CA Identity Manager

Notes de parution

r12

Produits CA référencés

Ce document contient des références aux produits CA suivants :

- CA Identity Manager
- CA SiteMinder® Web Access Manager
- CA Security Command Center (CA SCC)
- CA Audit
- eTrust® Directory, également nommé CA Directory

Support technique

Pour obtenir une assistance technique en ligne, ainsi que la liste complète des centres et de leurs coordonnées et heures d'ouverture, contactez notre service d'assistance clientèle à l'adresse : http://www.ca.com/worldwide.

Table des matières

Chapitre 1 : Bienvenue

Ce document contient des informations importantes relatives aux systèmes d'exploitation pris en charge, à l'installation, aux problèmes connus et au support technique de CA.

Chapitre 2 : Nouvelles fonctionnalités

Ce chapitre traite des sujets suivants :

Plates-formes et versions prises en charge

Dans Identity Manager r12, des ajouts ont été faits aux versions, bases de données et répertoires de serveurs d'applications pris en charge.

Remarque : Pour obtenir la liste complète des plates-formes et des versions prises en charge, reportez-vous à la matrice de support d'Identity Manager disponible sur le site d'assistance Identity Manager http://ca.com/support.

Architecture Identity Manager

Par rapport aux versions précédentes, l'architecture d'Identity Manager r12 comprend les évolutions ci-après.

- **Serveur de provisionnement et gestionnaire de provisionnement incorporés**

  Le serveur de provisionnement est le serveur qui gère les comptes supplémentaires affectés à un utilisateur Identity Manager. Lorsque vous affectez un rôle de provisionnement à un utilisateur Identity Manager, le serveur de provisionnement crée des comptes sur des terminaux satisfaisant aux exigences de ce rôle. Par exemple, si vous affectez un rôle de provisionnement incluant un modèle de compte Exchange, le serveur de provisionnement affecte un compte Exchange à l'utilisateur.

  Le gestionnaire de provisionnement est l'interface utilisateur qui permet de gérer les types de terminaux, comme Exchange ou Oracle, et les terminaux, comme un système spécifique hébergeant Exchange. Cette interface était précédemment appelée eTrust Admin Manager. Le gestionnaire de provisionnement comporte d'autres fonctionnalités, comme l'exploration et la corrélation de compte ; toutefois, cette fonctionnalité supplémentaire est à présent dupliquée dans la console d'utilisateur Identity Manager, où elle est plus accessible.

  Les versions précédentes d'Identity Manager reposaient sur eTrust Admin pour le provisionnement.

  Remarque : Le serveur de provisionnement et le gestionnaire de provisionnement sont des composants facultatifs.

- **Intégration d'Identity Manager à SiteMinder**

  SiteMinder n'est plus une condition préalable à l'installation d'Identity Manager. Désormais, vous pouvez également effectuer l'intégration à SiteMinder pour obtenir des fonctionnalités avancées, notamment l'authentification SiteMinder et les stratégies de mot de passe avancées.

  Les versions précédentes d'Identity Manager reposaient sur eTrust Admin pour les fonctionnalités ci-après.

  – Authentification

  – Stockage des informations liées aux rôles et aux tâches (dans le magasin de stratégies)

  – Connexion à un magasin d'utilisateurs

  – Stratégies de mot de passe

  Identity Manager dispose, à l'origine, de cette fonctionnalité.

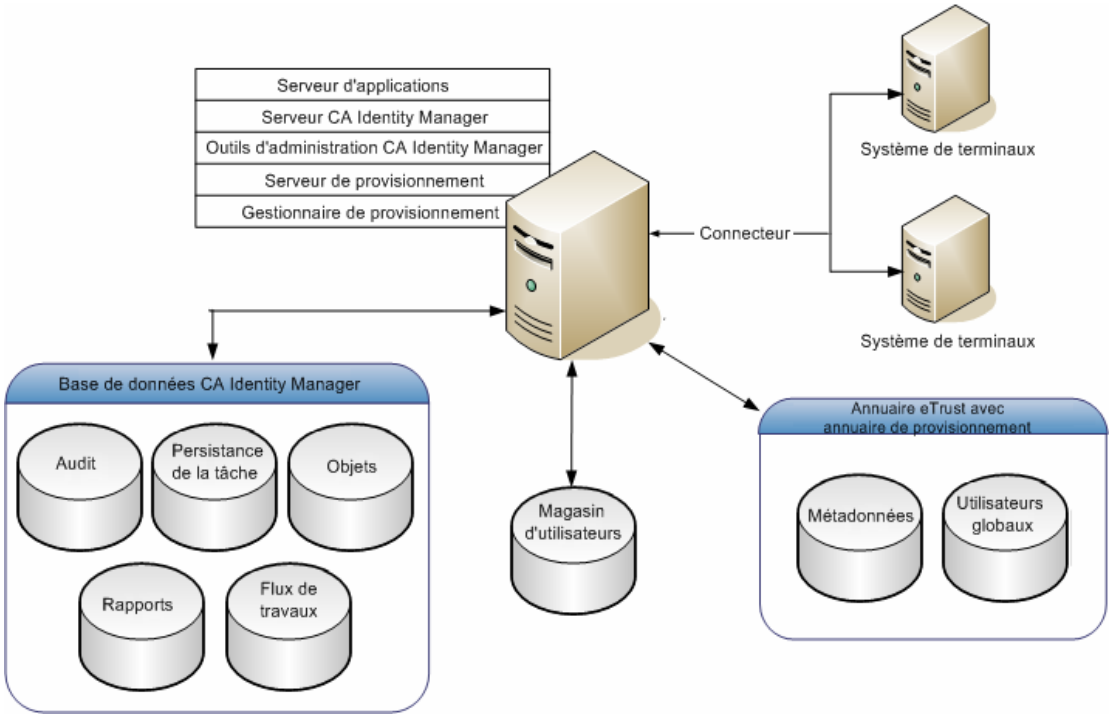
  Remarque : Vous pouvez effectuer l'intégration à SiteMinder pour obtenir des fonctionnalités avancées, notamment l'authentification SiteMinder et les stratégies de mot de passe avancées.

- **Magasin d'objets**

  Désormais, Identity Manager r12 stocke des informations liées aux rôles et aux tâches dans un nouveau magasin d'objets. Le magasin d'objets est une base de données relationnelles configurée automatiquement par Identity Manager à l'exécution.

L'illustration qui suit décrit une implémentation Identity Manager qui comprend le provisionnement.

Remarque : L'annuaire de provisionnement, qui stocke les informations requises pour utiliser le provisionnement et des informations sur les utilisateurs globaux, doit être installé dans eTrust Directory, condition préalable à l'installation d'Identity Manager avec provisionnement.



Améliorations du programme d'installation

Tous les composants nécessaires à l'installation du serveur Identity Manager sont désormais installés avec un seul programme d'installation, qui comprend des composants pour le provisionnement et des extensions vers un serveur de stratégies SiteMinder.

Le programme d'installation d'Identity Manager fournit le serveur de provisionnement, l'annuaire de provisionnement et le gestionnaire de provisionnement Identity Manager. Il configure également les connexions avec les bases de données qui stockent les données d'objet et les données pour le flux de travaux, la persistance des tâches, la création de rapports et l'audit.

Les modifications apportées à l'installation d'Identity Manager sont répertoriées ci-après.

- Identity Manager n'a plus besoin de SiteMinder pour l'authentification.
- La persistance des tâches n'est plus facultative, elle est activée à l'installation.
- Un schéma de base de données est étendu automatiquement pour chaque base de données utilisée par Identity Manager.
- Les outils d'administration sont désormais installés aux emplacements indiqués ci-après.
  - **Windows :** C:\Program Files\CA\IAM Suite\Identity Manager\tools
  - **UNIX :** *HOME*/CA/IAM_Suite/Identity_Manager/tools
- Les scripts de post-installation ne sont plus nécessaires.

Améliorations des rapports

Les rapports d'Identity Manager permettent de voir l'état actuel d'un environnement Identity Manager. Vous pouvez utiliser ces informations pour vous assurer de la conformité avec les stratégies métier internes ou les réglementations externes.

Identity Manager r12 comprend les améliorations ci-après pour les rapports.

- **Intégration au serveur de rapports IAM**

  Identity Manager r12 utilise Business Objects Enterprise XI pour concevoir, gérer et afficher des rapports de la base de données de rapports. Comme Identity Manager fournit une version d'exécution de Business Objects, aucune licence séparée n'est requise.

- **Nouvelles tâches d'administration pour l'exportation de données vers la base de données de rapports**

  Identity Manager comprend de nouvelles tâches par défaut, qui permettent d'exporter des données d'Identity Manager vers la base de données de rapports. Chaque fois que vous exportez des données vers la base de données de rapports, vous créez un *instantané*, une représentation de l'état actuel d'objets spécifiés par l'utilisateur dans un environnement Identity Manager.

  Grâce à ces nouvelles tâches par défaut, vous pouvez créer des définitions d'instantanés et capturer un instantané à partir duquel vous pouvez générer un rapport.

- **Rapports prédéfinis supplémentaires**

  Identity Manager contient les rapports prédéfinis ci-après, que vous pouvez utiliser comme des rapports installés. Vous pouvez également les personnaliser pour répondre à vos besoins commerciaux.

  - **Comptes de terminaux**

    Liste de comptes par nom du compte, propriétaire et heure de création pour chaque terminal, triée par type de terminal.

  - **Comptes non standard**

    Liste des comptes non standard, comme les comptes orphelins et les comptes système.

  - **Tendances des comptes non standard**

    Tendances des comptes non standard par type de compte non standard, affichées sous forme de graphiques.

  - **Comptes orphelins**

    Liste des comptes non associés à un utilisateur. Les comptes orphelins sont répertoriés par nom du compte, propriétaire et heure de création pour chaque terminal et sont triés par type de terminal.

  - **Stratégies**

    Liste des stratégies, incluant les conditions de stratégies, ainsi que des actions Action lors de l'application de la stratégie et Action lors de la suppression de la stratégie.

  - **Administrateurs de rôles**

    Liste des administrateurs de rôles.

  - **Membres de rôles**

    Liste des membres de rôles.

  - **Propriétaires de rôles**

    Liste des propriétaires de rôles.

- **Rôles**

  Liste des rôles et de leur description.

- **Clichés**

  Liste de tous les instantanés disponibles dans la base de donnes de rapports.

- **Rôles des tâches**

  Liste des tâches par description, catégorie et type. Pour chaque tâche, spécifiez tous les rôles associés.

- **Comptes d'utilisateurs**

  Liste des comptes par utilisateur. Les comptes d'utilisateurs sont répertoriés par nom du compte, attributs de compte et terminal, triés par type de terminal.

- **Etat de synchronisation des stratégies d'utilisateur**

  Liste des utilisateurs, qui comprend des stratégies actuellement affectées et des stratégies devant être affectées de nouveau.

- **Profil d'utilisateur**

  Liste des utilisateurs avec toutes les informations disponibles sur eux.

- **Droits d'utilisateurs**

  Liste d'utilisateurs et de leurs comptes, rôles et groupes associés.

Gestion des connexions

La gestion des connexions est utilisée pour configurer les détails de connexion du serveur de base de données dans Identity Manager. Lorsque Identity Manager doit se connecter à un serveur de base de données, il utilise les détails de connexion pour accéder à ce serveur. La gestion des connexions permet de créer plusieurs connexions avec différents serveurs de base de données sous un seul type de connexion. Pour chaque type de connexion, vous pouvez spécifier une connexion par défaut. Vous devez configurer un type de connexion principal pour Identity Manager via la console de gestion.

Améliorations du provisionnement

Avec cette version, vous pouvez effectuer plus d'actions dans la console d'utilisateur Identity Manager. Certaines d'entre elles étaient précédemment disponibles dans eTrust Admin Manager. Vous pouvez utiliser la console d'utilisateur pour réaliser les actions ci-après.

- Explorer et corréler des comptes sur des terminaux
- Corréler des comptes orphelins et système avec un utilisateur Identity Manager
- Auditer des actions de provisionnement, comme l'affectation d'un rôle de provisionnement à un utilisateur global

Cette version contient également les éléments ci-après.

- Connector Xpress, outil graphique pour créer des connecteurs personnalisés
- Prise en charge des connecteurs dynamiques (JNDI et JDBC) pour les utiliser avec les métadonnées XML générées par Connector Xpress
- Serveur de connecteurs Java, qui traite les requêtes des connecteurs Java
- Fonctions de haute disponibilité pour le serveur de connecteurs C++, précédemment appelé Super Agent
- Nouveaux connecteurs Java pour Kerberos pour administrer les principaux Kerberos et les polices des mots de passe Kerberos sur les serveurs Solaris.
- Nouveaux connecteurs Java pour SAP (avec prise en charge de l'interface commune d'accès)
- Nouveaux connecteurs Java pour Oracle, MS-SQL et 0S/400, fournis avec le serveur de connecteurs Java

  Ces trois connecteurs remplacent les options d'échantillon, qui ne sont plus prises en charge.
- Améliorations du gestionnaire de provisionnement pour proposer une interface utilisateur générique pour les types de terminaux dynamiques JDBC et JNDI, créés à l'aide de Connector Xpress.

DYN GUI

Nous avons amélioré le DYN GUI du gestionnaire de provisionnement pour fournir un ensemble de fonctionnalités améliorées vous permettant de manipuler de manière arbitraire les objets terminaux avec un seul module de gestionnaire de provisionnement.

