# CA Identity Manager™

## Manuel d'implémentation

12.6.4

La présente Documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA. La présente Documentation est la propriété exclusive de CA et ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA.

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

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

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

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

CA est le fabricant de la présente Documentation.

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

Copyright © 2014 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

# Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

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

# Support technique

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

# Table des matières

# Chapitre 1: Gestion des identités et des accès

Ce chapitre traite des sujets suivants :



## Gestion des utilisateurs et accès aux applications

Les services informatiques reçoivent un afflux constant de demandes relatives à la gestion des comptes d'utilisateurs. Les administrateurs informatiques doivent résoudre les besoins urgents des utilisateurs : réinitialisation des mots de passe oubliés, création de nouveaux comptes et demandes de fournitures de bureau.

Ils doivent également accorder aux utilisateurs différents niveaux d'accès aux applications. Par exemple, un responsable de département génère des bons de commande et a besoin d'un compte dans une application financière.

Pour limiter le nombre de demandes envoyées au service informatique, CA Identity Manager offre une méthode intégrée de gestion des utilisateurs et des accès aux applications comprenant :

- L'affectation de droits à l'aide de rôles. Plus précisément :
  - Des rôles qui permettent aux administrateurs de créer et de gérer les comptes d'utilisateurs.
  - Des rôles qui provisionnent des comptes supplémentaires pour les utilisateurs existants (prise en charge du provisionnement requise).
- La délégation de la gestion des utilisateurs et de l'accès aux applications.
- Des options d'auto-administration pour que les utilisateurs puissent gérer leurs propres comptes.
- L'intégration d'applications métier à CA Identity Manager.
- Des options de personnalisation et d'expansion de CA Identity Manager.

# Droits basés sur les rôles

Vous affectez des droits à des utilisateurs en affectant des rôles. Un *rôle* contient des tâches qui correspondent aux fonctions d'application dans CA Identity Manager, telles que la tâche Créer un utilisateur, aux fonctions dans une application, telles que la fonction de création de bon de commande ou de modèles de compte fournissant les comptes d'utilisateurs, tels que le compte SAP. Lorsqu'un rôle est affecté à des utilisateurs, ceux-ci reçoivent les droits correspondants.

CA Identity Manager fournit les types de rôles suivants :

- Rôles de gestion des utilisateurs, appelés *rôles d'administration*.

  Rôles d'administration peuvent également inclure les tâches qui s'affichent dans la console d'utilisateur.
- Rôles d'affectation de compte, appelés *rôles de provisionnement*
- Rôles de fonction d'application, appelés des *rôles d'accès*.

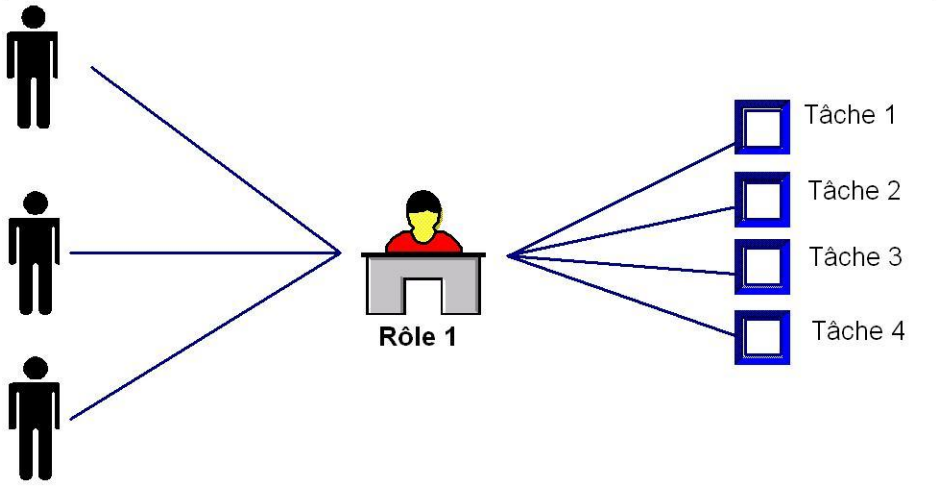
Si vous supprimez un modèle de tâche ou de compte pour un rôle, l'utilisateur ne pourra plus effectuer cette tâche, utiliser un compte de terminal ou utiliser une fonction d'application.

## Rôles d'administration

Les rôles d'administration contrôlent ce qu'un utilisateur peut faire dans CA Identity Manager. Un administrateur système affecte un rôle à un utilisateur ; ce rôle définit un ensemble de tâches que l'utilisateur peut effectuer. Les utilisateurs peuvent effectuer des *tâches* administratives pour des comptes d'utilisateurs, par exemple changer un mot de passe ou mettre à jour un poste.

Les utilisateurs disposent de niveaux d'accès différents à ces tâches. Par exemple, un rôle Employé peut inclure des tâches qui permettent aux utilisateurs de modifier leur nom et leur adresse, tandis que le rôle Responsable des ressources humaines contient des tâches permettant de modifier le titre de l'utilisateur et le salaire.

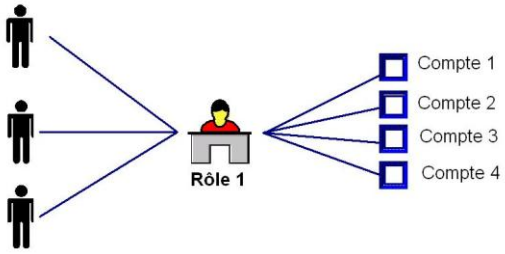
L'illustration suivante affiche quatre tâches combinées dans un rôle d'administration et affectées à trois utilisateurs :




## Rôles de provisionnement

Pour octroyer aux utilisateurs l'accès aux comptes dans des applications supplémentaires, telles qu'un système de messagerie, affectez des rôles de provisionnement. Les rôles de provisionnement contiennent des modèles de compte qui définissent les attributs existant dans un type de compte. Par exemple, un modèle de compte pour un compte Exchange définit des attributs tels que la taille de la boîte aux lettres. Les modèles de compte définissent également la manière dont les attributs d'utilisateurs CA Identity Manager sont mappés vers les comptes.

L'illustration suivante affiche quatre comptes combinés dans un rôle de provisionnement et affectés à trois utilisateurs : Chaque utilisateur reçoit quatre comptes lorsque vous affectez le rôle de provisionnement à cet utilisateur



## Rôles d'accès

Les rôles d'accès permettent de fournir des droits dans CA Identity Manager ou une autre application. Par exemple, vous pouvez utiliser les rôles d'accès pour effectuer les tâches suivantes :

- Fournir l'accès indirect à un attribut d'utilisateur
- Créer des expressions complexes
- Définir un attribut dans un profil d'utilisateur, qui est utilisé par une autre application pour définir des droits

Les rôles d'accès sont similaires aux stratégies d'identité, car ils appliquent un ensemble de modifications à un utilisateur ou à un groupe d'utilisateurs. Toutefois, lorsque vous utilisez un rôle d'accès pour appliquer des modifications, vous pouvez voir les utilisateurs auxquels les modifications s'appliquent en affichant les membres du rôle d'accès.

Dans la plupart des cas, les rôles d'accès ne sont pas associés à des tâches.

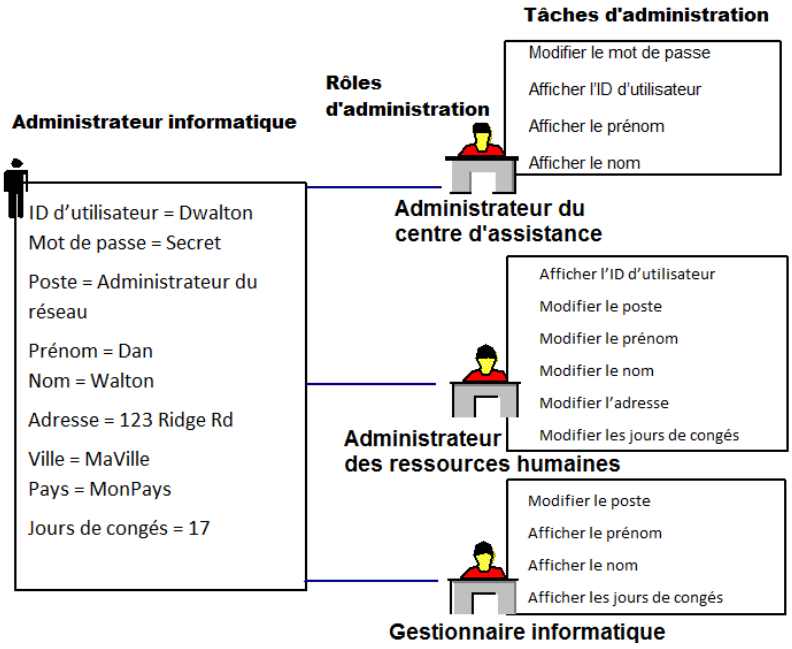
**Remarque :** Lorsque CA Identity Manager s'intègre à CA SiteMinder, les rôles d'accès peuvent également fournir l'accès aux applications qui sont protégées par CA SiteMinder. Dans ce cas, les rôles d'accès incluent des tâches d'accès. Pour plus d'informations, reportez-vous au chapitre relatif à l'intégration de SiteMinder dans le manuel *Configuration Guide*.

# Rôles d'administration pour la gestion de comptes d'utilisateur

Dans CA Identity Manager, vous gérez des objets de référentiel d'utilisateurs (utilisateurs, groupes et organisations) à l'aide de rôles d'administration. Vous utilisez également ces rôles pour gérer les rôles et les tâches qui vous permettent de gérer les objets de référentiel d'utilisateurs. Par exemple, vous utilisez des rôles d'administration pour modifier des attributs de profil d'utilisateurs, offrir des options aux utilisateurs pour gérer leurs propres comptes et approuver les tâches qui utilisent des flux de travaux.

## Gestion des profils au niveau des attributs

Vous pouvez créer des rôles d'administration pour différents administrateurs qui doivent accéder en lecture ou en écriture à des attributs de profil. Par exemple, une société peut avoir plusieurs employés qui effectuent des opérations avec des profils d'utilisateur, chacun accédant à des attributs différents. L'illustration suivante comprend trois rôles et leurs tâches associées. Chaque rôle dispose d'un accès différent aux attributs de profil.




Dans cet exemple, trois rôles peuvent gérer des attributs différents pour le même utilisateur, Dan Walton :

- Un administrateur de centre d'assistance affiche les noms et les adresses des utilisateurs, et réinitialise leurs mots de passe.
- Un administrateur des ressources humaines modifie les ID, les noms, les adresses, les titres et le nombre de jours de vacances des utilisateurs.
- Un responsable informatique modifie le titre des utilisateurs et affiche leur nom et leur nombre de jours de vacances.

Indépendamment des rôles qui vous sont attribués, lorsque vous vous connectez à CA Identity Manager, une série d'onglets appelés catégories s'affichent selon le rôle d'administration affecté à votre compte CA Identity Manager. Cliquez sur un onglet pour afficher les tâches que vous pouvez effectuer dans cette catégorie, comme dans l'illustration suivante :


Les catégories et les tâches des catégories affichées sont déterminées par les rôles d'administration de l'utilisateur.

## Approbation par flux de travaux des tâches d'administration

Pour faciliter l'automatisation des processus métier, vous pouvez créer une tâche d'administration générant un processus de flux de travaux. Un *processus de flux de travaux* automatise une procédure définie qu'une société effectue régulièrement. CA Identity Manager inclut le moteur de flux de travaux WorkPoint.

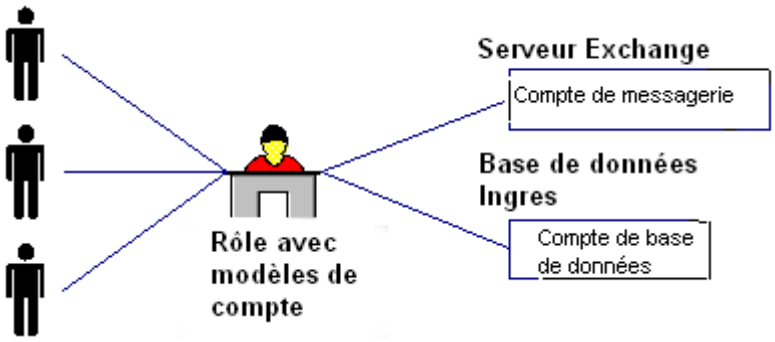
Les processus de flux de travaux sont déclenchés par des événements CA Identity Manager qui font partie d'une tâche d'administration. Par exemple, la tâche Créer un utilisateur inclut les événements CreateUserEvent et AddToGroupEvent. Lorsqu'un événement se produit, le moteur de flux de travaux peut :

- Demander des approbations : un approbateur doit approuver un événement, comme la modification d'un profil d'utilisateur, avant que CA Identity Manager procède à la mise à jour du référentiel d'utilisateurs. Les approbateurs sont des administrateurs qui ont le rôle Approbateur pour une tâche particulière.
- Envoyer des notifications : le moteur de flux de travaux peut notifier les utilisateurs du statut d'un événement à différentes étapes d'un processus, comme lorsqu'un utilisateur initialise un événement ou lorsqu'un événement est approuvé.
- Générer des listes de travail : les listes de travail spécifient les tâches qu'un utilisateur doit effectuer. Le moteur de flux de travaux met à jour automatiquement les listes de travail des administrateurs.

Pour des événements communs, vous pouvez utiliser les processus de flux de travaux fournis avec CA Identity Manager. Vous pouvez également créer des processus de flux de travaux personnalisés.

# Rôles de provisionnement pour des comptes supplémentaires

Dans CA Identity Manager, vous pouvez attribuer des comptes supplémentaires à des utilisateurs à l'aide de rôles de provisionnement. Ces rôles contiennent des modèles de compte définissant des comptes qui existent dans les terminaux gérés, comme un serveur de messagerie. Une fois que des utilisateurs sont définis dans CA Identity Manager, vous pouvez affecter des rôles de provisionnement à certains d'entre eux. L'utilisateur reçoit les comptes définis par les modèles dans le rôle.



Les modèles de compte définissent les caractéristiques du compte. Par exemple, un modèle de compte pour un compte Exchange peut définir la taille de la boîte aux lettres. Les modèles de compte définissent également la manière dont les attributs d'utilisateurs sont mappés aux comptes.

Pour pouvoir utiliser des rôles de provisionnement, vous devez installer le serveur de provisionnement avec le serveur CA Identity Manager. Vous créez ensuite des modèles de compte dans la console d'utilisateur.

# Gestion des mots de passe

Identity Manager comprend plusieurs fonctionnalités de gestion des mots de passe :

- Stratégies de mots de passe : les stratégies permettent de gérer les mots de passe des utilisateurs en appliquant des règles et des restrictions qui régissent l'expiration, la composition et l'utilisation des mots de passe.

  **Remarque :** Pour appliquer des stratégies de mot de passe avancées, configurez l'intégration à SiteMinder. Pour plus d'informations, reportez-vous au *Manuel d'installation*.

- Gestionnaires de mots de passe : les administrateurs qui ont le rôle Gestionnaire de mots de passe peuvent réinitialiser un mot de passe lorsqu'un utilisateur appelle le centre d'assistance.

- Auto-administration de la gestion de mots de passe : CA Identity Manager comprend plusieurs tâches d'auto-administration qui permettent aux utilisateurs de gérer leurs propres mots de passe. Parmi ces tâches figurent notamment :

  - Auto-enregistrement : les utilisateurs indiquent un mot de passe lorsqu'ils s'enregistrent sur un site Web d'entreprise.
  - Modifier mon mot de passe : les utilisateurs peuvent modifier leurs mots de passe sans aide du personnel informatique ou du service d'assistance.
  - Mot de passe oublié : les utilisateurs peuvent réinitialiser ou récupérer un mot de passe oublié après vérification de leur identité par CA Identity Manager.
  - ID d'utilisateur oublié : les utilisateurs peuvent récupérer un ID oublié après vérification de leur identité par CA Identity Manager.

- Synchronisation de mots de passe (avec provisionnement uniquement) : les mots de passe sont synchronisés dans CA Identity Manager et dans les comptes sur les systèmes cibles appelés terminaux. Les nouveaux mots de passe font l'objet d'une vérification par rapport aux stratégies de mots de passe d'Identity Manager.

# Options d'auto-administration des utilisateurs

Afin de réduire la charge de travail du service informatique, CA Identity Manager inclut des fonctionnalités permettant aux nouveaux utilisateurs de s'enregistrer et de récupérer un mot de passe oublié. Ces fonctionnalités ne requièrent aucune action de la part de l'administrateur. L'utilisateur accède à CA Identity Manager via une *console publique*, qui ne requiert aucun compte de connexion. A partir de cette console, un utilisateur peut s'auto-enregistrer sur un site ou effectuer une demande de récupération d'un mot de passe oublié.

Les utilisateurs de CA Identity Manager peuvent gérer leurs propres comptes et permettent ainsi de faire gagner du temps aux administrateurs informatiques. Le rôle d'autogestion des utilisateurs leur permet de :

- Gérer leurs informations personnelles
- Modifier leur mot de passe
- S'auto-abonner à des groupes

# Personnalisation et extensibilité de CA Identity Manager

Vous pouvez personnaliser les fonctionnalités CA Identity Manager suivantes :

- L'annuaire CA Identity Manager, qui décrit la structure de référentiel d'utilisateurs de CA Identity Manager.
- L'apparence et la fonctionnalité de l'interface utilisateur.
- Les fenêtres d'entrées utilisateur, qui déterminent les champs et la disposition de chaque fenêtre de tâche.
- La validation de la saisie des données de l'utilisateur, à l'aide d'une expression régulière, d'un script JavaScript ou des implémentations Java.
- Les flux de travaux, qui définissent les processus de flux de travaux automatisés. Créez ou modifiez des processus en associant des approbateurs et des actions dans le concepteur de processus WorkPoint.
- Les courriels, qui informent les utilisateurs du statut d'une tâche.
- La soumission de tâche, qui peut être envoyée par une application tierce au service Web d'exécution des tâches de CA Identity Manager. Ce service Web traite les demandes de tâche distantes. Ces demandes respectent les normes WSDL.

Vous pouvez étendre les fonctionnalités de CA Identity Manager à l'aide des API suivantes :

- API d'attribut logique : vous permet d'afficher un attribut indépendamment de la façon dont il est stocké physiquement dans un annuaire d'utilisateurs.
- API de gestionnaire de tâches métier : vous permet d'exécuter la logique métier personnalisée pendant la validation des données ou les opérations de transformation.
- API de flux de travaux : fournit des informations à un script personnalisé dans un processus de flux de travaux. Le script évalue les informations et détermine le chemin d'accès au processus de flux de travaux en conséquence.
- API d'outil de résolution de participants : vous permet de spécifier la liste des participants autorisés à approuver une activité de flux de travaux.
- API d'écouteur d'événements : vous permet de créer un écouteur d'événements personnalisé qui écoute un événement ou un groupe d'événements CA Identity Manager. Lorsque l'événement se produit, l'écouteur d'événements peut exécuter la logique métier personnalisée.
- API de règle de notification : vous permet de déterminer les utilisateurs qui doivent recevoir une notification par courriel.
- API de modèle de courriel : inclut des informations relatives à l'événement dans une notification par courriel.

**Remarque :** Pour plus d'informations sur les API CA Identity Manager, consultez le manuel *Programming Guide for Java*.

Lorsque la fonctionnalité de provisionnement est activée pour CA Identity Manager, vous pouvez également l'étendre comme suit :

- Connecteurs personnalisés : permettent à un serveur de provisionnement et à un système d'extrémité de communiquer. Le code qui constitue un connecteur peut inclure un module d'extension d'interface utilisateur graphique, un module d'extension de serveur et un module d'extension d'agent.

  Un connecteur dynamique peut être généré par Connector Xpress et vous pouvez développer un connecteur statique personnalisé en Java ou C++.
- Sorties de programme : vous permettent de référencer un code personnalisé à partir du flux de processus de serveur de provisionnement.

**Remarque :** Pour plus d'informations sur l'extension de la fonctionnalité de provisionnement, consultez le manuel *Programming Guide for Provisioning*.

# Intégration de CA Identity Governance

CA Identity Governance est une solution de gestion du cycle de vie des identités qui permet de développer, de maintenir et d'analyser rapidement et de manière précise les modèles de rôles. Les contrôles des stratégies de conformité des identités sont centralisés et les processus associés aux exigences de conformité et aux demandes de sécurité sont automatisés. CA Identity Governance permet d'effectuer les tâches suivantes :

- Vérifier que les droits d'utilisateurs CA Identity Manager accordés sont conformes aux stratégies de conformité métier
- Obtenir des rôles suggérés et la vérification de la conformité lors de la création ou de la modification des utilisateurs, des rôles et des comptes CA Identity Manager
- Comprendre les rôles existants dans votre organisation, établir les modèles de rôles correspondants et recréer les modèles de rôles souhaités dans CA Identity Manager
- Analyser et conserver ces modèles de rôles en fonction des besoins de l'entreprise

CA Identity Manager s'intègre à CA Identity Governance de deux façons :

- Connecteur CA Identity Governance pour CA Identity Manager

  Type de connecteur spécial qui synchronise automatiquement les données des droits entre CA Identity Manager et CA Identity Governance. Grâce à ce connecteur, vous pouvez importer des données de CA Identity Manager à CA Identity Governance ou exporter des données de CA Identity Governance à CA Identity Manager.

- Provisionnement intelligent

  Lorsque CA Identity Manager est intégré à CA Identity Governance, vous pouvez configurer des fonctionnalités supplémentaires permettant d'utiliser les informations relatives aux rôles et à la conformité afin de prendre en charge les opérations quotidiennes de gestion des identités. Ces informations sont disponibles dans les modèles de rôles. Les modifications effectuées dans CA Identity Manager génèrent une mise à jour dynamique des modèles de rôles dans CA Identity Governance.

**Remarque :** Pour plus d'informations sur l'intégration de CA Identity Governance à CA Identity Manager, consultez le manuel *CA Identity Manager Integration Guide* dans la bibliothèque CA Identity Governance.

# Intégration à CA User Activity Reporting

A partir de la version r12.6 de CA Identity Manager, CA Enterprise Log Manager change de nom et devient CA User Activity Reporting (CA UAR).

CA UAR utilise la grammaire commune aux événements (CEG, Common Event Grammar) de CA pour mapper les événements sous un format standard et stocke tous les événements, y compris ceux non encore mappés, à des fins d'analyse et de vérification. La solution CA UAR permet aux utilisateurs de gérer d'importants volumes de données et de générer des rapports sur les données collectées à l'aide de requêtes de bases de données configurables et/ou de rapports de recherche des différents types d'informations et d'événements.

CA UAR fournit une meilleure vision des systèmes non gérés et des systèmes situés en dehors du champ d'action et du contrôle de CA Identity Manager, vous permettant ainsi d'analyser de manière plus détaillée les différentes identités.

