CA Identity Manager™

Notes de parution

12.6.4

Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA CloudMinder™ Identity Management
- Annuaire de listes CA
- CA Identity Manager ™
- CA Identity Governance (anciennement CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

Support technique

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

Table des matières

Chapitre 1: Nouvelles fonctionnalités

Ce chapitre traite des sujets suivants :

12.6.4

Modifications apportées aux fonctionnalités existantes

Prise en charge de la nouvelle version de CABI

Dans cette version de CA Identity Manager, uniquement CA Business Intelligence (CABI) version 3.3 SP1 est pris en charge. Le kit d'installation de CA Identity Manager contient les programmes d'installation de CABI 3.3 et CABI 3.3 SP1. Vous devez installer CABI 3.3, puis installer CABI 3.3 SP1.

Nouvelles certifications

Les nouvelles plates-formes suivantes sont certifiées avec CA Identity Manager r12.6.4 :

Terminaux

- CA Control Minder r12.8 en tant que terminal
- Microsoft Windows 2012 R2 Active Directory en tant que terminal
- Base de données Oracle 12c en tant que terminal
- Microsoft Lync Server 2010 et 2013 en tant que terminal
- PeopleSoft Financials 9.2 en tant que terminal
- System for Cross-domain Identity Management (SCIM) en tant que terminal
- Lotus Notes Domino 9.x en tant que terminal

Terminaux de services Web (Layer7)

- Service Now
- Microsoft Azure
- Zendesk

Serveur d'applications

- JBoss 6.2.0 EAP

Référentiel d'utilisateurs pour CA Identity Manager

- Oracle 12c
- Microsoft Windows 2012 R2 Active Directory

Référentiel d'objets pour CA Identity Manager

- Oracle 12c

Fournisseur d'informations d'identification

- Microsoft Windows 8
- Microsoft Windows 8.1

Prise en charge supplémentaire

- Prise en charge de l'agent de synchronisation de mots de passe sur Windows Active Directory 2012 R2
- Intégration à CA SiteMinder r12.52 CR1, r12.52 SP1 et r12.51 CR3
- Prise en charge du navigateur Internet Explorer 11.x
- Prise en charge du navigateur Firefox 29.x

Amélioration du connecteur Top Secret v2 pour la prise en charge d'objets/attributs supplémentaires

Le connecteur Top Secret v2 a été amélioré pour afficher les ressources, les fonctionnalités, les segments et tous les autres attributs dans le mainframe.

Améliorations apportées à la modification de mot de passe dans l'application mobile

L'application mobile comprend des niveaux de sécurité supplémentaires lors de la réinitialisation du mot de passe, qui impliquent les flux de codes PIN et de question/réponse. Pour plus d'informations, reportez-vous au *Manuel d'administration*.

Améliorations apportées au client de chargement en bloc

Le client de chargement en bloc a été amélioré pour prendre en charge les transformations Kettle en tant que source de données et action secondaire, de manière identique à ce qui se trouve dans l'interface utilisateur de la fonctionnalité de tâches en bloc.

Prise en charge de l'application mobile pour le système d'exploitation Android

L'application mobile prend désormais en charge les dispositifs mobiles qui utilisent le système d'exploitation Android.

Prise en charge de la personnalisation de SCIM et du connecteur de services Web par le connecteur Connector Xpress

Le connecteur Connector Xpress a été amélioré afin de prendre en charge la personnalisation des métadonnées SCIM et du connecteur de services Web pour :

- Service Now
- Azure
- Zendesk

Prise en charge des services Web SOAP et REST par Policy Xpress

Policy Xpress a été amélioré afin de prendre en charge les services Web SOAP (avec la méthode d'authentification de base) et REST (avec les méthodes d'authentification de base, d'authentification de proxy et d'authentification OAuth), de façon à ce que vous pouviez l'intégrer à des applications externes qui fournissent une interface de service Web.

Fenêtre de recherche de la tâche Afficher ma liste de travail

Une nouvelle fenêtre de recherche a été ajoutée à la tâche Afficher ma liste de travail. Elle vous permet d'effectuer des recherches par l'ID d'utilisateur de l'objet de flux de travaux ou par l'initiateur de la tâche afin de filtrer les tâches.

12.6.3

Nouvelles certifications

Les nouvelles plates-formes suivantes sont certifiées avec CA Identity Manager r12.6.3 :

Terminaux

- Microsoft Active Directory Exchange Server 2013 en tant que terminal
- Salesforce v24 en tant que terminal
- Solaris 11.1 en tant que terminal
- SuSE 11 SP3 en tant que terminal
- CA Directory r12.0 SP12 GA en tant que terminal JNDI Connector Xpress
- CA ACF2 LDAP r15.1 en tant que terminal
- CA RACF LDAP r15.1 en tant que terminal
- CA TSS LDAP r15.1 en tant que terminal

Systèmes d'exploitation de serveur

- Windows 2012 Essentials

Systèmes d'exploitation de client de serveur

- Windows 2012 Essentials
- Windows 8

Serveur d'applications

- JBoss 6.1.1 EAP

Référentiel d'utilisateurs CA Identity Manager

- CA Directory r12.0 SP12 GA
- Microsoft Active Directory 2012 Essentials
- Microsoft ADAM 2012 Essentials

Prise en charge supplémentaire

- Prise en charge de l'agent de synchronisation de mots de passe sur Active Directory 2012 Essentials
- Internet Explorer 10.x
- Google Chrome 28.x
- Intégration à CA SiteMinder r12.5 CR3 et r12.51 CR1
- Prise en charge d'UNIX Agentless sur RHEL, SuSE, Solaris, AIX et HP-UX
- Prise en charge des protocoles de monodiffusion et de multidiffusion avec JBoss 6.1.0 EAP

- Prise en charge de CAM 1.14 avec les agents distants de cette version
- Prise en charge d'AXIS2 1.6.2 avec cette version

Prise en charge du protocole de monodiffusion pour JBoss 6.1 EAP

Pour les clients qui installent CA Identity Manager sur JBoss 6.1 EAP, le protocole de monodiffusion est un protocole de messagerie alternatif au protocole de multidiffusion. Il est recommandé de tester les deux protocoles afin de déterminer le protocole le mieux adapté à votre organisation.

Pour plus d'informations sur l'utilisation de ces protocoles, consultez le manuel *Upgrade Guide* pour JBoss.

Génération de courriels et de données d'audit par les nouveaux événements

Vous pouvez activer les notifications par courriel et les données d'audit pour deux nouveaux événements :

- ForgottenPasswordAuditEventQnAInitiated

  La tâche publique Mot de passe oublié génère cet événement lorsqu'un utilisateur affiche la page de questions et de réponses au cours de la réinitialisation du mot de passe.

- ForgottenPasswordAuditEventQnALocked

  La tâche publique Mot de passe oublié génère cet événement lorsque la page de questions et de réponses est verrouillée après plusieurs tentatives infructueuses de répondre aux questions de sécurité.

Vous configurez les notifications par courriel et l'audit à partir de la console de gestion.

Remarque : Pour plus d'informations sur la configuration des notifications par courriel, consultez le *Manuel d'administration*. Pour plus d'information sur la configuration de l'audit, consultez le *Manuel de configuration*.

Prise en charge de la fonctionnalité ID Vault de Lotus Notes Domino

La fonctionnalité ID Vault de Lotus Notes Domino est désormais prise en charge à compter de cette version. Cette fonctionnalité vous permet de façon native et sécurisée de récupérer et de réinitialiser des mots de passe, de récupérer des ID perdus, de renommer des utilisateurs, etc.

Capture d'informations d'en-tête HTTP

Le nouveau filtre de servlet ClientExtractFilter a été ajouté dans cette version. Ce filtre de servlet est l'outil principal permettant d'extraire toutes les informations associées à l'environnement de client Web. Il permet d'extraire des informations à partir d'en-têtes HTTP. Actuellement, seule l'adresse IP du client est extraite. Toutefois, cette information n'est extraite qu'une seule fois pour chaque demande.

Ce filtre de servlet est exécuté pour chaque demande, comme suggéré par la section URL pattern:/* du fichier web.xml.

La classe d'utilitaire WebClientInformation a été ajoutée. Elle sert d'espace réservé pour les informations de client Web extraites par le filtre. Actuellement, cette classe conserve uniquement l'adresse IP, mais elle pourra être améliorée à l'avenir.

Cette classe est ensuite placée dans TaskSession en tant qu'attribut identifié par la clé WebClientInfo. Tous les événements, tâches, interfaces utilisateur ou flux de travaux créés suite à une demande contiendront donc les informations du client à partir duquel la demande a été émise.

Améliorations des objets de service

Une nouvelle case à cocher Retirer le service de l'utilisateur permettant de déterminer si le service doit être retiré avant la suppression a été ajoutée dans la tâche Supprimer un utilisateur.

Le filtrage de la tâche Demander et afficher un accès est désormais pris en charge pour permettre à l'utilisateur d'accéder à la section de recherche pour les administrateurs et aux options de recherche de propriétaire.

Les informations spécifiques d'une demande de service, telles que la durée de la demande de service ou les données de l'utilisateur sont affichées dans l'élément de flux de travaux d'approbation de la demande de service. Ces informations sont également envoyées dans une notification par courriel lorsqu'une stratégie globale basée sur un flux de travaux est configurée pour l'événement AddServiceToUserEvent.

12.6.2

Nouvelles certifications

Les nouvelles plates-formes suivantes sont certifiées avec CA Identity Manager r12.6.2 :

Terminaux

- CA ControlMinder r12.6 SP2 en tant que terminal
- CA ControlMinder r12.7 en tant que terminal
- Windows Server 2012 en tant que terminal NT
- Windows Server 2012 (ADAM) en tant que terminal JNDI
- CA Directory r12.0 SP11 en tant que terminal JNDI
- Windows Server 2012 Active Directory en tant que terminal
- Java Mainframe Connector en tant que terminal
- Microsoft AD Exchange Server 2010 SP3 en tant que terminal
- Microsoft Office 365 en tant que terminal
- SAPJCO V.3 en tant que terminal

Serveurs d'applications

- JBoss 6.1 EAP
- WebSphere Application Server (WAS) 8.0
- WebSphere Application Server (WAS) 8.5

Référentiel d'utilisateurs CA Identity Manager

- CA Directory r12.0 SP11 GA

Référentiel d'utilisateurs et référentiel d'objets CA Identity Manager

- Microsoft SQL Server 2008 R2 SP2
- Microsoft SQL Server 2012 SP1

  Remarque : JBoss n'a pas confirmé la prise en charge de Microsoft SQL Server 2012.

