de données que vous souhaitez restaurer.

Exemple : Script shell de restauration

Dans l'exemple suivant, la commande est exécutée à partir du serveur CA Enterprise Log Manager sur lequel les fichiers de bases de données archivées doivent être restaurés. Elle est exécutée par un utilisateur dont les informations d'identification son Administrator1, calm_r12. Le serveur distant sur lequel ont été déplacées les bases de données archivées, depuis le stockage hors site, est appelé NY-Serv-Stockage. Ce serveur distant a été configuré avec un compte caelmservice disposant de droits de propriété pour le dossier .ssh, dans lequel la clé publique RSA a été copiée. Ce compte dispose également de droits complets pour la structure de répertoires /opt/CA/LogManager. Cette commande spécifie que les fichiers à restaurer se situent dans le répertoire data/archive du serveur NY-Serv-Stockage et identifie lm_calmrh12_20081206192014.db comme étant le fichier de base de données à restaurer.

restore-ca-elm.sh -euser Administrator1 -epasswd calm_r12 -rhost NY-Serv-Stockage -ruser caelmservice -rlocation /opt/CA/LogManager/data/archive -files lm_calmrh12_20081206192014.db

Informations complémentaires :

Restauration des fichiers archivés automatiquement (page 185)

Sauvegarde manuelle des bases de données archivées

CA Enterprise Log Manager crée automatiquement une nouvelle base de données archivée chaque fois que des données sont déplacées d'un stockage non compressé à un stockage compressé, conformément à vos paramètres. Bien qu'il soit recommandé de configurer l'archivage automatique pour qu'il transfère les bases de données tièdes vers un serveur distant, vous pouvez utiliser vos propres outils pour réaliser des sauvegardes des bases de données archivées, puis exécuter l'utilitaire LMArchive pour notifier le système de la sauvegarde effectuée.

Nous vous recommandons de sauvegarder vos bases de données tièdes quotidiennement, soit par la méthode automatisée, soit par la méthode manuelle décrite ici. Cette action est importante car les fichiers d'archive stockés à l'état compressé sont automatiquement supprimés au bout de la période de temps spécifiée ou lorsque l'espace disque descend en dessous du pourcentage que vous avez indiqué.

La procédure de sauvegarde manuelle des bases de données tièdes se compose des étapes suivantes.

1. Identifier les bases de données tièdes qui ne sont pas encore sauvegardées.
2. Effectuer les sauvegardes.
3. Enregistrer les sauvegardes effectuées.

Informations complémentaires

Identification des bases de données non sauvegardées (page 188)
Sauvegardes (page 190)
Enregistrement des sauvegardes (page 190)

Identification des bases de données non sauvegardées

Vous pouvez afficher la liste des bases de données archivées qui ne sont pas encore marquées comme sauvegardées à l'aide de l'utilitaire LMArchive. Pour obtenir des résultats fiables, cet utilitaire doit avoir été exécuté avec l'option *-notify arch* à chaque sauvegarde d'une base de données archivée.

Important : Pour éviter toute confusion, veillez toujours à notifier CA Enterprise Log Manager des sauvegardes réalisées.

Pour afficher les noms de tous les fichiers de bases de données actuellement archivée non marqués comme sauvegardés

1. Utilisez vos informations d'identification **caelmadmin** pour vous connecter au serveur CA Enterprise Log Manager qui héberge le magasin de journaux d'événements contenant les bases de données qui nécessitent d'être sauvegardées pour l'archivage.
2. A l'invite de commande, basculez sur le compte d'utilisateur root.

   ```
   su - root
   ```

3. Accédez au répertoire /opt/CA/SharedComponents/iTechnology à l'aide du raccourci suivant.

   ```
   cd $IGW_LOC
   ```

4. Exécutez la commande suivante, où *username* et *pwd* sont les informations d'identification d'un compte d'utilisateur CA Enterprise Log Manager avec le rôle Administrator.

   ```
   LMArchive -euser username -epassword pwd –list inc
   ```

Exemple : Afficher tous les fichiers CA Enterprise Log Manager actuellement archivés non marqués comme sauvegardés

La commande suivante émise par un administrateur demande d'afficher la liste de toutes les bases de données tièdes qui ne sont pas marquées comme sauvegardées.

```
LMArchive -euser Administrator1 -epassword calmr12 -list inc
```

La liste des fichiers d'archive non marqués comme sauvegardés apparaît sous la forme suivante.

```
CAELM Archived Files (not backed up):
    lm_calmsundev04_20071206192014.db
```

Sauvegardes

Si vous n'avez pas configuré l'archivage automatique depuis un serveur de rapports CA Enterprise Log Manager vers un serveur de stockage distant qui n'est pas un serveur CA Enterprise Log Manager, vous devez sauvegarder manuellement les bases de données archivées et les déplacer à un emplacement de stockage sécurisé, comme un disque ou un serveur séparé.

Important : Assurez-vous de sauvegarder les bases de données et de les déplacer avant leur *suppression* du serveur de rapports CA Enterprise Log Manager.

Les bases de données tièdes sont automatiquement supprimées lorsque la valeur configurée pour Nbre max. de jours d'archivage est atteinte ou que le pourcentage d'espace disque descend en dessous de la valeur configurée pour Espace disque d'archivage. Pour empêcher toute perte de données des fichiers supprimés, effectuez des sauvegardes régulièrement.

Pour sauvegarder manuellement les bases de données tièdes

1. Utilisez vos informations d'identification caelmadmin pour vous connecter au serveur de rapports CA Enterprise Log Manager qui héberge le magasin de journaux d'événements contenant les bases de données cibles.
2. Basculez sur le compte d'utilisateur root.

   ```
   su - root
   ```

3. Accédez au répertoire /opt/CA/LogManager/data/archive.
4. Sauvegardez les bases de données tièdes avec l'outil de sauvegarde de votre choix et déplacez-les vers un serveur de stockage provisoire sur site ou vers un emplacement hors site pour le stockage longue durée, conformément aux procédures de votre site.

Enregistrement des sauvegardes

Chaque fois que vous réalisez une sauvegarde d'une ou plusieurs bases de données archivées, assurez-vous d'enregistrer cette information dans le serveur CA Enterprise Log Manager sur lequel la sauvegarde a été effectuée.

Remarque : Le non-enregistrement de chaque sauvegarde peut entraîner des données incorrectes lors de l'utilisation de l'utilitaire LMArchive pour obtenir la liste des bases de données sauvegardées.

Pour enregistrer les sauvegardes de bases de données archivées spécifiques

1. Utilisez vos informations d'identification caelmadmin pour vous connecter au serveur CA Enterprise Log Manager qui héberge le magasin de journaux d'événements contenant les bases de données sauvegardées.
2. A l'invite de commande, basculez sur le compte d'utilisateur root.

   su - root
3. Accédez au répertoire /opt/CA/SharedComponents/iTechnology à l'aide du raccourci suivant.

   cd $IGW_LOC
4. Exécutez la commande suivante, où *username* et *pwd* sont les informations d'identification d'un compte d'utilisateur CA Enterprise Log Manager avec le rôle Administrator.

   LMArchive -euser *username* -epassword *pwd* –notify arch –files *file1*,*file2*,*file3*...

Exemple : Notifier CA Enterprise Log Manager que certains fichiers ont été sauvegardés

La commande suivante émise par l'administrateur nommé Administrator1 notifie le magasin de journaux d'événements CA Enterprise Log Manager que la base de données tiède lm_calmsundev04_20071206192014.db a été sauvegardée. Les bases de données sauvegardées peuvent être transférées manuellement vers un stockage externe en vue d'une conservation à long terme.

LMArchive -euser Administrator1 -epassword calmr12 -notify arch -files lm_calmsundev04_20071206192014.db

La notification de fichier archivé apparaît sous la forme suivante.

Archive notification sent for file lm_calmsundev04_20071206192014.db...

Restauration manuelle des archives dans le magasin de journaux d'événements d'origine

Il est possible que vous ayez parfois besoin de restaurer des fichiers de bases de données froides pour exécuter des requêtes ou générer des rapports dans le répertoire d'archivage d'un serveur CA Enterprise Log Manager, afin d'enquêter sur une brèche de sécurité ou de réaliser un audit de conformité annuel ou semi-annuel. Les procédures utilisées dépendent des deux facteurs suivants.

- Le fait que vous ayez ou non utilisé l'archivage automatique pour sauvegarder les fichiers que vous souhaitez à présent restaurer
- Le fait que vous restauriez ou non les fichiers sur le serveur de rapports d'origine ou sur un autre serveur, tel qu'un serveur de point de restauration dédié

  Si vous restaurez les fichiers sur un autre serveur, consultez la section "Restauration d'archives dans un nouveau magasin de journaux d'événements".

Respectez la procédure suivante lors de la restauration de fichiers sur le serveur de rapports d'origine.

1. Préparez la restauration des bases de données archivées en identifiant les fichiers à restaurer et en déterminant le répertoire d'archivage.
2. Déplacez les bases de données du stockage externe vers le répertoire d'archivage, soit à l'emplacement du serveur distant que vous avez configuré pour l'archivage automatique, soit sur le serveur de rapports d'origine.
3. Si vous avez déplacé les fichiers archivés sur le serveur de stockage distant configuré pour l'archivage automatique, connectez-vous au serveur CA Enterprise Log Manager de génération de rapports et restaurez les fichiers archivés automatique à partir du serveur de stockage distant à l'aide du script restore-ca-elm.sh.
4. Si vous avez déplacé les fichiers archivés dans le répertoire d'archivage sur leur serveur CA Enterprise Log Manager de génération de rapports d'origine, restaurez les fichiers archivés manuellement à l'aide de l'utilitaire LMArchive.
5. Vérifiez que la base de données dégivrée peut être interrogée : exécutez une requête avec pour date de fin la date de la base de données restaurée et examinez les résultats obtenus.

Informations complémentaires

Préparation à la restauration de bases de données archivées (page 194)
Transfert des bases de données archivées vers un répertoire d'archivage (page 196)
Restauration des fichiers archivés automatiquement (page 185)
Restauration de fichiers archivés manuellement (page 197)
Vérification de la restauration (page 199)

Préparation à la restauration de bases de données archivées

Pour restaurer des bases de données archivées, vous devez au préalable connaître les informations suivantes.

- Le nom des fichiers à restaurer
- Le chemin d'accès au répertoire d'archivage dans lequel vous souhaitez copier les fichiers récupérés à partir du système de stockage hors site ; le chemin est toujours /opt/CA/LogManager/data/archive

Vous pouvez effectuer une requête sur le catalogue d'archive par le biais de l'onglet CA Enterprise Log Manager Administration, dans l'Explorateur de collecte de journaux, où vous pouvez spécifier des filtres simples ou avancés. Vous pouvez aussi vous servir de l'utilitaire de ligne de commande, comme indiqué ci-dessous.

Si vous possédez déjà toutes les informations nécessaires, ignorez cette procédure.

Pour préparer la restauration de bases de données archivées

1. Utilisez vos informations d'identification caelmadmin pour vous connecter au serveur CA Enterprise Log Manager qui héberge le magasin de journaux d'événements dans lequel vous souhaitez restaurer les bases de données.
2. A l'invite de commande, basculez sur le compte d'utilisateur root.

   ```
   su - root
   ```

3. Accédez au répertoire /opt/CA/SharedComponents/iTechnology à l'aide du raccourci suivant.

   ```
   cd $IGW_LOC
   ```

4. Identifiez les bases de données que vous souhaitez restaurer dans la liste de fichiers des bases de données sauvegardées et transférées vers un stockage externe. Pour afficher la liste de tous les fichiers archivés dans ce catalogue, exécutez la commande suivante, où "userid" et "pwd" sont les informations d'identification d'un compte d'utilisateur CA Enterprise Log Manager avec le rôle Administrator.

   ```
   LMArchive -euser userid -epassword pwd -list all
   ```

   La liste de tous les fichiers archivés s'affiche.

5. Si vous effectuez la restauration à partir de sauvegardes manuelles, déterminez l'emplacement du répertoire d'archivage dans lequel les fichiers d'archive sauvegardés identifiés seront copiés (facultatif). Exécutez la commande suivante, où "userid" et "pwd" sont les informations d'identification d'un compte d'utilisateur CA Enterprise Log Manager avec le rôle Administrator.

   ```
   LMArchive -euser userid -epassword pwd -list loc
   ```

   Le répertoire d'archivage s'affiche.

Exemple : Affichage de tous les fichiers d'archive CA Enterprise Log Manager existants

La commande suivante, émise par l'administrateur CA Enterprise Log Manager (Administrator1), appelle une liste de toutes les bases de données situées dans le répertoire d'archivage du magasin de journaux d'événements.

```
LMArchive -euser Administrator1 -epassword calmr12 -list all
```

Une liste des fichiers d'archive existants s'affiche, dans un format similaire aux noms suivants.

```
Fichiers d'archive CAELM :
    lm_calmsundev04_20071206191941.db
    lm_calmsundev04_20071206191958.db
    lm_calmsundev04_20071206192014.db
```

Exemple : Affichage du répertoire d'archivage CA Enterprise Log Manager

La commande suivante, émise par l'administrateur CA Enterprise Log Manager (Administrator1), appelle l'emplacement du répertoire contenant les bases des données archivées.

```
LMArchive -euser Administrator1 -epassword calmr12 -list loc
```

Voici une réponse type :

```
Emplacement d'archivage CAELM (hôte local) :
../../LogManager/data/archive
```

Informations complémentaires :

Requête dans le catalogue d'archive (page 183)

Transfert des bases de données archivées vers un répertoire d'archivage

Si vous avez transféré vos fichiers archivés vers un emplacement hors site, suivez les procédures de votre site pour les récupérer et les rapatrier sur site.

Ramenez les bases de données archivées dans le répertoire d'archivage du serveur CA Enterprise Log Manager d'origine ou d'un serveur distant configuré pour une authentification non interactive. Le répertoire d'archivage est /opt/ca/LogManager/data/archive.

Pour déplacer une base de données archivée d'un stockage externe vers votre réseau

1. Rapatriez sur votre réseau les fichiers de bases de données à restaurer se trouvant actuellement sur un stockage externe de l'une des manières suivantes.
   - Si vous utilisez l'archivage automatique pour transférer automatiquement vos fichiers archivés sur le serveur distant, copiez-les de nouveau dans le répertoire d'archivage de ce serveur distant. Ce serveur distant est déjà configuré pour l'authentification non interactive avec le serveur CA Enterprise Log Manager sur lequel les bases de données archivées doivent être restaurées.
   - Si vous n'utilisez pas l'archivage automatique, copiez de nouveau vos fichiers archivés dans le répertoire d'archivage du serveur CA Enterprise Log Manager d'origine.
2. Procédez de l'une des manières suivantes, selon l'emplacement des fichiers archivés.
   - Si les fichiers archivés se trouvent sur le serveur distant configuré pour l'archivage automatique, restaurez les fichiers automatiquement archivés à l'aide du script restore-ca-elm.sh.
   - Si les fichiers archivés se trouvent dans le répertoire d'archivage sur leur serveur CA Enterprise Log Manager d'origine, notifiez CA Enterprise Log Manager que les fichiers archivés ont été restaurés à l'aide de l'utilitaire LMArchive. Suite à la notification, les fichiers restaurés sont placés à l'état dégivré.

Informations complémentaires :

Restauration des fichiers archivés automatiquement (page 185)
Restauration de fichiers archivés manuellement (page 197)

Restauration de fichiers archivés manuellement

Une fois que vous avez restauré une ou plusieurs bases de données d'un stockage à long terme vers le répertoire d'archivage, vous devez attribuer la propriété du répertoire d'archivage à l'utilisateur caelmservice avant de notifier CA Enterprise Log Manager que les bases de données ont été restaurées à l'aide de l'utilitaire LMArchive. Les fichiers archivés détenus par l'utilisateur root ne sont pas reconnus par l'utilitaire LMArchive.

L'exécution de LMArchive avec l'option -notify rest fait passer les fichiers de bases de données archivés de l'état froid à l'état dégivré ; ils deviennent ainsi disponibles pour les fonctions de requêtes et de rapports.

Les administrateurs configurent le nombre d'heures pendant lequel une base de données archivée dégivrée est conservée avant d'être automatiquement supprimée du répertoire d'archivage à l'aide du paramètre Exporter la stratégie dans la configuration du service du magasin de journaux d'événements.

Pour restaurer des fichiers de bases de données archivées manuellement

1. Utilisez vos informations d'identification **caelmadmin** pour vous connecter au serveur CA Enterprise Log Manager qui héberge le magasin de journaux d'événements contenant les bases de données restaurées.
2. A l'invite de commande, basculez sur le compte d'utilisateur root.

   ```
   su - root
   ```

3. Accédez au répertoire d'archivage. Par exemple :

   ```
   cd /opt/CA/LogManager/data/archive
   ```

4. Attribuez la propriété du répertoire d'archivage au compte caelmservice.

   ```
   chown -R caelmservice:caelmservice archive
   ```

   La propriété des fichiers archivés passe à caelmservice, l'utilisateur du système d'exploitation interne, qui est un compte sans connexion.

5. Accédez au répertoire /opt/CA/SharedComponents/iTechnology à l'aide du raccourci suivant.

   ```
   cd $IGW_LOC
   ```

6. Exécutez la commande suivante, où *username* et *pwd* sont les informations d'identification d'un compte d'utilisateur CA Enterprise Log Manager avec le rôle Administrator.

   LMArchive -euser *username* -epassword *pwd* –notify rest –files *file1*,*file2*,*file3*

   Un message de confirmation de la restauration apparaît. CA Enterprise Log Manager dégivre les fichiers spécifiés. Les fichiers dégivrés sont conservés pendant le nombre d'heures configuré ; la durée maximale de conservation des fichiers est de sept jours.

Remarque : Vous pouvez à présent exécuter des requêtes et générer des rapports sur les données d'événement contenues dans les fichiers d'archive restaurés.

Exemple : Notifier CA Enterprise Log Manager que certaines bases de données ont été restaurées

La commande suivante émise par un utilisateur CA Enterprise Log Manager avec un rôle Administrator notifie le magasin de journaux d'événements CA Enterprise Log Manager que la base de données froide, lm_calmsundev04_20071206192014.db, a été copiée dans le répertoire d'archivage.

```
LMArchive -euser Administrator1 -epassword calmr12 -notify rest -files lm_calmsundev04_20071206192014.db
```

Un message du type suivant s'affiche pour confirmer la restauration.

```
Restore notification sent for file lm_calmsundev04_20071206192014.db
```

Informations complémentaires :

Remarques sur le magasin de journaux d'événements (page 147)
LMArchive–Backup/Restore Tracking (page 203)

Vérification de la restauration

Il vous suffit d'exécuter une requête rapide pour vérifier en un instant que la base de données restaurée est disponible pour être examinée. Les requêtes normales affichent les données des bases de données restaurées ayant l'état tiède et dégivré.

Respectez la procédure ci-dessous.

1. Copiez une requête d'abonnement conçue pour afficher les types de détails d'événement contenus par la base de données restaurée.
2. Avancez jusqu'à l'étape de l'assistant de conception de la requête, où vous définissez les conditions de résultat et entrez une plage de dates correspondant aux fichiers de bases de données qui viennent d'être dégivrés.
3. Enregistrez la requête.
4. Exécutez la requête.

Restauration manuelle des archives dans un nouveau magasin de journaux d'événements

Il peut vous arriver d'avoir besoin de restaurer des fichiers stockés à l'état froid afin d'exécuter des requêtes ou de générer des rapports, pour un audit de conformité annuel ou semi-annuel par exemple. Si vous désignez un serveur CA Enterprise Log Manager en tant que point de restauration pour les investigations sur les données sauvegardées, vous devez forcer une reconstruction du catalogue chaque fois que vous restaurez une nouvelle base de données sur ce serveur CA Enterprise Log Manager. Une reconstruction du catalogue, ou recatalogage, est nécessaire uniquement lors de la restauration de données sur un serveur différent de celui sur lequel elles ont été générées.

Important : Assurez-vous que le paramètre Nbre max. de jours d'archivage pour le magasin de journaux d'événements de ce serveur est défini de manière appropriée. Dans le cas contraire, les fichiers restaurés sont supprimés immédiatement.

Un recatalogage est exécuté automatiquement au redémarrage d'iGateway, si nécessaire. Si les bases de données n'ont pas été entièrement cataloguées avant l'arrêt d'iGateway, le processus de recatalogage se termine lorsque qu'iGateway est redémarré. Si une ou plusieurs bases de données sont ajoutées au répertoire de bases de données d'archivage alors qu'iGateway est hors service, le processus de recatalogage est exécuté au prochain démarrage d'iGateway.

Le processus de restauration de fichiers archivés à partir d'un stockage externe vers un serveur CA Enterprise Log Manager autre que celui sur lequel ils étaient sauvegardés se compose des étapes suivantes.

1. Identification des bases de données à restaurer. Pour obtenir de l'aide, interrogez le catalogue d'archive à l'aide de filtres.
2. Transfert des fichiers d'archive sauvegardés identifiés du stockage externe vers votre réseau.
3. Copie des bases de données déplacées dans le répertoire d'archivage. Pour afficher le répertoire d'archivage, exécutez l'utilitaire LMArchive à l'aide de l'option -list loc.
4. Reconstruction du catalogue d'archive (recatalogage).

   La reconstruction du catalogue d'archive pour ajouter une seule base de données peut prendre plusieurs heures. Après avoir patienté jusqu'à la fin du processus de recatalogage, vous pouvez commencer vos investigations en exécutant des requêtes et des rapports sur les journaux d'événements issus des bases de données restaurées.
5. Vérification de la restauration par l'émission d'une requête.

Remarque : Si vous dédiez un serveur CA Enterprise Log Manager en tant que point de restauration, assurez-vous de l'exclure de la fédération.

Informations complémentaires :

Transfert des bases de données archivées vers un répertoire d'archivage (page 196)
Configuration du nombre maximal de jours d'archivage pour les archives restaurées (page 201)
Ajout de bases de données restaurées au catalogue (page 202)
Vérification de la restauration (page 199)
Exemple : Autorisation de gestion des archives par un non-administrateur (page 113)

Configuration du nombre maximal de jours d'archivage pour les archives restaurées

Lorsque vous configurez le magasin de journaux d'événements pour un serveur CA Enterprise Log Manager dédié en tant que point de restauration, nous vous recommandons de remplacer le paramètre global Nbre max. de jours d'archivage par la valeur maximale (28 000). Si le nombre de jours pendant lequel stocker les fichiers de bases de données archivés avant leur suppression est défini sur une valeur inférieure à l'ancienneté des fichiers de bases de données restaurés, ces fichiers sont supprimés par le système immédiatement après avoir été restaurés dans un état tiède.

Remarque : Cette procédure s'applique uniquement aux fichiers restaurés vers un nouveau magasin de journaux d'événements.

Pour définir le nombre maximal de jours d'archivage adapté à l'ancienneté des fichiers restaurés

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Dans la Liste de services, développez le dossier Magasin de journaux d'événements et sélectionnez CA Enterprise Log Manager servant de point de restauration dédié.
3. Cliquez sur le bouton de basculement en regard de Nbre max. de jours d'archivage pour passer en configuration locale et activer le champ de saisie.
4. Entrez une valeur en jours incluant le fichier le plus ancien à restaurer. La valeur maximale est 28 000.
5. Cliquez sur Enregistrer.

Ajout de bases de données restaurées au catalogue

Si vous copiez la base de données restaurée directement dans le répertoire d'archivage sur un autre serveur que celui sur lequel elle a été générée, recréez le catalogue d'archive pour ajouter la base de données restaurée.

N'utilisez *pas* le recatalogage dans les cas énumérés ci-dessous.

- Si vous utilisez le script restore-ca-elm.sh pour restaurer une base de données archivée. Le script shell de restauration procède au recatalogage pour vous.
- Si vous copiez la base de données restaurée directement dans le répertoire d'archivage sur le même serveur que celui sur lequel elle a été générée, notifiez ensuite à CA Enterprise Log Manager que la base de données est restaurée avec l'option LMArchive -notify rest.

Le processus de recatalogage place la base de données restaurée dans un état "tiède", et non dans un état "dégivré" comme avec l'option LMArchive -notify rest. Par conséquent, il suit les règles d'archivage normales, et non la stratégie d'exportation définie dans la configuration du magasin de journaux d'événements.

Pour recréer le catalogue d'archive afin d'ajouter la base de données restaurée

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier Requête de catalogue d'archive.

   Trois boutons, y compris Recataloguer, apparaissent au-dessus des onglets Filtres rapides et Filtres avancés.

3. Cliquez sur Recataloguer.

   Un message de confirmation d'opération s'affiche. La base de données restaurée est ajoutée au catalogue dans un état tiède.

Informations complémentaires :

Remarques sur le magasin de journaux d'événements (page 147)
Exemple : Autorisation de gestion des archives par un non-administrateur (page 113)

LMArchive–Backup/Restore Tracking

LMArchive est l'utilitaire de ligne de commande qui suit la sauvegarde et la restauration des bases de données tièdes vers le magasin de journaux d'événements d'un serveur CA Enterprise Log Manager. Utilisez LMArchive pour effectuer une requête sur la liste des fichiers de bases de données tièdes, prêts à être archivés. Après avoir sauvegardé la base de données répertoriée et l'avoir transférée sur un stockage à long terme (froid), utilisez LMArchive pour créer un enregistrement sur le serveur CA Enterprise Log Manager indiquant que cette base de données a été sauvegardée. Suite à la restauration d'une base de données froide sur son serveur CA Enterprise Log Manager d'origine, utilisez LMArchive pour notifier CA Enterprise Log Manager, qui place alors les fichiers de bases de données froides à un état dégivré, accessible aux requêtes.

La commande présente le format suivant

LMArchive -euser *nom_utilisateur* -epassword *mdp* {-list [loc|all|inc] | -notify [arch|rest] -files *fichier1*,*fichier2*,*fichier3*...}

-euser *username*

Spécifie le nom d'utilisateur d'un compte CA Enterprise Log Manager avec le rôle Administrator.

-epassword *mdp*

Spécifie le mot de passe CA Enterprise Log Manager associé au nom d'utilisateur.

-list [loc | all | inc]

Demande l'une des listes suivantes : emplacements des répertoires d'archivage, noms de toutes les bases de données tièdes et froides, noms des bases de données tièdes uniquement

loc

Demande l'emplacement du répertoire d'archivage.

all

Demande la liste de tous les noms de fichiers situés dans le répertoire d'archivage du magasin de journaux d'événements.

inc

Demande une liste incrémentielle des noms de fichiers des bases de données actuellement tièdes qui n'ont pas encore été archivées. La demande renvoie les noms des fichiers qui n'ont pas été sauvegardés, transférés vers un stockage externe et placés dans un état froid. Les fichiers sont placés dans un état froid suite à la notification du transfert par la commande notify de cet utilitaire.

-notify [arch | rest]

Notifie le magasin de journaux d'événements CA Enterprise Log Manager que les fichiers spécifiés ont été correctement sauvegardés ou restaurés.

arch

Notifie le magasin de journaux d'événements CA Enterprise Log Manager que les fichiers spécifiés ont été correctement sauvegardés.

rest

Notifie le magasin de journaux d'événements CA Enterprise Log Manager que les fichiers spécifiés ont été correctement restaurés.

-files *fichier1*,*fichier2*,*fichier3*...

Spécifie les noms des fichiers de bases de données que vous avez sauvegardés ou restaurés.

Informations complémentaires :

A propos du stockage des journaux (page 169)
Identification des bases de données non sauvegardées (page 188)
Enregistrement des sauvegardes (page 190)
Préparation à la restauration de bases de données archivées (page 194)
Restauration de fichiers archivés manuellement (page 197)

Chapitre 7 : Abonnement

Ce chapitre traite des sujets suivants :

Mise à jour d'un nouveau client d'abonnement

Si vous paramétrez "Nettoyage des mises à jour antérieures à (en jours)" sur une valeur bien inférieure à la valeur par défaut de 300, cette action peut supprimer les mises à jour dont un nouveau serveur a besoin. Dans ce cas, utilisez la procédure suivante à titre de précaution, pour ne pas risquer de manquer des mises à jour.

Pour mettre à jour un nouveau serveur CA Enterprise Log Manager pour l'abonnement

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Développez le Module d'abonnement et sélectionnez le serveur CA Enterprise Log Manager nouvellement installé.
3. Sélectionnez l'option Proxy d'abonnement pour configurer le nouveau serveur comme son propre proxy d'abonnement.

   En tant que proxy d'abonnement, le nouveau serveur contacte le serveur d'abonnement CA indépendamment pour sa mise à jour d'abonnement initiale. Le serveur d'abonnement CA détecte qu'aucune mise à jour n'a été demandée et propose toutes les mises à jour d'abonnement disponibles, dans l'ordre d'installation correct.

4. Déplacez les modules applicables à télécharger de la liste Disponible(s) vers la liste Sélectionné(s).

   La liste Disponible(s) contient les anciens modules qui ne sont plus disponibles pour aucun autre proxy d'abonnement.

5. Cliquez sur le bouton de basculement Proxies d'abonnement pour le client et assurez-vous que seul le nouveau serveur CA Enterprise Log Manager s'affiche dans la zone Sélectionné(s).

   Cette action garantit que ce proxy installe les mises à jour téléchargées à partir du serveur d'abonnement CA.

6. Cliquez sur Enregistrer.
7. Cliquez sur Mettre à jour.
8. Une fois la mise à jour terminée, passez en revue les informations contenues dans l'onglet Evénements d'autosurveillance pour ce serveur et vérifiez que toutes les mises à jour précédentes ont été installées.
9. Reconfigurez le nouveau serveur CA Enterprise Log Manager comme suit.
   a. Affichez à nouveau les paramètres d'abonnement pour le nouveau serveur.
   b. Désélectionnez la case à cocher Proxy d'abonnement.

   c. Supprimez le Serveur sélectionné auto-référant du champ Proxies d'abonnement pour le client.
   d. Sélectionnez un ou plusieurs proxies d'abonnement dans la liste Disponible(s) des Proxies d'abonnement pour le client.
10. Cliquez sur Enregistrer.

Modification de la configuration d'abonnement globale

Pendant la phase d'implémentation, un administrateur configure les paramètres d'abonnement globaux qui sont hérités par les différents CA Enterprise Log Manager. Par défaut, le premier CA Enterprise Log Manager installé est le proxy d'abonnement par défaut et l'ensemble de CA Enterprise Log Manager installés par la suite sont définis en tant que clients d'abonnement. Sans modification de la configuration, le proxy par défaut contacte directement le serveur d'abonnement CA et télécharge les mises à jour de produits sur tous les clients, y compris lui-même.

Vous pouvez modifier les paramètres globaux à tout moment. Toute modification apportée est hérité par l'ensemble de CA Enterprise Log Manager locaux pour lesquels il n'existe pas de valeurs de remplacement. Autrement dit, si un paramètre modifié a précédemment été écrasé au niveau local, ce remplacement continue de prévaloir.

Les paramètres ne pouvant être définis et modifiés qu'au niveau global sont répertoriés ci-dessous.

- URL du flux RSS
- Clé publique : version
- Nettoyage des mises à jour antérieures à (en jours)
- Redémarrage automatique après mise à jour du SE
- Proxies d'abonnement pour les mises à jour de contenu

Pour modifier la configuration d'abonnement globale

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Module d'abonnement et examinez les paramètres Configuration globale du service : Module d'abonnement dans le volet droit.
3. Vérifiez les paramètres et modifiez ceux qui ne sont pas acceptables.

   Remarque : Consultez l'aide en ligne pour obtenir plus de détails sur chaque champ.
4. Cliquez sur Enregistrer.

Informations complémentaires

Remarques sur l'abonnement (page 154)
Application des mises à jour d'abonnement (page 675)

Modification de la configuration d'un proxy en ligne

Pendant la phase d'implémentation, un administrateur configure les paramètres d'abonnement globaux. Les serveurs CA Enterprise Log Manager individuels héritent des paramètres globaux.

Tenez compte du rôle d'abonnement d'un serveur lors de la planification d'un remplacement des paramètres globaux. La procédure suivante s'applique aux serveurs CA Enterprise Log Manager définis comme proxies d'abonnement.

Remarque : Avant de modifier le rôle d'un proxy d'abonnement, modifiez les configurations des clients d'abonnement qui utilisent ce proxy. Dans Proxies d'abonnement pour le client, supprimez le serveur CA Enterprise Log Manager avec le rôle à modifier.

Pour modifier la configuration d'un proxy d'abonnement en ligne

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Développez le Module d'abonnement et sélectionnez un hôte configuré en tant que proxy d'abonnement.

   La Configuration du service du Module d'abonnement s'affiche pour le serveur CA Enterprise Log Manager sélectionné.
3. Pour modifier un paramètre global hérité, cliquez sur le bouton des paramètres globaux pour passer en configuration locale.

   Remarque : Pour restaurer le paramètre global, cliquez une nouvelle fois sur le bouton. La restauration s'effectue à l'issue de l'intervalle de mise à jour suivant, configuré sur la page Configuration globale du service.
4. Pour modifier le planning de mise à jour, modifiez la Fréquence de mise à jour.
5. Pour configurer un nouveau (ou un autre) serveur proxy HTTP, modifiez au moins l'un des champs applicables.
6. Si les modules corrects à télécharger sont différents des paramètres hérités, procédez aux modifications nécessaires. Les mises à jour des modules sélectionnés sont téléchargées, stockées et distribuées aux clients qui les demandent. Le remplissage des modules disponibles dépend de l'URL du flux RSS (paramètre d'abonnement global).
7. Cliquez sur Enregistrer.

Informations complémentaires :

Remarques sur l'abonnement (page 154)
Sélection de nouveaux modules à télécharger (page 212)

Modification de la configuration d'un proxy hors ligne

Pendant la phase d'implémentation, un administrateur configure les paramètres d'abonnement globaux qui sont hérités par les différents CA Enterprise Log Manager.

Si vous souhaitez modifier les paramètres globaux sur un serveur CA Enterprise Log Manager donné, tenez compte de son rôle. La procédure suivante s'applique aux serveurs CA Enterprise Log Manager avec le paramètre ci-dessous.

Un proxy d'abonnement hors ligne ne contacte pas le serveur d'abonnement CA. Par conséquent, l'heure de début de mise à jour, la fréquence de mise à jour et les paramètres de proxy HTTP ne s'appliquent pas.

Pour modifier la configuration d'un proxy d'abonnement hors ligne

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Développez le Module d'abonnement et sélectionnez un hôte configuré en tant que proxy d'abonnement hors ligne.

   La Configuration du service du Module d'abonnement s'affiche pour le serveur CA Enterprise Log Manager sélectionné.
3. Effectuez les modifications souhaitées, comme les exemples ci-dessous.
   - Pour modifier le rôle du serveur à partir d'un proxy d'abonnement hors ligne, désélectionnez la case à cocher du proxy d'abonnement hors ligne.
   - Pour le configurer en tant que client, la procédure s'arrête là.
   - Pour le configurer en tant que proxy d'abonnement en ligne, sélectionnez la case à cocher Proxy d'abonnement.
4. Vérifiez vos modifications, puis cliquez sur Enregistrer.

Modification de la configuration d'un client d'abonnement

Pendant la phase d'implémentation, un administrateur configure les paramètres d'abonnement globaux. La plupart de ces paramètres proviennent de serveurs CA Enterprise Log Manager individuels. La seule exception est l'heure et la fréquence auxquelles chaque client d'abonnement interroge un proxy pour des mises à jour. Un retard prédéfini permet aux proxies d'effectuer un téléchargement avant d'être interrogé par les clients afin de propager le téléchargement.

Si vous souhaitez modifier les paramètres globaux sur un serveur CA Enterprise Log Manager donné, tenez compte de son rôle. La procédure suivante s'applique aux serveurs CA Enterprise Log Manager qui sont des clients d'abonnement, c'est-à-dire aux serveurs paramétrés comme suit.

Pour modifier la configuration d'un client d'abonnement

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Développez le Module d'abonnement et sélectionnez un hôte configuré en tant que client d'abonnement.

   La Configuration du service du Module d'abonnement s'affiche pour le serveur CA Enterprise Log Manager sélectionné.
3. Pour modifier un paramètre global, cliquez sur le bouton des paramètres globaux pour passer en configuration locale, ce qui vous permet d'effectuer des modifications.

   Remarque : Pour restaurer le paramètre global, cliquez une nouvelle fois sur le bouton. La restauration s'effectue à l'issue de l'intervalle de mise à jour configuré sur la page Configuration globale du service.
4. Pour modifier la liste des proxies d'abonnement que ce client contacte pour les mises à jour de produits et du système d'exploitation, affichez le bouton des paramètres locaux pour l'option Proxies d'abonnement pour le client. Utilisez les contrôles de déplacement pour modifier les proxies d'abonnement que ce client doit contacter ou changez l'ordre dans lequel les serveurs existants sont contactés.
5. Modifiez les modules à télécharger si ce client ne reçoit pas les mises à jour pour les modules dont il a besoin.

   Remarque : Un client peut demander le téléchargement d'un module qui ne figure pas sur la liste de son proxy.
6. Cliquez sur Enregistrer.

Espace disque disponible pour les mises à jour

Pour être sûr de réaliser correctement les mises à jour d'abonnement sur les serveurs CA Enterprise Log Manager, il est recommandé de nettoyer régulièrement le disque. Les mises à jour d'abonnement ne peuvent pas être téléchargées d'un proxy d'abonnement vers un client d'abonnement lorsque l'utilisation de l'espace disque atteint ou dépasse la limite de 90 %.

Pour garantir un espace disque suffisant pour les mises à jour d'abonnement

1. Surveillez régulièrement l'espace disque disponible. Vous pouvez également configurer une alerte d'action vous avertissant lorsque l'espace disque disponible devient inférieur à 20 %.
2. Libérez de l'espace disque à l'aide d'un outil de nettoyage de disque.

   Remarque : Si l'espace disque disponible est de 10 % ou moins lorsque le processus de mise à jour d'abonnement commence, le service d'abonnement émet un événement d'autosurveillance et suspend le processus de téléchargement.
3. Si vous êtes averti de la nécessité de nettoyer le disque par un événement d'autosurveillance, libérez suffisamment d'espace disque pour permettre la poursuite du téléchargement.

Informations complémentaires :

Exemple : Création d'une alerte d'action pour un espace disque faible (page 481)

A propos des modules à télécharger

Un *module* est un groupement logique de mises à jour de composant, mis à disposition des utilisateurs en téléchargement, sur la base d'un abonnement. Un module peut contenir des mises à jour de fichier binaire, de contenu, ou les deux. Par exemple, tous les rapports sont réunis dans un même module ; toutes les mises à jour de fichier binaire de sponsor sont regroupées dans un autre module. CA définit le contenu de chaque module.

Durant la configuration de l'abonnement, vous sélectionnez en tant que paramètre global les modules que vous souhaitez télécharger, dans la liste des modules disponibles. Dans le cas d'un serveur proxy d'abonnement en ligne, vous pouvez utiliser le paramètre global ou l'ignorer et sélectionner les modules de votre choix, que vous mettrez à disposition des clients qui les demandent. Dans le cas d'un client, vous pouvez utiliser le paramètre global ou l'ignorer et sélectionner les modules de votre choix, que les clients devront télécharger et installer. Les modules disponibles au téléchargement varient en fonction du cycle de mise à jour ; vérifiez donc la liste des modules disponibles pour vous assurer que tous les modules requis sont sélectionnés. Les modules disponibles dans une mise à jour ou un cycle de mise à niveau incluent n'importe quelle combinaison des éléments suivants : OperatingSystem, LogManager, Rapports, Agents et Intégrations.

Vous pouvez sélectionner en toute sécurité tous les composants répertoriés dans la liste des modules disponibles en téléchargement, pour l'ensemble des serveurs CA Enterprise Log Manager. Le tableau suivant décrit chacun de ces modules et leur destination.

Module à télécharger	Description
OperatingSystem	Met à jour le système d'exploitation installé sur chaque dispositif CA Enterprise Log Manager, après le téléchargement et l'installation auto.
LogManager	Met à jour le produit CA Enterprise Log Manager sur chaque système, après le téléchargement et l'installation auto.
Rapports	Met à jour la Liste de requêtes et la Liste de rapports avec les nouveaux rapports et requêtes. Le serveur proxy de mise à jour du contenu envoie automatiquement ce contenu au niveau du référentiel du serveur de gestion.
Agents	Met à jour les agents lorsque vous exécutez l'Assistant d'abonnement et sélectionnez les mises à jours d'agent.
Intégrations (Mises à jour du connecteur)	Met à jour les connecteurs lorsque vous exécutez l'Assistant d'abonnement et sélectionnez les mises à jours de connecteur.

Sélection de nouveaux modules à télécharger

Les noms de module figurant dans la liste des modules disponibles au téléchargement dépendent des éléments déjà chargés dans le flux RSS. Par conséquent, le contenu de cette liste peut varier d'une mise à jour à une autre. Vous pouvez sélectionner de nouveaux modules à télécharger au niveau global ou séparément pour chaque serveur CA Enterprise Log Manager. Il est plus sûr de sélectionner tous les modules disponibles au téléchargement , quelle que soit l'utilisation que vous faites de chaque serveur.

Pour sélectionner de nouveaux modules à télécharger

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur le Module d'abonnement.

   Le paramètre Configuration globale de service (Module d'abonnement) apparaît dans le volet droit.
3. Pour le service global, vérifier que tous les modules affichés dans la liste des modules disponibles au téléchargement sont déplacés vers la liste des éléments sélectionnés.
4. Si vous remplacez les paramètres hérités pour un serveur donné, il est préférable d'accepter tous les modules pour le téléchargement.

   Important : Evitez de choisir un module pour un client d'abonnement qui n'a pas été sélectionné pour le proxy qu'il utilise, car cette configuration empêche toute mise à jour du contenu du module lancée depuis le serveur de gestion.

Récupération manuelle des mises à jour d'abonnement

Si vos stratégies d'entreprise interdisent l'accès à Internet par le biais d'un serveur CA Enterprise Log Manager, observez la procédure manuelle alternative pour récupérer les mises à jour d'abonnement auprès du serveur d'abonnement CA. Récupérez les mises à jour conformément au paramètre Fréquence de mise à jour, dans les paramètres globaux du module d'abonnement.

Avant d'effectuer la première récupération manuelle, créez la structure de fichiers suivante sur le serveur local cible : /opt/CA/LogManager/data/subscription/.

Important : Si le fichier ComponentConfig.xml, que vous avez créé manuellement, contient des erreurs, il est possible que les mises à jour souhaitées ne soient pas appliquées.

Utilisez l'exemple suivant en tant que référence.

Pour récupérer manuellement des mises à jour d'abonnement

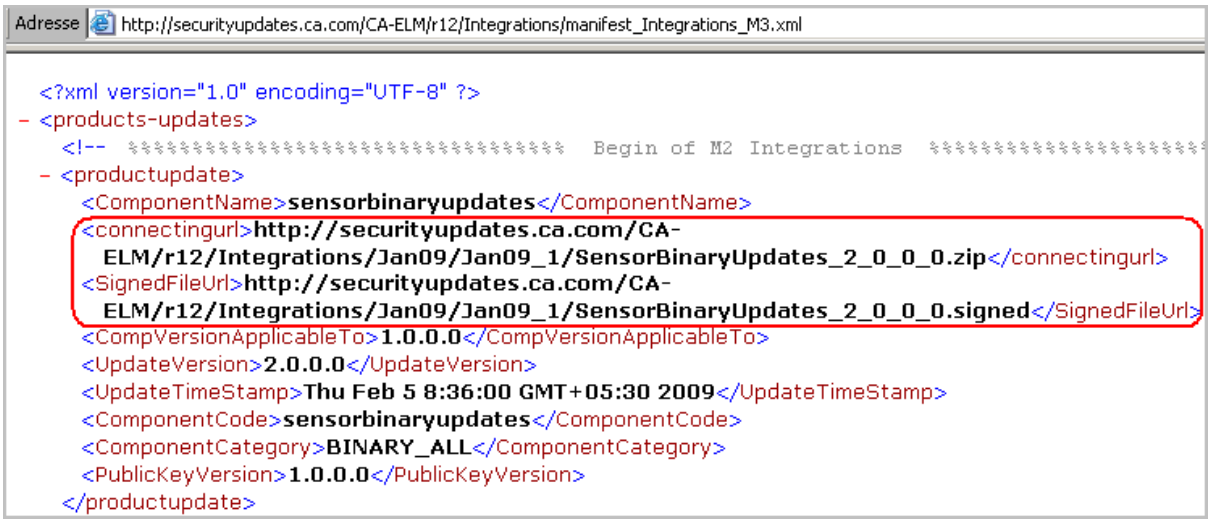
1. Cliquez sur l'onglet Administration, sur le sous-onglet Services, puis sélectionnez Module d'abonnement.
2. Copiez l'entrée pour l'URL du flux RSS.

3. Accédez à un serveur disposant d'un accès Internet et entrez l'URL copiée dans le navigateur pour y accéder.

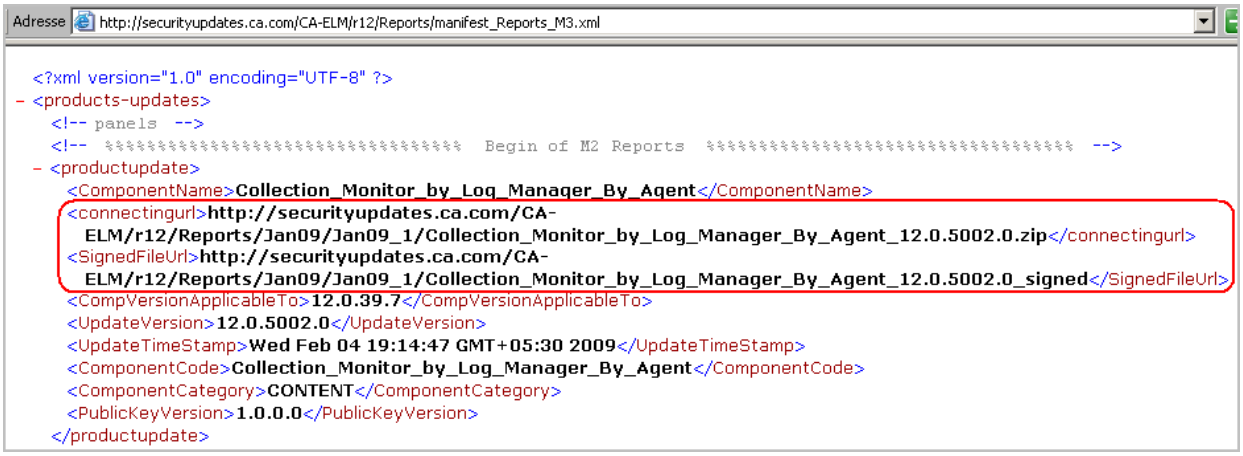
   Une page similaire à la page suivante apparaît.

4. Lancez chaque URL de mise à jour d'abonnement et enregistrez le fichier XML obtenu dans le dossier d'abonnement.

   Le fichier XML téléchargé via la première URL de cet exemple commence comme suit. Son nom est manifest_Integrations_M3.xml.



Le fichier XML téléchargé via la deuxième URL commence comme suit. Son nom est manifest_Reports_M3.xml.



5. Utilisez ces fichiers XML pour créer une structure de fichiers dans laquelle télécharger les modules et les fichiers de signature associés. Dans le dossier d'abonnement, créez un sous-dossier pour chaque fichier manifeste. Dans cet exemple, ajoutez un dossier Intégrations et un dossier Rapports dans le dossier d'abonnement. Le chemin complet recommandé est indiqué ci-dessous.

   /opt/CA/LogManager/data/subscription/<Nom_module>/<Nom_composant>/<Version_mise_à_jour>

   Dans le dossier Intégrations, vous pouvez ajouter un dossier pour le composant <Nom_composant> de chaque bloc <productupdate> </productupdate> du fichier manifeste XML des intégrations. Dans le dossier du composant, vous pouvez ajouter un dossier pour le numéro de version. Voici un exemple de structure avec les données des deux fichiers d'exemple.

   subscription
   - Agents
   - Integrations
     - sensorbinaryupdates
       - 2.0.0.0
   - LogManager
   - Reports
     - Collection_Monitor_by_Log_Manager_By_Agent
       - 12.0.5002.0

6. Placez deux fichiers dans chaque dossier de version de mise à jour créé, comme suit.

   - Dans le navigateur, saisissez la première URL, située entre les balises connectingurl, et téléchargez le fichier ZIP.

     La première URL du fichier Integrations_manifest.xml lance le téléchargement d'un fichier ZIP contenant les mises à jour pour le module du détecteur. Dans cet exemple, enregistrez le fichier SensoryBinaryUpdates_2_0_0_0.zip dans le dossier subscription/Integrations/sensorbinaryupdates/2.0.0.0.

   - Lancez l'URL pour télécharger le fichier de signature correspondant dans le même dossier que le composant.

     Dans cet exemple, le fichier de signature est SensorBinaryUpdates_2_0_0_0.signed.

7. Créez un fichier intitulé ComponentConfig.xml dans le dossier /opt/CA/LogManager/data/subscription, en utilisant la structure et les balises ci-dessous.

```
<?XML VERSION="1.0" ENCODING="UTF-8"?>
<ISPONSOR>
    <COMPONENT>NAME="valeur" CODE="valeur" VERSION="valeur"
    COMPVRSIONAPPLICABLE="valeur" CATEGORY="valeur" MODULE="valeur" PARTIAL="valeur"
    VALID="valeur" INSTALLEDINEEM="valeur" DOWNLOADEDFILEPATH="valeur"</COMPONENT>
</ISPONSOR>
```

8. Saisissez les valeurs récupérées dans les fichiers manifestes téléchargés dans les espaces entre guillemets.

   NAME=

   Indique le nom du composant. Cette valeur se situe entre les balises <ComponentName></ComponentNames>.

   CODE=

   Indique le nom de code du composant. Cette valeur se situe entre les balises <ComponentCode></ComponentCode>.

   VERSION=

   Indique la version de la mise à jour. Cette valeur se situe entre les balises <UpdateVersion></UpdateVersion>.

   COMPVRSIONAPPLICABLE=

   Indique la version pour laquelle cette version de mise à jour est applicable. Cette valeur se situe entre les balises <CompVersionApplicableTo></CompVersionApplicableTo>.

CATEGORY=

Indique si le composant constitue un nouveau contenu ou une mise à niveau du code. Cette valeur se situe entre les balises <ComponentCategory></ComponentCategory.

Valeurs valides : CONTENT, BINARY_ALL

MODULE=

Indique le nom du module à télécharger. La valeur <Nom_module> se situe dans l'URL du fichier manifeste.

PARTIAL=

Indique que le composant spécifié par la valeur Nom a été partiellement téléchargé. Si c'est le cas, le téléchargement reprend lors du cycle de mise à jour suivant.

Valeurs valides : TRUE, FALSE

Remarque : Si cette valeur est inconnue, spécifiez FALSE pour garantir que le téléchargement du module soit effectué.

VALID=

Indique si le composant spécifié par la valeur Nom est valide, c'est-à-dire si la signature a bien été vérifiée.

Valeurs valides : TRUE, FALSE

Remarque : Dans le cas d'un fichier créé manuellement, où ce statut est inconnu, saisissez TRUE. La vérification de la signature n'est pas effectuée.

INSTALLEDINEEM=

Si CATEGORY="CONTENT", indique si la version actuelle a été installée dans CA EEM. Si la valeur est False, le proxy hors ligne tente d'installer à nouveau ce composant lors du cycle de mise à jour suivant.

Valeurs valides : TRUE, FALSE

Remarque : Cette valeur s'applique aux mises à jour de contenu ; pour les mises à jour de fichiers binaires, la valeur est toujours FALSE. Dans le cas d'un fichier créé manuellement, où ce statut est inconnu, saisissez FALSE. Cela permet de garantir que la mise à jour est forcée sur le référentiel du serveur de gestion, que celui-ci existe ou non.

DOWNLOADEDFILEPATH=

Indique l'emplacement, sur le serveur d'abonnement, où vous avez téléchargé le fichier ZIP ; ce chemin d'accès se termine par le nom du fichier ZIP.

Exemple : Entrées du fichier ComponentConfig.xml pour un composant binaire

Voici un exemple de définition de composant binaire. Lorsque les mises à jour sont disponibles sur le proxy d'abonnement hors ligne, les clients d'abonnement téléchargent et installent les composants binaires selon le planning défini.

```
<?XML VERSION="1.0" ENCODING="UTF-8"?>
<ISPONSOR>
    ...
    <COMPONENT>NAME="sensorbinaryupdates" CODE="sensorbinaryupdates" VERSION="2.0.0.0"
    COMPVERSIONAPPLICABLE="1.0.0.0" CATEGORY="BINARY_ALL" MODULE="Integrations"
    PARTIAL="FALSE" VALID="TRUE" INSTALLEDINEEM="FALSE"
    DOWNLOADEDFILEPATH="Integrations/sensorbinaryupdates/2.0,0.0/SensoryBinaryUpdates_2_0_0
    _0.zip"</COMPONENT>
    ...
</ISPONSOR>
```

Exemple : Entrées du fichier ComponentConfig.xml pour un composant de contenu

Voici un exemple de définition de composant de contenu. Lorsque les mises à jour sont disponibles sur le proxy d'abonnement hors ligne, celui-ci envoie les composants de ce type au référentiel sur le serveur de gestion.

```
<?XML VERSION="1.0" ENCODING="UTF-8"?>
<ISPONSOR>
    ...
    <COMPONENT>NAME="Collection_Monitor_by_Log_Manager_By_Agent"
    CODE="Collection_Monitor_by_Log_Manager_By_Agent" VERSION="12.0.5002.0"
    COMPVERSIONAPPLICABLE="12.0.39.7" CATEGORY="CONTENT" MODULE="Reports"
    PARTIAL="FALSE" VALID="TRUE" INSTALLEDINEEM="TRUE"
    DOWNLOADEDFILEPATH="Reports/Collection_Monitor_by_Log_Manager_By_Agent/12.0.5002.0/
    Collection_Monitor_by_Log_Manager_By_Agent_12.0.5002.0.zip"</COMPONENT>
    ...
</ISPONSOR>
```

Copie de mises à jour sur un proxy hors ligne

Si votre environnement contient des serveurs proxy hors ligne, vous devez les mettre à jour manuellement, car ils ne contactent pas le serveur d'abonnement CA. Vous devez distribuer les fichiers de mise à jour manuellement à l'aide d'un disque à mémoire flash ou d'un autre dispositif de mémoire.

L'utilitaire scp, inclus dans votre installation initiale, vous permet de copier des fichiers de mise à jour depuis un serveur proxy d'abonnement en ligne vers un serveur hors ligne situé sur le même réseau. Vous devez copier *tous* les fichiers disponibles depuis le chemin de téléchargement du proxy en ligne vers le chemin de téléchargement du serveur proxy hors ligne. Le chemin de téléchargement source contient des fichiers de méta-informations qui doivent être copiés vers le chemin de destination. Le chemin de téléchargement depuis le répertoire racine est /opt/CA/LogManager/data/subscription.

Nous vous recommandons d'utiliser l'utilitaire scp récursif, à l'aide de la commande -r.

Important : Vous devez mettre à jour les serveurs proxy hors ligne dans les délais impartis pour que les serveurs CA Enterprise Log Manager clients puissent installer les mises à jour nécessaires avant la mise à jour d'abonnement des agents qui envoient les événements à ces clients. Des clients plus récents peuvent prendre en charge des agents plus anciens, mais des clients plus anciens ne peuvent pas prendre en charge des agents plus récents.

Pour copier des mises à jour sur un serveur proxy hors ligne

1. Ouvrez une invite de commande sur le serveur connecté à Internet sur lequel vous avez téléchargé les packages de mises à jour à partir du serveur d'abonnement CA à copier. Accédez au répertoire source.
2. Entrez la commande suivante.

   scp -r <répertoire_source_proxy_en_ligne> <destination_proxy_hors_ligne>

   -r

   Copiez les répertoires de manière récursive : copiez tous les fichiers et sous-répertoires ainsi que le contenu des sous-répertoires.

   <répertoire_source_proxy_en_ligne>

   Spécifie le répertoire à copier. Le chemin de téléchargement d'abonnement est /opt/CA/LogManager/data/subscription.

   <destination_proxy_hors_ligne>

   Spécifie l'emplacement auquel le matériel copié doit être placé à l'aide de la syntaxe suivante : user@offlineproxybox:/opt/CA/LogManager/data/subscription.

   Une invite vous demandant le mot de passe de l'adresse user@offlineproxybox apparaît.
3. Saisissez le mot de passe demandé pour le serveur proxy hors ligne.

   Le système procède à l'authentification, puis copie les répertoires de manière récursive, du proxy en ligne vers le proxy hors ligne.
4. Changez la propriété des fichiers copiés de manière récursive à la fois pour l'utilisateur et pour le groupe à l'aide de la commande suivante.

   chown -R caelmservice:caelmservice /opt/CA/LogManager/data/subscription/*

Exemple : Copie de mises à jour sur un proxy hors ligne

1. Ouvrez une invite de commande depuis le serveur de gestion qui constitue le proxy en ligne.
2. Entrez la commande suivante.

   scp –r /opt/CA/LogManager/data/subscription user@offlineproxybox:/opt/CA/LogManager/data/subscription
3. Répondez à l'invite vous demandant le mot de passe de l'adresse user@offlineproxybox.

   Le processus de copie démarre une fois l'authentification réussie.
4. Changez la propriété des fichiers de manière récursive pour l'utilisateur et le groupe, caelmservice, à l'aide de la commande suivante.

   chown -R caelmservice:caelmservice /opt/CA/LogManager/data/subscription/*

A propos des clés publiques d'abonnement

Le proxy d'abonnement conserve un jeu de clés publiques correspondant aux clés privées utilisées par le serveur d'abonnement CA. Le proxy d'abonnement télécharge les mises à jour d'abonnement sous la forme d'un fichier ZIP signé numériquement à l'aide d'une clé privée. La mise à jour identifie la clé publique à utiliser pour vérifier la signature de la mise à jour. En vérifiant la signature, le proxy d'abonnement s'assure que la mise à jour provient du serveur d'abonnement CA. Une seule paire de clés publique-privée est utilisée pour une opération d'abonnement donnée. Une clé privée est utilisée pour signer la mise à jour ; une clé publique est utilisée pour vérifier la signature. La clé publique est stockée sur chaque serveur CA Enterprise Log Manager et peut être mise à jour.

CA Enterprise Log Manager stocke la version initiale de la clé publique dans le fichier de configuration d'abonnement lors de l'installation. Si une nouvelle clé privée est requise, la clé publique associée est téléchargée avec la mise à jour d'abonnement avant le cycle de mise à jour nécessitant la nouvelle clé.

Important : Ne mettez pas à jour manuellement le champ Clé publique pour l'abonnement si cela ne vous a pas été clairement indiqué par le support technique CA.

Evénements d'autosurveillance pour un abonnement

Vous pouvez contrôler l'échec ou le succès d'une procédure de mise à jour d'abonnement impliquant des serveurs CA Enterprise Log Manager configurés en tant que :

- Serveur proxy d'abonnement par défaut
- Serveurs proxy d'abonnement en ligne supplémentaires, le cas échéant
- Serveurs proxy d'abonnement hors ligne, le cas échéant
- Clients d'abonnement

Remarque : Les événements décrits dans cette rubrique n'assurent pas le suivi des mises à jour d'abonnement pour les agents.

Les procédures réussies sont signalées dans les cas suivants.

- Démarrage et arrêt des serveurs CA Enterprise Log Manager, à la fois serveurs proxy et clients d'abonnement
- Téléchargement d'un composant, à partir d'un serveur proxy d'abonnement en ligne ou hors ligne, vers un client d'abonnement
- Installation d'un composant par un client d'abonnement

Un événement est généré dans les cas suivants.

- Lorsqu'une mise à jour du système d'exploitation est installée avec l'option de redémarrage désactivée, le message suivant est généré une fois : Mises à jour de système d'exploitation installées sur cet hôte... Redémarrez l'ordinateur pour que ces mises à jour prennent effet.

Les échecs de procédure sont signalés dans les cas suivants.

- Echec du téléchargement d'un composant, à partir d'un serveur proxy d'abonnement en ligne ou hors ligne, vers un client d'abonnement
- Echec de l'installation d'un composant par un client d'abonnement
- Conditions d'erreur

Surveillance des événements d'abonnement

Vous pouvez surveiller les réussites et les échecs des processus de mise à jour d'abonnement en affichant les événements d'autosurveillance liés à l'abonnement.

Pour surveiller les événements de traitement d'abonnement

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Module d'abonnement dans la Liste de services.
3. Cliquez sur l'onglet Evénements d'autosurveillance pour le Module d'abonnement ou pour un hôte répertorié sous le Module d'abonnement.

4. Examinez les détails des événements affichés.

   Certains des champs affichés pour les événements d'autosurveillance font référence aux dénominations CEG des actions communes aux différents fournisseurs. Le Modèle idéal est basé sur cette hiérarchie : event_category, event_class (au sein de la catégorie), event_action (au sein de la classe), event_result et event_severity. La Sévérité CA indiquée dans ce rapport est l'interprétation CA du niveau de sévérité.

   Sévérité CA

   Le niveau de sévérité de l'événement, lorsque

   - Inconnu : événements inconnus, événements non mappés sur la CEG ou événements non classés
   - Informations : informations générales sur le fonctionnement du système, informations de sécurité ou communiqué
   - Avertissement : modifications inhabituelles, condition normale mais significative, opérations en échec ou performances dégradées
   - Impact mineur : impact mineur sur un système, une fonction ou la sécurité
   - Impact majeur : impact majeur sur un système, une fonction ou la sécurité
   - Critique : action immédiate requise, brèche probable de la sécurité

   Date

   Date à laquelle l'événement a eu lieu.

   Récepteur

   Composant sur lequel le processus en cours n'a pas abouti. Il peut s'agir d'un proxy d'abonnement ou d'un client d'abonnement. Dans le cas d'un proxy d'abonnement, il peut s'agir du proxy par défaut, d'un proxy en ligne ou d'un proxy hors ligne.

   Hôte du récepteur

   Nom d'hôte du serveur CA Enterprise Log Manager ayant le statut de récepteur.

   Catégorie

   Catégorie de l'événement. Gestion de la configuration est la catégorie d'événement (event_category) des événements de module d'abonnement.

   Utilisateur

   Identité ou nom d'utilisateur ayant lancé l'action figurant dans les informations sur l'événement Il s'agit du champ source_username dans la CEG.

Action

Action ayant généré l'événement. Il s'agit du champ event_action dans la CEG.

Résultat

S pour opération réussie ; F pour échec. Le résultat de l'action d'événement est le champ event_result dans la CEG. Les autres options sont Accepté, Rejeté, Ignoré et Inconnu.

Description du résultat

Texte du message. Si la colonne Résultat affiche Echec, consultez le texte Description du résultat.

5. Affichez les détails dans la Visionneuse d'événements. Vous pouvez y consulter les modifications apportées, par exemple à une valeur de configuration telle que l'heure de début de mise à jour.

Informations complémentaires

Erreurs de comparaison de version. Format de version incorrect (page 240)

Affichage des détails de l'événement d'abonnement

Une fois que vous avez configuré l'abonnement, vous pouvez afficher les événements d'autosurveillance. Après la mise à jour de l'abonnement, vous pouvez vérifier que la mise à jour de chaque serveur a été correctement effectuée. Une fois les mises à niveau terminées, recherchez les messages d'événement d'autosurveillance suivants sur chaque serveur concerné.

- <composant> a été correctement téléchargé sur le proxy <nom_proxy> et installé dans EEM.
- <composant> a été correctement téléchargé sur le proxy <nom_proxy>.
- <composant> a été correctement installé sur le client <nom_client>.

Vous pouvez également afficher les événements d'autosurveillance d'abonnement à des fins de dépannage.

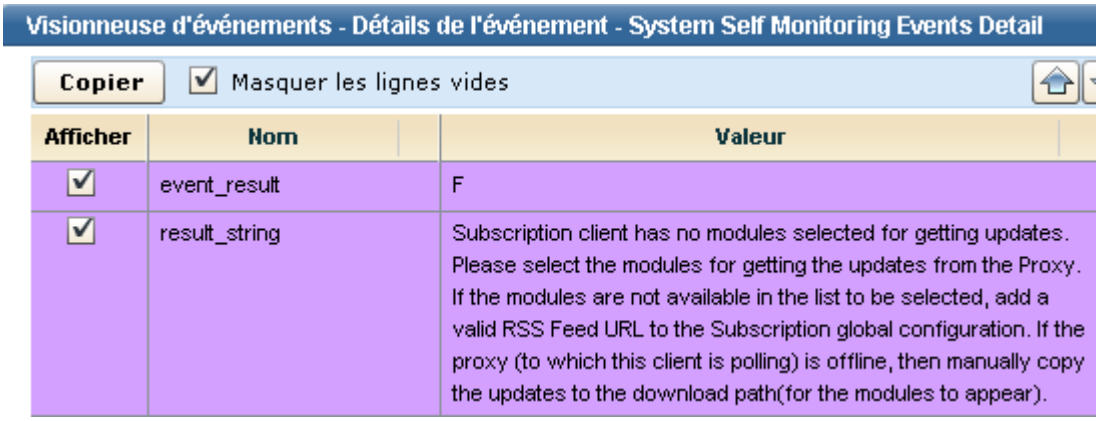
Pour afficher les détails de l'événement d'abonnement dans la visionneuse d'événements

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Module d'abonnement dans la Liste de services.
3. Cliquez sur l'onglet Evénements d'autosurveillance pour le Module d'abonnement ou pour un hôte répertorié sous le Module d'abonnement.
4. Examinez la colonne Description du résultat. Par exemple, cette colonne affiche parfois des événements du type "Aucun module n'a été sélectionné par le client d'abonnement pour la mise à jour".

Description du résultat
Subscription Client - calmrhbuildtest01 is communicating with the proxy - calmrhbuildtest01 for getting the Subscription updates.
Subscription client has no modules selected for getting updates. Please select the modules for getting the updates from the Proxy.
Unable to connect to the specified RSSFeed URL. Please check the URL again.
Unable to connect to the specified RSSFeed URL. Please check the URL again.
No modules are selected for getting updates. Please select the modules for getting the updates from the Subscription server.

5. Double-cliquez sur la description du résultat dont vous souhaitez consulter les détails.

   La visionneuse d'événements s'ouvre.
6. Faites défiler l'affichage jusqu'à la section des résultats et consultez le texte affiché pour result_string.



Avertissements et échecs d'événements d'abonnement

Vous pouvez afficher les événements d'autosurveillance d'abonnement afin d'assurer le suivi du traitement de l'abonnement. La colonne Description du résultat contient des messages. Utilisez la liste de messages suivante pour en savoir plus sur les conditions d'échec et l'action corrective recommandée. Si les actions recommandées ne résolvent pas le problème, demandez de l'aide. En cas de problème, contactez le support technique à l'adresse http://www.ca.com/fr/support.

Remarque : Les messages présentés dans cette section n'incluent pas les messages informatifs. Certains messages informatifs sont rédigés de la même manière que les messages d'erreur, toutefois les conditions de déclenchement et les actions correctives recommandées diffèrent. Par exemple, le message "INFORMATION : Aucun module à télécharger" indique une situation différente du message "ERREUR : Aucun module à télécharger". Les messages suivants sont tous des messages d'erreur ou d'avertissement.

Erreur d'authentification ! Le client ne s'est pas authentifié pour obtenir les mises à jour auprès du proxy.

Motif :

Le client d'abonnement ne s'est pas authentifié ; par conséquent, il ne peut récupérer les mises à jour auprès du serveur proxy d'abonnement. Pour pouvoir demander des informations à un proxy d'abonnement, le client d'abonnement doit s'authentifier à l'aide d'un certificat CA EEM. La communication est autorisée uniquement si l'authentification réussit. Une erreur d'authentification peut se produire si le serveur CA EEM est arrêté ou si le certificat d'authentification est refusé.

Action :

Essayez les actions suivantes pour restaurer l'authentification entre le client d'abonnement et le serveur proxy.

- Essayez d'envoyer une requête ping au serveur de gestion CA Enterprise Log Manager sur lequel le composant CA EEM est installé. Si le ping échoue, corrigez les paramètres de réseau de ce serveur CA Enterprise Log Manager.
- Etudiez en détail le certificat, afin de déterminer si le certificat et les informations d'identification utilisés pour l'authentification sont corrects. Ces détails sont stockés dans le fichier de configuration, à l'emplacement suivant : /opt/CA/SharedComponents/iTechnology/CALM.cnf. S'ils ne sont pas corrects, apportez les corrections nécessaires.

  Remarque : Consultez la section "Certificats personnalisés" de ce manuel pour en savoir plus sur la mise en oeuvre et le déploiement de nouveaux certificats.
- Déterminez si le serveur CA EEM fonctionne correctement sur le serveur de gestion CA Enterprise Log Manager en lançant l'interface EEM depuis un navigateur. Saisissez https://<adresse_IP_serveur_de_gestion>:5250/spin/eiam/about.csp. Si la page A propos de CA Embedded Entitlements Manager ne s'affiche pas, redémarrez le service iGateway.

Pour démarrer le service iGateway

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

   ```
   su -
   ```

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

   ```
   $IGW_LOC/S99igateway start
   ```

   S99igateway est le script de démarrage du processus igateway.

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

Le composant dépendant <CompDep> doit être installé avant l'installation du composant - <NomComp>. Le composant dépendant n'a pas été téléchargé avec cette mise à jour, ni installé préalablement. L'installation du composant est donc interrompue.

Motif :

Le composant requis, intitulé <NomComposant> dans le message, n'a pas pu être installé sur le client d'abonnement car ce dernier ne dispose pas d'un composant dont le composant requis dépend et le présent téléchargement ne contient pas ce composant dépendant. Cette erreur peut se produire lorsque le client demande des mises à jour avant que son proxy ait terminé de les télécharger auprès du serveur d'abonnement CA. Elle se produit également lorsque iGateway n'est pas correctement arrêté.

Action :

Essayez les actions ci-dessous pour tenter de résoudre le problème.

- Vérifiez la fréquence et l'heure de début de la mise à jour pour le client, en les comparant à celles définies pour le ou les proxies correspondants. Consultez la section "Exemples : Planification des mises à jour d'abonnement" du *Manuel d'implémentation* pour savoir comment échelonner les téléchargements.
- Si une panne d'iGateway s'est produite récemment, redémarrez iGateway en tant qu'utilisateur root. Saisissez : $IGW_LOC/S99igateway start.

  $IGW_LOC correspond à l'emplacement suivant : /opt/CA/SharedComponents/iTechnology.

Le composant dépendant <CompDep> doit être installé avant l'installation du composant - <NomComp>. L'installation du composant dépendant a échoué. L'installation du composant est donc interrompue.

Motif :

Le composant nommé en premier dans le message n'a pas pu être installé sur le client d'abonnement, en raison de l'échec de l'installation du composant dépendant, nommé en second dans le message.

Action :

Les modules téléchargés sont conçus pour satisfaire aux conditions requises. Pour obtenir de l'aide, contactez l'assistance technique à l'adresse http://ca.com/worldwide.

Le téléchargement s'est interrompu. msg - <msg>

Motif :

Les problèmes techniques décrits dans le message ont empêché le téléchargement de la mise à jour.

Action :

Essayez les actions suivantes pour résoudre le problème ayant entraîné l'interruption du téléchargement.

- Vérifiez que les configurations d'abonnement globale et locale sont complètes et valides. Par exemple, vérifiez les paramètres du proxy HTTP.
- Si le serveur CA Enterprise Log Manager sélectionné est configuré en tant que proxy pour les mises à jour de contenu, il est possible que le serveur de gestion vers lequel la tentative de téléchargement est faite ne réponde pas. Assurez-vous que le serveur de gestion est en marche. S'il ne l'est pas, démarrez-le.

Le serveur Http ne fonctionne pas ou la connexion a été refusée.

Motif :

Une erreur de connexion s'est produite car le serveur HTTP ne fonctionne pas ou la requête de connexion a été refusée.

Action :

Essayez d'appliquer les actions correctives suivantes.

- Vérifiez que les paramètres du serveur proxy HTTP sont corrects. Pour ce faire, contactez votre administrateur système.
- Depuis le serveur où l'événement d'autosurveillance a été consigné, envoyez une requête ping au serveur proxy HTTP configuré afin de déterminer si la connexion est active.
- Copiez dans un navigateur l'URL de flux RSS configurée et déterminez si une connexion est active. Si c'est le cas, le fichier décrivant les modules à télécharger s'affiche.

Une erreur (E/S) s'est produite lors de la récupération du fichier de mise à jour pour le composant - <NomComp>, du serveur proxy vers le client.

Motif :

Un problème technique est survenu lorsque le client d'abonnement a tenté de télécharger la mise à jour auprès du proxy d'abonnement.

Action :

Vérifiez la connexion entre le client d'abonnement sélectionné et les serveurs proxy d'abonnement sélectionnés, configurés pour ce client.

Remarque : S'il existe un problème de connexion que vous pouvez résoudre, le client d'abonnement relance le téléchargement après le délai spécifié.

Une erreur s'est produite lors de la récupération des mises à jour pour les modules <ModuleName> et <msg>.

Motif :

Lorsqu'un client d'abonnement est configuré pour télécharger un module non disponible au téléchargement sur son proxy d'abonnement, le proxy tente de récupérer les mises à jour pour ce module. Cet événement survient lorsqu'une erreur s'est produite durant la récupération des mises à jour. Le module d'abonnement consigne l'échec dans le journal et poursuit le traitement.

Action :

Aucune action n'est requise. Le proxy d'abonnement tente de récupérer les mises à jour lors de l'opération de mise à jour suivante.

Erreur lors de l'installation de -> contenu dans EEM : <NomComp> et <msg>. Ce contenu sera téléchargé et installé ultérieurement.

Motif :

Un problème technique est survenu lors de l'installation des mises à jour de contenu sur le serveur de gestion. La section *msg* indique la cause de l'erreur.

Action :

Aucune action n'est requise. Lisez la section *msg* du message pour en savoir plus sur cette erreur. Le premier serveur disponible dans la liste et configuré en tant que proxy d'abonnement pour les mises à jour de contenu tentera d'installer la mise à jour indiquée pour *NomComposant* lors de la prochaine mise à jour planifiée.

Un erreur s'est produite lors de la vérification de la signature de la mise à jour du composant <NomComp>. La mise à jour a été ignorée. Ce composant sera téléchargé ultérieurement.

Motif :

Un problème technique est survenu lors de la vérification de la signature de la mise à jour du composant nommé dans le message. Si la clé publique n'a pas été modifiée manuellement, le composant sera téléchargé lors du cycle suivant.

Action :

Si la clé publique n'a pas été modifiée, aucune action n'est requise. Si la clé publique a été modifiée manuellement, demandez de l'aide pour restaurer la clé publique associée à votre clé privée et obtenir une nouvelle paire de clés. Pour obtenir de l'aide, contactez l'assistance technique à l'adresse http://ca.com/worldwide.

Une erreur s'est produite lors du téléchargement du fichier de mise à jour du proxy vers le client, pour le composant - <NomComp> et <msg>.

Motif :

Un problème technique est survenu lors du téléchargement du fichier de mise à jour du proxy d'abonnement vers le client d'abonnement. Il peut s'agir d'une erreur d'E/S ou d'un problème iTech. Le client tentera de télécharger à nouveau le composant nommé dans le message lors du cycle suivant.

Action :

Sur le client d'abonnement, vérifiez la connectivité avec les Proxies d'abonnement pour le client, en envoyant une requête ping à chaque serveur sélectionné. Si le ping renvoie des données, aucune action supplémentaire n'est requise. En cas de problème de connexion, passez en revue la configuration et, si vous détectez des erreurs, corrigez-les.

Une erreur s'est produite lors de l'exportation du fichier bat pour la mise à jour du composant <NomComp> et <msg>.

Motif :

Les mises à jour d'abonnement peuvent inclure les mises à jour du module produit (fichiers binaires) sous la forme d'un fichier par lot (fichier bat) qui doit être exécuté pour mettre à jour le module. Les clients récupèrent le fichier bat téléchargé sur le proxy par le biais d'une exportation effectuée par ce dernier. Une erreur s'est produite lors de l'exportation du fichier bat téléchargé pour la mise à jour du module *NomComposant* nommé dans le message. La mise à jour prévue pour le module produit n'a pas eu lieu. Des détails supplémentaires sont fournis dans la section msg du message. La cause de cette erreur peut être un problème iTech ou un problème de réseau.

Action :

Essayez d'appliquer les actions correctives suivantes.

- Sur le client d'abonnement, vérifiez la connectivité avec les Proxies d'abonnement pour le client, en envoyant une requête ping à chaque serveur sélectionné. Si le ping renvoie des données, aucune action supplémentaire n'est requise. En cas de problème de connexion, passez en revue la configuration et, si vous détectez des erreurs, corrigez-les.
- Redémarrez iGateway. Saisissez : $IGW_LOC/S99igateway start.

  $IGW_LOC correspond à l'emplacement suivant : /opt/CA/SharedComponents/iTechnology.

Une erreur s'est produite lors de la récupération de la liste des composants auprès du proxy, pour le module - <NomModule> et <msg>.

Motif :

Une erreur s'est produite lors de la récupération de la liste des composants auprès du proxy, pour un module donné. Le message d'erreur est décrit dans la section <msg>. Il peut s'agir d'un problème iTech ou d'un problème de réseau.

Action :

Essayez d'appliquer les actions correctives suivantes.

- Sur le client d'abonnement, vérifiez la connectivité avec les Proxies d'abonnement pour le client, en envoyant une requête ping à chaque serveur sélectionné. Si le ping renvoie des données, aucune action supplémentaire n'est requise.
- En cas de problème de connexion, passez en revue la configuration et, si vous détectez des erreurs, corrigez-les.

Remarque : Si une action appliquée résout le problème, le client récupérera la liste des composants auprès de son proxy lors du cycle de mise à jour suivant.

Une erreur s'est produite lors de l'analyse du fichier xml ComponentInfo - fileName.

Motif :

Une erreur s'est produite lors de l'analyse du fichier xml ComponentInfo nommé dans le message.

Action :

Essayez d'appliquer les actions correctives suivantes.

- Déterminez s'il s'agit d'une erreur d'E/S ou d'une exception ayant entraîné l'interruption du téléchargement et donc un package incomplet.
- Si cet événement d'autosurveillance survient à nouveau, demandez de l'aide. Une récurrence pourrait indiquer que le package de mise à jour a été créé avec un fichier ComponentInfo.xml incorrect. Pour obtenir de l'aide, contactez l'assistance technique à l'adresse http://ca.com/worldwide.

  Remarque : Le proxy récupérera le fichier approprié lorsqu'un fichier ComponentInfo.xml correct sera disponible sur le serveur de mise à jour d'abonnement CA.

Une erreur s'est produite lors de l'analyse du fichier manifest - fileName.

Motif :

Une erreur s'est produite lors de l'analyse du fichier manifest nommé dans le message.

Action :

Essayez d'appliquer les actions correctives suivantes.

- Déterminez s'il s'agit d'une erreur d'E/S ou d'une exception ayant entraîné l'interruption du téléchargement et donc un package incomplet.
- Si cet événement d'autosurveillance survient à nouveau, demandez de l'aide. Une récurrence pourrait indiquer que le package de mise à jour a été créé avec un fichier ComponentInfo.xml incorrect. Pour obtenir de l'aide, contactez l'assistance technique à l'adresse http://ca.com/worldwide.

  Remarque : Le proxy récupérera le fichier approprié lorsqu'un fichier ComponentInfo.xml correct sera disponible sur le serveur de mise à jour d'abonnement CA.

Une erreur s'est produite lors de l'analyse du fichier XML RSS Feed - FileName.

Motif :

Une erreur s'est produite lors de l'analyse du fichier XML de flux RSS indiqué dans le message. Celui-ci indique que le téléchargement a été interrompu.

Action :

Examinez l'URL du flux RSS qui fait partie du service Configuration globale du service : Module d'abonnement. Vérifiez qu'elle est correcte et recommencez le téléchargement. La présence de données dans la liste Modules à télécharger indique que l'URL est correcte.

Echec de la connexion à EEMServer.

Motif :

La connexion entre le proxy d'abonnement et le serveur de gestion CA Enterprise Log Manager a échoué. Cet échec peut être dû à une indisponibilité temporaire du serveur CA EEM, au moment où il reçoit les mises à jour.

Action :

Aucune action n'est requise. Le système CA EEM du serveur de gestion CA Enterprise Log Manager est de nouveau disponible lorsqu'il n'est plus occupé, sans nécessiter une intervention de l'utilisateur.

Un composant non valide a été téléchargé pour <CompName> sur le proxy.

Motif :

La vérification de signature effectuée sur le composant téléchargé indiqué dans le message a échoué, entraînant la suppression du composant. Cet échec de vérification peut indiquer que le composant téléchargé a été altéré. Le proxy tente de télécharger ce composant à chaque cycle de mise à jour suivant et effectue la validation jusqu'à qu'un composant valide soit détecté.

Action :

Si la clé publique n'a pas été modifiée, aucune action n'est requise. Si la clé publique a été modifiée manuellement, demandez de l'aide pour restaurer la clé publique associée à votre clé privée et obtenir une nouvelle paire de clés. Pour obtenir de l'aide, contactez l'assistance technique à l'adresse http://ca.com/worldwide.

Aucun module n'a été sélectionné pour l'obtention des mises à jour. Sélectionnez les modules pour obtenir les mises à jour auprès du serveur d'abonnement.

Motif :

Aucun module à télécharger n'a été sélectionné lors de la configuration du proxy d'abonnement. Les modules disponibles au téléchargement sont spécifiés lors de la configuration de l'URL du flux RSS. Le traitement se poursuit ; le module d'abonnement se comporte conformément à la configuration.

Action :

Configurez les modules à télécharger pour ce proxy d'abonnement et ses clients d'abonnement.

Il n'existe aucun serveur proxy ou celui-ci est introuvable. Soit les serveurs proxy spécifiés pour ce client ne sont pas en cours d'exécution, soit aucun proxy n'a été spécifié pour le client.

Motif :

Le proxy par défaut n'est pas actif ; aucun serveur proxy n'a été configuré pour le client ou les serveurs proxy configurés ne sont pas actifs. Le module d'abonnement n'a pu effectuer la mise à jour planifiée.

Action :

Essayez d'appliquer les actions suivantes.

- Vérifiez la configuration d'abonnement pour le client.
  1. Cliquez sur l'onglet Administration, à gauche de l'onglet Evénements d'autosurveillance dans lequel ce message s'affiche.
  2. Vérifiez qu'un ou plusieurs serveurs sont répertoriés dans la liste des Proxies d'abonnement pour le client.
- Démarrez le proxy d'abonnement par défaut et les proxies d'abonnement en ligne configurés dans la liste de proxies du client.
  1. Cliquez sur l'onglet Administration, à gauche de l'onglet Evénements d'autosurveillance dans lequel ce message s'affiche.
  2. Identifiez les proxies en ligne en consultant la zone Sélectionné(e)(s) des Proxies d'abonnement pour le client.
  3. Dans la Liste de services, cliquez sur le noeud Module d'abonnement et notez l'entrée pour Proxy d'abonnement par défaut.
  4. Si un serveur CA Enterprise Log Manager identifié ne fonctionne pas, démarrez-le.
- Redémarrez iGateway. Saisissez : $IGW_LOC/S99igateway start.

  $IGW_LOC correspond à l'emplacement suivant : /opt/CA/SharedComponents/iTechnology.

Aucune mise à jour pour le composant – <CompName> n'a été téléchargée sur le client.

Motif :

Des mises à jour pour le composant *CompName* ont été téléchargées par le proxy d'abonnement à partir du serveur d'abonnement CA, mais ces mises à jour n'ont pas été téléchargées sur le client d'abonnement. Il s'agit d'une erreur de fichier, c'est-à-dire que le fichier téléchargé par le client ne contenait pas les données prévues.

Remarque : Comme *CompName* est un composant d'un module sélectionné pour le téléchargement, il sera téléchargé lors du prochain cycle de mise à jour.

Action :

Aucune action n'est requise.

L'hôte de proxy - <HostName> n'est pas un proxy ELM valide.

Motif :

Le proxy d'abonnement sélectionné n'est pas un proxy d'abonnement CA Enterprise Log Manager valide. Ce problème peut se produire lorsque l'hôte spécifié a été reconfiguré pour devenir un client d'abonnement.

Action :

Supprimez *HostName* de la liste de sélection des Proxies d'abonnement pour le client. S'il s'agissait du seul proxy sélectionné, choisissez un nouveau proxy d'abonnement.

L'hôte de proxy - <HostName> n'est pas un hôte valide.

Motif :

Le client d'abonnement tente de se connecter à chacun des proxies de la liste, mais aucun ne fonctionne. Lorsque le client tente d'utiliser le proxy par défaut, la connexion échoue car le proxy par défaut est également arrêté. Le client attend que les proxies configurés démarrent ou que l'utilisateur configure un proxy valide.

Action :

Essayez d'appliquer les actions suivantes.

- Examinez la configuration du client d'abonnement sélectionné et assurez-vous que les serveurs figurant dans la liste Sélectionné(e)(s) des Proxies d'abonnement pour le client sont configurés en tant que Proxy d'abonnement ou en tant que Proxy d'abonnement hors ligne.
- Si les serveurs sélectionnés comme Proxies d'abonnement pour le client ne sont pas définis en tant que proxies d'abonnement, supprimez-les de la liste Sélectionné(e)(s) et sélectionnez un ou plusieurs serveurs définis en tant que tels.
- Si les proxies configurés et le proxy par défaut ne fonctionnent pas, redémarrez iGateway. Saisissez : $IGW_LOC/S99igateway start.

  $IGW_LOC correspond à l'emplacement suivant : /opt/CA/SharedComponents/iTechnology.

La capacité de l'espace disque situé <chemin téléchargement temp> - <pathName> a dépassé la limite de 90 %. Libérez de l'espace disque. Les mises à jour n'ont pas pu être téléchargées du proxy au client.

Motif :

Généralement, les clients téléchargent les mises à jour depuis le proxy d'abonnement vers un emplacement temporaire avant de les installer. Le téléchargement ne peut se poursuivre que s'il dispose d'au moins 10 % d'espace disque libre. Ce message indique que l'espace disque utilisé de l'emplacement temporaire dépasse 90 %. Le processus d'abonnement arrête le téléchargement des mises à jour.

Action :

Pour récupérer et télécharger les mises à jour, vous devez libérer de l'espace disque avant le prochain téléchargement planifié, pour que le téléchargement arrêté puisse reprendre et se terminer. Pour gérer l'espace disque de manière proactive, créez une alerte d'action.

Impossible de trouver le fichier de mise à jour pour le composant – <CompName> sur le serveur proxy. Ce fichier n'a donc pas pu être téléchargé sur le client pour installation.

Motif :

Le client d'abonnement ne peut pas télécharger le fichier de mise à jour pour le composant indiqué dans le message, car ce fichier n'est pas disponible sur le serveur proxy d'abonnement configuré. Ce problème peut survenir lorsque le fichier de mise à jour a été supprimé manuellement ou qu'il a dépassé l'ancienneté (en jours) définie dans le paramètre Nettoyage des mises à jour antérieures à.

Remarque : Assurez-vous que ce client d'abonnement dispose d'une planification de mise à jour configurée et qu'il reste en marche, pour ne pas rater les mises à jour. Le proxy conserve les mises à jour uniquement durant le nombre de jours défini par le paramètre Nettoyage des mises à jour antérieures à (paramètre d'abonnement global).

Action :

Recherchez un proxy d'abonnement possédant encore le module contenant le composant requis, *CompName*. Copiez les répertoires d'abonnement de ce proxy vers le proxy d'abonnement de ce client. Pour ce faire, utilisez la procédure décrite pour la mise à jour d'un proxy hors ligne à partir d'un proxy en ligne.

Remarque : Il est important de copier les répertoires de manière récursive, car *CompName* se compose de nombreux fichiers et ce processus garantit que tous les fichiers requis sont disponibles.

Les mises à jour pour le composant – <CompName> s'appliquent aux versions supérieures ou égales à <CompVersionApplicableTo>. La version actuelle du composant installé sur le client est <CurrentVersion>. Cette mise à jour ne peut donc être appliquée.

Motif :

La mise à jour disponible pour le composant indiqué dans le message peut être appliquée uniquement si la version installée est égale ou supérieure à *CompVersionApplicableTo*. Toutefois, le composant installé affiche une version inférieure à celle à laquelle la mise à jour peut être appliquée. Par conséquent, la mise à jour ne peut pas être installée. Par exemple, si la mise à jour est la version r3 applicable à la version r2, mais que la version du composant installé est r1, la mise à jour ne peut pas être installée.

Action :

Estimez la nécessité de cette mise à jour. Si elle s'avère nécessaire, demandez la version spécifiée par *CompVersionApplicableTo*. Appliquez cette version prérequise. Par exemple, si vous disposez de la version r1 et que vous souhaitez installer la r3, vous devez tout d'abord télécharger et installer la version r2, puis la version r3. Si la version r3 ne vous intéresse pas, vous pouvez l'ignorer. Si la version r4 ne présente aucune dépendance, vous pouvez l'installer directement.

La mise à jour pour le composant <CompName> a été altérée. La mise à jour a été ignorée. Elle sera téléchargée ultérieurement, lorsqu'une mise à jour adaptée à ce composant sera disponible.

Motif :

La mise à jour pour le composant indiqué dans ce message n'est téléchargée sur aucun client car elle semble avoir été altérée. Il est possible que ce problème soit survenu durant la copie vers un proxy hors ligne. Une version valide de la mise à jour est téléchargée lors du cycle suivant, en attente d'authentification.

Action :

Si le champ Clé publique n'a pas été modifié manuellement, signalez le problème. Pour obtenir de l'aide, contactez l'assistance technique à l'adresse http://ca.com/worldwide.

Important : Ne modifiez jamais manuellement les données du champ Clé publique, dans la page Configuration globale du service : Module d'abonnement. Vous seriez à l'origine de problèmes de mise à jour de l'abonnement.

Erreurs de comparaison de version. Format de version incorrect

Motif :

Cet événement se produit lorsque l'une des entrées de champ de version affiche un format incorrect, par exemple version_on_the_client, version_on_updates_server.

Action :

Signalez le problème à CA pour qu'il puisse être corrigé. Pour obtenir de l'aide, contactez l'assistance technique à l'adresse http://ca.com/worldwide.

Remarque : Cet événement cessera de se produire une fois la correction effectuée sur le serveur d'abonnement CA.

A propos des mises à jour à la demande

Une mise à jour à la demande est différente d'une mise à jour planifiée en cela qu'elle est effectuée immédiatement et qu'elle met uniquement à jour le serveur sélectionné. Vous pouvez invoquer une mise à jour à la demande pour un seul serveur CA Enterprise Log Manager à la fois. Pour mettre à jour un client d'abonnement à la demande, commencez par mettre à jour son serveur proxy.

En général, les mises à jour planifiées conservent à jour l'ensemble de vos serveurs CA Enterprise Log Manager avec les derniers fichiers binaires. Elles conservent également à jour votre serveur CA Enterprise Log Manager de gestion avec les derniers fichiers de configuration et de contenu. Il est parfois approprié d'invoquer une mise à jour non planifiée vers un seul serveur.

Vous pouvez envisager des mises à jour à la demande dans les cas suivants.

- Un échec ou un avertissement d'événement d'abonnement est signalé pour le serveur de gestion, par exemple :

  Echec de la connexion à EEMServer

  Erreur lors de l'installation de contenu dans EEM

  Sélectionnez le serveur de gestion et cliquez sur Actualiser. Si le serveur de gestion est configuré en tant que proxy pour les mises à jour de contenu, le serveur télécharge de nouvelles mises à jour à partir du serveur d'abonnement CA et transmet les mises à jour de contenu et de configuration au composant EEM. Ensuite, il installe automatiquement les mises à jour des fichiers binaires sur son client.

- Un message d'échec d'événement d'abonnement indique que le téléchargement est interrompu. Si le téléchargement est interrompu sur un seul serveur proxy, effectuer une mise à jour à la demande lance une nouvelle tentative de téléchargement. Une mise à jour à la demande est conseillée si vous constatez l'échec peu après qu'il se soit produit. Si l'heure de début entre le proxy et le client est suffisante, une mise à jour à la demande du proxy peut se terminer avant que la mise à jour planifiée commence chez les clients qui obtiennent des mises à jour à partir de ce proxy.
- Vous installez un nouveau serveur CA Enterprise Log Manager, vous le configurez en tant que proxy et vous souhaitez faire en sorte que les dernières mises à jour soient appliquées avant de l'utiliser.
- Vous remarquez qu'un module requis par un client n'a pas été sélectionné comme module à télécharger. Toutefois, ce module était sélectionné par le proxy. Exécuter Actualiser sur le client installe les mises à jour manquantes.

Informations complémentaires :

Fonctionnement des mises à jour à la demande (page 242)
Lancement d'une mise à jour à la demande (page 243)

Fonctionnement des mises à jour à la demande

A la différence des cycles de mise à jour d'abonnement planifiés qui mettent à jours tous les proxies et clients, Actualiser affecte uniquement l'hôte sélectionné. Le traitement commence lorsque vous cliquez sur le bouton Actualiser, si la mise à jour planifiée n'est pas en cours. Si une mise à jour planifiée est en cours, le fait de cliquer sur Actualiser ne produit aucun effet. Si l'heure de début d'une mise à jour planifiée survient lorsque le traitement Actualiser est en cours, le processus planifié n'est pas exécuté. Lorsque le traitement à la demande se termine, les cycles de mise à jour planifiés reprennent.

Si vous modifiez des valeurs configurées, veillez à patienter jusqu'à la fin de l'intervalle d'actualisation avant d'exécuter une mise à jour à la demande. CA Enterprise Log Manager génère un événement d'autosurveillance une fois la mise à jour terminée.

Les tâches effectuées par une mise à jour à la demande dépendent du rôle d'abonnement du serveur sélectionné. Tenez compte des différences de résultats pour les rôles d'abonnement distincts dont un serveur peut disposer.

- Si le serveur sélectionné est un proxy d'abonnement pour les mises à jour de contenu (en ligne), il effectue les opérations suivantes.
  - Il extrait les dernières mises à jour pour les modules sélectionnés à télécharger à partir du serveur d'abonnement CA et les charge dans son chemin de téléchargement.
  - Il recherche de nouvelles mises à jour de contenu et de configuration dans son chemin de téléchargement et, le cas échéant, transmet ces mises à jour à l'EEM local.
  - Il recherche de nouvelles mises à jour des fichiers binaires dans son chemin de téléchargement et les installe automatiquement sur son client.
- Si le serveur sélectionné est un proxy d'abonnement pour les mises à jour de contenu (hors ligne), il effectue les opérations suivantes.
  - Il recherche de nouvelles mises à jour de contenu et de configuration dans son chemin de téléchargement et, le cas échéant, transmet ces mises à jour à l'EEM local.
  - Il recherche de nouvelles mises à jour des fichiers binaires dans son chemin de téléchargement et les installe automatiquement sur son client.

- Si le serveur sélectionné n'est pas un proxy d'abonnement pour les mises à jour de contenu, mais un proxy en ligne, il effectue les opérations suivantes.
  - Il extrait les dernières mises à jour pour les modules sélectionnés à télécharger à partir du serveur d'abonnement CA et les charge dans son chemin de téléchargement.
  - Il recherche de nouvelles mises à jour des fichiers binaires dans son chemin de téléchargement et les installe automatiquement sur son client.
- Si le serveur sélectionné est un client avec un proxy en ligne seulement, il effectue les opérations suivantes.
  - Il contacte l'un de ses serveurs proxy en ligne et télécharge les mises à jour disponibles.
  - Il recherche de nouvelles mises à jour des fichiers binaires dans son chemin de téléchargement et, le cas échéant, les installe automatiquement.
- Si le serveur sélectionné est un proxy hors ligne, il effectue les opérations suivantes.
  - Il recherche de nouvelles mises à jour des fichiers binaires dans son chemin de téléchargement et, le cas échéant, les installe automatiquement sur son client.
- Si le serveur sélectionné est un client avec un proxy hors ligne seulement, il effectue les opérations suivantes.
  - Il contacte son serveur proxy hors ligne et télécharge les mises à jour disponibles.
  - Il recherche de nouvelles mises à jour des fichiers binaires dans son chemin de téléchargement et, le cas échéant, les installe automatiquement.

Lancement d'une mise à jour à la demande

Vous pouvez mettre à jour un ou plusieurs serveurs à la demande à l'aide de la fonction Actualiser. Lorsque vous mettez à jour plusieurs serveurs d'affilée, pensez à vérifier que le traitement se termine sur un serveur avant de commencer sur le suivant. Vérifiez l'état des événements d'autosurveillance.

Pour mettre à jour un serveur sélectionné à la demande

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Développez Module d'abonnement dans la liste de services.

3. Sélectionnez le serveur à mettre à jour et analysez son rôle.
4. S'il s'agit d'un proxy d'abonnement pour les mises à jour de contenu, tel qu'indiqué sur la page de configuration globale du service, cliquez sur Actualiser.

   Le serveur est mis à jour avec les mises à jour de contenu et de configuration, ainsi qu'avec les mises à jour des fichiers binaires des modules sélectionnés pour le téléchargement.
5. S'il s'agit d'un proxy d'abonnement pour les clients, cliquez sur Actualiser.

   Le serveur est mis à jour avec les mises à jour des fichiers binaires des modules sélectionnés pour le téléchargement.
6. S'il s'agit d'un client avec un proxy en ligne, procédez comme suit.
   a. Dans la liste sélectionnée des Proxies d'abonnement pour le client, identifiez un proxy pour ce client.
   b. Sélectionnez le proxy pour le client et cliquez sur Actualiser.
   c. Sélectionnez le client et cliquez sur Actualiser.

   Le serveur est mis à jour avec les mises à jour des fichiers binaires des modules sélectionnés pour le téléchargement.
7. S'il s'agit d'un proxy d'abonnement hors ligne, procédez comme suit.
   a. Sélectionnez n'importe quel proxy en ligne et cliquez sur Actualiser.
   b. Copiez les mises à jour sur le chemin de téléchargement du proxy hors ligne.
   c. Sélectionnez le proxy hors ligne et cliquez sur Actualiser.

   Le serveur est mis à jour avec les mises à jour des fichiers binaires des modules sélectionnés pour le téléchargement.
8. S'il s'agit d'un client avec un proxy hors ligne, procédez comme suit.
   a. Mettez à jour le proxy hors ligne tel que décrit à l'étape 7.
   b. Sélectionnez le client et cliquez sur Actualiser.

   Le serveur est mis à jour avec les mises à jour des fichiers binaires des modules sélectionnés pour le téléchargement.

Application des mises à jour d'abonnement aux agents et aux connecteurs

Les mises à jour, les Service Packs et les parutions ponctuelles sont tous diffusés par le biais d'un abonnement. Souvent, les modules à télécharger incluent des agents et des intégrations. Lorsque ces modules sont téléchargés sur un client d'abonnement qui gère des agents, vous devez appliquer ces mises à jour aux agents, après avoir vérifié que le client qui gère les agents a bien été mis à jour. Les mises à jour d'agent doivent être appliquées avant les mises à jour de connecteur.

Pour mettre à niveau les agents CA Enterprise Log Manager avec des mises à jour d'abonnement

1. Si la mise à niveau inclut le module Agents, mettez à jour vos agents via la plate-forme, en procédant comme suit.
   a. Cliquez sur l'onglet Administration, puis sur le sous-onglet Collecte de journaux.
   b. Déterminez si vous souhaitez appliquer les mises à jour à tous les agents en une fois, à un groupe d'agents sélectionnés uniquement ou à un agent individuel, suivant le niveau d'application de la plate-forme.
      - Si tous vos agents sont installés sur la même plate-forme, sélectionnez Explorateur d'agent, puis cliquez sur Abonnement.
      - Si vos groupes d'agents sont composés d'agents installés sur la même plate-forme, développez l'Explorateur d'agent, sélectionnez un groupe d'agents et cliquez sur Abonnement.
      - Vous pouvez également développer l'Explorateur d'agent, puis un groupe d'agents afin de sélectionner un agent et de cliquer sur Abonnement.

      L'Assistant d'abonnement s'affiche.
   c. Si vous aviez sélectionné l'Explorateur d'agent ou un groupe d'agents, sélectionnez Mises à jour de l'agent, choisissez la plate-forme souhaitée dans la liste déroulante Plate-forme, cliquez sur Rechercher, puis sur l'étape Sélection de version.
   d. Si vous avez sélectionné un agent, sélectionnez Mises à jour de l'agent et cliquez sur l'étape Sélection de version.
   e. Sélectionnez Mise à jour de la version pour chaque agent répertorié.
   f. Cliquez sur Enregistrer et fermer.
   g. Vérifiez que l'opération a réussi. Cliquez sur Etat et commande. Cliquez sur Configuration réussie. Notez la version de configuration appliquée.
   h. Répétez l'opération, si nécessaire, pour mettre à jour tous les agents.

2. Si la mise à niveau inclut le module Intégrations, mettez à jour les connecteurs de vos agents, en procédant comme suit.
    a. Cliquez sur l'onglet Administration, puis sur le sous-onglet Collecte de journaux.
    b. Déterminez si vous souhaitez appliquer les mises à jour à tous les connecteurs de tous les agents simultanément, aux connecteurs d'un groupe d'agents sélectionnés uniquement ou aux connecteurs d'un agent individuel.
    c. Sélectionnez l'Explorateur d'agent, un groupe d'agents ou un agent unique. Cliquez ensuite sur Abonnement.
    d. Sélectionnez Mises à jour du connecteur dans la Liste de sélection des mises à jour.
    e. Vous pouvez également sélectionner une valeur dans une ou plusieurs listes déroulantes ci-après, pour modifier la valeur par défaut, Tous : Groupe d'agents, Plate-forme, Intégration. Cliquez sur Rechercher.
    f. Cliquez sur l'étape Sélection de version.
    g. Cliquez sur Tout sélectionner pour sélectionner tous les membres de la liste ou sélectionnez chaque ligne correspondant au connecteur que vous souhaitez mettre à jour. Pour chaque ligne sélectionnée, choisissez la version de mise à jour à appliquer.
    h. Cliquez sur Enregistrer et fermer.
3. Vérifiez les mises à jour. Exécutez à nouveau l'Assistant d'abonnement. Sélectionnez l'étape Sélection de version pour afficher la version actuelle et vérifier qu'il s'agit bien de la version choisie pour la mise à jour. Cliquez sur Annuler.

Informations complémentaires :

Application des mises à jour d'abonnement (page 675)
Ouverture de l'assistant de liste de mises à jour (page 676)
Sélection d'agents ou de connecteurs pour mise à jour (page 677)
Mise à jour des versions d'intégration d'un agent ou d'un connecteur (page 678)

Chapitre 8 : Filtres et profils

Ce chapitre traite des sujets suivants :

A propos des filtres et des profils

Vous pouvez définir ou modifier des filtres pour ajuster les informations sur les événements affichées dans vos requêtes et dans vos rapports. La fenêtre principale CA Enterprise Log Manager vous permet d'accéder à la boîte de dialogue des filtres globaux. Vous pouvez ajouter des filtres locaux à partir de l'affichage d'une requête ou d'un rapport donné. En définissant un profil, vous limitez la liste des balises, des requêtes et des rapports utilisés aux seuls rapports, balises et requêtes qui vous intéressent.

Cliquez sur un bouton de filtre de rapport pour ouvrir la boîte de dialogue de création correspondante. Sélectionnez le profil à appliquer dans la liste déroulante.

Filtre global 

S'applique à tous les rapports ou à toutes les requêtes que vous affichez, dans la session *actuelle* uniquement, et permet d'afficher une grande variété de types d'événements qualifiés de façon identique. Le bouton Filtre global apparaît au sommet de la fenêtre principale CA Enterprise Log Manager, à côté du menu Serveur du gestionnaire de journaux. Vous pouvez utiliser un filtre global afin d'afficher, par exemple, tous les événements reçus lors de la semaine écoulée ou pour un hôte donné. L'interface Filtre global vous permet également de contrôler certains paramètres concernant toute l'application.

Remarque : Par défaut, un filtre global renvoie les données relatives aux six heures écoulées.

Filtre local 

S'applique uniquement à la requête ou au rapport actuel. Le bouton Filtre local apparaît au sommet du volet Détails dans l'affichage d'une requête ou d'un rapport. Lorsque vous affichez un nouveau rapport, le filtre local n'est ni appliqué, ni enregistré, sauf si vous enregistrez ce rapport en tant que favori avec ce filtre. Les filtres locaux vous permettent de restreindre la vue actuelle, par exemple en affichant un seul hôte dans la vue d'un rapport sur plusieurs hôtes, sans modifier les autres vues du rapport.

Profil

Filtre spécifique au produit, qui s'applique à la liste des balises, la liste des requêtes et la liste des rapports. La liste déroulante Profil apparaît au sommet de la fenêtre principale CA Enterprise Log Manager, à côté du bouton Effacer les filtres.

A propos des filtre simples

Avant d'utiliser l'assistant de conception de requête ou l'Assistant de conception de profil, familiarisez-vous avec les filtres simples.

Exemples de filtres simples

Voici un exemple de chaque type de filtre simple.

Type de filtre	Valeur	Description
Modèle idéal	Antivirus	Affiche uniquement les données d'événement générées par les produits suivants et assimilés : ■ CA Anti-Virus ■ McAfee VirusScan ■ Symantec Antivirus Corporate Edition ■ TrendMicro OfficeScan
Catégorie d'événement/ Classe d'événement	Accès au système/ activité de connexion	Affiche uniquement les données d'événement relatives aux utilisateurs se connectant à un système.
Nom du journal d'événements	Cisco PIX Firewall	Affiche uniquement les données d'événement générées par les unités Cisco PIX Firewall.

A l'exception du Nom du journal d'événements, les filtres sont basés sur la grammaire commune aux événements (CEG).

- Pour en savoir plus sur les filtres basés sur la technologie, consultez la liste des modèles idéaux.
- Pour en savoir plus sur les filtres basés sur une catégorie de produit/une classe/une action, consultez la liste des catégories d'événement et la liste des classes d'événement.

Vous trouverez ces listes dans l'aide en ligne, à la rubrique Grammaire commune aux événements.

Définition d'un filtre simple

Vous pouvez définir des filtres simples pour établir des critères pour les données d'événement à afficher ou à soumettre à la génération de rapports. Lorsqu'ils sont définis dans le cadre de l'assistant de conception de requête, les filtres simples vous permettent de limiter les données d'événement renvoyées par une requête utilisée dans un rapport ou une alerte. Lorsqu'ils sont définis dans le cadre de l'Assistant de conception de profil, les filtres simples limitent les données affichées dans les résultats de rapport ou de requête lors de l'application du profil.

1. Ouvrez l'assistant.
2. Déterminez le type de filtre simple à créer.
   - Filtre basé sur la technologie
   - Filtre basé sur la catégorie, sur la classe et la catégorie, ou encore sur la classe, la catégorie et l'action
   - Filtre basé sur le produit
3. Pour définir un filtre basé sur la technologie, sélectionnez la case à cocher Modèle idéal :, puis sélectionnez une valeur dans la liste déroulante Modèle idéal.
4. Pour définir un filtre basé sur une catégorie d'événement de sécurité, sur une catégorie et une classe, ou encore sur une catégorie, une classe et une action, procédez comme suit.
   a. Sélectionnez la case à cocher Catégorie d'événement :, puis sélectionnez une valeur dans la liste déroulante correspondante.
   b. Sélectionnez la case à cocher Classe d'événement :, puis sélectionnez une valeur dans la liste déroulante (facultatif).
   c. Si vous avez choisi Classe d'événement, sélectionnez la case à cocher Action d'événement :, puis sélectionnez une valeur dans la liste déroulante (facultatif).

   Remarque : Vous pouvez également définir ce type de filtre par le biais d'un filtre basé sur la technologie.
5. Pour définir un filtre basé sur le produit, sélectionnez la case à cocher Nom du journal d'événements :, puis sélectionnez une valeur dans la liste déroulante.
6. Fermez l'assistant.

A propos des filtres de profil

Un profil est un ensemble de filtres. Vous pouvez créer un profil à partir de filtres de balises, de filtres de données ou d'une combinaison de ces deux types. Le filtre de balise de requête limite les requêtes disponibles à la sélection ; le filtre de balise de rapport a la même fonction pour les rapports. Les filtres de données limitent les données affichées dans les résultats d'une requête ou dans un rapport. Les filtres de profil s'appliquent aux requêtes, aux rapports, ainsi qu'aux alertes et rapports planifiés.

Vous pouvez sélectionner des filtres de balises séparément pour les rapports et les requêtes. Ils incluent, sans s'y limiter, les filtres ci-dessous.

- Balises normalisées : COBIT, FISMA, GLBA, HIPAA, NERC, PCI, SAS 70, SOX.

  Les filtres de balises normalisées s'appliquent aux balises de rapport, et non aux balises de requête.

- Balises de catégorie d'événement de sécurité, telles que Sécurité de contenu, Sécurité de l'hôte, Sécurité du réseau, Sécurité opérationnelle, Accès aux ressources, Accès au système.
- Balises produit, telles que CA Access Control, CA Identity Manager et CA SiteMinder.

Vous pouvez sélectionner un filtre de données simple ou créer un filtre de données avancé. Voici une brève description de chacun de ces types de filtre.

- Les filtres de données simples peuvent être basés sur l'un des éléments suivants.
  - Une technologie spécifique (logiciel système, application et services hôte, services et application de réseau)
  - Une catégorie d'événement CEG spécifique, une classe et une catégorie d'événement CEG spécifiques, ou encore une classe, une action et une catégorie d'événement CEG spécifiques
  - Un produit spécifique
- Les filtres de données avancés sont basés sur une requête SQL définie par l'utilisateur et composée d'une ou plusieurs clauses WHERE. La requête sélectionne une colonne CEG avec une clause WHERE composée de cette colonne CEG, d'un opérateur sélectionné et d'une valeur spécifiée.

Création d'un profil

Vous pouvez créer des profils, qui permettent de limiter les éléments affichés dans CA Enterprise Log Manager, en fonction des besoins de votre environnement. Par exemple, vous pouvez créer un profil CA Access Control, qui affiche uniquement les rapports, les requêtes et les événements relatifs à Access Control.

Le processus de création d'un profil à l'aide de l'assistant de profil se compose des étapes suivantes.

1. Ouverture de l'assistant de profil
2. Attribution d'un nom de profil et saisie d'une description
3. Identification des informations affichées à l'aide de filtres simples et avancés
4. Sélection des requêtes et des rapports affichés à l'aide de filtres de balises

Informations complémentaires :

Ouverture de l'assistant de profil (page 253)
Ajout des détails du profil (page 253)
Création de filtres de données (page 254)
Création de filtres de balises (page 255)

Ouverture de l'assistant de profil

Pour créer un nouveau profil ou modifier un profil existant, vous devez ouvrir l'assistant de profil.

Pour ouvrir l'assistant de profil

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

   La liste du dossier Collecte de journaux s'affiche.

2. Sélectionnez le dossier Profils.

   Les boutons Profils apparaissent dans le volet Détails.

3. Cliquez sur Nouveau profil :  .

   L'assistant de profil s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier de règle sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier de règle et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Ajout des détails du profil

Vous devez attribuer un nom au profil. Vous pouvez également saisir une description facultative pour référence.

Pour attribuer un nom au profil

1. Ouvrez l'assistant de profil.
2. Saisissez un nom pour le nouveau profil. Ce nom peut contenir jusqu'à 80 caractères, y compris des caractères spéciaux.
3. Saisissez une description (facultatif).
4. Avancez jusqu'à l'étape Filtres de données.

Création de filtres de données

Vous filtrez les informations affichées par votre profil à l'aide de filtres simples ou avancés. Chaque profil doit posséder au moins un filtre.

Pour définir des filtres de données pour un profil

1. Ouvrez l'assistant de profil.
2. Saisissez le nom du profil, si cela n'a pas déjà été fait, puis passez à l'étape Filtres de données.

   La boîte de dialogue Filtres s'ouvre sur l'onglet Filtres simples.
3. Créez tous les filtres simples souhaités. Par exemple, vous pouvez sélectionner la case à cocher Nom du journal d'événements, puis saisir "CA Access Control" pour rechercher les événements CA Access Control.
4. Cliquez sur l'onglet Filtres avancés (facultatif).

   La boîte de dialogue des filtres avancés s'affiche.
5. Créez les filtres avancés dont vous avez besoin.
6. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant de profil que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau profil apparaît dans la liste. Sinon, l'étape choisie s'affiche.

Informations complémentaires

Création d'un filtre d'événement simple (page 301)
Création d'un filtre d'événement avancé (page 303)
Utilisation des filtres avancés (page 301)

Création de filtres de balises

Vous pouvez créer des filtres de balises pour votre profil, afin de contrôler les requêtes ou les balises de catégories de rapport qui s'affichent dans l'interface CA Enterprise Log Manager lorsqu'un utilisateur applique le profil. Par exemple, si vous créez un filtre de balises pour CA SiteMinder, l'interface CA Enterprise Log Manager affiche uniquement les rapports et requêtes portant la balise CA SiteMinder.

Pour créer un filtre de balises

1. Ouvrez l'assistant de profil.
2. Saisissez le nom du profil, si cela n'a pas déjà été fait, puis passez à l'étape Filtres de balises.