Par exemple, lorsque vous mappez un champ dans Connector Xpress, un élément est placé dans les métadonnées pour représenter ce champ. Chaque fois que vous examinez un objet dans ce connecteur, le DYN GUI utilise les métadonnées pour afficher les champs appropriés.

Les changements de cette version étendent les capacités du DYN GUI grâce à un ensemble de fonctionnalités améliorées, facilitent les ajouts futurs de nouvelles fonctionnalités et offrent un meilleur affichage à l'utilisateur.

Connecteur Lotus Notes/Domino au stade de développement

Pour la version r12 de Identity Manager, le connecteur LND basé Java est encore au stade de développement.

Il **n'**est **pas** adapté aux environnements de production. Le connecteur certifié sera disponible dans une version cumulative. Pour plus d'informations, contactez le représentant chargé de votre compte CA.

Remarque : Veillez à ne pas installer les connecteurs LND C++ et Java dans le même environnement Identity Manager.

Amélioration de la création de rapports d'état

Identity Manager r12 comporte plusieurs fonctionnalités permettant d'afficher l'état des tâches Identity Manager.

Améliorations de l'affichage de la tâche soumise

Identity Manager r12 comprend l'onglet Afficher la tâche soumise, qui permet d'afficher l'état d'une tâche et la dépendance de celle-ci par rapport à d'autres tâches, événements et flux de travaux.

Dans Identity Manager r12, l'onglet Afficher la tâche soumise inclut les améliorations ci-après.

- L'onglet Afficher la tâche soumise affiche désormais plus de détails sur les tâches et les événements associés.
- Vous pouvez annuler des tâches en attente et resoumettre ou rejeter des tâches ayant échoué depuis l'onglet Afficher les tâches soumises.
- Vous pouvez désormais configurer l'onglet Afficher les tâches soumises.

La tâche Afficher l'activité de l'utilisateur

L'activité de l'utilisateur est historique des tâches engageant un utilisateur spécifique. Les administrateurs peuvent utiliser la tâche Afficher l'activité de k'utilisateur pour suivre les informations de l'utilisateur<;

- Tâches effectuées sur l'utilisateur
- Tâches effectuées par l'utilisateur
- Approbations des flux de travaux par l'utilisateur

Pour afficher l'activité de l'utilisateur

1. Cliquez sur Utilisateurs, Gérer les utilisateurs, Afficher l'activité de l'utilisateur..

   La boîte de dialogue Sélection de l'utilisateur s'affiche.

2. Rechercher un utilisateur et cliquez sur Sélectionner..

   La fenêtre Afficher l'activité de l'utilisateur apparaît..

   Pour plus d'informations sur l'activité de l'utilisateur qui est affichée, reportez-vous à la *console d'utilisateur de l'aide en ligne*.

Onglet Historique de l'utilisateur

L'onglet Historique de l'utilisateur permet d'afficher des tâches concernant un utilisateur. Vous pouvez ajouter cet onglet à une tâche Modifier ou Afficher un utilisateur.

Remarque : Cet onglet est inclus dans la vue par défaut de l'utilisateur de la tâche d'activité.

Les détails de la tâche qui sont affichés dans cet onglet sont également visibles dans l'onglet Afficher les tâches soumises.

Améliorations des flux de travaux

Identity Manager r12 dispose d'améliorations de la fonctionnalité de flux de travaux, qui simplifient le processus de création d'un flux de travaux et ajoutent de nouvelles fonctions. Ces améliorations sont décrites dans les sections qui suivent.

Modèles de processus de flux de travaux

Les modèles de processus de flux de travaux permettent de configurer et gérer le contrôle de flux de travaux, dans son intégralité, depuis la console d'utilisateur Identity Manager. Ces modèles de processus génériques peuvent être configurés pour contrôler la plupart des tâches et événements Identity Manager.

Les nouveaux modèles de processus permettent le contrôle de flux de travaux de niveau tâche et de niveau événement, la configuration simplifiée de l'outil de résolution de participants pour les approbateurs et des processus d'approbation à plusieurs étapes.

La liste des approbateurs peut également être déterminée de manière dynamique à l'exécution, en fonction des attributs de la tâche ou de l'événement en cours d'approbation.

Flux de travaux de niveau tâche

Vous pouvez associer des processus de flux de travaux avec des tâches et des événements. Les participants peuvent ainsi approuver ou rejeter l'intégralité d'une tâche Identity Manager ou seulement un événement précis d'une tâche.

Le flux de travaux de niveau tâche permet aux participants de consulter tous les événements avant de décider d'approuver ou de rejeter une requête. Quand un processus de flux de travaux est associé à un événement précis dans une tâche, il est impossible pour l'approbateur de voir le contexte global de la tâche objet de la requête.

Boutons d'action du flux de travaux

Vous pouvez ajouter de nouveaux boutons aux tâches d'approbation de flux de travaux pour compléter ou remplacer les boutons d'approbation ou de rejet standard. Cette fonction est illustrée par un exemple dans les tâches de requêtes en ligne.

Requêtes en ligne et historique

Dans la console d'utilisateur, les utilisateurs peuvent effectuer des requêtes de modification de leurs comptes et les administrateurs des requêtes de modification des comptes d'utilisateurs. Ces tâches déclenchent un modèle de processus de flux de travaux qui nécessite jusqu'à trois approbateurs : un consultant, pour commenter la requête ; un utilisateur commercial, pour approuver la requête ; un expert technique, pour implémenter la requête.

Les tâches de requête en ligne incluent également un nouveau contrôle de l'historique, qui permet aux approbateurs de joindre des remarques ou des commentaires à la tâche à différents niveaux de progression.

Planification de tâches

La planification permet d'automatiser l'exécution d'une tâche à une date ultérieure. Si vous planifiez une tâche associée à un processus de flux de travaux, Identity Manager exécute toutes les tâches telles que définies dans ce processus. L'état des tâches planifiées peut être affiché dans la page Afficher les tâches soumises.

Une tâche planifiée qu'Identity Manager n'a pas encore exécutée peut être replanifiée ou annulée via la page Afficher les tâches soumises.

Identity Manager fournit le planificateur en tant qu'onglet spécial. Pour accéder au planificateur, vous devez configurer une tâche avec l'onglet du planificateur.

Améliorations de la console d'utilisateur

Identity Manager r12 comporte de nombreuses améliorations permettant d'accroître la prise en charge des nouvelles fonctions et de simplifier l'utilisation. Ces améliorations sont présentées dans les sections qui suivent.

Aide personnalisée

Identity Manager vous permet de créer votre propre aide personnalisée pour les tâches et les onglets que vous avez personnalisés dans la console d'utilisateur. Pour implémenter l'aide personnalisée, vous pouvez créer un système d'aide contextuelle avec des fichiers d'aide HTML personnalisés ou des pages Wiki, puis rediriger les liens d'aide dans la console d'utilisateur Identity Manager pour accéder à votre aide personnalisée.

Cette fonction permet également de traduire l'aide par défaut (rédigée en anglais) dans n'importe quelle autre langue.

Tâches imbriquées

Une tâche imbriquée est une tâche d'administration pouvant être ouverte à partir de l'onglet Profil d'une autre tâche. L'utilisateur de la première tâche ouvre la tâche imbriquée en cliquant sur un lien ou un bouton. Par exemple, vous pouvez ajouter un bouton Supprimer un utilisateur à la tâche Modifier l'utilisateur. Si le compte d'utilisateur n'est plus valide, un administrateur peut cliquer sur le bouton Supprimer un utilisateur pour supprimer le compte sans devoir retourner au volet de navigation pour sélectionner une nouvelle tâche.

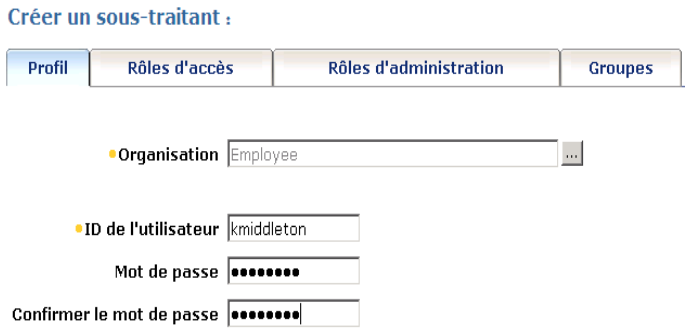
Contrôleurs d'onglets

Un contrôleur d'onglets détermine la manière dont les onglets d'une tâche sont affichés. Vous pouvez sélectionner l'un des contrôleurs d'onglets suivants :

- **Contrôleur d'onglets standard**

  Affiche les onglets de la tâche sous forme d'onglets indépendants. L'utilisateur peut utiliser les onglets de la tâche dans l'ordre de son choix.

  Il s'agit du contrôleur d'onglets par défaut.



- **Assistant de contrôleur d'onglets**

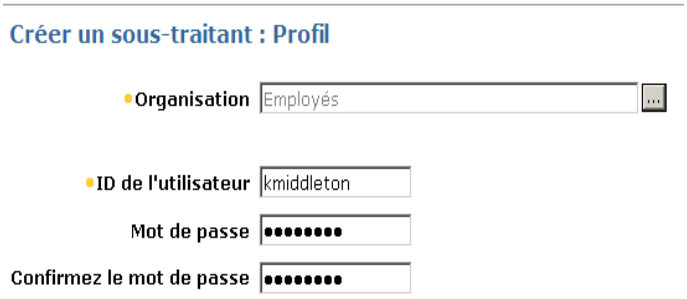
  Affiche les onglets de la tâche sous forme d'assistant. L'administrateur utilise chaque onglet dans l'ordre.

- **Contrôleur d'onglets de séquence**

  Affiche un onglet à la fois, sous la forme d'une page unique. L'utilisateur remplit un onglet, puis clique sur un bouton ou un lien personnalisé pour passer à l'onglet suivant.

  La séquence d'onglets et les boutons et les liens affichés sont déterminés par un script de programmation Java que vous écrivez lorsque vous configurez le contrôleur d'onglets de séquence.

  Dans le script Java personnalisé, vous pouvez spécifier l'apparence et l'ordre des onglets en fonction des entrées de l'utilisateur. Par exemple, si un utilisateur sélectionne une option dans le premier onglet, Identity Manager affiche une page. Si l'utilisateur sélectionne une autre option, une page différente s'affiche.



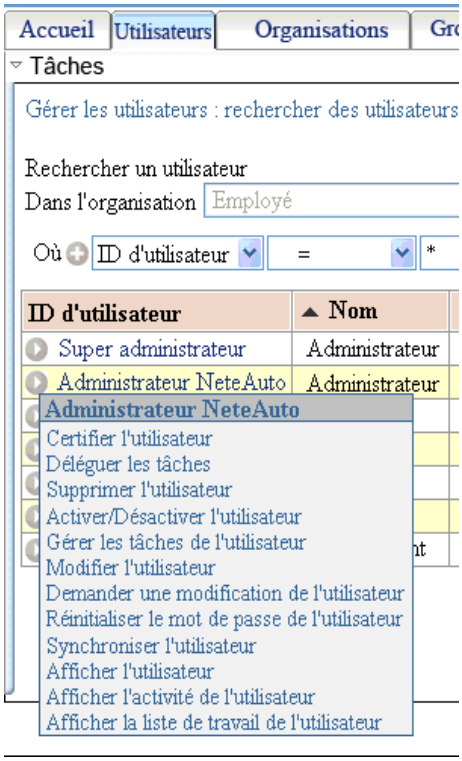
Listes des tâches

Identity Manager r12 comporte les nouvelles tâches par défaut ci-après, qui permettent de rechercher un objet à gérer.

- Gérer les utilisateurs
- Gérer les groupes
- Gérer les organisations
- Gérer les rôles d'administration
- Gérer les tâches d'administration
- Gérer les rôles d'accès
- Gérer les tâches d'accès

Une fois l'objet sélectionné, vous pouvez afficher une liste de tâches que vous pouvez utiliser pour gérer cet objet.

Par exemple, pour modifier un utilisateur selon cette méthode, sélectionnez la catégorie Utilisateurs, puis la tâche Gérer les utilisateurs. Recherchez et sélectionnez l'utilisateur que vous souhaitez gérer. Dans les résultats de recherche, cliquez sur une icône pour afficher la liste des tâches à utiliser pour gérer l'utilisateur sélectionné. Dans cette liste, vous pouvez sélectionner la tâche Modifier l'utilisateur ou une autre tâche appropriée.



Vous pouvez également configurer des listes de tâches dans des tâches autres que les tâches de gestion. Par exemple, vous pouvez ajouter une liste de tâches à un onglet Appartenance. Dans ce cas, une liste de tâches est disponible pour chaque membre figurant dans l'onglet Appartenance.

Améliorations de l'onglet Profil

Dans Identity Manager r12, l'onglet Profil comporte plusieurs nouveaux paramètres de configuration pour prendre en charge de nouvelles fonctionnalités. Ces nouveaux paramètres sont décrits dans les sections qui suivent.