Prise en charge supplémentaire

- Kit de développement Java 1.7.x
- Rôles et rôles de serveur Microsoft SQL Server 2012 SP1 définis par l'utilisateur
- Mozilla Firefox 18.x
- Serveur de rapports BusinessObjects XI 3.1 SP6 (CABI 3.3 SP1)
- Intégration à CA SiteMinder r12.5 CR1, r12.5 CR2, r12.5.1, r12.0 SP3 CR12 et r6 SP6 CR10

- Intégration à CA Identity Manager avec CA Identity Governance r12.5 SP8 et CA Identity Governance r12.6 SP1
- Prise en charge des applications mobiles
- Prise en charge de WorkPoint Designer version 3.4.2.20080602-33
- Prise en charge de Microsoft ADS, du mode sans agent, des groupes d'accès aux données et de la distribution de boîte aux lettres automatique
- Prise en charge de CA AuthMinder v7.1

Prise en charge des applications mobiles

L'application mobile CA Identity Manager permet d'exploiter l'infrastructure CA Identity Manager existante pour permettre aux utilisateurs d'effectuer les tâches suivantes sur une unité mobile, tel qu'un iPhone ou un iPad :

- Réinitialiser un mot de passe oublié

  Remarque : Lorsque vous permettez aux utilisateurs mobiles de réinitialiser un mot de passe oublié à partir de leur unité, CA Identity Manager utilise la sécurité de l'unité au lieu de questions de sécurité. Considérez renforcer la sécurité de l'unité, avec un code secret par exemple, avant d'activer la fonctionnalité de réinitialisation de mot de passe.
- Modifier un mot de passe
- Répondre aux demandes d'approbation
- Afficher les détails du responsable

  Cette fonctionnalité permet aux utilisateurs qui approuvent des demandes de flux de travaux d'afficher les informations sur le responsable d'un utilisateur.

Remarque : CA Identity Manager 12.6.4 ne prend pas en charge la version 1.0 de l'application mobile. Téléchargez la dernière version à partir de l'Apple Store.

Pour plus d'informations sur l'application mobile, consultez le *Manuel d'administration*.

Synchronisation/suppression des valeurs de modèle de compte des comptes

Vous pouvez désormais utiliser la fonctionnalité de synchronisation/suppression des valeurs de modèle de compte des comptes de l'attribut de liste Responsabilités du modèle Compte pour applications Oracle, afin de désactiver une entrée de responsabilité dans le compte Applications Oracle.

En outre, cette version comprend plusieurs améliorations des calculs de responsabilité pour empêcher des erreurs liées à l'absence de synchronisation.

Pour plus d'informations sur cette fonctionnalité, consultez la rubrique Responsibilities List and Account Synchronization du manuel *Connectors Guide*.

Configuration améliorée pour le connecteur LND

Pour améliorer les performances du connecteur LND pendant les opérations d'exploration et de corrélation, les paramètres configurables suivants sont disponibles :

- readExpirationDateInSearch
- readOuFromPrimaryAddressBookOnly
- readAcctFromPrimaryAddressBookOnly
- enableUouDetection

Remarque : Vous pouvez modifier les valeurs de ces attributs dans le fichier suivant :

```
CA\Identity Manager\Connector Server\conf\override\lnd\connector.xml
```

Schéma de base de données de persistance des tâches

Cette version inclut des améliorations des scripts SQL qui mettent à jour le schéma de base de données de persistance des tâches. Les scripts définissent la taille de colonne correcte et insèrent la procédure stockée relative aux détails du statut d'exécution.

Dans cette mise à jour, il n'y a aucune différence de taille entre la table runtimeStatusDetail12 et la table archive_runtimeStatusDetail12 correspondante pour les nouveaux systèmes ou les systèmes mis à niveau. Cette mise à jour corrige les échecs de la tâche Nettoyer les tâches soumises.

Prise en charge de la désactivation des mots de passe de comptes SAP

Dans cette version, l'attribut Mot de passe désactivé peut être utilisé à partir de l'onglet Compte. Cet attribut vous permet de créer un compte SAP avec un mot de passe désactivé. Vous pouvez également désactiver le mot de passe d'un compte SAP existant. Pour le réactiver, réinitialisez le mot de passe.

Modes de connexion à Exchange avec et sans agent

Dans cette version, vous pouvez vous connecter aux terminaux Exchange 2007 et 2010 sans utiliser d'agent. Il est recommandé d'utiliser le mode sans agent pour toutes nouvelles connexions à ces terminaux.

Remarquez que le mode sans agent ne fonctionne pas avec Exchange 2003 et vous devez donc vous connecter à l'aide de l'agent distant.

Le tableau suivant répertorie les versions d'Exchange prises en charge pour les modes avec et sans agent :

Versions de terminal	Agent	Sans agent
Exchange 2003	Oui	Non
Exchange 2007	Oui	Oui
Exchange 2003 et 2007	Oui	Non
Exchange 2010	Oui	Oui
Exchange 2007 et 2010	Oui	Oui

Prise en charge des groupes d'accès aux données Exchange (DAG)

Dans cette version, Exchange 2010 peut utiliser des groupes d'accès aux données (DAG) afin de garantir la haute disponibilité. Vous pouvez vous connecter à un DAG pour maintenir la connexion au terminal après un basculement.

Prise en charge de la distribution de boîte aux lettres automatique dans Exchange 2010

Dans cette version, le connecteur Exchange Active Directory peut gérer une distribution de boîte aux lettres automatique dans Exchange 2010.

Lorsque vous créez ou déplacez une boîte aux lettres, ou activer la boîte aux lettres d'un utilisateur existant, la boîte aux lettres doit être stockée dans une base de données de boîtes aux lettres. Avec les anciens serveurs Exchange, vous deviez spécifier la base de données de boîtes aux lettres pour effectuer l'une de ces opérations. Exchange Server 2010 sélectionne la base de données à l'aide de la fonctionnalité de distribution de boîte aux lettres automatique.

Connexion à SQL Server avec une base de données indisponible

Vous pouvez désormais effectuer les opérations d'exploration et de corrélation d'un terminal SQL Server lorsque sa base de données est hors ligne.

Tâche de création d'une définition de cliché pour les rapports

Il est recommandé d'utiliser la tâche Créer une définition de cliché pour créer un cliché afin de récupérer les données requises pour générer un rapport. Les fichiers XML de paramètres de cliché par défaut sont progressivement retirés. Pour plus de détails, consultez le *Manuel d'administration*.

12.6.1

Nouvelles certifications (page 22)

Référentiel d'utilisateurs de domaine JNDI compatible SSL (page 22)

Prise en charge des mots de passe chiffrés dans l'annuaire d'amorçage de la console de gestion (page 23)

Nouvelles certifications

Les nouvelles plates-formes suivantes sont certifiées avec CA Identity Manager r12.6.1 :

Terminaux

- Microsoft SQL 2012 comme terminal statique et dynamique
- CA Directory r12 SP10 CR2 comme terminal JNDI
- CA Embedded Entitlements Manager (EEM) : pris en charge par le gestionnaire de provisionnement

Référentiel d'utilisateurs CA Identity Manager

- CA Directory r12 SP10 CR2

Référentiel d'utilisateurs et référentiel d'exécution CA Identity Manager

- Microsoft SQL Server 2012 SP1

Prise en charge supplémentaire

- Mozilla Firefox 14.x
- Serveur de rapports BusinessObjects XI 3.1 SP5 (CA Business Intelligence 3.3)

  Cette version correspond à la version prise en charge par SiteMinder.
- Prise en charge du serveur de rapports dans une configuration de haute disponibilité
- Prise en charge de CA Identity Manager avec CA Identity Governance r12.6
- Prise en charge de CA Identity Manager avec CA SiteMinder r12.0 SP3 CR11

Référentiel d'utilisateurs de domaine JNDI compatible SSL

La vérification de certificat d'homologue est désormais appliquée. Cette fonctionnalité requiert l'ajout du certificat de serveur SSL du référentiel d'utilisateurs dans le référentiel de clés approuvé par défaut du JRE CA Identity Manager. Le référentiel de clés est le fichier cacerts ou jssecacerts sous :

JAVA_HOME\jre\lib\

Utilisez l'utilitaire keytool du kit de développement Java pour ajouter le certificat.

Prise en charge des mots de passe chiffrés dans l'annuaire d'amorçage de la console de gestion

Si vous décidez de sécuriser la console de gestion à l'aide de l'annuaire d'amorçage AuthenticationDirectory, vous pouvez chiffrer le mot de passe de l'administrateur de la console de gestion.

12.6

Nouveau nom et apparence

La console d'utilisateur par défaut a été mise à jour pour refléter le nouveau style et les nouvelles couleurs de CA.

Le serveur de connecteurs Java (JCS) a été renommé serveur de connecteurs CA IAM (CA IAM CS).

Expérience utilisateur simplifiée

Cette version inclut les améliorations de l'expérience utilisateur suivantes :

- Fenêtres de tâche d'auto-administration mises à jour

  Les fenêtres suivantes ont été mises à jour pour améliorer la facilité d'utilisation :

  - Apparence du portail pour la fenêtre de connexion
  - Auto-enregistrement/création d'identité
  - Modifier mon mot de passe
  - Réinitialisation du mot de passe oublié
  - ID de l'utilisateur oublié
- Certaines tâches d'administration utilisent des contrôles Web 2.0.

Améliorations du provisionnement

CA Identity Manager 12.6 inclut les nouvelles fonctionnalités et les modifications suivantes pour améliorer le provisionnement.

Serveur de provisionnement sur Linux

Outre Solaris, vous pouvez dorénavant installer le serveur de provisionnement sur Red Hat Linux.

Fonctionnalités du gestionnaire de provisionnement dans la console d'utilisateur

Plusieurs fonctionnalités du gestionnaire de provisionnement sont prises en charge dans la console d'utilisateur :

- Synchronisation d'utilisateurs, de rôles, de comptes de terminal et de modèles de compte

  L'intégration de terminaux et de comptes dans CA Identity Manager peut entraîner la perte de la synchronisation. Par exemple, les rôles de provisionnement affectés à un utilisateur peuvent différer des comptes réels de cet utilisateur. Les tâches de synchronisation corrigent ce problème.
- Les règles de corrélation contrôlent le mappage des attributs de compte de terminal aux attributs d'utilisateur dans la console d'utilisateur. Par exemple, CA Access Control a un attribut appelé AccountName. Vous pouvez créer une règle pour le mapper vers FullName dans la console d'utilisateur.

Améliorations des connecteurs

CA Identity Manager 12.6 inclut les nouvelles fonctionnalités et les modifications suivantes pour simplifier la création et le déploiement de nouveaux connecteurs.

Déploiement à chaud : installez un nouveau connecteur sans redémarrer CA IAM CS.

Le serveur de connecteurs CA IAM (CA IAM CS) est le nouveau nom du serveur de connecteurs Java (Java CS ou JCS).

CA IAM CS prend désormais en charge le *déploiement à chaud*. Le déploiement à chaud est le processus d'ajouter, de supprimer ou de mettre à jour un composant sans redémarrer CA IAM CS. Vous pouvez exécuter les tâches suivantes :

- Installer, désinstaller ou mettre à niveau un connecteur *sans* redémarrer CA IAM CS

  Vous pouvez déployer un nouveau connecteur ou un connecteur mis à jour, et l'installer sans redémarrer CA IAM CS ou vous connecter à son hôte. Contactez le support de CA pour obtenir les dernières versions de connecteur.

- Déployer des bibliothèques tierces sans redémarrer CA IAM CS

  Certains connecteurs requièrent des bibliothèques qui ne peuvent pas être incluses avec CA IAM CS. Vous devrez déployer ces bibliothèques au préalable et redémarrer CA IAM CS. Vous pouvez ensuite déployer ces bibliothèques lors de l'exécution du serveur de connecteurs.

