Guide de l'administrateur d'entreprise de Sun Identity Manager 8.1

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Référence : 821–0063
Juillet 2009

090806@22749

Table des matières

Préface

Ce guide explique comment utiliser le logiciel Sun™Identity Manager (Identity Manager) pour fournir aux utilisateurs un accès sécurisé aux systèmes et applications informatiques de l'entreprise. Il illustre les procédures et scénarios qui vous aideront à effectuer des tâches administratives régulières et périodiques avec le système Identity Manager.

Public cible

Ce *Guide de l'administrateur d'entreprise de Sun Identity Manager 8.1* a été conçu pour les administrateurs, les développeurs de logiciels et les fournisseurs de services informatiques qui implémentent une plate-forme de gestion des identités et d'accès Web intégrée en utilisant les serveurs et le logiciel Identity Manager.

La maîtrise des technologies suivantes est utile pour mettre en œuvre les informations contenues dans cet ouvrage :

- LDAP (Lightweight Directory Access Protocol),
- la technologie Java,
- la technologie JavaServer Pages™ (JSP™),
- HTTP (Hypertext Transfer Protocol),
- HTML (Hypertext Markup Language),
- XML (Extensible Markup Language).

Avant de lire ce guide

Identity Manager est un composant de Sun Java Enterprise System, l'infrastructure logicielle qui supporte les applications d'entreprise distribuées sur un environnement réseau ou Internet. Vous devez être familiarisé avec la documentation fournie avec Sun Java Enterprise System, accessible en ligne à l'adresse `http://docs.sun.com/coll/entsys_04q4`.

Identity Manager Directory Server étant utilisé en tant que magasin de données dans un déploiement Identity Manager, vous devez être familiarisé avec la documentation qui accompagne ce produit. La documentation de Directory Server est accessible en ligne à l'adresse `http://docs.sun.com/coll/DirectoryServer_04q2`.

Organisation de ce guide

Ce guide se compose des chapitres et annexes suivants :

Le Chapitre 1, “Présentation d’Identity Manager” explique comment Identity Manager et les différents objets Identity Manager peuvent vous aider à gérer les enjeux administratifs dans un environnement de travail dynamique.

Le Chapitre 2, “Démarrage de l'interface utilisateur d'Identity Manager ” détaille l'utilisation de l'interface utilisateur graphique d'Identity Manager.

Le Chapitre 3, “Gestion des utilisateurs et des comptes” explique la création et la gestion des utilisateurs au moyen de l'interface administrateur.

Le Chapitre 5, “Rôles et ressources” contient des informations qui vous permettront de comprendre les rôles et les ressources d'Identity Manager.

Le Chapitre 4, “Configuration des objets d'administration d'entreprise” renferme les informations et les procédures à suivre pour configurer et mettre à jour les objets d'administration d'entreprise d'Identity Manager, tels que les stratégies, les modèles d'e-mails, les groupes et les événements d'audit, et bien d'autres encore.

Le Chapitre 6, “Administration” explique l'utilisation de l'interface administrateur pour effectuer différentes tâches de niveau administrateur. De plus, ce chapitre contient des informations sur l'utilisation des rôles, des rôles administratifs et des capacités.

Le Chapitre 7, “Chargement et synchronisation des données” explique l'utilisation des fonctionnalités de chargement et de synchronisation des données d'Identity Manager pour maintenir vos données à jour.

Le Chapitre 8, “Génération de rapports” présente les différents types de rapports d'Identity Manager et explique la création et la gestion des rapports.

Le Chapitre 9, “Modèles de tâches” présente les modèles de tâches d'Identity Manager et leur utilisation pour configurer le comportement des flux de travaux.

Le Chapitre 10, “Journalisation d'audit” explique le système d'audit d'Identity Manager.

Le Chapitre 11, “PasswordSync” explique comment installer, configurer et utiliser la fonctionnalité PasswordSync pour détecter et synchroniser les changements de mot de passe.

Le Chapitre 12, “Sécurité” explique comment utiliser Identity Manager pour gérer la sécurité du système.

Le Chapitre 13, “Audit des identités : principes de base” présente les principes de l'audit des identités et les contrôles d'audit.

Le Chapitre 14, “Audit : stratégies d'audit” explique la création et la gestion des stratégies d'audit en utilisant l'Assistant Stratégie d’audit.

Le Chapitre 15, “Audit : contrôler la conformité” explique comment réaliser des examens d'audit et gérer la conformité aux réglementations fédérales obligatoires.

Le Chapitre 16, “Exportateur de données” présente la fonctionnalité Exportateur de données et en explique l'utilisation pour consigner des informations sur les utilisateurs, les rôles et d'autres types d'objets dans un entrepôt de données externe.

Le Chapitre 17, “Administration de Service Provider” décrit la configuration et l'administration de la fonctionnalité Service Provider.

L'Annexe A, “Références `lh`” explique comment utiliser l'interface de ligne de commande d'Identity Manager.

L'Annexe B, “Schéma de la base de données du journal d'audit” contient des informations sur les valeurs du schéma des données d'audit pour les types de bases de données pris en charge ainsi que les mappages du journal d'audit.

L'Annexe C, “Guide de référence rapide de l'interface utilisateur” constitue un guide de référence rapide indiquant comment accomplir des tâches couramment effectuées dans Identity Manager.

L'Annexe D, “Définitions des capacités” constitue un guide de référence rapide expliquant les capacités basées sur des tâches et fonctionnelles que vous pouvez assigner aux utilisateurs.

Manuels connexes

Sun fournit de la documentation et des informations supplémentaires pour vous aider à installer, utiliser et configurer Identity Manager. La bibliothèque Sun Identity Manager 8.1 se compose des publications suivantes.

Public principal	Titre	Description
Tous publics	*Présentation de Sun Identity Manager*	Présente les caractéristiques et les fonctionnalités d’Identity Manager. Contient des informations sur l'architecture du produit et explique l'intégration d'Identity Manager avec d'autres produits tels que Sun Open SSO Enterprise et Sun Role Manager.
	Notes de version de Sun Identity Manager 8.1	Décrivent les problèmes connus et corrigés ainsi que les informations de dernière minute ne figurant pas encore dans l'ensemble de documentation d'Identity Manager.

Public principal	Titre	Description
Administrateurs système	*Sun Identity Manager 8.1 Installation*	Décrit l'installation d'Identity Manager et des composants optionnels tels que Sun Identity Manager Gateway et PasswordSync.
	Sun Identity Manager 8.1 Upgrade	Contient les instructions à suivre pour effectuer une mise à niveau d'une version plus ancienne d'Identity Manager vers une version plus récente.
	Sun Identity Manager 8.1 System Administrator's Guide	Contient des informations et des instructions qui aideront les administrateurs à gérer, régler et dépanner leur installation d'Identity Manager.
Administrateurs d'entreprise	*Guide de l'administrateur d'entreprise de Sun Identity Manager 8.1*	Explique l'utilisation des fonctionnalités de provisioning et d'audit d'Identity Manager. Contient des informations sur les interfaces utilisateur, la gestion des utilisateurs et des comptes, la génération des rapports et bien plus encore.
Intégrateurs de systèmes	*Sun Identity Manager Deployment Guide*	Explique le déploiement d'Identity Manager dans les environnements informatiques complexes. Les sujets traités incluent le travail avec les attributs d'identité, le chargement et la synchronisation des données, la configuration des actions utilisateur, l'application de stratégies de marques personnalisées, etc.
	Sun Identity Manager Deployment Reference	Contient des informations sur les flux de travaux, les formulaires, les affichages et les règles ainsi que sur le langage XPRESS.
	Sun Identity Manager 8.1 Resources Reference	Fournit des informations sur l'installation, la configuration et l'utilisation des adaptateurs de ressources.
	Sun Identity Manager Service Provider 8.1 Deployment	Explique le déploiement de Sun Identity Manager Service Provider et en quoi les vues, formulaires et ressources diffèrent de ceux du produit Identity Manager standard.
	Sun Identity Manager 8.1 Web Services	Explique la configuration de la prise en charge de SPML, les fonctionnalités SPML prises en charge (et la raison de cette prise en charge) et comment étendre la prise en charge sur le terrain.

De plus, le site Web `http://docs.sun.com` permet d'accéder à la documentation technique en ligne de Sun. Vous pouvez explorer les archives ou rechercher un titre d'ouvrage ou un sujet spécifique.

Mises à jour de la documentation

Les corrections et mises à jour de cette et d'autres publications relatives à Identity Manager sont postées sur le site Web des mises à jour de documentation d'Identity Manager :

`http://blogs.sun.com/idmdocupdates/`

Un lecteur de flux RSS peut être utilisé pour contrôler périodiquement le site Web et vous avertir lorsque de nouvelles mises à jour sont disponibles. Pour vous abonner, téléchargez un lecteur de flux et cliquez sur un des liens sous Feeds (Flux) sur la droite de la page. Depuis la version 8.0, des flux séparés sont disponibles pour chacune des versions majeures.

Références à des sites Web tiers

Des URL tiers pointant vers des informations complémentaires sont cités dans ce document.

Remarque – Sun ne saurait être tenu responsable de la disponibilité des sites Web tiers mentionnés dans ce manuel. Sun décline toute responsabilité en ce qui concerne le contenu, la publicité, les produits ou tout autre matériel disponibles dans ou par l'intermédiaire de ces sites ou ressources. Sun ne pourra en aucun cas être tenu pour responsable, directement ou indirectement, de tous dommages ou pertes, réels ou invoqués, causés par ou liés à l'utilisation des contenus, biens ou services disponibles dans ou par l'intermédiaire de ces sites ou ressources.

Documentation, support et formation

Le site Web de Sun fournit des informations sur les ressources additionnelles suivantes :

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Formation (`http://www.sun.com/training/`)

Vos commentaires sont les bienvenus

Dans le souci d'améliorer notre documentation, nous vous invitons à nous faire parvenir vos commentaires et suggestions. Pour nous faire part de vos commentaires, accédez à l'adresse `http://docs.sun.com` et cliquez sur Envoyer des commentaires.

Conventions typographiques

Le tableau suivant indique les conventions typographiques utilisées dans cet ouvrage.

TABLEAU P–1 Conventions typographiques

Caractère ou symbole	Signification	Exemple
`AaBbCc123`	Noms de commandes, fichiers et répertoires ; messages système.	Modifiez le fichier `.login`. Utilisez `ls -a` pour dresser la liste des fichiers. `nom_machine% Vous avez du courrier.`
`AaBbCc123`	Caractères saisis par l'utilisateur, par opposition aux messages système.	`nom_machine%` **`su`** `Password:`
aabbcc123	Remplacez les variables de ligne de commande par des noms ou des valeurs réels.	Pour supprimer un fichier, tapez `rm` *nomfichier*.
AaBbCc123	Titres d'ouvrages, nouveaux mots ou termes, mots importants.	Lisez le chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie qui est stockée localement. N'enregistrez *pas* le fichier. **Remarque :** certains éléments mis en évidence apparaissent en caractères gras.

Invites de shell dans les exemples de commande

Le tableau suivant indique l'invite système UNIX® et les invites de superutilisateur par défaut pour le C shell, le Bourne shell et le Korn shell.

TABLEAU P–2 Invites de shell

Shell	Invite
C shell	`nom_machine%`
C shell pour superutilisateur	`nom_machine#`
Bourne shell et Korn shell	`$`
Bourne shell et Korn shell pour superutilisateur	`#`

◆ ◆ ◆ CHAPITRE 1

1 Présentation d'Identity Manager

Le système Sun Identity Manager permet de gérer et de contrôler l'accès aux comptes et aux ressources. En vous apportant les capacités et les outils nécessaires pour gérer rapidement les tâches de provisioning utilisateur et les tâches d'audit périodiques et quotidiennes, Identity Manager facilite la fourniture de services exceptionnels aux clients internes et externes.

Ce chapitre se compose des rubriques suivantes :

Vue d'ensemble

Les entreprises d'aujourd'hui ont besoin de services TI toujours plus souples et riches sur le plan fonctionnel. Historiquement, la gestion de l'accès aux informations de l'entreprise et aux systèmes nécessitait une interaction directe avec un nombre limité de comptes. Aujourd'hui, gérer l'accès signifie gérer des nombres grandissants de clients internes mais aussi de partenaires et de clients externes à l'entreprise.

La surcharge créée par ce besoin d'accès accru peut être considérable. En tant qu'administrateur, vous devez permettre efficacement et de manière sécurisée aux personnes, que celles-ci soient internes ou externes à l'entreprise, de faire leur travail. Après avoir fourni l'accès initial, vous devez faire face à des défis précis et continus tels que les mots de passe oubliés, les changements de rôle et l'évolution des relations interentreprises.

De plus, les entreprises doivent aujourd'hui satisfaire des exigences très strictes concernant la gestion de la sécurité et de l'intégrité des informations commerciales critiques. Dans un environnement régi par la législation sur la conformité (la Loi Sarbanes-Oxley (SOX), l'Health Insurance Portability and Accountability Act (HIPAA) et la Loi Gramm-Leach-Bliley (GLB) pour ne citer que quelques exemples), la surcharge associée aux activités de contrôle et de génération de rapports est conséquente et coûteuse. Vous devez être en mesure de répondre

rapidement aux changements en matière de contrôle d'accès tout en satisfaisant les exigences de collecte de données et de génération de rapports qui contribuent à assurer la sécurité de l'entreprise.

Identity Manager a été spécifiquement développé pour vous aider à gérer ces enjeux administratifs dans un environnement dynamique. En utilisant Identity Manager pour distribuer la surcharge de travail due à la gestion des accès et alléger le fardeau que constitue la conformité, vous disposez d'une solution permettant de répondre aux principaux problèmes auxquels vous serez confronté : Comment définir l'accès ? et L'accès défini, comment maintenir la souplesse et le contrôle ?

Sa conception à la fois souple et sécurisée permet de configurer Identity Manager en l'adaptant à la structure de votre entreprise et de répondre à ces problèmes. Mapper les objets Identity Manager aux entités que vous gérez (les utilisateurs et les ressources) permet d'accroître considérablement l'efficacité de votre travail.

Dans un environnement de fournisseur de services, Identity Manager étend ces capacités à la gestion des utilisateurs de l'extranet.

Objectifs du système Identity Manager

La solution Identity Manager permet d'atteindre les objectifs suivants :

- Gérer l'accès des comptes à toute une variété de systèmes et ressources.
- Gérer de manière sécurisée des informations de compte dynamiques pour toute la gamme des comptes de chaque utilisateur.
- Configurer des droits délégués pour créer et gérer les données des comptes utilisateur.
- Manipuler de grands nombres de ressources d'entreprise, ainsi qu'un nombre croissant de clients de l'extranet et de partenaires.
- Autoriser de manière sécurisée l'accès des utilisateurs aux systèmes d'information de l'entreprise. Avec Identity Manager, vous disposez de fonctionnalités entièrement intégrées permettant d'accorder, gérer et révoquer les privilèges d'accès pour les organisations internes et externes.
- Conserver les données synchronisées, en ne conservant *pas* les données. La solution Identity Manager prend en charge les deux principes-clés suivants que tout outil de gestion de système supérieur se doit de respecter :
  - Un produit doit avoir un impact minimal sur le système qu'il gère.
  - Un produit ne doit pas augmenter la complexité dans l'entreprise en ajoutant une ressource à gérer.

  Définir des stratégies d'audit pour gérer la conformité avec les privilèges d'accès des utilisateurs et gérer les violations au travers d'actions de résolution et d'alertes par e-mail automatisées.

- Effectuer des examens d'accès et définir des procédures d'examen d'attestation et d'approbation qui automatisent le processus de certification des privilèges des utilisateurs.
- Contrôler les informations-clés ainsi que les statistiques d'audit et d'examen par le biais du tableau de bord.

Définition de l'accès des utilisateurs aux ressources

Dans votre entreprise étendue, les *utilisateurs* peuvent être toute personne en relation avec votre entreprise, notamment ses employés, clients, partenaires, fournisseurs ou acquisitions. Dans le système Identity Manager, les utilisateurs sont représentés par des *comptes utilisateur*.

Selon leur relation avec l'entreprise et avec d'autres entités, les utilisateurs doivent pouvoir avoir accès à différents éléments qui peuvent être des systèmes informatiques, des données stockées dans des bases de données ou des applications informatiques spécifiques. Dans Identity Manager, ces éléments s'appellent des *ressources*.

Étant donné que les utilisateurs ont souvent une ou plusieurs identités sur chacune des ressources auxquelles ils accèdent, Identity Manager crée une unique *identité virtuelle* qui mappe vers des ressources variées. Ceci vous permet de gérer les utilisateurs comme une unique entité. Voir Figure 1–1.

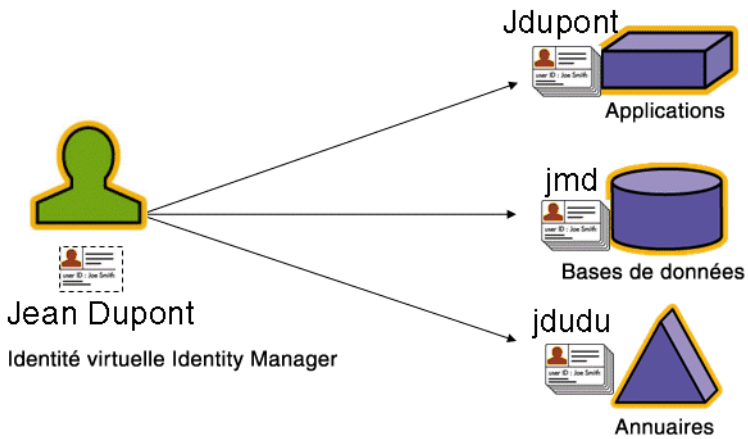


FIGURE 1–1 Relation entre un compte utilisateur Identity Manager et les ressources

Pour gérer efficacement de grands nombres d'utilisateurs, vous devez pouvoir les regrouper de maintes manières logiques. Dans la plupart des sociétés, les utilisateurs sont regroupés par services fonctionnels ou divisions géographiques. Chacun de ces services a en général besoin de pouvoir accéder à différentes ressources. Dans la terminologie d'Identity Manager, ce type de groupe s'appelle une *organisation*.

Un autre mode de regroupement consiste à regrouper les utilisateurs présentant des caractéristiques similaires, par exemple des relations avec l'entreprise ou des fonctions identiques. Dans Identity Manager, les regroupements de ce type s'appellent des *rôles*.

Au sein du système Identity Manager, vous assignez des rôles aux comptes utilisateur pour faciliter l'activation et la désactivation de l'accès aux ressources. L'assignation de comptes aux organisations permet une délégation efficace des responsabilités administratives.

Les utilisateurs d'Identity Manager sont également gérés directement ou indirectement par le biais de l'application de *stratégies* définissant des règles et les options d'authentification des utilisateurs et de mot de passe.

Comprendre les types d'utilisateurs

Identity Manager propose deux types d'utilisateurs : les *utilisateurs Identity Manager* et les *utilisateurs Service Provider*, si vous configurez le système Identity Manager pour une implémentation de type fournisseur de services. Ces types permettent de distinguer les utilisateurs susceptibles d'avoir des exigences de provisioning différentes en fonction de leurs relations avec l'entreprise, par exemple de distinguer les utilisateurs de l'extranet de ceux de l'intranet.

Un exemple typique d'implémentation fournisseur de services est celui d'un fournisseur de services ayant des utilisateurs internes et externes (ses clients) qu'il veut gérer avec Identity Manager. Pour toute information sur la configuration d'une implémentation fournisseur de services, consultez le document *Sun Identity Manager Service Provider 8.1 Deployment* (Déploiement de Sun Identity Manager Service Provider 8.1).

Vous spécifiez le type d'utilisateurs Identity Manager lorsque vous configurez un compte utilisateur. Pour toute information sur les utilisateurs de fournisseur de services, voir le Chapitre 17, "Administration de Service Provider"

Délégation de l'administration

Pour réussir la distribution de la responsabilité concernant la gestion des identités des utilisateurs, vous avez besoin d'un juste dosage de flexibilité et de contrôle. En accordant à des utilisateurs Identity Manager sélectionnés des privilèges d'administrateur et en déléguant des tâches administratives, vous réduisez votre charge de travail et augmentez l'efficacité en conférant la responsabilité de la gestion des identités à ceux qui connaissent le mieux les besoins des utilisateurs, par exemple le responsable du recrutement. Les utilisateurs qui ont de tels privilèges étendus sont les *administrateurs* Identity Manager.

La délégation ne fonctionne toutefois que dans le cadre d'un modèle sécurisé. Pour maintenir un niveau de contrôle approprié, Identity Manager permet d'assigner différent niveaux de *capacités* aux administrateurs. Les capacités autorisent des niveaux d'accès et d'action variés au sein du système.

Le modèle de flux de travaux d'Identity Manager inclut également une méthode permettant d'assurer que certaines actions nécessitent une approbation. En utilisant le flux de travaux, les administrateurs Identity Manager gardent le contrôle des tâches et peuvent en suivre la progression. Pour des informations détaillées sur le flux de travaux, voir le Chapitre 1, "Workflow" du *Sun Identity Manager Deployment Reference*.

Objets Identity Manager

Avoir une idée claire des objets Identity Manager et de la façon dont ils interagissent est capital pour une gestion et un déploiement réussis du système. Ces objets sont les suivants :

- "Comptes utilisateur Identity Manager" à la page 27 ;
- "Rôles Identity Manager" à la page 28 ;
- "Ressources et groupes de ressources" à la page 29 ;
- "Organisations et organisations virtuelles" à la page 30 ;
- "Jonctions d'annuaires" à la page 31 ;
- "Capacités Identity Manager" à la page 31 ;
- "Rôles admin" à la page 32 ;
- "Stratégies Identity Manager" à la page 32 ;
- "Stratégies d'audit" à la page 32 ;
- "Relations entre les objets" à la page 33.

Remarque – Lorsque vous nommez des objets Identity Manager, n'utilisez pas les caractères suivants :

' (apostrophe), . . (point), | (barre verticale), [(crochet gauche),] (crochet droit), , (virgule), : (deux points), $ (signe du dollar), " (guillemets doubles), \ (barre oblique inverse) ou = (signe égal).

Vous devez également éviter les caractères suivants : _ (trait de soulignement), % (signe du pourcentage), ^ (accent circonflexe) et * (astérisque).

Comptes utilisateur Identity Manager

On appelle utilisateur toute personne ayant un compte sur le système Identity Manager. Identity Manager stocke un éventail de données pour chaque utilisateur. Collectivement, ces informations forment l'identité Identity Manager d'un utilisateur.

Les comptes utilisateur Identity Manager :

- permettent aux utilisateurs d'accéder à une ou plusieurs ressources et de gérer les données de compte utilisateur sur ces ressources ;
- se voient assigner des rôles définissant l'accès des utilisateurs aux différentes ressources ;

- font partie d'une organisation, qui détermine comment et par qui ils sont administrés.

La configuration des comptes utilisateur est un processus dynamique. Selon le rôle sélectionné lors de la configuration des comptes, vous devrez fournir des informations plus ou moins spécifiques de la ressource pour créer le compte. Le nombre et le type des ressources associées au rôle assigné déterminent la quantité des informations requises à la création d'un compte.

Les administrateurs sont des utilisateurs jouissant de privilèges supplémentaires leur permettant de gérer les comptes utilisateur, les ressources et d'autres objets et tâches du système Identity Manager. Les administrateurs Identity Manager gèrent les organisations et se voient assigner toute une gamme de capacités à appliquer aux objets de chacune des organisations gérées.

Pour plus d'informations sur les comptes utilisateur, voir le Chapitre 3, "Gestion des utilisateurs et des comptes". Pour plus d'informations sur les comptes administrateur, voir le Chapitre 6, "Administration".

Rôles Identity Manager

Un rôle est un objet Identity Manager permettant de regrouper des droits d'accès aux ressources en vue de les assigner efficacement à des utilisateurs. Les rôles sont organisés en quatre types :

- les rôles professionnels,
- les rôles informatiques,
- les applications,
- le matériel.

Les *rôles professionnels* permettent d'organiser en groupes les droits d'accès dont les personnes effectuant des tâches semblables au sein d'une organisation ont besoin dans l'exercice de leur fonction. En général, les rôles professionnels correspondent aux fonctions professionnelles des utilisateurs.

Les *rôles informatiques, les applications* et le *matériel* permettent d'organiser les habilitations de ressources (ou *droits d'accès*) en groupes. Pour fournir aux utilisateurs l'accès aux ressources, les rôles informatiques, les applications et le matériel sont assignés à des rôles professionnels, ce qui permet aux utilisateurs d'accéder aux ressources dont ils ont besoin dans l'exercice de leur fonction.

Les rôles informatiques, les applications et le matériel peuvent être *obligatoires, conditionnels* ou *optionnels*.

- Les **rôles obligatoires** sont toujours assignés à l'utilisateur.
- Les **rôles conditionnels** sont associés à des conditions qui doivent être remplies pour pouvoir assigner le rôle en question.
- Les **rôles optionnels** peuvent être demandés séparément et, sous réserve d'approbation, assignés à l'utilisateur.

Les rôles pouvant être conditionnels ou optionnels, des utilisateurs ayant la même description de fonction générale pourront avoir le même rôle professionnel mais des droits d'accès différents. Cette approche permet au concepteur d'un rôle professionnel de définir des droits d'accès génériques aux rôles afin d'assurer la conformité aux réglementations, tout en laissant au responsable de l'utilisateur la liberté d'adapter de manière plus précise les droits d'accès de l'utilisateur. Avec une telle approche, il devient inutile de définir un nouveau rôle professionnel à chaque permutation des besoins d'accès dans l'entreprise, problème connu sous le nom d'*explosion des rôles*.

Un utilisateur peut se voir attribuer un, plusieurs ou aucun rôles.

Remarque – Pour plus d'informations sur les rôles, voir la section "Comprendre et gérer les rôles" à la page 121.

Ressources et groupes de ressources

Identity Manager stocke des informations sur la procédure de connexion à un système ou ressource. Identity Manager permet d'accéder aux ressources suivantes :

- Des ressources numériques telles que les suivantes :
  - gestionnaires de sécurité de mainframe,
  - bases de données,
  - services d'annuaires (par ex. LDAP),
  - applications,
  - systèmes d'exploitation,
  - systèmes ERP (par ex. SAP™).
- Des ressources non numériques ou `externes` qui sont externes à Identity Manager, telles que les suivantes :
  - téléphones portables,
  - ordinateurs de bureau,
  - ordinateurs portables,
  - badges de sécurité.

Chaque ressource Identity Manager stocke des les types d'informations suivants :

- paramètres des ressources,
- paramètres d'Identity Manager,
- informations des comptes (attributs de compte et modèle d'identité compris).

Il existe deux manières d'assigner des ressources aux utilisateurs. Une ressource peut être assignée directement à un utilisateur (on parle alors d'assignation individuelle ou directe) ou être assignée à un rôle qui sera à son tour assigné à un utilisateur (on parle alors d'assignation basée sur le rôle ou indirecte).

- **Assignation individuelle**. Des ressources individuelles sont assignées directement aux comptes utilisateur.
- **Assignation basée sur le rôle**. Une ou plusieurs ressources sont assignées à un rôle (une application, du matériel ou un rôle informatique). Les rôles (application, matériel ou rôle informatique) sont ensuite assignés à un rôle professionnel. Enfin, un ou plusieurs rôles professionnels sont assignés à un compte utilisateur.

Un objet Identity Manager connexe, un *groupe de ressources*, peut être assigné aux comptes utilisateur de la même façon que les ressources. Les groupes de ressources corrèlent les ressources vous permettant de créer des comptes sur des ressources dans un ordre spécifique. Ils simplifient aussi le processus d'assignation de ressources multiples aux comptes utilisateur.

Pour plus d'informations sur les groupes de ressources, voir la section "Groupes de ressources" à la page 171.

Organisations et organisations virtuelles

Les organisations sont les conteneurs Identity Manager utilisés pour activer la délégation administrative. Elles définissent l'étendue des entités gérées ou contrôlées par un administrateur Identity Manager.

Les organisations peuvent aussi représenter des liens directs vers des ressources basées dans un annuaire. Elles sont alors qualifiées d'*organisations virtuelles*. Les organisations virtuelles permettent de gérer directement les données des ressources sans charger les informations dans le référentiel d'Identity Manager. En reflétant les membres et la structure d'un annuaire existant par le biais d'une organisation virtuelle, Identity Manager élimine les tâches de configuration doubles et laborieuses.

Les organisations qui contiennent d'autres organisations sont des *organisations parentes*. Vous pouvez créer des organisations au sein d'une structure plate ou les organiser dans une hiérarchie. La hiérarchie peut représenter des services, des zones géographiques ou d'autres divisions logiques au moyen desquelles vous gérez les comptes utilisateur.

Pour plus d'informations sur les organisations, voir la section "Comprendre les organisations d'Identity Manager" à la page 209.

Jonctions d'annuaires

Une *jonction d'annuaires* est un ensemble d'organisations reliées hiérarchiquement qui reflète le jeu courant de conteneurs hiérarchiques d'une ressource d'annuaire. Une *ressource d'annuaire* est une ressource qui emploie un espace de noms hiérarchique à travers l'utilisation de conteneurs hiérarchiques. Les serveurs LDAP et les ressources de Windows Active Directory sont des exemples de ressources d'annuaire.

Toute organisation contenue dans une jonction d'annuaires est une *organisation virtuelle*. L'organisation virtuelle supérieure d'une jonction d'annuaires est un miroir du conteneur représentant le contexte de base défini dans la ressource. Les organisations virtuelles restantes d'une jonction d'annuaires sont les enfants *directs* ou *indirects* de l'organisation virtuelle supérieure et reflètent également l'un des conteneurs de ressources d'annuaire enfants du conteneur de contexte de base de la ressource définie.

Vous pouvez rendre les utilisateurs Identity Manager membres d'une organisation virtuelle ou les mettre à disposition de celle-ci de la même façon qu'une organisation.

Pour plus d'informations sur les jonctions d'annuaires, voir la section "Comprendre les jonctions d'annuaires et les organisations virtuelles" à la page 213.

Capacités Identity Manager

Tout utilisateur peut se voir assigner des capacités, ou groupes de droits, lui permettant d'effectuer des actions administratives par le biais d'Identity Manager. Les capacités permettent à l'utilisateur administratif d'effectuer certaines tâches dans le système et d'agir sur les objets Identity Manager.

En règle générale, vous assignez les capacités en fonction de responsabilités professionnelles spécifiques telles que les réinitialisations de mot de passe ou les approbations de compte. En assignant des capacités et des droits aux utilisateurs individuels, vous créez une structure administrative hiérarchique qui fournit un accès et des privilèges ciblés sans compromettre la protection des données.

Identity Manager fournit un ensemble de capacités par défaut pour les fonctions administratives courantes. Vous pouvez également créer et assigner des capacités satisfaisant vos besoins spécifiques.

Pour plus d'informations sur les capacités, voir la section "Comprendre et gérer les capacités" à la page 216.

Rôles admin

Les rôles admin d'Identity Manager permettent de définir un ensemble unique de capacités pour chacun des ensembles d'organisations gérés par un utilisateur administratif. Un rôle admin se voit assigner des capacités et des organisations contrôlées, qui peuvent ensuite être assignées à un utilisateur administratif.

Les capacités et les organisations contrôlées peuvent être assignées directement à un rôle admin mais peuvent aussi l'être indirectement (dynamiquement) à chaque fois que l'utilisateur administratif se connecte à Identity Manager. Les règles d'Identity Manager contrôlent l'assignation dynamique.

Pour plus d'informations sur les rôles admin, voir la section "Comprendre et gérer les rôles admin" à la page 220.

Stratégies Identity Manager

Les *stratégies* définissent des limites pour les utilisateurs d'Identity Manager en établissant des contraintes s'appliquant aux caractéristiques des ID de compte, connexions et mots de passe. Les *stratégies de compte du système d'identité* fixent les options et contraintes s'appliquant aux utilisateurs, mots de passe et stratégies d'authentification. Les *stratégies de mot de passe et d'ID de compte de ressources* définissent les règles de longueur et de type de caractères, les mots et les valeurs d'attributs autorisés. Une *stratégie·de dictionnaire* permet à Identity Auditor de vérifier en confrontant les mots de passe à une base de données de mots, s'ils sont protégés contre les attaques de dictionnaire simples.

Pour plus d'informations sur les stratégies, voir la section "Définition des stratégies" à la page 102.

Stratégies d'audit

Se distinguant des autres stratégies système, une *stratégie d'audit* définit une violation de stratégie pour un groupe d'utilisateurs d'une ressource spécifique. Les stratégies d'audit permettent d'établir une ou plusieurs règles à travers lesquelles les utilisateurs sont évaluées afin de détecter d'éventuelles violations de conformité. Ces règles dépendent de conditions reposant sur un ou plusieurs attributs définis par une ressource. Lorsque le système scanne un utilisateur, il utilise les critères définis dans les stratégies d'audit assignées à ce dernier pour déterminer si des violations de compatibilité se sont produites.

Pour plus d'informations sur les stratégies d'audit, voir la section "À propos des stratégies d'audit" à la page 444.

Relations entre les objets

Le tableau ci-dessous donne un aperçu rapide des objets Identity Manager et de leurs relations.

TABLEAU 1–1 Relations des objets Identity Manager

Objet Identity Manager	Définition	Cas d'emploi
Compte utilisateur	Compte sur Identity Manager et sur une ou plusieurs ressources. Les données de l'utilisateur peuvent être chargées dans Identity Manager à partir des ressources. Une classe spéciale d'utilisateurs, les administrateurs Identity Manager, ont des privilèges étendus.	**Rôle**. En règle générale, tout compte utilisateur se voit assigner un ou plusieurs rôles. **Organisation**. Les comptes utilisateur sont classés de manière hiérarchique comme faisant partie d'une organisation. Les administrateurs Identity Manager gèrent en outre les organisations. **Ressource**. Des ressources individuelles peuvent être assignées aux comptes utilisateur. **Capacité**. Les administrateurs se voient assigner des capacités pour les organisations qu'ils gèrent.
Rôle	Les rôles professionnels organisent en groupes les droits d'accès dont les personnes effectuant des tâches semblables au sein d'une organisation ont besoin dans l'exercice de leurs fonctions. Les rôles informatiques et Application regroupent des ressources, ce qui permet d'assigner ces dernières aux utilisateurs par le biais de rôles professionnels. L'assignation de ressources basée sur le rôle simplifie la gestion des ressources dans les organisations de grande taille.	**Ressources et groupes de ressources**. Les ressources et les groupes de ressources sont assignés au rôles informatique, Application et Matériel. **Compte utilisateur** Les comptes utilisateur présentant des caractéristiques similaires sont assignés à des rôles professionnels. Les **rôles informatique, Application et Matériel** sont assignés aux rôles professionnels.

TABLEAU 1–1 Relations des objets Identity Manager *(Suite)*

Objet Identity Manager	Définition	Cas d'emploi
Ressource	Stocke les informations relatives à un système, une application ou une autre ressource sur laquelle les comptes sont gérés.	**Rôle**. Les ressources sont assignées aux rôles informatiques et Application, qui à leur tour sont assignés aux rôles professionnels. Un compte utilisateur « hérite » librement de l'accès aux ressources des assignations de son rôle professionnel. **Compte utilisateur**. Les ressources peuvent être assignées individuellement aux comptes utilisateur.
Groupe de ressources	Groupe ordonné de ressources.	**Rôle**. Les groupes de ressources sont assignés à des rôles ; un compte utilisateur « hérite » de l'accès aux ressources des assignations de son rôle professionnel. **Compte utilisateur** Les groupes de ressources peuvent être assignés directement aux comptes utilisateur.
Organisation	Définit l'étendue des entités gérées par un administrateur ; hiérarchique.	**Ressource**. Les administrateurs d'une organisation donnée peuvent accéder à tout ou partie des ressources. **Administrateur**. Les organisations sont gérées (contrôlées) par les utilisateurs jouissant de privilèges administratifs. Les administrateurs peuvent gérer une ou plusieurs organisations. Les privilèges administratifs dans une organisation donnée sont transmis aux organisations enfants de cette dernière. **Compte utilisateur**. Chaque compte utilisateur peut être assigné à une organisation Identity Manager et une ou plusieurs organisations d'annuaire.
Jonction d'annuaires	Ensemble d'organisations reliées hiérarchiquement qui reflète l'ensemble de conteneurs hiérarchiques effectif d'une ressource d'annuaire.	**Organisation**. Toute organisation contenue dans une jonction d'annuaires est une organisation virtuelle.

TABLEAU 1–1 Relations des objets Identity Manager *(Suite)*

Objet Identity Manager	Définition	Cas d'emploi
Rôle admin	Définit un ensemble unique de capacités pour chaque ensemble d'organisations assigné à un administrateur.	**Administrateur**. Les rôles admin sont assignés aux administrateurs. **Capacités et organisations** Les capacités et les organisations sont assignées, directement ou indirectement (dynamiquement) aux rôles admin.
Capacité	Définit un groupe de droits système.	**Administrateur**. Les capacités sont assignées aux administrateurs.
Stratégie	Établit les limites applicables aux mots de passe et à l'authentification.	**Compte utilisateur** Les stratégies sont assignées aux comptes utilisateur. **Organisation**. Les stratégies sont assignées à ou héritées par les organisations.
Stratégie d'audit	Définit les règles permettant d'évaluer les utilisateurs pour détecter les violations de compatibilité.	**Compte utilisateur** Les stratégies d'audit sont assignées aux comptes utilisateur. **Organisation**. Les stratégies d'audit sont assignées aux organisations.

◆ ◆ ◆ CHAPITRE 2

Démarrage de l'interface utilisateur d'Identity Manager

La lecture de ce chapitre vous fera découvrir les interfaces graphiques (IG) d'Identity Manager et vous mettra rapidement en condition de commencer à utiliser Identity Manager.

Il se compose des rubriques suivantes :

Interface administrateur d'Identity Manager

Le système Identity Manager inclut deux interfaces graphiques principales permettant aux utilisateurs d'effectuer des tâches : l'interface utilisateur final et l'interface administrateur. La première, qui est aussi appelée interface utilisateur, est examinée plus loin dans ce chapitre, dans la section "Interface utilisateur final d'Identity Manager" à la page 40. L'interface administrateur fait quant à elle l'objet des lignes suivantes.

L'interface administrateur d'Identity Manager est la principale vue administrative du produit. À travers cette interface, les administrateurs Identity Manager gèrent les utilisateurs, configurent et assignent les ressources, définissent les droits et les niveaux d'accès, et contrôlent la compatibilité dans le système Identity Manager.

L'organisation de l'interface est représentée par les éléments suivants :

- **Onglets de la barre de navigation**. Situés en haut de toutes les pages de l'interface, ces onglets permettent de naviguer dans les principales zones fonctionnelles.
- **Sous-onglets ou menus**. Selon votre implémentation, vous pourrez voir des onglets ou des menus secondaires sous chacun des onglets de la barre de navigation. Ces sous-onglets ou menus permettent d'accéder à des tâches relevant d'une zone fonctionnelle donnée.

Dans certaines zones, par exemple dans la zone Comptes, des *formulaires à onglets* divisent les formulaires longs en une ou plusieurs pages, ce qui facilite la navigation. Vous en trouverez une illustration à la Figure 2–1.

Remarque – Un guide de référence rapide relatif à l'exécution des tâches administratives dans l'IG est disponible dans l'Annexe C, “Guide de référence rapide de l'interface utilisateur”.

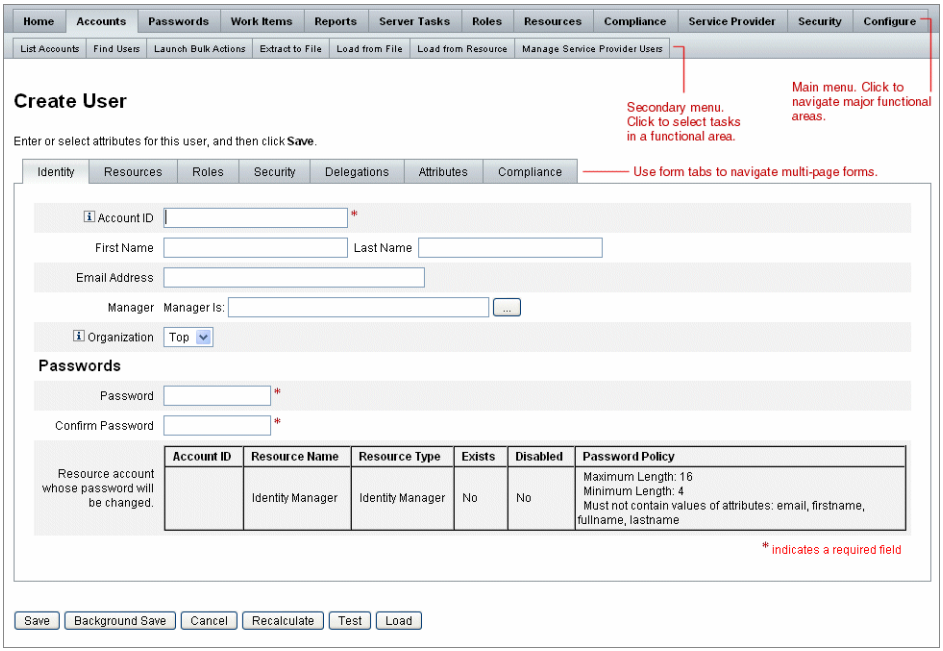


FIGURE 2–1 Interface administrateur d'Identity Manager

Connexion à l'interface administrateur d'Identity Manager

▼ Pour ouvrir l'interface administrateur

1 **Ouvrez un navigateur Web et saisissez l'URL suivant dans la barre d'adresse :**

`http://<AppServerHost>:<Port>/idm/login.jsp`

2 **Saisissez votre ID utilisateur et votre mot de passe et cliquez sur Connexion.**

L'interface administrateur s'ouvre si votre ID utilisateur a des capacités assignées et une organisation contrôlée assignée.

Limites des sessions et cookies

Si les cookies sont activés dans leur navigateur Web, les administrateurs resteront connectés à l'interface administrateur pendant toute la durée allouée par la limite de session configurée. Si les cookies sont désactivés dans le navigateur, certaines actions pousseront alors le système à inviter l'administrateur à se reconnecter en cours de session.

Ces actions sont les suivantes :

- l'annulation d'une opération de renommage d'administrateur, de rôle ou d'organisation,
- l'annulation de la suppression d'une organisation,
- la création de modules de connexion utilisateur et admin.

Les cookies doivent être activés pour éviter les demandes de connexion à répétition.

ID utilisateur oublié

Identity Manager permet à un administrateur de récupérer son ID utilisateur en cas d'oubli. Lorsqu'un administrateur clique sur ID d'utilisateur oublié ? dans la page de connexion, une page de recherche s'affiche et demande les informations d'attributs d'identité associées au compte telles que les nom et prénom, l'adresse e-mail ou le numéro de téléphone.

Identity Manager élabore ensuite une requête pour trouver un unique utilisateur correspondant aux valeurs saisies. Si aucune correspondance n'est trouvée ou s'il y en a plusieurs, un message d'erreur s'affiche sur la page Recherche d'ID d'utilisateur.

La fonctionnalité de recherche est activée par défaut, mais vous pouvez utiliser l'une des actions suivantes pour la désactiver :

- Définir `forgotUserIdMode` sur la valeur false dans `login.jsp`.
- Éditer l'objet Configuration système et définir l'attribut `disableForgotUserId` sur la valeur true pour l'attribut `admin` et/ou l'attribut `user`.

  Pour les instructions à suivre pour éditer un objet Configuration système, voir la section "Édition des objets Configuration Identity Manager" à la page 118.

Remarque – Si vous effectuez une mise à niveau à partir d'une version antérieure d'Identity Manager vers la version 8.1, la fonctionnalité ID d'utilisateur oublié ? sera *désactivée* par défaut.

Pour l'activer, vous devez modifier les attributs suivants dans l'objet Configuration système ("Édition des objets Configuration Identity Manager" à la page 118) :

```
ui.web.user.disableForgotUserId = false
ui.web.admin.disableForgotUserId = false
```

L'ensemble de noms d'attributs utilisateur présenté est configuré par le biais des attributs de configuration système `security.authn.lookupUserIdAttributes.<Administrator Interface | User Interface>`. Les attributs qui peuvent être spécifiés sont ceux définis comme interrogeables dans l'objet Configuration `IDM Schema Configuration` (Configuration du schéma IDM).

En cas de récupération, Identity Manager envoie un e-mail à l'adresse e-mail de l'utilisateur récupéré en utilisant le modèle d'e-mail Récupération d'ID d'utilisateur.

Interface utilisateur final d'Identity Manager

L'interface utilisateur final d'Identity Manager (aussi appelée « Interface utilisateur d'Identity Manager ») présente une vue limitée du système Identity Manager. Cette vue est spécifiquement adaptée aux utilisateurs dépourvus de capacités administratives.

Remarque – Pour les instructions de connexion à l'interface utilisateur final, voir la section "Connexion à l'interface utilisateur final d'Identity Manager" à la page 43.

Un utilisateur peut effectuer différentes opérations depuis l'interface utilisateur, notamment modifier son mot de passe, effectuer des tâches d'auto-provisioning et gérer les éléments de travail et les délégations.

Identity Manager peut être configuré de sorte que les utilisateurs puissent demander un compte en cliquant sur un lien sur la page de connexion de l'interface utilisateur final. Pour tout détail, voir la section "Inscription anonyme" à la page 97.

Les cinq onglets de l'interface utilisateur final

L'interface utilisateur final se divise en cinq parties :

Onglet Accueil

Quand un utilisateur se connecte à l'interface utilisateur d'Identity Manager, tous les éléments de travail et les délégations en attente pour cet utilisateur s'affichent dans l'onglet Accueil, comme illustré dans la figure suivante.

FIGURE 2–2 L'interface utilisateur (onglet Accueil)

L'onglet Accueil permet d'accéder rapidement à tous les éléments en attente. Les utilisateurs peuvent cliquer sur un élément dans la liste pour répondre à une demande d'élément de travail ou effectuer d'autres actions disponibles.

Onglet Éléments de travail

L'onglet Éléments de travail est lui-même divisé en plusieurs onglets distincts : Approbations, Attestations, Résolutions et Autre. Dans cette zone de l'interface utilisateur, les utilisateurs peuvent approuver ou rejeter tout élément de travail en attente dont ils sont le propriétaire ou sur lequel ils sont autorisés à agir.

Onglet Demandes

L'onglet Demandes comporte deux sous-onglets : Lancer les demandes et Afficher.

L'onglet Lancer les demandes offre deux choix aux utilisateurs : Mise à jour de mes rôles et Mise à jour de mes ressources.

- La page Mise à jour de mes rôles permet aux utilisateurs d'effectuer une demande à partir d'une liste de rôles disponibles susceptibles d'être appropriés à l'utilisateur. Lorsque l'utilisateur final envoie une demande de rôle, un élément de travail est généré et une notification d'approbation est envoyée aux approbateurs désignés pour ce rôle. Les utilisateurs finals peuvent également demander leur suppression ou *l'annulation de leur assignation* de un ou plusieurs rôles.

  Reportez-vous au Chapitre 5, “Rôles et ressources” pour toute informations sur la création de rôles optionnels auxquels les utilisateurs finals peuvent demander à accéder.
- La page Mise à jour de mes ressources permet aux utilisateurs d'effectuer une demande à partir d'une liste de ressources individuelles susceptibles d'être appropriées pour l'utilisateur. À l'instar des demandes de rôle, les demandes de ressources génèrent des éléments de travail qui requièrent une approbation pour pouvoir être traités.

Le sous-onglet Afficher affiche les détails d'état des demandes envoyées par l'utilisateur. Depuis cette zone, les utilisateurs peuvent afficher le statut des processus et les résultats des tâches pour les demandes qu'ils envoient.

Onglet Délégations

Depuis l'onglet Délégations, les utilisateurs peuvent déléguer des éléments de travail à d'autres utilisateurs Identity Manager. Par exemple, un utilisateur qui est l'approbateur désigné pour un ou plusieurs rôles peut décider que les éléments de travail d'approbation à venir seront envoyés à un collègue pendant un laps de temps donné alors que lui-même sera en congé. La page Délégations permet aux utilisateurs de créer et gérer des délégations sans devoir recourir aux services d'un administrateur.

Onglet Profil

Les utilisateurs finaux peuvent gérer leurs paramètres de mot de passe et d'attribut de compte Identity Manager depuis l'onglet Profil. Cet onglet se divise en quatre sous-onglets :

- **Changement du mot de passe**. Les utilisateurs finaux peuvent modifier leur mot de passe sur une ressource sélectionnée ou sur toutes les ressources.
- **Attributs de compte**. Les utilisateurs finaux peuvent modifier certains attributs, par exemple l'adresse e-mail du compte à laquelle Identity Manager envoie les notifications.
- **Questions d’authentification**. Permet de gérer les questions et réponses d'authentification pour le compte utilisateur.
- **Privilèges d'accès**. Liste les assignations de rôles et de ressources actuellement assignées à l'utilisateur.

Connexion à l'interface utilisateur final d'Identity Manager

Suivez les instructions ci-après pour vous connecter à l'interface utilisateur final d'Identity Manager.

▼ Pour ouvrir l'interface utilisateur final

1. **Ouvrez un navigateur Web et saisissez l'URL suivant dans la barre d'adresse :**

   `http://<AppServerHost>:<Port>/idm/user/login.jsp`

2. **Saisissez un ID utilisateur et un mot de passe et cliquez sur Connexion.**

   L'interface utilisateur final s'ouvre.

Récupération des ID utilisateur oubliés

Identity Manager permet aux utilisateurs finaux de récupérer leurs ID utilisateur en cas d'oubli. Pour plus d'informations, reportez-vous à"ID utilisateur oublié" à la page 39 dans la section "Connexion à l'interface administrateur d'Identity Manager" à la page 39.

Aide et instructions

Pour réussir à compléter certaines tâches, il est possible que vous deviez consulter l'aide et les *instructions*(informations relatives aux champs et instructions proprement dites) d'Identity Manager. L'aide et les instructions sont disponibles depuis les interfaces administrateur et utilisateur final d'Identity Manager.

Aide d'Identity Manager

Pour obtenir de l'aide et des informations sur les tâches, cliquez sur le bouton Aide qui figure dans le haut de toutes les pages des interfaces administrateur et utilisateur final, comme illustré à la figure suivante.

FIGURE 2–3 Le bouton Aide de l'interface d'Identity Manager

Le bas de chaque fenêtre d'aide comporte un lien Contents (Sommaire) qui vous amène à d'autres rubriques d'aide et au glossaire terminologique d'Identity Manager.

Instructions d'Identity Manager

Les instructions d'Identity Manager sont une aide succincte et ciblée qui s'affiche à proximité de nombreux champs de page. Leur objectif est de vous aider à saisir les informations ou à effectuer les sélections au fur et à mesure que vous progressez sur une page pour effectuer une tâche.

Un symbole marqué de la lettre « i » s'affiche en regard des champs qui comportent des instructions. En cliquant sur ce symbole, vous ouvrez une fenêtre contenant les informations associées.

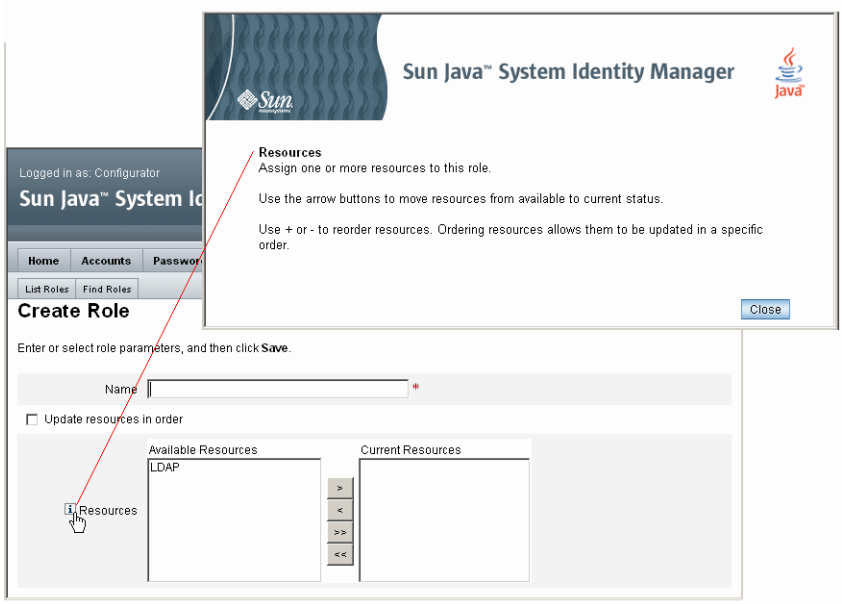


FIGURE 2–4 Instructions d'Identity Manager

Page de débogage d'Identity Manager

L'interface administrateur inclut des pages qui sont utiles pour optimiser Identity Manager ou dans le cadre du dépannage. Pour accéder à ces pages, ouvrez la page de débogage d'Identity Manager qui est aussi appelée page Paramètres du système.

Pour ouvrir la page de débogage d'Identity Manager, saisissez l'URL suivant dans votre navigateur (selon vos plate-forme et configuration, les URL peuvent être sensibles à la casse).

`http://<AppServerHost>:<Port>/idm/debug/session.jsp`

Les utilisateurs doivent avoir la capacité Déboguer pour afficher les pages `/idm/debug/`. Pour toute information sur les capacités, voir la section “Assignation de capacités aux utilisateurs ” à la page 219.

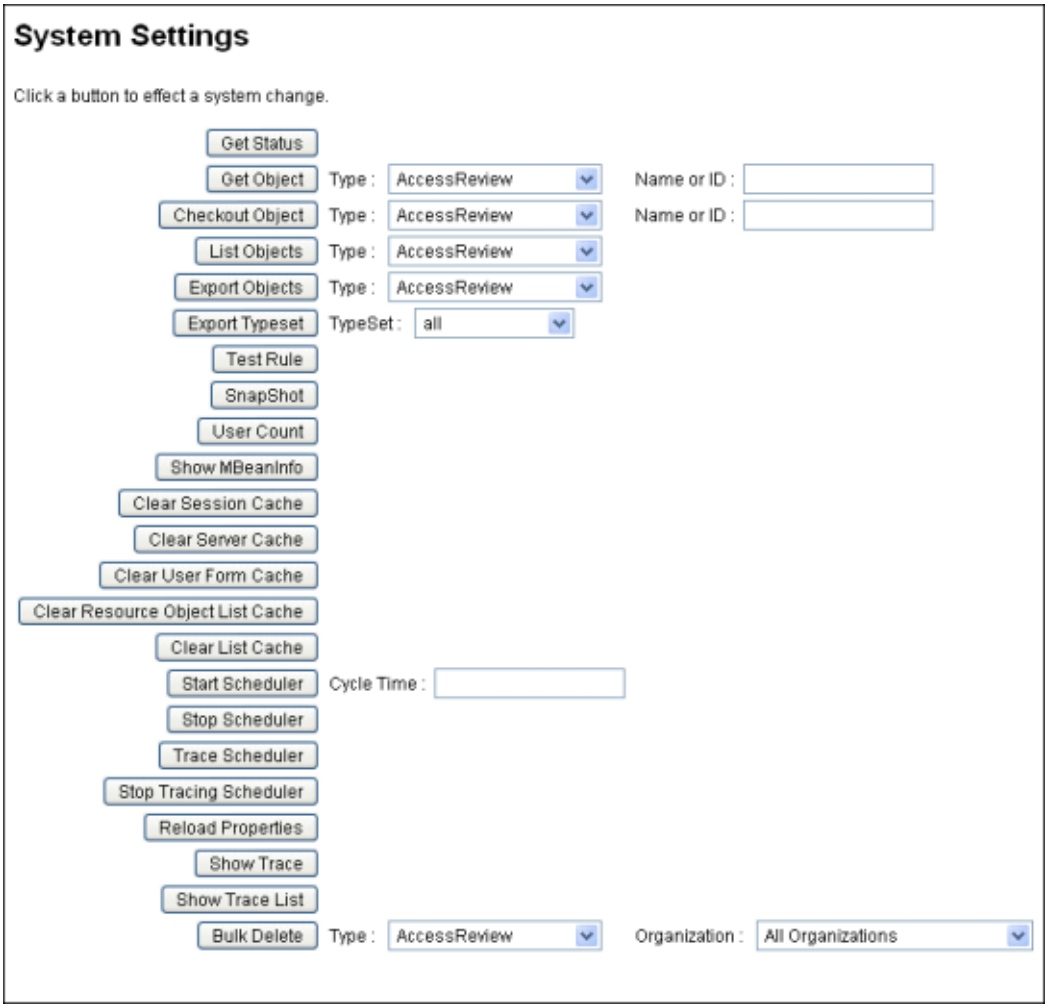


FIGURE 2–5 Page de débogage d'Identity Manager (Paramètres du système)

Pour toute information sur le dépannage d'Identity Manager, voir le Chapitre 5, "Tracing and Troubleshooting" du *Sun Identity Manager 8.1 System Administrator's Guide*.

Identity Manager IDE

L'environnement de développement intégré Sun Identity Manager (Identity Manager IDE) fournit une représentation graphique des formulaires, règles et flux de travaux d'Identity Manager. Il s'agit d'un plug-in NetBeans complètement intégré, distribué avec Identity Manager, dans le package de distribution d'Identity Manager.

En utilisant Identity Manager IDE, vous pouvez créer et éditer des formulaires qui établissent les fonctionnalités disponibles sur chaque page d'Identity Manager. Vous pouvez aussi modifier les *flux de travaux* d'Identity Manager, qui définissent les séquences d'actions suivies ou les tâches effectuées lorsque vous travaillez avec les comptes utilisateur Identity Manager. De plus, vous pouvez modifier les règles définies dans Identity Manager qui déterminent le comportement des flux de travaux.

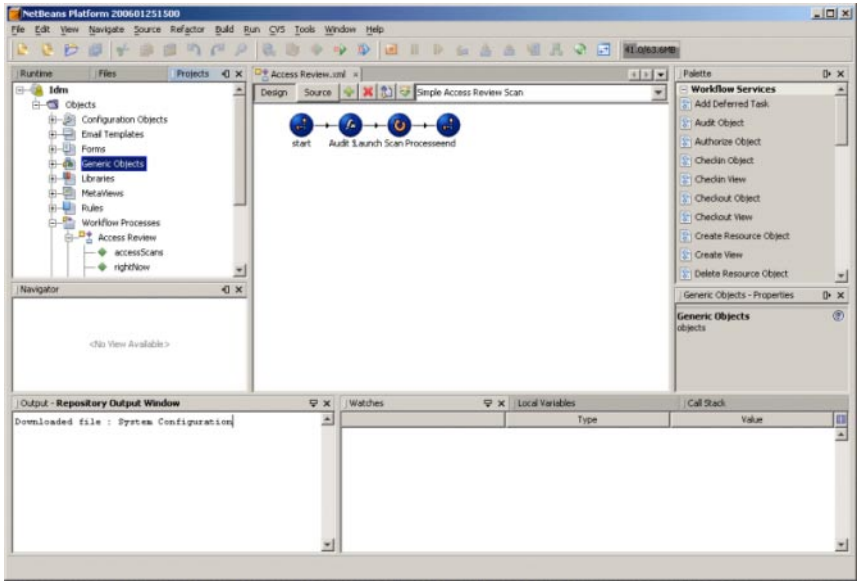


FIGURE 2–6 L'interface d'Identity Manager IDE

Pour télécharger Identity Manager IDE, visitez le site Web suivant :

`https://identitymanageride.dev.java.net/`

Vous pouvez aussi utiliser Business Process Editor (BPE) pour procéder à des personnalisations, si vous avez installé ce programme avec des versions antérieures d'Identity Manager.

Prochaines étapes

Maintenant que vous vous êtes familiarisé avec les interfaces d'Identity Manager et les méthodes permettant de trouver des informations, utilisez le tableau de référence suivant qui vous guidera vers les sujets que vous souhaitez approfondir :

Sujet du chapitre	Description
Chapitre 3, “Gestion des utilisateurs et des comptes”	Décrit la zone Comptes de l'interface et contient les procédures de gestion des comptes utilisateur.
Chapitre 5, “Rôles et ressources”	Explique comment travailler avec les rôles et les ressources d'Identity Manager.
Chapitre 4, “Configuration des objets d'administration d'entreprise”	Détaille les tâches de configuration ainsi que le paramétrage des objets Identity Manager.
Chapitre 6, “Administration”	Explique la création et la gestion des administrateurs et organisations Identity Manager.
Chapitre 7, “Chargement et synchronisation des données”	Constitue un guide des fonctionnalités et outils à votre disposition pour mettre à jour les données courantes dans Identity Manager.
Chapitre 8, “Génération de rapports”	Décrit les rapports et leur génération.
Chapitre 9, “Modèles de tâches”	Indique les modèles de tâches que vous pouvez utiliser pour configurer certains comportements de flux de travaux.
Chapitre 10, “Journalisation d'audit”	Présente en détail les journaux d'audit et le fonctionnement du système d'audit.
Chapitre 11, “PasswordSync”	Explique comment paramétrer l'utilitaire PasswordSync pour synchroniser les changements de mots de passe dans les domaines Windows Active Directory avec les changements survenant dans Identity Manager.
Chapitre 12, “Sécurité”	Décrit les fonctionnalités de sécurité et leur utilisation.
Chapitre 13, “Audit des identités : principes de base”	Présente les principes de contrôle de base.
Chapitre 14, “Audit : stratégies d'audit”	Détaille la création de stratégies d'audit.
Chapitre 15, “Audit : contrôler la conformité”	Explique comment réaliser des examens d'audit et implémenter des pratiques facilitant la gestion de la conformité aux réglementations fédérales obligatoires.
Chapitre 16, “Exportateur de données”	La fonction Exportateur de données permet de consigner des informations sur les utilisateurs, les rôles et d'autres types d'objets dans un entrepôt de données externe.

Sujet du chapitre	Description
Chapitre 17, “Administration de Service Provider”	Présente les fonctionnalités permettant de gérer les utilisateurs de Service Provider.
Annexe A, “Références `lh`”	Décrit les commandes disponibles depuis la ligne de commande d'Identity Manager.
Annexe B, “Schéma de la base de données du journal d'audit”	Indique les valeurs du schéma des données d'audit pour les types de bases de données pris en charge et les mappages de la base de données du journal d'audit.
Annexe C, “Guide de référence rapide de l'interface utilisateur”	Guide de référence rapide relatif à l'exécution des tâches administratives dans l'IG. Il indique le point de départ principal de chaque tâche ainsi que les points de départ ou méthodes de remplacement (le cas échéant) à votre disposition pour effectuer la tâche en question.
Annexe D, “Définitions des capacités”	Liste des capacités fonctionnelles et basées sur les tâches par défaut d'Identity Manager (définitions incluses). Cette annexe répertorie également les onglets et sous-onglets auxquels chaque capacité basée sur des tâches permet d'accéder.