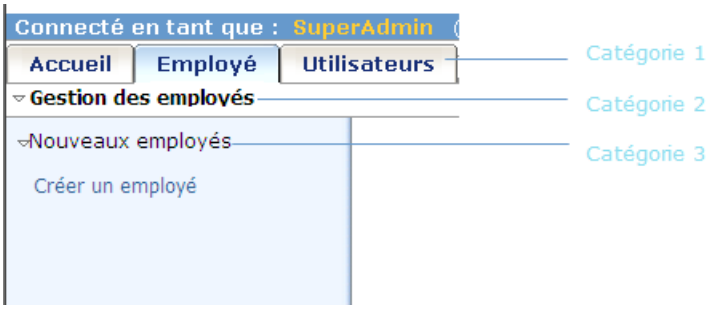
Catégories de tâches

Les catégories de tâches permettent d'organiser les tâches afin qu'elles soient plus faciles à rechercher et à localiser dans la console d'utilisateur.

Vous pouvez spécifier trois catégories de tâches :

- La catégorie 1 est la catégorie de niveau supérieur. Les catégories de niveau supérieur sont affichées sous forme d'onglets en travers de la partie supérieure de la console d'utilisateur.
- La catégorie 2 est la catégorie de second niveau. Cette catégorie permet de regrouper des tâches associées dans une catégorie de niveau supérieur. Si vous ne spécifiez pas de catégorie de second niveau, la catégorie par défaut est Tâches.
- La catégorie 3 comprend les tâches que les administrateurs utilisent. Lorsque les administrateurs cliquent sur le nom de la catégorie 3 dans la console d'utilisateur, une liste des tâches figurant dans cette catégorie s'affiche.

Dans chaque catégorie, vous pouvez déterminer l'ordre dans lequel les éléments de la catégorie s'affichent en spécifiant un ordre de catégorie. Par exemple, dans l'illustration suivante, l'onglet Employé comporte un ordre de catégorie de 3.



Remarque : Lorsqu'une catégorie comporte plusieurs tâches, l'ordre de catégorie spécifié dans le profil de chaque tâche doit être le même. S'il est différent, plusieurs instances de cet onglet de catégorie apparaissent. Par exemple, la catégorie Employé contient deux tâches : Créer un employé et Modifier un employé. Si l'ordre de catégorie de la tâche Créer un employé est 3 et celui de la tâche Modifier un employé 6, la catégorie Employé apparaît sous la forme de deux onglets.

Priorité des tâches

Dans Identity Manager r12, vous pouvez désormais indiquer une priorité des tâches, pour vous assurer qu'Identity Manager exécute d'abord les tâches les plus urgentes.

Vous pouvez définir la priorité des tâches sur Elevée, Moyenne ou Faible dans l'onglet Profil de la tâche. La priorité par défaut est Moyenne.

Remarque : Vous pouvez utiliser la tâche Afficher les tâches soumises pour rechercher des tâches présentant une priorité spécifique, puis en afficher l'état.

Données personnalisées pour sélectionner des boîtes

Les fenêtres de tâches Identity Manager incluent des champs qui permettent aux utilisateur de sélectionner une valeur. Ces tâches sont les suivantes :

- Case à cocher : sélection multiple
- Liste déroulante
- Liste modifiable déroulante
- Sélection multiple
- Sélecteur d'options
- Sélecteur modifiable d'options
- Sélection unique avec bouton d'options
- Sélection unique

Vous pouvez spécifiez des données personnalisées que vous souhaitez utiliser pour remplir des boîtes dans des fichiers XML. Par exemple, vous pouvez utiliser les fichiers XML de données de boîtes de sélection pour remplir des options dans une case déroulante de Ville ou d'Etat sur un onglet Profil pour la tâche Créer un utilisateur.

Vous pouvez aussi utiliser les fichiers XML de données de boîtes de sélection pour configurer une dépendance entre les deux champs dans une fenêtre de tâche. Par exemple, les options qui sont disponibles dans le champ Ville peuvent dépendre d'une option choisie par l'utilisateur dans le champ Etat.

Contrôle du sélecteur de dates

Désormais, la console d'utilisateur Identity Manager comporte un style Sélecteur de dates, qui peut être appliqué aux champs d'un onglet Profil qui recueillent et affichent des dates.

Lorsque le style Sélecteur de dates est appliqué, une icône de calendrier s'affiche en regard d'un champ de date. Les utilisateurs cliquent sur l'icône de calendrier pour afficher un contrôle de calendrier leur permettant de sélectionner la date souhaitée.

Contrôles Binaire et Image

Vous pouvez à présent configurer Identity Manager pour afficher une image dans un profil ou inclure un attribut binaire. Par exemple, vous pouvez configurer un écran de profil d'utilisateur, afin qu'il affiche une photographie numérique de l'utilisateur en cours de gestion, ou joindre un document à l'écran de profil.

Remarque : Prise en charge uniquement pour les magasins d'utilisateurs LDAP.

Attributs personnalisés définis par l'utilisateur pour les rôles

Identity Manager prend en charge les attributs personnalisés qui vous permettent de filtrer les rôles de votre organisation efficacement. Si vous devez par exemple créer plus de mille rôles dans l'environnement de votre entreprise. Vous pouvez classer ces rôles par unité commerciale ou par lieu géographique. Si vous souhaitez rechercher les rôles spécifiques à un lieu, vous pouvez utiliser les attributs personnalisés pour filtrer les rôles de votre organisation.

Vous pouvez utiliser les attributs personnalisés des onglets Créer, Modifier et Afficher les tâches pour les rôles suivants :

- Rôle d'accès
- Rôles d'administration

Vous devez effectuer les tâches suivantes pour ajouter les attributs personnalisés aux tâches d'administration et aux écrans de recherche.

1. Ajoutez les attributs personnalisés à l'une des tâches d'administration qui sont définies pour les rôles.
2. Configurez les écrans de recherche pour les rôles avec les attributs personnalisés.

Chargeur en bloc

Vous pouvez utiliser l'onglet Chargeur en bloc pour charger les fichiers du chargeur, utilisés pour manipuler simultanément de grands nombres d'objets gérés. Par exemple, vous pouvez créer 1 000 utilisateurs manuellement dans Identity Manager ou vous pouvez utiliser le chargeur en bloc. L'avantage de la méthode du chargeur en bloc est que vous pouvez automatiser le processus de manipulation d'un grand nombre d'objets gérés au moyen d'un fichier d'informations (chargeur). La tâche Chargeur en bloc peut également être mappée vers un processus de flux de travaux.

Remarque : Le format CSV est le format de fichier pris en charge pour le chargeur, mais vous pouvez créer un flux personnalisé pour d'autres formats de fichiers.

Recherche d'une organisation par défaut, en fonction de l'utilisateur

Pour simplifier la console d'utilisateur, Identity Manager permet à un administrateur de configurer une organisation par défaut pour la tâche Créer un utilisateur, en fonction de l'utilisateur tentant d'exécuter la tâche. Lorsqu'un utilisateur exécute une tâche Créer un utilisateur, l'organisation ne s'affiche pas dans l'onglet Créer un profil d'utilisateur, mais elle est définie par défaut en fonction de l'organisation de l'utilisateur.

Pour configurer une organisation par défaut en fonction d'un utilisateur :

1. Dans la console d'utilisateur Identity Manager, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
2. Sélectionnez la tâche Créer un utilisateur.
3. Dans l'onglet Onglets, cliquez sur l'icône flèche droite en regard de Profil.
4. Cliquez sur le bouton ... (points de suspension) pour afficher une liste de fenêtres à modifier.
5. Sélectionnez la fenêtre Créer un profil d'utilisateur et cliquez sur Modifier.
6. Recherchez l'organisation souhaitée et cliquez sur l'icône flèche droite pour la modifier.

   Remarque : Ce champ n'est pas présent dans un environnement dépourvu d'organisations.
7. Définissez Style sur Masqué.

8. Dans le champ Script Java par défaut, entrez les éléments ci-après.

```
function defaultValue(blthContext)
{
return blthContext.getAdministrator().getOrg(null).getUniqueName();
}
```

9. Cliquez sur Appliquer.

Prise en charge de IPv6

Lors de la configuration d'Identity Manager, vous pouvez saisir les deux adresses, IPv4 et IPv6.

Identity Manager prend en charge IPv6 sur les systèmes d'exploitation suivants :

- Solaris 8 ou supérieur ;
- Windows XP SP1 ou supérieur ;
- Windows 2003 ou supérieur.

Chaque serveur d'applications possède une configuration JDK (Java Development Kit) spécifique requise :

- Pour un serveur d'applications JBoss exécuté sur un système autonome, Identity Manager prend en charge IPv6 avec le JDK1.4.2_13 ou 1.5 (sous Solaris) ou le JDK1.5 (sous Windows).
- Pour un cluster JBoss, aucun JDK ne prend en charge IPv6 lancé en même temps que Identity Manager r12. Si un JDK prenant en charge IPv6 est lancé, la matrice de support pour plates-formes sera mise à jour.
- Toutefois, pour un cluster JBoss utilisant une pile IPv4/IPv6, Identity Manager prend en charge IPv6 avec le JDK1.4.2_13 ou 1.5 (sous Solaris) ou le JDK1.5 (sous Windows).
- Les serveurs d'applications WebLogic et WebSphere comprennent le JDK1.5 qui prend en charge les adresses IPv6.

Avant de configurer un environnement qui prend en charge IPv6 :

- Pour que les adresses IPv6 soient prises en charge sous Identity Manager, tous les composants d'Identity Manager, notamment le système d'exploitation, le JDK, les serveurs d'annuaires et les bases de données doivent également prendre en charge les adresses IPv6.
- Si Identity Manager comprend SiteMinder, le plug-in de serveur Web pour le serveur d'applications doit également prendre en charge IPv6.

- Lorsque vous vous connectez à SiteMinder ou à une base de données depuis Identity Manager via une connexion JDBC, spécifiez le nom d'hôte au lieu de l'adresse IP.
- Le serveur de rapports IAM peut être installé sur un hôte à double pile qui prend en charge IPv4 et IPv6, mais la connexion au serveur doit se faire via IPv4.

  Lorsque vous configurez une connexion au serveur de rapports dans la console de gestion, le nom de serveur doit être au format IPV4.

FIPS 140-2

Identity Manager r12 prend en charge FIPS 140-2 pour une nouvelle installation *uniquement*. Identity Manager comprend également un outil de modification de mot de passe fournissant une clé de chiffrement FIPS qui se trouve dans le répertoire suivant :

```
C:\Program Files\CA\IAM Suite\Identity Manager\tools\PasswordTool
```

Lors de l'activation de FIPS 140-2 pour un environnement Identity Manager :

- Une fois que la prise en charge de FIPS 140-2 a été activée pour un déploiement Identity Manager, vous ne pouvez plus la désactiver. De même, si vous installez Identity Manager sans avoir activé la prise en charge de FIPS 140-2, vous ne pouvez plus l'activer ultérieurement.
- Si vous souhaitez activer FIPS 140-2 pour un déploiement Identity Manager qui comprend SiteMinder, vous devez utiliser la version r12 de SiteMinder.

Prise en charge de la localisation améliorée

La console d'utilisateur Identity Manager et son aide en ligne sont disponibles dans les langues suivantes :

- Français
- Coréen
- Japonais
- Allemand

- Chinois (simplifié)
- Espagnol
- Italien

Remarque : Pour plus d'informations sur l'utilisation de Identity Manager dans l'une des langues mentionnées, reportez-vous au *Manuel de configuration*.

Informations complémentaires :

Installation d'environnements Identity Manager localisés (page 41)

Chapitre 3 : Modifications apportées aux fonctionnalités existantes

Ce chapitre traite des sujets suivants :

Agent de filtre de servlet déconseillé

L'agent de filtre de servlet est déconseillé dans Identity Manager r12. Nous recommandons d'utiliser un agent Web à la place d'un agent de filtre de servlet. Si un agent de filtre de servlet est déjà déployé dans un environnement Identity Manager *existant*, il fonctionne toujours et il est pris en charge.

Améliorations de la console de gestion

La console de gestion Identity Manager comporte les nouvelles fenêtres ou les fenêtres modifiées indiquées ci-après.

- Page Console d'utilisateur : utilisez cette page pour configurer les paramètres généraux d'une console d'utilisateur Identity Manager, y compris l'icône et le titre, ainsi que la classe d'authentification et la page de déconnexion.

  Remarque : Dans Identity Manager, vous configuriez les paramètres d'icône et de titre dans la page Thèmes. Les fonctionnalités de la page Thèmes ont été déplacées dans la page Console d'utilisateur et la page Thèmes a été supprimée.

- Page Environnements : vous pouvez désormais arrêter et démarrer un environnement Identity Manager à partir de la page Environnements. Vous n'avez plus besoin de redémarrer le serveur d'applications pour que les modifications apportées à l'environnement prennent effet.

- Page Provisionnement : cette page ne contient plus la configuration de la synchronisation entrante. Pour configurer la synchronisation entrante, reportez-vous au *Manuel du provisionnement*.
- Page Persistance des tâches : désormais, la persistance des tâches est configurée automatiquement lors de l'installation. Vous n'avez plus besoin de l'activer manuellement. Cette page a été supprimée.

Modifications des stratégies de mot de passe

Comme les nouvelles installations d'Identity Manager r12 ne nécessitent plus SiteMinder, certaines modifications ont été apportées à la fonctionnalité Stratégie de mot de passe par défaut. Dans les déploiements sans intégration à SiteMinder, Identity Manager permet de créer des stratégies de mot de passe de base pour gérer les mots de passe en appliquant des règles et des restrictions régissant l'expiration, la composition et l'utilisation des mots de passe.

Si vous configurez l'intégration d'Identity Manager à SiteMinder, vous pouvez créer des stratégies de mot de passe avancées qui permettent de définir les règles et restrictions supplémentaires ci-après.