  CA IAM CS inclut un ensemble principal de bibliothèques tierces que tous les connecteurs peuvent utiliser. Un connecteur peut également inclure une autre bibliothèque tierce requise.

Remarque : Le déploiement à chaud ne fonctionne pas pour les connecteurs en C++.

Générateur de groupe : nouvel outil pour la création de connecteurs

CA IAM CS requiert que les connecteurs soient fournis dans un groupe Open Services Gateway initiative. La structure OSGi est un système de module et de plate-forme de service pour le langage de programmation Java qui implémente un modèle de composant complet et dynamique. Le kit de développement logiciel pour le serveur de connecteurs inclut l'outil de générateur de groupe, qui vous permet d'encapsuler le connecteur dans un groupe.

Journalisation pour les connecteurs et CA IAM CS

Vous pouvez désormais vous connecter à CA IAM CS pour afficher les messages de journaux récents pour CA IAM CS et ses connecteurs. Vous pouvez toujours utiliser les fichiers journaux pour afficher tous les messages contenus dans le journal.

Certificats pour les connecteurs et CA IAM CS

Vous pouvez désormais vous connecter à CA IAM CS pour afficher et gérer des certificats pour CA IAM CS et ses connecteurs.

Utilisation de Connector Xpress pour mapper des attributs personnalisés et des attributs de capacité personnalisés

Utilisez Connector Xpress pour mapper des attributs personnalisés et des attributs de capacité personnalisés. L'utilisation du fichier XML <jcs-home>/conf/override/lnd/lnd_custom_metatdata.xml pour mapper des attributs n'est plus possible.

Configuration de CA IAM CS en tant que proxy pour le serveur de connecteurs C++

CA Identity Manager utilise désormais CA IAM CS comme proxy pour le serveur de connecteurs C++. Aucune communication directe ne se produit entre CA Identity Manager et le serveur de connecteurs C++.

Améliorations des performances

Des améliorations de performances ont été apportées dans les parties suivantes de CA Identity Manager 12.6.

Améliorations des performances du chargeur en bloc

Dans cette version, les performances du chargeur en bloc ont été améliorées. Les modifications apportées comprennent notamment :

- Un taux de soumission de tâches plus élevé via la tâche de chargeur en bloc parent : un plus grand nombre de tâches s'exécutent simultanément.
- Des optimisations dans la réutilisation de la connexion à la base de données : la mise en cache des définitions d'attributs d'objet géré aboutit à une exécution plus rapide des tâches du début à la fin.
- Des améliorations de certains modules d'extension et écouteurs pour accélérer le traitement des événements générés pendant l'exécution des tâches.

Pour encore améliorer les performances, il est recommandé d'effectuer les modifications suivantes pour la durée des opérations de chargement en bloc :

- Désactiver toutes les stratégies Policy Xpress, les gestionnaires de tâches métier et les indicateurs de synchronisation superflus au niveau de la tâche.
- Exécuter la tâche de chargeur en bloc en tant qu'utilisateur dédié avec le moins possible de rôles d'administration et de tâches d'administration dans la portée.

Remarque : Pour plus d'informations sur les améliorations de performances supplémentaires, consultez la section sur le chargeur en bloc du *Manuel d'administration*.

Performances d'exportation de cliché améliorées

Dans cette version, le processus d'exportation des données de cliché pour des rapports a été mis à jour afin d'améliorer les performances et la facilité d'utilisation. A l'aide de l'Assistant de définition de cliché, vous définissez ou personnalisez les règles de chargement des utilisateurs, des terminaux, des rôles d'administration, des rôles de provisionnement, des groupes et des organisations.

Cette fonctionnalité vous permet d'utiliser une tâche de console d'utilisateur pour sélectionner et exporter uniquement les attributs souhaités pour une instance de cliché. Dans les versions précédentes, vous deviez modifier un fichier XML manuellement.

Remarque : Vous pouvez toujours utiliser et personnaliser les fichiers XML par défaut afin de capturer des clichés.

Pour plus d'informations sur la création des définitions de cliché, reportez-vous au *Manuel d'administration*.

Améliorations de Policy Xpress

Les améliorations suivantes ont été apportées à Policy Xpress dans cette version :

- Modules d'extension d'attribut pour les objets gérés

  Les modules d'extension d'attribut d'objet géré suivants ont été ajoutés à Policy Xpress :

  - Attribut d'objet : permet d'extraire la valeur d'un attribut d'objet géré.
  - Possède une valeur d'attribut d'objet modifiée/Attribut d'objet spécifique : identiques aux modules d'extension Possède une valeur d'attribut d'utilisateur modifiée et Attribut d'un utilisateur, mais ils peuvent être utilisés avec tous les types d'objet géré.
  - Définir les valeurs d'objets : permet de modifier l'attribut des objets gérés.

- Fonction Supprimer

  La fonction Supprimer vous permet de supprimer les espaces de début et de fin superflus d'un élément de données ou d'une chaîne.

- Prise en charge de règles d'action supplémentaires

  Dans les versions précédentes, lorsque vous vouliez ajouter entre 60 et 70 règles d'action à une stratégie, Policy Xpress ne les ajoutait pas. Aucune erreur ou exception n'était incluse dans les journaux. Désormais, les stratégies Policy Xpress peuvent prendre en charge jusqu'à 500 règles d'action.

- Wiki de Policy Xpress

  La documentation de Policy Xpress a été mise à jour et se trouve dans un Wiki de la communauté internationale d'utilisateurs des produits de sécurité CA.

Console de gestion sécurisée

La console de gestion permet aux administrateurs de créer et de gérer des annuaires et des environnements CA Identity Manager.

L'installation de CA Identity Manager inclut une option sélectionnée par défaut, qui permet de sécuriser la console de gestion. Au cours de l'installation, vous créez un compte qui peut accéder à la console de gestion dans un annuaire prédéfini.

Après l'installation, vous pouvez ajouter les administrateurs supplémentaires qui doivent accéder à la console de gestion.

Remarque : Pour plus d'informations, reportez-vous au *Manuel de configuration*.

Demandes d'accès de base

Les utilisateurs de CA Identity Manager peuvent demander l'accès aux services dont ils ont besoin pour effectuer leurs fonctions.

Un *service* regroupe tous les droits (tâches, rôles, groupes et attributs) dont un utilisateur a besoin pour un rôle professionnel donné. L'utilisateur peut accéder aux services par l'intermédiaire des tâches Demande d'accès, dans la console d'utilisateur CA Identity Manager. Les tâches Demande d'accès permettent à un utilisateur ou à un administrateur de demander, d'affecter, de retirer et de renouveler un service.

Les services permettent aux administrateurs de combiner des droits d'utilisateur dans un package unique et de les gérer comme un ensemble. Par exemple, tous les nouveaux employés des ventes ont besoin d'accéder à un ensemble défini de tâches et de comptes sur des systèmes d'extrémité spécifiques. Ils ont également besoin d'informations spécifiques qui doivent être ajoutées à leurs profils de compte d'utilisateur. Un administrateur crée un service nommé Administration des ventes, contenant toutes les tâches, les rôles, les groupes et les informations d'attribut de profil requis pour un nouvel employé des ventes. Lorsqu'un administrateur affecte le service Administration des ventes à un utilisateur, cet utilisateur reçoit l'intégralité de l'ensemble des rôles, tâches, groupes et attributs de compte définis par le service.

Les utilisateurs peuvent également accéder aux services en effectuant eux-mêmes une demande d'accès. Dans la console d'utilisateur, chaque utilisateur dispose d'une liste des services disponibles qu'il peut demander. Cette liste contient les services définis sur Auto-abonnement par un administrateur avec des droits appropriés, généralement pendant la création du service. A partir de la liste des services disponibles, les utilisateurs peuvent demander l'accès aux services dont ils ont besoin. Lorsqu'un utilisateur demande l'accès à un service, la demande est exécutée automatiquement et les droits associés sont affectés à l'utilisateur immédiatement. Un administrateur disposant des droits appropriés peut également configurer l'exécution des services de sorte à requérir l'approbation de flux de travaux ou à générer des notifications par courriel.

Remarque : La version initiale prend en charge les fonctionnalités de demande d'accès de base. La fonctionnalité de demande d'accès permet aux utilisateurs finals de demander des droits gérés et non gérés par CA Identity Manager, de définir des flux d'approbation et d'utiliser des flux d'exécution.

Cette version ne prend pas en charge les fonctionnalités de demande d'accès avancées suivantes :

- Définition en bloc d'objets de services de demande d'accès
- Intégration à CA Identity Governance (anciennement CA GovernanceMinder)
- Filtres et recherches détaillés

La version initiale ne prend pas en charge les fonctionnalités suivantes :

- Définition en bloc d'objets de services
- Filtres détaillés
- Recherches
- Intégration à d'autres mécanismes d'exécution

Pour en savoir plus sur les services, reportez-vous au *Manuel d'administration*.

Nouvelle documentation pour Config Xpress

Config Xpress est un outil fourni avec CA Identity Manager. Vous pouvez l'utiliser pour analyser et utiliser les configurations de vos environnements CA Identity Manager.

Config Xpress vous permet d'effectuer les tâches suivantes :

- Déplacer les composants entre les environnements

  L'outil détecte automatiquement tous les autres composant requis et vous invite à les déplacer également. Cela vous permet de gagner du temps.

- Publier un rapport sur les composants système dans un fichier PDF.
- Publier la configuration XML d'un composant.

Pour plus d'informations sur l'importation de configuration, reportez-vous à la rubrique traitant de la gestion de la configuration, dans le *Manuel de configuration*.

Remplacement CA Identity Manager natif pour les services de mot de passe avancés de SiteMinder

Outre les stratégies de mot de passe de base, CA Identity Manager fournit les paramètres de mot de passe supplémentaires suivants provenant de SiteMinder :

- Expiration du mot de passe :
  - Suivi des échecs de connexion ou Suivi des connexions réussies : lorsque le suivi des échecs de connexion ou des connexions réussies est activé, ces informations sont enregistrées dans l'attribut de données de mot de passe de l'utilisateur dans le référentiel d'utilisateurs.
  - Authentifier en cas d'échec du suivi des connexions - si cette option est désactivée, les utilisateurs ne peuvent pas se connecter lorsque CA Identity Manager ne peut enregistrer aucune information de suivi dans le référentiel d'utilisateurs.
  - Modification du mot de passe pour éviter son expiration : configure le comportement de l'expiration. Si un mot de passe n'a pas été changé après le nombre de jours spécifié, les utilisateurs sont désactivés ou sont obligés de changer leur mot de passe. Permet également d'envoyer des avertissements d'expiration pendant un nombre de jours spécifié.
  - Inactivité de mot de passe : configure le comportement des utilisateurs inactifs. Si un utilisateur ne s'est pas connecté correctement après un nombre de jours spécifié, il est désactivé ou obligé de changer son mot de passe.
  - Mot de passe incorrect : configure le nombre d'échecs de connexion permis avant la désactivation de l'utilisateur.
  - Multiple regular expressions (Plusieurs expressions régulières) : spécifie des expressions régulières auxquelles doivent correspondre ou ne pas correspondre les mots de passe. Les stratégies de mot de passe de CA Identity Manager prennent en charge une expression unique de chaque type.
- Restrictions de mot de passe :
  - Nombre minimum de jours avant la réutilisation
  - Nombre minimum de mots de passe avant la réutilisation
  - Pourcentage de différence par rapport au dernier mot de passe
  - Ignorer la séquence lors de la vérification des différences : permet d'ignorer la position des caractères lors du calcul du pourcentage de différence.