L'intégration à CA Identity Manager permet d'afficher les rapports orientés identités et/ou les requêtes dynamiques de CA UAR dans la console d'utilisateur de CA UAR à l'aide de la console d'utilisateur de CA Identity Manager. Vous pouvez configurer le mode d'affichage et de modification des rapports et/ou des requêtes CA Identity Manager/CA UAR dans la console d'utilisateur, tout en continuant à analyser certaines identités.

## Rapports CA UAR

Les rapports CA UAR sont fournis avec les définitions de rôles CA UAR par défaut :

| Tâche | Rapport appelé |
|---|---|
| Tous les événements du système par utilisateur | CA Identity Manager: tous les événements système filtrés par ID d'utilisateur |
| Gestion des comptes par hôte | Gestion des comptes par hôte |
| Créations de comptes par compte | Créations de comptes par compte |
| Suppressions de compte par compte | Suppressions de compte par compte |
| Verrouillages de comptes par compte | Verrouillages de comptes par compte |
| Activité de processus de certification par hôte | CA Identity Manager : activité de processus par hôte |
| Activité de modification de stratégie de mots de passe | CA Identity Manager : activité de modification de stratégie |

# Chapitre 2: Résolution des besoins métier

Ce chapitre traite des sujets suivants :



## Traitement des modifications métier

Vous pouvez automatiser le traitement de certaines tâches de gestion d'identité à l'aide des stratégies d'identité. Une stratégie d'identité désigne un ensemble de modifications métiers qui ont lieu lorsqu'un utilisateur satisfait à une certaine condition ou règle. Vous pouvez utiliser des ensembles de stratégies d'identité aux fins suivantes.

- Automatiser certaines tâches de gestion d'identité, telles que l'affectation de rôles, d'appartenances à un groupe ou de ressources, ou encore la modification d'attributs de profils d'utilisateurs).
- Appliquer la séparation des fonctions (page 26). Par exemple, vous pouvez créer un ensemble de stratégies d'identité qui interdit aux membres du rôle Signataire de chèque de disposer du rôle Approbateur de chèque et empêche quiconque dans l'entreprise de rédiger un chèque supérieur à 10 000 euros.
- Appliquer la conformité. Par exemple, vous pouvez effectuer un audit sur les utilisateurs disposant d'un certain titre et générant plus de 100 000 euros.

  Les stratégies d'identité qui appliquent la conformité sont nommées *stratégies de conformité*.

Les modifications métiers associées à une stratégie d'identité sont notamment les suivantes.

- L'affectation ou le retrait de rôles, y compris des rôles de provisionnement (si CA Identity Manager prévoit un provisionnement)
- L'affectation ou le retrait d'une appartenance à un groupe.
- La mise à jour d'attributs dans un profil d'utilisateur.

Par exemple, une entreprise peut créer une stratégie d'identité selon laquelle tous les vice-présidents appartiennent au groupe Membre du Country Club et disposent du rôle Approbateur de salaire. Lorsque le titre d'un utilisateur est redéfini sur Vice-président et que cet utilisateur est synchronisé avec la stratégie d'identité, CA Identity Manager ajoute l'utilisateur au groupe et au rôle appropriés. Lorsqu'un vice-président est promu PDG, il ne remplit plus la condition spécifiée par la stratégie d'identité Vice-président. Les modifications apportées par cette stratégie sont donc révoquées et les nouvelles modifications basées sur la stratégie PDG sont appliquées.

Les actions de modification qui se produisent en fonction d'une stratégie d'identité contiennent des événements pouvant être placés sous le contrôle du flux de travaux et faire l'objet d'un audit. Dans l'exemple précédent, le rôle Approbateur de salaire accorde des droits significatifs à ses membres. Pour protéger le rôle Approbateur de salaire, l'entreprise peut créer un processus de flux de travaux qui nécessite un ensemble d'approbations avant l'affectation du rôle et configurer CA Identity Manager pour effectuer l'audit de l'affectation du rôle.

Pour simplifier la gestion des stratégies d'identité, celles-ci sont regroupées dans un ensemble. Par exemple, les stratégies Vice-président et PDG peuvent appartenir à l'ensemble de stratégies d'identité Droits des cadres.

# Conformité aux processus métier

La conformité correspond à la gouvernance d'entreprise qui inclut une vaste gamme de procédures permettant de garantir qu'une entreprise et ses employés se conforment aux stratégies métier établies. Ces procédures de conformité impliquent souvent la documentation, l'automatisation et l'audit de l'affectation des droits sur les applications et les systèmes.

CA Identity Manager inclut les fonctionnalités prenant en charge la gestion de la conformité suivantes :

- **Provisionnement intelligent**

  Dans un contexte d'intégration de CA Identity Manager à CA Identity Governance, l'ensemble des fonctionnalités de provisionnement intelligent simplifie les affectations de rôles de provisionnement. Ces fonctionnalités sont les suivantes.

  - Suggestions de rôles de provisionnement

    CA Identity Manager fournit aux administrateurs la liste des rôles de provisionnement susceptibles d'être affectés à un utilisateur. La liste des rôles de provisionnement est déterminée par CA Identity Governance, selon les critères entrés par l'administrateur.

    La suggestion de rôles de provisionnement garantit l'octroi de droits adéquats aux utilisateurs, tout en préservant les modèles de rôles de la société.

- Messages de conformité et de modèle

  Les administrateurs CA Identity Manager peuvent valider les modifications proposées par rapport à un modèle de rôle dans CA Identity Governance avant de les appliquer. La validation des modifications avant leur application permet aux sociétés de préserver le modèle de rôle défini pour leurs opérations.

  Les utilisateurs peuvent valider les propositions de modifications à apporter aux rôles de provisionnement (en les affectant ou les supprimant) ainsi que les modifications apportées aux attributs d'utilisateurs.

  CA Identity Manager effectue deux types de validation de stratégie.

  - Conformité

    Les modifications proposées sont validées par rapport au modèle de rôle CA Identity Governance afin de détecter d'éventuelles violations des règles de stratégie métier explicites prédéfinies dans CA Identity Governance.

  - Schéma

    Les modifications proposées sont comparées au modèle de rôle CA Identity Governance pour vérifier si l'objet du changement est "hors schéma". CA Identity Manager vérifie également que les modifications n'altèrent pas de manière significative un schéma établi dans le modèle de rôle.

    Vous pouvez configurer CA Identity Manager afin d'effectuer ces validations automatiquement lorsque les utilisateurs effectuent certaines tâches, ou afin de permettre aux utilisateurs de lancer la validation manuellement.

Vous pouvez implémenter le provisionnement intelligent dans un environnement CA Identity Manager s'il existe un modèle de rôle établi reposant sur des données CA Identity Manager dans CA Identity Governance.

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

- **Stratégies d'identité**

  Vous pouvez créer une stratégie de conformité, un type de stratégie d'identité, (page 21) qui empêche les utilisateurs de disposer de certains droits s'ils en ont d'autres. Par exemple, vous pouvez interdire aux utilisateurs qui peuvent approuver les chèques de les délivrer.

  Les stratégies de conformité renforcent la séparation des fonctions dans votre environnement.

- **Rapports de conformité**

  CA Identity Manager comprend des exemples de rapports affichant le statut de conformité des utilisateurs de votre environnement. Grâce à ces rapports, vous pouvez déterminer les utilisateurs non conformes aux processus métier en place.

## Rapports de conformité

CA Identity Manager inclut des exemples de rapports dans le tableau suivant que vous pouvez utiliser pour surveiller la conformité avec les stratégies métier de votre société.

| Rapport | Description |
|---|---|
| Membres avec rôles | Affiche les rôles dans la base de données de rapport et répertorie les membres de ces rôles. |
| Rôles | Affiche les informations suivantes pour chaque rôle de la base de données de rapport :<br>■ Tâches associées au rôle<br>■ Stratégies de membre et membres avec rôle<br>■ Stratégies d'administrateur et administrateurs de rôle<br>■ Stratégies de propriété et propriétaires de rôle |
| Rôles de tâches | Affiche les tâches dans la base de données de rapports et les rôles auxquels elles sont associées. |
| Rôles utilisateur | Affiche les utilisateurs dans la base de données de rapports et répertorie les rôles de chaque utilisateur. |
| Tendances des comptes non standard | Affiche les tendances des comptes non standard pour les comptes orphelins, les comptes système et les comptes d'exception. |
| Comptes non standard | Affiche tous les comptes orphelins, les comptes système et les comptes d'exception. |
| Comptes orphelins | Affiche tous les comptes de terminal sans utilisateur global dans le serveur de provisionnement. |
| Stratégies | Affiche toutes les stratégies d'identité. |

| Rapport | Description |
|---|---|
| Profil de l'utilisateur | Affiche les informations suivantes sur les utilisateurs :<br>■ Nom<br>■ ID de l'utilisateur<br>■ Les groupes dont l'utilisateur est membre ou administrateur.<br>■ Les rôles dont l'utilisateur est membre, administrateur ou propriétaire. |
| Comptes de terminal | Affiche les comptes par terminal. Vous pouvez choisir le terminal à afficher. |
| Administrateurs de rôles | Affiche les rôles et leurs administrateurs. |
| Propriétaires des rôles | Affiche les rôles et leurs propriétaires. |
| Clichés | Affiche tous les clichés exportés. |
| Compte d'utilisateur | Affiche une liste des utilisateurs et de leurs comptes. |
| Droits des utilisateurs | Affiche les rôles, les groupes et les comptes de l'utilisateur. |
| Statut de synchronisation des stratégies d'utilisateur | Affiche le statut de l'utilisateur par stratégie et indique les stratégies à allouer, à annuler ou à réallouer. |

Pour plus d'informations sur les rapports, reportez-vous au *Manuel d'administration*.

# Conditions de l'application de la séparation des fonctions

Les conditions d'application de la séparation des fonctions empêchent des utilisateurs de recevoir des droits qui peuvent déboucher sur un conflit d'intérêt ou sur une fraude. CA Identity Manager offre la fonctionnalité suivante pour la prise en charge de la séparation des fonctions :

- **Stratégies d'identité préventives**

  Ces stratégies, qui s'exécutent avant la soumission d'une tâche, permettent à un administrateur de contrôler les violations de stratégie avant d'affecter des droits ou de modifier des attributs de profil. S'il existe une violation, l'administrateur peut la résoudre avant de soumettre la tâche.

  Par exemple, une société peut créer une stratégie d'identité préventive qui empêche les utilisateurs disposant du rôle Gestionnaire d'utilisateurs de disposer également du rôle Approbateur d'utilisateurs. Si un administrateur utilise la tâche Modifier un utilisateur pour donner au gestionnaire d'utilisateurs le rôle d'approbateur d'utilisateurs, CA Identity Manager affiche un message informant de la violation. L'administrateur peut alors modifier les affectations de rôle pour résoudre la violation avant de soumettre la tâche.

- **Validation de stratégie à l'aide du provisionnement intelligent**

  Les administrateurs CA Identity Manager peuvent valider les modifications des rôles de provisionnement et des attributs d'utilisateur en utilisant les règles de processus métier dans CA Identity Governance avant d'accepter les modifications. Les règles de processus métier représentent différentes contraintes appliquées aux droits. Par exemple, une règle de processus métier peut empêcher les utilisateurs ayant un rôle Département des achats, qui permet aux membres de commander des stocks aux sous-traitants, de disposer également du rôle Paiement des sous-traitants. Les règles de processus métier sont créées par un administrateur système, un responsable commercial, un auditeur ou un ingénieur de rôle dans CA Identity Governance.

  **Remarque :** Pour plus d'informations sur les règles de processus métier, reportez-vous au manuel *CA Identity Governance Sage DNA User Guide (en anglais)*.

**Remarque :** Pour plus d'informations sur les stratégies d'identité préventives et le provisionnement intelligent, consultez le *Manuel d'administration de CA Identity Manager*.

# Transformation des données du référentiel d'utilisateurs

Dans certains cas, vous pouvez vouloir transformer des données avant de les stocker dans le référentiel d'utilisateurs. Par exemple, vous pouvez stocker des informations dans un format différent ou vous pouvez appliquer des modifications lorsque certains types d'informations sont présents.

CA Identity Manager inclut les fonctionnalités suivantes pour la transformation des données :

- Stratégies d'identité
- Gestionnaires d'attributs logiques

**Remarque :** Vous pouvez également utiliser des stratégies d'identité et des gestionnaires d'attributs logiques pour implémenter la logique métier personnalisée.

## Gestionnaires d'attributs logiques

Les gestionnaires d'attributs logiques sont des fonctionnalités Java personnalisées qui transforment les valeurs d'attribut d'utilisateur utilisées dans les fenêtres de tâche CA Identity Manager. Ces gestionnaires vous permettent de contrôler l'affichage d'un attribut physique dans une fenêtre de tâche. Ils vous permettent également de transformer une valeur d'affichage, comme le coût, dans la fenêtre de tâche en un ou plusieurs attributs physiques, comme le prix unitaire et la quantité, qui sont stockés dans le référentiel d'utilisateurs.

**Remarque :** Pour plus d'informations sur les gestionnaires d'attributs logiques, reportez-vous au manuel *Programming Guide for Java*.

# Application de la logique métier personnalisée

Vous pouvez personnaliser CA Identity Manager pour implémenter la logique métier requise par votre société. CA Identity Manager inclut les options suivantes pour implémenter la logique métier personnalisée :

- Stratégies d'identité : vous pouvez utiliser des stratégies d'identité pour définir un ensemble de modifications métier qui ont lieu lorsqu'un utilisateur satisfait à une certaine condition ou règle. Par exemple, les stratégies d'identité permettent d'automatiser certaines tâches de gestion d'identité, comme l'affectation de rôles, ou d'appliquer des règles métier, pour empêcher par exemple les utilisateurs de signer et d'approuver des chèques supérieurs à 20 000€.

  **Remarque :** Pour plus d'informations sur les stratégies d'identité, consultez le *Manuel d'administration*.

- Gestionnaires d'attributs logiques : vous pouvez associer ces gestionnaires à des fenêtres de tâche CA Identity Manager pour contrôler l'affichage et les modifications des valeurs d'attribut.

  Pour plus d'informations, reportez-vous au *manuel de programmation Java (en anglais).*

- Gestionnaires de tâches métier : vous permettent d'exécuter la logique métier personnalisée, pendant les opérations de validation de données pour une tâche CA Identity Manager, comme suit.

  - Application des règles métier personnalisées. Par exemple, vous n'autoriser pas un administrateur à gérer plus de cinq groupes.
  - Validation des champs de fenêtre de tâche du client. Par exemple, la valeur d'un champ ID d'employé doit exister dans la base de données de ressources humaines principale.

  Vous pouvez implémenter les gestionnaires de tâches métier en Java ou en JavaScript.

  **Remarque :** Pour plus d'informations, reportez-vous au manuel *Programming Guide for Java*.

- Flux de travaux : vous permet de créer les définitions de processus personnalisées qui sont associées à un événement CA Identity Manager.

**Remarque :** Avant de décider d'implémenter la logique métier dans un gestionnaire de tâches métier ou un processus de flux de travaux, consultez les sections suivantes :

- Remarques sur le gestionnaire de tâches métier (page 29)
- Remarques sur le processus de flux de travaux (page 29)

## Remarques sur le gestionnaire de tâches métier

Les gestionnaires de tâches métier effectuent la validation de la logique métier pendant la phase de traitement synchrone de la tâche, qui se produit avant la génération d'événements. Cela vous permet de :

- Configurer la validation de niveau tâche. Par exemple, vous pouvez ajouter ou supprimer des membres d'un groupe en fonction de l'emplacement de leur bureau, spécifié dans la fenêtre de profil d'utilisateur.
- Empêcher une tâche d'être soumise en cas d'échec de la validation.
- Transformer automatiquement toutes les informations d'une fenêtre de tâche pour s'assurer de leur conformité aux processus métier avant la soumission de la tâche.

**Remarque :** N'implémentez pas les activités qui mettent trop longtemps à se terminer dans un gestionnaire de tâches métier. Ce type d'activité retarde la soumission de la tâche et n'est pas adapté à la phase synchrone dans laquelle l'utilisateur intervient. A la place, utilisez un processus de flux de travaux, qui s'exécute pendant la phase asynchrone de la tâche.

## Remarques sur le processus de flux de travaux

Les processus de flux de travaux sont appelés pendant la phase asynchrone de la tâche et sont associés à l'exécution d'événements individuels. Cela vous permet de :

- Exécuter des activités d'approbation selon les données d'événement.
- Exécuter des longues activités de logique métier personnalisées.

L'API de flux de travaux vous permet d'obtenir des données de niveau de tâche à partir d'une activité de flux de travaux et vous opérez en général dans le contexte de l'événement inclus dans le flux de travaux.

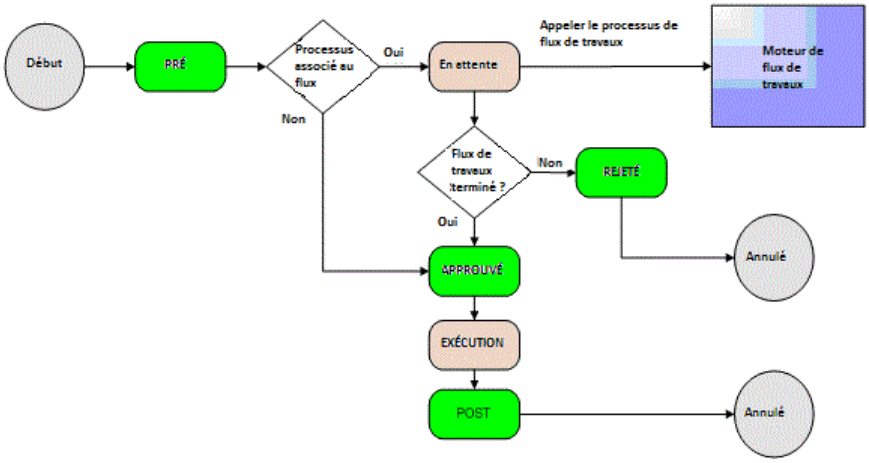
# Approbation des modifications métier

Le flux de travaux décrit un processus qui consiste en une ou plusieurs opérations qui doivent être effectuées afin de remplir certains objectifs métier, comme l'exécution d'une procédure d'embauche ou l'obtention du risque client d'un utilisateur à partir d'un système externe. En général, l'une des étapes d'un flux de travaux implique l'approbation ou le rejet de la modification métier.

Dans CA Identity Manager, un processus de flux de travaux est associé à un événement, une action qui se produit pendant le traitement de la tâche. Lorsqu'un événement entre dans l'état En attente dans son cycle de vie, CA Identity Manager appelle un processus de flux de travaux associé et met en pause l'exécution de l'événement jusqu'à ce que le processus se termine. CA Identity Manager effectue alors la tâche ou la rejette selon les résultats de ce processus.

Cette séquence est illustrée dans le diagramme suivant :

**Traitement du flux de travaux et cycle de vie des événements**




CA Identity Manager comprend le moteur de flux de travaux InSession WorkPoint pour la création et la gestion des processus de flux de travaux.

**Remarque :** Pour plus d'informations, reportez-vous au *manuel d'administration*.

# Chapitre 3: Architecture CA Identity Manager

Ce chapitre traite des sujets suivants :



## Composants CA Identity Manager

Une implémentation CA Identity Manager peut inclure les composants suivants :

- Serveurs
- Référentiels d'utilisateur
- Bases de données
- Connecteurs

### Serveurs

Une implémentation CA Identity Manager inclut un ou plusieurs types de serveurs, selon la fonctionnalité dont vous avez besoin.

**Serveur CA Identity Manager (requis)**

Exécute les tâches de CA Identity Manager. L'application CA Identity Manager J2EE inclut la console de gestion et la console d'utilisateur.

**Serveur de provisionnement CA Identity Manager**

Gère les comptes sur des systèmes d'extrémité.

Ce serveur est requis si l'installation CA Identity Manager prend en charge le provisionnement de comptes.

**Remarque :** Avant d'installer le serveur de provisionnement, assurez-vous de disposer d'un annuaire de provisionnement installé à distance sur un serveur CA Directory, ou localement dans le cadre d'un environnement de test uniquement.

**Serveur de stratégies SiteMinder**

Fournit l'authentification avancée pour CA Identity Manager et l'accès aux fonctionnalités SiteMinder, comme les services de mot de passe et l'authentification unique.

Ce serveur est facultatif.

## Référentiel d'utilisateurs et annuaire de provisionnement

CA Identity Manager utilise deux référentiels d'utilisateurs :

- Le *référentiel d'utilisateurs CA Identity Manager*, c'est-à-dire le référentiel d'utilisateurs géré par CA Identity Manager. En général, il s'agit d'un référentiel existant qui contient les identités d'utilisateur qu'une société doit gérer.

  Le référentiel d'utilisateurs peut être un annuaire LDAP ou une base de données relationnelles.

  Dans la console de gestion, vous créez un objet d'annuaire CA Identity Manager pour permettre la connexion au référentiel d'utilisateurs et décrire les objets du référentiel géré par CA Identity Manager.

- L'*annuaire de provisionnement*, c'est-à-dire le référentiel d'utilisateurs géré par le serveur de provisionnement.

  Il s'agit d'une instance de CA Directory incluant des utilisateurs globaux, qui associe des utilisateurs de l'annuaire de provisionnement avec des comptes sur des terminaux comme Microsoft Exchange, Active Directory ou SAP.

  Seuls certains utilisateurs CA Identity Manager disposent d'un utilisateur global correspondant. Lorsqu'un utilisateur CA Identity Manager reçoit un rôle de provisionnement, le serveur de provisionnement crée un utilisateur global.

## Séparation du référentiel d'utilisateurs et des annuaires de provisionnement

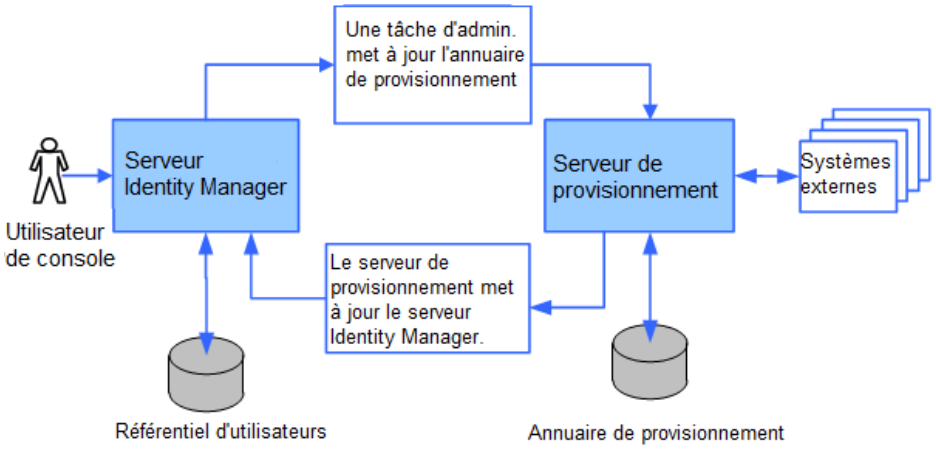
L'illustration suivante présente un référentiel d'utilisateurs et un annuaire de provisionnement distinct, qui correspondent au scénario pris en charge pour une nouvelle installation de CA Identity Manager. Notez que dans cette illustration :

- Un administrateur CA Identity Manager utilise une tâche d'administration qui modifie un utilisateur dans le référentiel d'utilisateurs, ce qui affecte l'annuaire de provisionnement.