- Filtres de répertoires
- Expiration du mot de passe :
  - Echec de connexion ou connexions réussies
  - Authentification à la connexion
  - Expiration du mot de passe s'il n'est pas modifié
  - Inactivité du mot de passe
  - Mot de passe incorrect
- Plusieurs expressions régulières
- Restrictions de mot de passe :
  - Nombre minimum de jours avant la réutilisation
  - Nombre minimum de mots de passe avant la réutilisation
  - Pourcentage différent du dernier mot de passe
  - Ignorer la séquence lors de la vérification des différences
  - Concordance des attributs de profil
  - Concordance du dictionnaire

Outil imrexport déconseillé

La fonctionnalité de l'outil imrexport a été intégrée à la console d'utilisateur Identity Manager. La tâche Données de clichés de capture, dans l'onglet Rapports, exécute désormais la fonctionnalité de l'outil imrexport dans Identity Manager r12.

Connecteurs z/OS de changement d'architecture

L'architecture des connecteurs z/OS (CA ACF2, CA Top Secret et RACF) a été refaite pour des raisons de performances et utilise à présent le serveur CA LDAP pour z/OS plutôt que le serveur CA DSI sur z/OS.

Toute option de fichier de configuration d'un serveur de provisionnement liée à un serveur CA LDAP est désormais entrée et stockée sur z/OS lorsque le serveur CA LDAP est installé. L'information de connexion du serveur mainframe LDAP est également désormais directement entrée dans la vue des tâches du terminal gestionnaire de provisionnement.

Fonctionnalités non prises en charge

Certaines fonctionnalités eTrust Admin ne sont plus disponibles dans Identity Manager r12. Le tableau suivant dresse la liste des nouvelles fonctionnalités à utiliser dans Identity Manager r12.

Fonctionnalité eTrust Admin	Fonctionnalité Identity Manager
Flux de travail avancé	Flux de travaux WorkPoint
Flux de travail hérité	Flux de travaux WorkPoint
Interface Web d'auto-administration	Auto-administration Identity Manager
Interface Web d'administration déléguée	Administration déléguée Identity Manager
IA Manager	Tâches d'auto-administration et d'administration déléguée Identity Manager
Génération de rapports eTrust Admin etaReport	Création de rapports Identity Manager
Ooption PeopleSoft Feed	Chargeur en bloc
Option Universal Feed	Chargeur en bloc
Option SAP (version C++)	Connecteur SAP (version Java)
Option MS SQL (version C++)	Connecteur MS SQL (version Java)

Fonctionnalité eTrust Admin	Fonctionnalité Identity Manager
Option Oracle (version C++)	Connecteur Oracle (version Java)
Option OS/400	Connecteur OS/400 (version Java)
Option CleverPath Portal	Aucun remplacement

Remarque : Les versions existantes (disponibles avec eTrust Admin 8.1 SP2) des options PeopleSoft Feed et Universal Feed continueront de fonctionner avec Identity Manager r12.

Chapitre 4 : Configuration système requise

La configuration matérielle minimale ci-après est nécessaire pour le système qui héberge le serveur Identity Manager.

- Processeur : processeur simple ou double, Intel Pentium III (ou compatible) 700 à 900 MHz ou poste de travail Sparc 440 MHz
- Mémoire : 2 Go
- Espace disque disponible : 1 Go

Remarque : Cette configuration matérielle minimale tient compte de la configuration minimale du serveur d'applications qui doit être installé sur le système où est installé le serveur Identity Manager.

Chapitre 5 : Remarques relatives à l'installation

Ce chapitre traite des sujets suivants :

Emplacement de la matrice de support

Pour obtenir la liste complète des logiciels pris en charge, reportez-vous à la matrice de support d'Identity Manager.

Pour accéder à la matrice de support :

1. Connectez-vous à support.ca.com.
2. Cliquez sur Support By Product or Solution (Support par produit et solution).
3. Sélectionnez CA Identity Manager dans la section Products (Produits) sur la page Select a Product or Solution (Sélectionner un produit ou une solution).

   La page CA Identity Manager s'ouvre.
4. Faites défiler jusqu'à Recommend Readings (Lectures recommandées).
5. Cliquez sur CA Identity Manager Informational Documentation Index (Index des documentations sur CA Identity Manager).

Des matrices de support pour plates-formes s'affichent sur une page pour les versions d'Identity Manager prises en charge.

Patches requis pour Solaris

Avant d'installer le provisionnement sur Solaris 9 ou 10, téléchargez et installez les patches suivants :

Pour télécharger les patches Sun Studio 10 patches pour le SDK :

1. Cliquez sur l'URL suivante :
   http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html
2. Téléchargez et installez le patch 117830.

   Remarque : Sun Studio 11 n'a pas besoin de patches.

Pour télécharger les patches Solaris 9 pour tous les composants :

1. Cliquez sur l'URL suivante :

   http://search.sun.com/search/onesearch/index.jsp
2. Téléchargez et installez 9_recommended.zip

Variable d'environnement pour intégration de SiteMinder

Lorsque vous installez Identity Manager sur un système Solaris et activez l'intégration via SiteMinder, l'erreur suivante peut s'afficher dans le journal du serveur d'applications et le démarrage d'Identity Manager peut échouer :

erreur "java: fatal: libetpki2,so : échec d'ouverture : Fichier ou répertoire inexistant"

Cette erreur se produit si l'installation ETPKI qui installe une bibliothèque de chiffrement requise par SiteMinder, n'ajoute pas la variable d'environnement CALIB correctement.

Remarque : Le programme d'installation Identity Manager installe ETPKI automatiquement.

Solution

Avant de démarrer le serveur Identity Manager, ajoutez la variable d'environnement CALIB comme indiqué ci-après :

```
bash# export CALIB=/opt/CA/SharedComponents/ETPKI/lib
```

Installation d'environnements Identity Manager localisés

Identity Manager comprend les versions traduites de la console d'utilisateur Identity Manager et de l'aide en ligne correspondante. La plupart des fichiers qui doivent utiliser une version traduite se trouvent à l'emplacement suivant :

im_admin_tools_dir\samples\Localization*language*

im_admin_tools_dir

Indique l'emplacement d'installation des outils d'administration d'Identity Manager.

language

Indique la langue que vous souhaitez utiliser.

Remarque : Pour les instructions d'installation, reportez-vous au *Manuel de configuration*.

Toutefois, des fichiers supplémentaires sont requis pour l'utilisation d'une version traduite de Identity Manager :

- Notes de parution
- Fichiers d'aide en ligne

  Remarque : Veillez à ne pas utiliser les fichiers d'aide en ligne qui sont disponibles sous *im_admin_tools_dir*\samples\Localization*language.*

Ces fichiers peuvent être téléchargés depuis CA Identity Manager r12 Localization Resources (Ressources localisées de CA Identity Manager r12) sur le site d'assistance de CA.

Pour installer les fichiers d'aide en ligne :

1. Téléchargez le fichier ZIP CA Identity Manager r12 Localization Resources.
2. Dézippez les fichiers sur un système accessible depuis le serveur d'applications qui héberge Identity Manager.
3. Copiez le fichier im_help_*language*.ZIP pour la langue correspondante vers *IdentityMinder.ear*\user_console.war\

   IdentityMinder.ear

   Emplacement de déploiement de l'application Identity Manager (IdentityManager.ear) sur le serveur d'applications.

   Remarque : Pensez à créer une copie de sauvegarde des fichiers d'aide en ligne d'origine avant de les remplacer par la version traduite. L'aide en ligne par défaut est remplacée par la version traduite.

4. Dézippez le répertoire im_help.zip in the user_console.war.
5. Redémarrez l'environnement Identity Manager.

   La version traduite de l'aide en ligne est disponible pour utilisation.

Les caractères non-ASCII provoquent des échecs lors de l'installation sur des systèmes non anglophones.

Pendant l'installation 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

À cause des caractères non-ASCII le programme d'installation affiche une page blanche de résumé de pré-installation puis l'installation échoue.

Pour éviter que l'installation n'échoue :

Changez la variable de l'environnement tmp afin que celle-ci renvoie à un dossier ne contenant que des caractères ASCII.

Modifications de configuration requises pour SiteMinder en mode FIPS 140-2 uniquement

Si SiteMinder est en mode FIPS 140-2 uniquement, vous devez effectuer des tâches de configuration supplémentaires.

Pour configurer Identity Manager afin qu'il fonctionne avec SiteMinder en mode FIPS 140-2 uniquement sur WebLogic ou JBoss :

1. Ouvrez *IdentityMinder.ear*\policyserver.rar\META-INF\ra.xml.
2. Recherchez l'élément suivant :

```
<config-property>
<config-property-name>FIPSMode</config-property-name>
<config-property-type>java.lang.String</config-property-type>
<config-property-value>false</config-property-value>
<config-property>
```

3. Modifiez Faux sur Vrai dans l'élément <config-property-value>.
4. Redémarrez le serveur d'applications.

Pour configurer Identity Manager afin qu'il fonctionne avec SiteMinder en mode FIPS 140-2 uniquement sur WebSphere :

1. Ouvrez la console d'administration WebSphere.
2. Allez à l'emplacement suivant :

   Enterprise Applications > IdentityMinder > Manage Modules > policyserver.rar > IdentityMinder.PolicyServerRA > J2C connection factories > PolicyServerConnection > Custom properties
3. Cliquez sur la valeur FIPSMode, puis modifiez la valeur sur Vrai. Cliquez sur OK, puis sur le lien Enregistrer en haut de la page.

JBoss : Configuration du support IPv6

Si vous installez la version JBoss de Identity Manager sur un système prenant en charge IPv6, une configuration minimale est requise.

Pour configurer IPv6 sur un serveur d'application JBoss

1. Ouvrez le fichier run_idm.sh qui se trouve dans :

   jboss_installation\bin
2. Modifiez *une* des propriétés suivantes dans l'entrée JAVA_OPTS :
   - Pour les environnements IPv6 uniquement, supprimez les commentaires de l'entrée suivante :

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv6Addresses=true
   - Pour les environnements IPv6/IPv4, supprimez les commentaires de l'entrée suivante :

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv6Addresses=true
3. Enregistrez le fichier.

Prise en charge SPML pour FIPS 140-2

Pour Identity Manager r12, le serveur SPML est compatible avec FIPS 140-2. Nous recommandons de déployer le service SPML sur :

- Apache Tomcat Server 4.1.36 ou version supérieure ;
- JDK 1.5.11 ou version supérieure. Tomcat doit être activé pour l'exécution en mode SSL. Pour plus d'informations, reportez-vous au manuel Apache's administrator guide for Tomcat 4, (http://jakarta.apache.org/tomcat/) section "SSL Configuration HOW-TO".

Si vous utilisez CA Tomcat au lieu de Apache Tomcat, Identity Manager r12 requiert les solutions suivantes pour SPML :

- Si vous utilisez JDK 1.4.xx avec CA Tomcat, FIPS 140-2 doit être désactivé. JDK 1.4.xx est compatible avec CA Tomcat car la bibliothèque RSA Jsafe CryptoJ 4.0 requise pour la prise en charge FIPS 140-2 ne peut pas être définie en tant que fournisseur de sécurité principal dans JDK1.4.

  Pour désactiver la prise en charge FIPS 140-2, ignorez l'indicateur JVM "-Dcom.ca.commons.security.fips=false" lors du démarrage de Tomcat.

  - Si vous exécutez Tomcat à partir de la ligne de commande, vous pouvez inclure l'indicateur JVM catalina.bat. Plus d'informations sont disponibles dans le fichier de traitement par lots.
  - Si vous exécutez Tomcat en tant que service Windows, ignorez l'indicateur comme suit :

    a. Via l'éditeur du registre, accédez à "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CA Tomcat 4.1.29 eTrustIAMWebServer\Parameters"

    b. Ajoutez une valeur chaîne "JVM Option Number n", "'n" étant le numéro provenant du paramètre JVM précédent. Spécifiez pour la valeur :

    Dcom.ca.commons.security.fips=false

    c. Augmentez d'une unité la valeur de Modifier la valeur DWORD "JVM Option Count" pour le paramètre récemment ajouté.

- Si vous utilisez JDK 1.5 avec CA Tomcat, un problème d'incompatibilité peut survenir. Pour résoudre ce problème :

  a. Supprimez manuellement les deux bibliothèques Xerces (xercesImpl.jar et xmlParserAPIs.jar) de %TOMCATHOME%\common\endorsed.

  b. Redémarrez Tomcat.

Connecteurs z/OS de changement d'architecture

L'architecture des connecteurs z/OS (CA ACF2, CA Top Secret et RACF) a été refaite pour des raisons de performances et utilise à présent le serveur CA LDAP pour z/OS plutôt que le serveur CA DSI sur z/OS.

Avant d'essayer de configurer un connecteur z/OS vous devez installer le serveur CA LDAP pour z/OS r12 qui peut être téléchargé sur support.ca.com.

Emplacement d'eTrust Directory

Le schéma de l'annuaire de provisionnement est installé dans eTrust Directory. Vous pouvez installer eTrust Directory à partir du média d'installation Identity Manager.

Réparation requise avant de désinstaller eTrust Directory

Si vous devez désinstaller eTrust Directory du système Windows, vous devez appliquer un patch avant de commencer la procédure de désinstallation.

Si vous n'appliquez pas le patch, la procédure de désinstallation peut supprimer les fichiers licence requis par d'autres produits CA.