   La boîte de dialogue Filtres s'ouvre sur le sous-onglet Filtres de balises de rapport.
3. Cliquez sur Nouveau filtre d'événement.

   La première ligne de la table des filtres de balises devient active.
4. Cliquez sur la cellule Balise et sélectionnez ou saisissez le nom de la balise de requête ou de rapport que vous souhaitez afficher. Si vous saisissez un nom, l'affichage propose les noms de balise disponibles au fur et à mesure de la frappe.
5. Cliquez une nouvelle fois sur Nouveau filtre d'événements pour ajouter des filtres supplémentaires (facultatif).

   La deuxième ligne de la table des filtres de balises devient active, affichant AND dans la colonne Logique.
6. Cliquez sur la cellule Logique pour sélectionner l'opérateur AND ou OR (facultatif).
7. Cliquez sur la cellule Balise et sélectionnez ou saisissez le nom de la balise que vous souhaitez afficher (facultatif). Si vous saisissez un nom, l'affichage propose les noms de balise disponibles au fur et à mesure de la frappe.
8. Cliquez sur les cellules des parenthèses d'ouverture et de fermeture et saisissez le nombre de parenthèses requis (facultatif).
9. Cliquez sur l'onglet Filtres de balises de requête, puis répétez les étapes 3 à 8 pour créer tous les filtres de balises de requête dont vous avez besoin (facultatif).
10. Cliquez sur Enregistrer après avoir saisi toutes les instructions de filtre souhaitées.

Informations complémentaires :

Création de filtres de données (page 254)

Importation d'un profil

Vous pouvez importer un profil, ce qui vous permet de déplacer des profils d'un environnement à un autre. Vous pouvez ainsi importer un profil créé dans un environnement de test dans votre environnement réel.

Pour importer un profil

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Profils pour le développer.

   Les boutons Profils apparaissent dans le volet Détails.

3. Cliquez sur Importer le profil.

   La boîte de dialogue d'importation de fichier s'affiche.

4. Recherchez le fichier que vous souhaitez importer et cliquez sur OK.

   L'assistant de profil apparaît et affiche les détails du profil sélectionné.

5. Effectuez les modifications souhaitées, puis cliquez sur Enregistrer et fermer. Si le profil importé porte le même nom qu'un profil déjà présent dans votre base de données de gestion, vous êtes invité à changer de nom.

   Le profil importé apparaît alors dans le dossier approprié.

Informations complémentaires

Exportation d'un profil (page 257)
Création d'un profil (page 252)

Exportation d'un profil

Vous pouvez exporter un profil. Cette opération vous permet de partager des profils entre plusieurs environnements. Vous pouvez ainsi exporter dans votre environnement réel un profil créé dans un environnement de test.

Pour exporter un profil

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Profils pour le développer.

   Les dossiers de profils s'affichent.

3. Cliquez sur le dossier contenant le profil que vous souhaitez exporter.

   Le dossier se développe et vous pouvez consulter les différents fichiers qu'il contient.

4. Sélectionnez le profil à exporter, puis cliquez sur Exporter le profil.

   Une boîte de dialogue vous permettant de sélectionner l'emplacement d'exportation s'ouvre.

5. Saisissez un chemin ou naviguez jusqu'à l'emplacement où vous souhaitez stocker le profil exporté, puis cliquez sur Enregistrer.

   Une boîte de dialogue vous confirmant l'exportation apparaît.

6. Cliquez sur OK.

   Le profil est exporté.

Informations complémentaires

Importation d'un profil (page 256)
Création d'un profil (page 252)

Configuration d'un profil

Vous pouvez sélectionner tout profil disponible à appliquer à votre environnement, en limitant les requêtes et les rapports disponibles, en fonction des termes du profil. Pour configurer un profil, sélectionnez-le dans le menu déroulant Profils, situé en haut de la fenêtre principale CA Enterprise Log Manager.

Création d'un filtre global

Vous pouvez créer un filtre global. Les filtres globaux vous permettent d'afficher toutes les requêtes et tous les rapports partageant les mêmes qualificateurs. Vous pouvez également utiliser l'interface de filtre global pour définir des paramètres de requête à l'échelle de l'application.

Pour créer un filtre global

1. Cliquez sur le bouton Filtres globaux en haut de la fenêtre principale.

   La boîte de dialogue Filtres et paramètres globaux apparaît en affichant l'onglet Filtres rapides.

2. Indiquez la période pendant laquelle votre filtre doit effectuer la recherche à l'aide du menu déroulant Période (facultatif).

3. Sélectionnez la case Correspondance pour saisir une valeur spécifique selon laquelle filtrer tous les événements bruts disponibles (facultatif).

   Remarque : Vous pouvez rechercher plusieurs valeurs, expressions ou valeurs partielles dans les événements bruts en utilisant la syntaxe de correspondance spécialisée.

4. Cliquez sur Ajouter un filtre pour spécifier les champs d'événement que vous souhaitez inclure dans le filtre.

   Le menu déroulant Colonne et le champ de saisie Valeur apparaissent.

5. Choisissez le champ d'événement que vous souhaitez inclure dans le filtre, puis saisissez la valeur que le champ doit contenir pour être affiché dans les rapports filtrés. Vous pouvez saisir plusieurs noms et valeurs de champs d'événement en cliquant à nouveau sur Ajouter un filtre. La sélection du bouton Exclure inclut toutes les valeurs *sauf* celle que vous avez saisie pour le nom de champ d'événement choisi.

   Remarque : Si vous créez un filtre global sur un champ de type chaîne, ce filtre est ajouté à la liste Filtres rapides. Si vous créez un filtre sur la base d'un champ numérique ou temporel (heure), il est ajouté à la liste Filtres avancés.

6. Cliquez sur l'onglet Filtres avancés pour ajouter des qualificateurs complexes supplémentaires (facultatif).

7. Cliquez sur l'onglet Paramètres pour choisir les paramètres globaux (facultatif). Ces paramètres sont appliqués à l'ensemble de l'application.

8. Sélectionnez Définir comme valeur par défaut en bas de la boîte de dialogue pour conserver les paramètres de filtre pour toutes vos sessions ultérieures, tant que vous restez connecté sous le même nom d'utilisateur (facultatif).

9. Cliquez sur Enregistrer.

   La boîte de dialogue Filtres et paramètres globaux se ferme et le nouveau filtre est appliqué aux rapports.

Informations complémentaires

Utilisation des filtres avancés (page 301)
Configuration de paramètres de requête globaux (page 259)

Configuration de paramètres de requête globaux

La boîte de dialogue Filtre global vous permet de définir des conditions à l'échelle de l'application qui s'appliquent à tous les rapports et toutes les requêtes de votre environnement. Les paramètres globaux s'appliquent jusqu'à la fin de la session en cours, à moins que vous ne les définissiez en tant que valeurs par défaut.

Pour configurer des paramètres de requête globaux

1. Cliquez sur le bouton Filtres globaux en haut de la fenêtre principale.

   La boîte de dialogue Filtres et paramètres globaux apparaît en affichant l'onglet Filtres rapides.

2. Cliquez sur l'onglet Paramètres.

   L'onglet s'ouvre sur les valeurs suivantes.

   Fuseau horaire local

   Contrôle le fuseau horaire pour tous les champs date/heure des rapports et requêtes. Vos rapports et requêtes adoptent le fuseau horaire que vous sélectionnez dans la liste déroulante, et non le fuseau horaire du serveur CA Enterprise Log Manager.

   Exécuter les requêtes sur les données fédérées

   Permet à la requête de s'appliquer sur tous les serveurs fédérés disponibles. Ce paramètre est activé par défaut. La désactivation de ce paramètre limite les requêtes aux seules données d'événement du magasin de journaux d'événements local. Cela vous permet de vérifier rapidement votre magasin de journaux d'événements local lorsque vous savez que vos événements cibles sont locaux.

   Activer l'actualisation automatique des requêtes

   Permet à l'affichage de s'actualiser automatiquement à l'intervalle défini pour chaque requête.

3. Sélectionnez Définir comme valeur par défaut en bas de la boîte de dialogue pour conserver les paramètres en tant que valeurs par défaut au-delà de la session en cours (facultatif).

4. Apportez les modifications nécessaires, puis cliquez sur Enregistrer.

   La boîte de dialogue Filtres et paramètres globaux se ferme et le nouveau filtre est appliqué.

Modification d'un filtre global

Vous pouvez modifier un filtre global existant.

Pour modifier un filtre global

1. Cliquez sur le bouton Filtres globaux en haut de la fenêtre principale.

   La boîte de dialogue Filtres et paramètres globaux apparaît en affichant l'onglet Filtres rapides.

2. Modifiez ou ajoutez des paramètres selon vos besoins. Vous pouvez supprimer un paramètre de filtre rapide individuel en cliquant sur l'icône Supprimer située en regard du paramètre.

3. Cliquez sur Enregistrer.

   La boîte de dialogue Filtres et paramètres globaux se ferme et le filtre modifié est appliqué.

Suppression d'un filtre global

Vous pouvez supprimer un filtre global, pour que tous les rapports reviennent à leur état par défaut.

Pour supprimer un filtre global, cliquez sur Effacer les filtres globaux en haut de la fenêtre CA Enterprise Log Manager principale : 

Création d'un filtre local

Vous pouvez créer un filtre local pour limiter le champ de la requête ou du rapport en cours d'affichage.

Pour créer un filtre local

1. Ouvrez la requête ou le rapport que vous souhaitez filtrer, puis cliquez sur le bouton Filtres locaux en haut du volet Détails.

   La boîte de dialogue Filtres locaux s'ouvre sur l'onglet Filtres rapides.

2. Sélectionnez la case Correspondance pour saisir une valeur spécifique selon laquelle rechercher tous les événements bruts disponibles (facultatif).

   Remarque : Vous pouvez rechercher plusieurs valeurs, expressions ou valeurs partielles dans les événements bruts en utilisant la syntaxe de correspondance spécialisée.

3. Cliquez sur Ajouter un filtre

4. Choisissez le champ d'événement que vous souhaitez inclure dans le filtre, puis saisissez la valeur que le champ doit contenir pour être affiché dans les rapports filtrés. Vous pouvez saisir plusieurs valeurs de colonne en cliquant à nouveau sur Ajouter un filtre. La sélection du bouton Exclure inclut toutes les valeurs *sauf* celle que vous avez saisie pour le nom de champ d'événement choisi.
5. Cliquez sur l'onglet Filtres avancés pour ajouter des qualificateurs supplémentaires (facultatif).
6. Cliquez sur Enregistrer.

   Le filtre est appliqué à l'affichage. Vous pouvez enregistrer la vue du rapport en la définissant en tant que favori.

Modification d'un filtre local

Vous pouvez modifier un filtre local existant.

Pour modifier un filtre local

1. Cliquez sur le bouton Filtres locaux en haut du volet de la requête ou du rapport.

   La boîte de dialogue Filtres locaux s'ouvre sur l'onglet Filtres rapides.
2. Modifiez ou ajoutez des valeurs selon vos besoins. Vous pouvez supprimer des paramètres de filtre individuels en cliquant sur l'icône Supprimer située en regard de chaque paramètre, ou supprimer la valeur de correspondance en décochant la case Correspondance.
3. Cliquez sur Enregistrer.

   Le filtre modifié est appliqué à l'affichage.

Suppression d'un filtre local

Vous pouvez supprimer un filtre local pour qu'une requête ou un rapport revienne à son état antérieur.

Pour supprimer un filtre local, cliquez sur le bouton Effacer le filtre local en haut de la requête ou du rapport actuellement affiché : 

Chapitre 9 : Requêtes et rapports

Ce chapitre traite des sujets suivants :

A propos des requêtes et des rapports

Vous pouvez utiliser les requêtes de différentes façons.

- Vous pouvez exécuter une requête pour afficher les données d'événement quasiment en temps réel.
- Vous pouvez sélectionner un rapport prédéfini pour afficher les résultats de plusieurs requêtes liées.
- Vous pouvez créer un rapport composé de requêtes que vous sélectionnez.
- Vous pouvez utiliser des requêtes d'invite pour rechercher des informations présélectionnées spécifiques.
- Vous pouvez planifier des requêtes à exécuter sur des données récentes sous forme d'alertes d'action, qui avertissent les parties responsables par courriel. Les alertes d'action sont également ajoutées à un flux RSS, qui peut être affiché à l'aide de lecteurs tiers.
- Vous pouvez créer vos propres requêtes pour afficher ou créer des alertes d'action, ou encore générer des rapports sur ces alertes.

Il existe deux types de requêtes et de rapports.

- Les requêtes et rapports *d'abonnement* sont prédéfinis par CA et fournis avec l'application CA Enterprise Log Manager lors de l'installation, ou ils sont ajoutés lors d'une mise à jour d'abonnement.
- Les requêtes et rapports *d'utilisateur* sont ceux créés par un utilisateur. Vous pouvez créer une requête ou un rapport de toutes pièces ou à partir d'une requête ou d'un rapport d'abonnement que vous souhaitez modifier.

CA Enterprise Log Manager propose une liste complète de requêtes et rapports par abonnement. Si un rôle Auditor, Analyst ou Administrator vous a été attribué, vous pouvez afficher l'ensemble des requêtes et rapports d'abonnement. Par ailleurs, vous pouvez effectuer les actions suivantes sur toute requête ou tout rapport d'abonnement en cours d'affichage.

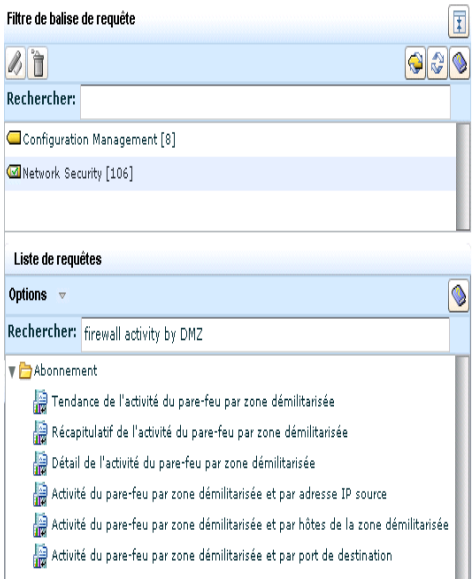
- Actualiser les données affichées
- Modifier les filtres locaux pour masquer les données que vous ne souhaitez pas afficher
- Effacer les filtres locaux pour réafficher la requête ou le rapport non filtré
- Ajouter la requête ou le rapport affiché à votre liste de favoris
- Imprimer la requête
- Changer l'option d'affichage de la requête ou du rapport sélectionné
- Fermer la requête ou le rapport affiché

Seuls les utilisateurs auxquels un rôle Analyst ou Administrator a été attribué peuvent effectuer les actions ci-dessous.

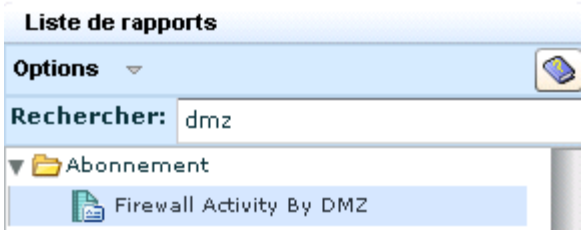
- Créer une nouvelle requête ou un nouveau rapport d'utilisateur de toutes pièces
- Copier une requête ou un rapport d'abonnement et l'utiliser en tant que base pour une requête ou un rapport d'utilisateur
- Modifier une requête ou un rapport d'utilisateur
- Exporter une requête ou un rapport d'utilisateur
- Supprimer une requête ou un rapport d'utilisateur
- Enregistrer les modifications apportées à la requête ou au rapport d'utilisateur sélectionné
- Importer une définition de requête ou de rapport d'utilisateur

Exemple de requêtes et de rapport lié

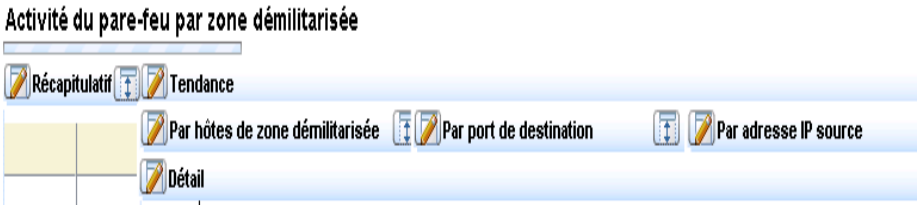
Prenons la balise de requête Activité du pare-feu par zone démilitarisée. Vous pouvez remarquer qu'elle est associée à six requêtes différentes.



Les requêtes contenues dans la liste des requêtes sont utilisées dans des rapports. Dans l'onglet Rapports, vous pouvez voir un rapport appelé Activité du pare-feu par zone démilitarisée.

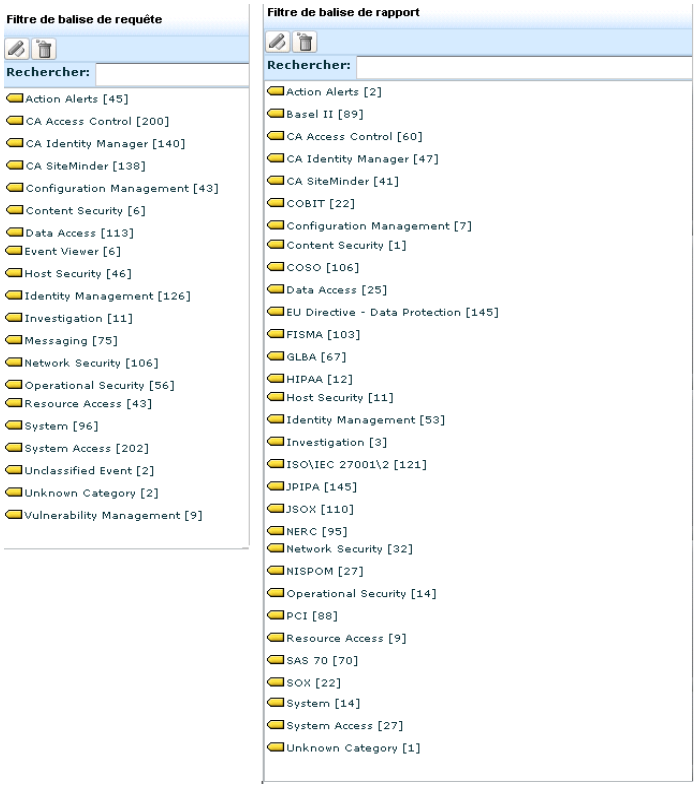


Seuls les noms apparaissent sur l'illustration suivante. Vous pouvez remarquer que chaque nom reflète l'une des six requêtes du rapport. La plupart des rapports incluent les résultats des trois types de requêtes suivants : récapitulatif, tendance et détail.

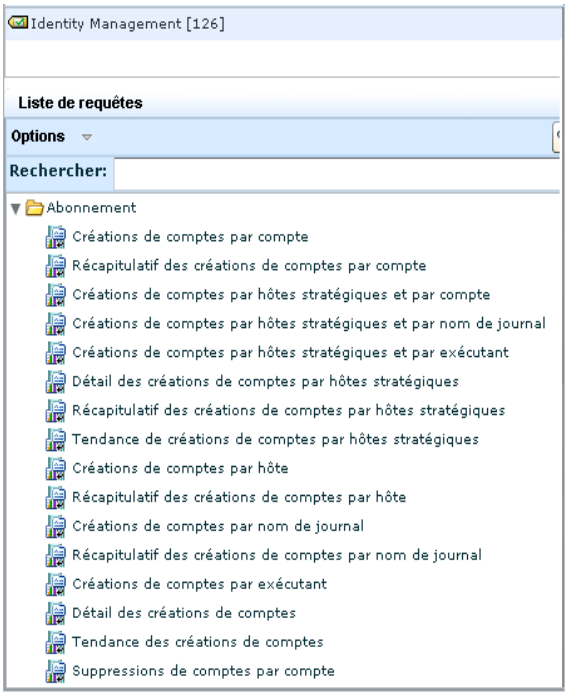


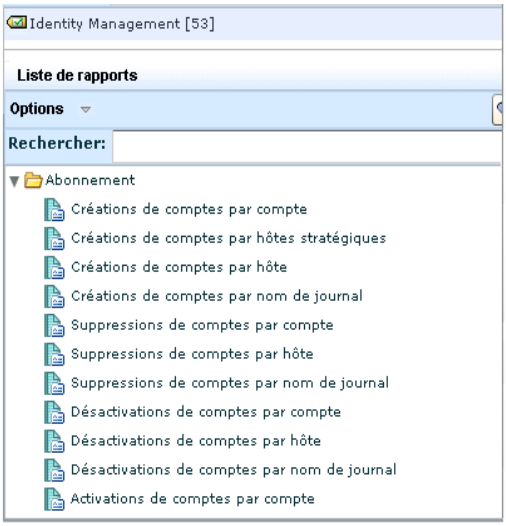
Balises de requêtes et de rapports

Pour sélectionner plus facilement les requêtes et rapports d'une catégorie particulière, vous pouvez cliquer sur leurs balises respectives afin de réduire la liste des éléments affichés. Les rapports et requêtes partagent un grand nombre de balises. Un même rapport ou requête peut également être associé à plusieurs balises.



Les balises de requêtes mappent vers un plus grand nombre de requêtes que les balises de rapports correspondantes, car les requêtes fournissent les informations réunies dans un rapport. Ainsi, lorsque vous rencontrez des résultats de rapports qui nécessitent un examen plus approfondi, vous pouvez procéder à une exploration descendante pour obtenir des détails ou des tendances au niveau de la requête.





Tâches liées aux balises

Les balises vous permettent de lier vos rapports et requêtes à des catégories pour un référencement facilité. Elles vous procurent un cadre organisationnel pour générer des rapports sur votre environnement. Les balises de catégories permettent également une division simple du travail par rôle ou par type d'événement.

Vous pouvez utiliser les balises prédéfinies ou créer vos balises personnalisées pour les rapports et requêtes. Par exemple, vous pouvez créer une balise "Mensuel" à ajouter à tout rapport que vous souhaitez planifier tous les mois pour un référencement et un affichage aisés. Vous pouvez ainsi ajouter ou supprimer des rapports à partir des jobs de rapport, sans modifier les jobs eux-mêmes, simplement en ajoutant la balise Mensuel à un nouveau job, ou en la supprimant d'un ancien job.

Vous pouvez ajouter des balises personnalisées à chaque requête ou rapport de votre choix dans le cadre du processus de création ou de modification. Une fois la nouvelle balise créée, son intitulé apparaît dans la liste des balises et vous pouvez la sélectionner pour l'ajouter à d'autres rapports ou requêtes.

Vous pouvez renommer ou supprimer des balises personnalisées. Vous pouvez supprimer des balises personnalisées des requêtes ou rapports qui les contiennent en modifiant la requête ou le rapport concerné.

Affichage d'une requête

Tous les utilisateurs auxquels un rôle Auditor, Analyst ou Administrator est attribué peuvent afficher toutes les requêtes. Les requêtes prédéfinies sont répertoriées dans le dossier Abonnement. Lorsque la première requête personnalisée est définie, un dossier Utilisateur est ajouté à la liste des requêtes pour conserver la requête personnalisée. Ensuite, toutes les requêtes personnalisées sont ajoutées à ce dossier Utilisateur.

Pour afficher une requête

1. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Requêtes.

   Le bouton d'agrandissement Filtre de balise de requête, la Liste de requêtes et le menu Options, ainsi qu'une zone de saisie Rechercher, apparaissent dans le volet gauche.

2. Sélectionnez la requête à afficher de l'une des manières répertoriées ci-dessous.
   - Faites défiler la liste des requêtes et sélectionnez une requête à afficher.
   - Entrez un mot clé dans la zone Rechercher, pour afficher uniquement les requêtes dont le nom contient ce mot.
   - Cliquez sur le bouton d'agrandissement pour afficher la liste Filtre de balise de requête. Sélectionnez une des balises ou saisissez un mot clé dans la zone de recherche de balise pour limiter le nombre de balises affichées. Sélectionnez une balise pour afficher les requêtes liées. Sélectionnez la requête à afficher.
   - Si vous recherchez une requête personnalisée, réduisez le dossier Abonnement, développez le dossier Utilisateur, puis faites défiler la liste du dossier Utilisateur.

   La requête sélectionnée s'affiche dans le volet principal de la page.
3. Effectuez l'une des actions répertoriées ci-dessous (facultatif).
   - Cliquez sur Modifier les filtres locaux pour définir les filtres de manière à afficher uniquement les données souhaitées. Pour restaurer l'affichage d'origine des requêtes, cliquez sur Effacer les filtres locaux.
   - Cliquez sur Ajouter aux favoris pour ajouter la requête ou le rapport affiché à votre liste de favoris.
   - Cliquez sur Actualiser pour voir apparaître les données qui ont été dernièrement ajoutées.
   - Cliquez sur Imprimer pour imprimer la requête.
4. Cliquez sur Fermer pour fermer la requête affichée.

Affichage d'un rapport

Tous les utilisateurs auxquels un rôle Auditor, Analyst ou Administrator est attribué peuvent afficher tous les rapports. Les rapports prédéfinis sont répertoriés dans le dossier Abonnement. Lorsque le premier rapport personnalisé est défini, un dossier Utilisateur est ajouté à la liste des rapports pour conserver le rapport personnalisé. Ensuite, tous les rapports personnalisés sont ajoutés à ce dossier Utilisateur.

La sélection d'un rapport dans la liste des rapports exécute les requêtes le composant sur les enregistrements de journaux qui se trouvent actuellement dans les magasins de journaux d'événements internes. Les résultats de rapports, affichés dans le volet droit, proviennent des magasins de journaux d'événements du serveur CA Enterprise Log Manager actif et de ses serveurs enfants.

Pour afficher un rapport

1. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Rapports.

   Le bouton d'agrandissement Filtre de balise de rapport, un champ de saisie Rechercher, la Liste de rapports et le menu Options apparaissent dans le volet gauche.

2. Dans le menu Options, sélectionnez Afficher le rapport sélectionné, si ce n'est pas déjà fait.

   Ceci vous permet d'afficher tout rapport sélectionné dans le volet droit.

3. Sélectionnez le rapport à afficher de l'une des manières répertoriées ci-dessous.

   - Faites défiler la liste des rapports et sélectionnez un rapport à afficher.
   - Entrez un mot clé dans le champ de saisie Rechercher et sélectionnez un rapport à afficher à partir de la liste filtrée.
   - Cliquez sur le bouton d'agrandissement pour afficher la liste Filtre de balise de rapport. Sélectionnez une des balises ou saisissez un mot clé dans la zone de recherche de balise pour limiter le nombre de balises affichées. Sélectionnez une balise pour afficher les rapports liés. Sélectionnez le rapport à afficher.
   - Si vous recherchez un rapport personnalisé, réduisez le dossier Abonnement, développez le dossier Utilisateur, puis faites défiler la liste du dossier Utilisateur.

   Le rapport sélectionné s'affiche dans le volet principal de la page.

4. Effectuez l'une des actions répertoriées ci-dessous (facultatif).
   - Cliquez sur Modifier les filtres locaux pour définir les filtres de manière à afficher uniquement les données souhaitées. Pour restaurer l'affichage d'origine des rapports, cliquez sur Effacer les filtres locaux.
   - Cliquez sur Ajouter aux favoris pour ajouter le rapport affiché à votre liste de favoris.
   - Cliquez sur Actualiser pour voir apparaître les données qui ont été dernièrement ajoutées.
   - Cliquez sur Imprimer pour imprimer le rapport.
5. Cliquez sur Fermer pour fermer le rapport affiché.

Désactivation de l'option Afficher le rapport sélectionné

Vous pouvez paramétrer votre liste de rapports de manière à effectuer des modifications sans charger les rapports. Normalement, la sélection d'un rapport dans la liste entraîne son affichage dans la fenêtre Détails.

La désactivation de ce mode par défaut vous fait gagner du temps en vous permettant de sélectionner un rapport dans la liste et de le modifier immédiatement, sans attendre qu'il s'affiche. Une fonction d'autant plus utile si vous devez modifier plusieurs rapports et que vous savez déjà quels changements y apporter.

Etant donné que seuls les utilisateurs avec le rôle Administrator ou Analyst peuvent créer ou modifier des rapports, seuls ces utilisateurs peuvent désactiver le paramètre Afficher le rapport sélectionné.

Pour désactiver l'option Afficher le rapport sélectionné

1. Cliquez sur Options en haut de la Liste de rapports.

   Le menu Options s'affiche.
2. Désélectionnez la case en regard de l'option Afficher le rapport sélectionné.

   Le rapport sélectionné dans la liste ne s'affiche pas tant que l'option Afficher le rapport sélectionné n'est pas réactivée.

Informations complémentaires

Création d'un rapport (page 313)
Modification d'un rapport (page 325)

Exemple : Exécution de rapports PCI

Le PCI Security Standards Council (conseil de normalisation en matière de sécurité) est un forum international ouvert, chargé de mettre au point la norme PCI DSS (Payment Card Industry Data Security Standard, norme de sécurité des données liées à l'industrie des cartes bancaires) incluant des consignes relatives aux procédures, aux stratégies et à la gestion des données. Les organisations chargées de stocker, de traiter ou de transférer les données des titulaires de carte doivent se conformer à la norme PCI DSS, version 1.2, qui comporte douze exigences.

CA Enterprise Log Manager fournit des rapports PCI prêts à l'emploi, que vous pouvez afficher dès que votre système commence à récupérer et traiter les journaux d'événements.

Les exemples présentés dans cette section vous aideront à vous familiariser avec les rapports PCI, ainsi qu'avec leur planification et leur diffusion. Ils font notamment référence aux exigences PCI DDS concernées par le rapport, ainsi qu'à leur numéro.

Informations complémentaires :

Affichage de la Liste des rapports avec la balise PCI (page 273)
Recherche de rapports pour une commande PCI DDS spécifique (page 274)
Utilisation d'un rapport PCI unique (page 277)

Affichage de la Liste des rapports avec la balise PCI

Afin de vous familiariser avec l'utilisation des rapports CA Enterprise Log Manager et de vérifier la conformité PCI, commencez par afficher la liste des rapports prédéfinis associés à la balise PCI.

Pour vous familiariser avec les rapports associés à la balise PCI

1. Cliquez sur l'onglet Requêtes et rapports et sur le sous-onglet Rapports.

   Les fenêtres Liste de rapports et Filtre de balise de rapport s'affichent.

2. Saisissez "PCI" dans le champ Rechercher, pour la balise.

   La balise PCI apparaît.

3. Passez en revue la liste de rapports associées à la balise PCI.

Recherche de rapports pour une commande PCI DDS spécifique

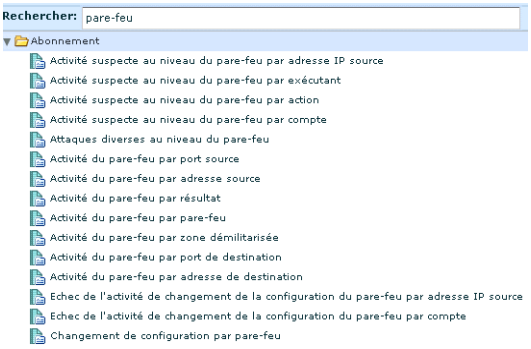
Vous pouvez rechercher des rapports prédéfinis à l'aide de mots-clés relatifs à des commandes PCI DDS spécifiques. La procédure suivante couvre plusieurs exemples.

Remarque : Les numéros indiqués correspondent aux exigences PCI DDS visées par le rapport.

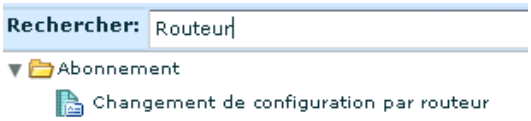
Pour afficher la liste des rapports relatifs aux commandes PCI DDS souhaitées

1. Cliquez sur l'onglet Requêtes et rapports et sur le sous-onglet Rapports.
2. Pour localiser le rapport traitant des modifications de configuration du pare-feu (1.1.1), saisissez "pare-feu" comme critère de recherche.

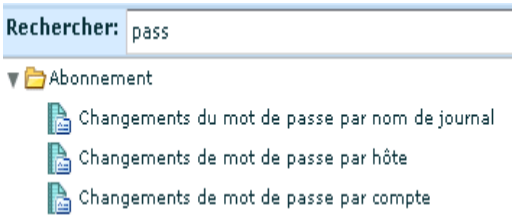
   Une liste de rapports similaire à celle illustrée ci-dessous s'affiche. Notez que l'un de ces rapports est intitulé "Changements de la configuration du pare-feu".



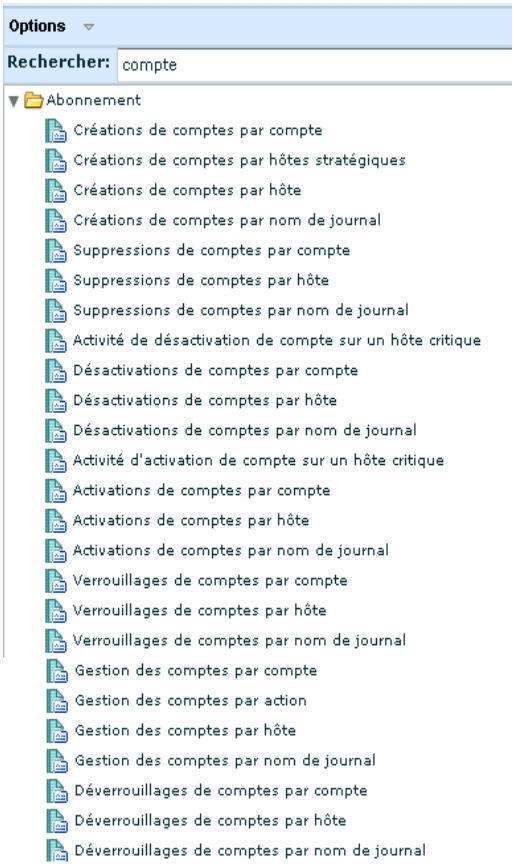
3. Pour localiser le rapport traitant des modifications de configuration du routeur, appliquées après vérification de la synchronisation (1.3.6), saisissez "routeur" comme critère de recherche.



4. Pour localiser les rapports traitant de la gestion des mots de passe (8.5), une des mesures de contrôle d'accès les plus puissantes, saisissez "mot de passe" comme critère de recherche.



5. Pour localiser les rapports traitant de l'ajout, de la modification et de la suppression des comptes d'utilisateur (12.5.4), une des mesures d'application de la stratégie de sécurité des données, saisissez "compte" comme critère de recherche.



Utilisation d'un rapport PCI unique

Vous pouvez utiliser n'importe quel rapport, y compris un rapport PCI, de la manière suivante.

- Afficher le rapport en sélectionnant son nom dans la Liste des rapports
- Imprimer le rapport
- Planifier le rapport, avec la possibilité de l'envoyer par courriel aux destinataires souhaités
- Afficher le job de rapport planifié
- Afficher le rapport généré

Pour afficher ou agir sur le rapport sélectionné

1. Cliquez sur l'onglet Requêtes et rapports et sur le sous-onglet Rapports.
2. Sélectionnez l'option Afficher le rapport sélectionné dans la liste déroulante Options de la fenêtre Liste des rapports, si cela n'est pas déjà fait.
3. Sélectionnez un nom de rapport dans la liste des rapports.

   Le rapport ainsi obtenu contient les résultats des requêtes sous-jacentes, qui incluent généralement un récapitulatif, la tendance et les détails, ainsi que les requêtes spécifiques au rapport.
4. Pour désactiver le chargement de requêtes particulières, sélectionnez Annuler.

5. Pour imprimer le rapport affiché, cliquez sur Imprimer le rapport, dans le volet droit.

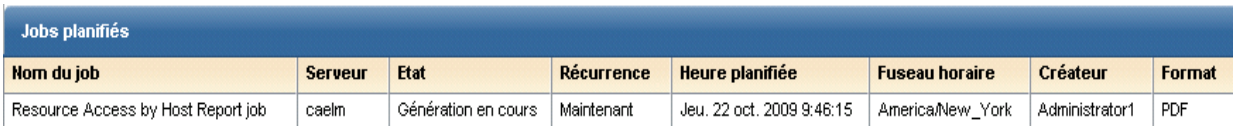
   Dans la boîte de dialogue Impression qui s'affiche, sélectionnez une imprimante, puis cliquez sur Imprimer.
6. Pour planifier un rapport que vous souhaitez générer ultérieurement pour affichage, cliquez sur Planifier un rapport.

   L'assistant de planification de rapport s'ouvre, le rapport souhaité affiché dans la zone Rapports sélectionnés.
7. Saisissez un nom de job, par exemple "Accès aux ressources par rapport hôte".

   Si vous acceptez tous les paramètres par défaut, l'exécution du job est immédiate, sans récurrence ; le rapport est généré au format PDF sans notification par courriel. Les données sont extraites du serveur actuel, ainsi que de ses pairs et descendants fédérés.
8. Cliquez sur Enregistrer et fermer.

9. Affichez le job planifié. Sélectionnez l'onglet Rapports planifiés, puis le sous-onglet Planification de rapport.

   Le job que vous venez de planifier s'affiche.



Jobs planifiés

Nom du job	Serveur	Etat	Récurrence	Heure planifiée	Fuseau horaire	Créateur	Format
Resource Access by Host Report job	caelm	Génération en cours	Maintenant	Jeu. 22 oct. 2009 9:46:15	America/New_York	Administrator1	PDF

10. Afficher le rapport généré

    a. Sélectionnez l'onglet Rapports planifiés, puis le sous-onglet Rapports générés.

    b. Limitez le nombre de lignes affichées en sélectionnant une récurrence autre que Tout, un format autre que Tout ou un intervalle de temps de dernière heure (facultatif).

    c. Cliquez sur Actualiser (facultatif).

11. Après avoir passé en revue le rapport généré, vous pouvez modifier le job du rapport si vous souhaitez le générer de manière récurrente. Procédez comme suit.

    a. Dans le sous-onglet Planification de rapport, sélectionnez le rapport généré et cliquez sur Modifier.

    b. Sélectionnez l'étape Planifier des jobs, puis l'option de fréquence d'occurrence.

    c. Cliquez sur Enregistrer et fermer.

Invites

Une invite est un type de requête spécial qui affiche des résultats en fonction de la valeur que vous saisissez et des champs CEG que vous sélectionnez. Les lignes sont uniquement renvoyées pour les événements dont la valeur saisie apparaît dans au moins un des champs CEG sélectionnés.

Vous pouvez effectuer l'une des actions suivantes sur des résultats de requêtes d'invite.

- Sélectionnez Afficher les événements bruts pour remplacer l'affichage des événements affinés par l'événement brut correspondant et l'heure à laquelle il s'est produit.
- Saisissez une chaîne dans le champ Correspondance et sélectionnez OK pour filtrer l'affichage des lignes contenant des données qui correspondent à votre saisie.
- Sélectionnez une option d'exportation des données de la requête pour exporter les résultats de la requête vers un document PDF, une feuille de calcul Excel ou un fichier XML.
- Sélectionnez Conditions de résultat pour filtrer l'affichage en fonction d'une plage de dates spécifique, définir la limite des lignes renvoyées ou modifier la granularité de l'heure affichée. Sinon, réinitialisez les conditions de résultat sur les valeurs par défaut.
- Sélectionnez Afficher/Modifier le filtre local pour spécifier les filtres rapides ou les filtres avancés.
- Imprimez la requête sur une imprimante locale sélectionnée.
- Actualisez manuellement les données de la requête ou sélectionnez Actualisation automatique.

Utilisation de l'invite du connecteur

Chaque connecteur configuré sur un agent collecte des événements bruts à partir d'une source d'événements spécifique et envoie les événements au magasin de journaux d'événements situé sur un serveur de collecte CA Enterprise Log Manager. Le processus d'affinement des événements convertit les événements bruts en événements affinés, puis les archive dans le serveur CA Enterprise Log Manager de génération de rapports. L'invite du connecteur lance une requête pour les événements se trouvant sur le serveur de génération de rapports qui ont été collectés comme des événements bruts par les connecteurs portant le nom que vous spécifiez. Les connecteurs peuvent avoir un nom par défaut ou un nom défini par l'utilisateur. Vous copiez le nom du connecteur à utiliser, puis vous le collez dans le champ de l'invite du connecteur. Ensuite, cliquez sur OK pour afficher les résultats de la requête de l'invite.

Utilisez l'invite du connecteur pour :

- Afficher des événements provenant de tous les connecteurs basés sur la même intégration. Cela est possible si vous acceptez le nom de connecteur par défaut lors du déploiement des connecteurs.
- Vérifiez qu'un nouveau connecteur est capable de récupérer des événements. Si plusieurs agents possèdent des connecteurs ayant le nom que vous spécifiez, saisissez le nom de l'agent dans le champ Correspondance afin de limiter les résultats de la requête aux événements récupérés par le nouveau connecteur.

Pour copier le nom d'un connecteur actif :

1. Cliquez sur l'onglet Administration.

   L'explorateur de collecte de journaux s'affiche.

2. Cliquez sur Explorateur d'agent.

   Le Contrôleur de l'état des agents s'affiche, l'une des colonnes indiquant les noms des connecteurs.

3. Cliquez avec le bouton droit sur le connecteur que vous voulez utiliser dans la requête d'invite, puis sélectionnez Copier le nom du connecteur.

Pour utiliser l'invite du connecteur :

1. Cliquez sur Requêtes et rapports.

   La liste de requêtes affiche le dossier Invites, le dossier Abonnement et probablement un dossier Utilisateurs.

2. Développez Invites et sélectionnez Connecteur.

   L'invite Connecteur affiche le champ Connecteur et le champ CEG suivant, qui doit rester sélectionné pour que l'invite fonctionne :

   agent_connector_name

   Représente le nom d'un connecteur.

3. Cliquez avec le bouton droit sur le champ Connecteur et sélectionnez Coller.

   Le nom du connecteur copié depuis le Contrôleur de l'état des agents s'affiche dans le champ Connecteur.

4. Cliquez sur OK.

   Les résultats de la requête de l'invite du connecteur s'affichent.

5. Utilisez les descriptions suivantes pour interpréter les résultats de la requête :

   Sévérité CA

   Indique la sévérité de l'événement, dans laquelle les valeurs dans l'ordre croissant de la sévérité incluent les éléments suivants : informations, avertissement, impact mineur, impact majeur, critique et irrécupérable.

   Date

   Date à laquelle l'événement a eu lieu.

   Catégorie

   Identifie la catégorie de niveau supérieur de l'action d'événement correspondante. Par exemple, Accès au système est la catégorie de l'action d'authentification.

   Action

   Identifie l'action, dans laquelle des actions possibles sont déterminées par la classe de l'événement.

   Nom de l'agent

   Identifie l'agent sur lequel le connecteur s'exécute.

   Hôte

   Identifie l'hôte de la source d'événements à partir de laquelle le connecteur collecte les événements.

Exécutant

Identifie l'acteur à l'origine de l'événement, c'est-à-dire, l'identité qui a initié l'action. L'exécutant peut porter le nom d'utilisateur source ou le nom du processus source.

Compte

Identifie le nom d'utilisateur du compte utilisé pour l'authentification quand le connecteur tente de se connecter à l'hôte à l'aide de la source d'événements dans laquelle les événements bruts sont collectés. Il s'agit en général d'un compte ayant peu de privilèges. Les informations de connexion pour ce compte sont configurés sur la source d'événements, ainsi que sur le détecteur de journaux du connecteur.

Résultat

Spécifie un code pour le résultat d'événement de l'action correspondante, où S signifie Réussi, E signifie échec, A signifie Accepté, D signifie Ignoré, R signifie Rejeté et U signifie Inconnu.

Nom du connecteur

Nom du connecteur saisi dans le champ du filtre de l'invite.

6. (Facultatif) Sélectionnez Afficher les événements bruts.

Le premier événement collecté par un nouveau connecteur concerne l'action de démarrage du système et se termine par : result_string=<nom du connecteur> Connector Started Successfully

Utilisation de l'invite Hôte

Les requêtes de l'invite Hôte pour les événements dont le nom d'hôte a été spécifié apparaissent dans les champs CEG sélectionnés de l'événement ajusté. Quand des données relatives à un événement brut sont ajustées, les détails de l'événement peuvent inclure plusieurs noms d'hôte CEG différents. Envisagez ce scénario :

1. L'initiateur d'événements sur source_hostname tente une action, event_action, sur une cible se trouvant sur dest_hostname.

   Remarque : Source_hostname et dest_hostname peuvent être des hôtes différents ou le même hôte.

2. Cet événement est enregistré dans un référentiel sur event_source_hostname.

   Remarque : Event_source_name peut être un hôte différent de source_hostname ou de dest_hostname ou être colocalisé.

3. Un agent CA Enterprise Log Manager installé sur agent_hostname effectue une copie de l'événement enregistré sur event_source_hostname.

   Remarque : Agent_hostname est identique à event_source_name dans la collecte de journaux de l'agent, mais il diffère dans une collecte de journaux directe et sans agent.

4. L'agent CA Enterprise Log Manager sur agent_hostname transmet la copie de l'événement situé dans event_logname à un serveur de collecte CA Enterprise Log Manager.

Pour utiliser l'invite Hôte, procédez comme suit :

1. Cliquez sur Requêtes et rapports.

   Cette liste de requêtes affiche le dossier Invites, ainsi qu'un ou plusieurs dossiers pour les autres requêtes.

2. Développez le dossier Invites et sélectionnez Hôte.

   L'invite Hôte s'affiche.

3. Saisissez le nom de l'hôte sur lequel cette requête sera fondée.

4. Sélectionnez les champs sur lesquels fonder la requête de données qui correspond à votre saisie du nom d'hôte.

   source_hostname

   Représente le nom de l'hôte qui a initié l'action.

   dest_hostname

   Représente le nom d'un hôte qui est la destination ou la cible de l'action.

event_source_hostname

Représente le nom d'un hôte qui enregistre l'événement quand celui-ci se produit.

Par exemple, vous pouvez déployer un connecteur basé sur WinRM pour collecter des événements à partir de la Visionneuse d'événements sur un hôte Windows Server 2008. Pour sélectionner des événements récupérés à partir d'un certain hôte Windows Server 2008, saisissez le nom d'hôte de ce serveur et sélectionnez ce champ.

receiver_hostname

Est identique à agent_hostname.

agent_hostname

Représente le nom de l'hôte dans lequel un agent CA Enterprise Log Manager a été déployé.

5. Cliquez sur OK.

   Les résultats de la requête de l'invite Hôte s'affichent.

6. Utilisez les descriptions suivantes pour interpréter les résultats de la requête :

   Sévérité CA

   Indique la sévérité de l'événement, dans laquelle les valeurs dans l'ordre croissant de la sévérité incluent les éléments suivants : informations, avertissement, impact mineur, impact majeur, critique et irrécupérable.

   Date

   Date à laquelle l'événement a eu lieu.

   Utilisateur de la source

   Identifie le nom de l'utilisateur sur source_hostname qui a initié l'action d'événement.

   Résultat

   Spécifie un code pour le résultat d'événement de l'action correspondante, où S signifie Réussi, E signifie échec, A signifie Accepté, D signifie Ignoré, R signifie Rejeté et U signifie Inconnu.

   Hôte de l'agent

   Identifie le nom de l'hôte dans lequel l'agent CA Enterprise Log Manager qui a collecté l'événement est installé.

   Hôte du récepteur

   Identique à l'hôte de l'agent.

Catégorie

Identifie la catégorie de niveau supérieur de l'action d'événement correspondante. Par exemple, Accès au système est la catégorie de l'action d'authentification.

Action

Identifie l'action d'événement effectuée par l'utilisateur de la source.

Nom du journal

Identifie le nom du journal utilisé par le connecteur qui a collecté l'événement. Tous les connecteurs basés sur la même intégration transmettent les événements dans un fichier journal portant le même nom de journal.

Utilisation de l'invite IP

Les requêtes de l'invite IP pour les événements dont l'adresse IP a été spécifiée apparaissent dans les champs CEG sélectionnés de l'événement ajusté. Quand des données relatives à un événement brut sont ajustées, les détails de l'événement peuvent inclure plusieurs adresses IP CEG différentes. Envisagez ce scénario :

1. L'initiateur d'événements sur source_address tente une action, event_action, sur une cible se trouvant sur dest_hostname.

   Remarque : Source_address et dest_address peuvent être identiques ou différents.

2. Cet événement est enregistré dans un référentiel sur event_source_address.

   Remarque : Event_source_address peut être différent de source_address ou de dest_address ou être identique à un seul ou aux deux.

3. Un agent CA Enterprise Log Manager installé sur agent_address effectue une copie de l'événement enregistré sur event_source_address.

   Remarque : Agent_address est identique à event_source_address dans la collecte de journaux de l'agent, mais il diffère dans une collecte de journaux directe et sans agent.

4. L'agent sur agent_address transmet la copie de l'événement situé dans event_logname à un serveur de collecte CA Enterprise Log Manager.

Pour utiliser l'invite IP, procédez comme suit :

1. Cliquez sur Requêtes et rapports.

   Cette liste de requêtes affiche le dossier Invites, ainsi qu'un ou plusieurs dossiers pour les autres requêtes.

2. Développez le dossier Invites et sélectionnez Hôte.

   L'invite IP s'affiche.

3. Saisissez l'adresse IP sur laquelle fonder cette requête.

4. Sélectionnez un ou plusieurs champs suivants pour lancer une requête concernant les données correspondant à votre saisie d'adresse IP.

   source_address

   Représente l'adresse IP de l'hôte via laquelle l'action a été initiée.

   dest_address

   Représente l'adresse IP d'un hôte qui est la destination ou la cible de l'action.

   event_source_address

   Représente l'adresse IP d'un hôte qui enregistre l'événement quand celui-ci se produit.

   Par exemple, vous pouvez déployer un connecteur basé sur WinRM pour collecter des événements à partir de la Visionneuse d'événements sur un hôte Windows Server 2008. Pour sélectionner des événements récupérés à partir d'un certain hôte Windows Server 2008, saisissez l'adresse IP de ce serveur et sélectionnez ce champ.

   receiver_hostaddress

   Est identique à agent_address.

   agent_address

   Représente l'adresse IP d'un hôte dans lequel un agent CA Enterprise Log Manager a été déployé.

5. Cliquez sur OK.

   Les résultats de la requête de l'invite IP s'affichent.

6. Utilisez les descriptions suivantes pour interpréter les résultats de la requête :

Sévérité CA

Indique la sévérité de l'événement, dans laquelle les valeurs dans l'ordre croissant de la sévérité incluent les éléments suivants : informations, avertissement, impact mineur, impact majeur, critique et irrécupérable.

Date

Date à laquelle l'événement a eu lieu.

Résultat

Fournit un code pour le résultat de l'action correspondante. La lettre affichée a la signification suivante : S pour Réussi, E pour échec, A pour Accepté, D pour Ignoré, R pour Rejeté et U pour Inconnu.

Port de destination

Identifie le port de communication sur l'hôte de destination, la cible de l'action d'événement.

IP source

Identifie l'adresse IP à partir de laquelle l'action d'événement a été initiée.

IP de destination

Identifie l'adresse IP de l'hôte qui était la cible de l'action d'événement.

Adresse IP source de l'événement

Identifie l'adresse IP de l'hôte avec le référentiel où l'événement a été enregistré à l'origine.

Adresse IP de l'agent

Identifie le nom de l'hôte avec l'agent CA Enterprise Log Manager responsable de la collecte des événements à partir de la source d'événement.

Adresse IP du récepteur

Identique à l'adresse IP de l'agent.

Catégorie

Identifie la catégorie de niveau supérieur de l'action d'événement correspondante. Par exemple, Accès au système est la catégorie de l'action d'authentification.

Action

Identifie l'action d'événement.

Nom du journal

Identifie le nom du journal utilisé par le connecteur qui a collecté l'événement

Utilisation de l'invite Nom du journal

Chaque connecteur basé sur la même intégration renvoie des journaux d'événements collectés à partir de la source d'événements vers le serveur de collecte CA Enterprise Log Manager dans un fichier journal muni d'un nom prédéfini. L'invite Nom du journal lance une requête pour les événements concernant le nom de journal que vous spécifiez.

Utilisez l'invite Nom du journal pour lancer une requête concernant les événements transférés dans un fichier journal muni du nom spécifié. Chaque connecteur est fondé sur une intégration. Chaque intégration utilise un nom de journal prédéfini. Une requête pour un nom de journal donné renvoie des résultats d'événements collectés par des agents différents, qui utilisent des connecteurs basés sur la même intégration ou sur des intégrations similaires.

Plusieurs conventions sont utilisées pour nommer les journaux :

- Nom de l'intégration. CA Federation est le nom de journal de l'intégration CA_Federation_Manager.
- Nom du produit. McAfee Vulnerability Manager est le nom de journal pour McAfee_VM et McAfee_VM_CM. MS AD Rights Management Services est le nom de journal pour Microsoft_Active_Directory_RMS et Microsoft_Active_Directory_RMS_ODBC.
- Nom de l'éditeur : Oracle est le nom de journal pour Oracl10g, Oracle9i, Oracle_AppLog et Oracle_Syslog.
- Type de journal : Unix est le nom de journal pour les intégrations suivantes : AIX_Syslog, HPUX_Syslog, Linux_Syslog, SLES_Syslog et Solaris_Syslog.

Certains noms de journal sont réutilisés à mesure que de nouvelles versions ou plateformes sont ajoutées. Par exemple, NT-Security est le nom de journal des journaux de sécurité pour les intégrations suivantes : NTEventLog, Windows2k8 et WinRM.

Pour utiliser l'invite Nom du journal, procédez comme suit :

1. Cliquez sur Requêtes et rapports.

   Cette liste de requêtes affiche le dossier Invites, ainsi qu'un ou plusieurs dossiers pour les autres requêtes.

2. Développez le dossier Invites et sélectionnez Nom du journal.

   Le filtre de l'invite Nom du journal affiche le champ suivant :

   event_logname

   Représente le nom d'un fichier journal associé à une intégration spécifique.

3. Sélectionnez le nom du journal utilisé pour transmettre des événements que vous voulez afficher, puis cliquez sur OK.

   Les résultats de la requête de l'invite du nom de journal s'affichent.

4. Utilisez les descriptions suivantes pour interpréter les résultats de la requête :

   Sévérité CA

   Indique la sévérité de l'événement, dans laquelle les valeurs dans l'ordre croissant de la sévérité incluent les éléments suivants : informations, avertissement, impact mineur, impact majeur, critique et irrécupérable.

   Date

   Date à laquelle l'événement a eu lieu.

   Catégorie

   Identifie la catégorie de niveau supérieur de l'action d'événement correspondante. Par exemple, Accès au système est la catégorie de l'action d'authentification.

   Action

   Identifie l'action d'événement effectuée par l'exécutant correspondant.

   Hôte

   Identifie l'hôte de la source d'événements à partir de laquelle le connecteur collecte les événements.

   Exécutant

   Identifie l'acteur à l'origine de l'événement, c'est-à-dire, l'identité qui a initié l'action. L'exécutant peut porter le nom d'utilisateur source ou le nom du processus source.

Compte

Identifie le nom d'utilisateur du compte utilisé pour l'authentification. Quand le connecteur tente de se connecter à la source d'événement, une authentification se produit. En général, l'authentification utilise un compte ayant peu de privilèges. Pendant le déploiement du connecteur, l'administrateur configure les informations de connexion de ce compte sur la source de l'événement, puis identifie ce compte sur le détecteur de journaux.

Résultat

Spécifie un code pour le résultat d'événement de l'action correspondante, où S signifie Réussi, E signifie échec, A signifie Accepté, D signifie Ignoré, R signifie Rejeté et U signifie Inconnu.

Nom du journal

Nom du journal saisi dans le champ du filtre de l'invite.

Utilisation de l'invite Port

Les requêtes de l'invite Hôte pour les événements dont le nom d'hôte a été spécifié apparaissent dans les champs CEG sélectionnés de l'événement ajusté. Quand des données relatives à un événement brut sont ajustées, les détails de l'événement peuvent inclure plusieurs numéros de port CEG différents. Envisagez ce scénario :

1. L'initiateur d'événement sur l'hôte source utilise le port de communications sortantes source_port pour initialiser l'action d'événement sur une cible se trouvant sur un hôte de destination via le port de communications entrantes dest_port.

   Remarque : Source_port et dest_port sont identiques pour les événements locaux. Sinon, ils sont spécifiques à l'hôte.

2. Cet événement est enregistré dans un référentiel de la source d'événement.
3. Un agent CA Enterprise Log Manager effectue une copie de l'événement enregistré sur la source d'événement.
4. L'agent transmet la copie de l'événement via le port sortant, receiver_port, à un serveur de collecte CA Enterprise Log Manager.

   Remarque : L'agent utilise le port 17001, par défaut, pour sécuriser les communications vers le serveur de collecte CA Enterprise Log Manager.

Pour utiliser l'invite Port, procédez comme suit :

1. Cliquez sur Requêtes et rapports.

   Cette liste de requêtes affiche le dossier Invites, ainsi qu'un ou plusieurs dossiers pour les autres requêtes.

2. Développez le dossier Invites et sélectionnez Port.

   L'invite Port s'affiche.

3. Saisissez le numéro du port sur lequel cette requête sera fondée.

4. Sélectionnez les champs sur lesquels fonder la requête de données correspondant à votre saisie du numéro de port.

   source_port

   Représente le port de communications utilisé pour initier l'action.

   dest_port

   Représente le port de communication sur l'hôte de destination qui est la cible de l'action.

   receiver_port

   Représente le port que l'agent utilise pour communiquer avec le serveur de collecte CA Enterprise Log Manager.

5. Cliquez sur OK.

   Les résultats de la requête de l'invite Port s'affichent.

6. Utilisez les descriptions suivantes pour interpréter les résultats de la requête :

   Sévérité CA

   Indique la sévérité de l'événement, dans laquelle les valeurs dans l'ordre croissant de la sévérité incluent les éléments suivants : informations, avertissement, impact mineur, impact majeur, critique et irrécupérable.

   Date

   Date à laquelle l'événement a eu lieu.

   IP source

   Identifie l'adresse IP de l'hôte à partir de laquelle l'action d'événement a été initiée.

   Résultat

   Spécifie un code pour le résultat d'événement de l'action correspondante, où S signifie Réussi, E signifie échec, A signifie Accepté, D signifie Ignoré, R signifie Rejeté et U signifie Inconnu.

Port source

Identifie le port sortant utilisé pour initier l'action.

Port de destination

Identifie le port entrant sur l'hôte de destination.

Hôte du récepteur

Identifie le port sortant sur l'agent utilisé pour envoyer des journaux d'événements au serveur CA Enterprise Log Manager.

Catégorie

Identifie la catégorie de niveau supérieur de l'action d'événement correspondante. Par exemple, Accès au système est la catégorie de l'action d'authentification.

Action

Identifie l'action d'événement.

Nom du journal

Identifie le nom du journal utilisé par le connecteur qui a collecté l'événement.

Utilisation de l'invite Utilisateur

Chaque événement indique des informations sur deux acteurs : la source et la destination.

- L'acteur source initie l'action à l'origine de l'événement.

  L'acteur source peut être un utilisateur, source_username ou un processus, source_processname.

- La destination ou l'acteur "dest" est la cible de l'action.

  L'acteur de destination peut être un utilisateur, dest_username ou un objet, dest_objectname.

Les requêtes de l'invite Hôte pour les événements dont le nom d'hôte a été spécifié apparaissent dans les champs CEG sélectionnés de l'événement ajusté. Envisagez ce scénario :

1. L'acteur source, source_usernamer ou source_processname tente une action sur l'acteur cible, destination_username ou destination_objectname.
2. Cet événement est enregistré dans un référentiel de la source d'événement.
3. Un agent CA Enterprise Log Manager effectue une copie de l'événement enregistré sur la source d'événement et la transmet à un serveur CA Enterprise Log Manager.

Pour utiliser l'invite Utilisateur, procédez comme suit :

1. Cliquez sur Requêtes et rapports.

   Cette liste de requêtes affiche le dossier Invites, ainsi qu'un ou plusieurs dossiers pour les autres requêtes.

2. Développez le dossier Invites et sélectionnez Utilisateur.

   L'invite Utilisateur apparaît.

3. Saisissez le nom de l'utilisateur sur lequel cette requête sera fondée.

4. Sélectionnez les champs sur lesquels fonder la requête de données qui correspond à votre saisie du nom d'utilisateur.

   source_username

   Représente le nom de l'utilisateur qui a initié l'action d'événement.

   dest_username

   Représente le nom de l'utilisateur ciblé par l'action.

   source_objectname

   Désigne le nom de l'objet impliqué dans l'action figurant dans les informations sur l'événement.

   dest_objectname

   Représente le nom de l'objet ciblé par l'action.

5. Cliquez sur OK.

   Les résultats de la requête de l'invite Utilisateur s'affichent.

6. Utilisez les descriptions suivantes pour interpréter les résultats de la requête :

   Sévérité CA

   Indique la sévérité de l'événement, dans laquelle les valeurs dans l'ordre croissant de la sévérité incluent les éléments suivants : informations, avertissement, impact mineur, impact majeur, critique et irrécupérable.

   Date

   Date à laquelle l'événement a eu lieu.

   Hôte de destination

   Identifie le nom de l'hôte avec l'utilisateur qui était la cible de l'action d'événement.

   Résultat

   Spécifie un code pour le résultat d'événement de l'action correspondante, où S signifie Réussi, E signifie échec, A signifie Accepté, D signifie Ignoré, R signifie Rejeté et U signifie Inconnu.

Utilisateur de la source

Identifie l'utilisateur qui a initié l'action d'événement.

Objet de la source

Identifie l'objet sur l'hôte source qui était impliqué dans l'événement d'action.

Utilisateur de destination

Identifie l'utilisateur qui était la cible de l'action d'événement.

Objet de destination

Identifie l'objet sur l'hôte de destination qui était impliqué dans l'événement d'action.

Catégorie

Identifie la catégorie de niveau supérieur de l'action d'événement correspondante. Par exemple, Accès au système est la catégorie de l'action d'authentification.

Action

Identifie l'action d'événement.

Nom du journal

Identifie le nom du journal utilisé par le connecteur qui a collecté l'événement.

Création d'une requête

Vous pouvez créer de nouvelles requêtes à inclure dans vos rapports personnalisés ou alertes d'action à l'aide de l'assistant de conception de la requête.

Vous pouvez également supprimer des requêtes personnalisées et exporter des informations de requête ou copier une requête d'abonnement pour créer une requête personnalisée, puis modifier cette requête à l'aide de l'assistant de conception de la requête. Seuls les utilisateurs disposant des rôles Administrator ou Analyst sont autorisés à créer, supprimer ou modifier des requêtes.

La procédure de création d'une requête à l'aide de l'assistant de conception de la requête se compose des étapes suivantes.

1. Ouverture de l'assistant de conception de la requête
2. Ajout d'informations d'identité et de balises
3. Sélection des colonnes de la requête
4. Définition des conditions et filtres de la requête (facultatif)
5. Définition de la plage de dates et des conditions de résultats (facultatif)
6. Choix des options de visualisation pour l'affichage de la requête (facultatif)
7. Ajout de valeurs de vue d'exploration descendante pour la requête (facultatif)

Informations complémentaires :

Ouverture de l'assistant de conception de la requête (page 296)
Ajout des détails de la requête (page 297)
Création d'une instruction SQL de requête (page 297)
Utilisation des filtres avancés (page 301)
Création d'une visualisation d'un affichage de requête (page 309)
Ajout d'un rapport de vue d'exploration descendante (page 310)

Ouverture de l'assistant de conception de la requête

Pour créer une nouvelle requête personnalisée, créer une copie d'une requête ou modifier une requête existante, vous devez ouvrir l'assistant de conception de la requête.

Pour ouvrir l'assistant de conception de la requête

1. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Requêtes.

   La Liste de requêtes s'affiche.

2. Cliquez sur Options et sélectionnez Créer.

   L'assistant de conception de la requête s'affiche.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer la requête sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer la requête et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires

Ajout des détails de la requête (page 297)
Création d'une instruction SQL de requête (page 297)
Définition des conditions de résultats (page 304)
Création d'une visualisation d'un affichage de requête (page 309)
Ajout d'un rapport de vue d'exploration descendante (page 310)

Ajout des détails de la requête

La première étape de création d'une nouvelle requête consiste à saisir les informations d'identification et à définir les balises à inclure.

Pour ajouter une nouvelle requête

1. Ouvrez l'assistant de conception de la requête.
2. Saisissez un nom de requête (obligatoire) et un nom abrégé (facultatif) à utiliser dans les rapports. Le nom abrégé apparaît dans le volet de requête du rapport lorsque la requête est incluse dans le rapport.
3. Si vous le souhaitez, entrez des remarques de conception dans le champ de saisie Description.

   Remarque : Nous recommandons d'utiliser ce champ pour entrer des informations sur la structure de la requête. Vous pouvez par exemple y expliquer de manière détaillée pourquoi la requête contient certains champs et fonctions.
4. Sélectionnez une ou plusieurs balises auxquelles associer votre requête à l'aide du contrôle de déplacement Balises.
5. Pour ajouter une balise de catégorie personnalisée, saisissez un nom de balise dans le champ de saisie Ajouter une balise personnalisée et cliquez sur le bouton Ajouter une balise (facultatif).

   La balise personnalisée apparaît, déjà sélectionnée, dans le contrôle de déplacement Balises.
6. Cliquez sur la flèche appropriée pour passer à l'étape de conception de la requête suivante que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape de conception de la requête choisie s'affiche.

Création d'une instruction SQL de requête

Pour créer une requête, écrivez une instruction SQL qui récupère les informations d'événement souhaitées du magasin de journaux d'événements. L'assistant de conception de la requête aide à automatiser ce processus.

Pour créer une instruction SQL de requête

1. Ouvrez l'assistant de conception de la requête.
2. Saisissez le nom et la balise, s'ils ne sont pas déjà spécifiés, puis passez à l'étape Colonnes de requêtes.
3. Sélectionnez la case Evénements uniques seulement (facultatif).

4. Définissez les colonnes CEG à interroger en les faisant glisser depuis la liste Colonnes disponibles située sur la gauche vers le champ Colonne du volet Colonnes sélectionnées. Elles apparaissent dans l'affichage de la requête, dans l'ordre de saisie.
5. Sélectionnez les paramètres souhaités pour chaque colonne (facultatif).

Nom d'affichage

Vous permet de saisir un autre nom pour la colonne au format Table ou Visionneuse d'événements. Si vous ne saisissez aucun Nom d'affichage, le nom du champ natif est utilisé en tant que nom de colonne, "nombre_événements" par exemple.

Fonction

Vous permet d'appliquer l'une des fonctions SQL suivantes aux valeurs de la colonne.

- COUNT : renvoie le nombre total d'événements.
- AVG : renvoie la moyenne des valeurs nombre_événements. Cette fonction est uniquement disponible pour les champs nombre_événements.
- SUM : renvoie la somme des valeurs nombre_événements. Cette fonction est uniquement disponible pour les champs nombre_événements.
- TRIM : supprime tous les espaces dans la chaîne de texte de la recherche.
- TOLOWER : convertit la chaîne de texte de la recherche en minuscules.
- TOUPPER : convertit la chaîne de texte de la recherche en majuscules.
- MIN : renvoie la valeur d'événement la plus basse.
- MAX : renvoie la valeur d'événement la plus haute.
- UNIQUECOUNT : renvoie le nombre total d'événements.

Ordre de regroupement

Définit l'affichage de la requête pour afficher les colonnes sélectionnées regroupées par l'attribut désigné. Par exemple, vous pouvez définir la requête pour regrouper les événements par nom de source. Vous pouvez contrôler l'ordre dans lequel il est appliqué aux différentes colonnes. Si les valeurs de la première colonne sont identiques, celles de la deuxième sont appliquées. Par exemple, vous pouvez regrouper plusieurs événements provenant de la même source par nom d'utilisateur.

Ordre de tri

Contrôle l'ordre dans lequel la valeur sélectionnée est triée. Vous pouvez contrôler l'ordre dans lequel il est appliqué aux différentes colonnes. Si les valeurs de la première colonne sont identiques, celles de la deuxième sont appliquées.

Décroissant

Définit les valeurs de colonne à afficher dans l'ordre décroissant (de la plus haute à la plus basse) plutôt que dans l'ordre croissant défini par défaut.

Non nul

Détermine si la ligne est affichée au format Table ou Visionneuse d'événements si elle ne contient aucune valeur. Lorsque la case Non nul est sélectionnée, la ligne est supprimée du résultat de la requête si elle ne contient aucune valeur affichable.

Visible

Détermine si la colonne est visible au format Table ou Visionneuse d'événements. Vous pouvez utiliser ce paramètre pour rendre les données de la colonne disponibles dans l'affichage en détails, sans l'afficher dans l'affichage lui-même.

6. Utilisez les flèches haut et bas situées en haut du volet Colonnes sélectionnées pour modifier l'ordre des colonnes selon vos besoins (facultatif).
7. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Informations complémentaires :

Création d'une requête (page 295)
Ajout des détails de la requête (page 297)
Utilisation des filtres avancés (page 301)
Création d'une visualisation d'un affichage de requête (page 309)
Ajout d'un rapport de vue d'exploration descendante (page 310)

Définition de filtres de requête

Vous pouvez filtrer les informations renvoyées par votre requête en utilisant des filtres simples ou avancés. Les filtres simples vous permettent de créer facilement et rapidement des instructions de filtre comprenant un seul terme. Les filtres avancés vous permettent de créer des instructions en langage SQL plus complexes, y compris des instructions imbriquées.

Pour définir des filtres de requête

1. Ouvrez l'assistant de conception de la requête.
2. Saisissez le nom et la balise, s'ils ne sont pas déjà spécifiés, puis passez à l'étape Filtres de requête.

   La boîte de dialogue Filtres de requête s'ouvre sur l'onglet Filtres simples.
3. Créez n'importe quel filtre simple de votre choix, pour rechercher des valeurs de champ CEG déclarées.
4. Cliquez sur l'onglet Filtres avancés (facultatif).
5. (Facultatif) Créez tous les filtres avancés souhaités.
6. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête sélectionnée s'affiche.

Informations complémentaires :

Création d'un filtre d'événement simple (page 301)
Création d'un filtre d'événement avancé (page 303)
Utilisation des filtres avancés (page 301)

Création d'un filtre d'événement simple

Les filtres simples permettent de définir les paramètres de recherche pour les champs CEG communs. Par exemple, vous pouvez définir le champ Modèle idéal sur Gestion du contenu afin d'identifier tous les événements comportant cette valeur dans le champ CEG Modèle idéal. Plusieurs fonctions utilisent les filtres simples, notamment les requêtes, les règles de suppression et de récapitulation, ainsi que les règles de transfert d'événement.

Pour créer un filtre simple :

1. Cochez la case en regard du champ Modèle idéal ou de tout autre champ Evénement que vous voulez définir, puis sélectionnez une valeur dans la liste déroulante ou saisissez la valeur de votre choix dans le champ de saisie de texte.
2. Lorsque vous créez un filtre de requête, cochez la case en regard de l'un des champs Source, Destination ou Agent, puis saisissez la valeur de votre choix dans le champ de saisie de texte (facultatif).
3. Répétez les étapes 1 à 2 pour ajouter d'autres filtres simples.
4. Cliquez sur Enregistrer après avoir ajouté tous les filtres de votre choix.

Informations complémentaires :

Utilisation des filtres avancés (page 301)
Création d'un filtre d'événement avancé (page 303)

Utilisation des filtres avancés

Vous pouvez utiliser des filtres avancés en langage SQL pour qualifier une fonction qui interroge le magasin de journaux d'événements, y compris pour limiter des requêtes ou personnaliser des filtres rapides. L'interface Filtres avancés vous aide à créer la syntaxe de filtre appropriée grâce à un formulaire de saisie des colonnes logiques, opérateurs et valeurs, selon vos besoins de filtrage.

Remarque : Cette section contient une brève présentation des termes SQL utilisés dans les filtres avancés. Pour utiliser les filtres avancés au maximum de leur potentiel, vous devez posséder une connaissance approfondie de la grammaire SQL et de la grammaire commune aux événements.

Les termes SQL suivants permettent d'associer plusieurs instructions de filtre;

And

Affiche les informations de l'événement si *tous* les termes ajoutés sont vrais.

Or

Affiche les informations de l'événement si *l'un* des termes ajoutés est vrai.

Having

Restreint les termes de l'instruction SQL principale en ajoutant une instruction de qualification. Par exemple, vous pouvez définir un filtre avancé pour les événements issus d'hôtes spécifiés et ajouter une instruction "having" afin de limiter les résultats aux événements d'un niveau de sévérité défini.

Les opérateurs SQL suivants sont utilisés par les filtres avancés pour créer les conditions de base.

Opérateurs relationnels

Inclut les informations de l'événement si la colonne porte la relation appropriée à la valeur saisie. Les opérateurs relationnels suivants sont disponibles.

- Egal à
- Différent de
- Inférieur à
- Supérieur à
- Inférieur ou égal à
- Supérieur ou égal à

Par exemple, l'utilisation de *Supérieur à* inclut les informations de l'événement à partir de la colonne choisie si sa valeur est supérieure à la valeur définie.

Comme

Inclut les informations de l'événement si la colonne contient le modèle que vous avez saisi à l'aide du signe %. Par exemple, L% renvoie toutes les valeurs commençant par L, %L% renvoie toutes les valeurs contenant L comme valeur mais pas comme première ou dernière lettre.

Distinct de

Inclut les informations de l'événement si la colonne ne contient pas le modèle spécifié.

Dans l'ensemble

Inclut les informations de l'événement si la colonne contient au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Hors ensemble

Inclut les informations de l'événement si la colonne ne contient pas au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Correspondance

Inclut toute information d'événement qui correspond au moins à un des caractères que vous avez saisis, ce qui vous permet de rechercher des mots clés.

A clés

Inclut toute information d'événement définie comme une valeur clé pendant la configuration du serveur de rapports. Vous pouvez utiliser les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Sans clé

Inclut toute information d'événement non définie comme une valeur clé pendant la configuration du serveur de rapports. Vous pouvez utiliser les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Création d'un filtre d'événement avancé

Les filtres avancés sont utilisés par de nombreuses fonctionnalités, dont la création d'une requête, la planification des rapports et les filtres locaux et globaux.

Pour créer un filtre avancé

1. Cliquez sur Nouveau filtre d'événement.

   La première ligne du tableau du filtre d'événement devient active et les colonnes Logique et Opérateur sont respectivement renseignées à l'aide des valeurs par défaut "Et" et "Egal à".

2. Cliquez sur la cellule Logique et modifiez la valeur logique si besoin (facultatif).
3. Cliquez sur la cellule Colonne et sélectionnez la colonne d'informations de l'événement souhaitée dans le menu déroulant.
4. Cliquez sur la cellule Opérateur et sélectionnez l'opérateur souhaité dans le menu déroulant.
5. Cliquez sur la cellule Valeur et saisissez la valeur souhaitée.
6. Cliquez sur les cellules des parenthèses d'ouverture et de fermeture et saisissez le nombre de parenthèses requis (facultatif).
7. Répétez les étapes 1 à 6 selon vos besoins pour ajouter des instructions de filtre supplémentaires (facultatif).
8. Cliquez sur Enregistrer une fois que vous avez saisi toutes les instructions de filtre souhaitées.

Informations complémentaires :

Utilisation des filtres avancés (page 301)
Création d'une requête (page 295)
Planification d'un job de rapport (page 508)

Définition des conditions de résultats

Vous pouvez définir une plage de dates et d'autres conditions de résultat pour la requête, notamment les limites des lignes et la période d'affichage de base. Les conditions de résultats peuvent être modifiées à tout moment jusqu'à l'heure d'exécution de la requête, ce qui en fait une méthode pratique pour modifier des requêtes sans remanier la requête de base ou ses filtres.

Vous pouvez définir les types suivants de conditions de résultats.

- Les conditions de plage de dates régissant la période de recherche de la requête
- Les conditions d'affichage, telles que le nombre maximum de lignes
- Les conditions d'événements regroupés, comme les événements regroupés les plus récents après une date donnée ou les événements regroupés contenant un nombre défini d'événements

  Remarque : Si vous ne regroupez pas au moins une colonne lors de la création d'une requête, les utilisateurs ne pourront pas modifier les conditions de résultats depuis l'affichage de la requête.

Définition d'une période ou d'une plage de dates

Vous pouvez définir des conditions de période ou de plage de dates pour votre requête. Cela améliore l'efficacité de votre requête en limitant la zone de recherche du magasin de journaux d'événements.

Vous pouvez sélectionner une plage horaire prédéfinie ou créer une plage personnalisée. Pour qu'une plage puisse fonctionner correctement, vous devez définir une heure de début et de fin. Si vous ne rentrez qu'un seul de ces paramètres, la période est exprimée par une clause "Where" dans la requête SQL.

Pour définir des conditions de résultat

1. Ouvrez la boîte de dialogue Conditions de résultats.
2. Sélectionnez une plage horaire prédéfinie dans la liste déroulante. Si vous souhaitez par exemple afficher les événements reçus hier, sélectionnez "jour précédent".

   Remarque : Lors de la création d'une alerte d'action ou d'un rapport planifié, l'interface affiche les périodes suivantes par défaut.

   - Alerte d'action : les 5 dernières minutes
   - Rapport planifié : les 6 dernières heures
3. Créez une plage personnalisée, en suivant les étapes ci-après (facultatif) :

   a. Dans la zone Sélection d'une plage de dates, cliquez sur Modifier en regard du champ de saisie Heure de fin dynamique. Cela vous permet de définir la fin de la période dans laquelle vous souhaitez effectuer la requête.

      La boîte de dialogue Spécification de la période dynamique s'affiche.

   b. Sélectionnez l'heure de référence pour le paramètre, puis cliquez sur Ajouter.

   c. Sélectionnez le paramètre d'heure de votre choix, puis cliquez sur Ajouter. Vous pouvez ajouter plusieurs paramètres d'heure.

   d. Cliquez sur OK lorsque vous avez terminé.

      Fermez la boîte de dialogue Spécification de la période dynamique. La valeur choisie s'affiche dans la zone Heure de fin dynamique. Dans ce cas, ils forment une instruction de temps complète, chaque paramètre se référant au premier. Par exemple, les valeurs Début du mois et Jour de la semaine - mardi ajoutées à la zone Heure de fin dynamique terminent votre requête le premier mardi du mois.

Remarque : Lorsque vous utilisez les valeurs Nombre de, telles que Nombre de jours ou Nombre d'heures, vous devez saisir un nombre *négatif* pour définir une période dans le passé. Un nombre positif définit une heure de fin dans le futur et la requête risque de continuer à envoyer des résultats, au moins jusqu'à ce qu'un événement qualifié figure dans le magasin de journaux.

Par exemple, les valeurs maintenant et nombre de minutes - 10 ajoutées à la zone Heure de début dynamique débutent votre requête 10 minutes avant l'heure de fin sélectionnée.

e. Dans la zone Heure de début dynamique, répétez l'étape 2 pour définir le début de la période sur laquelle vous souhaitez effectuer une requête.

Si vous n'entrez pas de plage de dates, la requête s'applique à tous les événements du magasin de journaux.

4. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Informations complémentaires :

Création d'une requête (page 295)
Définition des conditions de résultats (page 304)
Définition des conditions d'affichage et de groupe (page 307)

Définition des conditions d'affichage et de groupe

Vous pouvez définir des conditions qui vous permettent de contrôler l'affichage des requêtes et les conditions de recherche des événements en fonction de leur regroupement.

Pour définir des conditions d'affichage et de groupe

1. Ouvrez la boîte de dialogue Conditions de résultats.
2. Utilisez les cases à cocher Résultats pour activer, si besoin, les qualifications d'affichage suivantes.

   Limite des lignes

   Définit le nombre maximum de lignes d'événements affichés par la requête, en commençant par les plus récents.

   Minimum : 1

   Maximum : 5 000

   Afficher d'autres infos

   Indique la présence d'autres résultats qui ne sont pas affichés en raison de la limite de lignes, ce qui vous permet de comparer les événements sélectionnés dans le contexte de tous les événements du même type. Par exemple, si vous choisissez une limite de 10 lignes dans l'affichage de la visionneuse d'événements et si vous sélectionnez Afficher d'autres infos, les événements au-delà de 10 s'affichent dans une entrée particulière intitulée Autres, qui présente l'ensemble des événements restants. Le paramètre n'est actif que lorsque l'option Limites des lignes est sélectionnée.

   Granularité temporelle

   Définit le niveau de détail du champ de période utilisé dans l'affichage des requêtes.

3. Utilisez Conditions de résultats pour effectuer une requête sur plusieurs types de conditions d'événements regroupés. Par exemple, vous pouvez définir votre requête de façon à rechercher le dernier événement regroupé à partir d'une date sélectionnée ou un certain nombre d'événements regroupés. Un événement regroupé est un événement ajusté pour lequel vous avez défini une Fonction et un Ordre de regroupement à l'étape Création d'une requête.

   Les conditions de groupe utilisent le même système d'instruction de temps que les champs de période.

4. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Informations complémentaires

Création d'une requête (page 295)
Définition des conditions de résultats (page 304)

Création d'une visualisation d'un affichage de requête

Pour créer un nouvel affichage de requête, vous devez définir les Détails de visualisation qui contrôlent la manière dont les informations de l'événement apparaissent.

Pour créer une visualisation d'un affichage de requête

1. Ouvrez l'assistant de conception de la requête.
2. Saisissez le nom et la balise, s'ils ne sont pas déjà spécifiés, puis passez à l'étape Visualisation.
3. Déterminez si vous souhaitez que votre affichage de requête utilise une Visionneuse d'événements ou un Graphique.

   Si vous choisissez la Visionneuse d'événements, l'étape de visualisation est terminée. Les colonnes des événements apparaissent dans l'affichage Visionneuse d'événements dans l'ordre dans lequel vous les avez placées lors de l'étape de création des Colonnes de requêtes.
4. Si vous choisissez un Graphique, vous pouvez sélectionner un ou plusieurs types de graphiques. La sélection de plusieurs types de graphique permet aux utilisateurs de passer de l'un à l'autre dans l'affichage du rapport. Les flèches haut et bas en regard de chaque type contrôlent l'ordre dans lequel ils apparaissent dans le menu Changer la visualisation.

   Remarque : Le format Table reste disponible en tant que mode de visualisation même si vous ne l'ajoutez pas à cette étape.
5. Sélectionnez l'événement que vous souhaitez afficher comme axe X (horizontal) dans la liste déroulante de la colonne, saisissez le texte de l'étiquette le cas échéant et sélectionnez l'une des options suivantes dans le menu de type d'affichage.
   - Catégorie : utilisez cette option pour les colonnes de valeur de chaîne ou de texte, telles que nom_utilisateur_source.
   - Linéaire : utilisez cette option pour les valeurs numériques, telles que nombre_événements. Lorsque les valeurs sont étendues, vous pouvez utiliser la case Axe logarithmique pour permettre à l'axe de devenir logarithmique.
   - Date/Heure : utilisez cette option pour afficher les valeurs de date et heure locales.
6. Répétez l'étape 4 en utilisant les menus Paramètres de l'axe Y pour définir les options colonne, étiquette et type de l'axe Y (vertical).
7. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Ajout d'un rapport de vue d'exploration descendante

Vous pouvez ajouter un ou plusieurs rapports de vue d'exploration descendante à votre requête. Ces rapports permettent aux utilisateurs de cliquer sur un élément d'affichage d'une requête et de consulter un rapport connexe.

Pour ajouter une rapport de vue d'exploration descendante

1. Ouvrez l'assistant de conception de la requête.
2. Saisissez le nom et la balise, s'ils ne sont pas déjà spécifiés, puis passez à l'étape Vue d'exploration descendante.
3. Cliquez sur Ajouter une vue d'exploration descendante.
4. Saisissez le nom ou naviguez vers le rapport que vous souhaitez rendre disponible sous la forme d'une vue d'exploration descendante.
5. Sélectionnez au moins un paramètre disponible pour orienter le rapport et déplacez-le dans la liste Paramètres sélectionnés. Les rapports de vue d'exploration descendante utilisent les paramètres sélectionnés pour conserver l'orientation de votre requête.
6. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Modification d'une requête

Vous pouvez modifier des requêtes personnalisées existantes. Vous ne pouvez pas modifier une requête d'abonnement ; en revanche, vous pouvez en faire une copie et la modifier. Lorsque vous modifiez une requête, les changements effectués peuvent avoir un impact sur tous les rapports utilisant cette requête.

Pour modifier une requête

1. Cliquez sur l'onglet Requêtes et rapports et sur le sous-onglet Requêtes.

   La liste Filtre de balise de requête et la Liste de requêtes s'affichent.
2. Développez le dossier Utilisateur dans la Liste de requêtes et sélectionnez la requête à modifier.
3. Cliquez sur Options en haut de la liste, puis sélectionnez Modifier.

   L'assistant de conception de la requête s'ouvre. Il contient les spécifications de la requête que vous avez sélectionnée.
4. Effectuez les changements souhaités, puis cliquez sur Enregistrer.

Suppression d'une requête personnalisée

Vous pouvez supprimer une requête personnalisée. Vous ne pouvez pas supprimer une requête d'abonnement.

Pour supprimer une requête

1. Sélectionnez la requête que vous souhaitez supprimer.
2. Cliquez sur Options en haut de la liste, puis sélectionnez Supprimer.

   Une boîte de dialogue de confirmation apparaît.
3. Cliquez sur Oui.

   La requête supprimée disparaît de la Liste de requêtes.

Informations complémentaires :

Désactivation de l'option Afficher la requête sélectionnée (page 311)
Modification d'une requête (page 310)
Exportation et importation de définitions de requêtes (page 312)

Désactivation de l'option Afficher la requête sélectionnée

Vous pouvez paramétrer votre liste de requêtes de manière à effectuer des modifications sans charger les requêtes. Normalement, la sélection d'une requête dans la liste entraîne son affichage dans la fenêtre Détails.

La désactivation de ce mode par défaut vous fait gagner du temps en vous permettant de sélectionner une requête dans la liste et de la modifier immédiatement, sans attendre qu'elle s'affiche. Une fonction d'autant plus utile si vous devez modifier plusieurs requêtes et que vous savez déjà quels changements y apporter.

Remarque : Etant donné que seuls les utilisateurs avec le rôle Administrator ou Analyst peuvent créer ou modifier des requêtes, seuls ces utilisateurs peuvent désactiver le paramètre Afficher la requête sélectionnée.

Pour désactiver l'option Afficher la requête sélectionnée

1. Cliquez sur Options en haut de la Liste de requêtes.

   Le menu Options s'affiche.
2. Désélectionnez la case à cocher en regard de l'option Afficher la requête sélectionnée.

   La requête sélectionnée dans la liste ne s'affiche pas tant que l'option Afficher la requête sélectionnée n'est pas réactivée.

Exportation et importation de définitions de requêtes

Vous pouvez exporter et importer les détails des requêtes personnalisées pour les utiliser sur d'autres serveurs de gestion. Cela vous permet de transférer des requêtes personnalisées réussies entre différents environnements CA Enterprise Log Manager ou d'un environnement de test à un environnement réel.

Informations complémentaires

Création d'une requête (page 295)
Importation de définitions de requêtes (page 313)
Exportation de définitions de requêtes (page 312)

Exportation de définitions de requêtes

Vous pouvez exporter les détails des requêtes créées par l'utilisateur pour les utiliser sur d'autres serveurs de gestion. L'export est enregistré sous forme de fichier XML.

Pour exporter les détails d'une requête

1. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Requêtes.

   La Liste de requêtes s'affiche.

2. Cliquez sur Options en haut de la liste, puis sélectionnez Exporter.

   La boîte de dialogue Exporter les définitions de requête de l'utilisateur apparaît et affiche les rapports disponibles créés par l'utilisateur.

3. Sélectionnez la ou les requêtes que vous souhaitez exporter à l'aide du contrôle de déplacement, puis cliquez sur Exporter.

   Une boîte de dialogue d'exportation s'affiche.

4. Saisissez ou recherchez l'emplacement où vous souhaitez enregistrer les fichiers d'exportation XML, puis cliquez sur Enregistrer.

   Les fichiers de requêtes sont enregistrés à l'emplacement choisi et une boîte de dialogue de confirmation s'affiche.

5. Cliquez sur OK, puis sur Fermer.

   La boîte de dialogue Exporter les définitions de requête de l'utilisateur se ferme.

Informations complémentaires

Exportation et importation de définitions de requêtes (page 312)
Importation de définitions de requêtes (page 313)

Importation de définitions de requêtes

Vous pouvez importer des fichiers XML de définition de requête pour les utiliser sur le serveur de gestion local.

Pour importer les informations de rapport

1. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Requêtes.

   La Liste de requêtes s'affiche.

2. Cliquez sur Options en haut de la liste, puis sélectionnez Importer.

   La boîte de dialogue Importer un fichier s'ouvre.

3. Saisissez ou recherchez l'emplacement du fichier que vous souhaitez importer, puis cliquez sur OK.

   La fenêtre Résultats de l'importation apparaît.

4. Cliquez sur Importer un autre fichier pour répéter l'étape 3 ou cliquez sur Fermer.

   La fenêtre Résultats de l'importation se ferme.

Informations complémentaires

Exportation et importation de définitions de requêtes (page 312)
Exportation de définitions de requêtes (page 312)

Création d'un rapport

Vous pouvez créer des rapports personnalisés pour votre environnement, soit en créant un rapport entièrement nouveau conformément à la procédure décrite dans cette section, soit en utilisant un rapport prédéfini comme modèle. Vous pouvez afficher les rapports personnalisés ou les définir en tant que modèles de rapports planifiés.

Vous pouvez également modifier ou supprimer des rapports personnalisés et exporter les informations d'un rapport. Toutes ces tâches de personnalisation ne sont accessibles que si vous êtes connecté en tant qu'utilisateur possédant le rôle Administrator ou Analyst.

La procédure de création d'un nouveau rapport à l'aide de l'assistant de conception de rapport se compose des étapes suivantes.

1. Ouverture de l'assistant de conception de rapport
2. Ajout des informations du rapport : nommer le nouveau rapport et lui attribuer des balises de catégories.
3. Conception de la disposition du rapport : choisir les requêtes à inclure dans le rapport et la manière dont elles seront affichées.

Ouverture de l'assistant de conception de rapport

Pour créer un nouveau rapport personnalisé en partant de zéro ou d'un rapport existant, vous devez ouvrir l'assistant de conception de rapport.

Pour ouvrir l'assistant de conception de rapport

1. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Rapports.

   La Liste de rapports s'affiche.

2. Cliquez sur Options, puis sélectionnez Créer ou Copier.

   L'assistant de conception de rapport s'affiche.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le rapport et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Ajout des informations du rapport

Vous pouvez créer un nouveau rapport à partir de zéro ou d'une copie d'un rapport existant. Lorsque vous créez un rapport, vous le nommez et vous ajoutez les abonnements ou balises personnalisées que vous souhaitez lui associer.

Pour ajouter les informations du rapport

1. Ouvrez l'assistant de conception de rapport.
2. Saisissez un nom de rapport. Vous pouvez également saisir une description facultative pour référence.
3. Sélectionnez au moins une balise à associer au rapport à l'aide du contrôle de déplacement Balises.
4. Pour ajouter une balise de catégorie personnalisée, saisissez un nom de balise dans le champ de saisie Ajouter une balise personnalisée et cliquez sur Ajouter une balise (facultatif).

   La balise personnalisée apparaît dans la liste Balises sélectionnées.

5. Passez à l'étape Disposition ou cliquez sur Enregistrer et fermer si au moins une requête a déjà été sélectionnée.

Conception d'une disposition de rapport

Vous pouvez concevoir votre structure de rapport en spécifiant la taille et les dimensions de la grille, puis en sélectionnant les requêtes à afficher dans chaque section de la grille.

Pour concevoir une disposition de rapport

1. Ouvrez l'assistant de conception de rapport. S'il s'agit d'un nouveau rapport, entrez un nom, sélectionnez une balise et passez à l'étape Disposition.
2. Sélectionnez ou entrez le nombre de lignes et colonnes devant s'afficher dans votre rapport, à l'aide des zones Lignes de la grille et Colonnes du volet Disposition du rapport. Ces paramètres contrôlent le nombre de zones d'affichage des requêtes contenues dans le rapport. Vous pouvez inclure jusqu'à 10 lignes et/ou colonnes.

   Le nombre approprié de lignes, de colonnes et d'affichages des requêtes correspondants apparaît dans le volet Disposition du rapport.

   Remarque : Vous pouvez utiliser les flèches situées en bas à droite des zones d'affichage des requêtes pour les agrandir ou les réduire horizontalement ou verticalement.
3. Entrez ou sélectionnez une taille minimale, en pixels, pour les zones d'affichage des requêtes dans les zones Largeur minimum et Hauteur minimum (facultatif).
4. Faites glisser la requête que vous souhaitez afficher dans chaque zone depuis la Liste de requêtes vers la zone appropriée dans la disposition du rapport.
5. Cliquez sur le bouton Modifier, en haut de chaque zone d'affichage des requêtes, pour modifier la requête qui s'y trouve ou créez une nouvelle requête personnalisée (facultatif).
6. Cliquez sur Enregistrer et fermer.

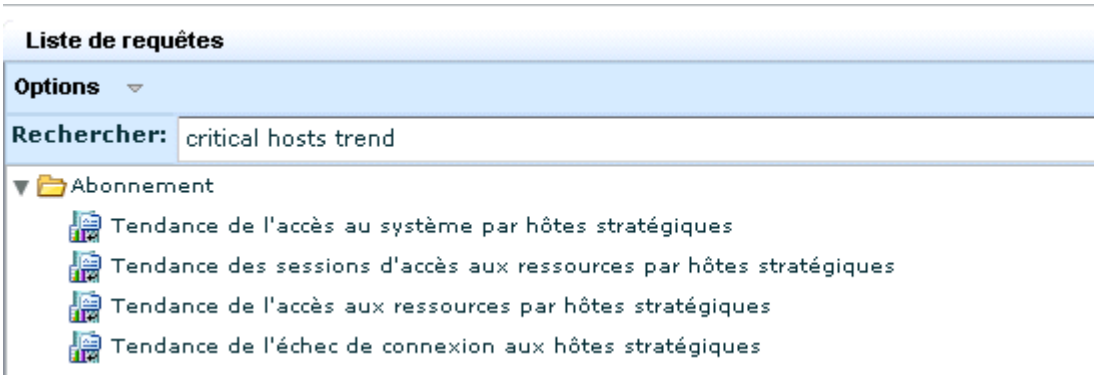
   L'assistant de conception de rapport se ferme. Le nouveau rapport apparaît dans la Liste de rapports, sous le dossier Utilisateur.

Exemple : Création d'un rapport à partir de requêtes existantes

Vous pouvez créer des rapports personnalisés composés de requêtes prédéfinies et les adapter à vos spécifications.

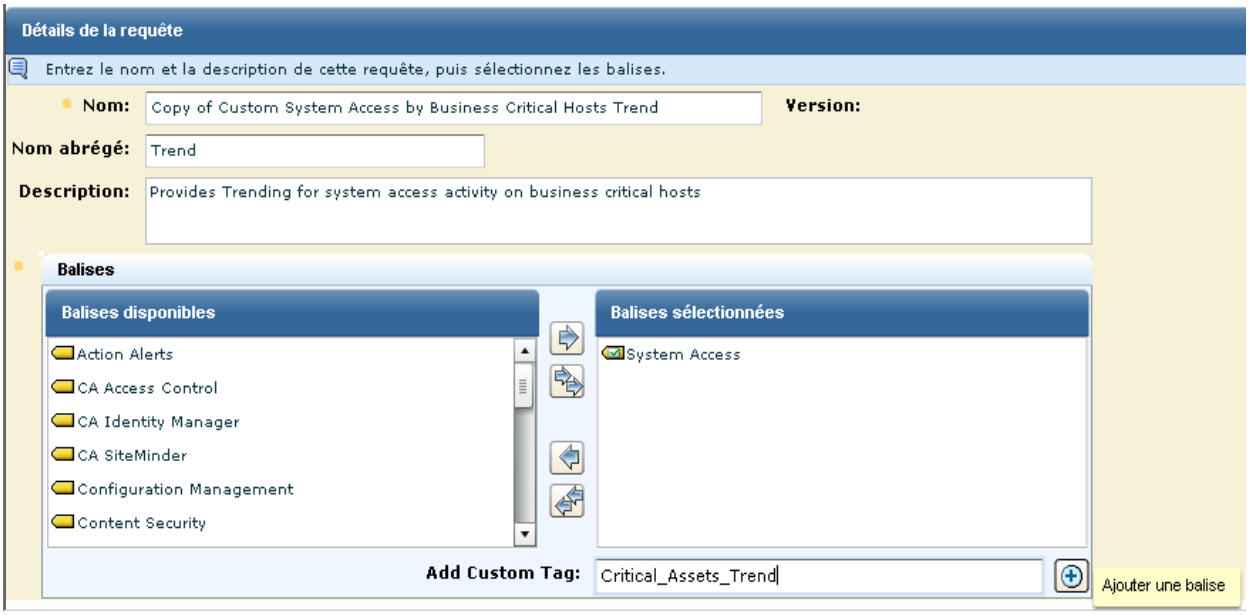
Pour créer un rapport à partir de requêtes existantes

1. Identifiez les requêtes à inclure dans le rapport personnalisé.
   a. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Requêtes, s'il n'est pas déjà affiché.
   b. Entrez un mot clé ou une expression clé dans le champ Rechercher, pour afficher les requêtes avec le contenu dans lequel vous souhaitez faire une sélection. Par exemple, entrez la tendance d'hôtes critiques.
   c. Notez les noms des requêtes que vous souhaitez inclure dans le rapport personnalisé. Vous pouvez ainsi définir un rapport des tendances associées aux hôtes stratégiques parmi celles répertoriées sur l'illustration suivante, par exemple, celles pour l'accès au système, l'accès aux ressources et les créations de comptes.



2. Pour la première requête à inclure dans le rapport, créez une copie et ajoutez une balise personnalisée.
   a. Sélectionnez une requête et sélectionnez Copier dans la liste déroulante Options.
   b. Renommez la requête et entrez une balise personnalisée à ajouter. Par exemple, renommez "Copie de Tendance de l'accès au système par hôtes stratégiques" en "Tendance personnalisée de l'accès au système par hôtes stratégiques".

c. Ajoutez une balise personnalisée. Par exemple, entrez Critical_Assets_Trend et cliquez sur Ajouter une balise.



d. Cliquez sur le bouton Déplacer pour déplacer la balise présélectionnée dans la zone Balises disponibles. Par exemple, déplacez Accès au système. La seule balise sélectionnée est celle que vous avez ajoutée.

e. Cliquez sur Enregistrer et fermer.

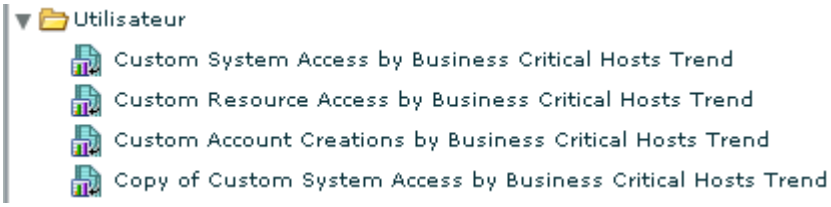
3. Pour que les autres requêtes soient incluses dans le rapport, créez une copie et sélectionnez la balise personnalisée que vous avez créée.

   a. Sélectionnez une requête et sélectionnez Copier dans la liste déroulante Options.

   b. Renommez la requête et sélectionnez la nouvelle balise personnalisée. Par exemple, renommez "Copie de Tendance de l'accès aux ressources par hôtes stratégiques" en "Tendance personnalisée de l'accès aux ressources par hôtes stratégiques", déplacez Critical_Assets_Trend dans la liste Balises sélectionnées et supprimez la balise présélectionnée.

   c. Cliquez sur Enregistrer et fermer.

   Les requêtes copiées s'affichent sous Utilisateur.

4. Si les requêtes sont associées à une liste à clés, définissez les valeurs pour cette liste à clés.

5. Démarrez le processus de création de rapport comme suit.

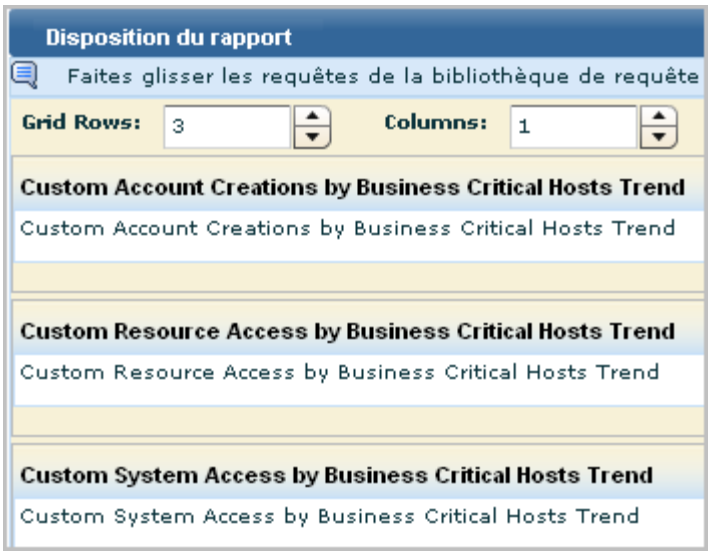
   a. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Rapports.

   b. Sélectionnez Créer dans la liste déroulante Options sous la Liste de rapports.

      L'assistant de conception de rapport s'affiche.

      Ajoutez la balise personnalisée Critical_Assets_Trend.

6. Concevez la disposition du rapport.



7. Cliquez sur Enregistrer et fermer.
8. Planifiez le rapport basé sur la balise personnalisée que vous avez créée.
9. Affichez le rapport.

Remarque : Il est recommandé d'examiner tout nouveau rapport pour vérifier qu'il contient bien les informations souhaitées.

Exemple : Configuration d'une fédération et de rapports fédérés

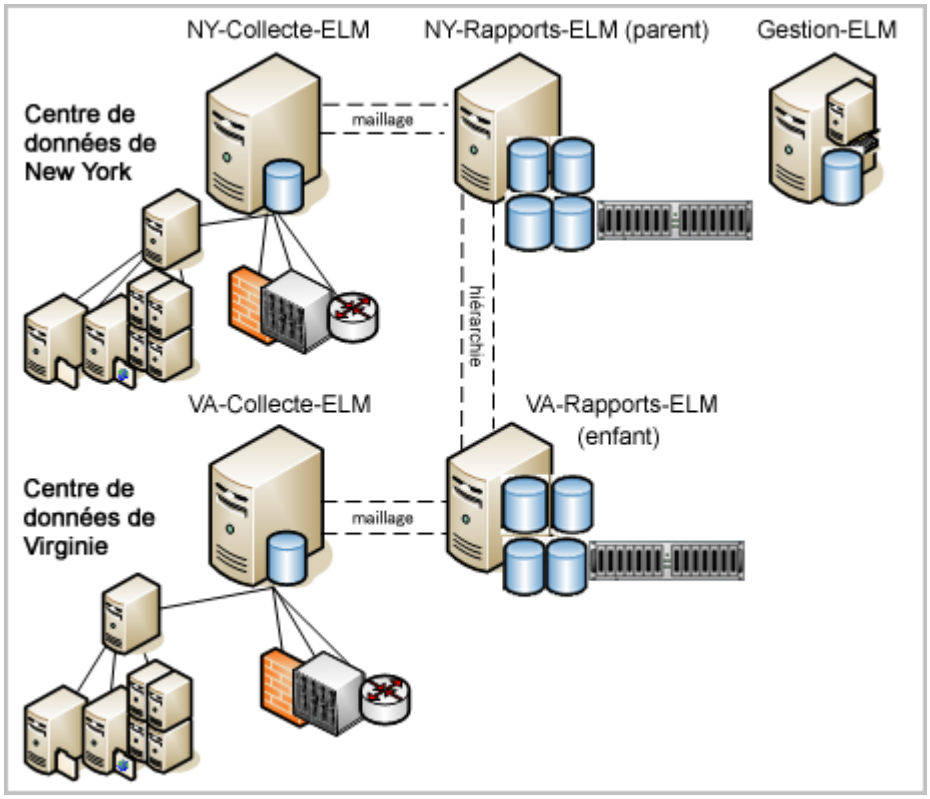
Vous pouvez collecter les journaux provenant de centres de données gros volume, géographiquement distincts, et configurer les rapports de manière à ce que les requêtes pour les données distribuées soient envoyées par un seul des centres de données.

Imaginez le scénario suivant : une société dont le siège se situe à New York dispose de deux centres de données gros volume, un à New York et un autre en Virginie. Chaque centre de données est équipé d'un serveur de collecte qui récupère et traite les journaux d'événements entrants et les envoie à son serveur de rapports. Ce dernier gère les requêtes, les alertes et les rapports. La plupart des requêtes, alertes et rapports concernent des données d'événement collectées par le biais d'agents ; consolider les données provenant de ces différentes sources d'événement exige une fédération entre les serveurs de rapports et les serveurs de collecte.

Certains rapports, requêtes et alertes concernent des événements d'autosurveillance générés par les serveurs CA Enterprise Log Manager ; consolider ce type de données exige l'inclusion du serveur de gestion dans la fédération. S'il n'est pas nécessaire de consolider les données des événements d'autosurveillance, le serveur de gestion peut être exclu de la fédération. Les événements d'autosurveillance provenant de ce serveur peuvent être contrôlés par le biais de rapports locaux non fédérés. Pour plus de simplicité, le serveur de gestion est exclu de cette fédération ; pour l'inclure, vous pouvez créer une fédération maillée entre NY-Rapports-ELM et Gestion-ELM.

Les noms de serveur sont les suivants.

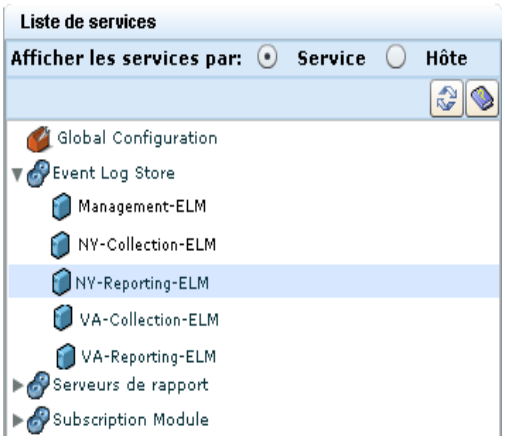
- Gestion-ELM
- NY-Collecte-ELM
- NY-Rapports-ELM
- VA-Collecte-ELM
- VA-Rapports-ELM



Imaginons que l'administrateur de New York souhaite que tous les rapports et alertes exécutés sur le site de New York incluent les données provenant du site de Virginie, mais que tous les rapports et alertes du site de Virginie incluent uniquement les données collectées localement.

L'exemple suivant vous explique comment fédérer les serveurs et configurer la génération de rapports pour répondre aux critères requis, dans le cadre de ce scénario. Les procédures de configuration de l'archivage automatique ne sont pas incluses dans cet exemple, toutefois il est possible de mettre en place un système d'archivage automatique pour n'importe quelle architecture à gros volume.

1. Connectez-vous à CA Enterprise Log Manager avec les informations d'identification de l'administrateur.
2. Cliquez sur l'onglet Administration, puis sélectionnez le sous-onglet Services.
3. Créez une fédération hiérarchique, où NY-Rapports-ELM est le parent et VA-Rapports-ELM l'enfant, en procédant comme suit.
   a. Développez le service Magasin de journaux d'événements, puis sélectionnez le nom du serveur qui sera parent dans la fédération hiérarchique, soit dans le cas présent NY-Rapports-ELM.



   b. Sélectionnez VA-Rapports-ELM dans la liste des enfants disponibles pour la fédération et déplacez-le dans la liste des éléments sélectionnés.

4. Créez une fédération maillée entre NY-Rapports-ELM et NY-Collecte-ELM, dans laquelle chacun est l'enfant de l'autre, en procédant comme suit.
   a. Sélectionnez NY-Rapports-ELM dans la liste Magasin de journaux d'événements.
   b. Sélectionnez NY-Collecte-ELM dans la liste des enfants disponibles pour la fédération et déplacez-le dans la liste des éléments sélectionnés.
   c. Sélectionnez NY-Collecte-ELM dans la liste Magasin de journaux d'événements.
   d. Sélectionnez NY-Rapports-ELM dans la liste des enfants disponibles pour la fédération et déplacez-le dans la liste des éléments sélectionnés.
5. Créez une fédération maillée entre VA-Rapports-ELM et VA-Collecte-ELM, dans laquelle chacun est l'enfant de l'autre, en procédant comme suit.
   a. Sélectionnez VA-Rapports-ELM dans la liste Magasin de journaux d'événements.
   b. Sélectionnez VA-Collecte-ELM dans la liste des enfants disponibles pour la fédération et déplacez-le dans la liste des éléments sélectionnés.
   c. Sélectionnez VA-Collecte-ELM dans la liste Magasin de journaux d'événements.
   d. Sélectionnez VA-Rapports-ELM dans la liste des enfants disponibles pour la fédération et déplacez-le dans la liste des éléments sélectionnés.
6. Définissez les paramètres de configuration globale du serveur de rapports et les remplacements locaux pour VA-Rapports-ELM, comme suit. Des serveurs géographiquement distants utilisent souvent des serveurs de messagerie distincts.
   a. Sélectionnez Serveur de rapports dans la Liste de services.
   b. Définissez les paramètres globaux pour le serveur de rapports, à partir de NY-Rapports-ELM. Si vous prévoyez d'envoyer des rapports par courriel, configurez les options du serveur de messagerie et les options de format PDF.

c. Configurez également les autres options relatives à la conservation des alertes et des rapports.

d. Développez l'option Serveur de rapports, puis sélectionnez VA-Rapports-ELM.

e. Remplacez les paramètres globaux du serveur de messagerie pour VA-Rapports-ELM.

7. Pour chaque rapport dont l'exécution est planifiée à partir de NY-Rapports-ELM, procédez comme suit.

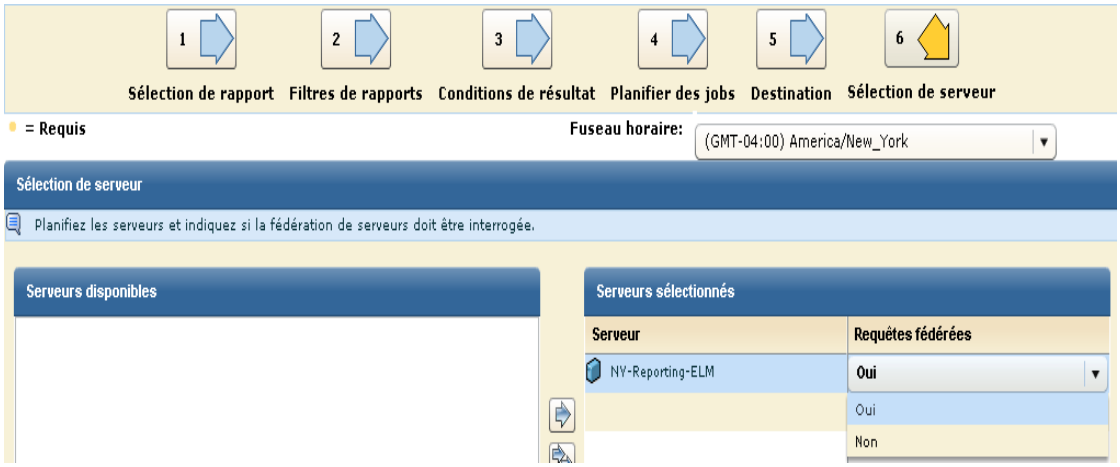
a. Sélectionnez l'onglet Rapports planifiés, puis l'onglet Planification de rapport.

b. Cliquez sur Planifier un rapport.

c. Sélectionnez le rapport à planifier et effectuez les étapes 2, 3, 4 et 5, le cas échéant.

d. Cliquez sur l'étape Sélection de serveur, sélectionnez NY-Rapports-ELM dans la liste des serveurs disponibles et déplacez-le jusqu'à la liste des serveurs sélectionnés, validez la valeur par défaut (Oui) pour la requête fédérée.

e. Cliquez sur Enregistrer et fermer.



Les rapports ainsi obtenus incluent les données provenant de NY-Rapports-ELM, son pair, NY-Collecte-ELM, son enfant, VA-Rapports-ELM, et le pair de son enfant, VA-Collecte-ELM.

Remarque : Une requête fédérée exécutée depuis VA-Rapports-ELM inclut les données provenant de VA-Rapports-ELM et de son pair VA-Collecte-ELM. Elle n'inclut pas les données provenant de NY-Rapports-ELM, car ce serveur est son parent dans le cadre de la fédération hiérarchique.

Modification d'un rapport

Vous pouvez modifier un rapport personnalisé.

Remarque : Vous pouvez désactiver l'option Afficher le rapport sélectionné lors de la modification de plusieurs rapports. Vous pouvez alors sélectionner et modifier des rapports sans attendre qu'ils s'affichent dans le volet Détails.

Pour modifier un rapport

1. Sélectionnez le rapport que vous souhaitez modifier dans la Liste de rapports.
2. Cliquez sur Options en haut de la liste, puis sélectionnez Modifier.

   L'assistant de conception de rapport s'ouvre. Il contient les spécifications du rapport que vous avez sélectionné.
3. Effectuez les changements souhaités, puis cliquez sur Enregistrer et fermer.