Remarque : Cette version ne prend pas en charge les données de mot de passe historiques à partir d'un déploiement CA Identity Manager qui utilise des services de mot de passe CA SiteMinder (historique de mots de passe) vers un déploiement qui inclut uniquement des services de mot de passe de CA Identity Manager r12.6.

Clés dynamiques pour le chiffrement de données

Dans un environnement, vous pouvez créer des clés dynamiques qui chiffrent ou déchiffrent les données. Si vous pensez qu'un utilisateur dispose d'un accès non autorisé à une clé, vous pouvez changer le mot de passe du référentiel de clés. Le référentiel de clés est la base de données de stockage des clés secrètes. Une fois que vous changez ce mot de passe, CA Identity Manager chiffre de nouveau les valeurs des clés.

Pour plus d'informations, consultez la section sur la gestion des clés secrètes du *Manuel d'administration*.

Synchronisation de serveur Active Directory

Vous pouvez configurer CA IAM CS pour permettre aux utilisateurs disposant d'un serveur Active Directory de synchroniser les informations d'identité locales avec les informations de terminal cloud. Par exemple, vous pouvez configurer la synchronisation du serveur AD avec une installation SalesForce basée sur le cloud. Les ajouts ou les modifications apportées à un groupe d'utilisateurs local synchronisé sont alors propagés à l'environnement SalesForce.

Cette fonctionnalité requiert CA IAM CS, un terminal pris en charge et le connecteur approprié.

Remarque sur la fonctionnalité de synchronisation d'Active Directory :

- Cette fonctionnalité prend en charge uniquement Active Directory. Aucun autre annuaire LDAP n'est pris en charge pour cette fonctionnalité dans cette version.
- Cette fonctionnalité prend uniquement en charge les terminaux basés sur le cloud pour lesquels un connecteur existe. Dans cette version, les applications prises en charge incluent Google Apps et SalesForce.

Pour plus d'informations sur cette fonctionnalité, reportez-vous au manuel *Connectors Guide*.

Audit des événements de connexion et de déconnexion

Pour améliorer la surveillance des accès utilisateur à l'environnement CA Identity Manager, vous pouvez configurer CA Identity Manager pour auditer les événements de connexion et de déconnexion d'utilisateur dans un environnement. Vous pouvez afficher ces événements journalisés dans le rapport de détails de l'audit par défaut.

Remarque : Vous ne pouvez pas journaliser les événements de connexion et de déconnexion d'utilisateur pour CA SiteMinder.

Vous pouvez configurer ces paramètres dans le fichier des paramètres d'audit. Pour plus d'informations sur la configuration des événements de connexion et déconnexion, consultez le chapitre Audit dans le *Manuel de configuration*.

Prise en charge de l'algorithme SHA-2

Le hachage SHA-2 de certificat SSL est un algorithme cryptographique développé par le National Institute of Standards and Technology (NIST) et la NSA. Les certificats SHA2 sont plus sécurisés que tous les algorithmes existants auparavant. Dans CA Identity Manager, vous pouvez configurer des certificats SSL signés en SHA-2 à la place des certificats signés avec la fonction d'hachage SHA-1.

Chapitre 2: Remarques relatives à l'installation

Ce chapitre traite des sujets suivants :

Activation de la prise en charge de Policy Xpress pour les services Web SOAP et REST

Policy Xpress a été amélioré afin de prendre en charge les services Web SOAP (avec la méthode d'authentification de base) et REST (avec les méthodes d'authentification de base, d'authentification de proxy et d'authentification OAuth), afin de permettre son intégration à des applications externes fournissant une interface de service Web. Pour utiliser les services Web de Policy XPress (SOAP et REST) avec JBoss 5.1 (Community Edition), copiez les fichiers JAR suivants dans le répertoire \lib\endorsed de JBoss 5.1 (Community Edition) à partir du répertoire client, puis redémarrez le serveur d'applications :

- jbossws-native-jaxrpc.jar
- jbossws-native-jaxws.jar
- jbossws-native-jaxws-ext.jar
- jbossws-native-saaj.jar

Remarque : Il n'est pas nécessaire de copier ces fichiers pour les versions EAP.

Plates-formes et versions prises en charge

CA Identity Manager 12.6.4 inclut plusieurs changements portant sur les versions des serveurs d'applications prises en charge, les annuaires et les bases de données.

Remarque : Pour obtenir la liste complète des versions et des plates-formes prises en charge, consultez la matrice de prise en charge de CA Identity Manager sur le site de support de CA.

Composants désapprouvés et abandonnés

Certains composants sont désapprouvés, c'est-à-dire qu'ils ne seront plus pris en charge dans les futures versions. D'autres composants sont abandonnés, c'est-à-dire qu'ils ne sont plus inclus ou testés avec le produit. Ces composants sont répertoriés dans la section CA Identity Manager Deprecation Policy sur le site de support de CA.

Co-installation d'agents distants UNIX avec d'autres produits CA

Dans cette version, les agents distants UNIX (à l'exception des plates-formes TRU64) sont installés et permettent de rechercher les composants logiciels dépendants, comme CA ITCM.

Si vous voulez mettre à niveau l'agent distant UNIX, la nouvelle méthode de suivi ne met pas à jour les références des composants logiciels dépendants. Si vous voulez désinstaller le produit après la mise à niveau, utilisez le fichier de désinstallation suivant :

```
<répertoire_installation>/scripts/uninstall-force.sh
```

Remarque : Vérifiez que le fichier uninstall-force.sh n'est pas utilisé sur des hôtes sur lesquels d'autres logiciels CA sont installés. Ces produits peuvent dépendre des packages logiciels que ce script supprime.

Mots de passe non chiffrés

Les nouvelles installations ne chiffrent pas les mots de passe d'utilisateur par défaut. En outre, lorsque SiteMinder est intégré à CA Identity Manager, vous ne pouvez pas activer le chiffrement de mot de passe à l'aide de l'attribut AttributeLevelEncrypt. Cet attribut fonctionne uniquement lorsque SiteMinder n'est pas installé.

Ce problème sera corrigé dans une version future.

Utilisation d'Oracle 11g R2 RAC en tant que référentiel d'utilisateurs et référentiel d'objets

Lorsque vous utilisez Oracle 11g R2 RAC comme référentiel d'utilisateurs et référentiel d'exécution, effectuez les opérations suivantes pour utiliser les fonctionnalités d'un cluster de base de données Oracle :

- Utilisez le nom SCAN (Single Client Access Name) lors de l'installation de CA Identity Manager avec Oracle 11g R2 RAC.
- Lorsque vous créez l'espace disque logique, créez l'*espace disque logique* de la base de données sur le groupe de disques partagé.

Oracle 12c RDB en tant que référentiel d'utilisateurs et référentiel d'objets

Lorsque vous utilisez Oracle 12c RDB en tant que référentiel d'utilisateurs et référentiel d'exécution, utilisez uniquement le mode de base de données non-conteneur. L'option de SGBDR de la base de données de conteneur Oracle 12c (hébergement multiclient) n'est pas disponible pour la version entreprise du produit.

ADAM 2008 en tant que magasin d'utilisateurs

Si vous utilisez ADAM 2008 en tant que magasin d'utilisateurs de CA Identity Manager et que vous intégrez celui-ci à SiteMinder, vous devez installer SiteMinder r6.0 SP6/r6.x QMR6.

Echec de l'installation sur les systèmes non anglais lié aux caractères non ASCII

Pendant l'installation de CA Identity Manager, le programme d'installation extrait les fichiers dans un répertoire temporaire. Sur certains systèmes localisés, le chemin par défaut du répertoire temporaire contient des caractères non ASCII. Par exemple, le chemin par défaut du répertoire temporaire sur un système Windows espagnol est le suivant :

C:\Documents and Settings\Administrador\Configuración local\Temp

En raison de la présence de caractères non ASCII, le programme d'installation affiche une page vide de résumé de pré-installation, ce qui entraîne l'échec de l'installation.

Solution

Modifiez la variable tmp de l'environnement afin qu'elle pointe vers un dossier contenant uniquement des caractères ASCII.

Contournement du pare-feu sous Windows 2008 SP2

Lors de l'installation dans des déploiements Windows 2008 SP2, le pare-feu bloque la communication avec des composants CA Identity Manager, tels que le serveur de provisionnement, le serveur de connecteurs Java et le serveur de connecteurs C++.

Pour contourner ce problème, ajoutez des exceptions de port ou désactivez le pare-feu Windows pour accéder à des composants CA CA Identity Manager distribués dans des déploiements Windows 2008 SP2.

Déploiement des pages JSP pour les actions d'administrateur

Le serveur CA Identity Manager inclut des exemples de pages JSP pour effectuer les actions suivantes :

- Effectuer un test Ping sur le serveur principal
- Répertorier les GTM déployés
- Répertorier les informations sur les types d'objets et les fournisseurs d'objets gérés
- Répertorier les informations sur les modules d'extension
- Modifier les niveaux de journalisation

Les pages JSP sont installées dans cet emplacement :

outils_admin\samples\admin

Le dossier contient un fichier readme.txt avec des instructions pour utiliser les pages JSP.

Remarque : Vous verrez une erreur 404 si vous utilisez ces pages JSP sans suivre les instructions du fichier readme.txt.

Installation de l'annuaire de provisionnement sous Linux

Si vous installez l'annuaire de provisionnement sous un système Linux, celui-ci utilise automatiquement des adresses IPv6, même si vous souhaitez utiliser IPv4. Tous les adaptateurs DSA semblent être en cours d'exécution, mais lorsque vous essayez de vous y connecter via Jxplorer ou d'installer le serveur de provisionnement, un message d'erreur indiquant un refus de connexion peut s'afficher.

Pour désactiver IPv6 sous Linux :

1. Avant l'installation de l'annuaire de provisionnement, suivez les étapes indiquées dans l'article de base de connaissances Red Hat sur la Désactivation d'IPv6 sous LINUX.
2. Assurez-vous que /etc/hosts ne possède aucune entrée pour l'adresse suivante :

   127.0.0.1 *nom_hôte*

Linux : configuration du JDK pour l'installation

CA Identity Manager 12.6.4 requiert le kit de développement Java 1.6 d'Oracle.

RedHat 6.x inclut OpenJDK 1.6, qui peut entraîner le blocage indéfini du programme d'installation de CA Identity Manager. Vérifiez que vous utilisez la version du JDK Oracle requise, comme spécifiée dans le Tableau de prise en charge de CA Identity Manager.

Erreurs de connectivité CA Identity Manager sous Linux 64 bits avec SiteMinder

Lorsque vous sélectionnez Se connecter à SiteMinder, le programme d'installation signale des erreurs avec CA Identity Manager sous Linux 64 bits. La configuration requise de l'agent dans SiteMinder n'est pas correcte.

Important : Avant de déployer un répertoire ou un environnement, suivez les étapes de correction proposée ci-dessous.