◆ ◆ ◆ CHAPITRE 3

Gestion des utilisateurs et des comptes

Ce chapitre contient les informations et procédures à suivre pour créer et gérer des utilisateurs depuis l'interface administrateur d'Identity Manager.

Il se compose des sections suivantes :

Zone Comptes de l'interface

On appelle utilisateur toute personne ayant un compte système Identity Manager. Identity Manager stocke une gamme de données pour chaque utilisateur. Collectivement, ces informations forment l'identité Identity Manager d'un utilisateur.

La page Comptes / Liste des utilisateurs d'Identity Manager permet de gérer les utilisateurs Identity Manager. Pour accéder à cette zone, cliquez sur **Comptes** sur la barre de menu de l'interface administrateur.

La liste des comptes affiche tous les comptes utilisateur Identity Manager. Les comptes sont regroupés en organisations et organisations virtuelles, lesquelles sont représentées de manière hiérarchique par des dossiers.

Vous pouvez trier la liste des comptes par nom complet (Nom complet), nom de famille d'utilisateur (Nom) ou prénom d'utilisateur (Prénom). Cliquez sur la barre de titre pour effectuer le tri en fonction d'une colonne. Un nouveau clic sur le même titre permet de basculer entre les ordres de tri croissant et décroissant. Lorsque vous effectuez un tri par nom complet (colonne Nom complet), tous les éléments de la hiérarchie, à tous les niveaux, sont triés par ordre alphabétique.

Pour développer l'affichage hiérarchique et voir tous les comptes d'une organisation, cliquez sur l'indicateur en regard du dossier. Un nouveau clic sur cet indicateur permet de réduire l'affichage.

Listes d'actions de la zone Comptes

Utilisez les listes d'actions (situées en haut et en bas de la zone des comptes, comme indiqué dans "Listes d'actions de la zone Comptes" à la page 52), pour effectuer tout un éventail d'actions.

Les sélections de listes d'actions sont divisées en :

- **Nouvelles actions**. Créer des utilisateurs, des organisations et des jonctions d'annuaires.
- **Actions de l'utilisateur** Éditer, afficher et modifier le statut des utilisateurs ; modifier et réinitialiser les mots de passe ; supprimer, activer, désactiver, déverrouiller, déplacer, mettre à jour et renommer des utilisateurs ; et exécuter un rapport d'audit.
- **Actions d'organisation**. Effectuer tout un éventail d'actions d'organisation et d'utilisateur.

Recherche dans la zone Liste des comptes

La fonctionnalité de recherche de la zone des comptes permet de localiser des utilisateurs et des organisations. Sélectionnez Organisations ou Utilisateurs dans la liste, entrez la ou les premières lettres du nom d'utilisateur/organisation dans la zone de recherche puis cliquez sur **Rechercher**. Pour plus d'informations sur la fonctionnalité de recherche de la zone des comptes, reportez-vous à "Recherche et affichage des comptes utilisateur" à la page 62.

Statut des comptes utilisateur

Les icônes affichées en regard de chaque compte utilisateur en indiquent le statut attribué. Le Tableau 3–1 indique la signification des différentes icônes.

TABLEAU 3–1 Description des icônes de statut des comptes utilisateur

Indicateur	Statut
	Le compte Identity Manager de l'utilisateur est verrouillé. Vous remarquerez que cette icône ne reflète que l'état verrouillé du compte Identity Manager, pas celui des comptes de ressources de l'utilisateur. Les utilisateurs sont verrouillés lorsque le nombre maximum d'échecs de connexion à Identity Manager, défini dans la Stratégie de compte Identity Manager, est dépassé. Seules les connexions par mot de passe ou par questions aux comptes Identity Manager sont prises en compte dans les calculs pour le maximum. Par conséquent, si une application de connexion à Identity Manager (c'est-à-dire l'interface administrateur, l'interface utilisateur final, etc.) n'inclut pas le module de connexion à Identity Manager dans son groupe de modules de connexion, la stratégie relative aux échecs de connexion à Identity Manager par mot de passe ne sera pas prise en compte. Cependant, quelle que soit la pile de modules de connexion configurée pour une application de connexion à Identity Manager donnée, les échecs de connexion par questions qui dépassent le maximum configuré dans la Stratégie de compte Identity Manager peuvent entraîner le verrouillage de l'utilisateur et l'affichage de cette icône. Pour plus d'informations sur le déverrouillage des comptes, reportez-vous à "Déverrouillage des comptes utilisateur" à la page 79.
	Le compte Identity Manager de l'administrateur est verrouillé. Vous remarquerez que cette icône reflète uniquement l'état verrouillé du compte Identity Manager, pas celui des comptes de ressources de l'administrateur. Pour plus d'informations, reportez-vous à la description de l'icône utilisateur verrouillé, ci-dessus.
	Le compte est désactivé sur toutes les ressources assignées et sur Identity Manager (lorsqu'un compte est activé, aucune icône ne s'affiche). Pour toute information sur l'activation des comptes désactivés, reportez-vous à "Désactivation, activation et déverrouillage des comptes utilisateur" à la page 76.
	Le compte est partiellement désactivé, ce qui signifie qu'il est désactivé sur une ou plusieurs ressources assignées.
	Le système tente mais échoue dans sa tentative de créer ou mettre à jour le compte utilisateur Identity Manager sur une ou plusieurs ressources (lorsqu'un compte est mis à jour sur toutes les ressources assignées, aucune icône ne s'affiche).

Remarque – Un nom d'utilisateur de responsable s'affiche entre parenthèses dans la colonne Responsable si Identity Manager ne trouve aucun compte Identity Manager correspondant au nom listé.

Pages relatives aux utilisateurs (Créer/Éditer/Afficher)

Cette section décrit les pages Créer un utilisateur, Éditer l'utilisateur et Afficher l'utilisateur disponibles dans l'interface Administrateur. Les instructions d'utilisation de ces pages figurent plus loin dans ce chapitre.

Remarque – Cette documentation explique le jeu par défaut de pages Créer un utilisateur, Éditer l'utilisateur et Afficher l'utilisateur fourni avec Identity Manager. Cependant, pour mieux tenir compte des processus de votre entreprise ou de capacités administrateur spécifiques, il vous convient de créer des formulaires utilisateur personnalisés pour votre environnement. Pour plus d'informations sur la personnalisation du formulaire utilisateur, voir le Chapitre 2, "Identity Manager Forms" du *Sun Identity Manager Deployment Reference*.

Les pages utilisateur par défaut d'Identity Manager sont organisées en onglets ou sections comme suit :

- Identité
- Assignations
- Sécurité
- Délégations
- Attributs
- Conformité

Onglet Identité

La zone Identité définit l'ID de compte, le nom, les informations de contact d'un utilisateur ainsi que le mot de passe de son compte Identity Manager. Elle identifie également les ressources auxquelles l'utilisateur a accès ainsi que la stratégie de mot de passe gouvernant chaque compte de ressources.

Remarque – Pour toute information sur la configuration des stratégies de mot de passe pour les comptes utilisateur, lisez la section "Gestion de la sécurité des comptes et des privilèges" à la page 88 de ce même chapitre.

La figure suivante illustre la zone Identité de la page Créer un utilisateur.

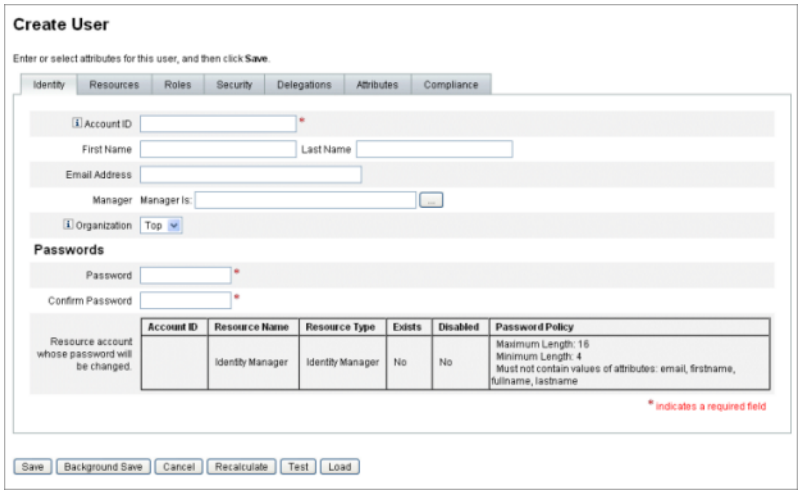


FIGURE 3–1 Créer un utilisateur - Identité

Onglet Ressources

La zone Ressources indique les attributions directes de ressources et de groupes de ressources d'un utilisateur. Il est également possible d'assigner des exclusions de ressources.

Les ressources assignées directement complètent les ressources assignées indirectement à l'utilisateur par le biais de l'*assignation de rôles*. L'assignation de rôles établit un profil pour une classe d'utilisateurs. Les rôles définissent l'accès d'un utilisateur aux ressources par le biais de l'assignation indirecte.

Onglet Rôles

L'onglet Rôles permet d'assigner un ou plusieurs rôles à un utilisateur et de gérer ces assignations de rôles.

Pour plus d'informations sur cet onglet, reportez-vous à "Pour assigner des rôles à un utilisateur" à la page 146.

Onglet Sécurité

Dans la terminologie d'Identity Manager, un utilisateur auquel des capacités étendues ont été assignées est un *administrateur* Identity Manager. L'onglet Sécurité permet d'assigner des privilèges d'administrateur à un utilisateur.

Pour plus d'informations sur l'utilisation de l'onglet Sécurité pour créer des administrateurs, reportez-vous à "Création et gestion des administrateurs" à la page 203.

Le formulaire **Sécurité** se compose des sections suivantes.

- **Rôles admin**. Assigne un ou plusieurs rôles d'administrateur à l'utilisateur. Un rôle est une association spécifique de capacités et d'organisations contrôlées, qui facilite l'assignation d'obligations administratives aux utilisateurs de manière coordonnée.
- **Capacités**. Active des droits dans le système Identity Manager. Chaque administrateur Identity Manager se voit attribuer une ou plusieurs capacités, en général alignées sur les responsabilités de son poste.

  Les capacités sont examinées à la section "Comprendre et gérer les capacités" à la page 216. Une liste de capacités basées sur des tâches est inclue dans l'Annexe D, "Définitions des capacités", Définitions des capacitésAnnexe D, "Définitions des capacités". Cette annexe répertorie également les onglets et sous-onglets auxquels chaque capacité permet d'accéder.
- **Organisations contrôlées**. Assigne des organisations que cet utilisateur a le droit de gérer en tant qu'administrateur. Il peut gérer des objets dans l'organisation assignée et dans n'importe quelle organisation se trouvant sous cette organisation dans la hiérarchie.

Remarque – Pour avoir des capacités d'administrateur, un utilisateur doit se voir assigner au moins un rôle admin ou une ou plusieurs capacités ET une ou plusieurs organisations contrôlées. Pour plus d'informations sur les administrateurs Identity Manager, reportez-vous à "Comprendre l'administration d'Identity Manager" à la page 201.

- **Formulaire utilisateur**. Spécifie le formulaire utilisateur qui sera utilisé par l'administrateur pour créer et éditer des utilisateurs. Si **Aucun(e)** est sélectionné, l'administrateur héritera du formulaire utilisateur assigné à son organisation.
- **Formulaire d'affichage utilisateur**. Spécifie le formulaire utilisateur qui sera utilisé par l'administrateur pour afficher les utilisateurs. Si **Aucun(e)** est sélectionné, l'administrateur héritera du formulaire d'affichage utilisateur assigné à son organisation.
- **Stratégie de compte**. Établit les limites applicables aux mots de passe et à l'authentification.

Onglet Délégations

L'onglet Délégations de la page Créer un utilisateur permet de déléguer des éléments de travail à d'autres utilisateurs pendant un laps de temps donné. Pour plus d'informations sur la délégation des éléments de travail, lisez "Délégation des éléments de travail" à la page 234.

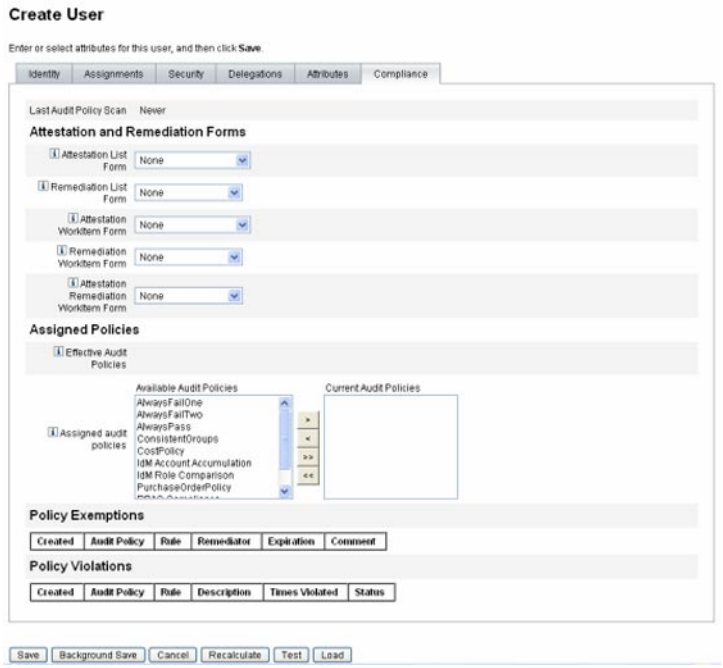
Onglet Attributs

L'onglet Attributs de la page Créer un utilisateur définit les attributs de compte associés aux ressources assignées. Les attributs listés sont classés par ressource assignée et diffèrent selon les ressources qui sont assignées.

Onglet Conformité

L'onglet Conformité :

- Permet de sélectionner les formulaires d'attestation et de résolution pour le compte utilisateur.
- Spécifie les stratégies d'audit assignées au compte utilisateur, notamment celles appliquées via l'assignation d'organisation de l'utilisateur. Ces assignations de stratégie peuvent uniquement être modifiées en éditant l'organisation courante de l'utilisateur ou en déplaçant l'utilisateur dans une autre organisation.
- Indique l'état courant des scannages, violations et dispenses de stratégie (comme illustré dans la figure suivante), si applicable pour le compte utilisateur. Les informations incluent la date et l'heure du dernier scannage de stratégie pour l'utilisateur sélectionné.



Pour assigner des stratégies d'audit, déplacez les stratégies sélectionnées de la liste **Stratégies d'audit disponibles** à la liste **Stratégies d'audit en cours**.

Remarque – Vous pouvez afficher les violations de conformité consignées pour un utilisateur pendant une période de temps spécifique en sélectionnant **Afficher le journal des violations de conformité** depuis la liste **Actions de l'utilisateur** et en spécifiant la plage d'entrées à afficher.

Création d'utilisateurs et utilisation des comptes utilisateur

Vous pouvez effectuer depuis la page Comptes/Liste des utilisateurs de l'interface Administrateur tout un éventail d'actions sur les objets système suivants :

- **Administrateurs et utilisateurs** Afficher, créer, éditer, déplacer, renommer, suspendre, activer, désactiver, mettre à jour, déverrouiller, supprimer, annuler une assignation, supprimer un lien et vérifier.

  Pour plus d'informations sur la création et l'édition des comptes administrateur, reportez-vous à "Comprendre l'administration d'Identity Manager" à la page 201.
- **Organisations**. Créer, éditer, actualiser et effectuer des actions d'utilisateur sur des membres de l'organisation.

  Pour plus d'informations sur les organisations, reportez-vous à "Comprendre les organisations d'Identity Manager" à la page 209.
- **Jonctions d'annuaires** . Créer un ensemble d'organisations reliées hiérarchiquement pour refléter le jeu courant de conteneurs hiérarchiques d'une ressource d'annuaire.

  Pour plus d'informations sur les jonctions d'annuaires, reportez-vous à"Comprendre les jonctions d'annuaires et les organisations virtuelles" à la page 213.

Activation des schémas de processus

L'activation des schémas de processus décrit le flux de travaux suivi par Identity Manager quand il crée ou agit de quelque autre manière sur un compte utilisateur. Lorsqu'ils sont activés, les schémas de processus s'affichent sur la page des résultats ou la page de récapitulatif de la tâche qui est créée lorsqu'Identity Manager complète la tâche.

Dans Identity Manager version 8.0, les schémas de processus étaient désactivés tant pour les nouvelles installations que pour les mises à jour.

▼ Pour activer les schémas de processus pour les utiliser dans Identity Manager

1 **Ouvrez l'objet Configuration système pour l'éditer en suivant la procédure de la section "Édition des objets Configuration Identity Manager" à la page 118.**

2 **Localisez l'élément XML suivant :**

```
<Attribute name='disableProcessDiagrams'>
  <Boolean>true</Boolean>
</Attribute>
```

3 **Remplacez la valeur `true` par la valeur `false`.**

4 **Cliquez sur Enregistrer.**

5 **Redémarrez votre ou vos serveurs pour que le changement soit appliqué.**

Les schémas de processus peuvent également être activés dans l'interface utilisateur final à condition d'avoir été activés au préalable dans l'interface administrateur en suivant les étapes indiquées plus haut. Pour de plus amples détails, voir la section "Pour activer les schémas de processus dans l'interface utilisateur final" à la page 114.

▼ Pour créer un utilisateur dans Identity Manager

Vous pouvez créer et gérer des utilisateurs depuis l'onglet Comptes de la barre de menu de l'interface administrateur.

1 **Dans l'interface administrateur, cliquez sur Comptes.**

2 **Pour créer un utilisateur dans une organisation spécifique, sélectionnez cette dernière puis sélectionnez Nouvel utilisateur dans la liste Nouvelles actions.**

Sinon, pour créer un utilisateur dans l'organisation supérieure, sélectionnez Nouvel utilisateur dans la liste Nouvelles actions.

3 **Indiquez les informations requises dans les onglets ou sections suivants.**

- **Identité**. Nom, organisation, mot de passe et autres détails (voir "Onglet Identité" à la page 54).
- **Ressources**. Assignations de ressources individuelles et groupes de ressources, exclusions de ressources (voir "Onglet Ressources" à la page 55).
- **Rôles**. Assignations de rôle. Pour plus d'informations sur les rôles, voir la section "Comprendre et gérer les rôles" à la page 121. Pour les instructions à suivre pour compléter l'onglet Rôles, reportez-vous à "Pour assigner des rôles à un utilisateur" à la page 146.
- **Sécurité**. Rôles admin, organisations contrôlées et capacités. Également, paramètres des formulaires utilisateur et stratégie de compte (voir "Onglet Sécurité" à la page 55).
- **Délégations**. Délégations d'éléments de travail (voir "Onglet Délégations" à la page 56).
- **Attributs**. Attributs spécifiques pour ressources assignées (voir "Onglet Attributs" à la page 56).

- **Conformité**. Sélectionne les formulaires d'attestation et de résolution pour le compte utilisateur. La zone Conformité permet également de spécifier les stratégies d'audit assignées au compte utilisateur, notamment celles appliquées via l'assignation d'organisation de l'utilisateur. Cet onglet indique le statut actuel des scannages, violations et dispenses de stratégie, et comprend des informations sur le dernier scannage de stratégie d'audit de l'utilisateur (voir "Onglet Attributs" à la page 56).

  Vous remarquerez que les sélections disponibles dans une zone dépendent des sélections effectuées dans une autre zone.

Cependant, pour mieux tenir compte des processus de votre entreprise ou de capacités administrateur spécifiques, il vous convient de créer des formulaires utilisateur personnalisés pour votre environnement. Pour plus d'informations sur la personnalisation du formulaire utilisateur, voir le "Customizing Forms" du *Sun Identity Manager Deployment Reference*.

4 Lorsque vous avez terminé, enregistrez le compte.

Deux options s'offrent à vous pour enregistrer un compte utilisateur :

- **Enregistrer**. Enregistre le compte utilisateur. Si vous assignez un grand nombre de ressources au compte, ce processus peut prendre du temps.
- **Enregistrer en arrière-plan**. Ce processus enregistre un compte utilisateur en tant que tâche d'arrière-plan, ce qui permet de continuer à travailler dans Identity Manager. Un indicateur de statut de tâche s'affiche sur la page Comptes, la page de résultat de recherche d'utilisateurs et la page Accueil, pour chaque enregistrement en cours.

  Les indicateurs de statut, comme décrit dans le tableau suivant, facilitent le contrôle de la progression du processus d'enregistrement.

Indicateur de statut	Statut
	Le processus d'enregistrement est en cours.
	Le processus d'enregistrement a été suspendu. Ceci signifie généralement que le processus attend une approbation.
	Le processus a été exécuté avec succès. Ceci signifie que le processus s'est terminé sans erreur et non que l'utilisateur a été enregistré correctement.
	Le processus n'a pas encore démarré.
	Le processus s'est terminé avec une ou plusieurs erreurs.

En déplaçant votre souris sur l'icône utilisateur s'affichant avec l'indicateur de statut, vous pouvez obtenir des détails sur le processus d'enregistrement en arrière-plan.

Remarque – Si l'ouverture est configurée, créer un utilisateur crée un élément de travail qui peut être affiché depuis l'onglet Approbations. Approuver cet élément ignore la date d'ouverture et crée le compte. Rejeter l'élément annule la création du compte. Pour plus d'informations sur la configuration de l'ouverture, reportez-vous à "Configuration de l'onglet Ouverture et clôture " à la page 333.

Création de comptes de ressource multiples pour un utilisateur

Identity Manager offre la possibilité d'assigner plusieurs comptes de ressources à un même utilisateur. Le logiciel permet en effet de définir plusieurs types de comptes de ressources ou *types de comptes* pour chaque ressource. Les types de comptes de ressources doivent être créés de façon à correspondre à chacun des types de comptes fonctionnels figurant sur la ressource. Par exemple, AIX SuperUser ou AIX BusinessAdmin.

Raison de l'assignation de comptes de ressource multiples à un utilisateur

Dans certaines situations, un utilisateur Identity Manager peut avoir besoin de plusieurs comptes sur une même ressource. Un utilisateur peut, en effet, avoir plusieurs fonctions professionnelles liées à la ressource en question. Il peut, par exemple, être à la fois utilisateur et administrateur de cette ressource. Les pratiques recommandées suggèrent d'utiliser des comptes séparés pour chaque fonction. De la sorte, si l'un des comptes est compromis, l'accès accordé par le biais de l'autre compte reste sécurisé.

Configuration des types de comptes

Pour qu'une ressource prenne en charge plusieurs comptes pour un même utilisateur, les types de comptes de la ressource doivent être définis au préalable dans Identity Manager. Pour définir les types de comptes de ressource pour une ressource, utilisez l'assistant Ressource. Pour toute informations, reportez-vous à "Gestion de la liste des ressources" à la page 162.

Vous devez activer et configurer les types de comptes de ressource avant de les assigner aux utilisateurs.

Assignation des types de comptes

Une fois les types de comptes définis, vous pouvez les assigner à une ressource. Identity Manager traite chaque assignation de type de comptes comme un compte séparé. Résultat, toute assignation distincte dans un rôle peut avoir un ensemble d'attributs différent.

À l'instar du cas où nous avons un unique compte par ressource, toutes les assignations d'un type spécifique ne créent qu'un compte, quel que soit leur nombre.

Bien que vous puissiez assigner les utilisateurs à tout nombre de types de comptes différents sur une ressource, chaque utilisateur ne peut se voir assigner qu'un compte d'un type donné sur une ressource. L'exception à cette règle est le type « default » (par défaut) intégré. Les utilisateurs peuvent avoir n'importe quel nombre de comptes du type par défaut sur une ressource. Ceci n'est cependant pas recommandé car cela peut engendrer une certaine confusion au moment de référencer les comptes dans les formulaires et les vues.

Recherche et affichage des comptes utilisateur

La fonctionnalité de recherche d'Identity Manager permet de rechercher des comptes utilisateur. Une fois les paramètres de recherche saisis et sélectionnés, Identity Manager trouve tous les comptes correspondant à vos sélections.

Pour rechercher des comptes, sélectionnez Comptes → Rechercher des utilisateurs dans la barre de menu. Vous pouvez rechercher des comptes en utilisant un ou plusieurs des types de recherche suivants :

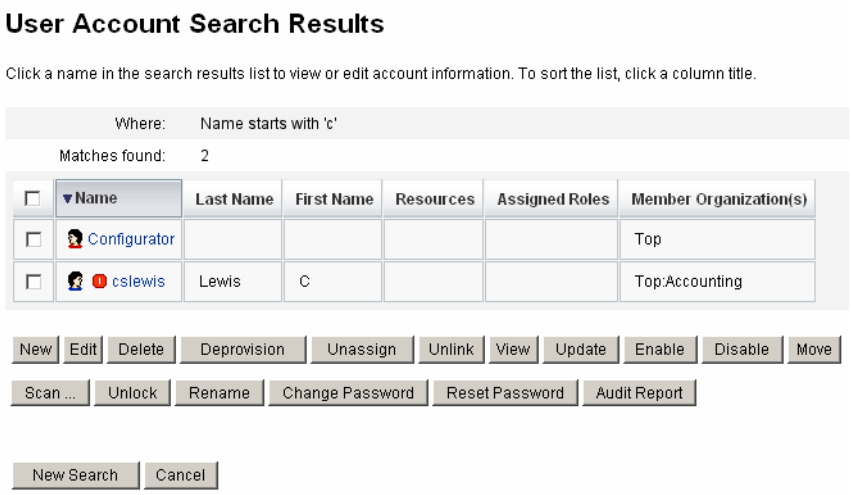
- **Détails du compte** (tels que ses nom d'utilisateur, adresse e-mail, nom ou prénom). Ces choix dépendent de l'implémentation Identity Manager spécifique de votre entreprise.
- **Responsable de l'utilisateur**. Le nom d'utilisateur du responsable s'affiche entre parenthèses si le nom d'utilisateur ne correspond à aucun compte existant dans Identity Manager.
- **Statut du compte de ressource**. Les options possibles sont les suivantes :
  - **Désactivé**. L'utilisateur ne peut accéder à aucun compte Identity Manager ou compte de ressource assigné.
  - **Désactivé partiellement**. L'utilisateur ne peut pas accéder à un ou plusieurs comptes de ressources.
  - **Activé**. L'utilisateur a accès à tous les comptes de ressources assignés.
- **Ressource assignée**. Les options possibles sont les suivantes :
  - **Rôle** (voir "Pour rechercher des utilisateurs assignés à un rôle spécifique" à la page 154),
  - **Organisation**,
  - **Contrôle organisationnel**,
  - **Capacités**,
  - **Rôle admin**.
- **Statut du compte utilisateur**. Les options possibles sont les suivantes :
  - **Verrouillé**. Le compte utilisateur est verrouillé car le nombre maximal d'échecs de connexion par mot de passe ou questions a dépassé le maximum autorisé.
  - **Pas verrouillé**. L'accès au compte utilisateur n'est pas limité.
- **Statut de mise à jour**. Les options possibles sont les suivantes :
  - **non**. Comptes utilisateur qui n'ont été mis à jour sur aucune ressource.

- **quelques**. Comptes utilisateur qui ont été mis à jour sur au moins une, mais pas sur toutes les ressources assignées.
- **tous**. Comptes utilisateur qui ont été mis à jour sur toutes les ressources assignées.

La liste des résultats de recherche affiche tous les comptes correspondant à votre recherche.

Depuis la page des résultats, vous pouvez :

- Sélectionner des comptes utilisateur à éditer. Pour éditer un compte, cliquez dessus dans la liste des résultats de recherche ; ou sélectionnez-le dans la liste puis cliquez sur Éditer.
- Effectuer des actions (par exemple activer, désactiver, déverrouiller, supprimer, mettre à jour ou changer/définir les mots de passe) sur un ou plusieurs comptes. Pour effectuer une action, sélectionnez un ou plusieurs comptes dans la liste des résultats de recherche puis cliquez sur l'action appropriée.
- Créer des comptes utilisateur.



Édition des utilisateurs

Les informations de cette section couvrent l'affichage, l'édition, la réassignation et le renommage des comptes utilisateur.

▼ Pour afficher les comptes utilisateur

Utilisez la page Afficher l'utilisateur et exécutez les étapes suivantes pour afficher les informations relatives aux comptes.

1. **Dans l'interface administrateur, cliquez sur Comptes dans le menu.**

   La page Liste des utilisateurs s'ouvre.

2. **Sélectionnez la case en regard de l'utilisateur dont vous voulez afficher les comptes.**

3. **Dans le menu déroulant Actions de l'utilisateur, sélectionnez Afficher.**

   La page Afficher l'utilisateur affiche un sous-ensemble des informations relatives à l'identité, les assignations, la sécurité, les délégations, les attributs et la conformité de l'utilisateur. Les informations de la page Afficher l'utilisateur sont en simple consultation et ne peuvent pas être éditées.

4. **Cliquez sur Annuler pour revenir à la liste Comptes.**

▼ Pour éditer les comptes utilisateur

Utilisez la page Éditer l'utilisateur et exécutez les étapes suivantes pour éditer les informations relatives aux comptes.

1. **Dans l'interface administrateur, cliquez sur Comptes dans le menu.**

2. **Sélectionnez la case en regard de l'utilisateur dont vous voulez éditer le compte.**

3. **Dans le menu déroulant Actions de l'utilisateur, sélectionnez Éditer.**

4. **Apportez les modifications de votre choix et enregistrez-les.**

   Identity Manager affiche la page de mise à jour des comptes de ressources. Cette page indique les comptes de ressources assignés à l'utilisateur et les changements qui vont être appliqués au compte.

5. **Sélectionnez Mettre tous les comptes de ressources à jour pour appliquer les changements à toutes les ressources assignées, ou sélectionnez un, plusieurs ou aucun des comptes de ressources associés à l'utilisateur concerné par la mise à jour.**

6. **Cliquez de nouveau sur Enregistrer pour terminer l'édition ou cliquez sur Retourner à Éditer pour apporter d'autres changements.**

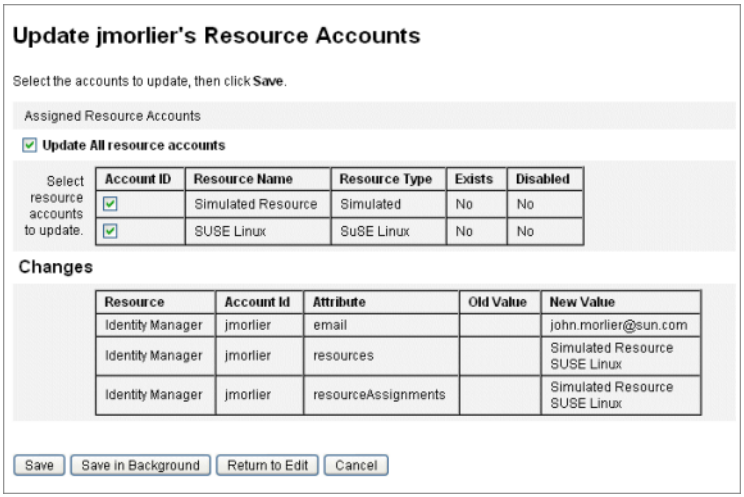


FIGURE 3–2 Éditer l'utilisateur (Mettre à jour les comptes de ressources)

Réassignation des utilisateurs à une autre organisation

L'action de déplacement permet de supprimer un ou plusieurs utilisateurs d'une organisation et de réassigner, ou déplacer, les utilisateurs dans une nouvelle organisation.

▼ Pour déplacer un utilisateur

1. **Dans l'interface administrateur, cliquez sur Comptes dans le menu.**

   La page Liste des utilisateurs s'ouvre.

2. **Sélectionnez la case en regard du ou des utilisateurs à déplacer.**

3. **Dans le menu déroulant Actions de l'utilisateur, sélectionnez Déplacer.**

   La page Modification de l'organisation des utilisateurs s'ouvre.

4. **Sélectionnez l'organisation que vous voulez réassigner à l'utilisateur et cliquez sur Lancer.**

Renommage des utilisateurs

En règle générale, le renommage d'un compte est une opération complexe. C'est pour cette raison qu'Identity Manager fournit une fonctionnalité distincte permettant de renommer le compte Identity Manager d'un utilisateur, ou un ou plusieurs des comptes de ressources associés à cet utilisateur.

Pour utiliser cette fonctionnalité de renommage, sélectionnez un compte utilisateur dans la liste puis sélectionnez l'option Renommer dans la liste Actions de l'utilisateur.

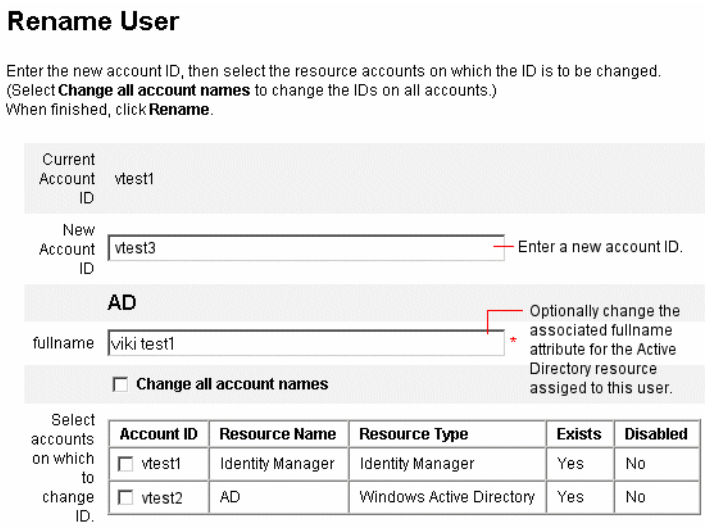
La page Renommer des utilisateurs permet de changer le nom du compte utilisateur, les noms de comptes de ressources associés et les attributs de comptes de ressources associés au compte Identity Manager de l'utilisateur.

Remarque – Certains types de ressources ne prennent pas en charge le renommage des comptes.

Comme illustré dans la figure suivante, l'utilisateur a une ressource Active Directory assignée.

Pendant le processus de renommage, vous pouvez changer :

- le nom du compte utilisateur Identity Manager,
- le nom du compte de ressources Active Directory,
- l'attribut de ressource Active Directory (nom complet).



Mise à jour des ressources associées à un compte

Dans le cadre d'une action de mise à jour, Identity Manager met à jour les ressources associées à un compte utilisateur. Les mises à jour effectuées depuis la zone Comptes envoient tous les changements en attente apportés au préalable à un utilisateur aux ressources sélectionnées.

Ce cas de figure peut se présenter si :

- une ressource n'était pas disponible au moment des mises à jour ;
- un changement apporté à un rôle ou un groupe de ressources devait être diffusé à tous les utilisateurs assignés à ce rôle/groupe de ressources. Dans ce cas, vous devez utiliser la page Rechercher des utilisateurs pour rechercher les utilisateurs puis sélectionner un ou plusieurs utilisateurs sur lesquels exécuter l'action de mise à jour.

Lorsque vous mettez à jour le compte utilisateur, vous avez les options suivantes :

- Choisir si les comptes de ressources assignés recevront les informations mises à jour.
- Mettre à jour tous les comptes de ressources ou sélectionner des comptes individuels dans une liste.

Mise à jour des ressources sur un unique compte utilisateur

Pour mettre à jour un compte utilisateur, sélectionnez-le dans la liste puis sélectionnez l'option Mettre à jour dans la liste Actions de l'utilisateur.

Sur la page de mise à jour des comptes de ressources, sélectionnez une ou plusieurs ressources à mettre à jour ou sélectionnez Mettre tous les comptes de ressources à jour pour mettre à jour tous les comptes de ressources assignés. Lorsque vous avez terminé, cliquez sur OK pour commencer le processus de mise à jour. Vous pouvez aussi cliquer sur Enregistrer en arrière-plan pour effectuer l'action en tant que processus d'arrière-plan.

Une page de confirmation confirme les données envoyées à chaque ressource.

La Figure 3–3 illustre la page de mise à jour des comptes de ressources.

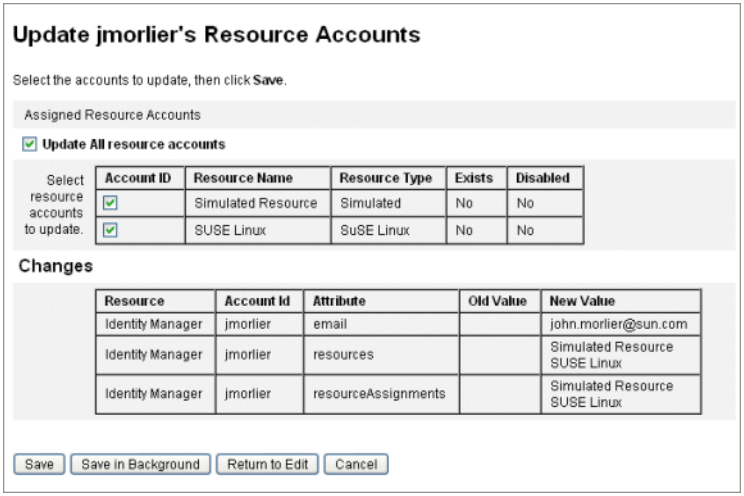


FIGURE 3–3 Mettre à jour les comptes de ressources

Mise à jour de ressources sur plusieurs comptes utilisateur

Vous pouvez mettre à jour deux comptes utilisateur Identity Manager ou plus en même temps. Sélectionnez plusieurs comptes utilisateur dans la liste puis sélectionnez Mettre à jour dans la liste Actions de l'utilisateur.

Remarque – Lorsque vous choisissez de mettre à jour plusieurs comptes utilisateur, vous ne pouvez pas sélectionner de comptes de ressources assignés individuellement dans chaque compte utilisateur. Ce processus met en effet à jour toutes les ressources de tous les comptes utilisateur que vous sélectionnez.

Suppression des comptes utilisateur Identity Manager

Dans Identity Manager, les comptes utilisateur Identity Manager se suppriment de la même façon que les comptes de ressources distants. Suivez les mêmes étapes que pour supprimer un compte de ressource en sélectionnant un compte Identity Manager pour la suppression au lieu d'un compte de ressource distant.

Remarque – Si un utilisateur a des éléments de travail en suspens ou des éléments de travail en suspens qui ont été délégués à un autre utilisateur, Identity Manager ne permettra pas de supprimer son compte Identity Manager. Pour pouvoir supprimer le compte Identity Manager de l'utilisateur, les éléments de travail délégués doivent soit être résolus soit être transmis à un autre utilisateur.

Pour plus d'informations, reportez-vous à "Suppression de ressources d'un unique compte utilisateur" à la page 70 et "Suppression de ressources de plusieurs comptes utilisateur" à la page 71.

Suppression des ressources des comptes utilisateur

Identity Manager fournit plusieurs opérations de suppression pouvant être utilisées pour supprimer l'accès à un compte utilisateur Identity Manager depuis une ressource :

- **Supprimer**. Pour chaque ressource sélectionnée, Identity Manager supprime le compte de l'utilisateur sur la ressource distante (pour supprimer un utilisateur Identity Manager, sélectionnez Identity Manager en tant que ressource).
  - Les comptes de ressources supprimés voient leur *lien automatiquement supprimé* de l'utilisateur Identity Manager.
  - L'assignation des comptes de ressources supprimés à l'utilisateur n'est pas *annulée*. La ressource reste assignée à l'utilisateur à moins que l'action d'annulation d'assignation ne soit également sélectionnée.
- **Annuler l'assignation**. Identity Manager supprime chacune des ressources sélectionnées de la liste des ressources assignées de l'utilisateur.
  - Les comptes de ressources dont l'assignation est annulée voient automatiquement leur *lien supprimé* de l'utilisateur Identity Manager.
  - Le compte utilisateur sur la ressource distante n'est *pas* supprimé. Le compte reste intact à moins que l'action de suppression ne soit également sélectionnée.
- **Annuler le lien**. Pour chaque ressource sélectionnée, les informations de compte de ressource de l'utilisateur sont supprimées d'Identity Manager.
  - Le compte de l'utilisateur sur la ressource distante reste intact à moins qu'une action de suppression ne soit également sélectionnée.
  - La ressource continue à figurer dans la liste des ressources assignées de l'utilisateur à moins qu'une action d'annulation d'assignation ne soit également sélectionnée.
  - Si vous supprimez le lien d'un compte assigné indirectement à l'utilisateur via un rôle ou un groupe de ressources, ce lien pourra être restauré lorsque l'utilisateur sera mis à jour.

Bien que suspendre figure parmi les actions de l'utilisateur dans les menus de la page Liste des utilisateurs, il n'y a actuellement que trois actions de suppression dans Identity Manager : supprimer, annuler l'assignation et annuler le lien.

Pour suspendre une ressource distante, utilisez les actions supprimer et annuler l'assignation sur la ressource.

Suppression de ressources d'un unique compte utilisateur

Suivez la procédure ci-après pour effectuer une opération de suppression sur un unique utilisateur Identity Manager. En travaillant avec un compte utilisateur à la fois, vous pouvez spécifier des opérations supprimer, annuler l'assignation et/ou annuler le lien différentes pour les comptes de ressources individuels.

▼ Pour démarrer une action Supprimer, Annuler l'assignation ou Supprimer le lien pour un unique compte utilisateur

1. **Dans l'interface administrateur, cliquez sur Comptes dans le menu principal.**

   La page Liste des utilisateurs s'affiche sur l'onglet Lister les comptes.

2. **Sélectionnez un utilisateur et cliquez sur le menu déroulant Actions de l'utilisateur.**

3. **Sélectionnez une des actions de suppression (Supprimer, Suspendre, Annuler l'assignation ou Supprimer le lien) dans la liste.**

   Identity Manager affiche la page Supprimer des comptes de ressources (Figure 3–4).

4. **Remplissez le formulaire. Pour plus d'informations sur les actions Supprimer, Annuler l'assignation et Supprimer le lien, reportez-vous à "Suppression des ressources des comptes utilisateur" à la page 69.**

5. **Cliquez sur OK.**

   La Figure 3–4 illustre la page Supprimer des comptes de ressources. Dans la capture d'écran, l'utilisateur jrenfro a un compte actif sur une ressource distante (la ressource simulée). L'action Supprimer est sélectionnée, ce qui signifie qu'à la soumission du formulaire, le compte de jrenfro sur la ressource sera supprimé. Les comptes supprimés voyant automatiquement leur lien supprimé, les informations de compte de cette ressource seront supprimées d'Identity Manager. La ressource simulée restera assignée à jrenfro car l'action Annuler l'assignation n'est pas sélectionnée.

   Pour supprimer le compte Identity Manager de jrenfro, l'action Supprimer doit être sélectionnée pour Identity Manager.

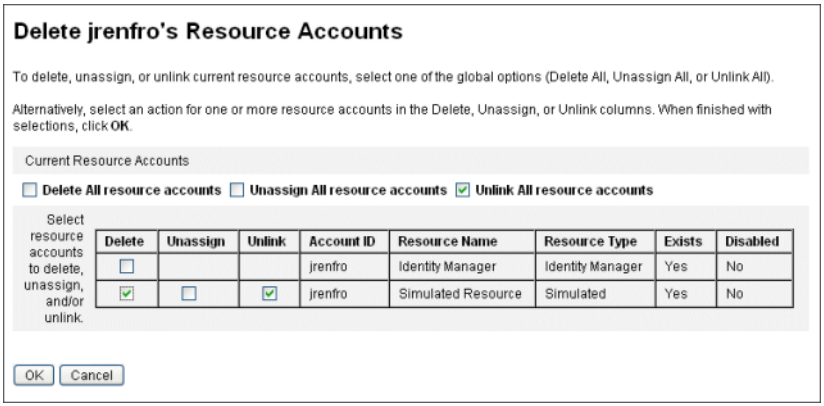


FIGURE 3–4 Page Supprimer des comptes de ressources.

Suppression de ressources de plusieurs comptes utilisateur

Vous pouvez effectuer une opération de suppression sur plusieurs comptes utilisateur Identity Manager à la fois, mais pouvez uniquement effectuer l'opération de suppression sélectionnée sur *tous* les comptes de ressources de l'utilisateur.

Les opérations de suppression peuvent également être effectuées en utilisant la fonctionnalité Actions de compte en masse d'Identity Manager. Voir les "Commandes Delete, DeleteAndUnlink, Disable, Enable, Unassign et Unlink" à la page 82.

▼ Pour démarrer une action Supprimer, Annuler l'assignation ou Annuler le lien pour plusieurs utilisateurs

1. **Dans l'interface administrateur, cliquez sur Comptes dans le menu principal.**

   La page Liste des utilisateurs s'affiche sur l'onglet Lister les comptes.

2. **Sélectionnez un ou plusieurs utilisateurs et cliquez dans le menu déroulant Actions de l'utilisateur.**

3. **Sélectionnez une des actions de suppression (Supprimer, Suspendre, Annuler l'assignation ou Supprimer le lien) dans la liste.**

   Identity Manager affiche la page Confirmez la suppression, l'annulation de l'assignation ou la suppression du lien (Figure 3–5).

4. **Spécifiez l'action à effectuer.**

Les options sont les suivantes :

- **Supprimer l'utilisateur uniquement**. Supprime les comptes Identity Manager du ou des utilisateurs sélectionnés. Cette option ne supprime pas les comptes de ressources des utilisateurs et n'en annule pas l'assignation.
- **Supprimer l'utilisateur et les comptes de ressources**. Supprime les comptes Identity Manager des utilisateurs et l'ensemble de leurs comptes de ressources.
- **Supprimer seulement les comptes de ressources**. Supprime tous les comptes de ressources des utilisateurs. Cette option n'annule pas l'assignation des comptes de ressources ni ne supprime les comptes Identity Manager des utilisateurs.
- **Supprimer les comptes de ressources et annuler l'assignation des ressources directement assignées à l'utilisateur**. Cette option supprime et annule l'assignation de tous les comptes de ressources des utilisateurs mais ne supprime pas les comptes Identity Manager des utilisateurs.
- **Annuler l'assignation des comptes de ressources directement assignés à l'utilisateur**. Annule les assignations des comptes de ressources assignés directement. Cette option ne supprime pas les comptes des utilisateurs sur les ressources distantes. Les comptes de ressources assignés via un rôle ou un groupe de ressources ne sont pas concernés.
- **Annuler les liens entre les comptes de ressources et l'utilisateur**. Les informations de compte de ressource des utilisateurs sont supprimées d'Identity Manager. Les comptes des utilisateurs situés sur les ressources distantes ne sont pas supprimés et leur assignation n'est pas annulée. Les comptes indirectement assignés aux utilisateurs par le biais d'un rôle ou d'un groupe de ressources peuvent être restaurés lors de la mise à jour des utilisateurs.

5 Cliquez sur OK.

La Figure 3–5 illustre la page Confirmez la suppression, l'annulation de l'assignation ou la suppression du lien. La partie supérieure de cette page affiche les six actions disponibles pouvant être effectuées pour plusieurs utilisateurs. La partie inférieure de la page indique les utilisateurs qui seront concernés par l'action sélectionnée.

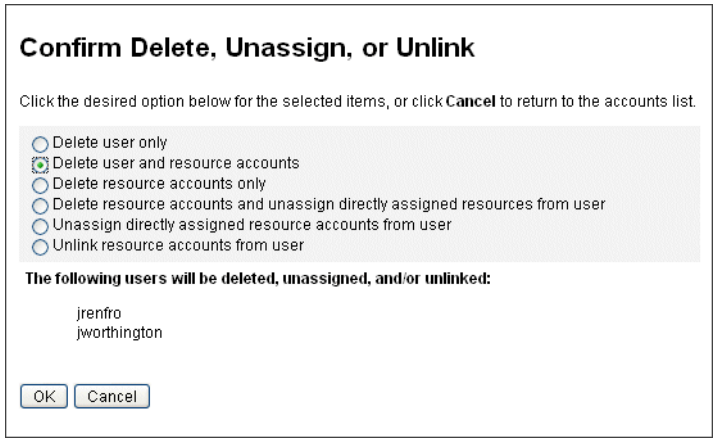


FIGURE 3–5 Page Confirmez la suppression, l'annulation de l'assignation ou la suppression du lien

Changement des mots de passe utilisateur

Tous les utilisateurs Identity Manager se voient assigner un mot de passe. Lorsqu'il est défini, le mot de passe utilisateur Identity Manager est utilisé pour synchroniser les mots de passe des comptes de ressources de l'utilisateur. Si un ou plusieurs mots de passe de comptes de ressources ne peuvent pas être synchronisés (par exemple, afin que les stratégies de mots de passe soient respectées), vous pouvez les définir individuellement.

Remarque – Pour toute information sur les stratégies de mot de passe de compte et pour des informations d'ordre général sur l'authentification des utilisateurs, lisez la section "Gestion de la sécurité des comptes et des privilèges" à la page 88 dans ce même chapitre.

▼ Changement des mots de passe depuis la page Liste des utilisateurs

Vous pouvez utiliser l'action utilisateur Modifier le mot de passe de la page Liste des utilisateurs (Comptes → Lister les comptes) pour modifier le mot de passe d'un utilisateur depuis la page Liste des utilisateurs. Procédez comme suit :

1. **Dans l'interface administrateur, cliquez sur Comptes dans le menu principal.**
   La page Liste des utilisateurs s'affiche sur l'onglet Lister les comptes.
2. **Sélectionnez un utilisateur et cliquez sur le menu déroulant Actions de l'utilisateur.**
3. **Pour changer le mot de passe, sélectionnez Modifier le mot de passe.**
   La page Changement du mot de passe s'ouvre.
4. **Saisissez le nouveau mot de passe et cliquez sur le bouton Modifier le mot de passe.**

▼ Pour modifier les mots de passe depuis le menu principal

Pour modifier le mot de passe d'un compte utilisateur depuis le menu principal, suivez les étapes ci-dessous :

1 **Dans l'interface administrateur, cliquez sur Mots de passe dans le menu principal.**

La page Changement du mot de passe s'ouvre par défaut.

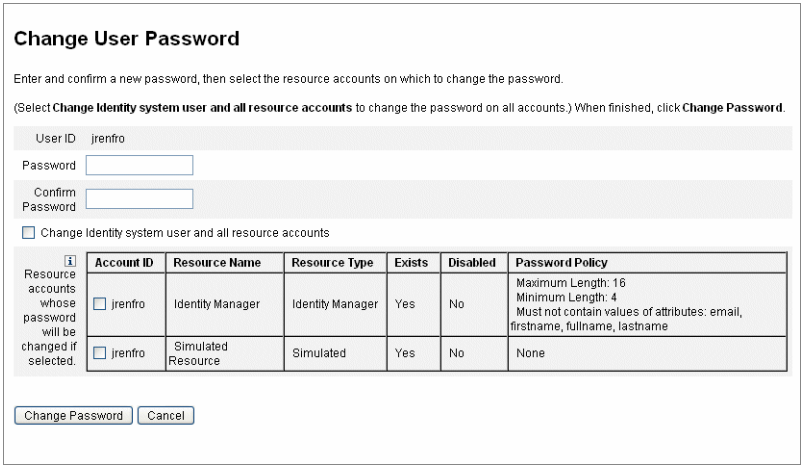


FIGURE 3–6 Changer le mot de passe de l'utilisateur

2 **Sélectionnez un terme à rechercher (par exemple un nom de compte, une adresse e-mail, un nom ou un prénom) puis un type de recherche (commence par, comprend ou est).**

3 **Saisissez la ou les premières lettres du terme à rechercher dans le champ d'entrée puis cliquez sur Trouver. Identity Manager retourne la liste des utilisateurs dont les ID contiennent les caractères saisis. Cliquez pour sélectionner un utilisateur et revenir à la page Changer le mot de passe de l'utilisateur.**

4 **Saisissez et confirmez les nouvelles informations de mot de passe puis cliquez sur Modifier le mot de passe pour changer le mot de passe utilisateur sur les comptes de ressources listés. Identity Manager affiche un schéma de flux de travaux indiquant la séquence d'actions entreprise pour modifier le mot de passe.**

Réinitialisation des mots de passe utilisateur

Le processus de réinitialisation des mots de passe de compte utilisateur Identity Manager est similaire au processus de changement des mots de passe. La différence par rapport à un

changement de mot de passe est que vous ne devez pas spécifier de nouveau mot de passe. Dans ce cas en effet, Identity Manager génère un nouveau mot de passe de manière aléatoire (selon vos sélections et les stratégies de mot de passe) pour le compte utilisateur, les comptes de ressource ou une combinaison de ces éléments.

La stratégie assignée à l'utilisateur (par assignation directe ou au travers de l'organisation de l'utilisateur) contrôle plusieurs options de réinitialisation, notamment :

- le nombre de fois où un mot de passe peut être réinitialisé avant que les réinitialisations ne soient désactivées ;
- l'endroit où le nouveau mot de passe s'affiche ou auquel il est envoyé.

  Selon l'Option de notification de la réinitialisation sélectionnée pour le rôle, Identity Manager envoie le nouveau mot de passe par e-mail à l'utilisateur ou l'affiche (sur la page Résultats) pour l'administrateur Identity Manager demandant la réinitialisation.

▼ Réinitialisation des mots de passe depuis la page Liste des utilisateurs

L'action utilisateur Réinitialisation du mot de passe est disponible sur la page Liste des utilisateurs (Comptes > Lister les comptes).

Pour réinitialiser un mot de passe depuis la page Liste des utilisateurs, suivez les étapes ci-après :

1. **Dans l'interface administrateur, cliquez sur Comptes dans le menu principal. La page Liste des utilisateurs s'affiche sur l'onglet Lister les comptes.**
2. **Sélectionnez un utilisateur et cliquez sur le menu déroulant Actions de l'utilisateur.**
3. **Pour réinitialiser le mot de passe, sélectionnez Réinitialiser le mot de passe.**

   La page Réinitialiser le mot de passe de l'utilisateur s'ouvre.
4. **Cliquez sur le bouton Réinitialiser le mot de passe.**

▼ Pour faire expirer les mots de passe en utilisant la stratégie de compte Identity Manager

Lorsque vous réinitialisez un mot de passe utilisateur, ce dernier expire immédiatement par défaut. Par conséquent, la première fois que les utilisateurs se connectent après une réinitialisation de mot de passe, ils doivent sélectionner un nouveau mot de passe pour pouvoir accéder au système. Vous pouvez éditer le formulaire Réinitialiser le mot de passe de l'utilisateur de sorte que le mot de passe de l'utilisateur expire selon la stratégie d'expiration des mots de passe définie dans la Stratégie de compte Identity Manager associée à cet utilisateur.

Utilisez le processus suivant pour ignorer la nécessité de changer par défaut le mot de passe :

1 **Éditez le formulaire Réinitialiser le mot de passe de l'utilisateur et définissez la valeur suivante sur `false`.**

```
resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword
```

2 **Utilisez l'option Réinitialiser de la stratégie de compte Identity Manager pour spécifier quand un mot de passe expire.**

Les paramètres sont les suivants :

- **permanent**. Identity Manager utilise la période de temps spécifiée dans l'attribut de stratégie `passwordExpiry` pour calculer la date relative, par rapport à la date courante, à laquelle le mot de passe sera réinitialisé puis définir cette date sur l'utilisateur. Si aucune valeur n'est spécifiée, le mot de passe changé ou réinitialisé n'expire jamais.
- **temporaire**. Identity Manager utilise la période de temps spécifiée dans l'attribut de stratégie `tempPasswordExpiry` pour calculer la date relative, par rapport à la date courante, à laquelle le mot de passe sera réinitialisé puis définir cette date sur l'utilisateur. Si aucune valeur n'est spécifiée, le mot de passe changé ou réinitialisé n'expire jamais. Si `tempPasswordExpiry` est défini sur la valeur 0, le mot de passe expire immédiatement.

  L'attribut `tempPasswordExpiry` s'applique uniquement en cas de réinitialisation (modification aléatoire) des mots de passe. Il ne s'applique pas aux changements de passe.

Désactivation, activation et déverrouillage des comptes utilisateur

Cette section explique la désactivation et l'activation des comptes utilisateur Identity Manager. Elle indique également comment venir en aide aux utilisateurs dont les comptes Identity Manager ont été verrouillés.

▼ Pour désactiver des comptes utilisateur

Lorsque vous désactivez un compte utilisateur, vous modifiez ce compte de sorte que l'utilisateur ne puisse plus se connecter à Identity Manager ni à ses comptes de ressources assignés.

Il faut savoir que les administrateurs peuvent désactiver les comptes utilisateur depuis l'interface administrateur, mais ne peuvent pas verrouiller les comptes utilisateur. Les comptes ne sont verrouillés que dans le cas où l'utilisateur dépasse le nombre de tentatives de connexion ayant échoué autorisé défini par la stratégie de compte Identity Manager.

Remarque – Si une ressource assignée n'a pas de prise en charge native pour la désactivation des comptes mais prend en charge les changements de mot de passe, Identity Manager peut être configuré pour désactiver les comptes utilisateur sur cette ressource en assignant de nouveaux mots de passe générés de manière aléatoire.

Utilisez les étapes suivantes pour vous assurer que cette fonctionnalité fonctionne correctement :

1 **Ouvrez la page Paramètres du système d'identité dans l'assistant Éditer une ressource (voir "Gestion des ressources" à la page 168 pour les instructions sur l'ouverture de l'assistant).**

2 **Dans le tableau Configuration des caractéristiques du compte, vérifiez qu'aucune des fonctionnalités Mot de passe et Désactiver ne présente de coche dans la colonne Désactiver ? (pour afficher la fonctionnalité Désactiver, sélectionnez Afficher toutes les caractéristiques).**

Si la fonctionnalité Désactiver n'a pas de coche dans la colonne Désactiver ?, il est impossible de désactiver les comptes dans la ressource.

Informations supplémentaires

Désactivation d'un unique compte utilisateur

Pour désactiver un compte utilisateur, sélectionnez-le dans la Liste des utilisateurs puis sélectionnez l'option Désactiver dans la liste Actions de l'utilisateur.

Sélectionnez les comptes de ressources à désactiver sur la page Désactiver qui s'affiche puis cliquez sur OK. Identity Manager affiche les résultats de la désactivation du compte utilisateur Identity Manager et de tous les comptes de ressources associés. La liste des comptes indique que l'utilisateur est désactivé.

Désactivation de plusieurs comptes utilisateur

Vous pouvez désactiver deux comptes utilisateur Identity Manager ou plus en même temps. Sélectionnez plusieurs comptes utilisateur dans la liste puis sélectionnez Désactiver dans la liste Actions de l'utilisateur.

Remarque – Lorsque vous choisissez de désactiver plusieurs comptes utilisateur, vous ne pouvez pas sélectionner de comptes de ressources assignés individuellement dans ces différents comptes utilisateur. Ce processus désactive en effet toutes les ressources de tous les comptes utilisateur que vous sélectionnez.

▼ Pour activer les comptes utilisateur sur une ressource entre deux réinitialisations de mot de passe

L'activation des comptes utilisateur est l'inverse du processus de désactivation.

Selon les options de notification sélectionnées, Identity Manager affiche également le mot de passe sur la page de résultats de l'administrateur.

L'utilisateur peut alors réinitialiser son mot de passe (via le processus d'authentification) qui peut aussi être réinitialisé par un utilisateur disposant de privilèges d'administrateur.

Remarque – Si une ressource assignée est dépourvue de prise en charge native pour l'activation des comptes, mais prend en charge les changements de mot de passe, Identity Manager peut être configuré pour activer les comptes utilisateur sur cette ressource entre deux réinitialisations de mot de passe.

Pour que cette fonctionnalité fonctionne correctement, procédez comme suit :

---

1 **Ouvrez la page Paramètres du système d'identité dans l'assistant Éditer une ressource (voir "Gestion des ressources" à la page 168 pour les instructions d'ouverture de l'assistant).**

2 **Dans le tableau Configuration des caractéristiques du compte, vérifiez qu'aucune des fonctionnalités Mot de passe et Activer ne présente de coche dans la colonne Désactiver ? (pour afficher la fonctionnalité Activer, sélectionnez Afficher toutes les caractéristiques).**

Si la fonctionnalité Activer n'a pas de coche dans la colonne Désactiver ?, il est impossible d'activer les comptes dans la ressource.

Informations supplémentaires

Activation d'un unique compte utilisateur

Pour activer un compte utilisateur, sélectionnez-le dans la liste puis sélectionnez l'option Activer dans la liste Actions de l'utilisateur.

Sélectionnez les ressources à activer sur la page Activer qui s'affiche puis cliquez sur OK. Identity Manager affiche les résultats de l'activation du compte utilisateur Identity Manager et de tous les comptes de ressources associés.

Activation de plusieurs comptes utilisateur

Vous pouvez activer deux comptes utilisateur Identity Manager ou plus en même temps. Sélectionnez plusieurs comptes utilisateur dans la liste puis sélectionnez Activer dans la liste Actions de l'utilisateur.

Remarque – Lorsque vous choisissez d'activer plusieurs comptes utilisateur, vous ne pouvez pas sélectionner de comptes de ressources assignés individuellement dans ces différents comptes utilisateur. Ce processus active en effet toutes les ressources de tous les comptes utilisateur que vous sélectionnez.

Déverrouillage des comptes utilisateur

Les comptes des utilisateurs sont verrouillés lorsque les tentatives de connexion à Identity Manager des utilisateurs échouent. Pour que son compte soit verrouillé, l'utilisateur doit dépasser le nombre de tentatives de connexion ayant échoué autorisé défini par la stratégie de compte d'Identity Manager.

Remarque – Seules les tentatives de connexion effectuées sur une interface utilisateur d'Identity Manager sont prises en compte pour le verrouillage d'un compte Identity Manager (c'est-à-dire, l'interface administrateur, l'interface administrateur final, l'interface de ligne de commande ou l'interface API SPML). Les tentatives de connexion à des comptes de ressources ayant échoué ne sont pas comptabilisées et n'entraînent pas le verrouillage des comptes Identity Manager des utilisateurs.

La stratégie de compte Identity Manager établit le nombre maximal de tentatives de connexion par mot de passe ou questions ratées autorisées.

- Pour les utilisateurs qui dépassent ce nombre maximal d'échecs de connexion par mot de passe, toutes les interfaces de l'application Identity Manager sont alors verrouillées, interface Mot de passe oublié incluse.
- Les utilisateurs qui dépassent le nombre maximal d'échecs de connexion par questions peuvent quant à eux s'authentifier sur toute interface de l'application Identity Manager à l'exception de Mot de passe oublié.