  Cette modification peut également mettre à jour un terminal, tel qu'un serveur de messagerie, qui a un connecteur au serveur de provisionnement.

  Une modification effectuée dans le serveur de provisionnement, ou sur un terminal avec un connecteur au serveur de provisionnement, met à jour le référentiel d'utilisateurs CA Identity Manager et l'annuaire de provisionnement.

Par exemple, un terminal, comme une application de ressources humaines, peut mettre à jour les adresses électroniques des utilisateurs.




# Bases de données

CA Identity Manager utilise des sources de données pour la connexion aux bases de données qui stockent les informations requises pour prendre en charge la fonctionnalité CA Identity Manager. Ces bases de données peuvent résider dans une instance physique unique d'une base de données ou dans des instances distinctes.

**Base de données d'objet (requise)**

Contient des informations sur la configuration de CA Identity Manager.

**Base de données de persistance des tâches (requise)**

Conserve les informations relatives aux activités CA Identity Manager et aux événements associés dans le temps. Cela permet au système de suivre de façon précise les activités CA Identity Manager, même si vous redémarrez le serveur CA Identity Manager.

**Base de données d'archives (requise)**

Données d'archives de la base de données de persistance des tâches.

**Base de données de flux de travaux**

Enregistre les définitions, les jobs, les scripts et d'autres données de processus de flux de travaux requises par le moteur de flux de travaux.

**Base de données d'audit**

Fournit un enregistrement sous forme d'historique des opérations réalisées dans un environnement CA Identity Manager.

**Remarque :** Vous pouvez configurer la quantité et le type d'informations stockées par CA Identity Manager dans la base de données d'audit. Pour plus d'informations, reportez-vous au *manuel de configuration*.

**Base de données de rapports**

Enregistre les données de cliché, qui reflètent l'état actuel des objets dans CA Identity Manager au moment de la prise du cliché. Vous pouvez générer des rapports à partir de ces informations pour afficher la relation entre les objets, comme les utilisateurs et les rôles.

Lorsque vous utilisez le programme d'installation, CA Identity Manager configure une connexion à une base de données unique, appelée base de données CA Identity Manager, qui contient les tables pour chaque type de base de données.

**Remarque :** Vous pouvez créer un référentiel de données pour la persistance des tâches, les flux de travaux, les audits ou les rapports dans une base de données distincte et configurer CA Identity Manager pour s'y connecter. Pour plus d'informations, reportez-vous au *Manuel d'installation*.

## Composants de connecteur

Un connecteur est l'interface logicielle d'un terminal. Le serveur de provisionnement utilise le connecteur pour communiquer avec le terminal. Cela permet de convertir les actions du serveur de provisionnement en modifications concrètes sur le terminal, comme par exemple la création d'un compte de messagerie sur un terminal Microsoft Exchange.

Les terminaux peuvent être des stations de travail UNIX, des PC Windows ou une application de messagerie comme Microsoft Exchange.

## Serveurs de connecteurs

Un serveur de connecteurs est un composant du serveur de provisionnement qui gère les connecteurs. Vous pouvez l'installer sur le système du serveur de provisionnement ou sur un système distant.

Un serveur de connecteurs utilise plusieurs terminaux. Par exemple, si vous avez plusieurs stations de travail UNIX, vous pouvez définir un serveur de connecteurs pour gérer tous les connecteurs qui gèrent des comptes UNIX. Un autre serveur de connecteurs peut gérer tous les connecteurs qui demandent des comptes Windows.

Le serveur de connecteurs distribué fonctionne avec plusieurs serveurs de connecteurs. Cela permet d'équilibrer la charge lorsqu'un serveur de connecteurs est occupé et fournit une haute disponibilité lorsqu'un serveur de connecteurs est hors service.

Il existe deux types de serveurs de connecteurs.

- Le serveur de connecteurs CA IAM (CA IAM CS) gère les connecteurs écrits en Java.
- Le serveur de connecteurs C++ gère les connecteurs écrits en C++.

### Serveur de connecteurs C++

Le serveur de connecteurs *C++* est un serveur de connecteurs qui gère les connecteurs C++. Vous pouvez l'installer sur le serveur de provisionnement ou sur un système distant. Le serveur de connecteurs C++ fournit une structure d'application orientée objets qui simplifie le développement de connecteurs, qui sont responsables des communications entre le serveur de connecteurs C++ et le terminal.

## CA IAM CS

CA IAM CS est un composant de serveur qui gère les connecteurs Java, leur hébergement et leur routage. CA IAM CS fournit une alternative Java au serveur de connecteurs C++. Il est architecturalement et fonctionnellement similaire au serveur de connecteurs C++, si ce n'est qu'il a une API Java au lieu d'une API C++ et permet à vos connecteurs d'être implémenté en Java. De plus, CA IAM CS est orienté données plutôt que code, ce qui permet au conteneur (ou CA IAM CS) de résoudre plus de fonctionnalités que les connecteurs mêmes.

Le serveur de provisionnement gère le provisionnement d'utilisateurs, puis délègue aux connecteurs la gestion des groupes et des comptes de terminal à l'aide du serveur de connecteurs C++ ou de CA IAM CS.

## Connecteurs et agents

Les connecteurs CA Identity Manager font partie de l'architecture de serveur de provisionnement et communiquent avec les systèmes gérés dans votre environnement. Un connecteur agit comme une passerelle vers une technologie de système de type terminal native. Par exemple, vous pouvez gérer des ordinateurs exécutant des services Active Directory uniquement si le connecteur ADS est installé sur un serveur de connecteurs avec lequel le serveur de provisionnement peut communiquer. Les connecteurs gèrent les objets qui résident sur les systèmes. Les objets gérés incluent des comptes, des groupes et des objets de type terminal.

Les connecteurs sont installés sur le serveur de connecteurs et certains composants sont installés sur le serveur de provisionnement (par exemple, à l'aide du module d'extension de serveur) ou sur le gestionnaire de provisionnement (modules d'extension d'interface utilisateur).

Certains connecteurs requièrent un agent sur les systèmes qu'ils gèrent pour effectuer le cycle de communication, auquel cas, vous pouvez les installer à l'aide du programme d'installation de provisionnement. Les agents peuvent être divisés selon les catégories suivantes :

Agents distants

Ces agents sont installés sur les systèmes d'extrémité gérés.

Agents d'environnement

Ces agents sont installés sur des systèmes, comme CA ACF2, CA Top Secret et RACF.

Certains composants fonctionnent sur UNIX et Windows, y compris les options de serveur du connecteur C++ suivantes :

- UNIX (ETC, NIS)
- Connecteur CA Access Control

  **Remarque :** Le connecteur CA Access Control pour UNIX peut gérer uniquement les terminaux de connecteur CA Access Control sur UNIX. Le connecteur CA Access Control pour Windows est requis pour gérer les terminaux de connecteur CA Access Control sur Windows, mais peut également les gérer sur UNIX.
- CA ACF2
- RACF
- CA Top Secret

L'accès aux autres connecteurs de serveur C++ peut être effectué à partir du serveur de provisionnement Solaris en utilisant la structure de serveurs de connecteurs. La structure de serveurs de connecteurs permet à un serveur de provisionnement Solaris de communiquer avec des connecteurs Windows.

**Remarque :** La structure de serveurs de connecteurs doit être exécutée sur Windows pour permettre l'utilisation des connecteurs.

## Connector Xpress

Connector Xpress est un utilitaire CA Identity Manager pour la gestion des connecteurs dynamiques, leur mappage vers des terminaux et la définition de règles de routage pour les terminaux. Vous pouvez l'utiliser pour configurer des connecteurs dynamiques pour permettre le provisionnement et la gestion des bases de données SQL et des annuaires LDAP.

Connector Xpress vous permet de créer et de déployer des connecteurs personnalisés sans devoir faire appel aux compétences techniques généralement requises lors de la création de connecteurs gérés par le gestionnaire de provisionnement.

Vous pouvez également configurer, modifier et supprimer une configuration de serveur de connecteurs (Java et C++) à l'aide de Connector Xpress.

Les informations principales à saisir dans Connector Xpress concernent le schéma natif d'un système d'extrémité. Par exemple, vous pouvez utiliser Connector Xpress pour vous connecter à un SGBDR et pour récupérer le schéma SQL de la base de données. Vous pouvez alors utiliser Connector Xpress pour créer des mappages à partir des parties du schéma natif relatives à la gestion d'identité et au provisionnement. Un mappage décrit la représentation d'un élément du schéma natif par la couche de provisionnement.

Connector Xpress génère des métadonnées qui décrivent à un connecteur dynamique les mappages d'exécution sur un système cible.

La sortie de Connector Xpress est un document de métadonnées généré lors de la configuration des mappages. Les métadonnées sont regroupées dans un fichier XML qui décrit la structure du connecteur à CA IAM CS.

Il décrit les classes de serveur de provisionnement, les attributs et leur mappage au schéma natif.

Les métadonnées sont utilisées pour créer des types de terminal dynamiques sur un ou plusieurs serveurs de provisionnement.

**Remarque :** Pour plus d'informations sur l'utilisation de Connector Xpress, consultez le Manuel *Connector Xpress Guide* dans la *bibliothèque CA Identity Manager*.

# Composants supplémentaires

CA Identity Manager inclut plusieurs composants supplémentaires, qui prennent en charge la fonctionnalité CA Identity Manager. Certains de ces composants sont installés avec CA Identity Manager et d'autres doivent être installés séparément.

## Flux de travaux WorkPoint

Le moteur de flux de travaux WorkPoint et Workpoint Designer sont installés automatiquement lors de l'installation de CA Identity Manager.

Ces composants vous permettent de placer une tâche CA Identity Manager sous le contrôle du flux de travaux et de modifier les définitions de processus de flux de travaux existantes ou de créer de nouvelles définitions.

**Remarque :** Pour plus d'informations sur les flux de travaux, reportez-vous au *Manuel d'administration*.

## Gestionnaire de provisionnement

Le gestionnaire de provisionnement CA Identity Manager gère le serveur de provisionnement à l'aide d'une interface graphique. Ce gestionnaire est utilisé pour des tâches administratives comme la gestion des options du serveur de provisionnement. Dans certains cas, vous pouvez également l'utiliser pour gérer certains attributs de terminal, que vous ne pouvez pas gérer dans la console d'utilisateur CA Identity Manager.

Le gestionnaire de provisionnement fait partie des outils d'administration de CA Identity Manager.

**Remarque :** Cette application s'exécute sur les systèmes Windows uniquement.

Pour plus d'informations sur le gestionnaire de provisionnement, reportez-vous au manuel *Provisioning Reference Guide*.

### Serveur de rapports CA IAM

CA Identity Manager fournit des rapports que vous pouvez utiliser pour surveiller le statut d'un environnement CA Identity Manager. Pour utiliser ces rapports, installez le serveur de rapports CA IAM, qui est inclus avec CA Identity Manager.

Le serveur de rapports CA IAM est basé sur BusinessObjects Enterprise XI. Si vous disposez d'un serveur BusinessObjects existant, vous pouvez l'utiliser pour générer des rapports CA Identity Manager à la place du serveur de rapports CA IAM.

**Remarque :** Pour obtenir des instructions sur l'installation, consultez le *Manuel d'installation*.

## Exemples d'installation de CA Identity Manager

CA Identity Manager vous permet de contrôler les identités des utilisateurs et leur accès aux applications et aux comptes sur des systèmes d'extrémité. Selon la fonctionnalité dont vous avez besoin, vous sélectionnez les composants CA Identity Manager à installer.

Dans toutes les installations CA Identity Manager, le serveur CA Identity Manager est installé sur un serveur d'applications. Vous utilisez le programme d'installation CA Identity Manager pour installer les autres composants dont vous avez besoin.

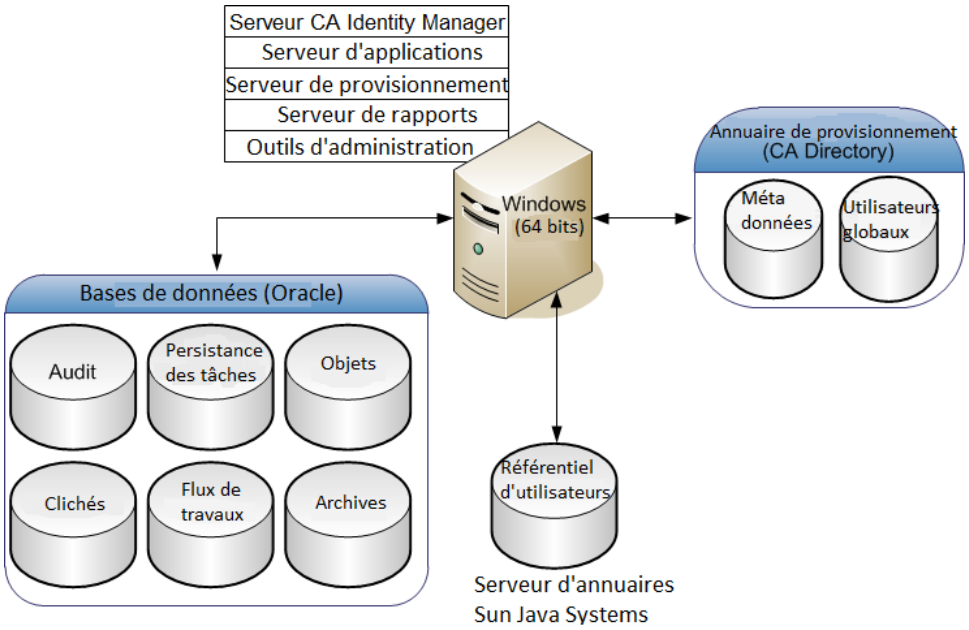
Les sections suivantes fournissent plusieurs exemples généraux d'implémentations de CA Identity Manager.

### Installation avec des composants de provisionnement

Le provisionnement de CA Identity Manager vous permet de créer un environnement qui se connecte à un serveur de provisionnement afin de provisionner des comptes sur différents systèmes d'extrémité. Vous pouvez affecter des rôles de provisionnement à des utilisateurs que vous créez à partir de CA Identity Manager. Les rôles de provisionnement sont des rôles comprenant des modèles de compte, qui définissent des comptes que les utilisateurs peuvent recevoir sur des systèmes d'extrémité. Les comptes permettent aux utilisateurs d'accéder à des ressources supplémentaires, comme un compte de messagerie.

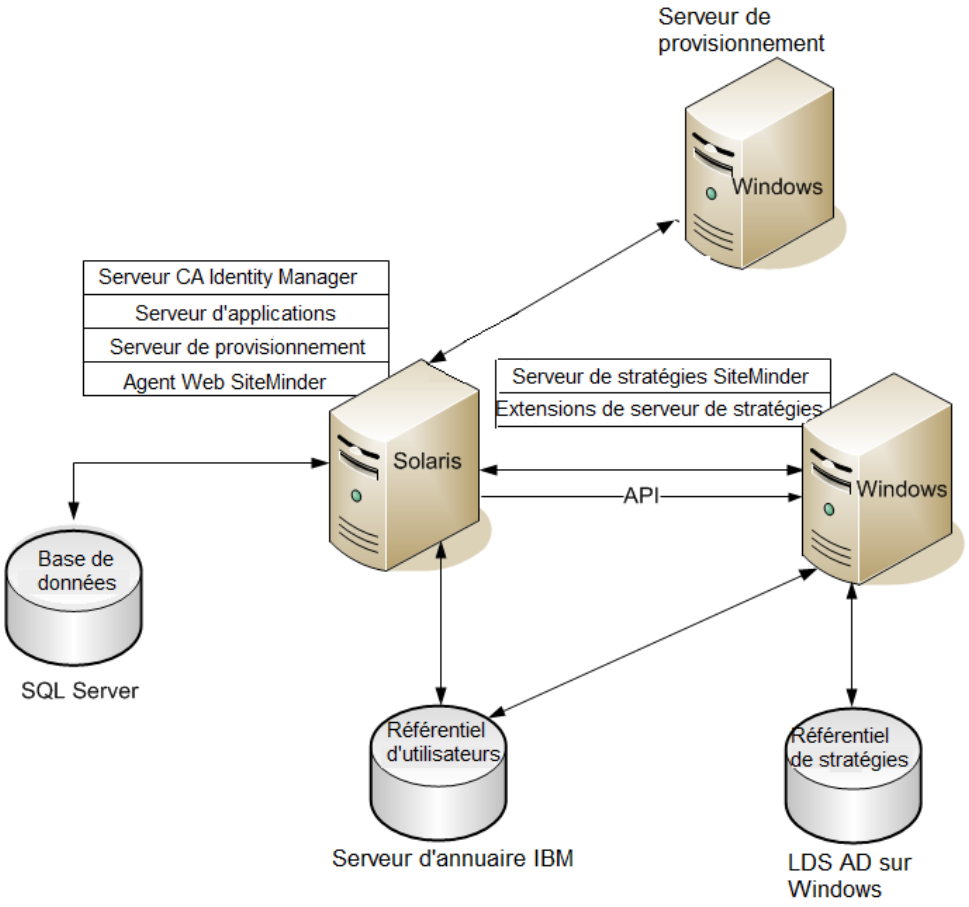
Lorsque vous affectez un rôle de provisionnement à un utilisateur, il reçoit les comptes définis par les modèles de compte dans le rôle. Les modèles de compte définissent également la manière dont les attributs d'utilisateurs sont mappés aux comptes. Les comptes sont créés dans les terminaux gérés définis par les modèles de compte.

L'illustration suivante est un exemple d'installation CA Identity Manager avec provisionnement :



## Installation avec un serveur de stratégies SiteMinder

Un serveur de stratégies SiteMinder fournit une authentification et une protection avancée pour l'environnement CA Identity Manager. L'illustration suivante est un exemple d'installation CA Identity Manager avec un serveur de stratégies SiteMinder :




Une implémentation CA Identity Manager incluant SiteMinder comprend tous les composants de l'installation de base ou de l'installation avec provisionnement, plus les composants supplémentaires suivants :

**Agent Web SiteMinder**

Utilisé avec le serveur de stratégies SiteMinder pour protéger la console d'utilisateur. L'agent Web est installé sur le système comprenant le serveur CA Identity Manager.

**Serveur de stratégies SiteMinder**

Fournit une fonctionnalité d'authentification et d'autorisation avancée pour CA Identity Manager et d'autres fonctionnalités comme les services de mot de passe et l'authentification unique.

**Extensions pour le serveur de stratégies SiteMinder**

Permet à un serveur de stratégies SiteMinder de prendre en charge CA Identity Manager. Installez les extensions sur chaque système de serveur de stratégies SiteMinder dans votre implémentation CA Identity Manager.

**Référentiel de stratégies SiteMinder**

Stocke les informations requises par SiteMinder pour gérer l'accès aux ressources Web.

Lorsque CA Identity Manager est intégré à SiteMinder, le référentiel de stratégies inclut également des informations sur les annuaires et les environnements CA Identity Manager pour que SiteMinder permette l'authentification avancée.

**Remarque :** Les composants sont installés sur des plates-formes différentes à des fins d'exemple. Toutefois, vous pouvez choisir d'autres plates-formes. Les bases de données CA Identity Manager se trouvent sur le serveur Microsoft SQL Server et le référentiel d'utilisateurs se trouve sur le serveur d'annuaire IBM. Le référentiel de stratégies SiteMinder se trouve sur le serveur AD LDS Windows.

# Chapitre 4: Planification de l'implémentation

Planifier une implémentation CA Identity Manager consiste à déterminer la méthode utilisée par CA Identity Manager pour gérer les utilisateurs et la fonctionnalité dont vous avez besoin pour réaliser vos objectifs métier. Les points à considérer sont les suivants :

- Quelle méthode de gestion des utilisateurs appliquer ?
- Le provisionnement des comptes est-il nécessaire ?
- Quels sont les besoins métiers personnalisés et un flux de travaux est-il nécessaire à leur implémentation ?

Les réponses que vous apportez à ces questions vous permettent de déterminer la meilleure façon d'implémenter CA Identity Manager dans votre environnement.

Ce chapitre traite des sujets suivants :



## Détermination des éléments à gérer

Déterminer les éléments à gérer vous permettra de décider des composants à installer. CA Identity Manager vous permet de gérer les éléments suivants :

- Identités d'utilisateur
- Accès aux comptes sur des systèmes d'extrémité.

### Identités d'utilisateur

Les identités d'utilisateur représentent les personnes qu'une société doit gérer, comme les employés, les prestataires, les fournisseurs, etc.

Pour gérer les identités d'utilisateur, vous devez installer uniquement le serveur CA Identity Manager et les outils d'administration.

## Configuration de la prise en charge de la gestion des utilisateurs

Dans CA Identity Manager, vous gérez des utilisateurs à l'aide de rôles d'administration, qui déterminent les tâches CA Identity Manager que les administrateurs peuvent effectuer.

**Remarque :** Avant d'implémenter la gestion des utilisateurs dans CA Identity Manager, déterminez les fonctionnalités dont vous avez besoin et planifiez (page 60) l'implémentation progressive de ces fonctionnalités.

Pour configurer la prise en charge de la gestion des utilisateurs, effectuez les opérations principales suivantes :

1. Installez le serveur et les outils d'administration CA Identity Manager.

   Si vous devez provisionner des comptes pour des utilisateurs gérés, vous devrez également installer la prise en charge du provisionnement (page 45).

   **Remarque** : Pour plus d'informations, consultez le *Manuel d'installation*.

2. Dans la console de gestion CA Identity Manager, créez les éléments suivants :

   - **Annuaire CA Identity Manager**

     Décrit un référentiel d'utilisateurs dans CA Identity Manager. Elle contient :

     - Un pointeur vers un référentiel d'utilisateurs, qui stocke les objets gérés, comme les utilisateurs, les groupes et les organisations.
     - Des métadonnées qui décrivent la façon dont les objets gérés sont stockés dans l'annuaire et représentés dans CA Identity Manager.

   - **Environnement CA Identity Manager**

     Fournit un espace de noms de gestion qui permet aux administrateurs CA Identity Manager de gérer des objets, comme les utilisateurs, les groupes et les organisations, avec un ensemble de rôles et de tâches associé. L'environnement CA Identity Manager contrôle la gestion et la présentation graphique d'un annuaire.