   Le rapport modifié apparaît dans la Liste de rapports sous le dossier Utilisateur.

Suppression d'un rapport personnalisé

Vous pouvez supprimer un rapport personnalisé. Vous ne pouvez pas supprimer un rapport d'abonnement.

Pour supprimer un rapport personnalisé

1. Sélectionnez le rapport personnalisé que vous souhaitez supprimer de la Liste de rapports.
2. Cliquez sur Options en haut de la liste, puis sélectionnez Supprimer.

   Une boîte de dialogue de confirmation apparaît.
3. Cliquez sur Oui.

   Le rapport supprimé disparaît de la Liste de rapports.

Informations complémentaires :

Création d'un rapport (page 313)
Modification d'un rapport (page 325)

Exemple : Suppression de rapports quotidiens datant de plus de 30 jours

Vous pouvez mettre en oeuvre des stratégies de conservation de rapports par le biais de la configuration globale des serveurs de rapports. Vous pouvez également définir une stratégie de conservation différente pour chaque occurrence de rapport planifié.

- Conservation des rapports uniques
- Conservation des rapports quotidiens
- Conservation des rapports hebdomadaires
- Conservation des rapports mensuels
- Conservation des rapports annuels

Vous devez choisir une fréquence autre que la fréquence par défaut (Jamais d'exécution) pour l'Utilitaire de conservation des rapports. Veillez à ce que la fréquence d'exécution choisie pour l'utilitaire corresponde à la fréquence de suppression configurée. Par exemple, si vous souhaitez supprimer vos rapports quotidiens un jour après leur exécution et si vous planifiez l'exécution de vos rapports quotidiens à 6:00 et à 18:00, vous pouvez choisir d'exécuter l'utilitaire de conservation des rapports toutes les 12 heures, au minimum.

Exemple : Suppression de rapports quotidiens datant de plus de 30 jours

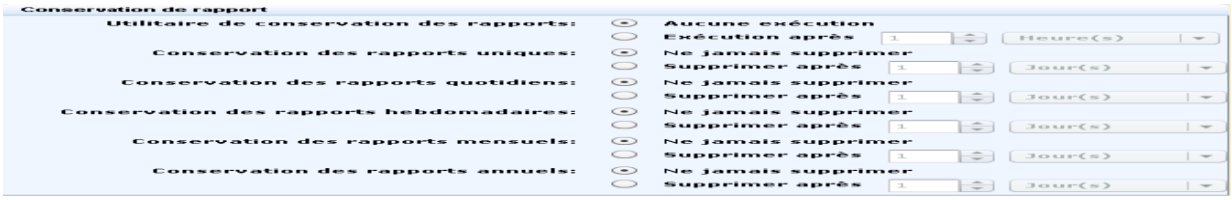
1. Cliquez sur l'onglet Administration et le sous-onglet Services.

   La Liste de services s'affiche, service par service.

2. Cliquez sur Serveur de rapports.

   La fenêtre Configuration globale de service (Serveur de rapports) s'affiche.

3. Observez les instructions suivantes pour terminer la configuration.
   - Pour automatiser la suppression de tous les rapports quotidiens 30 jours après leur création, configurez la fonction de conservation des rapports quotidiens en conséquence.
   - Veillez à configurer l'exécution de l'Utilitaire de conservation des rapports à la fréquence souhaitée (heures, jours ou semaines).



4. Cliquez sur Enregistrer.

Exportation des définitions de rapports

Vous pouvez exporter les détails des fichiers créés par l'utilisateur pour les utiliser dans d'autres serveurs de gestion. L'export est enregistré dans un fichier XML. Une définition de rapport exportée inclut les définitions de toutes les requêtes de ce rapport.

Pour exporter les informations d'un rapport

1. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Rapports.

   La Liste de rapports s'affiche.

2. Cliquez sur Options en haut de la liste, puis sélectionnez Exporter.

   La boîte de dialogue Exporter les définitions de rapports de l'utilisateur apparaît en affichant les rapports disponibles créés par l'utilisateur.

3. Sélectionnez le ou les rapports que vous souhaitez exporter à l'aide du contrôle de déplacement, puis cliquez sur Exporter.

   La boîte de dialogue Exporter apparaît.

4. Saisissez ou naviguez vers l'emplacement où vous souhaitez enregistrer les fichiers d'export XML, puis cliquez sur Enregistrer.

   Les fichiers Rapport sont enregistrés à l'emplacement choisi et une boîte de dialogue de confirmation apparaît.

5. Cliquez sur OK, puis sur Fermer.

   La boîte de dialogue Exporter les définitions de rapports de l'utilisateur se ferme.

Informations complémentaires :

Importation des définitions de rapports (page 328)

Importation des définitions de rapports

Vous pouvez importer des fichiers XML de définition de rapport pour les utiliser dans le serveur de gestion local.

Pour importer les informations du rapport

1. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Rapports.

   La Liste de rapports s'affiche.

2. Cliquez sur Options en haut de la liste, puis sélectionnez Importer.

   Une boîte de dialogue Importation de fichier s'ouvre.

3. Saisissez ou naviguez vers l'emplacement du fichier que vous souhaitez importer, puis cliquez sur OK.

   La fenêtre Résultats de l'importation apparaît.

4. Cliquez sur Importer un autre fichier pour répéter l'étape 3 ou cliquez sur Fermer.

   La fenêtre Importer les définitions de rapport et de requête de l'utilisateur se ferme.

Informations complémentaires :

Exportation des définitions de rapports (page 327)

Préparation à l'utilisation de rapports avec des listes à clés

Tous les rapports sont créés à partir d'au moins une requête. Certaines requêtes utilisées dans les rapports prédéfinis sont conçues pour sélectionner toutes les valeurs d'une table donnée dans laquelle un champ d'attribut particulier contient une valeur utilisée comme critère de compilation de la liste des valeurs clés. Par exemple, une table de ressources contient un champ IsCritical. Une requête qui sélectionne tous les noms de ressource de cette table pour lesquels IsCritical est égal à Oui est une requête qui sélectionne uniquement les noms des ressources critiques. Ces noms peuvent être renvoyés à CA Enterprise Log Manager afin de réactualiser les valeurs de la clé Critical_Assets.

La préparation de l'utilisation des rapports prédéfinis avec des listes à clés comprend les opérations ci-dessous.

- Activation de l'importation des valeurs dynamiques, si vous utilisez CA IT PAM (facultatif)
- Création des listes à clés pour les clés prédéfinies ne contenant aucune valeur prédéfinie
- Personnalisation des listes à clés pour les clés prédéfinies contenant des valeurs prédéfinies
- Gestion des listes à clés utilisées dans les rapports prédéfinis à utiliser Mise à jour de chaque liste à clés avec les valeurs actuelles

Par ailleurs, vous pouvez ajouter de nouvelles clés aux rapports personnalisés utilisant des listes à clés, puis ajouter des valeurs à chaque nouvelle clé. Vous avez également la possibilité d'ajouter des valeurs aux clés Business_Critical_Sources et ELM_System_Lognames pour les requêtes à la demande que vous avez créées.

Informations complémentaires :

Ajout de clés pour les requêtes ou les rapports personnalisés (page 334)
Mise à jour manuelle d'une liste à clés (page 335)
Mise à jour d'une liste à clés avec Exporter/Importer (page 336)
Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)
Préparation à l'utilisation d'alertes avec des listes à clés (page 493)

Activation de l'importation de valeurs dynamiques

Les procédures requises pour activer l'importation de valeurs dynamiques s'appliquent uniquement aux utilisateurs CA IT PAM.

Si vous utilisez CA IT PAM et disposez de feuilles de calcul ou de tableaux dans lesquels vous conservez vos listes de fichiers, de bases de données, d'hôtes et d'utilisateurs, par exemple, vous pouvez tirer parti de ces données. Vous pouvez créer un processus chargé de lire le tableau ou le fichier, de sélectionner les valeurs pertinentes pour la clé et de renvoyer ces valeurs à la liste de valeurs CA Enterprise Log Manager pour cette clé.

Pour importer des valeurs dynamiques

1. Créez un processus dans CA IT PAM pour chaque liste de valeurs clés que vous souhaitez générer à la demande.

   Remarque : Si un processus est chargé de lire une table de base de données, installez un agent CA IT PAM sur le serveur contenant la base de données SQL Server 2005.

2. Configurez l'intégration de CA IT PAM pour des valeurs dynamiques dans CA Enterprise Log Manager.

Informations complémentaires :

Création d'un processus CA IT PAM pour générer une liste de valeurs (page 331)
Configuration de l'intégration de CA IT PAM pour les valeurs dynamiques (page 332)

A propos du traitement des valeurs dynamiques

Un traitement des valeurs dynamiques est un processus CA IT PAM que vous pouvez invoquer pour renseigner ou mettre à jour la liste de valeurs d'une clé donnée utilisée dans des rapports ou des alertes. Il est supposé que vous stockez déjà la liste principale des fichiers, des bases de données, des hôtes, des utilisateurs, etc. composant votre environnement de travail, et que cette liste principale a été conçue avec des attributs vous permettant de définir une requête pour un ensemble de valeurs pertinentes. Si vous utilisez CA IT PAM, vous pouvez créer des processus pouvant être invoqués pour exécuter les requêtes renvoyant les données à CA Enterprise Log Manager, lesquelles données seront utilisées en tant que valeurs clés dans les rapports et les alertes basés sur des clés. Créer de manière dynamique une liste de valeurs est un moyen pratique de tenir à jour une liste de clés changeante.

Création d'un processus CA IT PAM pour générer une liste de valeurs

Vous pouvez créer un processus dans CA IT PAM pour chaque liste de valeurs clés que vous souhaitez pouvoir générer à la demande. Pour en savoir plus sur la création de processus, utilisez la documentation CA IT PAM. Chaque processus doit répondre aux exigences de CA Enterprise Log Manager concernant InputKey, les paramètres de processus locaux ValueList et FaultString, ainsi que les opérateurs de calcul Opération réussie et Echec.

Suivez les instructions ci-dessous.

- Ce processus doit accepter la clé sélectionnée en tant qu'InputKey.
- Le processus doit définir les deux paramètres de processus locaux suivants.
  - ValueList extrait la liste des valeurs.
  - FaultString extrait la chaîne d'erreur.

  Remarque : CA Enterprise Log Manager nécessite que ces noms de paramètres exacts soient utilisés en tant que paramètres d'interface de sortie.
- Le processus doit contenir les deux opérateurs de calcul suivants.
  - Opérateur de calcul Opération réussie : Process.ValueList =<variable contenant une liste de valeurs séparées par une virgule>
  - Opérateur de calcul Echec : Process.FaultString =<variable contenant un message d'erreur>

Si vous créez un script, tenez compte des instructions supplémentaires suivantes.

- Si votre script sélectionne des colonnes d'une table de base de données, un agent CA IT PAM doit exister sur le serveur où SQL Server 2005 est installé. Les serveurs SQL doivent être répertoriés dans votre domaine sous Tous les points de contact. Le serveur SQL contenant des données clés doit afficher le nom de l'agent du serveur SQL.
- Le script en ligne doit exécuter l'utilitaire sqlcmd pour extraire la liste souhaitée.

Informations complémentaires :

Configuration de l'intégration de CA IT PAM pour les valeurs dynamiques (page 332)
Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)

Configuration de l'intégration de CA IT PAM pour les valeurs dynamiques

Vous pouvez configurer l'intégration de CA IT PAM pour utiliser l'un des types de processus CA IT PAM suivants ou les deux.

- Processus de sortie de l'événement/de l'alerte : processus qui invoque le traitement sur un système tiers tel qu'un produit d'assistance.
- Traitement des valeurs dynamiques : processus qui accepte une clé d'entrée et renvoie des valeurs actuelles pour cette clé sous la forme d'un fichier de valeurs séparées par une virgule (*.csv)

Dans les deux cas, la configuration requiert la capacité de lancer CA IT PAM et de s'y connecter. Collectez les valeurs suivantes.

- Nom d'hôte complet ou adresse IP du serveur CA IT PAM
- Port (la valeur par défaut est 8080)
- Nom d'utilisateur et mot de passe que CA Enterprise Log Manager doit utiliser pour se connecter à CA IT PAM

La configuration de CA IT PAM pour les valeurs dynamiques vous permet d'importer la liste des valeurs générées de manière dynamique par le traitement des valeurs dynamiques configuré. L'importation est effectuée lors de la configuration ou de l'actualisation des valeurs à clés utilisées dans certains rapports et alertes.

La procédure suivante traite à la fois les paramètres communs et ceux spécifiques aux valeurs dynamiques.

Pour configurer l'intégration de CA IT PAM pour le traitement des valeurs dynamiques

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   La fenêtre Configuration globale de service (Serveur de rapports) s'affiche.
3. Faites défiler jusqu'à la zone CA IT PAM.
4. Procédez aux entrées suivantes pour activer l'accès CA IT PAM.
   a. Saisissez le nom d'hôte complet du serveur sur lequel est installé CA IT PAM.
   b. Acceptez le numéro de port par défaut, 8080.
   c. Saisissez des informations d'identification valides pour CA IT PAM.

5. Saisissez le chemin d'accès d'un processus dans le champ Traitement des valeurs dynamiques.

   Ce chemin d'accès devient la valeur par défaut lors de l'importation des valeurs dynamiques.

6. Cliquez sur Enregistrer.

   Le message suivant apparaît : "Confirmation : Les changements de configuration ont été enregistrés".

Approches de la gestion des listes à clés

Les listes à clés sont utilisées dans certaines requêtes et certains rapports prédéfinis, marqués comme appropriés pour les alertes d'action. Si vous prévoyez d'utiliser ces rapports ou de créer des alertes utilisant ces requêtes, vous pouvez combiner les approches suivantes pour gérer vos listes à clés.

- Vous pouvez ajouter directement des valeurs clés à n'importe quelle clé. Vous pouvez également sélectionner une valeur clé et la modifier ou la supprimer.
- Vous pouvez importer des valeurs clés stockées dans une liste CSV. Ou encore, vous pouvez exporter la liste de valeurs actuelle sous forme de fichier CSV, mettre à jour ce fichier, puis importer le fichier mis à jour pour renseigner la liste de valeurs.
- Vous pouvez exécuter un processus CA IT PAM chargé de générer de manière dynamique une liste et de renvoyer les valeurs sous forme de fichier CSV, pour renseigner la liste de valeurs.

Si vous prévoyez de créer des rapports personnalisés utilisant une liste à clés, vous pouvez ajouter une clé personnalisée, puis ajouter ou importer ses valeurs.

Vous pouvez identifier la ou les listes à clés utilisées dans une requête, puis les mettre à jour avant de planifier un rapport ou une alerte incluant cette requête.

Informations complémentaires :

Mise à jour manuelle d'une liste à clés (page 335)
Mise à jour d'une liste à clés avec Exporter/Importer (page 336)
Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)
Ajout de clés pour les requêtes ou les rapports personnalisés (page 334)
Détermination de l'utilisation de listes à clés pour une requête (page 342)

Ajout de clés pour les requêtes ou les rapports personnalisés

Vous pouvez spécifier des clés prédéfinies en ajoutant vos propres clés. Vous pouvez alors créer des rapports personnalisés utilisant ces clés.

Pour ajouter une nouvelle clé pour des rapports ou des alertes

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Sélectionnez Serveur de rapports dans la Liste de services.

   Les Listes définies par l'utilisateur (clés) s'affichent dans la section Configuration globale de service (Serveur de rapports).
3. Cliquez sur Ajouter une clé.
4. Saisissez une clé, puis cliquez sur OK.

   La nouvelle clé apparaît dans la liste à clés.
5. Ajoutez des valeurs pour cette clé, de l'une des manières suivantes.
   - Ajoutez les valeurs souhaitées manuellement.
   - Importez les valeurs à partir d'un fichier CSV.
   - Importez les valeurs mises à jour par un processus CA IT PAM.

Informations complémentaires :

Mise à jour manuelle d'une liste à clés (page 335)
Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)
Exemple : Mise à jour d'une liste à clés avec un fichier CSV (page 338)

Mise à jour manuelle d'une liste à clés

Vous pouvez mettre à jour les valeurs d'une liste à clés de plusieurs manières. Vous pouvez par exemple ajouter, modifier et supprimer les valeurs manuellement.

Pour mettre à jour une liste à clés manuellement

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Sélectionnez Serveur de rapports dans la Liste de services.

   Les valeurs clés apparaissent dans la fenêtre Configuration globale du service (Serveur de rapports).
3. Pour ajouter une valeur à la liste à clés
   a. Sélectionnez la clé pour laquelle vous souhaitez ajouter une valeur.
   b. Cliquez sur Ajouter une valeur.
   c. Entrez le nom de la valeur dans le champ Nom, puis cliquez sur OK.

      La valeur ajoutée apparaît dans la liste Valeurs, pour la clé sélectionnée.
   d. Répétez ces étapes pour chaque valeur à ajouter.
4. Pour supprimer une valeur dans la liste à clés
   a. Sélectionnez la clé contenant la valeur à supprimer.
   b. Sélectionnez la valeur à supprimer, puis cliquez sur Supprimer la valeur.

      Un message de confirmation apparaît.
   c. Cliquez sur OK.

      La valeur est supprimée de la liste Valeurs, pour la clé sélectionnée.
   d. Répétez ces étapes pour chaque valeur à supprimer.
5. Pour modifier une valeur dans la liste à clés
   a. Sélectionnez la clé pour laquelle vous souhaitez modifier une valeur.
   b. Sélectionnez la valeur à modifier, puis cliquez sur Modifier la valeur.
   c. Modifiez l'entrée du champ Nom, puis cliquez sur OK.

      La valeur s'affiche avec le nom modifié dans la liste Valeurs, pour la clé sélectionnée.
   d. Répétez ces étapes pour chaque valeur à modifier.
6. Cliquez sur Enregistrer.

   Les valeurs des clés sélectionnées sont mises à jour.

Mise à jour d'une liste à clés avec Exporter/Importer

Si vous stockez des valeurs qui correspondent à une clé dans une feuille de calcul Excel, vous pouvez enregistrer cette feuille de calcul en tant que liste de valeurs séparées par une virgule (*.csv) et remplir la liste à clés pour la sélection à l'aide d'une importation.

Vous pouvez mettre à jour les valeurs de la liste à clés que vous stockez dans un fichier CSV comme suit.

- Si le fichier CSV contient des valeurs actuelles pour une clé donnée et que la liste des valeurs affichées n'est pas à jour, vous pouvez importer les valeurs directement à partir du fichier CSV.
- Si vous souhaitez créer un fichier CSV ou mettre à jour un fichier présentant des valeurs obsolètes, utilisez une séquence exporter, modifier, importer.

Pour mettre à jour une liste à clés avec Exporter ou Importer

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Sélectionnez Serveur de rapports dans la Liste de services.

   Les valeurs clés apparaissent dans la fenêtre Configuration globale du service (Serveur de rapports).
3. Pour mettre à jour les valeurs pour une clé sélectionnée à partir d'un fichier CSV qui contient des valeurs actuelles
   a. Sélectionnez la clé dans la liste de valeurs clés pour les valeurs à mettre à jour.

      Ses valeurs obsolètes apparaissent dans la liste de valeurs.
   b. Cliquez sur Importer des valeurs sur la barre d'outils de liste des valeurs.

      La boîte de dialogue d'importation de fichier s'affiche.
   c. Cliquez sur Parcourir.

      La fenêtre Sélectionner le fichier à charger par <nom> CA Enterprise Log Manager apparaît, avec l'option Fichiers de type définie sur Fichiers CSV (séparés par des virgules).
   d. Accédez à l'emplacement du fichier CSV contenant les valeurs de la clé sélectionnée.
   e. Sélectionnez le fichier à importer, puis cliquez sur Ouvrir.

      Le nom du fichier sélectionné apparaît dans le champ Fichier.
   f. Cliquez sur OK.

   La liste de valeurs est mise à jour avec les valeurs du fichier CSV.

4. Pour mettre à jour les valeurs d'une clé sélectionnée à un emplacement où le fichier CSV n'existe pas ou n'est pas à jour

   a. Sélectionnez la clé dans la liste de valeurs clés pour les valeurs à mettre à jour.

   b. Dans la barre d'outils Valeurs, cliquez sur Exporter des valeurs.

      La fenêtre Sélectionner l'emplacement à télécharger par <nom du gestionnaire de journaux> apparaît, avec le fichier file.csv dans le champ Nom de fichier.

   c. Accédez à l'emplacement où le fichier CSV se trouve ou doit se trouver. Sélectionnez-le ou entrez le nouveau nom de fichier manuellement dans le champ Nom de fichier, puis cliquez sur Enregistrer.

      Une confirmation d'opération réussie s'affiche.

   d. Cliquez sur OK.

   e. Ouvrez l'explorateur Windows et accédez au fichier exporté.

   f. Ouvrez la feuille de calcul, modifiez ou supprimez les colonnes existantes selon les besoins. Faites défiler l'affichage jusqu'à la dernière colonne, puis ajoutez de nouvelles entrées. Enregistrez ensuite le fichier en tant que fichier CSV.

   g. Sélectionnez la même clé et cliquez sur Importer des valeurs.

   h. Cliquez sur Parcourir, sélectionnez le fichier enregistré, puis cliquez sur Ouvrir.

   i. Cliquez sur OK.

   Le fichier est téléchargé. Vous pouvez naviguer jusqu'en bas de la liste Valeurs, afin de vérifier la présence de l'entrée que vous avez ajoutée.

Informations complémentaires :

Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)

Exemple : Mise à jour d'une liste à clés avec un fichier CSV

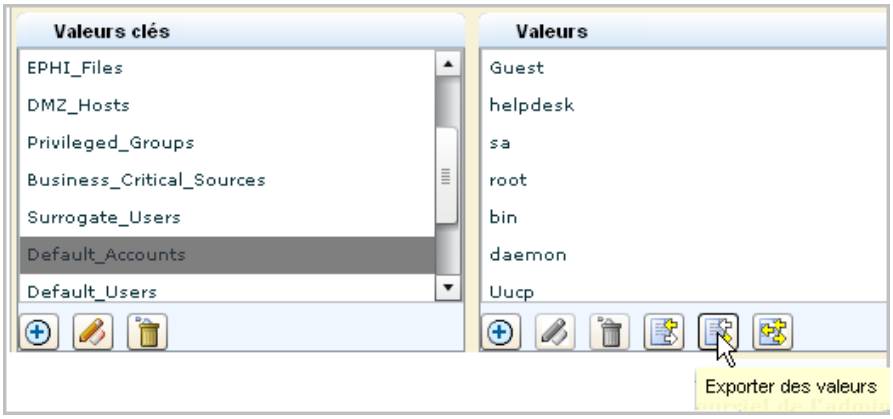
Vous pouvez spécifier des valeurs de liste à clés de l'une des trois manières suivantes.

- Saisissez manuellement les valeurs clés.
- Importez les valeurs clés à partir d'un fichier CSV.
- Importez les valeurs clés depuis un processus CA IT PAM.

Basez-vous sur l'exemple suivant pour la mise à jour des valeurs dans n'importe quelle liste à clés définie par l'utilisateur où les valeurs sont stockées dans une feuille de calcul Excel enregistrée sous la forme d'une liste de valeurs séparées par une virgule (*.csv).

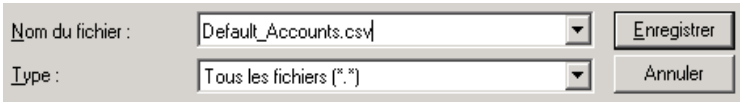
Pour mettre à jour une liste à clés avec un fichier CSV

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Sélectionnez Serveur de rapports.
3. Sélectionnez une clé, telle que Default_Accounts, puis cliquez sur Exporter des valeurs.



La boîte de dialogue Sélection de l'emplacement de téléchargement apparaît, avec le file.csv comme nom de fichier par défaut.

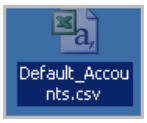
4. Sélectionnez le répertoire dans lequel vous souhaitez enregistrer le fichier exporté, par exemple, le Bureau. Saisissez un nom pour le fichier, par exemple, Default_Accounts.csv, puis cliquez sur Enregistrer.



Une confirmation d'exportation s'affiche.

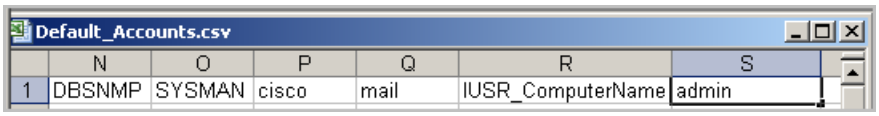
5. Cliquez sur OK.

   Une icône correspondant à la feuille de calcul exportée apparaît sur le bureau.



6. Ouvrez le fichier, faites défiler l'écran jusqu'à la dernière colonne, puis ajoutez l'entrée que vous souhaitez inclure.

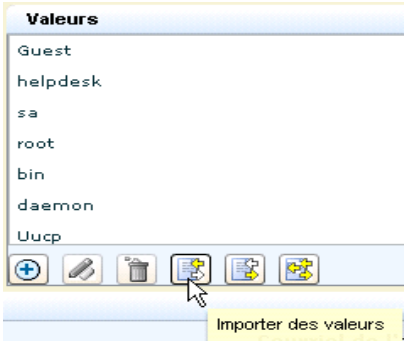
   Par exemple, saisissez *admin*, puis cliquez sur Enregistrer. Vous pouvez également supprimer la colonne de chaque entrée par défaut que vous souhaitez exclure de la liste à clés Default_Accounts.



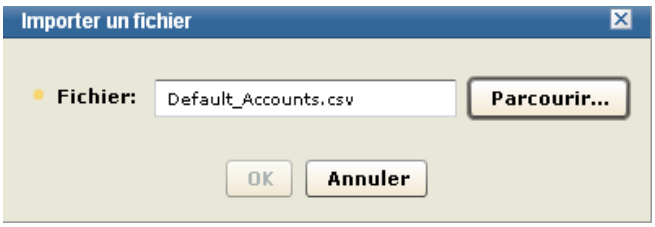
   La boîte de dialogue Enregistrer sous s'affiche, le nom de fichier qui y figure est Default_Accounts.csv.

7. Cliquez sur Enregistrer. Cliquez sur OK pour remplacer le fichier portant déjà ce nom.

8. Cliquez sur Importer des valeurs pour la liste mise à jour ; dans ce cas, il s'agit de la liste à clés Default_Accounts.



9. Cliquez sur Parcourir, sélectionnez le fichier enregistré, puis cliquez sur Ouvrir.



10. Cliquez sur OK.

    Le fichier est téléchargé. Vous pouvez naviguer jusqu'en bas de la liste Valeurs, afin de vérifier la présence de l'entrée que vous avez ajoutée.

Informations complémentaires :

Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)

Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques

Si vous utilisez des processus CA IT PAM pour générer une liste des valeurs associées à une clé utilisée dans les requêtes CA Enterprise Log Manager, exécutez le traitement des valeurs dynamiques CA IT PAM à partir de CA Enterprise Log Manager et mettez à jour les valeurs pour une clé donnée. L'importation vous fait économiser le temps nécessaire à la saisie manuelle de l'ensemble des valeurs d'une clé donnée. Lorsque les valeurs de l'une des quatre clés changent, vous pouvez les actualiser dans CA Enterprise Log Manager en sélectionnant la clé et en répétant l'importation des valeurs dynamiques.

Configurez l'intégration de CA IT PAM pour les valeurs dynamiques avant d'essayer d'importer les valeurs de la liste à clés à partir de CA IT PAM.

Pour importer les valeurs d'une liste à clés à partir de CA IT PAM

1. Cliquez sur l'onglet Administration et le sous-onglet Services.

   La liste de services apparaît.

2. Sélectionnez Serveur de rapports.

   Le panneau Configuration globale du service : Serveur de rapports s'affiche.

3. Pour créer une clé pour les valeurs à importer
   a. Faites défiler jusqu'à la zone Valeurs clés.
   b. Dans la barre d'outils Clé de la zone Valeurs clés, cliquez sur Ajouter.

      La boîte de dialogue Nom de la liste (clé) apparaît.

   c. Saisissez le nom de la nouvelle clé, puis cliquez sur OK.

      Le nom de la clé apparaît dans la liste de clés.

   d. Cliquez sur Enregistrer.

4. Pour actualiser les valeurs dynamiques d'une clé existante
   a. Faites défiler jusqu'à la zone Valeurs clés.
   b. Sélectionnez la clé.
   c. Cliquez sur Importer la liste des valeurs dynamiques. Ce bouton se trouve dans la barre d'outils Valeurs.

      Importer la liste des valeurs dynamiques apparaît.

   d. Entrez le nom du traitement des valeurs dynamiques CA IT PAM qui génère les valeurs de la clé sélectionnée, puis cliquez sur OK.

      Le processus CA IT PAM associé est exécuté, un fichier avec les résultats est renvoyé et les valeurs de la clé sélectionnée sont actualisées.

   e. Cliquez sur Enregistrer.

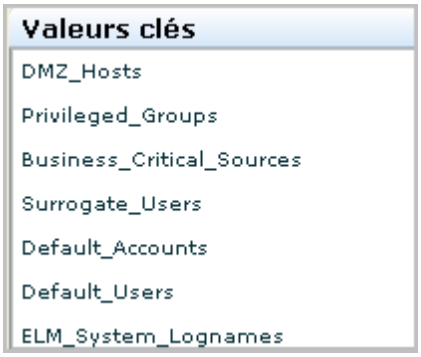
Informations complémentaires :

Activation de l'importation de valeurs dynamiques (page 330)
A propos du traitement des valeurs dynamiques (page 330)
Création d'un processus CA IT PAM pour générer une liste de valeurs (page 331)
Configuration de l'intégration de CA IT PAM pour les valeurs dynamiques (page 332)
Détermination de l'utilisation de listes à clés pour une requête (page 342)

Détermination de l'utilisation de listes à clés pour une requête

Il est recommandé de conserver les listes à clés à jour avec les valeurs actuelles. Pour mettre à jour une liste à clés utilisée dans un rapport ou une alerte, commencez par identifier les requêtes utilisées dans le rapport ou l'alerte. Déterminez ensuite la liste à clés utilisée dans la requête ou la requête source.

Les listes à clés sont affichées dans la configuration Serveur de rapports.



Les requêtes qui utilisent une liste à clés référencent souvent le nom de la liste à clés dans leur propre nom. Par exemple, le nom de certaines requêtes inclut "Default Accounts" ou "Privileged Group".

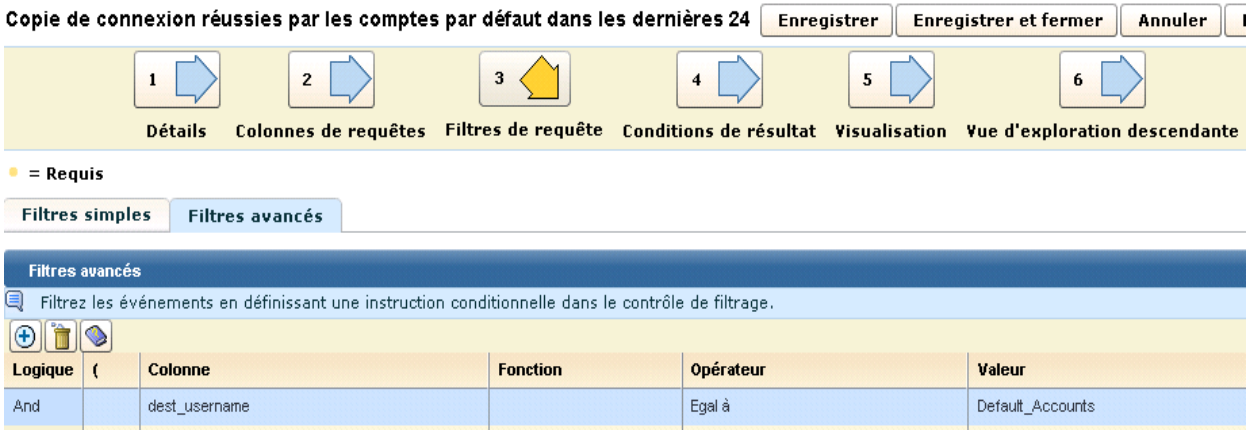
Pour trouver un nom de liste à clés afin de mettre à jour ses valeurs, vous pouvez envisager d'utiliser l'une des étapes de la procédure suivante.

Pour déterminer l'utilisation de listes à clés, le cas échéant, pour une requête

1. Vérifiez les filtres de requête avancés dans une copie de la requête.
   a. Cliquez sur Requêtes et rapports.
   b. Sélectionnez une balise de requête (facultatif).
   c. Sélectionnez une requête dans la liste de requêtes et sélectionnez la copie dans la liste déroulante Options.

      L'assistant Conception de requête apparaît.
   d. Cliquez sur l'étape Filtres de requête, puis sur l'onglet Filtres avancés.

      Une requête utilisant une liste à clés dispose d'un filtre avec l'opérateur A clés. La valeur est le nom de la liste à clés. Dans l'exemple suivant, Default_Accounts est la liste à clés.
   e. Cliquez sur Annuler. La copie de la requête définie par l'utilisateur n'est pas enregistrée.



2. Vous pouvez également exporter une copie de la requête vers un fichier XML et vérifier l'instruction Filter logic pour val=value où oper="KEYED".

   a. Cliquez sur Requêtes et rapports.

   b. Sélectionnez une balise de requête (facultatif).

   c. Sélectionnez une requête dans la liste de requêtes et sélectionnez la copie dans la liste déroulante Options.

      L'assistant Conception de requête apparaît.

   d. Cliquez sur Enregistrer et fermer.

      La copie de requête que vous avez créée apparaît sous Utilisateur dans la liste de requêtes.

   e. Sélectionnez cette requête définie par l'utilisateur dans la liste de requêtes, développez la liste déroulante Options, puis sélectionnez Exporter la définition de la requête.

      Le volet Exporter les définitions de requête de l'utilisateur apparaît avec la requête dans la liste des requêtes sélectionnées.

   f. Cliquez sur Exporter.

   g. Sélectionnez l'emplacement de téléchargement et remplacez le nom du fichier User Queries.xml par un nom unique. Cliquez ensuite sur Enregistrer.

   h. Ouvrez le fichier XML.

   i. Faites défiler jusqu'à l'instruction Filter logic et remarquez oper="KEYED" val="<nom de la liste à clés>".

      Voici un exemple.

```
    <Filter logic="AND" lparens="0" col="dest_username" colfunc="" oper="KEYED" val="Default_Accounts"
      rparens="0" />
  </Query>
- <Display>
    <Visualization type="VizEventViewer" />
  </Display>
</Panel>
```

Création de valeurs à clés pour des rapports prédéfinis

Certaines clés prédéfinies, utilisées dans des rapports prédéfinis, ne disposent pas de valeurs prédéfinies. Pour utiliser ces rapports de manière efficace, vous devez spécifier des valeurs pour les listes à clés correspondantes.

Vous pouvez spécifier des valeurs de liste à clés de l'une des trois manières suivantes.

- Saisissez manuellement les valeurs clés.
- Importez les valeurs clés à partir d'un fichier CSV statique.
- Importez les valeurs clés à partir d'un processus CA IT PAM chargé de générer de manière dynamique une liste à jour et de renvoyer un fichier CSV.

Informations complémentaires :

Création de valeurs à clés pour Critical_Assets (page 346)
Personnalisation des valeurs à clés pour Critical_Database (page 348)
Personnalisation des valeurs à clés pour Critical_Recipient (page 350)
Création de valeurs à clés pour DMZ_Hosts (page 352)
Création de valeurs à clés pour EPHI_Database (page 353)
Création de valeurs à clés pour EPHI_Files (page 354)
Approches de la gestion des listes à clés (page 333)

Création de valeurs à clés pour Critical_Assets

Vous pouvez utiliser trois rapports prédéfinis et les requêtes associées afin de contrôler les activités par hôte stratégique. Pour ce faire, vous devez tout d'abord identifier ces hôtes en tant que valeurs dans la liste de valeurs clés pour Critical_Assets. Aucune valeur n'est prédéfinie.

Les rapports utilisant vos valeurs personnalisées incluent les éléments suivants.

- Créations de comptes par hôtes stratégiques
- Echec de la connexion aux hôtes stratégiques
- Sessions d'accès aux ressources par hôtes stratégiques
- Accès aux ressources par hôtes stratégiques
- Accès au système par hôtes stratégiques

Des rapports similaires pour CA Access Control, CA Identity Manager et CA SiteMinder utilisent la liste à clés Critical_Assets, par exemple : CA Access Control - Créations de comptes par hôtes stratégiques.

Les requêtes suivantes utilisent la liste à clés Critical_Assets.

- Connexions (5 minimum) via les comptes d'administrateur sur les systèmes critiques au cours de la dernière nuit
- Connexions (5 minimum) via les comptes d'administrateur sur les systèmes critiques au cours des week-ends de la dernière semaine
- Activité d'exception système...

Si vous créez une requête personnalisée sur des actifs critiques, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_hostname	A clés	Critical_Assets

Pour créer des valeurs à clés pour Critical_Assets :

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous pouvez ajouter des valeurs personnalisées s'affiche.
3. Sélectionnez la clé Critical_Assets.
4. Exécutez l'une des actions suivantes pour créer la liste.
   - Cliquez sur Ajouter une valeur et saisissez chaque nouvelle valeur à inclure dans la liste à clés.
   - Créez une feuille de calcul Excel contenant une ligne, où chaque colonne correspond à une valeur unique. Enregistrez-la en tant que fichier CSV. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Informations complémentaires :

Mise à jour manuelle d'une liste à clés (page 335)
Mise à jour d'une liste à clés avec Exporter/Importer (page 336)
Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)

Personnalisation des valeurs à clés pour Critical_Database

Vous pouvez utiliser des rapports prédéfinis et les requêtes associées afin de surveiller les activités impliquant des bases de données critiques. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. Les valeurs prédéfinies incluent Master, mysql, information_schema, Distribution, Msdb, TempDB et sys.

Les rapports utilisant vos valeurs personnalisées incluent les éléments suivants.

- Activité d'échec d'autorisation sur une base de données critiques par {Nom du journal | Hôte | Base de données | Compte}
- Echec d'activité des bases de données critiques par {Exécutant | Nom du journal | Hôte | Base de données | Catégorie | Action}
- Gestion des bases de données critiques par {Nom du journal | Hôte | Base de données | Action | Compte}
- Activité de purge des bases de données critiques par {Nom du journal | Hôte | Base de données | Compte}
- Echec de la connexion à la base de données critiques par {Exécutant | Nom du journal | Hôte | Base de données | Compte}

Si vous créez une requête personnalisée sur des bases de données critiques, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_objectname	A clés	Critical_Database

Pour créer des valeurs à clés pour Critical_Database

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous pouvez ajouter des valeurs personnalisées s'affiche.
3. Sélectionnez ou créez la clé, Critical_Database.
4. Exécutez l'une des actions suivantes pour créer la liste.
   - Cliquez sur Ajouter une valeur et saisissez chaque nouvelle valeur à inclure dans la liste à clés.
   - Créez une feuille de calcul Excel contenant une ligne, où chaque colonne correspond à une valeur unique. Enregistrez-la en tant que fichier CSV. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Informations complémentaires :

Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)
Exemple : Mise à jour d'une liste à clés avec un fichier CSV (page 338)
Mise à jour manuelle d'une liste à clés (page 335)

Personnalisation des valeurs à clés pour Critical_Recipient

Vous pouvez utiliser des rapports prédéfinis et les requêtes associées afin de surveiller les activités impliquant des destinataires critiques. Pour ce faire, identifiez ces destinataires en tant que valeurs dans la liste de valeurs clés pour Critical_Recipient. La seule valeur prédéfinie est Administrator.

Les rapports utilisant vos valeurs personnalisées incluent les éléments suivants.

- Activité suspecte des courriels par destinataire
- Echec de l'activité d'authentification des courriels par destinataire
- Echec de l'activité de remise des courriels par destinataire
- Activité d'authentification des courriels par destinataire
- Activité de remise des courriels par destinataire
- Activité de retard des courriels par destinataire
- Activité des courriels par destinataire

Si vous créez une requête personnalisée qui doit utiliser cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_username	A clés	Critical_Recipient

Pour personnaliser des valeurs à clés pour Critical_Recipient

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous pouvez ajouter des valeurs personnalisées s'affiche.
3. Sélectionnez la clé, Critical_Recipient.
4. Exécutez l'une des actions suivantes pour créer la liste.
   - Cliquez sur Ajouter une valeur et saisissez chaque nouvelle valeur à inclure dans la liste à clés.
   - Créez une feuille de calcul Excel contenant une ligne, où chaque colonne correspond à une valeur unique. Enregistrez-la en tant que fichier CSV. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM, sélectionnez Critical_Assets et cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Informations complémentaires :

Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)
Exemple : Mise à jour d'une liste à clés avec un fichier CSV (page 338)
Mise à jour manuelle d'une liste à clés (page 335)

Création de valeurs à clés pour DMZ_Hosts

Vous pouvez utiliser des rapports prédéfinis et les requêtes associées afin de contrôler les serveurs de votre zone démilitarisée. Pour ce faire, vous devez tout d'abord identifier les serveurs de votre environnement hébergés dans la zone démilitarisée. Ajoutez pour cela des valeurs à la liste de valeurs clés pour DMZ_Hosts. Aucune valeur n'est prédéfinie.

Le rapport utilisant vos valeurs personnalisées est intitulé "Activité du pare-feu par zone démilitarisée".

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_hostname	A clés	DMZ_Hosts

Pour créer des valeurs à clés pour DMZ_Hosts

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, DMZ_Hosts.
4. Exécutez l'une des actions suivantes pour créer la liste.
   - Cliquez sur Ajouter une valeur et saisissez chaque nouvelle valeur à inclure dans la liste à clés.
   - Créez une feuille de calcul Excel contenant une ligne, où chaque colonne correspond à une valeur unique. Enregistrez-la en tant que fichier CSV. Cliquez sur Importer des valeurs pour importer votre liste de valeurs.
   - Si les valeurs de cette clé sont générées de manière dynamique par le processus CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Création de valeurs à clés pour EPHI_Database

Si vous avez des obligations de conformité dans le cadre de la loi HIPAA, vous pouvez utiliser les rapports prédéfinis et les requêtes associées pour contrôler les activités de votre base de données EPHI. Pour ce faire, vous devez tout d'abord identifier les bases de données contenant les données médicales des patients créées ou transmises par voie électronique. Ajoutez pour ce faire des valeurs à la liste de valeurs clés pour EPHI_Database. Il n'existe aucune valeur prédéfinie pour cette liste à clés.

Les rapports utilisant vos valeurs personnalisées et les valeurs prédéfinies incluent les éléments suivants.

- Activité d'accès aux bases de données EPHI
- Activité de contrôle d'accès aux bases de données EPHI

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_objectname	A clés	EPHI_Database

Pour créer des valeurs à clés pour EPHI_Database

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, EPHI_Database.
4. Exécutez l'une des actions suivantes pour créer la liste.
   - Cliquez sur Ajouter une valeur et saisissez chaque nouvelle valeur à inclure dans la liste à clés, pour les noms de bases de données utilisées avec les données EPHI (Electronic Private Health Information, données médicales électroniques confidentielles).
   - Créez une feuille de calcul Excel contenant une ligne, où chaque colonne correspond à une valeur unique. Enregistrez-la en tant que fichier CSV. Cliquez sur Importer des valeurs pour importer votre liste de valeurs.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Vous pouvez commencer à afficher et à planifier des rapports qui utilisent cette clé.

Création de valeurs à clés pour EPHI_Files

Si vous avez des obligations de conformité dans le cadre de la loi HIPAA, vous pouvez utiliser les rapports prédéfinis et les requêtes associées pour contrôler les activités de vos fichiers EPHI. Pour ce faire, vous devez tout d'abord identifier les fichiers contenant les données médicales des patients créées ou transmises par voie électronique. Ajoutez pour ce faire des valeurs à la liste de valeurs clés pour EPHI_Files. Il n'existe aucune valeur prédéfinie pour cette liste à clés.

Les rapports utilisant vos valeurs personnalisées et les valeurs prédéfinies incluent les éléments suivants.

- Activité d'accès aux fichiers EPHI
- Activité de contrôle d'accès aux fichiers EPHI

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_objectname	A clés	EPHI_Files

Pour créer des valeurs à clés pour EPHI_Files

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, EPHI_Files.
4. Exécutez l'une des actions suivantes pour créer la liste.
   - Cliquez sur Ajouter une valeur et saisissez chaque nouvelle valeur à inclure dans la liste à clés pour les noms de fichiers EPHI.
   - Créez une feuille de calcul Excel contenant une ligne, où chaque colonne correspond à une valeur unique. Enregistrez-la en tant que fichier CSV. Cliquez sur Importer des valeurs pour importer votre liste de valeurs.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Vous pouvez commencer à utiliser des rapports basés sur cette liste à clés.

Personnalisation des valeurs à clés pour les rapports prédéfinis

Certaines listes à clés utilisées dans des rapports prédéfinis présentent des valeurs prédéfinies. Vous pouvez utiliser ces rapports avec les valeurs de liste à clés par défaut uniquement ou spécifier vos propres valeurs pour la liste à clés prédéfinie.

Vous pouvez spécifier des valeurs de liste à clés de l'une des trois manières suivantes.

- Saisissez manuellement les valeurs clés.
- Importez les valeurs clés à partir d'un fichier CSV statique.
- Importez les valeurs clés à partir d'un processus CA IT PAM chargé de générer de manière dynamique une liste à jour et de renvoyer un fichier CSV.

Après avoir personnalisé des valeurs pour une liste à clés, affichez les résultats d'une requête ou d'un rapport qui utilise cette liste à clés.

Informations complémentaires :

Personnalisation des valeurs à clés pour Administrateurs (page 356)
Personnalisation des valeurs à clés pour Surrogate_Users (page 368)
Personnalisation des valeurs à clés pour Anonymous_Accounts et Guest_Accounts (page 358)
Personnalisation des valeurs à clés pour Critical_DDL_Actions (page 360)
Personnalisation des valeurs à clés pour Default_Users (page 362)
Personnalisation des valeurs à clés pour Error_Action (page 364)
Personnalisation des valeurs à clés pour Exception_Actions (page 366)
Approches de la gestion des listes à clés (page 333)

Personnalisation des valeurs à clés pour Administrateurs

Vous pouvez utiliser des rapports prédéfinis et les requêtes associées afin de contrôler les activités par administrateur. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. Les valeurs prédéfinies incluent Administrator, root, sa et admin.

Pour personnaliser la liste, vous devez identifier les autres comptes de votre environnement disposant de droits d'administration, afin de les utiliser comme valeurs dans la liste des valeurs clés pour Administrateurs.

Les rapports utilisant les valeurs à clés pour Administrator incluent les éléments suivants.

- Activité de la ressource d'administration
- Activité d'accès au système d'administration

Par ailleurs, des rapports similaires pour CA Access Control utilisent la liste à clés Administrators, par exemple : CA Access Control - Activité de la ressource d'administration par action.

Les requêtes utilisant les valeurs à clés pour Administrator incluent les éléments suivants.

- Connexions (5 minimum) via les comptes d'administrateur sur les systèmes critiques au cours de la dernière nuit
- Connexions (5 minimum) via les comptes d'administrateur sur les systèmes critiques au cours des week-ends de la dernière semaine

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_username	A clés	Administrateurs

Pour personnaliser des valeurs à clés pour Administrators

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, Administrateurs.

   Les valeurs prédéfinies s'affichent.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Mettez la liste à jour manuellement.
     - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
     - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
     - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Mettez à jour la liste par une exportation/importation.
     a. Cliquez sur Exporter des valeurs pour exporter la liste actuelle.
     b. Ouvrez la liste exportée, modifiez les valeurs de votre choix, puis enregistrez le fichier.
     c. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Cliquez sur Importer des valeurs pour importer les valeurs dans un fichier CSV mis à jour.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Informations complémentaires :

Approches de la gestion des listes à clés (page 333)

Personnalisation des valeurs à clés pour Anonymous_Accounts et Guest_Accounts

Vous pouvez utiliser un rapport prédéfini et les requêtes associées pour contrôler l'accès système par compte anonyme ou invité. Anonymous_Accounts ne dispose pas de valeurs prédéfinies. Guest_Accounts dispose de la valeur prédéfinie Guest. Vous pouvez utiliser les liste à clés par défaut uniquement ou leur ajouter des valeurs personnalisées.

Pour personnaliser la liste des comptes invités, identifiez tous les comptes invités de votre environnement et ajoutez-les comme valeurs de la liste de valeurs clés pour Guest_Accounts. Pour personnaliser la liste des comptes anonymes, identifiez tous les comptes anonymes de votre environnement et ajoutez-les comme valeurs de la liste de valeurs clés pour Anonymous_Accounts. Les rapports utilisant vos valeurs personnalisées et les valeurs prédéfinies incluent les éléments suivants.

- Accès au système par compte anonyme ou invité ...
- CA Access Control - Accès au système par compte anonyme ou invité ...
- CA SiteMinder - Accès au système par compte anonyme ou invité ...

Si vous créez une requête personnalisée utilisant ces deux clés, définissez le filtre comme suit.

Logique	Colonne	Opérateur	Valeur
And	dest_username	A clés	Guest_Accounts
Or	dest_username	A clés	Anonymous_Accounts

Pour modifier les valeurs à clés pour Anonymous_Accounts ou Guest_Accounts

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, Anonymous_Accounts ou Guest_Accounts.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Mettez la liste à jour manuellement.
     - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
     - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
     - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Mettez à jour la liste par une exportation/importation.
     a. Cliquez sur Exporter des valeurs pour exporter la liste actuelle.
     b. Ouvrez la liste exportée, modifiez les valeurs de votre choix, puis enregistrez le fichier.
     c. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Cliquez sur Importer des valeurs pour importer les valeurs dans un fichier CSV mis à jour.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Si la mise à jour concerne les deux clés, sélectionnez l'autre clé et mettez ses valeurs à jour.
6. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Personnalisation des valeurs à clés pour Critical_DDL_Actions

Vous pouvez utiliser un rapport prédéfini et les requêtes associées pour contrôler l'occurrence des actions DDL (Data Definition Language, langage de définition des données) critiques. Vous pouvez utiliser la liste à clés par défaut uniquement ou la modifier. Les valeurs prédéfinies incluent Interruption d'assemblage, Interruption d'édition, Suppression d'une fonction, Modification d'une fonction, Suppression d'un package, Modification d'un package, Suppression d'une procédure, Modification d'une procédure, Suppression d'une table, Modification d'une table, Purge d'une table, Suppression d'un déclencheur et Désactivation d'un déclencheur.

Pour personnaliser la liste, vous pouvez supprimer une valeur prédéfinie pour une action DDL. La liste prédéfinie inclut toutes les actions DDL valides enregistrées dans les champs CEG.

Le rapport utilisant cette liste à clés inclut les éléments suivants.

- Activités excessives (5) du langage de définition des données sur la base de données de production au cours de la dernière heure

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
event_action	A clés	Critical_DDL_Actions

Pour personnaliser des valeurs à clés pour Critical_DDL_Actions

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, Critical_DDL_Action.

   Les valeurs prédéfinies s'affichent.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Mettez la liste à jour manuellement.
     - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
     - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
     - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Mettez à jour la liste par une exportation/importation.
     a. Cliquez sur Exporter des valeurs pour exporter la liste actuelle.
     b. Ouvrez la liste exportée, modifiez les valeurs de votre choix, puis enregistrez le fichier.
     c. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Cliquez sur Importer des valeurs pour importer les valeurs dans un fichier CSV mis à jour.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Personnalisation des valeurs à clés pour Default_Users

Vous pouvez utiliser des rapports prédéfinis et les requêtes associées afin de contrôler les activités par utilisateur par défaut. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. Les valeurs prédéfinies incluent administrador, administrateur, administrator, bin, cisco, démon, DBSNMP, Guest, centre d'assistance, Imnadm, invscout, IUSR_ComputerName, messagerie, Nobody, root, sa, sshd, sys, SYSMAN, système et Uucp.

Pour personnaliser la liste, vous devez identifier les utilisateurs par défaut créés lors de l'installation du système d'exploitation, de la base de données ou de l'application en tant que valeurs de la liste de valeurs clés pour Default_Users.

Les rapports utilisant les valeurs à clés pour Default_Users incluent :

- CA Access Control - Accès au système par compte par défaut ...
- Accès au système par compte par défaut ...

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_username	A clés	Default_Users

Pour personnaliser des valeurs à clés pour Default_Users

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, Default_Users.

   Les valeurs prédéfinies s'affichent.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
   - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
   - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Cliquez sur Exporter des valeurs pour exporter la liste en cours, la modifier afin d'ajouter d'autres valeurs et enregistrer le fichier. Cliquez ensuite sur Importer des valeurs pour importer votre fichier modifié.
   - Si les valeurs de cette clé sont générées de manière dynamique par le processus CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Informations complémentaires :

Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par ligne (page 422)

Personnalisation des valeurs à clés pour Error_Action

Vous pouvez utiliser des rapports prédéfinis et les requêtes associées afin de surveiller les activités impliquant des erreurs. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. Les valeurs prédéfinies incluent Erreur d'application, Erreur de certificat, Erreur de configuration, Erreur de connexion, Erreur d'unité, Erreur de chiffrement, Erreur matérielle, Erreur de licence, Erreur d'analyse, Erreur logicielle et Erreur système.

Pour personnaliser la liste, vous devez identifier d'autres types d'erreurs en tant que valeurs dans votre liste de valeurs clés pour Error_Action.

Les rapports utilisant ces valeurs contiennent tous "Surveillance des erreurs ". En voici quelques exemples :

- Surveillance des erreurs par action
- Surveillance des erreurs par hôte
- Surveillance des erreurs par nom de journal
- Surveillance des erreurs par exécutant

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
event_action	A clés	Error_Action

Pour personnaliser des valeurs à clés pour Error_Action

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous pouvez ajouter des valeurs personnalisées s'affiche.
3. Sélectionnez la clé, Error_Action.

   Les valeurs prédéfinies s'affichent.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Mettez la liste à jour manuellement.
     - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
     - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
     - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Mettez à jour la liste par une exportation/importation.
     a. Cliquez sur Exporter des valeurs pour exporter la liste actuelle.
     b. Ouvrez la liste exportée, modifiez les valeurs de votre choix, puis enregistrez le fichier.
     c. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Cliquez sur Importer des valeurs pour importer les valeurs dans un fichier CSV mis à jour.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Informations complémentaires :

Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)
Exemple : Mise à jour d'une liste à clés avec un fichier CSV (page 338)
Mise à jour manuelle d'une liste à clés (page 335)

Personnalisation des valeurs à clés pour Exception_Actions

Vous pouvez utiliser des rapports prédéfinis et les requêtes associées afin de contrôler les activités système impliquant des exceptions. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. Les valeurs prédéfinies incluent Blocage du système, Erreur système, Arrêt du système et Avertissement système.

Pour personnaliser la liste, vous devez identifier les autres types d'exception en tant que valeurs de votre liste de valeurs clés pour Exception_Actions.

Les rapports utilisant ces valeurs contiennent tous "Activité d'exception système". En voici quelques exemples :

- Détail de l'activité d'exception système
- Activité d'exception système par nom de journal

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Logique	Colonne	Opérateur	Valeur
	dest_hostname	A clés	Critical_Assets
And	event_action	A clés	Exception_Actions

Pour personnaliser des valeurs à clés pour Exception_Actions

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous pouvez ajouter des valeurs personnalisées s'affiche.
3. Sélectionnez la clé, Exception_Actions.

   Les valeurs prédéfinies s'affichent.

4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Mettez la liste à jour manuellement.
     - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
     - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
     - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Mettez à jour la liste par une exportation/importation.
     a. Cliquez sur Exporter des valeurs pour exporter la liste actuelle.
     b. Ouvrez la liste exportée, modifiez les valeurs de votre choix, puis enregistrez le fichier.
     c. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Cliquez sur Importer des valeurs pour importer les valeurs dans un fichier CSV mis à jour.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Informations complémentaires :

Mise à jour manuelle d'une liste à clés (page 335)
Exemple : Mise à jour d'une liste à clés avec un fichier CSV (page 338)
Mise à jour d'une liste à clés avec un traitement des valeurs dynamiques (page 341)

Personnalisation des valeurs à clés pour Surrogate_Users

Vous pouvez utiliser un rapport prédéfini et les requêtes associées pour contrôler l'accès SU par compte. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. La seule valeur prédéfinie est root.

Pour personnaliser la liste, vous devez identifier les comptes de votre environnement faisant l'objet d'une activité de substitution et ajouter ces valeurs à la liste des valeurs clés pour Surrogate_Users. Le rapport utilisant les valeurs personnalisées et prédéfinies est intitulé "Accès SU par compte".

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_username	A clés	Surrogate_Users

Pour modifier les valeurs à clés pour Surrogate_Users

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, Surrogate_Users.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Mettez la liste à jour manuellement.
     - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
     - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur.
     - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.

- Mettez à jour la liste par une exportation/importation.
  a. Cliquez sur Exporter des valeurs pour exporter la liste actuelle.
  b. Ouvrez la liste exportée, modifiez la liste, puis enregistrez le fichier.
  c. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
- Cliquez sur Importer des valeurs pour importer les valeurs dans un fichier CSV mis à jour.
- Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.

5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Affichage d'un rapport à l'aide d'une liste à clés

Vous pouvez afficher les résultats d'un rapport avant de planifier sa création. Certains rapports prédéfinis utilisent des listes à clés, où la clé est prédéfinie mais les valeurs personnalisées par l'utilisateur. Lorsque vous avez ajouté ou importé des valeurs pour une clé, il est recommandé d'afficher le rapport à l'aide de la liste à clés.

Pour afficher un rapport à l'aide d'une liste à clés

1. Cliquez sur l'onglet Requêtes et rapports et sur le sous-onglet Rapports.
2. Sélectionnez un rapport utilisant une liste à clés.
3. Affichez les résultats.

Chapitre 10 : Alertes d'action

Ce chapitre traite des sujets suivants :

A propos des alertes d'action

Les alertes d'action sont des rapports spécialisés qui génèrent un événement lorsque leurs conditions de requêtes sont remplies. Elles peuvent vous aider à surveiller votre environnement grâce à des notifications automatiques pour une grande variété de situations et d'occurrences. Par exemple, vous pouvez définir des alertes d'action qui délivrent des informations de tendance d'événement, suivent l'utilisation de l'espace disque ou envoient des notifications en cas de dépassement des seuils d'échec d'accès.

Les alertes d'action sont un bon moyen de passer au crible des montagnes de données collectées afin de détecter les quelques événements auxquels vous devez réagir immédiatement. Vous pouvez utiliser les alertes d'action pour être averti de la quasi-totalité des événements survenant sur votre réseau de collecte de journaux. Les alertes que vous créez vous informent notamment des pointes de trafic entrant ou sortant, du trafic sur certains ports, des accès à certaines ressources soumises à des droits, des changements de configuration de diverses entités réseau comme les pare-feu, les bases de données ou les serveurs clés, etc.

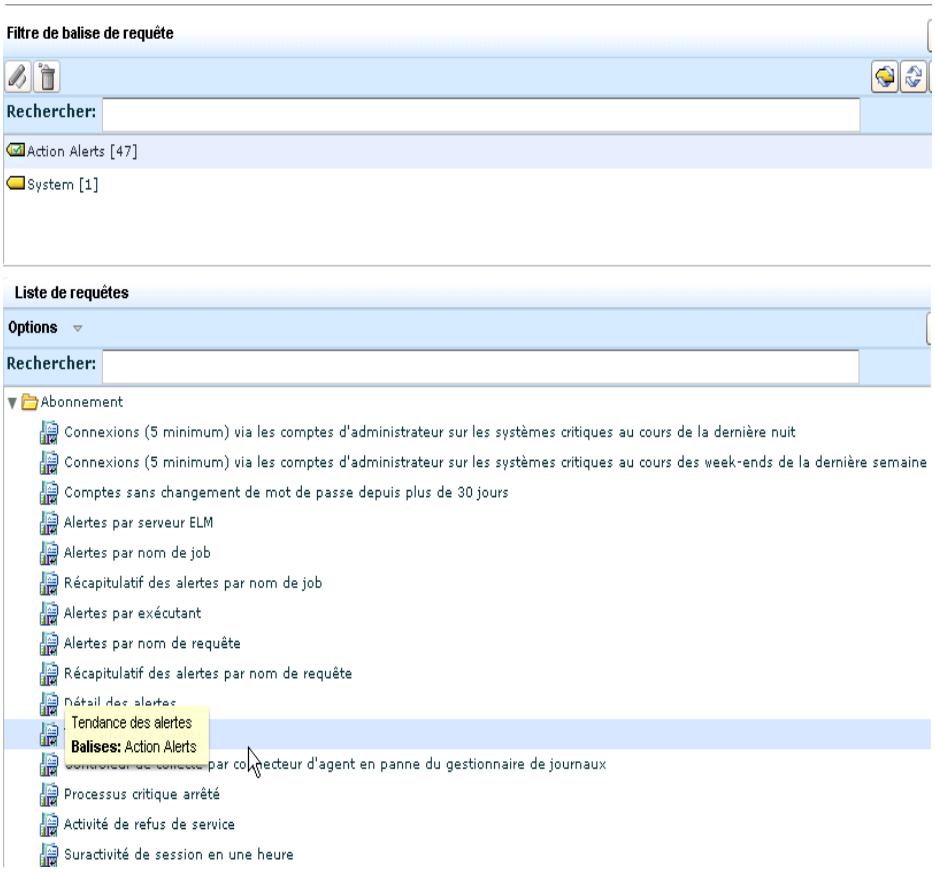
Vous pouvez créer des alertes d'action des manières suivantes.

- A l'aide de l'assistant d'alerte d'action
- A partir d'un affichage de requête
- A l'aide d'une requête personnalisée

Les options de planification représentent une part importante du processus de création d'une alerte, car elles vous permettent de contrôler la durée et la fréquence d'exécution de votre job d'alerte.

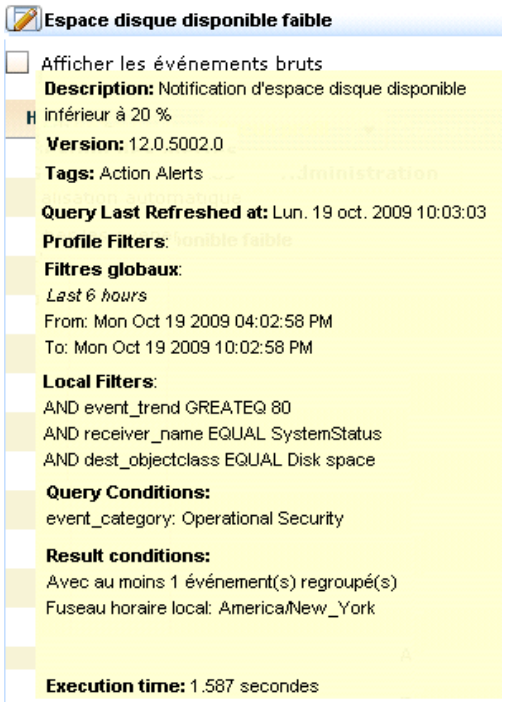
Utilisation de requêtes marquées en tant qu'alertes d'action

CA Enterprise Log Manager propose un certain nombre de requêtes marquées de la balise Alertes d'action. Pour afficher la liste des requêtes marquées Alertes d'action, cliquez sur l'onglet Requêtes et rapports et le sous-onglet Requêtes, puis sélectionnez la balise Alertes d'action. Les requêtes marquées de cette balise apparaissent dans la Liste des requêtes. Lorsque vous déplacez le curseur sur un nom de requête, sa ou ses balises s'affichent.



Avant de planifier des alertes d'action depuis ces requêtes, vous pouvez obtenir davantage d'informations sur l'objectif de chacune de ces requêtes. Pour afficher la description et les détails d'une requête, par exemple "Espace disque disponible faible", sélectionnez la requête dans la liste des requêtes, puis placez le curseur sur son nom.

Un récapitulatif de la requête s'affiche, comprenant une description, les filtres et les conditions de la requête.



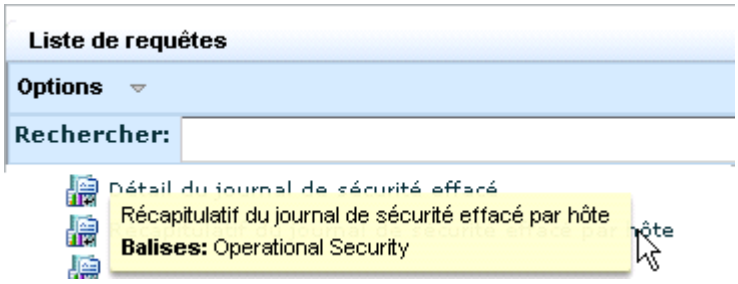
Vous pouvez planifier la requête telle quelle ou bien la copier sous un nouveau nom et la personnaliser en fonction de vos besoins. Par exemple, vous pouvez générer une alerte quand l'espace disque disponible est inférieur à 25 % au lieu de 20 %. Vous pouvez créer une requête définie par l'utilisateur en fonction de la requête prédéfinie, puis la sélectionner pour votre alerte d'action.

Remarque : Avant d'utiliser des requêtes contenant la mention "Groupes avec droits" ou "Compte par défaut" dans leur titre, veillez à ajouter vos valeurs à clés personnalisées dans les listes à clés correspondantes.

Identification d'autres requêtes à utiliser pour les alertes

Certaines requêtes qui ne sont pas balisées comme alertes d'action peuvent être intéressantes à inclure dans une alerte d'action planifiée du fait qu'elles récupèrent uniquement les événements évalués comme graves.

Par exemple, la requête Détail du journal de sécurité effacé par hôte récupère tous les événements dont l'action est Suppression du journal d'activité. La seule balise de cette requête est Sécurité opérationnelle.



L'action, Suppression du journal de sécurité, est répertoriée dans le composant CEG. Le composant CEG définit les deux types d'événement suivants avec le niveau de sécurité 6, qui correspond au niveau grave.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Sécurité opérationnelle	Activité du journal de sécurité	Suppression du journal de sécurité	Terminé	6
Sécurité opérationnelle	Activité du journal de sécurité	Suppression du journal de sécurité	Echec	6

Il est fortement recommandé de planifier une alerte avec cette requête.

Informations complémentaires :

Identification du filtre simple pour les événements graves (page 377)

Personnalisation de requêtes pour les alertes d'action

Les alertes ont été conçues pour avertir l'utilisateur, le processus ou le produit approprié lorsqu'un événement grave se produit. Pour identifier les requêtes appropriées sur lesquelles baser une alerte, étudiez les requêtes conçues pour récupérer les événements présentant un niveau de sécurité élevé.

Une fois identifiées les définitions pour les événements graves, vous pouvez identifier les requêtes chargées de récupérer ces événements. S'il n'existe pas de requête de ce type, vous pouvez en créer.

Respectez la procédure ci-dessous.

1. Identifiez les types d'événement que CA considère comme très graves ; ces types étant définis par catégorie, classe, action et résultat.
2. Identifiez les requêtes prédéfinies conçues pour récupérer uniquement ce type d'événement.
3. Identifiez les requêtes prédéfinies conçues pour récupérer des événements pouvant inclure des événements graves, et qui peuvent être personnalisées pour inclure uniquement les événements graves.
4. Créez des requêtes personnalisées lorsqu'il n'existe aucune requête prédéfinie.
5. Planifiez des alertes pour exécuter ces requêtes fréquemment.

Informations complémentaires :

Identification du filtre simple pour les événements graves (page 377)
Personnalisation de requêtes pour récupérer les événements graves uniquement (page 381)
Création d'une requête pour récupérer les événements graves uniquement (page 378)

Identification du filtre simple pour les événements graves

Le niveau de sévérité d'un événement peut varier de Information à Irrécupérable. CA affecte une valeur comprise entre 2 et 7 pour indiquer la sévérité d'un événement sur la base du modèle CEG : Catégorie, Classe, Action et Résultat. Le niveau de sévérité 7 est attribué aux événements d'arrêt du système. Le niveau de sévérité 6 est attribué aux événements ayant d'importantes implications en matière de sécurité ou exigeant une attention immédiate.

Si vous prévoyez de créer des requêtes personnalisées ou de personnaliser des requêtes prédéfinies pour les utiliser dans des alertes, il peut être intéressant d'étudier les définitions du modèle CEG concernant les types d'événements graves. Les définitions du modèle sont à la base des filtres simples. Vous pouvez créer des requêtes chargées de récupérer des événements sur la base des éléments que vous avez spécifiés pour la catégorie, la classe, l'action et le résultat de ces événements.

Pour identifier le filtre simple d'événements graves

1. Cliquez sur le lien Aide.
2. Développez Grammaire commune aux événements et sélectionnez Affectation du niveau de sécurité.
3. Copiez le tableau dans une feuille de calcul et triez le Niveau de sécurité du plus élevé au plus faible.

   Le tableau ainsi obtenu répertorie les types d'événement, en commençant par le plus grave, suivant le Niveau de sécurité CA attribué.

   Voici un exemple. Vos résultats refléteront les définitions CEG existantes.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Sécurité	Activité du système	Arrêt du système	Terminé	7

Catégorie	Classe	Action	Résultat	Niveau de sécurité
opérationnelle				
Sécurité opérationnelle	Activité du système	Arrêt du système	Echec	7
Gestion de la configuration	Gestion de la configuration	Erreur de configuration	Terminé	6
Accès aux données	Gestion des objets	Création d'un fichier de contrôle	Terminé	6
Sécurité de l'hôte	Activité antivirus	Erreur d'analyse	Terminé	6
Sécurité de l'hôte	Activité antivirus	Nettoyage de virus	Echec	6
Sécurité de l'hôte	Activité antivirus	Virus détecté	Terminé	6
Sécurité de l'hôte	Activité antivirus	Mise en quarantaine de virus	Echec	6
Sécurité de l'hôte	Activité IDS/IPS	Violation de signature	Terminé	6
Sécurité du réseau	Activité de violation de signature	Violation de signature	Terminé	6
Sécurité opérationnelle	Activité du système	Démarrage du système	Echec	6
Sécurité opérationnelle	Activité du journal de sécurité	Suppression du journal de sécurité	Terminé	6
Sécurité opérationnelle	Activité du journal de sécurité	Suppression du journal de sécurité	Echec	6
Accès au système	Activité d'authentification	Reprise d'authentification	Echec	6
Accès au système	Activité d'authentification	Démarrage d'authentification	Echec	6

Création d'une requête pour récupérer les événements graves uniquement

Vous pouvez créer une requête sans modèle si vous ne trouvez pas de requête prédéfinie capable de récupérer les types d'événement pour lesquels vous souhaitez être averti. Examinez les types d'événements graves suivants.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Sécurité de l'hôte	Activité antivirus	Mise en quarantaine de virus	Echec	6
Sécurité de l'hôte	Activité IDS/IPS	Violation de signature	Terminé	6
Sécurité du réseau	Activité de violation de signature	Violation de signature	Terminé	6

Exemple : Création d'une requête pour récupérer uniquement les événements d'échec de mise en quarantaine d'un virus

Imaginons, par exemple, que vous souhaitez être averti en cas d'échec de mise en quarantaine d'un virus. Il est possible que le mot quarantaine n'apparaisse pas dans la liste de requêtes. Dans un tel cas, vous pouvez créer la requête souhaitée et planifier une alerte pour l'exécuter.

Pour créer une requête chargée de récupérer les événements d'échec de mise en quarantaine d'un virus

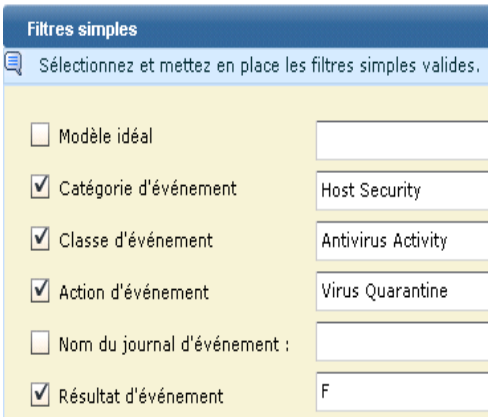
1. Cliquez sur Requêtes et rapports.
2. Sélectionnez Nouveau sous Options de la liste de requêtes.

   L'Assistant de conception de la requête s'ouvre sur l'étape Détails.
3. Saisissez un nom.

   Par exemple, Alerte : échec de mise en quarantaine d'un virus.
4. Entrez une balise personnalisée.

   Par exemple, entrez Mise en quarantaine de virus
5. Cliquez sur Colonnes de requêtes et ajoutez les colonnes de votre choix.
6. Cliquez sur l'étape Filtres de requête.
7. Entrez un filtre simple basé sur l'entrée CEG correspondant à l'événement.

   Par exemple, sélectionnez la catégorie Sécurité de l'hôte, la classe Activité antivirus, l'action Mise en quarantaine de virus et le résultat F (échec).



8. Sélectionnez l'étape Conditions de résultat, puis, dans la liste déroulante Plages prédéfinies, sélectionnez 5 dernières minutes afin d'être alerté en temps voulu.
9. Cliquez sur Enregistrer et fermer.

Personnalisation de requêtes pour récupérer les événements graves uniquement

Les requêtes prédéfinies qui ne sont pas marquées comme alertes d'action sont conçues pour les rapports. Il est normal que les rapports contiennent des données reflétant tous les types de sévérité d'événement. Vous pouvez personnaliser les requêtes sélectionnées afin qu'elles récupèrent uniquement les événements graves. Pour ce faire, vous devez identifier une requête chargée de récupérer des événements de sévérité variable, la copier, entrer des filtres indiquant de récupérer uniquement les événements graves, puis enregistrer la requête pour pouvoir la sélectionner avec une alerte.

Avant de commencer, ouvrez la feuille de calcul répertoriant les définitions des événements graves. Cet exemple est basé sur les informations CEG suivantes.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Sécurité opérationnelle	Activité du système	Arrêt du système	Terminé	7
Sécurité opérationnelle	Activité du système	Arrêt du système	Echec	7

La requête à personnaliser récupère les événements d'arrêt et de démarrage du système.

Pour personnaliser une requête afin qu'elle récupère uniquement les événements graves

1. Cliquez sur l'onglet Requêtes et rapports.
2. Sélectionnez un filtre de balise de requête correspondant à la catégorie de l'événement de cette sévérité.

   Par exemple, sélectionnez Sécurité opérationnelle.

3. Passez en revue la liste en recherchant les requêtes dont le nom contient les mots clés indiqués dans la classe ou l'action du type d'événement identifié.

   Par exemple, les mots clés Arrêt du système apparaissent dans la requête commençant par Démarrage ou arrêt du système par hôte.

4. Copiez la requête Détail du démarrage ou de l'arrêt du système par hôte. Mettez la requête en surbrillance et sélectionnez Copier dans la liste déroulante Options.
5. Cliquez sur Filtres de requête et comparez la valeur par défaut aux entrées du tableau pour le type d'événement de cette sévérité.

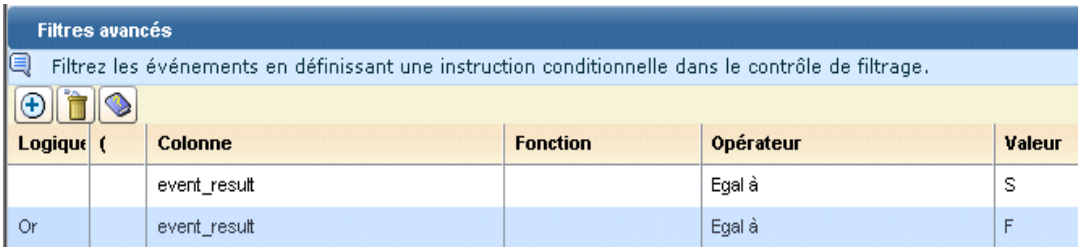
   Pour cette requête, seule Sécurité opérationnelle est sélectionnée.
6. Reportez-vous au tableau pour connaître les valeurs à saisir pour Classe et Action.

   Par exemple, sélectionnez la classe Activité du système et l'action Arrêt du système.

7. Sélectionnez l'onglet Filtres avancés pour déterminer si une modification est nécessaire.

   Supprimer chaque ligne car le filtre indiquant qu'event_action est égal à Arrêt ou Démarrage du système n'est pas pertinent pour cette requête personnalisée.
8. Remplacez-le par un filtre pour le résultat.

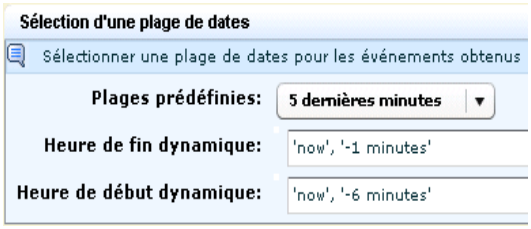
   Par exemple, créez un filtre où event_result est égal à échec ou réussite.



9. Cliquez sur Détails et spécifiez un nom pour la requête, indiquant explicitement que vous souhaitez l'utiliser pour une alerte.

   Par exemple, saisissez Alerte : détail de l'arrêt du système par hôte. Modifiez la description en fonction.
10. Cliquez sur Conditions de résultats. Pour les conditions graves, exécutez une requête fréquemment.

Par exemple, sélectionnez la plage prédéfinie des 5 dernières minutes afin de rechercher toutes les 5 minutes l'occurrence d'un événement de cette sévérité.



11. Cliquez sur Enregistrer.

    Vous pouvez créer une alerte avec cette requête, afin d'avertir un utilisateur, un processus ou un produit de la réussite ou de l'échec d'une tentative d'arrêt du système. La notification au produit s'effectue par le biais d'interruptions SNMP ; la notification des processus par une sortie d'événement/d'alerte CA IT PAM.

Modification des requêtes candidates

Vous pouvez modifier les requêtes prédéfinies sélectionnées afin de les utiliser avec des alertes. Pour personnaliser la requête, ajoutez un filtre simple basé sur l'analyse CEG. Dans la boîte de dialogue Sélection d'une plage de dates, dans la liste déroulante Plages prédéfinies, sélectionnez 5 dernières minutes afin d'être notifié immédiatement. Voici quelques exemples.

Requête d'erreur de configuration réussie

1. Copiez Détail de l'activité d'erreur de configuration.

   Cette requête renvoie aussi bien les réussites que les échecs. Toutefois, seules les réussites vous intéressent.

2. Définissez le filtre simple comme décrit ci-dessous.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Gestion de la configuration	Gestion de la configuration	Erreur de configuration	Terminé	6

3. Enregistrez sous Alerte : erreur de configuration réussie.

Requête de création réussie d'un fichier de contrôle

1. Copiez Détail de l'activité de manipulation des données.

   Cette requête récupère toutes les actions d'accès aux données.

2. Définissez le filtre simple comme décrit ci-dessous.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Accès aux données	Gestion des objets	Création d'un fichier de contrôle	Terminé	6

3. Enregistrez sous Alerte : création réussie d'un fichier de contrôle.

Requête d'échec de l'analyse antivirus

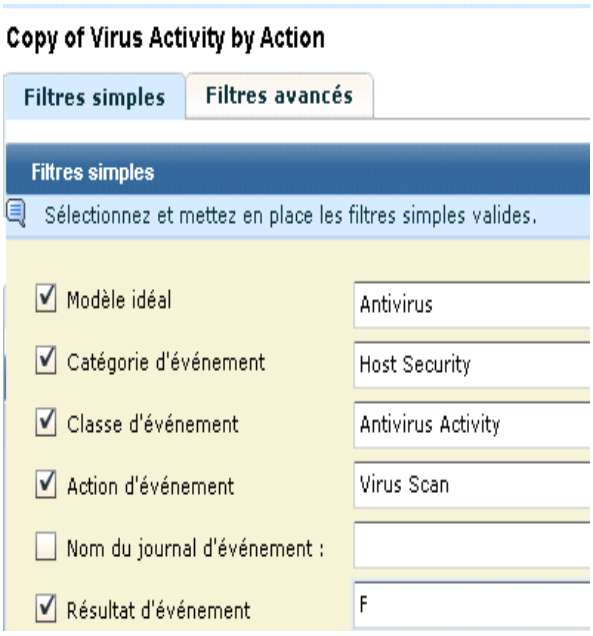
1. Copiez Activité virale par action

   Cette requête filtre toutes les actions antivirales pour la sécurité de l'hôte.

2. Aidez-vous de la définition suivante.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Sécurité de l'hôte	Activité antivirus	Erreur d'analyse	Terminé	6

3. Définissez le filtre simple comme suit.



4. Enregistrez sous Alerte : échec de l'analyse antivirus.

Requête d'échec du nettoyage des virus

Vous pouvez utiliser la requête prédéfinie Détail de l'activité de nettoyage ou de détection des virus pour récupérer les actions ayant réussi ou échoué. Cela peut vous suffire. Vous avez toutefois la possibilité de créer deux requêtes séparées basées sur cette requête où vous spécifiez le résultat conformément aux indications de la table CEG pour les événements graves.

1. Copiez Détail de l'activité de nettoyage ou de détection de virus.
2. Créez un filtre simple dans lequel vous spécifiez Echec comme résultat.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Sécurité de l'hôte	Activité antivirus	Nettoyage de virus	Echec	6

3. Supprimez le filtre avancé.
4. Enregistrez sous Alerte : échec du nettoyage des virus

Requête de détection d'un virus

Vous pouvez utiliser la requête prédéfinie Détail de l'activité de nettoyage ou de détection des virus pour récupérer les actions ayant réussi ou échoué. Cela peut vous suffire. Vous avez toutefois la possibilité de créer deux requêtes séparées basées sur cette requête où vous spécifiez le résultat conformément aux indications de la table CEG pour les événements graves.

1. Copiez Détail de l'activité de nettoyage ou de détection de virus.
2. Créez un filtre simple dans lequel vous spécifiez Opération réussie comme résultat, mais uniquement pour l'activité de détection.

Catégorie	Classe	Action	Résultat	Niveau de sécurité
Sécurité de l'hôte	Activité antivirus	Virus détecté	Terminé	6

3. Supprimez le filtre avancé.
4. Enregistrez sous Alerte : virus détecté.

Remarques sur les alertes d'action

Vous pouvez afficher les résultats de n'importe quelle alerte d'action de CA Enterprise Log Manager sans configuration particulière. Par ailleurs, une alerte d'action peut être envoyée aux destinations suivantes.

- Flux RSS
- Destinataires du courriel
- Destinations des interruptions SNMP, telles que CA Spectrum ou CA NSM
- Processus de sortie de l'événement/de l'alerte CA IT PAM

Les administrateurs configurent ces destinations à partir de l'onglet Administration, sous-onglet Services, sous Configuration globale ou Configuration globale du service (Serveur de rapports).

Veillez à ce que ces destinations soient configurées comme suit avant de tenter de planifier une alerte.

- Pour utiliser le lecteur de flux, vérifiez que la case à cocher "Pour afficher les alertes d'action, l'authentification est requise" est désélectionnée, dans la fenêtre Configuration globale.

  L'URL du flux RSS est la suivante, où *nomhôteelm* est le nom d'hôte du serveur CA Enterprise Log Manager.

  https://{*nomhôteelm*}:5250/spin/calm/getActionQueryRssFeeds.csp

- Pour envoyer des alertes à des destinataires de courriel, veillez à ce que la section Paramètres de messagerie soit configurée dans Configuration globale du service (Serveur de rapports).
- (Facultatif) Pour envoyer des alertes à des destinations SNMP, veillez à ce que la section Configuration SNMP soit configurée dans Configuration globale du service : Serveur de rapports.
- Pour envoyer des alertes au processus de sortie de l'événement/de l'alerte CA IT PAM, veillez à ce que la section CA IT PAM soit configurée dans Configuration globale du service (Serveur de rapports). La seule valeur qui n'est pas requise pour les alertes est celle pour le traitement des valeurs dynamiques.

Quand vous spécifiez des conditions de résultat pour une alerte d'action, pensez aux éléments suivants :

- Utilisez l'heure de début et l'heure de fin dynamiques préconfigurées pour les plages prédéfinies.
  - La plage prédéfinie, 5 dernières minutes, est paramétrée avec l'heure de fin définie sur Maintenant, -2 minutes, et l'heure de début sur Maintenant, -7 minutes. Cette plage prédéfinie et les autres plages horaires prédéfinies permettent la sauvegarde opportune des événements dans la base de données.

    Remarque : Ne modifiez pas l'heure de fin dynamique par *Maintenant* ou *Maintenant, - 1 minute*. Une telle modification de la valeur prédéfinie peut entraîner l'affichage de données incomplètes lors du lancement de l'URL à partir de la destination. Par exemple, si le nombre d'événements est l'une des valeurs, le nombre affiché, lors d'une consultation via l'URL, risque d'être inférieur à celui qui s'affiche dans CA Enterprise Log Manager.
- Prolongez l'heure de fin dynamique, si des données incomplètes s'affichent avec le paramètre par défaut. Par exemple, paramétrez-la sur Maintenant, -10 minutes

Lorsque vous créez une planification d'alerte d'action, prenez en compte les éléments suivants.

- L'intervalle de récurrence est la fréquence à laquelle la requête est exécutée. Par conséquent, un intervalle de récurrence de 5 minutes signifie que la requête est exécutée toutes les cinq minutes, ou 12 fois par heure. Une alerte d'action est générée seulement si la requête renvoie des résultats lors de son exécution.
- Définissez l'intervalle de récurrence en fonction du degré de priorité de votre réponse lorsque les conditions indiquées sont réunies.
  - Si vous devez entreprendre une action immédiate pour faire face à ces conditions, définissez l'intervalle de récurrence sur une fréquence élevée de manière à être averti le plus rapidement possible.
  - Si les conditions exigent un suivi, mais pas d'intervention immédiate, définissez l'intervalle sur une fréquence faible.
- Evitez de définir l'intervalle de récurrence sur une fréquence élevée, telles que toutes les cinq minutes, si l'heure de votre serveur CA Enterprise Log Manager n'est pas synchronisée avec votre serveur NTP.

  Important : L'heure de votre serveur CA Enterprise Log Manager doit être synchronisée avec votre serveur NTP afin de garantir le renvoi de résultats complets lorsque la requête est paramétrée pour s'exécuter à une fréquence élevée.

Prenez en compte les options de filtrage suivantes.

- Pour utiliser les filtres qui sont définis avec les requêtes incluses, aucune action n'est nécessaire.
- Pour appliquer des filtres supplémentaires aux requêtes incluses dans une alerte, définissez-les à l'étape Filtres d'alerte.
- Pour appliquer le même ensemble de filtres à plusieurs jobs d'alerte, utilisez un profil.

Avant de configurer les seuils d'alertes d'action pour un serveur de rapports CA Enterprise Log Manager, prenez en compte les éléments suivants.

- Pour que la taille du flux RSS reste raisonnable, définissez un nombre maximum d'alertes autorisé. Plus l'intervalle de récurrence des alertes activées est court, plus le flux se remplit vite si la ou les requêtes renvoient des résultats.
- Pour vous assurer que le flux RSS ne conserve pas les alertes plus longtemps que nécessaire, définissez la valeur de conservation d'alerte d'action sur l'âge maximum (en jours) de l'enregistrement le plus ancien à conserver.
- Choisissez à quelle fréquence vous souhaitez vérifier les alertes du flux RSS. Cette fréquence vous aide à décider combien de temps les enregistrements sont conservés.
- Si vous souhaitez que le flux RSS affiche en permanence les résultats les plus récents pour chaque job, configurez les valeurs de conservation de manière à ce que les alertes peu fréquentes ne soient pas supprimées du fait de leur antériorité par rapport aux alertes plus fréquentes qui sature la file d'attente.

Informations complémentaires :

Modification de configurations globales (page 143)
Configuration de la conservation d'alerte d'action (page 493)
Exemple : Création d'une alerte d'action pour un espace disque faible (page 481)

Utilisation de processus de sortie de l'événement/de l'alerte CA IT PAM

L'utilisation de processus de sortie de l'événement/de l'alerte CA IT PAM qui sont intégrés à CA Enterprise Log Manager implique une combinaison des tâches suivantes.

- Importation de l'exemple de processus de sortie de l'événement/de l'alerte
- Dans CA IT PAM, création des processus de sortie de l'événement/de l'alerte qui sont conformes aux conditions d'intégration
- Configuration de l'intégration de CA IT PAM et spécification du processus de sortie de l'événement/de l'alerte par défaut
- Exécution de processus de sortie de l'événement/de l'alerte à partir de résultats de requête sélectionnés
- Planification d'alertes qui exécutent un processus CA IT PAM par ligne
- Planification d'alertes qui exécutent un processus CA IT PAM par requête

Informations complémentaires :

Importation de l'exemple de processus de sortie de l'événement/de l'alerte (page 399)
Instructions pour la création d'un processus de sortie de l'événement/de l'alerte (page 406)
Configuration de l'intégration de CA IT PAM pour la sortie de l'événement/de l'alerte (page 414)
Exemple : Exécution d'un processus de sortie de l'événement/de l'alerte avec les résultats de requête sélectionnés (page 416)
Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par ligne (page 422)
Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par requête (page 427)

A propos des processus de sortie de l'événement/de l'alerte CA IT PAM

CA Enterprise Log Manager détecte les événements qui nécessitent une intervention. Vous pouvez générer des alertes dès que des événements indésirables se produisent. Grâce à l'intégration avec CA IT PAM, une alerte peut exécuter un processus de sortie de l'événement/de l'alerte. Les processus de sortie de l'événement/de l'alerte sont conçus pour invoquer des actions correctives appropriées par d'autres produits. En d'autres termes, les processus de sortie de l'événement/de l'alerte sont des processus CA IT PAM qui donnent l'ordre à d'autres produits d'effectuer des actions sur des objets donnés.

CA Enterprise Log Manager, CA IT PAM et les produits tiers fonctionnent conjointement pour protéger votre environnement. CA Enterprise Log Manager automatise la détection des événements indésirables et le processus de sortie de l'événement/de l'alerte CA IT PAM invoque d'autres produits pour qu'ils prennent la série de mesures appropriées.

L'intégration implique la configuration de la connexion au serveur CA IT PAM, la spécification du processus à exécuter, ainsi que des paramètres de processus avec les valeurs par défaut.

L'exécution du processus CA IT PAM peut être effectuée à la demande à partir d'un résultat (ligne) de requête affiché ou par le biais d'alertes planifiées. Dans les deux cas, les valeurs des paramètres telles que le récapitulatif et la description peuvent être adaptées pour fournir des détails de prise en charge au produit de destination du processus CA IT PAM.

Informations complémentaires :

Architecture prenant en charge l'intégration de CA IT PAM (page 392)
Processus d'utilisation des processus de sortie de l'événement/de l'alerte (page 392)
Fonctionnement de l'intégration de CA IT PAM (page 394)
Exemple : Flux de données pour le processus de sortie de l'événement/de l'alerte (page 397)

Architecture prenant en charge l'intégration de CA IT PAM

Vous devez disposer des composants réseau suivants pour exécuter un processus de sortie de l'événement/de l'alerte CA IT PAM à partir d'une alerte.

- Un environnement CA Enterprise Log Manager fonctionnel, par exemple :
  - Des agents avec des connecteurs qui capturent des événements bruts à partir de sources d'événement
  - Des serveurs de collecte CA Enterprise Log Manager qui ajustent les événements bruts et les envoient à des serveurs de rapports
  - Des serveurs de rapports CA Enterprise Log Manager qui traitent les alertes planifiées et les requêtes à la demande
- Un serveur CA IT PAM (Process Automation Manager) r2.1 configuré avec des processus qui invoquent un autre produit pour effectuer une action corrective.
- Un serveur avec un produit utilisé par le processus CA IT PAM, par exemple, un serveur avec un produit d'assistance.

Processus d'utilisation des processus de sortie de l'événement/de l'alerte

Voici une présentation du flux de travail pour l'utilisation d'un processus de sortie de l'événement/de l'alerte CA IT PAM.

1. Déterminez si vous devez configurer l'intégration de CA IT PAM avec ou sans l'exemple de processus. L'utilisation de l'exemple de processus présente l'avantage de vous permettre de découvrir immédiatement les résultats. Vous pouvez différer la mise à jour de votre propre processus jusqu'à ce que vous ayez assimilé les résultats de l'intégration. L'utilisation de l'exemple de processus nécessite CA Service Desk.
2. Effectuez l'une des actions suivantes ou les deux.
   - Importez l'exemple de processus et spécifiez les paramètres de connexion CA ServiceDesk.
   - Créez des processus de sortie de l'événement/de l'alerte qui répondent aux exigences de l'intégration de CA Enterprise Log Manager.
3. Rassemblez des détails pour l'intégration de CA IT PAM à partir de l'exemple de processus ou du processus que vous avez créé.
4. Configurez l'intégration de CA IT PAM pour la sortie de l'événement/de l'alerte.

5. Assurez-vous que les utilisateurs qui surveillent les résultats de processus de sortie de l'événement/de l'alerte au niveau du produit tiers disposent de comptes d'utilisateur dans CA Enterprise Log Manager et qu'ils connaissent les informations d'identification pour se connecter. Vous pouvez affecter le rôle Auditor à ces comptes.

   Remarque : Lorsque des utilisateurs se connectent, ils peuvent uniquement afficher la page avec les résultats de la requête associés.

6. Préparez-vous à automatiser l'exécution d'un processus de sortie de l'événement/de l'alerte.

   a. Identifiez la ou les requêtes qui renvoient des données sur lesquelles le produit tiers peut effectuer des actions conformément au processus CA IT PAM configuré.

   b. Si la requête utilise une liste à clés, veillez à ce que cette liste soit renseignée avec les valeurs dont vous avez besoin.

   c. Exécutez le processus de sortie de l'événement/de l'alerte sur les résultats de la requête et vérifiez que le processus s'exécute correctement.

7. Planifiez une alerte d'action à l'aide de la procédure indiquée et procédez comme suit.

   a. A l'étape Sélection d'alerte

      - Saisissez un nom de job.
      - Vérifiez que le type de sélection est Requêtes.
      - Sélectionnez la ou les requêtes que vous avez identifiées lors de la planification.

   b. A l'étape Destination, sélectionnez l'onglet Processus CA IT PAM et spécifiez les détails de sortie de l'événement/de l'alerte comme suit.

      - Sélectionnez les requêtes sur lesquelles vous souhaitez baser l'alerte.
      - Spécifiez si vous souhaitez exécuter le processus une fois par requête qui renvoie des résultats ou une fois par ligne renvoyée.
      - Spécifiez les valeurs des paramètres du processus CA IT PAM. Vous pouvez inclure des valeurs de champ et du texte pour les valeurs des paramètres Récapitulatif et Description uniquement si vous exécutez le processus par ligne.

   c. Spécifiez des détails pour les étapes restantes, comme pour toute alerte d'action que vous planifiez, puis enregistrez et fermez l'assistant.

8. Surveillez les résultats.

   a. Vérifiez que la liste Jobs d'alertes d'action inclut ce job.

   b. Surveillez les événements d'autosurveillance, l'action de notification d'événement, pour vérifier que le résultat de l'exécution du processus CA IT PAM est réussi.

   c. Connectez-vous au produit tiers qui a répondu aux informations de sortie de l'événement/de l'alerte provenant de CA Enterprise Log Manager, transmises à ce serveur par le processus CA IT PAM (facultatif).

Informations complémentaires :

Importation de l'exemple de processus de sortie de l'événement/de l'alerte (page 399)
Instructions pour la création d'un processus de sortie de l'événement/de l'alerte (page 406)
Configuration de l'intégration de CA IT PAM pour la sortie de l'événement/de l'alerte (page 414)
Exemple : Exécution d'un processus de sortie de l'événement/de l'alerte avec les résultats de requête sélectionnés (page 416)
Conception de requêtes pour les événements à envoyer au processus de sortie de l'événement/de l'alerte (page 420)
Définition de destinations des notifications (page 476)
Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par ligne (page 422)

Fonctionnement de l'intégration de CA IT PAM

Supposons la configuration suivante.

- Vous avez configuré CA IT PAM sur la page de configuration Serveur de rapports et spécifié le processus de sortie de l'événement/de l'alerte à exécuter.
- Vous avez planifié une alerte avec CA IT PAM comme destination et spécifié l'exécution du processus une fois par ligne. Pour les paramètres qui permettent la saisie d'instructions récapitulatives et descriptives, vous avez saisi des instructions qui incluaient des champs CEG.
- Vous avez planifié une autre alerte avec CA IT PAM comme destination et spécifié l'exécution du processus une fois par requête. Pour les paramètres qui permettent la saisie d'instructions récapitulatives et descriptives, vous avez saisi du texte littéral.

Le processus de bout en bout implique des actions par plusieurs sources.

- Génération d'événements bruts par des sources d'événement
- Collecte et ajustement d'événements par CA Enterprise Log Manager
- Génération d'alertes lorsque des événements ajustés répondent aux critères de requête par CA Enterprise Log Manager
- Envoi de sortie de l'événement et de l'alerte par CA Enterprise Log Manager à CA IT PAM
- Exécution du processus de sortie de l'événement/de l'alerte configuré par CA IT PAM sur un système tiers
- L'une des solutions suivantes :
  - Evaluation des données par un utilisateur du système tiers qui détermine l'action correcte et l'effectue
  - Réponse automatisée de ce système tiers lorsque les événements se produisent

Vous trouverez ci-dessous un récapitulatif du traitement.

1. Les sources d'événement génèrent des événements bruts.
2. Les agents collectent certains de ces événements bruts en fonction de leurs connecteurs et transfèrent les événements bruts à un serveur de collecte.
3. Le serveur de collecte normalise et classe les événements bruts, puis transfère les événements ajustés à un serveur de rapports.

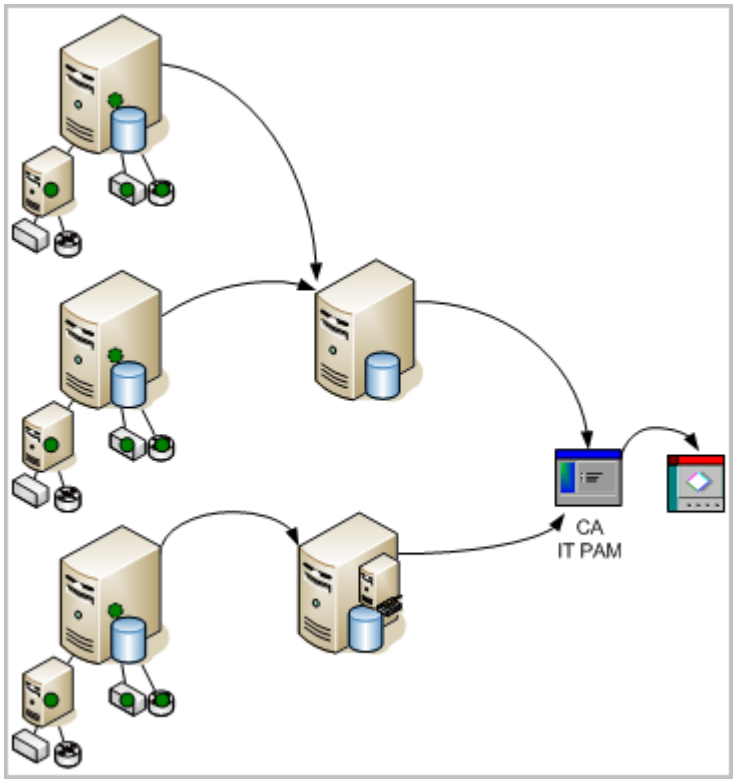
   Par exemple, lorsqu'un changement de configuration est effectué sur un système, un journal est créé et classé comme changement de configuration. L'événement capture l'heure du changement, l'hôte sur lequel ce changement a été apporté, l'utilisateur qui l'a effectué, ainsi que le résultat de la tentative de changement.
4. Le serveur de rapports exécute les requêtes sélectionnées pour chaque alerte planifiée.

5. Lorsque des événements ajustés répondent aux critères de requête, le serveur de rapports génère une alerte et transfère les informations suivantes à CA IT PAM.
   - Détails de l'alerte
     - Paramètres de processus affichés et leurs valeurs
     - Champs CEG envoyés pour les paramètres de processus non affichés
   - Détails de l'événement
     - Pour l'exécution par ligne, les détails de l'événement sont transmis par les entrées dans les champs disponibles pour les instructions récapitulatives et descriptives, où les utilisateurs décrivent l'événement avec les variables de champ CEG composant la requête sélectionnée pour l'alerte.
     - Pour l'exécution par requête, les détails de l'événement sont transmis avec une URL à une page CA Enterprise Log Manager qui affiche les détails de l'événement au niveau de la ligne.
6. En cas de réussite de l'envoi, CA IT PAM continue le traitement tel qu'il est défini dans le processus de sortie de l'événement/de l'alerte configuré.
7. Si le produit tiers est CA Service Desk et que le processus est le processus de sortie de l'événement/de l'alerte, les événements suivants se produisent.
   - Un ticket d'assistance est ouvert et un numéro lui est affecté. Les champs du ticket sont remplis avec les valeurs de paramètre de la définition d'alerte. Si l'utilisateur reçoit une URL, celle-ci est affichée avec l'instruction récapitulative.
   - CA Service Desk renvoie le numéro du ticket à CA IT PAM.
8. CA IT PAM retransmet le numéro du ticket à CA Enterprise Log Manager.
9. CA Enterprise Log Manager affiche le numéro du ticket en tant qu'événement d'autosurveillance.

Exemple : Flux de données pour le processus de sortie de l'événement/de l'alerte

Les flèches sur le diagramme suivant illustrent le flux de données.

- Des serveurs de collecte vers des serveurs de rapports
- Des serveurs de rapports vers CA IT PAM
- De CA IT PAM vers le produit auquel le processus CA IT PAM envoie la sortie CA Enterprise Log Manager, par exemple, CA Service Desk

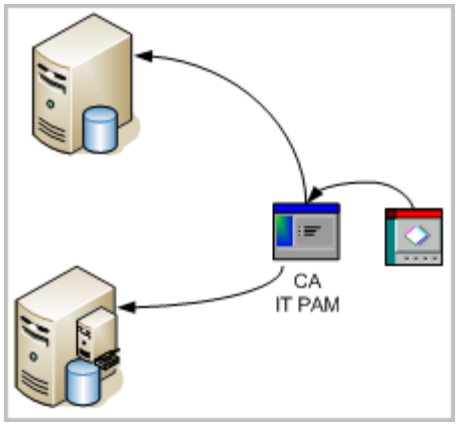


Lorsque CA Enterprise Log Manager est averti de la réussite de l'envoi, il interroge CA IT PAM pour connaître l'état du processus exécuté. Dès que CA IT PAM envoie la mise à jour de l'état, CA Enterprise Log Manager crée un événement d'autosurveillance avec le résultat. Voici la séquence de traitement.

1. CA IT PAM avertit CA Enterprise Log Manager de la réussite ou de l'échec du processus exécuté.
2. CA Enterprise Log Manager génère un événement d'autosurveillance de création de notification avec le résultat reçu.

Examinez l'exemple où le processus CA IT PAM crée un ticket d'assistance avec les valeurs des paramètres du processus et les données d'événement récupérées par la requête. Les flèches sur le diagramme ci-dessous illustrent les flux de données suivants.

- Du produit d'assistance vers CA IT PAM
- De CA IT PAM vers les serveurs de rapports CA Enterprise Log Manager sources



Importation de l'exemple de processus de sortie de l'événement/de l'alerte

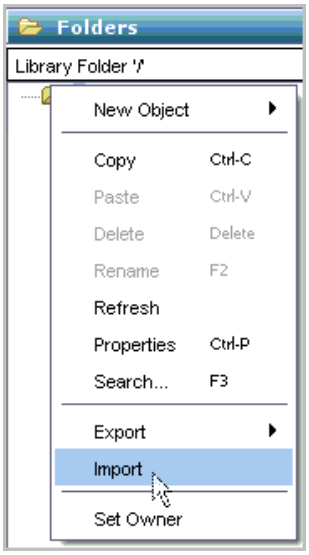
Pour vous permettre de tester immédiatement l'intégration de CA IT PAM et de vous exercer avec la procédure de configuration avec des valeurs connues, CA fournit un exemple de processus à cette fin. Il se trouve sur le DVD avec l'application. L'utilisation de cet exemple de processus CA IT PAM suppose que vous utilisiez CA Service Desk comme application d'assistance.

Vous pouvez ensuite configurer CA IT PAM dans CA Enterprise Log Manager et tester l'exécution de cet exemple de processus CA IT PAM avec les résultats de la requête que vous avez sélectionnés. Une fois que vous vous êtes familiarisé avec le fonctionnement de CA Enterprise Log Manager avec CA IT PAM, vous pouvez vous assurer de la conformité de votre propre processus et remplacer les valeurs dans la configuration CA IT PAM pour l'intégration de votre production.

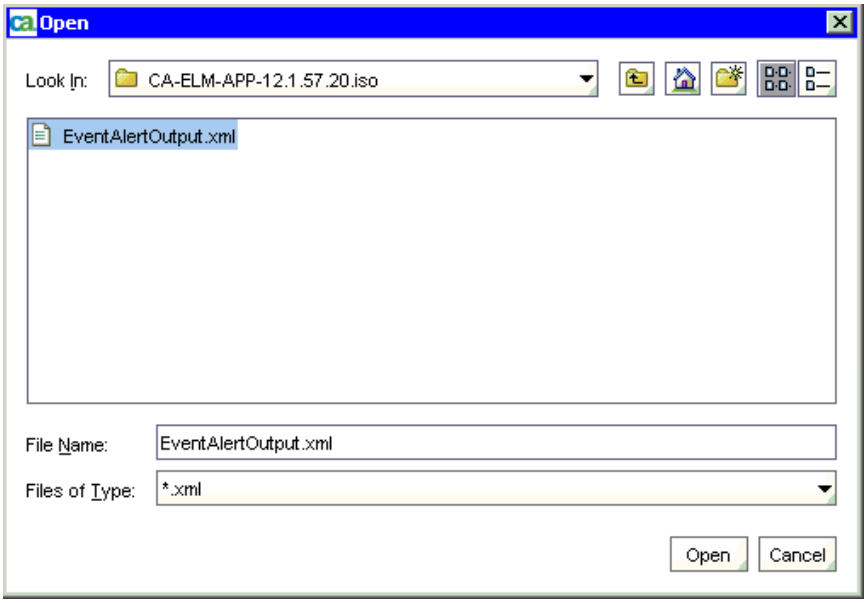
Pour importer un exemple de processus et tester l'intégration de CA IT PAM

1. Lancez CA IT PAM et connectez-vous.
2. Lancez le client CA IT PAM.

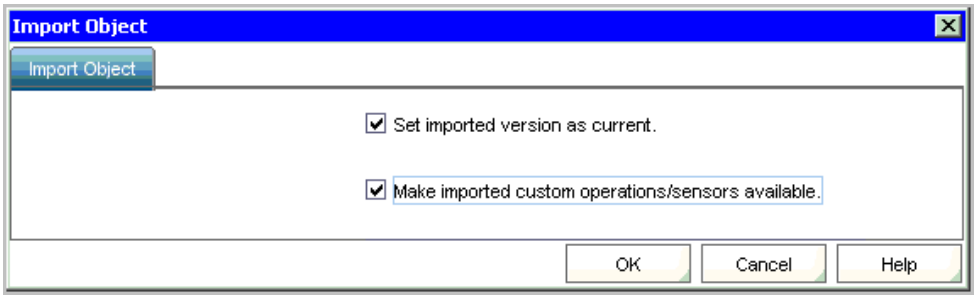
3. Importez l'exemple de processus CA IT PAM, EventAlertOutput.xml, fourni sur le DVD de l'application sous CA/IT PAM. Dans cet exemple, toutes les valeurs requises sont définies.
   a. Sélectionnez Fichier, Ouvrir le navigateur de la bibliothèque.
   b. Cliquez sur Dossiers dans le volet gauche, puis au niveau du dossier racine, cliquez sur Importer.



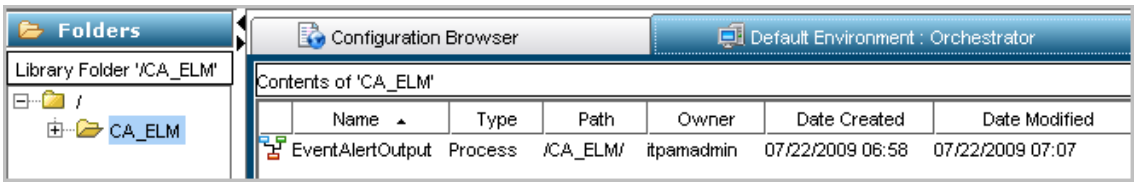
c. Sélectionnez l'exemple de processus CA IT PAM, EventAlertOutput.xml, dans l'image ISO extraite avant de cliquer sur Ouvrir.



d. Dans la boîte de dialogue Importer l'objet, sélectionnez les deux options et cliquez sur OK.



L'affichage obtenu indique le nom et le chemin d'accès exacts. Par exemple, le nom est EventAlertOutput et le chemin /CA_ELM/.



4. Spécifiez les paramètres de connexion Service Desk.
   a. Cliquez sur l'onglet Paramètres de connexion ServiceDesk pour Request_Create afin d'afficher les paramètres de connexion ServiceDesk.
   b. Utilisez la syntaxe suivante pour spécifier l'URL de Service Desk.

      "http://<nom du serveur>:8080/axis/services/USD_R11_WebService"

   c. Entrez un ID d'utilisateur et un mot de passe Service Desk valides.
5. Testez le processus importé pour vous assurer qu'il fonctionne comme processus autonome (facultatif).
6. Fermez le client CA IT PAM, puis cliquez sur Se déconnecter pour quitter CA IT PAM.

Affichage de l'exemple de processus de sortie de l'événement/de l'alerte

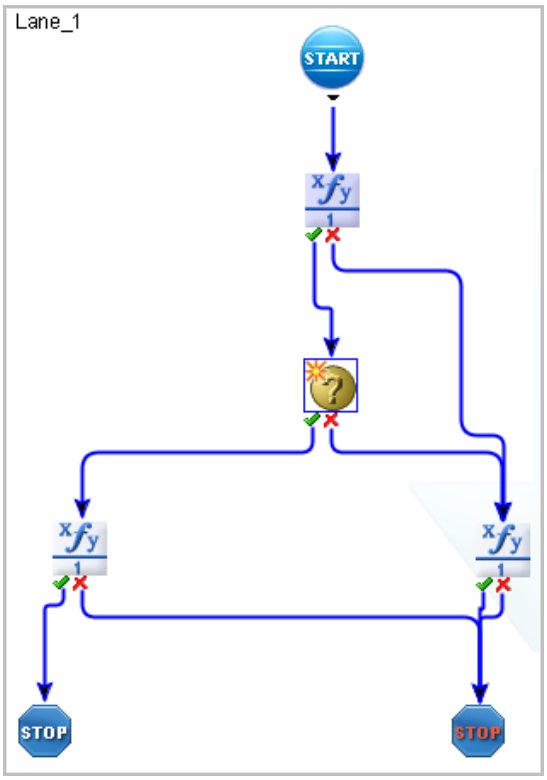
Si vous importez l'exemple de processus de sortie de l'événement/de l'alerte, vous pouvez examiner sa conception dans CA IT PAM. Suivez les instructions ci-dessous pour vous familiariser avec les conditions de CA Enterprise Log Manager dans le contexte de l'exemple de processus. Lors de cette présentation, vous découvrirez à quel endroit définir les paramètres de connexion au service Web et de quelle manière les opérateurs de calcul sont définis. En outre, vous noterez les conditions spécifiques aux produits. Par exemple, la configuration de CA Service Desk en tant que produit tiers nécessite l'utilisation de l'opérateur Request_Create à partir du module CA Service Desk et d'un opérateur de précalcul qui maintient les valeurs de sévérité et de priorité.

Pour vous familiariser avec l'exemple de processus de sortie de l'événement/de l'alerte

1. Affichez le modèle de votre processus cible.
   a. Lancez CA IT PAM et connectez-vous.
   b. Cliquez sur Client CA IT PAM.
   c. Dans le menu Fichier, sélectionnez Ouvrir le navigateur de la bibliothèque.
   d. Dans l'onglet Dossiers, sélectionnez le dossier de bibliothèque contenant le modèle de votre processus cible.

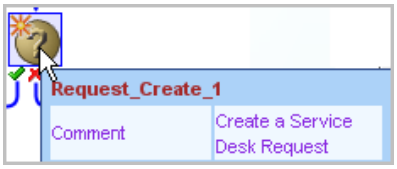
      Le nom de votre processus et le chemin d'accès apparaissent dans le volet principal.
   e. Double-cliquez sur la ligne contenant le chemin d'accès et le nom de votre processus.

Un modèle similaire au modèle suivant apparaît. Cet exemple de modèle contient les conditions minimales requises pour CA Enterprise Log Manager.



2. Notez de quelle manière les paramètres de base ServiceDesk se conforment aux conditions de CA Enterprise Log Manager.

   a. Double-cliquez sur l'icône Request_Create_1.

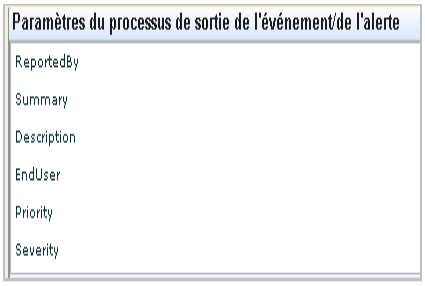


   L'opérateur Request_Create transmet les données renvoyées par la requête d'alerte d'action à votre produit cible (application). Un opérateur similaire est requis pour tout processus devant être exécuté à partir de CA Enterprise Log Manager.

b. Sous Paramètres de base ServiceDesk, notez que les paramètres de processus locaux sont spécifiés avec la syntaxe suivante.