Solution

1. Prenez note du nom de l'agent et du mot de passe indiqués lors de l'installation. Vous pouvez également lire la valeur de la propriété AgentName dans le fichier suivant :

   ```
   \iam_im.ear\policyserver.rar\META-INF\ra.xml
   ```

2. Ouvrez l'interface utilisateur de SiteMinder WAM et créez un agent avec le nom de l'agent. Assurez-vous de sélectionner la case à cocher "Agent 4.x".

3. Démarrez le serveur d'applications et vérifiez qu'il n'y ait aucun problème de connectivité du serveur de stratégies.

   Une ligne sans exceptions doit apparaître comme dans l'exemple suivant :

   ```
   13:40:43, 156 WARN  [default] * Startup Step 2 : Attempting to start
   PolicyServerService
   ```

Amélioration des performances sur WebSphere et AIX

Pour une installation de WebSphere sur AIX, vous pouvez obtenir de meilleures performances dans la console d'utilisateur en définissant la taille de segment de mémoire maximum.

Procédez comme suit:

1. Recherchez le fichier server.xml à l'emplacement suivant :
   WAS_HOME/profiles/*profil*/config/cells/*cellule*/nodes/*noeud*/servers/*serveur*
2. Ajoutez maximumHeapSize="1000" à l'élément jvmEntries.

   Vous pouvez utiliser une valeur plus élevée si nécessaire. Par exemple, pour définir l'élément maximumHeapSize sur 2 Go (2048 Mo), vous l'ajoutez comme affiché en gras dans l'extrait du fichier suivant :

```
<jvmEntries xmi:id="JavaVirtualMachine_1183122130078"
verboseModeClass="false"
   verboseModeGarbageCollection="false" maximumHeapSize="2048"
verboseModeJNI="false" runHProf="false" hprofArguments=""
debugMode="false" debugArgs="-
agentlib:jdwp=transport=dt_socket,server=y,suspend=n,address=77
77" genericJvmArguments="">
      <systemProperties xmi:id="Property_1"
name="com.ibm.security.jgss.debug" value="off"
required="false"/>
      <systemProperties xmi:id="Property_2"
name="com.ibm.security.krb5.Krb5Debug" value="off"
required="false"/>
    </jvmEntries>
```

Omission des erreurs WebSphere 7Oracle

Lorsque CA Identity Manager est installé à l'aide d'un référentiel d'exécution Oracle et du JRE WebSphere 7 par défaut, l'erreur suivante s'affiche dans les journaux CA Identity Manager.

> Oracle does not support the use of version 10 of their JDBC driver with the version of the Java runtime environment that is used by the application server. (Oracle ne prend pas en charge l'utilisation de la version 10 du pilote JDBC avec la version du JRE utilisée par le serveur d'applications.)

Vous pouvez ignorer cette erreur.

Chapitre 3: Mises à niveau

Les problèmes de mise à niveau suivants ont été détectés dans CA Identity Manager r12.5 SP1.

Ce chapitre traite des sujets suivants :

Définition de l'étendue des rôles d'administration requise pour le rôle Responsable du système après une mise à niveau de la version 12.6

Lorsque vous mettez à niveau CA Identity Manager 12.6 ou une version ultérieure, le rôle de responsable du système requiert la définition de l'étendue des rôles d'administration.

Remarque : Si l'étendue n'est pas définie, il se peut que les recherches de rôles d'administration ne renvoient aucun résultat.

Suivez une de ces étapes :

- Dans la console de gestion, cliquez sur Responsable du système, puis sélectionnez un utilisateur.
- Vous pouvez également ajouter l'étendue du rôle d'administration au rôle de responsable du système à l'aide des options Modifier un rôle d'administration, Responsable du système.

Chemins de mise à niveau pris en charge

Vous pouvez réaliser une mise à niveau vers CA Identity Manager 12.6.4 à partir des versions suivantes :

- CA Identity Manager r12
- CA Identity Manager r12.5 ou 12.5 SPx
- CA Identity Manager r12.6 ou 12.6 SPx

Si vous avez une version antérieure à CA Identity Manager r12, procédez d'abord à la mise à niveau vers la version 12, 12.5 ou l'une des versions comprises entre 12.5 SP1 et 12.5 SP6. Ces versions incluent l'outil imsconfig, qui est requis pour mettre à niveau une version antérieure à la version 12. Vous pouvez ensuite procéder à la mise à niveau vers CA Identity Manager 12.6.4.

Nouveaux scripts de mise à jour des schémas de persistance des tâches et d'archivage

Cette version comprend de nouveaux scripts vous permettant de mettre à jour des schémas de persistance des tâches et d'archivage. La mise à jour s'exécute automatiquement lorsque vous démarrez CA Identity Manager après une mise à niveau. Pour plus d'informations sur les nouveaux scripts, reportez-vous au *Manuel d'installation*.

Nouveaux fichiers JCO pour SAP R3

Si vous souhaitez utiliser le nouveau connecteur pour SAP R3, vous devez mettre à jour les fichiers JCO. Pour plus d'informations, consultez le manuel de terminal pour le connecteur SAP R3.

Nouveau fichier de définition de rôle Active Directory

Assurez-vous que vous importez le nouveau fichier de définition de rôle pour Active Directory dans chaque environnement. L'environnement CA Identity Manager actuel peut avoir une version antérieure du fichier de définition de rôle Active Directory. Importez le fichier pour mettre à niveau les définitions de rôle vers la version 1.08. Pour plus d'informations sur l'importation de fichiers de définition de rôle, suivez les procédures du manuel *Upgrade Guide*.

Mise à jour du fichier jboss.xml

Lors du redémarrage de JBoss ou de l'initialisation de CA Identity Manager, plusieurs messages d'erreurs sont journalisés dans le fichier server.log de CA Identity Manager. Ces messages sont associés à des événements gérés par JMX, mais le bean de message récepteur n'est pas encore initialisé. Pour corriger ce problème, le fichier suivant inclut désormais une clause depends :

```
iam_im.ear\iam_im_identityminder_ejb.jar\META-INF\jboss.xml
```

La clause dépends est incluse dans cette section :

```
<message-driven>
<ejb-name>SubscriberMessageEJB</ejb-name>
<destination-jndi-
name>queue/iam/im/jms/queue/com.netegrity.ims.msg.queue
</destination-jndi-name>
<depends>jboss.web.deployment:war=/iam/im</depends>
</message-driven>
```

Assurez-vous d'inclure cette section dans le fichier jboss.xml. Une fois incluse, le bean de message récepteur est initialisé avant que JMX démarre le traitement de la file d'attente d'événements.

Serveurs d'applications 64 bits

CA Identity Manager 12.6.4 prend en charge les serveurs d'applications 64 bits, qui fournissent de meilleures performances que les serveurs d'applications 32 bits. Les versions de serveur d'applications 64 bits suivantes sont prises en charge :

- JBoss 5.0, 5.1 et 6.1 Enterprise Application Platform (EAP)
- JBoss 5.1 Open Source
- Oracle WebLogic 11g (10.3.5)
- IBM WebSphere 7.0, 8.0, 8.5

Pour obtenir des détails complets sur la mise à niveau de votre serveur d'applications, consultez le manuel *Upgrade Guide*.

Problème de mise à niveau de clusters à partir de CA Identity Manager r12 CR6 (ou version ultérieure)

Si vous mettez un cluster à niveau à partir de CA Identity Manager r12 CR6 (ou version ultérieure) vers CA Identity Manager r12.5 SP1, il se peut que la mise à niveau échoue suite à l'effacement de certaines propriétés du cluster dans le fichier d'installation.

Solution

Avant d'effectuer la mise à niveau, vérifiez que les propriétés suivantes figurent dans le fichier im-installer.properties :

- WebSphere : vérifiez si le nom du cluster est rempli dans DEFAULT_WAS_CLUSTER. Si ce nom est manquant, rajoutez-le manuellement.
- WebLogic : vérifiez si le nom du cluster est rempli dans DEFAULT_BEA_CLUSTER. Si ce nom est manquant, rajoutez-le manuellement.

Remarque : Ce problème ne concerne pas les clusters JBoss.

Par défaut, le fichier d'installation se trouve aux emplacements suivants :

- Windows : C:\Program Files\CA\CA Identity Manager\install_config_info\im-installer.properties
- Unix : /opt/CA/CA_Identity_Manager/install_config_info/im-installer.properties

Erreur de flux de travaux après la mise à niveau des versions antérieures à la version 12.5 SP7

Symptôme :

Si vous procédez à la mise à niveau à partir d'une version antérieure à la version 12.5 SP7 sur le serveur d'applications WebLogic, l'erreur suivante s'affiche au démarrage du flux de travaux :

```
WARN  [ims.default] * Startup Step 25 : Attempting to start SchedulerService
ERROR [ims.bootstrap.Main] The IAM FW Startup was not successful
ERROR [ims.bootstrap.Main] org.quartz.SchedulerException: JobStore class
'org.quartz.impl.jdbcjobstore.JobStoreCMT' props could not be configured.
[See nested exception: java.lang.NoSuchMethodException: No setter for
property 'lockHandler.class']
```

Solution :

1. Arrêtez WebLogic
2. Accédez au dossier <IAM-EAR>/APP-INF/lib.
3. Renommez les fichiers suivants :
   - common-pool-1.3.jar
   - annotations.jar
   - eurekifyclient.jar
   - quartz-all-1.5.2.jar
4. Lancez le serveur d'applications.
5. L'erreur au démarrage du flux de travaux ne s'affiche plus.

Erreur de migration d'environnement

Symptôme :

Lors d'une mise à niveau à partir de CA CA Identity Manager r12 CR1/CR2/CR3, il se peut que le message d'erreur suivant apparaisse lors de l'importation des environnements :

Attribute "accumulateroleeventsenabled" is not allowed to appear in element "Provisioning". (L'affichage de l'attribut accumulateroleeventsenabled n'est pas autorisé dans l'élément Provisionnement.)

Solution :

Dans le zip exporté Env.zip, ouvrez le fichier envsettings.xml et mettez à jour "accumulateroleeventsenabled" en supprimant le deuxième "c" dans "accumulate" : acumulateroleeventsenabled.

Erreur de mise à niveau du fournisseur d'informations d'identification

Après avoir mis à niveau le fournisseur d'informations d'identification de CA CA Identity Manager r12 sur une plate-forme Windows 32 bits, la case à cocher Désactiver Microsoft Password Credential Provider est désactivée dans l'application CAIMCredProvConfig.

Solution

Ouvrez l'application CAIMCredProvConfig et sélectionnez la case à cocher.

Erreur interne du fournisseur d'informations d'identification Vista

Symptôme :

Lorsque je mets à niveau le fournisseur d'informations d'identification Vista de CA CA Identity Manager sur des plates-formes Windows 64 bits, je reçois le message *Erreur interne 2324.2.*

Solution :

Aucune action n'est requise, car le processus de mise à niveau s'est déroulé correctement.

Absence de fenêtre de recherche avec la tâche d'exploration et de corrélation

Si vous avez effectué la mise à niveau à partir de CA Identity Manager r12 *ou* de CA Identity Manager r12.5 *et* que vous avez migré la tâche d'exploration et de corrélation vers le nouveau modèle de récurrence, le bouton Parcourir ne fonctionne pas correctement.

Solution

Configurez une fenêtre de recherche pour cette tâche, afin qu'une fenêtre de recherche s'affiche lorsque vous cliquez sur le nouveau bouton Parcourir.