   Pour plus d'informations sur les annuaires et les environnements CA Identity Manager, consultez le *Manuel de configuration*.

3. Modifiez les rôles et les tâches d'administration par défaut pour répondre aux besoins métier.

   Les modifications de rôle incluent l'ajout ou la suppression des tâches par défaut des rôles d'administration existants, ou la création de nouveaux rôles d'administration basés sur les rôles par défaut.

Les modifications de tâche incluent la personnalisation des onglets de profil d'utilisateur par défaut pour inclure uniquement les informations à gérer. Les onglets de profil par défaut incluent tous les attributs qui sont définis pour des utilisateurs.

Pour plus d'informations sur la modification des rôles et des tâches d'administration par défaut, consultez le *Manuel de conception de la console d'utilisateur*.

4. Affectez les rôles d'administration à des utilisateurs qui effectueront les tâches de gestion des utilisateurs.

## Provisionnement de comptes à partir d'autres applications

La décision d'implémenter le provisionnement dépend du type d'informations que vous devez gérer. Si vous gérez un annuaire d'utilisateurs central et que vous ne voulez pas gérer de comptes d'utilisateurs dans d'autres systèmes, vous n'avez pas besoin du provisionnement. Si vous voulez gérer des comptes d'utilisateurs sur différents systèmes, vous devez implémenter la prise en charge du provisionnement.

Les fonctionnalités de provisionnement sont fournies par le serveur de provisionnement, qui est intégré à CA Identity Manager. Le serveur de provisionnement comprend les fonctionnalités suivantes pour le provisionnement de comptes :

- Gestion des terminaux
- Synchronisation des comptes
- Modèles de compte
- Fonctionnalités d'exploration et de corrélation

**Remarque :** Les informations de provisionnement sont stockées dans un annuaire de provisionnement. Si CA Identity Manager utilise un autre type d'annuaire, votre déploiement devra inclure un référentiel d'utilisateurs et un annuaire de provisionnement CA Identity Manager.

## Gestion des terminaux

Pour provisionner des comptes, vous définissez et gérez des terminaux dans la console d'utilisateur CA Identity Manager. Un *terminal* est un système pour lequel les utilisateurs requièrent un accès. Les terminaux peuvent être des bases de données Oracle, des serveurs NIS UNIX, des serveurs Windows et des serveurs Microsoft Exchange. Utilisez des *modèles de compte* (page 46) pour créer des comptes et déterminer les capacités des utilisateurs sur les terminaux gérés.

**Remarque :** Vous pouvez également utiliser le gestionnaire de provisionnement pour définir et gérer des terminaux. Bien qu'il soit recommandé d'utiliser la console d'utilisateur pour la plupart des tâches de gestion des terminaux, certaines tâches requièrent l'utilisation du gestionnaire de provisionnement, comme la gestion de certains attributs de terminal et des objets de terminal autres que les comptes. Pour plus d'informations sur le gestionnaire de provisionnement, reportez-vous au manuel *Provisioning Reference Guide*.

## Synchronisation des comptes

Vous pouvez synchroniser des comptes d'utilisateurs sur plusieurs terminaux gérés. Lorsque la synchronisation de comptes est activée, une modification apportée à un profil d'utilisateur dans le serveur de provisionnement est propagée à tous les terminaux sur lesquels l'utilisateur a un compte.

**Remarque :** Vous spécifiez les paramètres de synchronisation de comptes dans l'onglet Profil pour une tâche CA Identity Manager. Pour plus d'informations sur la configuration de la synchronisation de comptes, reportez-vous au *Manuel d'administration*.

## Modèles de compte

Les modèles de compte définissent la représentation d'un utilisateur dans un terminal géré. Par exemple, un modèle pour un compte Exchange peut définir le format de l'adresse électronique d'un utilisateur, comme <première_initiale><nom>@mycompany.com.

Les modèles de compte déterminent également les droits de gestion d'un utilisateur sur un système géré. Par exemple, en plus de définir le format d'une adresse électronique, un modèle pour un compte Exchange peut également limiter la taille de la boîte aux lettres d'un utilisateur.

Vous créez et gérez des modèles de compte dans la console d'utilisateur.

## Fonctionnalités d'exploration et de corrélation

Les fonctionnalités d'exploration et de corrélation simplifient la gestion des terminaux en permettant la détection et la synchronisation des modifications sur les systèmes gérés.

La fonctionnalité d'exploration permet de rechercher des objets, y compris des comptes, dans des terminaux et de stocker leurs références dans l'annuaire de provisionnement. Vous pouvez utiliser la fonctionnalité d'exploration pour détecter tous les nouveaux objets à gérer. Par exemple, si vous provisionnez des comptes dans un annuaire LDAP et que de nouvelles organisations sont ajoutées à cet annuaire, vous pouvez utiliser la fonctionnalité d'exploration pour permettre l'utilisation de ces organisations dans des modèles de compte.

La fonctionnalité de corrélation associe un compte dans un terminal géré avec un utilisateur global dans l'annuaire de provisionnement. Lorsqu'une modification est apportée au compte sur le terminal, la fonctionnalité de corrélation peut synchroniser ces modifications avec le compte d'utilisateur global.

**Remarque :** Pour plus d'informations sur les fonctionnalités d'exploration et de corrélation, consultez le *Manuel d'administration*.

## Configuration de la prise en charge du provisionnement

Après avoir décidé d'implémenter le provisionnement, effectuez les opérations principales suivantes.

1. Utilisez le programme d'installation de serveur CA Identity Manager pour installer le serveur CA Identity Manager, le serveur de provisionnement, l'initialisation d'annuaire de provisionnement et les outils d'administration.

   **Remarque :** Pour plus d'informations sur l'installation des composants CA Identity Manager, reportez-vous au *Manuel d'installation*.

2. Configurez le gestionnaire de provisionnement de manière à ce qu'il se connecte au serveur CA Identity Manager.

3. Configurez le provisionnement dans la console de gestion CA Identity Manager :

   a. Activez le provisionnement.

   b. Configurez un environnement de provisionnement en effectuant les opérations suivantes :

      - Importation des définitions de rôle personnalisées
      - Configuration d'un administrateur entrant
      - Connexion de l'environnement au serveur de provisionnement

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

4. Créez des terminaux dans la console d'utilisateur.

   Cela permet à CA Identity Manager de gérer le terminal.

   **Remarque :** Pour plus d'informations sur la gestion des terminaux, consultez le *Manuel d'administration*.

5. Explorez le terminal et effectuez une corrélation.

   Lorsque vous explorez un terminal, CA Identity Manager recherche les objets qui s'y trouvent et stocke les instances correspondantes dans l'annuaire de provisionnement. Cette opération remplit l'annuaire de provisionnement avec les comptes et d'autres objets appartenant au terminal.

   Lorsque vous établissez une corrélation entre des comptes et un terminal, CA Identity Manager les associe avec un utilisateur global de l'annuaire de provisionnement. Vous pouvez choisir si la fonction de corrélation crée les utilisateurs globaux qui ne sont pas présents ou si elle associe les comptes sans utilisateur global associé à l'utilisateur global par défaut.

6. Créez et gérez des comptes de terminal à l'aide des modèles de compte, qui contiennent les attributs utilisés pour la création de comptes.

7. Associez les modèles de compte à des rôles de provisionnement.

   Lorsque vous affectez des rôles de provisionnement à des utilisateurs, CA Identity Manager crée des comptes dans les terminaux associés pour ces utilisateurs.

   **Remarque :** Pour plus d'informations sur les modèles de comptes et les rôles de provisionnement, reportez-vous au *Manuel d'administration*.

# Détermination des conditions d'audit

CA Identity Manager inclut des fonctionnalités d'audit qui vous permettent de surveiller les activités d'un environnement CA Identity Manager.

Ces informations sont stockées dans une base de données d'audit. La quantité et le type d'informations stockées dans la base de données d'audit est configurable.

Vous affichez les données d'audit dans la console d'utilisateur à l'aide de la tâche Afficher les tâches soumises. Cette tâche permet aux administrateurs de rechercher et d'afficher les tâches exécutées dans le système. Les administrateurs peuvent afficher des informations sur les tâches à un niveau général ou afficher les détails des tâches et des événements.

# Remarques sur l'audit CA Identity Manager

Les données d'audit contiennent un enregistrement sous forme d'historique des opérations réalisées dans un environnement CA Identity Manager. Pour auditer les données dans CA Identity Manager, les éléments suivants sont requis :

- Une base de données d'audit
- Un fichier de paramètres d'audit

## Base de données d'audit

Lorsque vous utilisez le programme d'installation, CA Identity Manager configure une connexion à une base de données unique, appelée base de données CA Identity Manager, et crée une source de données qui se connecte aux tables de la base de données à auditer.

**Remarque :** La base de données CA Identity Manager inclut également des données qui sont utilisées par d'autres fonctionnalités CA Identity Manager, notamment la persistance des tâches, les flux de travaux et la génération de rapports. A des fins de modularité, vous pouvez créer une nouvelle instance d'une base de données à auditer.

**Remarque :** Pour plus d'informations sur la base de données d'audit, consultez le *Manuel d'installation*.

## Paramètres d'audit

Vous configurez des paramètres d'audit dans un fichier de paramètres d'audit. Un fichier de paramètres d'audit détermine la quantité et le type des informations auditées par CA Identity Manager. Vous pouvez configurer un fichier de paramètres d'audit pour :

- Activer l'audit pour un environnement CA Identity Manager.
- Activer l'audit pour les événements CA Identity Manager générés par les tâches d'administration.
- Enregistrer les informations d'événement correspondant à un état, par exemple, lorsqu'un événement se termine ou est annulé.
- Journaliser les informations sur les attributs impliqués dans un événement. Par exemple, vous pouvez journaliser les attributs modifiés au cours d'un événement ModifyUserEvent.
- Définir le niveau d'audit pour la journalisation d'attribut.

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

## Remarques sur CA Audit

CA Audit est un système de gestion d'audit qui vous permet de collecter et de stocker les données liées à la sécurité pour l'audit, la génération de rapports, la vérification de conformité et la surveillance d'événements.

Pour configurer l'intégration à CA Audit, installez le composant iRecorder lors de l'installation du serveur CA Identity Manager. iRecorder récupère les événements de CA Identity Manager. Selon les stratégies du gestionnaire de stratégies CA Audit, iRecorder ignore les événements ou les envoie vers CA Audit.

# Conditions requises pour le référentiel d'utilisateurs

Une implémentation CA Identity Manager doit inclure un référentiel d'utilisateurs qui contient les identités des utilisateurs gérés par CA Identity Manager. En général, il s'agit d'un référentiel d'utilisateurs existant qu'une entreprise utilise pour stocker les informations relatives aux utilisateurs, tels que les employés et les clients.

Si votre implémentation inclut le provisionnement, CA Identity Manager requiert également un annuaire de provisionnement qui inclut des utilisateurs globaux associés à des comptes sur des terminaux, comme Microsoft Exchange, Active Directory et Oracle.

## Gestion de plusieurs référentiels d'utilisateur

Une entreprise peut avoir plusieurs référentiels d'utilisateurs. Dans chaque référentiel d'utilisateurs, l'identité d'utilisateur permet l'accès à différentes ressources de votre société.  Vous pouvez utiliser l'une des méthodes suivantes pour gérer plusieurs référentiels d'utilisateurs :

- Utilisez CA Identity Manager pour gérer directement l'annuaire de provisionnement et utilisez le serveur de provisionnement pour gérer indirectement les utilisateurs et les comptes dans les différents référentiels d'utilisateurs.

  Cette approche vous permet de :

  - Gérer de manière centralisée les utilisateurs auxquels plusieurs ressources d'entreprise peuvent être affectées à partir d'un emplacement.
  - Implémenter une sécurité commune et les règles métier sur les ressources d'entreprise. Les ressources suivantes peuvent être incluses :
    - Contrôle d'accès basé sur les rôles
    - Délégation d'administration
    - Tâches et fenêtres personnalisées selon le type d'identités d'entreprise gérées

- Stratégies d'identité pour la gestion d'identités basée sur des règles
- Personnalisation et extensibilité

**Remarque :** Pour plus d'informations sur ces fonctionnalités, reportez-vous au *Manuel d'administration*.

- Créer un environnement CA Identity Manager distinct pour gérer chaque référentiel d'utilisateurs.

  Avec cette méthode, les informations ne sont pas partagées entre les environnements.

# Sélection des composants à installer

Le tableau suivant répertorie les composants à installer pour la prise en charge de la fonctionnalité à implémenter.

**Remarque :** Pour obtenir des instructions sur l'installation de ces composants, consultez le *Manuel d'installation*.

| Si vous voulez... | Installer les composants |
|---|---|
| Gérer des identités d'utilisateur dans un référentiel d'utilisateurs d'entreprise existant | ■ Serveur CA Identity Manager |
| Provisionner des comptes dans des systèmes d'extrémité | ■ Serveur de provisionnement<br>■ Annuaire de provisionnement<br>■ Gestionnaire de provisionnement<br>■ Connecteurs<br>■ Serveurs de connecteurs<br>**Remarque :** Pour obtenir des instructions sur l'installation de connecteurs, consultez le *Manuel du connecteur* pour le type de connecteurs que vous voulez installer. |

| Si vous voulez... | Installer les composants |
| --- | --- |
| Implémenter les fonctionnalités suivantes :<br>■ Authentification avancée<br>■ Stratégies de mot de passe avancées<br>■ Différentes apparences de console pour des ensembles d'utilisateurs<br>■ Configurer les préférences de paramètres régionaux des utilisateurs | ■ Serveur de stratégies SiteMinder<br>■ Référentiel de stratégies<br>■ Agent Web SiteMinder<br>■ Extensions CA Identity Manager sur le serveur de stratégies<br>**Remarque :** Pour obtenir des instructions sur l'installation du serveur de stratégies SiteMinder et du référentiel de stratégies, consultez le manuel *CA SiteMinder Web Access Manager Policy Server Installation Guide.* Pour obtenir des instructions sur l'installation de l'agent Web, consultez le manuel *CA SiteMinder Web Access Manager Web Agent Installation Guide.* |
| Générer des rapports sur les activités CA Identity Manager | Serveur de rapports CA IAM |

# Configuration matérielle requise

La configuration matérielle requise pour une installation CA Identity Manager dépend des fonctionnalités que vous voulez implémenter et de la taille du déploiement.

Les sections suivantes décrivent des implémentations CA Identity Manager typiques et leur configuration matérielle requise.

## Types de déploiement

Lorsque vous planifier la configuration matérielle requise pour un déploiement CA Identity Manager, considérez les fonctionnalités que vous voulez implémenter et la taille initiale du déploiement. Utilisez l'une des catégories suivantes pour estimer la taille du déploiement.

**Remarque :** Le type de déploiement que vous sélectionnez détermine la taille du fichier DxGrid utilisé par l'annuaire de provisionnement. Vous spécifiez le type de déploiement lorsque vous installez le serveur CA Identity Manager.

**Démonstration**

Un déploiement de serveur unique pour des démonstrations ou des tests de base dans un environnement de développement. Un déploiement de démonstration prend en charge jusqu'à 10 000 comptes provisionnés.

**Remarque :** Ce type d'implémentation ne prend pas en charge les implémentations de production.

**De base**

Une implémentation de haute disponibilité appropriée pour la plupart des petites ou moyennes implémentations. Un déploiement de base prend en charge jusqu'à 400 000 comptes provisionnés.

Ce type d'implémentation requiert deux serveurs pour l'exécution de l'application CA Identity Manager et de ses composants et deux serveurs pour l'exécution de la base de données CA Identity Manager et du référentiel d'utilisateurs.

**Intermédiaire**

Une implémentation de haute disponibilité appropriée pour la plupart des implémentations moyennes. Un déploiement intermédiaire prend en charge jusqu'à 600 000 comptes provisionnés.

**Grande entreprise**

Une implémentation de haute disponibilité qui inclut des clusters de serveurs supplémentaires pour prendre en charge des utilisateurs supplémentaires et un nombre supérieur de transactions. Ce type de déploiement prend en charge plus de 600 000 comptes provisionnés.

**Remarque :** Pour plus d'informations sur les implémentations de haute disponibilité, consultez le *Manuel d'installation*.

## Configuration supplémentaire pour le provisionnement

Outre les composants requis pour une implémentation CA Identity Manager de base, les composants supplémentaires suivants sont requis lorsque CA Identity Manager prend en charge le provisionnement :

- Serveur de provisionnement

  Peut être installé sur le même ordinateur que le serveur CA Identity Manager.

- Initialisation d'annuaire de provisionnement

  **Important :** L'outil d'initialisation d'annuaire de provisionnement doit être installé sur CA Directory.

- Gestionnaire de provisionnement

  Peut être installé sur un ordinateur Windows qui peut accéder au serveur de provisionnement.

**Remarque :** Dans un environnement de développement, vous pouvez installer ces composants sur un ordinateur qui inclut également les composants d'installation de base.

## Configuration supplémentaire pour l'intégration à SiteMinder

Lorsque CA Identity Manager est intégré à SiteMinder, l'implémentation doit inclure les composants de l'installation CA Identity Manager de base, ainsi que les composants supplémentaires suivants :

- **Serveur de stratégie**

  Fournit des services de gestion des stratégies, d'authentification, d'autorisation et de comptabilisation.

  Vous pouvez installer le serveur de stratégies sur le même ordinateur que le serveur CA Identity Manager, si le serveur de stratégies est dédié à CA Identity Manager. Si le serveur de stratégies protège d'autres applications, il est recommandé de l'installer sur un ordinateur distinct pour garantir des performances optimales.

- **Référentiel de stratégies**

  Contient toutes les données du serveur de stratégies. Vous pouvez configurer un référentiel de stratégies dans un annuaire LDAP ou une base de données relationnelles prise en charge. Dans les implémentations de haute disponibilité, il est recommandé d'installer le référentiel de stratégies sur un serveur distinct.

- **Extensions sur le serveur de stratégies**

  Permet à un serveur de stratégies SiteMinder de prendre en charge CA Identity Manager. Installez les extensions sur chaque système de serveur de stratégies SiteMinder dans votre implémentation CA Identity Manager.

- **Agent Web SiteMinder**

  Utilisé avec le serveur de stratégies SiteMinder pour protéger la console d'utilisateur. L'agent est installé sur le système avec le serveur CA Identity Manager.

# Sélection d'une méthode d'importation des utilisateurs

Si vous devez importer des utilisateurs dans un référentiel d'utilisateurs existant, la méthode que vous sélectionnez doit correspondre aux besoins de votre entreprise.

Les sections suivantes décrivent différentes options permettant d'importer des utilisateurs.

## Importation d'utilisateurs dans un nouveau référentiel d'utilisateurs

Après avoir déterminé la méthode de stockage des données d'utilisateur, vous devrez peut-être importer des utilisateurs d'un référentiel dans un autre. Selon votre implémentation, vous pouvez utiliser différentes méthodes pour importer des utilisateurs.

**Remarque :** Après avoir importé des utilisateurs dans un nouveau référentiel d'utilisateurs, vous pouvez utiliser des stratégies d'identité (page 57) pour appliquer des modifications aux utilisateurs importés.

## Importation d'utilisateurs à l'aide de CA Identity Manager

CA Identity Manager fournit les méthodes suivantes pour ajouter des utilisateurs à un référentiel d'utilisateurs géré directement.

| Méthode | Fonctionnalités | Restrictions |
|---|---|---|
| Chargeur en bloc | Vous pouvez utiliser la tâche Bulk Loader (Chargeur en bloc) dans la console d'utilisateurs pour charger les fichiers de chargeur qui sont utilisés pour manipuler de grands nombres d'objets gérés simultanément.<br>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. | Si vous utilisez le chargeur en bloc, vous pouvez recevoir des exceptions de mémoire insuffisante en fonction du nombre d'utilisateurs que vous importez.<br>Pour résoudre ce problème, augmentez les paramètres de mémoire de la machine virtuelle Java. |
| Appel de tâche distante via le service Web d'exécution des tâches | Permet l'exécution des tâches CA Identity Manager pour lesquelles les services Web sont activés, y compris la tâche Créer un utilisateur.<br>Si la tâche est configurée pour la synchronisation de l'utilisateur, CA Identity Manager exécutera toutes les stratégies d'identité applicables. | Les caractéristiques de performances du modèle de service Web peuvent ne pas répondre de manière optimale aux exigences de haut débit nécessaires pour les opérations d'importation en bloc. |
| API IM | ■ Fournit des API basées sur les utilisateurs que vous pouvez appeler directement via un client Java pour créer des utilisateurs.<br>■ Fournit les capacités de débit les plus élevées. | ■ Ignore les mécanismes d'audit et de sécurité mis en place par le serveur de tâches.<br>■ Ne prend pas en charge l'exécution de stratégies d'identité. |

**Remarque :** Pour plus d'informations sur le chargeur en bloc, consultez le *Manuel d'administration*. Pour plus d'informations sur le service Web d'exécution des tâches et l'API IM, consultez le manuel *Programming Guide for Java*.

## Exécution de stratégies d'identité sur des utilisateurs importés

Une *stratégie d'identité* désigne un ensemble de modifications métiers qui ont lieu lorsqu'un utilisateur satisfait à une certaine condition ou règle. Ces modifications peuvent inclure l'affectation ou la révocation des rôles, y compris le provisionnement de rôles pour les utilisateurs dans l'annuaire de provisionnement, l'affectation ou la révocation de l'appartenance à un groupe et la mise à jour des attributs d'un profil d'utilisateur.

Vous pouvez utiliser des stratégies d'identité pour appliquer des modifications aux comptes d'utilisateurs une fois qu'ils ont été importés dans un nouveau référentiel d'utilisateurs.

Cette section décrit les méthodes d'exécution de stratégies d'identité pour les utilisateurs importés en une ou deux étapes.

## Approche d'une étape

Vous pouvez utiliser les méthodes d'importation suivantes pour exécuter des stratégies d'identité sur des utilisateurs que vous importez dans un nouveau référentiel d'utilisateurs en une seule étape :

- Chargeur en bloc dans la console d'utilisateur
- Exécution de la tâche Créer un utilisateur via le service Web d'exécution des tâches
- Synchronisation entrante

## Approche en deux étapes

L'approche en deux étapes consiste à importer les utilisateurs, puis à exécuter des stratégies d'identité sur ces utilisateurs. Vous pouvez utiliser cette méthode lorsque CA Identity Manager gère des utilisateurs dans le serveur de provisionnement. Cette méthode peut être plus flexible, mais cela dépend des conditions d'importation requises.

1. Utilisez l'un des outils d'importation pour ajouter des utilisateurs dans l'annuaire de provisionnement.
2. Appelez la tâche de synchronisation d'utilisateurs CA Identity Manager via le service Web d'exécution des tâches pour chaque utilisateur importé.