Tentatives de connexion par mot de passe ayant échoué

Les utilisateurs pour lesquels Identity Manager est verrouillé à cause d'un trop grand nombre d'échecs de connexion par mot de passe ne pourront se connecter que lorsqu'un administrateur déverrouillera le compte en question ou à l'expiration du verrou.

- Un administrateur peut déverrouiller un compte à condition d'avoir le contrôle administratif de l'organisation dont l'utilisateur est membre ainsi que la capacité `Déverrouiller un utilisateur`.
- Si une valeur de `Délai d'attente de verrouillage` est définie dans la stratégie de compte Identity Manager, un verrou placé sur un compte pourra expirer. La valeur `Délai d'attente de verrouillage` pour les tentatives de connexion par mot de passe ayant échoué est définie par la valeur Désactivation du verrou du compte créé par trop de tentatives de connexion par mot de passe ayant échoué dans.

Tentatives de connexion par questions ayant échoué

Les utilisateurs pour lesquels l'interface Mot de passe oublié est verrouillée à cause d'un trop grand nombre d'échecs de connexion par questions pourront uniquement se connecter

lorsqu'un administrateur déverrouillera le compte en question, lorsque l'utilisateur verrouillé (ou un utilisateur ayant les capacités appropriées) changera ou réinitialisera le mot de passe de l'utilisateur ou à l'expiration du verrou.

- Un administrateur peut déverrouiller un compte à condition d'avoir le contrôle administratif de l'organisation dont l'utilisateur est membre ainsi que la capacité `Déverrouiller un utilisateur`.
- Si une valeur de `Délai d'attente de verrouillage` est définie dans la stratégie de compte Identity Manager, un verrou placé sur un compte pourra expirer. La valeur `Délai d'attente de verrouillage` pour les tentatives de connexion par questions ayant échoué est définie par la valeur Désactivation du verrou du compte créé par trop de tentatives de connexion par questions ayant échoué dans.

Un administrateur doté des capacités appropriées peut effectuer les opérations suivantes sur un utilisateur à l'état verrouillé :

- une mise à jour (reprovisioning de ressources compris),
- un changement ou une réinitialisation de mot de passe,
- une désactivation ou une activation,
- une opération de renommage,
- une opération de déverrouillage.

Pour déverrouiller des comptes, sélectionnez un ou plusieurs comptes utilisateur dans la liste puis sélectionnez Déverrouiller les utilisateurs dans la liste Actions de l'utilisateur ou Actions d'organisation.

Actions de compte en masse

Vous pouvez effectuer plusieurs actions *en masse* sur les comptes Identity Manager, ce qui permet d'agir sur plusieurs comptes en même temps.

Vous pouvez lancer les actions en masse de la manière suivante :

- **Supprimer**. Supprime les comptes de ressource sélectionnés, en annule l'assignation et en supprime les liens. Sélectionnez l'option Appliquer au compte Identity Manager pour supprimer également le compte Identity Manager de chaque utilisateur.
- **Supprimer et Supprimer le lien**. Supprime les comptes de ressources sélectionnés et les liens établis entre les comptes et les utilisateurs.
- **Désactiver**. Désactive les comptes de ressource sélectionnés. Sélectionnez l'option Appliquer au compte Identity Manager pour désactiver également le compte Identity Manager de chaque utilisateur.
- **Activer**. Active les comptes de ressource sélectionnés. Sélectionnez l'option Appliquer au compte Identity Manager pour activer également le compte Identity Manager de chaque utilisateur.

- **Annuler l'assignation, Annuler le lien**. Supprime les liens de tous les comptes de ressource sélectionnés et annule les assignations de tous les comptes utilisateur Identity Manager. L'annulation de l'assignation n'entraîne pas la suppression du compte de la ressource. Vous ne pouvez pas annuler l'assignation d'un compte ayant été indirectement assigné à l'utilisateur Identity Manager via un rôle ou un groupe de ressources.
- **Annuler le lien**. Supprime l'association (lien) d'un compte de ressource avec le compte utilisateur Identity Manager. La suppression du lien n'entraîne pas celle du compte de la ressource. Si vous supprimez le lien d'un compte assigné indirectement à l'utilisateur Identity Manager via un rôle ou un groupe de ressources, ce lien pourra être restauré lorsque l'utilisateur sera mis à jour.

Les actions en masse fonctionneront de façon optimale si vous disposez d'une liste d'utilisateurs dans un fichier ou une application, par exemple un client de messagerie ou un tableur. Vous pouvez copier la liste et la coller dans un champ de cette page d'interface ou charger la liste des utilisateurs à partir d'un fichier.

Vous pouvez exécuter la plupart de ces actions sur les résultats d'une recherche d'utilisateurs. Utilisez la page Rechercher des utilisateurs (Compte → Rechercher des utilisateurs) pour rechercher des utilisateurs.

Vous pouvez enregistrer les résultats d'une opération de compte en masse dans un fichier CSV en cliquant sur Télécharger CSV lorsque les résultats de la tâche s'affichent à la fin de la tâche.

Lancement d'actions de compte en masse

▼ Pour lancer des actions de compte en masse

1. **Dans l'interface administrateur, cliquez sur Comptes dans le menu principal.**
2. **Cliquez sur Lancer des actions en masse dans le menu secondaire.**
3. **Remplissez le formulaire et cliquez sur Lancer.**

   Identity Manager lance une tâche d'arrière-plan pour exécuter les actions en masse.

   Pour contrôler le statut de la tâche d'actions en masse, cliquez sur Tâches du serveur dans le menu principal puis cliquez sur Toutes tâches.

Utilisation des listes d'actions

Vous pouvez spécifier une liste d'actions en masse en utilisant le format CSV (valeurs séparées par des virgules). Ceci permet de combiner différents types d'action dans une liste d'actions. De plus, vous pouvez spécifier des actions de création et de mise à jour plus complexes.

Le format CSV se compose de deux lignes d'entrée minimum. Chaque ligne comprend une liste de valeurs séparées par des virgules. La première ligne contient des noms de champ. Les autres lignes correspondent chacune à une action à exécuter sur un utilisateur Identity Manager, sur les comptes de ressource de l'utilisateur ou sur ces deux éléments. Chaque ligne doit contenir le même nombre de valeurs. Les valeurs vides ne modifient pas la valeur des champs correspondants.

Deux champs sont obligatoires pour toute entrée CSV d'action en masse:

- **user (utilisateur)**. Contient le nom de l'utilisateur Identity Manager.
- **command (commande)**. Contient le nom de l'action entreprise sur l'utilisateur Identity Manager. Les commandes valides sont les suivantes :
  - **Delete (Supprimer)**. Supprime, annule les assignations et supprime les liens des comptes de ressources, du compte Identity Manager ou de ces deux éléments.
  - **DeleteAndUnlink (Supprimer et supprimer le lien)**. Supprime les comptes de ressources et en supprime les liens.
  - **Disable (Désactiver)**. Désactive les comptes de ressources, le compte Identity Manager ou tous ces éléments.
  - **Enable (Activer)**. Active les comptes de ressources, le compte Identity Manager ou tous ces éléments.
  - **Unassign (Annuler l'assignation)**. Annule les assignations et supprime les liens des comptes de ressources.
  - **Unlink (Annuler le lien)**. Supprime les liens des comptes de ressources.
  - **Create (Créer)**. Crée le compte Identity Manager. Crée en option des comptes de ressources.
  - **Update (Mettre à jour)**. Met à jour le compte Identity Manager. En option, crée, met à jour ou supprime les comptes de ressources.
  - **CreateOrUpdate (Créer ou mettre à jour)**. Exécute une action de création si le compte Identity Manager n'existe pas. Sinon, cette commande exécute une opération de mise à jour.

Commandes Delete, DeleteAndUnlink, Disable, Enable, Unassign et Unlink

Si vous exécutez une action de type Delete, DeleteAndUnlink, Disable, Enable, Unassign ou Unlink, le seul champ supplémentaire à spécifier est le champ resources (ressources). Ce dernier permet de spécifier les comptes qui seront concernés sur les différentes ressources.

Le champ resources peut présenter les valeurs suivantes :

- **all**. Traite tous les comptes de ressource, y compris le compte Identity Manager.
- **resonly**. Traite tous les comptes de ressource, sauf le compte Identity Manager.

- *nom_ressource* [| *nom_ressource* ...]. Traite les comptes de ressource spécifiés. Spécifie à Identity Manager de traiter le compte Identity Manager.

Voici un exemple de format CSV pour plusieurs de ces actions :

```
command,user,resources
Delete,John Doe,all
Disable,Jane Doe,resonly
Enable,Henry Smith,Identity Manager
Unlink,Jill Smith,Windows Active Directory|Solaris Server
```

Commandes Create, Update et CreateOrUpdate

Si vous exécutez des commandes Create, Update ou CreateOrUpdate, en plus des champs user et command, vous pouvez spécifier des champs à partir de la vue utilisateur. Les noms de champ utilisés sont les expressions de chemin des attributs figurant dans les vues. Pour toute information sur les attributs disponibles dans la vue utilisateur, reportez-vous à "User View Attributes" du *Sun Identity Manager Deployment Reference*. Si vous utilisez un formulaire d'utilisateur personnalisé, les noms de champ du formulaire contiennent certaines des expressions de chemin que vous pouvez utiliser.

Voici certaines des expressions de chemin les plus courantes dans les actions en masse :

- **waveset.roles**. Liste d'un ou plusieurs noms de rôle à assigner au compte Identity Manager.
- **waveset.resources**. Liste d'un ou plusieurs noms de ressource à assigner au compte Identity Manager.
- **waveset.applications**. Liste d'un ou plusieurs noms de rôle à assigner au compte Identity Manager.
- **waveset.organization**. Nom de l'organisation dans laquelle placer le compte Identity Manager.
- **accounts**[*nom_ressource*].*nom_attribut*. Attribut d'un compte de ressource. Les noms des attributs sont listés dans le schéma de la ressource.

Voici un exemple de format CSV pour des actions de création et de mise à jour :

```
command,user,waveset.resources,password.password,
password.confirmPassword,accounts[Windows Active Directory].description,
accounts[Corporate Directory].location Create,John Doe,
Windows Active Directory|Solaris Server,changeit,changeit,John Doe - 888-555-5555,
Create,Jane Smith,Corporate Directory,changeit,changeit,,New York
CreateOrUpdate,Bill Jones,,,,,California
```

La commande `CreateOrUpdate` permet de spécifier un type de compte spécifique sur une ressource prenant en charge plusieurs types de comptes. Ainsi, si un utilisateur possède plusieurs comptes sur une ressource donnée, chacun d'un type différent, l'exemple suivant illustre comment mettre à jour le type de compte `admin` pour l'utilisateur `userAye` :

```
command,user,accounts[Sim1|admin].emailAddress
CreateOrUpdate,userAye,bbye8@example.com
```

Remarque –

Bien que la commande `CreateOrUpdate` permette de définir des attributs propres aux différents comptes d'un utilisateur, n'oubliez pas que les valeurs suivantes de la section globale de la vue Utilisateur sont appliquées à *tous* les comptes spécifiés :

- `accountId`,
- `email`,
- `password`,
- `disable`,
- tous les attributs étendus.

Par conséquent, une commande `BulkOps` de la forme suivante *pourrait* ne pas fonctionner comme prévu.

```
command,user,accounts[Sim1].email
CreateOrUpdate,userAye,bbye8@example.com
```

Si `userAye` dispose déjà d'une valeur pour `email`, celle-ci sera appliquée à l'attribut email de la ressource `Sim1`. Il n'existe aucun moyen de modifier ce comportement.

Champs comportant plusieurs valeurs

Certains champs peuvent contenir plusieurs valeurs. Ils sont appelés champs à valeurs multiples. Par exemple, le champ `waveset.resources` peut être utilisé pour assigner·plusieurs ressources à un utilisateur. Vous pouvez utiliser une barre verticale (|) pour séparer des valeurs multiples dans un champ. Pour spécifier des valeurs multiples, respectez la syntaxe suivante :

```
value0 | value1 [ | value2 ... ]
```

Lorsque vous mettez à jour des champs à valeurs multiples pour des utilisateurs existants, le remplacement des valeurs actuelles des champs par une ou plusieurs nouvelles valeurs peut ne pas donner le résultat escompté. Vous pouvez vouloir supprimer certaines valeurs ou ajouter d'autres valeurs courantes. Vous pouvez utiliser des directives de champ pour spécifier comment traiter les valeurs existantes des champs. Ces directives se placent devant la valeur du champ et sont encadrées par une barre verticale comme suit :

```
|directive [ ; directive ] | field values
```

Vous pouvez choisir parmi les directives suivantes :

- **Remplacer**. Remplace les valeurs actuelles par les valeurs spécifiées. C'est la valeur par défaut si aucune directive (ou seule la directive Lister) est spécifiée.
- **Fusionner**. Ajoute les valeurs spécifiées aux valeurs actuelles. Les valeurs en double sont filtrées.
- **Supprimer**. Supprime les valeurs spécifiées des valeurs actuelles.
- **Lister**. Force le champ à traiter la valeur comme si elle était multiple, même s'il ne s'agit que d'une seule valeur. Cette directive n'est habituellement pas nécessaire, car la plupart des champs sont traités de façon appropriée quel que soit le nombre de valeurs. C'est la seule directive qui peut être spécifiée avec une autre directive.

Remarque – Les valeurs de champ sont sensibles à la casse. Ceci est important lorsque vous spécifiez les directives Fusionner et Supprimer. Les valeurs doivent être exactement identiques pour permettre une suppression correcte ou éviter d'avoir plusieurs valeurs similaires lors de la fusion.

Caractères spéciaux dans les valeurs de champ

Si une valeur de champ comporte une virgule (`,`) ou un guillemet (`"`) ou si vous voulez préserver les espaces de tête ou de queue, vous devez insérer votre valeur de champ dans une paire de guillemets doubles (`"valeur_champ"`). Vous devez ensuite remplacer les guillemets doubles contenus dans la valeur de champ par deux guillemets doubles (`""`). Par exemple, `"John ""Johnny"" Smith"` donne la valeur de champ `John "Johnny" Smith`.

Si une valeur de champ contient une barre verticale (`|`) ou une barre oblique (`\`), vous devez la faire précéder d'une barre oblique (`\|` ou `\\`).

Attributs de la vue d'une action en masse

Lors de l'exécution des actions Create, Update ou CreateOrUpdate, la vue utilisateur comporte des attributs supplémentaires exclusivement utilisés ou disponibles pendant le traitement de l'action en masse. Ces attributs peuvent être référencés dans le formulaire utilisateur pour permettre un comportement spécifique aux actions en masse.

Ces attributs sont les suivants :

- Les attributs `waveset.bulk.fields.nom_champ` contiennent les valeurs des champs lus à partir de l'entrée CSV, où *nom_champ* désigne le champ. Par exemple, les champs command et user figurent dans les attributs avec, respectivement, les expressions de chemin `waveset.bulk.fields.command` et `waveset.bulk.fields.user`.
- Les attributs `waveset.bulk.fieldDirectives.nom_champ` sont uniquement définis pour les champs pour lesquels une directive a été spécifiée. La valeur est la chaîne de la directive.

- Définissez l'attribut booléen `waveset.bulk.abort` sur true pour abandonner l'action courante.
- Définissez `waveset.bulk.abortMessage` sur une chaîne de message qui s'affichera lorsque `waveset.bulk.abort` aura pour valeur true. Si cet attribut n'est pas défini, un message d'abandon générique s'affichera.

Règles de corrélation et de confirmation

Utilisez des règles de corrélation et de confirmation lorsque vous ne disposez pas d'un nom d'utilisateur Identity Manager à entrer dans le champ user (utilisateur) de vos actions. Si vous ne spécifiez pas de valeur pour le champ user, vous devez indiquer une règle de corrélation lors du lancement de l'action en masse. Si vous ne spécifiez pas de valeur pour le champ user, les règles de corrélation et de confirmation ne seront pas évaluées pour cette action.

Une règle de corrélation recherche les utilisateurs Identity Manager correspondant aux champs de l'action. Une règle de confirmation teste un utilisateur Identity Manager en le confrontant aux champs de l'action pour vérifier s'il correspond. Cette méthode en deux étapes permet à Identity Manager d'optimiser la corrélation en trouvant rapidement des utilisateurs possibles (d'après le nom ou des attributs) et en limitant l'exécution des contrôles coûteux à ces derniers.

Créez une règle de corrélation ou de confirmation en créant un objet Règle avec, respectivement, le sous-type `SUBTYPE_ACCOUNT_CORRELATION_RULE` ou `SUBTYPE_ACCOUNT_CONFIRMATION_RULE`.

Pour plus d'informations sur les règles de corrélation et de confirmation, voir le Chapitre 3, “Data Loading and Synchronization” du *Sun Identity Manager Deployment Guide*.

Règles de corrélation

L'entrée pour toute règle de corrélation est une mappe des champs d'action. La sortie doit être l'une des suivantes :

- une chaîne (contenant un nom ou un ID utilisateur) ;
- une liste d'éléments String (chacun étant un nom ou un ID utilisateur) ;
- une liste d'éléments `WSAttribute` ;
- une liste d'éléments `AttributeCondition`.

Une règle de corrélation type génère une liste de noms d'utilisateur d'après les valeurs des champs de l'action. Une règle de corrélation peut également générer une liste de conditions d'attributs (se référant à des attributs interrogeables de `Type.USER`) qui seront utilisées pour sélectionner des utilisateurs.

Une règle de corrélation doit être relativement peu coûteuse et la plus sélective possible. Si possible, reportez le traitement coûteux sur une règle de confirmation.

Les conditions d'attribut doivent faire référence à des attributs interrogeables de `Type.USER`. Ces derniers sont configurés dans l'objet Configuration Identity Manager nommé `Configuration du schéma IDM`.

La corrélation sur un attribut étendu requiert une configuration spéciale.

L'attribut étendu doit être spécifié comme interrogeable.

▼ Pour définir un attribut étendu comme interrogeable

1. **Ouvrez `Configuration du schéma IDM`. Vous devez avoir la capacité Configuration du schéma IDM pour afficher ou éditer `Configuration du schéma IDM`.**
2. **Localisez l'élément `<IDMObjectClassConfiguration name='User'>`.**
3. **Localisez l'élément `<IDMObjectClassAttributeConfiguration name=' xyz '>`, où `xyz` est le nom de l'attribut que vous voulez définir comme interrogeable.**
4. **Définissez `queryable='true'`**

   Dans les "Règles de corrélation" à la page 86, l'attribut étendu `email` est défini comme interrogeable.

Exemple 3–1 Extrait XML définissant l'attribut étendu email comme interrogeable

```
<IDMSchemaConfiguration>
  <IDMAttributeConfigurations>
    <IDMAttributeConfiguration name='email' syntax='STRING'/>
    </IDMAttributeConfiguration>
  </IDMAttributeConfigurations>
  <IDMObjectClassConfigurations>
    <IDMObjectClassConfiguration name='User' extends='Principal' description='User description'>
      <IDMObjectClassAttributeConfiguration name='email' queryable='true'/>
    </IDMObjectClassConfiguration>
  </IDMObjectClassConfigurations>
 </IDMSchemaConfiguration>
```

Vous devez redémarrer l'application Identity Manager (ou le serveur d'application) pour que le changement de `Configuration du schéma IDM` soit appliqué.

Règles de confirmation

Les entrées dans toute règle de confirmation prennent la forme suivante :

- Utilisez `userview` pour une vue complète d'un utilisateur Identity Manager.
- Utilisez `account` pour une mappe des champs d'action.

Une règle de confirmation retourne une valeur booléenne sous forme de chaîne true si l'utilisateur correspond aux champs d'action, sinon elle retourne la valeur false.

Une règle de confirmation typique confronte les valeurs internes de la vue utilisateur aux valeurs des champs d'action. À titre de deuxième étape facultative du traitement de corrélation, la règle de confirmation effectue des contrôles qui ne peuvent pas être exprimés dans une règle de corrélation (ou qui sont trop coûteux à évaluer dans une règle de corrélation).

En règle générale, vous n'aurez besoin d'une règle de confirmation que quand :

- la règle de corrélation peut retourner plusieurs utilisateurs correspondants ;
- les valeurs utilisateur qui doivent être comparées ne sont pas interrogeables.

Une règle de confirmation est exécutée une fois pour chaque utilisateur correspondant renvoyé par la règle de corrélation.

Gestion de la sécurité des comptes et des privilèges

Cette section examine les actions à votre disposition pour fournir un accès sécurisé aux comptes utilisateur et gérer les privilèges des utilisateurs dans Identity Manager :

- "Définition de stratégies de mot de passe" à la page 88 ;
- "Authentification des utilisateurs" à la page 92 ;
- "Assignation de privilèges administratifs" à la page 96.

Définition de stratégies de mot de passe

Les stratégies de mot de passe de ressource établissent les limites applicables aux mots de passe. Les stratégies de mot de passe fortes assurent une sécurité supplémentaire pour protéger les ressources contre les tentatives de connexion non autorisées. Vous pouvez éditer une stratégie de mot de passe pour définir ou sélectionner des valeurs pour tout un éventail de caractéristiques.

Pour commencer à travailler avec les stratégies de mot de passe, cliquez sur Sécurité dans le menu principal, puis sur Stratégies.

Pour éditer une stratégie de mot de passe, cliquez dessus dans la liste Stratégies. Pour créer une stratégie de mot de passe, sélectionnez Stratégie de qualité de chaîne dans la liste d'options Nouveau.

Remarque – Pour plus d'informations sur les stratégies, reportez-vous à "Configuration des stratégies d'Identity Manager" à la page 101.

Création d'une stratégie

Les stratégies de mot de passe constituent le type par défaut des stratégies de qualité chaîne. Après avoir nommé la nouvelle stratégie et avoir entré une brève description, sélectionnez les options et les paramètres des règles qui la définissent.

Règles de longueur

Les règles de longueur définissent les nombres de caractères minimum et maximum requis pour un mot de passe. Sélectionnez cette option pour activer la règle puis saisissez une valeur seuil.

Type de la stratégie

Choisissez l'un des boutons de type de stratégie suivants : Si vous choisissez l'option Autre, vous devez saisir le type dans le champ de texte fourni.

Règles de type de caractère

Les règles de type de caractères fixent les nombres de caractères minimum et maximum requis de certains types et les chiffres pouvant être inclus dans un mot de passe.

Elles incluent les éléments suivants :

- les nombres minimum et maximum de caractères alphabétiques, numériques, majuscules, minuscules et spéciaux ;
- les nombres minimum et maximum de caractères numériques imbriqués ;
- le nombre maximum de caractères répétés et en séquence ;
- les nombres minimum de caractères alphabétiques et numériques de début.

Saisissez une valeur limite numérique pour chaque règle de type de caractères ou saisissez Tous pour indiquer que tous les caractères doivent être de ce type.

Nombre minimal de règles de type de caractères

Vous pouvez aussi définir le nombre minimal de règles de type de caractères devant réussir la validation comme illustré à la Figure 3–7. Le nombre minimal de règles devant réussir est de une règle. Le maximum ne peut pas dépasser le nombre des règles de type de caractères que vous avez activées.

Remarque – Pour définir le nombre minimal de règles de type de caractères devant réussir sur la valeur la plus haute, sélectionnez Tous.

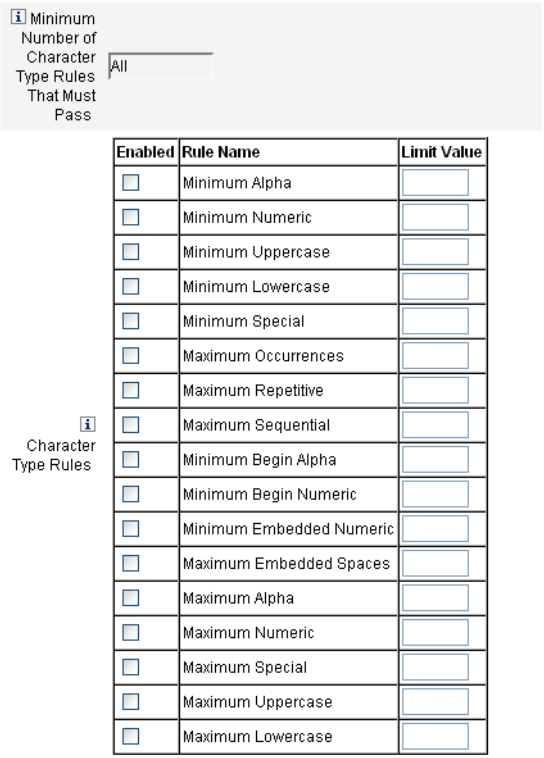


FIGURE 3–7 Règles des stratégies de mot de passe (type de caractères)

Sélection de la stratégie de dictionnaire

Vous pouvez choisir de contrôler les mots de passe par rapport à un dictionnaire pour vous protéger contre les attaques par dictionnaire simples.

Pour pouvoir utiliser cette option, vous devez :

- configurer le dictionnaire ;
- charger les mots du dictionnaire.

Vous configurez le dictionnaire depuis la page Stratégies. Pour plus d'informations sur la configuration du dictionnaire, reportez-vous à "Stratégie de dictionnaire" à la page 104.

Stratégie d'historique de mot de passe

Vous pouvez interdire la réutilisation des derniers mots de passe précédents pour un mot de passe nouvellement sélectionné.

Dans le champ Nombre de mots de passe antérieurs ne pouvant pas être réutilisés, saisissez une valeur numérique supérieure à un pour empêcher toute réutilisation des mots de passe actuels et précédents. Par exemple, si vous saisissez le chiffre 3, le nouveau mot de passe ne pourra pas être le même que le mot de passe actuel ni que les deux mots de passe le précédant.

Vous pouvez aussi interdire la réutilisation de caractères similaires à ceux employés dans les mots de passe précédents. Dans le champ Nombre maximal de caractères identiques à ceux des mots de passe précédents ne pouvant être réutilisés, indiquez le nombre de caractères consécutifs contenus dans les mots de passe précédents ne pouvant pas être réutilisés dans le nouveau mot de passe. Par exemple, si vous indiquez 7 et que le mot de passe précédent était password1, le nouveau mot de passe ne pourra pas être password2 ni password3.

Si vous entrez la valeur 0, tous les caractères doivent être différents indépendamment de leur ordre. Par exemple, si le mot de passe précédent était abcd, le nouveau mot de passe ne peut pas contenir les caractères a, b, c et d.

Cette règle peut s'appliquer à un ou plusieurs mots de passe précédents. Le nombre de mots de passe précédents vérifiés correspond à la valeur indiquée dans le champ Nombre de mots de passe précédents ne pouvant être réutilisés.

Ne doit pas contenir les mots

Vous pouvez entrer un ou plusieurs mots que le mot de passe ne doit en aucun cas contenir. Dans la zone d'entrée, saisissez un mot par ligne.

Vous pouvez également exclure des mots en configurant et en implémentant la stratégie de dictionnaire. Pour plus d'informations, reportez-vous à “Stratégie de dictionnaire” à la page 104.

Ne doit pas contenir les attributs

Vous pouvez entrer un ou plusieurs attributs que le mot de passe ne doit en aucun cas contenir.

Vous pouvez spécifier les attributs suivants :

- `accountID`,
- `email`,
- `firstname`,
- `fullname`,
- `lastname`.

Vous pouvez modifier l'ensemble d'attributs « ne doit pas contenir » dans l'objet Configuration `UserUIConfig`. Pour plus d'informations, reportez-vous à “Ne doit pas contenir les attributs dans les stratégies” à la page 104.

Implémentation des stratégies de mot de passe

Les stratégies de mot de passe sont établies pour chaque ressource. Pour mettre une stratégie de mot de passe en place pour une ressource spécifique, sélectionnez-la dans la liste d'options Stratégie de mot de passe, figurant dans la zone Configuration de la stratégie des pages de l'assistant Créer ou Éditer la ressource : Paramètres Identity Manager.

Authentification des utilisateurs

Si un utilisateur oublie son mot de passe ou que son mot de passe est réinitialisé, il peut répondre à une ou plusieurs questions d'authentification pour accéder à Identity Manager. Vous établissez ces questions ainsi que les règles qui les régissent, dans une stratégie de compte Identity Manager. Contrairement aux stratégies de mot de passe, les stratégies de compte Identity Manager sont assignées à l'utilisateur directement ou au travers de l'organisation qui lui est assignée (sur les pages Créer un utilisateur et Éditer l'utilisateur).

▼ Pour configurer l'authentification d'une stratégie de compte

1. **Cliquez sur Sécurité dans le menu principal, puis sur Stratégies.**

2. **Sélectionnez Stratégie de compte Identity Manager par défaut dans la liste des stratégies.**

   Les sélections d'authentification sont proposées dans la zone Options de stratégie d'authentification de second niveau de la page.

   Important ! Lors de la première installation, l'utilisateur doit se connecter à l'interface utilisateur et fournir les réponses initiales à ses questions d'authentification. Si ces réponses ne sont pas définies, l'utilisateur ne pourra pas se connecter sans son mot de passe.

   La stratégie des questions d'authentification détermine ce qui se passe quand un utilisateur clique sur le bouton Mot de passe oublié ? sur la page de connexion ou lorsqu'il accède à la page Changer mes réponses. "Authentification des utilisateurs" à la page 92 décrit les différentes options.

Option	Description
Tous	Exige de l'utilisateur qu'il réponde à toutes les questions définies par la stratégie et personnalisées.
N'importe lequel	Identity Manager affiche toutes les questions définies par la stratégie et personnalisées. Vous devez spécifier le nombre des questions auxquelles l'utilisateur devra répondre.

Option	Description
Suivant	Exige de l'utilisateur qu'il réponde à toutes les questions définies par la stratégie la première fois qu'il se connecte. Si l'utilisateur clique sur le bouton Mot de passe oublié ? pendant la connexion, Identity Manager affiche la première question. Si l'utilisateur ne répond pas correctement, Identity Manager affiche la question suivante et ce jusqu'à ce que l'utilisateur réponde correctement à une question d'authentification et se connecte, ou soit bloqué pour avoir atteint le nombre limite spécifié de tentatives ratées. Les questions générées par un utilisateur ne sont pas prises en charge pour cette stratégie.
Aléatoire	Permet à l'administrateur de spécifier le nombre des questions auxquelles l'utilisateur devra répondre. Identity Manager sélectionne de manière aléatoire dans la liste des questions définies dans la stratégie et parmi celles définies par l'utilisateur le nombre de questions spécifié et les affiche. L'utilisateur doit répondre à toutes les questions affichées.
À tour de rôle	Identity Manager sélectionne la question suivante de la liste des questions configurées et l'assigne à l'utilisateur. Le premier utilisateur se voit assigner la première question de la liste des questions d'authentification, le second la deuxième question et ainsi de suite jusqu'à ce qu'il n'y ait plus de questions. À ce stade, les questions sont assignées aux utilisateurs en ordre séquentiel. Par exemple, s'il y a dix questions, le 11e et le 21e utilisateurs se verront assigner la première question. Seule la question sélectionnée s'affiche. Si vous souhaitez que l'utilisateur réponde à une question différente à chaque fois, choisissez la stratégie Aléatoire et définissez le nombre de questions sur 1. Les utilisateurs ne peuvent pas définir leurs propres questions d'authentification. Pour plus d'informations sur cette fonctionnalité, reportez-vous à "Questions d'authentification personnalisées" à la page 94.

Vous pouvez vérifier vos choix d'authentification en vous connectant à l'interface utilisateur d'Identity Manager en cliquant sur le bouton Mot de passe oublié ? et en répondant à la/aux questions posées.

La Figure 3–8 représente un exemple d'écran d'authentification de compte utilisateur.

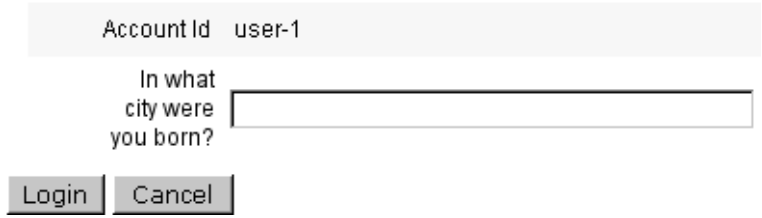


FIGURE 3–8 Authentification de compte utilisateur

Questions d'authentification personnalisées

Dans la stratégie de compte Identity Manager, vous pouvez sélectionner une option permettant aux utilisateurs de fournir leurs propres questions d'authentification dans les interfaces utilisateur et administrateur. Vous pouvez de plus définir le nombre minimum de questions que l'utilisateur doit fournir et auxquelles il devra répondre pour parvenir à se connecter en utilisant les questions d'authentification personnalisées.

Les utilisateurs peuvent ajouter et changer des questions depuis la page Changer les réponses aux questions d'authentification. Un exemple de cette page est illustré à la Figure 3–9.

FIGURE 3–9 Changer les réponses : Questions d'authentification personnalisées

Ignorer la demande de changement de mot de passe suivant l'authentification par questions

Quand un utilisateur réussit à s'authentifier en répondant à une ou plusieurs questions, il est par défaut invité par le système à fournir un nouveau mot de passe. Vous pouvez cependant configurer Identity Manager pour ignorer cette demande de changement de mot de passe en définissant la propriété de configuration système `bypassChangePassword` pour une ou plusieurs applications Identity Manager.

Pour les instructions à suivre pour éditer un objet Configuration système, voir "Édition des objets Configuration Identity Manager" à la page 118.

Pour ignorer une demande de changement de mot de passe pour toutes les applications après une authentification réussie, définissez la propriété `bypassChangePassword` comme suit dans l'objet Configuration système.

EXEMPLE 3–2 Définition de l'attribut pour ignorer la demande de changement de mot de passe

```
<Attribute name="ui"
 <Object>
   <Attribute name="web">
     <Object>
       <Attribute name=’questionLogin’>
         <Object>
           <Attribute name=’bypassChangePassword’>
             <Boolean>true</Boolean>
           </Attribute>
         </Object>
       </Attribute>
   ...
 </Object>
...
```

Pour désactiver cette demande de mot de passe pour une application spécifique, définissez-la comme suit.

EXEMPLE 3–3 Définition de l'attribut pour désactiver la demande de changement de mot de passe

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name=’user’>
          <Object>
            <Attribute name=’questionLogin’>
              <Object>
                <Attribute name=’bypassChangePassword’>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
        </Object>
       </Attribute>
     ...
  </Object>
...
```

Assignation de privilèges administratifs

Vous pouvez assigner des privilèges administratifs Identity Manager, ou capacités, aux utilisateurs de la manière suivante :

- Rôles admin. Les utilisateurs auxquels un rôle admin a été assigné héritent des capacités et des organisations contrôlées définies par ce rôle. Par défaut, tous les comptes utilisateur Identity Manager se voient assigner le `rôle User Admin` à leur création. Pour des informations détaillées sur les rôles admin et sur la création d'un rôle admin, reportez-vous à "Comprendre et gérer les ressources Identity Manager externes" à la page 160 dans le Chapitre 5, "Rôles et ressources".
- Capacités. Les capacités sont définies par des règles. Identity Manager fournit des ensembles de capacités regroupées en capacités fonctionnelles que vous pouvez sélectionner. L'assignation de capacités autorise une majeure granularité dans l'assignation des privilèges administratifs. Pour plus d'informations sur les capacités et leur création, reportez-vous à "Comprendre et gérer les capacités" à la page 216 au Chapitre 6, "Administration".
- Organisations contrôlées. Les organisations contrôlées accordent des privilèges de contrôle administratif sur des organisations spécifiées. Pour plus d'informations, reportez-vous à "Comprendre les organisations d'Identity Manager" à la page 209 au Chapitre 6, "Administration".

Pour plus d'informations sur les administrateurs Identity Manager et les tâches administratives, voir le Chapitre 6, "Administration".

Détection automatique des utilisateurs

L'interface utilisateur final d'Identity Manager permet aux utilisateurs finaux de *détecter* les comptes de ressource. Autrement dit, un utilisateur ayant une identité Identity Manager peut l'associer à un compte de ressource existant mais non associé.

Activation de la détection automatique

Pour activer l'auto-détection, vous devez éditer un objet Configuration spécial (End User Resources) et l'ajouter au nom de chacune des ressources sur lesquelles l'utilisateur sera autorisé à détecter des comptes.

▼ Pour activer la détection automatique

1 Éditez l'objet Configuration « End User Resources » (Ressources de l'utilisateur final).

Pour les instructions à suivre pour éditer les objets Configuration d'Identity Manager, reportez-vous à "Édition des objets Configuration Identity Manager" à la page 118.

2 **Ajoutez <`String`>*Ressource* </`String`>, où *Ressource* correspond au nom d'un objet Ressource dans le référentiel comme illustré à la Figure 3–10.**

FIGURE 3–10 L'objet Configuration « End User Resources ».

3 **Cliquez sur Enregistrer.**

Lorsque la détection automatique est activée, l'utilisateur se voit présenter une nouvelle sélection sous l'onglet de menu Profil dans l'interface utilisateur Identity Manager (Détection automatique). Cette zone permet à l'utilisateur de sélectionner une ressource dans une liste de ressources disponibles puis de saisir l'ID et le mot de passe du compte de ressource pour lier le compte à cette identité Identity Manager.

Remarque – Pour donner aux utilisateurs finaux l'accès aux objets Configuration d'Identity Manager, les administrateurs peuvent aussi utiliser l'organisation « Utilisateur final ». Pour de plus amples détails, reportez-vous à "L'organisation Utilisateur final" à la page 231.

Inscription anonyme

La fonctionnalité d'inscription anonyme permet à un utilisateur n'ayant pas de compte Identity Manager d'en obtenir un via une simple demande.

Activation de l'inscription anonyme

Par défaut, la fonctionnalité d'inscription anonyme est désactivée.

▼ Pour activer la fonctionnalité d'inscription anonyme

1 **Dans l'interface administrateur, cliquez sur Configurer puis sur Interface utilisateur.**

2 **Dans la zone Inscription anonyme, sélectionnez l'option activer puis cliquez sur Enregistrer.**

Lorsqu'un utilisateur se connecte à l'interface utilisateur, la page de connexion affiche le texte Nouvel utilisateur ? suivi du lien Demander un compte.

Remarque – Le texte Nouvel utilisateur ? Demander un compte est personnalisable. Pour de plus amples détails, consultez le *Sun Identity Manager Deployment Guide*.

FIGURE 3–11 Page Interface utilisateur avec le lien Demander un compte activé

Configuration de l'inscription anonyme

La zone Inscription anonyme de la page Interface utilisateur permet de configurer les options suivantes pour le processus d'inscription anonyme :

- **Modèle de notification**. Indiquez l'ID du modèle d'e-mail à utiliser pour envoyer des notifications à l'utilisateur demandant un compte.
- **Stratégie de confidentialité requise**. Lorsque cette option est activée, l'utilisateur doit accepter la politique de confidentialité avant de pouvoir demander la création d'un compte. Cette option est activée par défaut.

- **Activer la validation**. Lorsque cette option est activée, l'utilisateur doit valider son embauche avant de pouvoir demander la création d'un compte. Cette option est activée par défaut.
- **URL de lancement de processus**. Indiquez l'URL servant à définir le flux de travaux à utiliser pour le processus d'inscription anonyme.
- **Activer les notifications**. Lorsque cette option est activée, un e-mail de notification est envoyé à l'utilisateur une fois que son compte a été créé.
- **Domaine de messagerie**. Indiquez le nom du domaine de messagerie électronique à utiliser pour construire l'adresse e-mail de l'utilisateur.

Cliquez sur Enregistrer lorsque vous avez fini.

Processus d'inscription d'utilisateur

Tout utilisateur se connectant à l'interface utilisateur peut demander un compte en cliquant sur le lien Demander un compte de la page de connexion.

Identity Manager affiche la première des deux pages d'inscription dans lesquelles l'utilisateur doit indiquer ses nom, prénom et ID d'employé. Si l'attribut Activer la validation est défini sur oui (paramétrage par défaut), ces informations doivent alors être validées pour que l'utilisateur puisse passer à la page suivante.

Les règles `verifyFirstname`, `verifyLastname`, `verifyEmployeeId` et `verifyEligibility` dans `EndUserLibrary` valident les informations pour chaque attribut.

Remarque – Il est possible que vous deviez modifier une ou plusieurs de ces règles. En particulier, vous devez modifier la règle qui vérifie l'ID de l'employé pour qu'elle utilise un appel de services Web ou une classe Java pour vérifier ces informations.

Si l'attribut Activer la validation est désactivé, la première page d'inscription ne s'affiche pas. Dans ce cas, vous devez modifier le formulaire End User Anonymous Enrollment Completion pour permettre à l'utilisateur de saisir les informations normalement capturées par le premier formulaire de validation.

À partir des informations indiquées sur la page Enregistrement, Identity Manager génère les éléments suivants :

- Un ID de compte (respectant la convention initiale du prénom, initiale du nom et ID de l'employé).
- Une adresse e-mail de la forme suivante :

  Prénom. *Nom*@*DomaineEmail*

  Où *DomaineEmail* est le domaine défini par l'attribut Domaine de messagerie dans la configuration d'inscription anonyme.
- L'attribut de responsable (`idmManager`). Vous pouvez définir cet attribut en modifiant la règle `EndUserRuleLibrary:getIdmManager`. Par défaut, le responsable est défini sur Configurator (Configurateur). L'administrateur désigné en tant que responsable doit approuver la demande de l'utilisateur pour que le compte de ce dernier soit provisionné.
- L'attribut d'organisation. Vous pouvez définir cet attribut en personnalisant la règle `EndUserRuleLibrary:getOrganization`. Par défaut, les utilisateurs sont assignés au niveau supérieur de la hiérarchie d'organisations (« Haut »).

Si les informations indiquées par l'utilisateur sur la page Enregistrement sont validées avec succès, Identity Manager présente à l'utilisateur la deuxième page Enregistrement. L'utilisateur doit alors entrer un mot de passe et le confirmer. Si l'attribut Vous devez accepter la politique de confidentialité est défini sur oui, l'utilisateur doit également sélectionner une option pour accepter les conditions de la stratégie de confidentialité.

Lorsque l'utilisateur clique sur Enregistrer, Identity Manager présente une page de confirmation. Si l'attribut Activer les notifications est défini sur oui, la page indique alors que l'utilisateur recevra un e-mail après la création du compte.

Le compte est créé une fois le processus Créer un utilisateur standard (approbations requises par l'attribut `idmManager` et paramètres de stratégie compris) terminé.

◆ ◆ ◆ CHAPITRE 4

Configuration des objets d'administration d'entreprise

Ce chapitre contient des informations et des procédures relatives à l'utilisation de l'interface administrateur pour paramétrer et actualiser les objets Identity Manager. Pour plus d'informations sur les objets Identity Manager, voir la section “Objets Identity Manager” à la page 27 au chapitre Présentation.

Remarque – Pour toute information sur la configuration d'Identity Manager pour une implémentation Service Provider (fournisseur de services), voir le Chapitre 17, “Administration de Service Provider”.

Ce chapitre se compose des sections suivantes :

Configuration des stratégies d'Identity Manager

Vous trouverez dans cette section des informations relatives à la configuration des stratégies utilisateur.

Cette section se compose des rubriques suivantes :

Définition des stratégies

Les stratégies d' Identity Manager définissent des limites pour les utilisateurs Identity Manager en établissant des contraintes concernant les caractéristiques des ID de compte, connexions et mots de passe d'Identity Manager.

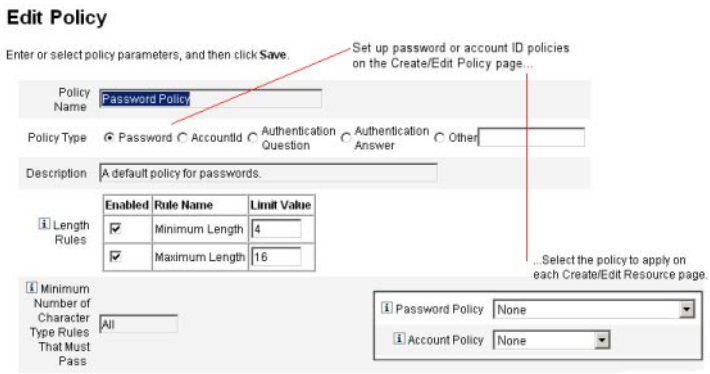
Remarque – Identity Manager fournit également des stratégies d'audit spécialement conçues pour contrôler la compatibilité des utilisateurs. Les stratégies d'audit font l'objet du Chapitre 13, “Audit des identités : principes de base”.

Les stratégies sont classées en catégories comme suit :

- **Stratégies de compte Identity System**. Ces stratégies établissent les options et contraintes concernant les utilisateurs, mots de passe et stratégies d'authentification. Vous assignez des stratégies de compte Identity System aux organisations à partir des pages Créer une organisation et Éditer l'organisation ou aux utilisateurs depuis les pages Créer un utilisateur et Éditer l'utilisateur.

  Vous pouvez définir ou sélectionner les options suivantes :

  - **Options de stratégie de compte utilisateur**. Ces options spécifient la façon dont Identity Manager traite les comptes utilisateur si un utilisateur ne parvient pas à répondre correctement aux questions d'authentification.
  - **Options de stratégie de mot de passe**. Ces options définissent l'expiration du mot de passe, le préavis avant l'expiration et les options de réinitialisation.
  - **Options de stratégie d'authentification de second niveau**. Ces options déterminent la façon dont les questions d'authentification sont présentées à l'utilisateur, si l'utilisateur peut fournir ses propres questions d'authentification, appliquer l'authentification à la connexion et établir la banque des questions pouvant être posées à un utilisateur.
- **Stratégies de compte système de Service Provider**. Dans une implémentation de fournisseur de services, ce type de stratégie permet d'établir les options et les contraintes en matière de stratégies d'utilisateur, de mots de passe et d'authentification pour les utilisateurs de fournisseur de services. Vous assignez les stratégies aux organisations à partir des pages Créer une organisation et Éditer l'organisation ou aux utilisateurs depuis les pages Créer un utilisateur et Éditer l'utilisateur.
- **Stratégies de qualité de chaîne**. Cette catégorie comprend des types de stratégie tels que ceux de mot de passe, ID de compte et authentification. Ces stratégies permettent de définir les règles de longueur, les règles de type de caractères, les mots autorisés et les valeurs d'attributs. Ce type de stratégie est lié à chaque ressource Identity Manager et défini sur chaque page de ressource. La figure suivante donne un exemple.



Vous pouvez définir les options et règles suivantes pour les mots de passe et ID de compte :

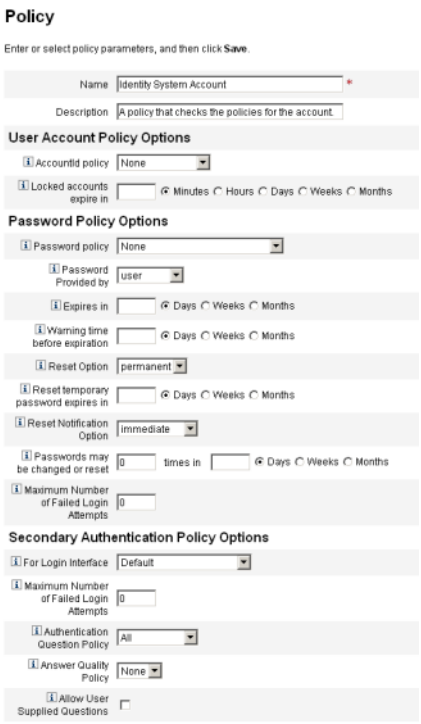
- **Règles de longueur**. Ces règles déterminent la longueur minimum et maximum.
- **Règles de type de caractères**. Ces règles définissent les valeurs minimum et maximum admises pour les caractères alphabétiques, numériques, majuscules, minuscules, répétés et séquentiels.
- **Limites de réutilisation des mots de passe**. Ces limites spécifient le nombre des mots de passe précédant le mot de passe actuel qui ne peuvent pas être réutilisés. Lorsqu'un utilisateur essaie de changer son mot de passe, le nouveau mot de passe est confronté à l'historique des mots de passe pour vérifier qu'il s'agit d'un mot de passe unique. Pour des raisons de sécurité, une signature numérique des mots de passe précédents est enregistrée et les nouveaux mots de passe sont confrontés à cette dernière.
- **Mots et valeurs d'attribut interdits**. Cette option spécifie les mots et les attributs qui ne peuvent en aucun cas constituer tout ou partie d'un ID ou d'un mot de passe.

▼ Pour ouvrir la page Stratégies

Vous créez et éditez les stratégies utilisateur Identity Manager depuis la page Stratégies. Pour ouvrir cette page, procédez comme suit :

1. **Connectez-vous à l'interface administrateur.**
2. **Cliquez sur l'onglet Sécurité puis sur le sous-onglet Stratégies.**

   La page Stratégies, représentée dans la figure suivante, s'ouvre.



Ne doit pas contenir les attributs dans les stratégies

Vous pouvez modifier l'ensemble autorisé d'attributs « Ne doit pas contenir » dans l'objet configuration `UserUIConfig`.

Les attributs sont listés dans `UserUIConfig` comme suit :

- attribut `<PolicyPasswordAttributeNames>` : mot de passe du type de stratégie ;
- attribut `<PolicyAccountAttributeNames>` : ID de compte du type de stratégie ;
- attribut `<PolicyOtherAttributeNames>` : autre élément du type de stratégie.

Stratégie de dictionnaire

Une stratégie·de dictionnaire permet à Identity Manager de vérifier, par rapport à une base de données de mots, que les mots de passe sont protégés d'une attaque de dictionnaire simple. Cette stratégie, utilisée avec d'autres paramètres de stratégie pour imposer la longueur et l'arrangement des mots de passe, permet à Identity Manager de rendre difficile l'utilisation d'un dictionnaire pour deviner les mots de passe générés ou changés dans le système.

La stratégie de dictionnaire étend la liste d'exclusion de mots de passe que vous pouvez configurer avec la stratégie (cette liste est implémentée par l'option Ne doit pas contenir les mots sur la page Éditer la stratégie de mot de passe de l'interface administrateur).

▼ Pour configurer une stratégie de dictionnaire

Pour configurer une stratégie de dictionnaire, vous devez :

- configurer la prise en charge du serveur du dictionnaire ;
- charger le dictionnaire.

1 Ouvrez la page Stratégies comme décrit dans "Pour ouvrir la page Stratégies" à la page 103.

2 Cliquez sur Configurer le dictionnaire pour afficher la page Configuration du dictionnaire.

3 Sélectionnez et saisissez les informations relatives à la base de données.

Ces informations sont les suivantes :

- **Type de la base de données**. Sélectionnez le type de la base de données (Oracle, DB2, SQLServer ou MySQL) que vous utiliserez pour stocker le dictionnaire.
- **Hôte**. Entrez le nom de l'hôte sur lequel la base de données sera exécutée.
- **Utilisateur**. Saisissez le nom d'utilisateur à utiliser pour la connexion à la base de données.
- **Mot de passe**. Saisissez le mot de passe à utiliser lors de la connexion à la base de données.
- **Port**. Entrez le port sur lequel la base de données écoute.
- **Connexion URL**. Saisissez l'URL à utiliser lors de la connexion. Les variables de modèles suivantes sont disponibles :
  - `%h` (hôte),
  - `%p` (port),
  - `%d` (nom de la base de données).

  Classe de pilote. Saisissez la classe du pilote JDBC à utiliser lors de l'interaction avec la base de données.
- **Nom de la base de données**. Saisissez le nom de la base de données dans laquelle le dictionnaire sera chargé.
- **Nom de fichier du dictionnaire**. Saisissez le nom du fichier à utiliser lors du chargement du dictionnaire.

4 Cliquez sur Test pour tester la connexion à la base de données.

5 Si le test de connexion réussit, cliquez sur Charger mots pour charger le dictionnaire. La tâche de chargement peut prendre quelques minutes.

6 Cliquez sur Test pour vérifier que le chargement du dictionnaire a réussi.

▼ Pour implémenter une stratégie de dictionnaire

Suivez les étapes ci-après pour implémenter une stratégie de dictionnaire :

1. **Ouvrez la page Stratégies comme décrit dans "Pour ouvrir la page Stratégies" à la page 103.**
2. **Cliquez sur le lien Stratégie de mot de passe pour éditer la stratégie de mot de passe.**
3. **Dans la page Éditer la stratégie, sélectionnez l'option Vérifier les mots de passe dans le dictionnaire.**
4. **Cliquez sur Enregistrer pour enregistrer vos modifications.**

   Une fois la stratégie implémentée, tous les mots de passe générés et changés sont confrontés au dictionnaire.

Personnalisation des modèles d'e-mails

Identity Manager utilise des modèles d'e-mails pour envoyer des informations et des requêtes d'actions aux utilisateurs et aux approbateurs. Le système comprend des modèles pour les éléments suivants :

- **Avis de vérification d'accès**. Envoie une notification spécifiant que les droits d'accès d'un utilisateur doivent être revus. Le système envoie cette notification lorsqu'une violation de stratégie d'accès doit être résolue ou atténuée.
- **Approbation de création de compte**. Envoie à un approbateur une notification l'avertissant qu'un nouveau compte attend son approbation. Le système envoie cette notification lorsque l'option de notification de provisioning pour le rôle associé est définie sur approval.
- **Notification de création de compte**. Envoie une notification spécifiant qu'un compte a été créé avec une assignation de rôle particulière. Le système envoie cette notification lorsqu'un ou plusieurs administrateurs sont sélectionnés dans le champ Destinataires de la notification des pages Créer un rôle ou Éditer un rôle.
- **Approbation de suppression de compte**. Envoie une notification à un approbateur, selon laquelle un action de suppression de compte utilisateur attend son approbation. Le système envoie cette notification lorsqu'un ou plusieurs administrateurs sont sélectionnés dans le champ Destinataires de la notification des pages Créer un rôle ou Éditer un rôle.
- **Notification de suppression de compte**. Envoie une notification spécifiant qu'un compte a été supprimé.
- **Notification de mise à jour de compte**. Envoie aux adresses e-mail ou aux comptes utilisateur spécifiés une notification indiquant qu'un compte a été mis à jour.
- **Ressource externe**. Avertit un approvisionneur de ressources externe qu'une tâche de provisioning doit être effectuée.

- **Réinitialisation du mot de passe**. Envoie une réinitialisation indiquant qu'un mot de passe Identity Manager a été réinitialisé. Selon la valeur du paramètre Option de notification de la réinitialisation sélectionnée pour la stratégie Identity Manager associée, le système affiche immédiatement la notification (dans le navigateur Web) à l'administrateur réinitialisant le mot de passe ou envoie un e-mail à l'utilisateur dont le mot de passe est en cours de réinitialisation.
- **Avis de synchronisation du mot de passe**. Avertit l'utilisateur qu'un changement de mot de passe a été appliqué correctement à l'ensemble des ressources. L'avis indique les ressources mises à jour et signale l'origine de la requête de changement de mot de passe.
- **Avis d'échec de la synchronisation du mot de passe**. Informe l'utilisateur qu'un changement de mot de passe n'a pas pu être appliqué correctement à l'ensemble des ressources. L'avis présente une liste des erreurs et indique l'origine de la requête de changement de mot de passe.
- **Avis de violation de stratégie**. Envoie un avis indiquant qu'une violation de stratégie de compte s'est produite.
- **Événement de réconciliation de compte**. Événement de réconciliation de ressource, Récapitulatif de réconciliation. Appelé depuis, dans l'ordre, les flux de travaux par défaut Notify Reconcile Response, Notify Reconcile Start et Notify Reconcile Finish. La notification est envoyée selon la configuration de chaque flux de travaux.
- **Rapport**. Envoie un rapport généré à une liste de destinataires spécifiée.
- **Demande de ressource**. Prévient un administrateur de ressource qu'une ressource a été demandée. Le système envoie cette notification lorsqu'un administrateur demande une ressource de la zone Ressources.

Remarque – Les ressources Request sont désapprouvées au profit des ressources externes dans la version 8.1 d'Identity Manager. Vous ne pouvez plus créer de nouvelles connexions en utilisant l'adaptateur Request. Utilisez à la place l'adaptateur External Resource. Pour plus d'informations, reportez-vous à "Comprendre et gérer les ressources externes" à la page 175.

- **Notification de relance**. Prévient un administrateur qu'une opération particulière a été tentée un certain nombre de fois sur une ressource, mais sans succès.
- **Analyse de risque**. Envoie un rapport d'analyse de risque. Le système envoie ce rapport lorsqu'un ou plusieurs destinataires d'e-mail sont spécifiés lors d'un scannage des ressources.
- **Réinitialisation du mot de passe temporaire**. Envoie une notification à l'utilisateur ou à l'approbateur de rôle indiquant qu'un mot de passe temporaire a été fourni pour le compte. Selon la valeur du paramètre Option de notification de réinitialisation du mot de passe sélectionnée pour la stratégieIdentity Manager associée, le système affiche immédiatement la notification (dans le navigateur Web) à l'utilisateur, envoie un e-mail à l'utilisateur ou envoie un e-mail aux approbateurs de rôles.

- **Récupération d'ID utilisateur**. Envoie un ID utilisateur récupéré à l'adresse e-mail spécifiée.

Édition d'un modèle d'e-mail

Vous pouvez personnaliser les modèles d'e-mail pour fournir au destinataire des instructions spécifiques lui indiquant comment accomplir une tâche ou afficher les résultats. Par exemple, vous pouvez personnaliser le modèle Approbation de création de compte pour diriger un approbateur vers une page d'approbation de compte en ajoutant le message suivant :