BasicParameter = Process.LocalParameter

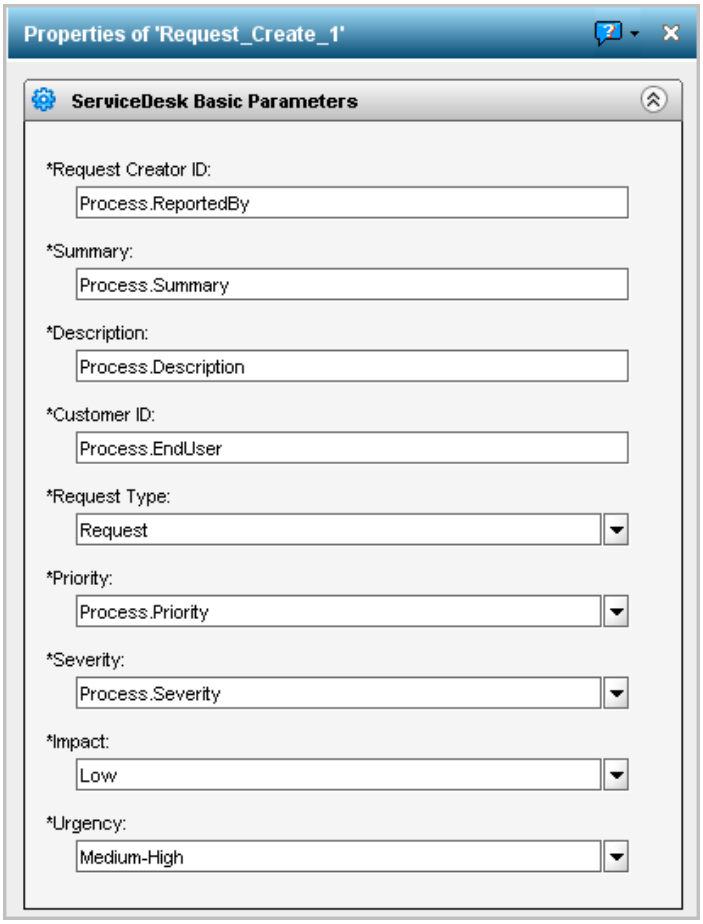
Remarque : Les paramètres de processus locaux sont les paramètres de processus de sortie de l'événement/de l'alerte que vous ajoutez à CA Enterprise Log Manager lorsque vous configurez CA IT PAM.



c. Etant donné que l'application cible est le produit CA Service Desk, les paramètres de processus locaux suivants sont définis comme indiqué dans le tableau ci-dessous.

Paramètre de base ServiceDesk	Paramètre local	Champ Service Desk	Remarques
ID de créateur de demande	Process.ReportedBy	Assignee,Reported By	"Contact" valide dans CA Service Desk
Résumé	Process.Summary	Résumé	(Laisser vide)
Description	Process.Description	Description	(Laisser vide)
ID client	Process.EndUser	Utilisateur final concerné	"Contact" valide dans CA Service Desk
Priorité	Process.Priority	Priorité	1-5
Severity	Process.Severity	Severity	1-5

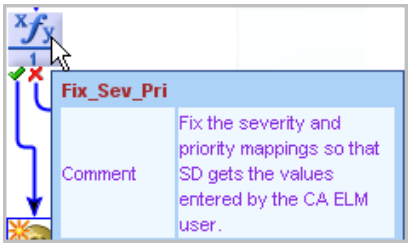
L'exemple suivant illustre les paramètres locaux valides pour les paramètres de base ServiceDesk. Les entrées sont sensibles à la casse. Vous devez saisir Process.ReportedBy, par exemple, exactement comme indiqué, avec un "R" majuscule et un "B" majuscule.



3. Cliquez sur l'onglet Paramètres de connexion ServiceDesk pour Request_Create afin d'afficher les paramètres de connexion ServiceDesk.
   - URL de Service Desk :"http://<nom du serveur>:8080/axis/services/USD_R11_WebService"
   - ID d'utilisateur de Service Desk :"<utilisateur SD>"
   - Mot de passe :"<mot de passe SD>"

4. Notez que pour CA Service Desk, un ajustement est nécessaire pour veiller à ce que les valeurs de sévérité et de priorité entrées dans CA Enterprise Log Manager soient correctement interprétées par CA Service Desk.

   a. Un opérateur de précalcul apparaît après Démarrer et avant l'opérateur Create_Process. Dans l'exemple suivant, il est nommé Fix_Sev_Pri.



   b. Dans Propriétés > Calculer, les mappages suivants sont définis.

```
if (Process.Priority == 1) Process.Priority = "pri:504";
else if (Process.Priority == 2) Process.Priority = "pri:503";
else if (Process.Priority == 3) Process.Priority = "pri:502";
else if (Process.Priority == 4) Process.Priority = "pri:501";
else if (Process.Priority == 5) Process.Priority = "pri:500";

if (Process.Severity == 1) Process.Severity = "sev:800";
else if (Process.Severity == 2) Process.Severity = "sev:801";
else if (Process.Severity == 3) Process.Severity = "sev:802";
else if (Process.Severity == 4) Process.Severity = "sev:803";
else if (Process.Severity == 5) Process.Severity = "sev:804";
```

5. Notez que les paramètres de valeur renvoyée, ou interface de sortie, suivants sont formatés conformément aux conditions de CA Enterprise Log Manager.

   - ResultString
   - FaultString

6. Affichez l'opérateur de calcul pour l'opération réussie de création de demande. Ce format doit être utilisé dans tout processus de sortie de l'événement/de l'alerte à exécuter à partir de CA Enterprise Log Manager.

   a. Cliquez sur l'icône de l'opérateur de calcul pour l'opération réussie de création de demande.

   b. Sélectionnez l'onglet Calculer et cliquez sur ... dans le champ de code source.

   c. Notez la définition de l'opérateur de calcul d'opération réussie dans le code source.

```
Process.ResultString = "Request " + Request_Create_1.newRequestNumber + " created in CA Service Desk.";
```

7. Affichez l'opérateur de calcul d'échec. Ce format est requis pour tout processus de sortie de l'événement/de l'alerte à exécuter à partir de CA Enterprise Log Manager.
   a. Cliquez sur l'icône de l'opérateur de calcul d'échec.
   b. Sélectionnez l'onglet Calculer et cliquez sur ... dans le champ de code source.
   c. Notez la définition de l'opérateur de calcul d'échec dans le code source, où Process.FaultString est mis en correspondance avec la variable SOAP appropriée.

      ```
      Process.FaultString = Request_Create_1.SoapErrorResponse;
      ```

Instructions pour la création d'un processus de sortie de l'événement/de l'alerte

Vous devez respecter certaines instructions pour pouvoir exécuter un processus CA IT PAM dans CA Enterprise Log Manager. Avant d'exécuter un processus CA IT PAM dans CA Enterprise Log Manager, vérifiez que celui-ci contient les éléments suivants :

- Les paramètres de connexion au service Web.
- Un opérateur de calcul Opération réussie qui mappe Process:ResultString vers une instruction, avec des symboles littéraux et des variables, qui exprime la réponse du produit tiers.
- Un opérateur de calcul Echec qui mappe Process:FaultString vers la variable de réponse SOAP appropriée.

Si votre processus CA IT PAM cible est destiné à un produit d'assistance tiers, vérifiez qu'il contient les éléments suivants :

- L'opérateur spécifique au produit.

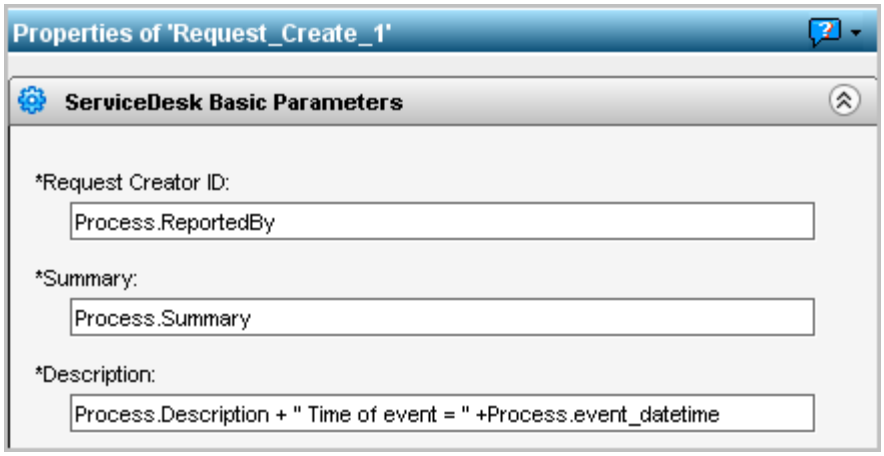
  Par exemple, un processus qui cible le module BMC Remedy serait défini avec l'opérateur Create_Help_Desk_Case.
- Les paramètres spécifiques au produit mappés vers les paramètres de processus locaux : ReportedBy, Summary, Description, EndUser, Priority et Severity.

  Par exemple, un processus ciblant le module BMC Remedy mapperait les paramètres locaux vers les paramètres HelpDesk Create Case.

En général, un processus CA IT PAM inclut uniquement les paramètres de processus par défaut, qui sont individuellement mappés vers un champ du produit tiers. Vous pouvez également ajouter des champs CEG comme paramètres pour un processus donné. L'exemple suivant indique les champs CEG de l'ensemble de données :

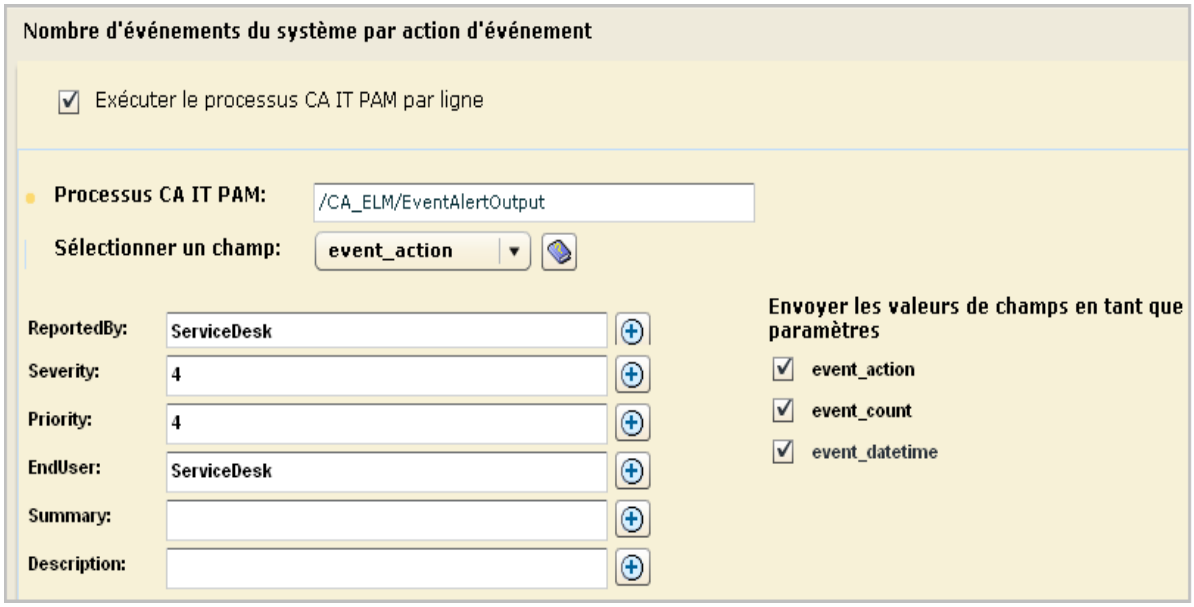
- event_severity
- event_count
- event_datetime

Chaque paramètre de base est mappé vers un champ Service Desk. Par exemple, le paramètre du processus ReportedBy est mappé vers le champ CA Service Desk intitulé Destinataire. Lorsque des champs CEG sont ajoutés comme paramètres de processus, ils peuvent être référencés comme des valeurs d'un paramètre de base. Par exemple, vous pouvez définir la valeur du champ CEG event_datetime de sorte qu'elle s'affiche par défaut dans le champ Description de CA Service Desk. Pour y parvenir, ajoutez le paramètre Process.event_datetime dans le champ Description des paramètres de base de Service Desk.

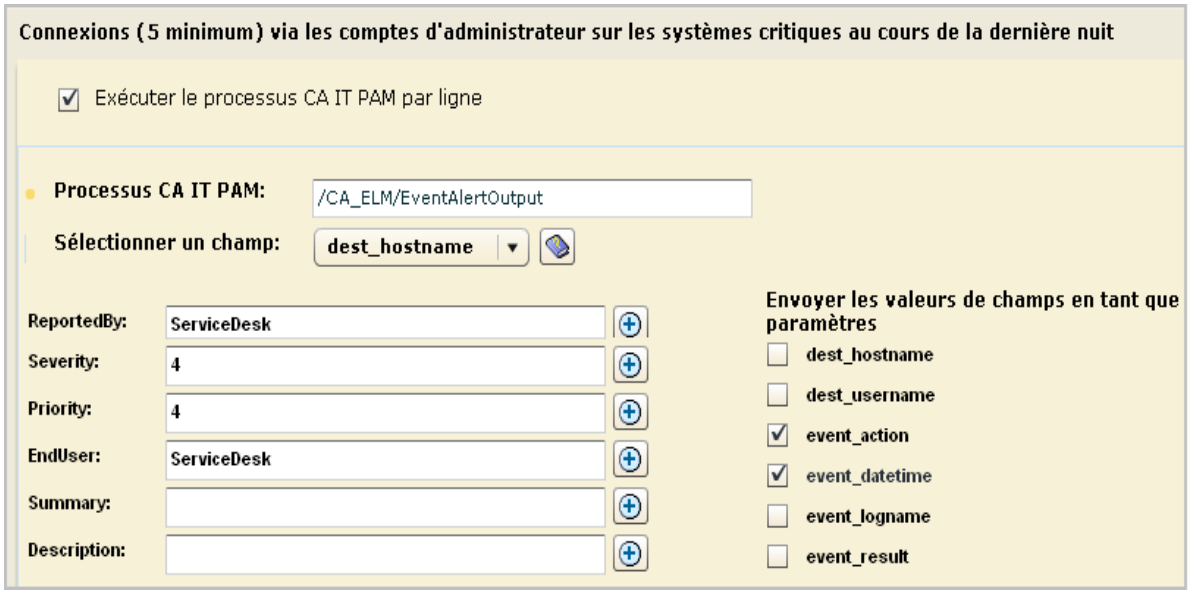


Lorsque vous créez une alerte qui exécute ce processus, examinez les champs CEG répertoriés dans Envoyer les valeurs de champs en tant que paramètres. Si un paramètre répertorié est un champ CEG que vous avez défini comme paramètre de processus, sélectionnez ce champ. Etudiez les exemples ci-après.

- Les trois champs CEG définis dans l'ensemble de données s'affichent pour la requête Nombre d'événements du système par action d'événement. Par conséquent, vous pouvez sélectionnez les trois champs à envoyer en tant que paramètres à CA IT PAM.



- Deux des trois champs CEG définis dans l'ensemble de données s'affichent pour la requête Connexions (5 minimum) via les comptes d'administrateur. Vous pouvez sélectionnez ces deux champs à envoyer en tant que paramètres à CA IT PAM.



Informations complémentaires :

Affichage de l'exemple de processus de sortie de l'événement/de l'alerte (page 401)

Collecte de détails pour l'intégration de CA IT PAM

La plupart des détails requis pour l'intégration de CA IT PAM font partie du produit CA IT PAM et des configurations du processus. Vous pouvez lancer CA IT PAM et rechercher les détails nécessaires pour la configuration. Vous pouvez également commencer par collecter les détails, les enregistrer, puis configurer rapidement CA IT PAM en entrant les valeurs enregistrées.

Vous pouvez référencer les exemples de processus que vous avez importés ou vos propres processus que vous avez modifiés pour vous conformer aux conditions de CA Enterprise Log Manager.

Pour collecter des détails pour l'intégration de CA IT PAM

1. Connectez-vous à votre serveur CA IT PAM local et vérifiez qu'il s'agit bien de CA IT Process Automation Manager 2.1.
2. Cliquez sur le lien Client CA IT PAM.

3. Collectez des détails pour les quatre premiers champs de la configuration CA IT PAM.
   a. Cliquez sur Navigateur de configuration.
   b. Cliquez sur l'onglet Propriétés.
   c. Enregistrez la valeur Nom du serveur comme votre valeur pour le serveur CA IT PAM.
   d. Acceptez le port 8080 comme port CA IT PAM.
   e. Demandez à l'administrateur CA IT PAM les informations d'identification pour CA Enterprise Log Manager et enregistrez-les pour Nom d'utilisateur et Mot de passe.

Champ Configuration IT PAM	Description	Votre valeur
Serveur CA IT PAM	Nom de domaine complet du serveur sur lequel est installé CA IT PAM. Cette valeur apparaît dans le champ Nom du serveur de l'onglet Propriétés du navigateur de configuration.	
Port CA IT PAM	Le port par défaut est 8080. Cette valeur apparaît dans le champ URL de domaine de l'onglet Propriétés du navigateur de configuration.	8080
Nom d'utilisateur	ID d'utilisateur que CA Enterprise Log Manager doit utiliser pour se connecter à CA IT PAM et exécuter un processus. Demandez-le à votre administrateur CA IT PAM. Exemple : itpamadmin	
Mot de passe	Mot de passe associé au nom d'utilisateur. Demandez-le à votre administrateur CA IT PAM.	

4. Enregistrez le chemin d'accès du processus et les noms des processus que vous envisagez d'exécuter à partir de CA Enterprise Log Manager.
   a. Dans le menu Fichier du client CA IT PAM, sélectionnez Ouvrir le navigateur de la bibliothèque.
   b. Dans l'onglet Dossiers, sélectionnez le dossier de bibliothèque contenant le processus de sortie de l'événement/de l'alerte.
   c. Enregistrez le chemin d'accès et le nom du processus de sortie de l'événement/de l'alerte.
   d. En cas de différence, sélectionnez le dossier de bibliothèque contenant le processus qui renvoie des valeurs actuelles pour une clé spécifiée.
   e. Enregistrez le chemin d'accès et le nom du traitement des valeurs dynamiques.

Champ spécifique au processus CA IT PAM	Description et exemple	Votre valeur
Processus de sortie de l'événement/de l'alerte	Chemin d'accès et nom de fichier Identifie le processus conçu pour transmettre les détails configurés avec l'alerte ou une URL à un produit externe tel que CA Service Desk. Exemple : /CA_ELM/EventAlertOutput	
Traitement des valeurs dynamiques	Chemin d'accès et nom de fichier Identifie le processus conçu pour collecter des valeurs pour la clé d'entrée et les renvoyer pour analyse dans un fichier CSV. Exemple : /CA_ELM/ValuesList	

5. Collectez des paramètres du processus de sortie de l'événement/de l'alerte.
   a. Double-cliquez sur le processus de sortie de l'événement/de l'alerte que vous avez référencé pour ouvrir le processus.
   b. Sur l'onglet Editeur principal, cliquez sur l'icône Request_Create pour afficher les propriétés.
   c. Affichez les Paramètres de base ServiceDesk.
   d. Enregistrez les paramètres comportant le préfixe Process: dans la première colonne ci-dessous s'ils ne correspondent pas exactement à ce qui est affiché.
   e. Cliquez sur l'onglet Jeu de données.
   f. Cliquez sur chaque paramètre pour Local_Dataset et enregistrez sa valeur par défaut le cas échéant.

Paramètres du processus de sortie de l'événement/de l'alerte	**Description et exemple**	**Votre valeur**
ReportedBy	Identifie l'utilisateur ServiceDesk par défaut. Exemple : ServiceDesk	
Résumé	Laisser vide	---
Description	Laisser vide	---
EndUser	Laissez ce champ vide afin de pouvoir le configurer en fonction de l'alerte ou entrez un nom d'espace réservé. Exemple : ServiceDesk	
Priorité	Définit la priorité par défaut. Si aucune valeur par défaut n'est configurée, enregistrez une valeur comprise entre 1 et 5. Exemple : 3	
Severity	Définit la sévérité par défaut. Si aucune valeur par défaut n'est configurée, enregistrez une valeur comprise entre 1 et 5. Exemple : 4	

Configuration de l'intégration de CA IT PAM pour la sortie de l'événement/de l'alerte

Vous pouvez configurer l'intégration de CA IT PAM pour utiliser l'un des types de processus CA IT PAM suivants ou les deux.

- Processus de sortie de l'événement/de l'alerte : processus qui invoque le traitement sur un système tiers
- Traitement des valeurs dynamiques : processus qui accepte une clé d'entrée et renvoie des valeurs actuelles pour cette clé sous la forme d'un fichier de valeurs séparées par une virgule (*.csv)

La procédure suivante traite à la fois les paramètres communs et les paramètres spécifiques à la sortie de l'événement/de l'alerte. Reportez-vous aux détails que vous avez enregistrés lors de la configuration de l'intégration de CA IT PAM pour la sortie de l'événement/de l'alerte.

Pour configurer l'intégration de CA IT PAM pour le processus de sortie de l'événement/de l'alerte

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   La fenêtre Configuration globale de service (Serveur de rapports) s'affiche.
3. Faites défiler jusqu'à la zone CA IT PAM.
4. Saisissez le nom d'hôte complet du serveur sur lequel est installé CA IT PAM, acceptez le numéro de port par défaut, 8080, puis saisissez des informations d'identification de connexion valides pour CA IT PAM.
5. Si vous avez importé l'exemple EventAlertOutput.xml pour utilisation, acceptez l'entrée par défaut pour le processus de sortie de l'événement/de l'alerte. Dans le cas contraire, remplacez cette entrée par votre nom de processus de sortie de l'événement/de l'alerte personnalisé, précédé par son chemin d'accès.

   Remarque : Vous pouvez afficher le Nom et le Chemin d'accès du processus sous Dossiers dans le client CA IT PAM.

6. Si vous avez importé l'exemple EventAlertOutput.xml pour utilisation, définissez les valeurs par défaut pour ReportedBy, Severity, Priority et EndUser comme suit.

   a. Sélectionnez un paramètre et cliquez sur Ajouter une valeur par défaut.

      La boîte de dialogue Ajouter une valeur apparaît.

   b. Entrez la valeur par défaut et cliquez sur OK.

   Remarque : Les valeurs par défaut ne sont pas requises pour Summary et Description.

7. Si vous avez spécifié un processus de sortie de l'événement/de l'alerte personnalisé, supprimez les paramètres affichés et ajoutez les vôtres. Définissez ensuite la valeur par défaut de chacun.

8. Cliquez sur Enregistrer.

   Le message suivant apparaît : "Confirmation : Les changements de configuration ont été enregistrés".

Informations complémentaires :

Collecte de détails pour l'intégration de CA IT PAM (page 410)

Exemple : Exécution d'un processus de sortie de l'événement/de l'alerte avec les résultats de requête sélectionnés

Tous les utilisateurs sont autorisés à exécuter un processus CA IT PAM à la demande. Vous pouvez exécuter le processus de sortie de l'événement/de l'alerte CA IT PAM configuré avec les résultats de la requête sélectionnés pour l'un des objectifs suivants.

- Effectuer un processus de sortie de l'événement/de l'alerte à la demande en fonction des besoins actuels.
- Tester les résultats du traitement avant de créer une alerte planifiée pour cette requête avec le processus CA IT PAM comme destination.

Vous pouvez exécuter un processus CA IT PAM à partir d'une ligne de résultat de la requête affichée. Cela suppose que les résultats soient affichés sous la forme d'un tableau plutôt que d'un graphique. Vous pouvez afficher les lignes de résultat de la requête de l'une des manières suivantes.

- Sélectionnez une requête dans la liste de requêtes qui renvoie les résultats.
- Sélectionnez un rapport dans la liste de rapports, sélectionnez une requête qui renvoie des résultats.
- Entrez une invite qui renvoie des résultats.

Remarque : La rubrique suivante suppose qu'une ligne de résultat de la requête apparaît lorsque vous sélectionnez la requête dans la liste de requêtes.

Pour vous familiariser avec le type de données renvoyées pour les champs CEG, consultez le manuel de *référence traitant de la grammaire commune aux événements* dans l'aide en ligne.

Pour exécuter le processus CA IT PAM configuré manuellement en fonction d'une ligne de résultat de la requête affichée

1. Cliquez sur l'onglet Requêtes et rapports et sur le sous-onglet Requêtes.

   Le filtre de balise de requête et la liste de requêtes s'affichent.

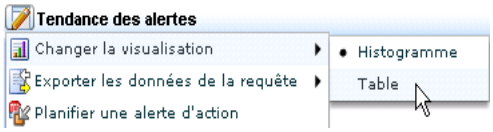
2. Saisissez des critères de recherche, tels que des comptes par défaut, dans la liste de requêtes (facultatif).

   Les événements qui reflètent des connexions par les comptes par défaut sont d'excellents candidats pour le transfert de votre processus de sortie de l'événement/de l'alerte CA IT PAM.

3. Sélectionnez la requête dans la liste de requêtes pour laquelle vous souhaitez afficher les résultats.

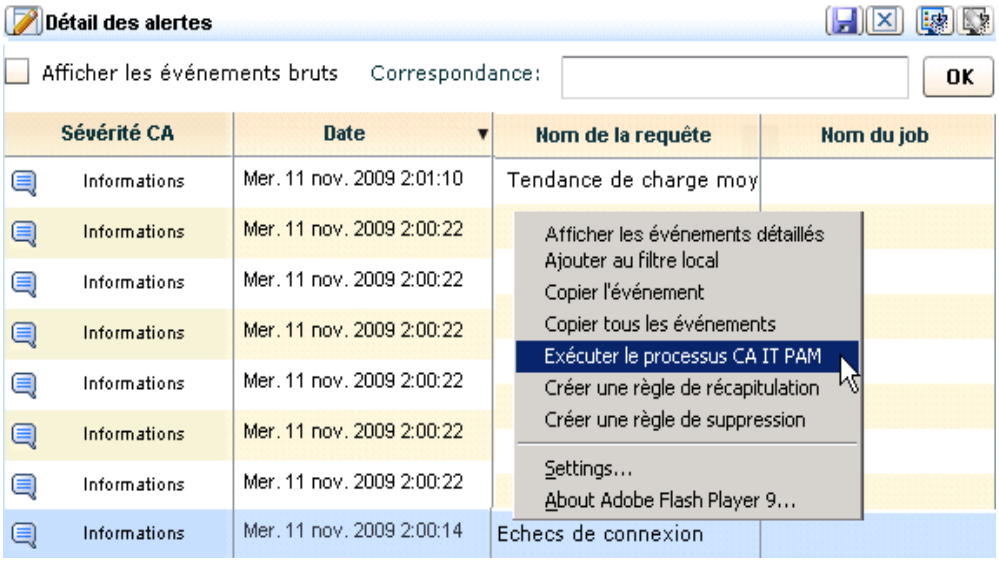
   Vous pouvez également afficher le sous-onglet Rapports, sélectionner une option dans la liste de rapports, afficher uniquement la requête et sélectionner la requête à partir de cet affichage.

4. Si les résultats s'affichent dans un graphique, sélectionnez Changer la visualisation dans la liste déroulante Nom de la requête et sélectionnez Tableau.



5. Sélectionnez la ligne de résultat de la requête pour laquelle vous souhaitez exécuter le processus CA IT PAM.

6. Cliquez avec le bouton droit de la souris sur cette ligne de résultat de la requête et sélectionnez Exécuter le processus CA IT PAM dans la liste déroulante.



La boîte de dialogue Exécuter le processus CA IT PAM apparaît. Elle contient le nom du processus, ainsi que les paramètres du processus définis dans la configuration CA IT PAM du service Serveur de rapports. Par ailleurs, elle contient une liste déroulante Sélectionner un champ qui vous permet de saisir les données de variables renvoyées au champ CEG sélectionné.

7. Remplissez les champs comme suit.

   a. Vérifiez les valeurs par défaut affichées pour les paramètres de processus affichés et identifiez les valeurs à modifier.

      Ces paramètres et leurs valeurs sont dérivés de la configuration de l'intégration de CA IT PAM.

   b. Pour modifier la valeur par défaut affichée, saisissez la nouvelle valeur.

   c. Pour spécifier une valeur de variable, sélectionnez ce champ CEG dans la liste déroulante Sélectionner un champ dans la partie supérieure de la boîte de dialogue, puis cliquez sur Ajouter un champ à côté de la zone de texte correspondante.

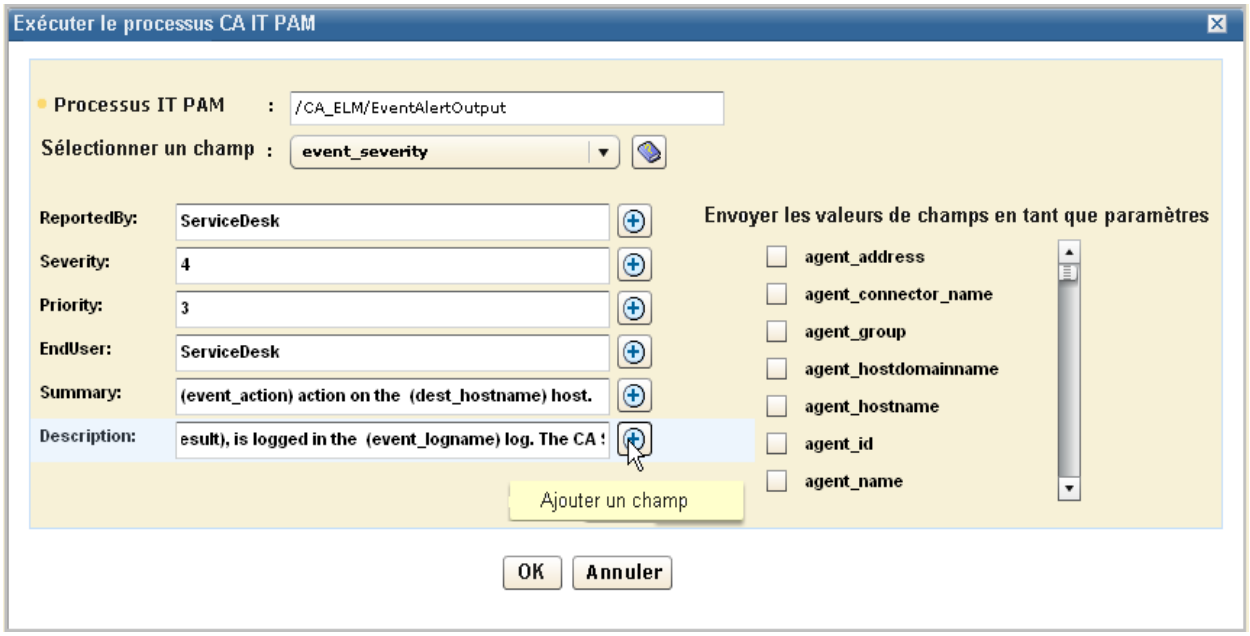
   d. Pour tout champ vide, saisissez une valeur, sélectionnez une variable et ajoutez-la, ou saisissez une phrase qui inclut les variables sélectionnées.

      Exemple de récapitulatif : Le (event_datetime), le compte (dest_username) a effectué une action (event_action) sur l'hôte (dest_hostname).

      Exemple de description : Le résultat de l'action (event_result) est consigné dans le journal (event_logname). La sévérité CA est (event_severity).

   e. Si le processus CA IT PAM spécifie des paramètres qui font référence à des champs CEG supplémentaires, sélectionnez ces champs dans la liste affichée à envoyer en tant que paramètres.

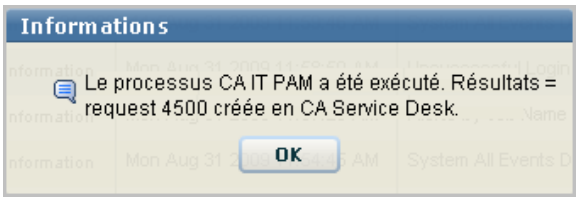
   Voici un exemple. Votre affichage peut inclure d'autres champs définis dans le processus de sortie de l'événement/de l'alerte CA IT PAM personnalisé.



8. Cliquez sur OK.

   La boîte de dialogue de progression apparaît, suivie par un message indiquant si le processus CA IT PAM a bien été exécuté et, le cas échéant, par les résultats de l'exécution du processus.

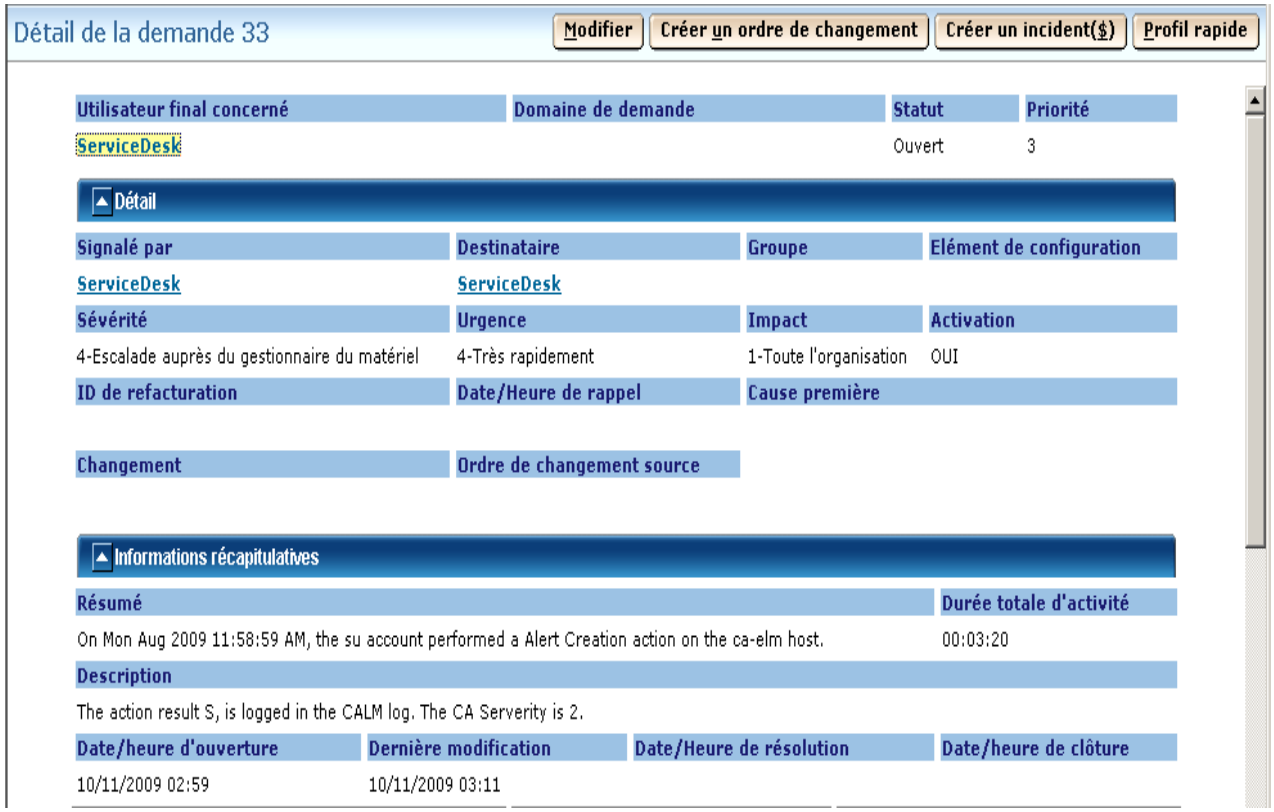
   Voici un exemple où le résultat est la demande 4590 créée dans Service Desk.



9. Cliquez sur OK.
10. Pour afficher les résultats dans CA Service Desk, connectez-vous et recherchez "Demande" avec le numéro dans le message.

    Par exemple, sélectionnez Demande et saisissez 4590.

11. Des résultats Service Desk similaires aux suivants apparaissent.



12. Comparez les données récapitulatives et descriptives planifiées déterminées à l'étape 7 avec les données récapitulatives et descriptives affichées dans Informations récapitulatives. Elles incluent les données de sévérité CA.

Conception de requêtes pour les événements à envoyer au processus de sortie de l'événement/de l'alerte

Une fois l'intégration de CA IT PAM configurée, vous pouvez passer à la première étape de planification des alertes qui génèrent la sortie de l'événement/de l'alerte, qui consiste à compiler une liste des requêtes sur lesquelles seront basées les alertes. Il s'agit généralement de requêtes pour des événements qui insinuent une violation de stratégie. Vous pouvez combiner plusieurs approches.

- Analysez les alertes actuellement planifiées pour identifier n'importe quelle alerte susceptible d'exécuter le processus de sortie de l'événement/de l'alerte. Par exemple, si le processus de sortie de l'événement/de l'alerte notifie une application d'assistance, identifiez les alertes qui doivent ouvrir un ticket d'assistance.
- Analysez vos stratégies pour identifier celles où une violation pourrait permettre de remonter jusqu'à un événement journalisé, puis créez une requête pour rechercher un événement de ce type.
- Examinez les résultats d'autres requêtes prédéfinies pour identifier les données qu'un produit tiers, tel qu'un produit d'assistance, pourrait utiliser pour prendre des mesures correctives.
- Si votre processus de sortie de l'événement/de l'alerte CA IT PAM crée des tickets dans un produit d'assistance tiers, vérifiez si les types de tickets d'assistance par défaut présentent des causes pouvant être capturées comme journaux d'événements.

Pour identifier ou concevoir des requêtes sur lesquelles vous pouvez baser des alertes qui exécutent le processus de sortie de l'événement/de l'alerte CA IT PAM

1. Pour chaque type d'événement nécessitant un ticket d'assistance, identifiez, modifiez ou créez une ou plusieurs requêtes qui capturent les données d'un tel événement.
   - Identifiez chaque requête prédéfinie qui collecte des événements en fonction de ces conditions.
   - Si une requête prédéfinie nécessite une personnalisation, copiez la requête, puis personnalisez-la selon vos besoins.
   - Si aucune requête prédéfinie n'existe pour collecter un type particulier d'événement nécessitant une notification d'assistance, créez la ou les requêtes dont vous avez besoin.

2. Pour toute requête dont l'objectif est de rechercher un événement informatique dont l'un des champs peut présenter plusieurs valeurs connues, utilisez une liste à clés prédéfinie, personnalisez une liste à clés ou créez-en une nouvelle. Si les valeurs d'une clé de ce type existent dans un fichier CSV, importez-les. Pour une liste générée par un processus CA IT PAM, configurez ce processus comme Traitement des valeurs dynamiques, créez la clé, puis importez les valeurs à partir de CA IT PAM.
3. Déterminez s'il faut exécuter le processus de sortie de l'événement/de l'alerte CA IT PAM par requête qui renvoie des résultats ou par ligne de résultat.
4. Testez la requête.
    a. Créez la condition qui produit l'événement que vous souhaitez capturer.
    b. Exécutez la requête ou l'ensemble de requêtes manuellement.
    c. Déterminez si les résultats de la requête sont suffisants pour que le personnel d'assistance puisse effectuer le suivi nécessaire.
    d. Dans le cas contraire, modifiez la requête ou l'ensemble de requêtes pour fournir les informations requises et procédez à un nouveau test.

Cette préparation vous garantit que lorsque vous planifiez une alerte qui exécute une requête ou un ensemble de requêtes de ce type, la sortie de l'événement/de l'alerte obtenue contient les données requises pour la résolution.

Informations complémentaires :

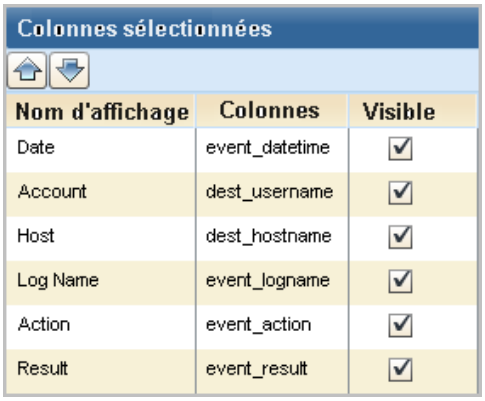
Création d'une requête (page 295)
Personnalisation de requêtes pour les alertes d'action (page 376)

Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par ligne

Vous pouvez envoyer une alerte qui entraîne l'exécution du processus de sortie de l'événement/de l'alerte CA IT PAM, pour chaque ligne ou requête. Cet exemple illustre la procédure d'exécution du processus par ligne. Il illustre notamment ce que le personnel utilisant à la fois CA IT PAM et le produit tiers voit avec ce type d'alerte lorsque CA IT PAM lui envoie des informations détaillées.

Avant de créer une alerte pour exécuter un processus CA IT PAM pour une requête donnée, il est recommandé d'identifier les colonnes CEG qui renvoient des données. Ces colonnes sont celles à sélectionner lors de la création d'une instruction récapitulative et descriptive pour l'alerte.

Remarque : Copiez la requête et cliquez sur Colonnes de requêtes. Pour les champs conçus pour être visibles, notez le nom de colonne correspondant au nom d'affichage. Par exemple, le champ CEG utilisé pour remplir la colonne Compte est dest_username.


Colonnes sélectionnées

Nom d'affichage	Colonnes	Visible
Date	event_datetime	☑
Account	dest_username	☑
Host	dest_hostname	☑
Log Name	event_logname	☑
Action	event_action	☑
Result	event_result	☑

Pour créer une alerte lorsqu'un membre de compte par défaut se connecte

1. Cliquez sur l'onglet Gestion des alertes, puis sur le sous-onglet Planification d'alerte.
2. Cliquez sur Planifier une alerte d'action.

   L'assistant de planification des alertes d'action s'ouvre.

3. Effectuez l'étape Sélection d'alerte, comme suit.
   a. Saisissez le nom du job, par exemple, Connexions du compte par défaut.
   b. Cliquez sur la balise Alertes d'action.
   c. Sélectionnez la requête "Connexion établie par des comptes par défaut au cours des dernières 24 heures" et déplacez-la jusqu'à la liste Requêtes sélectionnées.

4. Sélectionnez une plage de dates pour l'exécution de la requête et le nombre maximum de lignes à afficher.
   a. Cliquez sur Conditions de résultats.
   b. Sélectionnez une plage de dates de type "Maintenant" et "Maintenant" "-1 heure".
   c. Sélectionnez des paramètres d'affichage des résultats tels qu'une limite des lignes de 10 et une granularité temporelle comme event_datetime.
   d. Ignorez les événements regroupés.
5. Définissez la planification.
6. Définissez les données de l'alerte à transmettre au processus CA IT PAM en même temps que les données d'événement récupérées par la requête.
   a. Cliquez sur l'étape Destination.
   b. Sélectionnez l'onglet Processus CA IT PAM.
   c. Sélectionnez Connexion établie par des comptes par défaut au cours des dernières 24 heures.
   d. Sélectionnez Exécuter le processus CA IT PAM par ligne.
   e. Si le processus CA IT PAM configuré n'est pas celui que vous souhaitez exécuter, modifiez le chemin d'accès du processus CA IT PAM. Le processus CA IT PAM doit contenir le chemin complet commençant par une barre oblique (/).

f. Créez une instruction récapitulative avec du texte littéral et des variables (facultatif). Dans ce contexte, les variables sont dérivées des champs CEG lorsque les données collectées pour une ligne sont ajustées. Voici un exemple d'instruction récapitulative utilisant des variables.

   Le compte (dest_username) a effectué l'action (event_action) sur le (dest_hostname)

   La première instruction est créée comme suit.

   - Saisissez le mot, "Le"
   - Dans la liste déroulante Sélectionner un champ, sélectionnez dest_username, puis cliquez sur le signe + à côté du champ Récapitulatif.
   - Saisissez l'expression "compte a effectué"
   - Dans la liste déroulante Sélectionner un champ, sélectionnez event_action, puis cliquez sur le signe + à côté du champ Récapitulatif.
   - Saisissez l'expression "l'action le"
   - Dans la liste déroulante Sélectionner un champ, sélectionnez dest_hostname, puis cliquez sur le signe + à côté du champ Récapitulatif.

g. Créez une description avec du texte littéral et du texte dérivé des champs CEG (facultatif). Dans la liste déroulante Sélectionner un champ, sélectionnez le champ souhaité, puis cliquez sur le signe +. Par exemple :

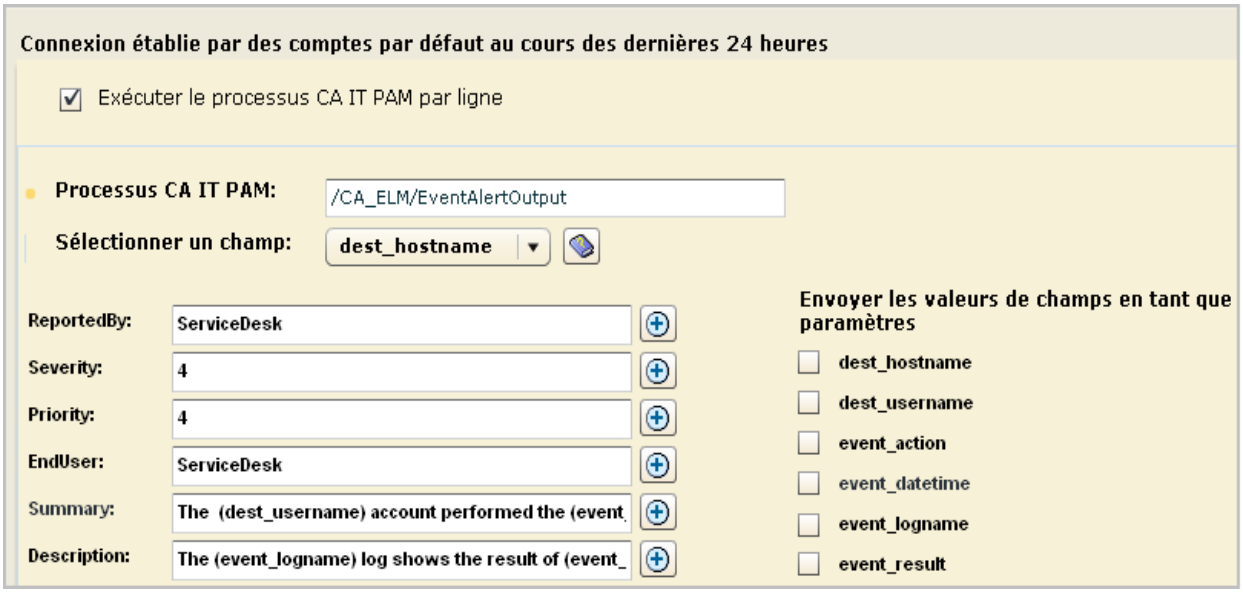
   Le journal (event_logname) affiche le résultat de (event_result) le (event_datetime)

   Le (event_result) de (event_action) est consigné dans le journal (event_logname).

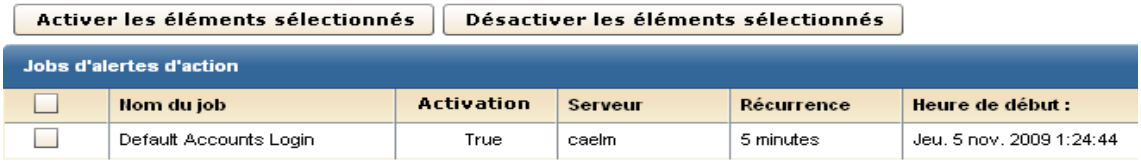
   Le journal (event_logname) affiche l'action (event_action) qui a un résultat de (event_result).

h. Pour Envoyer les valeurs de champs en tant que paramètres, sélectionnez chaque champ CEG que le processus CA IT PAM spécifié utilise comme paramètre de processus.

Remarque : Etant donné que le processus sélectionné n'utilise aucun nom de champ CEG en tant que paramètre, aucun champ n'est sélectionné dans cet exemple. Pour déterminer si un processus personnalisé utilise ce type de paramètres, affichez l'onglet Jeu de données dans le processus de sortie de l'événement/de l'alerte CA IT PAM.



7. Sélectionnez un serveur.
8. Cliquez sur Enregistrer et fermer.
   Le job apparaît dans la liste Jobs d'alertes d'action.



9. Cliquez sur Gestion des alertes > Evénements d'autosurveillance pour afficher les résultats. Voici un affichage partiel des lignes d'informations.

Action	Résultat	Description du résultat
Resource Modify	S	Update RSSFeed Alert Name [login attempts] on reportServer [ca-elm] recurrence [5] recurrenceType [Minutes] was Successful.
Alert Creation	S	Alert job [Default Account Logins] created successfully.
Alert Job Setup	S	Schedule Action Query Alert Name [Default Account Logins] on reportServer [ca-elm] was Successful.

10. Cliquez sur l'onglet Gestion des alertes, sous-onglet Alertes d'action. Sélectionnez l'alerte que vous avez planifiée pour afficher les résultats de la requête.

Nom de l'alerte	Catégorie	Date
Default Account Logins	Connexion établie par des comptes par défaut au cours des dernières 24 heures	Ven. 13 nov. 2009 15:33:24

Default Account Logins

Alert name(Default Account Logins) Alert created by(su) Federated job(Yes) Tags (Action Alerts)
Time Zone (America/New_York) Reports on successful login activity by user accounts listed in Default_Accounts keyed list during the last 24 hour time frame Rows Returned(1)

Date	Compte	Hôte	Nom du journal	Action	Résultat
Ven. 13 nov. 2009 15:33:24	su	ca-elm	CALM	Login Attempt	S

11. Dans l'onglet Evénements d'autosurveillance, recherchez les résultats renvoyés par CA IT PAM.

    Voici un exemple partiel de message d'opération réussie. Ce message apparaît dans les événements d'autosurveillance du serveur de rapports. Notez le numéro de ticket suivant Résultats =.

Action	Résultat	Description du résultat
Notification Creation	S	IT PAM process ran successfully. Results = [Request 631 created in CA Service Desk.]

12. Passez en revue les résultats sur CA Service Desk comme suit (facultatif).
    a. Connectez-vous à CA Service Desk.
    b. Sélectionnez Demande et entrez le numéro d'incident.
    c. Cliquez sur le lien du numéro de la demande pour passer en revue les détails de l'incident et les informations récapitulatives.

Informations complémentaires :

Instructions pour la création d'un processus de sortie de l'événement/de l'alerte (page 406)

Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par requête

Vous pouvez envoyer une alerte qui entraîne l'exécution du processus de sortie de l'événement/de l'alerte CA IT PAM, pour chaque ligne ou requête. Cet exemple illustre la procédure d'exécution du processus par requête. Il illustre notamment ce que le personnel travaillant avec un produit tiers voit avec ce type d'alerte lorsque CA IT PAM lui envoie des informations détaillées.

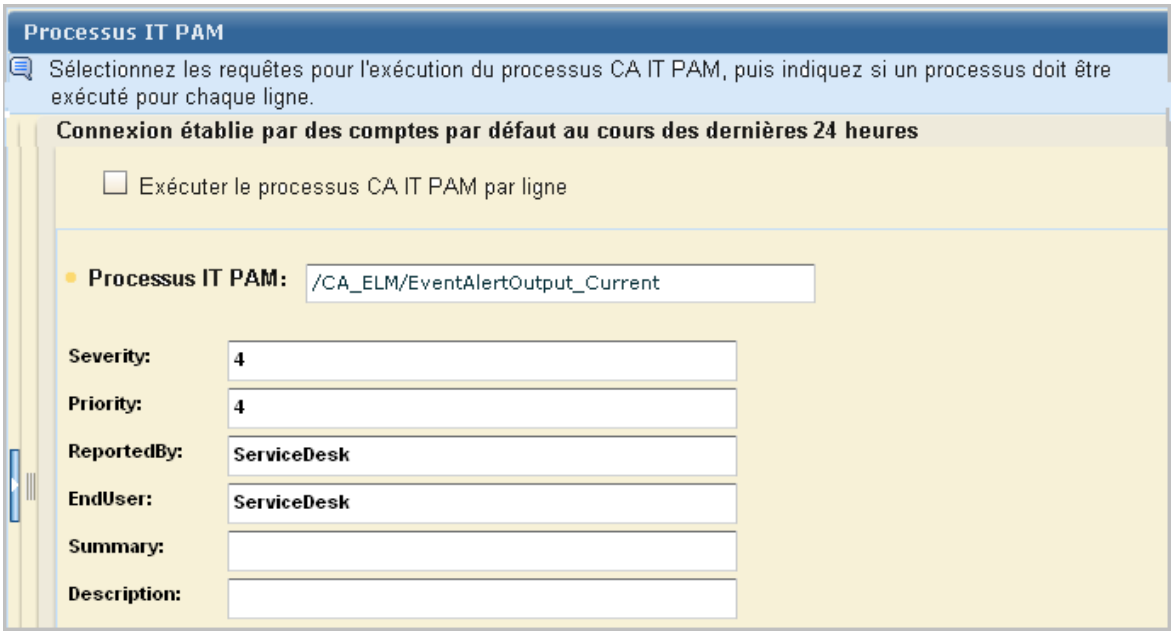
Pour envoyer une alerte déclenchant l'exécution d'un processus de sortie de l'événement/de l'alerte CA IT PAM par requête

1. Cliquez sur l'onglet Gestion des alertes, puis sur le sous-onglet Planification d'alerte.
2. Cliquez sur Planifier une alerte d'action.

   L'assistant de planification des alertes d'action s'ouvre.
3. Effectuez l'étape Sélection d'alerte, comme suit.
   a. Saisissez un nom pour le job.
   b. Sélectionnez une requête.
4. Sélectionnez une plage de dates pour l'exécution de la requête et le nombre maximum de lignes à afficher (facultatif).
   a. Cliquez sur Conditions de résultats.
   b. Sélectionnez une plage de dates de type "Maintenant" et "Maintenant" "-1 heure".
   c. Sélectionnez les paramètres d'affichage des résultats.
5. Définissez la planification.
6. Définissez les données de l'alerte à transmettre au processus CA IT PAM en même temps que les données d'événement récupérées par la requête.
   a. Cliquez sur l'étape Destination.
   b. Sélectionnez l'onglet Processus CA IT PAM.
   c. Sélectionnez la requête à envoyer.

d. Si vous souhaitez que les résultats soient affichés par requête, laissez la case à cocher Exécuter le processus CA IT PAM désélectionnée.

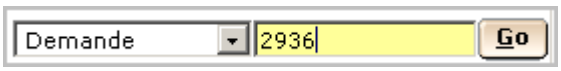
e. Vous pouvez aussi, de manière facultative, saisir du texte dans les champs Récapitulatif et Description.



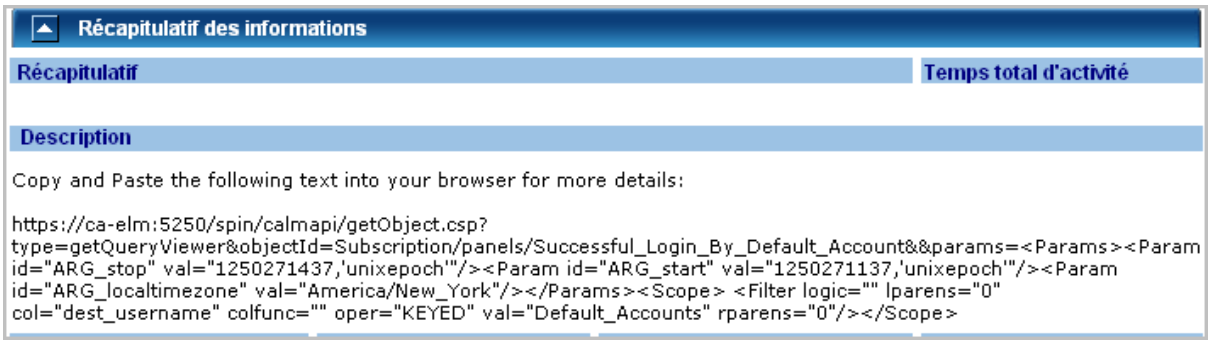
7. Sélectionnez un serveur.
8. Cliquez sur Enregistrer et fermer.
   Le job apparaît dans la liste Jobs d'alertes d'action.
9. Cliquez sur l'onglet Gestion des alertes, sous-onglet Alertes d'action. Sélectionnez l'alerte que vous avez planifiée pour afficher les résultats de la requête.
10. Dans l'onglet Evénements d'autosurveillance, recherchez l'action Création d'une notification, avec les résultats renvoyés par CA IT PAM. Un message de confirmation s'affiche, indiquant le numéro de requête créé dans l'application tierce, s'il s'agit d'un produit de service d'assistance.

Action	Résultat	Description du résultat
Notification Creation	S	IT PAM process ran successfully. Results = Request 2936 created in CA Service Desk.

11. Pour savoir ce que verra le personnel du service d'assistance, consultez les résultats sur CA Service Desk, comme suit (facultatif).
    a. Connectez-vous à CA Service Desk.
    b. Sélectionnez Requête et saisissez le numéro indiqué dans la description de résultat pour la création d'une notification. Cliquez sur OK.



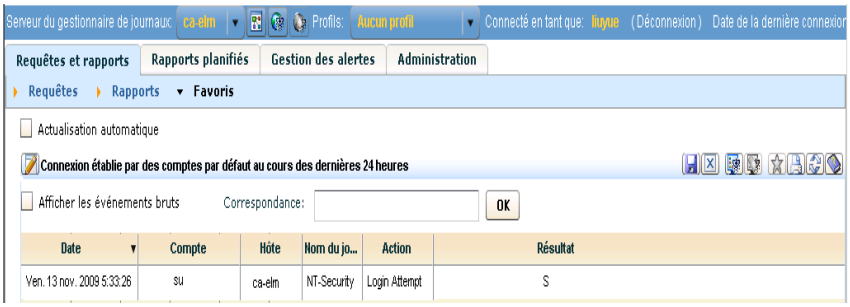
c. Copiez l'URL qui s'affiche dans la section Récapitulatif des informations et collez-la dans la barre d'adresse de votre navigateur.



La boîte de dialogue de connexion CA Enterprise Log Manager s'affiche.

d. Connectez-vous à CA Enterprise Log Manager. Vous pouvez utiliser un compte disposant de peu de droits, par exemple le rôle Auditor.

Les données d'événement renvoyées par la requête sont présentées au format d'affichage par défaut de la requête, c'est-à-dire sous forme de tableau ou de graphique.



Dans le cas d'un tableau, vous pouvez afficher les données d'événement brut.

Informations complémentaires :

Définition de destinations des notifications (page 476)

Utilisation des interruptions SNMP

Dans votre environnement d'entreprise, vous pouvez disposer de systèmes capables de recevoir des interruptions SNMP. Les systèmes de gestion des anomalies et les NOC (Network Operations Centers, centres d'opérations réseau) sont représentatifs des systèmes qui sont généralement capables de recevoir des interruptions SNMP. Vous pouvez envoyer des alertes à ces systèmes telles que des interruptions SNMP v2 ou SNMP v3, en fonction du produit de destination.

Les tâches obligatoires pour l'utilisation des interruptions SNMP sont les suivantes :

- Préparer les produits de destination à recevoir des interruptions SNMP provenant de CA Enterprise Log Manager.
- Planifier des alertes avec une ou plusieurs destinations d'interruption SNMP.

La configuration d'une destination d'interruption SNMP est facultative.

Informations complémentaires :

Préparation de CA Spectrum pour recevoir des interruptions SNMP à partir d'alertes (page 442)
Préparation de CA NSM pour recevoir des interruptions SNMP à partir d'alertes (page 452)
Configuration de l'intégration avec une destination d'interruption SNMP (page 441)
Exemple : Alerter CA Spectrum des changements de configuration (page 447)
Exemple : Alerter CA NSM des changements de configuration (page 457)

A propos des interruptions SNMP

SNMP est l'acronyme de Simple Network Management Protocol (protocole de gestion de réseau simple), une norme ouverte de transmission de messages d'alerte vers une destination spécifiée. SNMP existe en trois versions : SNMP v1, SNMP v2 et SNMP v3. CA Enterprise Log Manager peut utiliser SNMP v2 ou SNMP v3 pour alerter un ou plusieurs systèmes de gestion tiers lorsqu'un événement qui génère une alerte se produit.

Dans CA Enterprise Log Manager, une alerte est générée lorsqu'une requête planifiée renvoie des résultats à partir des bases de données de journaux d'événements récemment ajustés. Une requête planifiée peut être configurée avec une interruption SNMP comme destination. Les récepteurs d'interruptions, les systèmes de gestion des destinations, peuvent traiter les interruptions à 200 interruptions par seconde environ. En général, les récepteurs d'interruptions écoutent le port UDP 162, port bien connu de snmptrap.

CA Enterprise Log Manager vous permet de créer vos propres alertes à envoyer sous forme d'interruptions SNMP. Vous pouvez, par exemple, définir des alertes qui enverront une notification indiquant qu'un événement critique s'est produit. Vous pouvez également définir des alertes pour des événements, tels que des changements de configuration. Vous décidez des alertes à envoyer sous forme d'interruptions SNMP.

A propos des fichiers MIB

Les interruptions SNMP sont définies dans des fichiers MIB (Management Information Base) standard ou des fichiers MIB spécifiques à l'entreprise.

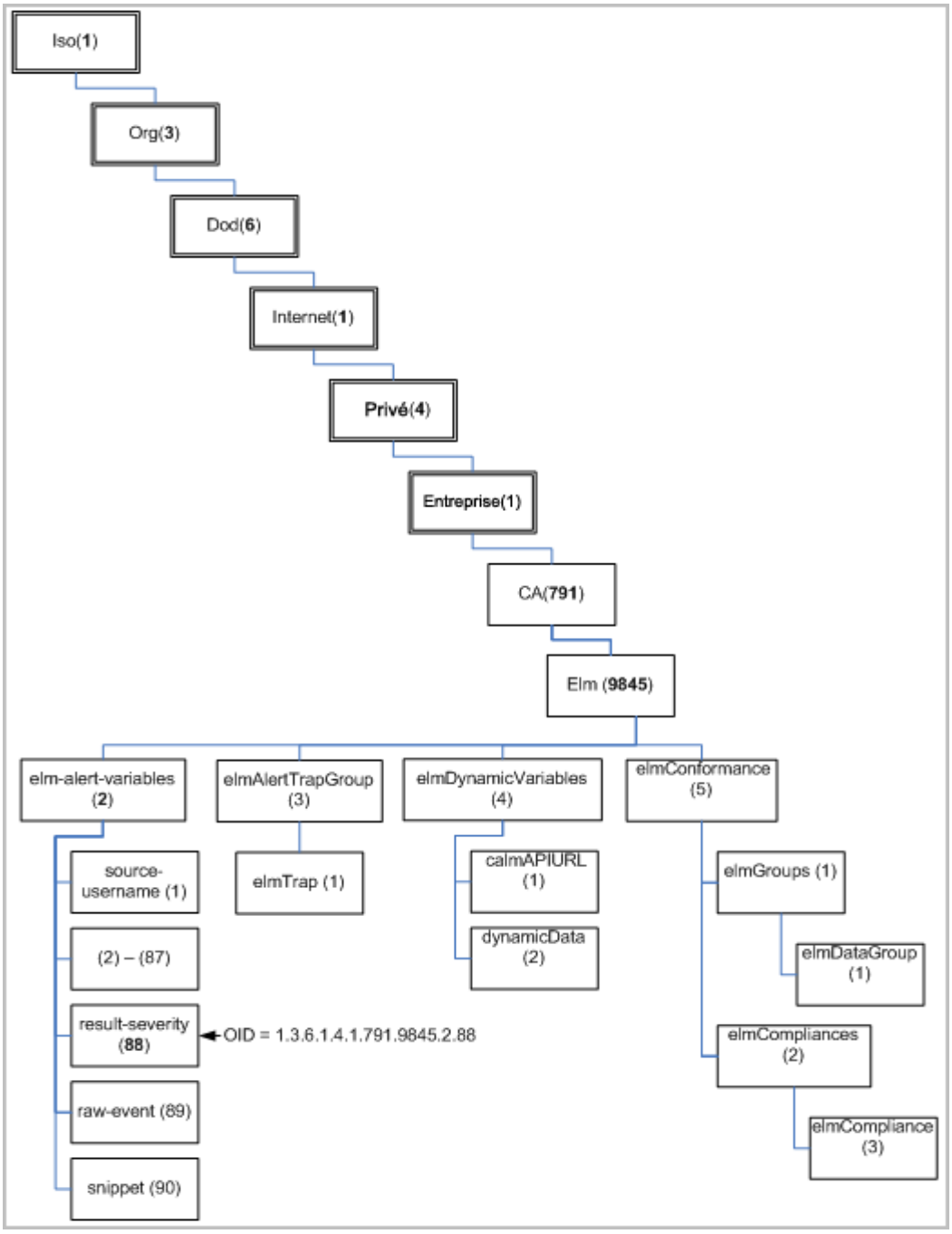
Chaque entreprise privée sur l'arborescence MIB présente un numéro unique précédé des numéros de ses noeuds parents. L'IANA a affecté à CA, Inc. le numéro d'entreprise privée 791. Toutes les données envoyées dans les interruptions SNMP par une application CA sont associées à des ID d'objet qui commencent par 1.3.6.1.4.1.791. L'identificateur de l'application CA Enterprise Log Manager qui appartient à CA est 9845. Toutes les données d'interruption SNMP envoyées par des alertes d'action CA Enterprise Log Manager sont associées à des identifiants d'objet (OID) commençant par 1.3.6.1.4.1.791.9845.

CA Enterprise Log Manager fournit un fichier MIB. Le nom de ce fichier MIB est CA-ELM.MIB. Ce fichier MIB définit tous les champs pouvant être envoyés par des alertes d'action avec une interruption. Cette interruption inclut des champs CEG disponibles dans CA Enterprise Log Manager.

Quand une alerte d'action est envoyée à une destination d'interruption SNMP, les données envoyées incluent un URL. Les interruptions entrantes de surveillance individuelles peuvent ouvrir l'URL envoyée par l'alerte d'action. L'ouverture de l'URL lance une page CA Enterprise Log Manager qui affiche les résultats de la requête dans un format simple à lire. Cette fonctionnalité rend inutile l'utilisation de fichiers MIB pour interpréter des données envoyées en tant qu'interruptions SNMP.

Arborescence MIB CA-ELM

Vous pouvez afficher la structure du fichier CA-ELM.MIB dans le formulaire d'arborescence MIB. Les champs CEG sont définis sous elmAlertVariables avec des OID SNMP uniques. Par exemple, result_severity présente un OID de 1.3.6.1.4.1.791.9845.2.88.



Fichier CA-ELM.MIB

Le fichier MIB CA Enterprise Log Manager, CA-ELM.MIB, se trouve sur le DVD d'installation. La MIB CA Enterprise Log Manager est générée à partir du document source CEG, qui contient les OID de chaque champ CEG (elmAlertVariables).

Le fichier CA-ELM.MIB commence par des importations comme suit :

```
CAELM-MIB DEFINITIONS ::= BEGIN

 IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
        FROM SNMPv2-SMI
    MODULE-COMPLIANCE, OBJECT-GROUP,NOTIFICATION-GROUP
        FROM SNMPv2-CONF                                    DisplayString
        FROM SNMPv2-TC;
```

Voici la structure de l'arborescence MIB CA Enterprise Log Manager.

```
ca  ::= { 1 org(3) dod(6) internet(1) private(4) enterprises(1) 791}
            elm    ::= { ca 9845 }
                        elmAlertVariables      ::= { elm 2 }
                                    source-username    ::= { elmAlertVariables 1 }
                                    source-domainname  ::= { elmAlertVariables 2 }
                                    source-groupname   ::= { elmAlertVariables 3 }
                ...
                                    result-severity    ::= { elmAlertVariables 88 }
                                    raw-event          ::= { elmAlertVariables 89 }
                                    snippet            ::= { elmAlertVariables 90 }
                        elmAlertTrapGroup      ::= { elm 3 }
                                    elmTrap            ::= { elmAlertTrapGroup 1 }
                        elmDynamicVariables    ::= { elm 4 }
                                    calmAPIURL         ::= { elmDynamicVariables 1 }
                                    dynamicData        ::= { elmDynamicVariables 2 }
                        elmConformance         ::= { elm 5 }
                                    elmGroups          ::= { elmConformance 1 }
                                                elmDataGroup   ::= { elmGroups 1 }
                                    elmCompliances     ::= { elmConformance 2 }
                                                elmCompliance  ::= { elmCompliances 3 }
```

Le fichier CA-ELM.MIB définit une interruption. Cette interruption est définie de la façon suivante :

```
elmTrap NOTIFICATION-TYPE
   OBJECTS { source-username,source-domainname,source-groupname,source-uid,source-gid,source-
hostname,source-hostdomainname,source-address,source-mac-address,source-port,source-
processname,source-objectname,source-objectattr,source-objectid,source-objectclass,source-objectvalue,dest-
username,dest-domainname,dest-groupname,dest-uid,dest-gid,dest-hostname,dest-hostdomainname,dest-
address,dest-mac-address,dest-port,dest-objectname,dest-objectattr,dest-objectid,dest-objectclass,dest-
objectvalue,agent-name,agent-address,agent-hostname,agent-hostdomainname,agent-version,agent-id,agent-
connector-name,agent-group,event-source-hostname,event-source-hostdomainname,event-source-
address,event-source-processname,receiver-name,receiver-hostname,receiver-hostaddress,receiver-
hostdomainname,receiver-port,receiver-time-gmt,receiver-timezone,receiver-version,event-protocol,event-
logname,event-euuid,event-count,event-summarized,event-duration,event-time-year,event-time-month,event-
time-monthday,event-time-weekday,event-time-hour,event-time-minute,event-time-gmt,event-datetime,event-
year-datetime,event-month-datetime,event-day-datetime,event-hour-datetime,event-quarterhour-datetime,event-
minute-datetime,event-timezone,event-sequence,event-trend,event-action,event-id,event-category,event-
class,ideal-model,event-severity,event-result,result-string,result-signature,result-code,result-version,result-
priority,result-scope,result-severity,raw-event,snippet }
   STATUS  current
   Description
        "L'interruption SNMP ELM SNMP".
   elmTrap          ::= { elmAlertTrapGroup 1 }
```

Les identifiants de l'interruption personnalisée définie par l'utilisateur sont compris entre les plages 1,3.6,1.4,1.791,9845.3,1 et 1,3.6,1.4,1.791,9845.3,999. Le paramètre elmAlertTrapGroup est 1,3.6,1.4,1.791,9845.3 et elmTrap est défini par le prochain nœud.

Informations complémentaires :

Object ID (OID) to CEG Field Mapping (page 435)
MIB personnalisés (page 439)

Object ID (OID) to CEG Field Mapping

Le tableau suivant illustre le champ CEG correspondant à chaque OID sous elmAlertVariables dans l'arborescence MIB. L'ajout de nouveaux champs CEG entraîne la croissance de cette branche de l'arborescence. Pensez à vérifier les mises à jour de la MIB et assurez-vous que la dernière version est disponible pour vos produits de destination des interruptions SNMP.

ID d'objet (OID)	Champ CEG
1.3.6.1.4.1.791.9845.2.1	source-username
1.3.6.1.4.1.791.9845.2.2	source-domainname
1.3.6.1.4.1.791.9845.2.3	source-groupname

ID d'objet (OID)	Champ CEG
1.3.6.1.4.1.791.9845.2.4	source-uid
1.3.6.1.4.1.791.9845.2.5	source-gid
1.3.6.1.4.1.791.9845.2.6	source-hostname
1.3.6.1.4.1.791.9845.2.7	source-hostdomainname
1.3.6.1.4.1.791.9845.2.8	source-address
1.3.6.1.4.1.791.9845.2.9	source-mac-address
1.3.6.1.4.1.791.9845.2.10	source-port
1.3.6.1.4.1.791.9845.2.11	source-processname
1.3.6.1.4.1.791.9845.2.12	source-objectname
1.3.6.1.4.1.791.9845.2.13	source-objectattr
1.3.6.1.4.1.791.9845.2.14	source-objectid
1.3.6.1.4.1.791.9845.2.15	source-objectclass
1.3.6.1.4.1.791.9845.2.16	source-objectvalue
1.3.6.1.4.1.791.9845.2.17	dest-username
1.3.6.1.4.1.791.9845.2.18	dest-domainname
1.3.6.1.4.1.791.9845.2.19	dest-groupname
1.3.6.1.4.1.791.9845.2.20	dest-uid
1.3.6.1.4.1.791.9845.2.21	dest-gid
1.3.6.1.4.1.791.9845.2.22	dest-hostname
1.3.6.1.4.1.791.9845.2.23	dest-hostdomainname
1.3.6.1.4.1.791.9845.2.24	dest-address
1.3.6.1.4.1.791.9845.2.25	dest-mac-address
1.3.6.1.4.1.791.9845.2.26	dest-port
1.3.6.1.4.1.791.9845.2.27	dest-objectname
1.3.6.1.4.1.791.9845.2.28	dest-objectattr
1.3.6.1.4.1.791.9845.2.29	dest-objectid
1.3.6.1.4.1.791.9845.2.30	dest-objectclass
1.3.6.1.4.1.791.9845.2.31	dest-objectvalue
1.3.6.1.4.1.791.9845.2.32	agent-name
1.3.6.1.4.1.791.9845.2.33	agent-address

ID d'objet (OID)	Champ CEG
1.3.6.1.4.1.791.9845.2.34	agent-hostname
1.3.6.1.4.1.791.9845.2.35	agent-hostdomainname
1.3.6.1.4.1.791.9845.2.36	agent-version
1.3.6.1.4.1.791.9845.2.37	agent-id
1.3.6.1.4.1.791.9845.2.38	agent-connector-name
1.3.6.1.4.1.791.9845.2.39	agent-group
1.3.6.1.4.1.791.9845.2.40	event-source-hostname
1.3.6.1.4.1.791.9845.2.41	event-source-hostdomainname
1.3.6.1.4.1.791.9845.2.42	event-source-address
1.3.6.1.4.1.791.9845.2.43	event-source-processname
1.3.6.1.4.1.791.9845.2.44	receiver-name
1.3.6.1.4.1.791.9845.2.45	receiver-hostname
1.3.6.1.4.1.791.9845.2.46	receiver-hostaddress
1.3.6.1.4.1.791.9845.2.47	receiver-hostdomainname
1.3.6.1.4.1.791.9845.2.48	receiver-port
1.3.6.1.4.1.791.9845.2.49	receiver-time-gmt
1.3.6.1.4.1.791.9845.2.50	receiver-timezone
1.3.6.1.4.1.791.9845.2.51	receiver-version
1.3.6.1.4.1.791.9845.2.52	event-protocol
1.3.6.1.4.1.791.9845.2.53	event-logname
1.3.6.1.4.1.791.9845.2.54	event-euuid
1.3.6.1.4.1.791.9845.2.55	event-count
1.3.6.1.4.1.791.9845.2.56	event-summarized
1.3.6.1.4.1.791.9845.2.57	event-duration
1.3.6.1.4.1.791.9845.2.58	event-time-year
1.3.6.1.4.1.791.9845.2.59	event-time-month
1.3.6.1.4.1.791.9845.2.60	event-time-monthday
1.3.6.1.4.1.791.9845.2.61	event-time-weekday
1.3.6.1.4.1.791.9845.2.62	event-time-hour
1.3.6.1.4.1.791.9845.2.63	event-time-minute

ID d'objet (OID)	Champ CEG
1.3.6.1.4.1.791.9845.2.64	event-time-gmt
1.3.6.1.4.1.791.9845.2.65	event-datetime
1.3.6.1.4.1.791.9845.2.66	event-year-datetime
1.3.6.1.4.1.791.9845.2.67	event-month-datetime
1.3.6.1.4.1.791.9845.2.68	event-day-datetime
1.3.6.1.4.1.791.9845.2.69	event-hour-datetime
1.3.6.1.4.1.791.9845.2.70	event-quarterhour-datetime
1.3.6.1.4.1.791.9845.2.71	event-minute-datetime
1.3.6.1.4.1.791.9845.2.72	event-timezone
1.3.6.1.4.1.791.9845.2.73	event-sequence
1.3.6.1.4.1.791.9845.2.74	event-trend
1.3.6.1.4.1.791.9845.2.75	event-action
1.3.6.1.4.1.791.9845.2.76	event-id
1.3.6.1.4.1.791.9845.2.77	event-category
1.3.6.1.4.1.791.9845.2.78	event-class
1.3.6.1.4.1.791.9845.2.79	ideal-model
1.3.6.1.4.1.791.9845.2.80	event-severity
1.3.6.1.4.1.791.9845.2.81	event-result
1.3.6.1.4.1.791.9845.2.82	result-string
1.3.6.1.4.1.791.9845.2.83	result-signature
1.3.6.1.4.1.791.9845.2.84	result-code
1.3.6.1.4.1.791.9845.2.85	result-version
1.3.6.1.4.1.791.9845.2.86	result-priority
1.3.6.1.4.1.791.9845.2.87	result-scope
1.3.6.1.4.1.791.9845.2.88	result-severity
1.3.6.1.4.1.791.9845.2.89	raw-event

MIB personnalisés

Vous pouvez créer des fichiers MIB en utilisant le contenu du fichier CA-ELM.MIB comme référence. Un fichier MIB personnalisé pour une seule alerte contient un sous-ensemble du contenu du fichier CA-ELM.MIB. Un fichier MIB personnalisé pour une alerte diffère du fichier CA-ELM.MIB de la façon suivante.

- Le fichier MIB personnalisé définit uniquement les champs envoyés par cette alerte.
- Le fichier MIB personnalisé définit une interruption qui répertorie ces champs dans l'ordre dans lequel ils sont envoyés.
- L'interruption MIB personnalisée est définie par l'identifiant d'objet (OID), 1.3.6.1.4.1.791.9845.3.x, où x est une valeur comprise entre 1 et 999.

  Remarque : Une alerte qui utilise un fichier MIB personnalisé indique cet OID comme la valeur de l'identifiant de l'interruption personnalisée.

Remarques sur l'utilisation de la base de données d'informations de gestion

Pour comprendre une interruption SNMP envoyée par CA Enterprise Log Manager à l'aide de fichiers MIB, un système doit savoir ce que définissent les OID (Object Identifier, identificateur d'objets) qui la composent. Les conditions requises pour y parvenir varient de la façon suivante en fonction du système :

- CA Spectrum peut interpréter des interruptions SNMP envoyées par CA Enterprise Log Manager, si le fichier CA-ELM.MIB a été importé et compilé.
- CA NSM peut interpréter des interruptions SNMP envoyées par CA Enterprise Log Manager, si les fichiers CA-ELM.MIB et MIB personnalisés ont été importés et compilés.

Les personnes qui surveillent les interruptions SNMP reçues par le produit de destination peuvent interpréter les interruptions envoyées par CA Enterprise Log Manager de deux façons différentes :

- En lançant la page des résultats d'interruptions SNMP grâce à l'URL fournie dans l'interruption.
- En utilisant une application qui répertorie les fichiers MIB importés.

Processus d'utilisation des interruptions SNMP

L'utilisation d'interruptions SNMP implique les procédures suivantes.

1. Préparez CA Enterprise Log Manager pour envoyer des interruptions SNMP.
   - Configurez la destination par défaut des interruptions SNMP.
   - Identifiez l'adresse IP et le port de chaque destination d'interruption SNMP supplémentaire que vous pouvez spécifier lors de l'envoi d'alertes en tant qu'interruptions SNMP.
   - Identifiez les alertes dont les résultats de requête sont susceptibles d'intéresser CA Spectrum, CA NSM ou un autre récepteur d'interruptions SNMP.
2. Préparez les produits de destination d'interruption SNMP à recevoir des interruptions SNMP provenant de CA Enterprise Log Manager.
   - Si CA Spectrum doit être une destination :
     - Créez un modèle d'événement en fonction de la documentation de Spectrum. Sans modèle d'événement, vous ne pourrez pas afficher les résultats des interruptions au niveau de la destination.
   - Si CA NSM doit être une destination :
     - Installez NSM r11.2 version GA sur Windows Server 2003 EE SP1 et appliquez le patch pour mettre à jour le fichier aws_snmpex.dll.
     - Configurez CA NSM pour recevoir des interruptions SNMP, y compris des interruptions SNMP v3.
3. Préparez la destination d'interruption SNMP à interpréter des interruptions SNMP provenant de CA Enterprise Log Manager à l'aide des MIB (facultatif).
   - Téléchargez la MIB CA Enterprise Log Manager sur un emplacement accessible depuis votre produit de destination des interruptions SNMP.

     Remarque : Le fichier CA-ELM.MIB est fourni sur le DVD d'installation. Vous pouvez télécharger la dernière version de cette MIB à partir de la page de produit CA Enterprise Log Manager.
   - Pour CA Spectrum, importez et compilez le fichier CA-ELM.MIB à l'aide des outils MIB OneClick CA Spectrum.
   - Pour CA NSM, compilez la définition CA-ELM.MIB et chargez le résultat. Créez votre propre fichier d'interruption pour interpréter chaque alerte et chargez-le.

   Important : Cette étape est facultative car les interruptions provenant de CA Enterprise Log Manager peuvent être interprétées en lançant la page de résultats des interruptions via l'URL envoyée dans l'interruption.
4. Planifiez des alertes avec des destinations d'interruption SNMP.

5. Vérifiez que l'envoi de l'alerte en tant qu'interruption SNMP a abouti.
6. (Facultatif) Contrôlez les résultats des interruptions SNMP envoyées à partir de la destination d'interruption.
   - Affichez les résultats de l'interruption SNMP au niveau de la destination d'interruption.
   - Lancez l'URL pour afficher les données envoyées par l'alerte sous forme de tableau ou de graphique.

Informations complémentaires :

Configuration de l'intégration avec une destination d'interruption SNMP (page 441)
Préparation de CA Spectrum pour recevoir des interruptions SNMP à partir d'alertes (page 442)
Préparation de CA NSM pour recevoir des interruptions SNMP à partir d'alertes (page 452)
Envoi d'interruptions SNMPv2 à CA Spectrum (page 447)
Envoi des interruptions SNMPv3 à CA NSM (page 457)

Configuration de l'intégration avec une destination d'interruption SNMP

Configurez l'intégration SNMP dans le cadre de la configuration globale du service pour le serveur de rapports. La configuration est l'adresse IP et le port d'une destination d'interruption SNMP.

Vous pouvez configurer l'intégration SNMP avant ou après avoir préparé le produit de destination à recevoir et à interpréter les interruptions SNMP de CA Enterprise Log Manager.

Lorsque vous créez une alerte destinée à un destinataire d'interruption SNMP, vous pouvez spécifier une ou plusieurs destinations. Cette configuration est la configuration par défaut. Elle s'applique à tous les serveurs répertoriés dans Serveur de rapports.

Pour configurer l'intégration SNMP

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   La fenêtre Configuration globale de service (Serveur de rapports) s'affiche.
3. Faites défiler jusqu'à la zone Configuration SNMP.
4. Saisissez l'adresse IP ou le nom d'hôte du serveur de destination des interruptions SNMP.
5. Acceptez le numéro de port par défaut (162) ou indiquez-en un autre.
6. Cliquez sur Enregistrer.

Préparation de CA Spectrum pour recevoir des interruptions SNMP à partir d'alertes

Vous pouvez envoyer des alertes sous la forme d'interruptions SNMP à partir de CA Enterprise Log Manager vers n'importe quelle destination de votre réseau capable de recevoir et d'interpréter des interruptions. Chaque produit récepteur d'interruptions a ses propres exigences.

Préparez CA Spectrum de la façon suivante afin qu'il reçoive des interruptions envoyées par les alertes d'action CA Enterprise Log Manager :

- Création d'une intégration de CA Spectrum Southbound Gateway, un point d'intégration qui peut prendre en charge tout format de flux de données d'alerte entrant à partir d'un système tiers, y compris des interruptions SNMP telles que celles générées par CA Enterprise Log Manager
- Création d'un modèle de nœud CA Enterprise Log Manager pour activer la réception des interruptions SNMP v3
- Téléchargement de la MIB CA Enterprise Log Manager
- Importation de la MIB CA Enterprise Log Manager dans CA Spectrum

Le processus de création d'une intégration de Southbound Gateway, y compris le mappage d'interruptions SNMP vers des événements CA Spectrum dans un fichier AlertMap et la définition des modèles requis, est détaillé dans le *manuel de la boîte à outils Spectrum Southbound Gateway*. Le point d'intégration de Southbound Gateway accepte les données d'alerte provenant de systèmes tiers et les affiche dans OneClick.

Après avoir téléchargé le fichier MIB à partir de la page du produit CA Enterprise Log Manager sur Support en ligne ou après avoir extrait ce fichier du DVD d'installation, vous pouvez l'importer dans CA Spectrum. Pour en savoir plus sur l'utilisation de l'outil MIB pour l'importation dans CA Spectrum OneClick, reportez-vous au *manuel de l'utilisateur pour la gestion des périphériques CA Spectrum*.

Informations complémentaires :

Configuration de CA Spectrum pour l'acceptation des interruptions SNMP v3 (page 443)
Téléchargement de la base de données d'informations de gestion CA Enterprise Log Manager (page 445)
Importation de CAELM-MIB dans CA Spectrum (page 446)

Configuration de CA Spectrum pour l'acceptation des interruptions SNMP v3

Avant d'envoyer des interruptions SNMP V3 depuis CA Enterprise Log Manager vers CA Spectrum, vous devez créer un modèle du dispositif CA Enterprise Log Manager dans CA Spectrum. Les interruptions SNMP v3 sont ensuite dirigées vers le nœud CA Enterprise Log Manager que vous avez modélisé.

Pour créer un modèle qui permet à Spectrum de recevoir des interruptions SNMP v3 à partir d'alertes d'action :

1. Connectez-vous au serveur Windows sur lequel CA Spectrum est installé.
2. Ouvrez la console Spectrum OneClick :
   a. Dans le menu Démarrer, cliquez sur Tous les programmes, CA, Panneau de configuration SPECTRUM.

      Le panneau de configuration SPECTRUM s'affiche avec un indicateur d'état au bas de l'écran.

   b. Si l'état n'indique pas RUNNING (EN COURS D'EXECUTION), cliquez sur Start SpectroSERVER (Démarrer SpectroSERVER) dans Process Control (Contrôle du processus).

   c. Quand l'état affiche RUNNING (EN COURS D'EXECUTION), cliquez sur OneClick Administration (Administration OneClick).

      Le panneau de configuration OneClick Administration - SPECTRUM s'affiche avec localhost comme Hôte et le port 80.

   d. Cliquez sur OK.

      Une boîte de dialogue de connexion apparaît.

   e. Indiquez vos informations de connexion.

      La page Spectrum NFM OneClick s'affiche.

   f. Cliquez sur Démarrer la console.

      La connexion - La boîte de dialogue de connexion SPECTRUM OneClick s'affiche pour vous connecter à SPECTRUM OneClick sur l'hôte local.

   g. Cliquez sur OK.

      La console - SPECTRUM OneClick affiche plusieurs panneau : Navigation (navigation), Contents (contenu) et Component Detail (détail du composant).

3. Dans l'onglet Explorer (Explorateur) du panneau Navigation, développez le nœud supérieur et sélectionnez Universe (Univers).

   Les titres des panneaux Contents (Contenu) et Component Detail (Détail du composant) affichent Universe (Univers) du type Universe (Univers).

4. Dans le panneau Contents (Contenu), cliquez sur l'onglet Topology (Topologie).

   Le second bouton de l'onglet vous permet de créer un modèle en fonction du type et de l'ajouter à cette fenêtre.

5. Cliquez sur Create a new model (Créer un modèle).

   La boîte de dialogue Select Model Type (Sélectionner le type de modèle) - SPECTRUM OneClick apparaît.

6. Sélectionnez l'onglet All Model Types (Tous les types de modèle).

7. Saisissez une chaîne dans le champ Filter (Filtre). Saisissez, par exemple, gn.

   Les types de modèles commençant par Gn s'affichent dans la liste.

8. Sélectionnez le modèle souhaité et cliquez sur OK. Par exemple, sélectionnez GnSNMPDev et cliquez sur OK.

   La boîte de dialogue Create Model of Type (Créer un type de modèle) <type de modèle sélectionné> s'affiche.

9. Complétez la boîte de dialogue Create Model of Type (Créer un modèle du type) de la façon suivante.

   a. Entrez le nom d'hôte d'un serveur CA Enterprise Log Manager dans le champ Name (Nom).

   b. Entrez la même adresse IP que celle du serveur indiqué dans le champ Network Address (Adresse réseau).

   c. Entrez un port dans le champ Agent Port (Port de l'agent), si le port 161 par défaut n'est pas celui que vous voulez utiliser. Par exemple, entrez 162.

   d. Sélectionnez SNMP v3 comme option de communication SNMP.

   e. Cliquez sur Profiles (Profils).

   La fenêtre Edit SNMP v3 Profiles (Modifier les profils SNMP v3) affiche une liste des profils existants, s'ils existent.

10. Pour ajouter un profil, procédez de la façon suivante.
    a. Saisissez le nom du profil et l'identifiant utilisateur.
    b. Puisque cela concerne SNMP v3, sélectionnez Authentication with Privacy (Authentification avec confidentialité) comme type d'authentification.
    c. Dans les quatre champs suivants, saisissez deux fois un mot de passe d'authentification à 8 caractères, ainsi qu'un mot de passe de confidentialité à 8 caractères.
    d. Cliquez sur Add (Ajouter) pour ajouter le destinataire à la liste.
    e. Cliquez sur OK.

    Le profil que vous avez ajouté apparaît dans la liste déroulante des profils V3 de la boîte de dialogue Create Model of Type (Créer un modèle du type).
11. Sélectionnez Discover Connections (Découvrir les connexions) et cliquez sur OK.

    L'indicateur de progression Creating Model (Création d'un modèle) s'affiche. Une fois le traitement terminé, le modèle créé apparaît sur l'onglet Topology (Topologie) sous forme d'image avec le nom d'hôte que vous avez saisi et le type de modèle sélectionné.

Téléchargement de la base de données d'informations de gestion CA Enterprise Log Manager

Vous pouvez télécharger le fichier de la base de données d'informations de gestion (MIB) à partir de la page de produit CA Enterprise Log Manager, sur le site de support en ligne, ou bien le récupérer sur le DVD d'installation. Une fois la MIB CA Enterprise Log Manager téléchargée, vous pouvez l'importer/la compiler dans chaque produit configuré, en tant que destination d'interruption SNMP.

Pour télécharger la MIB CA Enterprise Log Manager

1. Connectez-vous au serveur sur lequel vous avez installé CA Spectrum.
2. Démarrez le support en ligne de CA et ouvrez une session.
3. Accédez à la page de produit CA Enterprise Log Manager.
4. Téléchargez le fichier MIB CA Enterprise Log Manager sur votre réseau.
5. Si vous prévoyez d'envoyer des interruptions SNMP à CA Spectrum, importez la MIB CA Enterprise Log Manager dans CA Spectrum.
6. Si vous prévoyez d'envoyer des interruptions SNMP à CA NSM, importez la MIB CA Enterprise Log Manager dans CA NSM. Pour connaître la procédure à suivre, reportez-vous à la documentation CA NSM.

Importation de CAELM-MIB dans CA Spectrum

Avant d'envoyer des interruptions SNMP depuis CA Enterprise Log Manager vers CA Spectrum, vous pouvez importer et compiler la MIB CA Enterprise Log Manager à l'aide des outils MIB OneClick CA Spectrum.

Remarque : Les MIB SNMPv2 référencées dans le fichier CA-ELM.MIB sont préchargées dans CA Spectrum.

Pour importer CA-ELM.MIB dans CA Spectrum

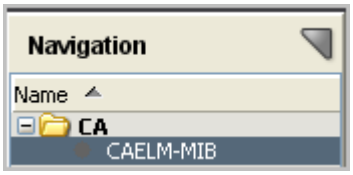
1. Connectez-vous à CA Spectrum.
2. Lancez la console OneClick.
3. Cliquez sur Outils, Utilitaires, Outils MIB.

   La boîte de dialogue Outils MIB : Ajouter MIB s'affiche.
4. Cliquez sur Parcourir, naviguez jusqu'à l'emplacement où vous avez téléchargé CA-ELM.MIB et sélectionnez le fichier.
5. Cliquez sur Compiler.

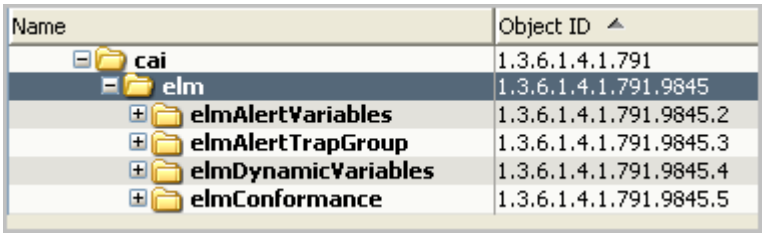
   Un message de confirmation s'affiche, indiquant que la MIB CA Enterprise Log Manager a bien été stockée dans le répertoire suivant du serveur Web OneClick.

   <$SPECROOT>/MibDatabase/userContrib
6. Fermez la boîte de dialogue Outils MIB : Ajouter MIB.

   CAELM-MIB est ajouté à la barre de navigation sous CA.



Dans la hiérarchie, cai est développé pour afficher elm et ses objets d'arborescence subordonnés, ainsi que les OID associés.



Exemple : Alerter CA Spectrum des changements de configuration

Avant d'envoyer des interruptions SNMP à CA Spectrum pour la première fois, il est recommandé d'identifier les requêtes qui renvoient des résultats appropriés à cette destination. Lorsque vous planifiez votre première alerte avec Spectrum comme destination, vous pouvez suivre la progression et comparer les résultats affichés dans CA Enterprise Log Manager avec ceux qui apparaissent dans l'interface CA Spectrum. Lorsque vous vous êtes familiarisé avec l'envoi d'interruptions à CA Spectrum, vous pouvez décider de ne plus effectuer ces étapes de préparation et de suivi.

L'exemple suivant décrit le processus initial, notamment :

- La préparation de l'envoi d'interruptions SNMP à CA Spectrum
- L'envoi d'interruptions SNMP à CA Spectrum
- La vérification de la réussite de l'envoi des interruptions SNMP
- L'affichage des interruptions SNMP reçues par CA Spectrum.

Informations complémentaires :

Envoi d'interruptions SNMPv2 à CA Spectrum (page 447)
Suivi de la progression du job d'alerte (page 450)
Affichage des interruptions SNMP dans CA Spectrum (page 451)

Envoi d'interruptions SNMPv2 à CA Spectrum

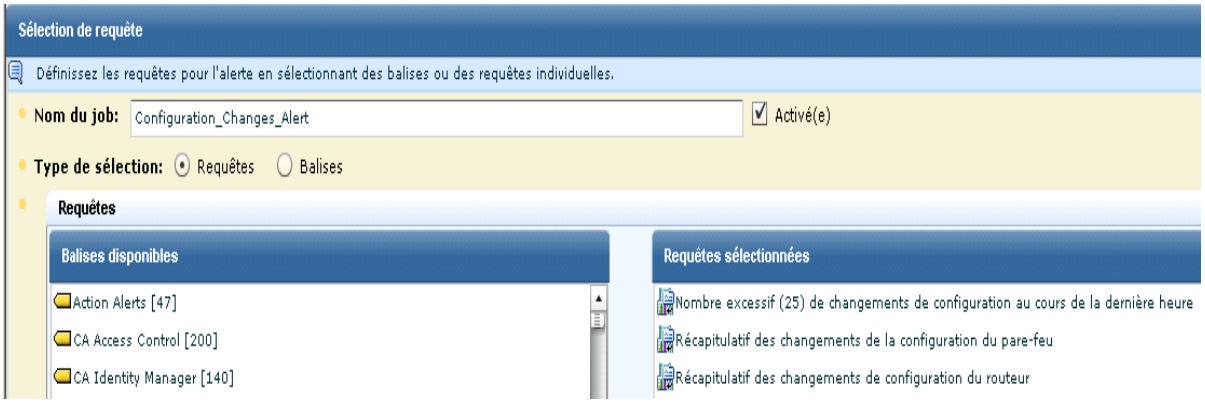
L'exemple suivant illustre la création d'une alerte qui avertit CA Spectrum des modifications de configuration à l'aide d'interruptions SNMPv2.

Pour envoyer des interruptions SNMPv2 à CA NSM :

1. Ouvrez l'assistant de planification d'alerte.
   a. Cliquez sur l'onglet Gestion des alertes, puis sur le sous-onglet Planification d'alerte.
   b. Cliquez sur le bouton Planifier une alerte d'action.

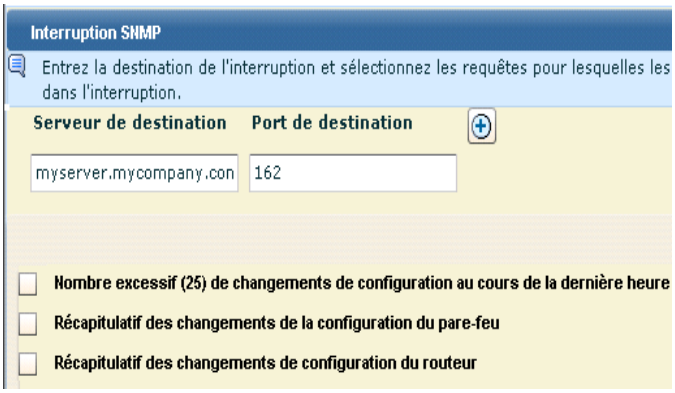
2. Complétez l'étape Sélection d'alerte.
   a. Saisissez un nom de job. Cette opération est requise quel que soit le type d'alerte.
   b. Vérifiez que le type de sélection est Requêtes.

      Dans le cas d'alertes basées sur des balises, vous ne pouvez pas choisir la destination des interruptions SNMP.
   c. Si les requêtes que vous voulez sélectionner sont des alertes d'action balisées, cliquez sur la balise Alertes d'action pour filtrer la liste affichée.
   d. Sélectionnez les requêtes que vous avez identifiées précédemment.



3. Complétez les étapes Filtres d'alerte, Conditions de résultat et Planifier des jobs en vous référant, si nécessaire, à l'aide en ligne de cet assistant (facultatif).
4. Paramétrez l'interruption SNMP.
   a. Cliquez sur l'étape Destination.
   b. Cliquez sur l'onglet Interruption SNMP.

      La destination de l'interruption SNMP configurée et les requêtes sélectionnées à l'étape 1 de l'assistant s'affichent.

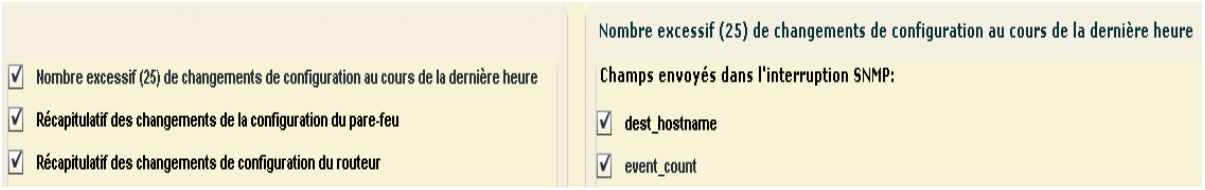


Remarque : Par défaut, SpectroSERVER écoute sur le port standard des interruptions SNMP, le port 162. Si vous décidez de changer de port, utilisez la même valeur que celle du paramètre snmp_trap_port du fichier SPECTRUM .vnmrc, qui se trouve dans le répertoire SS.

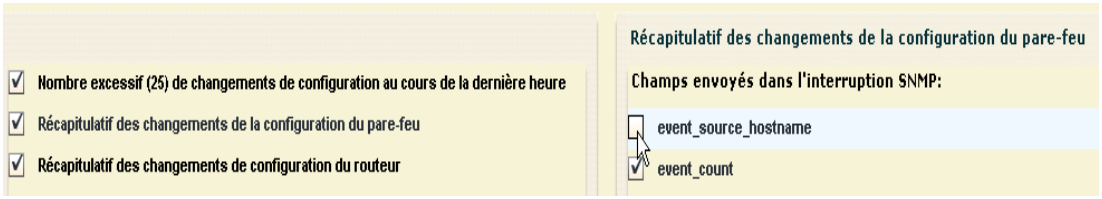
c. (Facultatif). Pour envoyer l'interruption à un maximum de neuf serveurs en plus du serveur de destination configuré, cliquez sur le bouton Ajouter et entrez l'adresse IP et le numéro de port du serveur.

d. Dans le cas d'une requête dont tous les champs doivent être inclus dans l'interruption, sélectionnez simplement la requête.

Par défaut, lorsque vous sélectionnez une requête, tous les champs qu'elle contient sont sélectionnés. Le nom de la requête sélectionnée apparaît au-dessus de la liste des champs.



e. Dans le cas d'une requête dont seulement certains champs doivent être inclus dans l'interruption, sélectionnez la requête et désélectionnez les champs que vous ne souhaitez pas envoyer.



f. Sélectionnez la version SNMP prise en charge par la destination d'interruption sélectionnée pour les interruptions en provenance d'applications.

Remarque : Certaines destinations d'interruption acceptent les interruptions version 3 envoyées directement par des périphériques, et d'autres seulement les interruptions version 2 envoyées par les applications collectionnant les événements à partir de périphériques. Dans cet exemple, la version 2 est acceptée.

5. Sélectionnez le serveur et indiquez si la requête doit renvoyer les résultats uniquement des serveurs sélectionnés, ou de ce serveur et de tous ses serveurs fédérés enfants (fédération hiérarchique) ou pairs (fédération maillée).

6. Cliquez sur Enregistrer et fermer.

   Le job apparaît dans la liste Jobs d'alertes d'action. Il apparaît comme activé (True dans la colonne Activation), sauf si vous avez désélectionné la case Activation à la première étape de l'assistant. Un exemple abrégé est présenté ci-dessous.

Jobs d'alertes d'action

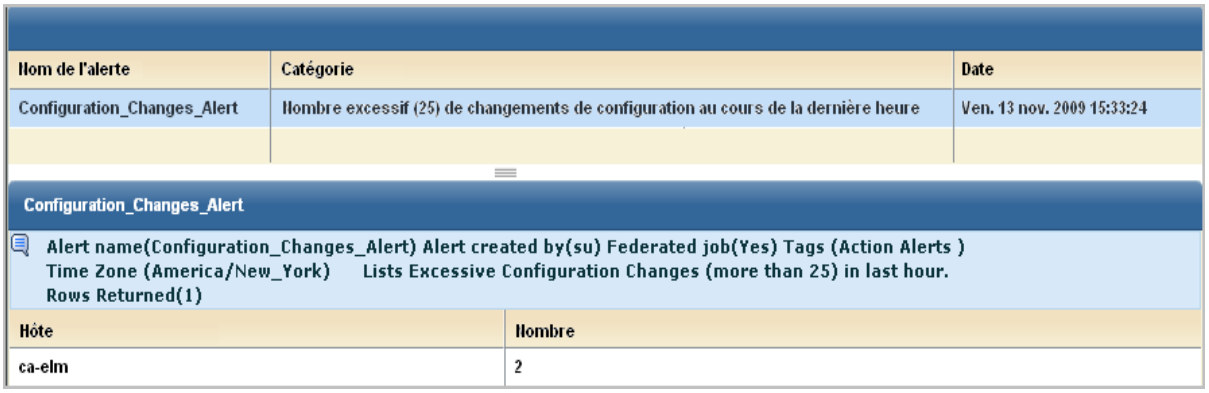
	Nom du job	Activé(e)	Serveur	Récurrence	Heure de début :	Heure de fin	Fuseau horaire	Créateur
☐	Configuration_Changes_Alert	True	ca-elm	5 minutes	Mer. 11 nov. 2009 12:56:08		America/New_York	su

Suivi de la progression du job d'alerte

Vous pouvez afficher les résultats renvoyés par les requêtes sélectionnées pour l'alerte que vous avez créée. Dans notre exemple, les résultats de Configuration_Changes_Alert apparaissent dans CA Enterprise Log Manager sous les en-têtes Hôte et Nombre.

1. Sélectionnez l'onglet Gestion des alertes, puis le sous-onglet Alertes d'action.
2. Cliquez sur le nom de l'alerte que vous avez planifiée.
3. Affichez les résultats de cette alerte.

   Résultats de notre exemple :



Nom de l'alerte	Catégorie	Date
Configuration_Changes_Alert	Nombre excessif (25) de changements de configuration au cours de la dernière heure	Ven. 13 nov. 2009 15:33:24

Configuration_Changes_Alert

Alert name(Configuration_Changes_Alert) Alert created by(su) Federated job(Yes) Tags (Action Alerts)
Time Zone (America/New_York) Lists Excessive Configuration Changes (more than 25) in last hour.
Rows Returned(1)

Hôte	Nombre
ca-elm	2

Affichage des interruptions SNMP dans CA Spectrum

Vous pouvez afficher les interruptions SNMP envoyées par des alertes CA Enterprise Log Manager dans le modèle d'événements CA Spectrum que vous avez créé pour recevoir ces interruptions. Les interruptions reçues s'affichent dans l'onglet Evénements. Dans l'exemple Configuration_Changes_Alert, les résultats, ca-elm et 2, sont affichés dans CA Spectrum avec les OID 1,3.6,1.4,1.791,9845.2,22 et 1,3.6,1.4,1.791,9845.2,2.

Pour afficher des interruptions SNMP dans CA Spectrum

1. Connectez-vous à CA Spectrum avec vos informations d'identification CA Spectrum.
2. Affichez le panneau de configuration Spectrum et démarrez Spectroserver.

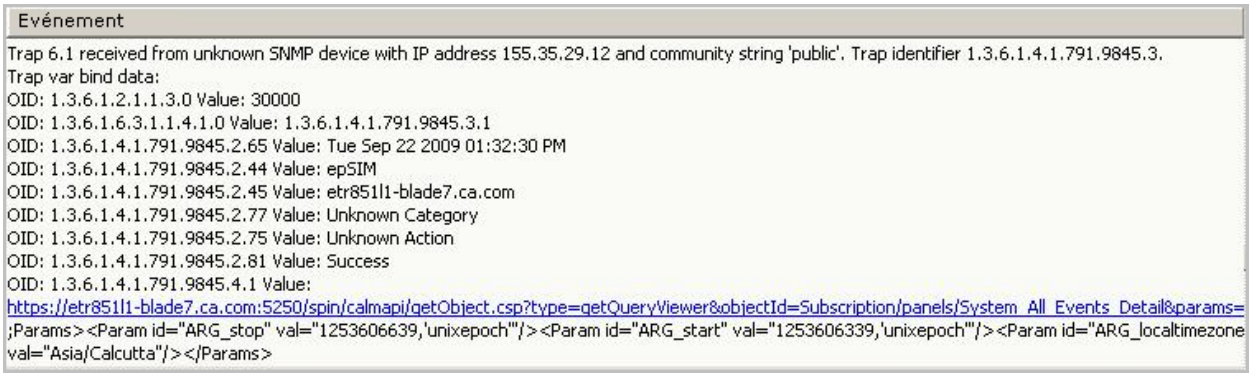
   Spectroserver démarre.
3. Cliquez sur Administrateur OneClick et ouvrez une session.

   L'application Spectrum NFM OneClick s'affiche.
4. Cliquez sur Démarrer la console.

   La console Spectrum OneClick apparaît.
5. Développez le dossier créé pour CA Enterprise Log Manager.
6. Sous Univers, sélectionnez le modèle d'événement que vous avez créé pour recevoir les interruptions envoyées par CA Enterprise Log Manager.
7. Dans le volet droit, sélectionnez l'onglet Evénements pour afficher les interruptions envoyées par CA Enterprise Log Manager.

   La valeur ca-elm et event_count=2 sont les mêmes que les données que vous pouvez consulter dans CA Enterprise Log Manager.

Vous trouverez ci-dessous un autre exemple d'affichage dans CA Spectrum OneClick d'une interruption SNMP envoyée par une alerte CA Enterprise Log Manager. Le lien correspond à l'URL que vous pouvez coller dans votre navigateur pour affiche le tableau CA Enterprise Log Manager contenant les données détaillées au format CEG.



Informations complémentaires :

Exemple : Alerter CA Spectrum des changements de configuration (page 447)

Préparation de CA NSM pour recevoir des interruptions SNMP à partir d'alertes

Vous pouvez envoyer des alertes sous la forme d'interruptions SNMP à partir de CA Enterprise Log Manager vers n'importe quelle destination de votre réseau capable de recevoir et d'interpréter des interruptions. Chaque produit récepteur d'interruptions a ses propres exigences.

Préparez CA NSM à recevoir des interruptions à partir d'alertes par :

- Vérification de la conformité du système CA NSM de destination à la configuration système requise pour la réception de données d'interruption SNMP provenant de CA Enterprise Log Manager
- Configuration de CA NSM pour la réception d'interruptions SNMP, y compris l'activation de la prise en charge de SNMP v3, la modification des affectations de ports dans divers fichiers et le lancement des services requis

Préparez CA NSM à interpréter des interruptions à partir d'alertes d'action par :

- Création d'un fichier d'interruption pour chaque alerte devant être envoyée comme interruption SNMP à CA NSM.
- Garantie du chargement des fichiers CA-ELM.MIB et d'interruption respectifs.

Informations complémentaires :

Configuration système requise pour CA NSM (page 453)
Configuration de CA NSM pour la réception d'interruptions SNMP (page 454)

Configuration système requise pour CA NSM

Vous pouvez envoyer des interruptions SNMP à CA NSM si votre système présente la configuration d'interface CA Enterprise Log Manager suivante.

- La version de CA NSM est CA NSM r12.2 (version GA).
- CA NSM est installé sur Windows Server 2003 EE SP1.
- Vous avez appliqué le patch T5MK056.caz, qui met à jour le fichier aws_snmpex.dll et permet à CA NSM de recevoir des interruptions SNMP v3 provenant de CA Enterprise Log Manager.

Pour appliquer le patch

1. Téléchargez le patch sur le site de support de CA.
2. Connectez-vous au serveur avec CA NSM.
3. Arrêtez le service des interruptions SNMP.
   a. Dans le menu Démarrer, sélectionnez Programmes > Outils d'administration > Services.

      La liste de services apparaît.

   b. Sélectionnez le service des interruptions SNMP, cliquez avec le bouton droit de la souris et sélectionnez Arrêter dans le menu contextuel.
4. Arrêtez tous les services CA NSM.
   a. Accédez à l'invite de commande.
   b. Entrez la commande suivante.

      ```
      Unicntrl stop all
      ```
5. Copiez le fichier patch téléchargé, T5MK056.caz, dans le dossier C:\temp.
6. Décompressez le fichier patch à l'aide de cazipxp.

   ```
   Cazipxp.exe –u T5MK056.caz
   ```
7. Sauvegardez le fichier aws_snmpex.dll existant avant de le remplacer.
   a. Accédez à C:\Program Files\CA\SC\CCS\AT\SERVICES\BIN.
   b. Cliquez avec le bouton droit de la souris sur le fichier aws_snmpex.dll et sélectionnez Copier.

      Une copie du fichier aws_snmpex.dll est ajoutée au dossier.
8. Copiez le fichier aws_snmpex.dll du dossier temp vers le dossier bin (C:\Program Files\CA\SC\CCS\AT\SERVICES\BIN)

   CA NSM présente désormais la configuration système requise. Vous pouvez configurer CA NSM pour recevoir des interruptions SNMP provenant de CA Enterprise Log Manager.

Configuration de CA NSM pour la réception d'interruptions SNMP

Avant de pouvoir diriger des alertes à envoyer à CA NSM sous la forme d'interruptions SNMP, vous devez configurer CA NSM pour recevoir des interruptions. Vous pouvez envoyer des interruptions SNMP v2 comme SNMP v3 à CA NSM.

Pour configurer CA NSM pour recevoir des interruptions SNMP provenant d'alertes CA Enterprise Log Manager

1. Connectez-vous à CA NSM.
2. Activez la prise en charge de SNMP v3 comme suit.
   a. Affichez l'invite de commande. Dans le menu Démarrer, cliquez sur Exécuter, saisissez cmd, puis cliquez sur OK.
   b. Saisissez la commande suivante.

      caugui settings

      La fenêtre Paramètres EM apparaît.
   c. Cliquez sur l'onglet Gestion des événements.
   d. Faites défiler pour afficher la description : SNMP - Activer la prise en charge de SNMP v3.
   e. Sélectionnez la ligne et saisissez O pour sélectionner OUI dans la colonne de paramètre pour SNMP - Activer la prise en charge de SNMP v3.
   f. Cliquez sur Oui pour confirmer la modification.
   g. Fermez la fenêtre.

3. Remplacez le port utilisé par le service SNMP à partir du port actuel, 5162 par exemple, par le port 162 comme suit.
   a. Ouvrez l'explorateur Windows.
   b. Accédez au dossier .../System32/drivers/etc, en général situé sous C:\WINDOWS.
   c. Sauvegardez le fichier Services. Cliquez avec le bouton droit sur Services et sélectionnez Copier.
   d. Ouvrez le fichier Services dans un éditeur de texte, le Bloc-notes par exemple, puis faites défiler jusqu'à l'entrée qui ressemble à ce qui suit.