Vous pouvez télécharger le patch sur le site du support CA.

Trouver l'emplacement du patch

1. Connectez-vous sur support.ca.com.

   Le site du support CA s'affiche.

2. Cliquez sur Licence dans la liste des liens à gauche de la page.

3. Cliquez sur package Licence 1.8 est désormais disponible.

   Une page s'ouvre décrivant les changements du package licence et comprenant un lien pour le téléchargement.

4. Suivez les instructions pour le téléchargement et installez le patch Windows.

Chapitre 6 : Problèmes connus

Ce chapitre traite des sujets suivants :

Général

Les problèmes connus dans Identity Manager r12 sont décrits ci-après.

Identity Manager EAR ne se déploie pas automatiquement avec WebLogic

Si vous utilisez WebLogic 8 ou 9 en mode production, Identity Manager EAR ne se déploiera pas automatiquement lors du premier démarrage du serveur d'application après une installation ou une mise à niveau. Si ceci venait à se produire, déployez IdentityMinder.ear manuellement à partir du dossier user_projects\applications.

Flux de travaux et membres du groupe en tant qu'approbateurs.

Si un processus de flux de travaux est configuré dans Workpoint Designer pour avoir des membres d'un groupe spécifique en tant qu'approbateurs, un élément du flux de travaux ne sera peut-être pas créé pour l'événement sous un contrôle de flux et la session de la tâche risque d'échouer.

La solution est de placer la tâche sous contrôle de flux de travaux à l'aide d'une méthode de modèle (avec les modèles SingleStepApproval ou TwoStageApprovalProcess) et des membres de groupe définis en tant qu'approbateurs (ou des outils de résolution de participants).

De nouvelles propriétés Workpoint doivent être définies

Identity Manager comprend une nouvelle version de Workpoint. Dans cette version, vous pouvez configurer de nouvelles propriétés supplémentaires dans GeneralMonitor.properties et workpoint-server.properties. Veuillez noter que ces nouvelles propriétés sont optionnelles et qu'elles ne doivent être ajoutées que si nécessaire.

Les nouvelles propriétés du flux de travaux sont les suivantes :

- Dans le fichier GeneralMonitor.properties :
  - #JMX_HTML_ADAPTOR_PORT=9092

    Cette propriété a été commentée par défaut. La propriété, lorsqu'elle est définie comme vraie, permet une page HTML qui utilise l'adaptateur générique Sun JMX qui est un port Web non sécurisé séparé de l'application de la console de gestion Workpoint. Nous recommandons aux clients de laisser cette propriété commentée ou de la définir comme fausse et d'utiliser plutôt la console de gestion Workpoint pour l'accès JMX à Workpoint.
  - JOB_ERROR_STATE_ON_MAIL_ERROR=false

    Cette propriété n'est applicable que pour les clients qui utilisent la fonctionnalité courriel de Workpoint. Cette propriété contrôle la gestion des erreurs dans la surveillance des courriels. Si les clients Identity Manager utilisent la fonction courriel de Workpoint, cette propriété est disponible.

    Remarque : JOB_ERROR_STATE_ON_MAIL_ERROR défini comme vrai par défaut. Vous souhaiterez peut-être le définir comme faux si vous utilisez le courriel de flux de travaux et que vous ne souhaitez pas que des erreurs de courriel affectent l'état de votre travail..
  - ENABLE_SCRIPT_TASK_GROUPING=false

    Cette propriété contrôle si la surveillance de script peut regrouper tous les scripts concurrents exécutant le même travail. Si vrai, ceci provoquera l'assignation de tous les scripts pour un travail particulier à la même thread du travailleur où elles seront exécutées une par une. Il est utile de prévenir les exceptions de concurrence lorsque vous avez de multiples activités dans un travail utilisant un script asynchrone par automatisme et pouvant être actives en même temps.

    Si vous avez personnalisé les scripts de flux d travaux et faites l'expérience des exceptions de concurrence, examinez cette propriété.

    Les courriels supplémentaires et les relations liées sont contenus dans le fichier GeneralMonitor.properties.
- Dans le fichier workpoint-server.properties :
  - server.automated.delay=500

    Cette propriété contrôle les nœuds des serveurs automatisés pour garantir que ces nœuds ne sont pas mis dans la file d'attente avant la transaction avec la base de données qui les met dans la file d'attente et leur donne la chance de persister. Ceci empêche les échecs des nœuds du serveur automatisé à cause de problèmes de temps. Cette propriété est recommandée lorsque les nœuds du serveur automatisé sont utilisés.

Impossible de créer une copie de gestionnaire d'attributs logiques

Lorsque vous essayez de créer une copie de gestionnaire d'attributs logiques dans la console d'utilisateur, l'erreur suivante s'affiche :

"Cet objet n'est pas connecté"

La création d'un nouveau gestionnaire d'attributs logiques, qui n'est pas basée sur un gestionnaire d'attributs logiques existant, fonctionne correctement.

Utiliser Filtres groupe dans les stratégies de rôle

Lorsque Identity Manager gère une banque utilisateur dans une base de données relationnelles, les filtres groupe de membre et stratégies d'administration risquent de ne pas fonctionner correctement. Par exemple, si vous utilisez un filtre tel que « Utilisateurs membres d'un groupe dont le nom commence par un A » dans une stratégie de membre, Identity Manager risque d'appliquer la stratégie à tous les utilisateurs plutôt qu'aux utilisateurs faisant partie d'un groupe dont le nom commence par la lettre A.

Pour éviter ce problème, assurez-vous que les tableaux, tblGroupMembers et tblGroupAdministrators, sont définis pour l'objet de l'utilisateur dans le fichier de configuration du répertoire (directory.xml).

La définition de l'objet de l'utilisateur dans directory.xml doit ressembler à cela :

```
<ImsManagedObject name="User" description="My Users" objecttype="USER">
<!-- COMMENT Table -->
    <Table name="tblUsers" primary="true" />
    <Table name="tblUserAddress">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserRoles">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserDelegators">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserPasswordhints">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserIdentityPolicy">
    <Reference childcol="userid" primarycol="id"/>
    </Table>
```

```
<Table name="tblOrganizations">
<Reference childcol="id" primarycol="org"/>
</Table>

<Table name="tblGroupMemebers">
<Reference childcol="userid" primarycol="id"/>
</Table>

<Table name="tblGroupAdmins">
<Reference childcol="userid" primarycol="id"/>
</Table>
```

Après avoir modifié le fichier de configuration du répertoire, importez-le à l'aide de la console de gestion.

Remarque : Pour plus d'informations concernant la modification des fichiers de configuration, reportez-vous au *Guide de configuration*.

Configurer les rôles et les fenêtres de recherche de tâches

Lorsque vous configurez les fenêtres de recherche de rôles ou de tâches, vous pouvez limiter les rôles et tâches qui sont retournés par la recherche à l'aide de l'option « Afficher uniquement les rôles d'administration correspondant aux règles suivantes ». Les attributs utilisés lorsque vous configurez cette option ne doivent pas être ajoutés comme des champs de recherche disponibles sur l'écran de recherche.

Par exemple, si vous configurez l'écran de recherche pour n'afficher que les rôles lorsque l'attribut activé est Oui, supprimez l'attribut activé de la liste des attributs que les utilisateurs peuvent spécifier comme critère de recherche.

Sinon, le critère entré par l'utilisateur est ignoré.

Création d'un environnement Identity Manager dans le navigateur Firefox

Si vous accédez à la console de gestion via un navigateur Firefox, la création d'un environnement Identity Manager peut être ralentie et même bloquée. Dans ce cas, la création de l'environnement continue, mais le navigateur n'est pas actualisé ce qui vous empêche de voir si la création est terminée.

Remarque : Si vous fermez la fenêtre du navigateur, Identity Manager poursuit la création de l'environnement.

Mises à niveau

Les problèmes suivants se rapportent aux mises à niveau dans Identity Manager r12.

Les terminaux MS SQL et Oracle indisponibles après une mise à niveau à partir d'eTrust Admin 8.1 SP2

Après une mise à niveau à partir d'eTrust Admin 8.1 SP2 vers Identity Manager r12, tout terminal MS SQL ou Oracle acheté avant la mise à niveau nécessite une reconfiguration manuelle pour utiliser les URL JDBC plutôt que le nom de la source de données. Ceci est dû au passage du SuperAgent au Java CS pour la gestion des terminaux MS SQL et Oracle.

Oracle : Modifiez les détails de la feuille des propriétés du terminal Oracle.

Exemple :

```
jdbc:oracle:thin:@oracle_server_host:1521:ORACLE
```

MS SQL : Cliquez avec le bouton droit de la souris sur le terminal et sélectionnez Personnaliser, Changer le mot de passe Admin. Les informations d'identification de l'URL et de la connexion peuvent être modifiées à ce stade sans avoir besoin du détail des autres terminaux.

Exemple :

```
jdbc:sqlserver://serverHost:1433;instanceName=instance1
```

Remarque : Les étapes de la migration et un e liste exhaustive des syntaxes URL possibles peuvent être trouvées au « Chapitre 4 : Connecteurs de base de données » du *Guide des connecteurs*.

L'agent distant UNIX n'est pas disponible pour la plate-forme Solaris x86 (Intel)

Le package d'agent distant Unix ne contient pas les fichiers requis pour l'exécution de l'installation ou la mise à niveau de l'agent distant UNIX sur la plate-forme Solaris x86 (Intel).

Connecteurs Z/OS de changement d'architecture

L'architecture des connecteurs z/OS (CA ACF2, CA Top Secret et RACF) a été refaite pour des raisons de performances et utilise à présent le serveur CA LDAP pour z/OS plutôt que le serveur CA DSI sur z/OS.

Avant d'essayer de configurer un connecteur z/OS vous devez installer le serveur CA LDAP pour z/OS r12 qui peut être téléchargé sur support.ca.com.

Une fois que vous avez effectué la mise à niveau vers Identity Manager r12, réalisez les étapes suivantes pour chaque terminal défini pour votre système :

À partir de la vue des tâches du terminal

1. Sélectionnez le terminal CA ACF2, CA Top Secret ou RACF dans Type d'objet
2. Cliquez sur le bouton Rechercher. Cliquez avec le bouton droit de la souris sur le terminal et sélectionnez Propriétés. Renseignez les champs suivants :

   Dans la section Information du serveur mainframe :

   - **Adresse IP/Nom de la machine** spécifie l'adresse IP du système géré par RACF sur lequel le serveur CA LDAP est configuré et fonctionne.
   - **Port LDAP** spécifie le numéro du port que vous avez indiqué pendant l'installation du serveur CA LDAP pour z/OS. Si vous n'êtes pas sûr du port mainframe LDAP, reportez-vous à la section « Vérifier votre serveur CA LDAP pour les informations de configuration z/OS ».
   - **Suffixe LDAP** spécifie le suffixe à utiliser pour ce terminal. Cette zone de liste modifiable est automatiquement remplie avec tous les suffixes valides et disponibles lorsque vous cliquez sur le bouton « Obtenir des suffixes ». Les suffixes peuvent être retrouvés une fois que les valeurs valides ont été renseignées pour les champs adresse IP/nom de la machine et ports mainframe LDAP.

Génération de rapports

Les problèmes suivants se rapportent à la génération de rapports dans Identity Manager r12.

Limitation de la génération de rapports

Plusieurs clichés associés avec une seule tâche de rapport ne doivent pas utiliser le même intervalle récurrent.

Satisfy=All ne fonctionne pas correctement dans le fichier XML

Dans un fichier XML de paramètres de cliché, satisfy=all et satisfy=any se comportent tous les deux de la même façon que satisfy=any (similaire à l'opérateur OR).

Activer les cookies pour la tâche Afficher mes rapports

Afin d'afficher les rapports dans Identity Manager en utilisant la tâche Afficher mes rapports, activez les cookies d'une session tierce dans le navigateur.

ExportALL.xml et les environnements sans organisation d'assistance

En utilisant le fichier de paramètres XML Snapshot (par exemple : ExportAll.xml) qui exporte des objets et des attributs de l'organisation, une exception se produit lorsque l'environnement n'a aucun soutient pour les organisations. Pour résoudre ce problème, commenter les objets et attributs de l'organisation dans le fichier ExportAll.xml.

Provisionnement

Les abréviations des composants du provisionnement pour la liste des problèmes suivants sont définies comme suit :

- ACC : connecteur de contrôle CA Access
- ADS : connecteur Active Directory Services
- DBZ : base de données universelle DB2 pour connecteur z/OS
- DYN : connecteur dynamique
- E2K : connecteur Exchange 2000
- EEM : connecteur Entitlements Manager intégré
- ETC : ETC UNIX
- FND : connecteur d'applications Oracle
- INS : installation
- KRB : connecteur Kerberos
- LND : connecteur Lotus Notes/Domino
- NDS : connecteur Novell Directory Services
- N16 : agent distant Windows NT
- AS4 : connecteur OS/400

- PKI : connecteur Entrust PKI
- PLS : connecteur pour stratégie serveur avancée CA SSO
- PSA : agent sync mot de passe
- RSA : connecteur RSA SecurID
- SAP : connecteur SAP
- SBL : connecteur Siebel
- UPO : connecteur de provisionnement universel
- VMS : connecteur OpenVMS
- z/OS : connecteurs CA ACF2, CA Top Secret, RACF

Général

Les problèmes suivants concernent le provisionnement dans Identity Manager r12.