```
Consultez le site http://host.example.com:8080/idm/approval/approval.jsp pour
approuver la création de compte pour $(fullname).
```

Utilisez la procédure suivante pour personnaliser un modèle d'e-mail en utilisant le modèle Approbation de création de compte en tant qu'exemple.

▼ Pour personnaliser un modèle d'e-mail

1. **Dans l'interface administrateur, cliquez sur l'onglet Configurer puis sur le sous-onglet Modèles d'e-mail.**

   La page Modèles d'e-mail s'ouvre.

2. **Cliquez pour sélectionner le modèle Approbation de création de compte.**

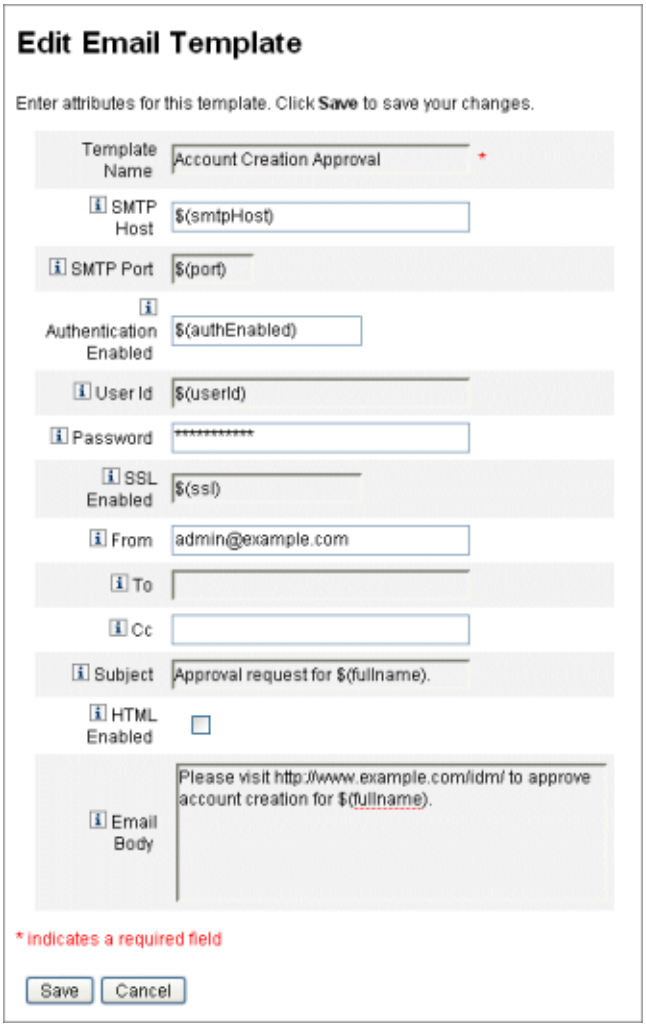


FIGURE 4–1 Édition d'un modèle d'e-mail

3 Saisissez les détails concernant ce modèle.

Vous pouvez entrer les informations suivantes :

- Entrez dans le champ Hôte SMTP le nom du serveur SMTP pour permettre l'envoi de la notification par e-mail.
- Dans le champ De, personnalisez l'adresse e-mail d'origine.
- Dans les champs À et Cc, saisissez une ou plusieurs adresses e-mail ou comptes Identity Manager qui seront les destinataires de la notification par e-mail.

- Dans le champ Corps de l'e-mail, personnalisez le contenu pour fournir un pointeur vers votre emplacement Identity Manager.

4 **Cliquez sur Enregistrer.**

Vous pouvez aussi modifier des modèles d'e-mail en utilisant environnement de développement intégré Sun Identity Manager (Identity Manager IDE). Pour toute information sur Identity Manager IDE, allez au site Web suivant : `https://identitymanageride.dev.java.net/`.

Remarque – Vous devez vous enregistrer sur ce site et vous y connecter.

HTML et liens dans les modèles d'e-mail

Vous pouvez insérer du contenu au format HTML dans un modèle d'e-mail : ce contenu s'affichera dans le corps du message. Le contenu peut inclure du texte, des graphiques et des liens Web pointant sur des informations. Pour autoriser le contenu au format HTML, sélectionnez l'option HTML activé.

Variables admissibles dans le corps de l'e-mail

Vous pouvez aussi inclure des références à des variables dans le corps du modèle d'e-mail, sous la forme `$(`*Nom*`)`; par exemple : `Votre mot de passe $(mot de passe) a été récupéré.`

Les variables admissibles pour les différents modèles sont définies dans le tableau suivant

.

TABLEAU 4–1 Variables des modèles d'e-mails

Modèle	Variables admissibles
Réinitialisation du mot de passe	`$(password)` : mot de passe nouvellement généré
Mise à jour de l'approbation	`$(fullname)` : nom complet de l'utilisateur
	`$(role)` : rôle de l'utilisateur
Notification de mise à jour	`$(fullname)` : nom complet de l'utilisateur
	`$(role)` : rôle de l'utilisateur

TABLEAU 4–1 Variables des modèles d'e-mails *(Suite)*

Modèle	Variables admissibles
Rapport	`$(report)` : rapport généré
	`$(id)` : ID codé de l'instance de tâche
	`$(timestamp)` : heure d'envoi de l'e-mail
Demande de ressource	`$(fullname)` : nom complet de l'utilisateur
	`$(resource)` : type de ressource
Analyse de risque	`$(report)` : rapport de l'analyse de risque
Réinitialisation du mot de passe temporaire	`$(password)` : mot de passe nouvellement généré
	`$(expiry)` : date d'expiration du mot de passe

Configuration de groupes et d'événements d'audit

Configurer des groupes de configuration d'audit permet d'enregistrer des événements système que vous sélectionnez et de générer des rapports connexes. La configuration de groupes d'audit permet également d'exécuter ultérieurement les rapports AuditLog.

▼ Pour ouvrir la page Configuration d'audit

La page Configuration d'audit permet de configurer les groupes d'audit. Pour ouvrir la page Configuration d'audit, procédez comme suit :

1. **Ouvrez l'interface administrateur.**
2. **Cliquez sur l'onglet Configurer puis sur le sous-onglet Audit.**

   La page Configuration d'audit s'ouvre.

▼ Pour configurer des groupes d'audit

Configurer des groupes et des événements d'audit requiert la capacité administrative Configurer l'audit.

1. **Ouvrez la page Configuration d'audit comme décrit dans la section précédente.**

   La page Configuration d'audit affiche la liste des groupes d'audit, chacun de ces groupes pouvant contenir un ou plusieurs événements. Vous pouvez enregistrer les réussites, les échecs ou ces deux catégories d'événements, pour chacun de ces groupes.

2. **Cliquez sur un groupe d'audit dans la liste pour afficher la page Éditer le groupe de configuration d'audit. Cette page permet de sélectionner les types d'événements de contrôle à enregistrer dans le cadre d'un groupe de configuration d'audit, dans le journal d'audit du système.**

3. **Contrôlez que la case Activer l'audit est sélectionnée. Désélectionnez la case à cocher pour désactiver le système d'audit.**

Remarque – Pour plus d'informations sur les groupes d'audit, voir la section "Configuration d'audit" à la page 348 au Chapitre 10, "Journalisation d'audit".

▼ Pour ajouter des événements à un groupe de configuration d'audit

Suivez les étapes ci-après pour ajouter un événement au groupe :

1. **Cliquez sur Nouveau.**

   Identity Manager ajoute un événement au bas de la page.

2. **Sélectionnez un type d'objet dans la liste de la colonne Type d'objet, puis déplacez un ou plusieurs éléments de la colonne Actions de la zone Disponible à la zone Sélectionné pour le nouveau type d'objet.**

3. **Cliquez sur OK pour ajouter l'événement au groupe.**

▼ Pour éditer des événements dans le groupe Configuration d'audit

Vous pouvez éditer des événements dans le groupe en ajoutant ou en supprimant des actions pour un type d'objet, comme suit :

1. **Déplacez les éléments de la colonne Actions de la zone Disponible à la zone Sélectionné pour le type d'objet en question.**

2. **Cliquez sur OK.**

Intégration Remedy

Vous pouvez intégrer Identity Manager avec un serveur Remedy en permettant à ce dernier d'envoyer des tickets Remedy conformément à un modèle spécifié.

Paramétrez l'intégration Remedy dans deux zones de l'interface administrateur :

- **Paramètres du serveur Remedy** . Paramétrez la configuration de Remedy en créant une ressource Remedy depuis la zone Ressources (voir "Gestion de la liste des ressources" à la page 162). Après la configuration de la ressource, testez la connexion pour vous assurer que l'intégration est activée.
- **Modèle Remedy**. Après avoir configuré la ressource Remedy, définissez un modèle Remedy. Pour cela, ouvrez l'interface administrateur, cliquez sur l'onglet Configurer puis sur Intégration Remedy. Vous sélectionnerez ensuite le schéma et la ressource Remedy.

La création de tickets Remedy se configure par le biais du flux de travaux Identity Manager. Selon vos préférences, un appel peut être effectué à une heure appropriée en utilisant le modèle défini pour ouvrir un ticket Remedy. Pour plus d'informations sur la configuration des flux de travaux, voir le Chapitre 1, "Workflow" du *Sun Identity Manager Deployment Reference*.

Configuration de l'interface utilisateur final

Les administrateurs peuvent configurer certains aspects de l'interface utilisateur final en modifiant un formulaire dans l'interface administrateur.

▼ Pour définir les options d'affichage d'informations dans l'interface utilisateur final

1. **Dans l'interface administrateur, cliquez sur Configurer dans le menu principal.**
2. **Cliquez sur Interface utilisateur dans le menu secondaire.**

   La page Interface utilisateur s'ouvre.
3. **Remplissez et enregistrez la partie Tableau de bord de l'utilisateur final du formulaire. Cliquez sur Aide si vous avez besoin d'aide avec le formulaire.**

   Pour toute information sur le remplissage de la partie Inscription anonyme du formulaire, voir la section "Inscription anonyme" à la page 97.

▼ Pour activer les schémas de processus dans l'interface utilisateur final

Les schémas de processus illustrent le flux de travaux suivi par Identity Manager quand les utilisateurs finaux lancent une demande ou mettent à jour leur profil. Lorsqu'ils sont activés, les schémas des processus s'affichent sur la page des résultats une fois que l'utilisateur final a envoyé un formulaire.

Les schémas de processus doivent être activés dans l'interface administrateur pour pouvoir l'être dans l'interface 'utilisateur final. Pour plus d'informations, voir "Activation des schémas de processus" à la page 58.

1. **Ouvrez la page de configuration de l'interface utilisateur en suivant les étapes de la section "Configuration de l'interface utilisateur final" à la page 113.**
2. **Sélectionnez l'option Activer les schémas des processus, qui se trouve dans la section Pages de résultats du formulaire.**

   Si l'option Activer les schémas des processus n'est pas disponible, vous devez d'abord activer les schémas de processus dans l'interface administrateur. Voir "Activation des schémas de processus" à la page 58.
3. **Cliquez sur Enregistrer.**

Enregistrement d'Identity Manager

Les administrateurs sont invités à enregistrer leur installation d'Identity Manager.

Pour l'enregistrement, vous devez avoir un compte Sun en ligne et un mot de passe. Si vous n'êtes pas propriétaire d'un compte Sun en ligne, vous pouvez vous enregistrer en remplissant le formulaire disponible à l'adresse suivante :

```
https://reg.sun.com/register
```

Identity Manager peut être enregistré à partir de la console ou via l'interface administrateur.

L'enregistrement depuis la console permet également de créer une étiquette de service locale, qui peut être utilisée avec le logiciel Sun Service Tag pour suivre automatiquement vos systèmes, logiciels et services Sun. Le package client Service Tag doit être installé avant de créer une étiquette de service locale. Ce package peut être téléchargé en cliquant sur le bouton Download Service Tags (Télécharger les étiquettes de service) à l'adresse suivante :

```
http://inventory.sun.com/inventory
```

Pour enregistrer Identity Manager, vous devez vous connecter à un compte administrateur vous permettant de configurer des objets Identity Manager. Ce compte doit avoir la capacité Enregistrement du produit. Pour toute information sur les capacités, voir “Assignation de capacités aux utilisateurs ” à la page 219.

Remarque – Pour que la fonctionnalité d'enregistrement du produit fonctionne, Java doit être correctement configuré pour SSL sur vos serveurs d'application Identity Manager. Tous les JAR référencés dans votre fichier `java.security` (ou équivalent) doivent être présents.

Le reste de cette section fournit des informations et des instructions qui vous aideront à enregistrer Identity Manager. Les informations sont organisées dans les rubriques suivantes :

- “Enregistrement d'Identity Manager depuis la console” à la page 115 ;
- “Pour enregistrer Identity Manager depuis l'interface administrateur” à la page 117.

Enregistrement d'Identity Manager depuis la console

Cette section contient les informations dont vous avez besoin pour enregistrer Identity Manager depuis la console.

Utilisation de la commande `register`

La commande `register` permet d'enregistrer Identity Manager depuis la console. Cette section contient des informations sur l'utilisation de cette commande.

Utilisation de la commande `register`

```
register -local
register -remote [-u <userid> [-p <password>]] [-prompt] -userSOA <userid>
-passSOA <password> [-proxy <proxyHost> [-port <proxyPortNumber>]]
register [-help | -?]
```

Options de la commande `register`

Le tableau suivant décrit les options que vous pouvez utiliser avec la commande `register`.

TABLEAU 4–2 Options de la commande

Option	Description
`-local`	Crée une étiquette de service sur cet hôte.

TABLEAU 4–2 Options de la commande *(Suite)*

Option	Description
`-remote`	Enregistre cette installation d'Identity Manager directement auprès de Sun via le réseau.
`-u <idUtilisateur>`	ID utilisateur Identity Manager de l'administrateur Identity Manager autorisé à procéder à l'enregistrement.
`-p <motDePasse>`	Mot de passe Identity Manager de l'administrateur Identity Manager autorisé à procéder à l'enregistrement.
`-prompt`	Invite de manière interactive l'administrateur à saisir son mot de passe si ce dernier manque.
`-userSOA <idUtilisateur>`	ID utilisateur du compte Sun en ligne qui sera utilisé pour l'enregistrement. Est nécessaire si l'enregistrement se fait avec l'option `-remote`.
`-passSOA <motDePasse>`	Mot de passe du compte Sun en ligne qui sera utilisé pour l'enregistrement. Est nécessaire si l'enregistrement se fait avec l'option `-remote`.
`-proxy <hôteProxy>`	Proxy réseau à utiliser pour accéder au service d'enregistrement en ligne de Sun. Est nécessaire si l'enregistrement se fait avec l'option `-remote` et que votre réseau est configuré pour utiliser un proxy pour atteindre les adresses Internet externes.
`-port <numéroPortProxy>`	Port de proxy réseau à utiliser pour accéder au service d'enregistrement en ligne de Sun. Est nécessaire si l'enregistrement se fait avec l'option `-remote` et que votre réseau est configuré pour utiliser un proxy pour atteindre les adresses Internet externes.
`-help | -?`	Imprime l'aide relative à cette commande sur la console.

▼ Pour enregistrer Identity Manager depuis la console

Pour enregistrer Identity Manager depuis la console, vous devez créer une étiquette de service locale ou enregistrer le produit auprès de Sun via Internet. Utilisez les instructions suivantes :

1 Démarrez l'interface de console (ligne de commande) d'Identity Manager.

- Depuis une ligne de commande Windows, saisissez ce qui suit :

  `%WSHOME%\bin\lh`

- Depuis une ligne de commande UNIX, saisissez ce qui suit :

  `$WSHOME/bin/lh`

2 Utilisez la commande `register` comme suit :

- Pour créer une étiquette de service locale

  `register -local`

- Pour enregistrer Identity Manager via Internet, utilisez la commande suivante :

register -remote -u <*idUtilisateur*> **-p** <*motDePasse*> **-userSOA** <*idUtilisateurSoa*> **-passSOA** <*motDePasseSoa* > **-proxy** <*hôteProxy*> **-port** < *numéroPortProxy*>

Où :

- **idUtilisateur** est l'ID utilisateur Identity Manager de l'administrateur Identity Manager autorisé à procéder à l'enregistrement.
- **motDePasse** est le mot de passe Identity Manager de l'administrateur Identity Manager autorisé à procéder à l'enregistrement.
- **idUtilisateurSoa** est l'ID utilisateur du compte Sun en ligne qui sera utilisé pour l'enregistrement.
- **motDePasseSoa** est le mot de passe du compte Sun en ligne qui sera utilisé pour l'enregistrement.
- **hôteProxy** est le proxy réseau à utiliser pour accéder au service d'enregistrement en ligne de Sun. Il n'est nécessaire que si votre réseau est configuré pour utiliser un proxy pour atteindre les adresses Internet externes.
- **numéroPortProxy** est le port de proxy réseau à utiliser pour accéder au service d'enregistrement en ligne de Sun. Il n'est nécessaire que si votre réseau est configuré pour utiliser un proxy pour atteindre les adresses Internet externes.

▼ Pour enregistrer Identity Manager depuis l'interface administrateur

Si vous n'avez pas besoin de créer d'étiquette de service locale, enregistrez Identity Manager depuis l'interface administrateur.

1. **Dans l'interface administrateur, cliquez sur Configurer.**
2. **Dans le menu secondaire, cliquez sur Enregistrement du produit.**

   La page Enregistrement du produit s'ouvre.
3. **Remplissez le formulaire et cliquez sur M'enregistrer maintenant. Cliquez sur les i-Helps pour toute information sur les différents champs du formulaire.**

Remarque –

- Si votre serveur d'application n'est pas configuré pour permettre les connexions SSL sortantes, le message d'erreur suivant peut s'afficher :

  ```
  Failed to register on Sun Connection server
  due to invalid Sun Online Account user/password.
  ```

  Pour résoudre ce problème, ajoutez les certificats racine de confiance appropriés au keystore de votre serveur d'application. Pour plus de détails, consultez la documentation de votre serveur d'application.
- Si d'anciennes versions de `xml-apis.jar` et `xercesImpl.jar` sont présentes dans le classpath du serveur d'application, le message d'erreur suivant peut s'afficher :

  ```
  java.lang.NoSuchMethodError:org.w3c.dom.Node.getTextContent()Ljava/lang/String;
  ```

  Pour résoudre ce problème, modifiez le classpath de manière à ce que seules les versions les plus récentes de `xml-apis.jar` et `xercesImpl.jar` soient présentes.

Édition des objets Configuration Identity Manager

Dans le cadre de l'administration d'Identity Manager, vous serez occasionnellement invité à éditer l'objet Configuration système Identity Manager (aussi appelé Fichier de configuration système) ou d'autres objets similaires.

1. **Ouvrez la page de débogage d'Identity Manager en saisissant l'URL suivant dans votre navigateur :**

   `http://<` *`HôteServeurApp`*`>:<`*`Port`*`>/idm/debug/session.jsp`

   La page System Settings (Paramètres du système) s'ouvre.

   Remarque – Vous devez avoir la capacité Déboguer pour pouvoir afficher les pages `/idm/debug/`.

2. **Trouvez le bouton List Objects (Lister les objets) puis sélectionnez Configuration dans la liste déroulante Type adjacente.**
3. **Cliquez sur le bouton List Objects (Lister les objets).**

   Page List Objects of type (Lister les objets de type) : Configuration s'ouvre.
4. **Dans la liste des objets, recherchez l'objet dont vous avez besoin et cliquez sur edit (éditer).**

   Par exemple, pour éditer l'objet Configuration système, cherchez System Configuration (Configuration système) et cliquez sur edit (éditer).

5. **Éditez l'objet comme indiqué et cliquez sur Save (Enregistrer).**
6. **Si cela vous est demandé, redémarrez votre/vos serveurs.**

◆ ◆ ◆ CHAPITRE 5

Rôles et ressources

Ce chapitre examine les rôles et les ressources d'Identity Manager.

Les informations qu'il contient sont organisées en rubriques comme suit :

Comprendre et gérer les rôles

Vous trouverez dans cette section des informations relatives à la configuration des rôles dans Identity Manager. Dans les entreprises de grande taille, les assignations de ressources basées sur les rôles simplifient considérablement la gestion des ressources.

Remarque – Ne confondez pas les *rôles* avec les *rôles admin*. Les rôles sont utilisés pour gérer l'accès des utilisateurs finaux aux ressources tandis que les rôles admin le sont principalement pour gérer l'accès des administrateurs aux objets Identity Manager internes que sont les utilisateurs, les organisations et les capacités.

Les informations contenues dans cette section sont relatives aux rôles. Pour plus d'informations sur les rôles admin, voir la section "Comprendre et gérer les rôles admin" à la page 220.

Définition des rôles

Un rôle est un objet Identity Manager permettant de regrouper des droits d'accès aux ressources en vue de les assigner efficacement à des utilisateurs.

Les rôles sont organisés en quatre types :

- les rôles professionnels,
- les rôles informatiques,
- les applications,
- le matériel.

Les *rôles professionnels* permettent d'organiser en groupes les droits d'accès dont les personnes effectuant des tâches semblables au sein d'une organisation ont besoin dans l'exercice de leurs fonctions. En général, les rôles professionnels correspondent aux fonctions professionnelles des utilisateurs. Dans un établissement bancaire par exemple, les rôles professionnels peuvent correspondre à des fonctions financières telles que celles de guichetier, responsable des prêts, directeur de succursale, chargé de clientèle, comptable ou assistant administratif.

Les *rôles informatiques, applications* et *matériel* permettent d'organiser les habilitations de ressources en groupes. Pour fournir aux utilisateurs l'accès aux ressources, les rôles informatiques, les applications et le matériel sont assignés à des rôles professionnels, lesquels permettent aux utilisateurs d'accéder aux ressources dont ils ont besoin dans l'exercice de leurs fonctions. Les rôles informatiques contiennent un ensemble spécifique d'applications, matériel et/ou ressources, incluant des habilitations spécifiques pour ces ressources assignées. Les rôles informatiques peuvent aussi contenir d'autres rôles informatiques.

Remarque – Le concept de type de rôle est une nouveauté de la version Identity Manager 8.0. Si votre entreprise a effectué une mise à niveau vers la version 8.0 à partir d'une version antérieure d'Identity Manager, les rôles existants auront été importés sous forme de rôles informatiques. Pour plus d'informations, voir "Gestion des rôles créés dans des versions antérieures à la version 8.0." à la page 123.

Les rôles informatiques, les applications et le matériel peuvent être *obligatoires, conditionnels* ou *optionnels*.

- Tout rôle obligatoire est toujours assigné à l'utilisateur final.
- Dans le cas d'un rôle conditionnel, certaines conditions doivent être remplies pour que le rôle soit assigné.
- Un rôle optionnel peut être demandé séparément et, sous réserve d'approbation, assigné à l'utilisateur final.

Les rôles obligatoires, conditionnels et optionnels permettent à un concepteur de rôle professionnel de définir des droits d'accès génériques aux rôles contenus afin d'assurer la conformité aux réglementations, tout en laissant au responsable d'un utilisateur final la liberté d'adapter de manière plus précise les droits d'accès de l'utilisateur. Les utilisateurs auxquels des rôles conditionnels ou optionnels ont été assignés peuvent toujours partager les mêmes rôles professionnels assignés mais ont des droits d'accès assignés différents. Avec une telle approche, il devient inutile de définir un nouveau rôle professionnel à chaque permutation des besoins d'accès dans l'entreprise (problème connu sous le nom d'*explosion des rôles)*.

Pour un fonctionnement efficace des types de rôles

Les lignes suivantes expliquent comment utiliser efficacement les types de rôles. Pour la description des types de rôles, voir la section précédente.

Gestion des rôles créés dans des versions antérieures à la version 8.0.

Les organisations qui passent à la version 8.0 d'Identity Manager à partir d'une version précédente verront automatiquement leurs rôles existants convertis en rôles informatiques. Les rôles informatiques resteront directement assignés aux utilisateurs. Les rôles existants ne se verront pas assigner de propriétaire de rôle dans le cadre du processus de mise à niveau. Un propriétaire de rôle pourra cependant être assigné ultérieurement (pour toute information sur les propriétaires de rôles, voir "Désignation des propriétaires et approbateurs de rôles" à la page 134).

Par défaut, les organisations qui effectuent une mise à niveau vers la version 8.0 peuvent assigner directement des rôles informatiques et professionnels aux utilisateurs (voir Figure 5–2).

Les organisations qui ont des rôles existants doivent envisager de créer de nouveaux rôles en suivant les directives esquissées dans la section suivante.

Utilisation des types de rôles pour concevoir des rôles flexibles

Les rôles informatiques, les applications et le matériel sont les blocs fonctionnels du concepteur de rôles. Ces trois types de rôles sont utilisés en combinaison pour élaborer des habilitations utilisateur (ou *droits d'accès*). Les rôles informatiques, les applications et le matériel sont ensuite assignés à des rôles professionnels.

Conception de rôles professionnels

Dans Identity Manager, un utilisateur peut se voir assigner un, plusieurs ou aucun rôles. Avec l'introduction des types de rôles dans Identity Manager 8.0, il est recommandé de n'assigner directement aux utilisateurs que des rôles professionnels. En effet, par défaut, vous ne pouvez pas assigner directement d'autres types de rôles aux utilisateurs à moins que votre entreprise n'ait installé une version antérieure à la version 8.0 d'Identity Manager et effectué une mise à jour vers la version 8.0 minimum. Cette restriction par défaut peut être changée en modifiant l'objet Configuration de rôle ("Configuration des types de rôles " à la page 156, Configuration des types de rôles).

Pour réduire la complexité, les rôles professionnels ne peuvent pas être imbriqués. Autrement dit, un rôle professionnel ne peut pas contenir à son tour un rôle professionnel. De plus, les rôles professionnels ne peuvent pas contenir directement des ressources et des groupes de ressources. Les ressources et groupes de ressources doivent être assignés à un rôle informatique ou à une application, qui peut à son tour être assigné à un ou plusieurs rôles professionnels.

Conception de rôles informatiques

Les rôles informatiques peuvent contenir des applications, du matériel ainsi que d'autres rôles informatiques. Ils peuvent aussi contenir des ressources et des groupes de ressources.

Les rôles informatiques sont conçus pour être créés et gérés soit par le personnel informatique de votre entreprise soit par les propriétaires des ressources qui comprennent les habilitations requises pour activer des privilèges spécifiques au sein de la ressource.

Conception d'applications et de matériel

Les applications et le matériel sont des types de rôles conçus pour représenter des termes professionnels communément utilisés pour décrire des éléments dont les utilisateurs finaux ont besoin dans l'exercice de leurs fonctions. Par exemple, un rôle Application peut être nommé « Outils de support client » ou « Outil admin RH intranet ».

- Les applications ne peuvent pas contenir de rôles, mais peuvent contenir des ressources et des groupes de ressources. Elles peuvent également définir des habilitations spécifiques qui restreignent l'accès à des applications spécifiques sur les ressources contenues.
- Le matériel est (en règle générale) constitué de ressources non connectées et non numériques telles que des téléphones et des ordinateurs portables, exigeant un provisioning manuel. Par conséquent, le matériel ne peut pas contenir de rôles, de ressources ou de groupes de ressources.

Les applications et le matériel sont conçus pour être assignés à des rôles professionnels et des rôles informatiques.

Remarque –

Une ou plusieurs des capacités suivantes doivent être assignées aux administrateurs de rôles :

- Administrateur du matériel,
- Administrateur des applications,
- Administrateur des rôles professionnels,
- Administrateur des rôles informatiques.

Pour plus d'informations, voir "Assignation de capacités aux utilisateurs " à la page 219.

Récapitulatif des types de rôles

La figure suivante indique les types de rôles, ressources et groupes de ressources qui peuvent être assignés à chacun des quatre types de rôles. Elle indique aussi les exclusions de type de rôles pouvant être assignées aux quatre types de rôles (pour la description des exclusions de rôles, voir "Pour assigner des ressources et groupes de ressources" à la page 129).

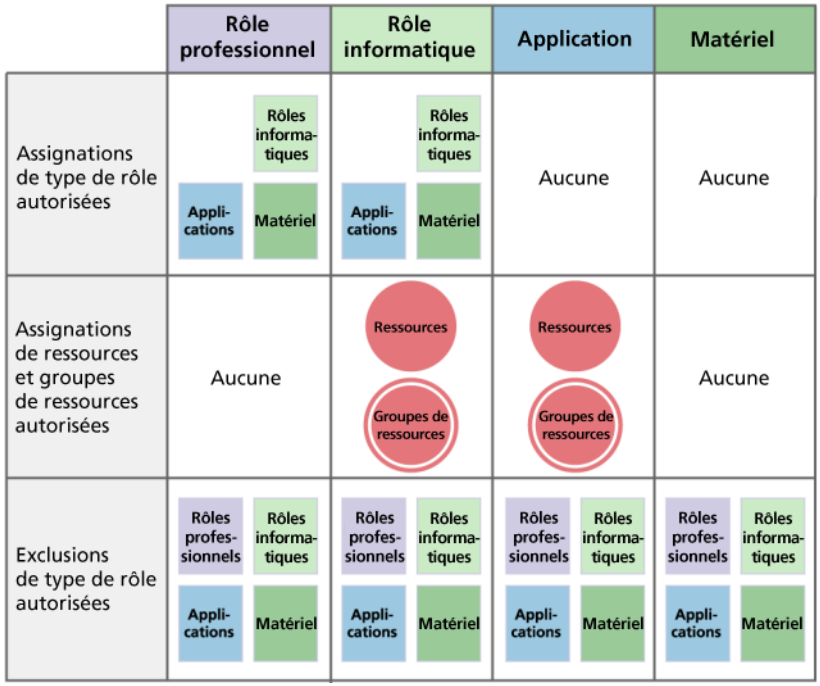


FIGURE 5–1 Les types de rôles Rôle professionnel, Rôle informatique, Application et Matériel

Les rôles contenus optionnels, conditionnels et obligatoires ("Définition des rôles" à la page 121) accroissent la flexibilité. Les définitions de rôle flexibles peuvent réduire le nombre total de rôles que l'entreprise sera amenée à gérer.

La Figure 5–2 montre que les rôles professionnels et informatiques peuvent être directement assignés aux utilisateurs si une version antérieure à la version 8.0 d'Identity Manager est mise à niveau vers la version 8.0 minimum. Lors de la mise à niveau, les rôles existants sont convertis en rôles informatiques, lesquels pour assurer la compatibilité ascendante sont directement assignés aux utilisateurs. Si Identity Manager n'a pas été mis à niveau à partir d'une version antérieure à la 8.0, seuls les rôles professionnels sont directement assignés aux utilisateurs.

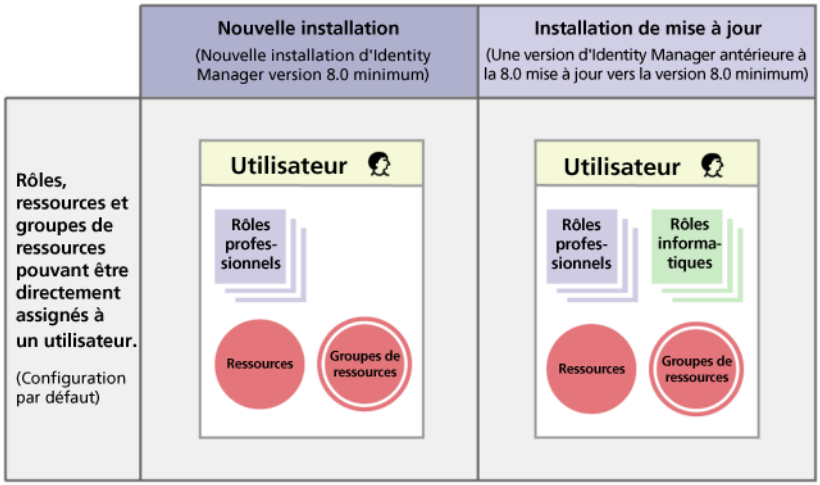


FIGURE 5–2 Rôles et ressources pouvant être directement assignés aux utilisateurs.

Création de rôles

Cette section décrit la création des rôles. Ces informations sont organisées de la manière suivante :

- “Pour créer des rôles en utilisant le formulaire Créer un rôle” à la page 126 ;
- “Pour assigner des ressources et groupes de ressources” à la page 129 ;
- “Pour éditer des valeurs d'attributs de ressources assignées” à la page 130 ;
- “Pour assigner des rôles et des exclusions de rôles” à la page 132 ;
- “Désignation des propriétaires et approbateurs de rôles” à la page 134 ;
- “Désignation de notifications” à la page 136.
- “Lancement d'éléments de travail d'approbation de changement et d'approbation” à la page 137

Remarque – Pour des conseils en matière de conception de rôles, reportez-vous à “Utilisation des types de rôles pour concevoir des rôles flexibles” à la page 123.

Lorsque vous créez ou éditez un rôle, Identity Manager lance le flux de travaux `ManageRole`. Ce flux de travaux enregistre le rôle nouveau ou mis à jour dans le référentiel et vous permet d'insérer des approbations ou d'autres actions avant la création ou l'enregistrement du rôle.

▼ Pour créer des rôles en utilisant le formulaire Créer un rôle

1 Dans l'interface administrateur, cliquez sur Rôles dans le menu principal.

La page Rôles (onglet Lister les rôles) s'ouvre.

2 **Cliquez sur Nouveau au bas de cette page.**

La page Créer Rôle informatique s'ouvre. Pour créer un autre type de rôle, utilisez le menu déroulant Type.

3 **Remplissez les champs du formulaire sur l'onglet Identité.**

La figure suivante illustre l'onglet Identité.

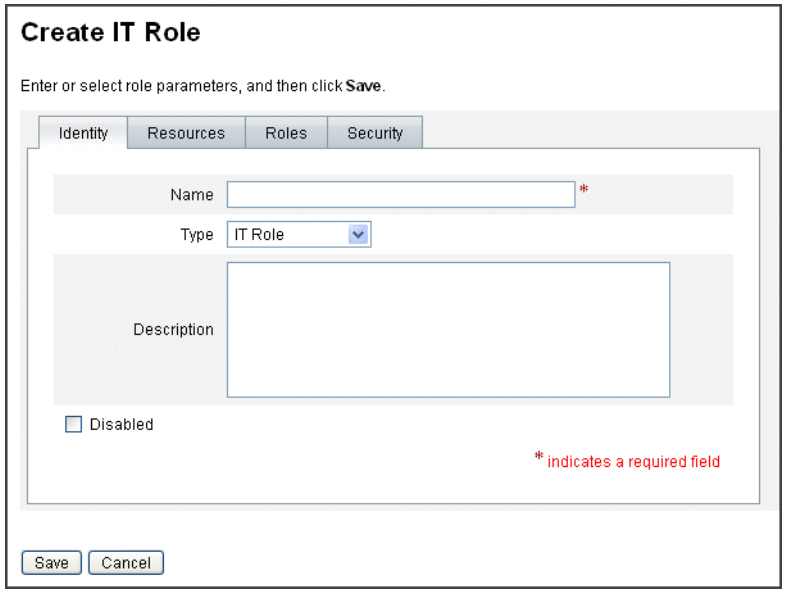


FIGURE 5–3 L'onglet Identité de la page Créer Rôle informatique

4 **Remplissez les champs du formulaire dans l'onglet Ressources (le cas échéant). Si vous avez besoin d'aide pour remplir les champs de cet onglet, consultez l'aide en ligne ainsi que la section "Pour assigner des ressources et groupes de ressources" à la page 129.**

Si vous avez besoin d'aide pour définir les valeurs des attributs étendus sur les rôles, reportez-vous à "Pour afficher ou éditer les attributs des comptes de ressources" à la page 170.

La figure suivante illustre l'onglet Ressources.

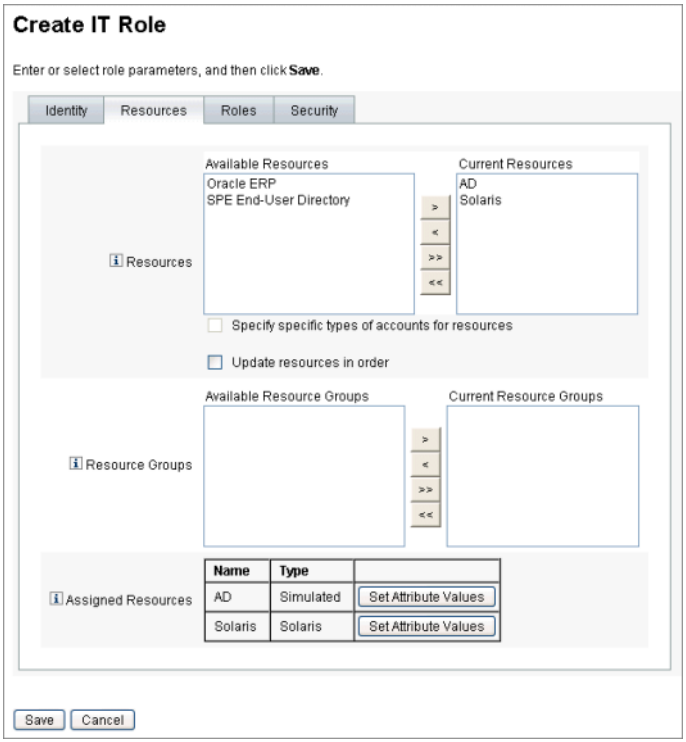


FIGURE 5–4 L'onglet Ressources de la page Créer Rôle informatique

5 **Remplissez les champs du formulaire sur l'onglet Rôles (le cas échéant). Si vous avez besoin d'aide pour remplir les champs de cet onglet, consultez l'aide en ligne ainsi que la section "Pour assigner des rôles et des exclusions de rôles" à la page 132.**

La Figure 5–6 illustre l'onglet Rôles.

6 **Remplissez les champs du formulaire sur l'onglet Sécurité. Si vous avez besoin d'aide pour remplir les champs de cet onglet, consultez l'aide en ligne ainsi que la section "Désignation des propriétaires et approbateurs de rôles" à la page 134 et la section "Désignation de notifications" à la page 136.**

"Désignation des propriétaires et approbateurs de rôles" à la page 134 affiche l'onglet Sécurité.

7 **Cliquez sur Enregistrer au bas de cette page.**

8 **Saisissez un nom de rôle et une description dans l'onglet Identité du formulaire Créer un rôle. Si vous créez un nouveau rôle, utilisez le menu déroulant Type afin de sélectionner le type de rôle à créer.**

La Figure 5–4 représente la partie Identité de l'onglet Identité du formulaire Créer un rôle. Si vous avez besoin d'aide pour utiliser ce formulaire, reportez-vous à l'aide en ligne.

▼ Pour assigner des ressources et groupes de ressources

Les ressources et groupes de ressources peuvent être assignés directement à des rôles informatiques et des rôles applications en utilisant l'onglet Ressources du formulaire Créer un rôle. Les ressources sont décrites plus loin dans la section "Comprendre et gérer les ressources Identity Manager externes" à la page 160. Les groupes de ressources sont décrits dans la section "Groupes de ressources" à la page 171.

- Il est impossible d'assigner directement des ressources et groupes de ressources à des rôles professionnels, car les rôles professionnels ne peuvent se voir assigner que des rôles.
- Il est impossible d'assigner des ressources et des groupes de ressources à des rôles de type Matériel, car ceux-ci sont réservés aux ressources non connectées ou non numériques nécessitant un provisioning manuel.

Cette procédure décrit l'assignation des ressources et groupes de ressources à un rôle lors du remplissage du formulaire Créer un rôle. Pour le démarrage, voir "Pour créer des rôles en utilisant le formulaire Créer un rôle" à la page 126.

1. **Cliquez sur l'onglet Ressources sur la page Créer un rôle.**
2. **Pour assigner une ressource, sélectionnez-la dans la colonne Ressources disponibles et déplacez-la dans la colonne Ressources actuelles en cliquant sur les touches fléchées.**
3. **Si vous assignez plusieurs ressources, vous pouvez définir l'ordre dans lequel celles-ci seront mises à jour : cochez la case Mettre ressources à jour en ordre et utilisez les boutons + et - pour changer l'ordre des ressources dans la colonne Ressources actuelles.**
4. **Pour assigner un groupe de ressources à ce rôle, sélectionnez-le dans la colonne Groupes de ressources disponibles et déplacez-le dans la colonne Groupes de ressources actuels en cliquant sur les touches fléchées. Un groupe de ressources est un ensemble de ressources offrant un autre moyen de spécifier l'ordre dans lequel les comptes de ressources sont créés et mis à jour.**
5. **Pour définir les attributs de compte s'appliquant à ce rôle par ressource, cliquez sur Définir des valeurs d'attribut dans la section Ressources assignées. Pour plus d'informations, voir "Pour afficher ou éditer les attributs des comptes de ressources" à la page 170.**
6. **Cliquez sur Enregistrer pour enregistrer le rôle ou sur les onglets Identité, Rôles ou Sécurité pour poursuivre le processus de création de rôle.**

   La figure suivante représente l'onglet Ressources du formulaire Créer un rôle.

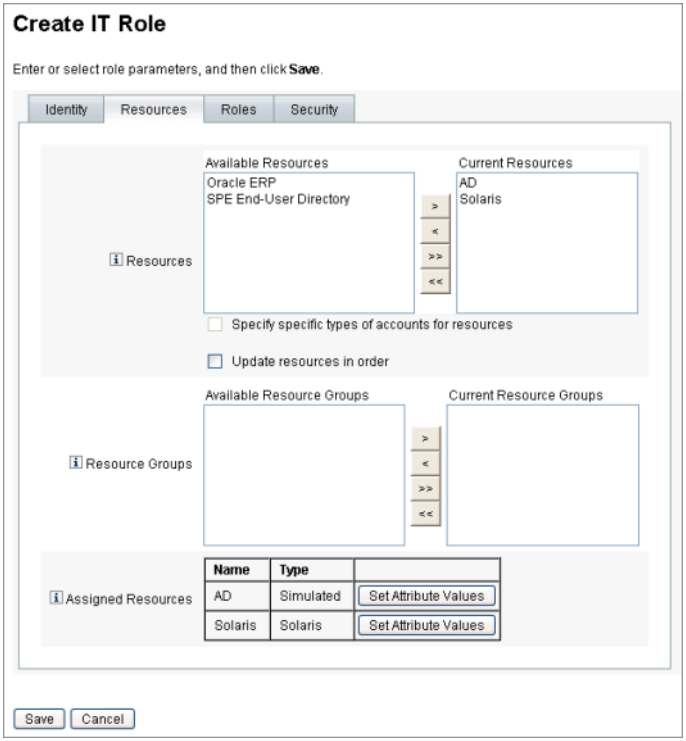
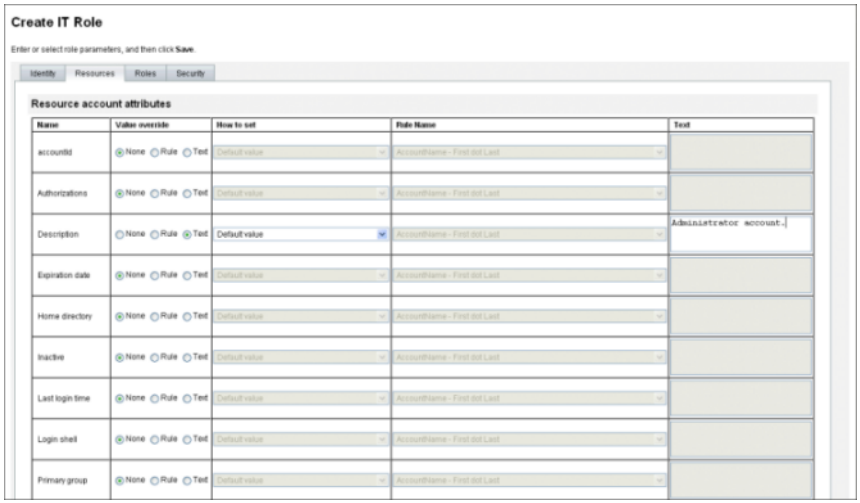


FIGURE 5–5 La section Ressources du formulaire à onglets Créer un rôle

▼ Pour éditer des valeurs d'attributs de ressources assignées

Utilisez le tableau Ressources assignées pour définir ou modifier les valeurs d'attributs de ressources sur des ressources assignées à un rôle. Une ressource peut avoir différentes valeurs d'attributs définies par rôle. Cliquer sur le bouton Définir des valeurs d'attribut ouvre la page Attributs de compte de ressources.

La figure suivante représente la page Attributs de compte de ressources qui est utilisée pour définir les valeurs des attributs étendus sur les ressources assignées à un rôle.



1 **Depuis la page Attributs de compte de ressources, spécifiez les nouvelles valeurs de chaque attribut et déterminez la façon dont sont définies les valeurs des attributs.**

Identity Manager vous permet de définir directement les valeurs ou d'utiliser une règle pour définir les valeurs et fournit toute une gamme d'options pour ignorer les valeurs existantes ou fusionner les valeurs avec les valeurs existantes. Pour toute information d'ordre général sur les valeurs des attributs de ressource, reportez-vous à "Pour afficher ou éditer les attributs des comptes de ressources" à la page 170.

Utilisez les options suivantes pour fixer les valeurs des différents attributs de compte de ressource :

- **Annuler valeur**. Choisissez l'une des options suivantes :
  - **Aucun** *(par défaut)*. Aucune valeur n'est établie.
  - **Règle**. Utilise une règle pour définir la valeur.

    Si vous sélectionnez cette option, vous devez sélectionner le nom d'une règle dans la liste.
  - **Texte**. Utilise le texte spécifié pour définir la valeur.

    Si vous sélectionnez cette option, vous devez saisir le texte dans le champ Texte adjacent.
- **Comment définir**. Choisissez l'une des options suivantes :
  - **Valeur par défaut**. Définit la règle ou le texte comme valeur d'attribut par défaut.

    L'utilisateur peut modifier ou annuler cette valeur.
  - **Définir sur la valeur**. Définit la valeur d'attribut conformément à la spécification de la règle ou du texte.

    La valeur ainsi définie remplace toute modification apportée par un utilisateur.
  - **Fusionner avec la valeur**. Permet de fusionner la valeur d'attribut actuelle avec les valeurs spécifiées par la règle ou le texte.

- **Fusionner avec la valeur, supprimer cet existant**. Supprime les valeurs d'attribut actuelles et définit la valeur sur une fusion des valeurs spécifiées par ce rôle et les autres rôles assignés.
- **Supprimer de la valeur**. Supprime de la valeur d'attribut la valeur spécifiée par la règle ou le texte.
- **Déterminer à la valeur par voie d'autorité**. Définit la valeur de l'attribut conformément à la spécification de la règle ou du texte.

  La valeur ainsi définie remplace toute modification apportée par un utilisateur. Si vous supprimez le rôle, la nouvelle valeur est NULL, même s'il existait précédemment sur cet attribut.
- **Fusionner avec la valeur par voie d'autorité**. Permet de fusionner la valeur d'attribut actuelle avec les valeurs spécifiées par la règle ou le texte.

  La suppression du rôle supprime la valeur qui avait été assignée à l'assignation du rôle et laisse telle quelle la valeur originale de l'attribut.
- **Fusionner avec la valeur par voie d'autorité, supprimer cet existant**. Supprime les valeurs d'attribut actuelles et définit la valeur sur une fusion des valeurs spécifiées par ce rôle et les autres rôles assignés.

  Supprime la valeur d'attribut spécifiée par ce rôle si le rôle est supprimé, même s'il existait précédemment sur l'attribut.

- **Nom de la règle**. Si vous sélectionnez Règle dans la zone Annuler valeur, sélectionnez une règle dans la liste.
- **Texte**. Si vous sélectionnez Texte dans la zone Annuler valeur, saisissez le texte à ajouter ou à supprimer de la valeur de l'attribut, ou à utiliser comme valeur d'attribut.

2 Cliquez sur OK pour enregistrer vos modifications et retourner à la page Créer ou Éditer un rôle.

▼ Pour assigner des rôles et des exclusions de rôles

Des rôles peuvent être assignés à des rôles professionnels et informatiques via l'onglet Rôles du formulaire Créer un rôle. Les rôles assignés doivent être ajoutés au tableau Rôles contenus.

- Il est impossible d'assigner des rôles à des rôles de type Application et Matériel.
- Les rôles professionnels ne peuvent être assignés à aucun type de rôle.

Des exclusions de rôles peuvent être assignées à l'ensemble des quatre types de rôles en utilisant l'onglet Rôles du formulaire Créer un rôle. Si un rôle présentant une exclusion de rôle est assigné à un utilisateur, le rôle exclu ne peut pas être assigné à l'utilisateur. Les exclusions de rôles doivent être ajoutées au tableau Exclusions de rôles.

Cette procédure décrit l'assignation de un ou plusieurs rôles à un rôle lors du remplissage du formulaire Créer un rôle. Pour le démarrage, voir "Pour créer des rôles en utilisant le formulaire Créer un rôle" à la page 126.

Pour remplir l'onglet Rôles

1. **Cliquez sur l'onglet Rôles sur la page Créer un rôle.**

2. **Cliquez sur Ajouter dans la section Rôles contenus.**

   L'onglet est actualisé et affiche le formulaire Rechercher rôles à contenir.

3. **Recherchez le ou les rôles que vous assignerez à ce rôle. Commencez par les rôles *obligatoires* (vous ajouterez les rôles conditionnels et optionnels ultérieurement).**

   Si vous avez besoin d'aide pour remplir le formulaire de recherche, reportez-vous à "Pour rechercher des rôles" à la page 138. Les rôles professionnels ne peuvent être imbriqués ni assignés à d'autres types de rôles.

4. **Utilisez les cases à cocher pour sélectionner un ou plusieurs rôles à assigner puis cliquez sur Ajouter.**

   L'onglet est actualisé et affiche le formulaire Ajouter un rôle contenu.

5. **Sélectionnez Obligatoire (ou Conditionnel ou Optionnel selon le cas) dans le menu déroulant Type d'association.**

   Cliquez sur OK.

6. **Répétez les quatre étapes précédentes pour ajouter des rôles conditionnels (le cas échéant). Répétez les quatre étapes précédentes pour ajouter des rôles optionnels (le cas échéant).**

7. **Cliquez sur Enregistrer pour enregistrer le rôle ou sur les onglets Identité, Ressources ou Sécurité pour poursuivre le processus de création de rôle.**

   La Figure 5–6 représente l'onglet Rôles du formulaire Créer un rôle. Si vous avez besoin d'aide pour ce formulaire, reportez-vous à l'aide en ligne.

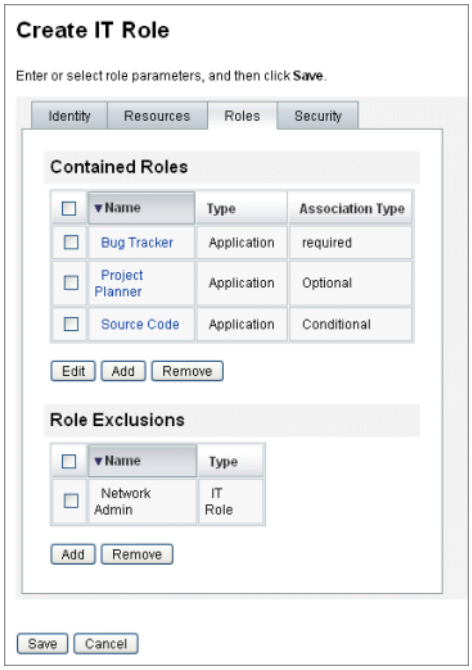


FIGURE 5–6 La section Rôles du formulaire à onglets Créer un rôle

Désignation des propriétaires et approbateurs de rôles

Les rôles ont des *propriétaires* et des *approbateurs* désignés. Seuls les propriétaires d'un rôle peuvent autoriser l'apport de modifications aux paramètres définissant un rôle tandis que seuls les approbateurs d'un rôle peuvent autoriser l'assignation de ce rôle aux utilisateurs finaux.

Remarque – Si Identity Manager est intégré avec Sun™ Role Manager, vous devez autoriser Role Manager à gérer l'ensemble des approbations et notifications de changement de rôle en désactivant manuellement la capacité d'Identity Manager d'effectuer ces actions.

Vous devez éditer l'objet Configuration `RoleConfiguration` dans Identity Manager comme suit :

- Trouvez toutes les instances de `changeApproval` et définissez la valeur sur **`false`**.
- Trouvez toutes les instances de `changeNotification` et définissez la valeur sur **`false`**.

Être le propriétaire d'un rôle revient à être le propriétaire professionnel responsable des droits des comptes de ressources sous-jacents qui sont assignés par le biais de ce rôle. Si un administrateur modifie un rôle, le propriétaire du rôle doit approuver les changements pour qu'ils puissent être appliqués. Cette fonction permet d'empêcher un administrateur de modifier

un rôle sans que le propriétaire professionnel du rôle ne le sache et n'y consente. Cependant, si les approbations de changement ont été désactivées dans l'objet Configuration du rôle, l'approbation du propriétaire du rôle n'est pas nécessaire pour appliquer les changements.

Outre pour les changements de rôle, l'approbation du propriétaire est nécessaire pour activer, désactiver ou supprimer un rôle.

Les propriétaires et approbateurs peuvent indifféremment être ajoutés directement à un rôle ou l'être dynamiquement en utilisant une règle d'assignation de rôle. Dans Identity Manager, il est possible (même si cela n'est pas recommandé) de créer des rôles sans propriétaire ni approbateur.

Remarque – Les règles d'assignation de rôles ont pour `authType` `RoleUserRule`.

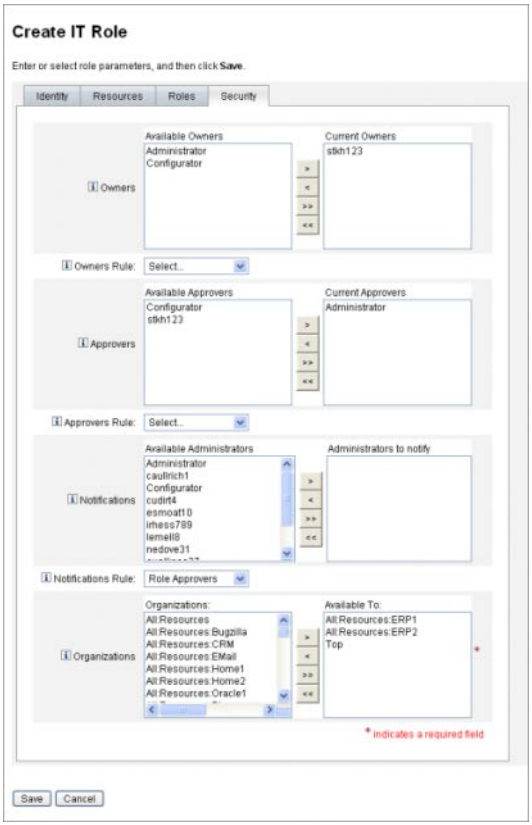
Si vous devez créer une règle d'assignation de rôles personnalisée, reportez-vous aux trois objets de règle d'assignation de rôles et utilisez-les comme un exemple :

- approbateurs de rôles,
- notifications de rôle,
- propriétaires de rôles.

Les propriétaires et les approbateurs sont avertis par e-mail si un élément de travail requiert leur approbation. Les éléments de travail de type approbation de changement et approbation sont examinés dans la section “Lancement d'éléments de travail d'approbation de changement et d'approbation” à la page 137.

Les propriétaires et les approbateurs sont ajoutés aux rôles sur l'onglet Sécurité dans le formulaire Créer un rôle.

“Désignation des propriétaires et approbateurs de rôles” à la page 134 montre l'onglet Sécurité du formulaire Créer un rôle. Si vous avez besoin d'aide pour ce formulaire, reportez-vous à l'aide en ligne.



Désignation de notifications

Un ou plusieurs administrateurs peuvent recevoir des notifications lorsqu'un rôle est assigné à un utilisateur.

La spécification d'un destinataire des notifications est optionnelle. Vous pouvez choisir d'avertir un administrateur si vous décidez de ne pas exiger d'approbation quand un rôle est assigné à un utilisateur. Vous pouvez aussi désigner un administrateur qui servira d'approbateur et un autre administrateur qui servira de destinataire des notifications une fois l'approbation effectuée.

Comme avec les propriétaires et approbateurs, les notifications peuvent indifféremment être ajoutées directement à un rôle ou l'être dynamiquement en utilisant une règle d'assignation de rôle. Les destinataires des notifications sont avertis par e-mail quand un rôle est assigné à un utilisateur. Aucun élément de travail n'est toutefois créé puisqu'aucune approbation n'est nécessaire.

Les notifications sont assignées aux rôles dans l'onglet Sécurité du formulaire Créer un rôle. "Désignation des propriétaires et approbateurs de rôles" à la page 134 montre l'onglet Sécurité du formulaire Créer un rôle.

Lancement d'éléments de travail d'approbation de changement et d'approbation

Lorsque des changements sont apportés à un rôle, les propriétaires de ce rôle peuvent recevoir un e-mail d'*approbation de changement*, un e-mail de *notification de changement* ou ne pas recevoir d'e-mail du tout. Lorsqu'un rôle est assigné à un utilisateur, les approbateurs de rôles reçoivent des e-mails d'*approbation* de rôle.

Par défaut, les propriétaires de rôles reçoivent des e-mails approbation de changement à chaque fois que les rôles dont ils sont propriétaires changent. Ce comportement peut cependant être configuré par type de rôle. Par exemple, vous pouvez choisir d'activer les approbations de changement pour les rôles professionnels et informatiques, et d'activer les notifications de changement pour les rôles applications et matériel.

Pour les instructions à suivre pour activer et désactiver les e-mails d'approbation de changement et de notification de changement, reportez-vous à “Configuration des types de rôles ” à la page 156.

Le fonctionnement des approbations et notifications de changement est le suivant :

- Si les *approbations de changement* sont activées lorsqu'un administrateur modifie un rôle, un élément de travail est généré et un e-mail d'approbation est envoyé au propriétaire du rôle. Le propriétaire du rôle doit approuver l'élément de travail pour que le changement soit appliqué. Les éléments de travail d'approbation de changement peuvent être délégués. Pour plus d’informations, voir “Approbation des comptes utilisateur” à la page 238.

  Si les approbations de changement sont désactivées, aucun élément de travail n'est généré et aucun e-mail d'approbation n'est envoyé au propriétaire du rôle.
- Si les *notifications de changement* sont activées lorsqu'un administrateur modifie un rôle, le changement est immédiatement appliqué et un e-mail de notification est envoyé au propriétaire du rôle.

  Si les notifications de changement sont désactivées, aucune notification n'est envoyée au propriétaire du rôle.

Lorsqu'un rôle est assigné à un utilisateur, les approbateurs de rôles reçoivent des e-mails d'*approbation* de rôle. Les e-mails d'approbation de rôle ne peuvent pas être désactivés dans Identity Manager.

Pour les approbations de rôle, un élément de travail est généré lorsqu'un rôle est assigné à un utilisateur et un e-mail d'approbation est envoyé à l'approbateur du rôle. L'approbateur d'un rôle doit approuver l'élément de travail pour que le rôle soit assigné à l'utilisateur.

Les éléments de travail d'approbation de changement et d'approbation peuvent être délégués. Pour plus d'informations sur la délégation des éléments de travail, voir “Délégation des éléments de travail” à la page 234.

Édition et gestion des rôles

La plupart des tâches d'édition et de gestion de rôles peuvent être effectuées en utilisant les onglets Rechercher des rôles et Lister les rôles, qui se trouvent sous l'onglet Rôles dans le menu principal.

Cette section se compose des rubriques suivantes :

▼ Pour rechercher des rôles

Utilisez l'onglet Rechercher des rôles pour rechercher des rôles remplissant les critères spécifiés.

L'onglet Rechercher des rôles permet de rechercher des rôles en fonction d'un vaste éventail de critères tels que les propriétaires et approbateurs des rôles, les types de comptes assignés, les rôles contenus, etc.

Pour toute information sur la recherche d'utilisateurs assignés à un rôle, reportez-vous à "Pour rechercher des utilisateurs assignés à un rôle spécifique" à la page 154.

1 Dans l'interface administrateur, cliquez sur l'onglet Rôles.

L'onglet Lister les rôles s'ouvre.

2 Cliquez sur l'onglet secondaire Rechercher des rôles.

La Figure 5–7 illustre l'onglet Rechercher des rôles. Si vous avez besoin d'aide pour ce formulaire, reportez-vous à l'aide en ligne.

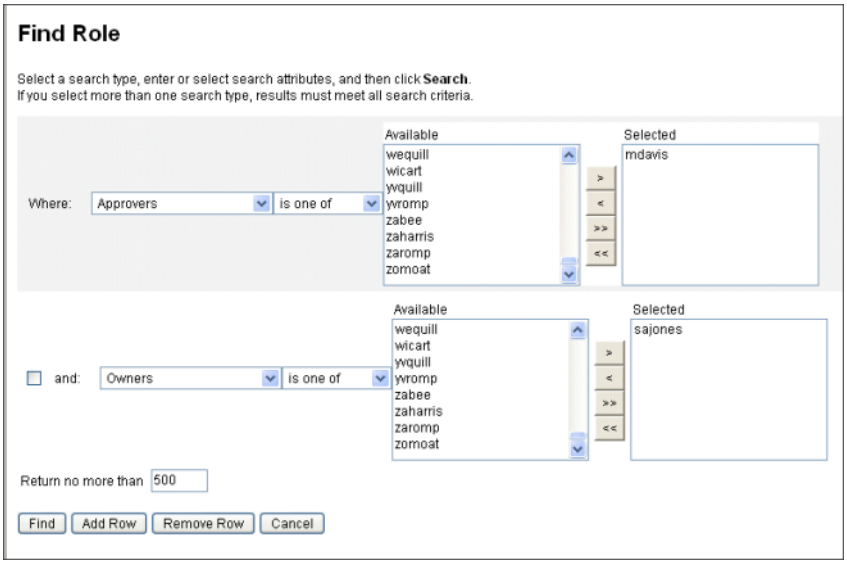


FIGURE 5–7 L'onglet Rechercher des rôles

Utilisez les menus déroulants pour définir les paramètres pour votre recherche. Cliquez sur le bouton Ajouter une ligne pour ajouter des paramètres supplémentaires.

▼ Pour afficher des rôles

Utilisez l'onglet Lister les rôles pour afficher les rôles. Utilisez les champs de filtre dans le haut de la page Lister les rôles pour rechercher des rôles par nom ou type de rôle. Le filtrage n'est pas sensible à la casse.

- **Dans l'interface administrateur, cliquez sur l'onglet Rôles.**

  Le sous-onglet Lister les rôles s'ouvre.

  La Figure 5–8 illustre l'onglet Lister les rôles. Si vous avez besoin d'aide pour ce formulaire, reportez-vous à l'aide en ligne.

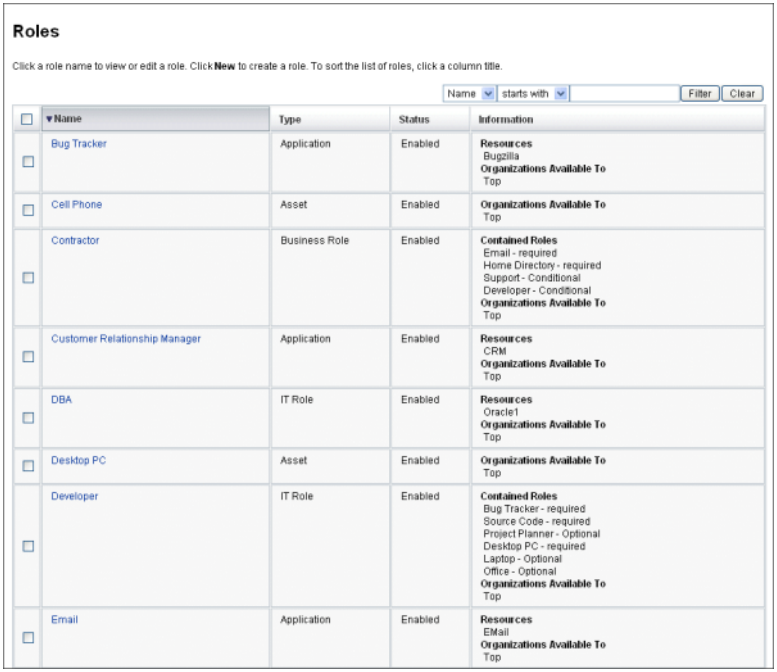


FIGURE 5–8 L'onglet Lister les rôles

▼ Pour éditer un rôle

Recherchez les rôles à éditer en utilisant l'onglet Lister les rôles ou l'onglet Rechercher des rôles. Si vous apportez des changements à un rôle et que les approbations de changement sont définies sur true, le propriétaire de ce rôle doit approuver les changements effectués pour qu'ils puissent entrer en vigueur.

Pour toute information sur la mise à jour des utilisateurs avec les changements de rôle, reportez-vous à "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.

1. **Recherchez le rôle à éditer en suivant les instructions de la section "Pour rechercher des rôles" à la page 138 ou "Pour afficher des rôles" à la page 139.**

2. **Cliquez sur le nom du rôle à éditer.**

   La page Éditer un rôle s'ouvre.

3. **Éditez le rôle comme nécessaire. Pour toute aide pour remplir les onglets Identité, Ressources, Rôles et Sécurité, reportez-vous à "Pour créer des rôles en utilisant le formulaire Créer un rôle" à la page 126.**

   Cliquez sur Enregistrer. La page Confirmer les changements de rôle s'ouvre.

4. **Si ce rôle est assigné à des utilisateurs, vous pouvez sélectionner quand mettre à jour les utilisateurs avec les changements de rôle. Pour plus d'informations, voir "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.**

5. **Cliquez sur Enregistrer pour enregistrer vos modifications.**

▼ Pour cloner un rôle

1. **Recherchez le rôle que vous voulez éditer en suivant les instructions de la section "Pour rechercher des rôles" à la page 138 ou celles de la section "Pour afficher des rôles" à la page 139.**

2. **Cliquez sur le nom du rôle à cloner.**

   La page Éditer un rôle s'ouvre.

3. **Entrez un nouveau nom dans le champ Nom et cliquez sur Enregistrer.**

   Page Rôle : Créer ou Renommer ? s'ouvre.

4. **Cliquez sur Créer pour faire une copie du rôle.**

▼ Pour assigner un rôle à un autre rôle

Les exigences d'Identity Manager en matière d'assignation de rôles sont détaillées dans les sections "Définition des rôles" à la page 121 et "Pour un fonctionnement efficace des types de rôles " à la page 123. Vous devez prendre connaissance de ces informations avant d'assigner des rôles.

Identity Manager peut modifier les assignations de rôles à un rôle sur approbation du propriétaire du rôle parent.

1. **Recherchez le rôle professionnel ou informatique auquel vous assignerez un ou plusieurs rôles *contenus* (les rôles peuvent uniquement être assignés aux rôles professionnels et informatiques). Utilisez les instructions de la section "Pour rechercher des rôles" à la page 138 ou de "Pour afficher des rôles" à la page 139 pour rechercher des rôles.**

2. **Cliquez sur le rôle professionnel ou informatique de votre choix pour l'ouvrir.**

   La page Éditer un rôle s'ouvre.

3. **Cliquez sur l'onglet Rôles sur la page Éditer un rôle.**

4. **Cliquez sur Ajouter dans la section Rôles contenus.**

   L'onglet est actualisé et affiche le formulaire Rechercher rôles à contenir.

5 **Recherchez le ou les rôles que vous assignerez à ce rôle. Commencez par les éventuels rôles *obligatoires* (vous ajouterez les rôles conditionnels et optionnels ultérieurement).**

Si vous avez besoin d'aide pour remplir le formulaire de recherche, reportez-vous à "Pour rechercher des rôles" à la page 138. Les rôles professionnels ne peuvent pas être imbriqués ni assignés à d'autres types de rôles.

6 **Utilisez les cases à cocher pour sélectionner un ou plusieurs rôles à assigner puis cliquez sur Ajouter.**

L'onglet est actualisé et affiche le formulaire Ajouter un rôle contenu.

7 **Sélectionnez Obligatoire (ou Conditionnel ou Optionnel selon le cas) dans le menu déroulant Type d'association.**

Cliquez sur OK.

8 **Répétez les quatre étapes précédentes pour ajouter des rôles conditionnels (le cas échéant). Répétez de nouveau les quatre étapes précédentes pour ajouter des rôles optionnels (le cas échéant).**

9 **Cliquez sur Enregistrer pour ouvrir la page Confirmer les changements de rôle.**

La page Confirmer les changements de rôle s'ouvre.

10 **Dans la section Mettre à jour les utilisateurs assignés, sélectionnez une option du menu Mettre à jour les utilisateurs assignés puis cliquez sur Enregistrer pour enregistrer vos assignations de rôle.**

Pour plus d'informations, voir "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.

▼ Pour supprimer un rôle assigné à un autre rôle

Identity Manager peut supprimer un rôle contenu dans un autre rôle sur approbation du propriétaire du rôle parent. Le rôle supprimé sera supprimé des utilisateurs lorsque ceux-ci recevront les mises à jour de rôles (pour plus d'informations, voir "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149). Une fois le rôle supprimé, les utilisateurs perdent les habilitations qui y étaient associées.

- Pour toute information sur la suppression d'un rôle assigné à un ou plusieurs utilisateurs, reportez-vous à "Pour supprimer un ou plusieurs rôles d'un utilisateur" à la page 155.
- Pour toute information sur la désactivation d'un rôle, reportez-vous à "Pour activer et désactiver des rôles" à la page 143.
- Pour toute information sur la suppression d'un rôle d'Identity Manager, reportez-vous à "Pour supprimer un rôle" à la page 144.

1. **Recherchez le rôle professionnel ou informatique duquel vous voulez supprimer un rôle. Utilisez les instructions de la section "Pour rechercher des rôles" à la page 138 ou de "Pour afficher des rôles" à la page 139 pour rechercher des rôles.**

2. **Cliquez sur le rôle de votre choix pour l'ouvrir.**

   La page Éditer un rôle s'ouvre.

3. **Cliquez sur l'onglet Rôles sur la page Éditer un rôle.**

4. **Dans la section Rôles contenus, sélectionnez la case à cocher en regard du rôle à supprimer puis cliquez sur Supprimer. Pour supprimer plusieurs rôles, sélectionnez plusieurs cases à cocher.**

   Le tableau est mis à jour de façon à indiquer les rôles contenus restants.

5. **Cliquez sur Enregistrer.**

   La page Confirmer les changements de rôle s'ouvre.

6. **Dans la section Mettre à jour les utilisateurs assignés, sélectionnez une option du menu Mettre à jour les utilisateurs assignés. Pour plus d'informations, voir "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.**

7. **Cliquez sur Enregistrer pour terminer vos modifications.**

▼ Pour activer et désactiver des rôles

Les rôles peuvent être activés et désactivés sur l'onglet Lister les rôles. Le statut des rôles est affiché dans la colonne Statut. Cliquez sur l'en-tête de colonne Statut pour trier le tableau par statut de rôle.

Les rôles désactivés ne figurent pas sous l'onglet Rôles du formulaire Créer un/Éditer l'utilisateur et ne peuvent pas être assignés directement à des utilisateurs. Les rôles contenant des rôles désactivés peuvent être assignés à des utilisateurs, ce qui n'est pas le cas des rôles désactivés.

Les utilisateurs dont les rôles assignés sont par la suite désactivés ne perdent pas leurs habilitations. La désactivation d'un rôle bloque uniquement la création des *futures assignations de rôle*.

La désactivation et la réactivation d'un rôle nécessitent l'autorisation de son propriétaire.

Lors de l'activation ou de la désactivation d'un rôle ayant des utilisateurs assignés, Identity Manager vous invite à mettre à jour ces utilisateurs. Pour toute information, reportez-vous à "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.

1. **Recherchez le rôle à supprimer en suivant les instructions de la section "Pour rechercher des rôles" à la page 138 ou celles de la section "Pour afficher des rôles" à la page 139.**

2 **Cliquez sur les cases à cocher en regard des rôles à activer ou désactiver.**

3 **Cliquez sur Activer ou Désactiver au bas du tableau Rôles.**

La page de confirmation Activer le rôle ou Désactiver le rôle s'ouvre.

4 **Cliquez sur OK pour activer ou désactiver le rôle.**

▼ Pour supprimer un rôle

Cette section explique la procédure à suivre pour supprimer un rôle d'Identity Manager.

- Pour toute information sur la suppression d'un rôle assigné à un autre rôle, reportez-vous à "Pour supprimer un rôle assigné à un autre rôle" à la page 142.
- Pour toute information sur la suppression d'un rôle assigné à un ou plusieurs utilisateurs, reportez-vous à "Pour supprimer un ou plusieurs rôles d'un utilisateur" à la page 155.

Si vous supprimez un rôle actuellement assigné à un utilisateur, Identity Manager bloque la suppression lorsque vous tentez d'enregistrer le rôle. Vous devez annuler l'assignation de (ou réassigner) tous les utilisateurs associés à un rôle pour qu'Identity Manager puisse le supprimer. Vous devez également supprimer ce rôle des autres rôles dont il fait partie.

Identity Manager requiert l'approbation du propriétaire d'un rôle avant de supprimer ce dernier.

1 **Recherchez le rôle à supprimer en suivant les instructions de la section "Pour rechercher des rôles" à la page 138 ou "Pour afficher des rôles" à la page 139.**

2 **Sélectionnez la case à cocher en regard de chacun des rôles à supprimer.**

3 **Cliquez sur Supprimer.**

La page de confirmation Supprimer un rôle s'affiche.

4 **Cliquez sur OK pour supprimer un ou plusieurs rôles.**

▼ Pour assigner une ressource ou un groupe de ressources à un rôle

Les exigences d'Identity Manager en matière d'assignation de ressources et groupes de ressources sont décrites dans les sections "Définition des rôles" à la page 121 et "Pour un fonctionnement efficace des types de rôles " à la page 123. Vous devez prendre connaissance de ces informations avant d'assigner des ressources aux rôles.

Identity Manager peut modifier les assignations de ressources et de groupes de ressources d'un rôle sur approbation du propriétaire du rôle.

1. **Recherchez le rôle professionnel ou informatique auquel vous voulez ajouter une ressource ou un groupe de ressources. Pour les instructions à suivre pour rechercher un rôle, reportez-vous à "Pour rechercher des rôles" à la page 138 ou à "Pour afficher des rôles" à la page 139.**

2. **Cliquez sur le rôle de votre choix pour l'ouvrir.**

3. **Cliquez sur l'onglet Ressources sur la page Éditer un rôle.**

4. **Pour assigner une ressource, sélectionnez-la dans la colonne Ressources disponibles et déplacez-la dans la colonne Ressources actuelles en cliquant sur les touches fléchées.**

5. **Si vous assignez plusieurs ressources, vous pouvez définir l'ordre dans lequel celles-ci seront mises à jour : cochez la case Mettre ressources à jour en ordre et utilisez les boutons + et - pour changer l'ordre des ressources dans la colonne Ressources actuelles.**

6. **Pour assigner un groupe de ressources à ce rôle, sélectionnez-le dans la colonne Groupes de ressources disponibles et déplacez-le dans la colonne Groupes de ressources actuels en cliquant sur les touches fléchées. Un groupe de ressources est un ensemble de ressources offrant un autre moyen de spécifier l'ordre dans lequel les comptes de ressources sont créés et mis à jour.**

7. **Pour définir les attributs de compte s'appliquant à ce rôle par ressource, cliquez sur Définir des valeurs d'attribut dans la section Ressources assignées. Pour plus d'informations, voir "Pour afficher ou éditer les attributs des comptes de ressources" à la page 170.**

8. **Cliquez sur Enregistrer pour ouvrir la page Confirmer les changements de rôle.**

   La page Confirmer les changements de rôle s'ouvre.

9. **Dans la section Mettre à jour les utilisateurs assignés, sélectionnez une option du menu Mettre à jour les utilisateurs assignés. Pour plus d'informations, voir "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.**

10. **Cliquez sur Enregistrer pour enregistrer vos assignations de ressources.**

▼ Pour supprimer une ressource ou un groupe de ressources assigné à un rôle

Identity Manager peut supprimer une ressource ou un groupe de ressources d'un rôle sur approbation du propriétaire de ce rôle. La ressource supprimée sera supprimée des utilisateurs lorsque ceux-ci recevront les mises à jour de rôles (pour plus d'informations, voir "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149). À la suppression de la ressource, les utilisateurs perdent leurs habilitations concernant cette ressource à moins que celle-ci ne soit aussi directement assignée aux utilisateurs.

1. **Recherchez le rôle professionnel ou informatique dont vous voulez supprimer une ressource ou un groupe de ressources. Utilisez les instructions de la section "Pour rechercher des rôles" à la page 138 ou de "Pour afficher des rôles" à la page 139 pour rechercher des rôles.**

2. **Cliquez sur le rôle de votre choix pour l'ouvrir.**

   La page Éditer un rôle s'ouvre.

3. **Cliquez sur l'onglet Ressources sur la page Éditer un rôle.**

4. **Pour supprimer une ressource, sélectionnez-la dans la colonne Ressources actuelles et déplacez-la dans la colonne Ressources disponibles en cliquant sur les touches fléchées.**

   Pour supprimer un groupe de ressources, sélectionnez-le dans la colonne Groupes de ressources actuels et déplacez-le dans la colonne Groupes de ressources disponibles en cliquant sur les touches fléchées.

5. **Cliquez sur Enregistrer.**

   La page Confirmer les changements de rôle s'ouvre.

6. **Dans la section Mettre à jour les utilisateurs assignés, sélectionnez une option du menu Mettre à jour les utilisateurs assignés. Pour plus d'informations, voir "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.**

7. **Cliquez sur Enregistrer pour terminer vos modifications.**

Gestion des assignations de rôles aux utilisateurs

Les rôles sont assignés aux utilisateurs dans la zone Comptes d'Identity Manager.

▼ Pour assigner des rôles à un utilisateur

Utilisez la procédure suivante pour assigner un ou plusieurs rôles à un ou plusieurs utilisateurs.

Les utilisateurs finaux peuvent aussi effectuer des demandes d'assignation de rôles pour eux-mêmes (à condition de se limiter à demander des rôles optionnels dont le rôle parent a déjà été assigné à l'utilisateur). Pour toute information sur les méthodes à la disposition des utilisateurs finaux pour demander des rôles disponibles, reportez-vous à "Onglet Demandes" à la page 41 dans la section "Interface utilisateur final d'Identity Manager" à la page 40.

1. **Dans l'interface administrateur, cliquez sur l'onglet Comptes.**

   Le sous-onglet Lister les comptes s'ouvre.

2 Pour assigner un rôle à un utilisateur existant, procédez comme suit :

a. Cliquez sur le nom de l'utilisateur dans la Liste des utilisateurs.

b. Cliquez sur l'onglet Rôles.

c. Cliquez sur Ajouter pour ajouter un ou plusieurs rôles au compte utilisateur.

Par défaut, seuls les rôles professionnels peuvent être assignés directement aux utilisateurs. Si votre installation d'Identity Manager a été mise à niveau à partir d'une version antérieure à la 8.0, seuls les rôles professionnels peuvent être assignés directement aux utilisateurs.

d. Dans le tableau des rôles, sélectionnez les rôles que vous voulez assigner à l'utilisateur puis cliquez sur OK.

Pour trier le tableau par ordre alphabétique par Nom, Type ou Description, cliquez sur les en-têtes de colonne. Cliquez une seconde fois pour inverser l'ordre de tri. Pour filtrer la liste par type de rôle, effectuez une sélection dans le menu déroulant Actuel.

Le tableau met à jour les assignations de rôle sélectionnées ainsi que toutes les assignations de rôle connectées aux assignations de rôles parents.

e. Cliquez sur Ajouter pour afficher des assignations de rôles optionnels pouvant être également assignées à l'utilisateur.

Sélectionnez les rôles optionnels à assigner à l'utilisateur et cliquez sur OK.

f. (Facultatif) Dans la colonne Activé, sélectionnez la date à laquelle le rôle doit devenir actif. Si vous ne spécifiez pas de date, l'assignation de rôle deviendra active dès que l'approbateur de rôle désigné approuvera l'assignation de rôle.

Pour rendre temporaire l'assignation de rôle, sélectionnez la date à laquelle le rôle devra devenir inactif dans la colonne Désactivé. La désactivation du rôle entrera en vigueur au début du jour sélectionné.

Pour plus d'informations, voir "Pour activer et désactiver des rôles à des dates spécifiques" à la page 147.

g. Cliquez sur Enregistrer.

Pour activer et désactiver des rôles à des dates spécifiques

Lorsque vous assignez un rôle à un utilisateur, vous pouvez spécifier des dates d'activation et de désactivation. Les demandes d'élément de travail d'assignation de rôle sont créées au moment de l'assignation. Cependant, si une assignation de rôle n'est pas approuvée à la date d'activation programmée, le rôle ne sera pas assigné. Les activations et désactivations de rôle ont lieu peu après minuit (00h01) à la date sélectionnée.

Par défaut, seuls les rôles professionnels peuvent avoir des dates d'activation et de désactivation. Tous les autres types de rôles héritent des dates d'activation et de désactivation du rôle professionnel directement assigné à l'utilisateur. Identity Manager peut être configuré pour autoriser d'autres types de rôles à avoir des dates d'activation et de désactivation directement assignables. Pour les instructions, voir "Configuration des types de rôles " à la page 156.

▼ Pour éditer la planification du scannage des tâches différées

Le Scannage des tâches différées scanne les assignations de rôles aux utilisateurs et active et désactive les rôles en fonction des besoins. Par défaut, la tâche Scannage des tâches différées est exécutée toutes les heures.

1. **Dans l'interface administrateur, cliquez sur Tâches du serveur.**

2. **Cliquez sur Gérer la planification dans le menu secondaire.**

3. **Dans la section Tâches disponibles pour planification, cliquez sur la définition de tâche Scannage des tâches différées.**

   La page Créer un nouveau programme de tâches Scannage des tâches différées s'ouvre.

4. **Remplissez le formulaire. Si vous avez besoin d'aide, consultez les i-Helps et l'aide en ligne.**

   Pour spécifier la date et l'heure à laquelle une tâche doit être exécutée, utilisez dans Date de début le format `mm/jj/aaaa hh:mm:ss`. Par exemple, pour programmer une tâche devant démarrer à 19h00 le 29 septembre 2008, saisissez `09/29/2008 19:00:00`.

   Dans le menu déroulant Options de résultats, sélectionnez renommer. Si vous sélectionnez attendre, les futures instances de cette tâche ne s'exécuteront pas tant que vous ne supprimerez pas les résultats précédents. Reportez-vous à l'aide en ligne pour plus d'informations sur les différents paramètres d'Options de résultats.

5. **Cliquez sur Enregistrer pour enregistrer la tâche.**

   La Figure 5–9 représente le formulaire de tâche programmée pour la tâche Scannage des tâches différées.

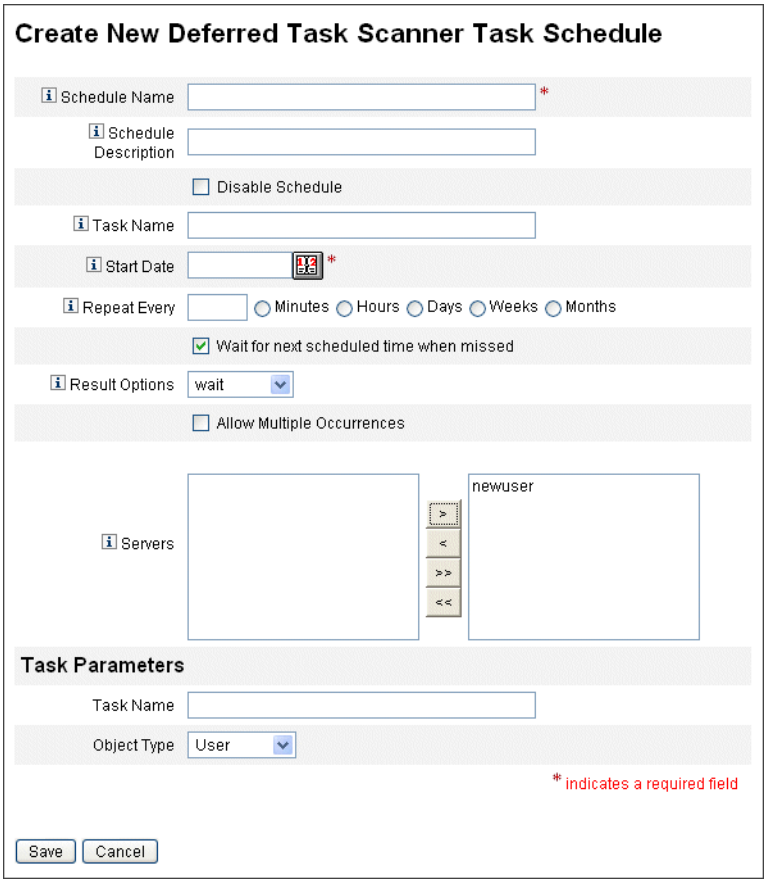


FIGURE 5–9 Formulaire de la tâche Scannage des tâches différées

Pour mettre à jour les rôles assignés aux utilisateurs

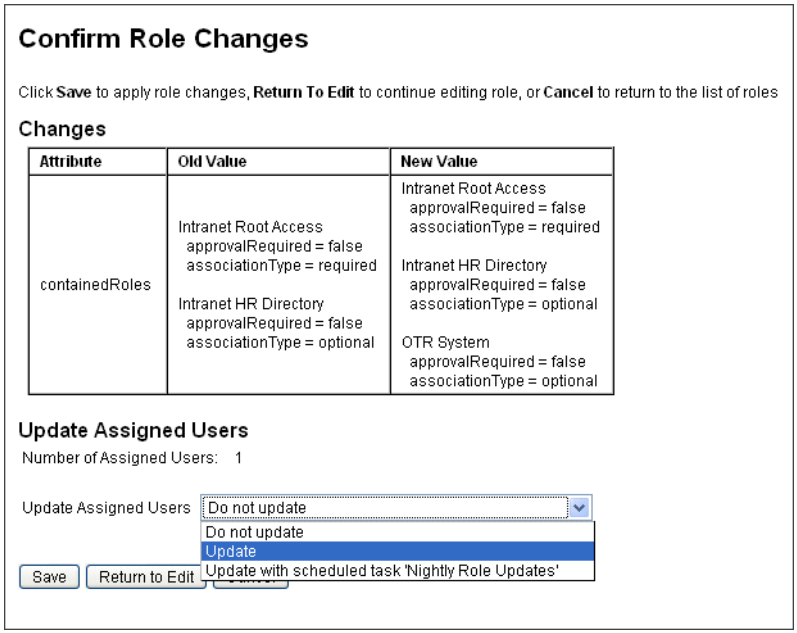
Lorsque vous éditez les rôles assignés aux utilisateurs, vous pouvez choisir de mettre immédiatement à jour les utilisateurs avec les nouveaux changements de rôle ou de reporter la mise à jour pour qu'elle soit exécutée pendant une fenêtre de maintenance programmée.

Lorsque vous apportez des changements à un rôle, la page Confirmer les changements de rôle s'ouvre. La page Confirmer les changements de rôle s'affiche dans "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.

- La section Mettre à jour les utilisateurs assignés de cette page affiche le nombre d'utilisateurs auxquels le rôle est assigné en ce moment.

- Utilisez le menu Mettre à jour les utilisateurs assignés pour sélectionner si mettre à jour les utilisateurs immédiatement en y intégrant les changements de rôle (Mettre à jour), différer l'opération (Ne pas mettre à jour) ou encore sélectionner une tâche de mise à jour programmée personnalisée.
  - Étant donné que l'action Mettre à jour actualise instantanément les utilisateurs, évitez de choisir cette option si un grand nombre d'utilisateurs sont concernés. En effet, la mise à jour d'utilisateurs peut prendre du temps et consommer des ressources. Si de nombreux utilisateurs sont concernés par la mise à jour, il est préférable de programmer l'opération en dehors des heures de pointe.
  - Lorsque vous appliquez l'action Ne pas mettre à jour à un rôle, les utilisateurs assignés à ce rôle ne recevront pas les mises à jour tant qu'aucun administrateur ne visualisera le profil utilisateur de la personne ou que l'utilisateur ne sera pas mis à jour via la tâche Mise à jour des utilisateurs pour le rôle. Pour plus d'informations sur la programmation de la tâche de mise à jour des utilisateurs pour un rôle, voir la section suivante.
  - Si vous avez créé un programme de tâche de mise à jour des utilisateurs pour le rôle, choisissez-le dans le menu. La tâche sélectionnée met à jour les utilisateurs assignés au rôle conformément à la planification définie. Pour plus de détails, voir la section suivante.

    "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149 affiche la page Confirmer les changements de rôle. La section Mettre à jour les utilisateurs assignés affiche le nombre d'utilisateurs auxquels le rôle est assigné en ce moment. Le menu déroulant Mettre à jour les utilisateurs assignés a deux options par défaut : Ne pas mettre à jour et Mettre à jour. Vous pouvez aussi sélectionner une tâche dans la liste de tâches Mise à jour des utilisateurs pour le rôle programmées. Pour les instructions relatives à la création des tâches Mise à jour des utilisateurs pour le rôle programmées, voir "Pour programmer une tâche Mise à jour des utilisateurs pour le rôle" à la page 152.



Pour mettre à jour manuellement les utilisateurs assignés

Vous pouvez mettre à jour les utilisateurs assignés aux rôles en sélectionnant un ou plusieurs rôles et en cliquant sur le bouton Mettre à jour les utilisateurs assignés. Cette procédure exécute une instance de la tâche Mettre à jour les utilisateurs assignés pour les rôles spécifiés.

1. **Recherchez le ou les rôles dont les utilisateurs assignés doivent être mis à jour en suivant les instructions de la section "Pour rechercher des rôles" à la page 138 ou celles de la section "Pour afficher des rôles" à la page 139.**

2. **Sélectionnez le ou les rôles en utilisant les cases à cocher.**

3. **Cliquez sur Mettre à jour les utilisateurs assignés.**

   La page Mise à jour des utilisateurs assignés à des rôles (Figure 5–10) s'affiche.

4. **Cliquez sur Lancer pour commencer la mise à jour.**

5. **Contrôlez le statut de la tâche Mettre à jour les utilisateurs assignés en cliquant sur Tâches du serveur dans le menu principal puis cliquez sur Toutes tâches dans le menu secondaire.**

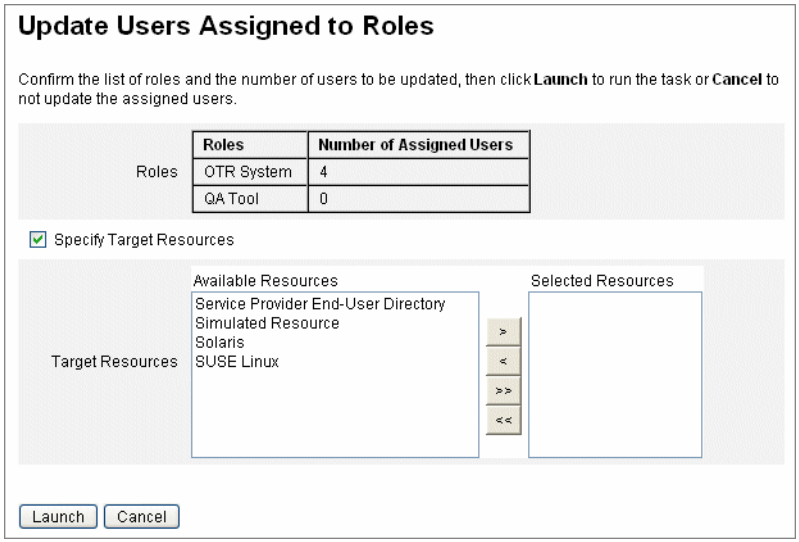


FIGURE 5–10 Page Mise à jour des utilisateurs assignés à des rôles

▼ Pour programmer une tâche Mise à jour des utilisateurs pour le rôle

Remarque – Vous devez programmer une tâche Mise à jour des utilisateurs pour le rôle pour qu'elle s'exécute régulièrement.

Programmez la tâche Mise à jour des utilisateurs pour le rôle pour mettre à jour les utilisateurs avec des changements de rôle en cours comme suit :

1. **Dans l'interface administrateur, cliquez sur Tâches du serveur.**

2. **Cliquez sur Gérer la planification dans le menu secondaire.**

3. **Dans la section Tâches disponibles pour planification, cliquez sur la définition de tâche Mise à jour des utilisateurs pour le rôle.**

   La page « Créer un nouveau programme de tâches Mise à jour des utilisateurs pour le rôle » s'ouvre ou, si vous éditez une tâche existante, la page « Éditer un programme de tâches » (Figure 5–11).

4. **Remplissez le formulaire. Si vous avez besoin d'aide, consultez les i-Helps et l'aide en ligne.**

   Pour spécifier la date et l'heure à laquelle une tâche doit être exécutée, utilisez dans Date de début le format `mm/jj/aaaa hh:mm:ss`. Par exemple, pour programmer une tâche devant démarrer à 19h00 le 29 septembre 2008, saisissez `09/29/2008 19:00:00`.

Dans le menu déroulant Options de résultats, sélectionnez renommer. Si vous sélectionnez attendre, les futures instances de cette tâche ne s'exécuteront pas tant que vous ne supprimerez pas les résultats précédents. Reportez-vous à l'aide en ligne pour plus d'informations sur les différents paramètres d'Options de résultats.

5 Cliquez sur Enregistrer pour enregistrer la tâche.

La Figure 5–11 représente le formulaire de tâche programmée pour la tâche Mise à jour des utilisateurs pour le rôle. Des rôles spécifiques peuvent être assignés à des tâches Mise à jour des utilisateurs pour le rôle spécifiques (comme indiqué dans la section Paramètres de tâche). Pour plus d'informations, voir "Pour mettre à jour les rôles assignés aux utilisateurs" à la page 149.

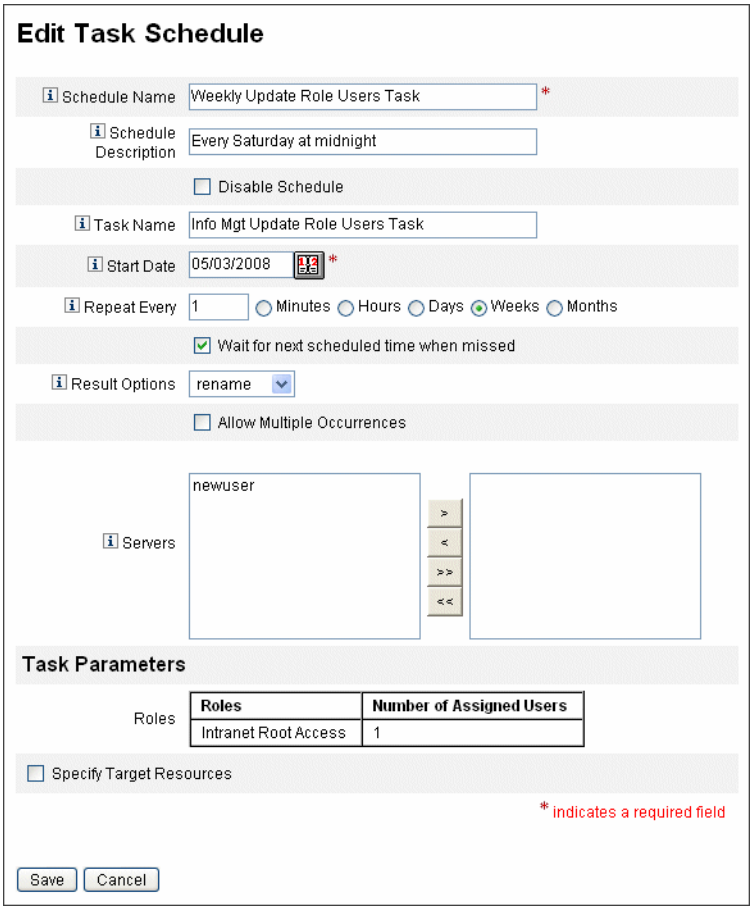


FIGURE 5–11 Formulaire de la tâche programmée Mise à jour des utilisateurs pour le rôle

▼ Pour rechercher des utilisateurs assignés à un rôle spécifique

Vous pouvez rechercher les utilisateurs auxquels un rôle spécifique a été assigné.

1. **Dans l'interface administrateur, cliquez sur Comptes.**
2. **Cliquez sur Rechercher des utilisateurs dans le menu secondaire. La page Rechercher des utilisateurs s'ouvre.**
3. **Localisez le type de recherche L'utilisateur s'est vu assigner [Sélectionnez le type de rôle] rôle(s).**
4. **Sélectionnez la case d'option et utilisez le menu déroulant Sélectionner un type de rôle pour filtrer la liste des rôles disponibles.**

   Un second menu de rôles s'ouvre.
5. **Sélectionnez un rôle.**
6. **Effacez les autres cases à cocher de type de recherche à moins que vous ne vouliez préciser davantage votre recherche.**
7. **Cliquez sur Rechercher.**

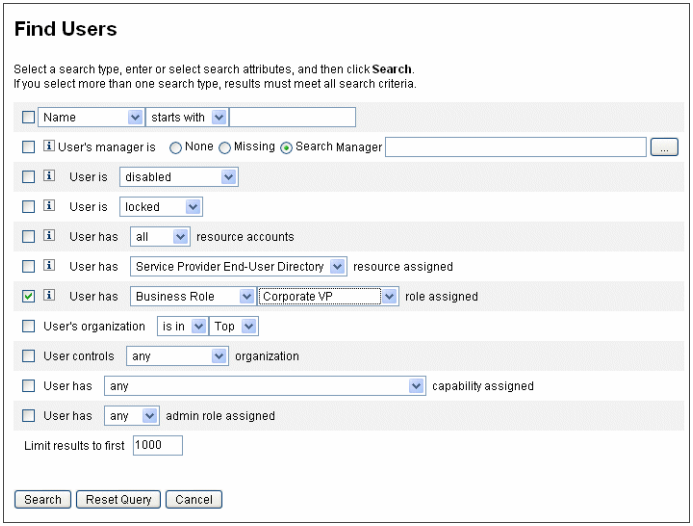


FIGURE 5–12 Recherche d'utilisateurs auxquels un rôle donné a été assigné en utilisant la page Rechercher des utilisateurs

▼ Pour supprimer un ou plusieurs rôles d'un utilisateur

La page Éditer l'utilisateur permet de supprimer un ou plusieurs rôles d'un compte utilisateur. Seul un rôle assigné directement peut être supprimé. Les rôles assignés indirectement (c'est-à-dire les rôles conditionnels et/ou les *rôles contenus* obligatoires) sont supprimés lorsque le rôle parent est supprimé. Une autre façon de supprimer un rôle assigné indirectement d'un utilisateur consiste à supprimer le rôle du rôle parent (voir "Pour supprimer un rôle assigné à un autre rôle" à la page 142).

Les utilisateurs finaux peuvent également demander la suppression des rôles assignés de leurs comptes utilisateur. Voir "Onglet Demandes" à la page 41 dans la section "Interface utilisateur final d'Identity Manager" à la page 40.

Pour les informations sur la suppression d'un rôle en utilisant une date de désactivation programmée, reportez-vous à "Pour activer et désactiver des rôles à des dates spécifiques" à la page 147.

1. **Dans l'interface administrateur, cliquez sur l'onglet Comptes.**

   Le sous-onglet Lister les comptes s'ouvre.

2. **Cliquez sur l'utilisateur duquel vous voulez supprimer une ou plusieurs règles.**

   La page Éditer l'utilisateur s'ouvre.

3. **Cliquez sur l'onglet Rôles.**

4. **Dans le tableau des rôles, sélectionnez les rôles que vous voulez supprimer de l'utilisateur puis cliquez sur OK.**

   Pour trier le tableau par ordre alphabétique par Nom, Type, Activé, Désactivé, Assigné par ou Statut, cliquez sur les en-têtes des colonnes. Cliquez une seconde fois pour inverser l'ordre de tri. Pour filtrer la liste par type de rôle, effectuez une sélection dans le menu déroulant Actuel.

   Le tableau affiche les assignations de rôles parents (les rôles qui peuvent être sélectionnés), ainsi que toutes les assignations de rôles qui sont connectées aux assignations de rôles parents (ces rôles ne peuvent pas être sélectionnés).

5. **Cliquez sur Supprimer.**

   Le tableau des rôles assignés est mis à jour de façon à indiquer les rôles assignés restants.

6. **Cliquez sur Enregistrer.**

   La page de mise à jour des comptes de ressources s'ouvre. Désélectionnez les comptes de ressources que vous ne voulez pas supprimer.

7. **Cliquez sur Enregistrer pour enregistrer vos modifications.**

Configuration des types de rôles

La fonctionnalité Type de rôle peut être modifiée en éditant l'objet configuration Rôle.

▼ Pour configurer les types de rôles pour qu'ils soient directement assignables aux utilisateurs

Par défaut, seuls certains types de rôles peuvent être assignés directement aux utilisateurs. Pour changer ces paramètres, procédez comme suit.

Remarque – Les pratiques recommandées suggèrent de n'assigner directement que des rôles professionnels aux utilisateurs. Pour plus d'informations, voir "Utilisation des types de rôles pour concevoir des rôles flexibles" à la page 123.

Pour changer les types de rôles pouvant être assignés directement aux utilisateurs, procédez comme suit :

1. **Ouvrez l'objet configuration Rôle pour l'éditer en suivant la procédure de la section "Édition des objets Configuration Identity Manager" à la page 118.**

2. **Localisez l'objet rôle correspondant au type de rôle à éditer.**

   - Pour éditer le rôle informatique, localisez `Object name='ITRole'`
   - Pour éditer le rôle application, localisez `Object name='ApplicationRole'`
   - Pour éditer le rôle matériel, localisez `Object name='AssetRole'`

3. **Spécifiez un jeu d'instructions pour mettre à jour votre configuration.**

   Selon la façon suivant laquelle vous voulez mettre à jour votre configuration, choisissez l'un des éléments suivants :

   - Pour modifier un type de rôle pour qu'il puisse être directement assigné à un utilisateur, localisez l'attribut `userAssignment` suivant dans l'objet rôle :

     ```
     <Attribute name='userAssignment'>
             <Object/>
         </Attribute>
     ```

     Et remplacez-le par ce qui suit :

     ```
     <Attribute name='userAssignment'>
             <Object>
                 <Attribute name='manual' value='true'/>
              </Object>
         </Attribute>
     ```

- Pour modifier un type de rôle pour qu'il ne puisse pas être assigné directement à un utilisateur, localisez l'attribut `userAssignment` dans l'objet rôle et supprimez l'attribut `manual` comme suit :