## Importation d'utilisateurs via le serveur de provisionnement

Le serveur de provisionnement inclut des options d'importation en bloc pour ajouter et gérer des utilisateurs dans l'annuaire de provisionnement. Le tableau suivant décrit les méthodes d'importation d'utilisateurs dans l'annuaire de provisionnement.

| Méthode | Fonctionnalités | Restrictions |
|---|---|---|
| Utilitaire de traitement par lots (etautil) | Utilitaire d'interface de ligne de commande qui vous permet de gérer des objets dans l'annuaire de provisionnement | ■ Actuellement pris en charge pour les systèmes Windows uniquement |
| Corrélation et exploration | ■ Permet de détecter de nouveaux objets que le serveur de provisionnement peut gérer dans un terminal connu, y compris des utilisateurs.<br>■ Fournit des fonctionnalités de corrélation pour des instances d'objet qui existent dans le terminal et dans le serveur de provisionnement.<br>Pour obtenir des informations supplémentaires, reportez-vous à la rubrique Fonctionnalités d'exploration et de corrélation. | ■ Par défaut, les fonctionnalités d'exploration et de corrélation sont disponibles pour les connecteurs actuellement pris en charge. Elles peuvent être étendues à l'aide de connecteurs personnalisés.<br>■ L'option Correlate (Corréler) peut affecter la modularité lorsque de grands volumes d'utilisateurs sont traités. Si vous sélectionnez cette option d'importation, assurez-vous de bien évaluer les implications sur les performances et la modularité. |

## Synchronisation des utilisateurs globaux avec le référentiel d'utilisateurs CA Identity Manager

Après avoir importé des utilisateurs dans le serveur de provisionnement, vous pouvez utiliser les méthodes suivantes pour les ajouter au référentiel d'utilisateurs CA Identity Manager :

- **Synchronisation entrante**

  La synchronisation entrante permet de mettre à jour les utilisateurs CA Identity Manager avec les modifications qui se produisent dans l'annuaire de provisionnement. Les modifications appliquées à l'annuaire de provisionnement sont effectuées par le gestionnaire de provisionnement ou les systèmes avec des connecteurs au serveur de provisionnement.

  Tenez compte des informations suivantes lorsque vous utilisez la synchronisation entrante pour l'importation d'utilisateurs :

  - Dans la console de gestion CA Identity Manager, vous pouvez personnaliser le mappage des attributs de la demande entrante vers les attributs de la tâche CA Identity Manager.

    **Remarque :** Pour plus d'informations, reportez-vous au *manuel d'administration*.

  - Déterminez les modifications du serveur de provisionnement qui doivent être synchronisées avec le référentiel d'utilisateurs d'entreprise. La synchronisation d'un grand nombre de modifications peut avoir des conséquences sur les performances et la modularité.

- **Rôles de provisionnement et modèles de compte**

  Le serveur de provisionnement peut gérer des comptes dans le référentiel d'utilisateurs CA Identity Manager à l'aide de rôles de provisionnement et de modèles de compte. Pour cela, un terminal géré qui pointe vers le référentiel d'utilisateurs CA Identity Manager doit être acquis et les modèles de compte et les rôles appropriés doivent exister. Dans ce cas, vous pouvez affecter un rôle de provisionnement aux utilisateurs globaux créés à l'aide de l'une des options décrites dans la rubrique Importation d'utilisateurs via le serveur de provisionnement, qui crée le compte d'utilisateur dans le référentiel d'utilisateurs CA Identity Manager.

# Développement d'un plan de déploiement

Lorsque vous planifiez une grande implémentation, déployez les fonctionnalités CA Identity Manager par étapes. L'ordre de déploiement suivant vous permet de tirer rapidement profit de CA Identity Manager, d'évaluer les modifications nécessaires à apporter à votre implémentation dans le temps et de construire avec précaution votre environnement pour des performances optimales et une meilleure modularité :

- Auto-administration et gestion de mots de passe
- Stratégies d'identité
- Approbations de flux de travaux
- Administration déléguée des objets d'utilisateur, de groupe et d'organisation
- Administration de rôle déléguée

Après chaque étape de déploiement, assurez-vous d'évaluer les performances et d'effectuer les ajustements nécessaires avant de continuer à l'étape suivante. Pour obtenir des informations sur les performances, les réglages et la modularité, consultez la rubrique Optimisation de CA Identity Manager (page 71).

## Déploiement de l'auto-administration et de la gestion de mots de passe

Déployez les tâches d'auto-administration et la gestion de mots de passe avant de déployer d'autres fonctionnalités CA Identity Manager pour les raisons suivantes :

- Les tâches d'auto-administration et la gestion de mots de passe sont faciles à déployer et apportent une valeur significative rapidement.
- Ces fonctionnalités sont indépendantes du modèle d'administration délégué et peuvent être reconfigurées si nécessaire pour répondre aux modifications des besoins métier.
- Ces fonctionnalités génèrent un volume élevé de tâches que CA Identity Manager traite régulièrement. Pour cette raison, elles permettent de tester la modularité de l'implémentation avant de déployer d'autres fonctionnalités.

Pour déployer des tâches d'auto-administration, procédez comme suit :

1. Configurez la tâche d'auto-enregistrement.

   Il s'agit d'une tâche publique activée par défaut pendant l'installation. Pour configurer cette tâche, ajoutez ou supprimez des champs de la tâche d'auto-enregistrement par défaut, si nécessaire.

2. Configurez le rôle Self Manager (Autogestionnaire).

   La règle de membre pour ce rôle doit être configurée de façon à s'appliquer à tous les utilisateurs ou doit inclure une règle de membre qui affecte automatiquement le rôle à de nouveaux utilisateurs. Par exemple, vous pouvez créer une règle de membre qui affecte le rôle Self Manager (Autogestionnaire) à tous les employés à temps plein. Lorsqu'un utilisateur s'auto-enregistre, CA Identity Manager peut définir le type d'employé sur temps plein, à l'aide d'un gestionnaire d'attributs logiques ou un gestionnaire de tâches métier. L'utilisateur répond aux critères de la règle de membre et reçoit le rôle Self Manager (Autogestionnaire) automatiquement.

   **Remarque :** Lorsque vous configurez des règles de membre pour le rôle Self Manager (Autogestionnaire), ne permettez pas aux administrateurs d'ajouter ou de supprimer des membres de rôle. Le rôle étant affecté automatiquement, il n'y a aucune raison pour qu'un administrateur doive affecter explicitement le rôle.

Pour déployer les fonctionnalités de gestion de mots de passe, procédez comme suit :

1. Configurez les tâches de gestion de mots de passe publiques, comme la tâche Mot de passe oublié.
2. Créez des stratégies de mot de passe qui déterminent la méthode de création des mots de passe et leur date d'expiration.
3. Déployez le rôle Gestionnaire de mots de passe, qui permet aux membres de rôle de réinitialiser les mots de passe d'utilisateur.

**Remarque :** Pour plus d'informations sur les rôles, les tâches et la gestion de mots de passe, consultez le *Manuel d'administration*.

## Déploiement de stratégies d'identité

Une stratégie d'identité désigne un ensemble de modifications métiers qui ont lieu lorsqu'un utilisateur satisfait à une certaine condition ou règle. Vous pouvez utiliser des stratégies d'identité pour accorder des droits métier avant le déploiement d'un modèle de délégation complet. Par exemple, vous pouvez créer une stratégie d'identité qui affecte le rôle de provisionnement de directeur commercial, qui accorde des droits d'accès aux applications de ventes, à tous les utilisateurs dont le titre est Directeur commercial. Lorsqu'un responsable de comptes est promu directeur commercial, il reçoit automatiquement l'accès à tous les systèmes nécessaires à ses fonctions sans attendre la confirmation d'un administrateur.

Pour déployer ces stratégies d'identité, procédez comme suit :

1. Configurez des stratégies d'identité qui sont déclenchées par des modifications apportées aux attributs de profil d'utilisateur.
2. Configurez le rôle Gestionnaire d'utilisateurs pour permettre à un petit nombre d'administrateurs d'utiliser les tâches d'utilisateur, comme Créer un utilisateur et Modifier un utilisateur, pour modifier les attributs qui déclenchent les stratégies d'identité.

   Assurez-vous de configurer les règles de portée dans les stratégies de membre du gestionnaire d'utilisateurs pour déterminer l'ensemble des utilisateurs que les membres de rôle peuvent gérer.

Tenez compte des points suivants lorsque vous déployez des stratégies d'identité :

- Créez initialement des stratégies d'identité qui accordent des droits qui ne requièrent *aucune* approbation de flux de travaux. Cela vous permet de déployer des stratégies d'identité sans devoir définir des processus de flux de travaux, des formulaires d'approbation et des modèles d'approbateur.
- Avant de créer des stratégies d'identité, familiarisez-vous avec les autres méthodes d'implémentation de règles métier dans CA Identity Manager, comme les règles de validation de données, les attributs logiques, les gestionnaires de tâches métier et les processus de flux de travaux, pour déterminer la méthode la plus appropriée.

  **Remarque :** Pour plus d'informations sur ces méthodes, consultez le *Manuel d'administration* et le manuel *Programming Guide for Java*.
- Les stratégies d'identité sont une façon efficace d'accorder des droits dans CA Identity Manager. Toutefois, elles peuvent affecter significativement les performances (page 87).
- Pour le déploiement initial des tâches d'utilisateur, supprimez ou masquez les onglets de relation, comme les onglets Rôles, qui gèrent les mêmes droits que les stratégies d'identité. Cette mesure permet de prévenir les attributions de droits non autorisés et d'éviter les conséquences liées aux rôles créés de manière incorrecte.

**Remarque :** Pour plus d'informations sur les stratégies d'identité, consultez le *Manuel d'administration*.

## Déploiement d'approbations de flux de travaux

Les approbations de flux de travaux peuvent ajouter un niveau supplémentaire de sécurité et d'automatisation à l'implémentation CA Identity Manager.

Pour déployer les approbations de flux de travaux, effectuez les opérations suivantes :

1. Déterminez les événements ou les tâches qui requièrent des approbations.
2. Définissez l'ensemble d'approbateurs (participants) pour chaque processus de flux de travaux.

   **Remarque :** Tous les participants sont déterminés de façon dynamique par des outils de résolution de participants. Pour obtenir des performances optimales, limitez le nombre de participants à trente utilisateurs.
3. Configurez des formulaires d'approbation.
4. Définissez des processus de flux de travaux personnalisés, si nécessaire.

### Approbations de flux de travaux de niveaux environnement et tâche

CA Identity Manager prend en charge deux types d'approbations : les approbations de niveau environnement et les approbations de niveau tâche. Les approbations de niveau environnement sont définies pour toutes les instances d'un événement, indépendamment des tâches auxquelles elles sont associées. Les approbations de niveau tâche sont définies pour un événement associé à une tâche spécifique. Les approbations de niveau tâche ont priorité sur celles de niveau environnement.

La plupart des approbations sont définies au niveau environnement afin de garantir que les mêmes activités de flux de travaux ont lieu pour un événement, indépendamment de la tâche à laquelle il est associé. Toutefois, implémentez des flux de travaux de niveau tâche dans les situations suivantes :

- Vous avez des tâches spécialisées qui appliquent des modifications métier spécifiques et qui génèrent des événements qui ne requièrent aucune approbation.
- Vous avez des modifications déclenchées par des stratégies d'identité, qui génèrent des événements qui ne requièrent aucune approbation de flux de travaux.
- Vous avez besoin de flexibilité pour associer des processus de flux de travaux à des modifications de tâche.

Les approbations de niveau environnement peuvent requérir un traitement et des ressources système importantes, car le volume des transactions augmente. Cela peut finalement occasionner des problèmes de performances et de modularité. L'utilisation d'approbations de niveau tâche peut réduire ou éliminer ces problèmes.

## Déploiement de l'administration déléguée pour des utilisateurs, des groupes et des organisations

L'administration déléguée consiste à attribuer la gestion des utilisateurs et de leurs droits à différents utilisateurs CA Identity Manager, qui effectuent les fonctions de modification, d'affection et d'utilisation d'un rôle.

**Remarque :** Les modèles de délégation doivent être créés avec précaution pour assurer des performances et une modularité optimales dans l'implémentation CA Identity Manager.

La délégation est appliquée par des règles de portée, qui sont définies dans des stratégies de membre et d'administration pour les rôles d'administration. Une règle de portée détermine les objets sur lesquels un membre de rôle peut utiliser le rôle. Par exemple, une règle de portée peut permettre à un gestionnaire d'utilisateurs de gérer des utilisateurs dans son département, mais non dans d'autres départements.

En général, les règles de portée doivent refléter la structure logique du référentiel d'utilisateurs. Par exemple, dans un référentiel d'utilisateur LDAP hiérarchique, la portée peut être définie par des organisations. Dans une base de données relationnelles, vous pouvez définir la portée à l'aide d'attributs comme l'ID de département.

Tenez compte des points suivants lorsque vous déployez l'administration déléguée pour des utilisateurs, des groupes et des organisations :

- Limitez l'accès aux onglets de relation, comme les onglets Rôles d'administration et Rôles de provisionnement, dans les tâches en rapport avec l'utilisateur. Ces onglets de relation sont inclus dans des tâches d'utilisateur par défaut, comme Créer un utilisateur et Modifier un utilisateur. Supprimez les des tâches par défaut et utilisez-les uniquement dans des tâches spécialisées qui sont associées à un petit nombre de rôles d'administration.
- CA Identity Manager évalue chaque règle de portée de façon dynamique ; les informations de portée ne sont pas mises en cache. Créez des règles de portée qui contiennent des requêtes d'annuaire simples pour garantir des performances optimales.
- Evaluez les performances des règles de portée en déterminant la durée que CA Identity Manager met à renvoyer les objets qu'un administrateur peut gérer.

## Déploiement de l'administration déléguée pour des rôles

L'administration de rôles déléguée accorde les droits les plus significatifs dans CA Identity Manager et peut affecter notablement (page 72) les performances. Pour ces raisons, déployez plutôt l'administration déléguée pour les rôles après le déploiement de toutes les autres fonctionnalités.

Lorsque vous déployez l'administration déléguée pour les rôles, tenez compte des points suivants :

- Limitez le nombre de rôles d'administration, de membres de rôle d'administration et d'administrateurs de rôle d'administration pour protéger l'environnement et optimiser les performances.
- Une fois que vous déployez l'administration déléguée pour les rôles, effectuez des tests de performance et de modularité. Optimisez l'environnement si nécessaire.

# Chapitre 5: Intégration à SiteMinder

Ce chapitre traite des sujets suivants :



## SiteMinder et CA Identity Manager

Lorsque CA Identity Manager est intégré à SiteMinder, la fonctionnalité SiteMinder suivante est ajoutée à l'environnement CA Identity Manager :

**Authentification avancée**

CA Identity Manager inclut une authentification native pour les environnements CA Identity Manager par défaut. Les administrateurs CA Identity Manager entrent un nom d'utilisateur et un mot de passe valides pour se connecter à un environnement CA Identity Manager. CA Identity Manager authentifie le nom et le mot de passe par rapport au référentiel d'utilisateurs géré par CA Identity Manager.

Si CA Identity Manager est intégré à SiteMinder, CA Identity Manager utilise l'authentification de base SiteMinder pour protéger l'environnement. Lorsque vous créez un environnement CA Identity Manager, un domaine de stratégie et un schéma d'authentification sont créés dans SiteMinder pour protéger l'environnement.

Lorsque l'intégration est configurée, vous pouvez également utiliser l'authentification SiteMinder pour protéger la console de gestion.

**Tâches et rôles d'accès**

Les rôles d'accès permettent aux administrateurs CA Identity Manager d'affecter des droits dans les applications protégées par SiteMinder. Ces rôles d'accès représentent une action unique qu'un utilisateur peut effectuer dans une application métier, telle que la génération d'un bon de commande dans une application financière.

**Mappage d'annuaires**

Un administrateur peut devoir gérer des utilisateurs dont les profils existent dans un référentiel d'utilisateurs différent de celui utilisé pour authentifier l'administrateur. Lors de la connexion à l'environnement CA Identity Manager, l'administrateur est authentifié à l'aide d'un annuaire et un autre annuaire est utilisé pour l'autoriser à gérer des utilisateurs.

Lorsque CA Identity Manager est intégré à SiteMinder, vous pouvez configurer un environnement CA Identity Manager de façon à utiliser des annuaires différents pour l'authentification et pour l'autorisation.

**Apparences pour différents ensembles d'utilisateurs**

Une apparence permet de personnaliser la console d'utilisateur. Lorsque CA Identity Manager est intégré à SiteMinder, vous pouvez autoriser des ensembles d'utilisateurs à afficher des apparences différentes. Pour cela, vous utilisez une réponse SiteMinder vous permettant d'associer une apparence à un ensemble d'utilisateurs. La réponse est associée avec une règle dans une stratégie, qui est associée à un ensemble d'utilisateurs. Lorsque la règle se déclenche, une réponse contenant les informations sur l'apparence CA Identity Manager est envoyée pour permettre la création de la console d'utilisateur.

**Remarque :** Pour plus d'informations, consultez le *Manuel de conception de la console d'utilisateur*.

**Préférences des paramètres régionaux dans un environnement localisé**

Lorsque CA Identity Manager est intégré à SiteMinder, vous pouvez définir des préférences de paramètres régionaux pour un utilisateur à l'aide d'un en-tête HTTP imlanguage. Dans le serveur de stratégies SiteMinder, vous définissez cet en-tête dans une réponse SiteMinder et spécifiez un attribut d'utilisateur comme valeur de celui-ci. Cet en-tête imlanguage est défini comme la préférence de paramètres régionaux prioritaire pour un utilisateur.

**Remarque :** Pour plus d'informations, consultez le *Manuel de conception de la console d'utilisateur*.

**Informations complémentaires :**

Installation avec un serveur de stratégies SiteMinder (page 41)

# Authentification SiteMinder

CA Identity Manager inclut les consoles suivantes, qui doivent être protégées :

**Console d'utilisateur**

Permet aux administrateurs CA Identity Manager d'effectuer des tâches dans un environnement CA Identity Manager.

**Console de gestion**

Permet aux administrateurs CA Identity Manager de créer et de configurer un annuaire CA Identity Manager, un annuaire de provisionnement et un environnement CA Identity Manager.

CA Identity Manager inclut une authentification native, qui protège la console d'utilisateurs par défaut. La console de gestion n'est pas protégée par défaut, mais vous pouvez configurer CA Identity Manager pour la protéger. Vous pouvez également utiliser CA SiteMinder pour la protéger.

Pour configurer d'autres types d'authentification pour la console d'utilisateur, comme l'authentification par certificat ou par clé, CA Identity Manager doit être intégré à SiteMinder.

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

# Chapitre 6: Optimisation de CA Identity Manager

Ce chapitre traite des sujets suivants :



## Performances de CA Identity Manager

Les performances de CA Identity Manager dépendent des performances des différentes fonctionnalités et composants.

Vous pouvez optimiser les fonctionnalités suivantes dans un environnement CA Identity Manager :

- Rôles
- Tâches
- Gestion de groupes et appartenance
- Stratégies d'identité

Pour des gains de performances supplémentaires, vous pouvez également ajuster les composants suivants :

- Référentiel d'utilisateurs
- Composants de provisionnement
- Les composants d'exécution, notamment les bases de données comme la base de données de persistance des tâches, et les paramètres du serveur d'applications

Pour optimiser les performances, configurez la fonctionnalité CA Identity Manager à l'aide des directives des sections suivantes. Mesurez ensuite les performances et ajustez les composants, si nécessaire. Les composants fonctionnent de manière conjointe. Cela peut donc prendre plusieurs itérations avant de trouver les meilleurs paramètres de réglage pour votre environnement.

# Optimisations de rôle

CA Identity Manager inclut trois types de rôles :

- Rôles d'administration

  Déterminent les droits d'un utilisateur dans la console d'utilisateur.

  Lorsqu'un utilisateur se connecte à un environnement CA Identity Manager, le compte de l'utilisateur a un ou plusieurs rôles d'administration. Chaque rôle d'administration contient des tâches, telle que Créer un utilisateur, qu'un utilisateur peut effectuer dans l'environnement CA Identity Manager. Les rôles d'administration d'un utilisateur déterminent les éléments affichés dans la console d'utilisateur. Par conséquent, seules les tâches associées à leurs rôles sont affichées.

- Rôles de provisionnement

  Attribuent des comptes d'utilisateur sur les terminaux gérés, comme un système de messagerie.

- Rôles d'accès

  Offrent une façon supplémentaire d'accorder des droits dans CA Identity Manager.

Ces rôles incluent des stratégies qui déterminent :

- Qui peut utiliser le rôle (rôles d'administration et d'accès uniquement) et où ils peuvent l'utiliser.
- Qui peut gérer des membres et des administrateurs de rôle.
- Qui peut modifier la définition de rôle.

L'évaluation des rôles et des droits associés peut avoir un impact considérable sur les performances de CA Identity Manager.

## Impact de l'évaluation de rôles sur les performances lors de la connexion

Lorsqu'un utilisateur CA Identity Manager se connecte à la console d'utilisateur, les opérations suivantes se produisent :

1. CA Identity Manager invite l'utilisateur à fournir des informations d'identification, comme un nom d'utilisateur et un mot de passe.
2. Les informations d'identification de l'utilisateur sont authentifiées à l'aide de l'une des méthodes suivantes :
   - Authentification native de CA Identity Manager
   - Authentification SiteMinder, si l'implémentation CA Identity Manager inclut SiteMinder.

3. CA Identity Manager évalue toutes les stratégies de membre pour tous les rôles d'administration dans l'environnement afin de déterminer les rôles d'administration qui s'appliquent à l'utilisateur.

   **Remarque :** Cette évaluation se produit une seule fois par utilisateur. Après l'évaluation initiale, CA Identity Manager met en cache les résultats. CA Identity Manager utilise les informations mises en cache jusqu'à ce qu'une modification soit appliquée à l'utilisateur ou à l'ensemble de stratégies de membre, ce qui force CA Identity Manager à actualiser les informations du cache.

4. La console d'utilisateur CA Identity Manager affiche les catégories que l'utilisateur peut afficher selon ses rôles.

Ce processus est effectué pour tous les utilisateurs qui se connectent à la console d'utilisateur. Si un environnement CA Identity Manager contient un grand nombre de rôles ou des stratégies de membre inefficaces, l'évaluation d'appartenance de rôle peut affecter négativement les performances. Dans ce cas, la fenêtre initiale de connexion à la console d'utilisateur peut s'afficher lentement.

**Remarque :** L'évaluation des stratégies de membre n'est pas nécessaire lorsqu'un utilisateur accède à une tâche publique pour s'auto-enregistrer ou pour demander un mot de passe oublié. Dans ce cas, CA Identity Manager ne requière aucune liste de rôles de l'utilisateur, car la console d'utilisateur complète ne s'affiche pas.

## Objets de rôle et performances

Pour prendre en charge chaque rôle, CA Identity Manager crée un nombre d'objets dans le référentiel d'objets (page 33) CA Identity Manager, selon la configuration du rôle.