Erreur non irrécupérable après la mise à niveau du gestionnaire de provisionnement depuis r12

Symptôme :

Après avoir mis à niveau le gestionnaire de provisionnement depuis CA CA Identity Manager r12 CRx, le programme d'installation affiche le message suivant :

```
L'assistant d'installation a terminé la mise à niveau de CA
Identity Manager, mais des erreurs non fatales ou des
avertissements se sont produits pendant l'opération. Pour plus
d'informations, reportez-vous au journal d'installation sous
C:\Program Files\CA\CA Identity Manager.
Des erreurs ou des avertissements ont été signalés au niveau des
composants suivants
```

Le journal d'installation de CA CA Identity Manager contient l'entrée suivante :

```
Install, com.installshield.product.actions.Files, err,
ServiceException: (error code = -30016; message = "Impossible
d'accéder au fichier car celui-ci est utilisé par un autre
processus."
```

Solution :

L'erreur se produit parce que le programme d'installation ne peut pas créer un répertoire qui existe. Toutefois, l'installation s'est déroulée correctement et le gestionnaire de provisionnement est entièrement fonctionnel.

Renommage des terminaux ACF2, RACF et TSS avant la mise à niveau

Les espaces dans les noms de terminaux ne sont plus pris en charge. Si vous avez créé des terminaux dont les noms contiennent des espaces dans une version précédente, supprimez les espaces avant de procéder à la mise à niveau vers la version 12.6.

Exécution du script SQL de mise à niveau

Après la mise à niveau, un script s'exécute au premier démarrage du serveur CA Identity Manager. Il met à jour la taille de la colonne Description de la table de persistance des tâches runtimeStatusDetail12 à 2 000 caractères.

Si un échec du script se produit, procédez comme suit :

1. Effectuez l'une des opérations suivantes :
   - Microsoft SQL Server : ouvrez l'analyseur de requêtes et sélectionnez le script dont vous avez besoin.
   - Oracle : ouvrez l'invite SQL pour le script dont vous avez besoin.
2. Sélectionnez l'un des scripts suivants :
   - Microsoft SQL Server : <chemin-installation>\tools\db\taskpersistence\sqlserver\archive_db_sqlserver_upgrade_to126sp2.sql
   - Oracle sur Windows : <chemin-installation>\tools\db\taskpersistence\oracle9i\archive_db_oracle_upgrade_to126sp2.sql
   - Oracle sur UNIX : <chemin-installation2>/tools/db/taskpersistence/oracle9i/archive_db_derby_upgrade_to126sp2.sql
3. Exécutez le script.
4. Vérifiez qu'aucune erreur ne s'est affichée lorsque vous avez exécuté le script.

Chapitre 4: Problèmes résolus

Ce chapitre traite des sujets suivants :

12.6.4

Les problèmes suivants ont été corrigés dans CA Identity Manager 12.6.4 :

Ticket de support	Problème signalé
20957471/07	Correction requise pour CQ 170096 sur IM 12.6 SP2
21517465/01	Portée du rôle d'administration dans la fenêtre de recherche
21536689/01	Mot de passe incorrect conservé lors de la création du répertoire IM
21539813/01	Echec de la mise à jour des quotas et du seuil pour les comptes LND si la liste de contrôle d'accès de fichier de messagerie est définie sur Gestionnaire.
21538682/01	Dans un IME avec jeton, lorsqu'une erreur se produit dans un champ de sélecteur de dates, le message d'erreur renvoyé affiche l'ID de clé au lieu de la valeur de paire du groupe de ressources.
21521403/04	La modification d'un objet de service entraîne le remplacement de la catégorie Service
21547136/01	Pour les nouveaux comptes d'applications Oracle, la date de début d'un élément responsibilityList n'est visible dans le gestionnaire de provisionnement que lors de la réexploration du terminal, si le compte est créé à l'aide d'un modèle sans aucune date de début définie.
21558292/01	Non-conformités 508
20957471/09	Les approbations de synchronisation inversée sont générées pour supprimer les responsabilités d'un compte d'applications Oracle lorsqu'une exploration a lieu après la création de comptes via IM avec des responsibilités déjà assignées.
21551822/01	Résultats de sélecteur d'objet erronés
21567422/01	Valeur manquante pour le mappage d'organisations dans gestionnaire de groupes après l'importation à partir d'IM
20957471/11	Le comportement des stratégies de compte modifié via la synchronisation inversée pour le serveur Oracle ne correspond pas au comportement attendu.
21576029/01	La description du terminal Windows NT n'est pas affichée dans la console d'utilisateur d'IM.

21559775/01	Echec de l'importation de rôles avec un caractère XML non valide (Unicode : 0x1f) généré par le sélecteur d'objet dans la tâche de rôle d'accès.
21593378/01	Les informations du gestionnaire de notification en temps réel ne sont pas correctes.
21590547/01	IM 12.6 SP2 : un attribut UserPrincipalName vide entraîne des erreurs de synchronisation pour les comptes Active Directory
21588715/01	Lorsqu'une règle d'affichage est définie dans une fenêtre de recherche de rôles d'administration, le filtre de recherche ne fonctionne pas.
21590303/01	Lors de l'exécution du nouveau client de chargeur en bloc d'IM r12.6 SP2, toutes ses tâches sont ouvertes et traitées, ce qui entraîne la consommation de toutes les ressources de la machine virtuelle Java et bloque les autres demandes de la file d'attente.
21594906/01	IM 12.6 SP1 : le niveau d'audit Les deux pour l'attribut n'est pas appliqué.
21574514/02	IM 12.6 SP2 : une tâche en cours de traitement est bloquée et le module PX est déclenché sur le flux de travaux de niveau événement.
21606642/02	Lorsqu'un groupe comprend 38 000 utilisateurs, les performances sont ralenties lors du traitement de la tâche Modifier les membres du groupe.
21557047/01	Possibles mappages d'attributs incorrects dans le connecteur Office 365
12345678/01	Nouvelle API d'agent Web SM requise pour IM 12.6 SP4.
21604197/01	Arrêt de l'importation de la définition de rôle pour le rôle de provisionnement dont le nom contient \00.
21604199/01	Echec de la recherche de rôles de provisionnement contenant le caractère \ avec le caractère générique *.
21609415/01	Erreur du connecteur Google : l'API peut être désapprouvée.
21626365/01	Erreur de script lors de l'affichage de la page 2 des détails des opérations du gestionnaire de provisionnement
21613942/01	Modification du filtre de conteneur de comptes
21419884/02	Durée de traitement excessive des clichés filtrés
21592259/01	Le filtre de mot de passe ne fonctionne pas comme prévu pour la validation de mot de passe.
21640856/01	Lorsqu'une approbation générée par synchronisation inversée pour l'ajout d'une responsabilité à un compte d'applications Oracle est rejetée, la responsabilité n'expire pas, même si elle s'affiche comme retirée dans la fenêtre Afficher les tâches soumises.
21633958/01	Rôles de provisionnement (PX) dupliqués
21641737/01	Niveaux de fonctionnalité Win2012 ADS signalés comme Win2008R2
21643258/01	Problème identique à celui décrit dans le ticket CQ176812, mais relatif à l'ordre de lecture.
21575724/01	La règle de portée d'utilisateur pour les stratégies d'administration des rôles d'administration empêche l'affichage des membres/administrateurs d'un rôle après un redémarrage de JBoss.

21584724/01	Journalisation supplémentaire pour le connecteur SAP
21500603/01	Echec de l'intégration de CA Identity Manager et SiteMinder
21639644/01	Exportation de modèle de compte Oracle
21657577/01	JCS ne référence plus le CCPP Apache, ce qui entraîne des échecs lorsque JavaScript est utilisé dans le connecteur CXP personnalisé.
21636774/01	Date de fin des responsabilités des comptes FND définie sur la date actuelle et message ORA/01422: exact fetch returns more than requested number of rows ORA-06512: at "APPS_APPLSYS3.FND_USER_PKG"
21641383/01	Blocage de la tâche Activer/Désactiver un utilisateur en cours si un email Policy Xpress est configuré.
21646678/01	Echec de l'utilitaire Ant lors du marquage des rôles si la propriété Titre est ajoutée dans les fenêtres de recherche.

21657600/01	Echec de l'importation des valeurs de champs personnalisés pour le rôle de provisionnement
21687010/01	Impossible de lancer certains rapports ELM
21668810/01	Problème lors de la suppression des utilisateurs affectés à des groupes dynamiques
21699782/01	Limitations de la liste des tâches. Ce ticket présente la procédure à suivre pour rendre facultative l'inclusion des éléments de la liste des tâches dans la page de connexion/bienvenue.
21650405/01	L'outil de configuration Xpress ne charge pas les flux de travaux de stratégie.
21539813/01	Modifications de la documentation requises pour la résolution du défaut PROD00176400.
21712883/01	IM 12.6 SP2 : les attributs de compte Active Directory relatifs à la date et l'heure ne s'affichent pas selon le fuseau horaire local dans la console d'utilisateur d'IM.
21669984/01	Une tâche privée (non publique) appelée sur l'alias public via TEWS peut être utilisée lorsqu'IDM et SM sont intégrés.
21711390/01	IM 12.6 : Faille de sécurité : l'URL permettant de demander une page d'image permet à un attaquant de définir contentType et d'exécuter du code dans le navigateur d'un utilisateur authentifié qui visite l'URL.
21713498/01	Le statut de tâche Terminé est affiché alors que les événements indiquent que la tâche est en cours.
21699782/01	Ajout de la recherche d'initiateur et d'ID d'utilisateur à la liste de travail de l'utilisateur
21704767/01	L'exemple AXIS Java pour ModifyGroupMembership.java ne fonctionne pas avec la version 12.6, quel que soit le Service Pack. Régression possible, car il fonctionnait avec la version 12.5
21651991/01	Ajout de l'option de configuration pour supprimer les notifications Modify_Account_Password IMPS dans IM

21730035/02	IM12.6 SP2 : terminal Active Directory : définir l'indicateur L'utilisateur doit changer de mot de passe après la réinitialisation du mot de passe sous l'onglet Configuration du terminal ne met pas à jour le provisionnement.
21730581/01	Inconsistance du type de certificateur entre le serveur de provisionnement et le terminal LND
21746621/01	Impossible d'explorer ou de corréler des comptes sous une unité organisationnelle dont le nom contient le caractère &.
21764131/01	L'attribut unique Office365 pour le blocage des informations d'identification est mappé vers eTDYN-str-multi-c/023 au lieu d'un attribut DYN à valeur unique, ce qui cause des erreurs lors de la synchronisation de compte avec un modèle de compte WEAK SYNC.