      ```
      snmptrap    162/udp    snmp-trap  #SNMP trap
      ```

   e. Modifiez la ligne snmptrap pour remplacer le numéro de port 162 par une alternative, 5162 par exemple. Ajoutez la ligne catrapmuxd où vous affectez le port 162.

      ```
      snmptrap    5162/udp
      catrapmuxd  162/udp    catrapmuxd  #CA Trap Multiplexer
      ```

   f. Enregistrez et fermez le fichier.
4. Modifiez le fichier de configuration CA Trap Multiplexer, catrapmux.conf, comme suit.
   a. Accédez à C:\Program Files\CA\SC\CCS\WVEM\CAIUSER.
   b. Ouvrez le fichier CATRAPMUX.CONF dans un éditeur de texte, le Bloc-notes par exemple.
   c. Faites défiler jusqu'à la fin du fichier. Modifiez le fichier comme vous le souhaitez pour inclure les entrées suivantes.

      ```
      CATRAPMUX_CMD:6161
      AWS_SNMP:6162
      catrapd:6163
      snmptrap:5162
      ```

      Remarque : Les trois premières entrées représentent les paramètres par défaut.
   d. Enregistrez et fermez le fichier.

5. Ajoutez une ligne au fichier de configuration snmpv3.dat pour configurer les paramètres de sécurité SNMP v3.

   a. Accédez à C:\Program Files\CA\SC\CCS\CommonResourcePackages\Misc.

   b. Ouvrez le fichier snmpv3.dat dans un éditeur de texte et ajoutez la ligne suivante à la fin du fichier.

      ```
      *.*.*.*.*:*          test1234:AuthPriv:MD5:test1234:DES:test1234
      ```

      Remarque : Il s'agit de paramètres identiques à ceux que vous devez saisir dans la boîte de dialogue Paramètres de sécurité SNMP v3 dans l'assistant d'alerte afin que CA NSM reçoive l'interruption SNMP. Le nom d'utilisateur et le mot de passe sont ceux que vous configurez ici, le protocole d'authentification est MD5 et le protocole de chiffrement DES.

   c. Enregistrez et fermez le fichier.

6. Installez le service CA Trap Multiplexer.

   a. Accédez à l'invite de commande.

   b. Exécutez la commande ci-dessous.

      ```
      catrapmuxd uniconfig
      ```

      CA Trap Multiplexer est ajouté à la liste de services avec un statut Démarré.

7. Vérifiez que CA Trap Multiplexer fonctionne et lancez le service des interruptions SNMP.

   a. Dans le menu Démarrer, sélectionnez Programmes > Outils d'administration > Services.

      La liste de services apparaît.

   b. Examinez l'état de CA Trap Multiplexer. Vérifiez que l'état est Démarré.

   c. Sélectionnez le service des interruptions SNMP, cliquez avec le bouton droit de la souris et sélectionnez Démarrer dans le menu contextuel.

8. Lancez tous les services avec un type de démarrage automatique.

   a. Accédez à l'invite de commande.

   b. Exécutez la commande ci-dessous.

      ```
      Unicntrl start all
      ```

   CA NSM est maintenant configuré pour recevoir des interruptions SNMP v3 basées sur des alertes planifiées envoyées par CA Enterprise Log Manager.

Exemple : Alerter CA NSM des changements de configuration

Avant d'envoyer des interruptions SNMP à CA NSM pour la première fois, il est recommandé d'identifier les requêtes qui renvoient des résultats appropriés vers cette destination. Les changements de configuration sont des événements susceptibles d'intéresser un gestionnaire de sécurité réseau.

L'exemple suivant a été conçu pour vous guider dans un processus d'alerte CA NSM des changements de configuration. Ce processus inclut les procédures suivantes :

- Envoi des interruptions SNMP à CA NSM
- Vérification de la réussite de l'envoi des interruptions SNMP
- Accès à la console EM sur CA NSM
- Affichage des interruptions SNMP reçues par CA Spectrum.

Informations complémentaires :

Envoi des interruptions SNMPv3 à CA NSM (page 457)
Suivi de la progression du job d'alerte (page 461)
Accédez à la console EM sur CA NSM. (page 462)
Affichage des interruptions SNMP sur CA NSM (page 463)

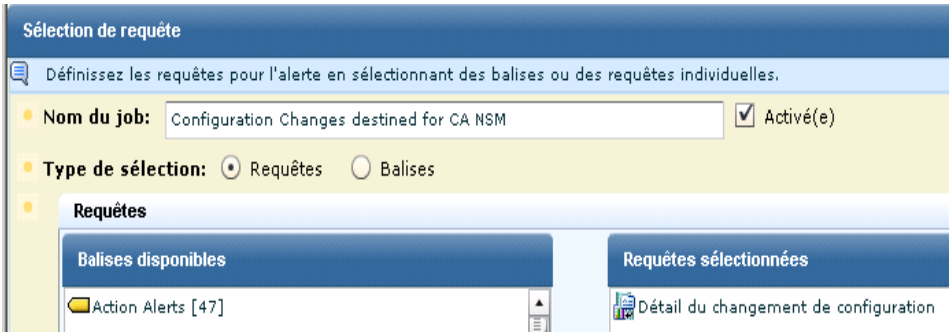
Envoi des interruptions SNMPv3 à CA NSM

Lors de la planification des alertes à envoyer à CA NSM, identifiez les résultats de requête susceptibles d'intéresser le centre des opérations réseau. Par exemple, pensez aux requêtes qui détectent les changements de configuration. L'exemple suivant illustre comment envoyer une alerte planifiée en fonction de la requête Détail du changement de configuration. Cette alerte indique CA NSM comme destination des interruptions SNMP.

Pour envoyer des interruptions SNMPv3 à CA NSM :

1. Ouvrez l'assistant de planification d'alerte.
    a. Connectez-vous à CA Enterprise Log Manager avec les informations d'identification du rôle Analyst ou Administrator.
    b. Cliquez sur l'onglet Gestion des alertes, puis sur le sous-onglet Planification d'alerte.
    c. Cliquez sur le bouton Planifier une alerte d'action.

2. Complétez l'étape Sélection d'alerte.
   a. Saisissez un nom de job. Par exemple, entrez les changements de configuration destinés à CA NSM.
   b. Vérifiez que le type de sélection est Requêtes. Dans le cas d'alertes basées sur des balises, vous ne pouvez pas choisir la destination des interruptions SNMP.
   c. Sélectionnez les requêtes que vous avez identifiées précédemment. Par exemple, sélectionnez Détail du changement de configuration.



3. Complétez les étapes Filtres d'alerte, Conditions de résultat et Planifier des jobs en vous référant, si nécessaire, à l'aide en ligne de cet assistant (facultatif).
4. Cliquez sur Destination, puis sur l'onglet Interruption SNMP.
5. Examinez les entrées du port et du serveur de destination. Si elles ne sont pas correctes, entrez l'adresse IP correcte du port et du serveur de destination. Pour ajouter des serveurs de destination supplémentaires, cliquez sur Ajouter, puis entrez la destination supplémentaire.

6. Spécifiez les informations sur la version SNMP. Par défaut, la version SNMP v2 est sélectionnée.

   a. Cliquez sur SNMP v3, étant donné que CA NSM est configuré pour accepter les interruptions SNMP v3.

   b. Cliquez sur Fonctionnalités de sécurité de la version 3.

      La boîte de dialogue Paramètres de sécurité SNMP v3 apparaît.

      Important : Les entrées de cette boîte de dialogue doivent correspondre aux paramètres du fichier snmpv3.dat que vous avez configurés pour permettre à CA NSM de recevoir des interruptions SNMP à partir des alertes CA Enterprise Log Manager. Voici la configuration recommandée.

      ::*:*:*:* <nom d'utilisateur>:AuthPriv:MD5:<mot de passe>:DES:<mot de passe>

   c. Sélectionnez Authentification. Saisissez le nom de l'utilisateur configuré pour Nom d'utilisateur, saisissez le mot de passe configuré pour Mot de passe et sélectionnez MD5 pour le protocole.

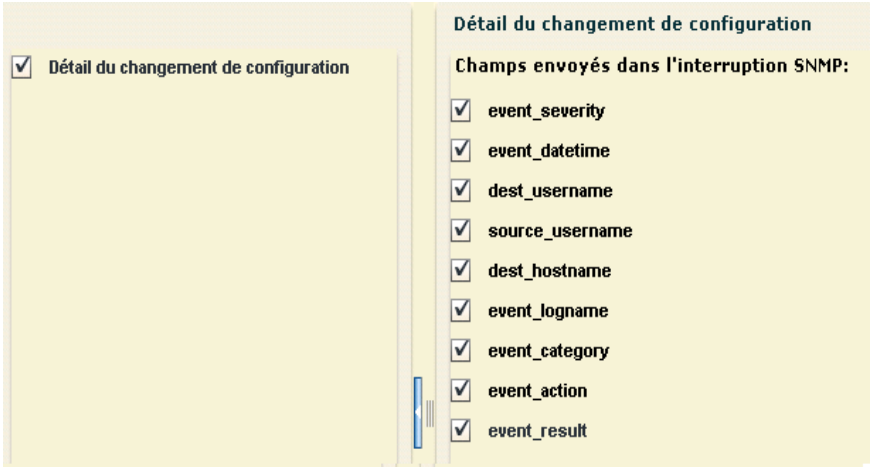
   d. Sélectionnez Chiffrement. Saisissez le mot de passe configuré pour Mot de passe et sélectionnez DES pour le protocole.

   e. Cliquez sur OK.

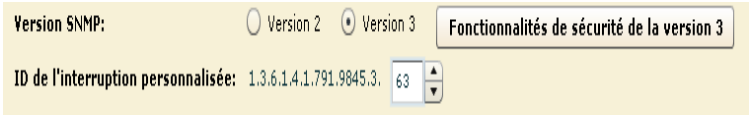
      Voici un exemple.

7. Sélectionnez la requête à envoyer en tant qu'interruption SNMP.

   Dans cet exemple, lorsque vous sélectionnez Détail du changement de configuration, les champs de cette requête s'affichent lorsqu'ils sont sélectionnés. Vous pouvez éventuellement effacer les champs que vous ne souhaitez pas inclure comme interruption.



8. Sélectionnez le numéro du nœud final pour le numéro elmTrap de l'OID, identifiant de l'interruption personnalisée. Ce numéro est spécifique au site et fait référence à un fichier semblable au fichier CA-ELM.MIB, sauf qu'il contient uniquement des valeurs destinées aux champs envoyés par cette interruption. Dans l'interruption personnalisée, les références aux champs sont répertoriées dans le même ordre que l'ordre d'envoi des champs. Si le fichier d'interruption personnalisé est nommé 1.3.6.1.4.1.791.9845.3.63, sélectionnez 63 dans la roue de nombres.



9. Sélectionnez Serveurs (facultatif).

10. Cliquez sur Enregistrer et fermer.

    Le job apparaît dans la liste Jobs d'alertes d'action avec le nom de job configuré.

Informations complémentaires :

Accédez à la console EM sur CA NSM. (page 462)

Suivi de la progression du job d'alerte

Quand vous planifiez une alerte, la bonne pratique consiste à suivre la progression du job d'alerte lors de sa première exécution. Quand vous suivez sa progression, vérifiez qu'il s'exécute correctement et que les résultats rapportés sont ceux que vous aviez l'intention d'envoyer.

Pour contrôler la progression du job d'alerte et prévisualiser les résultats :

1. Affichez le job d'alerte que vous avez créé sur la liste des jobs d'alertes d'action. Un exemple abrégé est présenté ci-dessous.

Jobs d'alertes d'action

	Nom du job	Activation	Serveur	Récurrence	Heure de début
☐	Configuration Changes destined for CA	True	etr851l1-blade3	5 minutes	Lun. 30 nov. 2009 5:13:14

2. Pour suivre la progression du job d'alerte, affichez Détail des événements d'autosurveillance du système (facultatif). Cliquez deux fois sur une ligne pour afficher la visionneuse d'événements. Faites défiler jusqu'à result_string pour afficher la totalité du message indiqué dans la Description du résultat.

Action	Résultat	Description du résultat
Notification Creation	S	SNMP trap for Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on report
Resource Creation	S	Creation of job file while executing action alert for Alert Name [Configuration Changes destined for CA NSM] was Successful.
Alert Creation	S	Run Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr
Resource Modify	S	Update RSSFeed Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr6511l1-sun104] recurrence [5
Resource Execution	S	Query [Configuration Change Detail] run over logDepot [localhost] was successful .

3. Affichez les résultats renvoyés par les requêtes sélectionnées pour l'alerte que vous avez créée.

   a. Sélectionnez l'onglet Gestion des alertes, puis le sous-onglet Alertes d'action.

   b. Cliquez sur le nom de l'alerte que vous avez planifiée.

   c. Affichez les résultats de cette alerte.

   Remarque : En général, les données affichées ici sont les données affichées lors de l'ouverture de l'URL envoyée vers le serveur de destination. S'il existe une différence que vous voulez supprimer, modifiez l'alerte d'action pour réinitialiser l'heure de fin dynamique des Conditions de résultat. Par exemple, paramétrez-la sur "now", "-10 minutes".

Accédez à la console EM sur CA NSM.

Vous pouvez afficher les interruptions SNMP envoyées par CA Enterprise Log Manager à partir de CA NSM. Les interruptions SNMP s'affichent sous forme de messages sur la console EM.

Pour accéder à la console EM sur CA NSM :

1. Connectez-vous au serveur où la destination des interruptions SNMP, CA NSM, est installée.
2. Dans le menu Démarrer, sélectionnez Programmes > CA > Unicenter > NSM > Enterprise Management et EM Classic.

   La fenêtre EM pour Windows apparaît.
3. Double-cliquez sur Windows.

   La fenêtre <nom d'hôte> (Windows) apparaît.
4. Double-cliquez sur Evénement.

   La fenêtre <nom d'hôte> de l'événement (Windows) apparaît.
5. Double-cliquez sur Journaux de console.

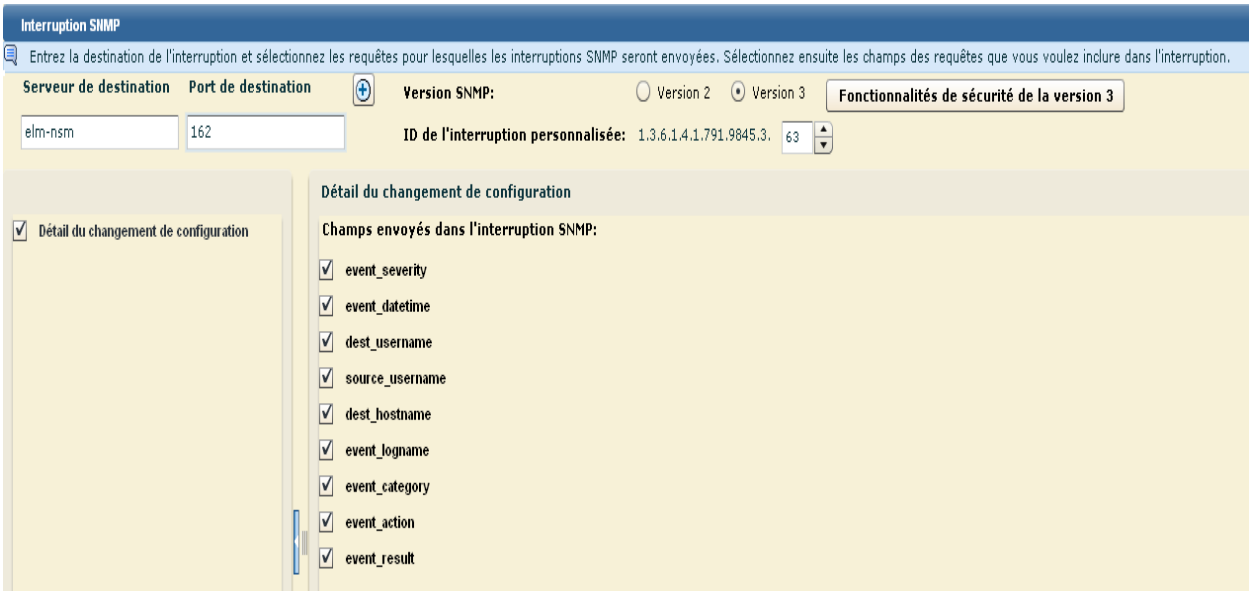
   La console EM (<nom d'hôte>) apparaît.

Informations complémentaires :

Affichage des interruptions SNMP sur CA NSM (page 463)

Affichage des interruptions SNMP sur CA NSM

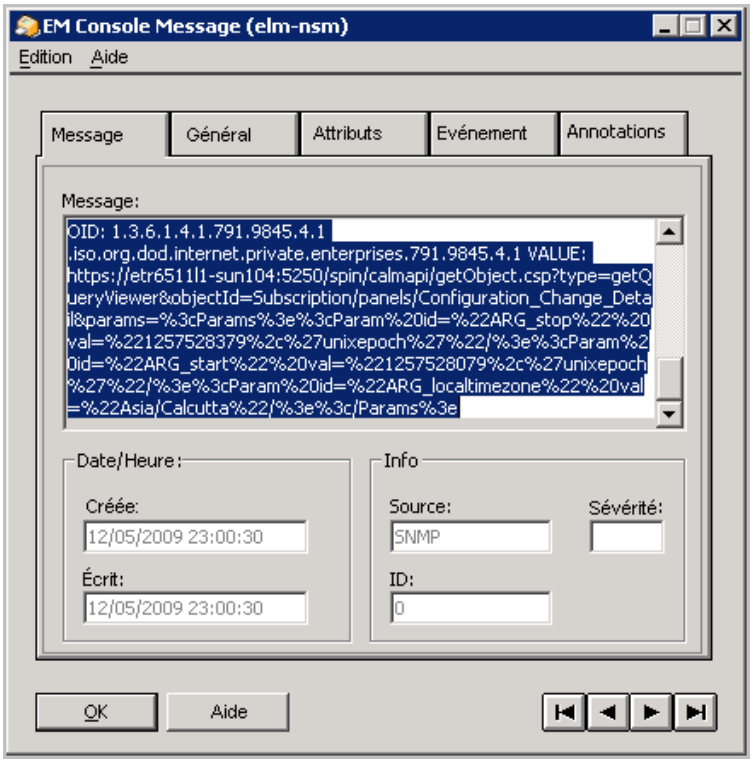
Imaginez l'exemple dans lequel une alerte est planifiée pour exécuter la requête Détail du changement de configuration. Dans cet exemple, l'identifiant d'interruption personnalisée est paramétrée sur 1.3.6.1.4.1.791.9845.3.63. Neuf champs sont envoyés en tant qu'interruption SNMP.



Pour afficher l'interruption SNMP envoyée par une alerte en fonction de la requête Détail du changement de configuration :

1. Quand un événement d'autosurveillance indique qu'une interruption SNMP a bien été envoyée à CA NSM, accédez à la console EM sur CA NSM.
2. Attendez jusqu'à ce qu'un message de journal s'affiche et indique la réception d'une interruption SNMP. Le message de cette interruption contient l'identifiant de l'interruption personnalisée, 1.3.6.1.4.1.791.9845.3.63.

3. Cliquez deux fois sur ce message pour le convertir dans un format qui permet la copie.



4. Copiez le message et collez-le dans un fichier texte temporaire.

   Le résultat devrait ressembler à ceci :

   %CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr6511l1-sun104.ca.com 6 63 0:05:00 12

   Indique que les données suivantes ont été reçues en tant qu'interruption SNMP.

   OID: 1.3.6.1.2.1.1.3.0 system.sysUpTime.0 VALUE: (30000) 0:05:00.00

   Spécifie l'identifiant de l'objet pour le temps de disponibilité en centièmes de secondes. Il s'agit d'un OID connu via SNMP.

   OID: 1.3.6.1.6.3.1.1.4.1.0 .iso.org.dod.internet.snmpV2.snmpModules.1.1.4.1.0 VALUE: **1.3.6.1.4.1.791.9845.3.63**

   Spécifie l'identifiant de l'objet pour snmpTrapOID. La valeur est l'identifiant d'interruption personnalisée que vous avez spécifié lors de la configuration de l'alerte.

   OID: 1.3.6.1.4.1.791.9845.2.80 .iso.org.dod.internet.private.enterprises.791.9845.2.80 VALUE: 2

   Spécifie l'identifiant d'objet (OID) pour event_severity et la valeur de sévérité de 2, qui signifie Information.

OID: 1.3.6.1.4.1.791.9845.2.65 .iso.org.dod.internet.private.enterprises.791.9845.2.65 VALUE: Fri Nov 06 2009 22:53:53

Spécifie l'identifiant d'objet (OID) pour event_datetime avec la valeur, le jour, la date et l'heure où l'événement doté de ces valeurs a eu lieu.

OID: 1.3.6.1.4.1.791.9845.2.17 .iso.org.dod.internet.private.enterprises.791.9845.2.17 VALUE:

Spécifie l'identifiant d'objet pour dest_username sans aucune valeur.

OID: 1.3.6.1.4.1.791.9845.2.1 .iso.org.dod.internet.private.enterprises.791.9845.2.1 VALUE:

Spécifie l'identifiant d'objet pour dest_username sans aucune valeur.

OID: 1.3.6.1.4.1.791.9845.2.22 .iso.org.dod.internet.private.enterprises.791.9845.2.22 VALUE: etr851l2-elm5:

Spécifie l'identifiant d'objet pour dest_hostname avec le nom d'hôte du serveur dans lequel les résultats de la requête sont affichés lorsque vous lancez l'URL.

OID: 1.3.6.1.4.1.791.9845.2.53 .iso.org.dod.internet.private.enterprises.791.9845.2.53 VALUE: EiamSdk

Spécifie l'identifiant d'objet pour event_logname, EiamSdk, le nom du fichier journal qui contient ces détails.

OID: 1.3.6.1.4.1.791.9845.2.77 .iso.org.dod.internet.private.enterprises.791.9845.2.77 VALUE: Configuration Management

Spécifie l'identifiant d'objet pour event_category et la valeur de la catégorie associée à la requête Détail du changement de configuration.

OID: 1.3.6.1.4.1.791.9845.2.75 .iso.org.dod.internet.private.enterprises.791.9845.2.75 VALUE: Configuration Change

Spécifie l'identifiant d'objet pour event_action et la valeur de l'action associée à la requête Détail du changement de configuration.

OID: 1.3.6.1.4.1.791.9845.2.81 .iso.org.dod.internet.private.enterprises.791.9845.2.81 VALUE: S

Spécifie l'identifiant d'objet pour event_result avec la valeur, S, pour Réussi.

OID: 1,3.6,1.4,1.791,9845.4,1 .iso.org.dod.internet.private.enterprises.791.9845.4.1 VALUE: https://etr6511l1-sun104:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/Configuration_Change_Detail&params=%3cParams%3e%3cParam%20id=%22ARG_stop%22%20val=%2212575283779%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_start%22%20val=%2212575280790%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_localtimezone%22%20val=%22Asia/Calcutta%22/%3e%3c/Params%3e

Spécifie l'identifiant d'objet pour calmAPIURL sous elmDynamicVariables. La valeur est l'URL vers l'API CA Enterprise Log Manager. Après la connexion, vous pouvez afficher les résultats de la requête sous forme de tableau ou de graphique.

5. Copiez l'URL à la fin du message, collez-le dans un navigateur et lancez l'URL.

6. Connectez-vous à CA Enterprise Log Manager.

   Le graphique s'affiche. dans l'exemple suivant s'affiche.

Création d'une alerte d'action

La procédure de création d'une alerte d'action, à l'aide de l'assistant de planification d'alerte d'action, se compose principalement des étapes suivantes.

1. Ouverture de l'assistant de planification d'alerte d'action
2. Choix de la requête ou des balises sur lesquelles l'alerte est basée
3. Définition de filtres avancés pour définir plus précisément la requête d'alerte (facultatif)
4. Définition de la plage de dates et des conditions de résultat (facultatif)
5. Définition de la fréquence du job d'alerte et de ses périodes d'activité (facultatif)
6. Configuration de courriels d'alerte automatiques et de destinataires (facultatif)
7. Choix entre deux possibilités : exécuter la requête sur les données pour le serveur sélectionné uniquement ou l'exécuter pour ce serveur et tous ses descendants (facultatif).

Informations complémentaires :

Ouverture de l'assistant de planification d'alerte d'action (page 467)
Création d'un filtre d'événement avancé (page 303)
Définition des conditions de résultats (page 304)
Définition de destinations des notifications (page 476)
Définition de la destination des requêtes de job d'alerte (page 481)

Ouverture de l'assistant de planification d'alerte d'action

Pour créer un job d'alerte d'action, vous devez utiliser l'assistant de planification d'alerte d'action.

Pour ouvrir l'assistant de planification d'alerte d'action

1. Cliquez sur l'onglet Gestion des alertes.

   La liste Serveurs d'alerte s'affiche.

2. Sélectionnez le serveur sur lequel planifier un job d'alerte.

   Le volet Détails du serveur affiche le serveur sélectionné ; l'onglet Rapports générés est ouvert par défaut.

3. Cliquez sur l'onglet Planification d'alerte, puis sur le bouton Planifier une alerte.

   L'assistant de planification des alertes d'action s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer et fermer pour enregistrer l'alerte d'action et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires

Définition de la destination des notifications par courriel (page 477)
Définition de la destination des requêtes de job d'alerte (page 481)

Sélection d'une requête d'alerte

Sélectionnez les balises ou requêtes sur lesquelles baser un nouveau job d'alerte d'action. La requête, ainsi que tout filtre que vous ajoutez, définit les circonstances dans lesquelles une alerte est générée. Par exemple, pour créer une alerte afin de surveiller le trafic depuis un hôte ou un port, utilisez la requête Tous les événements, ajoutez des filtres pour définir les hôtes source à surveiller, ainsi qu'un seuil d'événements.

Remarque : Une catégorie de requête appelée Alertes d'action est fournie. Cette balise de catégorie contient plusieurs requêtes conçues pour être utilisées dans les alertes d'action.

Pour sélectionner une requête d'alerte

1. Ouvrez l'assistant de planification d'alerte d'action.
2. Saisissez un nom de job.
3. Dans le menu déroulant de fuseau horaire, sélectionnez le fuseau horaire dans lequel vous souhaitez planifier le rapport.
4. Sélectionnez le bouton d'option Requêtes ou Balises pour sélectionner les rapports par balise ou de manière séparée.

   Remarque : La planification des alertes par balise vous permet d'ajouter des alertes sans modifier le job lui-même. Si vous sélectionnez la balise "Gestion des identités", toute alerte associée à cette balise est ajoutée au job à l'heure d'exécution planifiée. Vous pouvez ajouter une nouvelle alerte au job en attribuant la balise Gestion des identités à une requête. Cette fonction s'applique également aux balises personnalisées.

   (Facultatif) Désactivez la case Activer pour activer l'alerte d'action ultérieurement et non pas dès que vous l'avez terminée. Cette case à cocher est activée par défaut.

   Remarque : La possibilité de créer un job d'alerte désactivé a été conçue pour une utilisation avec des alertes récurrentes. Si vous désactivez la case à cocher Activé d'un job, puis que vous créez ce job avec une occurrence unique ("Maintenant" ou "Une fois"), il est supprimé de la liste Alerte planifiée.
5. Sélectionnez une ou plusieurs balises pour limiter le nombre de balises et de rapports affichés (facultatif). Cette fonction se comporte de la même manière que la Liste de rapports.
6. Sélectionnez les balises ou requêtes que vous souhaitez utiliser en tant que modèles et utilisez le contrôle de déplacement pour les ajouter à la zone Requêtes sélectionnées. La catégorie de requêtes Alertes d'action contient des requêtes conçues pour divers besoins d'alertes courants.
7. Accédez à la prochaine étape de planification que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

Si vous cliquez sur Enregistrer et fermer, le job d'alerte est planifié. Sinon, l'étape sélectionnée apparaît.

Informations complémentaires :

Création d'un filtre d'événement avancé (page 303)
Définition des conditions de résultats (page 304)

Utilisation des filtres avancés

Vous pouvez utiliser des filtres avancés en langage SQL pour qualifier une fonction qui interroge le magasin de journaux d'événements, y compris pour limiter des requêtes ou personnaliser des filtres rapides. L'interface Filtres avancés vous aide à créer la syntaxe de filtre appropriée grâce à un formulaire de saisie des colonnes logiques, opérateurs et valeurs, selon vos besoins de filtrage.

Remarque : Cette section contient une brève présentation des termes SQL utilisés dans les filtres avancés. Pour utiliser les filtres avancés au maximum de leur potentiel, vous devez posséder une connaissance approfondie de la grammaire SQL et de la grammaire commune aux événements.

Les termes SQL suivants permettent d'associer plusieurs instructions de filtre;

And

Affiche les informations de l'événement si *tous* les termes ajoutés sont vrais.

Or

Affiche les informations de l'événement si *l'un* des termes ajoutés est vrai.

Having

Restreint les termes de l'instruction SQL principale en ajoutant une instruction de qualification. Par exemple, vous pouvez définir un filtre avancé pour les événements issus d'hôtes spécifiés et ajouter une instruction "having" afin de limiter les résultats aux événements d'un niveau de sévérité défini.

Les opérateurs SQL suivants sont utilisés par les filtres avancés pour créer les conditions de base.

Opérateurs relationnels

Inclut les informations de l'événement si la colonne porte la relation appropriée à la valeur saisie. Les opérateurs relationnels suivants sont disponibles.

- Egal à
- Différent de
- Inférieur à
- Supérieur à
- Inférieur ou égal à
- Supérieur ou égal à

Par exemple, l'utilisation de *Supérieur à* inclut les informations de l'événement à partir de la colonne choisie si sa valeur est supérieure à la valeur définie.

Comme

Inclut les informations de l'événement si la colonne contient le modèle que vous avez saisi à l'aide du signe %. Par exemple, L% renvoie toutes les valeurs commençant par L, %L% renvoie toutes les valeurs contenant L comme valeur mais pas comme première ou dernière lettre.

Distinct de

Inclut les informations de l'événement si la colonne ne contient pas le modèle spécifié.

Dans l'ensemble

Inclut les informations de l'événement si la colonne contient au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Hors ensemble

Inclut les informations de l'événement si la colonne ne contient pas au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Correspondance

Inclut toute information d'événement qui correspond au moins à un des caractères que vous avez saisis, ce qui vous permet de rechercher des mots clés.

A clés

Inclut toute information d'événement définie comme une valeur clé pendant la configuration du serveur de rapports. Vous pouvez utiliser les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Sans clé

Inclut toute information d'événement non définie comme une valeur clé pendant la configuration du serveur de rapports. Vous pouvez utiliser les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Définition des conditions de résultats

Vous pouvez définir une plage de dates et d'autres conditions de résultat pour la requête, notamment les limites des lignes et la période d'affichage de base. Les conditions de résultats peuvent être modifiées à tout moment jusqu'à l'heure d'exécution de la requête, ce qui en fait une méthode pratique pour modifier des requêtes sans remanier la requête de base ou ses filtres.

Vous pouvez définir les types suivants de conditions de résultats.

- Les conditions de plage de dates régissant la période de recherche de la requête
- Les conditions d'affichage, telles que le nombre maximum de lignes
- Les conditions d'événements regroupés, comme les événements regroupés les plus récents après une date donnée ou les événements regroupés contenant un nombre défini d'événements

  Remarque : Si vous ne regroupez pas au moins une colonne lors de la création d'une requête, les utilisateurs ne pourront pas modifier les conditions de résultats depuis l'affichage de la requête.

Définition d'une période ou d'une plage de dates

Vous pouvez définir des conditions de période ou de plage de dates pour votre requête. Cela améliore l'efficacité de votre requête en limitant la zone de recherche du magasin de journaux d'événements.

Vous pouvez sélectionner une plage horaire prédéfinie ou créer une plage personnalisée. Pour qu'une plage puisse fonctionner correctement, vous devez définir une heure de début et de fin. Si vous ne rentrez qu'un seul de ces paramètres, la période est exprimée par une clause "Where" dans la requête SQL.

Pour définir des conditions de résultat

1. Ouvrez la boîte de dialogue Conditions de résultats.
2. Sélectionnez une plage horaire prédéfinie dans la liste déroulante. Si vous souhaitez par exemple afficher les événements reçus hier, sélectionnez "jour précédent".

   Remarque : Lors de la création d'une alerte d'action ou d'un rapport planifié, l'interface affiche les périodes suivantes par défaut.

   - Alerte d'action : les 5 dernières minutes
   - Rapport planifié : les 6 dernières heures
3. Créez une plage personnalisée, en suivant les étapes ci-après (facultatif) :

   a. Dans la zone Sélection d'une plage de dates, cliquez sur Modifier en regard du champ de saisie Heure de fin dynamique. Cela vous permet de définir la fin de la période dans laquelle vous souhaitez effectuer la requête.

      La boîte de dialogue Spécification de la période dynamique s'affiche.

   b. Sélectionnez l'heure de référence pour le paramètre, puis cliquez sur Ajouter.

   c. Sélectionnez le paramètre d'heure de votre choix, puis cliquez sur Ajouter. Vous pouvez ajouter plusieurs paramètres d'heure.

   d. Cliquez sur OK lorsque vous avez terminé.

      Fermez la boîte de dialogue Spécification de la période dynamique. La valeur choisie s'affiche dans la zone Heure de fin dynamique. Dans ce cas, ils forment une instruction de temps complète, chaque paramètre se référant au premier. Par exemple, les valeurs Début du mois et Jour de la semaine - mardi ajoutées à la zone Heure de fin dynamique terminent votre requête le premier mardi du mois.

Remarque : Lorsque vous utilisez les valeurs Nombre de, telles que Nombre de jours ou Nombre d'heures, vous devez saisir un nombre *négatif* pour définir une période dans le passé. Un nombre positif définit une heure de fin dans le futur et la requête risque de continuer à envoyer des résultats, au moins jusqu'à ce qu'un événement qualifié figure dans le magasin de journaux.

Par exemple, les valeurs maintenant et nombre de minutes - 10 ajoutées à la zone Heure de début dynamique débutent votre requête 10 minutes avant l'heure de fin sélectionnée.

e. Dans la zone Heure de début dynamique, répétez l'étape 2 pour définir le début de la période sur laquelle vous souhaitez effectuer une requête.

Si vous n'entrez pas de plage de dates, la requête s'applique à tous les événements du magasin de journaux.

4. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Informations complémentaires :

Création d'une requête (page 295)
Définition des conditions de résultats (page 304)
Définition des conditions d'affichage et de groupe (page 307)

Définition des conditions d'affichage et de groupe

Vous pouvez définir des conditions qui vous permettent de contrôler l'affichage des requêtes et les conditions de recherche des événements en fonction de leur regroupement.

Pour définir des conditions d'affichage et de groupe

1. Ouvrez la boîte de dialogue Conditions de résultats.
2. Utilisez les cases à cocher Résultats pour activer, si besoin, les qualifications d'affichage suivantes.

   Limite des lignes

   Définit le nombre maximum de lignes d'événements affichés par la requête, en commençant par les plus récents.

   Minimum : 1

   Maximum : 5 000

   Afficher d'autres infos

   Indique la présence d'autres résultats qui ne sont pas affichés en raison de la limite de lignes, ce qui vous permet de comparer les événements sélectionnés dans le contexte de tous les événements du même type. Par exemple, si vous choisissez une limite de 10 lignes dans l'affichage de la visionneuse d'événements et si vous sélectionnez Afficher d'autres infos, les événements au-delà de 10 s'affichent dans une entrée particulière intitulée Autres, qui présente l'ensemble des événements restants. Le paramètre n'est actif que lorsque l'option Limites des lignes est sélectionnée.

   Granularité temporelle

   Définit le niveau de détail du champ de période utilisé dans l'affichage des requêtes.

3. Utilisez Conditions de résultats pour effectuer une requête sur plusieurs types de conditions d'événements regroupés. Par exemple, vous pouvez définir votre requête de façon à rechercher le dernier événement regroupé à partir d'une date sélectionnée ou un certain nombre d'événements regroupés. Un événement regroupé est un événement ajusté pour lequel vous avez défini une Fonction et un Ordre de regroupement à l'étape Création d'une requête.

   Les conditions de groupe utilisent le même système d'instruction de temps que les champs de période.

4. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Informations complémentaires

Création d'une requête (page 295)
Définition des conditions de résultats (page 304)

Définition des paramètres de planification de jobs d'alerte

Vous pouvez contrôler le moment où vos alertes s'appliquent en définissant les heures de début et de fin. Vous pouvez également contrôler le degré de précision de l'alerte en déterminant la fréquence de la requête.

Pour définir les paramètres de planification d'un job d'alerte

1. Ouvrez l'assistant de planification d'alerte d'action, entrez les informations requises et avancez jusqu'à l'étape Planifier des jobs.
2. Définissez l'intervalle de récurrence souhaité. Un intervalle plus faible vous fait bénéficier d'une vue plus détaillée mais augmente le trafic réseau.

   Avant de définir un court intervalle, vérifiez que CA Enterprise Log Manager est synchronisé avec un serveur NTP.
3. Définissez les heures de début et de fin souhaitées pour le job d'alerte.
4. Accédez à la prochaine étape de planification que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le job d'alerte est planifié. Sinon, l'étape choisie apparaît.

Définition de destinations des notifications

Vous pouvez définir au moins l'une des destinations suivantes pour la notification d'une alerte.

- Courriel

  Vous pouvez définir une notification automatique par courriel pour une alerte, afin de vous assurer que le personnel concerné est informé des alertes liées à leurs rôles et responsabilités. Configurez un serveur de messagerie pour votre environnement CA Enterprise Log Manager avant d'envoyer des courriels de notification d'alerte.

- Processus CA IT PAM

  Vous pouvez exécuter le processus CA IT PAM spécifié si l'alerte concerne une condition nécessitant la notification du produit tiers. L'intégration avec CA IT PAM doit être configurée sous Serveur de rapports et le processus CA IT PAM doit être défini avant que vous puissiez exécuter le processus à partir des alertes.

- Interruption SNMP

  Vous pouvez envoyer des données d'événement capturées par une alerte à un ou plusieurs NOC. Vous pouvez cibler des serveurs de gestion tels que CA Spectrum ou CA NSM à l'aide d'interruptions SNMP v2 ou SNMP v3. Spécifiez les destinations lors du processus de planification de l'alerte. L'intégration avec SNMP doit être configurée avant que vous puissiez envoyer des alertes à l'aide de SNMP.

Remarque : Si vous ne définissez pas de destination, les résultats de l'alerte sont uniquement publiés dans le flux RSS.

Informations complémentaires :

Définition de la destination des notifications par courriel (page 477)
Définition des informations de CA IT PAM (page 478)
Exemple : Alerter CA Spectrum des changements de configuration (page 447)
Envoi des interruptions SNMPv3 à CA NSM (page 457)
Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par ligne (page 422)
Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par requête (page 427)

Définition de la destination des notifications par courriel

Vous pouvez paramétrer une notification automatique par courriel pour un job d'alerte, afin de vous assurer que le personnel concerné est informé des alertes liées à leurs rôles ou responsabilités. Cette étape est facultative.

Pour pouvoir définir des courriels de notification d'alerte, un serveur de messagerie doit être préalablement configuré pour votre environnement CA Enterprise Log Manager.

Pour paramétrer une notification d'alerte

1. Ouvrez l'assistant de planification d'alerte d'action, entrez les informations requises et avancez jusqu'à l'étape Destination.
2. Activez la case Activer les notifications par courriel.
3. Entrez au moins une adresse électronique de destinataire. Vous pouvez entrer plusieurs adresses en les séparant par des virgules.
4. Remplissez le champ De, indiquez un objet et rédigez le corps du message de notification (facultatif).

   Remarque : Le corps du message est écrit en langage HTML, si bien que l'ensemble du texte saisi apparaît sur une seule ligne. Pour insérer un saut de ligne, tapez
 à la fin de la ligne de texte.
5. Accédez à la prochaine étape de planification que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le job d'alerte est planifié. Sinon, l'étape sélectionnée apparaît.

Informations complémentaires :

Définition des informations de CA IT PAM (page 478)

Définition des informations de CA IT PAM

Vous pouvez définir votre job d'alerte pour exécuter un processus CA IT PAM lorsque l'alerte est générée.

Vous pouvez exécuter le processus une fois pour chaque ligne de résultat de la requête ou exécuter le processus configuré une fois, quel que soit le nombre de lignes. Si vous l'exécutez une fois par ligne, définissez les instructions récapitulatives et descriptives à l'aide des champs CEG pour transmettre les données d'événement à CA IT PAM. Sélectionnez les champs qui sont définis pour collecter les données par la requête. Si vous l'exécutez une fois par requête, une URL est automatiquement transmise à CA IT PAM qui, une fois lancé, affiche toutes les lignes des données d'événement. Dans le produit tiers qui répond au processus CA IT PAM, l'URL est annexée au texte récapitulatif que vous entrez. Par exemple, elle apparaît dans le champ Récapitulatif de CA Service Desk, s'il s'agit du produit tiers.

Pour exécuter un processus CA IT PAM lorsque l'alerte est générée

1. Ouvrez l'assistant de planification d'alerte d'action, entrez les informations requises et avancez jusqu'à l'étape Destination.
2. Cliquez sur l'onglet Processus CA IT PAM.

   Une case à cocher apparaît dans le volet gauche pour chaque requête de ce job d'alerte.
3. Sélectionnez une requête que vous souhaitez envoyer au processus CA IT PAM, puis effectuez l'une des actions suivantes.
   - Sélectionnez Exécuter le processus CA IT PAM par ligne pour exécuter le processus configuré une fois pour chaque ligne renvoyée.
   - Désélectionnez l'option Exécuter le processus CA IT PAM par ligne pour exécuter le processus configuré une fois, quel que soit le nombre de lignes renvoyées.
4. Vérifiez les entrées par défaut pour les paramètres de processus et modifiez-les si nécessaire. Pour les champs non définis qui permettent l'entrée d'informations récapitulatives ou descriptives, entrez une instruction significative. Si vous avez sélectionné Exécuter le processus CA IT PAM par ligne, utilisez les champs CEG pour transférer les données d'événement. Sélectionnez le champ CEG et cliquez sur Ajouter à côté du champ cible.
5. Si le processus CA IT PAM est défini avec les champs CEG en tant que paramètres locaux dans le jeu de données, sélectionnez ces champs CEG dans la liste Envoyer les valeurs de champs en tant que paramètres.
6. Sélectionnez une autre requête dans le volet gauche et répétez les étapes 3 à 6.

Remarque : Lorsque des requêtes pour un job d'alerte planifié renvoient des résultats, l'ensemble des informations et des paramètres requis pour l'exécution du processus configuré sont envoyés à CA IT PAM.

Informations complémentaires :

Définition de la destination des notifications par courriel (page 477)

Définition d'informations sur les interruptions SNMP

Vous pouvez définir des informations sur les interruptions SNMP pour un job d'alerte, ce qui vous permet d'envoyer l'alerte à un ou plusieurs systèmes de gestion tiers. Lorsque les requêtes sélectionnées renvoient des résultats, une interruption incluant les données renvoyées pour tous les champs sélectionnés à partir de l'ensemble des requêtes est envoyée à toutes les destinations d'interruption SNMP. Cette étape est facultative.

Pour définir des informations sur les interruptions SNMP

1. Ouvrez l'assistant de planification d'alerte d'action, entrez les informations requises et avancez jusqu'à l'étape Destination.
2. Sélectionnez l'onglet Interruption SNMP.

   L'onglet Interruption SNMP s'ouvre, affichant les champs Serveur de destination et Port de destination, ainsi qu'une liste des requêtes incluses dans l'alerte d'action, chacune avec une case à cocher.
3. Examinez les entrées du port et du serveur de destination par défaut. Si elles ne sont pas correctes, entrez l'adresse IP correcte ou le nom d'hôte complet et le numéro de port.
4. Cliquez sur Ajouter pour entrer des serveurs et des ports de destination supplémentaires (facultatif).
5. Pour envoyer l'alerte à l'aide de SNMP v3, sélectionnez SNMP v3 (facultatif). La version par défaut est SNMP v2.

6. Si vous sélectionnez SNMP v3, cliquez sur le bouton Fonctionnalités de sécurité de la version 3 pour définir l'authentification ou le chiffrement dans la boîte de dialogue Paramètres de sécurité.

   Important : Les entrées de cette boîte de dialogue doivent correspondre aux paramètres du fichier snmpv3.dat que vous avez configurés pour permettre à CA NSM de recevoir des interruptions SNMP à partir des alertes CA Enterprise Log Manager. Voici la configuration recommandée.

   ..*.*.*:* <nom d'utilisateur>:AuthPriv:MD5:<mot de passe>:DES:<mot de passe>

   a. Sélectionnez Authentification. Saisissez le nom de l'utilisateur configuré pour Nom d'utilisateur, saisissez le mot de passe configuré pour Mot de passe et sélectionnez MD5 pour le protocole.

   b. Sélectionnez Chiffrement. Saisissez le mot de passe configuré pour Mot de passe et sélectionnez DES pour le protocole.

7. (Facultatif et spécifique à CA NSM) Configurez le dernier nœud du fichier d'interruption personnalisé à utiliser. Ce paramètre permet à CA NSM de traiter correctement l'interruption. Le traducteur NSM affecte chaque champ de l'interruption de façon séquentielle à chaque paramètre varbind du fichier d'interruption. Le fichier d'interruption que vous spécifiez ici doit contenir les paramètres varbind extraits de la base de données d'informations de gestion pour chaque champ CEG de la séquence envoyée par l'interruption. Les valeurs valides sont comprises entre 1 et 999. La valeur par défaut est 1.

8. Sélectionnez la case à cocher à côté de toute requête que vous souhaitez inclure dans l'interruption SNMP. Par exemple, si vous avez trois requêtes dans la liste, vous pouvez définir SNMP pour en fournir une, deux ou les trois.

   La sélection d'une requête affiche les champs inclus dans chaque requête, chacune avec une case à cocher sélectionnée. Vous pouvez effacer n'importe quel champ sélectionné pour supprimer ce champ de l'alerte.

9. Accédez à la prochaine étape de planification que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le job d'alerte est planifié. Sinon, l'étape sélectionnée apparaît.

Définition de la destination des requêtes de job d'alerte

Vous pouvez choisir les magasins de journaux d'événements fédérés qui sont interrogés par le job d'alerte.

Pour choisir les destinations de rapport

1. Ouvrez l'assistant de planification d'alerte d'action, entrez les informations requises et avancez jusqu'à l'étape Sélection de serveur.
2. Sélectionnez tous les serveurs disponibles à interroger et déplacez-les dans la zone Serveurs sélectionnés à l'aide du contrôle de déplacement.
3. Si vous souhaitez désactiver les requêtes fédérées pour ce job d'alerte, sélectionnez Non dans le menu déroulant qui apparaît lorsque vous cliquez sur l'entrée Requêtes fédérées (facultatif). Les requêtes de rapport sont fédérées par défaut.
4. Accédez à la prochaine étape de planification que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le job d'alerte est planifié. Sinon, l'étape choisie apparaît.

Exemple : Création d'une alerte d'action pour un espace disque faible

La requête Espace disque disponible faible est l'une des requêtes prédéfinies avec la balise Alertes d'action. Les requêtes comprenant la balise Alertes d'action sont spécialement conçues pour être utilisées en tant qu'alertes, mais elles ne deviennent pas des alertes tant que vous ne les planifiez pas.

L'exemple suivant montre comment créer une alerte d'action à partir de la requête prédéfinie Espace disque disponible faible.

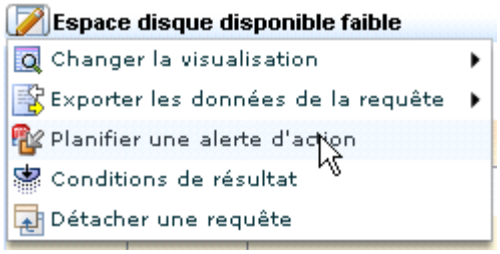
1. Cliquez sur l'onglet Requêtes et rapports et sur le sous-onglet Requêtes.

   Les volets Filtre de balise de requête et Liste de requêtes s'affichent.
2. Cliquez sur la balise Alertes d'action.

   La Liste de requêtes affiche les requêtes associées à la balise Alertes d'action.
3. Dans la liste, cliquez sur la requête Espace disque disponible faible.

   La requête Espace disque disponible faible apparaît dans le volet principal.

4. Cliquez sur Options et sélectionnez Planifier des alertes d'action.



L'assistant de planification des alertes d'action s'ouvre sur l'étape Sélection d'alerte. L'option Espace disque disponible faible est présélectionnée sous Requêtes sélectionnées.

5. Entrez un nom de job, tel que Espace disque faible. Désélectionnez la case à cocher Activé(e) pour le moment. Vous pouvez ainsi enregistrer et fermer la planification d'alerte d'action avant qu'elle ne soit complète sans risquer de tenter de l'exécuter.

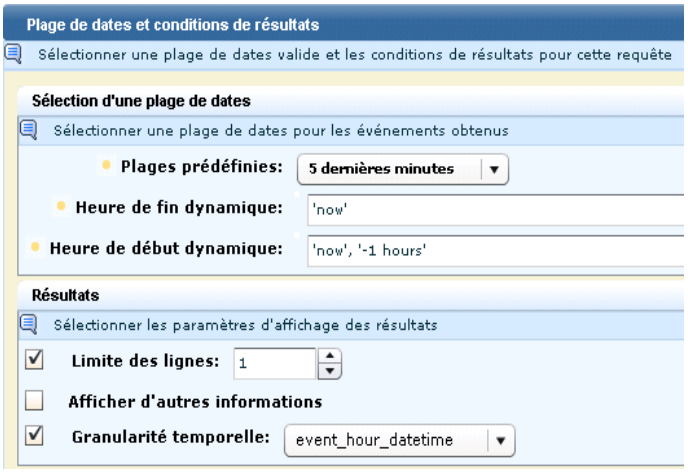
6. Vous pouvez entrer ou ignorer les Filtres d'alerte. Les filtres s'additionnent : lorsqu'une série de filtres est évaluée, ces filtres sont reliés les uns aux autres par l'opérateur logique AND.

7. Cliquez sur Conditions de résultat pour annuler ceux spécifiés dans la définition de requête.

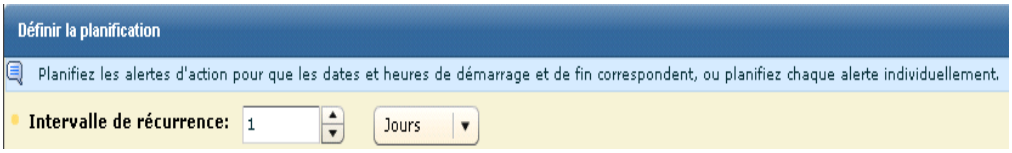
   a. Pour indiquer que l'alerte doit évaluer l'espace disque pour la dernière heure écoulée, entrez la plage de dates suivante : 'maintenant' pour Heure de fin dynamique et 'maintenant' '- 1 heure' pour Heure de début dynamique.

   b. Pour indiquer que vous souhaitez être averti uniquement si la requête renvoie un résultat et n'afficher que le premier résultat généré, sélectionnez Limite des lignes et la valeur 1. La plage de temps dynamique étant exprimée en heures, sélectionnez event_hour_datetime comme Granularité temporelle.

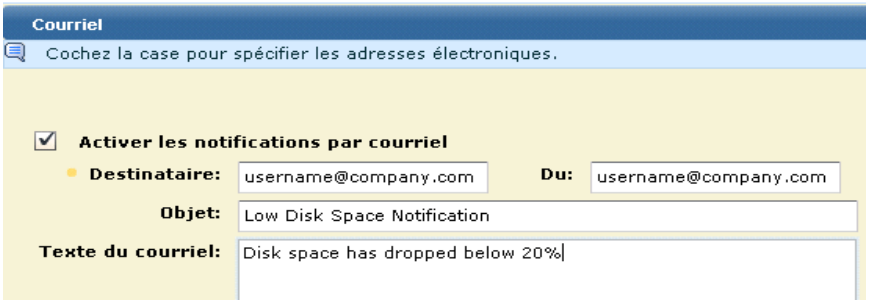
   c. Laissez l'option "événement(s) regroupé(s)" vide, car elle ne s'applique pas à cette requête.



8. Cliquez sur Planifier des jobs pour définir la planification. La méthode par défaut consiste à démarrer le job immédiatement sans date de fin. Définissez l'intervalle de récurrence. Par exemple, choisissez d'exécuter la requête toutes les heures.



9. Cliquez sur l'étape Destination. Sélectionnez Activer les notifications par courriel ; entrez votre adresse électronique dans le champ Destinataire. Entrez un objet et le texte du courriel si vous le souhaitez. Vous pouvez également envoyer le courriel aux destinataires désirés et entrez votre adresse électronique dans le champ De. Si vous entrez plusieurs adresses électroniques, séparez-les par une virgule (et non un point-virgule).



10. Cliquez sur Sélection de serveur. Par défaut, la requête s'exécute sur le serveur CA Enterprise Log Manager en cours. Sélectionnez Fédéré(e) pour exécuter la requête sur ce serveur et toutes les requêtes fédérées concernées.
11. Cliquez sur Sélection d'alerte. Sélectionnée Activé(e).
12. Cliquez sur Enregistrer et fermer.

    Le job d'alerte d'action s'affiche dans le sous-onglet Planification d'alerte.

Jobs d'alertes d'action

Nom du job	Activé(e) ▲	Serveur	Récurrence	Heure de début :	Heure de fin	Fuseau horaire	Créateur
Low Disk Space	True	caelm63	1 heure	Jeu. 15 oct. 2009 5:03:12		America/New_York	Administrator1

13. Cliquez sur l'onglet Gestion des alertes, Alertes d'action pour afficher les résultats de cette alerte d'action.

Vous recevrez une notification par courriel comme vous l'avez demandé. Voici un exemple.

CA Enterprise Log Manager

RSS Lien	https://calmrhbuildtest01:5250/spin/calm/getAc 8424346294223181834-calmrhbuildtest0112205 3207977576_actionquery_1220536215721
Nom de l'alerte	Low Disk Space
Date de génération	mercredi 21 octobre 2009 10 h 36 EDT
Balises	[Action Alerts]
Créateur	Administrator1
Serveur	caelm

Commentaires

Disk space has dropped below 20%

Si vous cliquez sur le lien RSS, une page du type suivant apparaît.

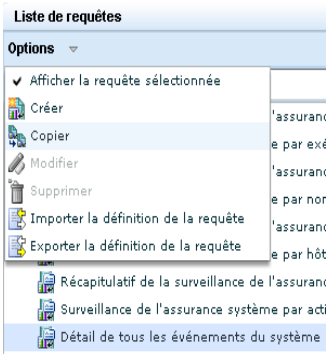
Exemple : Création d'une alerte pour un événement d'autosurveillance

La requête prédéfinie pour tous les événements d'autosurveillance est "Détail de tous les événements du système". Vous pouvez copier cette requête et l'utiliser comme base pour la définition d'une alerte reposant sur un événement d'autosurveillance spécifique.

Par exemple, un événement d'autosurveillance est généré lorsqu'un module exigeant un redémarrage du système d'exploitation est téléchargé dans le cadre d'une mise à jour d'abonnement. Cet événement d'autosurveillance est généré une seule fois. Vous pouvez choisir de créer une alerte pour vous rappeler de redémarrer le système d'exploitation, dans le cas où l'événement d'autosurveillance est oublié.

Utilisez l'exemple suivant en tant que référence.

1. Créez une requête basée sur la requête de tous les événements d'autosurveillance, en procédant comme suit.
   a. Cliquez sur l'onglet Requêtes et rapports, puis sur le sous-onglet Requêtes.
   b. Sélectionnez Détail de tous les événements du système, dans la Liste de requêtes, puis développez la liste déroulante Options et sélectionnez Copier.



   L'assistant de conception de la requête s'ouvre, sur l'étape Détails.
   c. Remplacez le nom de la requête copiée par un nouveau nom, par exemple Alerte de redémarrage SE. Vous pouvez également lui ajouter un nom abrégé et une nouvelle description.
   d. Dans les Balises disponibles, sélectionnez et déplacez Alertes d'action vers les Balises sélectionnées.

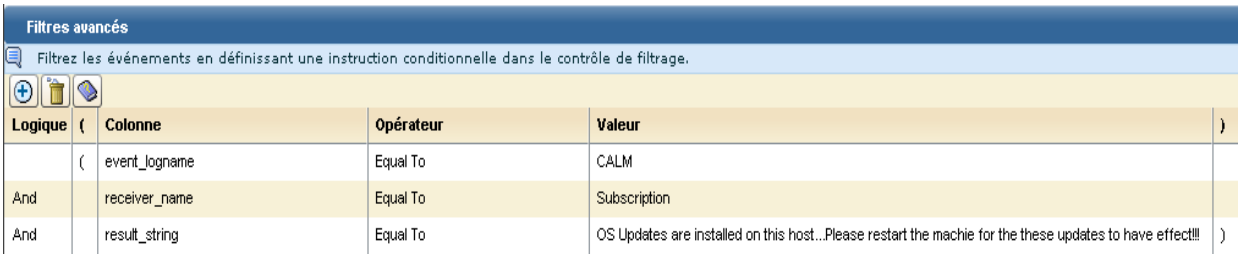
2. Créez des filtres de requête en procédant comme suit.

   a. Avancez jusqu'à l'étape Filtres de requête. Cliquez sur l'onglet Filtres avancés.

   b. Cliquez sur Nouveau filtre d'événement. Sélectionnez event_logname comme colonne, laissez Egal à comme opérateur et sélectionnez CALM comme valeur.

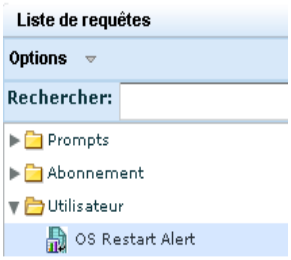
   c. Cliquez sur Nouveau filtre d'événement. Sélectionnez receiver_name comme colonne, laissez Egal à comme opérateur et saisissez Abonnement.

   d. Cliquez sur Nouveau filtre d'événement. Sélectionnez result_string comme colonne, laissez Egal à comme opérateur et saisissez le message "Mises à jour de système d'exploitation installées sur cet hôte... Redémarrez l'ordinateur pour que ces mises à jour prennent effet".



3. Cliquez sur Enregistrer et fermer.

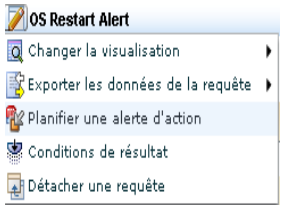
   La nouvelle alerte s'affiche dans la Liste de requêtes, sous le dossier Utilisateur.



4. Planifiez une alerte d'action pour la requête personnalisée, en procédant comme suit:

   a. Sélectionnez la requête dans le dossier Utilisateur.

   b. Cliquez sur le bouton Modifier du volet droit, pour afficher la liste déroulante Alerte de redémarrage SE, puis sélectionnez Planifier une alerte d'action.



   L'assistant de planification des alertes d'action s'ouvre sur l'étape Sélection de l'alerte. Alerte de redémarrage SE est présélectionnée dans la section Requêtes sélectionnées.

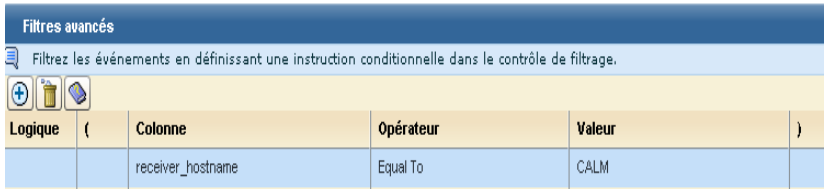
   c. Saisissez un nom pour le job, par exemple Alerte de redémarrage du système d'exploitation.

5. Ajoutez un filtre d'événement comme suit.

   a. Cliquez sur Filtres d'alerte.

   b. Cliquez sur Nouveau filtre d'événement.

   c. Sélectionnez receiver_hostname comme colonne, laissez Egal à comme opérateur et saisissez le nom du système CA Enterprise Log Manager local comme valeur.



6. Indiquez la fréquence à laquelle l'alerte doit être générée, lorsqu'un redémarrage est requis. Pour ce faire, procédez comme suit.

   a. Cliquez sur Planifier des jobs.

   b. Spécifiez l'intervalle de récurrence pour la fréquence de génération de l'alerte. Par exemple, sélectionnez 1 et Jours pour générer une alerte une fois par jour.

7. En procédant comme suit, indiquez votre adresse électronique pour recevoir une alerte par courriel.

   a. Cliquez sur l'étape Destination.

   b. Cliquez sur Activer les notifications par courriel et saisissez votre adresse électronique, ainsi que toute autre information souhaitée.

8. Limitez la notification aux moments où le serveur actuel doit être redémarré. Pour ce faire, procédez comme suit.
   a. Cliquez sur Sélection de serveur.
   b. Sélectionnez Non pour l'option Requêtes fédérées.
9. Cliquez sur Enregistrer et fermer pour enregistrer le job d'alerte.

   Le job Alerte d'action apparaît dans l'onglet Gestion des alertes, sous-onglet Planification d'alerte.

Jobs d'alertes d'action

Nom du job	Activé(e)	Serveur	Récurrence	Heure de début :	Heure de fin
Restart Operating System Alert	True	caelm63	1 jour	Ven. 16 oct. 2009 6:18:02	

Exemple : Envoi d'un courriel à l'administrateur lors de l'arrêt du flux d'événements

Les administrateurs doivent être avertis lorsqu'un connecteur ou un agent cesse de collecter des événements. Vous pouvez automatiser le déclenchement de cette notification lorsqu'un indicateur suggère que cette interruption s'est produite. Vous pouvez configurer l'indicateur, qui correspond à la durée écoulée depuis le moment où un serveur de collecte a cessé de recevoir des événements en provenance de connecteurs. Vous pouvez régler cette durée comme bon vous semble, de quelques minutes à plusieurs jours. Vous pouvez étendre la requête à tous les serveurs de collecte de la fédération.

Pour limiter le nombre de courriels envoyés lorsqu'un connecteur tombe en panne, il est conseillé de ne prendre en compte que les connecteurs qui ont collecté des événements jusqu'au moment de la panne. Par exemple, réglez l'alerte de sorte à renvoyer des lignes uniquement pour les connecteurs qui n'ont pas collecté d'événements au cours de la dernière heure mais qui en ont collecté au cours de l'heure d'avant.

Pour capturer ces données, sélectionnez la requête prédéfinie Contrôleur de collecte par connecteur d'agent en panne du gestionnaire de journaux. Cette requête renvoie les noms du connecteur et de l'agent lorsqu'aucun événement conforme aux conditions de résultats de l'alerte n'est reçu. Utilisez l'exemple suivant comme référence pour créer une alerte émise lorsqu'aucun événement n'est reçu au cours de la dernière heure depuis un connecteur qui a transmis des événements au cours de l'heure d'avant. Indiquez l'adresse électronique de la personne à avertir comme destination d'alerte. Spécifiez une fréquence supérieure ou égale à la période écoulée comme fréquence d'exécution de la requête.

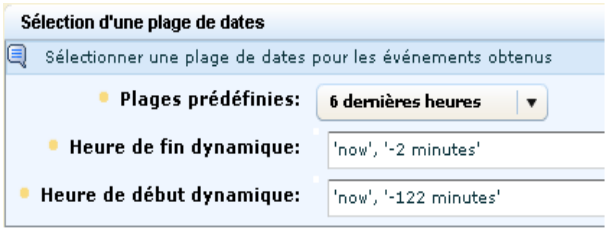
Remarque : Avant de créer l'alerte, vous devez configurer les paramètres de messagerie dans la fenêtre Serveur de rapports accessible depuis l'onglet Administration.

Pour envoyer un courriel à l'administrateur lorsqu'un connecteur cesse de collecter des événements

1. Sélectionnez le serveur à partir duquel exécuter l'alerte. Dans une configuration en étoile, sélectionnez l'un des serveurs de collecte pour capturer la condition dans les plus brefs délais.
2. Sélectionnez l'onglet Gestion des alertes, puis le sous-onglet Planification d'alerte.
3. Cliquez sur Planifier une alerte d'action.
4. Entrez un nom de job, par exemple Connecteur en panne.
5. Dans Requêtes disponibles, sélectionnez la requête Contrôleur de collecte par connecteur d'agent en panne du gestionnaire de journaux et déplacez-la vers la liste Requêtes sélectionnées.

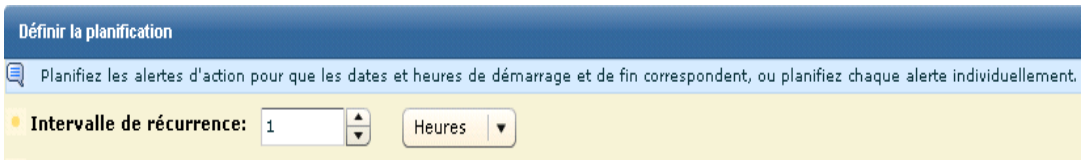
6. Cliquez sur Conditions de résultats.
7. Définissez comme période les 2 dernières heures.
   a. Dans le menu déroulant Plages prédéfinies, sélectionnez Dernière heure.

      Cela définit l'heure de fin dynamique sur Maintenant, -2 minutes
   b. Pour Heure de début dynamique, cliquez sur Modifier la chaîne de période dynamique.
   c. Dans le champ Chaîne de la période dynamique, remplacez 62 par 122.
   d. Cliquez sur OK.



8. Définissez les conditions de résultat.
   a. Sélectionnez Dernier événement regroupé dont la date est antérieure à, puis cliquez sur Modifier.
   b. Dans Heure de référence, sélectionnez Maintenant, puis cliquez sur Ajouter une période de référence à la chaîne de période dynamique.
   c. Cliquez une fois sur la flèche orientée vers le bas en regard de l'option Décalage par afin d'afficher -1, sélectionnez heure dans la liste déroulante, puis cliquez sur Ajouter un décalage à la chaîne de période dynamique.
   d. Cliquez sur OK.

9. Cliquez sur l'étape Planifier des jobs et définissez l'intervalle de récurrence. Par exemple, définissez un intervalle d'une heure.



10. Cliquez sur Destination et renseignez les champs de l'onglet Courriel.
    a. Sélectionnez Activer les notifications par courriel.
    b. Dans le champ Destinataire, entrez l'adresse électronique de l'administrateur.
    c. Dans le champ Expéditeur, entrez votre adresse électronique.
    d. Dans le champ Objet, entrez l'objet du courriel. Par exemple, saisissez Panne probable de connecteur.
    e. Entrez le texte du courriel. Par exemple, saisissez : Le connecteur a cessé d'envoyer des événements au cours de la dernière heure.
11. Cliquez sur l'étape Sélection de serveur et désélectionnez la case Fédéré(e), si vous le souhaitez.
12. Cliquez sur Enregistrer et fermer.

Vous pouvez définir pour cette alerte une plage de dates en jours et non pas en heures, et planifier une exécution quotidienne de la requête. Dans ce cas, Heure de fin dynamique est défini sur "maintenant", Heure de début dynamique sur "maintenant", "-2 jours", et Dernier événement regroupé dont la date est antérieure à sur "maintenant", "-1 jour".

Informations complémentaires :

Remarques sur le serveur de rapports (page 152)

Configuration de la conservation d'alerte d'action

Vous pouvez contrôler le nombre d'alertes d'action enregistrées par le serveur de rapports et leur durée de conservation.

Pour configurer la conservation d'alerte d'action

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.

   La Liste de services s'affiche.

2. Cliquez sur Serveur de rapports pour le paramétrage global ou sur l'hôte du serveur de rapports pour le paramétrage local.

   Le volet de configuration Serveur de rapports apparaît.

3. Entrez une valeur dans le champ de saisie Nombre maximum d'alertes d'action. Toutes les alertes au-delà de ce seuil sont supprimées, les plus anciennes en premier.

4. Dans le champ de saisie Durée de conservation des alertes d'action, entrez le nombre de jours au bout duquel les alertes sont supprimées.

   Remarque : Les alertes d'action sont supprimées dès que le seuil est dépassé.

5. Cliquez sur Enregistrer.

Préparation à l'utilisation d'alertes avec des listes à clés

Certaines des requêtes prédéfinies balisées comme alertes d'action utilisent des listes à clés. Vous pouvez utiliser les valeurs de liste à clés par défaut ou spécifier vos propres valeurs pour la liste à clés prédéfinie. Vous pouvez planifier des alertes avec les requêtes qui utilisent des listes à clés. Vous pouvez également créer vos propres requêtes utilisant des listes à clés. Dans ce cas, paramétrez l'opérateur sur A clés ou Sans clé.

Vous pouvez spécifier des valeurs de liste à clés de l'une des trois manières suivantes.

- Saisissez manuellement les valeurs clés.
- Importez les valeurs clés à partir d'un fichier CSV.
- Importez les valeurs clés depuis un processus CA IT PAM.

Informations complémentaires :

Personnalisation des valeurs à clés pour Critical_Processes (page 494)
Personnalisation des valeurs à clés pour Default_Accounts (page 496)
Personnalisation des valeurs à clés pour ELM_System_Lognames (page 497)
Personnalisation des valeurs à clés pour Privileged_Groups (page 499)
Approches de la gestion des listes à clés (page 333)

Personnalisation des valeurs à clés pour Critical_Processes

Vous pouvez utiliser une requête prédéfinie pour créer une alerte, lorsqu'un processus critique s'arrête. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. Les valeurs prédéfinies incluent : lsass.exe, winlogon.exe, dns.exe, ldap.exe, httpd, smbd, sshd, syslogd, KSecDD et Services IPSec.

Pour personnaliser la liste, vous devez identifier les processus critiques, c'est-à-dire ceux qui doivent toujours être en exécution, puis les ajouter à cette liste à clés. La requête qui utilise cette liste à clés est Processus critique arrêté.

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
source_processname	A clés	Critical_Processes

Pour personnaliser des valeurs à clés pour Critical_Processes

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, Critical_Processes.

   Les valeurs prédéfinies s'affichent.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
   - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
   - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Cliquez sur Exporter des valeurs pour exporter la liste en cours, la modifier afin d'ajouter d'autres valeurs et enregistrer le fichier. Cliquez ensuite sur Importer des valeurs pour importer votre fichier modifié.
   - Si les valeurs de cette clé sont générées de manière dynamique par le processus CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Si vous avez déjà planifié une alerte d'action pour la requête "Processus critique arrêté", cette alerte est générée sur la base de l'évaluation de toutes les valeurs de votre liste à clés modifiée pour Critical_Processes.

Personnalisation des valeurs à clés pour Default_Accounts

Vous pouvez utiliser une requête prédéfinie pour créer une alerte lorsqu'une connexion est correctement établie par un compte par défaut. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. Les valeurs prédéfinies incluent bin, cisco, démon, DBSNMP, Guest, centre d'assistance, Imnadm, invscout, IUSR_ComputerName, messagerie, Nobody, root, sa, sshd, sys, SYSMAN, système et Uucp.

Pour personnaliser la liste, vous devez identifier les comptes par défaut créés lors de l'installation du système d'exploitation, de la base de données ou de l'application en tant que valeurs de la liste de valeurs clés pour Default_Accounts. La requête utilisant vos valeurs personnalisées est intitulée Connexion établie par des comptes par défaut au cours des dernières 24 heures.

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_username	A clés	Default_Accounts

Pour personnaliser les valeurs à clés pour Default_Accounts

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, Default_Accounts.

   Les valeurs prédéfinies s'affichent.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
   - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
   - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.

- Cliquez sur Exporter des valeurs pour exporter la liste en cours, la modifier afin d'ajouter d'autres valeurs et enregistrer le fichier. Cliquez ensuite sur Importer des valeurs pour importer votre fichier modifié.
- Si les valeurs de cette clé sont générées de manière dynamique par le processus CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.

5. Cliquez sur Enregistrer.

   Si vous avez déjà planifié une alerte d'action pour la requête "Connexion établie par des comptes par défaut au cours des dernières 24 heures", cette alerte est générée sur la base de l'évaluation de toutes les valeurs de votre liste à clés modifiée pour Default_Accounts.

Informations complémentaires :

Exemple : Envoi d'une alerte qui exécute un processus CA IT PAM par ligne (page 422)

Personnalisation des valeurs à clés pour ELM_System_Lognames

La clé prédéfinie ELM_System_Lognames n'est utilisée dans aucune requête prédéfinie. Vous pouvez utiliser cette liste à clés dans vos propres requêtes personnalisées. Les valeurs prédéfinies sont CALM, caelmagent, EiamSdk, com.ca.iTechnology.iSponsor et com.ca.iTechnology.iClient. Vous pouvez utiliser les valeurs prédéfinies uniquement ou leur ajouter des valeurs personnalisées.

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
event_logname	A clés	ELM_System_Lognames

Pour personnaliser des valeurs à clés pour ELM_System_Lognames

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous pouvez ajouter des valeurs personnalisées s'affiche.
3. Sélectionnez la clé, ELM_System_Lognames.

   Les valeurs prédéfinies s'affichent.
4. Exécutez une ou plusieurs des actions suivantes pour mettre à jour la liste.
   - Mettez la liste à jour manuellement.
     - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
     - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
     - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Mettez à jour la liste par une exportation/importation.
     a. Cliquez sur Exporter des valeurs pour exporter la liste actuelle.
     b. Ouvrez la liste exportée, modifiez les valeurs de votre choix, puis enregistrez le fichier.
     c. Cliquez sur Importer des valeurs pour importer votre liste modifiée.
   - Cliquez sur Importer des valeurs pour importer les valeurs dans un fichier CSV mis à jour.
   - Si les valeurs de cette clé sont générées de manière dynamique par le traitement des valeurs dynamiques CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Les rapports utilisant cette liste à clés, qui sont générés par des jobs planifiés, commencent à refléter les données des valeurs mises à jour.

Informations complémentaires :

Création d'une requête (page 295)
Exemple : Création d'une alerte pour Business Critical Sources (page 500)

Personnalisation des valeurs à clés pour Privileged_Groups

Vous pouvez utiliser une requête prédéfinie pour créer une alerte lorsque des appartenance au groupe sont ajoutées ou supprimées par un membre d'un groupe avec droits. Vous pouvez utiliser la liste à clés par défaut uniquement ou lui ajouter des valeurs personnalisées. Les valeurs prédéfinies incluent dba, messagerie, ORA_DBA, sshd, uucp et wheel.

Pour personnaliser la liste, vous devez identifier les autres comptes en tant que valeurs de votre liste de valeurs clés pour Privileged_Groups.

Les requêtes utilisant vos valeurs personnalisées incluent les éléments suivants.

- Ajout d'appartenance au groupe par groupe avec droits au cours des dernières 24 heures
- Suppressions d'appartenance au groupe par groupe avec droits au cours des dernières 24 heures

Si vous créez une requête personnalisée utilisant cette clé, définissez le filtre comme suit.

Colonne	Opérateur	Valeur
dest_groupname	A clés	Privileged_Groups

Pour personnaliser des valeurs à clés pour Privileged_Groups :

1. Cliquez sur l'onglet Administration et le sous-onglet Services.
2. Cliquez sur Serveur de rapports.

   Une liste des clés auxquelles vous souhaitez ajouter des valeurs personnalisées s'affiche en bas du volet principal.
3. Sélectionnez la clé, Privileged_Groups.

4. Exécutez l'une des actions suivantes pour mettre à jour la liste.
   - Mettez la liste à jour manuellement.
     - Cliquez sur Ajouter une valeur et saisissez une nouvelle valeur à inclure dans la liste à clés.
     - Sélectionnez une valeur et cliquez sur Supprimer la valeur pour effacer cette valeur de la liste.
     - Sélectionnez une valeur, cliquez sur Modifier la valeur, modifiez la valeur et cliquez sur OK.
   - Cliquez sur Exporter des valeurs pour exporter la liste en cours, la modifier afin d'ajouter d'autres valeurs et enregistrer le fichier. Cliquez ensuite sur Importer des valeurs pour importer votre liste modifiée.
   - Si les valeurs de cette clé sont générées de manière dynamique par le processus CA IT PAM configuré, cliquez sur Importer la liste des valeurs dynamiques.
5. Cliquez sur Enregistrer.

   Si vous avez déjà planifié une alerte d'action avec l'une des requêtes utilisant la liste à clés Privileged_Groups, cette alerte est générée sur la base de l'évaluation des valeurs de votre liste à clés modifiée.

Informations complémentaires :

Approches de la gestion des listes à clés (page 333)

Exemple : Création d'une alerte pour Business_Critical_Sources

Vous pouvez créer une requête personnalisée avec la liste à clés Business_Critical_Sources et planifier une alerte sur la base de cette requête. Cette liste à clés ne possède aucune valeur par défaut et aucune requête ou alerte prédéfinie ne lui est associée. Utilisez la procédure suivante comme guide pour cette opération.

1. Installez un agent.
2. Configurez un connecteur pour cet agent, afin de collecter les événements de chaque source stratégique.

3. Définissez les valeurs de nom d'hôte pour les listes personnalisées Business_Critical_Sources (clés).
   a. Cliquez sur l'onglet Administration et sur le sous-onglet Services.
   b. Sélectionnez Serveur de rapports dans la Liste de services.
   c. Sélectionnez Business_Critical_Sources dans la zone Listes définies par l'utilisateur (clés).
   d. Cliquez sur Ajouter une valeur dans la section Valeurs, puis saisissez le nom d'hôte de la source stratégique.

   e. Répétez cette dernière étape pour chaque source stratégique à partir de laquelle les événements sont collectés.
   f. Cliquez sur Enregistrer.
4. Créez une requête sur la base des échecs de tentative de connexion sur les sources stratégiques.
   a. Cliquez sur Requêtes et rapports.
   b. Sous Liste de requêtes, saisissez "connexion" dans le champ Rechercher.
   c. Sélectionnez Echecs de connexion par hôte, puis choisissez Copier dans la liste déroulante Options.

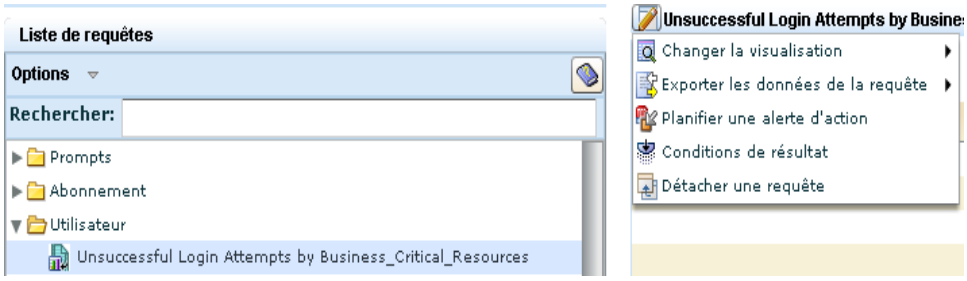
      L'assistant de conception de la requête s'ouvre avec le nom Copie de Echecs de connexion par hôte.

      Renommez la requête en saisissant Echecs de connexion par Business_Critical_Sources.
   d. Sélectionnez l'étape Filtres de requête.
   e. Cliquez sur l'onglet Filtres avancés.
   f. Cliquez sur Nouveau filtre d'événement.

   g. Sélectionnez source_hostname comme colonne, A clés comme opérateur et Business_Critical_Sources comme valeur.

   h. Cliquez sur Enregistrer et fermer.

5. Planifiez une alerte sur la base de cette requête personnalisée.
   a. Cliquez sur l'onglet Requêtes et rapports.
   b. Sélectionnez Echecs de connexion par Business_Critical_Sources sous le dossier Utilisateur de la Liste des requêtes.
   c. Sélectionnez Planifier une alerte d'action dans la liste déroulante Modifier.



   L'assistant de planification des alertes d'action s'ouvre.
   d. Entrez un nom de job, tel que Echecs de connexion par source stratégique.
   e. Cliquez sur Planifier des jobs et définissez la planification.
   f. Vous pouvez également spécifier des options de messagerie pour la Destination.
   g. Cliquez sur Enregistrer et fermer.
6. Vérifiez que le job a bien été planifié.
   a. Cliquez sur l'onglet Gestion des alertes, puis sur le sous-onglet Planification d'alerte.
   b. Vérifiez que le nom de job saisi figure dans la liste.

Jobs d'alertes d'action

Nom du job	Activé(e)
Unsuccessful Login Attempts by Business Critical Resources	True

7. Vérifiez qu'une alerte a été générée.
   a. Cliquez sur l'onglet Gestion des alertes. Le sous-onglet Alertes d'action s'affiche.
   b. Affichez les alertes répertoriées pour déterminer si le nom du job y figure.

Modification d'une alerte d'action

Vous pouvez modifier une alerte d'action existante.

Pour modifier une alerte d'action

1. Cliquez sur l'onglet Gestion des alertes.

   La liste Serveurs d'alerte s'affiche.

2. Sélectionnez le serveur sur lequel l'alerte d'action que vous souhaitez modifier est planifiée.

   Le volet Détails du serveur s'ouvre sur l'onglet Rapports générés par défaut.

3. Cliquez sur l'onglet Alertes planifiées, sélectionnez l'alerte de votre choix et cliquez sur Modifier en haut de la liste.

   L'assistant de planification des alertes d'action s'ouvre.

4. Effectuez les changements souhaités, puis cliquez sur Enregistrer et fermer.

   L'alerte d'action modifiée apparaît dans la liste Alertes d'action.

Désactivation ou activation des alertes d'action

Vous pouvez désactiver une ou plusieurs alertes d'action lorsque vous ne souhaitez plus que les requêtes planifiées associées à cette alerte d'action soient exécutées. Vous pouvez activer des alertes d'action qui étaient précédemment désactivées, afin qu'elles soient exécutées conformément à la planification enregistrée.

Pour désactiver ou activer un job d'alerte d'action

1. Cliquez sur l'onglet Gestion des alertes, puis sur le sous-onglet Planification d'alerte.

   La liste Jobs d'alertes d'action apparaît, indiquant l'état de chaque job dans la colonne Activé(e). Si le job est activé, la valeur Activé(e) est vraie. S'il est désactivé, la valeur Activé(e) est fausse.

2. Sélectionnez le ou les jobs de votre choix, puis cliquez sur Activer les éléments sélectionnés ou Désactiver les éléments sélectionnés.

   La liste Jobs d'alertes d'action affiche le nouvel état de tous les jobs que vous activez ou désactivez.

   Remarque : La possibilité de désactiver des jobs d'alertes est destinée à être utilisée avec les alertes récurrentes. Si vous désactivez un job d'alerte avec une seule occurrence ("Une fois"), il est supprimé de la liste Jobs d'alertes d'action.

Suppression d'une alerte d'action

Vous pouvez supprimer une alerte d'action inutile.

Pour supprimer une alerte d'action

1. Cliquez sur l'onglet Gestion des alertes.

   La liste Serveurs d'alerte s'affiche.

2. Sélectionnez le serveur qui contient l'alerte d'action que vous souhaitez supprimer.

   Le volet Détails du serveur apparaît.

3. Cliquez sur l'onglet Alertes planifiées, sélectionnez l'alerte de votre choix en cliquant sur la ligne, puis cliquez sur Supprimer en haut de la liste. Vous pouvez sélectionner plusieurs jobs d'alertes à supprimer.

   Remarque : Les cases à cocher en regard de chaque job d'alertes sont utilisées pour activer ou désactiver les jobs d'alertes.

   Une boîte de dialogue de confirmation s'affiche.

4. Cliquez sur Oui.

   Un message de confirmation de la suppression apparaît.

5. Cliquez sur OK.

   Le job d'alerte est supprimé de la liste Jobs d'alertes.

Chapitre 11 : Rapports planifiés

Ce chapitre traite des sujets suivants :

Affichage d'un rapport généré

Vous pouvez afficher un rapport généré ou en enregistrer une copie à l'emplacement de votre choix. Les rapports générés sont stockés sur le dispositif logiciel avec CA Enterprise Log Manager à l'emplacement suivant :

/opt/CA/LogManager/data/reports

Pour afficher un rapport généré

1. Cliquez sur l'onglet Rapports planifiés.

   L'onglet s'ouvre et l'hôte CA Enterprise Log Manager local est affiché par défaut.

2. Sélectionnez le serveur sur lequel les rapports générés que vous souhaitez afficher sont planifiés.

   Le serveur sélectionné s'affiche dans le volet Détails.

3. Cliquez sur l'onglet Rapports générés s'il n'est pas déjà affiché.

   La liste des rapports générés s'affiche.

4. Cliquez sur le nom du rapport que vous souhaitez afficher.

   La boîte de dialogue Enregistrer s'ouvre.

5. Cliquez sur Enregistrer pour spécifier un emplacement auquel enregistrer le rapport.

Informations complémentaires :

Filtrage des rapports (page 506)
Annotation d'un rapport généré (page 507)
Planification d'un job de rapport (page 508)
Evénements d'autosurveillance (page 526)

Filtrage des rapports

Vous pouvez définir des filtres pour restreindre l'affichage des rapports générés disponibles et des jobs de rapports planifiés.

Pour filtrer des rapports générés ou planifiés

1. Sélectionnez le serveur de rapports sur lequel se trouvent les rapports planifiés ou générés que vous souhaitez filtrer et cliquez sur l'onglet Rapports générés ou Rapports planifiés.

   La liste des rapports générés ou des rapports planifiés s'affiche.

2. A l'aide des menus déroulants appropriés, sélectionnez le type de récurrence ou le format selon lequel vous souhaitez filtrer les rapports affichés.

   La liste affiche les rapports qui remplissent les critères de votre filtre.

Informations complémentaires :

Affichage d'un rapport généré (page 505)
Annotation d'un rapport généré (page 507)

Annotation d'un rapport généré

Vous pouvez ajouter des annotations à un rapport généré, à des fins de suivi ou de vérification notamment.

Pour annoter un rapport généré

1. Sélectionnez le serveur de rapports sur lequel se trouvent les rapports générés à annoter et cliquez sur l'onglet Rapports générés.

   La liste des rapports générés s'affiche.

2. Cliquez sur l'icône Annotations en regard du rapport à annoter.

   La boîte de dialogue Annotations de rapports apparaît ; elle contient toutes les annotations précédentes avec le nom de leur créateur ainsi que la date et l'heure de création.

3. Saisissez votre annotation et cliquez sur Enregistrer.

   L'annotation s'affiche dans la boîte de dialogue, qui reste ouverte pour permettre la saisie d'autres annotations.

4. Répétez l'étape 3 pour ajouter des annotations supplémentaires (facultatif).

5. Cliquez sur Fermer lorsque vous avez terminé d'ajouter des annotations.

   La boîte de dialogue Annotations de rapports se ferme.

Informations complémentaires :

Affichage d'un rapport généré (page 505)
Filtrage des rapports (page 506)

Planification d'un job de rapport

La procédure de création d'un job de rapport à l'aide de l'assistant de planification de rapport se compose principalement des étapes suivantes.

1. Ouverture de l'assistant de planification de rapport
2. Sélection des modèles de rapport : pour commencer à planifier un job de rapport, vous devez sélectionner le rapport ou la balise à utiliser en tant que modèle pour le job. Vous pouvez sélectionner un seul modèle ou une seule balise, ou bien plusieurs modèles ou balises.
3. Création de filtres de rapports : vous pouvez appliquer des filtres d'événement avancés pour personnaliser davantage vos retours de rapports, si nécessaire.
4. Définition de la plage de dates et des conditions de résultats : vous pouvez définir la plage de dates sur laquelle portera la requête de rapport, ainsi que d'autres conditions.
5. Planification des jobs : vous devez définir le jour et l'heure d'exécution des rapports, pour les rapports à occurrence unique comme pour les rapports récurrents. Vous pouvez également choisir parmi les schémas de récurrence disponibles.
6. Sélection d'un format de rapport et d'une destination : vous pouvez choisir le format de rapport souhaité ainsi que les options de remise des courriels.
7. Sélection d'un serveur : vous devez sélectionner le serveur à interroger par le rapport et indiquer si les hôtes fédérés du serveur doivent également être interrogés.

Ouverture de l'assistant de planification de rapport

Pour créer un nouveau job de rapport pour un ou plusieurs rapports récurrents, vous devez utiliser l'assistant de planification de rapport.

Pour ouvrir l'assistant de planification de rapport

1. Cliquez sur l'onglet Rapports planifiés.

   La liste Serveurs de rapport s'affiche.

2. Sélectionnez le serveur sur lequel planifier un rapport.

   Le volet Détails du serveur de rapports affiche le serveur sélectionné ; l'onglet Rapports générés est ouvert par défaut.

3. Cliquez sur l'onglet Planification de rapport, puis cliquez sur Planifier un rapport.

   L'assistant de planification de rapport s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer et fermer pour enregistrer le rapport planifié et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires

Définition des paramètres de planification (page 517)
Création d'un filtre d'événement avancé (page 303)
Définition des conditions de résultats (page 304)
Choix d'une cible de requête de rapport (page 519)

Sélection d'un modèle de rapport

La première étape de la procédure de création d'un job de rapport consiste à sélectionner le modèle de rapport. Si vous souhaitez planifier plusieurs jobs de rapport partageant les mêmes filtres, paramètres de planification et paramètres de destination, vous pouvez sélectionner plusieurs rapports ou balises en tant que modèles.

Si vous sélectionnez plusieurs rapports, les jobs s'affichent séparément par rapport. Par exemple, si vous sélectionnez deux rapports différents, ils partagent les mêmes options de planification et de filtre, mais sont affichés séparément, intitulés d'après le nom du rapport, dans la liste Rapports générés.

Les utilisateurs avec le rôle Administrator peuvent créer des jobs de rapport dans un état désactivé, pour une utilisation ultérieure. Un utilisateur avec des rôles Administrator et Analyst peut activer et désactiver des jobs ultérieurement. Les rapports désactivés affichent la valeur *false* dans la colonne Activé, lors de l'affichage de l'onglet Rapports planifiés.

Pour sélectionner un modèle de rapport

1. Saisissez un nom pour le job,
2. Dans le menu déroulant de fuseau horaire, sélectionnez le fuseau horaire dans lequel vous souhaitez planifier le rapport.
3. Sélectionnez le bouton d'option Rapports ou Balises pour sélectionner les rapports par balise ou de manière séparée.

   Remarque : Planifier les rapports par balise vous permet d'ajouter des rapports sans modifier le job lui-même. Si vous sélectionnez la balise "Gestion des identités", tout rapport associé à cette balise est ajouté au job à l'heure d'exécution planifiée. Cette fonction s'applique également aux balises personnalisées.
4. Sélectionnez une ou plusieurs balises pour limiter le nombre de balises et de rapports affichés (facultatif). Cette fonction se comporte de la même manière que la Liste de rapports.
5. (Facultatif) Activez la case à cocher Activé pour créer ce job de rapport dans un état désactivé. La case à cocher Activé est activée par défaut.

   Remarque : La possibilité de créer un job de rapport désactivé a été conçue pour une utilisation avec des rapports récurrents. Si vous désactivez la case à cocher Activé d'un job, puis que vous créez ce job avec une occurrence unique ("Maintenant" ou "Une fois"), il est supprimé de la liste Rapport planifié.
6. Sélectionnez les balises ou rapports que vous souhaitez utiliser en tant que modèles de rapport et utilisez le contrôle de déplacement pour les ajouter à la zone Rapports sélectionnés.

7. Accédez à la prochaine étape de planification que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le rapport est planifié. Sinon, l'étape sélectionnée apparaît.

Utilisation des filtres avancés

Vous pouvez utiliser des filtres avancés en langage SQL pour qualifier une fonction qui interroge le magasin de journaux d'événements, y compris pour limiter des requêtes ou personnaliser des filtres rapides. L'interface Filtres avancés vous aide à créer la syntaxe de filtre appropriée grâce à un formulaire de saisie des colonnes logiques, opérateurs et valeurs, selon vos besoins de filtrage.

Remarque : Cette section contient une brève présentation des termes SQL utilisés dans les filtres avancés. Pour utiliser les filtres avancés au maximum de leur potentiel, vous devez posséder une connaissance approfondie de la grammaire SQL et de la grammaire commune aux événements.

Les termes SQL suivants permettent d'associer plusieurs instructions de filtre;

And

Affiche les informations de l'événement si *tous* les termes ajoutés sont vrais.

Or

Affiche les informations de l'événement si *l'un* des termes ajoutés est vrai.

Having

Restreint les termes de l'instruction SQL principale en ajoutant une instruction de qualification. Par exemple, vous pouvez définir un filtre avancé pour les événements issus d'hôtes spécifiés et ajouter une instruction "having" afin de limiter les résultats aux événements d'un niveau de sévérité défini.

Les opérateurs SQL suivants sont utilisés par les filtres avancés pour créer les conditions de base.

Opérateurs relationnels

Inclut les informations de l'événement si la colonne porte la relation appropriée à la valeur saisie. Les opérateurs relationnels suivants sont disponibles.

- Egal à
- Différent de
- Inférieur à
- Supérieur à
- Inférieur ou égal à
- Supérieur ou égal à

Par exemple, l'utilisation de *Supérieur à* inclut les informations de l'événement à partir de la colonne choisie si sa valeur est supérieure à la valeur définie.

Comme

Inclut les informations de l'événement si la colonne contient le modèle que vous avez saisi à l'aide du signe %. Par exemple, L% renvoie toutes les valeurs commençant par L, %L% renvoie toutes les valeurs contenant L comme valeur mais pas comme première ou dernière lettre.

Distinct de

Inclut les informations de l'événement si la colonne ne contient pas le modèle spécifié.

Dans l'ensemble

Inclut les informations de l'événement si la colonne contient au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Hors ensemble

Inclut les informations de l'événement si la colonne ne contient pas au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Correspondance

Inclut toute information d'événement qui correspond au moins à un des caractères que vous avez saisis, ce qui vous permet de rechercher des mots clés.

A clés

Inclut toute information d'événement définie comme une valeur clé pendant la configuration du serveur de rapports. Vous pouvez utiliser les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Sans clé

Inclut toute information d'événement non définie comme une valeur clé pendant la configuration du serveur de rapports. Vous pouvez utiliser les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Définition des conditions de résultats

Vous pouvez définir une plage de dates et d'autres conditions de résultat pour la requête, notamment les limites des lignes et la période d'affichage de base. Les conditions de résultats peuvent être modifiées à tout moment jusqu'à l'heure d'exécution de la requête, ce qui en fait une méthode pratique pour modifier des requêtes sans remanier la requête de base ou ses filtres.

Vous pouvez définir les types suivants de conditions de résultats.

- Les conditions de plage de dates régissant la période de recherche de la requête
- Les conditions d'affichage, telles que le nombre maximum de lignes
- Les conditions d'événements regroupés, comme les événements regroupés les plus récents après une date donnée ou les événements regroupés contenant un nombre défini d'événements

  Remarque : Si vous ne regroupez pas au moins une colonne lors de la création d'une requête, les utilisateurs ne pourront pas modifier les conditions de résultats depuis l'affichage de la requête.

Définition d'une période ou d'une plage de dates

Vous pouvez définir des conditions de période ou de plage de dates pour votre requête. Cela améliore l'efficacité de votre requête en limitant la zone de recherche du magasin de journaux d'événements.

Vous pouvez sélectionner une plage horaire prédéfinie ou créer une plage personnalisée. Pour qu'une plage puisse fonctionner correctement, vous devez définir une heure de début et de fin. Si vous ne rentrez qu'un seul de ces paramètres, la période est exprimée par une clause "Where" dans la requête SQL.

Pour définir des conditions de résultat

1. Ouvrez la boîte de dialogue Conditions de résultats.
2. Sélectionnez une plage horaire prédéfinie dans la liste déroulante. Si vous souhaitez par exemple afficher les événements reçus hier, sélectionnez "jour précédent".

   Remarque : Lors de la création d'une alerte d'action ou d'un rapport planifié, l'interface affiche les périodes suivantes par défaut.

   - Alerte d'action : les 5 dernières minutes
   - Rapport planifié : les 6 dernières heures
3. Créez une plage personnalisée, en suivant les étapes ci-après (facultatif) :

   a. Dans la zone Sélection d'une plage de dates, cliquez sur Modifier en regard du champ de saisie Heure de fin dynamique. Cela vous permet de définir la fin de la période dans laquelle vous souhaitez effectuer la requête.

      La boîte de dialogue Spécification de la période dynamique s'affiche.

   b. Sélectionnez l'heure de référence pour le paramètre, puis cliquez sur Ajouter.

   c. Sélectionnez le paramètre d'heure de votre choix, puis cliquez sur Ajouter. Vous pouvez ajouter plusieurs paramètres d'heure.

   d. Cliquez sur OK lorsque vous avez terminé.

      Fermez la boîte de dialogue Spécification de la période dynamique. La valeur choisie s'affiche dans la zone Heure de fin dynamique. Dans ce cas, ils forment une instruction de temps complète, chaque paramètre se référant au premier. Par exemple, les valeurs Début du mois et Jour de la semaine - mardi ajoutées à la zone Heure de fin dynamique terminent votre requête le premier mardi du mois.

Remarque : Lorsque vous utilisez les valeurs Nombre de, telles que Nombre de jours ou Nombre d'heures, vous devez saisir un nombre *négatif* pour définir une période dans le passé. Un nombre positif définit une heure de fin dans le futur et la requête risque de continuer à envoyer des résultats, au moins jusqu'à ce qu'un événement qualifié figure dans le magasin de journaux.

Par exemple, les valeurs maintenant et nombre de minutes - 10 ajoutées à la zone Heure de début dynamique débutent votre requête 10 minutes avant l'heure de fin sélectionnée.

e. Dans la zone Heure de début dynamique, répétez l'étape 2 pour définir le début de la période sur laquelle vous souhaitez effectuer une requête.

Si vous n'entrez pas de plage de dates, la requête s'applique à tous les événements du magasin de journaux.

4. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Informations complémentaires :

Création d'une requête (page 295)
Définition des conditions de résultats (page 304)
Définition des conditions d'affichage et de groupe (page 307)

Définition des conditions d'affichage et de groupe

Vous pouvez définir des conditions qui vous permettent de contrôler l'affichage des requêtes et les conditions de recherche des événements en fonction de leur regroupement.

Pour définir des conditions d'affichage et de groupe

1. Ouvrez la boîte de dialogue Conditions de résultats.
2. Utilisez les cases à cocher Résultats pour activer, si besoin, les qualifications d'affichage suivantes.

   Limite des lignes

   Définit le nombre maximum de lignes d'événements affichés par la requête, en commençant par les plus récents.

   Minimum : 1

   Maximum : 5 000

   Afficher d'autres infos

   Indique la présence d'autres résultats qui ne sont pas affichés en raison de la limite de lignes, ce qui vous permet de comparer les événements sélectionnés dans le contexte de tous les événements du même type. Par exemple, si vous choisissez une limite de 10 lignes dans l'affichage de la visionneuse d'événements et si vous sélectionnez Afficher d'autres infos, les événements au-delà de 10 s'affichent dans une entrée particulière intitulée Autres, qui présente l'ensemble des événements restants. Le paramètre n'est actif que lorsque l'option Limites des lignes est sélectionnée.

   Granularité temporelle

   Définit le niveau de détail du champ de période utilisé dans l'affichage des requêtes.

3. Utilisez Conditions de résultats pour effectuer une requête sur plusieurs types de conditions d'événements regroupés. Par exemple, vous pouvez définir votre requête de façon à rechercher le dernier événement regroupé à partir d'une date sélectionnée ou un certain nombre d'événements regroupés. Un événement regroupé est un événement ajusté pour lequel vous avez défini une Fonction et un Ordre de regroupement à l'étape Création d'une requête.

   Les conditions de groupe utilisent le même système d'instruction de temps que les champs de période.

4. Cliquez sur la flèche appropriée pour passer à l'étape Conception de la requête que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle requête apparaît dans la Liste de requêtes. Sinon, l'étape Conception de la requête choisie s'affiche.

Informations complémentaires

Création d'une requête (page 295)
Définition des conditions de résultats (page 304)

Définition des paramètres de planification

Vous pouvez déterminer le moment d'exécution des rapports planifiés, leur récurrence ou non, ainsi que l'intervalle de récurrence.

Pour définir des paramètres de planification

1. Ouvrez l'assistant de planification de rapport et avancez jusqu'à l'étape Planifier des jobs.
2. Utilisez les boutons radio Non récurrent ou Récurrent pour sélectionner l'heure de génération du rapport ainsi que le schéma de récurrence, le cas échéant.

   Remarque : Si vous utilisez l'heure d'été dans votre environnement, ne planifiez pas un rapport au moment du changement d'heure car il ne sera pas généré. Par exemple, si le passage à l'heure d'été s'effectue à 2:00 du matin le 8 mars, vous ne pouvez pas planifier un rapport entre 2:00:00 et 2:59:59.
3. Accédez à l'étape de planification suivante que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le rapport est planifié. Sinon, l'étape choisie apparaît.

Informations complémentaires :

Utilisation des filtres avancés (page 301)
Définition des conditions de résultats (page 304)
Choix d'une cible de requête de rapport (page 519)

Sélection du format et des paramètres de notification

Vous pouvez sélectionner le format dans lequel les rapports sont générés : PDF, Excel ou XML. Vous pouvez également configurer la notification automatique par courriel.

Pour définir le format et la notification

1. Ouvrez l'assistant de planification de rapport et avancez jusqu'à l'étape Destination.
2. Sélectionnez le format souhaité dans le menu déroulant Format du rapport.

   Remarque : Au format PDF, les graphiques sont limités à 100 points de données, ainsi, les étiquettes d'axe de graphique sont clairement lisibles. Si le graphique à afficher contient plus de 100 points, CA Enterprise Log Manager inclut uniquement les 100 premiers dans la sortie PDF publiée.
3. Cochez la case Courriel si vous souhaitez envoyer une notification lorsque le rapport est généré.

   Les champs de spécification des adresses électroniques apparaissent.
4. Entrez les adresses électroniques de tous les utilisateurs qui recevront la notification. Séparez-les par des virgules.
5. Saisissez toute autre donnée souhaitée, y compris l'objet, l'adresse électronique de retour et le corps de texte (facultatif).
6. Sélectionnez Joindre un rapport pour joindre au courriel de notification une copie du rapport dans le format de votre choix (facultatif).
7. Accédez à la prochaine étape de planification que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le rapport est planifié. Sinon, l'étape sélectionnée apparaît.

Informations complémentaires :

Utilisation des filtres avancés (page 301)
Définition des conditions de résultats (page 304)
Définition des paramètres de planification (page 517)
Choix d'une cible de requête de rapport (page 519)

Choix d'une cible de requête de rapport

Vous pouvez choisir le magasin de journaux d'événements fédérés qui stocke les recherches de requête de rapport.

Pour choisir les destinations de rapport

1. Ouvrez l'assistant de planification de rapport et avancez jusqu'à l'étape Sélection de serveur.
2. Sélectionnez tous les serveurs disponibles à interroger et déplacez-les dans la zone Serveurs sélectionnés à l'aide du contrôle de déplacement.
3. Si vous souhaitez désactiver les requêtes fédérées pour ce rapport, sélectionnez Non dans le menu déroulant qui apparaît lorsque vous cliquez sur l'entrée Requêtes fédérées (facultatif). Les requêtes de rapport sont fédérées par défaut.
4. Accédez à l'étape de planification suivante que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le rapport est planifié. Sinon, l'étape choisie apparaît.

Informations complémentaires :

Utilisation des filtres avancés (page 301)
Définition des conditions de résultats (page 304)
Définition des paramètres de planification (page 517)

Exemple : Planification de rapports avec une balise commune

Vous pouvez planifier la génération d'un ou plusieurs rapports selon la fréquence définie et la date de fin spécifiée.

Les auditeurs, analystes et administrateurs sont en mesure de planifier des rapports.

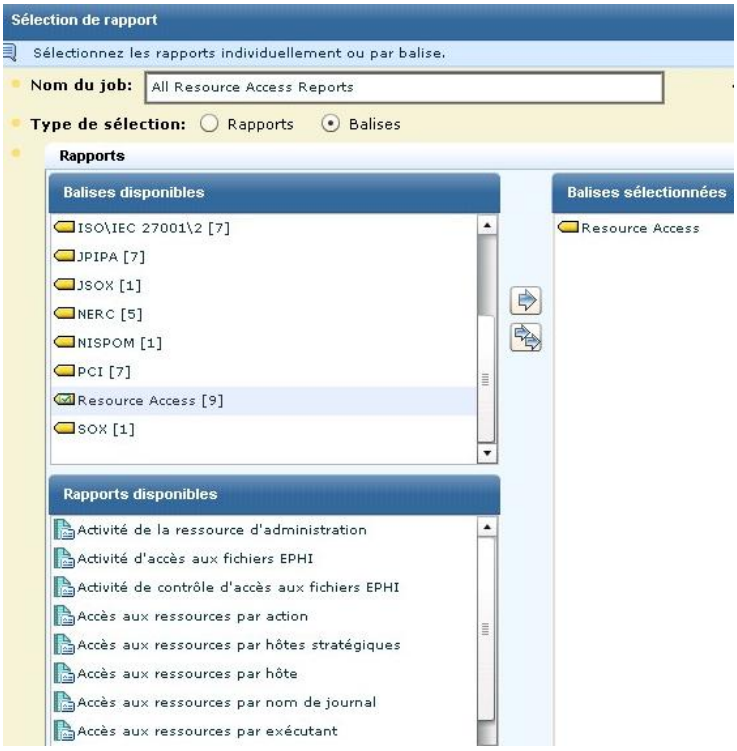
Pour planifier un rapport

1. Cliquez sur l'onglet Rapports planifiés, sur le sous-onglet Planification de rapport, puis sur Planifier un rapport.

L'assistant de planification de rapports s'affiche et son étape 1, Sélection de rapport, est sélectionnée.

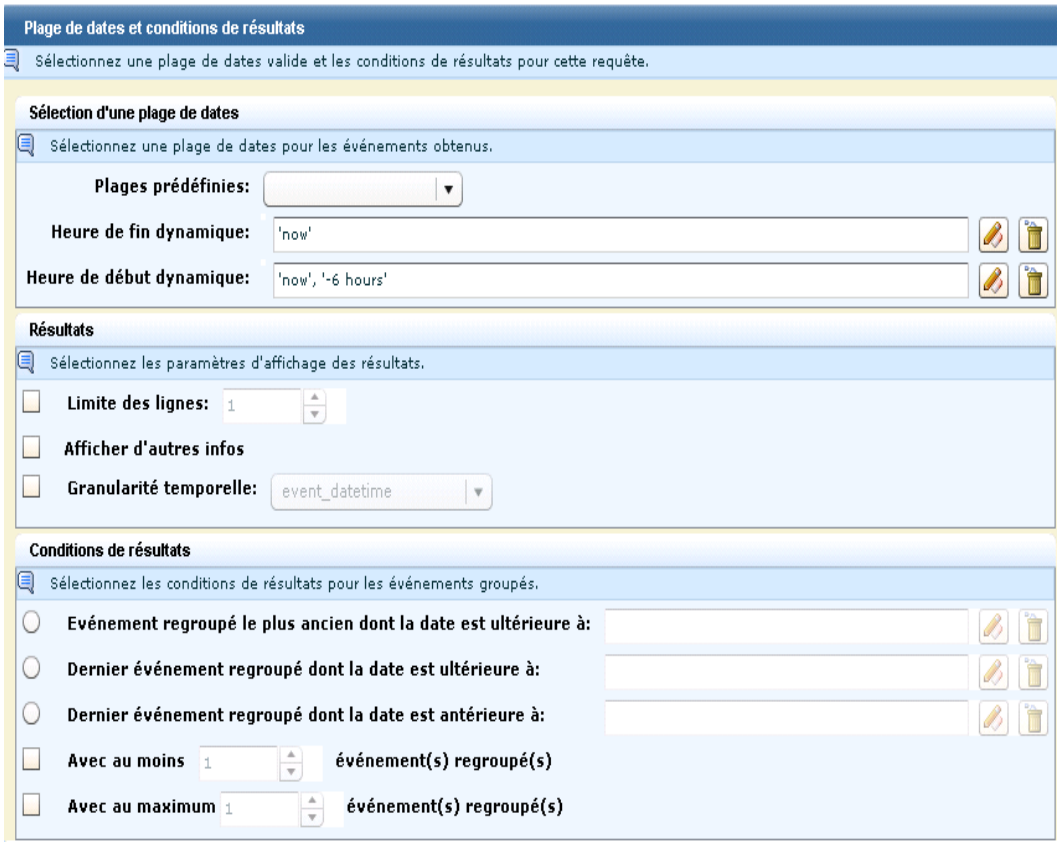
2. Entrez un nom de job, sélectionnez Rapports pour activer la sélection de rapports individuels ou sélectionnez Balises pour activer la sélection de tous les rapports associés à une balise sélectionnée.

   Dans l'exemple qui suit, la sélection des balises d'accès aux ressources permet de sélectionner facilement les six rapports associés à cette balise.



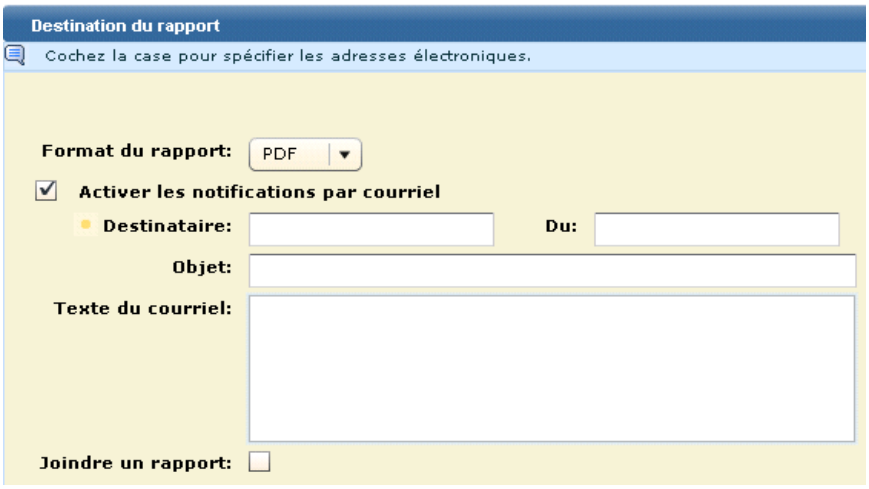
3. Cliquez sur Filtres de rapports et créez un nouveau filtre d'événement pour limiter le rapport aux données dont vous avez besoin (facultatif).

4. Cliquez sur Conditions de résultats et sélectionnez une plage de dates et/ou des conditions de résultats pour cette requête (facultatif). Par exemple, pour rechercher les événements survenus au cours des six dernières heures, sélectionnez "maintenant" en tant qu'heure de fin dynamique et sélectionnez "maintenant" et "- 6 heures" en tant qu'heure de début dynamique. Sélectionnez Limite des lignes et choisissez un chiffre, 250 par exemple.



5. Cliquez sur Jobs planifiés pour planifier la génération pour Maintenant ou sélectionnez une autre option et spécifiez les détails.

6. Cliquez sur Destination et indiquez le format du rapport (feuille de calcul Excel, PDF ou XML). Une feuille de calcul convient aux données tabulaires. Un PDF convient aux graphiques. Si vous le souhaitez, vous pouvez envoyer une notification par courriel. Utilisez la virgule pour séparer les adresses électroniques. Le courriel peut être envoyé sans le rapport, simplement pour confirmer que le rapport planifié a été généré, mais vous pouvez également envoyer le rapport en pièce jointe au courriel.



Remarque : L'administrateur peut configurer les rapports à supprimer après une période de conservation spécifiée. La conservation d'une copie de courriel peut faire figure d'alternative de sauvegarde à l'archivage manuel.

7. Cliquez sur Sélection de serveur, sélectionnez un ou plusieurs serveurs pour les rapports et indiquez si vous souhaitez ou non effectuer une requête sur la fédération du serveur.

8. Cliquez sur Enregistrer et fermer.

   La génération des rapports sélectionnés est planifiée.

Exemple : Envoi par courriel de rapports PCI quotidiens au format PDF

Vous pouvez automatiser la remise de certains rapports spécifiques au format, aux destinataires et à la fréquence de votre choix.

Pour indiquer que les rapports planifiés doivent être envoyés au format PDF, en pièce jointe d'un courriel, vous devez configurer les éléments suivants dans la Configuration globale du service pour le Serveur de rapports, dans l'onglet Administration et le sous-onglet Services.

- Options de serveur de messagerie
  - Serveur de messagerie
  - Port SMTP (25)
  - Messagerie de l'administrateur
  - Nom d'utilisateur et mot de passe SMTP
- Spécifications PDF
  - Société/Nom du produit
  - URL du logo du produit/de la société
  - Police de l'en-tête et taille de police
  - Police des données et taille de police
  - Orientation, largeur et hauteur de la page

Exemple : Remise de tous les rapports PCI quotidiens au format PDF, dans la boîte de réception de l'auditeur, tous les jours ouvrés

1. Cliquez sur l'onglet Rapports planifiés, puis sur le sous-onglet Planification de rapport.

   La barre d'outils s'affiche ; elle contient un bouton Planification d'un rapport.

2. Cliquez sur Planifier un rapport.

   La fenêtre Sélection de rapport s'affiche.

3. Sélectionnez un rapport en procédant comme suit.

   a. Saisissez Rapports PCI comme nom de job.

   b. Sélectionnez Balises comme type de sélection.

   c. Dans les Balises disponibles, sélectionnez et déplacez PCI vers les Balises sélectionnées.