```
<Attribute name='userAssignment'>
        <Object>
        </Object>
    </Attribute>
```

4 **Enregistrez l'objet Configuration Rôle. Vous n'avez pas besoin de redémarrer vos serveurs d'application pour que les changements soient appliqués.**

▼ Pour activer des types de rôles pour des dates d'activation et de désactivation assignables

Par défaut, ce n'est que pour les rôles professionnels que des dates d'activation et de désactivation peuvent être activées et spécifiées lorsque les rôles sont assignés. Tous les autres types de rôles héritent des dates d'activation et de désactivation du rôle professionnel directement assigné à l'utilisateur.

Remarque – Les pratiques recommandées suggèrent de n'assigner directement que des rôles professionnels aux utilisateurs. Pour plus d'informations, voir "Utilisation des types de rôles pour concevoir des rôles flexibles" à la page 123.

Si vous décidez d'autoriser un autre type de rôle à être directement assignable aux utilisateurs (par exemple, le type Rôle informatique), vous pouvez aussi vouloir pouvoir assigner des dates d'activation et de désactivation pour ce type de rôles.

Suivez les étapes ci-après pour changer les types de rôles pouvant avoir des dates d'activation et de désactivation assignables :

1 **Ouvrez l'objet configuration Rôle pour l'éditer en suivant la procédure de la section "Édition des objets Configuration Identity Manager" à la page 118.**

2 **Localisez l'objet rôle correspondant au type de rôle à éditer.**

- Pour éditer le rôle professionnel, localisez `Object name='BusinessRole'`.
- Pour éditer le rôle informatique, localisez `Object name='ITRole'`.
- Pour éditer le rôle application, localisez `Object name='ApplicationRole'`.
- Pour éditer le rôle matériel, localisez `Object name='AssetRole'`.

3 **Spécifiez un jeu d'instructions pour mettre à jour votre configuration.**

Selon la façon dont vous voulez mettre à jour votre configuration, choisissez l'un des éléments suivants :

- Pour modifier un type de rôle pour qu'il puisse avoir des dates d'activation et de désactivation assignables, localisez l'attribut `userAssignment` suivant dans l'objet rôle :

```
<Attribute name='userAssignment'>
        <Attribute name='manual' value='true'/>
     </Attribute>
```

  Et remplacez-le par ce qui suit :

```
<Attribute name='userAssignment'>
        <Object>
            <Attribute name='activateDate' value='true'/>
             <Attribute name='deactivateDate' value='true'/>
             <Attribute name='manual' value='true'/>
        </Object>
    </Attribute>
```

- Pour modifier un type de rôle pour qu'il ne puisse pas avoir de dates d'activation et de désactivation assignables, localisez l'attribut `userAssignment` dans l'objet rôle et supprimez les attributs `activateDate` et `deactivateDate` comme suit :

```
<Attribute name='userAssignment'>
        <Object>
        </Object>
    </Attribute>
```

4 Enregistrez l'objet configuration Rôle. Vous n'avez pas besoin de redémarrer vos serveurs d'application pour que les changements soient appliqués.

▼ Pour activer ou désactiver les éléments de travail d'approbation de changement et de notification de changement

Par défaut, les éléments de travail d'approbation de changement sont activés pour tous les types de rôles. Cela signifie qu'à chaque fois qu'un rôle est changé (qu'il s'agisse d'un rôle professionnel, informatique, d'une application ou de matériel), si ce rôle a un propriétaire, ce dernier doit approuver le changement pour qu'il soit effectué.

Pour plus d'informations sur les éléments de travail d'approbation de changement et de notification de changement, reportez-vous à "Lancement d'éléments de travail d'approbation de changement et d'approbation" à la page 137.

Pour activer ou désactiver les éléments de travail d'approbation de changement et de notification de changement pour des types de rôles, suivez les étapes ci-après :

1. **Ouvrez l'objet configuration Rôle pour l'éditer en suivant la procédure de la section "Édition des objets Configuration Identity Manager" à la page 118.**

2. **Localisez l'objet rôle correspondant au type de rôle à éditer.**

   - Pour éditer le rôle professionnel, localisez `Object name='BusinessRole'`.
   - Pour éditer le rôle informatique, localisez `Object name='ITRole'`.
   - Pour éditer le rôle application, localisez `Object name='ApplicationRole'`.
   - Pour éditer le rôle matériel, localisez `Object name='AssetRole'`.

3. **Localisez les attributs suivants dans l'élément `<Object>`, qui se trouve dans l'élément `<Attribute name='features'>` :**

   ```
   <Attribute name='changeApproval' value='true'/>
    <Attribute name='changeNotification' value='true'/>
   ```

4. **Définissez les valeurs d'attribut sur true ou false selon les besoins.**

5. **Si nécessaire, répétez les étapes 2 à 4 pour configurer un autre type de rôle.**

6. **Enregistrez l'objet configuration Rôle. Vous n'avez pas besoin de redémarrer vos serveurs d'application pour que les changements soient appliqués.**

▼ Pour configurer le nombre maximum de lignes pouvant être chargées par la page Lister les rôles

La page Lister les rôles de l'interface administrateur peut afficher un nombre de lignes maximum configurable. Le nombre par défaut est 500. Suivez les étapes de cette section pour changer ce nombre.

Pour changer le nombre maximum de lignes pouvant être chargées par la page Lister les rôles, suivez les étapes ci-après.

1. **Ouvrez l'objet configuration Rôle pour l'éditer en suivant la procédure de la section "Édition des objets Configuration Identity Manager" à la page 118.**

2. **Localisez l'attribut suivant et changez-en la valeur :**

   ```
   <Attribute name='roleListMaxRows' value='500'/>
   ```

3. **Enregistrez l'objet configuration Rôle. Vous n'avez pas besoin de redémarrer vos serveurs d'application pour que les changements soient appliqués.**

Synchronisation des rôles Identity Manager et des rôles de ressource

Vous pouvez synchroniser les rôles Identity Manager avec les rôles créés en natif sur une ressource. Une fois synchronisée, la ressource est assignée, par défaut, au rôle. Ceci s'applique aux rôles créés à l'aide de la tâche de synchronisation, ainsi qu'aux rôles Identity Manager existants qui correspondent à l'un des noms de rôle de ressource.

▼ Pour synchroniser un rôle Identity Manager avec un rôle de ressource

1. **Dans l'interface administrateur, cliquez sur Tâches du serveur dans le menu principal.**
2. **Cliquez sur Exécuter des tâches. La page Tâches disponibles s'ouvre.**
3. **Cliquez sur la tâche Synchroniser les rôles Identity System et les rôles de ressources.**
4. **Remplissez le formulaire. Cliquez sur Aide pour plus d'informations.**
5. **Cliquez sur Lancer.**

Comprendre et gérer les ressources Identity Manager externes

Lisez cette section pour connaître les informations et les procédures qui vous aideront à configurer les ressources Identity Manager.

Définition des ressources

Les ressources d'Identity Manager stockent des informations sur la procédure de connexion à une ressource ou un système sur lequel sont créés les comptes. Les ressources d'Identity Manager définissent les attributs pertinents pour une ressource et aident à spécifier la façon dont les informations des ressources s'affichent dans Identity Manager.

Identity Manager fournit des ressources pour une vaste gamme de types de ressources, notamment pour :

- les gestionnaires de sécurité de mainframe,
- les bases de données,
- les services d'annuaires,
- les systèmes d'exploitation,

- les systèmes ERP (Enterprise Resource Planning - planification des ressources),
- les plates-formes de messagerie.

Zone Ressources de l'interface

Identity Manager affiche les informations relatives aux ressources existantes sur la page Ressources.

Pour accéder aux ressources, sélectionnez Ressources sur la barre de menu.

Dans la liste des ressources, les ressources sont regroupées par type. Chaque type de ressources est représenté par l'icône d'un dossier. Pour afficher les ressources actuellement définies, cliquez sur l'indicateur à proximité du dossier. Un nouveau clic sur cet indicateur permet de réduire l'affichage.

Lorsque vous développez le dossier d'un type de ressources, ce dernier est mis dynamiquement à jour et affiche le nombre d'objets Ressource qu'il contient (s'il s'agit d'un type de ressources prenant en charge les groupes).

Certaines ressources ont des objets supplémentaires que vous pouvez gérer, notamment des :

- organisations,
- unités organisationnelles,
- groupes,
- rôles.

Sélectionnez un objet depuis la liste des ressources puis effectuez des sélections à partir de l'une de ces listes d'options pour lancer une tâche de gestion :

- **Actions de ressource**. Permet d'effectuer toute une gamme d'actions sur les ressources, notamment éditer, activer la synchronisation, renommer et supprimer ; et de travailler avec des objets Ressource et gérer la connexion aux ressources.
- **Actions de l'objet de ressource**. Permet d'éditer, créer, supprimer, renommer, enregistrer sous et rechercher des objets Ressource.
- **Actions du type de ressources**. Permet d'éditer des stratégies de ressource, travailler avec l'index des comptes et configurer des ressources gérées.

Lorsque vous créez ou éditez une ressource, Identity Manager lance le flux de travaux `ManageResource`. Ce flux de travaux enregistre la ressource nouvelle ou mise à jour dans le référentiel et vous permet d'insérer des approbations ou d'autres actions avant la création ou l'enregistrement de la ressource.

Gestion de la liste des ressources

Pour pouvoir créer une nouvelle ressource, vous devez indiquer à Identity Manager les types de ressources que vous souhaitez pouvoir gérer. Pour activer les ressources et en créer de personnalisées, utilisez la page Configurer les ressources gérées.

▼ Pour ouvrir la page Configurer les ressources gérées

Utilisez les étapes suivantes pour ouvrir la page Configurer les ressources gérées.

1. **Connectez-vous à l'interface administrateur.**

2. **Cliquez sur l'onglet Ressources.**

   Utilisez l'une des méthodes suivantes pour ouvrir la page Configurer les ressources gérées :

   - Localisez la liste déroulante Actions du type de ressources et choisissez Configurer les ressources gérées.
   - Cliquez sur l'onglet Configurer les types.

   La page Configurer les ressources gérées s'ouvre.

   Cette page présente trois sections :

   - **Connecteurs de ressources**. Cette section liste les types de connecteurs de ressources, la version des connecteurs et leur serveur.
   - **Adaptateurs de ressources**. Cette section liste les types de ressources couramment répandus dans les environnements d'entreprise de grande taille. La version de l'adaptateur Identity Manager qui assure la connexion avec la ressource est indiquée dans la colonne Version.
   - **Adaptateurs de ressources personnalisés**. Cette section est utilisée pour ajouter des ressources personnalisées dans la liste Ressources.

▼ Pour activer des types de ressources

Vous pouvez activer un type de ressources depuis la page Configurer les ressources gérées en procédant comme indiqué ci-après.

1. **Si ce n'est pas déjà fait, ouvrez la page Configurer les ressources gérées ("Gestion de la liste des ressources" à la page 162).**

2. **Dans la section Ressources, sélectionnez la case de la colonne Gérés ? correspondant au type de ressources à activer.**

   Pour activer tous les types de ressources listés, sélectionnez Gérer toutes les ressources.

3 **Cliquez sur Enregistrer au bas de cette page.**

La ressource est ajoutée à la liste Ressources.

▼ Pour ajouter une ressource personnalisée

Vous pouvez ajouter une ressource personnalisée depuis la page Configurer les ressources gérées en procédant comme indiqué ci-après.

1 **Si ce n'est pas déjà fait, ouvrez la page Configurer les ressources gérées ("Gestion de la liste des ressources" à la page 162).**

2 **Dans la section Adaptateurs de ressources personnalisés, cliquez sur Ajouter un adaptateur de ressources personnalisé pour ajouter une ligne dans le tableau.**

3 **Saisissez le classpath de ressource pour la ressource ou saisissez votre ressource développée personnalisée. Pour les adaptateurs fournis avec Identity Manager, voir le *Sun Identity Manager 8.1 Resources Reference* pour le classpath complet.**

4 **Cliquez sur Enregistrer pour ajouter la ressource à la liste Ressources.**

▼ Pour créer une ressource

Une fois un type de ressources activé, vous pouvez créer une instance de cette ressource dans Identity Manager. Pour créer une ressource, utilisez l'*assistant Ressource*.

L'assistant Ressource vous guidera dans la configuration des éléments suivants :

- **Paramètres propres à la ressource**. Vous pouvez modifier ces valeurs depuis l'interface d'Identity Manager lorsque vous créez une instance spécifique de ce type de ressource.
- **Attributs de compte**. Sont définis dans la carte schématique de la ressource. Ces éléments déterminent la façon dont les attributs d'utilisateur Identity Manager mappent vers des attributs sur la ressource.
- **DN de compte ou modèle d'identité**. Inclut la syntaxe des noms de compte pour les utilisateurs, laquelle revêt une importance particulière pour les espaces de noms hiérarchiques.
- **Paramètres d'Identity Manager pour la ressource**. Paramètre les stratégies, établit les approbateurs de ressource et configure l'accès de l'organisation à la ressource.

1 **Connectez-vous à l'interface administrateur.**

2 **Cliquez sur l'onglet Ressources. Vérifiez que le sous-onglet Lister les ressources est sélectionné.**

3 **Localisez la liste déroulante Actions du type de ressources et choisissez Nouvelle ressource.**

La page Nouvelle ressource s'ouvre.

4 **Sélectionnez un type de ressource dans la liste déroulante (si le type de ressource que vous recherchez ne figure pas dans la liste, vous devez l'activer, reportez-vous à "Gestion de la liste des ressources" à la page 162).**

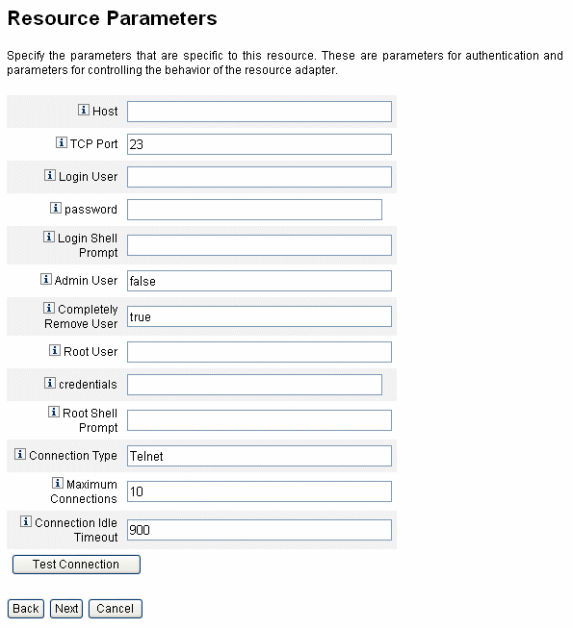
5 **Cliquez sur Nouveau pour afficher la page de bienvenue de l'assistant Ressource.**

6 **Cliquez sur Suivant pour commencer à définir la ressource.**

Les étapes et les pages de l'assistant Ressource s'affichent dans l'ordre suivant :

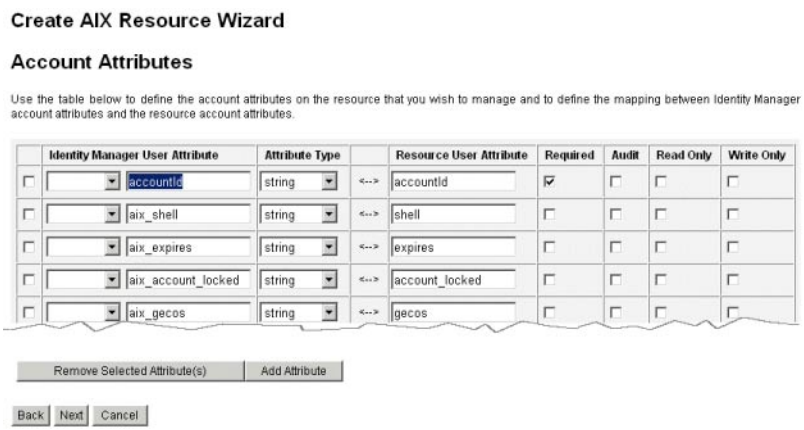
- **Paramètres de ressource**. Configurez les paramètres propres à la ressource qui contrôlent l'authentification et le comportement de l'adaptateur de ressources. Saisissez les paramètres puis cliquez sur Vérifier la connexion pour vous assurer que la connexion est valide. À la confirmation, cliquez sur Suivant pour paramétrer les attributs de compte.

  La figure suivante illustre la page Paramètres de ressource pour les ressources Solaris. Les champs de formulaire de cette page diffèrent selon les ressources.



- **Attributs de compte** *(carte schématique)*. Mappe les attributs de compte Identity Manager vers des attributs de compte de ressource. Pour plus d'informations sur les attributs de compte de ressource, reportez-vous à "Pour afficher ou éditer les attributs des comptes de ressources" à la page 170.
  - Pour ajouter un attribut, cliquez sur Ajouter un attribut.
  - Pour supprimer un ou plusieurs attributs, sélectionnez les cases en regard de ce ou ces attributs puis cliquez sur Supprimer Les attributs sélectionnés.

    La figure suivante illustre la page Attributs de compte de l'assistant Ressource.



Remarque – Si vous voulez exporter des attributs vers le tableau `EXT_RESOURCEACCOUNT_ACCTATTR`, vous devez contrôler la case Vérification informatique de chaque attribut à exporter.

Lorsque vous avez terminé, cliquez sur Suivant pour configurer le modèle d'identité.

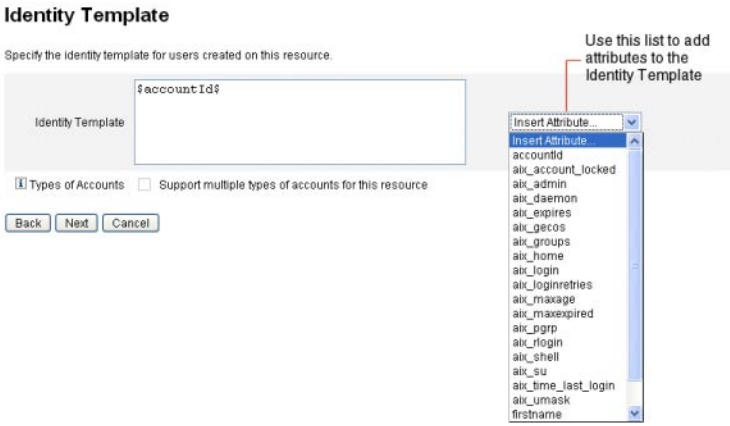
- **Modèle d'identité**. Définir la syntaxe des noms de comptes pour les utilisateurs. Cette fonctionnalité est particulièrement importante pour les espaces de noms hiérarchiques.
  - Pour ajouter un attribut au modèle, sélectionnez-le dans la liste Insérer attribut.
  - Pour supprimer un attribut, mettez-le en surbrillance dans la chaîne et utilisez la touche Suppression du clavier. Supprimez le nom de l'attribut, ainsi que les signes `dollar ($)` précédant et suivant.
  - **Type de comptes**. Identity Manager offre la possibilité d'assigner plusieurs comptes de ressources à un même utilisateur. Par exemple, un utilisateur peut avoir besoin d'un compte de niveau administrateur et d'un compte utilisateur classique pour une ressource particulière. Pour assurer la prise en charge de plusieurs types de comptes sur une même ressource, cochez la case Type de compte.

    Remarque – Vous ne pouvez pas activer l'option Type de compte si vous n'avez pas créé dans le Générateur d'identités une ou plusieurs règles identifiées par le sous-type `IdentityRule`. Les ID de compte devant être distincts, les différents types de comptes doivent générer des ID de compte différents pour un utilisateur donné. Les règles de génération d'identités spécifient la procédure de création de ces ID de compte uniques.

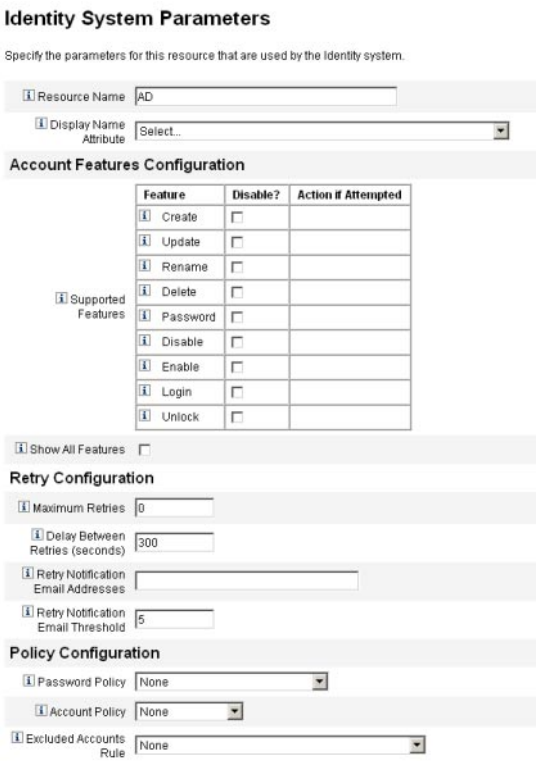
    Des exemples de règles d'identité sont disponibles dans le fichier `sample/identityRules.xml`.

Vous ne pouvez pas supprimer un type de compte tant qu'il est encore référencé par d'autres objets au sein d'Identity Manager. Vous ne pouvez pas non plus renommer un type de comptes.

Pour plus d'informations sur le remplissage du formulaire Type de compte, reportez-vous à l'aide en ligne d'Identity Manager. Pour plus d'informations sur la création de plusieurs comptes de ressources pour un utilisateur, reportez-vous à "Création de comptes de ressource multiples pour un utilisateur" à la page 61.



- **Paramètres du système d'identité**. Cette option définit les paramètres d'Identity Manager pour la ressource, configuration de la relance et des stratégies comprises, comme indiqué dans "Pour créer une ressource" à la page 163.



7 **Utilisez Suivant et Précédent pour vous déplacer d'une page à l'autre. Une fois toutes les sélections terminées, cliquez sur Enregistrer pour enregistrer la ressource et revenir à la page de la liste.**

Gestion des ressources

Cette section décrit la gestion des ressources existantes.

Les rubriques sont organisées comme suit :

▼ Pour afficher la liste des ressources

Vous pouvez afficher les ressources existantes à partir de la Liste des ressources.

1 **Connectez-vous à l'interface administrateur.**

2 **Cliquez sur Ressources dans le menu principal.**

La Liste des ressources s'affiche dans le sous-onglet Lister les ressources.

▼ Pour éditer une ressource en utilisant l'assistant Ressource

Utilisez l'assistant Ressource pour éditer les paramètres de ressource, les attributs de compte et les paramètres du système d'identité. Vous pouvez aussi spécifier le modèle d'identité à utiliser pour les utilisateurs créés sur la ressource.

1 **Dans l'interface administrateur d'Identity Manager, cliquez sur Ressources dans le menu principal.**

La Liste des ressources s'affiche dans le sous-onglet Lister les ressources.

2 **Sélectionnez la ressource à éditer.**

3 **Dans le menu déroulant Actions de ressource, sélectionnez l'assistant Ressource (sous Éditer).**

L'assistant Ressource s'ouvre en mode Édition pour la ressource sélectionnée.

▼ Pour éditer une ressource en utilisant les commandes de la liste des ressources

En plus de l'assistant Éditer une ressource, vous pouvez utiliser les commandes de la Liste des ressources pour effectuer tout un éventail d'actions d'édition sur une ressource.

1 **Choisissez une ou plusieurs options dans la Liste des ressources.**

Ces options sont les suivantes :

- **Supprimer des ressources**. Sélectionnez une ou plusieurs ressources, puis sélectionnez Supprimer dans la liste Actions de ressource. Vous pouvez sélectionner des ressources de plusieurs types en même temps. Vous ne pouvez pas supprimer une ressource si des rôles ou des groupes de ressources y sont associés.
- **Recherche d'objets de ressource**. Sélectionnez une ressource puis Rechercher l'objet de ressource dans la liste Actions de l'objet de ressource pour trouver un objet Ressource (par exemple une organisation, une unité organisationnelle, un groupe ou une personne) en fonction de ses caractéristiques.
- **Gestion des objets Ressource**. Vous pouvez créer de nouveaux objets pour certains types de ressources. Sélectionnez la ressource puis sélectionnez Créer un objet ressource dans la liste Actions de l'objet de ressource.
- **Renommer des ressources**. Sélectionnez une ressource puis sélectionnez Renommer dans la liste Actions de ressource. Saisissez un nouveau nom dans la case d'entrée qui s'affiche et cliquez sur Renommer.

- **Cloner des ressources**. Sélectionnez une ressource puis sélectionnez Enregistrer sous dans la liste Actions de ressource. Saisissez un nouveau nom dans la case d'entrée qui s'affiche. La ressource clonée s'affiche dans la liste des ressources avec le nom sélectionné.
- **Effectuer des opérations en masse sur les ressources**. Spécifiez une liste de ressources et d'actions à appliquer (depuis une entrée au format CSV) à toutes les ressources de la liste. Lancez ensuite les opérations en masse pour engager une tâche d'opération en masse en arrière-plan.

2 Enregistrez vos modifications.

▼ Pour afficher ou éditer les attributs des comptes de ressources

Les attributs de compte de ressources (ou carte schématique) fournissent une méthode abstraite permettant de faire référence aux attributs sur les ressources gérées. La carte schématique permet de spécifier la façon Identity Manager référencie les attributs (côté gauche de la carte schématique) et celle dont les noms sont mappés vers les noms d'attribut sur la ressource proprement dite (côté droit de la carte schématique). Vous pourrez ensuite faire référence au nom d'attribut Identity Manager dans les formulaires ou les définitions de flux de travaux et référencer efficacement l'attribut sur la ressource, elle-même.

Voici un exemple de mappage entre des attributs Identity Manager et ceux d'une ressource LDAP :

Attribut Identity Manager		Attribut de ressource LDAP
`firstname`,	`<-->`	`givenName`
`lastname`	`<-->`	`sn`

Toute référence à l'attribut Identity Manager, `firstname`, est en fait une référence à l'attribut LDAP, `givenName` quand une action est entreprise sur cette ressource.

Dans le cadre de la gestion de ressources multiples depuis Identity Manager, mapper un attribut de compte Identity Manager commun à plusieurs attributs de ressource peut simplifier considérablement la gestion des ressources. Par exemple, l'attribut Identity Manager `fullname` peut être mappé vers l'attribut de ressource Active Directory `displayName`. Parallèlement, sur une ressource LDAP, le même attribut Identity Manager `fullname` peut être mappé vers l'attribut LDAP `cn`. Résultat, l'administrateur n'a besoin d'indiquer qu'une seule fois la valeur `fullname`. À l'enregistrement de l'utilisateur, la valeur `fullname` est transférée aux ressources qui ont des noms d'attribut différents.

En configurant une carte schématique sur la page Attributs de compte de l'assistant Ressource, vous pouvez effectuer ce qui suit :

- définir les noms d'attribut et les types de données pour les attributs provenant de ressources gérées ;
- limiter les attributs de ressource à ceux strictement nécessaires pour votre entreprise ou organisation ;
- créer des noms d'attribut Identity Manager qui seront utilisés avec des ressources multiples ;
- identifier les attributs utilisateur requis et les types d'attributs.

Pour afficher ou éditer les attributs de compte de ressource, procédez comme suit :

1. **Dans l'interface administrateur, cliquez sur Ressources.**
2. **Sélectionnez la ressource pour laquelle vous voulez afficher ou éditer les attributs de compte.**
3. **Dans la liste Actions de ressource, cliquez sur Éditer un schéma de ressources.**

   La page d'édition des attributs de compte de ressources s'ouvre.

   La colonne de gauche de la carte schématique (intitulée Attribut utilisateur Identity System) contient les noms des attributs de compte Identity Manager qui sont référencés par les formulaires utilisés dans les interfaces administrateur et utilisateur d'Identity Manager. La colonne de droite de la carte schématique (intitulée Attribut d'utilisateur de ressources) contient les noms des attributs provenant de la source externe.

Groupes de ressources

Utilisez la zone Ressources pour gérer des groupes de ressources ce qui vous permettra de mettre à jour vos groupes de ressources dans un ordre spécifique. En intégrant et en classant les ressources dans un groupe et en assignant ce groupe à un utilisateur, vous déterminez l'ordre dans lequel les ressources de cet utilisateur sont créées, mises à jour et supprimées.

Les activités sont effectuées sur chacune des ressources à tour de rôle. Si une action échoue sur une ressource, les ressources suivantes ne sont pas mises à jour. Ce type de relation revêt une importance particulière pour les ressources liées.

Par exemple, toute ressource Exchange Server 2007 repose sur un compte Windows Active Directory existant. Ce compte doit exister pour que le compte Exchange puisse être créé. En créant un groupe de ressources avec (dans l'ordre) une ressource Windows Active Directory et une ressource Exchange Server 2007, l'ordre sera correct quand vous créerez des utilisateurs. Inversement, cet ordre assure que les ressources seront supprimées dans le bon ordre quand vous supprimerez les utilisateurs.

Sélectionnez Ressources, puis sélectionnez Lister les groupes de ressources pour afficher la liste des groupes de ressources actuellement définis. Depuis cette page, cliquez sur Nouveau pour définir un groupe de ressources. Lorsque vous définissez un groupe de ressources, une zone de sélection vous permet de choisir puis de classer les ressources choisies, ainsi que de sélectionner les organisations pour lesquelles le groupe de ressources sera disponible.

Stratégie de ressource globale

Cette section explique comment éditer la Stratégie de ressource globale et définir les valeurs de délai d'attente pour une ressource.

▼ Pour éditer les attributs de stratégie

Vous pouvez éditer les attributs de stratégie de ressource depuis la page Éditer les attributs de stratégie de ressources globales.

1 Ouvrez la page Éditer les attributs de stratégie de ressources globales et éditez les attributs comme requis.

Ces attributs sont les suivants :

- **Délai d'attente de capture par défaut**. Saisissez une valeur, en millisecondes, qui indique la durée maximum pendant laquelle l'adaptateur doit attendre l'invite de la ligne de commande avant la temporisation. Cette valeur s'applique uniquement aux adaptateurs GenericScriptResourceAdapter ou ShellScriptSourceBase. Utilisez ce paramètre lorsque les résultats d'une commande ou d'un script sont importants et seront analysés par l'adaptateur.

  La valeur par défaut de ce paramètre est 30000 (30 secondes).
- **Intervalle par défaut entre les opérations**. Saisissez une valeur, en millisecondes, qui indique la durée maximum pendant laquelle l'adaptateur sous forme de script doit attendre l'invite de la ligne de commande avant la temporisation. Cette valeur s'applique uniquement aux adaptateurs GenericScriptResourceAdapter ou ShellScriptSourceBase. Utilisez ce paramètre lorsque les résultats d'une commande ou d'un script ne sont pas examinés par l'adaptateur.
- **Wait for Ignore Case**. Saisissez une valeur, en millisecondes, qui indique la durée maximum pendant laquelle l'adaptateur doit attendre l'invite de la ligne de commande avant la temporisation. Cette valeur s'applique uniquement aux adaptateurs GenericScriptResourceAdapter ou ShellScriptSourceBase. Utilisez ce paramètre lorsque la casse (majuscules ou minuscules) n'a pas d'importance.
- **Stratégie de mot de passe de compte de ressources**. Le cas échéant, sélectionnez une stratégie de mot de passe de compte de ressources à appliquer à la ressource sélectionnée. Aucune est la sélection par défaut.
- **Règle de comptes de ressources exclus**. Le cas échéant, sélectionnez une règle qui gouverne les comptes de ressources exclus. Aucune est la sélection par défaut.

2 **Vous devez cliquer sur Enregistrer pour enregistrer les modifications apportées à la stratégie.**

▼ Pour définir des valeurs de délai d'attente supplémentaires

Vous pouvez modifier la propriété `maxWaitMilliseconds` en éditant le fichier `Waveset.properties`. Cette propriété, `maxWaitMilliseconds`, contrôle la fréquence à laquelle le délai d'attente d'une opération sera contrôlé. Si vous ne spécifiez pas cette valeur, le système utilise la valeur par défaut : 50.

1 **Ajoutez la ligne suivante au fichier** `Waveset.properties` **:**