CA Identity Manager crée un objet de base pour chaque rôle. Outre l'objet de base, CA Identity Manager crée un objet pour chaque stratégie.

Un trop grand nombre d'objets de rôle peut affecter les performances des recherches dans le référentiel d'objets et les évaluations de stratégie.

### Performances du référentiel d'objets

CA Identity Manager stocke les informations requises pour gérer les utilisateurs et les droits dans un référentiel d'objets. Un grand nombre d'objets de rôle dans le référentiel d'objets peut entraîner les problèmes suivants :

- Les recherches d'objets gérés dans les fenêtres de tâches CA Identity Manager peuvent prendre plus longtemps.

  Pour réduire l'impact sur les recherches, indexez les attributs utilisés dans les recherches (page 92).

- L'exécution des tâches de gestion des rôles peut être lente.

  Exemples de tâches de gestion des rôles affectées par un référentiel d'objets étendu :

  - Une tâche Créer un rôle d'administration est lente, car CA Identity Manager doit confirmer que le nom de rôle est unique dans le référentiel d'objets.
  - La tâche Supprimer un rôle d'administration doit supprimer tous les objets créés pour la prise en charge du rôle et le cache d'objet doit être mis à jour.

- L'évaluation des stratégies de rôle prend longtemps.

CA Identity Manager met les informations en cache dans le référentiel d'objets pour améliorer les performances.

## Optimisation de l'évaluation de stratégie de rôle

Pour chaque rôle d'administration, vous pouvez créer trois types de stratégies :

- Stratégies de membre

  Ce type de stratégie permet de définir une règle de membre, qui détermine les utilisateurs qui reçoivent le rôle, et des règles de portée, qui déterminent les objets que les membres de rôle peuvent gérer.

- Stratégies d'administration

  Ce type de stratégie permet de définir des règles d'administration, des règles de portée et des droits d'administration pour un rôle.

- Stratégies de propriété

  Ce type de stratégie permet de définir les utilisateurs qui peuvent modifier un rôle.

Pour optimiser les performances lorsque CA Identity Manager évalue les stratégies de rôle, tenez compte des points suivants :

- Limitez le nombre de rôles d'administration dans un environnement CA Identity Manager.
- Suivez les directives pour la création de règles de stratégie (page 75).
- Ajustez le référentiel d'utilisateurs.
- Ajustez le référentiel de stratégies, si CA Identity Manager inclut CA SiteMinder.

## Directives pour la création de règles de stratégie

Un des facteurs clés permettant de déterminer les performances globales des évaluations de stratégie de rôle est la durée d'évaluation d'une seule règle de stratégie. Pour améliorer la durée d'évaluation d'une règle de stratégie, effectuez les opérations suivantes lors de la création d'une stratégie :

- Lorsque cela est possible, limitez le nombre d'objets de stratégie que CA Identity Manager crée et le nombre de recherches dans le référentiel d'utilisateurs effectuées en créant des règles de stratégie à l'aide d'expressions complexes.

  Une règle unique avec une expression complexe est plus efficace que plusieurs règles avec des expressions simples.

- Lorsque cela est possible, sélectionnez le type de règle de stratégie le plus efficace et le plus adaptable.
- Activez l'option d'évaluation de mémoire pour les règles de stratégie.

  L'option d'évaluation de mémoire réduit significativement la durée d'évaluation de stratégie. Elle permet de récupérer les informations sur un utilisateur à évaluer dans le référentiel d'utilisateurs et de stocker une représentation de cet utilisateur dans la mémoire. CA Identity Manager utilise la représentation dans la mémoire pour comparer les valeurs d'attribut par rapport aux règles de stratégie.

  **Remarque :** Pour plus d'informations sur l'option d'évaluation de mémoire, consultez le *Manuel de configuration*.

- Ajustez le référentiel d'utilisateurs.
- Ajustez le référentiel de stratégies, si l'implémentation CA Identity Manager inclut SiteMinder.

## Limitation du nombre d'objets de stratégie et des recherches dans le référentiel d'utilisateurs

Chaque règle dans une stratégie de rôle requiert un ensemble d'objets dans le référentiel d'objets. Lorsque CA Identity Manager évalue une règle, les objets sont chargés et les recherches requises sont effectuées dans le référentiel d'utilisateurs.

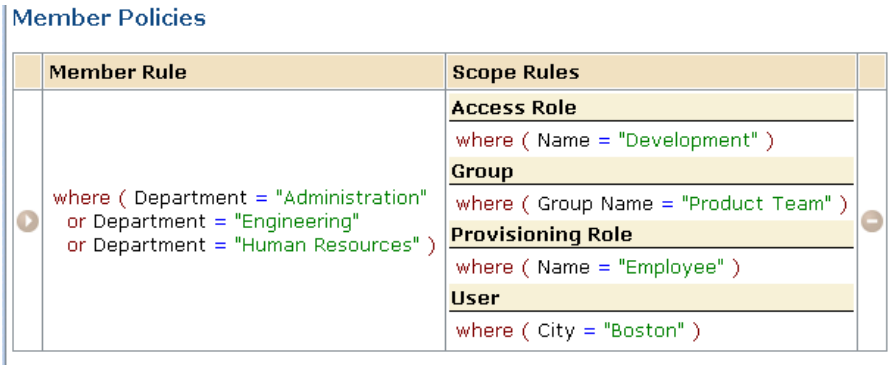
L'exemple suivant présente une stratégie de membre qui inclut trois règles de membre. Chaque règle inclut quatre règles de portée.

Dans cet exemple, CA Identity Manager crée les objets et effectue les recherches dans le référentiel d'utilisateurs décrites dans le tableau suivant lors de l'évaluation et de l'application de la stratégie de membre.

| Règle | Objets de stratégie | Recherches potentielles dans le référentiel d'utilisateurs |
|---|---|---|
| ■ Règle du membre : where (Department = "Administration")<br>■ Règle de portée d'utilisateur : City = "Boston"<br>■ Règle de portée de groupe : Group Name = "Product Team"<br>■ Provisioning role scope (Portée du rôle de provisionnement) : Name = "Employee"<br>■ Access Task Scope (Portée de la tâche d'accès) :Name = "Development" | 5 | 5 (un pour chaque objet de définition de règle) |
| ■ Règle du membre : where (Department = "Engineering")<br>■ Règle de portée d'utilisateur : City = "Boston"<br>■ Règle de portée de groupe : Group Name = "Product Team"<br>■ Provisioning role scope (Portée du rôle de provisionnement) : Name = "Employee"<br>■ Access Task Scope (Portée de la tâche d'accès) :Name = "Development" | 5 | 5 |
| ■ Règle du membre : where (Department = "Human Resources")<br>■ Règle de portée d'utilisateur : City = "Boston"<br>■ Règle de portée de groupe : Group Name = "Product Team"<br>■ Provisioning role scope (Portée du rôle de provisionnement) : Name = "Employee"<br>■ Access Task Scope (Portée de la tâche d'accès) :Name = "Development" | 5 | 5 |

Dans cet exemple, CA Identity Manager crée 15 objets et exécute 15 recherches dans l'annuaire pour déterminer l'appartenance et la portée.

Pour limiter le nombre d'objets de stratégie et de recherches dans le référentiel d'utilisateurs effectuées par CA Identity Manager, regroupez les règles dans des expressions complexes. L'exemple suivant spécifie les mêmes droits que dans le premier exemple, mais en une seule règle de membre.




Dans cet exemple, CA Identity Manager crée dix objets de stratégie et effectue uniquement cinq recherches dans le référentiel d'utilisateurs.

| Règle | Objets de stratégie | Recherches potentielles dans le référentiel d'utilisateurs |
|---|---|---|
| ■ Règle du membre :<br>where (Department = "Administration") OR<br>where (Department = "Engineering") OR<br>where (Department = "Human Resources")<br>■ Règle de portée d'utilisateur : City = "Boston"<br>■ Règle de portée de groupe : Group Name = "Product Team"<br>■ Provisioning role scope (Portée du rôle de provisionnement) : Name = "Employee"<br>■ Access Task Scope (Portée de la tâche d'accès) :Name = "Development" | 5 | 5 |

## Sélection de types de règle de stratégie adaptables

Outre le nombre de règles de stratégie, le type de règle de stratégie peut également affecter les performances. En général, les règles de stratégie sont créées selon la structure du référentiel d'utilisateurs et la manière dont les droits sont déterminés. Par exemple, vous pouvez créer des règles de stratégie basées sur des attributs d'appartenance au groupe, d'organisation ou d'utilisateur. Toutefois, lorsqu'il y a plusieurs modalités pour créer des règles de stratégie, considérez les directives de performances dans le tableau suivant avant de décider du type de règle à créer.

**Remarque :** Les types de règle de stratégie du tableau suivant sont répertoriés dans l'ordre des performances, en commençant par le type de règle le plus efficace.

| Type de règle de stratégie | Remarques sur les performances |
|---|---|
| Organisation | ■ Meilleures performances globales<br>■ Ne requiert aucune recherche dans les annuaires LDAP. CA Identity Manager utilise le nom unique de l'utilisateur évalué et le nom unique de l'organisation dans la règle de stratégie. |
| Rôle | ■ CA Identity Manager stocke les informations d'objet de rôle et les évaluations précédentes dans le cache du référentiel d'objets.<br>■ Dans la plupart des cas, les performances sont équivalentes à celles des règles de stratégie d'organisation. |
| Attribut d'utilisateur | ■ Fournit les meilleures performances de recherche dans le référentiel d'utilisateurs et est peu affecté par un grand nombre d'utilisateurs.<br>■ Vous permet d'activer l'évaluation de mémoire pour des gains de performances significatifs. |
| Appartenance à un groupe | ■ Les performances dépendent de la taille de groupe et du type de référentiel d'utilisateurs. |

# Optimisations de tâche

Dans CA Identity Manager, les tâches affichées dans la console d'utilisateur dépendent des droits spécifiques de l'utilisateur. Pour afficher et exécuter des tâches, CA Identity Manager doit effectuer plusieurs évaluations de sécurité, qui peuvent affecter significativement les performances lorsqu'elles sont appliquées sur tous les utilisateurs d'un environnement CA Identity Manager.

CA Identity Manager effectue les évaluations de sécurité lorsque les actions suivantes se produisent :

- Un utilisateur se connecte à la console d'utilisateur.

  Dans ce cas, CA Identity Manager doit évaluer les rôles de l'utilisateur pour déterminer les tâches auxquelles il peut accéder dans la console d'utilisateur.

- Un utilisateur appelle une tâche.

  Lorsqu'une tâche est appelée, CA Identity Manager doit déterminer les objets que l'utilisateur peut gérer avec cette tâche.

- Un utilisateur accède à un onglet de relation.

  Un onglet de relation est un onglet dans lequel un utilisateur peut afficher ou gérer une relation un-à-plusieurs entre l'objet de la tâche et un ensemble de droits. L'onglet Rôles d'administration est un exemple d'onglet de relation, qui affiche les rôles d'un utilisateur.

- Un utilisateur ajoute des objets dans un onglet de relation.

  Par exemple, CA Identity Manager effectue des contrôles de sécurité supplémentaires lorsqu'un utilisateur ajoute des rôles à un autre utilisateur dans l'onglet Rôles d'administration.

Les performances de tâche sont affectées par :

- La portée de la tâche, qui détermine la portée d'une tâche selon l'administrateur.
- Les onglets de relation, qui affichent la relation d'un objet avec d'autres objets

## Evaluation de la portée de la tâche et performances

Lorsqu'un administrateur utilise une tâche d'administration qui implique la recherche d'un objet géré, tel qu'un utilisateur, un groupe, une organisation, une tâche ou un rôle, CA Identity Manager évalue et applique des règles de portée de tâche. Ces règles peuvent affecter significativement la durée que CA Identity Manager tarde à afficher la liste d'objets à sélectionner pour la tâche.

**Remarque :** Contrairement aux évaluations de stratégie de membre, d'administration et de propriété, les informations relatives aux évaluations de règle de portée ne sont pas mises dans un cache.

La portée de la tâche est déterminée par :

- Le type d'objet que la tâche gère.
- Les règles de portée qui s'appliquent au rôle d'administration qui inclut la tâche. Les règles de portée sont définies dans les stratégies de membre, de propriété et d'administration.
- Tous les critères de recherche définis par l'utilisateur.

Par exemple, considérez une tâche Modifier un utilisateur, qui est incluse dans le rôle Gestionnaire d'utilisateurs. Le rôle Gestionnaire d'utilisateurs a une stratégie de membre avec une règle de portée qui permet aux gestionnaires d'utilisateurs de gérer des utilisateurs dans l'organisation Employés. Un administrateur ouvre la tâche Modifier un utilisateur et entre les critères de recherche : nom commençant par A. Dans ce cas, la portée de la tâche Modifier un utilisateur est limitée à tous les utilisateurs dans l'organisation Employés dont le nom commence par A.

## Rendu des onglets de relation dans CA Identity Manager

Un onglet de relation permet aux utilisateurs d'afficher et de gérer la relation que l'objet d'une tâche maintient avec un ensemble de droits. Par exemple, l'onglet Rôles de provisionnement affiche les rôles de provisionnement d'un utilisateur.

Pour déterminer les objets qui s'affichent dans un onglet de relation, CA Identity Manager effectue de nombreuses évaluations de sécurité, qui peuvent affecter significativement les performances.

Les exemples suivants présentent les étapes que CA Identity Manager suit pour afficher l'onglet Rôles de provisionnement :

1. L'administrateur clique sur l'onglet Rôles de provisionnement dans la tâche Modifier un utilisateur.
2. CA Identity Manager récupère les rôles de provisionnement desquels l'utilisateur sélectionné est membre.
3. Si l'onglet est configuré pour permettre la gestion des administrateurs de rôle, CA Identity Manager effectue un deuxième appel pour récupérer la liste des rôles de provisionnement desquels l'utilisateur sélectionné est administrateur.
4. CA Identity Manager évalue chaque rôle de provisionnement que l'utilisateur doit pouvoir afficher si l'administrateur qui a initialisé la tâche peut gérer l'appartenance du rôle.

   Si l'administrateur peut gérer des membres de rôle, CA Identity Manager affiche une case à cocher activée dans la colonne Appartenance de ce rôle, dans la liste des rôles de l'onglet.
5. CA Identity Manager évalue chaque rôle de provisionnement que l'utilisateur doit pouvoir afficher si l'administrateur qui a initialisé la tâche peut gérer les droits d'administration du rôle.

   Si l'administrateur peut gérer des droits d'administration, CA Identity Manager affiche une case à cocher activée dans la colonne Administrateur de ce rôle, dans la liste des rôles de l'onglet.

   CA Identity Manager doit effectuer les étapes 2 à 5 pour afficher les rôles de provisionnement actuels de l'utilisateur. Si l'administrateur doit affecter un nouveau rôle de provisionnement, les étapes supplémentaires suivantes sont requises.
6. L'administrateur clique sur Ajouter pour rechercher les nouveaux rôles de provisionnement à affecter.
7. CA Identity Manager affiche une fenêtre de recherche que l'administrateur peut utiliser pour rechercher ces rôles.
8. L'administrateur entre ensuite un filtre de recherche.

9. CA Identity Manager renvoie la liste des rôles de provisionnement qui correspondent aux critères suivants :
   - Les rôles correspondent au filtre de recherche défini par l'administrateur.
   - L'administrateur peut gérer l'appartenance aux rôles.
   - L'utilisateur se trouve dans la portée administrative de l'administrateur pour les rôles.
   - L'utilisateur n'a aucun rôle de provisionnement.
10. CA Identity Manager répète l'étape 9 pour déterminer les rôles qui permettent à l'administrateur de gérer les droits d'administration.

## Onglets de relation et performances

A cause du nombre d'évaluations de sécurité effectuées par CA Identity Manager, le rendu d'un onglet de relation peut affecter significativement les performances. Les facteurs qui déterminent les performances varient selon le type d'onglet.

Pour des onglets de relation de rôle, les facteurs suivants peuvent affecter les performances :

- Le nombre de rôles dont l'objet de la tâche est membre.
- Le nombre de rôles pour lesquels l'objet de la tâche est administrateur.
- Le nombre total d'objets dans le système que CA Identity Manager requiert pour calculer les rôles de l'objet.
- Le nombre de stratégies de membre/d'administration par rôle
- La complexité des règles de portée de stratégie de membre/d'administration
- La capacité de maintenir des autorisations mises en cache pour que les utilisateurs appelants la tâche limitent les effets de la sécurité.

Pour déterminer l'appartenance au groupe et les droits d'administration dans les onglets de relation de groupe, CA Identity Manager doit effectuer des recherches sur tous les groupes dans le référentiel d'utilisateurs. Les performances de ces recherches dépendent des facteurs suivants :

- Le nombre d'objets de groupe dans le référentiel d'utilisateurs
- Le nombre de membres dans un groupe
- Les performances de la base de données ou de l'annuaire dans lequel le référentiel d'utilisateurs existe.

## Traitement des tâches et performances

Les tâches d'administration incluent des événements, actions qu'CA Identity Manager effectue pour réaliser la tâche. Une tâche peut inclure plusieurs événements. Par exemple, la tâche Créer un utilisateur peut inclure des événements qui créent le profil de l'utilisateur, ajoutent l'utilisateur à un groupe et affectent des rôles.

Lorsqu'une tâche est traitée, tous les événements qui y sont associés sont également traités. Pendant le traitement des événements, CA Identity Manager enregistre chaque événement quatre fois. Cela permet de faire appel à des actions en cours de traitement en cas d'arrêt imprévu du système.

Lorsque plusieurs événements sont traités simultanément, ils sont ajoutés à une file d'attente. Lorsque la première étape du cycle de vie du premier événement se termine, il est enregistré, puis placé à nouveau dans la file d'attente pour la deuxième étape de traitement. La première étape du traitement de l'événement suivant dans la file d'attente est effectuée et l'événement est placé à la fin de la file d'attente. Le processus se poursuit jusqu'à ce que la première étape de traitement de tous les événements de la file d'attente soit terminée. Le premier événement de la file d'attente commence ensuite la deuxième phase de traitement. Cela se poursuit jusqu'à ce que les quatre étapes de traitement de tous les événements dans la file d'attente soient effectuées.

Dans des conditions de charge normales, ce comportement n'affecte pas les performances. Toutefois, si le système traite un grand nombre de tâches et d'événements, comme pendant un chargement en bloc de volumes d'utilisateurs étendus, la durée de mise en file d'attente des événements et des tâches est plus importante et par conséquent, le délai de traitement est plus long.

Pour prévenir les problèmes de performance dans de telles conditions de charge, prenez les mesures suivantes :

- Utilisez le paramètre Priorité des tâches dans l'onglet Profil d'une tâche.

  Ce paramètre vous permet de définir la priorité d'une tâche sur Elevée, Moyenne ou Faible.

  Les tâches qui doivent être traitées immédiatement doivent être définies sur Elevée. Les tâches impliquées dans un chargement en bloc doivent être définies sur Faible.

  Si la priorité d'une tâche est définie, les événements qui y sont associés sont traités avec d'autres tâches de la même priorité. Par exemple, si la priorité de la tâche Modifier un utilisateur est définie sur Elevée et qu'un administrateur modifie un profil d'utilisateur, CA Identity Manager traite cette tâche avant les tâches de priorité Moyenne ou Faible. S'il existe d'autres tâches de priorité élevée, CA Identity Manager effectue la première étape de traitement pour le premier événement de priorité élevée, puis place cet événement à la fin de la liste des autres événements de priorité élevée.
- Installez un serveur CA Identity Manager distinct dédié à la gestion des opérations de chargement en bloc.

## Directives pour l'optimisation des tâches

Les tâches par défaut déployées lors de la création d'un environnement CA Identity Manager sont configurées pour prendre en charge un large éventail de scénarios d'administration. La plupart des implémentations de CA Identity Manager ne requièrent pas toutes les fonctionnalités fournies dans les tâches par défaut. Après avoir créé un environnement CA Identity Manager, modifiez ces tâches pour répondre à vos besoins d'administration.

Les étapes suivantes fournissent des directives pour modifier ces tâches :

- **Création de tâches de gestion d'utilisateurs spécialisées**

  Les tâches par défaut Créer un utilisateur, Modifier un utilisateur et Afficher l'utilisateur fournissent des fonctionnalités administratives complètes. Dans la plupart des implémentations, seul un petit nombre d'administrateurs requièrent toutes les fonctionnalités disponibles.

  Créez des tâches qui incluent uniquement les fonctionnalités requises. Par exemple, si la plupart des tâches de gestion d'utilisateurs impliquent uniquement la gestion de profils et de groupes, créez une tâche Modifier un utilisateur qui inclut uniquement les onglets Profil et Groupe. Supprimez les onglets Rôles d'administration, Rôles d'accès, et Rôles de provisionnement, qui sont disponibles dans la tâche Modifier un utilisateur par défaut.

  Les onglets non utilisés peuvent occasionner des surcharges importantes si vous les conservez dans les tâches fréquemment utilisées. Cela est particulièrement vrai lorsque vous utilisez un client de service Web d'exécution des tâches, dans lequel ces onglets peuvent être involontairement activés via la classe Java tab fournie avec CA Identity Manager.

  Les tâches spécialisées que vous créez doivent correspondre au modèle d'administration déléguée (page 65) que vous avez défini pour votre environnement.

- **Désactivation de la gestion des administrateurs dans les onglets de relation**

  Par défaut, tous les onglets de relation permettent de gérer des droits d'administration pour l'objet géré par l'onglet, comme les rôles et les groupes. Cette fonctionnalité n'est pas nécessaire aux administrateurs dans la plupart des implémentations.

Pour éliminer les surcharges supplémentaires qui se produisent lors de l'évaluation des droits administratifs, désactivez l'option Gérer les administrateurs dans les onglets suivants, si cette fonctionnalité n'est pas requise :

- Rôles d'administration
- Rôles de provisionnement
- Rôles d'accès
- Groupes

Pour permettre aux utilisateurs de gérer des droits d'administration dans des onglets spécifiques, créez des copies des onglets par défaut, activez l'option Gérer les administrateurs et désactivez l'option Gérer les membres. Ajoutez les nouveaux onglets à des tâches spécialisées, qui sont uniquement utilisées par les administrateurs qui en ont besoin.

- **Activation des recherches figurant dans la portée dans les onglets de relation de rôle**

  Vous pouvez configurer chaque onglet de rôle pour inclure des recherches qui permettent aux administrateurs de spécifier des critères pour les nouveaux rôles à affecter à un utilisateur. Les recherches de rôle limitent le nombre de règles de stratégies de membre et d'administration à évaluer pour déterminer les rôles qu'un administrateur peut affecter à un utilisateur.