4. Planifiez le job en procédant comme suit.
   a. Cliquez sur l'étape Planifier des jobs.
   b. Sélectionnez Tous les jours dans l'option Récurrent.
   c. Sélectionnez Chaque jour de la semaine.
5. Spécifiez le format et la destination du rapport, en procédant comme suit.
   a. Cliquez sur l'onglet Destination.
   b. Acceptez le format de rapport par défaut (PDF).
   c. Sélectionnez Activer les notifications par courriel.
   d. Saisissez l'adresse électronique de l'auditeur. Utilisez la syntaxe suivante : <nom_messagerie>@<société>.com
   e. Sélectionnez Joindre un rapport.
6. Cliquez sur Enregistrer et fermer.

Modification d'un job de rapport planifié

Vous pouvez modifier un job de rapport planifié.

Pour modifier un job de rapport planifié

1. Cliquez sur l'onglet Rapports planifiés.

   La liste Serveurs de rapport s'affiche.
2. Sélectionnez le serveur sur lequel le rapport que vous souhaitez modifier est planifié.

   Le serveur sélectionné apparaît dans le volet Détails du serveur de rapports.
3. Sélectionnez le job de rapport souhaité, puis cliquez sur Modifier en haut de la liste.

   L'assistant de planification de rapport s'ouvre.
4. Effectuez les changements souhaités, puis cliquez sur Enregistrer et fermer.

   Le rapport modifié apparaît dans la liste Jobs planifiés dans un délai de 5 minutes, dès que la liste est actualisée. Cliquez sur Actualiser pour l'afficher immédiatement.

Informations complémentaires :

Planification d'un job de rapport (page 508)
Suppression d'un job de rapport planifié (page 526)

Activation et désactivation de jobs de rapports planifiés

Vous pouvez désactiver un ou plusieurs jobs de rapports planifiés lorsque vous ne souhaitez plus que les requêtes associées à ce rapport soient exécutées. Vous pouvez également activer des jobs de rapports planifiés qui étaient précédemment désactivés, afin qu'ils soient exécutés conformément à la planification enregistrée.

Pour désactiver ou activer des jobs de rapports planifiés

1. Cliquez sur l'onglet Rapports planifiés, puis sur le sous-onglet Planification de rapport.

   La liste Jobs planifiés apparaît, indiquant l'état de chaque job dans la colonne Activé(e). Si le job est activé, la valeur Activé(e) est vraie. S'il est désactivé, la valeur Activé(e) est fausse.

2. Sélectionnez le ou les jobs de votre choix, puis cliquez sur Activer les éléments sélectionnés ou Désactiver les éléments sélectionnés.

   La liste Jobs planifiés affiche le nouvel état de tous les jobs que vous activez ou désactivez.

   Remarque : La possibilité de désactiver des jobs de rapports est destinée à être utilisée avec les rapports récurrents. Si vous désactivez un job de rapport avec une seule occurrence ("Une fois"), il est supprimé de la liste Jobs planifiés.

Suppression d'un job de rapport planifié

Vous pouvez supprimer un job de rapport planifié.

Pour supprimer un job de rapport planifié

1. Cliquez sur l'onglet Rapports planifiés.

   La liste Serveurs de rapport s'affiche.

2. Sélectionnez le serveur sur lequel le rapport que vous souhaitez supprimer est planifié.

   Le serveur sélectionné apparaît dans le volet Détails du serveur de rapports.

3. Cliquez sur l'onglet Planification de rapport, sélectionnez le job de votre choix en cliquant sur la ligne et cliquez sur Supprimer en haut de la liste. Vous pouvez sélectionner plusieurs jobs à supprimer.

   Remarque : Les cases à cocher en regard de chaque job de rapport sont utilisées pour activer ou désactiver les jobs de rapport.

   Une boîte de dialogue de confirmation s'affiche.

4. Cliquez sur Oui.

   Le job de rapport est supprimé de la liste Jobs planifiés.

Informations complémentaires :

Planification d'un job de rapport (page 508)
Modification d'un job de rapport planifié (page 524)

Evénements d'autosurveillance

La plupart des actions utilisateur génèrent des événements d'autosurveillance. Ces événements vous permettent de suivre les actions entreprises sur le serveur ou impliquant le serveur, ainsi que leur réussite ou leur échec. Les événements d'autosurveillance s'affichent au format Visionneuse d'événements pour chaque serveur, sur les onglets Rapports planifiés et Gestion des alertes. Il est également possible d'y accéder en tant que rapports normaux ou planifiés à l'aide du rapport Evénements d'autosurveillance.

Informations complémentaires :

Affichage d'un événement d'autosurveillance (page 527)
Planification d'un job de rapport (page 508)

Affichage d'un événement d'autosurveillance

Vous pouvez afficher les événements d'autosurveillance appropriés pour chaque serveur depuis les onglets Gestion des alertes et Rapports planifiés. Les vues de chaque onglet sont filtrées pour afficher les événements d'alerte ou de surveillance de rapport appropriés. Vous pouvez supprimer le filtre afin d'afficher l'intégralité des événements d'autosurveillance.

Pour afficher des événements d'autosurveillance

1. Cliquez sur l'onglet Rapports planifiés ou Gestion des alertes.

   La liste des serveurs de rapports ou d'alerte apparaît.

2. Sélectionnez le serveur dont vous souhaitez afficher les événements d'autosurveillance locaux.

   Le serveur sélectionné s'affiche dans le volet Détails.

3. Cliquez sur l'onglet Evénements d'autosurveillance.

   Le volet d'affichage Evénements d'autosurveillance apparaît ; il affiche les événements d'autosurveillance liés aux rapports ou aux alertes. Vous pouvez exécuter toutes les tâches normales liées aux rapports à partir du volet Evénements d'autosurveillance, notamment les tâches suivantes.

   - Tâches liées à la visionneuse d'événements
   - Filtrage global ou local
   - Définition de favoris
   - Exportation

Informations complémentaires :

Suppression d'un filtre local (page 261)

Chapitre 12 : Suppression et récapitulation

Ce chapitre traite des sujets suivants :

Versions de composant pour l'ajustement d'événement

Le système CA Enterprise Log Manager conserve les anciennes versions de certains composants d'ajustement d'événement personnalisés, lorsque vous les créez ou les modifiez. Cela vous permet de vous référer à ces versions antérieures, le cas échéant. Vous pouvez afficher ou copier d'anciennes versions pour les composants suivants.

- Fichiers d'analyse de message
- Fichiers de mappage des données
- Règles de suppression
- Règles de récapitulation

A chaque fois que vous créez un nouveau composant personnalisé, son numéro de version est 1.0. Lorsque vous modifiez et enregistrez une nouvelle version d'un même objet, celle-ci est appelée version 2.0. Les deux versions apparaissent dans la zone d'interface appropriée, à des fins de sélection et d'application.

Par exemple, si vous créez une règle de suppression personnalisée appelée "NouvelleRègle", celle-ci apparaît en tant que NouvelleRègle version 1.0 dans la liste de l'interface du magasin de journaux d'événements, afin que vous puissiez l'appliquer. Si vous modifiez ensuite ce fichier, la version modifiée apparaîtra en tant que NouvelleRègle version 2.0 dans la liste du magasin de journaux d'événements.

Vous pouvez consulter les anciennes versions d'un composant d'ajustement d'événement dans la liste appropriée. Ces versions sont en lecture seule et ne peuvent être modifiées. Vous pouvez copier une ancienne version et la modifier, afin qu'elle soit considérée comme une toute nouvelle version. Par exemple, en reprenant l'exemple précédent, vous ne pouvez pas modifier NouvelleRègle version 1.0 une fois qu'une version 2.0 a été créée. Vous devez copier la version 1.0 et la modifier. En enregistrant ces modifications, vous créez la version 3.0.

Informations complémentaires :

Modification d'une règle de suppression ou de récapitulation (page 547)

Tâches liées aux règles de suppression et de récapitulation

Les règles de suppression et de récapitulation vous permettent de contrôler votre flux d'événements et de gérer la taille du magasin de journaux d'événements en éliminant ou en combinant certains événements. Les règles de suppression empêchent tout enregistrement des événements natifs correspondant à leurs critères de qualification. Les règles de récapitulation regroupent plusieurs événements natifs dans un seul événement ajusté, qui apparaît en lieu et place des événements de composant d'origine.

Important : Créez et utilisez les règles de suppression et de récapitulation avec précaution. Elles peuvent en effet empêcher l'enregistrement et l'apparition de certains événements natifs. Nous recommandons de tester les règles de suppression et de récapitulation personnalisées dans un environnement de test avant de les déployer.

Les tâches de suppression et de récapitulation peuvent toutes être exécutées à partir de la zone Collecte de journaux de l'interface. Vous pouvez créer, modifier et supprimer des règles de suppression et de récapitulation personnalisées.

Informations complémentaires :

Création d'une règle de suppression (page 532)
Création d'une règle de récapitulation (page 537)
Application d'une règle de suppression ou de récapitulation (page 543)
Copie d'une règle de suppression ou de récapitulation (page 546)
Modification d'une règle de suppression ou de récapitulation (page 547)
Suppression d'une règle de suppression ou de récapitulation (page 548)
Importation d'une règle de suppression ou de récapitulation (page 549)
Exportation d'une règle de suppression ou de récapitulation (page 550)

Effets des règles de suppression

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

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

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

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

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

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

Création d'une règle de suppression

Vous pouvez utiliser des règles de suppression pour empêcher de grands nombres de transactions de routine ou de transactions connues et prévisibles de faire gonfler votre magasin de journaux d'événements et de brouiller l'image de votre environnement. Vous pouvez ainsi utiliser une règle de suppression pour éliminer les événements d'information Syslog inutiles, en particulier dans les cas où la source des événements ne peut pas être configurée pour envoyer uniquement l'ensemble des données requis.

Le processus de création d'une règle de suppression, à l'aide de l'Assistant de règles de suppression, se compose des étapes suivantes

1. Ouverture de l'Assistant de règles de suppression
2. Attribution d'un nom à la règle : saisir le nom de la règle et une description.
3. Sélection d'événement : identifier un événement à supprimer à l'aide des attributs de normalisation CEG et d'un filtrage avancé facultatif.

Remarque : Une fois créée, vous devez appliquer la règle de suppression pour la rendre disponible dans votre environnement.

Informations complémentaires :

Ouverture de l'assistant de suppression (page 533)
Attribution d'un nom à une règle de suppression (page 533)
Application d'une règle de suppression ou de récapitulation (page 543)

Ouverture de l'assistant de suppression

Pour créer une nouvelle règle de suppression ou modifier une règle existante, ouvrez l'assistant de suppression.

Pour ouvrir l'assistant de suppression

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Suppression et récapitulation.

   Les boutons Suppression et Récapitulation apparaissent dans le volet Détails.

3. Cliquez sur Nouvelle règle de suppression :  .

   L'assistant de suppression s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier de règle sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier de règle et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires

Attribution d'un nom à une règle de suppression (page 533)

Attribution d'un nom à une règle de suppression

Toute règle de suppression doit être nommée. Vous pouvez également saisir une description facultative pour référence.

Pour nommer une règle de suppression

1. Ouvrez l'assistant de suppression.
2. Saisissez un nom pour la nouvelle règle.
3. Saisissez une description (facultatif).
4. Avancez jusqu'à l'étape Filtrage.

Informations complémentaires

Création d'une règle de suppression (page 532)

Sélection d'un événement à supprimer

Spécifiez l'événement natif que la règle doit supprimer, en paramétrant un filtre simple pour les champs de normalisation d'événement CEG. Ces quatre champs, qui font partie de la classe propre aux événements, sont fournis pour tous les événements exprimés dans la CEG, ce qui vous permet d'identifier un événement natif avec précision.

Vous pouvez spécifier la combinaison des champs de normalisation d'événement de votre choix, à l'aide de l'onglet Filtres simples. Vous pouvez également utiliser les filtres avancés pour détailler davantage l'identification des événements. Vous devez définir au moins un filtre simple pour une règle de suppression.

Pour sélectionner un événement de règle de suppression

1. Ouvrez l'assistant de suppression, entrez les informations requises et avancez jusqu'à l'étape Filtrage en cours.
2. Créez des filtres simples pour sélectionner l'événement de votre choix, en cochant la case appropriée, puis en sélectionnant ou en saisissant la valeur de votre choix. Les champs disponibles sont les suivants :

   Modèle idéal

   Décrit la classe générale de technologies impliquée dans l'événement, Pare-feu ou Unité réseau, par exemple.

   Catégorie d'événement

   Décrit les grandes catégories d'événement au sein du Modèle idéal. Par exemple, tous les événements de compte et de groupe d'utilisateurs, ainsi que les évènements liés aux rôles sont enregistrés dans la Catégorie d'événement "Gestion des identités". Chaque catégorie d'événement comporte une ou plusieurs classes (sous-catégories), si bien que tout choix modifie les sélections disponibles dans le menu Classe d'événement.

   Classe d'événement

   Fournit une classification plus détaillée des événements dans une catégorie d'événement spécifique. Par exemple, les événements Gestion des identités sont répartis en trois classes : compte, groupe et identité. Chaque catégorie d'événement compte une ou plusieurs actions associées, si bien que tout choix modifie les sélections disponibles dans le menu Action d'événement.

Action d'événement

Décrit les actions courantes pour chaque catégorie d'événement et classe. Par exemple, Gestion des comptes, une classe de la catégorie Gestion des identités, contient des actions de création, suppression et modification d'un compte.

3. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle règle apparaît dans la liste. Sinon, l'étape choisie s'affiche.

Lorsque vous créez une nouvelle règle, elle est enregistrée en version 1.0. Si vous modifiez la règle ultérieurement, une copie distincte de la règle est stockée en tant que nouvelle version. Vous pouvez afficher des versions antérieures et les appliquer ou les copier comme bon vous semble.

Informations complémentaires :

Création d'un filtre d'événement simple (page 301)
Création d'un filtre d'événement avancé (page 303)
Utilisation des filtres avancés (page 535)

Utilisation des filtres avancés

Les filtres avancés permettent de qualifier toute requête du magasin de journaux d'événements concernant la suppression ou la récapitulation. L'interface Filtres avancés vous aide à créer la syntaxe de filtre appropriée grâce à un formulaire de saisie des colonnes logiques, opérateurs et valeurs, selon vos exigences en matière de règles de suppression et de récapitulation.

Remarque : Cette section contient une brève présentation des termes utilisés dans les filtres avancés pour les règles de suppression et de récapitulation. Pour utiliser les filtres avancés au maximum de leur potentiel, vous devez posséder une connaissance approfondie des termes de filtre et de la grammaire commune aux événements.

Les termes suivants permettent d'associer plusieurs instructions de filtre.

And

Affiche les informations de l'événement si *tous* les termes ajoutés sont vrais.

Or

Affiche les informations de l'événement si *l'un* des termes ajoutés est vrai.

Les opérateurs SQL suivants sont utilisés par les filtres avancés pour créer les conditions de base pour les règles de suppression et de récapitulation.

Correspondance

Inclut toute information d'événement qui correspond au moins à un des caractères alphanumériques que vous avez saisis, ce qui vous permet de rechercher des mots clés. Cette recherche est sensible à la casse.

Correspondance (ignorer la casse)

Inclut toute information d'événement qui correspond au moins à un des caractères alphanumériques que vous avez saisis, ce qui vous permet de rechercher des mots clés. Cette recherche n'est pas sensible à la casse.

Aucune correspondance

Inclut toute information d'événement qui ne correspond pas au moins à un des caractères alphanumériques que vous avez saisis. Cette recherche est sensible à la casse.

Aucune correspondance (ignorer la casse)

Inclut toute information d'événement qui ne correspond pas au moins à un des caractères alphanumériques que vous avez saisis. Cette recherche n'est pas sensible à la casse.

Correspondance d'expression régulière

Inclut toute information d'événement qui correspond au moins à un des caractères d'expression régulière que vous avez saisis Cet opérateur permet d'effectuer des recherches dans un environnement multi-octet, en utilisant les caractères génériques.

Aucune correspondance d'expression régulière

Inclut toute information d'événement qui ne correspond pas au moins à un des caractères d'expression régulière que vous avez saisis Cet opérateur permet d'effectuer des recherches dans un environnement multi-octet, en utilisant les caractères génériques.

Opérateurs relationnels

Inclut les informations de l'événement si la colonne porte la relation appropriée à la valeur saisie. Les opérateurs relationnels suivants sont disponibles.

- Egal à (numérique)
- Différent de (numérique)
- Plus grand (numérique)
- Plus grand ou égal (numérique)
- Plus petit (numérique)
- Plus petit ou égal (numérique)

Par exemple, l'utilisation de *Plus grand* inclut les informations de l'événement à partir de la colonne choisie si sa valeur est supérieure à la valeur définie.

Tous ces opérateurs localisent uniquement des chiffres ; pour rechercher d'autres caractères, sélectionnez l'un des opérateurs de type "correspondance", le cas échéant.

Informations complémentaires :

Attribution d'un nom à une règle de suppression (page 533)
Création d'un filtre d'événement avancé (page 303)

Création d'une règle de récapitulation

Vous pouvez utiliser des règles de récapitulation pour regrouper certains événements natifs d'un type courant dans un seul événement ajusté. Vous économisez ainsi de l'espace dans votre magasin de journaux d'événements et simplifiez l'analyse des événements.

Vous pouvez par exemple créer une règle de récapitulation qui enregistre un seul événement ajusté pour trois échecs de connexion successifs par un même utilisateur. Votre magasin de journaux d'événements enregistre ainsi un seul événement au lieu de trois.

Le processus de création ou de modification d'une règle de récapitulation à l'aide de l'Assistant de règle de récapitulation se compose principalement des étapes suivantes.

1. Ouverture de l'Assistant de règle de récapitulation
2. Seuils de récapitulation : définir le nombre ou la fréquence d'événements natifs à regrouper dans un événement récapitulé.
3. Sélection d'événement : identifier un événement à récapituler à l'aide des attributs de normalisation CEG et d'un filtrage avancé facultatif.
4. Récapitulation : contrôler la manière dont l'événement récapitulé final sera présenté dans les rapports.

Remarque : Une fois créée, vous devez appliquer la règle de récapitulation pour la rendre disponible dans votre environnement.

Informations complémentaires :

Ouverture de l'assistant de récapitulation (page 538)
Définition de seuils de récapitulation (page 538)
Configuration d'un affichage de récapitulation (page 541)
Application d'une règle de suppression ou de récapitulation (page 543)

Ouverture de l'assistant de récapitulation

Pour créer une nouvelle règle de récapitulation ou modifier une règle existante, ouvrez l'assistant de récapitulation.

Pour ouvrir l'assistant de suppression

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Suppression et récapitulation.

   Les boutons Suppression et Récapitulation apparaissent dans le volet Détails.

3. Cliquez sur Nouvelle règle de récapitulation :  .

   L'assistant de récapitulation s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier de règle sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier de règle et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires

Définition de seuils de récapitulation (page 538)
Configuration d'un affichage de récapitulation (page 541)

Définition de seuils de récapitulation

Pour créer ou modifier une règle de récapitulation, entrez les informations générales et définissez des seuils de récapitulation. Les seuils peuvent être un nombre d'événements, une fréquence d'occurrence ou une combinaison de ces deux cas, qui déclenchent la création d'un événement récapitulé.

Pour définir des seuils de récapitulation

1. Ouvrez l'assistant de récapitulation.
2. Attribuez un nom à la nouvelle règle. Vous pouvez également saisir une description facultative pour référence.

3. Définissez la combinaison en spécifiant le nombre d'événements natifs et le temps écoulé utilisés par votre règle pour créer un seul événement ajusté, à l'aide des menus Récapitulation d'événement.

   Activer le seuil de nombre d'événements

   Détermine si la règle utilise ou non un seuil d'événements. Le seuil d'événements doit être supérieur à un. La sélection de cette option définit un nombre maximal d'événements. Si cette case à cocher est désélectionnée et que le délai d'expiration d'événement est activé, seule la période de temps est prise en compte dans la récapitulation des événements. Si les deux paramètres sont activés, un événement récapitulé est créé pour chaque période de temps spécifiée, tant que survient au moins un événement brut qualifié.

   Nombre maximum d'événements

   Définit le nombre d'événements natifs déclenchant un événement récapitulé. Lorsque le nombre d'événements natifs spécifié survient, un événement récapitulé est créé.

   Minimum : 2

   Maximum : 5 000

   Activer le délai d'expiration d'événement

   Détermine si la règle utilise ou non un seuil de période. La sélection de cette option définit une valeur temporelle. Si cette case à cocher est désélectionnée, un événement récapitulé se produit uniquement lorsque le seuil de nombre d'événements est atteint.

   Période

   Définit le temps, en secondes, qui s'écoule avant le déclenchement un événement récapitulé, si des événements du type spécifié sont survenus. Lorsque ce seuil est atteint, un événement récapitulé est créé dès lors qu'au moins un événement natif qualifié s'est produit. Vous pouvez définir la période sur zéro, ce qui entraîne la création d'un événement récapitulé uniquement lorsque le seuil maximum d'événements est atteint.

   Minimum : 0

   Maximum : 86 400

   Par exemple, dans le cas d'une règle récapitulant les échecs de connexion, la sélection de la valeur 3 dans le menu Nombre maximum d'événements et de la valeur 10 dans le menu Période génère un événement récapitulé au bout de trois échecs de connexion ou toutes les 10 secondes dès lors qu'au moins une connexion échoue.

4. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle règle apparaît dans la liste. Sinon, l'étape choisie s'affiche.

Informations complémentaires

Configuration d'un affichage de récapitulation (page 541)

Sélection d'un événement de récapitulation

Spécifiez l'événement natif que la règle doit résumer, en paramétrant un filtre simple pour les champs de normalisation d'événement CEG (Common Event Grammar, Grammaire commune aux événements). Ces quatre champs, qui font partie de la classe propre aux événements, sont fournis pour tous les événements exprimés dans la CEG, ce qui vous permet d'identifier un événement.

Vous pouvez spécifier la combinaison des champs de normalisation d'événement de votre choix, à l'aide de l'onglet Filtres simples. Vous pouvez également utiliser les filtres avancés pour détailler davantage l'identification des événements. Spécifiez au moins un filtre simple pour une règle de suppression.

Pour sélectionner un événement de règle de récapitulation

1. Ouvrez l'assistant de récapitulation et avancez jusqu'à l'étape Filtrage en cours.
2. Créez des filtres simples pour sélectionner l'événement de votre choix, en activant la case à cocher appropriée, puis en sélectionnant ou en entrant la valeur que vous voulez. Les champs disponibles sont les suivants :

   Modèle idéal

   Décrit la classe générale de technologies impliquée dans l'événement. Par exemple, Pare-feu et Unité réseau sont des modèles idéaux.

   Catégorie d'événement

   Décrit les grandes catégories d'événement. Par exemple, tous les événements de compte et de groupe d'utilisateurs, ainsi que les évènements liés aux rôles sont enregistrés dans la Catégorie d'événement "Gestion des identités". Chaque catégorie d'événement comporte une ou plusieurs classes (sous-catégories), si bien que tout choix modifie les sélections disponibles dans le menu Classe d'événement.

   Classe d'événement

   Fournit une classification plus détaillée des événements dans une catégorie d'événement spécifique. Par exemple, les événements Gestion des identités sont répartis en trois classes : compte, groupe et identité. Chaque catégorie d'événement compte une ou plusieurs actions associées, si bien que tout choix modifie les sélections disponibles dans le menu Action d'événement.

   Action d'événement

   Décrit les actions courantes pour chaque catégorie d'événement et classe. Par exemple, Gestion des comptes, une classe de la catégorie Gestion des identités, contient des actions de création, suppression et modification d'un compte.

3. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle règle apparaît dans la liste. Sinon, l'étape sélectionnée s'affiche.

Informations complémentaires :

Création d'un filtre d'événement simple (page 301)
Création d'un filtre d'événement avancé (page 303)
Configuration d'un affichage de récapitulation (page 541)
Définition de seuils de récapitulation (page 538)

Configuration d'un affichage de récapitulation

Les règles de récapitulation contrôlent la manière dont les événements natifs s'affichent dans l'événement ajusté. Un affichage de récapitulation peut être configuré à l'aide des champs Récapitulés selon et Cumulés.

Pour configurer un affichage de règle de récapitulation

1. Ouvrez l'assistant de récapitulation et avancez jusqu'à l'étape Récapitulation.
2. A l'aide du contrôle de déplacement, sélectionnez le ou les champs qui doivent récapituler l'événement ajusté.

   Récapitulés selon

   Contrôle le ou les champs selon lesquels les informations récapitulées sont regroupées. Par exemple, dans le cas d'une règle récapitulant les échecs de connexion, sélectionnez source_username pour afficher le nombre d'événements d'échec de connexion pour chaque utilisateur unique. Pour que la règle soit complète, vous devez sélectionner au moins un champ Récapitulés selon.

3. Sélectionnez le ou les champs selon lesquels cumuler l'événement ajusté (facultatif).

   Cumulés

   Contrôle le ou les champs selon lesquels les informations récapitulées sont subdivisées, en fonction du champ de récapitulation. Par exemple, dans le cas d'une règle récapitulant les échecs de connexion, sélectionnez source_username en tant que champ Récapitulés selon et dest_hostname en tant que champ Cumulés. Ainsi s'affiche le nombre d'événements d'échec de connexion pour chaque utilisateur unique, subdivisés en fonction de l'hôte auquel l'utilisateur a tenté de se connecter.

   Les informations des champs Cumulés sont conservées dans le champ d'événement brut des événements récapitulés. Dans l'exemple précédent, chaque hôte unique auquel l'utilisateur a tenté de se connecter est stocké avec le nombre d'occurrences au format suivant : *nomd'hôte1:2,nomd'hôte2:5*. Dans cet exemple, on peut relever 2 tentatives de connexion sur l'hôte 1 et 5 tentatives sur l'hôte 2.

   Les champs Cumulés sont facultatifs ; il n'est pas nécessaire de sélectionner un champ de ce type pour finaliser une règle.

4. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle règle apparaît dans la liste. Sinon, l'étape choisie s'affiche.

Lorsque vous créez une nouvelle règle, elle est enregistrée en version 1.0. Si vous modifiez la règle ultérieurement, une copie distincte de la règle est stockée en tant que nouvelle version. Vous pouvez afficher des versions antérieures et les appliquer ou les copier comme bon vous semble.

Informations complémentaires :

Définition de seuils de récapitulation (page 538)

Application d'une règle de suppression ou de récapitulation

Après avoir créé une règle de suppression ou de récapitulation, vous devez l'appliquer pour la rendre disponible dans votre environnement. Cette fonction évite l'application de règles de suppression ou de récapitulation sans effectuer des tests et une validation appropriés.

Pour appliquer une règle de suppression ou de récapitulation

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.

   La Liste de services s'affiche.

2. Cliquez sur l'icône Magasin de journaux d'événements.

   Le volet de configuration du Magasin de journaux d'événements apparaît.

3. Localisez et sélectionnez la règle de suppression ou de récapitulation à appliquer grâce au contrôle de déplacement approprié.

4. Cliquez sur Enregistrer.

   Un message de confirmation s'affiche lorsque la règle a été correctement appliquée.

Application de la suppression et de la récapitulation à des composants d'agents

Vous pouvez affecter des règles de suppression, de récapitulation ou les deux à des groupes d'agents, des agents ou des connecteurs de votre environnement. Ces règles peuvent remplacer ou compléter toute règle de suppression ou de récapitulation appliquée au serveur CA Enterprise Log Manager. Vous pouvez ainsi rationaliser le processus de transmission/réception d'événements en contrôlant l'emplacement où s'effectue l'ajustement des événements.

Par exemple, si vous disposez d'un groupe d'agents Windows, vous pouvez associer une règle de suppression qui élimine les événements Windows indésirables sur les agents du groupe. Cela évite à l'ensemble des événements entrants d'être soumis à un contrôle Windows au niveau du serveur CA Enterprise Log Manager.

Vous pouvez appliquer des règles de suppression et de récapitulation à différents niveaux de la hiérarchie des dossiers d'agents.

- Dans le dossier Explorateur d'agent, vous pouvez appliquer des règles à tout groupe d'agents, agent ou connecteur.
- Dans un dossier de groupe d'agents spécifique, vous pouvez appliquer des règles à tous les agents de ce groupe ainsi qu'à tous les connecteurs qui leur sont affectés.
- A partir d'un agent, vous pouvez appliquer des règles à ce seul agent et à tous les connecteurs qui lui sont affectés.

La procédure d'application de règles de suppression ou de récapitulation à des composants d'agents comprend les étapes ci-dessous.

1. Ouverture de l'Assistant de gestion des règles
2. Sélection des cibles (groupes d'agents, agents ou connecteurs)
3. Choix des règles de suppression à appliquer
4. Choix des règles de récapitulation à appliquer

L'Assistant de gestion des règles vous permet également de supprimer des règles de suppression ou de récapitulation de plusieurs groupes d'agents, agents ou connecteurs.

Informations complémentaires :

Ouverture de l'assistant de gestion des règles de récapitulation (page 544)
Sélection des cibles de la suppression et de la récapitulation (page 545)
Choix des règles de suppression à appliquer (page 545)
Choix des règles de récapitulation à appliquer (page 545)

Ouverture de l'assistant de gestion des règles de récapitulation

Pour appliquer des règles de suppression ou de récapitulation à des groupes d'agents, à des agents ou à des connecteurs, vous pouvez utiliser l'Assistant de gestion des règles.

Pour ouvrir l'Assistant de gestion des règles

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier Explorateur d'agent, puis sur Gérer les règles de suppression et de récapitulation : 

   L'Assistant de gestion des règles s'affiche.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Sélection des cibles de la suppression et de la récapitulation

Pour appliquer des règles de suppression et de récapitulation à des composants d'agents, sélectionnez les cibles des règles.

Pour sélectionner des cibles

1. Ouvrez l'Assistant de gestion des règles.
2. Indiquez à qui vous souhaitez appliquer les règles : groupes d'agents, agents ou connecteurs.
3. Sélectionnez Supprimer si vous souhaitez supprimer des règles et non pas en ajouter (facultatif).
4. Sélectionnez les cibles qui vous intéressent à l'aide du contrôle de déplacement.

   Remarque : Vous pouvez rechercher des noms d'agents ou de connecteurs. Si aucun agent ou connecteur n'apparaît dans la liste des éléments disponibles, cliquez sur Rechercher pour afficher tous les agents ou connecteurs disponibles.
5. Avancez jusqu'à l'étape d'application des règles qui vous intéresse.

Choix des règles de suppression à appliquer

Pour finir d'affecter des règles de suppression à un groupe d'agents, agent ou connecteur, sélectionnez les règles à appliquer.

Pour choisir des règles de suppression

1. Ouvrez l'assistant d'application des règles de suppression et avancez jusqu'à l'étape Appliquer les règles de suppression.
2. Choisissez les règles, parmi celles disponibles, à appliquer à l'aide du contrôle de déplacement.

   Remarque : Vous pouvez rechercher des règles de suppression à l'aide du champ Schéma de règle de suppression.
3. Cliquez sur Enregistrer et fermer.

   Les règles sélectionnées sont appliquées aux cibles choisies.

Choix des règles de récapitulation à appliquer

Pour finir d'affecter des règles de récapitulation à un groupe d'agents, à un agent ou à un connecteur, sélectionnez les règles à appliquer.

Pour sélectionner les règles de récapitulation

1. Ouvrez l'assistant de gestion des règles de récapitulation et avancez jusqu'à l'étape Appliquer les règles de récapitulation.

2. Choisissez, à l'aide du contrôle de déplacement, les règles à appliquer parmi celles disponibles.

   Remarque : Vous pouvez rechercher des règles de récapitulation à l'aide du champ Schéma de règle de récapitulation.

3. Cliquez sur Enregistrer et fermer dès que vous avez terminé.

4. Les règles sélectionnées sont appliquées aux cibles choisies. Si vous avez sélectionné Supprimer à l'étape Sélectionner des cibles, les règles que vous venez de sélectionner sont supprimées.

Copie d'une règle de suppression ou de récapitulation

Vous pouvez copier une règle de suppression ou de récapitulation, ce qui vous permet de créer une nouvelle règle basée sur une règle existante.

Pour copier une règle de suppression ou de récapitulation

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Suppression et récapitulation.

   Les boutons de suppression et de récapitulation apparaissent dans le volet Détails.

3. Cliquez sur le dossier Suppression et récapitulation qui contient la règle que vous souhaitez copier.

   Le dossier qui s'ouvre affiche les règles.

4. Choisissez la règle à copier, puis cliquez sur Copier l'élément sélectionné  .

   L'assistant de suppression ou de récapitulation s'ouvre et affiche la règle.

5. Effectuez les modifications souhaitées, puis cliquez sur Enregistrer et fermer.

   La règle s'affiche dans la liste appropriée.

Modification d'une règle de suppression ou de récapitulation

Vous pouvez modifier une règle de suppression ou de récapitulation.

Pour modifier une règle de suppression ou de récapitulation

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Suppression et récapitulation.

   Les boutons de suppression et de récapitulation apparaissent dans le volet Détails.

3. Cliquez sur le dossier Suppression et récapitulation qui contient la règle que vous souhaitez modifier.

4. Sélectionnez la règle à modifier, puis cliquez sur l'icône Modifier une règle de récapitulation ou de suppression.

   L'assistant de suppression ou l'assistant de récapitulation s'ouvre et affiche la règle sélectionnée.

5. Effectuez les changements souhaités, puis cliquez sur Enregistrer et fermer.

   La règle apparaît dans la liste appropriée comme une nouvelle version de la règle modifiée.

Informations complémentaires :

Versions de composant pour l'ajustement d'événement (page 529)

Suppression d'une règle de suppression ou de récapitulation

Vous pouvez supprimer une règle de suppression ou de récapitulation inutile.

Pour supprimer une règle de suppression ou de récapitulation

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Suppression et récapitulation.

   Les boutons de suppression et de récapitulation apparaissent dans le volet Détails.

3. Cliquez sur le dossier Suppression et récapitulation qui contient la règle que vous souhaitez supprimer.

4. Sélectionnez la règle à supprimer, puis cliquez sur l'icône Supprimer une règle de récapitulation ou de suppression. La version actuelle est sélectionnée par défaut. Vous pouvez sélectionner une version plus ancienne à supprimer dans la liste déroulante Version du volet Détails.

   Une boîte de dialogue de confirmation apparaît. Si vous avez appliqué la règle à une intégration, un avertissement s'affiche. Une fois supprimée, la règle disparaît également de l'intégration.

5. Cliquez sur Oui.

   La règle supprimée disparaît de la liste appropriée.

Importation d'une règle de suppression ou de récapitulation

Vous pouvez importer une règle de suppression ou de récapitulation. Cette opération vous permet de déplacer les règles d'un environnement à un autre. Vous pouvez ainsi importer des règles créées dans un environnement de test dans votre environnement réel.

Pour importer une règle de suppression ou de récapitulation

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Règles de récapitulation et de suppression.

   Les boutons Importer une règle de récapitulation ou de suppression et Exporter une règle de récapitulation ou de suppression apparaissent dans le volet Détails.

3. Cliquez sur Importer une règle de récapitulation ou de suppression.

   La boîte de dialogue d'importation de fichier s'affiche.

4. Recherchez le fichier que vous souhaitez importer et cliquez sur OK.

   L'assistant de suppression ou de récapitulation s'ouvre sur les détails de la règle que vous avez sélectionnée.

5. Effectuez les changements souhaités, puis cliquez sur Enregistrer et fermer. Si la règle importée partage le même nom qu'une règle déjà présente dans votre base de données de gestion, vous êtes invité à changer de nom.

   La règle importée apparaît dans le dossier de suppression ou de récapitulation approprié.

Exportation d'une règle de suppression ou de récapitulation

Vous pouvez exporter une règle de suppression ou de récapitulation. Cette opération vous permet de partager des règles entre plusieurs environnements. Vous pouvez par exemple exporter des règles créées dans un environnement de test dans votre environnement réel.

Pour exporter une règle de suppression ou de récapitulation

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Règles de récapitulation et de suppression.

   Le bouton Exporter une règle de récapitulation ou de suppression s'affiche dans le volet Détails.

3. Cliquez sur le dossier Règles de suppression ou Règles de récapitulation qui contient le fichier à exporter.

   Le dossier se développe et vous pouvez consulter les différents fichiers qu'il contient.

4. Sélectionnez la règle à exporter, puis cliquez sur Exporter une règle de récapitulation ou de suppression. La version actuelle est sélectionnée par défaut. Vous pouvez sélectionner une version plus ancienne à exporter dans la liste déroulante Version du volet Détails.

   Une boîte de dialogue vous permettant de sélectionner l'emplacement d'exportation s'ouvre.

5. Saisissez un chemin ou naviguez jusqu'à l'emplacement où vous souhaitez stocker la règle exportée, puis cliquez sur Enregistrer.

   Une boîte de dialogue vous confirmant l'exportation apparaît.

6. Cliquez sur OK.

   La règle est exportée.

Création d'une règle de suppression des événements Windows 560

Lorsqu'il est activé sur un serveur Windows, l'audit des accès aux objets génère un volume important de trafic d'événements, pour certains inutilement redondants. Par exemple, Windows génère deux événements chaque fois qu'un administrateur ouvre Microsoft Management Console (mmc.exe). Ces événements sont identifiés par les numéros 560 et 562.

Dans cet exemple, vous pouvez créer une règle qui supprime les événements Windows avec une valeur event_id de 560. Les étapes de la procédure suivante vous montrent comment utiliser l'assistant et obtenir une règle de suppression que vous pouvez utiliser dans votre environnement réseau.

Pour commencer, vous devez vous connecter à un serveur CA Enterprise Log Manager en tant qu'utilisateur possédant le rôle Administrator et les droits associés. Vous ne pouvez pas créer ou modifier des règles de suppression en étant connecté en tant qu'utilisateur EiamAdmin.

Pour créer une règle de suppression des événements Windows 560

1. Ouvrez l'Assistant de règles de suppression.
2. Tapez "Suppression des événements Windows 560" dans le champ de saisie du nom et ajoutez la description suivante : "Cette règle supprime l'événement Windows 560 car un événement 562 est déjà créé par le SE pour le même type d'accès aux ressources. Il n'est pas nécessaire, pour des raisons de conformité, de conserver les deux événements."
3. Avancez jusqu'à l'étape Filtrage en cours et sélectionnez les filtres simples suivants.
   a. Valeur Modèle idéal, Système d'exploitation.
   b. Valeur Catégorie d'événement, Accès aux ressources.
   c. Valeur Classe d'événement, Ouverture d'une ressource.
   d. Valeur Action d'événement, Activité de la ressource.

4. Cliquez sur l'onglet Filtres avancés et sur le bouton Nouveau filtre d'événement.

   Une nouvelle ligne de filtre apparaît dans le tableau. Cliquez sur une valeur ou sur l'espace vide dans chaque cellule du tableau pour sélectionner une valeur ou en entrer une nouvelle.

   Le champ d'opérateur logique prend sa valeur par défaut AND. Si vous souhaitez supprimer plusieurs types d'événements, vous pouvez entrer leurs ID en ajoutant de nouvelles lignes et en utilisant l'opérateur logique OR.

5. Définissez les valeurs de filtre de champ avancé.

   a. Cliquez sur la valeur du champ Colonne et sélectionnez le champ event_id.

   b. Cliquez sur le champ Opérateur et sélectionnez Egal à.

   c. Cliquez sur le champ Valeur et entrez la valeur 560.

6. Cliquez sur Enregistrer et fermer.

   L'assistant crée automatiquement un dossier Utilisateur destiné à contenir vos règles de suppression. Vous pouvez voir ce dossier en développant le dossier Règles de suppression.

Chapitre 13 : Mappage et analyse

Ce chapitre traite des sujets suivants :

Etats d'événement

Les informations sur les événements dans votre environnement passent par plusieurs étapes, de l'occurrence initiale à l'affichage final éventuel par CA Enterprise Log Manager. Etant donné que le terme "événement" peut faire référence à n'importe laquelle de ces étapes, nous utilisons la terminologie suivante pour distinguer les états possibles des événements dans votre environnement.

Evénement natif

Fait référence à l'occurrence d'origine de l'état ou de l'action déclenchant l'événement, un échec d'authentification ou une violation de pare-feu, par exemple. Les événements natifs sont envoyés par le service de connecteur ou d'écouteur approprié. Ils sont analysés, mappés, puis insérés dans le magasin de journaux d'événements, où ils peuvent être affichés en tant qu'événements bruts et/ou ajustés.

Evénement brut

Fait référence à la communication envoyée par l'agent de surveillance approprié. Les événements bruts contiennent des informations sur l'événement natif, souvent sous la forme d'une chaîne Syslog ou d'une paire nom-valeur. Ces informations sont stockées et peuvent être interrogées sauf en cas d'altération par des règles de suppression ou de récapitulation. Les événements supprimés ne sont pas enregistrés dans le magasin de journaux d'événements ; un ensemble d'événements récapitulés est enregistré sous la forme d'un seul événement exprimant le résultat de la récapitulation.

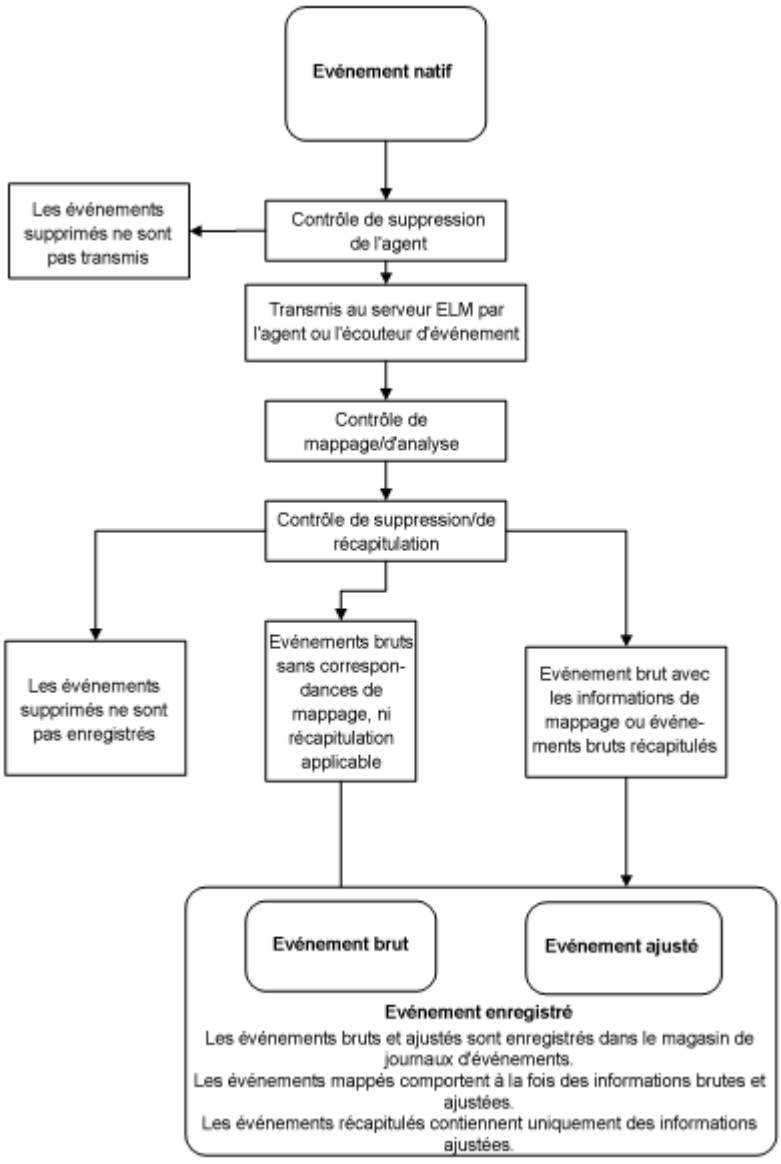
Evénement ajusté

Fait référence aux informations d'événement mappées et/ou récapitulées par CA Enterprise Log Manager. Ces informations sont stockées et peuvent être interrogées.

Evénement enregistré

Fait référence aux informations d'événement brut ou ajusté dans le magasin de journaux d'événements. Les événements bruts et les événements ajustés sont toujours enregistrés sauf s'ils sont supprimés ou récapitulés. Les événements mappés comportent normalement à la fois des informations brutes et ajustées. Ces informations sont stockées et peuvent être interrogées.

Consultez le diagramme suivant pour plus d'informations sur les états d'événement.



Informations complémentaires :

Tâches liées aux règles de mappage et d'analyse (page 555)
Tâches liées aux règles de suppression et de récapitulation (page 530)
Remarques sur le magasin de journaux d'événements (page 147)

Tâches liées aux règles de mappage et d'analyse

Les paires de fichiers d'analyse de message (XMP) et de mappage de données (DM) recueillent et normalisent les données issues de certains types de sources d'événement. La plupart des événements natifs entrants font l'objet de processus d'analyse, puis de mappage afin de créer un événement pouvant donner lieu à un rapport et qui est inséré dans le magasin de journaux d'événements. Les événements transmis par SAPI ou iTechnology ne nécessitent pas d'analyse et accèdent directement à l'étape de mappage des données.

Remarque : Pour profiter pleinement de ces fonctions avancées, vous devez posséder une connaissance approfondie des événements bruts et collectés dans votre environnement, des champs cibles que vous souhaitez analyser, de la syntaxe des expressions régulières, du composant CEG, ainsi que des fichiers DM et XMP et de la manière dont ils analysent les événements.

Les fichiers XMP de type XML lisent les données d'événements bruts entrants et créent des paires nom-valeur, selon vos spécifications. Les fichiers DM mappent ensuite les paires nom-valeur des événements attribuées par l'analyse de message dans la grammaire commune aux événements. Lorsque vous créez de nouveaux fichiers d'analyse et de mappage, considérez-les comme faisant partie d'un processus. Une analyse efficace et complète entraîne un mappage lui-même rapide et efficace au sein du processus.

Informations complémentaires :

Versions de composant pour l'ajustement d'événement (page 529)
Création d'un fichier d'analyse de message (page 556)
Création d'un fichier de mappage de données (page 574)

Création d'un fichier d'analyse de message

Vous pouvez utiliser l'Assistant de fichier d'analyse pour créer, modifier et analyser un fichier d'analyse de message (XMP). Les fichiers d'analyse lisent les données d'événements bruts entrants et créent des paires nom-valeur, ce qui vous permet d'établir des mappages avant même le processus de mappage des données. L'efficacité globale du mappage en est améliorée.

Remarque : Les noms conformes à la CEG ne sont pas obligatoires pour l'analyse des événements, ce qui vous offre une flexibilité supplémentaire pour créer des paires nom/valeur. Les champs CEG peuvent être sélectionnés, mais les noms et valeurs des champs ne sont pas limités aux valeurs CEG.

Le processus de création ou de modification d'un fichier XMP se compose des étapes suivantes.

1. Ouverture de l'Assistant de fichier d'analyse
2. Indication des détails du fichier : nom du fichier, nom du journal et informations de support, notamment
3. Localisation d'exemples d'événements pour le test et la construction de fichier
4. Définition de valeurs globales qui s'appliquent à tous les événements analysés par le fichier
5. Création ou modification de chaînes de précorrespondance pour commencer l'analyse des événements
6. Sélection de filtres de précorrespondance pour joindre des filtres d'analyse
7. Création ou modification des filtres d'analyse pour terminer l'analyse des événements
8. Analyse et enregistrement du fichier XMP nouveau ou modifié

Informations complémentaires :

Ouverture de l'Assistant de fichier d'analyse (page 557)
Définition des détails de fichier (page 557)
Chargement d'exemples d'événements (page 559)
Ajout de champs globaux (page 560)
Création d'un filtre de précorrespondance (page 561)
Analyse du fichier XMP (page 573)

Ouverture de l'Assistant de fichier d'analyse

Pour créer un nouveau fichier d'analyse de message ou modifier un fichier existant, vous devez ouvrir l'Assistant de fichier d'analyse.

Pour ouvrir l'Assistant de fichier d'analyse

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche située en regard du dossier Bibliothèque d'ajustement d'événement, afin de développer ce dossier, puis sélectionnez le dossier Mappage et analyse.

   Les boutons d'intégration d'un produit apparaissent dans le volet Détails.

3. Cliquez sur Nouvelle règle d'analyse de message :  .

   L'Assistant de fichier d'analyse s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires

Définition des détails de fichier (page 557)
Chargement d'exemples d'événements (page 559)
Création d'un filtre de précorrespondance (page 561)
Analyse du fichier XMP (page 573)

Définition des détails de fichier

Vous pouvez ajouter de nouveaux détails du fichier d'analyse, y compris le nom, la source et des informations de référence. Les fichiers nouvellement créés ou modifiés s'affichent dans le dossier Utilisateur de la zone Mappage et analyse.

Pour ajouter de nouveaux détails de fichier d'analyse

1. Ouvrez l'Assistant de fichier d'analyse.
2. Remplissez la zone Informations sur le fichier d'analyse comme indiqué aux sous-étapes suivantes.
   a. Entrez un nom pour le fichier. Le nom du fichier est obligatoire et ne peut pas contenir les caractères suivants : / \ : * ? " < > ^;'`,&{}[]. ou |.
   b. Tapez le nom du journal source pour identifier le nom du journal du type d'événement que le fichier doit analyser. La fonction de saisie semi-automatique vous présente les noms de journaux disponibles au fur et à mesure de la frappe. Le nom du journal que vous choisissez s'affiche dans le champ event_logname de l'événement ajusté.
   c. Ajoutez une description à titre de référence si nécessaire.
3. Ajoutez des Informations de support à titre de référence, comme indiqué aux sous-étapes suivantes (facultatif).
   a. Cliquez sur Ajouter un produit dans la zone Informations de support.

      Une nouvelle ligne d'informations de support apparaît.
   b. Cliquez sur le texte Nouveau produit ou Nouvelle version pour activer les champs de saisie et saisissez les informations de produit/version souhaitées.
4. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier d'analyse. Sinon, l'étape choisie apparaît.

Chargement d'exemples d'événements

Vous pouvez fournir des exemples d'événements à utiliser pour tester le nouveau fichier XMP en lançant une recherche dans le magasin de journaux d'événements ou en accédant à un fichier journal. Les exemples d'événements servent de modèles qui permettent de tester le fichier d'analyse à mesure que vous le construisez lors des autres étapes de l'assistant. Vous pouvez également utiliser les exemples d'événements pour tester la sortie d'analyse lors de l'étape finale de l'assistant.

Pour fournir des exemples d'événements

1. Ouvrez l'Assistant de fichier d'analyse et avancez jusqu'à l'étape de chargement des événements.

   L'écran de chargement des événements apparaît.

2. Sélectionnez le bouton radio Magasin de journaux ou Fichier journal dans la zone Rechercher des exemples d'événements.

   - Si vous sélectionnez Magasin de journaux

     a. Sélectionnez le type de source d'exemples d'événements souhaité dans le menu déroulant Colonne d'analyse. Choisissez result_string pour les sources d'événement WMI ou raw_event pour les sources d'événement Syslog.

     b. Sélectionnez la requête à utiliser pour fournir des exemples d'événements à l'aide du Filtre de balise de requête et de la Liste de requêtes.

     La requête apparaît, affichant des exemples d'événements que vous pouvez utiliser pour tester l'analyse au fur et à mesure de votre progression dans l'assistant.

     Remarque : Vous pouvez utiliser toute requête disponible ou personnalisée pour localiser des exemples d'événements. Si vous envisagez d'utiliser une requête personnalisée, nous vous recommandons de la créer et de la tester avant d'entamer le processus de conception de fichier d'analyse de message. Nous recommandons d'utiliser un fichier d'exemples d'événements comportant moins de 1 500 événements pour faciliter l'analyse.

   - Si vous sélectionnez Fichier journal, naviguez jusqu'au fichier journal de votre choix et cliquez sur Charger.

     Les événements du fichier journal apparaissent dans le volet Exemples d'événements. Vous pouvez utiliser les événements pour tester l'analyse au fur et à mesure de votre progression dans l'assistant.

     Remarque : L'assistant considère que chaque ligne du fichier est un événement. Les événements répartis sur plusieurs lignes ne sont pas pris en charge.

3. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier d'analyse. Sinon, l'étape choisie apparaît.

Ajout de champs globaux

Vous pouvez ajouter des champs globaux, qui sont des paires statiques associant un nom de champ à une valeur donnée. Le processus d'analyse ajoute les champs globaux à tous les événements analysés ; ces champs sont donc particulièrement adaptés aux valeurs par défaut comme le modèle idéal.

Pour ajouter des champs globaux

1. Ouvrez l'Assistant de fichier d'analyse, puis avancez jusqu'à l'étape Champs globaux.

   L'écran Champs globaux s'affiche.

2. Dans la zone Champs globaux, cliquez sur Ajouter un champ global.

   Une nouvelle ligne de champs globaux apparaît dans la table des champs et présente les entrées Nouveau champ global et Nouvelle valeur.

3. Cliquez sur le texte Nouveau champ global pour entrer les informations de nom souhaitées. La fonction de saisie semi-automatique vous présente les noms de champs CEG disponibles au fur et à mesure de la frappe. Vous pouvez cliquer sur l'un de ces champs pour le sélectionner ou saisir un nom de champ non CEG.

4. Cliquez sur le texte Nouvelle valeur pour entrer les informations de nom souhaitées.

5. Répétez les étapes 2 à 4 pour ajouter d'autres champs globaux, si nécessaire (facultatif).

6. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier d'analyse. Sinon, l'étape sélectionnée apparaît.

Création d'un filtre de précorrespondance

Vous pouvez créer un filtre de précorrespondance pour aider le fichier XMP à concentrer sa recherche d'informations d'événement à analyser. Le filtre de précorrespondance identifie une chaîne de texte sélectionnée pour restreindre le processus de sélection d'événement effectué ensuite par les filtres d'analyse. On peut considérer le fichier d'analyse comme un entonnoir dont le filtre de précorrespondance serait le cône et le filtre d'analyse le tube.

Plus le filtrage de précorrespondance est complet, plus le processus d'analyse est efficace. En effet, les catégories de précorrespondance affinées contribuent à réduire le travail de traitement requis pour analyser les événements.

Par exemple, pour analyser les événements de tentative d'accès, vous pouvez créer un filtre de précorrespondance qui recherche le texte "login" et lui ajouter des filtres d'analyse appropriés.

Remarque : La suppression d'un filtre de précorrespondance supprime également le(s) filtre(s) associé(s).

Pour créer un filtre de précorrespondance

1. Ouvrez l'Assistant de fichier d'analyse et avancez jusqu'à l'étape de définition de la correspondance et d'analyse des événements.

   L'assistant affiche tous les filtres de précorrespondance existants dans la liste Filtres de précorrespondance. En regard de chacun d'eux s'affiche entre parenthèses le nombre de précorrespondances à des exemples d'événements.

2. Cliquez sur Ajouter une chaîne de précorrespondance en haut de la liste Filtres de précorrespondance ou sélectionnez un filtre de précorrespondance à modifier.

3. Saisissez le texte que le filtre doit rechercher dans le champ de saisie Chaîne de précorrespondance.

   Les exemples d'événements qui correspondent au texte saisi apparaissent immédiatement, avec le nombre d'événements correspondants trouvés et analysés.

4. Cliquez sur Ajouter une précorrespondance sur la base des événements sans correspondance pour afficher tous les exemples d'événements sans correspondance (facultatif).

   Tous les exemples d'événements actuellement sans correspondance apparaissent dans la zone Evénements pour faciliter la création d'un nouveau filtre de précorrespondance.

5. Ajoutez ou modifiez autant de filtres de précorrespondance supplémentaires que nécessaire (facultatif).

6. Définissez l'ordre dans lequel vous souhaitez que le processus d'analyse recherche les précorrespondances à l'aide des flèches haut et bas en regard de la liste Filtres de précorrespondance. Pour améliorer l'efficacité de votre processus d'analyse, pensez à placer plus haut dans la liste des priorités les filtres de précorrespondance générant un plus grand nombre d'événements.

7. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier d'analyse. Sinon, l'étape choisie apparaît.

Création d'un filtre d'analyse

Vous pouvez créer un filtre d'analyse pour définir la manière dont le fichier XMP analyse les données d'événement. Chaque filtre d'analyse est relié à un filtre de précorrespondance. Après avoir localisé une chaîne de précorrespondance, le processus d'analyse utilise tour à tour chaque filtre d'analyse associé à cette précorrespondance pour localiser les informations qui y sont spécifiées. Le processus d'analyse renvoie la première correspondance positive établie.

Lorsque vous cliquez sur le bouton Ajouter un filtre d'analyse à l'étape de définition de la correspondance et d'analyse des événements de l'assistant d'analyse de message, vous démarrez l'Assistant de filtre de fichier d'analyse. Pour créer des filtres d'analyse efficaces, vous devez posséder une bonne connaissance de la syntaxe des expressions régulières.

Pour créer un filtre d'analyse

1. Ouvrez l'Assistant de filtre de fichier d'analyse et saisissez un nom de filtre et une description (facultative) sur la page Détails du filtre.
2. Cliquez sur Ajouter nouveau pour ajouter une valeur de champ statique que vous souhaitez voir apparaître dans tous les événements analysés par le filtre.

   Une ligne de champ statique apparaît, avec les cellules Nouveau champ et Nouvelle valeur.
3. Saisissez une entrée dans la cellule Nouveau champ, puis dans la cellule Nouvelle valeur. La fonction de saisie semi-automatique restreint les noms de champs CEG disponibles au fur et à mesure de la frappe dans la cellule Nouveau champ et vous présente un menu de choix.
4. Répétez les étapes 2 à 3 pour ajouter les valeurs de champs statiques nécessaires (facultatif).
5. Avancez jusqu'à l'étape Expression régulière.

   La fenêtre Test d'expression d'analyse s'ouvre ; elle affiche toutes les expressions régulières en cours. Juste en dessous de l'expression régulière se trouve le volet Evénement. Cette zone contient un ou plusieurs exemples d'événements si vous en avez précédemment chargés. L'assistant peut tester ces événements par rapport à l'expression régulière au fur et à mesure qu'elle est créée.
6. Cliquez sur Ajouter/Supprimer des jetons dans la bibliothèque pour afficher la liste des expressions régulières prédéfinies que vous pouvez ajouter afin de les utiliser dans le filtre en cours. Sélectionnez les jetons à ajouter, puis cliquez sur OK pour les ajouter à la liste Jetons d'analyse.

7. Cliquez sur Nouveau jeton d'expression régulière pour créer un jeton d'analyse et entrez sa syntaxe d'expression régulière dans le volet Détails du jeton (facultatif). Vous pouvez à présent créer des expressions personnalisées pour votre environnement. Vous pouvez ajouter un jeton personnalisé à votre bibliothèque locale en cliquant sur Ajouter le jeton sélectionné à la bibliothèque en haut du volet Jetons d'analyse.

   Remarque : Lorsque vous créez un nouveau jeton date/heure, sélectionnez la case Traiter comme valeur de date/heure pour entrer un format d'analyse de la valeur temporelle. Cette valeur n'influe pas sur le format d'affichage.

8. Ajoutez des instructions d'expression régulière pour le filtre dans le champ de saisie Expression régulière. Vous pouvez faire glisser et déposer les expressions depuis la liste Jetons d'analyse. Vous pouvez également saisir ou modifier l'expression directement dans le champ de saisie Expression régulière.

   Remarque : La sélection d'un jeton dans la liste Jetons d'analyse affiche sa syntaxe d'expression régulière dans le volet Détails du jeton. Vous pouvez afficher le mappage de jeton d'analyse d'une règle donnée afin de le répéter dans d'autres règles d'analyse.

9. Sélectionnez la case Paires de valeurs/noms dynamiques si vos événements cibles incluent des paires de clés que vous souhaitez afficher (facultatif). Pour plus d'informations, consultez la section "Analyse dynamique".

10. Si vous souhaitez utiliser l'analyse dynamique, entrez une expression d'analyse dynamique dans le champ de saisie des paires dynamiques (facultatif). Par exemple, entrez :

    (_PAIR_KEY_)=(_PAIR_VALUE_);

    Affiche toutes les paires séparées par un signe égal et espacées par un point-virgule. Vous pouvez entrer d'autres expressions pour rechercher les paires affichées dans d'autres formats. Pour plus d'informations, consultez la section "Analyse dynamique".

11. Prévisualisez la manière dont le fichier analyse les exemples d'événements à l'aide des volets Evénement et Evénement analysé. Pendant que vous modifiez l'expression régulière du filtre d'analyse, les portions analysées de l'exemple d'événement sont surlignées en bleu tandis que les paires analysées de manière dynamique apparaissent en vert. Vous pouvez vérifier l'efficacité de l'analyse.

12. Pour procéder à des tests supplémentaires, changez d'exemple d'événement à l'aide des flèches précédent et suivant situées sous le volet Evénement et qui vous permettent de vous déplacer entre les exemples d'événements disponibles (facultatif).

13. Cliquez sur Enregistrer et fermer lorsque vous êtes satisfait de l'expression régulière. Vous pouvez utiliser Réinitialiser pour revenir à l'expression régulière dans son état initial.

L'Assistant de filtre de fichier d'analyse se ferme et vous revenez à l'étape de définition de la correspondance et d'analyse des événements de l'Assistant de fichier d'analyse.

Informations complémentaires :

Analyse dynamique (page 565)
Jetons d'analyse (page 566)
Ajout d'un jeton personnalisé à la bibliothèque (page 570)

Analyse dynamique

L'analyse dynamique vous permet d'afficher plusieurs paires nom-valeur inchangées. Elle se distingue de l'analyse statique, qui extrait des valeurs et les affecte à des champs CEG ou à d'autres champs prédéfinis. L'analyse dynamique est particulièrement utile lorsque des applications ou des formats enregistrent des données d'événement par paires clés que vous souhaitez afficher sans changement, c'est-à-dire non analysées dans des noms CEG ou d'autres valeurs. Dans les cas où cette analyse peut être utilisée, ses performances sont meilleures que celles d'une analyse statique.

L'expression régulière permettant une analyse dynamique est composée de quatre éléments.

1. Un indicateur de clé de paire "(_PAIR_KEY_)".
2. Un indicateur de valeur de paire "(_PAIR_VALUE_)"
3. Un séparateur clé-valeur entre la valeur de paire et la valeur de clé
4. Un séparateur de paire entre l'expression complète et l'expression suivante

Les séparateurs que vous utilisez doivent correspondrent à la structure de la source d'événement que vous analysez. Si votre source sépare les événements par des virgules, votre expression régulière doit également utiliser des virgules.

Exemple

```
(_PAIR_KEY_)=(_PAIR_VALUE_);
```

Dans cet exemple, le séparateur clé-valeur est "=" et le séparateur de paires est ";".

Le fichier XMP, en utilisant cette expression après d'autres expressions régulières, peut rechercher et afficher toutes les paires de clé apparaissant dans les événements analysés.

Jetons d'analyse

Un jeton d'analyse est un modèle d'expression régulière que vous pouvez utiliser pour créer des filtres d'analyse. CA Enterprise Log Manager inclut une bibliothèque de jetons d'analyse contenant des jetons prédéfinis. Par exemple, le jeton _IP_ définit l'expression régulière qui analyse le format d'adresse IP typique. Si vous souhaitez qu'un filtre d'analyse extraie une adresse IP, vous pouvez insérer le jeton _IP_ dans le filtre au lieu de créer à chaque fois l'expression régulière complète.

Vous avez également la possibilité de créer vos propres jetons d'analyse personnalisés et de les ajouter à la bibliothèque locale ou de les exporter afin de les utiliser dans un autre environnement CA Enterprise Log Manager. Avant d'exporter un jeton personnalisé, vous devez l'ajouter à la bibliothèque. Vous pouvez aussi importer des jetons personnalisés depuis un autre environnement CA Enterprise Log Manager pour créer des jetons d'analyse dans un environnement de test, que vous transférez ensuite vers un environnement réel.

Informations complémentaires :

Jetons date/heure (page 567)
Ajout d'un jeton personnalisé à la bibliothèque (page 570)
Suppression d'un jeton d'analyse de la bibliothèque (page 571)
Importation de jetons d'analyse (page 572)
Exportation de jetons d'analyse (page 573)

Jetons date/heure

CA Enterprise Log Manager prend en charge diverses options de syntaxe pour les jetons d'analyse date/heure. Vous pouvez utiliser ces options, au format date/heure du fichier d'analyse, pour personnaliser l'horodatage.

Chaque jeton date/heure se compose d'au moins l'un des éléments ci-dessous.

- Un caractère standard (à l'exception de l'espace et du caractère de pourcentage "%") qui sera affiché tel que saisi, par exemple le caractère ":" pour séparer les heures des minutes apparaît tel quel.

  ou

- Une spécification de conversion. Chaque spécification de conversion se compose d'un caractère "%" suivi d'un caractère de conversion qui définit la donnée affichée : par exemple, %m permet d'afficher le mois.

CA Enterprise Log Manager prend en charge les spécifications de conversion énumérées ci-dessous.

%a ou %A

Affiche le nom du jour de la semaine local, en forme développée ou abrégée. Sous Windows, cette spécification est disponible uniquement en anglais américain.

%b ou %B ou %h

Affiche le nom du mois local, en forme développée ou abrégée. Sous Windows, cette spécification est disponible uniquement en anglais américain.

%c

Affiche la date et l'heure locales.

%C

Affiche les deux derniers chiffres du siècle (0 à 99).

%d ou %e

Affiche le jour du mois (1 à 31).

%D

Affiche la date au format américain : mois/jour/année. Cela revient à saisir %m/%d/%y.

Remarque : La syntaxe %d/%m/%y est utilisée en Europe. Le format de la norme ISO 8601 est %Y-%m-%d.

%H

Affiche l'heure au format 24 heures (0 à 23).

%I

Affiche l'heure au format 12 heures (1 à 12).

%j

Affiche le numéro du jour dans l'année (1 à 366).

%m

Affiche le numéro du mois (1 à 12).

%M

Affiche les minutes (0 à 59).

%n

Insère un espace arbitraire.

%p

Affiche l'équivalent local de AM ou PM, le cas échéant.

%r

Affiche l'heure au format 12 heures : Heures:Minutes:Secondes AM/PM. Cela revient à saisir %I:%M:%S %p. Si t_fmt_ampm est vide dans la section LC_TIME locale, le comportement est indéfini.

%R

Affiche l'heure au format 24 heures : Heures:Minutes. Cela revient à saisir %H:%M.

%S

Affiche les secondes (0 à 60 ; 60 peut se produire pour les secondes intercalaires).

%t

Affiche un espace arbitraire.

%T

Affiche l'heure au format 24 heures : Heures:Minutes:Secondes. Cela revient à saisir %H:%M:%S.

%U

Affiche le numéro de la semaine. Dimanche est considéré comme le premier jour de la semaine (0 à 53). Le premier dimanche de janvier correspond au premier jour de la semaine 1.

%w

Affiche le numéro du jour de la semaine (0 à 6), dimanche correspondant à 0.

%W

Affiche le numéro de la semaine, lundi étant considéré comme le premier jour de la semaine (0 à 53). Le premier lundi de janvier correspond au premier jour de la semaine 1.

%x

Affiche la date en utilisant le format de date local.

%X

Affiche l'heure en utilisant le format d'heure local.

%y

Affiche l'année du siècle en cours (0 à 99). Si aucun siècle n'est spécifié, les valeurs comprises entre 69 et 99 font référence aux années du vingtième siècle (1969 à 1999). Les valeurs comprises entre 00 et 68 font référence aux années du vingt-et-unième siècle (2000 à 2068).

%Y

Affiche l'année, y compris le siècle (par exemple, 1991).

%z

Affiche une spécification de fuseau horaire conforme à la norme RFC-822/ISO 8601. Cette spécification n'est pas disponible sous Windows.

Le format de jeton date/heure CA Enterprise Log Manager par défaut est le suivant.

%d/%b/%Y:%H:%M:%S %z

Ajout d'un jeton personnalisé à la bibliothèque

Vous pouvez ajouter des jetons d'analyse personnalisés à la bibliothèque de jetons afin de les mettre à disposition des autres utilisateurs. Par exemple, si vous créez un jeton personnalisé au cours du processus de création d'un fichier d'analyse de message et que vous estimez qu'il pourrait servir à d'autres analyses, vous pouvez l'ajouter à la bibliothèque afin de le réutiliser par la suite.

La procédure suivante décrit l'ajout de jetons au cours de la création de fichiers d'analyse ou de filtres.

Pour ajouter un jeton personnalisé à la bibliothèque

1. Ouvrez l'assistant d'analyse de message et avancez jusqu'à l'étape Correspondance et analyse.
2. Ouvrez l'assistant de filtre de fichier d'analyse et avancez jusqu'à l'étape Expression régulière.
3. Cliquez sur Nouveau jeton d'expression régulière pour créer un jeton d'analyse et entrez sa syntaxe d'expression régulière dans le volet Détails du jeton (facultatif).
4. Sélectionnez le nouveau jeton d'analyse, puis cliquez sur Ajouter le jeton sélectionné à la bibliothèque.

   Une boîte de dialogue de confirmation apparaît.
5. Cliquez sur Oui.
6. Cliquez sur Ajouter/Supprimer des jetons dans la bibliothèque pour afficher le nouveau jeton (facultatif).

   La boîte de dialogue de la bibliothèque de jetons d'analyse s'affiche. Les jetons personnalisés apparaissent en noir et les jetons prédéfinis en vert.

Suppression d'un jeton d'analyse de la bibliothèque

Vous pouvez supprimer les jetons personnalisés inutiles ou obsolètes de la bibliothèque de jetons. Vous ne pouvez pas supprimer les jetons prédéfinis.

Pour supprimer des jetons personnalisés de la bibliothèque

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche située en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Mappage et analyse.

   Les boutons d'intégration d'un produit apparaissent dans le volet Détails.

3. Cliquez sur Nouvelle règle d'analyse de message :  .

   L'Assistant de fichier d'analyse s'ouvre.

4. Avancez jusqu'à l'étape Correspondance et analyse.

5. Sélectionnez le filtre de précorrespondance qui vous intéresse et cliquez sur Modifier ou sur Ajouter un filtre d'analyse, au début de la liste Filtres d'analyse.

   L'Assistant de filtre de fichier d'analyse s'affiche.

6. Avancez jusqu'à l'étape Expression régulière.

7. Cliquez sur Ajouter/Supprimer des jetons dans la bibliothèque.

   La boîte de dialogue de la bibliothèque de jetons d'analyse s'affiche. Les jetons personnalisés apparaissent en noir et les jetons prédéfinis en vert.

8. Sélectionnez le ou les jetons personnalisés à supprimer, puis cliquez sur Supprimer le jeton sélectionné de la bibliothèque.

   Une boîte de dialogue de confirmation s'affiche.

9. Cliquez sur Oui, puis sur OK.

Importation de jetons d'analyse

Vous pouvez importer sur votre serveur actuel des jetons d'analyse personnalisés créés sur un autre serveur de gestion, par exemple d'un environnement de test à un environnement réel.

Pour importer des jetons d'analyse

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche située en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Mappage et analyse.

   Les boutons d'intégration d'un produit apparaissent dans le volet Détails.

3. Cliquez sur Nouvelle règle d'analyse de message :  .

   L'Assistant de fichier d'analyse s'ouvre.

4. Avancez jusqu'à l'étape Correspondance et analyse.

5. Sélectionnez le filtre de précorrespondance qui vous intéresse et cliquez sur Modifier ou sur Ajouter un filtre d'analyse, au début de la liste Filtres d'analyse.

   L'Assistant de filtre de fichier d'analyse s'affiche.

6. Avancez jusqu'à l'étape Expression régulière.

7. Cliquez sur Importer les jetons d'utilisateur en haut du volet Jetons d'analyse.

   La boîte de dialogue d'importation de fichier s'affiche.

8. Recherchez le fichier de jetons (.tok) à importer et cliquez sur OK.

   Une boîte de dialogue de confirmation s'affiche.

9. Cliquez sur Oui pour importer le fichier. Cette opération écrasera les autres jetons d'utilisateur de la bibliothèque.

Exportation de jetons d'analyse

Vous pouvez exporter vers un autre serveur des jetons d'analyse personnalisés créés sur le serveur de gestion actuel et figurant dans la bibliothèque de jetons. Vous pouvez par exemple transférer vos jetons personnalisés d'un environnement de test vers votre environnement réel.

Pour exporter des jetons d'analyse

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche située en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Mappage et analyse.

   Les boutons d'intégration d'un produit apparaissent dans le volet Détails.

3. Cliquez sur Nouvelle règle d'analyse de message :  .

   L'Assistant de fichier d'analyse s'ouvre.

4. Avancez jusqu'à l'étape Correspondance et analyse.

5. Sélectionnez le filtre de précorrespondance qui vous intéresse et cliquez sur Modifier ou sur Ajouter un filtre d'analyse, au début de la liste Filtres d'analyse.

   L'Assistant de filtre de fichier d'analyse s'affiche.

6. Avancez jusqu'à l'étape Expression régulière.

7. Cliquez sur Exporter les jetons d'utilisateur en haut du volet Jetons d'analyse.

   Une boîte de dialogue Emplacement de téléchargement s'affiche.

8. Choisissez l'emplacement où vous souhaitez enregistrer le fichier exporté, puis cliquez sur Enregistrer.

   Le fichier exporté est enregistré à l'emplacement de votre choix.

Analyse du fichier XMP

Vous pouvez utiliser l'utilitaire Analyse de message pour analyser votre fichier créé ou modifié et déterminer le degré d'efficacité du fichier d'analyse par rapport aux exemples d'événements. L'analyse vous permet d'apporter des modifications en vue d'améliorer l'efficacité du fichier avant de l'enregistrer.

L'utilitaire analyse un fichier XMP par rapport à l'ensemble d'exemples d'événements sélectionné à l'aide du processus suivant.

1. Localisation de tous les événements contenant les chaînes de précorrespondance définies dans le fichier XMP. L'utilitaire exécute une recherche distincte pour chaque chaîne de précorrespondance, afin de détecter tous les événements contenant cette chaîne.
2. Recherche du premier filtre d'analyse pour chacun des événements en précorrespondance pouvant analyser l'événement en jetons.

Pour analyser le fichier XMP

Ouvrez l'assistant d'analyse et avancez jusqu'à l'étape Analyse. L'assistant affiche le nombre de correspondances pour les chaînes de précorrespondance et les filtres. Plus vous obtenez de correspondances, plus le fichier XMP créé ou modifié sera efficace. Cela vous permet également de déterminer si une quantité significative d'informations n'a pas encore été analysée.

L'exécution de l'analyse XMP peut être plus longue si le fichier XMP et le nombre d'exemples d'événements sont tous deux volumineux. Elle n'excède généralement pas une minute. Vous pouvez annuler ce processus s'il est trop long et réanalyser ensuite un plus petit nombre d'événements.

Lorsque vous créez une nouvelle règle, elle est enregistrée en version 1.0. Si vous modifiez la règle ultérieurement, une copie distincte de la règle est stockée en tant que nouvelle version. Vous pouvez afficher des versions antérieures et les appliquer ou les copier comme bon vous semble.

Création d'un fichier de mappage de données

Vous pouvez utiliser l'Assistant de fichier de mappage pour créer et modifier des fichiers de mappage de données, qui convertissent les événements natifs en événements ajustés en mappant la chaîne de texte analysée ou les paires champ/valeur à des champs compatibles CEG. L'Assistant de fichier de mappage vous permet de créer et de modifier divers types de mappage pour y parvenir.

Le processus de création ou de modification d'un fichier de mappage de données se compose des étapes suivantes.

1. Ouverture de l'Assistant de fichier de mappage
2. Indication des détails de fichier
3. Localisation et ajout d'exemples d'événements à l'aide de fichiers d'analyse
4. Définition des mappages directs selon les besoins
5. Définition des mappages de fonctions selon les besoins

6. Définition des mappages conditionnels selon les besoins
7. Définition des mappages de blocs selon les besoins

   Remarque : Vous pouvez définir des mappages directs ou de fonctions à l'aide de mappages de blocs. Il s'agit d'une alternative à la définition de mappages des étapes 4 et 5.
8. Analyse et enregistrement du fichier de mappage de données terminé.

Lors de la création d'un fichier de mappage de données, vous devez considérer les priorités de mappage de données du fichier lui-même, ainsi que les différents types de mappage au sein du fichier. Le fichier de mappage de données terminé vérifie les informations d'événement dans l'ordre des écrans de type de mappage (étapes 4 à 7 de l'assistant). Si des types de mappage sont dupliqués, la dernière valeur trouvée par le fichier de mappage de données est celle qui est assignée.

Par exemple, si un fichier de mappage de données trouve un mappage direct pour une valeur d'événement natif, puis un autre mappage conditionnel pour la même valeur, l'événement ajusté utilise le résultat du mappage conditionnel.

Les mappages dupliqués *au sein* d'un type de mappage sont gérés différemment, selon leur type.

- Mappages directs et mappages de fonctions : le fichier de mappage de données utilise la dernière valeur correspondante trouvée. Si un mappage de fonctions dupliqué est trouvé, la dernière fonction est celle qui est appelée. Par exemple, vous pouvez définir un mappage dupliqué pour appeler une deuxième fonction si la première n'a pas été trouvée ou n'a pas fonctionné de la manière attendue.
- Mappages conditionnels et mappages de blocs : le fichier de mappage de données applique la première valeur trouvée et arrête la recherche. Pour améliorer les performances, il est recommandé de placer les conditions les plus courantes en premier dans le fichier pour ces deux types de mappage.

Vous trouverez plus d'informations sur les implications de l'ordre de mappage en matière de conception dans les procédures des différents types de mappage.

Informations complémentaires :

Ouverture de l'Assistant de fichier de mappage (page 576)
Définition de mappages de blocs (page 585)
Analyse de mappage (page 586)

Ouverture de l'Assistant de fichier de mappage

Pour créer un nouveau fichier de mappage de données ou modifier un fichier existant, vous devez ouvrir l'Assistant de fichier de mappage.

Pour ouvrir l'Assistant de fichier de mappage

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche située en regard du dossier Bibliothèque d'ajustement d'événement, afin de développer ce dossier, puis sélectionnez le dossier Mappage et analyse.

   Les boutons d'intégration d'un produit apparaissent dans le volet Détails.

3. Cliquez sur Nouveau fichier de mappage :  .

   L'Assistant de fichier de mappage s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires

Définition de mappage de fonctions de concaténation (page 582)
Définition de mappages de blocs (page 585)
Analyse de mappage (page 586)

Indication des détails de fichier

Fournissez les détails d'un nouveau fichier de mappage de données. Vous pouvez enregistrer un fichier d'abonnement en tant que fichier personnalisé sous un autre nom.

Pour fournir les détails du fichier de mappage

1. Ouvrez l'Assistant de fichier de mappage.
2. Entrez un nom pour le fichier de mappage de données. Le nom du fichier est obligatoire et ne peut pas contenir les caractères suivants : / \ : * ? " < > ^;'`,&{}[]. ou |.
3. Dans la liste déroulante Fichier d'analyse, sélectionnez le nom et la version du fichier d'analyse à utiliser pour analyser les exemples d'événements.

   Le champ du nom du journal est renseigné automatiquement avec le nom du fichier d'analyse que vous avez entré.
4. Saisissez une description (facultatif).
5. Dans la zone Informations de support, cliquez sur Ajouter un produit pour entrer le nom et les versions du produit à des fins de référence (facultatif).
6. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier de mappage. Sinon, l'étape sélectionnée s'affiche.

Indication d'exemples d'événements

Vous pouvez utiliser l'Assistant de fichier de mappage pour rechercher des exemples d'événements à utiliser pour l'analyse du fichier de mappage de données. Vous pouvez lancer une recherche dans le magasin de journaux d'événements ou fournir des exemples d'événements directement à partir d'un fichier journal. Les exemples d'événements servent de modèles qui permettent de tester la sortie de mappage lors de l'étape finale de l'assistant.

Pour fournir des exemples d'événements

1. Ouvrez l'Assistant de fichier de mappage et avancez jusqu'à l'étape Exemples d'événements.

   L'écran Exemples d'événements apparaît.

2. Sélectionnez le bouton d'option Magasin de journaux ou Fichier journal dans la zone Rechercher des exemples d'événement.
3. Si vous sélectionnez Magasin de journaux
   a. Sélectionnez le type de source d'exemples d'événements souhaité dans le menu déroulant Colonne d'analyse. Sélectionnez result_string pour les sources d'événement WMI ou raw_event pour les sources d'événement Syslog.
   b. Sélectionnez la requête à utiliser pour fournir des exemples d'événements à l'aide du Filtre de balise de requête et de la Liste de requêtes.

      La requête apparaît ; elle affiche les exemples d'événements.

      Remarque : Vous pouvez utiliser toute requête disponible ou personnalisée pour localiser des exemples d'événements. Si vous envisagez d'utiliser une requête personnalisée, nous vous recommandons de la créer et de la tester avant d'entamer le processus de conception de fichier de mappage de données.
4. Si vous sélectionnez Fichier journal
   a. Recherchez le fichier journal souhaité et cliquez sur Charger.

      Les événements du fichier journal apparaissent dans le volet Exemples d'événements.

      Remarque : L'assistant considère que chaque ligne du fichier est un événement. Les événements répartis sur plusieurs lignes ne sont pas pris en charge.
   b. Cliquez sur Extraire des champs dynamiques si votre exemple de fichier journal contient des valeurs de paires dynamiques à inclure dans l'exemple analysé.
5. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier de mappage. Sinon, l'étape sélectionnée s'affiche.

Informations complémentaires :

Analyse dynamique (page 565)

Définition de mappages directs

Les mappages directs définissent des correspondances 1-1 entre un événement natif et une seule valeur d'événement ajusté. Par conséquent, il est préférable d'utiliser des mappages directs uniquement pour les valeurs par défaut, ou des valeurs courantes qui varient rarement, telles que le champ ideal_model.

Un mappage peut être défini de différentes manières pour dériver une valeur d'événement ajusté.

Valeur de texte

Définit un texte spécifique pour un champ CEG spécifique. Cette valeur apparaît chaque fois qu'un événement approprié est mappé. Par exemple, si vous définissez le champ CEG ideal_model sur "Pare-feu", ce champ indique "Pare-feu" pour toutes les règles qui contiennent ce mappage.

Valeur de champ

Définit un champ d'événement brut dont le contenu est inclus pour un champ CEG ou un champ analysé spécifique. On distingue une valeur de champ d'une valeur de texte en la faisant précéder d'un symbole de dollar, $. Par exemple, si vous définissez le champ CEG event_logname sur "$Journal", tout événement mappé affiche le texte qui apparaît dans le champ Journal de l'événement natif.

Pour définir des mappages directs

1. Ouvrez l'Assistant de fichier de mappage, entrez un nom et sélectionnez un nom de journal pour le fichier de mappage, puis avancez jusqu'à l'étape Mappages directs.

   L'écran Mappages directs apparaît ; il affiche les mappages en cours ou par défaut. La colonne Nom indique le nom du champ CEG ou analysé. La colonne Valeur indique soit une valeur de texte, soit une valeur de champ.

   Remarque : Sélectionnez un fichier d'analyse à l'étape Fournissez des exemples d'événements pour afficher les valeurs du champ analysé.

2. Cliquez sur Ajouter un mappage direct pour ajouter une nouvelle entrée de mappage en bas du tableau, puis sélectionnez-la, ou bien sélectionnez un mappage direct existant à modifier.

   Les mappages directs pour le champ apparaissent le cas échéant dans la zone Détails du mappage.

3. Dans le menu déroulant Champ, sélectionnez un champ CEG ou un champ d'événement analysé (si disponible) à mapper. Au fur et à mesure de la frappe, la fonction de saisie semi-automatique propose les champs CEG disponibles.
4. Entrez une nouvelle valeur dans le champ de saisie Ajouter une valeur et cliquez sur l'option Ajouter un mappage direct qui se trouve en regard de ce champ. Faites précéder la valeur du symbole "$" pour indiquer qu'il s'agit d'une valeur de champ, et non d'une valeur de texte.

   La valeur apparaît dans la zone Champs sélectionnés.
5. Vous pouvez entrer plusieurs mappages directs pour un même champ ; utilisez les flèches haut et bas pour définir l'ordre dans lequel le fichier de mappage de données les considère (facultatif). L'événement ajusté affiche le dernier mappage direct localisé par le fichier de mappage de données.

   Remarque : L'ajout de plusieurs valeurs réduit les performances du mappage. Par conséquent, utilisez cette fonction avec modération.
6. Utilisez le contrôle de déplacement pour déplacer les valeurs inutiles dans la zone Champs disponibles afin qu'elles ne soient pas prises en compte dans le mappage en cours (facultatif).
7. Une fois tous les mappages directs souhaités ajoutés, cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer, ou cliquez sur Enregistrer et fermer.

Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier de mappage. Sinon, l'étape sélectionnée s'affiche.

Définition de mappages de fonctions

Les mappages de fonctions relient un champ CEG à une valeur à l'aide d'une fonction qui récupère ou définit les informations d'événement ajusté qui apparaissent dans l'événement ajusté. Tous les mappages de fonctions se composent d'un nom de champ CEG, d'une valeur de champ prédéfinie ou de classe, ainsi que de la fonction.

Par exemple, un mappage de fonctions peut concaténer une série de valeurs d'événement natif dans un même champ CEG à l'aide de la fonction de concaténation.

En cas de mappages de fonctions dupliqués, le fichier de mappage de données utilise la dernière fonction trouvée. Vous pouvez ainsi définir qu'un mappage dupliqué appelle une deuxième fonction si la première n'a pas été trouvée ou n'a pas fonctionné de la manière attendue.

Pour définir des mappages de fonctions

1. Ouvrez l'Assistant de fichier de mappage, entrez un nom et sélectionnez un nom de journal pour le fichier de mappage, puis avancez jusqu'à l'étape Mappages de fonctions.

   L'écran Mappages de fonctions apparaît ; il affiche les mappages en cours ou par défaut. La colonne Nom affiche un champ CEG ou analysé, la colonne Fonction affiche l'actuelle fonction de liaison et la colonne Valeur affiche une valeur de texte ou de champ.

   Remarque : Sélectionnez un fichier d'analyse à l'étape Fournissez les détails du fichier pour afficher les valeurs du champ analysé.

2. Cliquez sur Ajouter un mappage de fonctions pour ajouter une nouvelle entrée de mappage, ou sélectionnez un mappage existant à modifier.

   L'entrée de mappage apparaît dans le volet Détails du mappage.

3. Sélectionnez un champ CEG à mapper dans le menu déroulant Champ. Au fur et à mesure de la frappe, la fonction de saisie semi-automatique propose les champs CEG disponibles.

4. Sélectionnez une fonction à utiliser pour le mappage dans le menu déroulant Fonction.

   Remarque : La fonction de concaténation (concat) fonctionne différemment des autres étant donné que vous devez spécifier plusieurs valeurs cibles. Pour plus d'informations, consultez la section Définition de mappage de fonctions de concaténation.

5. Entrez une valeur cible pour le mappage dans le champ de saisie Ajouter une valeur et cliquez sur le bouton Ajouter une valeur situé en regard. Vous pouvez faire précéder la valeur du symbole "$" pour indiquer qu'il s'agit d'une valeur de champ, et non d'une valeur spécifique.

   La valeur apparaît dans la zone Champs sélectionnés.

6. Vous pouvez entrer plusieurs mappages pour un même champ ; utilisez les flèches haut et bas pour définir l'ordre dans lequel le fichier de mappage de données les considère (facultatif).

   Remarque : L'ajout de plusieurs valeurs réduit les performances du mappage. Par conséquent, utilisez les mappages de fonctions autonomes seulement si nécessaire.

7. Utilisez le contrôle de déplacement pour déplacer les valeurs inutiles dans la zone Champs disponibles afin qu'elles ne soient pas prises en compte dans le mappage en cours (facultatif).

8. Une fois tous les mappages de fonctions ajoutés, cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer, ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier de mappage. Sinon, l'étape sélectionnée s'affiche.

Définition de mappage de fonctions de concaténation

Un mappage de fonctions de concaténation est un type de mappage de fonctions. Contrairement aux autres mappages de fonctions, qui spécifient un champ ou une valeur cible, la fonction de concaténation spécifie plusieurs cibles de mappage, qu'elle concatène en un seul champ CEG.

Vous pouvez utiliser l'assistant de mappage de données pour créer des mappages de fonctions de concaténation. Etant donné que les mappages de concaténation sont différents des autres mappages de fonctions, la procédure à suivre pour les créer est quelque peu différente également.

Pour définir un mappage de fonctions de concaténation

1. Ouvrez l'Assistant de fichier de mappage, entrez un nom et sélectionnez un nom de journal pour le fichier de mappage, puis avancez jusqu'à l'étape Mappages de fonctions.

   L'écran Mappages de fonctions apparaît ; il affiche les mappages en cours ou par défaut. La colonne Nom affiche un champ CEG, la colonne Fonction affiche l'actuelle fonction de liaison et la colonne Valeur affiche une valeur de texte ou de champ.

2. Cliquez sur Ajouter un mappage de fonctions pour ajouter une nouvelle entrée de mappage.

   L'entrée de mappage apparaît dans le volet Détails du mappage.

3. Sélectionnez un champ CEG à mapper dans le menu déroulant Champ.

4. Sélectionnez la fonction de concaténation dans le menu déroulant Fonction.

   Les champs Format et Valeur apparaissent.

   Remarque : La valeur pour la fonction de concaténation s'affiche sous la forme {…} dans le volet Mappages de fonctions. Ce signe indique un ensemble de valeurs, plutôt qu'une seule valeur.

5. Entrez un spécificateur dans le champ Format pour contrôler la position des champs cibles (facultatif). Le spécificateur de format, %s, indique une position de champ. Toutes les valeurs autres que %s sont considérées comme des données de support statiques devant être incluses dans le champ de collecteur du tableau final. Par exemple, pour séparer deux champs cibles par un signe deux-points, saisissez "%s:%s" dans le champ Format.

6. Cliquez sur Ajouter une valeur concaténée dans la zone Valeurs concaténées pour ajouter une paire entrée/valeur cible.

7. Entrez une valeur dans le champ de saisie Ajouter une valeur et cliquez sur Ajouter une valeur.

   La valeur apparaît dans la zone Champs sélectionnés.

8. Répétez les étapes 6 et 7 pour ajouter des valeurs supplémentaires à concaténer. Vous devez ajouter au moins deux valeurs cibles.

9. Une fois tous les mappages de concaténation souhaités ajoutés, cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer, ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier de mappage. Sinon, l'étape choisie apparaît.

Définition de mappages conditionnels

Les mappages conditionnels relient un champ CEG à différents résultats possibles, ce qui vous permet de définir des valeurs conditionnelles et par défaut pour un champ donné. Vous pouvez par exemple utiliser des mappages conditionnels pour mapper des valeurs de réussite ou d'échec, ou pour identifier les sources d'événement par nom ou par groupe.

Les mappages conditionnels assignent une valeur par défaut et une ou plusieurs valeurs conditionnelles à un champ CEG donné. Vous pouvez définir des critères pour chaque valeur conditionnelle. Si un événement remplit ces critères, la valeur conditionnelle appropriée est assignée au champ choisi. Sinon, le champ d'événement ajusté affiche la valeur par défaut.

En présence de mappages conditionnels dupliqués, le fichier de mappage de données utilise le premier mappage trouvé, sans tenir compte des suivants. Pour améliorer les performances, placez les conditions les plus courantes en premier.

Remarque : Le mappage conditionnel autonome est plus lent que le mappage de blocs. Nous vous recommandons par conséquent de ne l'utiliser que lorsque cela s'avère nécessaire.

Pour définir des mappages conditionnels

1. Ouvrez l'Assistant de fichier de mappage, entrez un nom et sélectionnez un nom de journal pour le fichier de mappage, puis avancez jusqu'à l'étape Mappages conditionnels.

   L'écran Mappages conditionnels apparaît ; il affiche tous les mappages par défaut en cours. La colonne Champ affiche le nom du champ CEG ou analysé et la colonne Valeur affiche l'actuelle valeur par défaut.

   Remarque : Sélectionnez un fichier d'analyse à l'étape Fournissez les détails du fichier pour afficher les valeurs du champ analysé.

2. Cliquez sur Ajouter un mappage conditionnel dans la liste Mappages de champs conditionnels et sélectionnez la nouvelle ligne.

   Le volet Détails du mappage apparaît, affichant la liste déroulante Champ et le contrôle de déplacement Valeur.

3. Dans le menu Champ, sélectionnez le champ CEG que vous souhaitez mapper. Au fur et à mesure de la frappe, la fonction de saisie semi-automatique propose les champs CEG disponibles.

4. Entrez le mappage par défaut souhaité dans le champ de saisie Ajouter une valeur et cliquez sur Ajouter une valeur pour l'afficher dans le volet Champs sélectionnés. Vous pouvez supprimer les valeurs indésirables en les déplaçant dans le volet Champs disponibles.

5. Cliquez sur Ajouter une valeur conditionnelle dans la liste Valeurs conditionnelles.

   Une nouvelle valeur apparaît.

6. Sélectionnez le texte Nouvelle valeur pour le mettre en surbrillance et changer le nom.

   Le nouveau nom apparaît dans la liste et la boîte de dialogue Filtres s'affiche dans le volet Détails.

7. Créez un filtre pour définir la valeur conditionnelle. Vous pouvez par exemple créer un ou plusieurs filtres pour lier le champ event_source_address à des adresses IP, de manière à identifier les sources d'événement avec un groupe géographique ou tout autre groupe stratégique.

8. Une fois tous les mappages conditionnels ajoutés, cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer, ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier de mappage. Sinon, l'étape sélectionnée s'affiche.

Définition de mappages de blocs

Les mappages de blocs relient une condition sélectionnée à une série de mappages, vous permettant de créer une cascade de mappages déclenchés par cette condition. Un mappage de blocs peut utiliser toute combinaison de mappages directs ou de fonctions. Les deux types de mappage de blocs interne fonctionnent exactement de la même manière que des mappages autonomes.

Vous pouvez créer autant de blocs que vous le souhaitez pour un même fichier de mappage. Chacun inclut un nom et une condition.

En présence de mappages dupliqués dans un bloc, le fichier de mappage de données utilise le premier mappage trouvé, sans tenir compte des suivants. Pour améliorer les performances, il est recommandé de placer les conditions les plus courantes en premier.

Pour définir des mappages de blocs

1. Ouvrez l'Assistant de fichier de mappage, entrez un nom et sélectionnez un nom de journal pour le fichier de mappage, puis avancez jusqu'à l'étape Mappages de blocs.

   L'écran Mappages de blocs apparaît ; il affiche tous les mappages de blocs actuels.

2. Cliquez sur Ajouter un mappage de blocs dans le volet Mappages de blocs.

   Un nouveau bloc apparaît dans la liste Mappages de blocs.

3. Sélectionnez le texte Nouveau bloc.

   Le volet Définition de bloc s'ouvre sur l'étape 1. Définissez une condition.

4. Entrez un nom de bloc et créez un filtre pour définir la condition pour ce bloc. Vous pouvez par exemple définir que event_result doit être égal à "S", ce qui appelle les mappages de blocs lorsqu'une opération réussie (Success) est détectée pour le processus d'événement.

5. Cliquez sur la barre de l'étape 2 et entrez tous les mappages directs souhaités en suivant la même procédure qu'à l'étape correspondante d'un mappage autonome.

6. Cliquez sur la barre de l'étape 3 et entrez tous les mappages de fonctions souhaités en suivant la même procédure qu'à l'étape correspondante d'un mappage autonome.

7. Une fois tous les mappages de blocs ajoutés, cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer, ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouveau fichier apparaît dans le dossier Utilisateur de fichier de mappage. Sinon, l'étape choisie apparaît.

Informations complémentaires :

Utilisation des filtres avancés (page 301)

Analyse de mappage

Vous pouvez utiliser l'assistant de mappage pour analyser un fichier de mappage de données, ce qui vous permet de le tester et d'y apporter les modifications nécessaires afin d'accroître son efficacité. Les exemples d'événements sont testés par rapport au fichier de mappage de données et les résultats sont ensuite validés par rapport à la CEG.

Pour réaliser une analyse de mappage, cliquez sur l'étape Analyse de mappage de l'Assistant de fichier de mappage. L'assistant affiche un tableau contenant les résultats d'analyse des exemples d'événements que vous avez entrés à l'étape Exemples d'événements.

Le fichier de mappage de données finalisé enregistre vos mappages et considère les informations d'événement dans l'ordre des écrans de type de mappage (étapes 4 à 7 de l'assistant). Si des mappages sont dupliqués, la dernière valeur trouvée par le fichier de mappage de données est celle qui est assignée. Par exemple, si un fichier de mappage de données trouve un mappage direct pour une valeur d'événement natif, puis un autre mappage conditionnel pour la même valeur, l'événement ajusté affiche le résultat du mappage conditionnel. Vous trouverez plus d'informations sur les implications de l'ordre de mappage en matière de conception dans les procédures des différents types de mappage.

Lorsque vous créez une nouvelle règle, elle est enregistrée en version 1.0. Si vous modifiez la règle ultérieurement, une copie distincte de la règle est stockée en tant que nouvelle version. Vous pouvez afficher des versions antérieures et les appliquer ou les copier comme bon vous semble.

Tâches des règles de transfert d'événement

Les règles de transfert d'événement vous permettent de sélectionner les événements CA Enterprise Log Manager à transférer vers des écouteurs distants appartenant à des applications ou des systèmes extérieurs. Vous pouvez utiliser les règles de transfert pour identifier les événements à transférer, définir le moment de leur transfert et contrôler leur méthode de réception. Lorsqu'un événement entrant satisfait aux critères d'un filtre de la règle de transfert, CA Enterprise Log Manager crée une copie de l'événement, puis le transfère. L'événement reste enregistré dans le magasin de journaux d'événements.

Les tâches des règles de transfert d'événement sont effectuées depuis la zone Collecte de journaux de l'interface CA Enterprise Log Manager. Vous pouvez créer, modifier et supprimer des règles de transfert d'événement. Vous avez aussi la possibilité d'en importer et d'en exporter.

Informations complémentaires :

Création de règles de transfert d'événement (page 587)
Modification d'une règle de transfert (page 595)
Importation d'une règle de transfert (page 597)
Exportation d'une règle de transfert (page 598)

Création de règles de transfert d'événement

Vous pouvez utiliser des règles de transfert d'événement pour envoyer des événements CA Enterprise Log Manager à des applications extérieures. Vous pouvez par exemple envoyer des événements à CA NSM en utilisant Syslog. Les règles de transfert d'événement vous permettent de définir des critères pour les événements à transférer, ainsi qu'un ou plusieurs destinataires.

Le processus de création de règles de transfert d'événement à l'aide de l'Assistant de règle de transfert se compose des étapes suivantes.

1. Ouverture de l'Assistant de règle de transfert
2. Définition d'un nom et d'une description facultative pour la règle
3. Création de filtres simples et avancés pour identifier les événements à transférer
4. Définition des attributs de la règle, notamment de la destination du transfert et des champs CEG à inclure dans l'événement transféré

Informations complémentaires :

Ouverture de l'Assistant de règle de transfert (page 588)
Attribution d'un nom à une règle de transfert (page 589)
Création d'un filtre d'événement simple (page 301)
Création d'un filtre d'événement avancé (page 303)
Utilisation des filtres avancés (page 535)
Définition des attributs d'une règle de transfert (page 593)

Ouverture de l'Assistant de règle de transfert

Pour créer ou modifier une règle de transfert, ouvrez l'Assistant de règle de transfert.

Pour ouvrir l'Assistant de règle de transfert

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Règles de transfert.

   Les boutons de règle de transfert apparaissent dans le volet Détails.

3. Cliquez sur Nouvelle règle de transfert : 

   L'Assistant de règle de transfert apparaît.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier de règle sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier de règle et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Attribution d'un nom à une règle de transfert

Toute règle de transfert doit être nommée. Vous pouvez également saisir une description pour référence.

Pour nommer une règle de transfert

1. Ouvrez l'Assistant de règle de transfert.
2. Attribuez un nom à la règle. Le nom est obligatoire et ne peut pas contenir les caractères suivants : / \ : * ? < >;'`,&{}[]. ou |.
3. Entrez une description de la règle pour référence (facultatif).
4. Avancez jusqu'à l'étape Filtrage.

Création d'un filtre d'événement simple

Les filtres simples permettent de définir les paramètres de recherche pour les champs CEG communs. Par exemple, vous pouvez définir le champ Modèle idéal sur Gestion du contenu afin d'identifier tous les événements comportant cette valeur dans le champ CEG Modèle idéal. Plusieurs fonctions utilisent les filtres simples, notamment les requêtes, les règles de suppression et de récapitulation, ainsi que les règles de transfert d'événement.

Pour créer un filtre simple :

1. Cochez la case en regard du champ Modèle idéal ou de tout autre champ Evénement que vous voulez définir, puis sélectionnez une valeur dans la liste déroulante ou saisissez la valeur de votre choix dans le champ de saisie de texte.
2. Lorsque vous créez un filtre de requête, cochez la case en regard de l'un des champs Source, Destination ou Agent, puis saisissez la valeur de votre choix dans le champ de saisie de texte (facultatif).
3. Répétez les étapes 1 à 2 pour ajouter d'autres filtres simples.
4. Cliquez sur Enregistrer après avoir ajouté tous les filtres de votre choix.

Informations complémentaires :

Utilisation des filtres avancés (page 301)
Création d'un filtre d'événement avancé (page 303)

Utilisation des filtres avancés

Vous pouvez utiliser des filtres avancés en langage SQL pour qualifier une fonction qui interroge le magasin de journaux d'événements, y compris pour limiter des requêtes ou personnaliser des filtres rapides. L'interface Filtres avancés vous aide à créer la syntaxe de filtre appropriée grâce à un formulaire de saisie des colonnes logiques, opérateurs et valeurs, selon vos besoins de filtrage.

Remarque : Cette section contient une brève présentation des termes SQL utilisés dans les filtres avancés. Pour utiliser les filtres avancés au maximum de leur potentiel, vous devez posséder une connaissance approfondie de la grammaire SQL et de la grammaire commune aux événements.

Les termes SQL suivants permettent d'associer plusieurs instructions de filtre;

And

Affiche les informations de l'événement si *tous* les termes ajoutés sont vrais.

Or

Affiche les informations de l'événement si *l'un* des termes ajoutés est vrai.

Having

Restreint les termes de l'instruction SQL principale en ajoutant une instruction de qualification. Par exemple, vous pouvez définir un filtre avancé pour les événements issus d'hôtes spécifiés et ajouter une instruction "having" afin de limiter les résultats aux événements d'un niveau de sévérité défini.

Les opérateurs SQL suivants sont utilisés par les filtres avancés pour créer les conditions de base.

Opérateurs relationnels

Inclut les informations de l'événement si la colonne porte la relation appropriée à la valeur saisie. Les opérateurs relationnels suivants sont disponibles.

- Egal à
- Différent de
- Inférieur à
- Supérieur à
- Inférieur ou égal à
- Supérieur ou égal à

Par exemple, l'utilisation de *Supérieur à* inclut les informations de l'événement à partir de la colonne choisie si sa valeur est supérieure à la valeur définie.

Comme

Inclut les informations de l'événement si la colonne contient le modèle que vous avez saisi à l'aide du signe %. Par exemple, L% renvoie toutes les valeurs commençant par L, %L% renvoie toutes les valeurs contenant L comme valeur mais pas comme première ou dernière lettre.

Distinct de

Inclut les informations de l'événement si la colonne ne contient pas le modèle spécifié.

Dans l'ensemble

Inclut les informations de l'événement si la colonne contient au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Hors ensemble

Inclut les informations de l'événement si la colonne ne contient pas au moins une valeur de l'ensemble délimité par des guillemets que vous avez saisi. Les différentes valeurs au sein de l'ensemble doivent être séparées par des virgules.

Correspondance

Inclut toute information d'événement qui correspond au moins à un des caractères que vous avez saisis, ce qui vous permet de rechercher des mots clés.

A clés

Inclut toute information d'événement définie comme une valeur clé pendant la configuration du serveur de rapports. Vous pouvez utiliser les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Sans clé

Inclut toute information d'événement non définie comme une valeur clé pendant la configuration du serveur de rapports. Vous pouvez utiliser les valeurs clés pour définir la pertinence par rapport à l'entreprise ou d'autres groupes organisationnels.

Création d'un filtre d'événement avancé

Les filtres avancés sont utilisés par de nombreuses fonctionnalités, dont la création d'une requête, la planification des rapports et les filtres locaux et globaux.

Pour créer un filtre avancé

1. Cliquez sur Nouveau filtre d'événement.

   La première ligne du tableau du filtre d'événement devient active et les colonnes Logique et Opérateur sont respectivement renseignées à l'aide des valeurs par défaut "Et" et "Egal à".

2. Cliquez sur la cellule Logique et modifiez la valeur logique si besoin (facultatif).
3. Cliquez sur la cellule Colonne et sélectionnez la colonne d'informations de l'événement souhaitée dans le menu déroulant.
4. Cliquez sur la cellule Opérateur et sélectionnez l'opérateur souhaité dans le menu déroulant.
5. Cliquez sur la cellule Valeur et saisissez la valeur souhaitée.
6. Cliquez sur les cellules des parenthèses d'ouverture et de fermeture et saisissez le nombre de parenthèses requis (facultatif).
7. Répétez les étapes 1 à 6 selon vos besoins pour ajouter des instructions de filtre supplémentaires (facultatif).
8. Cliquez sur Enregistrer une fois que vous avez saisi toutes les instructions de filtre souhaitées.

Informations complémentaires :

Utilisation des filtres avancés (page 301)
Création d'une requête (page 295)
Planification d'un job de rapport (page 508)

Définition des attributs d'une règle de transfert

Vous devez définir des attributs pour la règle de transfert créée, notamment les points de sortie du transfert, les champs CEG inclus dans l'événement transféré et les paramètres de destination.

Pour définir les attributs d'une règle

1. Ouvrez l'Assistant de règle de transfert et avancez jusqu'à l'étape Attributs de stratégie.
2. Définissez les actions de la règle de transfert dans la zone Actions.
   a. Sélectionnez une fonctionnalité et une sévérité Syslog dans les listes déroulantes correspondantes. Tous les événements transmis suite à l'application de la règle contiennent les attributs Syslog que vous avez définis.
3. Spécifiez les informations sur la transmission d'événements CA Enterprise Log Manager dans la zone Informations générales.
   a. Indiquez si vous voulez envoyer les événements identifiés par la règle avant ou après la suppression et la récapitulation.
   – Si vous décidez de les envoyer avant, tous les événements entrants sont vérifiés par rapport aux filtres de la règle de transfert.
   – Si vous décidez de les envoyer après, seuls les événements ajustés sont vérifiés par rapport aux filtres de la règle de transfert. Les événements supprimés ne sont pas transférés et les événements récapitulés sont transférés uniquement sous leur forme récapitulée, pas sous leur forme précédente.

   Remarque : Si vous choisissez avant, les performances s'en trouvent fortement dégradées, car les événements ne sont pas ajustés.

   a. Sélectionnez les champs CEG à afficher dans l'événement transmis. Si vous ne choisissez aucun champ CEG, seule la valeur de l'événement brut est envoyée. Si vous sélectionnez un champ CEG, *quel qu'il soit*, sélectionnez également raw_event pour transférer l'événement brut.
4. Définissez la destination de transfert dans la zone Destination.
   a. Cliquez sur Ajouter une destination pour créer une ligne de destination.
   b. Cliquez sur le texte de la colonne Hôte pour ajouter le nom d'hôte ou l'adresse IP de la destination. Les adresses IP peuvent être au format IPv4 ou IPv6.
   c. Cliquez sur la cellule de la colonne Port pour ajouter le numéro du port d'écoute de l'application cible.
   d. Cliquez sur le texte de la colonne Protocole pour sélectionner le protocole (TCP ou UDP) à utiliser pour la transmission.
   e. Répétez les étapes a à d pour ajouter d'autres destinations.

5. Cliquez sur Enregistrer ou sur Enregistrer et fermer.

   La nouvelle règle apparaît dans le sous-dossier Utilisateur du dossier Règles de transfert.

A propos des événements Syslog transférés

La taille maximum du paquet syslog (y compris les champs PRI, Header, Tag et Content) est de 1 024 octets. Il se peut donc que l'événement expédié ne puisse pas inclure toutes les paires nom-valeur CEG que l'utilisateur a spécifiées.

Quand cela est nécessaire, CA Enterprise Log Manager tronque la valeur du message pour que sa longueur reste inférieure à 1024 octets. Si la règle de transfert indique les champs CEG à inclure dans l'événement syslog généré, alors le champ Content de celui-ci contiendra les paires nom-valeur CEG spécifiées.

Les paires nom-valeur ont le format *nom_du champ_CEG*: *valeur_du champ* défini à partir de l'événement qui correspond à la règle de filtre simple. La chaîne "null" désigne une valeur de champ CEG nulle. Ces champs CEG sont dans l'ordre spécifié dans la règle de transfert.

L'ordre des champs CEG spécifié dans la règle de transfert est important. CA Enterprise Log Manager peut tronquer la portion de valeur spécifiée, mais il ne tronquera pas les noms des champs CEG. Si CA Enterprise Log Manager ne peut pas accepter le prochain nom du champ CEG et les deux points, ainsi qu'au moins un octet de la valeur associée, alors il complètera le champ du contenu syslog par la précédente paire nom-valeur CEG.

Modification d'une règle de transfert

Vous pouvez modifier une règle de transfert.

Pour modifier une règle de transfert

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Règles de transfert d'événement.

   Les boutons de transfert d'événements apparaissent dans le volet Détails.

3. Cliquez sur le dossier contenant la règle à modifier.

4. Sélectionnez la règle à modifier, puis cliquez sur l'icône Modifier une règle de transfert.

   L'Assistant de règle de transfert apparaît et affiche la règle sélectionnée.

5. Modifiez la règle tel que requis, puis cliquez sur Enregistrer et fermer.

   La règle apparaît dans la liste appropriée comme une nouvelle version de la règle modifiée.

Suppression d'une règle de transfert

Vous pouvez supprimer une règle de transfert inutile.

Pour supprimer une règle de transfert

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Règles de transfert d'événement.

   Les boutons de transfert d'événements apparaissent dans le volet Détails.

3. Cliquez sur le dossier contenant la règle à supprimer.

4. Sélectionnez la règle à supprimer, puis cliquez sur l'icône Supprimer la règle de transfert. La version actuelle est sélectionnée par défaut. Vous pouvez sélectionner une version à supprimer plus ancienne dans la liste déroulante Version du volet Détails.

   Une boîte de dialogue de confirmation s'affiche.

5. Cliquez sur Oui.

   La règle supprimée disparaît de la liste appropriée.

Importation d'une règle de transfert

Vous pouvez importer une règle de transfert. Cette opération vous permet de déplacer des règles d'un environnement à un autre. Vous pouvez ainsi importer des règles créées dans un environnement de test dans votre environnement réel.

Pour importer une règle de transfert

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Règles de transfert d'événement.

   Les boutons de règle de transfert apparaissent dans le volet Détails.

3. Cliquez sur Importer une règle de transfert.

   La boîte de dialogue d'importation de fichier s'affiche.

4. Recherchez la règle à importer, puis cliquez sur OK.

   L'Assistant de règle de transfert apparaît et affiche les détails de la règle que vous avez sélectionnée.

5. Modifiez la règle tel que requis, puis cliquez sur Enregistrer et fermer. Si la règle importée partage le même nom qu'une règle déjà présente dans votre base de données de gestion, vous êtes invité à changer de nom.

La règle importée apparaît dans le dossier utilisateur Règles de transfert d'événement.

Exportation d'une règle de transfert

Vous pouvez exporter une règle de transfert. Cette opération vous permet de déplacer des règles d'un environnement à un autre. Vous pouvez ainsi exporter des règles créées dans un environnement de test vers votre environnement réel.

Pour exporter une règle de transfert

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Règles de transfert d'événement.

   Les boutons de règle de transfert apparaissent dans le volet Détails.

3. Cliquez sur le dossier Règles de transfert d'événement contenant le fichier à exporter.

   Le dossier se développe et vous pouvez consulter les différents fichiers qu'il contient.

4. Sélectionnez la règle à exporter, puis cliquez sur Exporter une règle de transfert. La version actuelle est sélectionnée par défaut. Vous pouvez sélectionner une version à exporter plus ancienne dans la liste déroulante Version du volet Détails.

   Une boîte de dialogue vous permettant de sélectionner l'emplacement d'exportation s'ouvre.

5. Saisissez un chemin ou naviguez jusqu'à l'emplacement où vous souhaitez stocker la règle exportée, puis cliquez sur Enregistrer.

   Une boîte de dialogue vous confirmant l'exportation apparaît.

6. Cliquez sur OK.

   La règle est exportée.

   Remarque : Lorsque vous examinez la règle exportée, les valeurs de Fonctionnalité et Sévérité s'affichent uniquement sous forme numérique. Vous pouvez utiliser l'interface de l'assistant pour déterminer les descriptions associées à ces valeurs.