Synchronisation des comptes pour la tâche Réinitialiser le mot de passe de l'utilisateur

Pour activer le provisionnement pour un environnement Identity Manager, vous devez importer le fichier de configuration ProvisioningOnly-RoleDefinitions.xml, qui permet de créer les rôles et les tâches pour le provisionnement de l'utilisateur.

Dans ce fichier, le paramètre de synchronisation des comptes par défaut est défini sur Désactivé pour la tâche Réinitialiser le mot de passe de l'utilisateur. Avant d'activer le provisionnement, le paramètre de provisionnement est défini sur A la fin de la tâche.

Pour lancer la tâche Réinitialiser le mot de passe de l'utilisateur en vue de déclencher la synchronisation des comptes, définissez l'option de synchronisation après avoir importé le fichier ProvisioningOnly-RoleDefinitions.xml pour activer le provisionnement.

La console des utilisateurs ne peuvent pas explorer et corréler certains types de terminaux

Les tâches Explorer et Corréler dans la console utilisateur ne trouvent pas les types de terminaux suivants :

- Kerberos
- UNIX NIS
- Entrust PKI

- Siebel
- Base de données universelle pour z/OS
- Types de terminaux développés personnalisés

Pour explorer et corréler ces types de terminaux vous pouvez utiliser les gestionnaires de provisionnement. Puis vous pouvez réaliser des fonctions de compte de routine dans la console utilisateur telles que les assignations pour l'un de ses terminaux.

Exploration et corrélation fonctionne dans le même fuseau horaire

Dans la console d'utilisateur, vous pouvez planifier une définition Exploration et corrélation. Pour cette opération le navigateur client doit être défini dans le même fuseau horaire que le serveur. Par exemple, si l'heure du client est 22:00 le mardi, alors que l'heure du serveur est 07:00, la définition Exploration et corrélation ne fonctionnera pas.

Serveur de provisionnement Core Dump sur Solaris

Le serveur de provisionnement sur Solaris produira un fichier core lors de l'arrêt du service.

Ceci n'affecte aucune fonctionnalité et peut être ignoré sans problème.

Le provisionnement du programme d'installation Directory requiert un nom d'hôte correctement résolu.

Le programme d'installation requiert un nom d'hôte avec une résolution de nom correctement configurée lors de l'installation de l'annuaire de provisionnement et du serveur de provisionnement sur la même machine. L'installation du serveur de provisionnement échouera ou conduira à des résultats non prévus si la machine ne peut pas résoudre son propre nom de machine dans l'adresse IP prévue. Deux scénarios sont possibles :

- Vous avez un résultat de nom de résolution différent pour FQDN et le nom d'hôte. (Par exemple, sur un réseau IPv4/6, vous enregistrez une adresse IPv6 dans DNS mais vous avez une adresse IPv4 pour le nom d'hôte dans le bios net ou le fichier d'hôte). Si vous configurez l'annuaire de provisionnement pour écouter IPV6 uniquement puis que vous installez le serveur de provisionnement à l'aide de FQDN, l'installation échouera car le programme d'installation essaye de résoudre le nom d'hôte plutôt que le FQDN pendant certaines étapes de l'installation. La solution est d'ajouter le nom d'hôte et son adresse IPv6 au fichier hôte. Toutefois, ceci est une mauvaise configuration.
- Sur une machine sans DNS ou tout autre aperçu de nom, si vous essayez d'installer l'annuaire de provisionnement et le serveur de provisionnement à l'aide de l'adresse IP, l'installation échouera pour les mêmes raisons.

  Remarque : CA ne prend pas en charge l'installation par une adresse IP.

Certaines configuration de domaine réalisées en même temps que des changements de mots de passe utilisateur généraux peuvent causer l'arrêt brutal du serveur de provisionnement.

Si la configuration du domaine « Utiliser des stratégies de mot de passe externe/Serveur Identity Manager » est définie par Oui et que vous réalisez de nombreux changements de mot de passe utilisateur généraux simultanément. Le résultat sera une performance dégradée et le serveur de provisionnement peut s'arrêter brutalement.

Le niveau INFO logging Solaris ECS ci-dessus peut affecter les performances du serveur de provisionnement

Activer le niveau INFO logging ECS ci-dessus provoque une écriture des journaux avant que vous ne receviez une réponse. C'est ce qui retarde votre requête pendant l'écriture du journal. Si vous rencontrez de mauvaises performances du serveur de provisionnement lors de l'utilisation d'ECS logging, les tâches s'y rapportant s'arrêteront.

Les mises à jour SPML ont échoué lorsque JIAM spécifie des noms Objectclass incorrects

Parfois JIAM API peut commencer l'utilisation de noms Objectclass incorrects, abrégés dans des requêtes envoyées au serveur de provisionnement et le serveur de provisionnement refusera la requête et renverra une erreur « Erreur de consistance interne dans le serveur de provisionnement ». Par exemple, lorsque vous réalisez une mise à jour de l'objet « eTSBLDirectory », l'Objectclass incorrect « eTDirectory » est envoyé au serveur de provisionnement. Ce problème peut être résolu en redémarrant le service SPML.

Utilisation de caractères spéciaux dans les noms d'utilisateur

Le gestionnaire de provisionnement permet de créer des noms d'utilisateur comprenant des caractères spéciaux, tels que la barre oblique inverse (\). Toutefois, le serveur Identity Manager ne prend pas en charge les noms d'utilisateur comportant des caractères spéciaux.

Lorsque vous créez un utilisateur global dans le gestionnaire de provisionnement avec un caractère spécial, Identity Manager tente de créer un utilisateur correspondant dans le magasin d'utilisateurs Identity Manager. Des erreurs se produisent et la tâche Créer un utilisateur échoue dans le magasin d'utilisateurs Identity Manager.

Des erreurs se produisent également si vous essayez de supprimer un utilisateur global comportant des caractères spéciaux dans le gestionnaire de provisionnement.

Le gestionnaire de provisionnement inclut les références SAWI/DAWI obsolètes

Le gestionnaire de provisionnement comprend des boîtes de dialogue avec des commandes pour les fonctionnalités SAWI et DAWI, qui ne sont plus prises en charge. Utilisez les fonctionnalités d'auto-administration d'Identity Manager au lieu de SAWI ou DAWI.

Il existe déjà des erreurs lors de l'ajout d'un terminal

Si vous supprimez et ajoutez à nouveau un terminal avec exactement le même nom, parfois le serveur de provisionnement rapporte un échec en déclarant que le terminal avec ce nom existe déjà. Ceci peut se produire lorsque vous configurez de multiples serveurs de connecteurs pour gérer ce terminal. L'échec provient d'un problème pendant la suppression du terminal où tous les serveurs de connecteurs sont avertis de la suppression.

Pour résoudre ce problème, redémarrez tous les serveurs de connecteurs configurés pour gérer le terminal.

Serveur de connecteurs Java (Java CS)

Les problèmes suivants sont liés au serveur connecteur Java dans Identity Manager r12.

L'exploration du connecteur Java échoue lors de l'utilisation des séquences de caractères " / pour représenter les noms différents

Un problème non résolu existe dans CS Java concernant les séquences de deux caractères suivantes :

"/

Il est important pour la prise en charge des noms de composite utilisés par la norme JNDI API de représenter les noms différents qui utilisent de multiples technologies.

Pour plus d'informations concernant les autres caractères spéciaux dans les noms différents passés dans CS Java, reportez-vous à LDAP RFC 2253 sur :

http://ietf.org

et au JavaDoc pour javax.naming.ldap.LdapName

Erreur de pointeur nul dans Connector Xpress

Si vous essayez de modifier les informations de routage du serveur de connecteurs en cliquant avec le bouton droit de la souris sur un type de terminal et en sélectionnant Gestion CS, ou en modifiant directement la configuration CS dans les environnements avec plusieurs serveurs de provisionnement via Connector Xpress, Connector Xpress peut afficher une erreur de pointeur nul. Si vous devez exécuter le routage du serveur de connecteurs avancé, utilisez l'outil csfconfig.

Impossible de redémarrer le service CS Java via les services Windows

Lors du redémarrage du service CS Java via les services Windows, vous pouvez démarrer le service CS Java avant qu'il soit complètement arrêté, ce qui entraine ainsi l'échec du démarrage du service. Si vous rencontrez ce problème, utilisez les boutons d'arrêt et de démarrage au lieu des boutons de redémarrage des Services Windows dans le Panneau de configuration.

Message d'erreur si vous ne sélectionnez pas une procédure enregistrée

Si vous ne sélectionnez pas une procédure enregistrée dans la liste déroulante Sélectionner une procédure à l'écran Mapper les données du tableau dans l'assistant Connector Xpress et si vous cliquez sur Suivant, le message d'erreur suivant s'affiche :

Spécifiez un tableau pour le mappage.

Le message correct est le suivant :

Spécifiez une procédure pour le mappage.

Les conteneurs explorés du terminal DYN JNDI n'apparaissent pas dans le gestionnaire de provisionnement

Après la réalisation d'une exploration sur un niveau du conteneur sur un terminal DYN JNDI neuf, le panneau du contenu du gestionnaire de provisionnement risque de ne pas montrer le conteneur nouvellement exploré bien que le compte d'exploration indique le nouvel enregistrement ayant été ajouté. Fermer et rouvrir le gestionnaire de provisionnement forcera le conteneur à apparaître.

Les attributs suspendus du modèle de compte DYN apparaissent en gras dans le gestionnaire de provisionnement

Le gestionnaire de provisionnement affiche l'attribut de la suspension du compte pour les modèles de compte DYN en gras ce qui indique par erreur que c'est un attribut de capacité.

Les étiquettes des attributs de capacité DYN peuvent être tronquées dans le gestionnaire de provisionnement

Les attributs de capacité précisés à la création des types de terminaux DYN JDBC ou DYN JNDI dans Connector Xpress peuvent être tronqués ou sans étiquette lorsqu'ils sont affichés dans le gestionnaire de provisionnement. Il est possible d'y remédier en précisant un caractère supplémentaire à la fin de l'étiquette, « *NomEtiquette a* » par exemple lorsque vous précisez le nom d'affichage dans Connector Xpress. Ceci ne se produit as avec les attributs de capacité pour l'appartenance.

Vous pouvez également modifier les métadonnées existantes d'une des manières suivantes :

Après avoir chargé le projet dans Connector Xpress

- Exécutez l'Assistant
- Développez l'arborescence des métadonnées, rentrez dans les classes -> eTDYNPolicy -> Propriétés -> Attribut de capacité -> Métadonnées et modifiez la valeur du nom d'affichage.

Si vous choisissez l'une des deux méthodes pour modifier les métadonnées existantes pour un type de terminal DYN, assurez-vous que le type de terminal DYN est à jour avec les nouvelles métadonnées.

Connecteurs

Les problèmes suivants se rapportent aux connecteurs de provisionnement dans Identity Manager r12.

Résultats incorrects pendant la recherche dans le sous-arbre avec le connecteur ADS

Pendant une recherche dans le sous-arbre dans un sous-arbre contenant des unités d'organisation multiples et de nombreux objets dans chacune d'entre elles, la recherche peut ne retourner aucun objet par erreur. Par exemple, une taille de recherche limitée à 500 et le nombre d'objets de chaque unité d'organisation ci-dessus qui limite, aucun résultat ne sera retourné. Même si le filtre de recherche s'approche de la taille limite de recherche de 500, la recherche peut continuer de ne retourner aucun objet par erreur. Le travail de remédiation à ce problème augmentera la taille limite de recherche.

Évitez de paramétrer les dates d'expiration d'ADS après 2038

Si vous paramétrez la date d'expiration sur un compte ADS à une date supérieure à 2038, le gestionnaire de provisionnement s'arrêtera brutalement.

Connecteur EEM non pris en charge par IE7

Le connecteur EEM n'est pas pris en charge si le serveur de connecteurs C++ (CCS) pour le connecteur EEM donné est installé sur un ordinateur équipé d'IE7.

Remarque : Dans la documentation produit d'Identity Manager r12, Embedded Entitlements Manager (EEM) se réfère au connecteur Embedded Identity and Access Manager (EIAM).

Voir les modèles de compte EEM avec le gestionnaire de provisionnement

Le gestionnaire de provisionnement peut ne plus répondre lors du visionnage des modèles de compte EEM.

La solution est de fermer et de redémarrer le gestionnaire de provisionnement.

Rouvrir le gestionnaire de provisionnement pour acquérir un nouveau terminal EEM

Une fois un nom d'hôte défini au cours d'une acquisition, vous devez fermer, puis rouvrir le gestionnaire de provisionnement pour faire l'acquisition d'un autre terminal. Cela est vrai même si l'opération a été annulée.

Impossible de sélectionner ou de modifier les attributs utilisateur du modèle de compte EEM

Lorsque vous créez des modèles de compte pour un terminal EEM, vous devez cliquer sur l'onglet Propriétés de l'application après avoir sélectionné le terminal, puis cliquez sur OK pour terminer le processus de création du modèle de compte.

L'acquisition d'un terminal DB2 z/OS cause un arrêt brutal du CCS

Les connecteurs DB2 UDB et DB2 z/OS ne doivent pas acheminer des requêtes au même serveur de connecteurs C++ (CCS).

La solution consiste à installer un deuxième CCS sur une autre machine afin que chacun des connecteurs DB2 UDB et DB2 z/OS soit hébergé sur leurs propres serveurs de connecteurs C++.