```
com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds.
```

2 **Enregistrez le fichier.**

Actions de ressource en masse

Vous pouvez effectuer des opérations en masse sur les ressources en utilisant un fichier au format CSV ou en créant ou spécifiant les données à appliquer pour l'opération.

La Figure 5–13 représente la page de lancement d'opérations en masse avec une action de création.

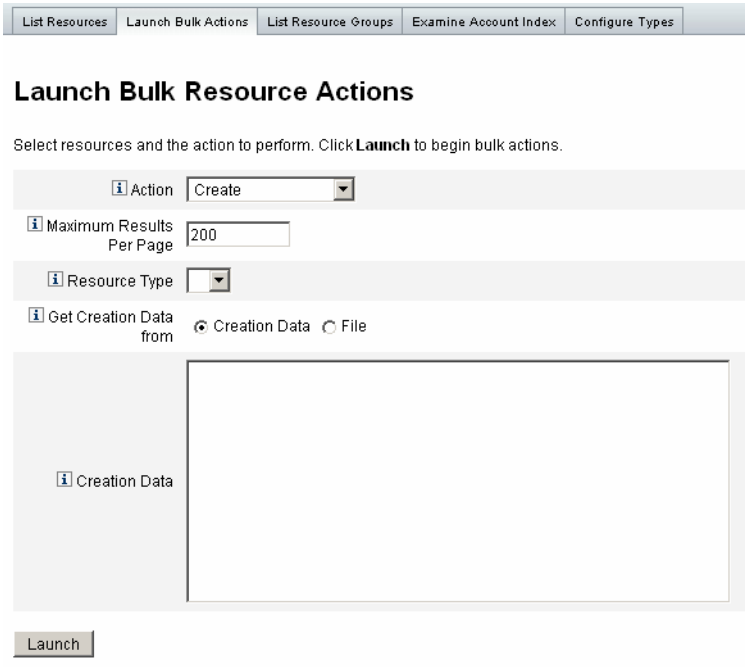


FIGURE 5–13 Lancement d'actions de ressource en masse

Les options disponibles pour l'opération de ressource en masse dépendent de l'Action sélectionnée pour l'opération. Vous pouvez spécifier une unique action à appliquer à l'opération ou sélectionner De la liste des actions pour spécifier plusieurs actions.

- **Actions**. Pour spécifier une unique action, sélectionnez l'une des options suivantes : Créer, Cloner, Mettre à jour, Supprimer, Changement du mot de passe ou Réinitialisation du mot de passe.

  Si vous sélectionnez une unique action, vous vous verrez proposer des options permettant de spécifier la ressource concernée par l'action. Pour une action Créer, vous spécifierez le type de la ressource.

  Si vous spécifiez De la liste des actions, utilisez la zone Prendre liste des actions de pour spécifier soit le fichier contenant les actions à utiliser soit les actions de votre choix dans la zone d'entrée.

  Remarque – Les actions que vous saisissez dans la liste de la zone d'entrée ou dans le fichier doivent suivre le format CSV.

- **Maximum de résultats par page**. Utilisez cette option pour spécifier le nombre maximum de résultats d'action en masse qui s'afficheront sur chaque page de résultats de tâche. La valeur par défaut est 200.

Cliquez sur Lancer pour démarrer l'opération qui s'exécutera en arrière-plan.

Comprendre et gérer les ressources externes

Vous pouvez aussi utiliser Identity Manager pour créer, provisionner et gérer de manière centralisée des *ressources externes* pour votre entreprise.

Cette section explique comment travailler avec les ressources externes. Les informations sont organisées de la manière suivante :

Définition des ressources externes

Une *ressource externe* est un type de ressource unique qui ne stocke pas directement les informations de compte utilisateur. En fait, c'est une ressource qui est extérieure au fonctionnement d'Identity Manager. Ces ressources peuvent être des ordinateurs de bureau, des ordinateurs portables, des téléphones portables, des badges de sécurité, etc.

Le provisioning des ressources externes requiert pratiquement toujours un ou plusieurs processus manuels. Par exemple, après avoir effectué la demande initiale et obtenu les dues approbations pour provisionner un ordinateur portable pour un nouvel employé, vous devrez probablement envoyer une demande d'achat au système de commande de l'entreprise. Une fois la commande remplie, une autre personne devra sans doute préconfigurer cet ordinateur portable avec les applications de l'entreprise avant de le remettre personnellement au nouvel employé pour clore la demande de provisioning.

Raisons de l'utilisation de ressources externes

Utiliser Identity Manager pour provisionner des ressources externes vous permet d'avertir un ou plusieurs approvisionneurs des demandes en cours, en leur fournissant des informations détaillées sur l'objet du provisioning.

Par exemple, un approvisionneur de ressources externes peut être un responsable informatique amené à devoir commander et préconfigurer un ordinateur portable pour un utilisateur.

Par ailleurs, Identity Manager conserve des informations sur les ressources externes provisionnées pour un utilisateur donné, lesquelles sont mises à jour à la fin de la demande de provisioning. Identity Manager rend ensuite ces informations disponibles pour l'affichage, l'édition, la validation de la compatibilité d'audit et l'exportation.

Remarque – Pour configurer des ressources externes, vous devez avoir la capacité Administrateur des ressources externes. Pour créer de nouvelles ressources externes, vous devez avoir la capacité Administrateur de ressources.

Configuration de ressources externes

Cette section explique le processus consistant à configurer le magasin de données des ressources externes et la notification adressée à l'approvisionneur des ressources externes.

Configuration du magasin de données des ressources externes

Le magasin de données de ressources externes d'Identity Manager est un magasin de données unique qui contient des informations relatives aux ressources externes et aux assignations relatives à ces mêmes ressources. Ce magasin de données peut être une base de données ou un annuaire.

- Si c'est une *base de données*, le magasin de données est géré par le ScriptedJdbcResourceAdapter.
- Si c'est un *annuaire*, il l'est par le LDAPResourceAdapter.

Remarque – Vous devez avoir la capacité Administrateur des ressources externes pour configurer le magasin de données de ressources externes.

Le magasin de données de ressources externes vous permet de stocker les données dans n'importe quelles valeurs d'attribut et de stocker ces valeurs dans une ou plusieurs tables.

Par exemple, si vous utilisez la base de données MySQL, Identity Manager stocke les informations relatives aux ressources externes dans les tables suivantes :

- La table `extres.accounts` contient les ID de compte et de ressource. Le magasin de données des ressources externes étant unique, Identity Manager fournit une unique clé d'ID, `<idCompte>@<iDRessource>` , qui identifie de manière univoque un compte par son ID de ressource.
- La table `extres.attributes` contient un ensemble d'attributs sous forme de paires nom/valeur. Ce sont ces attributs que vous définissez dans le mappage schématique lorsque vous créez une ressource externe.

Les exemples de scripts utilisés pour créer les tables de la base de données sont copackagés avec Identity Manager dans l'emplacement suivant :

wshome`/sample/ScriptedJdbc/External`

Identity Manager prend en charge plusieurs types de bases de données et fournit un exemple pour chacun. Vous pouvez modifier ces scripts en fonction de votre environnement spécifique.

Le magasin de données des ressources externes prend également en charge LDAP par le biais du LDAPResourceAdapter, ce qui permet de stocker les données dans des classes existantes ou personnalisées. Un exemple de script LDIF est également copackagé avec Identity Manager dans l'emplacement suivant :

wshome`/sample/other/externalResourcePerson.ldif`

Vous pouvez modifier ce script dans le cadre de la configuration d'un magasin de données de type annuaire de ressources.

▼ Pour configurer un magasin de données de type base de données

Bien que vous puissiez effectuer facilement des modifications, le magasin de données des ressources externes n'est en général configuré qu'une fois. Si vous en modifiez la configuration, Identity Manager met automatiquement à jour toutes les ressources externes existantes pour qu'elles utilisent le magasin de données nouvellement configuré.

Pour configurer un magasin de données de type base de données, procédez comme suit :

1. **Sélectionnez Configurer → Ressources externes depuis la barre de menu de l'interface administrateur d'Identity Manager.**

2. **Lorsque la page Configuration du magasin de données s'affiche, choisissez Base de données dans le Type de magasin de données. Des options supplémentaires s'affichent.**

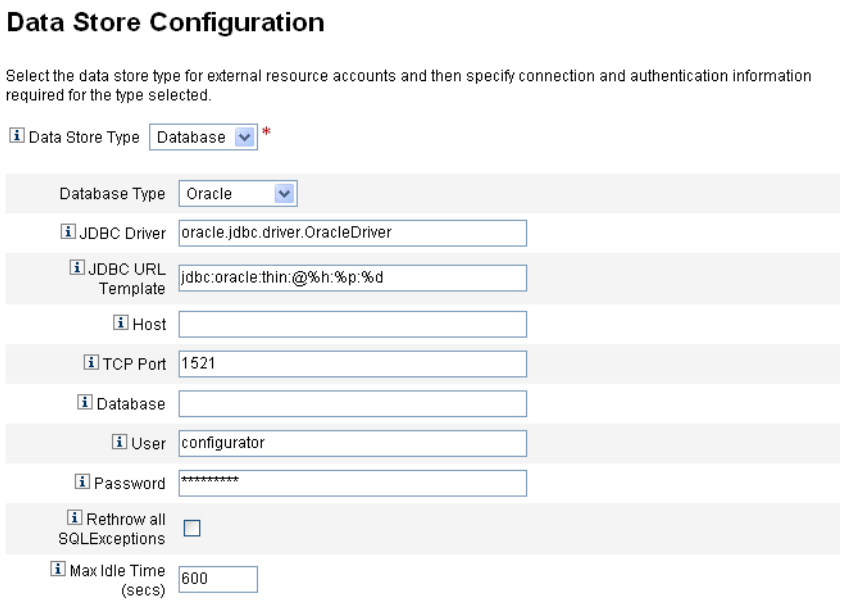


FIGURE 5–14 La Page Configuration du magasin de données : Base de données

3 Spécifiez les informations de connexion et d'authentification suivantes :

Remarque – Identity Manager remplit automatiquement les champs Pilote JDBC, Modèle JDBC URL, Port et Délai d'attente maxi (secondes) avec les valeurs par défaut. Vous pouvez changer ces valeurs par défaut si besoin est.

- **Pilote JDBC**. Spécifiez le nom de classe du pilote JDBC.
- **Modèle JDBC URL**. Spécifiez le modèle d'URL du pilote JDBC.
- **Hôte**. Entrez le nom de l'hôte sur lequel vous exécutez la base de données.
- **Port TCP**. Saisissez le numéro du port d'écoute utilisé par la base de données.
- **Base de données**. Saisissez le nom de la base de données du serveur de base de données, qui contient la table du magasin de données.
- **Utilisateur**. Saisissez l'ID d'un utilisateur de la base de données autorisé à lire, mettre à jour et supprimer des lignes de la table du magasin de données. Par exemple : root.
- **Mot de passe**. Saisissez le mot de passe de l'utilisateur de la base de données.
- **Rejeter toutes les exceptions SQL**. Cochez cette case pour rejeter les exceptions SQL aux instructions SQL quand les codes d'erreur des exceptions sont 0.

  Si vous n'activez pas cette option, Identity Manager détecte et supprime ces exceptions.

- **Délai d'attente maxi**. Spécifiez la durée maximum en secondes pendant laquelle vous voulez que les connexions JDBC restent inutilisées dans un pool.

  Si la connexion n'est pas utilisée avant l'expiration du délai indiqué, Identity Manager la ferme et la supprime du pool.

  - La valeur par défaut est de 600 secondes.
  - La valeur `-1` empêche à jamais la connexion d'expirer.

4 **Une fois connecté au magasin de données, vous devez spécifier un ou plusieurs scripts à exécuter pour chaque action de ressource prise en charge. Pour les instructions, voir "Pour configurer les scripts d'action" à la page 179.**

▼ Pour configurer les scripts d'action

Vous devez spécifier un ensemble de scripts BeanShell (`bsh`) pouvant être utilisés par Identity Manager pour suivre et exécuter les états Get, Create, Update, Delete, Enable, Disable et Test d'une demande donnée.

Des exemples de scripts d'action sont disponibles dans :

wshome`/sample/ScriptedJdbc/External/beanshell`

Remarque – Vous pouvez modifier ces exemples pour créer vos propres scripts d'action personnalisés. Les scripts personnalisés sont ajoutés à l'outil de sélection Scripts d'action puis affichés sous la ligne dans les listes Disponible et Sélectionné.

Identity Manager fournit des exemples de scripts pour les actions de ressource de tout type de base données prises en charge pour les ressources externes. Pour accéder à ces scripts, utilisez le script ResourceAction qui se trouve dans l'emplacement suivant :

wshome`/sample/ScriptedJdbc/External/beanshell`

Le nom de la base de données, le nom d'utilisateur et le mot de passe par défaut sont tous `extres`.

- Si vous choisissez l'une des autres options de base de données ou préférez utiliser un autre nom d'utilisateur ou nom de base de données, vous devez modifier les scripts de création de base de données d'exemple et les scripts ResourceAction avec différentes valeurs.

  Par exemple, si vous choisissez une base de données MySQL, mais voulez changer le nom de la base de données, le nom d'utilisateur et le mot de passe existants, vous devez effectuer les changements suivants : vous devez mettre à jour le script `create_external_tables.mysql` en remplaçant le nom de la base de données, le nom d'utilisateur et le mot de passe par défaut, `extres`, par, dans l'ordre, `externalresources`, `externaladmin` et `externalpassword`.

- Vous devez ensuite changer les scripts ResourceAction en remplaçant les valeurs par défaut, `extres.accounts` et `extres.attributes`, par, dans l'ordre, `externalresources.accounts` et `externalresources.attributes` .

Suivez les étapes ci-après pour configurer les scripts Action :

1 **Utilisez les outils de sélection Scripts d'action de la page Configuration du magasin de données pour spécifier un ou plusieurs scripts d'action pour chaque action de ressource. Vous devez sélectionner au moins un script par action de ressource.**

FIGURE 5–15 La zone Scripts d'action

Vous devez sélectionner le script d'action par défaut correspondant à l'action de ressource. Par exemple, vous devez utiliser

- `External-getUser-bsh` pour les Actions de ressource GetUser.

  Remarque – Les Actions de ressource GetUser sont utilisées pour les opérations Rechercher.

- `External-createUser-bsh` pour les Actions de ressource CreateUser.
- `External-deleteUser-bsh` pour les Actions de ressource DeleteUser.
- `External-updateUser-bsh` pour les Actions de ressource UpdateUser.
- `External-disableUser-bsh` pour les Actions de ressource DisableUser.
- `External-enableUser-bsh`pour les Actions de ressource EnableUser.
- `External-test-bsh` pour les Actions de ressource de test.

  Remarque – Les Actions de ressource de test sont utilisées pour permettre la pleine fonctionnalité du bouton Vérifier la connexion.

Sélectionner l'un quelconque des autres scripts `bsh` dans les exemples de scripts de la liste ne fonctionnera pas.

2 **Choisissez un Mode contexte de l'action dans le menu pour spécifier la façon dont les valeurs d'attribut seront transmises aux scripts d'action.**

- **Chaînes**. Transmet les valeurs d'attribut sous forme de chaînes.
- **Assignation directe**. Transmet les valeurs d'attribut sous la forme d'un objet `com.waveset.object.AttributeValues`.

3 **Il convient maintenant de tester la configuration de connexion de votre magasin de données. Cliquez sur le bouton Vérifier la connexion situé au bas de la page.**

Un message s'affiche confirmant que la connexion a réussi ou indiquant une erreur de configuration.

4 **Lorsque vous avez terminé, cliquez sur Suivant pour passer à la page Configuration de la notification de l'approvisionneur.**

▼ Pour configurer un magasin de données de type annuaire

Pour configurer un magasin de données de type annuaire, procédez comme suit :

1 **Choisissez Annuaire dans le menu Type de magasin de données. Des options supplémentaires s'affichent.**

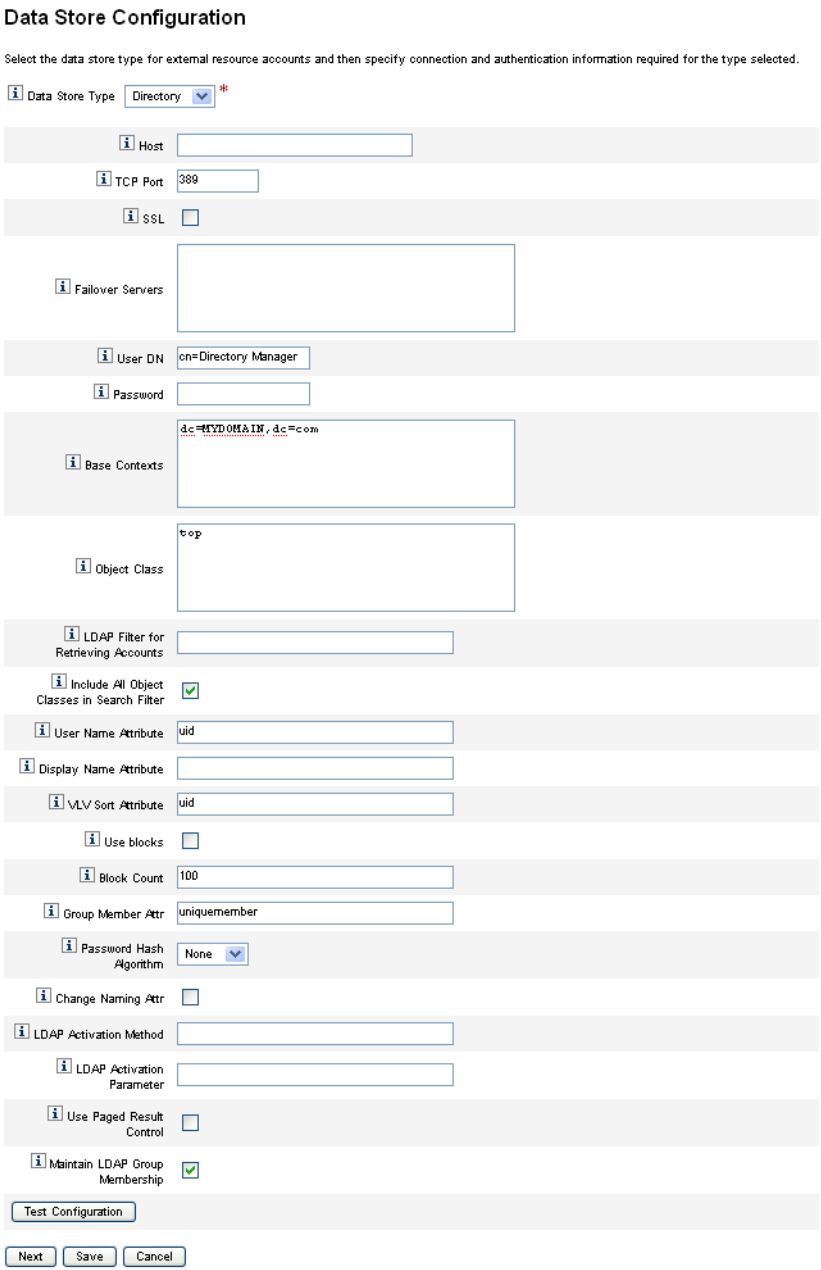


FIGURE 5–16 La Page Configuration du magasin de données : Annuaire

2 Vous devez spécifier les informations de connexion et d'authentification suivantes pour un magasin de données de type Annuaire.

Configurez les options suivantes :

- **Hôte**. Entrez l'adresse IP ou le nom de l'hôte sur lequel le serveur LDAP est exécuté.
- **Port TCP**. Saisissez le port TCP/IP utilisé pour communiquer avec le serveur LDAP.
  - Si vous utilisez SSL, ce port est en général le 636.
  - Si vous n'utilisez pas SSL, ce port est en général le 389.
- **SSL**. Cochez cette option pour connecter le serveur LDAP en utilisant SSL.
- **Serveurs de basculement**. Liste tous les serveurs utilisés pour le basculement en cas de panne du serveur préféré. Saisissez les informations suivantes dans le format indiqué, conforme aux URL LDAP version 3 standard décrites dans le document RFC 2255 :

  ```
  ldap://ldap.example.com:389/o=LdapFailover
  ```

  Seule la partie de l'hôte, du port et du nom distinctif (dn) de l'URL sont pris en compte dans ce paramètre.

  Ainsi, si le serveur préféré tombe en panne, JNDI se connecte automatiquement au prochain serveur disponible de la liste.
- **Utilisateur DN**. Saisissez le DN utilisé pour l'authentification sur le serveur LDAP lors de la réalisation des mises à jour (par défaut `cn=Directory Manager`).
- **Password** (Mot de passe). Saisissez le mot de passe de l'utilisateur principal.
- **Contextes de base**. Spécifiez un ou plusieurs points de départ pouvant être utilisés par Identity Manager pour rechercher des utilisateurs dans l'arborescence LDAP (par défaut `dc=MYDOMAIN,dc=com`).

  Identity Manager effectue des recherches lorsqu'il essaie de découvrir des utilisateurs depuis le serveur LDAP ou lorsqu'il recherche les groupes dont sont membres les utilisateurs.
- **Classe d'objets**. Saisissez une ou plusieurs classes d'objets à utiliser pour créer de nouveaux objets utilisateur dans l'arborescence LDAP (la valeur par défaut est la classe supérieure).

  Chaque entrée doit figurer sur une ligne distincte. N'utilisez pas de virgules ni d'espaces pour séparer les entrées.

  Certains serveurs LDAP exigent que vous spécifiiez toutes les classes d'objets dans une hiérarchie de classes. Par exemple, il se peut que vous ayez besoin de spécifier `top`, `person`, `organizationalperson` et `inetorgperson`, au lieu de seulement `inetorgperson`.
- **Filtre LDAP pour la récupération de comptes**. Saisissez un filtre LDAP pour contrôler les comptes qui seront retournés de la ressource LDAP. Si vous ne spécifiez pas de filtre, Identity Manager retourne tous les comptes qui incluent toutes les classes d'objets spécifiées.
- **Inclure toutes les classes d'objet dans le filtre de recherche**. Cochez cette case pour que tous les comptes incluent toutes les classes d'objets spécifiées et correspondent au Filtre LDAP pour la récupération des comptes.

Remarque – Vous devez activer cette option lorsqu'aucun filtre de recherche n'est spécifié. Si vous désactivez cette option, les comptes qui n'incluent pas toutes les classes d'objets spécifiées peuvent être chargés dans Identity Manager en utilisant la fonctionnalité Réconciliation ou Charger à partir de la ressource.

Après le chargement, l'attribut `objectclass` du compte n'est pas mis à jour automatiquement. Si un attribut d'une classe d'objet manquante apparaît au niveau de l'interface administrateur, l'attribution d'une valeur à cet attribut, sans modification de l'attribut `objectclass`, échoue. Pour éviter un tel problème, annulez la valeur `objectclass` dans le formulaire Réconciliation ou Charger à partir de la ressource.

- **Attribut de nom d'utilisateur**. Saisissez le nom de l'attribut LDAP mappé vers le nom de l'utilisateur Identity Manager lors de la détection des utilisateurs depuis l'annuaire. Ce nom est souvent `uid` ou `cn`.
- **Attribut de nom d'affichage**. Saisissez le nom d'attribut du compte de ressource dont la valeur est utilisée pour l'affichage du nom de ce compte.
- **Attribut de tri VLV**. Saisissez le nom d'un attribut de tri à utiliser pour les index VLV sur la ressource.
- **Utiliser blocs**. Cochez cette case pour récupérer et traiter les utilisateurs par blocs.

  Lorsque vous effectuez des opérations sur un grand nombre d'utilisateurs, traiter les utilisateurs par blocs réduit le volume de mémoire utilisé par l'opération.
- **Comptage de blocs**. Saisissez le nombre maximal d'utilisateurs à regrouper en blocs pour le traitement.
- **Attr. de membre de groupe** Saisissez le nom de l'attribut membre de groupe à mettre à jour avec le nom distinctif de l'utilisateur quand un utilisateur est ajouté au groupe.

  Le nom de cet attribut dépend de la classe d'objet du groupe. Par exemple, Sun Java™ System Enterprise Edition Directory Server et d'autres serveurs LDAP utilisent des groupes avec la classe d'objets `groupOfUniqueNames` et l'attribut `uniqueMember`. D'autres serveurs LDAP utilisent des groupes avec la classe d'objets `groupOfUniqueNames` et l'attribut membre.
- **Algorithme de hachage du mot de passe**. Saisissez un algorithme pouvant être utilisé par Identity Manager pour hacher le mot de passe. Les valeurs prises en charge sont les suivantes :
  - `SSHA`,
  - `SHA`,
  - `SMD5`,
  - `MD5`.

  Si vous spécifiez 0 ou laissez ce champ vide, Identity Manager ne hachera pas les mots de passe et stockera les mots de passe en clair dans LDAP à moins que le serveur LDAP ne procède au hachage. Sun Java System Enterprise Edition Directory Server, par exemple, hache les mots.

- **Attribut de changement de nom**. Cochez cette case pour autoriser les modifications visant à changer l'attribut utilisateur représentant le nom distinctif (DN) relatif le plus à gauche. Les modifications changent fréquemment les attributs de nommage en `uid` ou `cn`.
- **Méthode d'activation LDAP**.
  - Laissez ce champ vide pour que la ressource utilise l'assignation de mots de passe pour les actions d'activation et de désactivation.
  - Saisissez le mot-clé `nsmanageddisabledrole`, le mot-clé `nsaccountlock` ou le nom de la classe à utiliser dans le cadre d'une action d'activation pour les utilisateurs de cette ressource.
- **Paramètre d'activation LDAP**. Saisissez une valeur en fonction de la façon dont vous avez rempli le champ Méthode d'activation LDAP :
  - Si vous avez spécifié le mot-clé `nsmanageddisabledrole`, vous devez entrer une valeur au format suivant :

    IDMAttribute`=CN=nsmanageddisabledrole,`*baseContext*
  - Si vous avez spécifié le mot-clé `nsaccountlock`, vous devez entrer une valeur au format suivant :

    IDMAttribute`=true`
  - Si vous avez spécifié un nom de classe, vous devez entrer une valeur au format suivant :

    IDMAttribute

Remarque – Pour plus d'informations sur les champs Méthode d'activation LDAP et Paramètre d'activation LDAP, voir le document *Sun Identity Manager 8.1 Resources Reference*.

- **Utiliser le contrôle des résultats paginés**. Cochez cette case pour utiliser le contrôle des résultats paginés de LDAP à la place du contrôle VLV pour l'itérateur de compte lors de la réconciliation.

Remarque – La ressource doit prendre en charge le contrôle de pagination simple.

- **Maintenir l'appartenance au groupe LDAP**. Cochez cette case pour que l'adaptateur conserve l'appartenance au groupe LDAP lors du renommage ou de la suppression d'utilisateurs.

  Si vous n'activez pas cette option, la ressource LDAP conserve l'appartenance au groupe.

3 **Testez la configuration de votre magasin de données en cliquant sur le bouton Vérifier la connexion.**

Un message s'affiche confirmant que la connexion a réussi ou indiquant une erreur de configuration.

4 **Lorsque vous avez terminé, cliquez sur Enregistrer puis sur Suivant pour passer à la page Configuration de la notification de l'approvisionneur.**

Remarque – Pour pouvoir créer des utilisateurs sur une ressource LDAP, vous devez commencer par définir des attributs de compte valides, ainsi qu'un modèle d'identification.

Configuration de la notification de l'approvisionneur

Une fois le magasin de données des ressources externes configuré vous devez configurer les notifications aux approvisionneurs. Vous devez aussi configurer les notifications au demandeur. Cette section décrit le processus consistant à configurer les notifications utilisant l'e-mail ou Remedy.

▼ Pour configurer la notification par e-mail

Remarque – Pour plus d'informations sur les modèles d'e-mails, voir Configuration des modèles de tâches.

Utilisez les instructions suivantes pour configurer et envoyer des notifications par e-mail à un ou plusieurs approvisionneurs :

1 **Dans la page Configuration de la notification de l'approvisionneur, sélectionnez E-mail dans le menu Type de notification de l'approvisionneur. Des options supplémentaires s'affichent comme indiqué sur la figure suivante.**

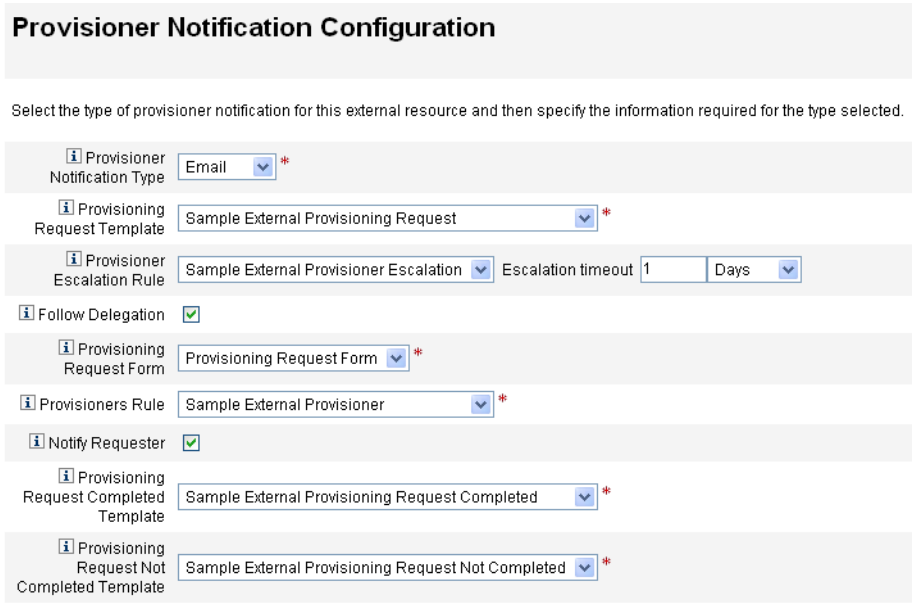


FIGURE 5–17 Page Configuration de la notification de l'approvisionneur : Type de notification de l'approvisionneur

2 Configurez les options suivantes :

- **Modèle de demande de provisioning**. Choisissez Exemple de demande de provisioning externe dans le menu. Ce modèle d'e-mail permet de configurer l'e-mail utilisé pour avertir les approvisionneurs des demandes de ressources externes.
- **Suivre la délégation**. Cochez cette case pour qu'Identity Manager suive les délégations définies pour l'approvisionneur.
- **Règle de signalisation à un approvisionneur** (*facultatif*). Choisissez une règle pour déterminer l'approvisionneur auquel une requête sera signalée si l'approvisionneur courant ne répond pas à la demande dans le délai d'attente spécifié.

Remarque – Bien que plusieurs exemples de règles soient disponibles sur ce menu, vous devez choisir l'exemple de règle *Sample External Provisioner Escalation* ou utiliser votre propre règle personnalisée. La règle Sample External Provisioner Escalation utilise une règle External Provisioner Escalation pour déterminer un approvisionneur pour les signalisations.

- **Délai de signalisation**. Spécifiez la durée maximale qui devra s'écouler avant la signalisation d'une demande de provisioning à l'approvisionneur suivant.

Remarque –

- Si vous laissez ce champ vide ou saisissez un zéro, la demande ne sera jamais signalée.
- Si vous spécifiez un délai d'attente sans sélectionner de Règle de signalisation à un approvisionneur, Identity Manager signale la demande au Configurator quand celle-ci dépasse le délai d'attente spécifié. En l'absence de Configurator, la demande est classée comme « not complete » (non terminée) à l'expiration du délai d'attente.

- **Formulaire de demande de provisioning**. Choisissez un formulaire pouvant être utilisé par l'approvisionneur de ressources externes pour marquer une demande de provisioning comme étant terminée ou non terminée.
- **Règle pour les approvisionneurs**. Vous devez choisir une règle pour définir l'approvisionneur auquel les demandes sont envoyées lorsque les ressources externes sont assignées aux utilisateurs.

Remarque –

- À ces fins, vous pouvez écrire vos propres règles. Vous pouvez aussi définir plusieurs approvisionneurs. Lorsqu'un approvisionneur termine la tâche, cette dernière est supprimée des files d'attente de tous les approvisionneurs. Pour plus d'informations sur l'écriture de règles personnalisées, voir le Chapitre 4, “Working with Rules” du *Sun Identity Manager Deployment Reference*.
- Bien que plusieurs exemples de règles soient disponibles dans ce menu, vous devez choisir la règle *Sample External Provisioner* ou utiliser votre propre règle personnalisée. La règle Sample External Provisioner fait de Configurator l'approvisionneur.

- **Avertir le demandeur** Cochez cette case pour envoyer au demandeur d'origine un e-mail contenant des informations sur le traitement de la demande. Par exemple, si la demande de provisioning est ou non terminée, si des informations supplémentaires sont nécessaires, etc.

  Lorsque vous activez cette option, les champs supplémentaires suivants s'affichent :

Remarque –

- **Modèle de demande de provisioning effectuée**. Choisissez le Modèle de demande de provisioning effectuée pour avertir les demandeurs lorsque leurs demandes sont effectuées.
- **Modèle de demande de provisioning non effectuée**. Choisissez le Modèle de demande de provisioning non effectuée pour avertir les demandeurs lorsque leurs demandes ne sont pas effectuées.

3 **Cliquez sur Enregistrer.**

La page Configurer s'affiche indiquant que vous pouvez passer à l'exécution d'une autre tâche de configuration.

4 **Allez à l'onglet Ressources → Lister les ressources. Vous pouvez maintenant créer des ressources externes individuelles sur la base de cette configuration. Pour les instructions, voir "Pour créer une ressource" à la page 163.**

▼ Pour configurer la notification via Remedy

Utilisez les instructions suivantes pour créer et envoyer un ticket Remedy aux approvisionneurs :

1 **Sélectionnez Remedy dans le menu Type de notification de l'approvisionneur. Des options supplémentaires s'affichent comme indiqué sur la figure suivante.**

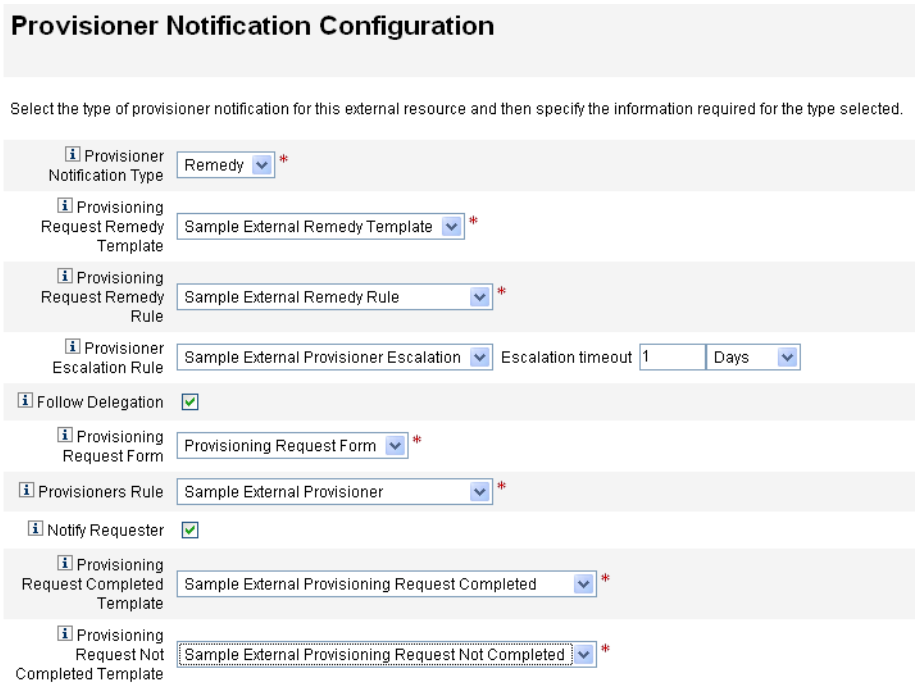


FIGURE 5–18 Page Configuration de la notification de l'approvisionneur : Type de notification Remedy

2 **Configurez les options suivantes :**

- **Modèle Remedy de demande de provisioning**. Choisissez l'exemple de modèle Remedy externe dans le menu.

  Remarque – Identity Manager fournit un exemple de modèle Remedy que vous pouvez utiliser ou modifier selon vos besoins.

  Un modèle Remedy contient un ensemble de champs utilisé pour créer un ticket Remedy. Identity Manager utilise aussi ce modèle pour interroger Remedy sur le statut du ticket, pour voir si une tâche a été ou non effectuée.

- **Règle Remedy de demande de provisioning**. Vous devez choisir une règle dans ce menu pour définir les paramètres de configuration pour Remedy.

  Remarque – Bien que plusieurs exemples de règles soient disponibles dans ce menu, vous devez choisir la règle *Sample External Remedy Rule* ou utiliser votre propre règle personnalisée. La règle Sample External Remedy Rule utilise une règle Remedy pour déterminer si le statut actuel d'un ticket Remedy est effectué ou non effectué.

  Un modèle Remedy contient un ensemble de champs utilisés pour créer un ticket Remedy. Identity Manager utilise aussi ce modèle pour interroger Remedy sur le statut du ticket, pour voir si une tâche a été ou non effectuée.

  Identity Manager utilise cette règle pour interroger un ticket Remedy afin d'obtenir les informations de statut. Si le statut du ticket est effectué ou non effectué, Identity Manager marque l'élément travail comme étant, dans l'ordre, effectué ou non effectué.

  Remarque – À ces fins, vous pouvez écrire vos propres règles. Un exemple de règle appelé Sample External Remedy Rule que vous pouvez utiliser ou modifier est fourni. Pour plus d'informations sur l'écriture de règles personnalisées, voir le Chapitre 4, “Working with Rules” du *Sun Identity Manager Deployment Reference*.

- **Suivre la délégation**. Cochez cette case pour qu'Identity Manager suive les délégations définies pour l'approvisionneur.
- **Règle de signalisation à un approvisionneur** (*facultatif*). Choisissez une règle pour déterminer l'approvisionneur auquel une demande sera signalée si l'approvisionneur courant n'y répond pas dans le délai d'attente spécifié.

Remarque – Bien que plusieurs exemples de règles soient disponibles dans ce menu, vous devez choisir la règle *Sample External Provisioner Escalation* ou utiliser votre propre règle personnalisée. La règle Sample External Provisioner Escalation utilise une règle External Provisioner Escalation pour déterminer un approvisionneur pour les signalisations.

- **Délai de signalisation**. Spécifiez la durée maximale qui devra s'écouler avant la signalisation d'une demande de provisioning à l'approvisionneur suivant.

Remarque –

- Si vous laissez ce champ vide ou saisissez un zéro, la demande ne sera jamais signalée.
- Si vous spécifiez un délai d'attente sans sélectionner de Règle de signalisation à un approvisionneur, Identity Manager signale la demande au Configurator quand celle-ci dépasse le délai d'attente spécifié. En l'absence de Configurator, la demande est classée comme « not complete » (non terminée) à l'expiration du délai d'attente.

- **Formulaire de demande de provisioning**. Choisissez un formulaire pouvant être utilisé par l'approvisionneur de ressources externes pour marquer une demande de provisioning comme étant terminée ou non terminée.
- **Règle pour les approvisionneurs**. Choisissez une règle qui détermine un ou plusieurs approvisionneurs pour cette demande de ressources externes.

Remarque – À ces fins, vous pouvez écrire vos propres règles. Vous pouvez aussi définir plusieurs approvisionneurs. Lorsqu'un approvisionneur termine la tâche, cette dernière est supprimée des files d'attente de tous les approvisionneurs. Pour plus d'informations sur l'écriture de règles personnalisées, voir le Chapitre 4, “Working with Rules” du *Sun Identity Manager Deployment Reference*.

  - **Exemple d'approvisionneur externe**. Faites du Configurator l'approvisionneur.
  - **Exemple de signalisation d'approvisionneur externe**. Utilisez une règle External Provisioner Escalation pour déterminer un approvisionneur pour les signalisations.
  - **Exemple de règle Remedy externe**. Définit les paramètres du configurateur pour Remedy.
- **Avertir le demandeur** Cochez cette case pour envoyer un e-mail au demandeur lorsque sa demande a été/n'a pas été effectuée. Lorsque vous activez cette option, les champs supplémentaires suivants s'affichent :
  - **Modèle de demande de provisioning effectuée**. Choisissez le modèle d'e-mail à utiliser lorsque les demandes ont été effectuées.

- **Modèle de demande de provisioning non effectuée**. Choisissez le modèle d'e-mail à utiliser lorsque les demandes n'ont pas été effectuées.

Remarque – Pour plus d'informations sur les modèles d'e-mails, voir "Configuration des modèles de tâches" à la page 306.

---

3 **Cliquez sur Enregistrer.**

La page Configurer s'affiche indiquant que vous pouvez passer à l'exécution d'une autre tâche de configuration.

4 **Allez à l'onglet Ressources → Lister les ressources. Vous pouvez maintenant créer des ressources externes individuelles sur la base de cette configuration. Pour les instructions, voir "Création de ressources externes" à la page 192.**

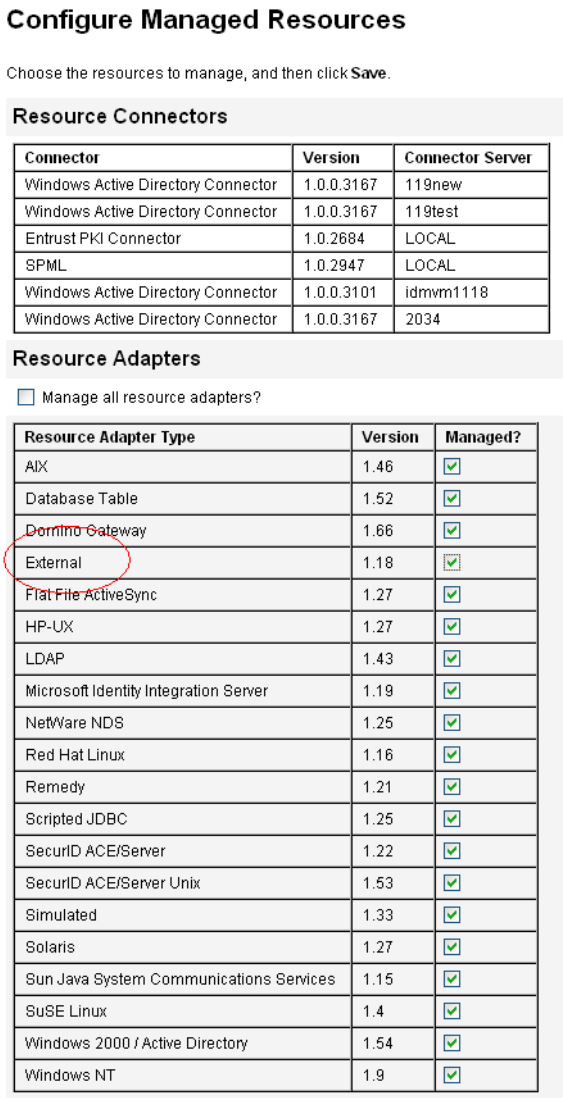
Création de ressources externes

Une fois le magasin de données des ressources externes et les notifications des approvisionneurs configurées, vous pouvez créer une nouvelle ressource externe.

Remarque – Vous devez avoir la capacité Administrateur de ressources pour créer de nouvelles ressources externes.

Pour créer une nouvelle ressource externe, procédez comme suit:

1. Choisissez l'onglet Ressources dans la barre de menu principale. L'onglet Lister les ressources s'affiche par défaut.
2. Cliquez sur l'onglet Configurer les types pour ouvrir la page Configurer les ressources gérées.



Configure Managed Resources

Choose the resources to manage, and then click **Save**.

Resource Connectors

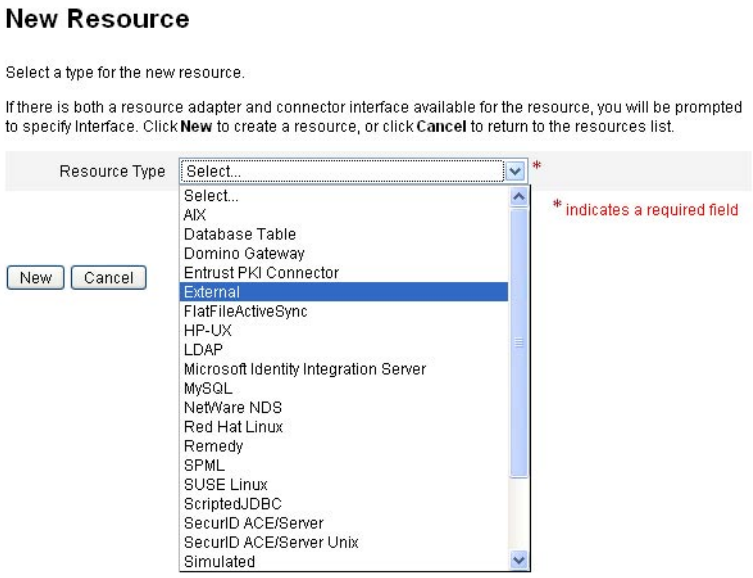
Connector	Version	Connector Server
Windows Active Directory Connector	1.0.0.3167	119new
Windows Active Directory Connector	1.0.0.3167	119test
Entrust PKI Connector	1.0.2684	LOCAL
SPML	1.0.2947	LOCAL
Windows Active Directory Connector	1.0.0.3101	idmvm1118
Windows Active Directory Connector	1.0.0.3167	2034

Resource Adapters

☐ Manage all resource adapters?

Resource Adapter Type	Version	Managed?
AIX	1.46	☑
Database Table	1.52	☑
Domino Gateway	1.66	☑
External	1.18	☑
Flat File ActiveSync	1.27	☑
HP-UX	1.27	☑
LDAP	1.43	☑
Microsoft Identity Integration Server	1.19	☑
NetWare NDS	1.25	☑
Red Hat Linux	1.16	☑
Remedy	1.21	☑
Scripted JDBC	1.25	☑
SecurID ACE/Server	1.22	☑
SecurID ACE/Server Unix	1.53	☑
Simulated	1.33	☑
Solaris	1.27	☑
Sun Java System Communications Services	1.15	☑
SuSE Linux	1.4	☑
Windows 2000 / Active Directory	1.54	☑
Windows NT	1.9	☑

3. Examinez le tableau Adaptateurs de ressources pour vérifier que le type Ressources externes est disponible.
4. Revenez à l'onglet Lister les ressources et choisissez Nouvelle ressource dans le menu Actions du type de ressources.
5. Lorsque la page Nouvelle ressource s'affiche, choisissez Externe dans le menu Type de ressource et cliquez sur Nouveau.



6. La page Bienvenue de l'assistant Create External Resource s'affiche. Cliquez sur Suivant.

   Une vue en lecture seule de la page Configuration du magasin de données s'affiche et indique les informations de connexion et d'authentification définies plus tôt.

   Comme mentionné précédemment, vous ne configurerez normalement qu'une fois ce magasin de données car la configuration s'applique à toutes les ressources externes. Si vous voulez changer certaines de ces informations, vous devez revenir à l'onglet Configurer → Ressources externes.

Remarque – Vous pouvez cliquer sur Vérifier la configuration, dans le bas de la page, pour retester la configuration de magasin de données courante avant d'aller plus loin.

---

7. Cliquez sur Suivant pour ouvrir la page Configuration de la notification de l'approvisionneur, qui est identique à celle configurée dans l'onglet Configurer → Ressources externes.
8. Examinez les paramètres de notification d'approvisionneur actuels et apportez les changements nécessaires pour la nouvelle ressource.

Remarque – Si nécessaire, reportez-vous aux instructions de configuration de "Configuration de la notification de l'approvisionneur" à la page 186. Les changements apportés à cette page ne concerneront que cette ressource.

---

9. Cliquez sur Suivant.

   À partir de ce point, le processus de création d'une ressource externe est identique à celui utilisé pour créer toute autre ressource. L'assistant vous amène à plusieurs autres pages :

   - **Page Attributs de compte**. Cette page permet de définir des attributs de compte optionnels pour la ressource et de mapper les attributs du système Identity vers de nouveaux attributs de compte de ressource. Par exemple, si vous créez une ressource externe appelée « portable », vous pouvez vouloir ajouter des attributs pour le modèle et la taille.

     Remarque – Aucune valeur par défaut n'est précisée pour cette page.

   - **Page Modèle d'identité**. Cette page permet de définir la syntaxe des noms de comptes pour les utilisateurs créés sur cette ressource externe. Vous pouvez utiliser le modèle d'identité par défaut, `$accountId$` ou en spécifier un autre.
   - **Page Paramètres du système d'identité**. Cette page permet de configurer les paramètres du système d'identité pour les ressources externes. Vous pouvez, par exemple, désactiver les stratégies, configurer les relances ou spécifier les approbateurs.

   Pour plus d'informations sur ces pages et les instructions nécessaires pour terminer la configuration de cette ressource, voir "Pour créer une ressource" à la page 163.

10. Lorsque vous avez terminé de configurer la page Paramètres du système d'identité, cliquez sur Enregistrer. Vous pouvez maintenant assigner cette ressource à un utilisateur, comme vous le feriez pour n'importe quelle autre ressource.

Provisioning de ressources externes

Cette section détaille le processus de provisioning actuel et plus précisément :

- "Pour assigner une ressource externe à un utilisateur" à la page 195 ;
- "Pour répondre à une demande de provisioning de ressource externe" à la page 197.

▼ Pour assigner une ressource externe à un utilisateur

Utilisez les étapes suivantes pour assigner une ressource externe à un utilisateur :

Remarque – Pour assigner des ressources externes, vous devez avoir la capacité Administrateur de ressources.

1 Cliquez sur Comptes → Lister les comptes puis sur le nom de l'utilisateur dans la page qui s'affiche.

2 **Lorsque la page Éditer l'utilisateur s'affiche, cliquez sur l'onglet Ressources.**

3 **Localisez la ressource externe dans la liste Ressources disponibles d'Assignation de ressource individuelle, déplacez-la dans la liste Ressources actuelles puis cliquez sur Enregistrer.**

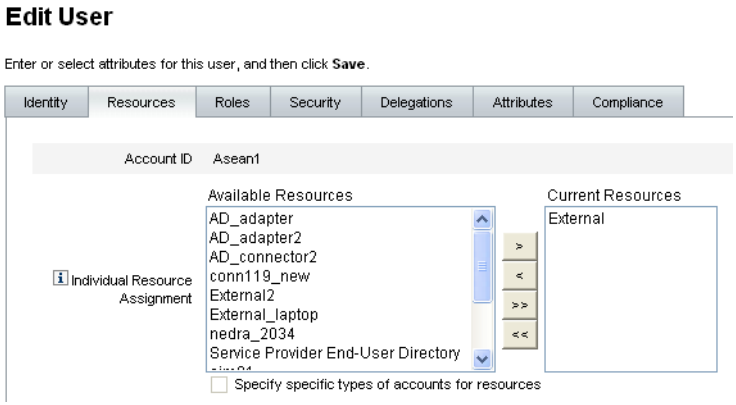


FIGURE 5–19 Page Éditer l'utilisateur

Identity Manager crée une tâche de provisioning et vous envoie un message indiquant quel en est le propriétaire. N'oubliez pas qu'un ou plusieurs approvisionneurs ont été définis, en utilisant la Règle pour les approvisionneurs, lors de la configuration de la page de notification des approvisionneurs pour cette ressource.

Identity Manager avertit également les approvisionneurs qu'ils ont une demande en attente en utilisant un e-mail ou un ticket Remedy.

Remarque – Comme avec d'autres ressources, vous pouvez définir des approbateurs, lesquels pourront approuver ou rejeter les demandes. Vous devez définir des approvisionneurs mais ceux-ci n'approuvent pas ni ne rejettent les requêtes : ils se limitent à terminer ou ne pas terminer pas les tâches.

---

4 **Cliquez sur OK pour revenir à la page Comptes Lister les comptes. Vous remarquerez qu'un sablier s'affiche en regard du nom de l'utilisateur, dans l'icône d'élément de travail, pour indiquer que la demande est en attente.**

▼ Pour répondre à une demande de provisioning de ressource externe

Lorsqu'une demande de provisioning est générée, elle interrompt le processus de provisioning jusqu'à ce qu'un approvisionneur termine le provisioning manuel ou marque la demande comme non effectuée ou le délai d'attente comme dépassé. Identity Manager contrôle ces réponses du provisioning.

Comme avec tout autre élément de travail, vous pouvez examiner l'ensemble de vos demandes de provisioning de ressources externes depuis l'onglet Éléments de travail → Demandes de provisioning.

Vous répondez aux demandes de provisioning comme suit :

1 **Cliquez sur les onglets Éléments de travail > Demandes de provisioning pour ouvrir la page En attente de provisioning.**

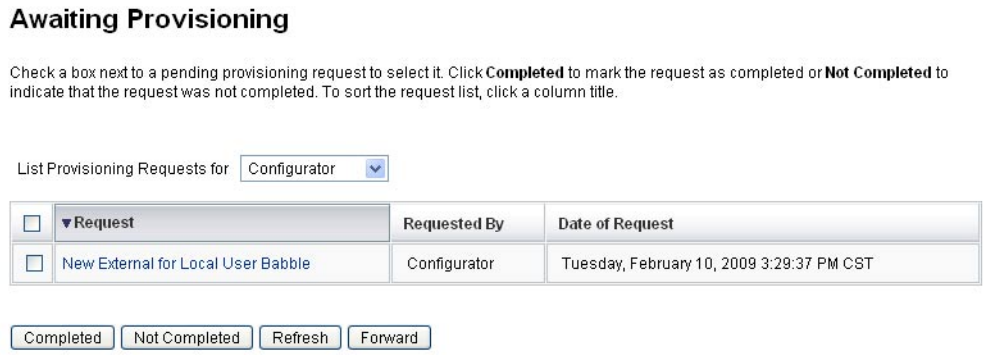


FIGURE 5–20 Page En attente de provisioning

2 **Localisez et sélectionnez la demande de provisioning en attente.**

3 **En option, vous pouvez ouvrir votre e-mail de demande de provisioning, cliquer sur un lien défini dans le Modèle de demande de provisioning et vous connecter pour afficher une page contenant les détails de la demande de provisioning.**

Cette page vous permet de mettre à jour tout attribut demandé de façon à refléter avec précision ce qui a été provisionné pour l'utilisateur. Par exemple, si l'utilisateur a demandé un ordinateur portable Sony, mais que ce modèle n'était pas disponible, vous pouvez mettre la page à jour avec le modèle effectivement provisionné.

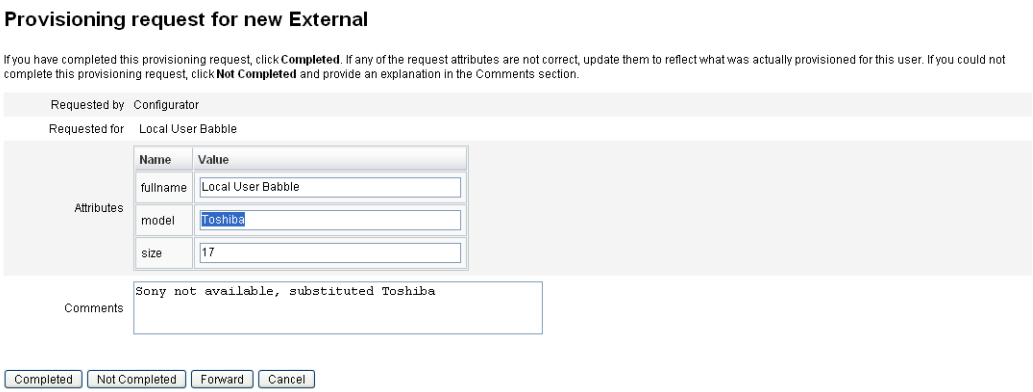


FIGURE 5–21 Demande de provisioning d'un nouvel ordinateur portable

4 Cliquez sur l'un des boutons suivants pour traiter la demande :

- Si vous pouvez provisionner la ressource, cliquez sur Terminé(e).

  Identity Manager met à jour les attributs de compte de ressources externes de l'utilisateur pour indiquer qu'il a effectivement été provisionné, supprime l'indicateur d'état en attente de provisioning et termine l'élément de travail de demande de provisioning mis à jour.

  Selon la configuration, Identity Manager avertit également le demandeur que la demande de provisioning a été effectuée en utilisant le modèle d'e-mail configuré à cette fin.

- Si vous ne pouvez pas provisionner la ressource, précisez le motif et cliquez sur Non terminé(e).

  Lorsque vous marquez une requête comme Non terminé(e) :

  - L'utilisateur n'est pas provisionné à la ressource externe.
  - La ressource externe reste assignée à l'utilisateur.
  - Une icône jaune indiquant qu'une mise à jour s'impose pour l'utilisateur s'affiche à proximité du nom de ce dernier.

    Si l'utilisateur est édité, un message d'erreur s'affiche indiquant qu'il est impossible de trouver l'utilisateur dans la ressource externe.

  - Selon la configuration, Identity Manager avertit également le demandeur en utilisant le modèle d'e-mail configuré à cette fin.

- Si vous ne pouvez pas provisionner la ressource, vous pouvez aussi cliquer sur Transférer pour transférer la demande à un tiers.

Une fois que l'élément de travail de demande de provisioning est effectué ou non effectué, Identity Manager efface l'état En attente de la ressource externe assignée et aucune mise à jour n'a lieu sur le magasin de données des ressources externes.

La ressource s'affiche dans la liste des ressources assignées de l'utilisateur et dans celle des comptes de ressources actuels, avec l'ID de compte de l'utilisateur sur cette ressource.

Remarque – Si l'approvisionneur assigné ne répond pas à une demande de provisioning avant le délai d'attente spécifié, Identity Manager annule l'élément de travail de demande de provisioning associé.

Informations supplémentaires

Réassignation des demandes de provisioning

- Si vous avez spécifiez un délai d'attente lors de la configuration de la page de notification de l'approvisionneur et qu'une demande de provisioning dépasse le délai d'attente, Identity Manager effectue l'une des actions suivantes :
  - Si vous avez spécifié une Règle de signalisation à un approvisionneur, Identity Manager l'utilisera pour déterminer l'approvisionneur suivant et réassignera la demande à cet approvisionneur.
  - Si vous n'avez pas spécifié de Règle de signalisation à un approvisionneur, Identity Manager signale la demande au Configurator. En l'absence de Configurator, la demande est classée comme « not complete » (non terminée) à l'expiration du délai d'attente.
- Si vous laissez le champ du délai d'attente de signalisation vide ou y indiquez un zéro, Identity Manager ne signalera jamais la demande.

Délégation des demandes de provisioning

Vous pouvez déléguer les éléments de travail de provisioning externe comme toutes les autres demandes de provisioning. Pour plus d'informations et les instructions, voir "Délégation des éléments de travail" à la page 234.

Annulation des assignations et suppression des liens des ressources externes

Vous pouvez annuler les assignations ou supprimer les liens de ressources externes depuis un utilisateur, depuis l'onglet Général comme avec toute autre ressource. "Création d'utilisateurs et utilisation des comptes utilisateur" à la page 58,

Remarque – L'annulation de l'assignation ou la suppression du lien d'une ressource externe d'un utilisateur ne crée pas de demande de provisioning ni d'élément de travail. Lorsque vous annulez l'assignation ou supprimez le lien d'une ressource externe, Identity Manager ne suspend pas ni ne supprime le compte de la ressource, vous n'avez donc rien à faire.

Dépannage des ressources externes

Vous ne pouvez pas supprimer des utilisateurs qui ont encore des ressources externes assignées. Vous devez d'abord suspendre ou supprimer ces ressources externes pour pouvoir supprimer les utilisateurs.

Identity Manager vous permet d'utiliser les méthodes suivantes pour déboguer et suivre les ressources externes :

- Vous pouvez suivre l'adaptateur Ressources externes.
  - Si le magasin de données que vous utilisez est une base de données, suivez les noms de classe de suivi `com.waveset.adapter.ScriptedJdbcResourceAdapter` et `com.waveset.adapter.JdbcResourceAdapter`.
  - Si le magasin de données que vous utilisez est un annuaire, suivez le nom de classe de suivi `com.waveset.adapter.LDAPResourceAdapter`.
- Vous pouvez utiliser le suivi des flux de travaux pour suivre des flux de données et de travaux supplémentaires et utiliser le plug-in NetBeans ou Eclipse Identity Manager IDE pour le débogage.
- Étant donné que vous configurez et contrôlez le magasin de données, vous pouvez utiliser l'inspection du magasin de données pour assurer que ce dernier contienne les informations adéquates.
- Identity Manager écrit des enregistrements d'audit pour toutes les activités qui ont lieu.

Pour plus d'informations sur le suivi et le dépannage, voir le *Sun Identity Manager 8.1 System Administrator's Guide*.

◆ ◆ ◆ CHAPITRE 6

Administration

Ce chapitre fournit des informations et des procédures permettant d'effectuer tout un éventail de tâches de niveau administratif dans le système Identity Manager notamment créer et gérer des administrateurs et organisations Identity Manager. Il détaille également l'utilisation des rôles, des capacités et des rôles administratifs dans Identity Manager.

Les informations qu'il contient sont organisées en rubriques comme suit :

Comprendre l'administration d'Identity Manager

Les administrateurs Identity Manager sont des utilisateurs disposant de privilèges Identity Manager étendus.

Les administrateurs Identity Manager gèrent les éléments suivants :

- les comptes utilisateur,
- les objets système tels que les rôles et les ressources,
- les organisations.

Contrairement aux utilisateurs, les administrateurs se voient assigner dans Identity Manager des capacités et des organisations contrôlées définies de la manière suivante :

- **Capacités**. Ensemble de permissions accordant des droits d'accès aux utilisateurs, organisations, rôles et ressources Identity Manager.
- **Organisations contrôlées**. Une fois assigné pour contrôler une organisation, l'administrateur peut gérer les objets se trouvant à l'intérieur de cette organisation ainsi que toutes les organisations situées sous celle-ci dans la hiérarchie.

Administration déléguée

Dans la plupart des entreprises, les employés qui effectuent des tâches administratives assument des responsabilités spécifiques. Par conséquent, les tâches de gestion de comptes que ces administrateurs peuvent effectuer sont d'une étendue limitée.

Par exemple, un administrateur peut être responsable de la seule création des comptes utilisateur Identity Manager. Compte tenu de son domaine, ou étendue, de responsabilité limité, cet administrateur n'aura probablement pas besoin d'informations spécifiques sur les ressources sur lesquelles les comptes utilisateur sont créés ni sur les rôles et organisations existant dans le système.

Identity Manager peut également limiter les administrateurs à des tâches spécifiques au sein d'un domaine ou d'une étendue spécifique défini.

Identity Manager prend en charge la séparation des responsabilités et un modèle d'administration déléguée suivant les points ci-après :

- Les **capacités** assignées limitent les administrateurs à des obligations professionnelles spécifiques.
- Les **organisations contrôlées** assignées limitent les administrateurs au seul contrôle d'organisations spécifiques (et des objets que celles-ci contiennent).
- Les vues filtrées des page Créer un utilisateur et Éditer l'utilisateur empêchent les administrateurs d'afficher des informations non pertinentes dans le cadre de leurs fonctions.

Vous pouvez spécifier des délégations pour un utilisateur depuis la page Créer un utilisateur lorsque vous configurez un nouveau compte utilisateur ou éditez un compte utilisateur existant.

Vous pouvez aussi déléguer des éléments de travail, par exemple des demandes d'approbation, depuis l'onglet Éléments de travail. Pour plus d'informations sur les délégations, voir “Délégation des éléments de travail” à la page 234.

Création et gestion des administrateurs

Cette section se compose des rubriques suivantes :

▼ Pour créer un administrateur

Pour créer un administrateur, vous devez assigner une ou plusieurs capacités à un utilisateur et désigner les organisations auxquelles ces capacités s'appliqueront.

1 **Dans l'interface administrateur, cliquez sur Comptes dans la barre de menu.**

La page Liste des utilisateurs s'ouvre.

2 **Pour conférer à un utilisateur existant des privilèges administratifs, cliquez sur son nom d'utilisateur (la page Éditer l'utilisateur s'ouvre) puis sur l'onglet Sécurité.**

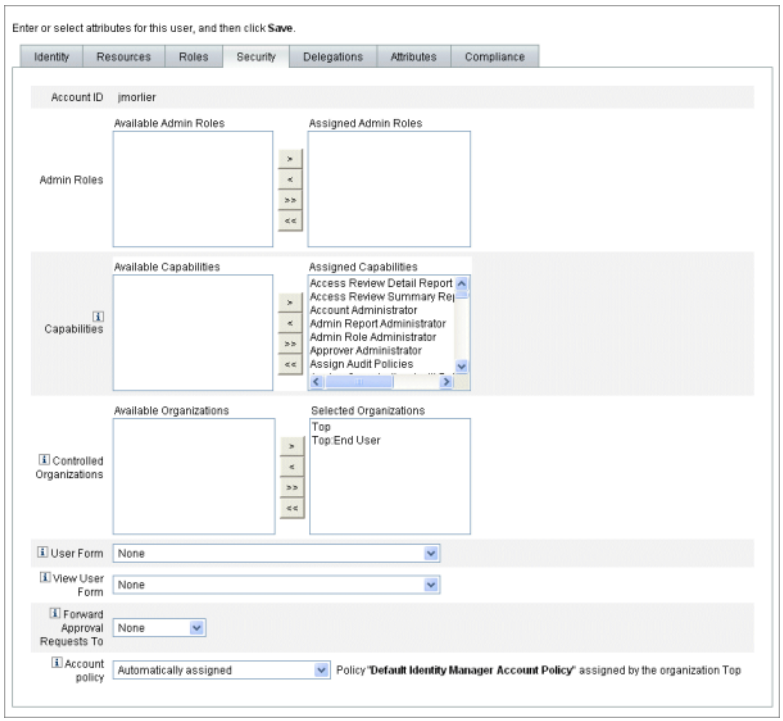
Pour créer un nouveau compte utilisateur, voir la section "Création d'utilisateurs et utilisation des comptes utilisateur" à la page 58.

3 **Spécifiez les attributs pour établir le contrôle administratif.**

Les attributs disponibles sont les suivants :

- **Capacités**. Sélectionnez une ou plusieurs capacités à assigner à cet administrateur. Ces informations sont obligatoires. Pour plus d'informations, voir "Comprendre et gérer les capacités" à la page 216.
- **Organisations contrôlées**. Sélectionnez une ou plusieurs organisations à assigner à cet administrateur. L'administrateur contrôlera les objets de l'organisation assignée et ceux de toutes les organisations situées sous celle-ci dans la hiérarchie. Ces informations sont obligatoires. Pour plus d'informations, voir "Comprendre les organisations d'Identity Manager" à la page 209.
- **Formulaire utilisateur**. Spécifie le formulaire utilisateur qui sera utilisé par l'administrateur pour créer et éditer des utilisateurs Identity Manager (si cette capacité est assignée). Si vous n'assignez pas directement de formulaire utilisateur, l'administrateur héritera de celui assigné à l'organisation dont il est membre. Le formulaire sélectionné ici remplace tout autre formulaire choisi dans l'organisation de cet administrateur.

- **Transmettre demandes d'approbation à**. Permet de sélectionner un utilisateur auquel toutes les demandes d'approbation actuellement en attente seront transmises. Ce paramètre relatif à l'administrateur peut aussi être défini sur la page Approbations.
- **Déléguer les éléments de travail à**. Si disponible, cette option permet de spécifier des délégations pour ce compte utilisateur. Vous pouvez spécifier le responsable de l'administrateur, un ou plusieurs utilisateurs sélectionnés ou utiliser une règle d'approbateurs délégués.



Filtrage des vues administrateur

En assignant des formulaires utilisateur aux organisations et administrateurs, vous établissez des vues administrateur spécifiques des informations des utilisateurs.

L'accès aux informations des utilisateurs se définit à deux niveaux :

- **Organisation**. Lorsque vous créez une organisation, vous assignez le formulaire utilisateur que tous les administrateurs de cette organisation utiliseront pour créer et éditer des utilisateurs Identity Manager. Tout formulaire défini au niveau administrateur remplace le formulaire défini ici. Si aucun formulaire n'est sélectionné pour l'administrateur ou l'organisation, Identity Manager hérite du formulaire sélectionné pour l'organisation parent. Si aucun formulaire n'est défini dans celle-ci, Identity Manager utilise le formulaire par défaut défini dans la configuration système.
- **Administrateur**. Lorsque vous assignez des capacités administratives à un utilisateur, vous pouvez assigner directement un formulaire utilisateur à l'administrateur. Si vous n'assignez pas de formulaire, l'administrateur hérite du formulaire assigné à son organisation (ou en l'absence de ce dernier du formulaire par défaut défini dans la configuration système).

"Comprendre et gérer les capacités" à la page 216 décrit les capacités Identity Manager intégrées que vous pouvez assigner.

Changement des mots de passe administrateur

Les mots de passe administrateur peuvent être changés par un administrateur auquel des capacités de changement de mots de passe administratifs ont été assignée ou par le propriétaire de l'administrateur.

Les administrateurs peuvent changer le mot de passe d'un autre administrateur en utilisant les formulaires suivants :

- **Formulaire Changer le mot de passe de l'utilisateur**. Vous pouvez ouvrir ce formulaire des deux manières suivantes :
  - Cliquez sur Comptes dans le menu. La Liste des utilisateurs s'ouvre. Sélectionnez un administrateur puis, dans la liste Actions de l'utilisateur, sélectionnez Changement du mot de passe. La page Changer le mot de passe de l'utilisateur s'ouvre.
  - Cliquez sur Mots de passe dans le menu. La page Changer le mot de passe de l'utilisateur s'ouvre.
- **Formulaire utilisateur à onglets**. Cliquez sur Comptes dans le menu. La Liste des utilisateurs s'ouvre. Sélectionnez un administrateur puis, dans la liste Actions de l'utilisateur, sélectionnez Éditer. La page Éditer l'utilisateur (Formulaire utilisateur à onglets) s'ouvre. Sur l'onglet Identité du formulaire, saisissez un nouveau mot de passe dans les champs Mot de passe et Confirmez le mot de passe.

Un administrateur peut changer son propre mot de passe depuis la zone Mots de passe. Cliquez sur Mots de passe dans le menu puis sur Changer mon mot de passe.

Remarque – La stratégie de compte Identity Manager appliquée au compte détermine les limites en matière de mots de passe telles que l'expiration du mot de passe, les options de réinitialisation et les sélections de notification. Des limites de mot de passe supplémentaires peuvent être fixées par les stratégies de mot de passe définies sur les ressources de l'administrateur.

Demande d'actions de la part de l'administrateur

Identity Manager peut être configuré pour inviter les administrateurs à saisir un mot de passe avant de traiter certains changements de compte. Si l'authentification échoue, les changements de compte en question sont annulés.

Les administrateurs peuvent utiliser trois formulaires pour changer les mots de passe des utilisateurs : le formulaire Utilisateur à onglets, le formulaire Changer le mot de passe de l'utilisateur et le formulaire Réinitialiser le mot de passe de l'utilisateur. Pour assurer que les administrateurs seront obligés de saisir leur mot de passe pour que Identity Manager puisse traiter les changements de compte utilisateur, veillez à mettre à jour l'ensemble de ces trois formulaires :

▼ Pour activer l'option de demande de mot de passe pour les formulaires utilisateur à onglets

Pour imposer une demande de mot de passe sur le formulaire Utilisateur à onglets, procédez comme suit :

1. **Dans l'interface administrateur, ouvrez la page de débogage d'Identity Manager ("Page de débogage d'Identity Manager" à la page 45) en saisissant l'URL suivant dans votre navigateur (vous devez avoir la capacité Déboguer pour pouvoir ouvrir cette page).**

   `http://<`*HôteServeurApp*`>:<` *Port*`>/idm/debug/session.jsp`

   La page System Settings (Paramètres du système, page de débogage d'Identity Manager) s'ouvre.

2. **Recherchez le bouton List Objects (Lister les objets), sélectionnez UserForm dans le menu déroulant puis cliquez sur le bouton ListObjects.**

   La page List Objects of type (Lister les objets de type) : UserForm s'ouvre.

3. **Localisez la copie du formulaire Utilisateur à onglets que vous avez en production et cliquez sur Edit (Éditer). Le formulaire Utilisateur à onglets (Tabbed User Form) distribué avec Identity Manager est un modèle et ne devrait pas être modifié.**

4 **Ajoutez le snippet de code suivant dans l'élément** `<Form>` **:**