- **Définition des options de synchronisation de tâches**

  Pour chaque tâche CA Identity Manager, vous pouvez spécifier une option de synchronisation de l'utilisateur, qui synchronise les utilisateurs avec des stratégies d'identité, et une option de synchronisation de compte de provisionnement, qui synchronise les utilisateurs avec des comptes provisionnés. Ces options vous permettent de synchroniser des utilisateurs lorsqu'une tâche ou un événement se termine.

  Pour réduire la durée d'évaluation et de traitement, définissez l'exécution de la synchronisation à la fin d'une tâche, et non à la fin des événements.

# Directives pour l'optimisation des membres de groupe/des administrateurs

Pour améliorer les performances de recherches de membres de groupe et d'administrateurs, tenez compte de ce qui suit :

- Définissez des attributs connus dans le fichier de configuration d'annuaire (directory.xml), qui décrit la structure et le contenu du référentiel d'utilisateurs à CA Identity Manager.

  Un attribut connu est un attribut qui a une signification spéciale dans CA Identity Manager.

  Pour améliorer les recherches de membres de groupe et d'administrateurs, définissez les attributs connus suivants pour l'objet d'utilisateur :

  **%MEMBER_OF%**

  Identifie un attribut dans l'objet d'utilisateur qui stocke une liste des groupes dont l'utilisateur est membre.

  Une fois défini, cet attribut peut empêcher CA Identity Manager d'effectuer des recherches sur tous les membres de tous les groupes du référentiel d'utilisateurs. Lorsque les recherches sont effectuées sur de grands groupes, les performances peuvent être affectées significativement.

  **%ADMINISTRATOR_OF%**

  Identifie un attribut dans l'objet d'utilisateur qui stocke une liste des groupes dont l'utilisateur est un administrateur.

  Comme l'attribut %MEMBER_OF%, cet attribut connu permet d'éliminer les longues recherches de groupe.

- Spécifiez le type de groupe dans le fichier de configuration d'annuaire.

  CA Identity Manager prend en charge trois types de groupes : les groupes standard, les groupes imbriqués et les groupes dynamiques.

  Lorsque vous définissez l'objet de groupe dans le fichier de configuration d'annuaire, vous pouvez spécifier le type des groupes que le référentiel d'utilisateurs prend en charge. Si votre implémentation ne prend pas en charge les groupes imbriqués ou dynamiques, définissez l'attribut GroupType comme suit :

  GroupType = NONE

  Le paramètre NONE spécifie la prise en charge des groupes standard.

  Le paramètre de type de groupe par défaut ALL peut affecter les performances.

  **Remarque :** Pour plus d'informations sur les attributs connus et les types de groupe dans le fichier de configuration d'annuaire, consultez le *Manuel de configuration*.

- Définissez les index de cache de l'annuaire de provisionnement pour améliorer les performances du groupe GlobalGroup.

  Pour les implémentations CA Identity Manager qui incluent un référentiel d'utilisateurs combiné à un annuaire de provisionnement, vous pouvez optimiser l'appartenance au groupe GlobalGroup pour l'évaluation de règle de stratégie pour les rôles et les stratégies d'identité.

  Pour activer cette optimisation, indexez les attributs suivants, que le serveur de provisionnement utilise pour résoudre l'appartenance au groupe, dans le cache d'annuaire de provisionnement :

  **eTID**

  Attribut d'ID d'objet unique. Pour les recherches d'appartenance au groupe, la valeur est un utilisateur ou un groupe impliqué dans la recherche.

  **eTPID**

  ID parent de l'objet utilisé lors de la recherche de relations d'appartenance

  **eTCID**

  ID enfant de l'objet utilisé lors de la recherche de relations d'appartenance

  En outre, ajoutez les entrées d'hachage suivantes :

  **eTSuperiorClass**

  Type de l'objet parent dans une recherche d'appartenance

  **eTSubordinateClass**

  Type de l'objet enfant dans une recherche d'appartenance

  **Remarque :** Pour plus d'informations sur le cache d'annuaire de provisionnement, consultez le *Manuel d'installation*.

# Optimisations de stratégie d'identité

Une *stratégie d'identité* désigne un ensemble de modifications métiers qui ont lieu lorsqu'un utilisateur satisfait à une certaine condition ou règle. Ces modifications peuvent inclure affecter ou retirer des rôles, affecter ou retirer l'appartenance à un groupe et la mise à jour des attributs d'un profil d'utilisateur.

CA Identity Manager évalue les stratégies d'identité lors de la synchronisation de l'utilisateur.

Les performances des stratégies d'identité sont affectées par :

- La configuration des stratégies d'identité
- La fréquence de synchronisation de l'utilisateur

## Synchronisation des utilisateurs et des stratégies d'identité

Lorsque vous utilisez des stratégies d'identité, il est important que vous compreniez l'évaluation des stratégies par CA Identity Manager et leur application aux utilisateurs. Si vous ne comprenez pas parfaitement le processus de synchronisation des utilisateurs, vous risquez de configurer des ensembles de stratégies d'identité qui génèrent des résultats indésirables.

La procédure suivante décrit l'évaluation et l'application des stratégies d'identité par CA Identity Manager.

1. Le processus de synchronisation des utilisateurs commence :
   - **Automatiquement** : vous pouvez configurer des tâches CA Identity Manager pour déclencher automatiquement la synchronisation des utilisateurs.
   - **Manuellement** : la tâche de synchronisation de l'utilisateur de la console d'utilisateur permet de synchroniser un utilisateur.
2. CA Identity Manager détermine l'ensemble de stratégies d'identité qui s'applique à un utilisateur.
3. CA Identity Manager compare cet ensemble à la liste des stratégies qui ont déjà été appliquées à cet utilisateur.

   **Remarque** : La liste des stratégies ayant été appliquées à un utilisateur est stockée dans l'attribut %IDENTITY_POLICY% du profil de l'utilisateur. Pour obtenir des informations sur la configuration de cet attribut, reportez-vous au *manuel de configuration*.
   - Si une stratégie d'identité figure dans la liste des stratégies applicables *et* qu'elle n'a *pas* déjà été appliquée à l'utilisateur, CA Identity Manager l'ajoute à une liste d'affectation.
   - Si une stratégie d'identité figure dans la liste des stratégies applicables, qu'elle a déjà été appliquée à l'utilisateur et que son paramètre Appliquer une fois est désactivé, CA Identity Manager l'ajoute à la liste de réaffectation.
   - Si une stratégie d'identité ne figure pas dans la liste des stratégies applicables, qu'elle a déjà été appliquée à l'utilisateur et que ce dernier ne remplit plus les conditions de cette stratégie, CA Identity Manager ajoute cette stratégie à une liste de désaffectation.
4. Une fois que CA Identity Manager a évalué toutes les stratégies d'un utilisateur, il les applique dans l'ordre suivant.
   a. Stratégies d'identité de la liste de désaffectation
   b. Stratégies d'identité de la liste d'affectation
   c. Stratégies d'identité de la liste de réaffectation

5. Une fois les stratégies d'identité appliquées, CA Identity Manager les réévalue pour savoir si des modifications supplémentaires sont requises, selon les modifications apportées au cours du premier processus de synchronisation (étapes 2 à 4).

   Cette étape vise à vérifier que les modifications apportées en appliquant les stratégies d'identité n'ont pas déclenché d'autres stratégies d'identité.

6. CA Identity Manager continue à réévaluer et à appliquer les stratégies d'identité jusqu'à ce que l'utilisateur soit synchronisé avec toutes les stratégies applicables ou jusqu'à ce que CA Identity Manager atteigne le niveau de traitement récursif maximum, défini dans la console de gestion.

   Par exemple, une stratégie d'identité peut modifier un département d'utilisateur lorsque qu'un rôle est affecté à ce dernier. Le nouveau département déclenche une autre stratégie d'identité. Cependant, si le niveau de récursion est défini sur 1, la modification suivante n'est pas effectuée tant que l'utilisateur n'a pas été synchronisé à nouveau.

   Pour plus d'informations sur la définition du niveau de récursion, reportez-vous à l'Aide en ligne de la console de gestion.

## Conception de stratégies d'identité efficaces

Utilisez les directives suivantes lorsque vous créez des stratégies d'identité :

- **Limitation du nombre d'objets de stratégie**

  CA Identity Manager crée des objets dans le référentiel d'objets qui prennent en charge les stratégies d'identité. Pour réduire le nombre d'objets dans le référentiel d'objets, créez des stratégies d'identité avec des expressions complexes.
  Une approche similaire est recommandée pour les stratégies de rôle (page 76).

- **Limitation des itérations d'ensemble de stratégies d'identité**

  Vous pouvez configurer le niveau de traitement récursif pour une stratégie d'identité, qui détermine le nombre de fois que CA Identity Manager évalue et applique des stratégies d'identité lors de la synchronisation d'un utilisateur. Par exemple, une stratégie d'identité peut modifier un département d'utilisateur lorsque qu'un rôle est affecté à ce dernier. Le nouveau département déclenche une autre stratégie d'identité. Cependant, si le niveau de récurrence est défini sur 1, la modification suivante n'est pas effectuée tant que l'utilisateur n'a pas été synchronisé à nouveau.

  Définir le niveau de traitement récursif permet de limiter le nombre d'évaluation des stratégies d'identité.

- **Limitation des dépendances entre les règles de stratégie d'identité**

  Vous pouvez créer une stratégie d'identité dans laquelle l'action de modification (Action lors de l'application de la stratégie ou Action lors de la suppression de la stratégie) d'une stratégie est utilisée dans la condition de stratégie d'identité d'une autre stratégie, comme illustré dans le tableau suivant.

| Condition de stratégie d'identité | Action lors de l'application de la stratégie | Action lors de la suppression de la stratégie |
|---|---|---|
| où (Job Code = "100") | Promouvoir en tant que membre du rôle de provisionnement Gestionnaire de comptes | Supprimer le membre du rôle de provisionnement Gestionnaire de comptes |
| Membres du rôle de provisionnement Gestionnaire de comptes | Promouvoir en tant que membre du groupe Gestionnaire de comptes | Supprimer le membre du groupe Gestionnaire de comptes |

  Lorsque ce type de stratégie est évalué, les modifications doivent être évaluées et appliquées deux fois au minimum pour confirmer que les deux conditions sont remplies. Le niveau de traitement récursif défini pour un environnement CA Identity Manager entier doit être supérieur à 1, ce qui déclenche des évaluations supplémentaires pour chaque ensemble de stratégies d'identité.

## Limitation des tâches déclenchant la synchronisation de l'utilisateur

Les stratégies d'identité sont évaluées et appliquées au cours du processus de synchronisation de l'utilisateur. Vous pouvez configurer la synchronisation automatique en spécifiant l'une des options de synchronisation suivantes pour une tâche :

**A la fin de la tâche**

CA Identity Manager démarre le processus de synchronisation de l'utilisateur une fois tous les événements d'une tâche terminés.

**A chaque événement**

CA Identity Manager démarre le processus de synchronisation de l'utilisateur à la fin de chaque événement d'une tâche.

Pour de meilleures performances, limitez le nombre de tâches qui déclenchent la synchronisation automatique de l'utilisateur.

Lors de la configuration de la synchronisation de l'utilisateur, tenez compte de l'approche suivante :

- **Désactivez la synchronisation de l'utilisateur pour les tâches de mot de passe.**

  Dans la plupart des cas, les mots de passe ne sont pas utilisés dans les conditions de stratégie d'identité.

- **Désactivez la synchronisation de l'utilisateur pour la tâche Synchroniser l'utilisateur.**

  Cette tâche déclenche l'évaluation de la stratégie d'identité et CA Identity Manager effectuera l'évaluation à nouveau si l'option de synchronisation de l'utilisateur est activée.

- **Créez des tâches spécialisées.**

  Lorsque cela est possible, créez des tâches qui effectuent des modifications qui déclenchent des conditions de stratégie d'identité et activent les synchronisations de l'utilisateur pour ces tâches uniquement.

## Optimisation de l'évaluation de règle de stratégie d'identité

Pour réduire le temps d'évaluation des conditions de stratégie d'identité, vous pouvez activer l'option d'évaluation dans la mémoire. Lorsque l'option d'évaluation de mémoire est activée, CA Identity Manager récupère des informations sur un utilisateur à évaluer à partir du référentiel d'utilisateurs et enregistre une représentation de celui-ci dans la mémoire. CA Identity Manager utilise la représentation dans la mémoire pour comparer les valeurs d'attribut par rapport aux conditions de stratégie. Cela limite le nombre d'appels effectué directement par CA Identity Manager au référentiel d'utilisateurs.

**Remarque :** Pour plus d'informations sur l'option d'évaluation de mémoire, consultez le *Manuel de configuration*.

# Réglage du référentiel d'utilisateurs

Le réglage du référentiel d'utilisateurs comporte un certain nombre d'étapes, notamment :

- L'optimisation de la structure du référentiel d'utilisateurs
- Le réglage des référentiels sous-jacents
- L'implémentation de l'équilibrage de la charge et de la réplication

Ces étapes dépendent du type de référentiel d'utilisateurs que vous utilisez. Pour ajuster des informations dans ces zones, consultez la documentation de la base de données ou de l'annuaire qui contient le référentiel d'utilisateurs.

Outre les remarques générales sur le réglage, les remarques suivantes sont propres à CA Identity Manager :

- **Mesure des performances de recherche du référentiel d'utilisateurs**

  Pour des performances optimales, les recherches d'évaluation de stratégie CA Identity Manager doivent prendre entre 10 et 20 millisecondes.

  Pour vous assurer que ces recherches peuvent être effectuées de façon cohérente dans les temps recommandés, testez les performances de recherche sous différentes conditions de charge.

  Vous pouvez également utiliser cette mesure pour déterminer lorsqu'un référentiel d'utilisateurs atteint ses limites physiques et que des serveurs supplémentaires sont requis pour l'équilibrage de la charge.

- **Indexage des attributs**

  Indexez chaque attribut utilisé dans une stratégie de rôle ou une stratégie d'identité. L'indexage des attributs peut améliorer significativement les performances.

  **Remarque :** Pour plus d'informations sur l'indexation des attributs, consultez la documentation de l'annuaire LDAP ou de la base de données relationnelles qui contient le référentiel d'utilisateurs.

- **Mise en cache des liaisons LDAP**

  Dans CA Identity Manager, toutes les liaisons LDAP d'annuaire sont exécutées par le proxy défini par l'utilisateur dans l'objet d'annuaire CA Identity Manager. Pour chaque connexion, la même liaison LDAP est effectuée pour le même utilisateur, à plusieurs reprises.

  Si vous utilisez un annuaire LDAP comme référentiel d'utilisateurs, configurez l'annuaire pour mettre en cache les liaisons ou les sessions LDAP, si cette option est prise en charge.

- **Activation des caches de référentiel d'utilisateurs**

  Lorsque CA Identity Manager évalue les décisions de stratégie pour un utilisateur, ces informations sont stockées dans un cache d'autorisation. Lorsque les informations mises en cache expirent, CA Identity Manager évalue à nouveau toutes les stratégies pour cet utilisateur.

  Pour améliorer les performances de recherches de référentiel d'utilisateurs dans les évaluations de règle de stratégie ultérieures, permettez au référentiel d'utilisateurs de mettre en cache les données recherchées, si cette option est prise en charge.

  CA Directory inclut le cache dxCache, qui est une implémentation de base de données dans la mémoire et qui peut effectuer des recherches dans les données mises en cache.

  **Remarque :** Pour en savoir plus sur CA Directory, reportez-vous au manuel *CA Directory Administrator Guide.*

# Réglage des composants de provisionnement

Lorsqu'une implémentation CA Identity Manager inclut le provisionnement, utilisez les optimisations suivantes pour obtenir des performances optimales :

- Optimisez la connexion entre le serveur CA Identity Manager et le serveur de provisionnement

  CA Identity Manager communique avec le serveur de provisionnement à l'aide de l'API Java IAM (JIAM). Pour améliorer les performances de communication, configurez les éléments suivants :

  - Pool de sessions JIAM pour plusieurs connexions au serveur de provisionnement

    **Remarque :** Il est recommandé de définir la valeur de sessions initiale sur 8 et le nombre maximum de sessions sur 128.

  - Cache JIAM pour les objets récupérés à partir du serveur de provisionnement

  **Remarque :** Pour plus d'informations sur les paramètres de configuration JIAM, consultez le *Manuel d'administration*.

- Définissez l'exécution de la synchronisation des comptes à la fin d'une tâche (page 84), au lieu de la fin d'un événement.
- Ajustez le serveur de provisionnement.

  **Remarque :** Pour plus d'informations, consultez le *Manuel d'administration* et le *Manuel d'installation*.

# Réglage des composants d'exécution

Dans CA Identity Manager, les modifications métier sont effectuées à l'aide de tâches. Une tâche inclut un ou plusieurs événements, qui représentent des activités effectuées par CA Identity Manager pour terminer la tâche. Par exemple, une tâche Créer un utilisateur peut inclure les événements CreateUserEvent et AddToGroupEvent.

CA Identity Manager inclut les composants suivants, qui traitent des tâches et des événements lors de l'exécution :

- Bases de données CA Identity Manager, qui prennent en charge la fonctionnalité CA Identity Manager.
- Messages JMS, qui sont responsables du traitement des événements.

## Réglage des bases de données CA Identity Manager

Lors de l'exécution des tâches, CA Identity Manager utilise les bases de données suivantes :

- Persistance des tâches

  Gère les informations sur les tâches et les événements CA Identity Manager dans le temps. Cela permet de restaurer le dernier état connu des événements et des tâches en cas d'échec système.

  **Remarque :** Cette base de données affecte le plus significativement les performances de CA Identity Manager, car une tâche et ses événements sont enregistrés et récupérés à partir de la base de données lors des transitions d'état.

- Audit

  Fournit un enregistrement sous forme d'historique des opérations réalisées dans un environnement CA Identity Manager.

- Flux de travaux

  Enregistre les définitions, les jobs, les scripts et d'autres données de processus de flux de travaux requises par le moteur de flux de travaux.

- Génération de rapports

  Enregistre les données de cliché, qui reflètent l'état actuel des objets dans CA Identity Manager au moment de la prise du cliché.

CA Identity Manager communique avec chaque base de données à travers un pool de connexions JDBC. Vous créez et configurez un pool de connexions JDBC dans le serveur d'applications qui héberge CA Identity Manager. Lorsque vous configurez le pool de connexions JDBC, tenez compte de ce qui suit :

- Considérez le nombre de tâches parallèles qui s'exécuteront simultanément.
- Considérez les autres composants d'exécution lorsque vous configurez la taille du pool de connexions JDBC. Chaque composant d'exécution fonctionne avec les autres composants d'exécution.

  **Remarque :** Il est recommandé de définir la valeur initiale du pool de sessions sur 128.
- Pour la base de données de persistance des tâches, le nombre de connexions à la base de données dans le pool doit permettre à chaque tâche s'exécutant de récupérer et de mettre à jour les données de tâche et d'événements pendant la vie de la tâche.
- La base de données de persistance des tâches utilise des instructions prédéfinies. Assurez-vous de configurer le cache d'instruction prédéfini pour la base de données que vous utilisez pour stocker les données de persistance de tâche.

  **Remarque :** Pour obtenir des informations sur la configuration du cache d'instruction prédéfini, consultez la documentation de la base de données que vous utilisez pour la persistance des tâches.

## Paramètres de JMS

Une tâche CA Identity Manager inclut des événements, c'est-à-dire des actions que CA Identity Manager effectue pour terminer une tâche.

Pendant le cycle de vie d'un événement, ses états sont les suivants :

- BEGIN
- APPROVED
- EXECUTING
- COMPLETED
- INVALID

Les événements contrôlés par les flux de travaux peuvent également avoir les états suivants :

- PENDING
- REJECTED

CA Identity Manager utilise les messages JMS pour contrôler les transitions d'état.

## Contrôle des transitions d'événement par les messages JMS

CA Identity Manager utilise des messages JMS pour contrôler les transitions d'état d'un événement. La procédure suivante décrit les étapes impliquées :

1. Un utilisateur soumet une tâche.
2. La tâche génère un ou plusieurs événements.
3. Lorsqu'un événement est prêt à être traité, CA Identity Manager définit l'état de l'événement sur BEGIN et la persistance de l'événement est effectuée dans la base de données de persistance des tâches.
4. CA Identity Manager crée un message JMS contenant l'ID d'événement et envoie ce message dans la file d'attente de message d'événement.
5. Une fois le message reçu, JMS invoque alors une instance du bean généré par message d'événement, qui est une implémentation du contrôleur d'événements.
6. Le contrôleur d'événements utilise l'ID de l'événement dans le message pour récupérer l'événement à partir de la base de données de persistance des tâches, puis exécute les actions pour l'état actuel de l'événement.
7. Une fois cet état terminé, l'événement est défini sur l'état suivant, la persistance est effectuée dans la base de données de persistance des tâches et un nouveau message JMS est envoyée pour le traitement de l'état suivant.

   Ce cycle se poursuit jusqu'à ce que l'événement ait terminé sa machine à états.

## Messages JMS et performances

Il existe trois à cinq états d'événement qui requièrent des messages JMS pour leur transition :

- BEGIN
- PENDING (uniquement sous le contrôle du flux de travaux)
- APPROVED ou REJECTED
- EXECUTING
- COMPLETED ou INVALID

Pour traiter un événement unique, les actions suivantes ont lieu :

- Entre et cinq envois dans la file d'attente de messages d'événements
- Entre trois et cinq appels du bean généré par message
- Entre six et dix connexions à la base de données de persistance des tâches (une action de lecture et une action d'écriture par état)

Ces actions peuvent affecter la durée de traitement d'une tâche.

Pour optimiser les performances pendant les transitions d'état, ajustez les ressources JMS dans le serveur d'applications qui héberge CA Identity Manager, afin que les ressources JMS adéquates soient disponibles.

## Réglage des paramètres JMS

Les paramètres de réglage JMS du serveur d'applications suivants définissent les connexions à la file d'attente et les pools d'instance de bean généré par message.

- **Réglage de JMS pour WebSphere**

  WebSphere fournit deux paramètres de sous-objets de connexion de file d'attente que vous pouvez configurer pour améliorer les performances. Utilisez la console d'administration WebSphere pour définir les propriétés suivantes :

  - Sous Ressources, recherchez les sous-objets de connexion de file d'attente iam-im-neteQCF et iam-im-wpConnectionFactory.
  - Pour chaque sous-objet, modifiez les propriétés du pool de connexions en définissant le nombre maximum de connexions sur 128.

- **Réglage de WebLogic**

  Dans les serveurs d'applications WebLogic, les sous-objets de connexion de file d'attente obtiennent des threads de gestion de connexion à partir du pool de threads JMS du serveur ou du pool d'exécution par défaut, selon la taille du pool de threads JMS. Si la taille du pool de threads JMS est 0, WebLogic utilise les threads du pool d'exécution.

  Il est recommandé de définir le nombre de threads du pool de threads JMS sur la même valeur que pour la taille maximum du pool du bean généré par message d'événement CA Identity Manager, défini sur 128 par défaut.