Chapitre 14 : Intégrations et connecteurs

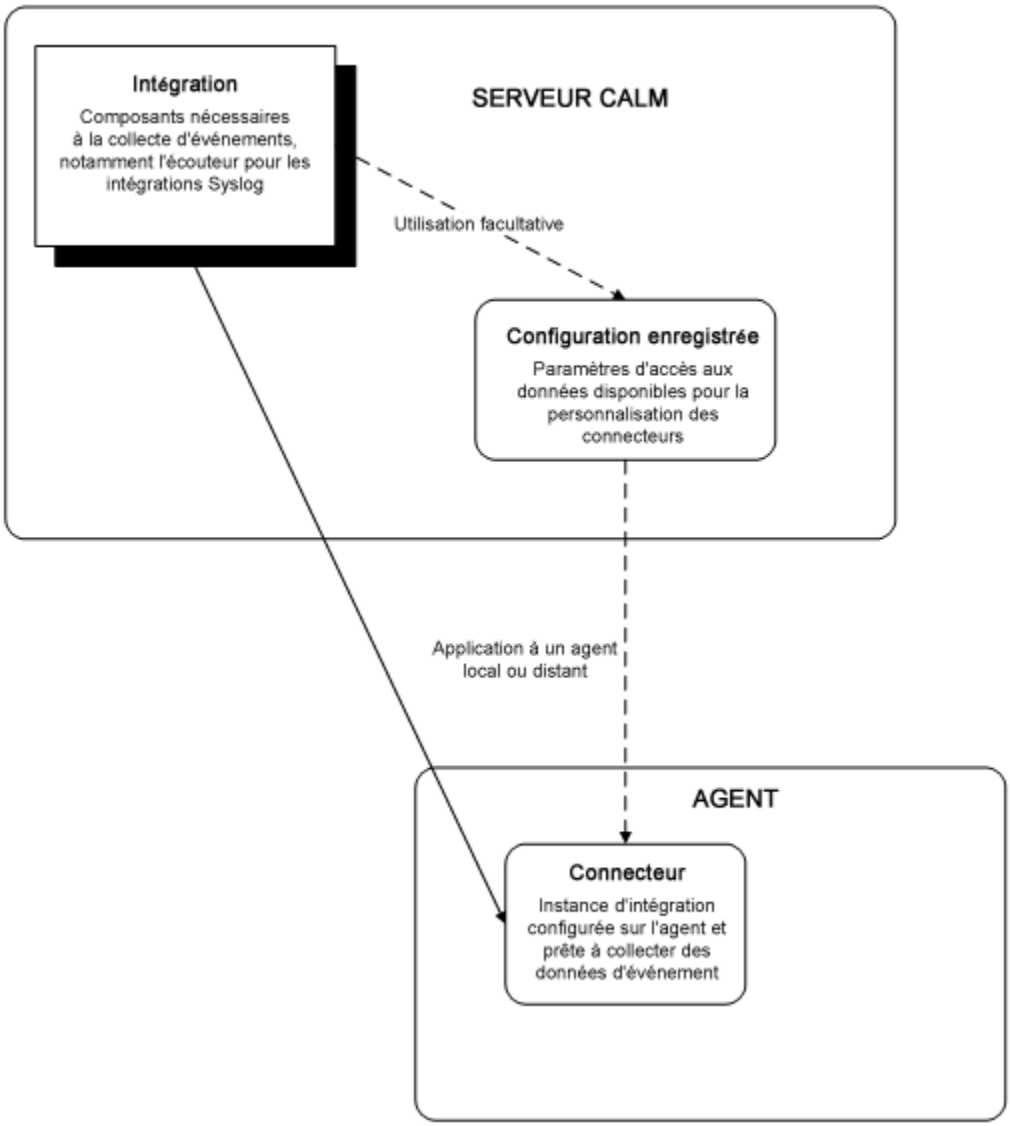
Ce chapitre traite des sujets suivants :

Tâches liées aux intégrations et connecteurs

Une intégration est un modèle pour les connecteurs. Elle comprend tous les composants nécessaires pour collecter des informations d'événements à partir d'un type donné de source : un détecteur de journaux, des fichiers XMP et de mappage de données, ainsi que des règles de suppression facultatives. Les intégrations sont fournies par CA. Les utilisateurs peuvent également créer leurs propres intégrations.

Vous pouvez créer une intégration personnalisée ou modifier la copie d'une intégration prédéfinie. Vous pouvez également créer vos propres fichiers XMP ou de mappage de données à utiliser dans des intégrations personnalisées, ainsi que dans des intégrations enregistrées, contenant des informations d'accès à des données spécifiques.

Après avoir analysé un événement et créé l'intégration requise, vous pouvez créer un connecteur, à l'aide des configurations enregistrées, et l'appliquer à un agent, comme indiqué sur l'illustration ci-dessous.



Informations complémentaires

Création d'une nouvelle version d'intégration (page 632)
Suppression d'une intégration (page 633)
Exportation et importation de définitions d'intégration (page 633)
A propos des configurations enregistrées (page 639)
Affichage d'un connecteur (page 638)
Modification d'un connecteur (page 639)

Création d'une intégration

Vous pouvez utiliser l'Assistant d'intégration pour créer ou modifier des intégrations, qui servent de modèles pour les connecteurs configurés qui rassemblent ou reçoivent les événements de votre environnement.

Vous pouvez créer des intégrations de plusieurs types, y compris des intégrations WMI et ODBC, qui réunissent activement les événements d'un type précis. Vous pouvez également créer des intégrations Syslog, qui reçoivent les événements de manière passive. Les intégrations Syslog peuvent recevoir des événements de plusieurs sources. Par conséquent, le processus de création d'une intégration Syslog et d'un connecteur est légèrement différent.

Pour tirer pleinement profit de cette fonction avancée, il est nécessaire de posséder une connaissance approfondie des sources d'événement de votre environnement et de leurs types de communication. Vous devez également avoir une excellente compréhension de la syntaxe d'expression régulière, de la grammaire commune aux événements (CEG), des fichiers de mappage de données et XMP, ainsi que de la manière dont ils analysent les événements.

La création d'une intégration inclut les étapes suivantes.

1. Ouverture de l'Assistant d'intégration
2. Ajout de composants d'intégration
3. Sélection des règles de suppression
4. Sélection des règles de récapitulation
5. Définition des configurations par défaut Cette étape ne s'applique pas aux intégrations Syslog.

Vous pouvez également créer une intégration utilisateur personnalisée en copiant une intégration d'abonnement.

Informations complémentaires :

Ouverture de l'Assistant d'intégration (page 602)
Ajout de composants d'intégration (page 603)
Application de règles de suppression et de récapitulation (page 604)
Définition des configurations par défaut (page 605)

Ouverture de l'Assistant d'intégration

Pour créer une nouvelle intégration ou modifier une intégration existante, ouvrez l'Assistant d'intégration.

Pour ouvrir l'Assistant d'intégration

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Intégrations.

   Les boutons Intégration s'affichent dans le volet Détails.

3. Cliquez sur Nouvelle intégration :  .

   L'Assistant d'intégration s'affiche.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires

Ajout de composants d'intégration (page 603)

Ajout de composants d'intégration

Lorsque vous créez une intégration, vous définissez des détails clés de celle-ci, notamment les détecteurs de journaux, les fichiers XMP et les fichiers de mappage de données utilisés pour collecter les événements.

Pour ajouter des composants d'intégration

1. Ouvrez l'Assistant d'intégration.
2. Attribuez un nom à la nouvelle intégration.
3. Sélectionnez les composants d'intégration requis ci-dessous dans les listes déroulantes.

   Détecteur

   Définit le détecteur de journaux utilisé par l'intégration pour lire les événements issus de la source de journaux.

   Aide à la configuration

   Celle-ci définit le fichier binaire de l'aide que l'intégration utilise pour se connecter au magasin de journaux sélectionné. La plupart des intégrations ne nécessitent pas d'aide à la configuration.

   Plate-forme

   Fait référence au système d'exploitation sur lequel peut s'exécuter l'agent d'intégration, et *non* au système d'exploitation de l'application que l'intégration est conçue pour surveiller. L'assistant sélectionne automatiquement le système d'exploitation en fonction des paramètres des détecteurs et de l'aide à la configuration.
4. Saisissez une description pour l'intégration.
5. A l'aide des contrôles de déplacement, sélectionnez les fichiers XMP et de mappage de données que l'intégration doit utiliser pour ajuster les événements.
6. Le cas échéant, dans le champ de saisie Champs cibles, saisissez le nom du champ natif contenant les informations d'événements bruts que l'intégration doit analyser. Certains types d'événements contiennent leurs informations d'événements bruts dans un champ particulier, ce qui implique que l'intégration soit ciblée sur ce champ. Par exemple, pour les événements de journaux d'événements NT, ce champ est appelé "Message".
7. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape choisie s'affiche.

Informations complémentaires :

Ouverture de l'Assistant d'intégration (page 602)
Mise à jour des configurations de plusieurs connecteurs (page 647)

Application de règles de suppression et de récapitulation

Vous pouvez appliquer des règles de suppression et de récapitulation à une intégration afin de rationaliser l'ajustement d'événement. Lorsque l'intégration est configurée en tant que connecteur, les règles de suppression et de récapitulation sont appliquées avant d'être envoyées au magasin de journaux d'événements. Ce contrôle de suppression et de récapitulation vient s'ajouter au contrôle de suppression et de récapitulation réalisé au niveau du magasin de journaux d'événements.

Par exemple, vous pouvez appliquer une règle de suppression afin que les événements Windows indésirables ne soient pas envoyés à un agent WMI. Le trafic réseau est ainsi réduit et ces événements n'atteignent jamais le magasin de journaux d'événements.

Important : Agissez avec précaution lorsque vous créez et utilisez les règles de suppression, car celles-ci empêchent la journalisation et l'apparition complète de certains événements natifs. Nous vous recommandons de tester les règles de suppression dans un environnement de test avant de les déployer.

Pour appliquer des règles de suppression et de récapitulation

1. Ouvrez l'Assistant d'intégration et avancez jusqu'à l'étape Règles de suppression ou Règles de récapitulation.
2. Commencez votre saisie dans le champ de saisie du schéma de règle pour rechercher les règles disponibles (facultatif). Au fur et à mesure, les règles qui correspondent à votre saisie s'affichent.
3. Sélectionnez les règles de votre choix à l'aide du contrôle de déplacement.
4. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape sélectionnée apparaît.

Informations complémentaires :

Tâches liées aux règles de suppression et de récapitulation (page 530)
Ouverture de l'Assistant d'intégration (page 602)
Ajout de composants d'intégration (page 603)
Définition des configurations par défaut (page 605)
Définition des configurations de journal de fichier (page 606)

Définition des configurations par défaut

Vous pouvez contrôler les paramètres d'accès aux données d'intégration en utilisant des configurations par défaut. Par exemple, vous pouvez paramétrer le contrôleur de domaine auquel se connecter pour les communications WMI.

Cette étape ne s'applique pas lors de la création d'une intégration Syslog, car les intégrations Syslog héritent de leurs valeurs de configuration de l'écouteur Syslog.

Pour définir des configurations par défaut

1. Ouvrez l'Assistant d'intégration et avancez jusqu'à l'étape Règles de suppression.
2. Remplissez les champs obligatoires.
3. Cliquez sur le bouton Masquer en regard d'une configuration par défaut quelconque pour qu'elle n'apparaisse pas lors de la création d'un connecteur (facultatif). Les configurations masquées ne sont pas visibles par l'utilisateur qui crée une connexion basée sur cette intégration. Ainsi, vous pouvez définir des configurations par défaut qui ne peuvent pas être modifiées lors de l'utilisation de l'intégration pour déployer un connecteur.
4. Cliquez sur la flèche appropriée pour accéder à l'étape à effectuer ensuite ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape sélectionnée apparaît.

Informations complémentaires :

Ajout de composants d'intégration (page 603)
Ouverture de l'Assistant d'intégration (page 602)

Définition des configurations de journal de fichier

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations, à l'aide du détecteur de journaux de fichiers. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour obtenir des intégrations personnalisées.

Pour définir des configurations de journal de fichier

1. Ouvrez l'Assistant d'intégration, sélectionnez le type de détecteur de journaux souhaité et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez le taux d'ancrage pour l'intégration.

   UpdateAnchorRate

   Pour les événements, indique le seuil auquel la valeur d'ancrage est créée. Si le traitement de l'événement est interrompu, l'agent se réfère au dernier ancrage pour recommencer le traitement. Définir un taux d'ancrage bas réduit les risques de perte d'événement, mais affecte les performances car la valeur d'ancrage est créée plus souvent. Définir un taux d'ancrage élevé augmente la charge de travail, car de nombreux événements devront être retraités en cas d'interruption du traitement.

   Par défaut : 4

   Lire depuis le début

   Indique si l'agent doit commencer la lecture du fichier au début de celui-ci, en cas d'interruption du traitement. Si cette case n'est pas sélectionnée, l'agent reprend la lecture des événements en fonction du taux d'ancrage. Si cette case à cocher est sélectionnée, le détecteur lit le fichier journal depuis le début lorsque vous déployez un connecteur pour la première fois. En fonction de la taille de la base de données et du taux de génération d'événements, le détecteur de journaux CA Enterprise Log Manager peut mettre un certain temps à se synchroniser avec des événements en temps réel.
3. Définissez ou modifiez les valeurs de configuration suivantes pour la source d'événement ciblée.

   Répertoire d'archivage du fichier

   Indique l'emplacement de sauvegarde du fichier journal après rotation. Le répertoire d'archivage et le nom de répertoire peuvent être identiques.

   Masque de fichier

   Définit une chaîne de texte utilisée pour identifier le fichier journal de la source d'événement. Le masque de fichier peut contenir des caractères génériques. Par exemple, pour identifier un fichier journal intitulé "messages.txt", vous pouvez saisir le masque *messages**.

Type de rotation de fichier

Définit l'intégration pour qu'elle corresponde au type de rotation de fichier utilisé par le produit ayant envoyé les événements. Le type de rotation actuel est défini par ce système (produit). Les paramètres suivants sont pris en charge par les intégrations CA Enterprise Log Manager.

- NewFile : utilisé lors de la rotation de la cible d'intégration par un utilitaire de type logrotate.
- FileSize : utilisé lorsque la cible d'intégration est basée sur un seuil de taille prédéfini.
- FileAge : utilisé lorsque la cible d'intégration est basée sur un laps de temps prédéfini. La mise à jour a généralement lieu aux alentours de minuit.

Nom de répertoire

Indique l'emplacement du fichier journal de la source d'événement.

Délimiteur d'événement

Définit l'expression régulière qui sépare les entrées individuelles, dans un fichier journal multiligne. Chaque fois que le détecteur de journal localise le délimiteur spécifié, il commence la lecture en recherchant les nouveaux événements. Cela permet à CA Enterprise Log Manager de recevoir plusieurs entrées d'événements à partir d'un même fichier journal. Par exemple, si chaque entrée de fichier journal contient un horodatage unique, vous pouvez utiliser comme délimiteur l'expression régulière de ce format d'horodatage.

4. Pour ajouter des valeurs de source d'événement supplémentaires, cliquez sur Répéter :  (facultatif).

   Un jeu supplémentaire de champs de valeurs de configuration s'affiche, vous permettant de saisir les valeurs de votre choix pour collecter des événements provenant d'une source différente.

5. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape choisie s'affiche.

Définition des configurations OPSEC

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations, à l'aide du détecteur OPSEC. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour obtenir des intégrations personnalisées.

Pour définir des configurations OPSEC

1. Ouvrez l'Assistant d'intégration, sélectionnez le détecteur OPSEC et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez les valeurs de configuration suivantes pour la source d'événement ciblée.

   EventLogName

   Indique le nom du journal créé pour cette intégration. Ce nom est utilisé pour l'association des éventuels fichiers XMP et DM relatifs à l'intégration.

   UpdateAnchorRate

   Pour les événements, indique le seuil auquel la valeur d'ancrage est créée. Si le traitement de l'événement est interrompu, l'agent se réfère au dernier ancrage pour recommencer le traitement. Définir un taux d'ancrage bas réduit les risques de perte d'événement, mais affecte les performances car la valeur d'ancrage est créée plus souvent. Définir un taux d'ancrage élevé augmente la charge de travail, car de nombreux événements devront être retraités en cas d'interruption du traitement.

   Par défaut : 1000

   Nom d'hôte du serveur

   Indique le nom de la source d'événement. Cette valeur peut être définie sur un nom de machine locale ou un nom de serveur distant.

   IP du serveur

   Indique l'adresse IP de la source d'événement. Cette valeur peut être définie sur un nom de machine locale ou un nom de serveur distant.

   Port du serveur

   Indique le port utilisé pour les communications OPSEC.

   Par défaut : 18184

   Objet

   Indique le nom de l'objet d'application OPSEC.

   Clé d'activation de l'objet

   Indique le mot de passe de l'objet d'application OPSEC.

MaxEventsPerSecond

Indique le nombre maximum d'événements pouvant être traités.

Signe de décalage FH

Indique si le fuseau horaire de la source d'événement est en avance ou en retard par rapport au fuseau horaire CA Enterprise Log Manager ; information indiquée par le signe plus (+) ou moins (-).

Heures de décalage FH

Indique le décalage, en heures, entre le fuseau horaire de la source d'événement et le fuseau horaire CA Enterprise Log Manager.

Minutes de décalage FH

Indique le décalage, en minutes, entre le fuseau horaire de la source d'événement et le fuseau horaire CA Enterprise Log Manager.

3. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape choisie s'affiche.

Définition des configurations ODBC

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations, à l'aide du détecteur ODBC. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour créer des intégrations personnalisées.

Pour définir des configurations ODBC

1. Ouvrez l'Assistant d'intégration, sélectionnez le détecteur ODBC et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez les valeurs de configuration principales suivantes, afin d'identifier la source d'événement souhaitée et d'y accéder.

   Chaîne de connexion

   Définit un ensemble de paires de mots-clés/valeurs qui permettent à l'agent de se connecter à la source d'événement et d'en collecter les événements. La chaîne de pilote utilise le format suivant.

   PILOTE={attribut-valeur}; paires-valeur-mot-clé-attribut-de-pilote

   Exemple : Pilote={Nom_pilote_ODBC_Oracle};Dbq=myDBName;

   Pour plus d'informations sur les paramètres de chaîne de connexion ODBC, reportez-vous au manuel du connecteur que vous configurez.

Nom d'utilisateur

Indique le nom de l'utilisateur disposant des droits d'accès appropriés pour la collecte des événements.

Mot de passe

Indique le mot de passe de l'utilisateur disposant des droits d'accès appropriés pour la collecte des événements.

Signe de décalage FH

Indique si le fuseau horaire de la source d'événement est en avance ou en retard par rapport au fuseau horaire CA Enterprise Log Manager ; information indiquée par le signe plus (+) ou moins (-).

Heures de décalage FH

Indique le décalage, en heures, entre le fuseau horaire de la source d'événement et le fuseau horaire CA Enterprise Log Manager.

Minutes de décalage FH

Indique le décalage, en minutes, entre le fuseau horaire de la source d'événement et le fuseau horaire CA Enterprise Log Manager.

EventLogName

Indique le nom du journal créé pour cette intégration. Ce nom est utilisé pour l'association des éventuels fichiers XMP et DM relatifs à l'intégration.

UpdateAnchorRate

Pour les événements, indique le seuil auquel la valeur d'ancrage est créée. Si le traitement de l'événement est interrompu, l'agent se réfère au dernier ancrage pour recommencer le traitement. Définir un taux d'ancrage bas réduit les risques de perte d'événement, mais affecte les performances, car la valeur d'ancrage est créée plus souvent. Définir un taux d'ancrage élevé augmente la charge de travail, car de nombreux événements devront être traités à nouveau en cas d'interruption du traitement.

Intervalle d'interrogation

Indique le laps de temps, en secondes, écoulé sans réception d'événement pour déclencher une interruption de durée égale dans l'interrogation. Par exemple, une valeur de 10 indique que, lorsque 10 secondes s'écoulent sans qu'aucun événement ne soit trouvé, l'agent attend 10 secondes avant de relancer l'interrogation.

MaxEventsPerSecond

Indique le nombre maximum d'événements pouvant être traités.

Lire depuis le début

Indique si l'agent doit commencer la lecture du fichier au début de celui-ci, en cas d'interruption du traitement des événements. Si cette case n'est pas sélectionnée, l'agent reprend la lecture des événements en fonction du taux d'ancrage. Si cette case est sélectionnée, le détecteur lit le fichier journal depuis le début lorsque vous déployez un connecteur. En fonction de la taille de la base de données et du taux de génération d'événements, le détecteur de journaux CA Enterprise Log Manager peut mettre un certain temps à se synchroniser avec des événements en temps réel.

3. Définissez ou modifiez les valeurs de collecte d'événements suivantes.

SourceName

Indique le nom de la source d'événement cible.

AnchorSQL

Indique la requête SQL utilisée pour définir la valeur d'ancrage. Le nom ou l'alias du champ référencé par AnchorSQL doit correspondre à la valeur du champ d'ancrage. La syntaxe AnchorSQL est basée sur le schéma de la base de données cible. Lors de la création d'une intégration personnalisée, reportez-vous à la documentation de votre schéma de base de données.

Champ d'ancrage

Indique le champ natif dans lequel rechercher des événements. La requête de collecte d'événements cible le champ d'ancrage que vous avez spécifié. La valeur du champ d'ancrage doit correspondre au nom ou à l'alias de la colonne incluse dans les instructions AnchorSQL et EventSQL. Par exemple, si le champ d'ancrage utilise l'alias "NTimestamp", les instructions que vous saisissez dans les champs AnchorSQL et EventSQL doivent également référencer "NTimestamp".

EventSQL

Indique la requête SQL utilisée pour collecter des événements depuis le fichier journal en identifiant la colonne cible. L'instruction EventSQL doit inclure le champ d'ancrage et correspondre au nom ou à l'alias que vous avez utilisé dans le champ d'ancrage. La syntaxe EventSQL est basée sur le schéma de la base de données cible. Lors de la création d'une intégration personnalisée, reportez-vous à la documentation du schéma de base de données pour votre application ou produit de base de données ODBC.

Activer les millisecondes

Indique si les millisecondes sont prises en charge pour les champs de date contenus dans les journaux d'événements collectés par la requête EventSQL.

4. Pour ajouter des valeurs de collecte d'événements supplémentaires, cliquez sur Répéter :  (facultatif).

   Des champs de collecte d'événements supplémentaires s'affichent, vous permettant de saisir les valeurs de votre choix pour collecter d'autres événements provenant de la même source.

5. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape sélectionnée apparaît.

Définition des configurations LocalSyslog

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations à l'aide du détecteur de journaux LocalSyslog pour collecter les événements. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour créer des intégrations personnalisées.

Pour définir les configurations LocalSyslog

1. Ouvrez l'Assistant d'intégration, sélectionnez le type de détecteur de journaux LocalSyslog et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez les valeurs de configuration suivantes pour la source d'événement ciblée.

   Serveur Syslog NG

   Indique, par le biais de la valeur True ou False, si le serveur cible est un serveur Syslog NG.

   Chemin d'accès au fichier de configuration Syslog

   Indique le fichier /etc/syslog.conf dans lequel les événements reçus sont consignés.

   UpdateAnchorRate

   Pour les événements, indique le seuil auquel la valeur d'ancrage est créée. Si le traitement de l'événement est interrompu, l'agent se réfère au dernier ancrage pour recommencer le traitement. Définir un taux d'ancrage bas réduit les risques de perte d'événement, mais affecte les performances, car la valeur d'ancrage est créée plus souvent. Définir un taux d'ancrage élevé augmente la charge de travail, car de nombreux événements devront être traités à nouveau en cas d'interruption du traitement.

   Par défaut : 1 000

   Lire depuis le début

   Indique si l'agent doit commencer la lecture du fichier au début de celui-ci, en cas d'interruption du traitement des événements. Si cette case n'est pas sélectionnée, l'agent reprend la lecture des événements en fonction du taux d'ancrage. Si cette case est sélectionnée, le détecteur lit le fichier journal depuis le début lorsque vous déployez un connecteur. En fonction de la taille de la base de données et du taux de génération d'événements, le détecteur de journaux CA Enterprise Log Manager peut mettre un certain temps à se synchroniser avec des événements en temps réel.

Définition des configurations TIBCO

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations, à l'aide du détecteur TIBCO. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événement, mais vous pouvez également les modifier pour obtenir des intégrations personnalisées.

Pour définir des configurations TIBCO

1. Ouvrez l'Assistant d'intégration, sélectionnez le détecteur de journaux TIBCO et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez les valeurs de configuration principales suivantes, afin d'identifier la source d'événement souhaitée et d'y accéder.

Serveur TIBCO

Indique le nom ou l'adresse IP du serveur TIBCO, au format suivant.

Protocole://nom ou IP du serveur:Numéro de port

Par exemple, lors de l'installation du serveur de rapports de contrôle d'accès CA, vous indiquez si vous souhaitez communiquer via SSL. En fonction de votre réponse, procédez de l'une des manières suivantes.

- Si vous ne sélectionnez pas SSL, spécifiez :

  tcp://tibcoTCPsrv:7222.

- Si vous sélectionnez SSL, spécifiez :

  ssl://tibcoSSLsrv:7243.

  La valeur de port par défaut est 7243. Si vous avez spécifié une valeur de port différente lors de l'installation du serveur de rapports, vous devez l'utiliser.

Utilisateur TIBCO

Indique le nom d'utilisateur pour l'authentification du serveur TIBCO.

Par exemple, lors de l'installation du serveur de rapports de contrôle d'accès CA, vous indiquez si vous souhaitez communiquer via SSL. En fonction de votre réponse, procédez de l'une des manières suivantes.

- Si vous ne sélectionnez pas SSL, il n'existe aucune valeur par défaut et vous pouvez spécifier le nom d'utilisateur de votre choix.
- Si vous sélectionnez SSL, spécifiez "reportserver".

Mot de passe TIBCO

Indique le mot de passe pour l'authentification du serveur TIBCO.

Par exemple, lors de l'installation du serveur de rapports de contrôle d'accès CA, vous indiquez si vous souhaitez communiquer via SSL. En fonction de votre réponse, procédez de l'une des manières suivantes.

- Si vous ne sélectionnez pas SSL, il n'existe aucune valeur par défaut et vous pouvez spécifier le mot de passe de votre choix.
- Si vous sélectionnez SSL, indiquez le mot de passe saisi lors de l'installation du serveur de rapports.

Nom du journal d'événements

Indique le nom du journal pour la source d'événement.

PollInterval

Indique le nombre de secondes que l'agent doit attendre avant l'interrogation des événements lorsque le serveur TIBCO est indisponible ou déconnecté.

SourceName

Spécifie l'identifiant pour la file d'attente TIBCO.

File d'attente TIBCO

Indique le nom de la file d'attente TIBCO dans laquelle le détecteur de journaux lit les messages (événements).

Nombre de threads de collecte

Indique le nombre de threads générés par le détecteur de journaux pour lire les messages dans la file d'attente TIBCO. La valeur minimum est 1. Le nombre maximum de threads pouvant être générés est 20.

Définition des configurations WMI

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations, à l'aide du détecteur WMI. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour obtenir des intégrations personnalisées.

Pour définir des configurations WMI

1. Ouvrez l'Assistant d'intégration, sélectionnez le détecteur de journaux WMI et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez les valeurs de configuration principales suivantes, afin d'identifier la source d'événement Windows souhaitée et d'y accéder.

   Nom de serveur WMI

   Indique le nom du serveur de la source d'événement.

   Domaine

   Indique le nom du domaine dans lequel la source d'événement est située.

   NameSpace

   Définit la classe à partir de laquelle vous souhaitez collecter des événements.

   Par défaut : root\cimv2

   Nom d'utilisateur

   Indique le nom de l'utilisateur disposant des droits d'accès appropriés pour la collecte des événements.

   Mot de passe

   Indique le mot de passe de l'utilisateur disposant des droits d'accès appropriés pour la collecte des événements.

   EventLogName

   Indique le nom du journal créé pour cette intégration. Ce nom est utilisé pour l'association des éventuels fichiers XMP et DM relatifs à l'intégration.

UpdateAnchorRate

Pour les événements, indique à quelle fréquence une valeur d'ancrage est créée. Si le traitement de l'événement est interrompu, pour quelque raison que ce soit, l'agent se réfère au dernier ancrage pour recommencer le traitement. Un taux d'ancrage bas réduit les risques de perte d'événement, mais affecte les performances, car la valeur d'ancrage est créée plus souvent. Un taux d'ancrage très élevé peut augmenter la charge de travail, car de nombreux événements devront être traités de nouveau en cas d'interruption.

3. Définissez ou modifiez les valeurs de collecte d'événements suivantes.

Champ d'ancrage

Indique le champ natif vérifié pour les événements. La requête de collecte d'événements cible le champ d'ancrage que vous avez spécifié.

Nom du fichier journal

Indique le fichier journal de la source de journaux NTEvent à consulter pour les événements. Si vous souhaitez seulement consulter les événements contenus dans le fichier journal d'application, définissez des valeurs pour Application uniquement.

Par défaut : Sécurité, Système, Application

Contrôle

Garantit que le fichier journal identifié par la valeur Nom du fichier journal est contrôlé pour les événements. Désélectionnez le paramètre Contrôle si vous souhaitez désactiver le contrôle d'un fichier journal donné, sans retirer la valeur de ce fichier journal de la configuration.

Requête

Indique l'instruction de requête SQL utilisée pour collecter des événements à partir d'un fichier journal et d'une source donnés.

4. Pour ajouter des valeurs de collecte d'événements supplémentaires, cliquez sur Répéter :  (facultatif).

Un jeu de champs de collecte d'événements supplémentaire s'affiche, vous permettant de saisir les valeurs de votre choix pour collecter des événements provenant de la même source. Par exemple, pour collecter des événements provenant de plusieurs fichiers journaux différents, ajoutez des champs de collecte d'événements supplémentaires.

5. Pour ajouter des valeurs de configuration générale et de collecte d'événements, cliquez sur le bouton Répéter, situé en haut, en-dehors de la zone bleue :  (facultatif).

   Un jeu complet de champs de configuration et de collecte s'affiche, vous permettant de saisir des valeurs de collecte et d'identification de la source d'événement. Par exemple, pour collecter des événements provenant de plusieurs sources Windows, ajoutez des valeurs de collecte d'événements et d'identification de source.

6. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape choisie s'affiche.

Définition des configurations de journal W3C

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations à l'aide du détecteur de journaux W3C. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour obtenir des intégrations personnalisées.

Pour définir des configurations de journal W3C

1. Ouvrez l'Assistant d'intégration, sélectionnez le type de détecteur de journaux W3C et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez le taux d'ancrage pour l'intégration.

   UpdateAnchorRate

   Pour les événements, indique le seuil auquel la valeur d'ancrage est créée. Si le traitement de l'événement est interrompu, l'agent se réfère au dernier ancrage pour recommencer le traitement. Définir un taux d'ancrage bas réduit les risques de perte d'événement, mais affecte les performances car la valeur d'ancrage est créée plus souvent. Définir un taux d'ancrage élevé augmente la charge de travail, car de nombreux événements devront être retraités en cas d'interruption du traitement.

   Par défaut : 1 000
3. Définissez ou modifiez les valeurs de configuration suivantes pour la source d'événement ciblée.

   Répertoire d'archivage du fichier

   Indique l'emplacement de sauvegarde du fichier journal après rotation. Le répertoire d'archivage et le nom de répertoire peuvent être identiques.

   Masque de fichier

   Définit une chaîne de texte utilisée pour identifier le fichier journal de la source d'événement. Le masque de fichier peut contenir des caractères génériques. Par exemple, pour identifier un fichier journal intitulé "messages.txt", vous pouvez saisir le masque *messages** .

   Type de rotation de fichier

   Définit l'intégration pour qu'elle corresponde au type de rotation de fichier utilisé par le produit ayant envoyé les événements. Le type de rotation actuel est défini par ce système (produit). Les paramètres suivants sont pris en charge par les intégrations CA Enterprise Log Manager.

   - NewFile : utilisé lors de la rotation de la cible d'intégration par un utilitaire de type logrotate.

- FileSize : utilisé lorsque la cible d'intégration est basée sur un seuil de taille prédéfini. Si vous sélectionnez FileSize, vous devez également entrer une valeur dans la zone liée à la taille maximale d'un fichier.
- FileAge : utilisé lorsque la cible d'intégration est basée sur un laps de temps prédéfini. La mise à jour a généralement lieu aux alentours de minuit.

Nom du répertoire source

Indique l'emplacement du fichier journal de la source d'événement.

Délimiteur de fichier journal

Sépare, avec une virgule (,), les valeurs de champs d'un événement pour que le détecteur de journaux puisse les lire.

Lire depuis le début

Indique si l'agent doit commencer la lecture du fichier au début de celui-ci, en cas d'interruption du traitement. Si cette case n'est pas sélectionnée, l'agent reprend la lecture des événements en fonction du taux d'ancrage.

Nom du journal d'événements

Définit le nom du fichier journal d'événements local à partir duquel vous souhaitez lire les événements.

4. Pour ajouter des valeurs de source d'événement supplémentaires, cliquez sur Répéter :  (facultatif).

   Un jeu supplémentaire de champs de valeurs de configuration s'affiche, vous permettant de saisir les valeurs de votre choix pour collecter des événements provenant d'une source différente.

5. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape choisie s'affiche.

Définition des configurations d'ACLogsensor

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations en utilisant le détecteur de journaux AC pour collecter les événements provenant des versions de CA Access Control antérieures à la version r12. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour créer des intégrations personnalisées.

Pour définir des configurations de journal AC

1. Ouvrez l'Assistant d'intégration, sélectionnez le type de détecteur de journaux AC et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez les valeurs de configuration suivantes pour la source d'événement ciblée.

   Port

   Indique le numéro de port sur lequel le détecteur de journaux écoute les événements entrants. Si vous ne spécifiez pas de numéro de port, le détecteur de journaux écoute un port affecté dynamiquement.

   Valeur par défaut : 0

   Chiffres

   Indique le type de chiffrement utilisé pour sécuriser les événements.

   Valeur par défaut : Désactivé

   Clé de chiffrement

   Définit la clé utilisée pour chiffrer la transmission des événements. Saisissez le nom de la clé créée lorsque vous avez configuré l'application ou la source d'événement ciblée par votre connecteur.

   Par défaut : Aucune

   EventLogName

   Définit le nom du journal d'événements de l'application ou de la source d'événements ciblée par votre connecteur.
3. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape choisie s'affiche.

Définition des configurations WinRM Linux

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations à l'aide du détecteur de journaux WinRM Linux. Le détecteur de journaux WinRM Linux vous permet de rassembler des événements provenant de certaines plates-formes Windows sans déployer d'agent.

Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour créer des intégrations personnalisées.

Pour définir des configurations WinRM Linux

1. Ouvrez l'Assistant d'intégration, sélectionnez le type de détecteur de journaux WinRM Linux et avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez les valeurs de configuration suivantes pour la source d'événement ciblée.

   Nom de l'ordinateur

   Nom du système Windows depuis lequel les événements sont reçus. Le service WinRM doit être configuré et écouter sur un port HTTP.

   Port

   Port utilisé par le service WinRM pour recevoir les événements. Le port par défaut est 80. Seule l'authentification HTTP de base est prise en charge.

   Nom d'utilisateur

   Nom de l'utilisateur du système de source d'événement Windows. Cet utilisateur doit être membre du groupe "Lecteurs de journaux d'événements" pour autoriser l'accès aux événements.

   Mot de passe

   Mot de passe pour le nom d'utilisateur indiqué.

   Nom du journal d'événements

   Nom du journal utilisé pour l'identification de l'intégration lorsque celle-ci est configurée comme connecteur.

   PollInterval

   Durée d'inactivité du détecteur de journaux, lorsqu'aucun événement ne se produit ou que les communications sont interrompues. Une fois ce délai expiré, le détecteur de journaux poursuit sa tentative de collecte d'événements.

   UpdateAnchorRate

Pour les événements, indique le seuil auquel la valeur d'ancrage est créée. Si le traitement de l'événement est interrompu, l'agent se réfère au dernier ancrage pour recommencer le traitement. Définir un taux d'ancrage bas réduit les risques de perte d'événement, mais affecte les performances, car la valeur d'ancrage est créée plus souvent. Définir un taux d'ancrage élevé augmente la charge de travail, car de nombreux événements devront être traités à nouveau en cas d'interruption du traitement.

Par défaut : 1 000

Lire depuis le début

Indique si l'agent doit commencer la lecture du fichier au début de celui-ci, en cas d'interruption du traitement des événements. Si cette case n'est pas sélectionnée, l'agent reprend la lecture des événements en fonction du taux d'ancrage. Si cette case est sélectionnée, le détecteur lit le fichier journal depuis le début lorsque vous déployez un connecteur. En fonction de la taille de la base de données et du taux de génération d'événements, le détecteur de journaux CA Enterprise Log Manager peut mettre un certain temps à se synchroniser avec des événements en temps réel.

SourceName

Indique un nom pour identifier la source du canal d'événements.

Nom de canal (Journal)

Nom du canal, ou journal, spécifique depuis lequel les événements sont reçus. Par exemple, Application.

Définition des configurations SDEE

Vous pouvez contrôler les paramètres d'accès aux données pour les intégrations, à l'aide du détecteur de journaux SDEE. Vous pouvez utiliser les paramètres par défaut fournis par CA pour la plupart des collectes d'événements, mais vous pouvez également les modifier pour créer des intégrations personnalisées.

Pour définir les configurations SDEE

1. Ouvrez l'Assistant d'intégration, sélectionnez SDEE comme type de détecteur de journaux, puis avancez jusqu'à l'étape Configurations par défaut.
2. Définissez ou modifiez les valeurs de configuration suivantes pour la source d'événement ciblée.

   Adresse du serveur SDEE

   Indique l'adresse IP ou le nom DNS du serveur à partir duquel vous souhaitez extraire les événements.

   Numéro de port du serveur SDEE

   Spécifie un numéro de port HTTP permettant l'accès au serveur SDEE, si vous utilisez un port autre que le port par défaut (433).

   ID de connexion au serveur SDEE

   Indique le nom d'utilisateur requis pour la connexion au serveur SDEE cible.

   Mot de passe du détecteur SDEE

   Indique le mot de passe de l'utilisateur spécifié dans le champ ID de connexion au serveur SDEE.

   PollingInterval

   Indique le laps de temps souhaité avant d'interroger le serveur SDEE pour rechercher les événements.

   Nombre maximum d'événements

   Indique la taille de lot pour les événements récupérés à partir du serveur SDEE.

   Remarque : La plage de taille recommandée est 100–500.

   Nom du journal d'événements

   Indique le nom du journal à partir duquel vous souhaitez extraire les événements.

   Expiration du délai de connexion

   Spécifie le laps de temps (en minutes) au bout duquel une connexion inactive est coupée.

3. Sélectionnez les types d'événement que vous souhaitez extraire à l'aide des cases à cocher de type d'événement. Les catégories d'événement suivantes sont disponibles.
   - Type d'événement
   - Sévérité de l'alerte d'événement
   - Sévérité de l'erreur d'événement

   Sélectionnez la case à cocher d'un événement donné pour extraire le type d'événement correspondant.

Création d'un écouteur Syslog

Vous pouvez utiliser l'Assistant d'écouteur pour créer ou modifier des écouteurs Syslog. L'écouteur contrôle la manière dont les événements Syslog sont acheminés vers le serveur CA Enterprise Log Manager.

Remarque : Vous pouvez utiliser l'écouteur Syslog d'inscription (prédéfini) dans la majorité des situations. Les instructions suivantes concernent les utilisateurs qui préfèrent configurer leur réception Syslog en utilisant des écouteurs personnalisés.

Pour profiter au mieux de cette fonctionnalité avancée, vous devez parfaitement comprendre les sources d'événement Syslog de votre environnement.

La création d'une intégration inclut les étapes suivantes.

1. Ouverture de l'Assistant d'écouteur
2. Ajout de composants
3. Sélection des règles de suppression
4. Sélection des règles de récapitulation
5. Définition des configurations par défaut

Informations complémentaires :

Ouverture de l'Assistant d'écouteur (page 626)
Ajout de composants d'écouteur (page 627)
Définition des configurations par défaut (page 629)
Application de règles de suppression et de récapitulation (page 628)
Ajout d'un fuseau horaire Syslog (page 631)

Ouverture de l'Assistant d'écouteur

Pour créer un nouvel écouteur Syslog ou modifier un écouteur existant, ouvrez l'Assistant d'écouteur.

Pour ouvrir l'Assistant d'écouteur

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur la flèche en regard du dossier Bibliothèque d'ajustement d'événement pour le développer, puis sélectionnez le dossier Ecouteurs.

   Les boutons Intégration s'affichent dans le volet Détails.

3. Cliquez sur Nouvel écouteur : 

   L'Assistant d'écouteur apparaît.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer l'écran de l'assistant avec les paramètres du dernier enregistrement.

Ajout de composants d'écouteur

Pour créer un écouteur Syslog, définissez les informations telles que le nom et l'aide à la configuration.

Pour ajouter des composants d'écouteur

1. Ouvrez l'Assistant d'écouteur.
2. Saisissez un nom pour le nouvel écouteur.
3. Sélectionnez le composant suivant dans la liste déroulante (facultatif).

   Aide à la configuration

   Celle-ci définit le fichier binaire de l'aide que l'intégration utilise pour se connecter au magasin de journaux sélectionné. La plupart des intégrations ne nécessitent pas d'aide à la configuration.

   Remarque : Le type de détecteur pour un écouteur est toujours Syslog.
4. Saisissez une description pour l'écouteur (facultatif).
5. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, la nouvelle intégration apparaît dans la liste du dossier Utilisateur. Sinon, l'étape sélectionnée apparaît.

Application de règles de suppression et de récapitulation

Vous pouvez appliquer des règles de suppression et de récapitulation à un écouteur Syslog, afin de rationaliser l'ajustement d'événement. Lorsque vous utilisez l'écouteur avec un connecteur, les événements entrants sont vérifiés par rapport à n'importe quelle règle de suppression et de récapitulation appliquée, avant d'être envoyés à CA Enterprise Log Manager.

Par exemple, si vous souhaitez créer un écouteur afin de recevoir les événements CA Access Control uniquement, vous pouvez appliquer la règle CA Access Control d'accès réussi au fichier. Vous évitez ainsi les traitements inutiles, car seules les règles nécessaires sont utilisées pour vérifier les événements entrants.

Important : Agissez avec précaution lorsque vous créez et utilisez les règles de suppression, car celles-ci empêchent la journalisation et l'apparition complète de certains événements natifs. Nous vous recommandons de tester les règles de suppression dans un environnement de test avant de les déployer.

Pour appliquer des règles de suppression ou de récapitulation

1. Ouvrez l'Assistant d'écouteur et avancez jusqu'à l'étape Règles de suppression ou Règles de récapitulation.
2. Commencez votre saisie dans le champ de saisie du schéma de règle pour rechercher les règles disponibles (facultatif). Au fur et à mesure, les règles qui correspondent à votre saisie s'affichent.
3. Sélectionnez les règles de votre choix à l'aide du contrôle de déplacement.
4. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouvel écouteur apparaît dans la liste du dossier Utilisateur. Sinon, l'étape sélectionnée s'affiche.

Définition des configurations par défaut

Vous pouvez contrôler les paramètres d'accès aux données de l'écouteur Syslog en utilisant des configurations par défaut. Par exemple, vous pouvez définir des hôtes fiables ou des ports de communication par défaut.

Pour définir des configurations par défaut

1. Ouvrez l'Assistant d'écouteur et avancez jusqu'à l'étape Configurations par défaut.
2. Modifiez ou ajoutez les valeurs de votre choix.

   Classement des événements

   Permet de s'assurer que les événements sont envoyés au magasin de journaux d'événements dans l'ordre exact de réception. En cas de désactivation du classement des événements, l'ordre peut ne pas être respecté si certains événements sont analysés et transmis plus rapidement que d'autres. L'activation du classement des événements peut avoir un impact sur les performances de par le ralentissement de la soumission et du traitement des événements.

   Nombre de threads par file d'attente

   Indique le nombre de threads de traitement par protocole. L'utilisation de nombreux threads de traitement accélère le traitement si le classement des événements est désactivé. Si le classement des événements est activé, le nombre de threads n'a aucune incidence. L'utilisation de nombreux threads peut nuire aux performances.

   Taille de file d'attente

   Indique la taille de la file d'attente, en nombre d'événements, pour les données d'événements entrants. Cette file d'attente est utilisée pour traiter et soumettre les événements. Si le tampon est plein, aucun événement supplémentaire ne peut être reçu tant que des événements n'ont pas été traités pour libérer de la place.

   Ports

   Indique les ports que l'écouteur utilise pour recevoir les événements via UDP ou TCP. Si vous spécifiez plusieurs ports, le service tente de se connecter à chacun d'eux à tour de rôle. Les ports Syslog par défaut sont déjà définis. Si vous avez routé des événements Syslog vers d'autres ports, vous devez configurer vos ports de réception CA Enterprise Log Manager en conséquence.

   Important : Si l'agent est exécuté en tant qu'utilisateur non root sur un système UNIX, modifiez les ports d'écouteur Syslog en sélectionnant des ports dont le numéro est supérieur à 1024. Dans un tel cas, le port UDP 514 par défaut n'est pas ouvert et aucun événement Syslog n'est collecté.

Hôte fiable

Indique les adresses IP fiables pour IPv4 ou IPv6 ; seules les communications provenant d'un hôte fiable sont acceptées. Si vous ne spécifiez aucun hôte fiable, les événements provenant de toutes les sources Syslog disponibles seront acceptés. Entrez l'adresse IP exacte telle qu'elle est enregistrée dans le champ event_source_address pour les hôtes fiables. Vous ne pouvez pas utiliser de caractères génériques ni d'adresses de sous-réseau.

Fuseaux horaires

Vous permet d'ajouter des fuseaux horaires pour les ordinateurs de source d'événement Syslog. Syslog n'enregistre généralement pas l'heure. Identifiez les systèmes sources à l'aide de leur adresse IP complète et de leur fuseau horaire pour recevoir et ajuster des événements provenant de sources Syslog qui se trouvent dans un fuseau horaire différent de celui du serveur CA Enterprise Log Manager. Ne répertoriez pas les sources Syslog figurant dans le même fuseau horaire que le serveur.

3. Cliquez sur la flèche appropriée pour accéder à l'étape de l'assistant que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le nouvel écouteur apparaît dans la liste du dossier Utilisateur. Sinon, l'étape sélectionnée s'affiche.

Ajout d'un fuseau horaire Syslog

Ajoutez un fuseau horaire à un ou plusieurs ordinateurs de source d'événement Syslog pour recevoir des événements et les ajuster correctement à partir de sources Syslog situées dans un fuseau horaire différent de celui du serveur CA Enterprise Log Manager.

Vous pouvez ajouter un fuseau horaire Syslog lors de la création d'une intégration, lors de la configuration d'un connecteur ou lors de la création d'une configuration enregistrée.

Remarque : Lors de l'ajout d'un fuseau horaire à un environnement appliquant l'heure d'été, assurez-vous qu'une entrée de fuseau horaire correspondante existe sur le système hôte de l'agent. Sans cette entrée, le fuseau horaire Syslog n'est pas en mesure de gérer le changement d'heure et les événements comportent un horodatage incorrect pendant la période d'heure d'été.

Pour ajouter un fuseau horaire Syslog

1. Accédez à l'interface de fuseau horaire Syslog de l'une des manières suivantes.
   - Ouvrez l'intégration Syslog à laquelle vous souhaitez ajouter des fuseaux horaires et avancez jusqu'à l'étape Configuration par défaut.
   - Ouvrez le connecteur Syslog auquel vous souhaitez ajouter des fuseaux horaires et avancez jusqu'à l'étape Configuration du connecteur.
   - Ouvrez la configuration enregistrée à laquelle ajouter des fuseaux horaires.

   L'interface de fuseau horaire Syslog apparaît.
2. Cliquez sur Créer un dossier en haut de la zone Fuseaux horaires.

   Un nouveau dossier de fuseau horaire apparaît dans la zone de liste et une liste déroulante de fuseaux horaires apparaît dans le volet droite.
3. Sélectionnez un fuseau horaire dans la liste déroulante.

   Le fuseau sélectionné apparaît en regard du dossier.
4. Cliquez sur la flèche en regard du dossier.

   Le dossier se développe ; il contient un seul ordinateur de source d'événement sans titre pour ce fuseau horaire.
5. Sélectionnez l'icône de l'ordinateur.

   Le champ de saisie de l'adresse IP apparaît.
6. Saisissez une adresse IP.

   L'adresse apparaît en regard de l'icône de l'ordinateur pendant la frappe.

7. Pour ajouter des ordinateurs de source d'événement supplémentaires, sélectionnez une source d'événement existante et cliquez sur Ajouter un élément (facultatif).

   Le dossier se ferme. Ouvrez-le pour afficher un nouvel ordinateur de source d'événement sans titre. Passez à l'étape 6.

8. Pour ajouter des fuseaux horaires supplémentaires, cliquez sur Créer un dossier (facultatif).

   Un nouveau dossier de fuseau horaire sans titre apparaît. Passez à l'étape 3.

9. Lorsque vous avez créé tous les dossiers de fuseau horaire et les éléments d'adresse de source d'événement souhaités, cliquez sur Enregistrer.

Informations complémentaires :

Définition de la configuration du connecteur (page 637)
Création d'une configuration enregistrée (page 640)

Création d'une nouvelle version d'intégration

Vous pouvez créer une nouvelle version d'une intégration créée par l'utilisateur (personnalisée) existante.

Pour créer une nouvelle version d'intégration

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

   La liste du dossier Collecte de journaux s'affiche.

2. Accédez au dossier Utilisateur contenant l'intégration souhaitée.
3. Sélectionnez l'intégration utilisateur et cliquez sur Créer une version.
4. L'assistant de nouvelle intégration apparaît et affiche les détails de l'intégration sélectionnée.
5. Effectuez les changements souhaités, puis cliquez sur Enregistrer et fermer.

   La nouvelle version d'intégration apparaît dans la liste.

Informations complémentaires

Suppression d'une intégration (page 633)

Suppression d'une intégration

Vous pouvez supprimer une intégration personnalisée. Vous ne pouvez pas supprimer une intégration d'abonnement.

Pour supprimer une intégration personnalisée

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

   La liste du dossier Collecte de journaux s'affiche.

2. Développez le dossier Bibliothèque d'ajustement d'événement, puis le dossier Intégrations.
3. Sélectionnez le dossier utilisateur contenant l'intégration à supprimer.
4. Sélectionnez l'intégration que vous souhaitez supprimer de la liste.
5. Cliquez sur Supprimer en haut de la liste.

   Une boîte de dialogue de confirmation s'affiche.

6. Cliquez sur Oui.

   L'intégration est supprimée de la liste.

Informations complémentaires

Création d'une nouvelle version d'intégration (page 632)

Exportation et importation de définitions d'intégration

Vous pouvez exporter et importer les détails d'intégration afin de les utiliser avec d'autres serveurs de gestion. Cela vous permet de transférer des intégrations personnalisées réussies entre des environnements CA Enterprise Log Manager ou d'un environnement de test à un environnement réel.

Informations complémentaires :

Importation de définitions d'intégration (page 634)
Exportation de définitions d'intégration (page 634)

Importation de définitions d'intégration

Vous pouvez importer des fichiers XML de définitions d'intégration, afin de les utiliser avec le serveur de gestion local.

Pour importer des détails d'intégration

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

   Le dossier Collecte de journaux s'affiche.

2. Développez le dossier Intégrations, puis accédez au sous-dossier dans lequel vous souhaitez importer une intégration.

3. Cliquez sur Importer l'intégration.

   Une boîte de dialogue Importation de fichier s'ouvre.

4. Saisissez ou naviguez vers l'emplacement du fichier que vous souhaitez importer, puis cliquez sur OK.

   Les fichiers requis sont importés dans le dossier en cours et une boîte de dialogue de confirmation s'affiche.

5. Cliquez sur OK.

Exportation de définitions d'intégration

Vous pouvez exporter les détails d'intégration afin de les utiliser avec d'autres serveurs de gestion. L'export est enregistré dans un fichier XML.

Pour exporter les informations d'intégration

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

   Le dossier Collecte de journaux s'affiche.

2. Développez le dossier Intégrations, puis accédez au sous-dossier contenant l'intégration que vous souhaitez exporter.

3. Cliquez sur Exporter les intégrations.

   Une boîte de dialogue de téléchargement s'affiche.

4. Saisissez ou naviguez vers l'emplacement dans lequel vous souhaitez enregistrer les fichiers d'export XML, puis cliquez sur Enregistrer.

   Les fichiers requis sont enregistrés à l'emplacement souhaité et une boîte de dialogue de confirmation apparaît.

5. Cliquez sur OK.

Création d'un connecteur

Vous pouvez créer un connecteur pour regrouper les événements d'un système d'exploitation ou d'une unité spécifique au sein de votre environnement. Vous utilisez une intégration ou un écouteur en tant que modèle pour créer un connecteur, à l'aide de l'assistant de création d'un connecteur. Chaque nouveau connecteur est appliqué à un agent dans votre environnement.

Vous pouvez créer des connecteurs de plusieurs types, y compris des intégrations WMI et ODBC, qui réunissent activement les événements d'un type précis. Vous pouvez également créer des intégrations Syslog, qui reçoivent les événements de manière passive. Contrairement aux autres types, les connecteurs Syslog peuvent recevoir des événements de plusieurs sources. Par conséquent, le processus de création d'un connecteur Syslog et d'un connecteur est légèrement différent.

Le processus de création d'un connecteur se compose des étapes ci-dessous.

1. Ouverture de l'assistant du connecteur
2. Ajout des détails du connecteur, avec sélection d'un écouteur pour les connecteurs Syslog
3. Application de règles de suppression
4. Application des règles de récapitulation.
5. Définition de configurations de connecteur

Informations complémentaires :

Ouverture de l'assistant du connecteur (page 635)
Ajout des détails du connecteur (page 636)
Application de règles de suppression et de récapitulation (page 637)
Définition de la configuration du connecteur (page 637)

Ouverture de l'assistant du connecteur

Pour créer un nouveau connecteur ou modifier un connecteur existant, vous devez ouvrir l'assistant du connecteur.

Pour ouvrir l'assistant du connecteur

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

   La liste du dossier Collecte de journaux s'affiche.

2. Développez le dossier Explorateur d'agent et sélectionnez le groupe d'agents au sein duquel vous souhaitez ajouter ou modifier un connecteur.

   Les agents appartenant au groupe sélectionné s'affichent.

3. Sélectionnez l'agent auquel ajouter ou modifier un connecteur.

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

4. Cliquez sur Nouveau connecteur :  .

   L'assistant du connecteur s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Ajout des détails du connecteur

Vous pouvez ajouter un nom et une description pour identifier votre connecteur. Vous devez également choisir l'intégration à utiliser en tant que modèle pour le connecteur.

Pour ajouter les détails du connecteur

1. Ouvrez l'assistant de conception de connecteur.

   L'assistant s'ouvre et affiche la plate-forme et la version de la plate-forme de l'agent en cours en haut de l'écran.

2. Saisissez un nom pour le connecteur.
3. Sélectionnez le bouton radio Ecouteur si vous souhaitez créer un connecteur Syslog ou le bouton radio Intégration pour tout autre type.
4. Sélectionnez l'intégration à utiliser en tant que modèle. La liste déroulante Intégration affiche toutes les intégrations disponibles pour la version de la plate-forme en cours et le type de source d'événement.
5. Sélectionnez Omettre la vérification de la version de plate-forme pour réaliser des intégrations pour *toutes* les versions de la plate-forme d'agent disponible dans la liste déroulante Intégration (facultatif).
6. Saisissez une description pour le connecteur.

7. Accédez à la prochaine étape que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le connecteur apparaît dans la liste des connecteurs.

Application de règles de suppression et de récapitulation

Lors de la création ou de la modification d'un connecteur, vous pouvez sélectionner les règles de suppression et de récapitulation à appliquer aux événements gérés par le connecteur. Toutes les règles de suppression ou de récapitulation que vous ajoutez sont appliquées avant que les événements ne soient transmis au serveur CA Enterprise Log Manager.

Pour appliquer des règles de suppression ou de récapitulation

1. Ouvrez l'Assistant de conception de connecteur et avancez jusqu'à l'étape Application de règles de suppression ou Règles de récapitulation.

   La liste des règles de suppression disponibles s'affiche.

2. Commencez votre saisie dans le champ de saisie du schéma de règle pour rechercher les règles disponibles (facultatif). Au fur et à mesure, les règles qui correspondent à votre saisie s'affichent.

3. Sélectionnez la ou les règles à appliquer à l'aide du contrôle de déplacement.

4. Accédez à la prochaine étape que vous souhaitez effectuer ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le connecteur apparaît dans la liste des connecteurs.

Définition de la configuration du connecteur

Lors de la création ou de la modification d'un connecteur, vous pouvez définir des configurations individuelles qui déterminent la réception et la transmission reçoit des événements par le connecteur. Vous pouvez définir les configurations pour chaque connecteur ou utiliser les configurations enregistrées.

Les configurations enregistrées sont des recueils de paramètres d'accès aux données réutilisables. Vous pouvez appliquer les configurations enregistrées à plusieurs connecteurs.

Pour définir des configurations de connecteur

1. Ouvrez l'assistant de conception de connecteur et avancez jusqu'à l'étape Configuration du connecteur.
2. Si vous avez sélectionné l'écouteur/le détecteur de journaux Syslog, sélectionnez la ou les intégrations que le connecteur doit utiliser.
3. Sélectionnez la configuration enregistrée de votre choix dans la liste déroulante ou modifiez les valeurs de configuration affichées. Les connecteurs héritent leurs paramètres de configuration de leur intégration, ou de l'écouteur dans le cas de connecteurs Syslog.
4. Cliquez sur le lien Aide pour afficher le manuel du connecteur pour l'intégration sélectionnée (facultatif). Le manuel qui s'affiche contient de nombreuses informations utiles.
5. Cliquez sur Enregistrer et fermer.

   Le connecteur s'affiche dans la liste des connecteurs.

Affichage d'un connecteur

Vous pouvez ouvrir la liste des connecteurs pour chaque agent afin d'afficher et de modifier les connecteurs liés à cet agent.

Pour afficher un connecteur

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

   La liste du dossier Collecte de journaux s'affiche.
2. Développez le dossier Explorateur d'agent et le dossier du groupe d'agents pour faire apparaître les différents agents.
3. Sélectionnez l'agent sur lequel le connecteur à afficher est déployé.
4. Cliquez sur Afficher les connecteurs :  .

   La liste Connecteurs de l'agent apparaît, affichant les connecteurs déployés sur l'agent sélectionné.

Modification d'un connecteur

Vous pouvez modifier un connecteur existant. La modification d'un connecteur crée une nouvelle version.

Pour modifier un connecteur

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

   La liste du dossier Collecte de journaux s'affiche.

2. Développez le dossier Explorateur d'agent et le dossier du groupe d'agents pour faire apparaître les différents agents.

3. Sélectionnez l'agent sur lequel le connecteur à afficher est déployé.

4. Cliquez sur Afficher les connecteurs :  .

   La liste Connecteurs de l'agent apparaît, affichant les connecteurs déployés sur l'agent sélectionné.

5. Cliquez sur Modifier en regard du connecteur à modifier.

   L'assistant du connecteur s'ouvre et affiche le connecteur sélectionné.

6. Effectuez les changements souhaités, puis cliquez sur Enregistrer et fermer.

   Le connecteur modifié apparaît dans la liste.

A propos des configurations enregistrées

Une configuration enregistrée est une collection réutilisable de paramètres qui permettent à un connecteur de collecter les événements d'une unité ou d'une source de journaux. Vous pouvez utiliser des configurations enregistrées pour autoriser un certain degré de personnalisation sans qu'il soit nécessaire de créer une intégration totalement nouvelle.

Les configurations diffèrent selon le type d'intégration. Par exemple, vous pouvez enregistrer des hôtes fiables pour un connecteur Syslog ou des informations de contact de serveur WMI pour un connecteur WMI.

Les configurations enregistrées vous permettent de conserver ces ensembles de données et de les appliquer à plusieurs connecteurs. Etant donné que chaque configuration enregistrée est associée à une intégration particulière, vous ne pouvez l'utiliser que sur des connecteurs utilisant cette intégration.

Informations complémentaires

Création d'une configuration enregistrée (page 640)
Tâches liées aux intégrations et connecteurs (page 599)

Création d'une configuration enregistrée

Vous pouvez créer une configuration enregistrée et l'associer à une intégration spécifique.

Pour créer une configuration enregistrée

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

   La liste du dossier Collecte de journaux s'affiche.

2. Ouvrez le dossier Bibliothèque d'ajustement d'événement et accédez à l'intégration sur laquelle vous souhaitez créer une configuration enregistrée.

   Les détails de l'intégration s'affichent dans le volet Détails.

3. Cliquez sur Configurations enregistrées :  .

   La Liste des configurations enregistrées s'affiche.

4. Cliquez sur Créer.

   La boîte de dialogue Configuration enregistrée s'ouvre et affiche les valeurs de configuration par défaut pour l'intégration sélectionnée.

5. Entrez les valeurs de configuration souhaitées, puis cliquez sur Enregistrer et fermer.

   Un message de confirmation s'affiche.

6. Cliquez sur OK.

   La configuration enregistrée apparaît dans la liste.

Configuration en bloc de connecteurs

Vous pouvez configurer des sources de collecte d'événements en créant plusieurs connecteurs en bloc. Vous pouvez créer plusieurs connecteurs simultanément en utilisant les mêmes intégrations et les déployer sur différents agents de votre environnement.

Le processus de configuration comprend la sélection des sources d'événement, l'application des règles de suppression et de récapitulation, et la définition des configurations des connecteurs. Avant de pouvoir tirer parti de cette fonction, vous devez créer la liste des informations d'identification, telles que les noms d'hôtes et les adresses IP, des sources d'événement à configurer. Cette liste doit être au format CSV.

La configuration des sources de collecte à l'aide de l'Assistant de déploiement de connecteur en bloc se compose des étapes suivantes.

1. Ouverture de l'Assistant de déploiement de connecteur en bloc
2. Sélection des détails de la source
3. Application de règles de suppression
4. Application de règles de récapitulation
5. Configuration des paramètres des connecteurs
6. Sélection des agents et des sources de mappage

Informations complémentaires :

Ouverture de l'assistant de configuration des sources de collecte (page 641)
Sélection des détails de la source (page 643)
Application de règles de suppression (page 644)
Application de règles de récapitulation (page 644)
Configuration des connecteurs (page 645)
Sélection d'agents et mappage de sources (page 646)

Ouverture de l'assistant de configuration des sources de collecte

Pour créer des connecteurs sur des agents, vous pouvez utiliser l'Assistant de déploiement de connecteur en bloc.

Pour ouvrir l'Assistant de déploiement de connecteur en bloc

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier Explorateur d'agent, puis sur Configurer les sources de collecte : 

   L'assistant de configuration des sources de collecte s'affiche.

   Dans l'assistant

   - Cliquez sur Enregistrer pour appliquer les modifications sans fermer l'assistant. Un message de confirmation apparaît.
   - Cliquez sur Enregistrer et fermer pour appliquer les modifications et fermer l'assistant. Aucun message de confirmation n'apparaît.

Sélection des détails de la source

Sélectionnez les détails de la source et identifiez l'intégration à connecter à chaque source d'événement. Pour mener à bien cette étape, vous devez disposer de la liste des informations de sources d'événement requises au format CSV.

Remarque : Le fichier .csv contient les informations requises pour créer les connecteurs. Chaque colonne du fichier .csv identifie un champ de configuration de connecteur et contient les valeurs pour ce champ. Par exemple, le fichier peut contenir une colonne Adresse IP qui répertorie les adresses IP des hôtes à partir desquels vous voulez recevoir les événements.

La section Création d'une intégration (page 601) contient des champs de configuration spécifiques par type de détecteur de journaux.

Pour sélectionner les détails de la source

1. Ouvrez l'Assistant de déploiement de connecteur en bloc.
2. Dans la liste déroulante Intégration, sélectionnez l'intégration utilisée par vos sources.
3. Dans la liste déroulante Version, sélectionnez la version de l'intégration.
4. Naviguez jusqu'à l'emplacement d'enregistrement du fichier de source de collecte à utiliser. Le fichier de source de collecte doit être au format CSV.

   Les 100 premières lignes du fichier de source de collecte sélectionné apparaissent dans la zone Contenu des fichiers sources pour que vous puissiez les examiner. La première ligne correspond aux en-têtes de colonne et reste inchangée, même si vous modifiez la taille de l'échantillon à l'étape 5.
5. Utilisez les listes déroulantes Jusqu'à la ligne et A partir de la ligne pour réduire la portion du fichier de source de collecte à utiliser.

   Cette portion du fichier apparaît dans la zone Contenu des fichiers sources pour que vous puissiez l'examiner. Les en-têtes de colonne ne sont pas affectés par l'attribution d'une valeur supérieure à 1 dans la liste A partir de la ligne.
6. Avancez jusqu'à l'étape suivante.

Informations complémentaires :

Création d'une intégration (page 601)

Application de règles de suppression

Vous pouvez sélectionner les règles de suppression à appliquer à la modification de configuration en bloc.

Pour appliquer des règles de suppression

1. Ouvrez l'Assistant de déploiement de connecteur en bloc et avancez jusqu'à l'étape Appliquer les règles de suppression.
2. Choisissez, à l'aide du contrôle de déplacement, les règles à appliquer parmi celles disponibles.

   Remarque : Vous pouvez rechercher des règles de suppression à l'aide du champ Schéma de règle de suppression.
3. Avancez jusqu'à l'étape suivante.

Application de règles de récapitulation

Vous pouvez sélectionner les règles de récapitulation à appliquer à la modification de configuration en bloc.

Pour appliquer des règles de récapitulation

1. Ouvrez l'Assistant de déploiement de connecteur en bloc et avancez jusqu'à l'étape Appliquer les règles de récapitulation.
2. Choisissez, à l'aide du contrôle de déplacement, les règles à appliquer parmi celles disponibles.

   Remarque : Vous pouvez rechercher des règles de récapitulation à l'aide du champ Schéma de règle de récapitulation.
3. Avancez jusqu'à l'étape suivante.

Configuration des connecteurs

Vous pouvez définir des configurations de connecteur pour la création de connexion en bloc. Chaque connecteur que vous créez partage les configurations définies au cours de cette étape, soit en utilisant les sources collectées à partir du fichier .csv à l'étape 1, soit en utilisant les configurations enregistrées.

Pour définir des configurations de connecteur

1. Ouvrez l'Assistant de déploiement de connecteur en bloc et avancez jusqu'à l'étape Configuration du connecteur.

   La page affiche les champs de source définis à l'étape 1. Chaque en-tête de colonne du fichier de source apparaît en tant que champ de source. Dans la zone Configuration des détecteurs, la page affiche également les configurations par défaut des détecteurs pour l'intégration choisie.

2. Définissez la configuration du connecteur en appliquant l'une des deux méthodes ci-dessous.

   - Sélectionnez une configuration enregistrée dans la liste déroulante correspondante.
   - Définissez chaque configuration dans la zone Configuration des détecteurs en déplaçant les entrées des champs de source par glisser-déposer dans les champs de configuration qui vous intéressent. Définissez manuellement les champs requis pour lesquels aucune valeur de champ de source n'existe.

     Par exemple, la liste des sources contient une colonne UserName. Déplacez-la dans le champ Configuration de détecteur de nom d'utilisateur, s'il existe pour le type de détecteur que vous configurez.

3. Cliquez sur Répéter pour ajouter d'autres champs dans la zone Configuration des détecteurs, selon vos besoins (facultatif).
4. Avancez jusqu'à l'étape suivante.

Sélection d'agents et mappage de sources

Vous pouvez sélectionner les agents pour lesquels vous souhaitez créer les connecteurs que vous avez configurés. Mappez les sources d'événement sélectionnées à l'étape 1 avec les agents que vous voulez cibler lors du déploiement des connecteurs.

Pour sélectionner des agents et mapper des sources

1. Ouvrez l'Assistant de déploiement de connecteur en bloc et avancez jusqu'à l'étape Sélectionner les agents et mapper les sources.

   La page affiche la liste des sources en fonction des sources que vous avez téléchargées à l'étape 1. Chaque source est référencée par son numéro de ligne, c'est-à-dire que la source 1 correspond à la première ligne spécifiée dans la liste des sources.

2. Recherchez les agents à cibler par groupe d'agents, plate-forme ou nom d'agent.

3. Déplacez la ou les sources requises dans chaque dossier d'agent cible, puis cliquez pour enregistrer ce mappage de connecteur.

4. Cliquez sur Enregistrer ou sur Enregistrer et fermer.

   Les connecteurs basés sur les sources que vous avez sélectionnées sont configurés sur les agents sélectionnés.

Mise à jour des configurations de plusieurs connecteurs

Vous pouvez mettre à jour plusieurs connecteurs utilisés par le même détecteur de journaux en modifiant au moins une des configurations par défaut. Par exemple, il est possible de modifier le type de rotation du fichier journal pour plusieurs connecteurs utilisant le détecteur de journaux de fichiers.

Pour mettre à jour les configurations de plusieurs connecteurs

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Collecte de journaux.
2. La liste du dossier Collecte de journaux s'affiche.
3. Développez les dossiers Ajustement d'événement, Intégrations et Abonnement.
4. Sélectionnez une intégration qui utilise le type de détecteur de journaux auquel vous souhaitez appliquer des modifications de configuration.
5. Cliquez sur Appliquer une mise à jour par lot aux connecteurs. 

   L'assistant de mise à jour des connecteurs s'ouvre sur la page Sélectionner les connecteurs.
6. Sélectionnez les connecteurs auxquels vous souhaitez appliquer des mises à jour, puis allez à la page Configurations par défaut.
7. Entrez la valeur souhaitée dans chaque champ à mettre à jour, puis sélectionnez la case à cocher située en regard.
8. Cliquez sur Exécuter.

   Un message de confirmation apparaît.

Informations complémentaires :

Définition des configurations de journal de fichier (page 606)
Définition des configurations OPSEC (page 608)
Définition des configurations WMI (page 616)
Définition des configurations TIBCO (page 614)

Chapitre 15 : Agents

Ce chapitre traite des sujets suivants :

Planification de l'installation des agents

Lorsque vous planifiez l'installation d'agents, vous devez déterminer le nombre d'agents requis et l'emplacement d'installation. La personne qui installe les agents peut réaliser ces tâches de planification, mais celles-ci peuvent également être effectuées par un administrateur réseau ou un concepteur de systèmes informatiques.

Pour planifier des installations d'agents

1. Créez une version électronique d'un tableau de planification d'installation d'agents qui servira à répertorier toutes les informations utiles. Pensez à utiliser les exemples de tableau et de titres de colonne suivants.

Plate-forme de la source d'événement	Nom d'hôte ou adresse IP d'exécution de la source d'événement	L'une des solutions suivantes : - Sans agent - Direct - Sans agent - Point de collecte - Agent sur le terminal	Nom d'hôte ou adresse IP d'installation de l'agent

2. Identifiez chaque source d'événement à cibler pour la collecte de journaux et notez l'emplacement et la plate-forme dans votre tableau de planification des agents.

3. Tenez compte des coûts et avantages suivants de chaque type de solution.

	Avantage	Coût ou limite
Sans agent - Directement depuis CA Enterprise Log Manager - pas d'agent installé	Aucune installation d'agent requise	Prend uniquement en charge la collecte des sources d'événements compatibles avec la plate-forme du dispositif logiciel. Les coûts liés à la solution Sans agent - Point de collecte s'appliquent également.
Sans Agent - Agent au point de collecte	Aucune installation d'agent n'est requise sur l'hôte exécutant la source d'événement. La consolidation de la collecte en un point commun réduit le nombre d'agents à installer, par rapport à une collecte avec agent.	Des règles de suppression peuvent être appliquées au niveau du serveur CA Enterprise Log Manager n'est pas chiffrée. Cette solution ne présente pas l'avantage de réduire le trafic réseau. La communication des événements entre la source et le serveur CA Enterprise Log Manager n'est pas chiffrée.. Il est nécessaire de pouvoir accéder à distance à la source d'événement.
Avec agent - Agent sur le terminal	Vous pouvez appliquer des règles de suppression à la source plutôt qu'au CA Enterprise Log Manager. Cette solution réduit le trafic réseau entre le point de collecte et le serveur CA Enterprise Log Manager. La communication des événements entre la source et le serveur CA Enterprise Log Manager est chiffrée. Peut prendre en charge le volume d'événements le plus élevé des trois solutions.	Un agent doit être installé à l'emplacement d'exécution de la source d'événement.

4. Enregistrez votre solution préférée pour chaque source d'événement.
5. Triez votre tableau de planification des agents en fonction de la colonne 3, puis de la colonne 2. Ainsi s'affichent toutes les sources d'événements avec agent qui s'exécutent sur le même hôte en blocs.

6. Pour les sources d'événements que vous avez mappées vers une configuration avec agent, recherchez la première occurrence dans un bloc du même nom et copiez ces données de la colonne 2 à la colonne 4. Vous obtenez ainsi une seule entrée pour chaque hôte sur lequel une ou plusieurs sources d'événements s'exécutent. Notez que vous n'avez jamais besoin de plus d'un agent par hôte, quel que soit le nombre de sources d'événements.
7. Pour les sources d'événements que vous avez mappées vers une configuration Sans agent - Point de collecte, planifiez l'emplacement d'installation des agents comme indiqué ci-après.
    a. Identifiez le nombre de points de collecte nécessaires pour prendre en charge les sources d'événements identifiées en tant que candidats pour les agents distants.
    b. Planifiez les regroupements de sources d'événements identifiées en tant que candidats pour les agents distants par zone d'emplacement réseau commune.
    c. Pour chaque groupe de sources d'événements, identifiez le serveur à utiliser comme point de collecte. Il peut s'agir d'un serveur dédié. Enregistrez votre choix dans la colonne 4.
8. Si vous avez enregistré des sources d'événements pour lesquelles il n'existe aucune solution mappée et si vous utilisez un ancien adaptateur CA, consultez le *Manuel d'implémentation CA Enterprise Log Manager pour de plus amples détails.*
9. Transmettez les données enregistrées dans la quatrième colonne de votre tableau de planification des agents à l'utilisateur chargé d'installer les agents.

Planification de la configuration d'agents

L'utilisateur EiamAdmin installe les agents après avoir déterminé la méthode de collecte la plus appropriée. Les méthodes à sa disposition sont répertoriées ci-dessous.

- Collecte de journaux sans agent, directement à partir du serveur CA Enterprise Log Manager ; cette méthode est parfois appelée "collecte directe"
- Collecte de journaux sans agent à partir d'un point de collecte.
- Collecte de journaux avec agent à partir de l'hôte sur lequel la source d'événement s'exécute

L'analyse qui précède l'installation peut déceler certaines informations nécessaires à l'administrateur qui configure les agents et connecteurs.

La première étape de la configuration d'agents consiste à obtenir la feuille de calcul de la planification des agents auprès de l'utilisateur EiamAdmin ou tout autre moyen utilisé pour documenter l'emplacement d'installation des agents. Après avoir configuré le premier administrateur, l'utilisateur EiamAdmin fournit à celui-ci la feuille de travail annotée relative à la planification de l'installation des agents. Le premier administrateur planifie alors les connecteurs nécessaires pour chaque agent avant de commencer la configuration.

L'administrateur configure chaque agent installé par l'utilisateur EiamAdmin. Il configure également un connecteur pour chaque source d'événement, quelle que soit la méthode de collecte (Sans agent - Direct, Sans agent - Point de collecte ou Avec agent). L'administrateur configure les connecteurs sur chaque agent tout en étant connecté au serveur CA Enterprise Log Manager qui doit recevoir les événements collectés par cet agent.

Remarque : Moins les connecteurs configurés sur un agent sont nombreux, meilleures sont les performances obtenues.

Le cas d'une installation silencieuse des agents fait exception à ce processus. Dans ce cas, c'est l'installateur qui configure les connecteurs. Les connecteurs configurés sur un agent permettent à cet agent de collecter les événements bruts de sources d'événements spécifiques. Les connecteurs convertissent les événements bruts en événements ajustés et transmettent ces derniers au serveur CA Enterprise Log Manager.

La création de groupes d'agents est facultative. Si aucun groupe d'agents personnalisé n'est créé, les agents sont affectés au groupe d'agents par défaut. Les administrateurs créent des groupes d'agents pour les raisons ci-dessous.

- Activer la génération de rapports sur les événements collectés par les agents du même groupe d'agents

- Permettre l'affectation d'un autre utilisateur administratif à d'autres groupes d'agents (notez que l'accès des utilisateurs peut être limité à des groupes d'agents spécifiés à l'aide de stratégies d'accès)

Les journaux d'événements collectés sont envoyés à un serveur CA Enterprise Log Manager en vue de leur traitement et de leur stockage initial. Les administrateurs doivent configurer le serveur devant recevoir les journaux pour chaque agent ou groupe d'agents. L'affectation d'un serveur à un groupe d'agents est un moyen rapide d'affecter le serveur à tous les agents du groupe d'agents.

Planification de la collecte directe de journaux

CA Enterprise Log Manager est installé avec un agent par défaut, qui peut être utilisé pour la collecte directe de journaux. On parle de collecte directe car l'utilisation de l'agent par défaut ne nécessite aucune installation d'agent. L'agent par défaut peut collecter les événements issus de quasiment toute source d'événement, avec les limitations suivantes.

- Le détecteur de journaux doit pouvoir s'exécuter sur le dispositif logiciel ; certains détecteurs de journaux, tels que le détecteur de journaux WMI, sont liés à une plate-forme spécifique.
- Il est nécessaire de pouvoir accéder à distance à la source d'événement.

L'agent par défaut se configure de la même manière qu'un agent installé séparément. La collecte directe de journaux par l'agent par défaut convient tout particulièrement aux systèmes de très petite taille.

Sources d'événement pour la collecte directe de journaux

CA Enterprise Log Manager fournit des détecteurs de journaux qui peuvent être exécutés sur le serveur CA Enterprise Log Manager dans le but de faciliter la collecte directe de journaux sans agent. A l'heure de la publication du présent document, les technologies suivantes sont prises en charge.

- Syslog
- WinRM
- ODBC
- TIBCO

Pour déterminer les intégrations prises en charge par l'agent par défaut

1. Sélectionnez un serveur CA Enterprise Log Manager à partir de l'Explorateur d'agent, dans l'onglet Administration, sous-onglet Collecte de journaux.
2. Cliquez sur Créer un connecteur.

Le menu déroulant Intégration contient les intégrations à partir desquelles vous pouvez créer un connecteur à déployer sur l'agent par défaut. Chaque intégration, sur laquelle des connecteurs sont basés, est conçue pour récupérer des événements à partir d'une source d'événement donnée.

Pour la liste complète des intégrations et des détecteurs de journaux pris en charge, reportez-vous à la page du produit CA Enterprise Log Manager disponible sur le site du support client.

Un **détecteur de journaux** est un composant d'intégration conçu pour lire un type de journal spécifique, comme une base de données, Syslog, un fichier ou SNMP.

Planification de la collecte de journaux sans agent

La collecte de journaux sans agent peut être implémentée en installant un agent sur un serveur de collecte qui traite les événements de plusieurs sources d'événements distantes.

Tenez compte des éléments ci-dessous lorsque vous planifiez la configuration d'une collecte de journaux sans agent à partir d'un serveur de collecte.

- Moins les connecteurs déployés sur un agent sont nombreux, meilleures sont les performances obtenues.
- Le nombre maximal de connecteurs à configurer sur un agent donné varie selon que l'agent est installé ou non sur un serveur dédié, selon la puissance de ce serveur et selon les types de sources d'événements ciblées. De manière générale, veillez à ne pas configurer plus de quarante ou cinquante connecteurs sur un même agent.
- Vous ne tirerez aucun bénéfice en termes de performances en regroupant sur le même serveur de collecte des connecteurs du même type configurés sur différents agents. Par extension, vous n'obtiendrez aucun gain de performance en dirigeant les événements de mêmes types de sources d'événements vers un serveur CA Enterprise Log Manager donné d'une fédération.

Planification de la collecte de journaux avec agent

Une fois un agent installé sur un serveur avec des sources d'événements locales, les administrateurs configurent un connecteur sur cet agent pour chaque source d'événement s'exécutant au niveau local.

Si vous disposez de plusieurs serveurs cibles avec les mêmes types de sources d'événements, envisagez de regrouper ces serveurs cibles en un groupe d'agents et d'effectuer la configuration au niveau du groupe d'agents.

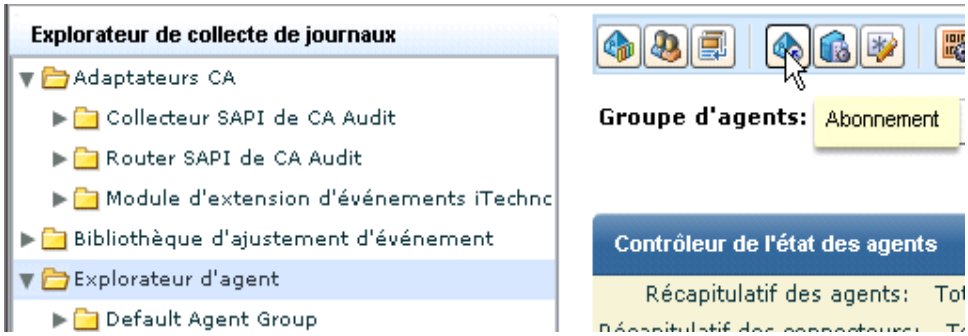
La remise garantie peut poser problème pour la collecte directe de Syslogs. Pour y remédier, configurez un écouteur Syslog sur un agent installé avec la source d'événement Syslog.

Sélection du niveau à configurer

Les options Abonnement, Appliquer les règles de suppression et Etat et commande peuvent être sélectionnées depuis différents niveaux. Par exemple, la configuration de l'abonnement peut s'effectuer depuis les niveaux suivants.

- Explorateur d'agent
- Groupe d'agents par défaut ou défini par l'utilisateur
- Agent

Pour configurer une option de manière à ce qu'elle s'applique à tous les agents de tous les groupes, sélectionnez Explorateur d'agent et cliquez sur le bouton de l'action que vous souhaitez effectuer.



Pour configurer une option de manière à ce qu'elle s'applique à tous les agents d'un groupe donné, sélectionnez le nom du groupe, puis cliquez sur le bouton de l'action que vous souhaitez effectuer.

Pour configurer une option de manière à ce qu'elle s'applique à un seul agent, sélectionnez cet agent et cliquez sur le bouton de l'action que vous souhaitez effectuer.

Tâches de gestion des agents

L'Explorateur d'agent vous permet d'afficher et de gérer les agents de collecte d'événements de votre environnement. Vous pouvez utiliser l'interface de l'Explorateur d'agent pour effectuer des tâches de gestion dans les domaines ci-dessous.

- Configuration d'agent : vous permet de renommer les agents et de configurer les groupes auxquels ils appartiennent, ainsi que les groupes associés.
- Groupes d'agents : vous permettent de regrouper les agents, par zone géographique, importance de l'entreprise ou type de source d'événement, par exemple. Vous pouvez également attribuer des agents regroupés à différents serveurs CA Enterprise Log Manager, suivant vos besoins.
- Abonnements : vous permettent d'afficher et d'appliquer les mises à jour disponibles aux agents.
- Etat et commandes d'agent : vous permettent d'afficher l'état actuel des agents et de les arrêter/démarrer si nécessaire.

Informations complémentaires

Affichage et contrôle de l'état d'un agent ou d'un connecteur (page 664)
Téléchargement des fichiers binaires de l'agent (page 659)
Mise à jour de la clé d'authentification d'un agent (page 658)
Création d'un groupe d'agents (page 665)
Application des mises à jour d'abonnement (page 675)
Configuration de la gestion des agents (page 668)

Mise à jour de la clé d'authentification d'un agent

Vous pouvez afficher et mettre à jour la clé utilisée par les agents pour s'enregistrer auprès du serveur CA Enterprise Log Manager. En modifiant régulièrement cette clé, vous empêchez l'installation d'agents non autorisés dans votre environnement. Par défaut, la clé est la même pour tous les serveurs CA Enterprise Log Manager de l'ensemble des instances d'application. Toutefois, vous pouvez définir une clé unique pour chaque instance d'application.

Le programme d'installation de l'agent doit entrer la clé de l'agent dans le champ Code d'authentification de l'assistant d'installation de l'agent.

Pour mettre à jour la clé d'authentification d'un agent

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier de l'Explorateur d'agent.

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

3. Cliquez sur Clé d'authentification d'agent :  .

   Le volet Clé d'authentification d'agent s'affiche.

4. Saisissez une nouvelle clé dans les champs Saisie clé et Confirmation clé, puis cliquez sur Enregistrer.

   Un message de confirmation d'opération s'affiche.

Téléchargement des fichiers binaires de l'agent

Vous pouvez télécharger les fichiers binaires de l'agent et les installer sur votre ordinateur local sans utiliser d'autres supports d'installation.

Pour plus d'informations sur l'installation d'un agent, consultez le *Manuel d'installation des agents CA Enterprise Log Manager*.

Pour télécharger les fichiers binaires de l'agent

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier de l'Explorateur d'agent.

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

3. Cliquez sur Télécharger des fichiers binaires d'agent : 

   La liste des fichiers binaires de l'agent apparaît, répertoriant les agents disponibles et leur version actuelle.

4. Cliquez sur l'agent à télécharger.

   La boîte de dialogue de téléchargement s'affiche.

5. Sélectionnez l'emplacement d'enregistrement du fichier binaire de l'agent, puis cliquez sur Enregistrer.

   Le fichier est enregistré à l'emplacement souhaité et un message de confirmation apparaît.

Configuration d'un agent

Vous pouvez configurer un agent installé et enregistré après y avoir accédé via l'Explorateur d'agent.

Pour configurer un agent

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier de l'Explorateur d'agent.

   Le dossier se développe et affiche les dossiers Groupe d'agents.

3. Sélectionnez l'agent que vous souhaitez configurer, puis cliquez sur Modifier, en haut du volet.

   Les détails relatifs à l'agent s'affichent dans le volet Détails.

4. Apportez les modifications souhaitées, notamment celles répertoriées ci-dessous.

   Nom d'utilisateur

   Définit le nom d'utilisateur sous lequel l'agent est exécuté.

   Port

   Indique le port que l'agent utilise pour communiquer avec CA Enterprise Log Manager.

   Groupe d'agents

   Définit le groupe auquel l'agent appartient.

   Nombre maximum de fichiers

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

   Taille maximum par fichier

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

Mode d'envoi des événements

Définit l'un des styles de transmission suivants que l'agent utilisera :

- Basculement : l'agent envoie des événements au premier serveur de la liste de serveurs du gestionnaire de journaux. Si la communication est interrompue, il essaie alors de communiquer avec chaque serveur dans l'ordre indiqué, jusqu'à ce que la communication soit rétablie.
- Round Robin : l'agent envoie à son tour des événements à chaque serveur de la liste de serveurs du gestionnaire de journaux, dans le but de contacter le prochain serveur de la liste après un délai d'une heure. Cette période n'est pas configurable.

Activer le chiffrement d'événements

Paramètre l'agent de sorte qu'il utilise le protocole AES128 pour chiffrer les événements qu'il transmet. L'activation du chiffrement des événements affectera les performances.

Activer la planification de distribution

Paramètre l'agent de sorte qu'il envoie des événements uniquement dans un intervalle de temps défini. Si vous cochez la case Activer la planification de distribution, les champs Heure de début et Heure de fin s'afficheront. Saisissez les valeurs de l'heure GMT de votre choix au format 24 heures, en respectant les instructions suivantes :

- L'heure de début et l'heure de fin doivent différer d'une heure.
- Si la valeur de l'heure de début est supérieure à celle de l'heure de fin, l'heure de fin sera définie pour le jour suivant. Par exemple, si vous définissez l'heure de début sur 23, et l'heure de fin sur 6, l'intervalle de transmission sera compris entre 23h00 GMT et 6h00 GMT le jour suivant.

Serveurs du gestionnaire de journaux

Contrôle les serveurs CA Enterprise Log Manager vers lesquels l'agent achemine les événements, ainsi que l'ordre dans lequel ils sont contactés. Vous pouvez utiliser le contrôle de déplacement pour sélectionner les serveurs disponibles et les boutons fléchés, situés à droite des serveurs sélectionnés, pour définir la priorité de communication.

Remarque : Mettez à jour vos serveurs CA Enterprise Log Manager avant de mettre à jour les agents. Les serveurs CA Enterprise Log Manager prennent en charge les agents à leur numéro de version actuel ou précédent. Pour que le stockage des événements collectés s'effectue correctement lors de la configuration ou de la mise à jour des agents, vérifiez que l'agent envoie les événements uniquement aux serveurs CA Enterprise Log Manager de même niveau que l'agent ou de niveau supérieur.

5. Cliquez sur Enregistrer.

Informations complémentaires

Affichage et contrôle de l'état d'un agent ou d'un connecteur (page 664)
Création d'un groupe d'agents (page 665)

Manipulation des fichiers de configuration utilisés

Les agents utilisent un fichier de configuration stocké en mémoire quand ils s'exécutent. Si une personne utilise un fichier de configuration alors que l'agent est en cours d'exécution, l'agent n'utilisera pas le fichier occupé. Quand un agent reçoit une nouvelle configuration du serveur CA Enterprise Log Manager, l'agent remplace le fichier du disque par le fichier reçu avant le redémarrage. De cette façon, un fichier utilisé est automatiquement remplacé par le bon fichier.

Si une personne redémarre l'agent à partir d'une source externe après avoir utilisé le fichier, l'agent détecte que ce fichier est utilisé et se ferme. L'agent n'accepte pas les données de configuration, notamment celles de la liste de serveurs CA Enterprise Log Manager provenant du fichier occupé.

L'Explorateur d'agent affiche que l'agent ne répond pas. Utilisez l'état du serveur CA Enterprise Log Manager et les outils de commande pour réinitialiser la configuration de l'agent. L'agent reprend son activité normalement après cette action.

Affichage du tableau de bord des agents

Vous pouvez afficher le tableau de bord des agents, qui regroupe les agents de votre environnement accompagnés de diverses informations d'utilisation telles que le nombre d'événements reçus par seconde, le pourcentage d'utilisation de l'UC, et la date et l'heure de la dernière mise à jour.

Pour afficher le tableau de bord des agents

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

   La liste du dossier Collecte de journaux s'affiche.

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

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

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

   Le panneau de recherche d'agents apparaît et affiche l'état de tous les agents disponibles dans un graphique détaillé. comme les exemples ci-dessous.

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

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

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

5. Cliquez sur Afficher l'état.

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

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

Affichage et contrôle de l'état d'un agent ou d'un connecteur

Dans votre environnement, vous pouvez surveiller l'état d'agents ou de connecteurs, redémarrer les agents, ou encore démarrer, arrêter et redémarrer les connecteurs, le cas échéant.

Vous pouvez afficher les agents ou les connecteurs des différents niveaux de la hiérarchie de dossiers de l'Explorateur d'agent. Chaque niveau restreint l'affichage disponible en conséquence.

- Depuis le dossier Explorateur d'agent, vous pouvez afficher tous les agents ou connecteurs affectés au serveur CA Enterprise Log Manager actuel.
- Depuis le dossier d'un groupe d'agents spécifique, vous pouvez afficher les agents et connecteurs affectés à ce groupe d'agents.
- Depuis un agent spécifique, vous pouvez afficher cet agent uniquement et les connecteurs qui lui sont affectés.

Pour afficher l'état d'un agent ou d'un connecteur

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

   La liste du dossier Collecte de journaux s'affiche.

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

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

3. Cliquez sur Etat et commande  .

   Le panneau d'état s'affiche.

4. Sélectionnez Agents ou Connecteurs.

   Le panneau de recherche d'agents ou de connecteurs s'affiche.

5. Sélectionnez les critères de recherche de mise à jour d'agent ou de connecteur (facultatif). Si vous n'entrez aucun terme de recherche, toutes les mises à jour disponibles s'affichent. Vous pouvez sélectionner un ou plusieurs critères ci-dessous pour restreindre votre recherche.

   - Groupe d'agents : renvoie uniquement les agents et les connecteurs affectés au groupe sélectionné.
   - Plate-forme : renvoie uniquement les agents et les connecteurs s'exécutant sur le système d'exploitation sélectionné.
   - Schéma de nom de l'agent : renvoie uniquement les agents et les connecteurs contenant le schéma spécifié.
   - Intégration (connecteurs uniquement) : renvoie uniquement les connecteurs qui utilisent l'intégration sélectionnée.

6. Cliquez sur Afficher l'état.

   Le graphique de détails qui s'affiche indique les agents ou les connecteurs correspondant à votre recherche. comme les exemples ci-dessous.

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

7. Cliquez sur l'état pour afficher les détails dans le volet Etat, au bas du graphique (facultatif).

   Remarque : Vous pouvez cliquer sur le bouton A la demande d'un agent ou d'un connecteur pour actualiser l'affichage de l'état.

8. Si vous affichez des connecteurs, sélectionnez l'un d'entre eux et cliquez sur Redémarrer, Démarrer ou Arrêter (facultatif). Si vous affichez des agents, sélectionnez n'importe quel agent et cliquez sur Redémarrer.

Informations complémentaires :

Création d'un groupe d'agents (page 665)
Application des mises à jour d'abonnement (page 675)

Création d'un groupe d'agents

Vous pouvez créer un groupe d'agents pour organiser vos agents suivant leur emplacement, leur système d'exploitation ou toute autre catégorie pertinente. Le processus de création d'un groupe d'agents à l'aide de l'assistant de groupe d'agents comporte les étapes ci-dessous.

1. Ouverture de l'assistant de groupe d'agents
2. Saisie des détails du groupe
3. Ajout d'agents

Informations complémentaires

Ouverture de l'assistant de groupe d'agents (page 666)
Ajout de détails à un groupe d'agents (page 666)
Ajout d'agents à un groupe d'agents (page 667)

Ouverture de l'assistant de groupe d'agents

Pour créer un groupe d'agents ou modifier un groupe existant, ouvrez l'assistant de groupe d'agents.

Pour ouvrir l'assistant de groupe d'agents

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier de l'Explorateur d'agent.

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

3. Cliquez sur Nouveau groupe d'agents :  .

   L'assistant de groupe d'agents s'affiche.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer le fichier sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer le fichier et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Ajout de détails à un groupe d'agents

Vous pouvez ajouter des informations d'identification à votre groupe d'agents.

Pour ajouter des détails à un groupe d'agents

1. Ouvrez l'assistant de groupe d'agents.
2. Saisissez un nom pour le groupe et une description (facultative) pour référence.
3. Passez à l'étape suivante ou cliquez sur Enregistrer et fermer.

   Si vous cliquez sur Enregistrer et fermer, le groupe est créé. Sinon, l'étape choisie apparaît.

Ajout d'agents à un groupe d'agents

Vous pouvez ajouter des agents à un groupe, à des fins administratives. Vous pouvez par exemple créer des groupes par région géographique ou par système d'exploitation.

Remarque : Les agents n'héritent *pas* des propriétés du groupe. Ainsi, lorsque vous ajoutez des agents à un groupe existant, vous devez affecter manuellement les propriétés du groupe, comme les règles de suppression, au nouvel agent.

Pour ajouter des agents à un groupe

1. Ouvrez l'assistant de groupe d'agents et avancez jusqu'à l'étape Agents.
2. Sélectionnez les critères de recherche d'agent (facultatif). Si vous n'entrez aucun terme de recherche, tous les agents s'affichent. Vous pouvez sélectionner un ou plusieurs critères ci-dessous pour restreindre votre recherche.
   - Groupe d'agents : renvoie uniquement les agents affectés au groupe sélectionné.
   - Plate-forme : renvoie uniquement les agents s'exécutant sur la plate-forme sélectionnée.
   - Schéma de nom de l'agent : renvoie uniquement les agents contenant le schéma spécifié.
3. Cliquez sur Rechercher.

   Les agents correspondant à votre recherche s'affichent dans la zone Agents disponibles.
4. A l'aide du contrôle de déplacement, sélectionnez les agents que vous souhaitez ajouter, puis, à l'aide des flèches haut et bas, placez-les dans l'ordre souhaité d'apparition dans l'affichage du groupe d'agents
5. Cliquez sur Enregistrer et fermer.

   Le groupe d'agents apparaît dans la liste.

Configuration de la gestion des agents

Vous pouvez configurer vos agents ou vos groupes d'agents afin qu'ils soient affectés à des serveurs CA Enterprise Log Manager différents, dans votre environnement fédéré. Cela vous permet de configurer les groupes ou les agents pour qu'ils envoient les informations d'événement vers les serveurs CA Enterprise Log Manager choisis.

La procédure de configuration de la gestion des agents, qui s'effectue par le biais de l'assistant d'affectation des serveurs du gestionnaire de journaux, se compose des étapes suivantes.

1. Ouverture de l'assistant d'affectation des serveurs du gestionnaire de journaux
2. Sélection des agents ou groupes d'agents cibles à affecter
3. Sélection des serveurs CA Enterprise Log Manager auxquels seront affectés les agents ou les groupes

Informations complémentaires :

Ouverture de l'assistant d'affectation des serveurs du gestionnaire de journaux (page 669)
Sélection des agents cibles (page 670)
Sélection des gestionnaires de journaux (page 670)

Ouverture de l'assistant d'affectation des serveurs du gestionnaire de journaux

Pour configurer l'affectation d'agents ou de groupes d'agents, ouvrez l'assistant d'affectation des serveurs du gestionnaire de journaux.

Pour ouvrir l'assistant d'affectation des serveurs du gestionnaire de journaux

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

   La liste du dossier Collecte de journaux s'affiche ; elle contient les boutons de gestion des agents dans le volet Détails.

2. Cliquez sur Serveurs du gestionnaire de journaux : 

   L'assistant d'affectation des serveurs du gestionnaire de journaux s'affiche.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer l'affectation et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Informations complémentaires :

Configuration de la gestion des agents (page 668)
Sélection des agents cibles (page 670)
Sélection des gestionnaires de journaux (page 670)

Sélection des agents cibles

Pour affecter des agents à un serveur, à des fins de réception d'événements et d'archivage, vous devez choisir quel agent ou groupe d'agents affecter à un serveur CA Enterprise Log Manager donné.

Pour sélectionner les agents cibles

1. Ouvrez l'assistant d'affectation des serveurs du gestionnaire de journaux.
2. Indiquez si vous souhaitez affecter les agents en groupe ou individuellement.
3. Si vous choisissez l'option Groupes, utilisez le contrôle de déplacement pour sélectionner les groupes à affecter. Vous pouvez utiliser le champ d'entrée Rechercher pour localiser les groupes souhaités en saisissant une partie du nom. Les groupes disponibles sont filtrés au fur et à mesure de la saisie.
4. Si vous choisissez l'option Agents, utilisez le contrôle de déplacement pour sélectionner les agents individuels à affecter. Vous pouvez utiliser les listes déroulantes Groupe d'agents et Plate-forme, ainsi que le champ d'entrée Rechercher, pour localiser les agents souhaités.
5. Avancez jusqu'à l'étape Sélection des gestionnaires de journaux.

Informations complémentaires :

Configuration de la gestion des agents (page 668)
Ouverture de l'assistant d'affectation des serveurs du gestionnaire de journaux (page 669)
Sélection des gestionnaires de journaux (page 670)

Sélection des gestionnaires de journaux

Vous devez choisir à quel serveur CA Enterprise Log Manager seront affectés les agents ou groupes d'agents définis.

Pour sélectionner les serveurs du gestionnaire de journaux

1. Ouvrez l'assistant d'affectation des serveurs du gestionnaire de journaux, choisissez les agents cibles, puis avancez jusqu'à l'étape Sélection des gestionnaires de journaux.
2. Utilisez le contrôle de déplacement pour sélectionner les serveurs auxquels vous souhaitez affecter les agents ou les groupes d'agents. Vous pouvez utiliser le champ d'entrée Schéma de nom pour accéder à la liste des serveurs disponibles.
3. Cliquez sur Enregistrer et fermer.

   Les agents ou groupes d'agents sont affectés aux serveurs sélectionnés.

Informations complémentaires :

Configuration de la gestion des agents (page 668)
Ouverture de l'assistant d'affectation des serveurs du gestionnaire de journaux (page 669)
Sélection des agents cibles (page 670)

Protection des agents en cas de modification de l'adresse IP du serveur

Lorsque vous installez un agent, vous lui affectez un serveur CA Enterprise Log Manager principal qu'il doit contacter en premier après avoir collecté des événements. Lorsque vous configurez un agent, vous ajoutez d'autres serveurs CA Enterprise Log Manager dans une liste hiérarchisée. Lorsqu'un agent est prêt à envoyer les journaux collectés au serveur principal, mais que ce dernier est inaccessible, l'agent contacte chaque serveur secondaire de la liste, jusqu'à en trouver un disponible. Définir une liste hiérarchisée de serveurs secondaires garantit la remise des journaux de l'agent vers le serveur. Un agent peut envoyer des événements à un seul serveur CA Enterprise Log Manager à la fois, c'est-à-dire sans duplication des événements.

Lorsqu'une nouvelle adresse IP est attribuée aux serveurs sélectionnés pour la gestion de l'agent, la capacité de ce dernier à transférer les événements collectés à un serveur de la liste peut en être affectée. En prenant certaines précautions, vous pouvez garantir un haut niveau de disponibilité des serveurs, même en cas de réaffectation manuelle ou dynamique des adresses IP.

L'adresse IP d'un serveur CA Enterprise Log Manager installé peut être modifiée dans les cas suivants.

- Réattribution automatique par DHCP

  Le serveur CA Enterprise Log Manager d'un système à un seul serveur est configuré avec une attribution automatique de son adresse IP par DHCP. Après que le serveur a été choisi pour la gestion d'agents, DHCP lui attribue une nouvelle adresse IP. Cette opération peut avoir lieu lorsque le serveur CA Enterprise Log Manager est hors ligne pendant suffisamment longtemps pour que le bail de l'adresse IP arrive à expiration. L'utilisateur n'est pas averti lorsque l'adresse IP est modifiée de manière dynamique.

- Réattribution manuelle

  Les serveurs CA Enterprise Log Manager sont configurés avec des adresses IP statiques. En raison d'un processus de site au cours duquel les adresses IP sont réattribuées dans le cadre du déploiement d'un nouveau sous-réseau, les nouvelles adresses IP sont attribuées manuellement à chaque serveur CA Enterprise Log Manager.

Prenez les mesures appropriées pour garantir la disponibilité des serveurs lors de la modification de leur adresse IP dans de telles conditions.

Informations complémentaires :

Disponibilité garantie des serveurs dotés d'adresses IP dynamiques (page 673)
Disponibilité garantie pour les serveurs lors de la réattribution des adresses IP statiques (page 673)

Disponibilité garantie des serveurs dotés d'adresses IP dynamiques

Si vous sélectionnez DHCP lors de l'installation d'un serveur CA Enterprise Log Manager unique, spécifiez le nom d'hôte (non pas l'adresse IP) de ce serveur CA Enterprise Log Manager lors de l'installation de chaque agent. Cela garantit que toute réattribution par DHCP de l'adresse IP du serveur CA Enterprise Log Manager n'aura pas d'impact sur les agents qui l'utilisent.

Si vous spécifiez l'adresse IP du serveur CA Enterprise Log Manager lors de l'installation des agents et que cette adresse IP dynamique change, vous devrez réinstaller les agents pour restaurer la disponibilité du serveur CA Enterprise Log Manager unique. Pour éviter ce problème, nous vous recommandons d'installer un serveur CA Enterprise Log Manager supplémentaire et de l'ajouter en tant que serveur secondaire pour tous les agents. Cela garantit une haute disponibilité des serveurs.

Disponibilité garantie pour les serveurs lors de la réattribution des adresses IP statiques

Si vous installez les serveurs CA Enterprise Log Manager avec des adresses IP statiques et que vous prévoyez ultérieurement de modifier ces adresses, observez la procédure suivante pour garantir aux agents une disponibilité continue des serveurs figurant dans leur liste hiérarchisée. Il n'est pas nécessaire de redémarrer l'agent après chaque étape, car l'agent actualise automatiquement ses données de configuration toutes les 5 minutes par défaut.

Important : Si l'agent est configuré avec un seul serveur CA Enterprise Log Manager dans un système comptant plusieurs serveurs, veillez à ajouter un second serveur à la liste hiérarchisée avant d'attribuer une nouvelle adresse IP. Dans le cas contraire, vous aurez peut-être à réinstaller et à reconfigurer l'agent après modification de l'adresse IP du serveur, pour rétablir la disponibilité de ce dernier.

Pour vous assurer que les agents pourront accéder à l'un des serveurs CA Enterprise Log Manager de leur liste hiérarchisée lors de la réattribution des adresses IP statiques des serveurs

1. Si vous prévoyez de réattribuer l'adresse IP d'un serveur CA Enterprise Log Manager, et que celui-ci est l'unique serveur CA Enterprise Log Manager, installez un serveur CA Enterprise Log Manager temporaire pointant vers le CA EEM du serveur CA Enterprise Log Manager original.

2. Si aucun serveur CA Enterprise Log Manager supplémentaire n'a été configuré pour les agents d'un système comptant plusieurs serveurs, affectez au moins un serveur supplémentaire à la liste hiérarchisée.
   a. Sélectionnez Explorateur d'agent, puis cliquez sur Serveurs du gestionnaire de journaux.

      L'assistant d'affectation des serveurs du gestionnaire de journaux s'ouvre sur l'étape Sélection des cibles.

   b. Sélectionnez Agents ou Groupes, suivant la façon dont vous souhaitez effectuer l'attribution.

   c. Sélectionnez les agents ou les groupes cibles dans la liste Disponible(s) et déplacez-les dans la liste Sélectionné(s).

   d. Cliquez sur l'étape Sélection des serveurs du gestionnaire de journaux.

   e. Sélectionnez un serveur CA Enterprise Log Manager dans la liste Disponible(s) et déplacez-le dans la liste Sélectionné(s).

   f. Cliquez sur Enregistrer et fermer.
3. Retirez la moitié de la liste hiérarchisée de serveurs CA Enterprise Log Manager de la configuration de l'agent ou du groupe d'agents, à l'aide de l'assistant d'affectation des serveurs du gestionnaire de journaux.
4. Attribuez les nouvelles adresses IP statiques aux serveurs retirés de la liste.
5. Replacez dans la liste les serveurs dotés de nouvelles adresses IP.
6. Attendez que l'agent actualise ses informations de configuration.

   Remarque : Vous pouvez redémarrer manuellement l'agent pour actualiser immédiatement sa configuration.
7. Retirez l'autre moitié de la liste hiérarchisée.

   Remarque : Si vous avez ajouté un serveur temporaire, vous pouvez le conserver à des fins de basculement ou le désinstaller et le supprimer.
8. Réattribuez les adresses IP.
9. Replacez les serveurs dans la liste pour restaurer la liste hiérarchisée originale.

Informations complémentaires :

Configuration de la gestion des agents (page 668)
Suppression d'un hôte de service (page 142)

Application des mises à jour d'abonnement

Vous pouvez appliquer des mises à jour d'abonnement CA à des agents ou connecteurs. Le processus d'application des packages d'abonnement à l'aide de l'assistant de liste de mises à jour comporte les étapes ci-dessous.

1. Ouverture de l'assistant de liste de mises à jour
2. Sélection de l'un des types de mise à jour suivants et définition des critères de recherche pour les packages de mise à jour disponibles
   - Mises à jour de l'agent
   - Mises à jour d'intégration pour les connecteurs

   Remarque : Si des mises à jour d'agent et de connecteur sont disponibles, vous devez d'abord appliquer les mises à jour d'agent pour que le processus se déroule correctement.
3. Sélection des agents ou connecteurs à mettre à jour avec la dernière version disponible

Informations complémentaires

Ouverture de l'assistant de liste de mises à jour (page 676)
Sélection d'agents ou de connecteurs pour mise à jour (page 677)
Mise à jour des versions d'intégration d'un agent ou d'un connecteur (page 678)
Affichage et contrôle de l'état d'un agent ou d'un connecteur (page 664)

Ouverture de l'assistant de liste de mises à jour

Pour mettre à jour les agents ou les connecteurs avec la version la plus récente, ouvrez l'assistant de liste de mises à jour.

Pour ouvrir l'assistant de liste de mises à jour

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

   La liste du dossier Collecte de journaux s'affiche.

2. Cliquez sur le dossier de l'Explorateur d'agent.

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

3. Cliquez sur Abonnement :  .

   L'assistant de liste de mises à jour s'ouvre.

   Dans l'assistant

   - Cliquez sur Enregistrer pour enregistrer sans fermer l'assistant.
   - Cliquez sur Enregistrer et fermer pour enregistrer votre progression et fermer l'assistant.
   - Cliquez sur Réinitialiser pour restaurer les derniers paramètres enregistrés.

Sélection d'agents ou de connecteurs pour mise à jour

Vous pouvez vérifier la disponibilité des mises à jour en indiquant des critères de recherche pour les agents ou les connecteurs concernés.

Pour sélectionner des agents ou des connecteurs pour mise à jour

1. Ouvrez l'assistant de liste de mises à jour.

   La Liste de sélection des mises à jour s'affiche.

2. Sélectionnez Mises à jour de l'agent ou Mises à jour du connecteur.

   Remarque : Si des mises à jour d'agent et de connecteur sont disponibles, vous devez d'abord appliquer les mises à jour d'agent pour que le processus se déroule correctement.

3. Finalisez les critères de recherche de mise à jour pour l'agent ou le connecteur.

   a. Sélectionnez un groupe d'agents dans la liste déroulante.

   b. Sélectionnez une plate-forme dans la liste déroulante.

   c. Saisissez le schéma de nom de l'agent, avec des caractères génériques.

   d. (Mises à jour d'intégration de connecteur uniquement) Sélectionnez une intégration dans la liste déroulante.

4. Cliquez sur Rechercher.

   Les packages de mise à jour correspondant à vos critères de recherche s'affichent dans l'étape suivante de l'assistant, intitulée Sélection de version. Vous devez passer à cette étape pour afficher et appliquer les mises à jour.

Informations complémentaires

Ouverture de l'assistant de liste de mises à jour (page 676)
Mise à jour des versions d'intégration d'un agent ou d'un connecteur (page 678)

Mise à jour des versions d'intégration d'un agent ou d'un connecteur

Vous pouvez comparer la version de chaque agent ou connecteur répertorié avec les versions de mise à jour téléchargées, afin de déterminer si une mise à jour est nécessaire ou non. Vous devez alors indiquer si la version en cours doit être remplacée par une version différente.

Pour mettre à jour des agents ou des connecteurs

1. Ouvrez l'assistant de liste de mises à jour et sélectionnez les agents ou connecteurs pour lesquels vous envisagez une mise à jour.
2. Avancez jusqu'à l'étape Sélection de version.

   La liste des agents ou connecteurs répondant à vos critères de recherche s'affiche.

   - Chaque agent est accompagné de sa version actuelle et d'une liste déroulante indiquant les versions disponibles pour la mise à jour.
   - Chaque connecteur est accompagné de sa version d'intégration actuelle et d'une liste déroulante indiquant les versions disponibles pour la mise à jour.
3. Sélectionnez Omettre la version du SE pour afficher toutes les mises à jour disponibles pour le système d'exploitation sélectionné, quelle qu'en soit la version (facultatif).
4. Sélectionnez les agents ou les connecteurs auxquels vous souhaitez appliquer les mises à jour, puis cliquez sur Enregistrer et fermer.

   L'agent installe les mises à jour, en remplaçant la version actuelle par la mise à jour d'agent ou d'intégration sélectionnée.

Remarque : Vous pouvez vérifier que tous les agents ou connecteurs disposent de la dernière version, en passant en revue les détails correspondants une fois la mise à jour appliquée.

Chapitre 16 : Certificats personnalisés

Ce chapitre traite des sujets suivants :

Mise en oeuvre de certificats personnalisés

Le processus d'installation génère deux certificats et les place dans le répertoire /opt/CA/SharedComponents/iTechnology du serveur CA Enterprise Log Manager. Vous pouvez utiliser les certificats installés tels quels. Ces certificats possèdent les noms suivants, où *ApplicationName* est CAELM pour le produit CA Enterprise Log Manager.

- *ApplicationName*Cert.p12

  Ce certificat est utilisé par tous les services CA Enterprise Log Manager pour communiquer avec le serveur de gestion. L'entrée pour ce certificat existe également dans le fichier CALM.cnf.

- *ApplicationName*_AgentCert.p12

  Ce certificat est utilisé par tous les agents afin de communiquer avec le serveur CA Enterprise Log Manager.

  Important : Le remplacement du certificat CAELM_AgentCert.p12 par un certificat personnalisé situé dans un environnement muni d'agents actifs nécessite la réinstallation de ces agents.

Pour utiliser des certificats personnalisés, vous devez tout d'abord obtenir un certificat de racine sécurisée auprès d'une autorité de certification de racine. Une autorité de certification peut émettre plusieurs certificats sous la forme d'une arborescence. Tous les certificats conformes au certificat de racine sécurisée héritent de la fiabilité du certificat de la racine. Ce processus suppose que si les deux certificats sont remplacés, le certificat de service personnalisé et le certificat d'agent personnalisé possèdent la même racine sécurisée.