```
<Properties>
  <Property name='RequiresChallenge'>
    <List>
      <String>password</String>
      <String>email</String>
      <String>fullname</String>
    </List>
  </Property>
</Properties>
```

La valeur de la propriété est une liste pouvant contenir un ou plusieurs des noms d'attributs de vue utilisateur suivants :

- `applications`,
- `adminRoles`,
- `assignedLhPolicy`,
- `capabilities`,
- `controlledOrganizations`,
- `email`,
- `firstname`,
- `fullname`,
- `lastname`,
- `organization`,
- `password`,
- `resources`,
- `roles`.

5 **Enregistrez vos modifications.**

▼ Pour activer l'option de demande de mot de passe pour les formulaires Changer le mot de passe de l'utilisateur et Réinitialiser le mot de passe de l'utilisateur

Pour imposer une demande de mot de passe pour les formulaires Changer le mot de passe de l'utilisateur et Réinitialiser le mot de passe de l'utilisateur, procédez comme suit :

1 **Dans l'interface administrateur, ouvrez la page de débogage d'Identity Manager ("Page de débogage d'Identity Manager" à la page 45) en saisissant l'URL suivant dans votre navigateur (vous devez avoir la capacité Déboguer pour pouvoir ouvrir cette page).**

`http://<`*HôteServeurApp*`>:<` *Port*`>/idm/debug/session.jsp`

La page System Settings (Paramètres du système, page Déboguer Identity Manager) s'ouvre.

2 **Recherchez le bouton List Objects (Lister les objets), sélectionnez UserForm dans le menu déroulant puis cliquez sur le bouton ListObjects.**

La page List Objects of type (Lister les objets de type) : UserForm s'ouvre.

3 **Localisez la copie du formulaire Changer le mot de passe de l'utilisateur que vous avez en production et cliquez sur edit (Éditer). Le formulaire Changer le mot de passe de l'utilisateur distribué avec Identity Manager est un modèle et ne devrait pas être modifié.**

4 **Localisez l'élément `<Form>` puis allez à l'élément `<Properties>`.**

5 **Ajoutez la ligne suivante à l'intérieur de l'élément `<Properties>` et enregistrez vos changements.**

```
<Property name='RequiresChallenge' value='true'/>
```

6 **Répétez les étapes 3 à 5 à l'exception de l'édition de la copie du formulaire Utilisateur à onglets que vous avez en production.**

Changement des réponses aux questions d'authentification

Utilisez la zone Mots de passe pour modifier les réponses que vous avez définies pour les questions d'authentification de compte. Dans la barre de menu, sélectionnez Mots de passe puis Changer mes réponses.

Pour plus d'informations sur l'authentification, voir la section "Authentification des utilisateurs" à la page 92 au Chapitre 3, "Gestion des utilisateurs et des comptes".

Personnalisation de l'affichage du nom de l'administrateur dans l'interface administrateur

Vous pouvez afficher un administrateur Identity Manager par l'un de ses attributs (par exemple son e-mail `email` ou son nom complet `fullname`) au lieu de le faire par son ID de compte dans certaines pages et zones de l'interface administrateur d'Identity Manager.

Par exemple, vous pouvez afficher les administrateurs Identity Manager par attribut dans les zones suivantes :

- Éditer l'utilisateur (liste de sélection pour faire suivre les approbations) ;
- le tableau Rôle ;
- Créer/Éditer un rôle ;
- Créer/Éditer une ressource ;
- Créer/Éditer une organisation/jonction d'annuaires ;

- Approbations.

Pour configurer Identity Manager pour utiliser un nom à afficher, ajoutez ce qui suit à l'objet `UserUIConfig` :

```
<AdminDisplayAttribute>
  <String>attribute_name</String>
</AdminDisplayAttribute>
```

Par exemple, pour utiliser l'attribut email (e-mail) en tant que nom à afficher, ajoutez le nom d'attribut suivant à `UserUIconfig` :

```
<AdminDisplayAttribute>
  <String>email</String>
</AdminDisplayAttribute>
```

Comprendre les organisations d'Identity Manager

Les organisations permettent de :

- gérer de manière logique et sécurisée les comptes utilisateur et les administrateurs ;
- limiter l'accès aux ressources, applications, rôles et autres objets Identity Manager.

Créer des organisations et assigner des utilisateurs à divers emplacements dans une hiérarchie organisationnelle permet de planter le décor pour l'administration déléguée. Les organisations qui contiennent une ou plusieurs autres organisations sont des *organisations parentes*.

Tous les utilisateurs Identity Manager (administrateurs compris) sont *assignés statiquement* à une organisation. Les utilisateurs peuvent aussi être *assignés dynamiquement* à des organisations supplémentaires.

Les administrateurs Identity Manager sont de plus assignés pour *contrôler* des organisations.

Création d'organisations

▼ Pour créer une organisation

Vous créez des organisations dans la zone Comptes d'Identity Manager.

1 **Dans l'interface administrateur, cliquez sur Comptes dans la barre de menu.**

La page Liste des utilisateurs s'ouvre.

2 **Dans le menu Nouvelles actions, sélectionnez Nouvelle organisation.**

Astuce – Pour créer une organisation dans un emplacement spécifique de la hiérarchie organisationnelle, sélectionnez une organisation dans la liste puis sélectionnez Nouvelle organisation dans le menu Nouvelles actions.

La Figure 6–1 illustre la page Créer une organisation.

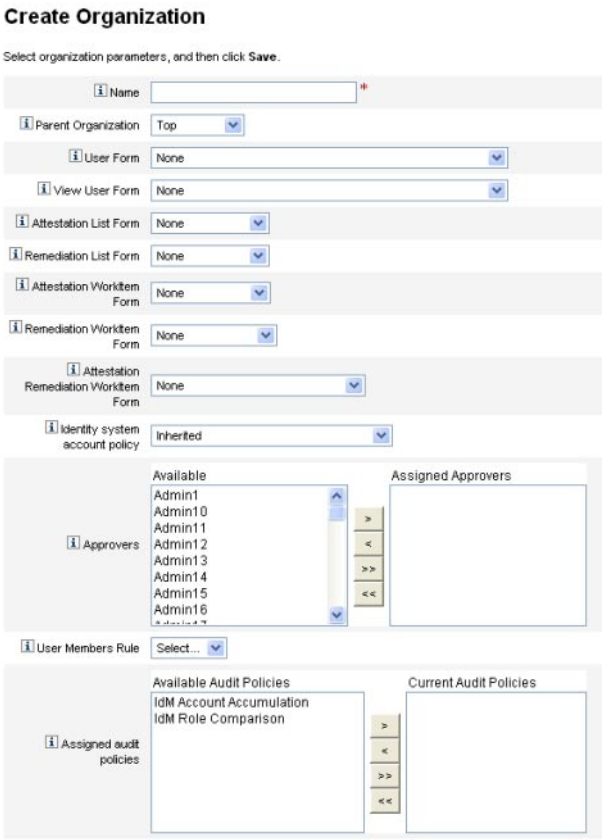


FIGURE 6–1 Page Créer une organisation

Assignation d'utilisateurs aux organisations

Tout utilisateur est un membre statique d'une organisation et peut être un membre dynamique de plusieurs organisations.

Vous définissez l'appartenance à une organisation en utilisant l'une des méthodes suivantes :

- **Assignation directe (statique)**. Sélectionnez l'onglet de formulaire Identité sur la page Créer un utilisateur ou la page Éditer l'utilisateur pour assigner directement les utilisateurs à une organisation. Tout utilisateur doit être assigné directement à une organisation.
- **Assignation gérée par règle (dynamique)**. Utilisez une Règle Membres utilisateurs assignée à une organisation pour assigner des utilisateurs à cette organisation. La règle, lorsqu'elle est évaluée, retourne un ensemble d'utilisateurs membres.

  Identity Manager évalue la Règle Membres utilisateurs au moment de :

  - lister les utilisateurs d'une organisation ;
  - rechercher des utilisateurs (par le biais de la page Rechercher des utilisateurs), notamment rechercher des utilisateurs se trouvant dans une organisation avec une Règle Membres utilisateurs ;
  - demander l'accès à un utilisateur, à condition que l'administrateur courant contrôle une organisation avec une Règle Membres utilisateurs.

Remarque – Pour plus d'informations sur la création et l'utilisation des règles dans Identity Manager, voir le Chapitre 4, "Working with Rules" du *Sun Identity Manager Deployment Reference*.

Sélectionnez une Règle Membres utilisateurs dans le menu Règle Membres utilisateurs sur la page Créer une organisation. La figure suivante donne un exemple de règle Membres utilisateurs.

L'exemple suivant illustre la syntaxe d'un exemple de Règle Membres utilisateurs utilisé pour contrôler de manière dynamique l'appartenance d'un utilisateur à une organisation.

Remarque –

Avant de créer une Règle Membres utilisateurs, vous devez savoir ce qui suit :

- Pour qu'une règle figure dans la case d'option Règle Membres utilisateurs, son `authType` doit être défini de la manière suivante : `authType='UserMembersRule'`.
- Le contexte est la session Identity Manager actuellement authentifiée de l'utilisateur.
- La variable définie `(defvar) Team players` obtient le nom distinctif (dn) de tout utilisateur membre de l'unité organisationnelle (organization unit, o.u.) Windows Active Directory `Pro Ball Team`.
- Pour chaque utilisateur trouvé, la logique append concatènera le dn de l'utilisateur membre de l'o.u. `Pro Ball Team` au nom de la ressource Identity Manager en utilisant le signe deux-points comme préfixe (par exemple `:smith-AD`).
- Les résultats retournés seront une liste de dn concaténés avec le nom de la ressource Identity Manager, de format *dn* `:smith-AD`.

EXEMPLE 6–1 Exemple de règle Membres utilisateurs

```
<Rule name='Get Team Players' authType='UserMembersRule'>
  <defvar name='Team players'>
    <block>
      <defvar name='player names'>
        <list/>
      </defvar>
  <dolist name='users'>
    <invoke class='com.waveset.ui.FormUtil' name='getResourceObjects'>
      <ref>context</ref>
      <s>User</s>
      <s>singleton-AD</s>
      <map>
        <s>searchContext</s>
        <s>OU=Pro Ball Team,DC=dev-ad,DC=waveset,DC=com</s>
        <s>searchScope</s>
        <s>subtree</s>
        <s>searchAttrsToGet</s>
        <list>
          <s>distinguishedName</s>
        </list>
      </map>
    </invoke>
    <append name='player names'>
    <concat>
      <get>
        <ref>users</ref>
```

EXEMPLE 6–1 Exemple de règle Membres utilisateurs *(Suite)*

```
        <s>distinguishedName</s>
      </get>
        <s>:sampson-AD</s>
    </concat>
    </append>
  </dolist>
    <ref>player names</ref>
  </block>
   </defvar>
    <ref>Team players</ref>
</Rule>
```

Remarque – Vous pouvez configurer plusieurs propriétés dans `Waveset. properties` pour contrôler le cache de la liste Utilisateurs membres gérée par règle, qui peut avoir un effet négatif sur la mémoire et les performances. Pour toute information, voir "Tracing Rule-Driven Members Caches" du *Sun Identity Manager 8.1 System Administrator's Guide*.

Assignation du contrôle des organisations

Assignez le contrôle administratif d'une ou plusieurs organisations depuis la page Créer un utilisateur ou Éditer l'utilisateur. Sélectionnez l'onglet de formulaire Sécurité pour afficher le champ Organisations contrôlées.

Vous pouvez aussi assigner le contrôle administratif des organisations en assignant un ou plusieurs rôles admin, depuis le champ Rôles admin.

Comprendre les jonctions d'annuaires et les organisations virtuelles

Une *jonction d'annuaires* est un ensemble d'organisations reliées hiérarchiquement qui reflète le jeu de conteneurs hiérarchiques courant d'une ressource d'annuaire. Une *ressources d'annuaire* est une ressource qui emploie un espace de noms hiérarchique à travers l'utilisation de conteneurs hiérarchiques. Les serveurs LDAP et les ressources de Windows Active Directory sont des exemples de ressources d'annuaire.

Toute organisation contenue dans une jonction d'annuaires est une *organisation virtuelle*. L'organisation virtuelle supérieure d'une jonction d'annuaires est un miroir du conteneur représentant le contexte de base défini dans la ressource. Les organisations virtuelles restantes d'une jonction d'annuaires sont les enfants *directs* ou *indirects* de l'organisation virtuelle

supérieure et reflètent également l'un des conteneurs de ressources d'annuaire enfants du conteneur de contexte de base de la ressource définie. Cette structure est illustrée à la Figure 6–2.

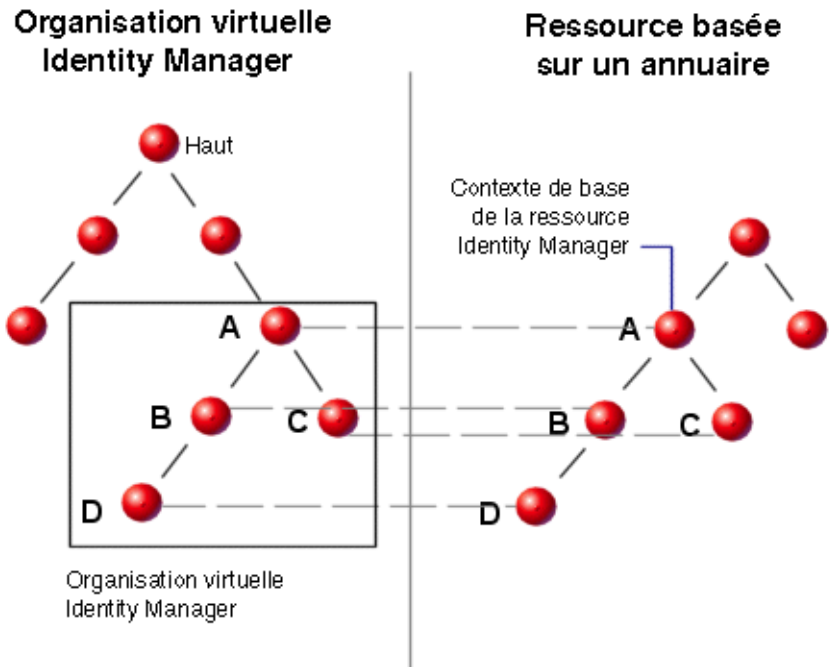


FIGURE 6–2 Organisation virtuelle d'Identity Manager

Les jonctions d'annuaires peuvent être collées en tout point de la structure organisationnelle Identity Manager existante. Elles ne peuvent toutefois pas être collées dans ou sous une jonction d'annuaires existante.

Une fois une jonction d'annuaires ajoutée à l'arborescence organisationnelle d'Identity Manager, vous pouvez créer ou supprimer des organisations virtuelles dans le contexte de cette jonction d'annuaires. De plus, vous pouvez actualiser l'ensemble d'organisations virtuelles englobant une jonction d'annuaires à tout moment pour assurer que celles-ci restent synchronisées avec les conteneurs de ressources d'annuaire. Vous ne pouvez pas créer une organisation non virtuelle au sein d'une jonction d'annuaire.

Vous pouvez rendre les objets Identity Manager (tels que les utilisateurs, ressources et rôles) membres d'une organisation virtuelle et les mettre à disposition de celle-ci de la même façon qu'une organisation Identity Manager.

Configuration des jonctions d’annuaires

Cette section décrit comment configurer une jonction d'annuaires.

▼ Pour configurer une jonction d'annuaires

1. **Dans l'interface administrateur, cliquez sur Comptes dans la barre de menu.**

   La page Liste des utilisateurs s'ouvre.

2. **Sélectionnez une organisation Identity Manager dans la liste Comptes.**

   L'organisation que vous sélectionnez deviendra l'organisation parent de l'organisation virtuelle que vous configurez.

3. **Dans le menu Nouvelles actions, sélectionnez Nouvelle jonction d’annuaires.**

   Identity Manager ouvre la page Créer une jonction d’annuaires.

4. **Utilisez les options de la page Créer une jonction d’annuaires pour configurer l'organisation virtuelle.**

   Ces options sont les suivantes :

   - **Organisation parent**. Ce champ contient l'organisation que vous avez sélectionnée dans la liste Comptes ; vous pouvez cependant sélectionner une autre organisation parent dans la liste.
   - **Ressource de répertoires**. Sélectionnez la ressource de répertoires qui gère l'annuaire existant dont vous voulez refléter la structure dans l'organisation virtuelle.
   - **Formulaire utilisateur**. Sélectionnez un formulaire utilisateur qui s'appliquera aux administrateurs de cette organisation.
   - **Stratégie de compte Identity Manager**. Sélectionnez une stratégie ou sélectionnez l'option par défaut (Hérité) pour hériter de la stratégie de l'organisation parent.
   - **Approbateurs**. Sélectionnez les administrateurs qui peuvent approuver les demandes relatives à cette organisation.

Actualisation des organisations virtuelles

Ce processus actualise et resynchronise l'organisation virtuelle avec la ressource d'annuaire associée, en partant de l'organisation. Sélectionnez l'organisation virtuelle dans la liste puis sélectionnez Actualiser l’organisation dans la liste Actions d’organisation.

Suppression des organisations virtuelles

Pour supprimer des organisations virtuelles, vous disposez des deux options suivantes :

- **Supprimer l'organisation Identity Manager uniquement**. Supprime uniquement la jonction d'annuaires Identity Manager.
- **Supprimer l'organisation Identity Manager et le conteneur de ressources**. Supprime la jonction d'annuaires Identity Manager et l'organisation correspondante sur la ressource native.

Choisissez une option, puis cliquez sur Supprimer.

Comprendre et gérer les capacités

Dans le système Identity Manager, les capacités sont des groupes de droits. Elles représentent des responsabilités administratives professionnelles telles que la réinitialisations de mots de passe ou l'administration des comptes utilisateur. Chaque utilisateur administratif Identity Manager se voit assigner une ou plusieurs capacités, qui fournissent un ensemble de privilèges sans compromettre la protection des données.

Il est inutile d'assigner des capacités à tous les utilisateurs Identity Manager. Seuls les utilisateurs qui seront amenés à effectuer une ou plusieurs actions administratives par le biais d'Identity Manager ont besoin de capacités. Par exemple, aucune capacité assignée n'est nécessaire pour permettre à un utilisateur de changer son mot de passe, mais il en faut une pour changer le mot de passe d'un autre utilisateur.

Les capacités qui vous sont assignées déterminent les zones de l'interface administrateur d'Identity Manager auxquelles vous pouvez accéder.

Tous les utilisateurs administratifs Identity Manager peuvent accéder aux zones suivantes d'Identity Manager :

- aux onglets **Accueil** et **Aide**,
- à l'onglet **Mots de passe** (sous-onglets Changer mon mot de passe et Changer mes réponses uniquement),
- à la zone **Rapports** (limitée aux types liés aux responsabilités spécifiques de l'administrateur).

Remarque – La liste des capacités fonctionnelles et basées sur des tâches par défaut d'Identity Manager (définitions incluses) figure à l'Annexe D, “Définitions des capacités”. Cette annexe répertorie également les onglets et sous-onglets auxquels chaque capacité basée sur des tâches permet d'accéder.

Catégories de capacités

Identity Manager définit des capacités des deux types suivants :

- **Capacités basées sur des tâches**. Ces capacités sont des capacités au plus simple niveau de tâche.
- **Capacités fonctionnelles**. Les capacités fonctionnelles contiennent une ou plusieurs autres capacités fonctionnelles ou basées sur des tâches.

Les capacités intégrées (fournies avec le système Identity Manager) sont *protégées*, ce qui signifie que vous ne pouvez pas les éditer. Vous pouvez cependant les utiliser au sein des capacités que vous créez.

Les capacités protégées (intégrées) sont signalées dans la liste par une icône en forme de clé rouge (ou une clé et un dossier rouges). Les capacités que vous créez et pouvez éditer sont signalées dans la liste des capacités par une icône en forme de clé verte (ou une clé et un dossier verts).

Travailler avec les capacités

Cette section explique la création, l'édition, l'assignation et le renommage des capacités. Ces tâches sont effectuées en utilisant la page Capacités.

Affichage de la page Capacités

La page Capacités figure sous l'onglet Sécurité.

▼ Pour ouvrir la page Capacités

1. **Dans l'interface administrateur, cliquez sur Sécurité dans le menu supérieur.**
2. **Cliquez sur Capacités dans le menu secondaire.**

   La page Capacité contenant une liste de capacités Identity Manager s'ouvre.

Création d'une capacité

Suivez la procédure ci-après pour créer une capacité. Pour *cloner* une capacité, voir “Sauvegarde et renommage d'une capacité” à la page 219.

▼ Pour créer une capacité

1. **Dans l'interface administrateur, cliquez sur Sécurité dans le menu supérieur.**
2. **Cliquez sur Capacités dans le menu secondaire.**
   La page Capacité contenant une liste de capacités Identity Manager s'ouvre.
3. **Cliquez sur Nouveau.**
   La page Créer une capacité s'ouvre.
4. **Remplissez le formulaire comme suit :**
   a. **Donnez un nom à la nouvelle capacité.**
   b. **Dans la section Capacités, utilisez les touches fléchées pour déplacer les capacités à assigner aux utilisateurs dans la zone Capacités assignées.**
   c. **Dans la zone Assignataires, sélectionnez le ou les utilisateurs qui seront autorisés à assigner cette capacité à d'autres utilisateurs.**
      - Si aucun utilisateur n'est sélectionné, le seul utilisateur qui sera en mesure d'assigner cette capacité sera celui qui l'a créée.
      - Si l'utilisateur qui a créé la capacité n'est pas associé à la capacité Assigner la capacité utilisateur, vous devez sélectionner un ou plusieurs utilisateurs pour qu'au moins un utilisateur puisse assigner cette capacité à un autre utilisateur.
   d. **Dans la zone Organisations, sélectionnez une ou plusieurs organisations pour lesquelles cette capacité sera disponible.**
   e. **Cliquez sur Enregistrer.**

Remarque – Le jeu d'utilisateurs dans lequel vous pouvez effectuer sélectionner des assignataires se compose des personnes disposant de la capacité d'assignation.

Édition d'une capacité

Vous pouvez éditer une capacité non protégée.

▼ Pour éditer une capacité non protégée

1. **Dans l'interface administrateur, cliquez sur Sécurité dans le menu supérieur.**
2. **Cliquez sur Capacités dans le menu secondaire.**

   Page Capacité contenant une liste de capacités Identity Manager s'ouvre.
3. **Cliquez avec le bouton droit sur la capacité de votre choix dans la liste puis sélectionnez Éditer. La page Éditer une capacité s'ouvre.**
4. **Apportez vos modifications puis cliquez sur Enregistrer.**

   Vous ne pouvez pas éditer les capacités intégrées. Vous pouvez cependant les enregistrer sous un autre nom pour vous créer une capacité propre. Vous pouvez aussi utiliser les capacités intégrées dans les capacités que vous créez.

Sauvegarde et renommage d'une capacité

Vous pouvez créer une nouvelle capacité en enregistrant une capacité existante sous un nouveau nom. On parle alors de *clonage* de capacité.

▼ Pour cloner une capacité

1. **Dans l'interface administrateur, cliquez sur Sécurité dans le menu supérieur.**
2. **Cliquez sur Capacités dans le menu secondaire.**

   La page Capacité contenant une liste de capacités Identity Manager s'ouvre.
3. **Cliquez avec le bouton droit sur la capacité de votre choix dans la liste puis sélectionnez Enregistrer sous.**

   Une boîte de dialogue s'ouvre vous demandant de saisir un nom pour la nouvelle capacité.
4. **Saisissez un nom puis cliquez sur OK.**

   Vous pouvez maintenant éditer la nouvelle capacité.

Assignation de capacités aux utilisateurs

Utilisez la page Créer un utilisateur ("Création d'utilisateurs et utilisation des comptes utilisateur" à la page 58) ou la page Éditer l'utilisateur ("Édition des utilisateurs" à la page 63) pour assigner des capacités aux utilisateurs. Vous pouvez aussi assigner des capacités à un utilisateur en lui assignant un rôle d'administrateur que vous configurerez par le biais de la zone Sécurité de l'interface. Pour plus d'informations, voir "Comprendre et gérer les rôles admin" à la page 220.

Remarque – La liste des capacités fonctionnelles et basées sur des tâches par défaut d'Identity Manager (définitions incluses) figure à l'Annexe D, “Définitions des capacités”. Cette annexe répertorie également les onglets et sous-onglets auxquels les différentes capacités basées sur des tâches permettent d'accéder.

Comprendre et gérer les rôles admin

Les *Rôles admin* définissent deux éléments : un ensemble de capacités et une étendue de contrôle (le terme étendue de contrôle fait référence à une ou plusieurs organisations gérées). Une fois définis, les rôles admin peuvent être assignés à un ou plusieurs administrateurs.

Remarque – Ne confondez pas les *rôles* avec les *rôles admin*. Les rôles sont utilisés pour gérer l'accès des utilisateurs finaux aux ressources externes tandis que les rôles admin sont principalement utilisés pour gérer l'accès des administrateurs Identity Manager à des objets Identity Manager.

Les informations présentées dans cette section sont limitées aux rôles admin. Pour plus d'informations sur les rôles, voir “Comprendre et gérer les rôles” à la page 121.

Vous pouvez assigner plusieurs rôles admin à un même administrateur. Cela permet à un administrateur d'avoir un ensemble de capacités donné dans une étendue de contrôle, et un ensemble de capacités différent dans une autre étendue de contrôle. Par exemple, un rôle admin peut accorder à l'administrateur le droit de créer et d'éditer des utilisateurs pour les organisations contrôlées spécifiées dans ce rôle admin. Un second rôle admin assigné au même administrateur, cependant, pourra n'accorder que le droit « change users' passwords » (Changer les mots de passe des utilisateurs) dans un ensemble distinct d'organisation contrôlées tel que défini dans ce rôle admin.

Les rôles admin permettent de réutiliser les associations de capacités et d'étendue de contrôle. Les rôles admin simplifient également la gestion des privilèges d'administrateur avec un grand nombre d'utilisateurs. Au lieu d'assigner directement des capacités et des organisations contrôlées aux utilisateurs individuels, il convient d'utiliser les rôles admin pour accorder des privilèges d'administrateur.

L'assignation de capacités ou d'organisations (ou de ces deux éléments) à un rôle admin peut être directe ou dynamique (indirecte).

- **Assignation directe**. En utilisant cette méthode, les capacités et/ou les organisations contrôlées sont explicitement assignées au rôle admin. Par exemple, un rôle admin peut se voir assigner la capacité Administrateur de rapports d'utilisateur et l'organisation contrôlée Haut.
- **Assignation dynamique** (*indirecte*). Cette méthode utilise des règles pour assigner des capacités et des organisations contrôlées. Les règles sont évaluées à chaque fois qu'un administrateur auquel le rôle admin est assigné se connecte. Une fois que l'administrateur a été authentifié, les règles déterminent de manière dynamique l'ensemble de capacités et/ou organisations contrôlées qui est assigné.

  Par exemple, lorsqu'un utilisateur se connecte :

  - Si son titre d'utilisateur Active Directory (AD) est *manager* (responsable), la règle de capacités pourra retourner Administrateur de comptes pour la capacité à assigner.
  - Si son service utilisateur Active Directory (AD) est *marketing*, la règle d'organisations contrôlées pourra retourner Marketing pour l'organisation contrôlée à assigner.

L'assignation dynamique des rôles admin aux utilisateurs peut être activée ou désactivée pour chaque interface de connexion (par exemple, pour l'interface utilisateur ou l'interface administrateur). Pour cela, définissez l'attribut de configuration système suivant sur `true` ou `false`:

```
security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.logininterface
```

La valeur par défaut pour toutes les interfaces est `false`.

Pour les instructions à suivre pour éditer un objet Configuration système, voir "Édition des objets Configuration Identity Manager" à la page 118.

Règles de rôle admin

Identity Manager fournit des exemples de règles pouvant être utilisés pour les rôles admin. Ces règles sont disponibles dans le répertoire d'installation d'Identity Manager dans `sample/adminRoleRules.xml`.

Le Tableau 6–1 indique les noms de ces règles et l'`authType` à spécifier pour chacune.

TABLEAU 6–1 Exemples de règles de rôle admin

Nom de la règle	`authType`
Règle d'organisations contrôlées	`ControlledOrganizationsRule`

TABLEAU 6–1 Exemples de règles de rôle admin *(Suite)*

Nom de la règle	authType
Règle de capacités	CapabilitiesRule
Règle du rôle admin d'assignation d'utilisateur	UserIsAssignedAdminRoleRule

Remarque – Pour toute information sur les exemples de règles fournis pour les rôles admin de fournisseur de services, voir "Administration déléguée pour les utilisateurs de Service Provider" à la page 551 au Chapitre 17, "Administration de Service Provider".

Le rôle admin utilisateur

Identity Manager inclut un rôle admin intégré, nommé User Admin Role (Rôle admin utilisateur). Par défaut, ce rôle n'a ni capacités ni organisations contrôlées assignées. Il ne peut pas être supprimé. Ce rôle admin est implicitement assigné à tous les utilisateurs (utilisateurs finaux et administrateurs) au moment de la connexion, quelle que soit l'interface depuis laquelle ils se connectent (par exemple, l'interface utilisateur ou administrateur, la console ou encore Identity Manager IDE).

Remarque – Pour toute information sur la création d'un rôle admin pour les utilisateurs de fournisseur de service, voir "Administration déléguée pour les utilisateurs de Service Provider" à la page 551 au Chapitre 17, "Administration de Service Provider".

Vous pouvez éditer le User Admin Role par le biais de l'interface administrateur (sélectionnez Sécurité puis Rôles admin).

Étant donné que les capacités ou les organisations contrôlées qui sont assignées de manière statique à travers ce rôle admin sont assignées à tous les utilisateurs, il est recommandé d'effectuer l'assignation des capacités et organisations contrôlées au moyen de règles. Avec cette solution des utilisateurs différents auront des capacités différentes ou n'en auront aucune. Par ailleurs, l'étendue des assignations sera calculée en fonction de facteurs variés, notamment les postes occupés par les utilisateurs, les services dans lesquels ils travaillent, leur titre, qui peuvent être déterminés par le biais d'interrogations dans le contexte des règles.

Le rôle admin utilisateur ne désapprouve pas ni ne remplace l'utilisation de l'indicateur `authorized=true` utilisé dans les flux de travaux. Cet indicateur reste approprié dans les cas où l'utilisateur ne doit pas avoir accès aux objets auxquels le flux de travail accède, sauf pendant l'exécution du flux de travail. Essentiellement, ceci permet à l'utilisateur de passer dans un mode *exécuter en tant que superutilisateur*.

Il peut cependant y avoir des cas dans lesquels un utilisateur doit avoir un accès spécifique à un ou plusieurs objets à l'extérieur (et potentiellement dans les) des flux de travaux. Dans de tels cas, l'utilisation de règles pour assigner dynamiquement les capacités et les organisations contrôlées permet de préciser les autorisations concernant ces objets.

Création et édition de rôles admin

Pour créer ou éditer un rôle admin, la capacité Administrateur de rôles admin doit vous être assignée.

Pour accéder aux rôles admin dans l'interface administrateur, cliquez sur Sécurité puis sur l'onglet Rôles admin. La page de liste Rôles admin vous permet de créer, éditer et supprimer des rôles admin pour les utilisateurs Identity Manager et pour les utilisateurs de fournisseur de services.

Pour éditer un rôle admin existant, cliquez sur un nom dans la liste. Cliquez sur Nouveau pour créer un rôle admin. Identity Manager affiche les options Créer un rôle Admin (illustrées à la Figure 6–3). La vue Créer un rôle Admin présente quatre onglets qui permettent de spécifier les attributs généraux, les capacités et l'étendue du nouveau rôle admin, ainsi que les assignations de rôle aux utilisateurs.

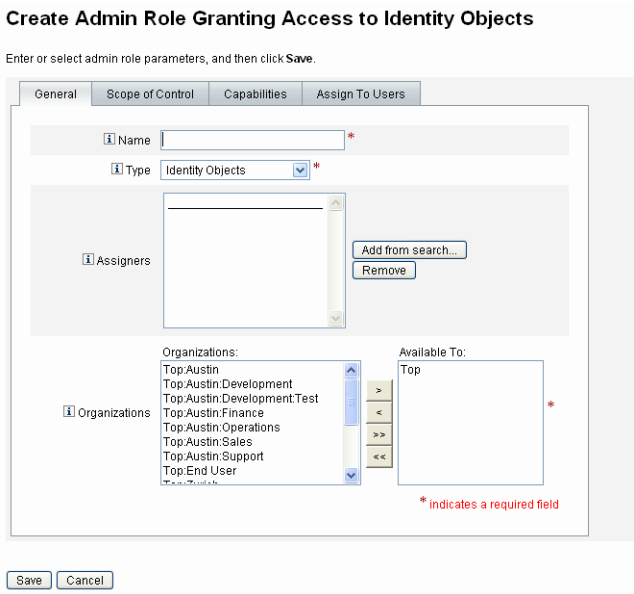


FIGURE 6–3 Page Créer un rôle Admin : onglet Général

Onglet Général

L'onglet Général de la vue Créer un rôle Admin ou Éditer un rôle Admin permet de spécifier les caractéristiques de base suivantes pour le rôle admin :

- **Nom**. Nom unique de ce rôle admin.

  Par exemple, vous pouvez créer le Rôle admin Finance pour les utilisateurs qui auront des capacités administratives pour les utilisateurs dans le service (ou l'organisation) Finance.

- **Type**. Sélectionnez au choix Objets Identity ou Utilisateurs de Service Provider pour le type. Ce champ est obligatoire.

  Sélectionnez Objets Identity si vous créez un rôle admin pour des utilisateurs (ou objets) Identity Manager. Sélectionnez Utilisateurs de Service Provider si vous créez ce rôle admin pour accorder l'accès aux utilisateurs de fournisseur de services.

Remarque – Pour toute information sur la création d'un rôle admin pour accorder l'accès aux utilisateurs Service Provider, voir "Administration déléguée pour les utilisateurs de Service Provider" à la page 551 au Chapitre 17, "Administration de Service Provider".

- **Assignataires**. Sélectionnez ou recherchez les utilisateurs qui seront autorisés à assigner ce rôle admin à d'autres utilisateurs. L'ensemble d'utilisateurs à partir duquel vous pouvez effectuer des sélections comprend les personnes auxquelles la capacité d'assignation a été assignée.

  Si aucun utilisateur n'est sélectionné, le seul utilisateur en mesure d'assigner ce rôle admin sera celui l'aura créé. Si l'utilisateur qui a créé le rôle admin ne dispose pas de la capacité d'assignation de capacité utilisateur, vous devez sélectionner un ou plusieurs utilisateurs en tant qu'assignataires pour assurer qu'au moins l'un d'eux puisse assigner le rôle admin à un autre utilisateur.

- **Organisations**. Sélectionnez une ou plusieurs organisations pour lesquelles ce rôle admin sera disponible. Ce champ est obligatoire.

  L'administrateur peut gérer des objets dans l'organisation assignée et dans n'importe quelle organisation située sous cette organisation dans la hiérarchie.

Portée du contrôle

Identity Manager permet de contrôler les utilisateurs qui rentrent dans la portée ou étendue de contrôle d'un utilisateur final.

Utilisez l'onglet Portée du contrôle (illustré à la Figure 6–4) pour spécifier les organisations que les membres de cette organisation peuvent gérer, ou spécifier la règle qui détermine les organisations qui seront gérées par les utilisateurs du rôle admin et pour sélectionner le formulaire utilisateur pour le rôle admin.

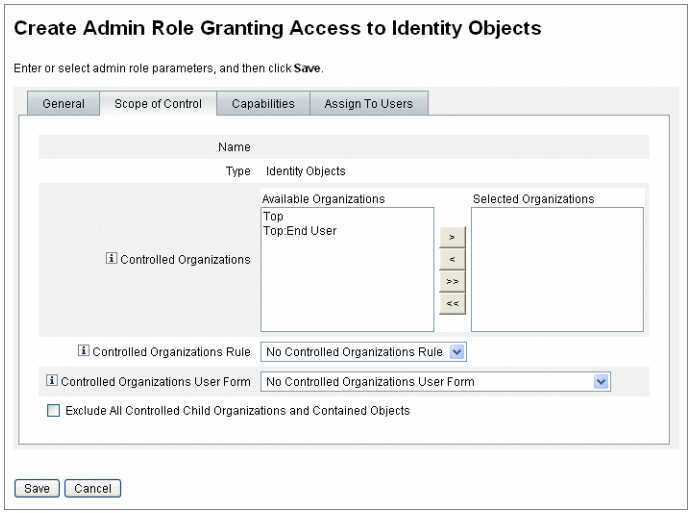


FIGURE 6–4 Créer un rôle Admin : Portée du contrôle

- **Organisations contrôlées**. Sélectionnez dans la liste Organisations disponibles les organisations que ce rôle admin a le droit de gérer.
- **Règle d'organisations contrôlées**. Sélectionnez une règle qui sera évaluée, à la connexion de l'utilisateur, pour que zéro ou plusieurs organisations soient contrôlées par un utilisateur auquel ce rôle admin aura été assigné. La règle sélectionnée doit être du type authType `ControlledOrganizationsRule`. Par défaut, aucune règle d'organisation contrôlée n'est sélectionnée.

  Vous pouvez utiliser la règle `EndUserControlledOrganizations` pour définir la logique nécessaire pour assurer que le bon ensemble d'utilisateurs soit disponible pour la délégation, en fonction de vos besoins organisationnels.

  Si vous voulez que la liste d'étendue d'utilisateurs soit la même pour les administrateurs, que ceux-ci soient connectés à l'interface administrateur ou à l'interface utilisateur final, vous devez changer la règle `EndUserControlledOrganizations`.

Modifiez la règle pour d'abord contrôler si l'utilisateur s'authentifiant est un administrateur puis configurez ce qui suit :

- Si l'utilisateur n'est pas un administrateur, la règle doit retourner l'ensemble d'organisations qui devrait être contrôlé par un utilisateur final, par exemple sa propre organisation (par exemple, `waveset.organization`).
- Si l'utilisateur est un administrateur, la règle ne doit retourner aucune organisation de sorte que l'utilisateur contrôle uniquement les organisations qui lui sont assignées en sa qualité d'administrateur.

  Par exemple :

```
<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'>
  <Comments>
    If the user logging in is not an Idm administrator,
    then return the organization that they are a member of.
    Otherwise, return null.
  </Comments>
  <cond>
    <and>
      <isnull><ref>waveset.adminRoles</ref></isnull>
      <isnull><ref>waveset.capabilities</ref></isnull>
      <isnull><ref>waveset.controlledOrganizations</ref></isnull>
    </and>
    <ref>waveset.organization</ref>
  </cond>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>
```

- Si l'utilisateur ou l'administrateur appartient à une organisation dynamique, ils ne sont pas retournés dans les résultats de recherche.

  Vous pouvez cependant créer une règle qui retourne les utilisateurs d'organisations dynamiques. Modifiez l'exemple de règle suivant en ajoutant un nouvel attribut à la définition du schéma utilisateur Identity Manager qui est défini dans l'objet `Idm Schema Configuration` (Configuration du schéma IDM), importez cet objet puis redémarrez le serveur Identity Manager.

```
<IDMAttributeConfigurations>
    ...
    <IDMAttributeConfiguration name='region'
                               syntax='STRING'
                               description='region of the country'/>
</IDMAttributeConfigurations>
```

```
        <IDMObjectClassConfigurations>
            ...
            <IDMObjectClassConfiguration name='User'
                                         extends='Principal'
                                           description='User description'>
                ...
                <IDMObjectClassAttributeConfiguration name='region'
                                                      queryable='true'/>
            </IDMObjectClassConfiguration>
        </IDMObjectClassConfigurations>
```

Next, import the following Identity Manager objects:

```
<!-- User member rule that will include all users whose region attribute
matches the region organization display name -->

<Rule name="Region User Member Rule" authType="UserMembersRule">
  <Description>User Member Rule</Description>
  <list>
    <new class='com.waveset.object.AttributeCondition'>
      <s>region</s>
      <s>equals</s>
      <ref>userMemberRuleOrganizationDisplayName</ref>
    </new>
  </list>
  <MemberObjectGroups>
    <ObjectRef type="ObjectGroup" id="#ID#All" name="All"/>
  </MemberObjectGroups>
</Rule>

<!-- North & South Region organizations with user member rule assigned -->

<ObjectGroup id='#ID#North Region' name='North Region'
displayName='North Region'> <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<ObjectGroup id='#ID#South Region' name='South Region'
displayName='South Region'>  <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
```

```
  </MemberObjectGroups>
</ObjectGroup>

<!-- Organization containing all employees -->

<ObjectGroup id='#ID#Employees' name='Employees' displayName='Employees'>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- End user controlled organization rule that give each user control
of the regional organization they are a member of -->

<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'
      primaryObjectClass='Rule'>
  <switch>
    <ref>waveset.attributes.region</ref>
    <case>
      <s>North Region</s>
      <s>North Region</s>
    </case>
    <case>
      <s>South Region</s>
      <s>South Region</s>
    </case>
    <case>
      <s>East Region</s>
      <s>East Region</s>
    </case>
    <case>
      <s>West Region</s>
      <s>West Region</s>
    </case>
  </switch>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>

<!-- 4 employees (2 in North and 2 in South region) -->

<User name='emp1' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee One'/>
```