  Vous utilisez la console de serveur WebLogic pour définir la taille du pool de threads JMS dans les propriétés des services JMS pour le domaine et le serveur sur lequel CA Identity Manager est installé.

La taille du pool de bean généré par message d'événement CA Identity Manager est définie en modifiant le paramètre max-beans-in-free-pool du fichier de descripteur à l'emplacement suivant :

WebLogic_home\domain\applications\iam_im.ear\identityminder_ejb.jar\META-INF\weblogic-ejb-jar.xml

```
<weblogic-enterprise-bean>
        <ejb-name>SubscriberMessageEJB</ejb-name>
        <message-driven-descriptor>
            <pool>
                <max-beans-in-free-pool>128</max-beans-in-free-pool>
                <initial-beans-in-free-pool>16</initial-beans-in-free-pool>
            </pool>
            <destination-jndi-name>com.netegrity.ims.msg.queue</destination-
jndi-name>
        </message-driven-descriptor>
    </weblogic-enterprise-bean>
```

- **Réglage pour JBoss**

  Dans les serveurs d'applications JBoss, les sous-objets de connexion de file d'attente obtiennent des threads de gestion de connexion à partir du sous-objet de session de pool JMS standard du serveur. Par défaut, le nombre de threads maximum est défini sur 15.

  Il est recommandé de définir cette valeur sur la même valeur que pour la taille maximum du conteneur de bean de message standard.

  Le sous-objet de section de pool de sessions JMS est placé dans l'élément MaximumSize de JMSContainerInvoker dans le fichier suivant :

  *répertoire_installation_jboss*\server\default\conf\standardjboss.xml

```
<invoker-proxy-binding>
         <name>message-driven-bean</name>
         ….
         <proxy-factory-config>

<JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>

<ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
            <MaximumSize>128</MaximumSize>
            <MaxMessages>1</MaxMessages>
            ….
         </proxy-factory-config>
     </invoker-proxy-binding>
```

La taille de pool du bean généré par message d'événement CA Identity Manager est définie en modifiant la valeur de taille maximum dans le fichier de descripteur suivant :

*répertoire_installation_jboss*\server\default\conf\standardjboss.xml

```
<container-configuration>
         <container-name>Standard Message Driven Bean</container-name>
         <call-logging>false</call-logging>
         <invoker-proxy-binding-name>message-driven-bean</invoker-proxy-
binding-name>
        ……
         <container-pool-conf>
            <MaximumSize>128</MaximumSize>
         </container-pool-conf>
   </container-configuration>
```

## Réglage des performances de JBoss 5

Dans une installation par défaut de JBoss 5, l'analyseur de déploiement à chaud de JBoss s'exécute toutes les 5 secondes, ce qui affecte les performances. Vous pouvez désactiver cette fonctionnalité, si vous n'en avez pas besoin ou vous pouvez modifier sa fréquence d'exécution.

**Pour désactiver ou modifier le déploiement à chaud :**

1. Modifiez le fichier hdscanner-jboss-beans.xml à l'emplacement :

   **Noeud unique :** *répertoire_installation_jboss*/server/default/deploy

   **Cluster :** *répertoire_installation_jboss*/server/all/deploy

2. Pour désactiver cette fonctionnalité, ajoutez la ligne suivante dans le bean HDScanner :
   `<attribute name="ScanEnabled">False</attribute>`

3. Pour modifier la fréquence d'analyse, augmentez la valeur de l'attribut scanPeriod sur une valeur supérieure à 5000 millisecondes.

**Remarque :** Pour obtenir plus d'informations, reportez-vous à l'adresse http://community.jboss.org/wiki/JBossASTuningSlimming.

**Pour résoudre les problèmes de mémoire insuffisante :**

Des exceptions de mémoire insuffisante peuvent s'afficher si la taille de segment de mémoire Java est trop petite. Une taille initiale de 1024 est recommandée.

# Chapitre 7: Création d'un plan de récupération après sinistre

Ce chapitre traite des sujets suivants :



## Perte de service suite à un sinistre

En cas de sinistre, les utilisateurs peuvent perdre l'accès aux services critiques pour leurs jobs et ils ne peuvent pas fournir de services à d'autres utilisateurs.

L'urgence à restaurer l'accès à ces services dépend de l'utilisation réelle de CA Identity Manager. Dans certaines organisations, les utilisateurs requièrent un accès ininterrompu aux services fournis par CA Identity Manager, alors que d'autres requièrent la restauration du système sous un jour. Dans tous les cas, il est recommandé d'effectuer les préparations nécessaires à la protection de votre implémentation CA Identity Manager contre les événements qui causent une perte partielle ou complète des systèmes.

La configuration d'une architecture CA Identity Manager redondante vous assure la haute disponibilité des services auprès des utilisateurs.  Lorsqu'un échec d'un composant principal se produit, le composant secondaire correspondant continue de fournir le même service. De plus, vous pouvez régulièrement sauvegarder les systèmes et les logiciels critiques, afin d'être en mesure de restaurer un système ou des données perdues.

Ce document fournit des directives générales sur la planification de ces scénarios. Utilisez ces directives pour développer des procédures de récupération après sinistre spécifiques qui répondent aux besoins de votre organisation.

# Planification de la récupération après sinistre

Pour développer un plan de récupération après sinistre efficace, effectuez les procédures qui sont détaillées dans ce chapitre.

| ✓ | Phase |
|---|---|
| | 1. Définition de conditions pour la récupération après sinistre (page 103)<br>En fonction des besoins de votre organisation, identifiez les types de sinistre à prévoir et le délai de restauration des services. |
| | 2. Conception d'une architecture redondante (page 104)<br>Selon vos besoins, concevez une architecture constituée de composants redondants à un emplacement distant. |
| | 3. Développement de plans de sauvegarde (page 106)<br>Pour protéger votre installation, développez des plans pour la sauvegarde des composants. |
| | 4. Développement de procédures de restauration (page 107)<br>Développez des procédures pour restaurer les composants perdus. |
| | 5. Documentation du plan de récupération (page 110)<br>Documentez les plans de récupération de CA Identity Manager après sinistre. |
| | 6. Test du plan de récupération (page 111)<br>Selon les procédures de récupération après sinistre que vous avez définies, vérifiez que vous pouvez rétablir l'implémentation CA Identity Manager telle qu'elle existait avant le sinistre. |
| | 7. Formation à la récupération après sinistre (page 112)<br>Finalisez votre planification par une formation des responsables de la récupération des systèmes après sinistre. |

# Définition de conditions pour la récupération après sinistre

Tenez compte des directives générales suivantes lorsque vous définissez les conditions du plan de récupération après sinistre.

1. Réunissez une équipe avec les connaissances suivantes :
   - Connaissances de l'architecture et des systèmes qui prennent en charge CA Identity Manager.
   - Connaissances de la sauvegarde des bases de données relationnelles et des référentiels d'utilisateur LDAP utilisés par CA Identity Manager
2. Identifiez les scénarios de sinistre potentiels à résoudre, y compris la perte partielle ou complète des systèmes sur un ou plusieurs sites.
3. Répertoriez les systèmes critiques de votre installation.
4. Définissez le temps d'indisponibilité maximum acceptable pour chacun de ces systèmes.

   Par exemple, la restauration des systèmes qui prennent en charge un serveur auxiliaire peut avoir une faible priorité.

# Conception d'une architecture redondante

Pour protéger l'installation contre l'échec d'un composant critique, tenez compte des actions de protections suivantes recommandées utilisant des composants secondaires (serveurs et annuaires) et des bases de données redondantes à des emplacements distants.

Pour configurer une architecture redondante pour CA Identity Manager, reportez-vous au *Manuel d'installation.* Incluez les composants suivants :

- Des noeuds de serveur d'applications CA Identity Manager redondants dans un cluster
- Un cluster de serveurs de stratégies pour le basculement (si vous utilisez CA SiteMinder pour protéger CA Identity Manager)
- Des serveurs de provisionnement, des annuaires de provisionnement et des serveurs de connecteurs secondaires. Si un composant principal est perdu, le système utilise le composant secondaire.

Configurez la redondance des bases de données et notamment :

- L'une des bases de données d'exécution qui font partie de CA Identity Manager, telles que la base de données de flux de travaux ou d'audit.

  Pour plus d'informations, consultez la documentation Oracle ou Microsoft SQL Server.
- La base de données BusinessObjects si vous utilisez un serveur de rapports.

  Consultez la documentation BusinessObjects Enterprise r2 et r2 SP4 sur le site Web de la documentation SAP.

## Serveurs auxiliaires CA Identity Manager

La configuration de noeuds de serveur d'applications redondants pour le serveur CA Identity Manager vous apporte différents avantages relatifs à la modularité, aux performances et à la récupération après sinistre en cas d'échec des serveurs. La méthode la plus commune pour configurer le basculement pour un serveur d'applications est de créer un cluster. Les procédures de création de cluster sont traitées dans la section de cluster du *Manuel d'installation*.

**Remarque :** Pour CA Identity Manager r12.0 et versions ultérieures, un cluster de serveur d'applications est la seule méthode valide pour implémenter un déploiement multi-noeud. Les environnements CA Identity Manager requièrent une architecture de cluster J2EE standard, qui utilise des files d'attente JMS pour la dorsale. En conséquence, la seule méthode valide pour avoir plusieurs noeuds dans une configuration CA Identity Manager est de définir un cluster de serveur d'applications.

Pour plus de détails sur ce changement, consultez le document TechDoc 545594.

## Composants de provisionnement secondaires

Vous pouvez définir un composant secondaire pour certains composants de provisionnement, afin de garantir leur haute disponibilité. Le composant secondaire doit se trouver sur un site distant pour une meilleure protection.

Pour obtenir des détails sur la configuration des serveurs et des annuaires secondaires, reportez-vous au chapitre traitant du provisionnement de haute disponibilité du *Manuel d'installation*.

**Annuaires de provisionnement multi-site**

Vous pouvez créer des annuaires de provisionnement principaux et des annuaires de provisionnement secondaires à un emplacement distant. CA Directory recommande l'installation de trois annuaires de provisionnement, un principal et deux annuaires secondaires.

**Serveurs de provisionnement multi-site**

Pour une protection efficace contre l'échec du serveur de provisionnement principal, vous pouvez configurer un serveur de provisionnement auxiliaire. La différence entre les serveurs de provisionnement principaux et auxiliaires est que l'installation du serveur principal remplit les entrées du conteneur d'annuaire de provisionnement. Ces entrées seront supprimées lors de la désinstallation du serveur principal. Mise à part ces différences à l'installation et à la désinstallation, le serveur principal et les serveurs auxiliaires fonctionnent de la même manière.

**Serveurs de connecteurs multi-site**

Vous pouvez configurer plusieurs serveurs de connecteurs Java ou C++ pour le même terminal ou type de terminal.

Pour chaque serveur de connecteurs que vous configurez, configurez un serveur de connecteurs auxiliaire sur un emplacement distant pour gérer les mêmes terminaux. Si un échec du serveur de connecteurs se produit, le serveur auxiliaire gère immédiatement les communications avec les terminaux.

## Base de données redondantes

Les logiciels de base de données pris en charge, Microsoft SQL Server et Oracle, prennent en charge les bases de données redondantes. Si un échec de la base de données principale se produit, la base de données redondante est disponible immédiatement. La base de données redondante doit se trouver sur un site distant en cas d'affectation complète du site.

# Développement de plans de sauvegarde

Pour une protection efficace contre la perte d'un ou de tous les systèmes, utilisez le stockage hors site pour toutes les données que vous sauvegardez et un plan de sauvegarde qui répond au temps d'indisponibilité maximum que vous définissez. Les procédures de sauvegarde et de restauration utilisent des applications différentes et doivent donc être coordonnées pour la récupération complète du système CA Identity Manager.

Incluez les composants suivants dans vos plans de sauvegarde :

| Composant | Description | Méthode de sauvegarde |
|---|---|---|
| Référentiel d'utilisateurs CA Identity Manager | Annuaire d'utilisateurs ou base de données relationnelles LDAP qui contient les enregistrements des utilisateurs CA Identity Manager. | Consultez la documentation fournie avec votre base de données ou le logiciel LDAP. |
| Bases de données CA Identity Manager | Bases de données de persistance de tâche, de flux de travaux, d'audit, de référentiel d'objets, de rapports et d'archivage de persistance de tâche.<br>Les bases de données de flux de travaux, de persistance de tâche et d'audit sont les plus fréquemment mise à jour et les sauvegardes doivent être planifiées en conséquence. | Consultez la documentation fournie avec le logiciel de la base de données. |
| Référentiel de stratégies SiteMinder | Annuaire d'utilisateurs ou base de données relationnelles LDAP contenant des objets destinés au serveur de stratégies SiteMinder, si vous utilisez CA SiteMinder. | Consultez la documentation fournie avec votre base de données ou le logiciel LDAP. |
| Annuaire de provisionnement | Annuaire d'utilisateurs LDAP qui contient des enregistrements pour le provisionnement des utilisateurs et des objets. | Consultez la documentation CA Directory. |
| Référentiels JMS persistants du serveur d'applications | Référentiels utilisés pour les messages de traitement d'événement de tâche CA Identity Manager | Consultez la documentation du serveur d'applications. |
| Bases de données de rapports | Base de données de clichés<br>Base de données BusinessObjects | Consultez la documentation fournie avec le logiciel de la base de données. |
| Rapports personnalisés | Rapports personnalisés et fichiers XML associés | Consultez la documentation BusinessObjects Enterprise r2 et r2 SP4 sur le site Web de la documentation SAP. |

Incluez les composants suivants dans vos plans de sauvegarde à l'aide d'un programme de sauvegarde de système de fichiers :

| Composant | Description |
|---|---|
| Composants de serveur Web | Configuration des composants de serveur Web déployés, tels que les modules d'extension de serveur d'applications et les agents Web SiteMinder.<br>Un serveur Web frontal est requis si vous utilisez l'équilibrage de la charge ou si vous utilisez CA SiteMinder pour protéger l'accès à la console d'utilisateur. |
| Fichiers de données XML | Tous les fichiers d'annuaire et d'environnement CA Identity Manager utilisés pour créer, gérer et archiver des objets de référentiel d'objets CA Identity Manager. |
| Composants de personnalisation CA Identity Manager | Fichiers qui se trouvent sous les dossiers iam_im.ear déployés suivants :<br>■ Config<br>■ User_console.war<br>WEB-INF\web.xml |
| Scripts et programmes | Scripts, programmes et sorties de programme du service Web d'exécution des tâches |
| Composants Connector Xpress | Connecteurs personnalisés<br>Fichiers de projet Connector Xpress |
| Documentation de récupération après sinistre | Une fois que vous avez créé la documentation pour la récupération après sinistre, sauvegardez-la régulièrement afin qu'elle soit toujours à jour. |

# Développement de procédures de restauration

Les procédures de restauration dépendent de la méthode de sauvegarde et la récupération d'un échec du système dépend des circonstances de celui-ci. Toutefois, dans la plupart des cas, la méthode de restauration consiste à réinstaller le logiciel. Pour plus d'informations, consultez le chapitre traitant du provisionnement de haute disponibilité du *Manuel d'installation*.

## Restauration du référentiel d'utilisateurs CA Identity Manager

Pour restaurer le référentiel d'utilisateurs CA Identity Manager, consultez la documentation fournie avec la base de données ou le logiciel LDAP que vous utilisez. Vérifiez que le référentiel de données de sauvegarde est intact et comprend l'accès à tous les référentiels d'utilisateurs.

## Restauration des bases de données CA Identity Manager

Pour restaurer les bases de données CA Identity Manager, consultez la documentation fournie avec la base de données que vous utilisez. Vérifiez que le référentiel de données de sauvegarde est intact et comprend l'accès à toutes les bases de données.

## Restauration du référentiel de stratégies SiteMinder

Pour restaurer le référentiel de stratégies SiteMinder, consultez la documentation fournie avec la base de données ou le logiciel LDAP que vous utilisez. Vérifiez que le référentiel de données de sauvegarde est intact et comprend l'accès à tous les référentiels d'utilisateurs.

## Restauration du serveur CA Identity Manager

Si vous perdez un noeud de cluster pour un serveur CA Identity Manager, effectuez la procédure suivante :

1. Utilisez la procédure documentée standard pour ajouter un noeud.

   Consultez le chapitre du *Manuel d'installation* traitant de l'installation de cluster.

2. Mettez à jour la connexion au serveur de provisionnement.

   Pour plus d'informations, reportez-vous à la section sur le basculement de provisionnement dans le chapitre traitant de la haute disponibilité du *Manuel d'installation*.

## Restauration d'un annuaire et d'un serveur de provisionnement

Vous pouvez restaurer un serveur de provisionnement perdu en installant un serveur auxiliaire. Si un échec de tous les systèmes s'est produit, restaurez les données perdues pendant le sinistre.

Utilisez la procédure suivante :

1. Copiez tous les fichiers de schéma personnalisé dans l'annuaire config\schema de CA Directory.
2. Installez le nouvel annuaire de provisionnement.

   Les référentiels de données seront vides.
3. Restaurez les données à partir de l'emplacement de sauvegarde.
4. Utilisez le programme d'installation de serveur de provisionnement et spécifiez les informations de l'annuaire de provisionnement nouvellement restauré.

   Les informations de domaine sont préremplies.
5. Restaurez tous les connecteurs personnalisés et les fichiers de configuration à partir de la sauvegarde.

**Remarque :** Pour plus d'informations, reportez-vous à la documentation CA Directory.

## Restauration des serveurs de connecteurs

Si un serveur de connecteurs est perdu, effectuez les opérations suivantes :

1. Utilisez le programme d'installation de serveur de connecteurs pour installer un nouveau serveur de connecteurs.

   Enregistrez-le auprès du serveur de provisionnement pendant l'installation.
2. Annulez l'enregistrement du serveur de connecteurs perdu à l'aide de csfconfig ou de Connector Xpress.

## Restauration d'un serveur de rapports

Si le serveur de rapports est perdu, consultez la documentation BusinessObjects pour déterminer les procédures à suivre. Sur le site Web de la documentation SAP, recherchez la documentation BusinessObjects Enterprise r2 et r2 SP4.

## Restauration des tâches d'administration

Si une tâche d'administration était en cours de traitement au moment du sinistre, vous pouvez la récupérer sous les conditions suivantes.

- Une tâche d'administration en attente d'approbations est toujours disponible si les référentiels utilisés pour conserver ces informations d'état sont intacts. Les référentiels incluent la base de données de persistance des tâches, le référentiel JMS qui contient la tâche et les messages JMS d'événement, et la base de données de flux de travaux.
- Les tâches dont l'état est En cours ou dans un état autre que En attente font l'objet de conditions supplémentaires.

  Une tâche dans cet état requiert l'envoi d'un nouveau message JMS dans la file d'attente de message d'événement CA Identity Manager pour que son traitement se poursuive. Les interruptions qui se produisent avant l'envoi de cet événement dans la file d'attente empêchent la poursuite de la tâche après la récupération.

  Dans ce cas, deux options existent pour récupérer la tâche :

  - Si la tâche est présente dans la tâche Afficher les tâches soumises avec un état Echec, accédez à sa page de détails et utilisez l'option Resoumettre cette tâche pour la resoumettre.
  - Soumettez une nouvelle tâche avec les mêmes modifications.

# Documentation du plan de récupération

Les directives contenues dans ce chapitre vous permettent de développer une documentation de récupération après sinistre spécifique à votre organisation.

Considérez l'approche suivante :

1. Identifiez les noms et les emplacements systèmes dans votre architecture et les composants secondaires pour chaque système.

   Pour chaque système, répertoriez les logiciels installés, tels que le kit de développement Java, la version de correctif d'un serveur d'applications et la quantité de mémoire installée. Ces informations sont nécessaires pour un système que vous décidez de reconstruire entièrement.
2. Ecrivez des procédures pour récupérer chaque composant ou pour reconstruire un système complet, si nécessaire.
3. Identifiez une méthode pour rechercher ou réinitialiser les noms d'utilisateur et les mots de passe des systèmes et des interfaces utilisateur CA Identity Manager s'ils ne sont connus que d'une ou deux personnes.
4. Pour protéger la documentation de récupération après sinistre contre les pertes, créez une copie de sauvegarde que vous stockez à un emplacement hors site connu.

# Test du plan de récupération

Pour vous assurer que la procédure de récupération après sinistre fonctionne, vous pouvez planifier une simulation de sinistre qui rend certains systèmes indisponibles. Considérez les tests suivants, qui sont décrits dans les sections ci-après.

1. Test du processus de basculement
2. Test de la restauration des systèmes

## Test du processus de basculement

Tous les serveurs ou les annuaires doivent avoir un serveur auxiliaire ou un annuaire secondaire sur un site distant, y compris les composants :

- Serveur CA Identity Manager
- Serveur de provisionnement
- Annuaires de provisionnement
- Serveurs de connecteurs Java et C++
- Serveur de rapports
- Serveur de stratégie

Arrêtez manuellement chaque composant et vérifiez que toutes les opérations continuent à l'aide du composant secondaire. Par exemple, vous pouvez effectuer le test suivant sur le serveur de provisionnement :

1. Sur le système sur lequel est installé le serveur de provisionnement principal, arrêtez les services de provisionnement à partir de la boîte de dialogue Services de Windows.

   Le serveur de provisionnement principal est arrêté.

2. Dans la console d'utilisateur, procédez comme suit :

   a. Affectez un rôle de provisionnement à un utilisateur.

   b. Vérifiez que les comptes de terminal sont créés pour cet utilisateur.

      Ces comptes dépendent du serveur de provisionnement auxiliaire gérant les communications avec le serveur CA Identity Manager.

Cette procédure est un exemple de test. Pour chaque composant que vous arrêtez, développez des tests similaires pour vérifier que le composant secondaire est utilisé.

## Test des procédures de restauration

Selon votre documentation de récupération après sinistre, effectuez un test de chaque composant critique pour confirmer que vous pouvez restaurer le système perdu.

# Formation à la récupération après sinistre

Une fois que avez conclu que les procédures de récupération sont fiables, assurez-vous que les personnes qui doivent implémenter la récupération sont capables de le faire. Les directives suivantes sont assez générales pour être appliquées dans un grand nombre de situations, même si des étapes supplémentaires peuvent être nécessaires à votre organisation :

1. Informez de l'emplacement de la documentation de récupération.
2. Effectuez la formation une première fois.
3. Modifiez la formation de façon à inclure tous les commentaires reçus pour vous assurer que les procédures de récupération après sinistre finales sont suffisantes.

**Remarque :** Vous pouvez également saisir l'opportunité apportée par la formation pour affecter des coordinateurs de récupération, notamment un coordinateur de récupération et un coordinateur auxiliaire. Ces personnes doivent se rencontrer à l'emplacement stipulé par la documentation pour commencer le plan de récupération après sinistre.