Seuls les certificats personnalisés portant une extension p12 sont pris en charge. Après avoir obtenu un certificat de racine sécurisée, les actions typiques pour implémenter des certificats personnalisés sont les suivantes :

1. Ajoutez le certificat de racine sécurisée à iAuthority.conf sur le serveur CA Enterprise Log Manager de gestion ou le serveur CA EEM autonome.
2. Si vous remplacez CAELM_AgentCert.p12, ajoutez le certificat de racine sécurisée à iControl.conf sur le serveur de gestion CA Enterprise Log Manager, puis répétez cet ajout sur les autres serveurs CA Enterprise Log Manager.
3. Si vous remplacez CAELMCert.p12, ajoutez ce nom commun de certificat personnalisé à la stratégie de portée AdministerObjects du serveur de gestion CA Enterprise Log Manager ou du serveur autonome CA EEM.
4. Ajoutez les certificats personnalisés au dossier iTechnology de chaque serveur CA Enterprise Log Manager et ajoutez le nom et le mot de passe de chaque certificat dans des fichiers de configuration distincts.

Informations complémentaires :

Ajoutez le certificat de racine sécurisée au serveur de gestion CA Enterprise Log Manager (page 680)
Ajoutez le certificat de racine sécurisée à tous les autres serveurs CA Enterprise Log Manager (page 682)
Ajout d'un nom commun de certificat à une stratégie d'accès (page 683)
Déploiement de nouveaux certificats (page 684)

Ajoutez le certificat de racine sécurisée au serveur de gestion CA Enterprise Log Manager

Tout d'abord, vous obtenez un certificat de racine sécurisée au format PEM auprès de l'autorité de certification. Puis, ajoutez ce certificat à l'interface Web iTechnology SPIN du serveur de gestion ou autonome CA EEM.

Pour ajouter le certificat de racine sécurisée au serveur de gestion CA Enterprise Log Manager, procédez comme suit :

1. Accédez à l'interface Web CA iTechnology SPIN du serveur de gestion CA Enterprise Log Manager ou du serveur autonome CA EEM.

   https://<nomhôte_serveurgestion_ELM>:5250/spin/

   https://<nomhôte_EEM>:5250/spin/

   La page CA iTechnology SPIN apparaît.
2. Sélectionnez Administrateur iTech dans la liste déroulante, puis cliquez sur OK.

   La page d'administration iTechnology affiche un lien de connexion.

3. Cliquez sur Connexion.

   La boîte de dialogue de connexion CA iTechnology s'affiche.

4. Saisissez les identifiants de connexion EiamAdmin, sélectionnez iAuthority, puis cliquez sur Connexion.

5. Sélectionnez l'onglet iAuthority et ajoutez la racine sécurisée à iAuthority.conf comme indiqué ci-dessous :

   a. Saisissez une étiquette pour le certificat. Ne saisissez pas "moi-même" comme étiquette.

   b. Parcourez la liste et sélectionnez le fichier PEM racine.

   c. Cliquez sur Ajouter une racine sécurisée.

   Le message de confirmation indique que le certificat de racine sécurisée a été ajouté à iAuthority.conf, un fichier qui n'existe que sur le serveur de gestion ou le serveur autonome CA EEM.

6. Si vous utilisez un serveur autonome CA EEM, passez à la dernière étape.

7. Si vous remplacez le certificat CAELM_AgentCert.p12 par un certificat personnalisé, ajoutez le certificat de racine sécurisée à iControl.conf comme suit :

   a. Sélectionnez l'onglet Configurer.

   b. Saisissez la même étiquette pour le certificat que celle saisie à l'étape précédente.

   c. Parcourez la liste et sélectionnez le même fichier PEM racine que vous avez sélectionné à l'étape précédente.

   d. Cliquez sur Ajouter une racine sécurisée.

   Le message de confirmation indique que la racine sécurisée du certificat personnalisé a été ajoutée au fichier iControl.conf dans le répertoire iTechnology du serveur de gestion CA Enterprise Log Manager.

8. Cliquez sur Se déconnecter et fermez iTechnology SPIN.

Ajoutez le certificat de racine sécurisée à tous les autres serveurs CA Enterprise Log Manager

Si vous remplacez le certificat CAELM_AgentCert.p12 par un certificat personnalisé, vous devez ajouter le certificat de racine sécurisée à l'interface Web iTechnology SPIN de chaque serveur CA Enterprise Log Manager supplémentaire. Dans cette procédure, vous ajoutez le certificat de racine sécurisée à CA iControl. Cette procédure n'est pas nécessaire si vous remplacez uniquement le certificat CAELMCert.p12.

Pour ajouter le certificat de racine sécurisée à CA iControl de chaque serveur de non-gestion CA Enterprise Log Manager, procédez comme suit :

1. Connectez-vous à l'interface utilisateur SPIN, sur le système iGateway où s'exécute le serveur de gestion. Utilisez l'URL suivante.

   https://<ELM_hostname>:5250/spin/

   La page CA iTechnology SPIN apparaît.

2. Sélectionnez Administrateur iTech dans la liste déroulante, puis cliquez sur OK.

   La page d'administration iTechnology affiche un lien de connexion.

3. Cliquez sur Connexion.

   La boîte de dialogue de connexion CA iTechnology s'affiche.

4. Saisissez les identifiants de connexion EiamAdmin, sélectionnez iAuthority, puis cliquez sur Connexion.

5. Sélectionnez l'onglet Configurer et ajoutez la racine sécurisée comme suit :

   a. Saisissez la même étiquette pour le certificat que celle saisie à l'étape précédente.

   b. Parcourez la liste et sélectionnez le même fichier PEM racine que vous avez sélectionné à l'étape précédente.

   c. Cliquez sur Ajouter une racine sécurisée.

   La racine sécurisée du certificat personnalisé est ajoutée au fichier iControl.conf dans le répertoire iTechnology. Un message de confirmation apparaît.

6. Cliquez sur Se déconnecter et fermez iTechnology SPIN.

Ajout d'un nom commun de certificat à une stratégie d'accès

Le certificat CAELMCert.p12 est utilisé par tous les services CA Enterprise Log Manager pour communiquer avec le serveur de gestion CA Enterprise Log Manager. Si vous remplacez CAELMCert.p12 par un certificat personnalisé, vous devez ajouter ce nom commun de certificat personnalisé à la stratégie AdministerObjects se trouvant sur le serveur de gestion ou le serveur CA EEM autonome.

Remarque : Il n'est pas nécessaire de supprimer l'identité [Utilisateur] CERT_CAELM, à savoir le nom commun du certificat par défaut, de cette stratégie.

Pour ajouter le nom commun du certificat personnalisé à la stratégie AdministerObjects

1. Accédez au serveur CA Enterprise Log Manager de gestion ou au serveur CA EEM autonome en saisissant l'URL appropriée.

   https://<nomhôte_serveur_gestion>:5250/spin/calm

   https://<nomhôte_serveur_EEM>:5250/spin/eiam

2. Connectez-vous avec des privilèges d'administration au serveur de gestion CA Enterprise Log Manager. En cas d'accès à un serveur CA EEM autonome, connectez-vous en tant qu'utilisateur EiamAdmin.

3. Cliquez sur l'onglet Administration, le sous-onglet Gestion des utilisateurs et des accès, puis le lien de la stratégie d'accès dans le volet de gauche. Si vous êtes connecté à un serveur CA EEM autonome, cliquez sur l'onglet Gestion des stratégies d'accès.

4. Cliquez sur le lien Stratégies de portée.

   La table des stratégies de portée s'affiche dans le volet principal.

5. Faites défiler jusqu'à la stratégie AdministerObjects et sélectionnez le lien AdministerObjects.

   La stratégie AdministerObjects s'ouvre en mode d'édition.

6. Ajoutez le nom commun du certificat personnalisé comme suit :

   a. Saisissez le nom commun du certificat personnalisé dans le champ Identité.

   b. Cliquez sur la flèche pour déplacer votre entrée.

      [Utilisateur}<*cn certificat personnalisé*> apparaît dans la liste Identités sélectionnées.

7. Cliquez sur Enregistrer.

   La stratégie AdministerObjects est enregistrée ; elle contient désormais le nom commun de votre certificat personnalisé en tant qu'identité disposant d'un accès en lecture et écriture aux ressources spécifiées.

8. Cliquez sur Fermer et déconnectez-vous de l'interface utilisateur CA Enterprise Log Manager.

Déploiement de nouveaux certificats

CA Enterprise Log Manager utilise deux certificats. Vous pouvez remplacer l'un des deux certificats prédéfinis ou les deux par des certificats personnalisés. Pour déployer de nouveaux certificats, connectez-vous au dispositif logiciel, arrêtez iGateway, ajoutez les nouveaux certificats, modifiez les fichiers de configurations respectifs, puis redémarrez iGateway.

Avant de déployer de nouveaux certificats, vérifiez les éléments suivants.

- Le certificat de la racine sécurisée a été ajouté à iTechnology iAuthority pour le serveur de gestion ou le serveur autonome que vos serveurs CA Enterprise Log Manager utilisent.
- Si vous remplacez CAELM_AgentCert.p12 par un certificat personnalisé, le certificat de la racine sécurisée sera ajouté au répertoire iTechnology iControl de chaque serveur CA Enterprise Log Manager.
- Le nom commun du certificat personnalisé a été ajouté à la stratégie d'accès AdministerObjects. Cela fait référence au certificat personnalisé qui doit remplacer CAELMCert.p12.

Pour déployer de nouveaux certificats

1. Accédez à l'hôte dans lequel le serveur CA Enterprise Log Manager a été installé.
2. Utilisez vos informations d'identification **caelmadmin** pour vous connecter au serveur CA Enterprise Log Manager.
3. A l'invite de commande, basculez sur le compte d'utilisateur root.

   ```
   su - root
   ```

4. Accédez au répertoire /opt/CA/SharedComponents/iTechnology à l'aide du raccourci suivant.

   ```
   cd $IGW_LOC
   ```

5. Arrêtez iGateway.

   ./S99igateway stop

6. Pour remplacer CAELMCert.p12 :

   a. Copiez le certificat personnalisé *ApplicationName*Cert.p12 dans le répertoire iTechnology.

   b. Ouvrez le fichier CALM.cnf. Remplacez le nom du certificat par le nouveau nom. Remplacez le mot de passe du certificat par le nouveau mot de passe en texte clair, par exemple "c certpassword".

7. Pour remplacer CAELM_AgentCert.p12 :

   a. Copiez le certificat personnalisé *ApplicationName*_AgentCert.p12 dans le répertoire iTechnology.

   b. Ouvrez le fichier AgentManager.conf. Remplacez le nom du certificat par le nouveau nom. Remplacez le mot de passe du certificat par le nouveau mot de passe en texte clair, par exemple "c certpassword".

8. Démarrez iGateway.

   ./S99igateway start

   Au démarrage, le mot de passe de certificat contenu dans le fichier CALM.cnf et celui contenu dans AgentManager.conf sont chiffrés/protégés. Tous les agents installés après ce déploiement utilisent automatiquement le certificat personnalisé, si CAELM_AgentCert.p12 a été remplacé.

Annexe A : Accessibility Features

CA s'engage à ce que tous ses clients puissent, quelles que soient leurs capacités, utiliser sans problème ses produits et les documentations associées pour réaliser des tâches commerciales cruciales. Cette section présente les fonctions d'accessibilité intégrées de CA Enterprise Log Manager.

Mode d'accessibilité

Vous pouvez configurer CA Enterprise Log Manager pour qu'il utilise un mode d'accessibilité, qui affiche tous les volets graphiques des requêtes et des rapports sous forme de tables. Pour passer en mode accessibilité, sélectionnez la case à cocher Activer l'accessibilité dans l'écran de connexion.

Commandes d'accessibilité

Vous pouvez utiliser les commandes du clavier pour naviguer dans le système CA Enterprise Log Manager, tel qu'indiqué dans la table ci-dessous.

Tâches	Commandes du clavier
Passer d'une application ouverte à l'autre	CTRL-TAB
Sélectionner un fichier dans une fenêtre ouverte	CTRL-TAB
Aide	F1
Cliquer sur un bouton	Barre d'espace ou touche Entrée
Sélectionner une case à cocher	Barre d'espace ou touche Entrée
Ouvrir un menu, une zone de liste modifiable	CTRL + flèche bas
Navigation dans les listes	CTRL + flèche bas pour sélectionner une cible de saisie Flèches haut/bas pour naviguer Barre d'espace ou touche Entrée pour sélectionner un élément dans la liste
Groupe Bouton radio	CTRL + flèche bas pour sélectionner une cible de saisie Flèches haut/bas pour naviguer Barre d'espace ou touche Entrée pour sélectionner un élément dans la liste

Tâches	Commandes du clavier
Fermer la fenêtre active	ALT + F4
Double-cliquer	CTRL + D

Paramètres d'affichage de langue de CA Enterprise Log Manager

L'interface de CA Enterprise Log Manager peut être affichée dans les langues suivantes, en plus de l'anglais.

- Français
- Italien
- Allemand
- Espagnol
- Japonais

Modifiez les paramètres de langue dans la fenêtre de votre navigateur. Par exemple, si vous utilisez Microsoft Internet Explorer, ouvrez la boîte de dialogue Options Internet, et ajoutez ou sélectionnez la langue principale à utiliser.

Si vous sélectionnez l'une des cinq langues prises en charge, l'interface de CA Enterprise Log Manager apparaît dans cette langue à l'ouverture suivante. Les balises et les étiquettes de l'interface sont traduites, mais d'autres éléments ne le sont pas. Par exemple, les titres des balises et les chaînes de données dans les résultats des rapports restent en anglais.

Remarque : Si CA Enterprise Log Manager est affiché au moment où vous modifiez la langue, vous devez réactualiser la fenêtre du navigateur pour que la modification soit prise en compte. Si vous êtes connecté lorsque vous procédez à cette modification, vous êtes renvoyé à l'écran de connexion, qui s'affiche dans la nouvelle langue.

Localisation manuelle de CA Enterprise Log Manager

Vous pouvez localiser manuellement CA Enterprise Log Manager en créant vos propres fichiers de langue. Ceci vous permet d'afficher l'interface CA Enterprise Log Manager dans d'autres langues que celles déjà prises en charge. Pour y parvenir, copiez les fichiers existants afin de les utiliser comme modèles.

Pour localiser manuellement CA Enterprise Log Manager

1. Connectez-vous à votre hôte du serveur CA Enterprise Log Manager, naviguez jusqu'à opt/CA/LogManager/local, puis sélectionnez les fichiers à utiliser comme modèles. Il existe deux fichiers pour chaque langue :

   - content.properties : contient le texte décrivant du contenu varié, tels que les noms de rapport et de requête, ainsi que des descriptions.
   - ui.properties : contient des chaînes de texte pour les titres des fonctions de l'interface, tels que les étiquettes et les en-têtes des onglets.

   Chaque fichier est précédé d'un préfixe de langue standard. Par exemple, le fichier du contenu allemand est nommé de_content.properties. Le fichier de l'interface en anglais est nommé en_ui.properties.

2. Copiez un fichier de chaque type, puis renommez-les en utilisant le préfixe standard. Par exemple, si vous voulez créer un fichier de localisation pour le portugais, vous devez copier les fichiers et les renommer pt_content.properties et pt__ui.properties.

   Remarque : Les préfixes de langue standard peuvent se trouver dans la liste des langues prises en charge dans votre navigateur.

3. Ouvrez les fichiers et traduisez les chaînes dans la langue de votre choix. Par exemple, si vous avez copié les fichiers anglais, vous devez remplacer chaque chaîne de texte en anglais par la langue de votre choix.

4. Enregistrez les fichiers traduits manuellement dans l'emplacement indiqué à l'étape 1, sur chaque serveur CA Enterprise Log Manager où vous voulez qu'ils soient disponibles.

5. Paramétrez votre navigateur sur la langue cible et connectez-vous à CA Enterprise Log Manager.

Informations complémentaires :

Paramètres d'affichage de langue de CA Enterprise Log Manager (page 688)

Annexe B : Accès aux événements collectés avec ODBC et JDBC

Ce chapitre traite des sujets suivants :

A propos de l'accès ODBC/JDBC dans CA Enterprise Log Manager

CA Enterprise Log Manager offre un accès ODBC et JDBC en lecture seule au magasin de journaux d'événements afin que vous puissiez réaliser les tâches ci-dessous.

- Configuration des rapports personnalisés à l'aide d'un utilitaire de génération de rapport externe tel que Crystal Reports de BusinessObjects
- Récupération des informations de journal sélectionnées à l'aide d'applications externes

Ces fonctions vous permettent de créer et de formater des rapports personnalisés en utilisant les informations de journal déjà récupérées par CA Enterprise Log Manager. Vous pouvez également récupérer des données afin de les utiliser avec vos moteurs de corrélation, des packages de détection de programmes malveillants et d'autres fonctions.

Après avoir installé le client fourni par CA sur le système que vous prévoyez d'utiliser pour accéder au magasin de journaux d'événements, vous devez configurer une connexion à la source de données, puis commencer la récupération des données. Le module d'abonnement installe les composants côté serveur.

Création de requêtes ODBC et JDBC à utiliser avec CA Enterprise Log Manager

La prise en charge d'ODBC et JDBC dans CA Enterprise Log Manager est limitée aux requêtes en lecture seule basées sur des instructions SELECT exécutées sur la table VIEW_EVENT.

Créez vos instructions SELECT en respectant les règles et le format SQL ANSI. Les composants côté serveur contiennent un moteur d'analyse SQL. L'analyseur met en oeuvre une grande partie des instructions SQL de base, tel que défini dans la spécification X3.135-1992, "Database Language SQL". L'analyseur prend également en charge les fonctions SQL de la norme SQL99 ANSI et les bases de données commerciales comme Microsoft SQL Server et Oracle. Il est conforme à la spécification de grammaire minimale ODBC.

La grammaire commune aux événements sert de schéma pour cette table. Pour plus d'informations sur le schéma, reportez-vous au *Manuel de référence CEG*.

Limitations de la prise en charge de SQL

CA Enterprise Log Manager ne prend pas en charge les appels de procédure stockée, ni les commandes DCL (Data Control Language, langage de contrôle de données) et DDL (Data Definition Language, langage de définition des données).

CA Enterprise Log Manager ne prend pas en charge les mots clés et les opérations DML (Data Manipulation Language, langage de manipulation de données) énumérés ci-dessous.

- UNION
- JOIN
- Instructions SELECT imbriquées
- INSERT
- MISE A JOUR
- DELETE
- Les opérateurs de contrôle des transactions tels que COMMIT, ROLLBACK, etc.

Fonctions SQL prises en charge

Les fonctions SQL ci-dessous peuvent être utilisées pour créer des instructions SELECT.

- ABS(*numeric_exp*)
- ROUND(*numeric_exp, integer_exp*)
- LCASE(*string_exp*)
- LOWER(*string_exp*)
- LENGTH(*string_exp*)
- LTRIM(*string_exp*)
- RTRIM(*string_exp*)
- SUBSTRING(*string_exp, start,length*)
- UCASE(*string_exp*)
- UPPER(*string_exp*)
- IFNULL (*expr, default_val*)
- ISNULL (*expr, default_val*)
- NVL (*expr, default_val*)
- CONVERT (*value_exp, data_type*)
- CURDATE()
- CURTIME()
- CURTIMESTAMP()
- DATEADD(*datepart, number, date*)
- TIMESTAMPADD(*datepart, number, date*)
- DATEDIFF(*datepart, startdate, enddate*) ; pour datepart, les valeurs Year, Day et Second sont autorisées.
- TIMESTAMPDIFF(*datepart, startdate, enddate*) ; pour datepart, les valeurs Year, Day et Second sont autorisées.
- DAYOFMONTH(*date_exp*)
- DAYOFWEEK(*date_exp*)
- DAYOFYEAR(*date_exp*)
- HOUR(*time_exp*)

- MINUTE(*time_exp*)
- MONTH(*date_exp*)
- NOW( )
- SECOND(*time_exp*)
- WEEK(*date_exp*)
- YEAR(*date_exp*)
- AVG([ALL | DISTINCT]*expression*)
- SUM([ALL | DISTINCT]*expression*)
- COUNT({[ALL | DISTINCT]*expression*] | *})
- MAX([ALL | DISTINCT]*expression*)
- MIN([ALL | DISTINCT]*expression*)

Traitement des requêtes

CA Enterprise Log Manager traite les requêtes lancées par un client ODBC ou JDBC de la manière suivante.

1. Une application cliente envoie une instruction SELECT au serveur CA Enterprise Log Manager via une connexion ODBC.
2. Le serveur CA Enterprise Log Manager procède à la validation de l'instruction SELECT. Si l'instruction est validée, le serveur CA Enterprise Log Manager crée une structure de données représentant la requête.

   Les erreurs éventuellement rencontrées sont renvoyées directement au pilote du client.
3. Le serveur CA Enterprise Log Manager convertit les éléments SQL en une requête qu'il peut utiliser. Si la conversion s'effectue correctement, le serveur CA Enterprise Log Manager exécute la requête.

   Les erreurs éventuellement rencontrées sont renvoyées au pilote du client.
4. Le serveur CA Enterprise Log Manager gère les informations d'état, y compris l'horloge d'expiration, de chaque requête afin qu'elles puissent être annulées en cas de fermeture de la session ou d'expiration de la requête.
5. Le serveur CA Enterprise Log Manager traduit les résultats de la requête et les renvoie au pilote du client ODBC, puis l'application cliente reçoit les données.

Alias des colonnes de résultats

Dans le cadre de la gestion des états de requête, CA Enterprise Log Manager prend en charge les alias des noms des colonnes de résultats. Vous pouvez ainsi afficher les champs CEG dans vos rapports personnalisés en utilisant vos propres étiquettes et en-têtes.

Les alias sont conservés et utilisés pour le mappage correct des données lorsque le serveur CA Enterprise Log Manager transfère un ensemble de résultats au pilote du client.

Limitation des résultats

Pour optimiser l'utilisation de l'espace disque, CA Enterprise Log Manager limite le nombre de lignes de résultat. CA Enterprise Log Manager utilise un sous-ensemble du mot clé Transact-SQL TOP contenant uniquement une valeur fixe. La version pourcentage du mot clé n'est pas prise en charge.

La valeur TOP par défaut utilisée dans CA Enterprise Log Manager est de 5 000 lignes et la valeur maximale est de 50 000 lignes.

Codes d'erreur de CA Enterprise Log Manager

Les codes d'erreur ODBC et JDBC ci-dessous peuvent apparaître lors de l'accès au magasin de journaux d'événements CA Enterprise Log Manager. Chaque message d'erreur fournit des précisions sur l'erreur en question.

- 88 – Problème de prise en charge

  Le message d'erreur associé apporte des précisions sur la fonctionnalité qui n'est pas prise en charge.

- 300 – Erreur générique

  Le message d'erreur associé apporte des précisions sur le problème.

- 301 – Erreur de conversion des paramètres comprenant des caractères multi-octet
- 302 – Erreur d'authentification
- 304 – Expression (colonne) non valide dans la clause OrderBy ou GroupBy

Les erreurs ci-dessous sont des erreurs d'exécution d'une instruction SQL.

- 305 – Erreur lors du déclenchement de la requête
- 306 – Erreur lors de la récupération de l'état de la requête
- 307 – Erreur lors de l'analyse des résultats XML de la requête

- 308 – Erreur lors de l'exécution de la requête
- 309 – Des erreurs se sont produites lors de l'exécution de la requête
- 310 – Erreur lors de l'extraction des résultats de la requête
- 311 – Expiration de la requête

Exemple : Utilisation d'un filtre d'accès pour limiter les résultats ODBC

Vous pouvez créer un filtre d'accès pour limiter le nombre de données renvoyées par une requête d'accès ODBC. Lorsque les membres du groupe d'applications nommé accèdent aux données d'événements CA Enterprise Log Manager à l'aide du client ODBC, ils ne peuvent voir que les informations autorisées par le filtre.

Cet exemple suppose que vous disposez d'un groupe d'applications appelé Analystes_UNIX et que vous voulez restreindre l'affichage aux événements UNIX du magasin de journaux d'événements, pour tous les membres de ce groupe. Le filtre créé dans cet exemple limite l'affichage des données d'événements dans l'interface utilisateur CA Enterprise Log Manager et les requêtes externes via ODBC.

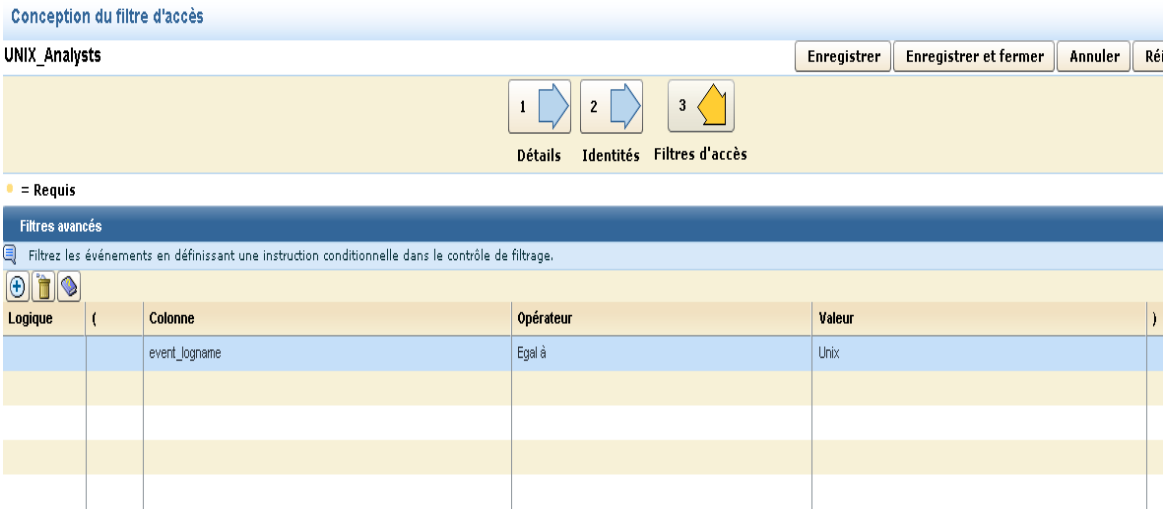
Vous trouverez davantage d'informations sur les filtres d'accès dans l'aide en ligne.

Pour créer un filtre d'accès

1. Connectez-vous à CA Enterprise Log Manager en tant qu'utilisateur Administrator.
2. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
3. Cliquez sur Nouveau filtre d'accès  . L'assistant de conception du filtre d'accès s'affiche.

4. Dans le champ Nom, entrez Analystes UNIX et dans le champ Description, saisissez Filtre d'accès Analystes UNIX. Ensuite, cliquez sur l'étape 2 Identités en haut de la boîte de dialogue.
5. Définissez le type Groupe d'applications, saisissez UNIX dans le champ Nom, puis cliquez sur Recherche d'identités.

   La liste des identités correspondant à vos critères de recherche apparaît dans un contrôle de déplacement afin que vous puissiez sélectionner les identités qui vous intéressent.
6. Dans la liste Identités disponibles, sélectionnez le groupe d'applications Analystes_UNIX et cliquez sur la flèche droite du contrôle de déplacement pour déplacer la sélection vers la liste Identités sélectionnées.
7. Cliquez sur l'étape 3 Filtres d'accès en haut de la boîte de dialogue.
8. Cliquez sur Nouveau filtre d'événement  pour ajouter une ligne, puis cliquez sur la zone de champ dans Colonne.
9. Dans la liste déroulante, sélectionnez event_logname, puis cliquez sur la zone de champ dans Valeur.
10. Dans la liste déroulante, sélectionnez Unix. La boîte de dialogue se présente comme suit.



11. Cliquez sur Enregistrer et fermer.

Exemple : Préparation de l'utilisation des clients ODBC et JDBC avec Crystal Reports

La préparation de l'accès du client ODBC ou JDBC aux événements CA Enterprise Log Manager en utilisant BusinessObjects Crystal Reports comprend les étapes ci-dessous.

1. Créez un utilisateur CA Enterprise Log Manager pour autoriser l'accès à la base de données.
2. Assurez-vous que le service ODBC utilise le chiffrement SSL et le port 17002.
3. Installez le client ODBC ou copiez les fichiers JDBC sur le serveur où réside Crystal Reports.

   Pour plus d'informations sur ces installations, reportez-vous au *manuel d'implémentation*.
4. Configurez les composants du système d'exploitation.
   a. Créez et testez une source de données ODBC dans le Panneau de configuration de Windows.
   b. Modifiez le fichier de configuration de Crystal Reports afin de pouvoir utiliser le client JDBC.
5. Créez des événements qui seront collectés par CA Enterprise Log Manager.

   Si vous êtes certain que le magasin de journaux d'événements contient déjà des événements du type interrogé, pour pouvez ignorer cette étape.

Remarque : Ce processus et l'exemple associé supposent que vous êtes familiarisé avec la création d'instructions SQL de base et l'utilisation de Crystal Reports. Pour plus d'informations sur l'utilisation de Crystal Reports, consultez l'aide en ligne de BusinessObjects.

Création d'un utilisateur CA Enterprise Log Manager pour un accès ODBC ou JDBC

Utilisez la procédure suivante pour créer un compte d'utilisateur appelé ELM_Access à utiliser avec vos clients JDBC et ODBC.

Les utilisateurs CA Enterprise Log Manager qui disposent de l'autorisation d'accès aux données peuvent utiliser ODBC ou JDBC pour accéder aux données d'événements. Tous les rôles d'utilisateur par défaut fournis avec CA Enterprise Log Manager disposent de cette autorisation. Pour cet exemple, vous pouvez créer un utilisateur avec n'importe quel rôle CA Enterprise Log Manager par défaut : Administrator, Analyst ou Auditor.

Pour créer un utilisateur

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur Administrator.
2. Cliquez sur l'onglet Administration, puis sur le sous-onglet Gestion des utilisateurs et des accès.
3. Cliquez sur le bouton Utilisateurs pour afficher l'interface utilisateur CA EEM intégrée.
4. Cliquez sur Nouvel utilisateur. La boîte de dialogue Nouvel utilisateur s'ouvre.
5. Cliquez sur Ajouter les détails de l'utilisateur de l'application et accordez des droits d'application Administrator au compte.

   Remarque : Dans un environnement de production, vous devez attribuer l'autorisation la plus faible qui permette à un utilisateur d'accéder aux données. Vous pouvez limiter l'accès de nombreuses manières, y compris par le biais de rôles d'utilisateur, de stratégies d'accès et de filtres d'accès. Pour plus d'informations, consultez l'*aide en ligne*.
6. Terminez l'enregistrement de l'utilisateur et définissez un mot de passe, sans oublier de noter celui-ci, car il sera requis plus tard dans cet exemple.
7. Enregistrez l'utilisateur et fermez la fenêtre Utilisateurs.

Configuration des paramètres du service ODBC

Utilisez la procédure suivante pour configurer les paramètres des services ODBC et JDBC CA Enterprise Log Manager.

Remarque : Les modifications effectuées dans cette zone nécessitent un redémarrage des processus côté serveur afin d'activer les communications ODBC et JDBC.

Pour configurer le service ODBC

1. Connectez-vous au serveur CA Enterprise Log Manager en tant qu'utilisateur Administrator.
2. Cliquez sur l'onglet Administration et le sous-onglet Services.
3. Cliquez sur le noeud Service ODBC.

4. Acceptez les paramètres par défaut.
   - Activer le service : True (autorise les connexions ODBC et JDBC au serveur CA Enterprise Log Manager)
   - Port : 17002
   - Chiffrement (SSL) est sélectionné
   - Délai d'expiration de la session : 15 minutes
   - Niveau de journalisation : acceptez la valeur par défaut, Non définie
5. Cliquez sur Enregistrer.

Création d'une source de données ODBC "elm"

Utilisez la procédure suivante pour créer la source de données "CA-ELM."

Remarque : Vous devez installer le client ODBC pour pouvoir configurer la source de données.

Pour créer une source de données

1. Ouvrez le Panneau de configuration de Windows.
2. Cliquez sur le dossier Outils d'administration et lancez l'utilitaire Sources de données (ODBC).
3. Cliquez sur Ajouter pour afficher la boîte de dialogue Créer une nouvelle source de données.
4. Sélectionnez l'entrée DataDirect OpenAccess SDK 6.0 et cliquez sur Terminer.

   L'utilitaire Installation du pilote ODBC DataDirect OpenAccess SDK affiche un écran de configuration.
5. Entrez CA-ELM dans le champ Nom de la source de données et saisissez une description.
6. Dans le champ Hôte du service, entrez le nom de votre serveur CA Enterprise Log Manager. Dans cet exemple, ca-elm est utilisé.
7. Dans le champ Port du service, entrez 17002.
8. Cochez la case Chiffrement SSL.
9. Entrez les propriétés personnalisées suivantes.

   querytimeout=600 (seconds);queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false

10. Cliquez sur Appliquer, puis sur Tester la connexion.

    Si les paramètres de connexion sont corrects, un message confirmant la réussite de la connexion s'affiche.

11. Cliquez sur OK pour revenir à la boîte de dialogue Administrateur de sources de données ODBC, puis cliquez à nouveau sur OK pour quitter l'utilitaire.

Considérations sur les sources de données ODBC

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

Nom de la source de données

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

Hôte du service

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

Port du service

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

Source de données du service

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

Chiffrement SSL

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

Propriétés personnalisées

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

querytimeout

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

querytimeout=300

queryfederated

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

queryfederated=true

queryfetchrows

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

queryfetchrows=1000

offsetmins

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

offsetmins=0

suppressNoncriticalErrors

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

Voici la syntaxe utilisée pour cette propriété.

suppressNoncriticalErrors=false

Modification du fichier de configuration de Crystal Reports

Avant de pouvoir utiliser Crystal Reports avec le client JDBC de CA Enterprise Log Manager, vous devez spécifier certains paramètres de configuration. Une fois le fichier de configuration XML de Crystal Reports paramétré, vous pouvez préparer et envoyer des requêtes conformes à la norme SQL ANSI au magasin de journaux d'événements CA Enterprise Log Manager.

Pour configurer les paramètres de Crystal Reports pour JDBC

1. Copiez les fichiers JAR du client JDBC sur le serveur où est exécuté Crystal Reports, avant de modifier le fichier de configuration.

   Pour plus d'informations, consultez le *manuel d'implémentation*.

2. Accédez au serveur sur lequel réside Crystal Reports.
3. Recherchez le fichier CRConfig.xml et ouvrez-le pour le modifier.
4. Recherchez la balise <DataDriverCommon> et la section de balise <Classpath> qui se trouve juste dessous.
5. Ajoutez au chemin de classes l'emplacement des fichiers JAR du client JDBC.
6. Modifiez la valeur des balises de l'URL JDBC pour obtenir l'URL suivante.

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

   Pour plus d'informations sur ces paramètres, reportez-vous à la section Considérations sur les URL JDBC.

   Consultez la documentation fournie avec Crystal Reports pour obtenir des informations supplémentaires sur la configuration des paramètres de connexion dans ce produit.

7. Modifiez la valeur des balises du nom de classe JDBC pour obtenir le nom suivant.

   com.ca.jdbc.openaccess.OpenAccessDriver

8. Enregistrez le fichier, puis fermez-le.

Informations complémentaires :

Considérations sur les URL JDBC (page 704)

Considérations sur les URL JDBC

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

Voici un exemple d'URL JDBC complète.

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

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

jdbc.ca-elm:

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

//adresse IP:port;

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

encrypted=0|1;

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

ServerDataSource=Default

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

CustomProperties=(x;y;z)

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

Informations complémentaires

Considérations sur les sources de données ODBC (page 701)

Création d'événements pour l'exemple d'ODBC

Pour afficher l'exemple de requête, créez des événements pertinents en provoquant l'échec d'activités de la manière suivante.

- Connectez-vous plusieurs fois de suite au serveur CA Enterprise Log Manager avec des informations d'identification incorrectes.
- Connectez-vous avec des informations d'identification incorrectes à un hôte d'agent dont les événements sont transférés à un serveur CA Enterprise Log Manager particulier.
- Accédez à une ressource réseau ou système avec des informations d'identification incorrectes.

Utilisation de Crystal Reports pour accéder au magasin de journaux d'événements avec ODBC

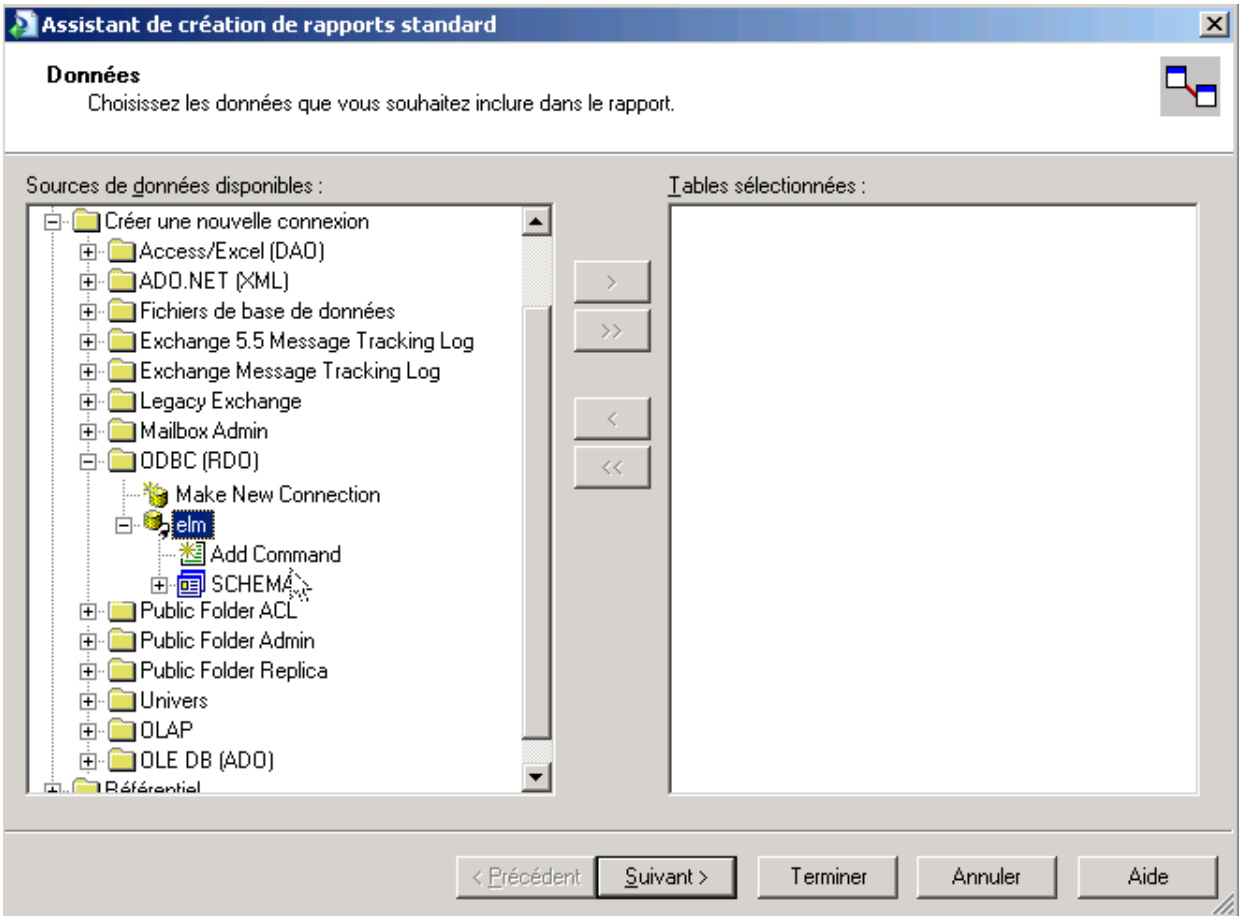
Vous pouvez utiliser la fonction d'accès ODBC pour interroger les données d'événements CA Enterprise Log Manager depuis un outil de génération de rapport tiers tel que BusinessObjects Crystal Reports. Une fois l'installation et les configurations requises effectuées, vous pouvez préparer et envoyer des requêtes conformes à la norme SQL ANSI au magasin de journaux d'événements CA Enterprise Log Manager.

La grammaire commune aux événements (CEG) est le schéma de base de données du magasin de journaux d'événements. L'aide en ligne de CA Enterprise Log Manager contient un composant de référence CEG pour vous aider à créer des requêtes. Vous pouvez également examiner les instructions SQL des requêtes prêtes à l'emploi, mais vous devez respecter la norme SQL ANSI pour accéder à la base de données depuis une application extérieure à CA Enterprise Log Manager.

Pour accéder aux données d'événements depuis Crystal Reports

1. Effectuez les tâches d'installation et de configuration requises.
2. Démarrez Crystal Reports et accédez à l'assistant de création de rapport standard.

3. Créez une connexion ODBC dans la boîte de dialogue Données, puis, dans le Panneau de configuration de Windows, sélectionnez la source de données ODBC que vous avez créée.



4. Utilisez la fonctionnalité Ajouter une commande pour créer une requête dans la zone de saisie SQL.

   Par exemple, vous pouvez créer la requête suivante.

   ```
   SELECT source_username as source_username , SUM(event_count) AS FUNC_SUM_event_count FROM view_event WHERE event_result = 'F' GROUP BY source_username ORDER BY FUNC_SUM_event_count DESC;
   ```

5. Cliquez sur OK pour terminer la saisie de la requête.

   Un modèle de rapport apparaît dans lequel vous pouvez placer les colonnes de données renvoyées par la requête.

6. Déplacez les champs depuis l'Explorateur de champ en haut à droite vers les colonnes du modèle de rapport.

   Lorsque vous exécutez la requête, les valeurs associées aux champs s'affichent. Vous pouvez utiliser Crystal Reports pour définir l'apparence des rapports et les personnaliser selon vos besoins.

7. Comparez les résultats du rapport avec ceux du rapport prêt à l'emploi Echec d'activité par exécutant (facultatif).

Accès à des événements à partir de Crystal Reports avec JDBC

Les tâches suivantes vous permettent d'utiliser JDBC pour accéder au magasin de journaux d'événements.

1. Copiez les fichiers JAR JDBC du client sur le serveur sur lequel réside Crystal Reports.
2. Modifiez le fichier de configuration de Crystal Reports.
3. Utilisez Crystal Reports pour envoyer une requête.

Remarque : Ce processus et l'exemple associé supposent que vous êtes familiarisé avec la création d'instructions SQL de base et l'utilisation de Crystal Reports. Pour plus d'informations sur l'utilisation de Crystal Reports, consultez l'aide en ligne de BusinessObjects.

Copie des fichiers JAR du pilote JDBC

Avant de pouvoir utiliser le pilote JDBC pour accéder aux événements à partir d'un serveur CA Enterprise Log Manager, vous devez copier les fichiers JAR correspondants sur le serveur à partir duquel vous voulez accéder aux événements.

Pour copier les fichiers

1. Ouvrez l'image ISO ou utilisez le DVD d'installation de l'application.
2. Accédez au répertoire \CA\ELM\JDBC.
3. Copiez les fichiers JAR sur le serveur sur lequel réside Crystal Reports.

   Le package de rapports que vous utilisez requiert un emplacement particulier pour ces fichiers. Consultez la documentation fournie avec votre application.

4. Notez le répertoire où vous avez copié ces fichiers, vous en aurez besoin pour configurer les connexions.

Utilisation de Crystal Reports pour accéder au magasin de journaux d'événements avec JDBC

Vous pouvez utiliser la fonction d'accès de JDBC pour interroger les données d'événements CA Enterprise Log Manager depuis un outil de génération de rapport tiers tel que BusinessObjects Crystal Reports.

La grammaire commune aux événements (CEG) est le schéma de base de données du magasin de journaux d'événements. L'aide en ligne de CA Enterprise Log Manager contient un composant de référence CEG pour vous aider à créer des requêtes. Vous pouvez également examiner les instructions SQL des requêtes prêtes à l'emploi, mais vous devez respecter la norme SQL ANSI pour accéder à la base de données depuis une application extérieure à CA Enterprise Log Manager.

Pour accéder aux données d'événements depuis Crystal Reports

1. Démarrez Crystal Reports et accédez à l'assistant de création de rapport standard.
2. Créez une connexion JDBC dans la boîte de dialogue Données.

   Remarque : Utilisez la valeur, *Par défaut*, pour le nom de la base de données dans la boîte de dialogue Informations de connexion.
3. Utilisez la fonctionnalité Ajouter une commande pour créer et exécuter la requête suivante dans la zone de saisie SQL.

   ```
   SELECT source_username as source_username , SUM(event_count) AS FUNC_SUM_event_count FROM view_event WHERE event_result = 'F' GROUP BY source_username ORDER BY FUNC_SUM_event_count DESC;
   ```
4. Déplacez les champs depuis l'Explorateur de champ à droite vers les colonnes du modèle de rapport.

   Lorsque vous exécutez la requête, les valeurs associées aux champs s'affichent. Vous pouvez utiliser les outils de Crystal Reports pour définir l'apparence des rapports et les personnaliser selon vos besoins.
5. Comparez les résultats du rapport avec ceux du rapport prêt à l'emploi Echec d'activité par exécutant (facultatif).

Suppression du client ODBC sur les systèmes Windows

Sur toutes les plates-formes Windows, l'option Supprimer du package d'installation client permet de supprimer du système les entrées et les fichiers du produit.

Important : Si vous avez créé des fichiers de sources IP dans le répertoire d'installation du client ODBC local, sauvegardez-les dans un autre répertoire avant de supprimer le client ODBC du système Windows.

Si le client ODBC local est déjà installé, mais que vous souhaitez le changer d'emplacement, utilisez l'option Supprimer. Supprimez le client ODBC local installé, puis réinstallez-le dans l'emplacement de votre choix.

Pour supprimer le client ODBC

1. Dans le Panneau de configuration Windows, sélectionnez Ajout/Suppression de programmes.
2. Recherchez et sélectionnez l'entrée Pilote ODBC CA Enterprise Log Manager.
3. Cliquez sur Supprimer.

Suppression du client JDBC

Pour désinstaller le client JDBC, supprimez le répertoire d'installation.

Glossaire

accès aux données

L'*accès aux données* est un type d'autorisation octroyé à l'ensemble de CA Enterprise Log Manager par le biais de la stratégie d'accès aux données par défaut, pour la classe de ressource CALM. Tous les utilisateurs ont accès à toutes les données, hormis celles dont l'accès est restreint par des filtres.

Accès ODBC et JDBC

L'accès ODBC et JDBC aux magasins de journaux d'événements CA Enterprise Log Manager prend en charge l'utilisation des données d'événements par un grand nombre de produits tiers, notamment la génération de rapports d'événements personnalisés à l'aide d'outils de génération de rapports tiers, la corrélation d'événements à l'aide de moteurs de corrélation et l'évaluation d'événements à l'aide de produits de détection d'intrusion et de programmes malveillants. Les systèmes Windows utilisent ODBC ; les systèmes UNIX ou Linux utilisent JDBC.

adaptateurs CA

Les *adaptateurs CA* constituent un groupe d'écouteurs qui reçoit des événements provenant de composants CA Audit tels que les clients CA Audit, les iRecorders et les SAPI Recorders, ainsi que les sources qui transmettent des événements de manière native via iTechnology.

agent

Un *agent* est un service générique, configuré avec des connecteurs chargés de collecter les événements bruts à partir d'une source d'événement unique, puis de les envoyer à CA Enterprise Log Manager pour traitement. Chaque CA Enterprise Log Manager dispose d'un agent intégré. De plus,vous pouvez installer un agent sur un point de collecte distant et collecter des événements sur des hôtes où l'installation d'agents est impossible. Vous pouvez également installer un agent sur l'hôte où s'exécutent les sources d'événement et bénéficier des possibilités d'application de règles de suppression et de chiffrement des transmissions vers CA Enterprise Log Manager.

agent par défaut

L'*agent par défaut* est l'agent intégré installé avec le serveur CA Enterprise Log Manager. Vous pouvez le configurer pour collecter directement des événements Syslog ainsi que des événements provenant de différentes sources non Syslog, par exemple CA Access Control r12 SP1, le service de certificats Microsoft Active Directory et les bases de données Oracle9i.

ajustement d'événement

L'*ajustement d'événement* est le processus par lequel une chaîne d'événement brut collecté est analysée en champs d'événement et mappée vers des champs CEG. Les utilisateurs peuvent exécuter des requêtes afin d'afficher les données d'événement ajusté ainsi obtenues. L'ajustement d'événement est l'étape qui suit la collecte des événements et qui précède leur stockage.

alerte d'action

Une *alerte d'action* est un job de requête planifié qui peut être utilisé pour détecter les violations de stratégie, les tendances d'utilisation, les schémas de connexion et d'autres actions d'événement nécessitant une attention à court terme. Par défaut, lorsque les requêtes d'une alerte renvoient des résultats, ces derniers sont affichés sur la page Alertes CA Enterprise Log Manager et ajoutés à un flux RSS. Lorsque vous planifiez une alerte, vous pouvez indiquer des destinations supplémentaires, y compris une adresse électronique, un processus de sortie d'événement/d'alerte CA IT PAM et des interruptions SNMP.

analyse

Le terme *analyse* (parfois analyse de message ou décomposition) désigne le processus d'extraction de données d'unités brutes et de conversion en paires de valeurs clés. L'analyse s'effectue sur la base d'un fichier XMP. Cette étape, qui précède le mappage de données, fait partie du processus d'intégration qui convertit les événements bruts collectés auprès d'une source d'événement en événements ajustés que vous pouvez consulter.

analyse (décomposition) d'un journal

L'*analyse (décomposition) d'un journal* est le processus qui permet d'extraire les données d'un journal, pour que les valeurs ainsi analysées (décomposées) puissent être utilisées lors des étapes suivantes du processus de gestion du journal.

analyse de fichiers XMP

L'*analyse de fichiers XMP* est le processus réalisé par l'utilitaire d'analyse de message pour rechercher tous les événements contenant chaque chaîne pré-associée, pour chaque événement associé, en décomposant l'événement en jetons à l'aide du premier filtre trouvé, qui utilise la même chaîne pré-associée.

analyse de mappage

L'*analyse de mappage* est une étape de l'Assistant de fichier de mappage, qui vous permet de tester et de modifier un fichier de mappage de données. Des exemples d'événement sont testés par rapport au fichier de mappage de données et les résultats sont validés avec la CEG.

analyse de message

L'*analyse de message* est le processus consistant à appliquer des règles à l'analyse d'un journal d'événements bruts, afin d'obtenir des informations pertinentes, telles que l'horodatage, l'adresse IP et le nom d'utilisateur. Les règles d'analyse utilisent la correspondance de caractères pour localiser un texte d'événement spécifique et le relier aux valeurs sélectionnées.

analyse des journaux

L'*analyse des journaux* est l'étude des entrées de journal, qui permet d'identifier les événements pertinents. Si les journaux ne sont pas analysés opportunément, leur valeur est considérablement réduite.

AppObjects

Les *AppObjects* (Application Objects), ou objets d'application, sont des ressources spécifiques à un produit ; ils sont stockés dans CA EEM sous l'instance d'application d'un produit donné. Pour l'instance d'application CAELM, ces ressources incluent le contenu des rapports et requêtes, les jobs planifiés pour les rapports et alertes, les configurations et le contenu des agents, les configurations de service, d'adaptateur et d'intégration, les fichiers de mappage de données et d'analyse de message, ainsi que les règles de suppression et de récapitulation.

archivage automatique

L'*archivage automatique* est un processus configurable qui permet d'automatiser le transfert des bases de données d'archivage entre deux serveurs. Lors de la première phase de l'archivage automatique, le serveur de collecte envoie les bases de données nouvellement archivées au serveur de rapports, à la fréquence que vous avez prédéfinie. Lors de la seconde phase, le serveur de rapports envoie les anciennes bases de données au serveur de stockage distant, pour un stockage à long terme, ce qui évite d'avoir à effectuer la sauvegarde et le transfert manuellement. Pour effectuer un archivage automatique, vous devez configurer une authentification sans mot de passe entre le serveur source et le serveur de destination.

archivage de journaux

L'*archivage de journaux* est le processus se déroulant lorsque la base de données chaude atteint sa taille maximale, auquel cas une compression au niveau des lignes est effectuée et la base passe de "l'état chaud" à "l'état tiède". Les administrateurs peuvent sauvegarder manuellement les bases de données tièdes, avant que le délai de suppression automatique ne soit écoulé, puis exécuter l'utilitaire LMArchive pour enregistrer le nom des sauvegardes. Ces informations sont alors disponibles à la consultation, via la requête d'archivage.

assistant de fichier d'analyse

L'*Assistant de fichier d'analyse* est une fonction CA Enterprise Log Manager que les administrateurs utilisent pour créer, modifier et analyser les fichiers d'analyse de message extensibles (XMP), stockés sur le serveur de gestion CA Enterprise Log Manager. Pour personnaliser l'analyse des données d'événements entrants, vous devez modifier les chaînes et filtres pré-associés. Les nouveaux fichiers, comme les fichiers modifiés, s'affichent dans l'Explorateur de collecte de journaux, la Bibliothèque d'ajustement d'événement, les fichiers d'analyse et le dossier Utilisateur.

balise

Une *balise* est un terme ou une expression clé, qui sert à identifier les requêtes ou rapports appartenant au même regroupement pertinent. Les balises permettent d'effectuer des recherches basées sur les regroupements pertinents. Le terme balise désigne également le nom de ressource utilisé dans une stratégie octroyant à l'utilisateur le droit de créer une balise.

bases de données archivées

Les *bases de données archivées* sur un serveur CA Enterprise Log Manager donné incluent : toutes les bases de données tièdes disponibles pour requête, mais nécessitant une sauvegarde manuelle avant expiration ; toutes les bases de données froides ; toutes les bases de données enregistrées comme restaurées à partir d'une sauvegarde.

bibliothèque d'ajustement d'événement

La *bibliothèque d'ajustement d'événement* est l'espace de stockage qui contient les intégrations, les fichiers de mappage et d'analyse, ainsi que les règles de suppression et de récapitulation, prédéfinis et définis par l'utilisateur.

bibliothèque d'analyse de message

La *bibliothèque d'analyse de message* est une bibliothèque qui accepte les événements provenant des files d'attente d'écouteur et qui utilise des expressions régulières pour marquer les chaînes en paires nom/valeur.

bibliothèque de la requête

La *bibliothèque de la requête* est la bibliothèque dans laquelle sont stockées toutes les requêtes, les balises de requête et les filtres d'invite, prédéfinis et définis par l'utilisateur.

bibliothèque de rapports

La *bibliothèque de rapports* est la bibliothèque dans laquelle sont stockés tous les rapports, les balises de rapports, les rapports générés et les jobs de rapports planifiés, prédéfinis et définis par l'utilisateur.

CA Enterprise Log Manager

CA Enterprise Log Manager est une solution qui vous permet de collecter des journaux à partir de sources d'événement très dispersées et de différents types, de contrôler la conformité avec les requêtes et les rapports, et de conserver des enregistrements des bases de données de journaux compressés stockées à long terme sur un système externe.

CA IT PAM

CA IT PAM est l'acronyme de CA IT Process Automation Manager. Le rôle de ce produit CA est d'automatiser les processus que vous définissez. CA Enterprise Log Manager utilise deux processus : la création d'un processus de sortie de l'événement/de l'alerte pour un produit local, par exemple CA Service Desk, et la génération dynamique de listes qui peuvent être importées sous la forme de valeurs à clés. L'intégration requiert CA IT PAM r2.1.

CA Spectrum

CA Spectrum est un produit de gestion des défaillances réseau qui peut être intégré à CA Enterprise Log Manager pour être utilisé comme destination des alertes envoyées sous la forme d'interruptions SNMP.

CAELM

CAELM est le nom de l'instance d'application que CA EEM utilise pour CA Enterprise Log Manager. Pour accéder à la fonctionnalité CA Enterprise Log Manager dans CA Embedded Entitlements Manager, saisissez l'URL https://<adresse_ip>:5250/spin/eiam/eiam.csp, sélectionnez CAELM comme nom d'application, puis saisissez le mot de passe de l'utilisateur EiamAdmin.

caelmadmin

Le nom d'utilisateur et le mot de passe *caelmadmin* sont les informations d'identification nécessaires pour accéder au système d'exploitation du dispositif logiciel. L'ID d'utilisateur caelmadmin est créé lors de l'installation de ce système d'exploitation. Durant l'installation du composant logiciel, l'installateur doit spécifier le mot de passe du compte de superutilisateur CA EEM, EiamAdmin. Le même mot de passe est affecté au compte caelmadmin. Nous recommandons que l'administrateur du serveur se connecte via ssh en tant qu'utilisateur caelmadmin et modifie ce mot de passe par défaut. Bien que l'administrateur ne puisse pas se connecter via ssh en tant que root, il peut basculer sur le compte root (su root) si nécessaire.

caelmservice

caelmservice est un compte de service qui permet d'exécuter iGateway et les services CA EEM locaux en tant qu'utilisateur non root. Le compte caelmservice est utilisé pour installer les mises à jour du système d'exploitation téléchargées avec les mises à jour d'abonnement.

calendrier

Un *calendrier* est un moyen de limiter la durée d'application d'une stratégie d'accès. Une stratégie permet aux identités spécifiées d'effectuer les actions indiquées sur la ressource spécifiée durant le laps de temps déterminé.

CALM

CALM est une classe de ressource prédéfinie qui inclue les ressources CA Enterprise Log Manager suivantes : Alerte, ArchiveQuery, calmTag, Données, EventGrouping, Intégration et Rapport. Les actions autorisées pour cette ressource sont : Annotation (Rapports), Création (Alerte, calmTag, EventGrouping, Intégration et Rapport), Dataaccess (Données), Exécution (ArchiveQuery) et Planification (Alerte, Rapport).

calmTag

calmTag est un attribut nommé de l'AppObject utilisé lors de la création d'une stratégie de portée afin de limiter l'accès aux requêtes et rapports appartenant à certaines balises. Tous les rapports et requêtes sont des objets d'application (AppObjects) et ont calmTag comme attribut (à ne pas confondre avec la balise de ressource).

catalogue

Le *catalogue* est la base de données stockée sur chaque CA Enterprise Log Manager, qui consigne l'état des bases de données archivées et joue le rôle d'index de haut niveau pour l'ensemble des bases de données. Les informations d'état (tiède, froid ou dégivré) sont conservées pour toutes les bases de données ayant jamais transité par ce CA Enterprise Log Manager, ainsi que toutes celles ayant été restaurées sur ce CA Enterprise Log Manager en tant que base de données dégivrée. La fonction d'indexation s'étend à toutes les bases de données chaudes et tièdes contenues dans le magasin de journaux d'événements de ce CA Enterprise Log Manager.

catalogue d'archive

Voir catalogue.

catégories d'événement

Les *catégories d'événement* sont les balises utilisées par CA Enterprise Log Manager pour classer les événements selon leur fonction, avant de les insérer dans le magasin d'événements.

Certificats

Les *certificats* prédéfinis utilisés par CA Enterprise Log Manager sont CAELMCert.p12 et CAELM_AgentCert.p12. Tous les services CA Enterprise Log Manager utilisent CALEMCert.p12 pour communiquer avec le serveur de gestion. Tous les agents utilisent CAELM_AgentCert.p12 pour communiquer avec leur serveur de collecte.

Champs CEG

Les champs CEG sont des étiquettes utilisées pour normaliser la présentation des champs d'événements bruts provenant de sources d'événement hétérogènes. Lors de l'ajustement d'événement, CA Enterprise Log Manager analyse les messages d'événements bruts dans une série de paires nom-valeur, puis mappe les noms des événements bruts avec les champs CEG standard. L'ajustement crée des paires nom-valeur composées des champs CEG et des valeurs issues de l'événement brut. En d'autres termes, au cours de l'ajustement des événements bruts, les différentes étiquettes utilisées dans les événements bruts correspondant au même objet de données ou élément de réseau sont converties au même nom de champ CEG. Les champs CEG sont mappés aux OID de la MIB utilisée pour les interruptions SNMP.

client d'abonnement

Un *client d'abonnement* est un serveur CA Enterprise Log Manager qui récupère les mises à jour de contenu auprès d'un autre serveur CA Enterprise Log Manager, appelé serveur proxy d'abonnement. Les clients d'abonnement interrogent le serveur proxy d'abonnement configuré de manière régulière et planifiée, et ils récupèrent les nouvelles mises à jour disponibles, le cas échéant. Après récupération des mises à jour, le client installe les composants téléchargés.

collecte d'événements

La *collecte d'événements* est un processus permettant de lire la chaîne d'événement brut à partir d'une source d'événement et de l'envoyer au CA Enterprise Log Manager configuré. La collecte est suivie d'un ajustement d'événement.

collecte directe de journaux

La *collecte directe de journaux* est la technique de collecte de journaux sans agent intermédiaire entre la source d'événement et le logiciel CA Enterprise Log Manager.

collecteur SAPI

Le *collecteur SAPI* est un adaptateur CA qui reçoit des événements provenant de clients CA Audit. Les envois des clients CA Audit reposent sur l'action Collecteur, qui propose le basculement intégré. Les administrateurs configurent le collecteur SAPI CA Audit avec, par exemple, les fichiers de mappage de données et les chiffres sélectionnés.

composants de visualisation

Les *composants de visualisation* sont des options disponibles pour l'affichage des données de rapport, par exemple une table, un graphique (en courbes, à barres, à colonnes, à secteurs) ou une visionneuse d'événements.

compte

Un *compte* est un utilisateur global qui est également un utilisateur d'applications CALM. Une même personne peut posséder plusieurs comptes, chacun disposant d'un rôle personnalisé différent.

configuration enregistrée

Une *configuration enregistrée* est une configuration stockée avec les valeurs d'attributs d'accès aux données provenant d'une intégration pouvant être utilisée comme modèle lors de la création d'une nouvelle intégration.

configuration globale

La *configuration globale* est un ensemble de paramètres qui s'appliquent à tous les serveurs CA Enterprise Log Manager utilisant le même serveur de gestion.

connecteur

Un *connecteur* est une intégration ciblant une source d'événement spécifique, configurée sur un agent donné. Un agent peut charger en mémoire plusieurs connecteurs, similaires ou non. Le connecteur permet de collecter les événements bruts à partir d'une source d'événement et d'effectuer une transmission régulée (sur règle) des événements convertis vers un magasin de journaux d'événements, où ils seront insérés dans la base de données chaude. Les intégrations prêtes à l'emploi permettent une collecte optimisée à partir d'une large gamme de sources d'événement, notamment des systèmes d'exploitation, des bases de données, des serveurs Web, des pare-feu et de nombreux types d'applications de sécurité. Vous pouvez définir entièrement un connecteur pour une source d'événement interne ou utiliser une intégration comme modèle.

Contenu d'une interruption SNMP

Une *interruption SNMP* se compose de paires nom-valeur, chaque nom étant un OID (identificateur d'objet) et chaque valeur une valeur renvoyée par l'alerte planifiée. Les résultats de requête renvoyés par une alerte d'action contiennent des champs CEG ainsi que leurs valeurs. L'interruption SNMP est renseignée en substituant un OID à chaque champ CEG utilisé pour le nom de la paire nom-valeur. Le mappage de chaque champ avec un OID est stocké dans la MIB. L'interruption SNMP inclut uniquement les paires nom-valeur des champs que vous avez sélectionnés lorsque de la configuration de l'alerte.

cumul d'événements

Le *cumul d'événements* est le processus par lequel des entrées de journal similaires sont regroupées en une entrée unique, contenant un compteur d'occurrences d'événement. Les règles de récapitulation définissent le regroupement des événements.

dégel

Le *dégel* est le processus qui consiste à faire passer une base de données de l'état froid à l'état dégivré. Cette opération est réalisée par CA Enterprise Log Manager lorsque l'utilitaire LMArchive l'avertit qu'une base de données froide connue a été restaurée. Si la base de données froide n'est pas restaurée sur son CA Enterprise Log Manager original, l'utilitaire LMArchive n'est pas utilisé et aucun dégel n'est requis ; la fonction de recatalogage ajoute la base de données restaurée en tant que base de données tiède.

Destinations d'une interruption SNMP

Lorsque vous planifiez une alerte d'action, vous avez la possibilité d'ajouter plusieurs *destinations pour l'interruption SNMP*. Chacune d'entre elles est définie par une adresse IP et un numéro de port. Généralement, la destination est un NOC ou un serveur de gestion tel que CA Spectrum ou CA NSM. Une interruption SNMP est envoyée aux destinations configurées lorsque les requêtes d'un job d'alerte planifié renvoient des résultats.

détecteur de journaux

Un *détecteur de journaux* est un composant d'intégration conçu pour lire un type de journal spécifique, comme une base de données, Syslog, un fichier ou SNMP. Les détecteurs de journaux peuvent être réutilisés. Généralement, les utilisateurs ne créent pas de détecteur de journaux personnalisé.

dispositif logiciel

Le *dispositif logiciel* comprend un composant système d'exploitation et le composant logiciel CA Enterprise Log Manager.

dossier

Un *dossier* est un emplacement de répertoire que le serveur de gestion CA Enterprise Log Manager utilise pour stocker les types d'objet CA Enterprise Log Manager. Vous référencez des dossiers dans des stratégies de portée afin de permettre ou d'interdire à certains utilisateurs d'accéder au type d'objet spécifié.

éléments d'intégration

Les *éléments d'intégration* incluent un détecteur, une aide à la configuration, un fichier d'accès aux données, un ou plusieurs fichiers d'analyse de message (XMP) et un ou plusieurs fichiers de mappage de données.

enregistrement de journal

Un *enregistrement de journal* est un enregistrement d'audit individuel.

enregistrements d'audit

Les *enregistrements d'audit* contiennent les événements de sécurité de type tentatives d'authentification, accès aux fichiers et modifications apportées aux stratégies de sécurité, comptes d'utilisateur ou droits d'utilisateur. Les utilisateurs Administrator spécifient les types d'événement à auditer et ce qui doit être journalisé.

entrée de journal

Une *entrée de journal* est, dans un journal, l'emplacement contenant des informations sur un événement spécifique qui s'est produit sur un système ou un réseau donné.

état chaud d'une base de données

L'*état chaud* correspond à une base de données du magasin de journaux d'événements, où sont insérés de nouveaux événements. Lorsqu'une base de données chaude atteint sa taille maximale prédéfinie sur le serveur de collecte, elle est compressée, cataloguée et déplacée sur un système de stockage non compressé sur le serveur de rapports. De plus, tous les serveurs stockent les nouveaux événements d'autosurveillance dans une base de données chaude.

état dégivré d'une base de données

L'*état dégivré* est l'état qualifiant une base de données qui a été restaurée dans le répertoire d'archivage après l'exécution de l'utilitaire LMArchive par l'administrateur pour indiquer à CA Enterprise Log Manager que la base de données a été restaurée. Les bases de données dégivrées sont conservées pendant le nombre d'heures configuré pour la stratégie d'exportation. Vous pouvez effectuer des requêtes sur des journaux d'événements dans les bases de données chaudes, tièdes et dégivrées.

état froid d'une base de données

L'*état froid* s'applique à une base de données tiède lorsqu'un administrateur exécute l'utilitaire LMArchive pour avertir CA Enterprise Log Manager que la base de données a été sauvegardée. Les administrateurs doivent sauvegarder les bases de données tièdes et exécuter cet utilitaire avant que ces bases de données ne soient supprimées. En effet, une base de données tiède est automatiquement supprimée lorsque son ancienneté dépasse la valeur Nbre max. de jours d'archivage définie ou lorsque le seuil Espace disque d'archivage est atteint, dès que l'une de ces deux conditions est remplie. Vous pouvez interroger la base de données d'archivage pour identifier les bases de données dont l'état est tiède ou froid.

état tiède d'une base de données

L'*état tiède* correspond à une base de données chaude de journaux d'événements, qui est déplacée lorsque sa taille atteint la limite maximale spécifiée (Nombre maximum de lignes) ou lorsqu'un recatalogage est effectué après restauration d'une base de données froide dans un nouveau magasin de journaux d'événements. Les bases de données tièdes sont conservées dans le magasin de journaux d'événements jusqu'à ce que leur ancienneté (en jours) dépasse la valeur configurée pour le paramètre Nbre max. de jours d'archivage. Vous pouvez effectuer des requêtes sur des journaux d'événements dans les bases de données chaudes, tièdes et dégivrées.

états de base de données

Les *états d'une base de données* incluent "chaude" pour une base de données de nouveaux événements, "tiède" pour une base de données d'événements compressés, "froide" pour une base de données sauvegardée et "dégivrée" pour une base de données restaurée dans le magasin de journaux d'événements où elle avait été sauvegardée. Vous pouvez lancer une requête sur les bases de données chaudes, tièdes et dégivrées. Toutes les requêtes d'archivage affichent les informations relatives aux bases de données froides.

événement ajusté

Un *événement ajusté* contient les données d'événements mappés ou analysés, dérivées d'événements bruts ou récapitulés. CA Enterprise Log Manager réalise le mappage et l'analyse pour permettre les recherches sur les données stockées.

événement brut

Un *événement brut* correspond aux informations déclenchées par un événement natif envoyé par un agent de surveillance au collecteur Log Manager. L'événement brut est souvent présenté sous la forme d'une chaîne Syslog ou d'une paire nom/valeur. Il est possible d'examiner un événement sous sa forme brute dans CA Enterprise Log Manager.

événement d'autosurveillance

Un *événement d'autosurveillance* est un événement journalisé par CA Enterprise Log Manager. Ce type d'événement est automatiquement généré sur la base d'actes effectués par l'utilisateur et de fonctions réalisées par différents modules, tels que les services et les écouteurs. Pour consulter le rapport précisant les détails des événements d'autosurveillance des opérations SIM, sélectionnez un serveur de rapports et ouvrez l'onglet Evénements d'autosurveillance.

événement distant

Un *événement distant* est un événement impliquant deux ordinateurs hôtes distincts, la source et la destination. Un événement distant est de type 2, sur les quatre types d'événement utilisés dans la grammaire commune aux événements.

événement enregistré

Un *événement enregistré* contient les données d'un événement brut ou ajusté, après son intégration dans la base de données. Les événements bruts sont toujours enregistrés, sauf s'ils sont supprimés ou récapitulés, comme des événements ajustés. Ces informations sont stockées et peuvent être interrogées.

événement local

Un *événement local* est un événement impliquant une entité unique, où la source et la destination de l'événement correspondent au même ordinateur hôte. Un événement local est de type 1, sur les quatre types d'événement utilisés dans la grammaire commune aux événements.

événement natif

Un *événement natif* constitue l'état ou l'action déclenchant un événement brut. Les événements natifs sont reçus et analysés/mappés, le cas échéant, puis transmis en tant qu'événements bruts ou ajustés. Un échec d'authentification est un événement natif.

événement observé

Un *événement observé* est un événement impliquant une source, une destination et un agent, où l'événement est observé et enregistré par un agent de collecte d'événements.

événement RSS

Un *événement RSS* est un événement généré par CA Enterprise Log Manager pour transmettre une alerte d'action à des produits et utilisateurs tiers. L'événement est un récapitulatif de chaque résultat d'alerte d'action et un lien vers le fichier de résultat. La durée d'un flux RSS donné peut être configurée.

événements

Dans CA Enterprise Log Manager, les *événements* sont des enregistrements de journal générés par chaque source d'événement spécifiée.

event_action

event_action est le champ de quatrième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il décrit les actions communes. Les types d'action d'événement (event_action) incluent par exemple : Lancement d'un processus, Arrêt d'un processus et Erreur d'application.

event_category

event_category est le champ de deuxième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il permet une classification plus approfondie des événements, avec une valeur ideal_model spécifique. Les types de catégories d'événement (event_category) incluent : Sécurité opérationnelle, Gestion des identités, Gestion de la configuration, Accès aux ressources et Accès au système.

event_class

event_class est le champ de troisième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il permet une classification plus approfondie des événements, avec une valeur event_category spécifique.

explorateur d'agent

L'*Explorateur d'agent* est l'espace de stockage qui contient les paramètres de configuration d'un agent. Les agents peuvent être installés sur un point de collecte ou sur un terminal où il existe des sources d'événement.

fédération hiérarchique

Une *fédération hiérarchique* de serveurs CA Enterprise Log Manager est une topologie qui établit une relation hiérarchique entre les serveurs. Dans sa forme la plus simple, le serveur 2 est un enfant du serveur 1, mais le serveur 1 n'est pas un enfant du serveur 2. La relation est donc unilatérale. Une fédération hiérarchique peut posséder de nombreux niveaux de relation parent-enfant et un seul serveur parent peut avoir de nombreux serveurs enfants. Une requête fédérée renvoie ses résultats depuis le serveur sélectionné et ses enfants.

fédération maillée

Une *fédération maillée* de serveurs CA Enterprise Log Manager est une topologie qui établit une relation de parité entre les serveurs. Dans sa forme la plus simple, le serveur 2 est un enfant du serveur 1 et le serveur 1 est un enfant du serveur 2. Une paire de serveurs maillée a une relation bilatérale. Une fédération maillée peut être définie pour qu'un grand nombre de serveurs soient les pairs les uns des autres. Une requête fédérée renvoie ses résultats depuis le serveur sélectionné et tous ses pairs.

fichier d'analyse de message (XMP, Message Parsing File)

Un *fichier d'analyse de message (XMP)* est un fichier XML associé à un type de source d'événement spécifique, qui applique des règles d'analyse. Les règles d'analyse décomposent les données pertinentes d'un événement brut collecté, afin d'obtenir des paires nom/valeur qui sont ensuite transmises au fichier de mappage de données à des fins de traitement. Ce type de fichier est utilisé dans toutes les intégrations, ainsi que dans les connecteurs, qui sont eux-mêmes basés sur des intégrations. Dans le cas d'adaptateurs CA, les fichiers XMP peuvent également être appliqués au serveur CA Enterprise Log Manager.

fichiers de mappage de données

Les *fichiers de mappage des données* sont des fichiers XML utilisant la grammaire commune aux événements (CEG) de CA pour transformer des événements d'un format source en un format conforme CEG pouvant être stocké à des fins de rapport et d'analyse dans le magasin de journaux d'événements. Un fichier de mappage de données doit être créé pour chaque nom de journal pour que les données d'événement puissent être stockées. L'utilisateur peut modifier une copie du fichier de mappage de données et l'appliquer à un connecteur spécifié.

filtrage d'événements

Le *filtrage d'événements* est le processus de tri des événements sur la base de filtres CEG.

filtre

Un *filtre* est un moyen permettant de limiter les requêtes sur le magasin de journaux d'événements.

filtre d'accès

Un *filtre d'accès* est un filtre que l'administrateur peut définir pour contrôler les données d'événement pouvant être consultées par les utilisateurs ou groupes ne détenant pas le rôle Administrator. Un filtre d'accès peut, par exemple, limiter les données que des identités spécifiées peuvent afficher dans un rapport. Les filtres d'accès sont automatiquement convertis en stratégies d'obligation.

filtre global

Un *filtre global* est un ensemble de critères que vous pouvez spécifier pour limiter les éléments présentés dans tous les rapports. Par exemple, un filtre global pour les 7 derniers jours renvoie les événements générés au cours des sept derniers jours écoulés.

filtre local

Un *filtre local* est un ensemble de critères que vous pouvez spécifier lors de la consultation d'un rapport, pour limiter les données affichées dans ce rapport en cours.

gestion des agents

La *gestion des agents* est le processus logiciel qui contrôle l'ensemble des agents associés à l'ensemble de CA Enterprise Log Manager fédérés. Ce processus authentifie les agents avec lesquels il communique.

gestion des droits

La *gestion des droits* est la méthode qui permet de contrôler ce que les utilisateurs sont autorisés à faire une fois authentifiés et connectés à l'interface CA Enterprise Log Manager. Ceci implique des stratégies d'accès associées à des rôles affectés aux utilisateurs. Ces rôles, ou groupes d'utilisateurs d'applications, et stratégies d'accès peuvent être prédéfinis ou définis par l'utilisateur. La gestion des droits est assurée par le magasin d'utilisateurs interne du système CA Enterprise Log Manager.

gestion des journaux de sécurité informatique

La *gestion des journaux de sécurité informatique* est définie par le National Institute of Standards and Technology (NIST) comme étant le "processus permettant de générer, de transmettre, de stocker, d'analyser et d'éliminer les données des journaux de sécurité des ordinateurs".

grammaire commune aux événements (CEG)

La *grammaire commune aux événements* est le cadre qui propose un format standard utilisé par CA Enterprise Log Manager pour convertir les événements à l'aide de fichiers d'analyse et de mappage, avant de les stocker dans le magasin de journaux d'événements. La CEG utilise des champs communs et normalisés pour définir les événements de sécurité provenant de plates-formes et de produits différents. Les événements ne pouvant faire l'objet d'une analyse ou d'un mappage sont stockés en tant qu'événements bruts.

groupe d'agents

Un *groupe d'agents* est une balise que les utilisateurs peuvent appliquer aux agents sélectionnés, qui permet d'appliquer simultanément une configuration à plusieurs agents et de récupérer les rapports basés sur les groupes. Un agent donné peut appartenir à un seul groupe à la fois. Les groupes d'agents sont basés sur des critères définis par l'utilisateur, comme la région géographique ou l'importance.

groupe d'applications

Un *groupe d'applications* est un groupe spécifique à un produit, pouvant être affecté à un utilisateur global. Les groupes d'applications (ou rôles) prédéfinis pour CA Enterprise Log Manager sont Administrator, Analyst et Auditor. Ces groupes d'applications sont disponibles uniquement pour les utilisateurs CA Enterprise Log Manager ; ils ne peuvent pas être affectés aux utilisateurs d'autres produits enregistrés sur le même serveur CA EEM. Des groupes d'applications définis par l'utilisateur doivent être ajoutés à la stratégie d'accès aux applications CALM par défaut, pour que les utilisateurs de ces groupes puissent accéder à CA Enterprise Log Manager.

groupe d'utilisateurs

Un *groupe d'utilisateurs* peut être un groupe d'applications, un groupe global ou un groupe dynamique. Les groupes d'applications CA Enterprise Log Manager prédéfinis sont les rôles Administrator, Analyst et Auditor. Les utilisateurs CA Enterprise Log Manager peuvent faire partie des groupes globaux par le biais d'appartenances distinctes de CA Enterprise Log Manager. Les groupes dynamiques sont définis par l'utilisateur et créés via une stratégie de groupe dynamique.

groupe d'utilisateurs dynamique

Un *groupe d'utilisateurs dynamique* est composé d'utilisateurs globaux qui partagent un ou plusieurs attributs communs. Un groupe d'utilisateurs dynamique est créé par le biais d'une stratégie de groupe d'utilisateurs dynamique particulière dans laquelle le nom de la ressource est le nom du groupe d'utilisateurs dynamique et l'appartenance repose sur un ensemble de filtres configurés sur les attributs d'utilisateur et de groupe.

groupe global

Un *groupe global* est un groupe partagé sur les instances d'application enregistrées auprès du même serveur de gestion CA Enterprise Log Manager. N'importe quel utilisateur peut être affecté à un ou plusieurs groupes globaux. Des stratégies d'accès peuvent être définies avec les groupes globaux en tant qu'identités, afin d'autoriser ou d'interdire à ces dernières d'effectuer certaines actions sur les ressources sélectionnées.

ideal_model

ideal_model correspond à la technologie exprimant l'événement. Il s'agit du premier champ de la grammaire commune aux événements (CEG) dans la hiérarchie des champs utilisés pour la normalisation et la classification des événements. Les types de modèles idéaux (ideal_model) incluent : Antivirus, DBMS, Pare-feu, Système d'exploitation et Serveur Web. Les produits de pare-feu Check Point, Cisco PIX et Netscreen/Juniper peuvent être normalisés en saisissant la valeur "Pare-feu" dans le champ ideal_model.

identité

Dans CA Enterprise Log Manager, une *identité* est un utilisateur ou un groupe autorisé à accéder à l'instance d'application CAELM et à ses ressources. Pour tout produit CA, une identité peut être un utilisateur global, un utilisateur d'applications, un groupe global, un groupe d'applications ou un groupe dynamique.

installateur

L'*installateur* est la personne qui se charge d'installer le dispositif logiciel et les agents. Lors de la procédure d'installation, les noms d'utilisateur caelmadmin et EiamAdmin sont créés et le mot de passe spécifié pour EiamAdmin est affecté à caelmadmin. Les informations d'identification de caelmadmin sont requises pour le premier accès au système d'exploitation ; celles de EiamAdmin sont nécessaires pour le premier accès au logiciel CA Enterprise Log Manager et pour l'installation des agents.

instance d'application

Une *instance d'application* est un espace commun dans le référentiel CA EEM, où sont stockés tous les utilisateurs, groupes, contenus, stratégies d'autorisation et configurations. En général, tous les serveurs CA Enterprise Log Manager d'une entreprise utilisent la même instance d'application (par défaut, CAELM). Vous pouvez installer des serveurs CA Enterprise Log Manager avec différentes instances d'application, mais seuls les serveurs partageant la même instance d'application peuvent être fédérés. Les serveurs configurés pour utiliser le même serveur CA EEM avec différentes instances d'application partagent uniquement le magasin d'utilisateurs, les stratégies de mots de passe et les groupes globaux. Les différents produits CA ont des instances d'application par défaut différentes.

intégration

L'*intégration* est une méthode permettant de traiter les événements non classés en événements ajustés, pour pouvoir les afficher dans les requêtes et les rapports. L'intégration est mise en oeuvre avec un ensemble d'éléments qui permettent à un connecteur et un agent donnés de collecter les événements à partir d'un ou de plusieurs types de source d'événement, puis de les envoyer à CA Enterprise Log Manager. Cet ensemble d'éléments inclut le détecteur de journaux ainsi que les fichiers XMP et de mappage de données, conçus pour être lus à partir d'un produit spécifique. Les intégrations permettant de traiter les événements Syslog et les événements WMI sont des exemples d'intégrations prédéfinies. Vous pouvez créer des intégrations personnalisées pour permettre le traitement d'événements non classés.

invite

Une *invite* est un type de requête spécial qui affiche des résultats en fonction de la valeur que vous saisissez et des champs CEG que vous sélectionnez. Les lignes sont uniquement renvoyées pour les événements dont la valeur saisie apparaît dans au moins un des champs CEG sélectionnés.

jeton d'analyse de message (ELM)

Un *jeton d'analyse de message* est un modèle réutilisable servant à la création de la syntaxe d'expression régulière utilisée lors de l'analyse de message CA Enterprise Log Manager. A chaque jeton sont associés un nom, un type et une chaîne d'expression régulière.

journal

Un *journal* est un enregistrement d'audit, ou message enregistré, concernant un événement ou un ensemble d'événements. Un journal peut afficher différents types : journal d'audit, journal de transaction, journal d'intrusion, journal de connexion, enregistrement des performances système, journal des activités utilisateur ou alerte.

liste de contrôle d'accès d'identité

Une *liste de contrôle d'accès d'identité* vous permet de spécifier différentes actions que chaque identité sélectionnée peut exécuter sur les ressources indiquées. Par exemple, avec une liste de contrôle d'accès d'identité, vous pouvez préciser qu'une identité donnée peut créer des rapports et qu'une autre peut planifier et annoter des rapports. La liste de contrôle d'accès d'identité diffère de la liste de contrôle d'accès classique dans le sens où elle est centrée sur l'identité, et non sur la ressource.

magasin de journaux d'événements

Le *magasin de journaux d'événements* est un composant du serveur CA Enterprise Log Manager, dans lequel les événements entrants sont stockés dans des bases de données. Les bases de données du magasin de journaux d'événements doivent être sauvegardées et déplacées manuellement vers un système de stockage distant de journaux, avant le délai de suppression configuré. Les bases de données archivées peuvent être restaurées dans un magasin de journaux d'événements.

magasin d'utilisateurs

Un *magasin d'utilisateurs* est le référentiel contenant les informations et stratégies de mots de passe d'utilisateurs globaux. Par défaut, le magasin d'utilisateurs CA Enterprise Log Manager est le référentiel local, mais il peut être configuré pour faire référence à CA SiteMinder ou à un répertoire LDAP pris en charge, comme Microsoft Active Directory, Sun One ou Novell eDirectory. Quelle que soit la configuration du magasin d'utilisateurs, le référentiel local sur le serveur de gestion contient des informations spécifiques aux applications concernant les utilisateurs, comme leur rôle et les stratégies d'accès associées.

mappage de données

Le *mappage de données* est un processus consistant à mapper les paires de valeurs clés vers la CEG. Le mappage de données s'effectue sur la base d'un fichier de mappage de données.

mappages de fonctions

Les *mappages de fonctions* constituent une partie facultative du fichier de mappage de données pour une intégration produit. Ils servent à renseigner un champ de la grammaire commune aux événements lorsque la valeur requise ne peut être extraite directement de la source d'événement. Tous les mappages de fonctions se composent d'un nom de champ CEG, d'une valeur de champ de classe ou prédéfinie, ainsi que de la fonction utilisée pour obtenir ou calculer la valeur.

MIB (base de données d'informations de gestion)

La *MIB (base de données d'informations de gestion)* pour CA Enterprise Log Manager, CA-ELM.MIB, doit être importée et compilée par chaque produit devant recevoir des alertes sous la forme d'interruptions SNMP depuis CA Enterprise Log Manager. La MIB indique l'origine de chaque identificateur d'objet numérique (OID) utilisé dans un message d'interruption SNMP accompagnée d'une description de l'objet de données ou de l'élément de réseau en question. Dans la MIB pour les interruptions SNMP envoyées par CA Enterprise Log Manager, la description de chaque objet de données est destinée au champ CEG associé. La MIB permet de s'assurer que toutes les paires nom-valeur transmises dans une interruption SNMP sont correctement interprétées au niveau de la destination.

mises à jour d'abonnement

Les *mises à jour d'abonnement* correspondent aux fichiers binaires et non binaires mis à disposition par le serveur d'abonnement CA. Les fichiers binaires sont des mises à jour du module produit, généralement installées sur les systèmes CA Enterprise Log Manager. Les fichiers non binaires, ou mises à jour de contenu, sont enregistrés sur le serveur de gestion.

mises à jour du contenu

Les *mises à jour de contenu* constituent la partie non binaire des mises à jour d'abonnement et elles sont enregistrées sur le serveur de gestion CA Enterprise Log Manager. Les mises à jour de contenu incluent les fichiers XMP, les fichiers de mappage de données, les mises à jour de configuration pour les modules CA Enterprise Log Manager et les mises à jour de clé publique.

module (à télécharger)

Un *module* est un groupement logique de mises à jour de composant, mis à disposition des utilisateurs en téléchargement, sur la base d'un abonnement. Un module peut contenir des mises à jour de fichier binaire, de contenu, ou les deux. Par exemple, tous les rapports sont réunis dans un même module ; toutes les mises à jour de fichier binaire de sponsor sont regroupées dans un autre module. CA définit le contenu de chaque module.

module d'abonnement

Le *module d'abonnement* est le service qui permet de télécharger automatiquement les mises à jour d'abonnement à partir du serveur d'abonnement CA et de les distribuer à tous les serveurs et agents CA Enterprise Log Manager. Les paramètres globaux s'appliquent aux serveurs CA Enterprise Log Manager locaux ; les paramètres locaux indiquent notamment si le serveur est un proxy hors ligne, un proxy en ligne ou un client d'abonnement.

module d'extension d'événements iTech

Le *module d'extension d'événements iTech* est un adaptateur CA qu'un administrateur peut configurer à l'aide de fichiers de mappage sélectionnés. Il reçoit des événements provenant d'iRecorders, de CA EEM, d'iTechnology ou de tout produit capable d'envoyer des événements via iTechnology.

NIST

Le *National Institute of Standards and Technology (NIST)* est l'agence technologique fédérale américaine qui propose des recommandations dans une publication intitulée "Special Publication 800-92 *Guide to Computer Security Log Management*" (en anglais), qui ont servi de base pour CA Enterprise Log Manager.

nom d'utilisateur EiamAdmin

EiamAdmin est le nom de superutilisateur par défaut affecté au programme d'installation des serveurs CA Enterprise Log Manager. Lors de l'installation du premier logiciel CA Enterprise Log Manager, le programme d'installation crée un mot de passe pour ce compte de superutilisateur, sauf si un serveur CA EEM distant existe déjà. Dans ce cas, le programme d'installation doit entrer le mot de passe existant. Une fois le dispositif logiciel installé, le programme d'installation ouvre un navigateur à partir d'une station de travail, entre l'URL de CA Enterprise Log Manager et se connecte en tant qu'utilisateur EiamAdmin avec le mot de passe associé. Ce premier utilisateur configure le magasin d'utilisateurs, crée les stratégies de mots de passe et crée le premier compte d'utilisateur doté du rôle Administrator. L'utilisateur EiamAdmin peut également effectuer n'importe quelle opération contrôlée par CA EEM.

OID (identificateur d'objet)

L'*OID (identificateur d'objet)* est l'identifiant numérique unique d'un objet de données apparié à une valeur dans un message d'interruption SNMP. Chaque OID utilisé dans une interruption SNMP envoyée par CA Enterprise Log Manager est mappé à un champ CEG dans la MIB. La syntaxe d'un OID mappé à un champ CEG est la suivante : 1.3.6.1.4.1.791.9845.x.x.x, où 791 est le numéro d'entreprise de CA et 9845 est l'identifiant produit de CA Enterprise Log Manager.

point de collecte

Un *point de collecte* est un serveur sur lequel un agent est installé ; sur le réseau, ce serveur est proche de tous les serveurs contenant les sources d'événements associées aux connecteurs de son agent.

pozFolder

pozFolder est un attribut d'AppObject, dont la valeur correspond à l'emplacement parent de l'AppObject. L'attribut et la valeur pozFolder sont utilisés dans les filtres de stratégies d'accès, qui restreignent l'accès aux ressources telles que les rapports, les requêtes et les configurations.

processus de sortie de l'événement/de l'alerte

Le *processus de sortie de l'événement/de l'alerte* est un processus CA IT PAM qui invoque un produit tiers pour répondre aux données d'alerte configurées dans CA Enterprise Log Manager. Vous pouvez sélectionner Processus CA IT PAM comme destination lorsque vous planifiez un job d'alerte. Lorsqu'une alerte déclenche l'exécution du processus CA IT PAM, CA Enterprise Log Manager envoie les données d'alerte CA IT PAM, lesquelles sont ensuite transférées par CA IT PAM avec leurs propres paramètres de traitement au produit tiers dans le cadre du processus de sortie de l'événement/de l'alerte.

profil

Un *profil* est un ensemble facultatif et configurable de filtres de données et de balises, qui peut être spécifique à un produit, à une technologie ou à une catégorie donnée. Le filtre de balise d'un produit, par exemple, limite les balises répertoriées à la balise du produit sélectionné. Les filtres de données d'un produit affichent uniquement les données pour le produit spécifié dans les rapports que vous générez, les alertes que vous planifiez et les résultats de requête que vous affichez. Une fois créé le profil de votre choix, vous pouvez le configurer de manière à ce qu'il soit appliqué dès que vous vous connectez au système. Si vous créez plusieurs profils, vous pouvez appliquer un profil différent à différentes activités, lors d'une même session. Des filtres prédéfinis sont livrés avec les mises à jour d'abonnement.

proxies d'abonnement (pour le client)

Les *proxies d'abonnement pour le client* définissent la liste des proxies d'abonnement que le client contacte de manière circulaire pour obtenir les mises à jour du système d'exploitation et du logiciel CA Enterprise Log Manager. Si un proxy est occupé, le suivant sur la liste est contacté. Si tous les proxies sont indisponibles et que le client est en ligne, le proxy d'abonnement par défaut est utilisé.

proxies d'abonnement (pour les mises à jour de contenu)

Les *proxies d'abonnement pour les mises à jour de contenu* sont les proxies d'abonnement choisis pour mettre à jour le serveur de gestion CA Enterprise Log Manager avec les mises à jour de contenu téléchargées sur le serveur d'abonnement CA. Il est recommandé de configurer plusieurs proxies, à des fins de redondance.

proxy d'abonnement (en ligne)

Un *proxy d'abonnement en ligne* est un serveur CA Enterprise Log Manager doté d'un accès à Internet et chargé de récupérer les mises à jour d'abonnement auprès du serveur d'abonnement CA, de manière régulière et planifiée. Un proxy d'abonnement en ligne donné peut être inclus dans la liste des proxies pour un ou plusieurs clients, qui contactent les proxies répertoriés de manière circulaire afin de demander les mises à jour de fichiers binaires. S'il est configuré pour le faire, un proxy en ligne donné peut envoyer les nouvelles mises à jour de contenu et de configuration au serveur de gestion, sauf si cela a déjà été fait par un autre proxy. Le répertoire des mises à jour d'abonnement d'un proxy en ligne sélectionné est utilisé comme source pour copier les mises à jour sur les proxies d'abonnement hors ligne.

proxy d'abonnement (hors ligne)

Un *proxy d'abonnement hors ligne* est un serveur CA Enterprise Log Manager qui obtient les mises à jour d'abonnement par une copie de répertoire manuelle (à l'aide de scp) depuis un proxy d'abonnement en ligne. Les proxies d'abonnement hors ligne peuvent être configurés pour télécharger les mises à jour de fichiers binaires sur les clients qui les demandent et pour envoyer la dernière version des mises à jour de contenu au serveur de gestion, si celui-ci ne l'a pas déjà reçue. Les proxies d'abonnement hors ligne n'ont pas besoin d'accès à Internet.

proxy d'abonnement (par défaut)

Le *proxy d'abonnement par défaut* est généralement le serveur CA Enterprise Log Manager installé en premier ; il peut également s'agir du serveur CA Enterprise Log Manager principal. Ce serveur sert également de proxy d'abonnement en ligne et doit, par conséquent, être doté d'un accès à Internet. Si aucun autre proxy d'abonnement en ligne n'est défini, ce serveur obtient les mises à jour d'abonnement auprès du serveur d'abonnement CA, puis télécharge les mises à jour de fichiers binaires sur tous les clients et envoie les mises à jour de contenu à CA EEM. Si d'autres proxies sont définis, le serveur obtient tout de même les mises à jour d'abonnement, mais il est contacté par les clients uniquement lorsque aucune liste de proxies d'abonnement n'est configurée ou lorsque la liste configurée est épuisée.

rapport

Un *rapport* est une représentation graphique ou tabulaire des données de journal d'événements qui est générée en exécutant des requêtes prédéfinies ou personnalisées à l'aide de filtres. Les données peuvent être issues de bases de données chaudes, tièdes et dégivrées dans le magasin de journaux d'événements du serveur sélectionné et, sur demande, de ses serveurs fédérés.

rapports EPHI

Les *rapports EPHI* (Electronic Protected Health Information) sont des rapports relatifs à la sécurité HIPAA (Health Insurance Portability and Accountability Act). Ces rapports peuvent vous aider à démontrer que toutes les informations médicales associées aux patients et identifiables individuellement, qui sont créées, stockées et transmises de manière électronique, sont protégées.

recatalogage

Le *recatalogage* est une révision forcée du catalogue. Un recatalogage est requis uniquement lors de la restauration de données dans un magasin de journaux d'événements situé sur un serveur différent de celui sur lequel les données ont été générées. Par exemple, si vous avez désigné CA Enterprise Log Manager comme point de restauration pour l'examen des données sauvegardées, vous devez imposer un recatalogage de la base de données après l'avoir restaurée depuis son point de restauration désigné. Un recatalogage est exécuté automatiquement au redémarrage d'iGateway, si nécessaire. Recataloguer un seul fichier de base de données peut prendre plusieurs heures.

règles de récapitulation

Les *règles de récapitulation* sont des règles combinant certains événements natifs, d'un même type, en un seul événement ajusté. Par exemple, une règle de récapitulation peut être configurée pour remplacer par un seul événement de récapitulation jusqu'à 1 000 événements dupliqués, dont les adresses IP et les ports source et de destination sont identiques. De telles règles simplifient l'analyse des événements et réduisent le trafic associé aux journaux.

règles de suppression

Les *règles de suppression* sont des règles que vous configurez pour éviter que certains événements ajustés n'apparaissent dans vos rapports. Vous pouvez créer des règles de suppression permanentes afin de supprimer des événements de routine sans rapport avec des problèmes de sécurité ; vous pouvez également créer des règles temporaires afin de supprimer la journalisation d'événements planifiés tels que la création de nombreux utilisateurs.

règles de transfert d'événement

Les règles de transfert d'événement stipulent que les événements sélectionnés sont transférés à des produits tiers, par exemple ceux qui mettent les événements en corrélation, après leur sauvegarde dans le magasin des journaux d'événements.

requête

Une *requête* est un ensemble de critères utilisés pour effectuer une recherche dans les magasins de journaux d'événements du serveur CA Enterprise Log Manager actif et, le cas échéant, de ses serveurs fédérés. Une requête cible les bases de données chaudes, tièdes ou dégivrées spécifiées dans la clause where de la requête. Par exemple, si la clause where limite la requête aux événements pour lesquels source_username="myname" sur une période donnée et que seules dix des 1 000 bases de données contiennent des enregistrements répondant à ces critères, sur la base des informations fournies dans la base de données de catalogue, la requête sera exécutée uniquement sur ces dix bases de données. Une requête peut renvoyer 5 000 lignes de données au maximum. Tout utilisateur doté d'un rôle prédéfini peut exécuter une requête. Seuls les analystes et les administrateurs peuvent planifier une requête pour diffuser une alerte d'action, créer un rapport en sélectionnant les requêtes à inclure, ou encore créer une requête personnalisée à l'aide de l'assistant de conception de requête. Voir également requête d'archivage.

requête d'action

Une *requête d'action* est une requête prenant en charge une alerte d'action. Elle est exécutée de manière planifiée et récurrente, pour tester les conditions définies par l'alerte d'action à laquelle elle est associée.

requête d'archivage

Une *requête d'archivage* est une requête du catalogue utilisée pour identifier les bases de données froides devant être restaurées et dégivrées à des fins de requête. Une requête d'archivage diffère d'une requête normale dans le sens où elle cible les bases de données froides, tandis que les requêtes normales ciblent uniquement les bases chaudes, tièdes et dégivrées. Les administrateurs peuvent émettre une requête d'archivage grâce à l'option Requête de catalogue d'archive du sous-onglet Collecte de journaux, dans l'onglet Administration.

ressource d'application

Le terme *ressource d'application* correspond à toutes les ressources spécifiques à CA Enterprise Log Manager, sur lesquelles les stratégies d'accès CALM autorisent ou interdisent à des identités données d'effectuer certaines actions spécifiques à l'application, par exemple créer, planifier et modifier. Rapport, alerte et intégration sont des exemples de ressource d'application. Voir également ressource globale.

ressource globale

Une *ressource globale*, pour le produit CA Enterprise Log Manager, est une ressource partagée avec les autres applications CA. Vous pouvez créer des stratégies de portée pour les ressources globales. Utilisateur, stratégie et calendrier sont des exemples de ressource globale. Voir également ressource d'application.

rôle Administrator

Le *rôle Administrator* accorde aux utilisateurs la possibilité d'effectuer toutes les actions valides existantes sur l'ensemble des ressources CA Enterprise Log Manager. Seuls les utilisateurs Administrator sont autorisés à configurer les services et la collecte de journaux, ou encore à gérer les utilisateurs, les stratégies d'accès et les filtres d'accès.

rôle Analyst

Le *rôle Analyst* accorde aux utilisateurs la possibilité de créer et de modifier des requêtes et rapports personnalisés, de modifier et d'annoter les rapports, de créer des balises, ou encore de planifier des rapports et alertes d'action. Les utilisateurs Analyst peuvent également réaliser toutes les tâches du rôle Auditor.

rôle Auditor

Le *rôle Auditor* accorde aux utilisateurs l'accès aux rapports et à leurs données. Les utilisateurs Auditor peuvent afficher les rapports, la liste des modèles de rapport, la liste des jobs de rapports planifiés et la liste des rapports générés. Les utilisateurs Auditor peuvent planifier et annoter des rapports. Ils n'ont pas accès aux flux RSS (Rich Site Summary), à moins qu'aucune authentification ne soit requise pour l'affichage des alertes d'action.

rôle d'utilisateur

Un *rôle d'utilisateur* peut être un groupe d'utilisateurs d'applications prédéfini ou un groupe d'applications défini par l'utilisateur. Des rôles d'utilisateur personnalisés sont nécessaires lorsque les groupes d'applications prédéfinis (Administrator, Analyst et Auditor) ne sont pas suffisamment affinés pour refléter les attributions de tâches. Les rôles d'utilisateur personnalisés nécessitent des stratégies d'accès personnalisées et une modification des stratégies prédéfinies pour inclure le nouveau rôle.

routeur SAPI

Le *routeur SAPI* est un adaptateur CA qui reçoit les événements provenant des intégrations, de type Mainframe, et les renvoie au routeur CA Audit.

SafeObject

SafeObject est une classe de ressource prédéfinie dans CA EEM. Il s'agit de la classe de ressource à laquelle appartient AppObjects, stockée dans la portée de l'application. Les utilisateurs définissant des stratégies et des filtres permettant d'accéder aux AppObjects se réfèrent à cette classe de ressource.

SAPI Recorder

SAPI Recorder était la technologie utilisée pour envoyer les données à CA Audit, avant l'apparition d'iTechnology. SAPI signifie Submit API (Application Programming Interface) ou API de soumission. Les enregistreurs CA Audit pour CA ACF2, CA Top Secret, RACF, Oracle, Sybase et DB2 sont des exemples de SAPI Recorders.

serveur d'abonnement CA

Le *serveur d'abonnement CA* est la source des mises à jour d'abonnement de CA.

serveur d'alerte

Le *serveur d'alerte* sert à stocker les alertes d'action et les jobs d'alerte d'action.

serveur de collecte

Le *serveur de collecte* est un rôle attribué à un serveur CA Enterprise Log Manager. Le serveur de collecte ajuste les journaux d'événement entrants, les intègre à la base de données chaude, compresse celle-ci et en effectue un archivage automatique ou bien la copie sur le serveur de rapports associé. Le serveur de collecte compresse la base de données chaude lorsqu'elle atteint la taille maximale prédéfinie et effectue un archivage automatique selon le planning indiqué.

serveur de gestion

Le *serveur de gestion* est un rôle attribué au premier serveur CA Enterprise Log Manager installé. Ce serveur CA Enterprise Log Manager contient le référentiel chargé de stocker le contenu de tous ses serveurs CA Enterprise Log Manager, notamment les stratégies. Ce serveur correspond généralement au proxy d'abonnement par défaut. Bien que cela ne soit pas recommandé dans la plupart des environnements de production, le serveur de gestion peut prendre en charge tous les rôles.

serveur de point de restauration

Le *serveur de point de restauration* est un rôle attribué à un serveur CA Enterprise Log Manager. Pour étudier des événements sauvegardés, vous pouvez transférer des bases de données depuis le serveur de stockage distant jusqu'au serveur de point de restauration à l'aide d'un utilitaire, puis ajouter ces bases au catalogue et exécuter les requêtes de votre choix. Transférer des bases de données froides vers un point de restauration dédié est une alternative intéressante à la restauration de ces bases sur le serveur de rapports original.

serveur de rapports

Le *serveur de rapports* est un rôle attribué à un serveur CA Enterprise Log Manager. Le serveur de rapports reçoit les bases de données tièdes archivées automatiquement en provenance d'un ou plusieurs serveurs de collecte. Il traite les requêtes, les rapports, ainsi que les alertes et les rapports planifiés.

serveur de rapports

Le *serveur de rapports* est le service qui stocke les informations de configuration, telles que le serveur de messagerie à utiliser lors de l'envoi des alertes par courriel, l'apparence des rapports enregistrés au format PDF, ainsi que la conservation des stratégies pour les rapports enregistrés sur le serveur de rapports et les alertes envoyées au flux RSS.

serveur de stockage distant

Le *serveur de stockage distant* est un rôle attribué à un serveur qui reçoit les bases de données archivées automatiquement en provenance d'un ou plusieurs serveurs de rapports. Le serveur de stockage distant conserve les bases de données froides pendant le nombre d'années requis. L'hôte distant utilisé pour le stockage ne dispose généralement pas d'un système CA Enterprise Log Manager ou autre. Pour l'archivage automatique, configurez une authentification non interactive.

serveur ODBC

Le *serveur ODBC* est le service configuré qui définit le port utilisé pour les communications entre le client ODBC ou JDBC et le serveur CA Enterprise Log Manager et détermine si le chiffrement SSL est activé ou non.

serveur proxy HTTP

Un *serveur proxy HTTP* est un serveur proxy qui joue le rôle de pare-feu et empêche le trafic Internet de pénétrer dans l'entreprise ou de la quitter, hormis via le proxy. Le trafic sortant peut spécifier un ID et un mot de passe pour contourner le serveur proxy. L'utilisation d'un serveur proxy HTTP local dans la gestion de l'abonnement est configurable.

serveurs de fédération

Les *serveurs de fédération* sont des serveurs CA Enterprise Log Manager connectés les uns aux autres sur un réseau, afin de répartir la collecte des données de journal, tout en cumulant les données collectées à des fins de génération de rapports. Les serveurs de fédération peuvent être connectés selon une topologie hiérarchique ou maillée. Les rapports de données fédérées incluent celles provenant du serveur cible, ainsi que de ses enfants ou pairs, le cas échéant.

services

Les *services* CA Enterprise Log Manager sont le magasin de journaux d'événements, le serveur de rapports et l'abonnement. Les administrateurs configurent ces services au niveau global, où tous les paramètres s'appliquent à l'ensemble de CA Enterprise Log Manager par défaut. La plupart des paramètres globaux de services peuvent être remplacés au niveau local, pour CA Enterprise Log Manager donné.

SNMP

SNMP est l'acronyme de Simple Network Management Protocol (protocole simple de gestion de réseau), une norme ouverte de transmission de messages d'alerte sous la forme d'interruptions SNMP depuis un agent vers un ou plusieurs systèmes de gestion.

source d'événement

Une *source d'événement* est l'hôte à partir duquel un connecteur collecte des événements bruts. Une source d'événement peut contenir plusieurs magasins de journaux, tous accessibles via un connecteur différent. En général, le déploiement d'un nouveau connecteur implique la configuration de la source d'événement de sorte que l'agent puisse y accéder et lire les événements bruts à partir de l'un de ses magasins de journaux. Les événements bruts du système d'exploitation, des bases de données différentes et une variété d'applications de sécurité sont stockés séparément sur la source d'événement.

stockage des journaux d'événements

Le *stockage des journaux d'événements* est le résultat du processus d'archivage, lorsque l'utilisateur sauvegarde une base de données tiède, avertit CA Enterprise Log Manager en exécutant l'utilitaire LMArchive et déplace la base de données sauvegardée depuis le magasin de journaux d'événements jusqu'à l'emplacement de stockage à long terme.

stratégie d'accès

Une *stratégie d'accès* est une règle qui accorde ou refuse à une identité (utilisateur ou groupe d'utilisateurs) des droits d'accès à une ressource d'application. CA Enterprise Log Manager détermine si les stratégies s'appliquent à l'utilisateur concerné en faisant correspondre les identités, les ressources, les classes de ressources et en évaluant les filtres.

stratégie d'accès aux applications CALM

La *stratégie d'accès aux applications CALM* est une stratégie de portée de type Liste de contrôle d'accès, qui détermine qui peut se connecter au serveur CA Enterprise Log Manager. Par défaut, la connexion est autorisée pour les rôles Administrator [Groupe], Analyst [Groupe] et Auditor [Groupe].

stratégie de délégation

Une *stratégie de délégation* est une stratégie d'accès qui permet à un utilisateur de déléguer son autorité à un autre utilisateur, groupe d'applications, groupe global ou groupe dynamique. Vous devez supprimer explicitement les stratégies de délégation créées par un utilisateur supprimé ou désactivé.

stratégie de portée

Une *stratégie de portée* est un type de stratégie d'accès qui octroie ou interdit l'accès aux ressources stockées sur le serveur de gestion, notamment les AppObjects, les utilisateurs, les groupes, les dossiers et les stratégies. Une stratégie de portée définit les identités pouvant accéder aux ressources spécifiées.

stratégie d'obligation

Une *stratégie d'obligation* est une stratégie générée automatiquement lorsque vous créez un filtre d'accès. Vous ne pouvez pas créer, modifier ou supprimer directement une stratégie d'obligation. Vous devez plutôt créer, modifier ou supprimer le filtre d'accès correspondant.

suppression

La *suppression* est le processus de tri des événements sur la base de filtres CEG. La suppression s'effectue sur la base de fichiers SUP.

traitement des valeurs dynamiques

Un *traitement des valeurs dynamiques* est un processus CA IT PAM que vous pouvez invoquer pour renseigner ou mettre à jour la liste de valeurs d'une clé donnée utilisée dans des rapports ou des alertes. Vous fournissez le chemin d'accès au traitement des valeurs dynamiques lors de la configuration de CA IT PAM dans la liste des services de serveurs de rapports de l'onglet Administration. Vous cliquez sur Importer la liste des valeurs dynamiques dans la section Valeur associée aux valeurs clés sur la même page de l'interface utilisateur. L'invocation du traitement des valeurs dynamiques est l'une des trois méthodes qui vous permettent d'ajouter des valeurs à vos clés.

URL de CA Embedded Entitlements Manager

L'*URL de CA Embedded Entitlements Manager* (CA EEM) est : https://<adresse_ip>:5250/spin/eiam. Pour ouvrir une session, sélectionnez CAELM comme application et saisissez le mot de passe associé au nom d'utilisateur EiamAdmin.

URL de CA Enterprise Log Manager

L'*URL de CA Enterprise Log Manager* est : https://<adresse_ip>:5250/spin/calm. Pour ouvrir une session, saisissez le nom d'utilisateur défini pour votre compte par l'administrateur, puis le mot de passe associé. Vous pouvez également saisir le nom de superutilisateur par défaut, EiamAdmin, puis entrer le mot de passe associé.

URL du flux RSS pour l'abonnement

L'*URL du flux RSS pour l'abonnement* est un lien préconfiguré, utilisé par les serveurs proxy d'abonnement en ligne lors de la récupération des mises à jour d'abonnement. Cette URL est destinée au serveur d'abonnement CA.

URL du flux RSS pour les alertes d'action

L'*URL du flux RSS pour les alertes d'action* est : https://{nomhôteelm}:5250/spin/calm/getActionQueryRssFeeds.csp. A partir de cette URL, vous pouvez afficher les alertes d'action soumises à la configuration définie en termes de quantité et d'ancienneté maximales.

utilisateur d'application

Un *utilisateur d'application* est un utilisateur global auquel ont été attribués des détails au niveau de l'application. Les détails d'utilisateur d'application CA Enterprise Log Manager incluent le groupe d'utilisateurs et les éventuelles restrictions d'accès. Si le magasin d'utilisateurs est le référentiel local, les détails de l'utilisateur d'application incluent également les informations d'identification de connexion et les stratégies de mots de passe.

utilisateur EEM

L'*utilisateur EEM*, configuré dans la section Archivage automatique du Magasin de journaux d'événements, spécifie l'utilisateur autorisé à exécuter une requête d'archivage, à recataloguer la base de données d'archivage, à exécuter l'utilitaire LMArchive et à exécuter le script shell restore-ca-elm pour restaurer les bases de données d'archivage à des fins d'examen. Cet utilisateur doit posséder le rôle prédéfini Administrator ou un rôle personnalisé associé à une stratégie personnalisée qui autorise l'action Modifier sur la ressource Base de données.

utilisateur global

Un *utilisateur global* se compose des informations de compte d'utilisateur, à l'exclusion des données propres aux applications. Les détails de l'utilisateur global et les appartenances au groupe global sont partagés par l'ensemble des applications CA intégrant le magasin d'utilisateurs par défaut. Les détails de l'utilisateur global peuvent être stockés dans le référentiel intégré ou dans un répertoire externe.

utilitaire LMArchive

LMArchive est l'utilitaire de ligne de commande qui suit la sauvegarde et la restauration des bases de données d'archive vers le magasin de journaux d'événements d'un serveur CA Enterprise Log Manager. Utilisez LMArchive pour effectuer une requête sur la liste des fichiers de bases de données tièdes, prêts à être archivés. Après avoir sauvegardé la base de données répertoriée et l'avoir transférée sur un stockage à long terme (froid), utilisez LMArchive pour créer un enregistrement sur CA Enterprise Log Manager, indiquant que cette base de données a été sauvegardée. Suite à la restauration d'une base de données froide sur son CA Enterprise Log Manager d'origine, utilisez LMArchive pour notifier CA Enterprise Log Manager, qui place alors les fichiers de bases de données dans un état dégivré, accessible aux requêtes.

utilitaire LMSEOSImport

LMSEOSImport est un utilitaire de ligne de commande utilisé pour importer SEOSDATA, ou des événements existants, dans CA Enterprise Log Manager dans le cadre de la migration depuis le générateur de rapports, la visionneuse ou le collecteur d'Audit. L'utilitaire est pris en charge uniquement par Microsoft Windows et Sun Solaris Sparc.

utilitaire scp

La copie sécurisée *scp* (programme de copie de fichiers à distance) est un utilitaire UNIX qui permet de transférer des fichiers entre les ordinateurs UNIX d'un réseau. Cet utilitaire est fourni lors de l'installation CA Enterprise Log Manager, pour que vous puissiez transférer les fichiers de mise à jour d'abonnement depuis le proxy d'abonnement en ligne jusqu'au proxy d'abonnement hors ligne.

valeurs clés

Les *valeurs clés* sont des valeurs définies par l'utilisateur et affectées à une liste définie par l'utilisateur (groupe clé). Lorsqu'une requête utilise un groupe clé, les résultats de la recherche incluent les correspondances avec toutes les valeurs clés du groupe. Il existe plusieurs groupes clés prédéfinis ; certains contiennent des valeurs clés prédéfinies, utilisées dans les requêtes et rapports prédéfinis.

Index

A

B

C

D

E

F

G

I

J

L

M

P

R

S

T

U

V