Mise à niveau automatique de l'agent distant UNIX ETC non prise en charge

Les mises à niveau automatiques d'un agent distant UNIX ETC d'eTrust Admin r8.1 SP2 vers Identity Manager r12 ne sont pas prises en charge. Vous devez effectuer la mise à niveau en mode assisté.

L'agent distant ETC sur Linux OS fonctionnant avec un S390 échoue

La tentative d'installation de l'agent distant ETC sur un système d'exploitation Linux fonctionnant sur un hôte S390 échoue avec l'erreur :

"linux098:/home/marty/LinuxS390 # ./IdentityManager.LinuxS390.sh
lsm.exe : erreur lors du chargement des bibliothèques partagées :
libncurses.so.4: impossible d'ouvrir les fichiers d'objets partagés : Aucun fichier ou répertoire similaire."

Pour résoudre ceci, vous devez localiser une version 4 de ncurses pour le système d'exploitation et l'installer.

L'exécution de la commande Cafthost provoque une erreur HP-UX UNIX

Vous pouvez voir une erreur « erreur Bus (mémoire vide) » lorsque vous exécutez la commande suivante :

```
cafthost -a <nom_hôte>
```

Pour ajouter des hôte(s), modifiez le fichier de configuration « cafthost.cfg » à l'aide d'un éditeur de texte dans le répertoire « cat /etc/catngcampath » et ajoutez chaque hôte à une nouvelle ligne.

La désinstallation de l'agent distant ETC peut laisser des fichiers orphelins

Lorsque l'agent distant ETC est mis à niveau de r8.1SP2 vers r12, les différents fichiers peuvent être laissés de côté. Si ces fichiers ne sont pas utilisés par d'autres packages installés, ils peuvent être supprimés :

- /usr/bin/uxsautil
- `cat /etc/catngdmopath.tng`/bin/uxsautil
- `cat /etc/catngdmopath.tng`/scripts/Config
- `cat /etc/catngdmopath.tng`/etc/ExitSetup.ini
- `cat /etc/catngdmopath.tng`/scripts/Config
- `cat /etc/catngdmopath.tng`/scripts/Config
- `cat /etc/catngdmopath.tng`/setup.gif

VMS modifie « Supprimer les échecs des droits des comptes » avec SPML

Vous ne pouvez pas supprimer une valeur dans les attributs droits des comptes dans un compte VMS sans utiliser SPML. Le client SPML retournera un message de réussite mais le compte ne sera pas mis à jour.

La solution consiste à utiliser le gestionnaire de provisionnement pour réaliser de telles modifications.

Impossible de définir un deuxième mot de passe pour les comptes OpenVMS

L'utilitaire d'agent distant OpenVMS ‘vmsautil’ n'utilise pas les sémantiques du mot de passe PRINCIPAL/SECONDAIRE OpenVMS pour les comptes utilisateur. Si vous tentez de préciser un deuxième mot de passe lorsqu'aucun mot de passe principal n'a été défini, l'opération échoue et le message d'erreur « mot de passe trop court » apparaît.

La solution d'est de toujours réinitialiser le mot de passe principal lorsque vous tentez de définir un mot de passe secondaire pour le compte.

Une instruction est manquante dans CAM/CAFT pour OpenVMS

Le fichier ETRUST_ADMIN_OPENVMS_INSTALLATION.TXT ne contient pas les informations sur la configuration de CAMCAFT.EXE sur un système OpenVMS. Le nom symbolique CAFTHOST doit être défini avant l'installation de CAM/CAFT. Pour définir CAFTHOST, ajoutez la commande suivante au fichier LOGIN.COM :

```
CAFTHOST :==$CAPOLY$BIN:CAFTHOST.EXE
```

Reconnectez-vous ensuite au système OpenVMS.

L'attribut VMS eTVMSPWDLifeTime n'est pas synchronisé

L'attribut Lifetime du mot de passe (eTVMSPWDLifeTime) est affiché comme non synchronisé après l'opération « Vérifier la synchronisation du compte » si l'attribut du modèle de compte « N'expire jamais » est défini comme vrai (vérifié).

Le statut du compte VMS est rapporté comme faux par SPML

Si un compte VMS est suspendu, le gestionnaire de provisionnement rapporte un statut « Actif (suspendu dans eTrust Admin) » pour le compte, pourtant SPML le rapporte faux pour la suspension uniquement

Impossible de définir les indicateurs de mot de passe VMS

L'attribut eTVMSPwdFlags n'est pas défini correctement pour une opération d'ajout ou de modification du compte si la requête ne définit pas de valeur pour eTVMSAccessFlags non plus.

La solution c'est que la requête d'ajout ou de modification doit contenir une valeur pour l'attribut eTVMSAccessFlags et eTVMSPwdFlags.

L'attribut de migration du mot de passe VMS est indiqué non synchronisé

Tout compte VMS ou modèle de compte avec le champ MIGRATEPW défini comme vrai (vérifié), montre eTVMSPwdFlags non synchronisé après l'opération « Vérifier la synchronisation du compte ».

Suspension du compte VMS

Suspendre un compte au niveau du compte à l'aide du gestionnaire de provisionnement suspend le compte correctement. Toutefois, cela ne conserve pas la mention « Suspendu » dans la page propriétés et transforme en « Actif » lorsque vous appliquez les changements. Vous disposez donc d'un compte suspendu mais la page des propriétés du compte a un attribut « Actif » ce qui signifie que vous ne pouvez pour le moment pas rendre le compte « Actif » à nouveau.

Il n'y a aucune solution dans le compte lui-même. Le seul moyen est de corréler le compte avec des utilisateurs globaux et contrôler les suspensions de comptes par le biais de la suspension des utilisateurs globaux

Les noms d'utilisateurs VMS ne peuvent pas contenir de caractères unicode.

La tentative de création d'un compte VMS avec un nom incorrect peut arrêter brutalement le serveur de provisionnement installé sur Solaris.

Le connecteur NDS ne peut pas explorer de nouveaux conteneurs

La première exploration tente de trouver et d'ajouter des conteneurs après l'acquisition d'un terminal NDS. Si vous ajoutez des conteneurs à l'aide d'outils locaux NDS, puis essayez de réexplorez le terminal, ni les conteneurs nouvellement ajoutés ni les sous-entrées n'apparaitront dans l'arborescence.

Vous devez supprimer le terminal du serveur de provisionnement, puis l'acquérir à nouveau et l'explorer afin de voir les nouveaux conteneurs.

La description du connecteur NDS est un champ à valeur unique

Dans le connecteur NDS, la description de compte est un champ à valeur unique. Toutefois, dans le terminal NDS, il s'agit d'un champ à valeurs multiples.

La variable environnement doit être supprimée ou modifiée après la mise à niveau pour éviter les problèmes de type de terminal connecteur UPO.

Pendant une mise à niveau d'un SuperAgent à un serveur de connecteurs r12 C++, la variable environnement ETAHOME peut contenir le chemin d'installation incorrect du CSS et causera des problèmes avec le type de terminal connecteur UPO. Vous devez supprimer manuellement la variable environnement ETAHOME ou la remplacer par le chemin d'installation correct du CSS après la mise à niveau avant de tenter d'acquérir ou utiliser le terminal UPO.

L'acquisition d'un terminal UPO ne valide pas le champ Domaine.

Un terminal UPO avec une valeur spécifiée incorrecte dans l'attribut domaine sera acquis correctement, toutefois le terminal renverra des erreurs « Échec de la recherche du serveur de connecteurs » pendant l'exploration.

Ceci peut être résolu en cliquant avec le bouton droit de la souris sur le terminal dans le gestionnaire de provisionnement, en sélectionnant Personnaliser -> Mettre à jour les références... et en spécifiant la valeur correcte pour le domaine.

La vérification du paramètre Kernel requise n'est pas réalisée avant la mise à niveau d'eTrust Common Services à Enterprise Common Services sur Solaris

Une vérification du paramètre Kernel requise n'est pas réalisée sur les produits qui mettent à niveau eTrust Common Services vers Enterprise Common Services sur Solaris (plus susceptible d'affecter Solaris 9 que Solaris 10). Une installation est permise pour continuer plutôt que d'être arrêté par un avertissement si les paramètres kernel ne sont pas suffisants. Ceci concerne :

- L'agent distant RSA sur Solaris
- IMPS sur Solaris
- SDK IMPS

Pour résoudre ce problème :

Exécuter

```
'<product installer dir>/solaris/ecs-installation/eCSinstall.sh'
```

Un message d'information s'affichera si kernel ne répond pas aux exigences. Si les exigences kernel ne sont pas respectées, le programme d'installation démarrera

Impossible de dupliquer les comptes KRB

Dans le gestionnaire de provisionnement, toute tentative de dupliquer un compte Kerberos entraine l'erreur "eTKRBFullNameCorrelate introuvable dans le registre d'attributs ! (...) - Code de retour : 111". Pour résoudre ce problème, ajoutez un nouveau compte au lieu de dupliquer le compte existant.

Erreur lors de la définition d'un domaine non valide lors de l'acquisition d'un terminal KRB

Si vous essayez d'acquérir un terminal KRB et spécifiez une valeur non valide pour le domaine, un message d'erreur de pointeur nul s'affichera.

Le terminal de sécurité z/OS a provoqué l'arrêt brutal du serveur de provisionnement Solaris

Si le terminal ne peut pas se connecter au serveur CA LDAP Server pour z/OS r12, le serveur de provisionnement s'arrêtera brutalement.

Pour résoudre ce problème, assurez-vous de configurer le terminal avec des informations de connexion valides.

Synchronisation z/OS à l'aide du terminal LDS

L'agent de synchronisation LDS n'est pas inclus dans le DVD du produit Identity Manager r12. Contactez l'assistance si vous avez besoin de cet agent.

Message E2K Error lors de la gestion des droits des boîtes courriels avec Exchange 2007

Les droits des boîtes courriels ne peuvent pas être gérés avec Exchange 2007. Vous recevrez un message d'erreur « Message CAFT : Accès refusé ou échec lors de l'exécution de la commande ».

Erreur E2K CAFT lors de la gestion des droits des boîtes courriels

Le message d'erreur « Message CAFT : Accès refusé ou échec lors de l'exécution de la commande » peut être retourné pendant la gestion des droits des boîtes courriels même lorsque votre agent d'échange distant est correctement configuré.

Ceci peut se produire lorsque la liste des droits des boîtes courriels contient de multiples privilèges pour le même objet et arrive généralement lorsque les objets gérés héritent de droits de l'objet parent.

Les multiples adresses électroniques principales E2K ne sont pas autorisées

Il est possible d'utiliser le gestionnaire de provisionnement pour ajouter une nouvelle électronique à une liste d'adresses existantes et définir la nouvelle adresse comme adresse électronique principale. Toutefois, une adresse électronique principale existante n'est pas rétrogradée. Ainsi, un compte peut avoir de multiples adresses électroniques principales que le système d'origine n'autorise pas. Ceci peut être évité en rétrogradant premièrement l'adresse électronique principale avant d'ajouter une nouvelle adresse électronique principale

Un long chemin PKI pour le fichier INI peut redémarrer le serveur de provisionnement

Les chemins UNC de plus de 77 caractères redémarreront le système d'exploitation. Pour résoudre ceci, évitez d'utiliser des chemins trop longs.

Les comptes PKI apparaissent comme des doublons

Le connecteur PKI ne prend pas en charge les terminaux hiérarchiques PKI Entrust et stocker tous les comptes dans une liste plate. À cause de cela, un compte unique PKI Entrust apparaît comme un doublon du connecteur PKI.

La feuille de propriétés des groupes PKI ne s'affiche pas correctement

Lorsque vous essayez d'ouvrir une feuille de propriétés d'un groupe PKI dans le gestionnaire de provisionnement, le message d'erreur « Impossible d'afficher la feuille de propriétés requise » s'affiche.

Avertissement de la notification des courriels lors de la création des comptes PKI

Si vous acquérez un terminal PKI utilisant un profil proxy et que la notification des courriels est activée, vous ne pouvez pas créer un nouveau compte PKI sans spécifier l'option « Créer profil ».

Pour résoudre ce problème, effectuez l'une des opérations suivantes :

- Acquérir le terminal sans le profil Proxy.
- Désactivez la notification des courriels lors de l'acquisition du terminal et allez dans le terminal pour vérifier le numéro de référence manuellement

Assignation des types d'utilisateur contractuel SAP

Lorsque vous assignez un type d'utilisateur contractuel à un utilisateur à l'onglet Licence des données, le changement ne peut qu'être appliqué au système Master, pas à l'ensemble des systèmes enfants.

Il est possible de changer les types de licence contractuelle pour les enfants d'origine.

Les champs obligatoires dans l'attribut du type d'utilisateur contractuel SAP

Le type d'utilisateur contractuel qui peut être spécifié dans l'onglet Licence de données du compte ne peut pas comporter de champs obligatoires autres que le champ LIC_TYPE. Par exemple, si vous devez spécifier le nom du système SAP R3 (SYSID) pour utiliser un type d'utilisateur contractuel, l'assignation échouera et une erreur indiquera qu'il manque une valeur pour le nom du système SAP R3.

Le serveur de connecteur C++peut s'arrêter brutalement pendant une requête au connecteur PLS.

Si vous trouvez que votre CSS s'est arrêté brutalement pendant une requête à un connecteur PLS, vous devez examiner l'installation de votre stratégie de serveur car ce peut être la cause du problème. Le symptôme que vous verrez dans les requêtes à la stratégie du serveur se résorbera progressivement en raison du redémarrage continu du service de contrôle d'accès.