12.6.3

Les problèmes suivants ont été corrigés dans CA Identity Manager 12.6.3 :

Ticket de support	Problème signalé
21088049/02	Aucune réponse du job de flux de travaux dans l'état Actif.
21227662/05	Lorsqu'un terminal ACF2 est exploré avec l'utilisateur connecté, vous ne pouvez pas basculer sur le compte de l'administrateur de proxy.
21240169/01	Erreur StringIndexOutOfBoundsException lors de l'exportation de l'environnement CA Identity Manager
21298884/01	L'affectation ou la suppression d'un service pour un utilisateur n'est pas enregistrée dans le référentiel d'utilisateurs ou déclenche une erreur PX pour des comptes.
21325322/03	Echec des suspensions en bloc de tous les comptes LND ou ajout de tous les comptes au groupe Refuser l'accès (suspendu 0)
21329912/02	La synchronisation de compte ne fonctionne pas dans CA Identity Manager 12.6.
21347968/01 21358148/01	Le serveur de stratégies s'arrête brutalement lorsqu'un rôle d'accès CA Identity Manager est affecté à un utilisateur ou supprimé.
21366658/01	La création d'un utilisateur via une tâche de chargeur en bloc renvoie une exception de pointeur nul avec une intégration CA SiteMinder.
21378657/01	Le flux de travaux prédéfini est escaladé prématurément s'il est défini à l'aide d'une tâche Configurer le flux de travaux utilisant des stratégies globales pour les événements.
21378803/01	L'erreur Le mot de passe précédent ne peut pas être réutilisé est renvoyée et la tâche échoue.
21385464/01	Erreur NullPointerException lorsque la stratégie d'identité est configurée avec l'expression MemberRule-Groups Where-Attribute.
21387236/01	Créer un utilisateur à partir d'une copie ne copie pas l'attribut Organisation.

Ticket de support	Problème signalé
21389685/01	Expiration du délai de connexion avec une intégration à CA SiteMinder.
21393295/01	Rôle de provisionnement manquant dans la liste d'utilisateurs CA Identity Manager des rôles de provisionnement.
21395953/01	Policy Xpress envoie des courriels en boucle.
21417960/01 21417960/03	La modification du rôle de provisionnement renvoie un pointeur nul.
21424762/02	Erreur d'utilisateur interdit.
21430655/01	Les événements de flux de travaux basés sur la stratégie globale sont soumis à l'approbateur des escalades.
21430868/02	Impossible de supprimer l'initiale des prénoms secondaires lors du renommage des comptes LND.
21438148/03	L'organisation LND racine n'est pas explorée et aucun compte n'est récupéré.
21438256/01	L'exemple de script Java ne fonctionne pas avec une tâche Auto-enregistrement.
21438937/01	Un caractère spécial non standard est incorporé dans l'ancienne valeur de la persistance des tâches et dans l'audit.
21439600/01	Le client est confronté à des fenêtres vides lorsqu'il se connecte à l'aide d'un compte d'utilisateur dont le mot de passe est expiré.
21441213/01	La tâche de gestion importée de l'environnement CA Identity Manager r12.5 renvoie l'erreur java.lang.ClassCastException.
21447986/01	Lorsqu'une stratégie Policy Xpress est déclenchée et enregistrée à l'aide de la langue norvégienne, l'erreur java.lang.IllegalArgumentException: Unmatched braces in the pattern est renvoyée.
21450831/01	Lors de l'ouverture d'un nouveau modèle à l'aide de Connector Xpress, la boîte de dialogue Operation Bindings ne s'affiche pas.
21468616/01	Longueur de l'attribut Initiales des prénoms secondaires
21470755/01	Dans l'application mobile, la carte du gestionnaire de cartes de visite ne fonctionne pas.
21470794/01	Dans l'application mobile, toutes les erreurs de réinitialisation de mots de passe sont signalées comme des problèmes liés à la complexité, même si vous soumettez le mot de passe incorrect actuel.
21473825/01	Dans l'application mobile CA Identity Manager, la connexion échoue après avoir réinitialisé un mot de passe à partir de l'application mobile.
21475033/01	Dans l'application mobile CA Identity Manager, vous pouvez uniquement utiliser l'option Réinitialisation du mot de passe oublié une seule fois.
21478278/01	Un champ CAPTCHA dans la fenêtre CA Identity Manager n'est pas affiché à nouveau lorsque la phase de validation rejette un autre champ.

Ticket de support	Problème signalé
21480621/01	Echec de l'installation de iam_im_compile_jsp.* et build.xml lors de l'installation de CA Identity Manager r12.6 SP2 sur JBoss 6 EAP
21481343/01	Aucun logement actif n'est disponible, car ils sont bloqués indéfiniment.
21486937/01	Lorsque l'indicateur En attente est sélectionné pour une règle d'action dans Policy Xpress pour la catégorie Exécuter une fonction (non principale) comme Code externe et le type Exécuter le code Java, l'événement JavaActionWaitEvent est généré par Policy Xpress et le statut En cours est maintenu.
21488801/01	La configuration de la stratégie de mot de passe pour laquelle un caractère de ponctuation est requis, a pour résultat un mot de passe incorrect.
21497995/01	Les opérations en bloc renvoient une erreur lors de la sélection d'un ou de plusieurs éléments de liste de travail de délégation.
21520525/01	<ETAHOME>\bin\ADSLDAPDiag.exe échoue avec l'erreur Error 10054 reading data from server, lors de la connexion manuelle à un serveur Active Directory 2012.
21522674/01	Erreur de réinitialisation de connexion à l'étape de démarrage 5.
21535004/01	Impossible d'ajouter un rôle SAP à l'aide de TEWS
21537907/01	ConfigXpress ne fonctionne pas avec l'installation de CA Identity Manager r12.6 SP2.
21539251/01	Erreur lors de la création d'une copie ou de la modification de la tâche d'administration Afficher l'historique des accès.
215544431/01	Echec de la création de stratégie de flux de travaux globale
21558358/01	L'agent pour Exchange sans agent recherche CA CloudMinder/CAFT.
21568224/01	ConfigXpress.air ne fonctionne pas et renvoie une erreur pour l'installation CA Identity Manager r12.6 SP2.
21572374/01	Dans l'application mobile CA Identity Manager, l'approbation rapide ne fonctionne pas.
21585328/01	Echec de l'installation de ConfigXpress.air sur CA Identity Manager r12.6 SP2

12.6.2

Les problèmes suivants ont été corrigés dans CA Identity Manager 12.6.2 :

Ticket de support	Problème signalé
21198613/01	Le mot de passe défini par PX n'est pas synchronisé pour l'utilisateur et les comptes globaux.
21230281/01	Impossible d'importer des gestionnaires d'attributs logiques dans la console de gestion

Ticket de support	Problème signalé
21263275/01	Problèmes avec la stratégie de mot de passe Arcot.
21269108/02	Problèmes lors de l'installation de l'agent de synchronisation de mots de passe CA Identity Manager r12.6.
21264877/01	Le nom unique de l'administrateur est ajouté à l'URL externe.
21275958/01	Exception de pointeur nul lors de l'obtention d'un terminal SAP
21272983/01	Erreurs lors de la lecture du terminal CA Access Control lorsque plusieurs bases de données de modèles de stratégie (PMDB) sont définies.
21173122/01	Les définitions de rôle importées ne sont pas affichées.
21270763/01	L'erreur se produit lorsqu'un répertoire d'approvisionnement est créé à l'aide de l'assistant.
21280342/01	DoSynchUserRoles n'active pas les cases à cocher Ajouter les comptes manquants et Supprimer les comptes supplémentaires pour le code WSDL du service Web d'exécution des tâches CA Identity Manager (TEWS).
21285651/01	Compatibilité de la tâche Synchroniser les comptes avec le modèle de compte avec le service TEWS.
21295778/01	L'erreur Error instantiating Policy Xpress plugin est renvoyée lors de la création ou de la modification d'une stratégie Policy Xpress.
21304316/01	Problème de performances lors de l'ajout de groupes à un utilisateur à l'aide d'une tâche de création ou de modification d'utilisateur.
21304316/02	Problème de performances lors de l'ajout de groupes à un utilisateur, à l'aide du bouton Ajouter des groupes de la tâche Modifier un utilisateur.
21306987/01	L'erreur NoClassDefFoundError est renvoyée lors de l'exécution de highavailability.bat.
21307126/01	RSA Secure ID 7 : impossible d'obtenir un terminal à cause de problèmes avec le script pour créer un groupe OSGI (Open Service Gateway Initiative).
21315277/04	Le serveur de connecteurs C++ s'arrête brutalement lors de la recherche de comptes d'utilisateurs Active Directory déplacés ou renommés.
21319140/01	Les données du fichier dir.xml basé sur SQL sont importées en majuscules.
21322022/01	Les connexions CA Identity Manager sont plus lentes après une période.
21325322/01	Fermeture de la session suite à des échecs de communication sur LND lors de la modification de comptes.
21331632/01	Le message d'avertissement lors de la révocation du service n'inclut pas le paramètre de nom d'utilisateur.
21335464/01	Erreur de script de gestionnaire de provisionnement lors de l'affichage d'une opération sur plusieurs pages.

Ticket de support	Problème signalé
21351855/01	CA Identity Manager ne parvient pas à créer l'environnement sans provisionnement et lorsque seul le rôle d'administrateur système est sélectionné.
21361599/01 21383034/01	L'erreur suivante s'affiche lorsque la tâche Modifier un utilisateur est utilisée : Echec de la tâche. Irrécupérable : Echec de l'exécution de SynchronizeAttributesWithAccountEvent: Message d'erreur : For input string
21393461/01	Exception lors de la mise à jour de l'attribut Activer/Désactiver un utilisateur ou d'un autre attribut d'utilisateur.

12.6.1

Les problèmes suivants ont été corrigés dans CA Identity Manager 12.6.1 :

Ticket de support	Problème signalé
20576709/02	Prise en charge du partage du serveur de rapports BusinessObjects commun requise pour CA Identity Manager et SiteMinder
20576725/02	Prise en charge du serveur de rapports BusinessObjects requise dans une configuration de haute disponibilité
20583665/02	Prise en charge du serveur de rapports BusinessObjects XI 3.1 SP5 (CABI 3.3) requise
20774861/02	Impossible d'inclure des données d'objet secondaires dans Policy Xpress
20777137/02	Améliorations apportées au flux de travaux basé sur une stratégie pour obtenir les objets secondaires (objets d'utilisateur) requis pour les objets principaux
20888199/01	Absence de documentation pour la convention d'attribution de nom unique pour les modèles de compte pour le service Web d'exécution des tâches
21073146/01	Synchronisation impossible avec la tâche Synchroniser les comptes avec le modèle de compte
21086870/01	Absence d'invite de saisie de clé FIPS dans le programme d'installation autonome de JCS, entraînant des problèmes de chiffrement
21108813/01	CA Identity Manager 12.6 ne fournit pas les définitions de rôle attendues.
21111634/01	Création des journaux de terminal JCS impossible
21131768/01	Problème d'attribut de flux de travaux de la stratégie global (type d'objet secondaire manquants dans les définitions d'événement)
21135604/01	Echec de la tâche de gestionnaires d'attributs logiques avec une erreur NullPointer
21136454/01	Correction de la faille de sécurité liée à l'injection SQL dans cette version