Suspension du compte SBL

En modifiant le compte SBL ou le modèle de compte SBL et en synchronisant les changements avec un compte, ne définissez pas eTSuspended avec d'autres modifications car ceci causerait l'ignorance d'autres modifications d'attribut.

Pour résoudre ceci, séparer les changements en deux requêtes différentes, l'une contenant les modifications eTSuspended et l'autre contenant les changements des valeurs de tout autre attribut.

Echec de l'exécution de la tâche Vérifier la synchronisation des comptes JIAM RSA

Lors de l'exécution de la tâche Vérifier la synchronisation des comptes pour un compte RSA utilisant JIAM, si le terminal ne contient pas ce compte, le serveur de connecteurs renvoie un message d'erreur "Echec de la lecture du serveur de connecteurs : Erreur Sd_GetSerialByLogin utilisateur non valide", au lieu d'afficher le message " Compte introuvable dans le terminal". Vérifiez que la synchronisation des comptes fonctionne correctement dans le gestionnaire de provisionnement.

La suppression des groupes multiples à partir d'un utilisateur OS/400 amortit le gestionnaire de provisionnement

La suppression des groupes multiples d'un utilisateur, dans une opération unique où un ou plusieurs groupes commence par « # », peut entraîner la non réponse du gestionnaire de provisionnement.

Pour résoudre ceci supprimez un groupe à la fois.

Le groupe principal du compte OS/400 ne peut pas être supprimé

L'appartenance à un groupe OS/400 peut être modifiée en modifiant le compte d'un groupe membre ou l'appartenance à un groupe. Lorsque vous modifiez l'appartenance à un groupe, les comptes ne peuvent pas être supprimés si l'appartenance à leur groupe est une appartenance principale.

Pour résoudre ce problème, modifiez le compte et supprimez l'appartenance principale au groupe.

Le connecteur FND doit contenir une date d'« entrée » et de « sortie » dans la liste des responsabilités

Le connecteur FND doit contenir une date d'« entrée » et de « sortie » dans la liste des responsabilités sinon la liste des responsabilités est instable et non recouvrable

Pour résoudre ceci, vous devez spécifier une date d'« entrée » et de « sortie » dans la liste des responsabilités pendant la création ou la modification du modèle de compte ou compte FND (par exemple à l'aide de dates lointaines ou futures plutôt que des dates d'« entrée » et de « sortie » vides).

L'hôte de la définition Caft sur VISTA ne fonctionne pas

Si vous avez installé l'agent distant N16 sur un terminal VISTA ou VISTA SP1 et que vous essayez d'ajouter le serveur de gestion via Tous les programmes -> CA -> Identity Manager -> Hôte de la définition Caft puis essayez d'acquérir cette machine VISTA en tant que terminal, vous obtiendrez un message d'erreur « Accès refusé ».

Pour résoudre ceci, ouvrez une invite de commande et tapez cette commande pour acquérir le terminal.

```
cafthost -a <hostname/IP>
```

Utilisez les chemins absolus pour accéder aux emplacements des ID des comptes personnalisés LND et des ID des certificats d'unité organisationnelle

À l'aide des chemins UNC, lorsque vous accédez au compte personnalisé, les emplacements des ID et les ID des certificats des unités organisationnelles ne fonctionnent pas toujours avec des dossiers partagés dans un chemin relatif. L'utilisation de chemins absolus (y compris les lettres du lecteur) est recommandée.

La requête de recherche LND dans SPML ne retourne aucun résultat.

La réalisation d'une requête de recherche dans SPML ou via le serveur SPML pour un compte ne retourne aucun résultat lorsque des attributs sont utilisés à côté du Nom et du serveur d'accueil

La corrélation des comptes LND et les utilisateurs globaux créés via SPML ne fonctionne pas

Dans le gestionnaire de provisionnement, la corrélation des comptes et des utilisateurs globaux créés via SPML ne fonctionne pas pour le moment.

Évitez d'utiliser les caractères japonais dans les noms de compte LND

Le changement de l'ID du mot de passe ne fonctionne pas avec les comptes contenant des caractères japonais dans le nom du compte. L'utilisation des caractères anglais dans le fichier ID du compte résout les problèmes.

Les comptes LND ne peuvent pas être créés avec « Utilisateur unique OU »

Les comptes ne peuvent pas être créés avec « Utilisateur unique OU » Le compte qui en résulte ne pourra pas être recherché ou accessible depuis le gestionnaire de provisionnement.

L'attribut nom court du compte LND ne peut contenir plus de 85 caractères japonais

L'utilisation de plus de 85 caractères dans l'attribut nom court du compte est connue pour entraîner l'arrêt brutal du serveur Domino. Ce problème ne se produit que lorsque le nom du compte comprend également des caractères japonais.

Le gestionnaire de provisionnement n'affiche aucune appartenance de groupe au compte LND s'ils contiennent des caractères japonais

Dans le gestionnaire de provisionnement, les comptes créés dans l'organisation et les unités organisationnelles contenant des caractères japonais ne présente aucune appartenance de groupe dans l'onglet Membre.

Impossible d'accéder au compte LND et aux ID du certificateur contenant des caractères japonais via le connecteur LND JCS

Impossible d'accéder au compte LND et aux ID du certificateur contenant des caractères japonais via le connecteur LND JCS Toutes les fonctions nécessitant un accès à ces fichiers ID sont connues pour échouer dans cette version.

Les caractères japonais des chemins DN des objets LND peuvent causer des problèmes pendant l'exploration du répertoire.

Certains caractères japonais dans les chemins DN objet sont connus pour entraîner la suspension du serveur de provisionnement pendant l'exploration du répertoire. Les exemples comprennent des caractères japonais avec de l'unicode 0x80fd, 0x4e88, and 0x5642.

Le connecteur LND ne peut pas être renommé ou déplacé dans la hiérarchie sur les comptes LND explorés.

Cette version du connecteur LND ne peut pas réaliser les actions de personnalisation pour renommer ou déplacer dans la hiérarchie les comptes LND explorés. Les champs attributs sont désactivés pour ces actions.

Il n'existe aucune solution pour ces actions.

Le compte LND et son fichier Courriel ne peut pas être supprimé à l'aide de l'action personnalisée

Supprimer un compte et le fichier courriel du compte malgré l'échec de l'action « Personnaliser ».

Aucun message d'erreur n'est généré par le gestionnaire de provisionnement mais une inspection du terminal montre que le copte est encore présent ainsi que son fichier courriel. Il n'existe aucune solution à l'aide du gestionnaire de provisionnement.

Les échecs des courriels du compte LND ne sont pas créés pendant l'enregistrement

La fenêtre de création du compte LND du gestionnaire de provisionnement contient une case à cocher « Créer des répliques » dans l'onglet profil.

Lorsque vous administrer un terminal Domino dans un environnement cluster et que la case « Créer des répliques » est cochée, les répliques du compte doivent être créées dans l'environnement cluster avec son fichier courriel. La création des répliques des fichiers courriel n'est pas prise en charge pendant l'enregistrement de cette version.

Chapitre 7 : Documentation

Les noms de fichier pour les guides Identity Manager r12 sont les suivants :

Nom du manuel	Nom du fichier
Notes de parution	im_release_enu.pdf
Manuel de mise en oeuvre	im_impl_enu.pdf
Guide d'installation pour WebLogic	im_install_weblogic_enu.pdf
Guide d'installation pour WebSphere	im_install_websphere_enu.pdf
Guide d'installation pour JBoss	im_install_jboss_enu.pdf
Manuel de configuration	im_config_enu.pdf
Guide de haute disponibilité	im_high_avail_enu.pdf
Manuel d'administration	im_admin_enu.pdf
Manuel de programmation pour Java	im_dev_enu.pdf
Manuel de programmation pour le provisionnement	im_dev_provisioning_enu.pdf
Guide de provisionnement	im_provisioning_enu.pdf
Guide des connecteurs	im_connectors_enu.pdf
Guide des connecteurs Xpress Guide	im_connector_xpress_enu.pdf
Manuel d'implémentation des serveurs de connecteurs Java	im_jcs_impl_enu.pdf
Guide de programmation pour les serveurs de connecteurs Java	im_jcsProg_Enu.pdf
Guide d'intégration de l'enregistreur	audit_im_irec_ref_enu.pdf
Glossaire	im_glossary.pdf
Bibliothèque	im_bookshelf_enu.zip

Les guides Identity Manager r12 peuvent être téléchargés sur :

- le site d'assistance CA

Pour visualiser des fichiers PDF, utilisez Adobe Reader 7 ou supérieur que vous pouvez télécharger sur le site Web d'Adobe s'il n'est pas déjà installé sur votre ordinateur.

Remarque : Pour de meilleures performances lorsque vous installez la bibliothèque sur le système distant, rendez la bibliothèque accessible depuis le serveur Web.

Ce chapitre traite des sujets suivants :

Bibliothèque

La bibliothèque permet d'accéder à l'ensemble des documents Identity Manager à partir d'une interface unique. Elle contient les informations ci-après.

- Liste extensible des contenus de tous les manuels au format HTML
- Recherche de texte intégral dans l'ensemble des manuels, avec classement des résultats de recherche et termes recherchés mis en surbrillance dans le contenu
- Chemins de navigation reliés aux rubriques du niveau supérieur
- Index HTML unique des rubriques pour tous les manuels
- Liens vers les versions PDF des manuels pour impression

Pour utiliser la Bibliothèque :

1. Téléchargez la bibliothèque sur le site de support CA.
2. Extrayez le contenu du fichier ZIP.
3. Affichez la bibliothèque comme indiqué ci-après.
   - Si la bibliothèque se trouve sur le système local et que vous utilisez Internet Explorer, ouvrez le fichier Bookshelf.hta.
   - Si la bibliothèque se trouve sur un système distant ou si vous utilisez Mozilla Firefox, ouvrez le fichier Bookshelf.html.

     Remarque : Pour de meilleures performances lorsque vous installez la bibliothèque sur le système distant, rendez la bibliothèque accessible depuis le serveur Web.

La bibliothèque nécessite Internet Explorer 6 ou 7, ou Mozilla Firefox 2. Pour les liens vers les manuels au format PDF, Adobe Reader 7 ou 8 est nécessaire. Vous pouvez télécharger Adobe Reader à l'adresse www.adobe.com.

Remarque : La bibliothèque SiteMinder CA a été publiée pour les versions r12 et r6.0 SP5 sur le site de support CA, avec le même format de bibliothèque que celui utilisé par Identity Manager.

Améliorations de l'aide en ligne

Désormais, l'aide en ligne de la console d'utilisateur et l'aide en ligne de la console de gestion disposent toutes deux des fonctions ci-après.

Chemins de navigation

Indiquent votre position dans la hiérarchie de l'aide, pour simplifier la navigation. Ils sont situés au sommet de la page d'aide.

Mise en surbrillance des recherches

Identifie le contexte de votre recherche dans les pages qui en résultent, à l'aide d'une surbrillance jaune.

Boutons de navigation

Boutons fléchés Précédent et Suivant, pour simplifier la navigation. Ils sont situés au sommet de la page d'aide, sous les chemins de navigation.

eTrust rebaptisé en CA

La marque de certains produits de sécurité CA est actuellement en transition de "eTrust" à "CA". Pendant cette transition, vous pouvez voir des références à des produits eTrust et à des produits CA dans la documentation. Par exemple, la prochaine version d'eTrust Directory sera rebaptisée CA Directory. Toute mention d'un produit eTrust dans la documentation équivaut au même produit portant la nouvelle marque CA.

Modifications de la terminologie du provisionnement

Les clients eTrust Admin existants peuvent remarquer la modification de certains termes, étant donné qu'eTrust Admin fait désormais partie de CA Identity Manager. Le tableau qui suit répertorie ces modifications.

Terme eTrust Admin	Nouveau terme dans Identity Manager
Serveur Admin eTrust	Serveur de provisionnement
Gestionnaire eTrust Admin	Gestionnaire de provisionnement
Répertoire	Terminal, terminaux
Espace de noms	Type de terminal
Stratégie ou stratégie de provisionnement	Modèle de compte
Rôles	Rôles de provisionnement
Structure de superagents répartis	Structure de serveurs de connecteurs
Superagent	Serveur de connecteurs C++
Option	Connecteur
Répertoire d'administration ou référentiel d'administration	Annuaire de provisionnement
Annuaire d'entreprise Identity Manager	Magasin d'utilisateurs Identity Manager
Utilisateur d'entreprise	Administrateur entrant

Nouveau nom pour le connecteur Embedded IAM (EIAM)

Dans la documentation produit de CA Identity Manager r12, Embedded Entitlements Manager (EEM) se réfère au connecteur Embedded Identity and Access Manager (EIAM).

Documentation de programmation

Deux manuels de programmation sont inclus dans la documentation Identity Manager r12.

Manuel de programmation pour Java

Précédemment intitulé Manuel du développeur d'Identity Manager, ce manuel fournit des informations concernant l'utilisation des API Java Identity Manager. La version HTML est intégrée aux pages Javadoc et comprend des liens hypertextes, le cas échéant, pour renvoyer aux informations pertinentes.

Manuel de programmation pour le provisionnement

Précédemment intitulé Manuel du développeur du SDK eTrust Admin, ce manuel fournit des informations de programmation concernant le SDK du serveur de provisionnement Identity Manager. Les développeurs doivent connaître la programmation avec C++.