Ticket de support	Problème signalé
21136456/01	Faille de sécurité
21136499/01	Les données des boîtes de sélection ne fonctionnent pas avec une fenêtre Profil associée à un service dans CA Identity Manager 12.6.
21137701/01	Réception d'une exception PxEnvironmentException lors des appels de la stratégie Policy Xpress au code Java externe
21140501-1	Prise en charge des déploiements cloud (gestion de clients hébergés)
21146621/01	Validation globale des attributs dans directory.xml
21156269/01	Différences entre les schémas de base de données générés par le programme d'installation et les scripts de base de données dans le dossier d'outils
21156269/01	Plus de scripts requis pour la création manuelle de base de données
21162602/01	La corrélation personnalisée pour TSS ne fonctionne pas sur UNIX.
21170706/01	Les résultats de l'affichage des tâches soumises sont triés de manière incorrecte lorsque les paramètres régionaux sont définis sur Danois.
21175201/01	La synchronisation de compte initialisée par la notification entrante ne se produit pas lorsque les rôles de provisionnement sont affectés à l'aide de stratégies Policy Xpress.
21181592/01	Echec du chargement de CA Identity Manager r12.6 avec une erreur de chemin d'accès de classe non valide
21183366/01	Nom d'utilisateur incorrect utilisé avec les sources de données
21187385/01	Arrêts intermittents de CA Identity Manager
21188814/01	Le serveur de stratégies de SiteMinder r12 SP3 CR11 tombe en panne lors de l'accès à la stratégie CA Identity Manager.
21190699/01	Impossible de récupérer les informations d'objet secondaires à partir de Policy Xpress sur les stratégies basées sur les événements ou sur les tâches. Les informations de valeur d'attribut d'origine sont également renvoyées, même lorsque Policy Xpress se déclenche après la fin de la tâche.
21190873/01	508 Problème de conformité : les info-bulles des cases à cocher sont incompréhensibles.
21193837/01	Création et suppression d'objets gérés
21194712-1	Policy Xpress avec itérateur s'interrompt lorsqu'une affectation de rôle d'accès déclenchée est rejetée par le flux de travaux.
21200396/01	508 Problème de conformité : problèmes avec le lien Passer directement au contenu principal
21200412/01	508 Problème de conformité : les messages d'erreur et d'avertissement ne sont pas lus correctement par le logiciel d'assistance aux utilisateurs handicapés.

Ticket de support	Problème signalé
21213029-1	Les variables de services de mot de passe stockées dans le cache de JSession ne sont pas effacées lors de la déconnexion et les demandes ultérieures sont redirigées vers la page pws.fcc.

Chapitre 5: Documentation

Les noms de fichier des manuels de CA Identity Manager sont les suivants :

Nom du manuel	Nom du fichier
Notes de parution	im_release_fra.pdf
Manuel d'implémentation	im_impl_enu.pdf
Installation Guide for WebLogic (Manuel d'installation pour WebLogic)	im_install_weblogic_enu.pdf
Installation Guide for WebSphere (Manuel d'installation pour WebLogic)	im_install_websphere_enu.pdf
Installation Guide for JBoss (Manuel d'installation pour WebLogic)	im_install_jboss_enu.pdf
Upgrade Guide (Manuel de mise à niveau)	im_upgrade_enu.pdf
Configuration Guide (Manuel de configuration)	im_config_enu.pdf
Administration Guide (Manuel d'administration)	im_admin_enu.pdf
User Console Design Guide (Manuel de conception de la console d'utilisateur)	im_uc_design_enu.pdf
Programming Guide for Java (Manuel de programmation pour Java)	im_dev_enu.pdf
Provisioning Reference Guide (Manuel de référence du provisionnement)	im_provisioning_reference_enu.pdf
Connectors Guide (Manuel des connecteurs)	im_connectors_enu.pdf
Connector Xpress Guide (Manuel des connecteurs Xpress)	im_connector_xpress_enu.pdf
Java Connector Server Implementation Guide (Manuel d'implémentation du serveur de connecteurs Java)	im_jcs_impl_enu.pdf
Programming Guide for Java Connector Server (Manuel de programmation du serveur de connecteurs Java)	im_jcsProg_Enu.pdf
Glossaire	im_glossary.pdf
Bibliothèque	im_bookshelf_enu.zip

Ce chapitre traite des sujets suivants :

Bibliothèque

La bibliothèque permet d'accéder à l'ensemble de la documentation CA Identity Manager à partir d'une interface unique. Elle contient :

- Une liste extensible du contenu de tous les manuels au format HTML
- Une fonctionnalité de recherche de texte intégral dans l'ensemble des manuels, avec classement des résultats des recherches et termes recherchés mis en surbrillance dans le contenu
- Des chemins de navigation reliés aux rubriques du niveau supérieur
- Un index HTML unique des rubriques pour tous les manuels
- Des liens vers les versions PDF des manuels pour impression

Pour utiliser la bibliothèque :

1. Téléchargez la bibliothèque sur le site de support de CA.
2. Extrayez le contenu du fichier ZIP.

   Remarque : Pour de meilleures performances lors de l'installation de la bibliothèque sur un système distant, accédez à cette bibliothèque à partir d'un serveur Web.
3. Affichez la bibliothèque comme indiqué ci-après.
   - Si la bibliothèque se trouve sur un système local et que vous utilisez Internet Explorer, ouvrez le fichier Bookshelf.hta.
   - Si la bibliothèque se trouve sur un système distant ou que vous utilisez Mozilla Firefox, ouvrez le fichier Bookshelf.html.

     Remarque : Pour de meilleures performances lors de l'installation de la bibliothèque sur un système distant, accédez à cette bibliothèque à partir d'un serveur Web.

La bibliothèque nécessite Internet Explorer 7 ou 8, ou Mozilla Firefox 2 ou 3. Pour les liens vers les manuels au format PDF, Adobe Reader 7 ou version supérieure est nécessaire. Vous pouvez télécharger Adobe Reader à l'adresse www.adobe.com.

Problèmes connus

Vous pouvez consulter une liste de tous les problèmes connus pour CA Identity Manager sur le site du support de CA.

Notes de parution relatives à l'intégration de CA Identity Manager et CA Identity Governance

Toutes les notes de parution relatives à l'intégration de CA Identity Manager et CA Identity Governance se trouvent dans les *Notes de parution de CA Identity Governance*. Vous pouvez accéder à la bibliothèque de CA Identity Governance à partir du site de support de CA.

Annexe A: Fonctionnalités d'accessibilité

CA Technologies 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 Identity Manager.

508 Conformité

CA Identity Manager est conforme à la Section 508 de la norme US Rehabilitation Act et au niveau AA des directives Web Content Accessibility Guidelines (WCAG2.0). Pour plus d'informations, reportez-vous à la rubrique Améliorations apportées au produit (page 65). Vous pouvez également demander à votre responsable de compte une copie du document Voluntary Product Accessibility Template (VPAT) de CA Technologies.

Améliorations du produit

Des améliorations relatives à l'accessibilité ont été apportées dans les zones suivantes de *CA Identity Manager* :

- Affichage
- Son
- Clavier
- Souris

Remarque : Les informations suivantes s'appliquent aux applications basées sur Windows et sur Macintosh. Les applications Java s'exécutent sur différents systèmes d'exploitation hôtes, qui disposent déjà de technologies d'assistance. Pour que les technologies d'assistance existantes puissent accéder aux programmes écrits en JPL, un pont est nécessaire entre ces technologies dans leurs environnements natifs et la prise en charge de Java Accessibility qui est disponible à partir de la machine virtuelle Java. Ce pont connecte la machine virtuelle Java et la plate-forme native, et sera donc légèrement différent selon la plate-forme utilisée. Sun développe actuellement les parties JPL et Win32 de ce pont.

Affichage

Pour augmenter la visibilité sur l'écran de votre ordinateur, vous pouvez ajuster les options suivantes :

Style de police, couleur et taille des éléments

Permet de choisir la couleur de la police, la taille et d'autres combinaisons visuelles.

Résolution d'écran

Permet de modifier le nombre de pixels pour agrandir des objets dans la fenêtre.

Largeur du curseur et fréquence de clignotement

Permet de rendre le curseur plus facile à trouver ou de réduire le clignotement.

Taille de l'icône

Permet d'agrandir les icônes pour augmenter la visibilité ou de réduire l'espace de la fenêtre.

Schémas de contraste élevé

Permet de sélectionner des combinaisons de couleur qui sont plus faciles à voir.

Son

Utilisez le son en cas de déficience visuelle ou pour faciliter l'écoute des sons émis par l'ordinateur en ajustant les options suivantes :

Volume

Permet de monter ou de baisser le son de l'ordinateur.

Conversion de texte par synthèse vocale

Permet d'écouter les options de commande et de lire le texte par synthèse vocale.

Avertissements

Permet d'afficher des avertissements visuels.

Avertissements

Permet d'émettre des avertissements visuels ou oraux selon que les fonctionnalités d'accessibilité sont activées ou désactivées.

Schémas

Permet d'associer les sons de l'ordinateur à des événements système spécifiques.

Légendes

Permet d'afficher des légendes pour la fonction vocale et les sons.

Remarque : Si vous utilisez un lecteur d'écran, il est recommandé d'installer la dernière version de l'outil pour une interprétation optimale.

Clavier

Vous pouvez effectuer les réglages de clavier suivants :

Vitesse de répétition

Permet de définir la vitesse de répétition d'un caractère lorsque vous appuyez sur une touche.

Tonalités

Permet d'émettre des tonalités lorsque vous appuyez sur certaines touches.

Touches collées

Permet à ceux qui utilisent le clavier avec une main ou un doigt de choisir des dispositions de clavier plus adaptées.

Lien Ignorer

Vous permet d'utiliser le lien Ignorer et revenir au contenu principal pour accéder rapidement au contenu principal.

Souris

Vous pouvez utiliser les options suivantes afin de rendre votre souris plus rapide et plus facile à utiliser :

Vitesse de clic

Permet de définir la vitesse de clic de la souris lorsque vous effectuez une sélection.

Verrouillage de clic

Permet une mise en surbrillance ou un glissement sans devoir maintenir le bouton de la souris enfoncé.

Inverser

Vous permet d'inverser les fonctions contrôlées par les touches de gauche et de droite de la souris.

Fréquence de clignotement

Vous permet d'activer le clignotement du curseur et de choisir sa vitesse.

Options du pointeur

Vous permet d'effectuer les opérations suivantes :

- Masquer le pointeur lors de la saisie
- Afficher l'emplacement du pointeur
- Définir la vitesse de déplacement du pointeur déplace dans la fenêtre
- Sélectionner la taille et la couleur du pointeur pour une meilleure visibilité
- Déplacer le pointeur vers un emplacement par défaut dans une boîte de dialogue

Exceptions Mozilla FireFox

Il est recommandé que les utilisateurs de clavier et de JAWS utilisent Internet Explorer 8, pour les raisons suivantes :

- Dans Firefox, les boîtes de dialogue ne reçoivent pas le focus d'entrée/de sortie.
- Le lien Ignorer et revenir au contenu principal n'est pas toujours lu d'abord par le lecteur d'écran.

Raccourcis clavier

La table suivante répertorie les raccourcis clavier pris en charge dans CA Identity Manager :

Clavier	Description
Ctrl+X	Couper
Ctrl+C	Copier
Ctrl+K	Rechercher le suivant
Ctrl+F	Rechercher ou remplacer
Ctrl+V	Coller
Ctrl+S	Enregistrer
Ctrl+Maj+S	Tout enregistrer
Ctrl+D	Supprimer la ligne
Ctrl+flèche droite	Mot suivant
Ctrl+flèche vers le bas	Défilement de la ligne vers le bas
End	Fin de ligne