```
  <Attribute name='lastname' type='string' value='One'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp2' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Two'/>
  <Attribute name='lastname' type='string' value='Two'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp4' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Four'/>
  <Attribute name='lastname' type='string' value='Four'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp5' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Five'/>
  <Attribute name='lastname' type='string' value='Five'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>
```

Connectez-vous ensuite via l'interface utilisateur final d'Identity Manager en tant qu'`emp1`, basé dans la région Nord. Sélectionnez Délégations → Nouvelle. Remplacez les critères de Recherche → par **`commence par`**, remplacez la valeur par **`emp`** et choisissez Rechercher. Cette sélection devrait retourner `emp2` dans la liste des utilisateurs disponibles.

- **Formulaire utilisateur Organisations contrôlées**. Sélectionnez le formulaire utilisateur qui sera employé par un utilisateur auquel ce rôle admin aura été assigné, pour créer ou modifier des utilisateurs appartenant aux organisations contrôlées de ce rôle admin. Par défaut, aucun Formulaire utilisateur Organisations contrôlées n'est sélectionné.

  Un formulaire utilisateur assigné par le biais d'un rôle admin remplace tout formulaire utilisateur hérité de l'organisation dont l'administrateur est membre. Il ne remplace pas un formulaire utilisateur qui serait directement assigné à l'administrateur.

Assignation de capacités au rôle admin

Les capacités assignées au rôle admin déterminent les droits administratifs dont disposent les utilisateurs auxquels le rôle admin est assigné. Par exemple, un rôle admin pourrait être limité à la création d'utilisateurs pour les seules organisations contrôlées de ce rôle admin. Dans ce cas, vous assigneriez la capacité Créer un utilisateur.

Sélectionnez les options suivantes dans l'onglet Capacités :

- **Capacités**. Capacités spécifiques (droits administratifs) que les utilisateurs du rôle admin auront pour leurs organisations contrôlées. Sélectionnez une ou plusieurs capacités dans la liste des capacités disponibles et amenez-les dans la liste Capacités assignées.
- **Règle de capacités**. Sélectionnez une règle qui, évaluée à la connexion de l'utilisateur, déterminera la liste de zéro capacités ou plus conférée aux utilisateurs auxquels ce rôle est assigné. L'authType de la règle sélectionnée doit être `CapabilitiesRule`.

Assignation de formulaires utilisateur au rôle admin

Vous pouvez spécifier un formulaire utilisateur pour les membres d'un rôle admin. L'onglet Assigner aux utilisateurs de la vue Créer un rôle Admin ou Éditer un rôle Admin permet de spécifier les assignations.

L'administrateur auquel le rôle admin est assigné utilisera ce formulaire utilisateur pour créer ou éditer des utilisateurs dans les organisations contrôlées par ce rôle admin. Un formulaire utilisateur assigné par le biais d'un rôle admin remplace tout formulaire utilisateur hérité de l'organisation dont l'administrateur est membre. Il ne remplace pas un formulaire utilisateur qui serait directement assigné à l'administrateur.

Le formulaire utilisateur qui est utilisé lors de l'édition d'un utilisateur est déterminé dans l'ordre de priorité suivant :

- Si un formulaire utilisateur est assigné directement à l'administrateur, ce formulaire est utilisé.
- Si aucun formulaire utilisateur n'est assigné directement à l'administrateur, mais que ce dernier s'est vu assigner un rôle admin qui contrôle l'organisation dont l'utilisateur en cours de création ou d'édition sera ou est membre et spécifie un formulaire utilisateur, ce formulaire utilisateur est utilisé.
- Si aucun formulaire utilisateur n'est assigné directement à l'administrateur, ni indirectement par le biais d'un rôle admin, le formulaire utilisateur assigné aux organisations dont cet administrateur est membre (en commençant par l'organisation dont l'administrateur est membre et en remontant jusque sous `Haut`) est utilisé.
- Si aucune des organisations dont l'administrateur est membre n'a de formulaire utilisateur assigné, le formulaire utilisateur par défaut est utilisé.

Si un administrateur se voit assigner plusieurs rôles admin contrôlant la même organisation mais spécifiant des formulaires utilisateur différents, une erreur s'affiche lorsqu'il tente de créer ou d'éditer un utilisateur dans cette organisation. Si un administrateur tente d'assigner deux rôles admin ou plus contrôlant la même organisation mais spécifiant des formulaires utilisateur différents, une erreur s'affiche. Les changements ne peuvent pas être enregistrés tant que le conflit n'est pas résolu.

L'organisation Utilisateur final

L'organisation Utilisateur final constitue un moyen pratique pour les administrateurs de mettre certains objets, par exemple des ressources et des rôles, à la disposition des utilisateurs finaux. Les utilisateurs finaux peuvent afficher et, potentiellement, s'assigner des objets désignés (sous réserve d'un processus d'approbation) en utilisant l'interface utilisateur final ("Connexion à l'interface utilisateur final d'Identity Manager" à la page 43).

Remarque – L'organisation Utilisateur final est une nouveauté d'Identity Manager Version 7.1.1.

Auparavant, pour accorder aux utilisateurs finaux l'accès aux objets Configuration d'Identity Manager, tels que les rôles, les ressources ou encore les tâches, les administrateurs devaient éditer les objets Configuration et utiliser les authTypes End User Tasks (Tâches utilisateur final), End User Resources (Ressources utilisateur final) et End User (Utilisateur final).

À partir d'aujourd'hui, Sun recommande d'utiliser l'organisation « Utilisateur final » pour accorder aux utilisateurs finaux l'accès aux objets Configuration d'Identity Manager.

L'organisation Utilisateur final est contrôlée de manière implicite par tous les utilisateurs auxquels elle permet d'afficher plusieurs types d'objets et, en particulier, les tâches, les règles, les rôles et les ressources. Au départ toutefois, cette organisation n'a pas d'objets membres.

L'organisation Utilisateur final est membre de `Haut` et ne peut pas avoir d'organisations enfants. De plus, l'organisation Utilisateur final ne s'affiche pas dans la liste de la page Comptes. Lors de l'édition d'objets (par exemple de rôles, rôles admin, ressources, stratégies, tâches, etc.) toutefois, vous pouvez rendre tout objet disponible pour l'organisation Utilisateur final en utilisant l'interface utilisateur administrateur.

Lorsque les utilisateurs finaux se connectent à l'interface utilisateur final, il se passe ce qui suit :

- Les utilisateurs finaux se voient accorder le contrôle de l'organisation `EndUser` (Utilisateur final) (`ObjectGroup`).
- Identity Manager évalue la règle End User Controlled Organization (Organisation contrôlée par les utilisateurs finaux), laquelle octroie automatiquement à l'utilisateur le contrôle de toutes les organisations dont elle retourne le nom (cette règle a été ajoutée dans Identity Manager Version 7.1.1, pour plus d'informations, voir la section "La règle End User Controlled Organization" à la page 232).
- Les utilisateurs finaux se voient accorder des droits d'accès aux types d'objets spécifiés dans la capacité `EndUser`.

La règle End User Controlled Organization

L'argument d'entrée de la règle End User Controlled Organization est la vue de l'utilisateur s'authentifiant. Identity Manager s'attend à ce que la règle retourne une ou plusieurs organisations que l'utilisateur se connectant à l'interface Utilisateur final contrôlera. Identity Manager s'attend à ce que la règle retourne une chaîne (pour une unique organisation) ou une liste (pour plusieurs organisations).

Pour gérer ces objets, les utilisateurs ont besoin de la capacité Administrateur des utilisateurs finaux. Les utilisateurs auxquels la capacité Administrateur des utilisateurs finaux est assignée peuvent afficher et modifier le contenu de la règle End User Controlled Organization. Les utilisateurs finaux se voient accorder des droits d'accès aux types d'objets spécifiés dans la capacité EndUser.

La capacité Administrateur des utilisateurs finaux est assignée par défaut à l'utilisateur Configurator. Les modifications apportées à la liste ou aux organisations retournées suite à l'évaluation de la règle End User Controlled Organization ne seront pas reflétées de manière dynamique pour les utilisateurs connectés. Ces utilisateurs devront se déconnecter puis se reconnecter pour voir ces modifications.

Si la règle End User Controlled Organization retourne une organisation non valable (par exemple, une organisation n'existant pas dans Identity Manager), le problème sera consigné dans le journal système. Pour corriger le problème, connectez-vous à l'interface utilisateur Administrateur et corrigez la règle.

Gestion des éléments de travail

Certains processus de flux de travaux générés par les tâches dans Identity Manager créent des éléments d'action ou *éléments de travail*. Ces éléments de travail peuvent être une demande d'approbation ou une autre demande d'action assignée à un compte Identity Manager.

Identity Manager regroupe tous les éléments de travail dans la zone Éléments de travail, ce qui vous permet d'afficher et de répondre à toutes les demandes en attente depuis un emplacement unique.

Types d'éléments de travail

Un élément de travail peut être de l'un des types suivants :

- **Approbations**. Demandes d'approbation de nouveaux comptes ou de changements apportés à des comptes.
- **Attestations**. Demandes d'examen et d'approbation des habilitations des utilisateurs.
- **Résolutions**. Demande de résolution ou d'atténuation des violations des stratégies de compte utilisateur.
- **Autre**. Demande d'élément d'action relative à un type autre que ceux standard. Il peut s'agir d'une demande d'action générée depuis un flux de travaux personnalisé.

Pour afficher les éléments de travail en attente par type, cliquez sur Éléments de travail dans le menu.

Remarque – Si vous êtes le propriétaire d'éléments de travail ayant des éléments de travail en attente (ou des éléments de travail délégués), votre liste Éléments de travail s'affiche lorsque vous vous connectez à l'interface utilisateur d'Identity Manager.

Travailler avec les demandes d'éléments de travail

Pour répondre à une demande d'éléments de travail, cliquez sur l'un des types d'éléments de travail dans la zone Éléments de travail de l'interface. Sélectionnez des éléments dans la liste des demandes puis cliquez sur l'un des boutons disponibles pour indiquer l'action à entreprendre. Les options relatives aux éléments de travail varient selon le type de l'élément de travail.

Pour plus d'informations sur la réponse aux demandes, reportez-vous aux rubriques suivantes :

- “Approbation des comptes utilisateur” à la page 238 ;
- “Gestion des obligations d'attestation” à la page 499 ;
- “Résolution et atténuation des violations de conformité” à la page 474 ;

Affichage de l'historique des éléments de travail

Utilisez l'onglet Historique de la zone Éléments de travail pour afficher les résultats des actions d'élément de travail précédentes.

La Figure 6–5 affiche un exemple de vue d'historique des éléments de travail.

FIGURE 6–5 Vue d'historique des éléments de travail

Délégation des éléments de travail

Les propriétaires d'éléments de travail peuvent gérer la charge de travail en déléguant des éléments de travail à d'autres utilisateurs pendant une durée spécifiée. Dans le menu principal, vous pouvez utiliser la page Éléments de travail → Déléguer mes éléments de travail pour déléguer les éléments de travail à venir (par exemple des demandes d'approbation) à un ou plusieurs utilisateurs (délégués). Les utilisateurs n'ont pas besoin d'être dotés des capacités d'approbateur pour devenir délégués.

Remarque – La fonction de délégation ne s'applique qu'aux éléments de travail à venir. Les éléments existants (listés sous Mes éléments de travail) doivent être transférés de manière sélective au moyen de la fonction de transfert.

D'autres pages permettent également de déléguer les éléments de travail :

- Dans l'interface administrateur, vous pouvez déléguer des éléments de travail depuis les pages Créer un utilisateur et Éditer l'utilisateur ("Pages relatives aux utilisateurs (Créer/Éditer/Afficher)" à la page 54). Cliquez sur l'onglet de formulaire Délégations.
- Dans l'interface utilisateur Utilisateur final ("Interface utilisateur final d'Identity Manager" à la page 40), les utilisateurs peuvent cliquer sur l'élément de travail Délégations.

Les délégués peuvent approuver des éléments de travail au nom du propriétaire de ces éléments pendant la période de délégation effective. Les éléments de travail délégués incluent le nom du délégué.

Tout utilisateur peut créer une ou plusieurs délégations pour ses éléments de travail futurs. Les administrateurs qui peuvent éditer un utilisateur peuvent également créer une délégation au nom de celui-ci. Un administrateur ne peut toutefois pas déléguer quoi que ce soit à une personne à laquelle l'utilisateur ne peut rien déléguer (concernant les délégations, l'étendue du contrôle de l'administrateur est identique à celle de l'utilisateur au nom duquel la délégation est effectuée).

Entrées du journal d'audit

Les entrées du journal d'audit listent le nom du délégant lorsque les éléments de travail délégués sont approuvés ou rejetés. Les modifications des informations d'approbateur délégué d'un utilisateur sont consignées dans la section réservées aux modifications détaillées de l'entrée du journal d'audit lorsqu'un utilisateur est créé ou modifié.

Affichage des délégations courantes

Vous affichez les délégations sur la page Délégations courantes.

▼ Pour afficher les délégations courantes

1. **Dans l'interface administrateur, cliquez sur Éléments de travail dans le menu principal.**
2. **Cliquez sur Déléguer mes éléments de travail dans le menu secondaire.**

   Identity Manager affiche la page Délégations courantes, laquelle vous permet d'afficher et éditer les délégations actuellement en vigueur.

Affichage des délégations précédentes

Vous affichez les délégations précédentes sur la page Délégations précédentes.

▼ Pour afficher les délégations précédentes

1 **Dans l'interface administrateur, cliquez sur Éléments de travail dans le menu principal.**

2 **Cliquez sur Déléguer mes éléments de travail dans le menu secondaire.**

La page Délégations courantes s'ouvre.

3 **Cliquez sur Précédente(s).**

La page Délégations précédentes s'ouvre. Les éléments de travail délégués précédemment peuvent être utilisés pour configurer de nouvelles délégations.

Création de délégations

Créez une délégation en utilisant la page Nouvelle délégation.

▼ Pour créer une délégation

1 **Dans l'interface administrateur, cliquez sur Éléments de travail dans le menu principal.**

2 **Cliquez sur Déléguer mes éléments de travail.**

La page Délégations courantes s'ouvre.

3 **Cliquez sur Nouveau.**

La page Nouvelle délégation s'ouvre.

4 **Remplissez le formulaire comme suit :**

a. **Sélectionnez un type d'élément de travail dans la liste de sélection Sélectionner un type d'élément de travail à déléguer. Pour déléguer l'ensemble de vos éléments de travail, sélectionnez Tous types d'éléments de travail.**

Si vous déléguez un élément de travail de type de rôle, organisation ou ressource, spécifiez les rôles, organisations ou ressources spécifiques qui devraient définir cette délégation en utilisant les flèches pour déplacer les sélections de la colonne Disponible à la colonne Sélectionné.

b. **Déléguer les éléments de travail à.**

Sélectionnez une des options suivantes :

- **Utilisateurs sélectionnés**. Sélectionnez cette option pour rechercher dans votre étendue de contrôle (par nom) des utilisateurs qui deviendront des délégués. Si l'un des délégués sélectionnés a à son tour délégué ses éléments de travail, vos futurs éléments de travail seront déléguées à ses propres délégués.
- **Sélectionnez un ou plusieurs utilisateurs dans la zone Utilisateurs sélectionnés**. Sinon, cliquez sur Ajouter à partir de la recherche pour ouvrir la fonctionnalité de recherche pour les utilisateurs. Cliquez sur Ajouter pour ajouter un utilisateur trouvé à la liste. Pour supprimer un délégué de la liste, sélectionnez-le et cliquez sur Supprimer.
  - **Mon responsable**. Sélectionnez cette option pour déléguer vos éléments de travail à votre responsable (si assigné).
  - **Déléguer WorkItemRule**. Sélectionnez une règle renvoyant une liste de noms d'utilisateur Identity Manager auxquels vous pouvez déléguer le type d'élément de travail sélectionné.

c. Date de début. Sélectionnez la date à laquelle la délégation de l'élément de travail sélectionné doit débuter. Par défaut, le jour sélectionné commence à 00h01 du matin.

d. Date de fin. Sélectionnez la date à laquelle la délégation de l'élément de travail sélectionné doit prendre fin. Par défaut, le jour sélectionné se termine à 11h59 du soir.

Remarque – Vous pouvez sélectionner la même date de début et de fin pour limiter la délégation des éléments de travail à une journée.

---

e. Cliquez sur OK pour enregistrer vos sélections et revenir à la liste des éléments de travail en attente d'approbation.

Remarque – Une fois la délégation configurée, tous les éléments de travail créés pendant la période de délégation effective sont ajoutés à la liste du délégué. Si vous mettez un terme à une délégation ou que l'échéance de celle-ci arrive, les éléments de travail délégués sont retournés à votre liste. Cela peut créer des éléments de travail en double dans votre liste. Toutefois, lorsque vous approuvez ou rejetez un élément de travail, le doublon est automatiquement supprimé de la liste.

Délégation à des utilisateurs supprimés

Identity Manager fonctionne de la manière suivante lorsqu'un utilisateur détenant des éléments de travail en attente est supprimé :

- Si les éléments de travail en attente ont été délégués et que le délégant n'a pas été supprimé, ils lui sont renvoyés.
- Si les éléments de travail n'ont pas été délégués ou s'ils l'ont été mais que le délégant a été supprimé, la tentative de suppression échoue tant que les éléments de travail en attente de l'utilisateur ne sont pas résolus ou transmis à un autre utilisateur.

Fin des délégations

Vous mettez fin à une ou plusieurs délégations sur la page Délégations courantes.

▼ Pour mettre fin à une ou plusieurs délégations

1. **Dans l'interface administrateur, cliquez sur Éléments de travail dans le menu principal.**
2. **Cliquez sur Déléguer mes éléments de travail dans le menu secondaire.**

   La page Délégations courantes s'ouvre.
3. **Sélectionnez une ou plusieurs délégations dans la liste, puis cliquez sur Annuler.**

   Identity Manager supprime les configurations de délégation sélectionnées et retourne les éventuels éléments de travail délégués du type sélectionné vers votre liste d'éléments de travail en attente.

Approbation des comptes utilisateur

Lorsqu'un utilisateur est ajouté au système Identity Manager, les administrateurs assignés en tant qu'*approbateurs* pour le nouveau compte doivent valider la validation du compte.

Identity Manager prend en charge trois catégories d'approbations :

- **Organisation**. L'approbation est nécessaire pour que le compte utilisateur soit ajouté à l'organisation.
- **Rôle**. L'approbation est nécessaire pour que le compte utilisateur soit assigné à un rôle.
- **Ressource**. L'approbation est nécessaire pour que le compte utilisateur se voit accorder l'accès à une ressource.

De plus, si les approbations de changement sont activées et que des changements sont apportés à un rôle, un élément de travail approbation de changement est envoyé à des propriétaires désignés du rôle.

Identity Manager prend en charge les approbations de changement par *Définition de rôle*. Si un administrateur change la définition d'un rôle, une approbation de changement provenant d'un propriétaire désigné de ce rôle est nécessaire. Le propriétaire du rôle doit approuver l'élément de travail pour que le changement soit appliqué.

Remarque –

- Vous pouvez configurer Identity Manager pour que les approbations comportent une signature numérique. Pour les instructions, voir "Configuration d'approbations et actions à signature numérique" à la page 241.
- Les administrateurs qui ne connaissent pas Identity Manager confondent parfois le concept d'approbation avec celui similaire en apparence d'attestation. Si les termes se ressemblent, il faut savoir que l'approbation et l'attestation ont lieu dans des contextes différents.

  Les approbations sont relatives à la validation des nouveaux comptes utilisateur. Lorsqu'un utilisateur est ajouté à Identity Manager, une ou plusieurs approbations peuvent être nécessaires pour valider l'autorisation du nouveau compte.

  Les attestations consistent quant à elles à vérifier que les utilisateurs existants ont uniquement des privilèges appropriés sur les ressources appropriées. Dans le cadre du processus Examen des accès périodique, un utilisateur Identity Manager (l'attestateur) peut être appelé à certifier que les détails du compte d'un autre utilisateur (c'est-à-dire les ressources assignées de l'utilisateur) sont valables et exacts. Ce processus est connu sous le nom d'attestation.

Configuration d'approbateurs de comptes

La configuration d'approbateurs de comptes pour les approbations relatives aux organisations, rôles et ressources est facultative mais recommandée. Pour chacune des catégories dans lesquelles des approbateurs sont configurés, une approbation minimum est requise pour la création d'un compte. Si un approbateur rejette une demande d'approbation, le compte n'est pas créé.

Vous pouvez assigner plus d'un approbateur par catégorie. Puisqu'une seule approbation est nécessaire par catégorie, vous pouvez configurer plusieurs approbateurs pour éviter tout retard ou arrêt du flux de travaux. Ainsi, si un approbateur n'est pas disponible, d'autres pourront gérer les demandes. L'approbation ne s'applique qu'à la création de comptes. Par défaut, les mises à jour et les suppressions de compte ne nécessitent pas d'approbation. Vous pouvez toutefois personnaliser ce processus pour en exiger.

Vous pouvez personnaliser les flux de travaux en utilisant Identity Manager IDE pour changer le flux d'approbations, capturer les suppressions de compte et capturer les mises à jour.

Pour toute information sur Identity Manager IDE, allez sur : `https://identitymanageride.dev.java.net/`. Pour des informations sur les flux de travaux et un exemple illustré d'altération de flux de travaux d'approbation, voir le Chapitre 1, "Workflow" du *Sun Identity Manager Deployment Reference*.

Les approbateurs Identity Manager peuvent approuver ou rejeter une demande d'approbation.

Les administrateurs peuvent afficher et gérer les approbations en attente depuis la zone Éléments de travail de l'interface d'Identity Manager. Dans la page Éléments de travail, cliquez sur **Mes éléments de travail** pour afficher les approbations en attente. Cliquez sur l'onglet **Approbations** pour gérer les approbations.

Signature des approbations

Pour approuver un élément de travail en utilisant une signature numérique, vous devez commencer par configurer la signature numérique comme décrit dans "Configuration d'approbations et actions à signature numérique" à la page 241.

▼ Pour signer une approbation

1. **Dans l'interface administrateur d'Identity Manager, sélectionnez Éléments de travail.**
2. **Cliquez sur l'onglet Approbations.**
3. **Sélectionnez une ou plusieurs approbations dans la liste.**
4. **Saisissez des commentaires pour l'approbation, puis cliquez sur Approuver.**
   Identity Manager vous demande si faire confiance à l'applet.
5. **Cliquez sur Toujours.**
   Identity Manager affiche un récapitulatif daté de l'approbation.
6. **Saisissez l'emplacement du keystore ou cliquez sur Parcourir pour le localiser. (Cet emplacement est défini pendant la configuration de l'approbation signée, comme décrit à l'étape 10m de la procédure "Pour activer la configuration côté serveur pour les approbations signées en utilisant PKCS12" à la page 243.)**
7. **Saisissez le mot de passe du keystore (ce mot de passe est défini pendant la configuration de l'approbation signée, comme décrit à l'étape 101 de la procédure "Pour activer la configuration côté serveur pour les approbations signées en utilisant PKCS12" à la page 243).**
8. **Cliquez sur Signer pour approuver la demande.**

Informations supplémentaires

Signature des approbations suivantes

Une fois une approbation signée, vous devrez uniquement dans le cadre d'autres actions d'approbation saisir le mot de passe de votre keystore et cliquer sur **Signer** (Identity Manager mémorise l'emplacement du keystore défini dans l'approbation précédente).

Configuration d'approbations et actions à signature numérique

Utilisez les informations et procédures suivantes pour configurer la signature numérique. Vous pouvez signer numériquement les éléments suivants :

- les approbations (approbations de changement incluses),
- les actions d'examen des accès,
- les résolutions de violations de conformité.

Les sujets traités dans cette section expliquent la configuration requise côté serveur et côté client pour ajouter le certificat et la LRC à Identity Manager pour les approbations signées.

▼ Pour activer la configuration côté serveur pour les approbations signées

1 **Ouvrez l'objet Configuration système pour l'éditer et définissez** `security.nonrepudiation.signedApprovals=true`.

Pour les instructions à suivre pour éditer un objet Configuration système, voir "Édition des objets Configuration Identity Manager" à la page 118.

Si vous utilisez PKCS11 vous devez aussi définir `security.nonrepudiation.defaultKeystoreType=PKCS11`.

Si vous utilisez un fournisseur de clés PKCS11 vous devez aussi définir `security.nonrepudiation.defaultKeystoreType=PKCS11`.

Remarque – Veuillez vous reporter aux points suivants dans le kit REF pour en savoir plus sur quand écrire un fournisseur personnalisé :

`com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)`
`REF/transactionsigner/SamplePKCS11KeyProvider`

Le kit REF (Resource Extension Facility) figure dans le répertoire `/REF` du CD de votre produit ou a été fourni avec votre image d'installation.

---

2 **Ajoutez les certificats de votre autorité de certification (AC) en tant que certificats de confiance. Pour cela, vous devez d'abord vous procurer une copie de ces certificats.**

Par exemple, si vous utilisez une AC Microsoft, procédez comme suit :

a. **Allez à** `http://`*AdresseIP*`/certsrv` **et connectez-vous avec des privilèges administratifs.**

b. **Sélectionnez Retrieve the CA certificate or certificate revocation list (Récupérer le certificat AC ou la liste de révocation de certificats) et cliquez sur Next (Suivant).**

c. **Téléchargez et enregistrez le certificat CA.**

3 **Ajoutez le certificat à Identity Manager en tant que certificat de confiance :**

a. **Depuis l'interface administrateur, sélectionnez Sécurité puis Certificats. Identity Manager affiche la page Certificats.**

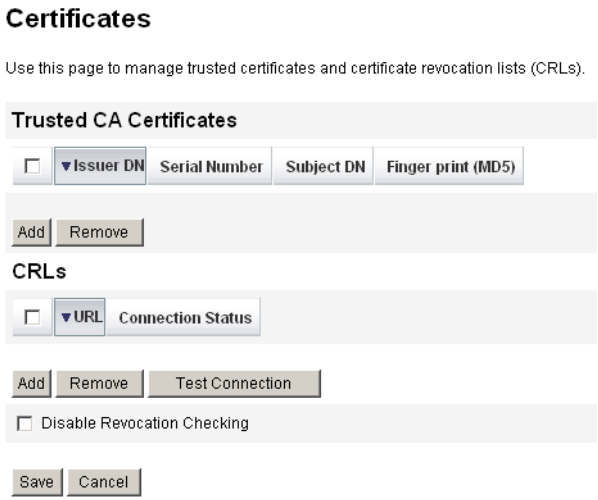


FIGURE 6–6 Page Certificats

b. **Dans la zone Certificats d'AC de confiance, cliquez sur Ajouter. Identity Manager affiche la page Importer le certificat.**

c. **Naviguez jusqu'au certificat de confiance, sélectionnez-le puis cliquez sur Importer.**

Le certificat est maintenant affiché dans la liste des certificats de confiance.

4. **Ajoutez la liste de révocation de certificats (LRC) de votre AC :**

   a. **Dans la zone CRL (LRC) de la page Certificats, cliquez sur Ajouter.**

   b. **Entrez l'URL de la LRC de votre AC.**

   Remarque –

   - Une liste de révocation de certificats ou LRC est une liste de numéros de série de certificats ayant été révoqués ou n'étant pas valides.
   - L'URL de la LRC de votre AC peut être http ou LDAP.
   - Chaque AC a un URL différent pour la distribution des LRC, vous pouvez déterminer cet élément en explorant l'extension CRL Distribution Points du certificat de l'AC.

5. **Cliquez sur Vérifier la connexion pour contrôler l'URL.**

6. **Cliquez sur Enregistrer.**

7. **Signez les applet s**`/ts2.jar`**en utilisant jarsigner.**

Remarque – Pour plus d'informations, voir `http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/jarsigner.html`. Le fichier `ts2.jar` fourni avec Identity Manager est signé en utilisant un certificat autosigné et ne doit pas être utilisé pour les systèmes de production. En production, ce fichier doit être signé de nouveau en utilisant un certificat signature code émis par votre AC de confiance.

▼ Pour activer la configuration côté serveur pour les approbations signées en utilisant PKCS12

Les informations de configuration suivantes sont relatives aux approbations signées en utilisant PKCS12. Procurez-vous un certificat et une clé privée puis exportez-les dans un keystore PKCS#12. Par exemple, si vous utilisez une AC Microsoft, vous devez procéder comme suit :

Avant de commencer Identity Manager requiert désormais JRE 1.5 minimum.

1. **En utilisant Internet Explorer, naviguez jusqu'à** `http://`*AdresseIP*`/certsrv` **et connectez-vous avec des privilèges administratifs.**

2. **Sélectionnez Request a certificate (Demander un certificat) puis cliquez sur Next (Suivant).**

3. **Sélectionnez Advanced request (Demande) avancée puis cliquez sur Next (Suivant).**

4. **Cliquez sur Next (Suivant).**

5. **Sélectionnez User for Certificate Template (Modèle utilisateur pour certificat).**
6. **Sélectionnez les options suivantes :**
   a. **Marquez les clés comme exportables.**
   b. **Activez une forte protection des clés.**
   c. **Utilisez le magasin de la machine locale.**
7. **Cliquez sur Submit (Envoyer) puis sur OK.**
8. **Cliquez sur Install this certificate (Installer le certificat).**
9. **Sélectionnez Run (Exécuter) → mmc pour lancer mmc.**
10. **Ajoutez le snap-in Certificate :**
    a. **Sélectionnez Console → Add/Remove Snap-in (Ajouter/Supprimer un composant logiciel enfichable).**
    b. **Cliquez sur Add (Ajouter).**
    c. **Sélectionnez le compte Computer (Ordinateur).**
    d. **Cliquez sur Next (Suivant) puis sur Finish (Terminer).**
    e. **Cliquez sur Close (Fermer).**
    f. **Cliquez sur OK.**
    g. **Allez à Certificates (Certificats) → Personal (Personnel) → Certificates (Certificats).**
    h. **Cliquez avec le bouton droit sur Administrator All Tasks (Toutes tâches administrateur) → Export (Exporter).**
    i. **Cliquez sur Next (Suivant).**
    j. **Cliquez sur Next (Suivant) pour confirmer l'exportation de la clé privée.**
    k. **Cliquez sur Next (Suivant).**
    l. **Indiquez un mot de passe puis cliquez sur Next (Suivant).**

m. Fichier *EmplacementCertificat***.**

n. Cliquez sur Next (Suivant) puis sur Finish (Terminer). Cliquez sur OK pour confirmer.

Remarque – Notez les informations que vous avez utilisées aux étapes 10l (mot de passe) et 10m (emplacement du certificat) de la configuration côté client. Vous aurez besoin des ces informations pour signer les approbations.

▼ Pour activer la configuration côté client pour les approbations signées en utilisant PKCS11

Si vous utilisez PKCS11 pour les approbations signées

- **Reportez-vous aux ressources suivantes du kit REF pour les informations de configuration :**

  `com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)`
  `REF/transactionsigner/SamplePKCS11KeyProvider`

  Le kit REF (Resource Extension Facility) figure dans le répertoire `/REF` du CD de votre produit ou a été fourni avec votre image d'installation.

Affichage de la signature des transactions

Cette section explique la procédure à suivre pour afficher les signatures de transaction dans un rapport AuditLog d'Identity Manager.

▼ Pour afficher une signature de transaction

1. **Dans l'interface administrateur d'Identity Manager, sélectionnez Rapports.**
2. **Sur la page Exécuter des rapports, sélectionnez Rapport de liste de contrôle dans la liste d'options Nouveau.**
3. **Dans le champ Titre du rapport, entrez un titre (par exemple, Approbations).**
4. **Dans la zone de sélection Organisations, sélectionnez toutes les organisations.**
5. **Sélectionnez l'option Actions puis Approuver.**
6. **Cliquez sur Enregistrer pour enregistrer le rapport et revenir à la page Exécuter des rapports.**
7. **Cliquez sur Exécuter pour exécuter le rapport Approbations.**
8. **Cliquez sur le lien des détails pour voir les informations relatives à la signature de la transaction.**

Les informations relatives à la signature de la transaction peuvent inclure ce qui suit :

- l'émetteur,
- l'objet,
- le numéro de série du certificat,
- le message signé,
- la signature,
- l'algorithme de signature.

Configuration des approbations signées au format XMLDSIG

Identity Manager vous permet d'ajouter des approbations signées au format XMLDSIG, incluant un horodatage numérique conforme RFC 316, au processus d'approbation d'Identity Manager. Lorsque vous configurez Identity Manager pour utiliser les approbations signées XMLDSIG, aucun changement n'est visible des approbateurs à moins qu'ils n'affichent l'approbation dans le journal d'audit. Seul le format de l'approbation signée stockée dans l'enregistrement du journal d'audit est changé.

Comme avec les approbations signées préalables d'Identity Manager, un applet est lancé sur la machine cliente et l'approbateur se voit présenter les informations d'approbation à signer. Il choisit ensuite un keystore et une clé avec laquelle signer l'approbation.

Une fois que l'approbateur a signé l'approbation, un document XMLDSIG contenant les données de l'approbation est créé. Ce document est renvoyé au serveur qui valide le document signé XMLDSIG. En cas de réussite et si les horodatages numériques RFC 3161 ont été configurés, un horodatage numérique est également généré pour ce document. L'horodatage récupéré de l'autorité d'horodatage (TSA) est contrôlé pour voir s'il ne présente pas d'erreurs et ses certificats sont validés. Enfin, en cas de réussite, Identity Manager génère un enregistrement de journal système qui inclut l'objet approbation signé au format XMLDSIG dans la colonne XML blob.

Format des données d'approbation

Le format d'un objet Approbation au format XMLDSIG est le suivant :

```
<XMLSignedData signedContent="...base64 transaction text ...">
   <XMLSignature>
      <TSATimestamp>
         ...The base64 encoded PKCS7 timestamp token returned by the TSA...
      </TSATimestamp
      <Signature>
        <SignedInfo>...XMLDSIG stuff...</SignedInfo>
        <SignatureValue>...base64 signature value</SignatureValue>
        <KeyInfo>...cert info for signer</KeyInfo>
```

```
      </Signature>
   </XMLSignature>
</XMLSignedData>
```

Où :

- Les données d'approbation `base64` consistent en le texte de données d'approbation réel qui est présenté à l'approbateur dans l'applet, codé au format `base64`.
- L'élément `<TSATimestamp>` contient la réponse d'horodatage PKCS7 codée en `base64` de l'autorité d'horodatage (Timestamp Authority, TSA).
- L'ensemble de la `<Signature>` englobe les données de signature XMLDSIG.

Ce document XMLDSIG est stocké dans la colonne XML de l'enregistrement d'approbation du journal d'audit.

Installation et configuration

Les exigences d'installation et de configuration pour l'utilisation des approbations signées XMLDSIG sont identiques à celles décrites dans “Pour activer la configuration côté serveur pour les approbations signées” à la page 241, exception faite d'une étape supplémentaire. Vous devez signer le fichier `xmlsec-1.4.2.jar` en plus de signer le fichier `ts2.jar`.

Configuration des approbations

Vous pouvez utiliser les attributs de configuration pour :

- Choisir le format `SignedData` ou le format `XMLSignedData`. Vous remarquerez que vous ne pouvez configurer qu'un format à la fois, bien que les administrateurs puissent changer ce paramètre si besoin est.
- Inclure un horodatage numérique récupéré d'une autorité d'horodatage RFC configurée.
- Spécifier un URL, HTTP uniquement, duquel récupérer cet horodatage.

Pour éditer ces attributs, utilisez les pages de débogage d'Identity Manager pour éditer l'objet Configuration système. Ces attributs figurent tous sous `security.nonrepudiation`, avec les autres attributs d'approbation signée.

Les attributs XMLDSIG sont les suivants :

- `security.nonrepudiation.useXmlDigitalSignatures` est une valeur booléenne qui active les signatures XMLDSIG.
- `security.nonrepudiation.timestampXmlDigitalSignatures` est une valeur booléenne qui inclut les horodatages numériques RFC 3161 dans les signatures XMLDSIG.
- `security.nonrepudiation.timestampServerURL` est une valeur de chaîne où l'URL pointe sur la TSA basée sur HTTP de laquelle sont récupérés les horodatages.

Remarque –

- Vous devez d'abord définir l'attribut `useSignedApprovals` existant sur **`true`** pour que les attributs précédents aient un effet.
- Identity Manager ne prend pas en charge les signatures multiples sur une approbation ni les approbations signées pour des demandes de provisioning plus générales.

◆ ◆ ◆ CHAPITRE 7

Chargement et synchronisation des données

Ce chapitre contient les informations et les procédures d'utilisation des fonctionnalités de chargement et synchronisation des données d'Identity Manager. Vous y apprendrez à utiliser les outils de synchronisation de données d'Identity Manager(la détection, la réconciliation et la synchronisation) pour maintenir les données à jour.

Ce chapitre se compose des rubriques suivantes :

Vous trouverez une explication détaillée du fonctionnement du chargement et de la synchronisation des données dans Identity Manager au Chapitre 3, "Data Loading and Synchronization" du *Sun Identity Manager Deployment Guide*.

Choix de l'outil de synchronisation des données

Identity Manager fournit plusieurs outils pouvant être utilisés pour importer et synchroniser les données des comptes. Pour savoir comment sélectionner le bon outil pour une tâche donnée, voir le Tableau 7–1.

Remarque – Vous trouverez une explication détaillée du fonctionnement du chargement et de la synchronisation des données dans Identity Manager au Chapitre 3, "Data Loading and Synchronization" du *Sun Identity Manager Deployment Guide*.

TABLEAU 7–1 Tâches à utiliser avec les outils de synchronisation de données

Pour	Choisissez cette fonctionnalité
Commencer par *tirer* les comptes de ressources dans Identity Manager sans les visualiser avant le chargement	Charger à partir de la ressource
Commencer par *tirer* les comptes de ressources dans Identity Manager en visualisant et en éditant éventuellement les données avant le chargement	Extraire vers le fichier, Charger à partir du fichier
Tirer régulièrement les comptes de ressources dans Identity Manager, en effectuant une action sur chaque compte conformément à une stratégie configurée	Réconcilier avec les ressources
Pousser ou *tirer* les changements apportés aux comptes de ressources dans Identity Manager	Synchronisation utilisant des adaptateurs Active Sync (plusieurs implémentations de ressources)

Fonctionnalités de détection de comptes

Les fonctionnalités de détection de comptes d'Identity Manager facilitent un déploiement rapide et accélèrent les tâches de création de comptes.

Ces fonctionnalités sont les suivantes :

- **Extraire vers le fichier**. Extrait les comptes de ressources retournés par un adaptateur de ressources dans un fichier (au format CSV ou XML). Vous pouvez manipuler ce fichier avant d'importer des données dans Identity Manager.
- **Charger à partir du fichier**. Lit les comptes dans un fichier (au format CSV ou XML) et les charge dans Identity Manager.
- **Charger à partir de la ressource**. Associe les deux fonctionnalités de détection précédentes en extrayant les comptes à partir d'une ressource et en les chargeant directement dans Identity Manager.

En utilisant ces outils, vous pouvez créer de nouveaux utilisateurs Identity Manager ou corréler des comptes sur une ressource avec des comptes utilisateur Identity Manager existants.

Remarque – Les pages de cette section sont consacrées à l'utilisation des fonctionnalités de détection d'Identity Manager. Pour des informations plus approfondies sur le chargement et la synchronisation des données, voir le Chapitre 3, “Data Loading and Synchronization” du *Sun Identity Manager Deployment Guide*.

Extraire vers le fichier

Cette fonctionnalité permet d'extraire les comptes de ressource d'une ressource dans un fichier XML ou de texte CSV. Ceci permet d'afficher les données extraites et de les modifier avant de les importer dans Identity Manager.

▼ Pour extraire des comptes

1. **Dans la barre de menu, sélectionnez Comptes puis Extraire vers le fichier.**
2. **Sélectionnez une ressource à partir de laquelle extraire les comptes.**
3. **Sélectionnez un format de fichier pour les informations de compte de sortie. Vous pouvez extraire les données dans un fichier XML ou dans un fichier texte avec les attributs de compte organisés dans un format CSV (valeurs séparées par des virgules).**
4. **Cliquez sur Télécharger. Identity Manager affiche la boîte de dialogue File Download (Télécharger le fichier), laquelle permet de choisir si enregistrer ou afficher le fichier extrait.**

   Si vous choisissez d'ouvrir le fichier, il est possible que vous deviez sélectionner un programme pour l'ouvrir.

Charger à partir du fichier

Cette fonctionnalité permet de charger des comptes de ressource, extraits d'une ressource au moyen d'Identity Manager ou d'une autre source de fichiers, dans Identity Manager. Les fichiers créés par la fonctionnalité Extraire vers le fichier d'Identity Manager adoptent le format XML. Si vous chargez une liste de nouveaux utilisateurs, le fichier de données sera en règle générale au format CSV.

À propos du format de fichier CSV

Souvent, les comptes à charger sont listé dans un tableau et enregistrés au format CSV (valeurs séparées par des virgules) pour être chargés dans Identity Manager.

Le contenu des fichiers CSV doit respecter les directives suivantes en matière de format :

- **Ligne 1**. Liste les en-têtes de colonne ou les attributs de schéma pour chaque champ, séparés par des virgules.
- **De la ligne 2 à la fin**. Liste les valeurs pour chaque attribut défini à la ligne 1, séparées par des virgules. S'il n'existe pas de données pour une valeur de champ, ce champ doit être représenté par des virgules adjacentes.

  À titre d'exemple, les trois premières lignes d'un fichier CVS pourraient ressembler aux entrées de fichier suivantes :

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Phone
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

Dans cet exemple, vous remarquerez que Jane Doe, le deuxième utilisateur, n'a pas de service. La valeur manquante est représentée par des virgules adjacentes („).

▼ Pour charger des comptes

1 **Dans l'interface administrateur, cliquez sur Comptes dans la barre de menu puis sur Charger à partir du fichier.**

Identity Manager affiche la page Charger les comptes à partir du fichier.

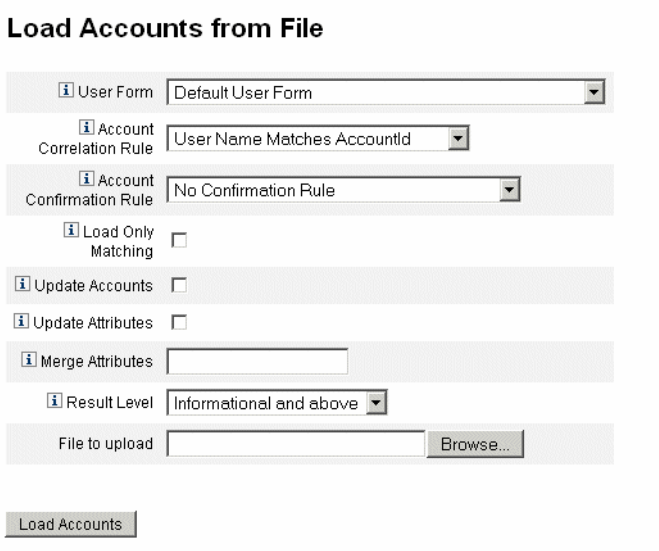


FIGURE 7–1 Charger à partir du fichier

2 **Utilisez cette page pour spécifier les options de chargement de comptes qui doivent l'être.**

Ces options sont les suivantes :

- **Formulaire utilisateur**. Lorsque le chargement crée un utilisateur Identity Manager, le formulaire utilisateur assigne à ce dernier une organisation en plus de rôles, ressources et autres attributs. Sélectionnez le formulaire utilisateur à appliquer à chaque compte de ressources.
- **Règle de corrélation de comptes**. Une règle de corrélation sélectionne les utilisateurs Identity Manager susceptibles d'être les propriétaires des comptes de ressources sans propriétaire. En fonction des attributs d'un compte de ressources sans propriétaire, la règle de corrélation retourne une liste de noms ou de conditions d'attributs qui sera utilisée pour sélectionner les propriétaires potentiels. Sélectionnez une règle pour rechercher les utilisateurs Identity Manager auxquels peuvent appartenir les comptes de ressources sans propriétaire.
- **Règle de confirmation de comptes**. Une règle de confirmation de comptes élimine tout non propriétaire de la liste des propriétaires potentiels sélectionnés par la règle de corrélation. Selon la vue complète d'un utilisateur Identity Manager et les attributs d'un compte de ressources sans propriétaire, une règle de confirmation retourne true si l'utilisateur possède le compte et false dans le cas contraire. Sélectionnez une règle pour tester chaque propriétaire potentiel d'un compte de ressources. Si vous sélectionnez Aucune règle de confirmation, le système accepte tous les propriétaires potentiels sans confirmation.

Remarque – Si, dans votre environnement, la règle de corrélation ne sélectionne pas plus d'un utilisateur par compte, vous n'avez pas besoin de règle de confirmation.

- **Charger seulement les comptes correspondants**. Sélectionnez cette option pour charger dans Identity Manager uniquement les comptes qui correspondent à un utilisateur Identity Manager existant. Si vous sélectionnez cette option, le chargement éliminera automatiquement tout compte de ressource sans correspondance.
- **Mettre attributs à jour**. Sélectionnez cette option pour remplacer les valeurs des attributs utilisateur Identity Manager courantes par les valeurs d'attributs du compte qui est chargé.
- **Fusionner attributs**. Entrez un ou plusieurs noms d'attribut, séparés par des virgules, pour lesquels les valeurs devraient être combinées (en éliminant les doublons) plutôt qu'écrasées. N'utilisez cette option que pour les attributs de type liste, tels que les groupes et listes de distribution. Vous devez aussi sélectionner l'option Mettre attributs à jour.
- **Niveau de résultat**. Sélectionnez le seuil auquel le processus de chargement enregistrera un résultat individuel pour un compte :
  - **Erreurs seules**. Enregistre un résultat individuel uniquement lorsque le chargement d'un compte entraîne un message d'erreur.
  - **Avertissements et erreurs**. Enregistre un résultat individuel uniquement lorsque le chargement d'un compte entraîne un avertissement ou un message d'erreur.

- **Informationnel et de plus**. Enregistre un résultat individuel pour chaque compte. Le processus de chargement s'exécute alors plus lentement.

3 **Spécifiez un fichier à charger dans le champ Fichier à télécharger puis cliquez sur Charger les comptes.**

Remarque –

- Si le fichier d'entrée ne contient pas de colonne utilisateur, vous devez sélectionner une règle de confirmation pour garantir un traitement correct du chargement.
- Le nom d'instance de tâche associé au processus de chargement est basé sur le nom du fichier d'entrée ; par conséquent, si vous réutilisez un nom de fichier, l'instance de tâche du dernier processus de chargement remplacera toute instance de tâche précédemment associée à ce nom de fichier.

  "À propos du format de fichier CSV" à la page 251 illustre les champs et options disponibles dans l'écran Charger à partir du fichier.

Si un compte correspond à (ou corrèle avec) un utilisateur existant, le processus de chargement fusionnera le compte dans l'utilisateur. Le processus créera également un nouvel utilisateur Identity Manager à partir de tout compte d'entrée ne correspondant à aucun utilisateur existant (à moins que Corrélation requise ne soit spécifié).

La variable de configuration `bulkAction.maxParseErrors` définit une limite pour le nombre d'erreurs pouvant être décelées lorsqu'un fichier est chargé. Par défaut, cette limite est de 10 erreurs. Si le nombre d'erreurs défini par `maxParseErrors` est décelé, l'analyse s'arrête.

Charger à partir de la ressource

Cette fonctionnalité permet d'extraire et importer directement des comptes dans Identity Manager en fonction d'options de chargement que vous définissez.

▼ Pour importer des comptes

1 **Dans l'interface administrateur, cliquez sur Comptes dans la barre de menu puis sur Charger à partir de la ressource.**

La page Charger les comptes à partir de la Ressource s'ouvre.

2 **Spécifiez les options de chargement dans la page Charger les comptes à partir de la Ressource.**

Les options de chargement de cette page sont identiques à celles de la page Charger à partir du fichier (voir "Charger à partir du fichier" à la page 251).

Réconciliation des comptes

La fonctionnalité de réconciliation permet de comparer régulièrement les comptes de ressources figurant dans Identity Manager aux comptes réellement présents sur les ressources. La réconciliation corrèle les données des comptes et met les différences en évidence.

Remarque – Les pages de cette section sont consacrées à l'exécution de tâches de réconciliation au moyen de l'interface administrateur. Pour des informations plus approfondies sur la réconciliation, voir le Chapitre 3, "Data Loading and Synchronization" du *Sun Identity Manager Deployment Guide*.

Réconciliation dans un Nutshell

Conçue pour une comparaison continue, la réconciliation présente les caractéristiques suivantes :

- Elle diagnostique les situations de compte plus spécifiquement et prend en charge un plus vaste éventail de réponses que le processus de détection.
- Elle peut être programmée ce qui n'est pas le cas de la détection.
- Elle offre un mode incrémentiel tandis que la détection est limitée au mode complet.
- Elle peut détecter les changements natifs ce qui n'est pas le cas de la détection.

Vous pouvez aussi configurer la réconciliation pour lancer un flux de travaux arbitraire à chacun des points suivants du traitement d'une ressource :

- avant de réconcilier un compte ;
- pour chaque compte ;
- après la réconciliation de tous les comptes.

Vous accédez aux fonctionnalités de réconciliation d'Identity Manager depuis la zone Ressources. La liste Ressources indique pour chaque ressource la date de la dernière réconciliation et son statut de réconciliation courant.

Remarque – La réconciliation est effectuée par le composant réconciliateur d'Identity Manager. Pour toute information sur les paramètres de configuration du réconciliateur, voir la section appropriée.

À propos des stratégies de réconciliation

Les stratégies de réconciliation permettent d'établir, pour chaque ressource, un ensemble de réponses possibles pour chaque tâche de réconciliation. Dans une stratégie, vous devez sélectionner le serveur qui doit exécuter la réconciliation, déterminer la fréquence et le moment

d'exécution de la réconciliation, et définir des réponses adaptées à chacune des situations rencontrées au cours de la réconciliation. Vous pouvez également configurer une réconciliation pour détecter les modifications apportées en mode natif (et non via Identity Manager) aux attributs de compte.

Édition des stratégies de réconciliation

▼ Pour éditer une stratégie de réconciliation

1. **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**
2. **Sélectionnez une ressource dans la liste Ressource.**
3. **Dans la liste Actions de ressource, cliquez sur Éditer la stratégie de réconciliation.**

   Identity Manager affiche la page Éditer la stratégie de réconciliation qui vous permet d'effectuer les sélections suivantes pour la stratégie :

   - **Serveurs de réconciliation**. Dans un environnement clustérisé, tout serveur peut exécuter la réconciliation. Spécifiez le serveur Identity Manager qui exécutera la réconciliation avec les ressources dans la stratégie.
   - **Modes de réconciliation**. La réconciliation peut être effectuée dans différents modes qui optimisent des qualités différentes :
     - **Réconciliation complète**. Optimise le caractère exhaustif de la réconciliation au détriment de la vitesse.
     - **Réconciliation incrémentielle** Optimise la vitesse de la réconciliation au détriment de son exhaustivité.

       Sélectionnez le mode dans lequel Identity Manager doit exécuter la réconciliation avec les ressources dans la stratégie. Sélectionnez Ne pas réconcilier pour désactiver la réconciliation pour des ressources cibles.
   - **Programme de réconciliation complète**. Si le mode Réconciliation complète est activé, la réconciliation est exécutée automatiquement selon un programme établi. Spécifiez la fréquence d'exécution de la réconciliation complète avec les ressources dans la stratégie.
     - Cochez la case Hériter de la stratégie par défaut pour hériter du programme indiqué d'une stratégie de niveau supérieur.
     - Désactivez la case à cocher Hériter de la stratégie par défaut pour spécifier un programme. Utilisez les champs fournis pour établir un programme récurrent ou la règle Répétition TaskSchedule pour créer un ajustement personnalisé d'un programme de réconciliation. Pour toute information sur la création d'une règle Répétition TaskSchedule, voir "Utilisation des règles Répétition TaskSchedule" à la page 264.

- **Programme de réconciliation incrémentielle**. Si le mode Réconciliation complète est activé, la réconciliation est exécutée automatiquement selon un programme établi.
  - Cochez la case Hériter de la stratégie par défaut pour hériter du programme d'une stratégie de niveau supérieur.
  - Désactivez la case à cocher Hériter de la stratégie par défaut pour spécifier un programme. Utilisez les champs fournis pour établir un programme récurrent ou la règle Répétition TaskSchedule pour créer un ajustement personnalisé d'un programme de réconciliation. Pour toute information sur la création d'une règle Répétition TaskSchedule, voir "Utilisation des règles Répétition TaskSchedule" à la page 264.

Remarque – Les ressources ne prennent pas toutes en charge la réconciliation incrémentielle.

- **Réconciliation au niveau d'attribut**. Vous pouvez également configurer une réconciliation pour détecter les changements apportés en mode natif (c'est-à-dire non via Identity Manager) aux attributs de compte. Spécifiez si la réconciliation doit détecter les changements natifs apportés aux attributs spécifiés dans Attributs de comptes réconciliés.
- **Règle de corrélation de comptes**. Une règle de corrélation sélectionne les utilisateurs Identity Manager susceptibles d'être les propriétaires des comptes de ressources sans propriétaire. En fonction des attributs d'un compte de ressources sans propriétaire, la règle de corrélation retourne une liste de noms ou de conditions d'attributs qui sera utilisée pour sélectionner les propriétaires potentiels. Sélectionnez une règle pour rechercher les utilisateurs Identity Manager auxquels peuvent appartenir les comptes de ressources sans propriétaire.
- **Règle de confirmation de comptes**. Une règle de confirmation de comptes élimine tout non propriétaire de la liste des propriétaires potentiels sélectionnés par la règle de corrélation. Selon la vue complète d'un utilisateur Identity Manager et les attributs d'un compte de ressources sans propriétaire, une règle de confirmation retourne true si l'utilisateur possède le compte et false dans le cas contraire. Sélectionnez une règle pour tester chaque propriétaire potentiel d'un compte de ressources. Si vous sélectionnez Aucune règle de confirmation, le système accepte tous les propriétaires potentiels sans confirmation.

Remarque – Si, dans votre environnement, la règle de corrélation ne sélectionne pas plus d'un utilisateur par compte, vous n'avez pas besoin de règle de confirmation.

- **Administrateur mandataire**. Spécifiez l'administrateur à utiliser lors de l'exécution des réponses de réconciliation. La réconciliation peut effectuer uniquement les opérations que l'administrateur mandataire désigné est autorisé à effectuer. La réponse utilisera le formulaire utilisateur (si nécessaire) associé à cet administrateur.

Vous pouvez également sélectionner l'option Pas d'administrateur proxy. Lorsque cette option est sélectionnée, les résultats de la réconciliation peuvent être affichés, mais aucune action en réponse ni aucun flux de travaux ne sont effectués.

- **Options de situation** (et réponses). La réconciliation reconnaît plusieurs types de situations. Les situations sont décrites ci-dessous. Spécifiez dans la colonne Réponse l'action devant être exécutée par la réconciliation.
  - **CONFIRMÉ**. Le compte attendu existe.

    Pour qu'il soit marqué CONFIRMÉ, les conditions suivantes doivent être remplies :

    - Identity Manager s'attend à ce que le compte existe.
    - Le compte existe sur la ressource.
  - **COLLISION**. Un même compte sur une ressource a été assigné à deux utilisateurs Identity Manager ou plus.
  - **SUPPRIMÉ**. Le compte attendu n'existe pas.

    Pour qu'il soit marqué SUPPRIMÉ, les conditions suivantes doivent être remplies :

    - Identity Manager s'attend à ce que le compte existe.
    - Le compte n'existe pas sur la ressource.
  - **TROUVÉ**. Le processus de réconciliation trouve un compte correspondant sur une ressource assignée.

    Pour qu'il soit marqué TROUVÉ, les conditions suivantes doivent être remplies :

    - Identity Manager s'attend à ce que le compte puisse ou ne puisse pas exister (un compte peut exister ou peut ne pas exister sur une ressource si la ressource a été assignée à l'utilisateur mais n'a pas encore été provisionnée).
    - Le compte existe sur la ressource.
  - **MANQUANT**. Il n'y a aucun compte correspondant sur une ressource assignée à l'utilisateur.

    Pour qu'il soit marqué MANQUANT, les conditions suivantes doivent être remplies :

    - Identity Manager s'attend à ce que le compte puisse ou ne puisse pas exister (un compte peut exister ou peut ne pas exister sur une ressource si la ressource a été assignée à l'utilisateur mais n'a pas encore été provisionnée).
    - Le compte n'existe pas sur la ressource.
  - **NON ASSIGNÉ**. Le processus de réconciliation trouve un compte correspondant sur une ressource non assignée à l'utilisateur.

    Pour qu'il soit marqué NON ASSIGNÉ, les conditions suivantes doivent être remplies :

    - Identity Manager ne s'attend pas à ce que le compte existe (Identity Manager ne s'attend pas à ce que le compte existe si cette ressource n'est pas assignée à l'utilisateur).
    - Le compte existe sur la ressource.

- **PAS DE CORRESPONDANCE**. Le compte de ressources ne correspond à aucun utilisateur.
- **CONTESTÉ**. Le compte de ressources correspond à plusieurs utilisateurs.

  Sélectionnez l'une des options de réponse suivantes (les options disponibles varient en fonction de la situation) :

  - **Créer un nouvel utilisateur Identity Manager basé sur le compte de ressources**. Exécute le formulaire utilisateur sur les attributs du compte de ressource pour créer un nouvel utilisateur. Le compte de ressources n'est pas mis à jour suite aux modifications.
  - **Créer un compte de ressources pour l'utilisateur Identity Manager**. Recrée le compte de ressources manquant en utilisant le formulaire utilisateur pour régénérer les attributs du compte de ressources.
  - **Supprimer le compte de ressources et Désactiver le compte de ressources**. Supprime/Désactive le compte sur la ressource.
  - **Lier le compte de ressources à l'utilisateur Identity Manager et Supprimer le lien entre le compte de ressources et l'utilisateur**. Ajoute ou annule l'assignation du compte de ressources à/de l'utilisateur. Aucun traitement de formulaire n'est exécuté.
  - **Ne faire rien**. Sélectionnez cette option si vous ne voulez pas que la réconciliation effectue de réparations.

    Vous pouvez réparer manuellement toute situation de compte détectée par la réconciliation. Dans le menu, cliquez sur Ressources → Examiner index de compte. De là, vous pouvez parcourir la situation enregistrée pour tous les comptes qui ont été réconciliés. Cliquez avec le bouton droit de la souris pour afficher la liste des options de réparation valides. Pour plus d'informations, voir "Examen de l'index de comptes" à la page 263.

- **Flux de travaux de pré-réconciliation**. La réconciliation peut être configurée pour exécuter un flux de travaux spécifié par l'utilisateur avant la réconciliation d'une ressource. Spécifiez le flux de travaux que la réconciliation doit exécuter. Sélectionnez Ne pas exécuter le flux de travaux si aucun flux de travaux ne doit être exécuté.
- **Flux de travaux par compte**. La réconciliation peut être configurée pour exécuter un flux de travaux spécifié par l'utilisateur après avoir répondu à la situation d'un compte de ressources. Spécifiez le flux de travaux que la réconciliation doit exécuter. Sélectionnez Ne pas exécuter le flux de travaux si aucun flux de travaux ne doit être exécuté.
- **Flux de travaux de post-réconciliation**. La réconciliation peut être configurée pour exécuter un flux de travaux spécifié par l'utilisateur après l'exécution de la réconciliation pour 'une ressource. Spécifiez le flux de travaux que la réconciliation doit exécuter. Sélectionnez **Ne pas exécuter le flux de travaux** si aucun flux de travaux ne doit être exécuté.
- **Expliquer la situation**. Lorsque cette option est activée, la réconciliation enregistre des informations complémentaires expliquant le mode de classification des situations de compte. Cette option est désactivée par défaut. L'enregistrement des explications allongera l'exécution de la procédure de réconciliation.

- **Nombre maximal d'erreurs**. Si cette option est activée, la réconciliation est interrompue automatiquement lorsque le nombre d'erreurs indiqué est atteint au cours du traitement. La valeur 0 indique l'absence de nombre maximal d'erreurs. Désactivez l'option Hériter de la stratégie par défaut pour afficher le champ du nombre maximal d'erreurs autorisées, puis entrez une valeur.
- **Proportion maximale de comptes supprimés en natif**. Cette option est une protection qui évalue le nombre de comptes manquants sur une ressource et, si un certain seuil est franchi, empêche le programme de réconciliation d'en supprimer les liens.

  Pour activer cette fonction, désactivez la case à cocher Hériter de la stratégie par défaut et spécifiez le pourcentage souhaité dans le champ Proportion maximale de comptes supprimés en natif. Le seuil doit être défini sous la forme d'une valeur de pourcentage entière comprise entre 0 et 100 (0 désactive cette fonction.)

  Si le pourcentage de comptes supprimés dépasse le seuil fixé, la réconciliation poursuit le traitement des tâches non liées aux comptes manquants et se termine en générant une erreur.

Cliquez sur Enregistrer pour enregistrer vos modifications de stratégie.

Lancement de la réconciliation

Cette section décrit deux options permettant de lancer les tâches de réconciliation :

- l'exécution de la réconciliation à intervalles programmés ;
- la réconciliation immédiate.

▼ Pour exécuter la réconciliation à intervalles réguliers

1. **Ouvrez la page Éditer la stratégie de réconciliation comme décrit dans "Édition des stratégies de réconciliation" à la page 256.**
2. **Spécifiez les paramètres de programmation de la réconciliation.**

   La réconciliation sera exécutée conformément aux paramètres définis dans la stratégie.

▼ Pour exécuter immédiatement la réconciliation

1. **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**
2. **Choisissez une ressource dans la liste Ressource.**
3. **Choisissez une option dans la liste Actions de ressource.**

Les options sont les suivantes :

- Réconciliation complète maintenant ;
- Réconciliation incrémentielle maintenant.

  La réconciliation est exécutée conformément aux paramètres définis dans la stratégie. Si la stratégie planifie une exécution régulière de la réconciliation, cette dernière continuera à s'exécuter comme spécifié.

▼ Pour annuler la réconciliation

1. **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**
2. **Choisissez dans la Liste des ressources la ressource pour laquelle vous voulez annuler la réconciliation.**
3. **Localisez la liste Actions de ressource et sélectionnez Annuler la réconciliation.**

Affichage de l'état de réconciliation

Il existe deux manières d'afficher l'état de réconciliation : Pour afficher l'état de réconciliation détaillé, ouvrez la page Résultats sommaires de réconciliation pour une ressource spécifique. L'état de réconciliation limité est également disponible directement dans la Liste des ressources.

▼ Pour afficher l'état de réconciliation détaillé

Affichez l'état de réconciliation détaillé en utilisant la page Résultats sommaires de réconciliation.

1. **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**
2. **Choisissez dans la Liste des ressources la ressource dont vous voulez afficher l'état de réconciliation.**
3. **Localisez la liste Actions de ressource et sélectionnez Visualiser l'état de réconciliation.**

   La page Résultats sommaires de réconciliation correspondant à la ressource s'ouvre.

▼ Pour afficher l'état de réconciliation dans la liste des ressources

Vous pouvez également afficher l'état de réconciliation à partir de la Liste des ressources.

1. **Ouvrez l'interface administrateur.**
2. **Cliquez sur Ressources dans le menu principal.**

La colonne **Statut** rapporte les conditions d'état de réconciliation suivantes :

- **inconnu**. L'état n'est pas connu. Les résultats de la dernière tâche de réconciliation ne sont pas disponibles.
- **désactivé**. La réconciliation est désactivée.
- **en échec**. L'exécution de la dernière tâche de réconciliation a échoué.
- **réussi**. La dernière réconciliation a réussi.
- **achevé avec des erreurs**. La dernière réconciliation s'est terminée mais avec des erreurs.

Remarque – Vous devez actualiser cette page pour afficher les changements d'état (les informations ne sont pas actualisées automatiquement).

Travailler avec l'index de comptes

L'index de comptes enregistre le dernier état connu de chaque compte de ressources reconnu par Identity Manager. Il est principalement mis à jour par la réconciliation, mais d'autres fonctions d'Identity Manager le mettent également à jour le cas échéant.

Les outils de détection ne mettent pas à jour l'index de comptes.

▼ Pour effectuer une rechercher dans l'index de comptes

Effectuez une recherche dans l'index de comptes pour afficher le dernier état connu d'un compte de ressource donné.

1. **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**
2. **Choisissez dans la Liste des ressources la ressource pour laquelle vous voulez effectuer une recherche dans l'index de comptes.**
3. **Localisez la liste Actions de ressource et sélectionnez Rechercher dans l'index de comptes.**

   La page Rechercher dans l'index de comptes s'ouvre.
4. **Sélectionnez un type de recherche, puis entrez les attributs de la recherche ou sélectionnez-les.**
   - **Nom de compte de ressources**. Sélectionnez cette option puis l'un des modificateurs (commence par, contient ou est) et saisissez tout ou partie d'un nom de compte.
   - **La ressource est l'une des suivantes :** Sélectionnez cette option, puis une ou plusieurs ressources dans la liste afin de rechercher les comptes réconciliés résidant sur les ressources spécifiées.

- **Propriétaire**. Sélectionnez cette option puis l'un des modificateurs (commence par, contient ou est) et saisissez tout ou partie d'un nom de propriétaire. Pour rechercher les comptes sans propriétaire, effectuez la recherche dans la situation PAS DE CORRESPONDANCE ou CONTESTÉ.
- **La situation est l'une des suivantes :**. Sélectionnez cette option, puis une ou plusieurs situations dans la liste afin de rechercher les comptes réconciliés se trouvant dans les situations spécifiées.

5 **Cliquez sur Rechercher pour rechercher des comptes en fonction des paramètres indiqués. Pour limiter les résultats de la recherche, vous pouvez indiquer le nombre de votre choix dans le champ Limiter les résultats aux premiers. Par défaut, la recherche est limitée aux 1 000 premiers comptes trouvés.**

Cliquez sur Réinitialiser la requête pour désélectionner tous les critères de la page et en sélectionner de nouveaux.

Examen de l'index de comptes

Il est également possible d'afficher tous les comptes utilisateur Identity Manager et, en option, de les réconcilier utilisateur par utilisateur.

▼ Pour examiner l'index de comptes

1 **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**

2 **Cliquez sur Examiner index de compte dans le menu secondaire.**

La page Examiner index de compte s'ouvre.

Le tableau affiche tous les comptes de ressources connus d'Identity Manager (que ces comptes appartiennent ou non à un utilisateur Identity Manager). Ces informations sont regroupées par ressource par l'organisation Identity Manager. Pour changer cette vue, effectuez une sélection dans la liste Changer index vue.

Travailler avec les comptes

Pour travailler avec les comptes sur une ressource, sélectionnez la vue d'index Grouper par ressource. Identity Manager affiche des dossiers pour chaque type de ressources. Naviguez vers une ressource spécifique en développant un dossier. Cliquez sur + ou - à proximité de la ressource pour afficher tous les comptes de ressources connus d'Identity Manager.

Les comptes qui ont été ajoutés directement à la ressource depuis la dernière réconciliation effectuée sur cette ressource ne sont pas affichés.

Selon la situation d'un compte donné en ce moment, vous serez en mesure d'effectuer différentes actions. Cliquez avec le bouton droit de la souris pour afficher la liste des options de réparation valides. Vous pouvez aussi afficher les détails du compte ou choisir de réconcilier ce compte.

Travailler avec les utilisateurs

Pour travailler avec les utilisateurs Identity Manager, sélectionnez la vue d'index Grouper par utilisateur. Dans cette vue, les utilisateurs et organisations Identity Manager sont affichés dans une hiérarchie similaire à la page Liste des comptes. Pour voir les comptes actuellement assignés à un utilisateur dans Identity Manager, naviguez jusqu'à cet utilisateur et cliquez sur l'indicateur en regard de son nom. Les comptes de cet utilisateur et leur état courant connu d'Identity Manager s'affichent sous le nom de l'utilisateur.

Selon la situation d'un compte donné en ce moment précis, vous serez en mesure d'effectuer différentes actions. Vous pouvez aussi afficher les détails du compte ou choisir de réconcilier ce compte.

Utilisation des règles Répétition TaskSchedule

Les règles Règle Répétition TaskSchedule permettent d'effectuer des ajustements sur un programme de réconciliation. Par exemple, pour reporter les réconciliations programmées le samedi au lundi suivant, vous utiliserez une règle Répétition TaskSchedule.

Les règles Répétition TaskSchedule permettent de procéder à des ajustements pour les réconciliations complètes et incrémentielles.

Pour toute information sur la sélection des règles Répétition TaskSchedule, voir "Édition des stratégies de réconciliation" à la page 256.

Modalités de programmation des heures d'exécution de réconciliation

À la fin d'une tâche de réconciliation, le composant réconciliateur contrôle l'heure de la prochaine exécution programmée.

Il commence par regarder la programmation par défaut pour connaître l'heure de la prochaine exécution. Il exécute ensuite toutes les règles Répétition TaskSchedule applicables pour voir si des ajustements de programmation s'imposent. Si un ajustement est nécessaire, la programmation de la règle ignore celle par défaut pour la réconciliation en question.

Remarque – Les règles Répétition TaskSchedule ne peuvent pas écraser la programmation par défaut. Elles peuvent seulement ignorer les heures de départ programmées tâche par tâche.

▼ Pour afficher l'exemple de règle Accepter toutes les dates

Cette section décrit l'exemple de règle Accepter toutes les dates.

1. **Dans un éditeur de texte, ouvrez** `ReconRules.xml`**, qui figure dans le répertoire** `sample` **d'Identity Manager.**

2. **Recherchez la règle nommée** `SCHEDULING_RULE_ACCEPT_ALL_DATES`**.**

   Pour qu'une règle soit listée dans le menu déroulant Règle Répétition TaskSchedule (sur la page Éditer la stratégie de réconciliation), l'attribut `subtype` de la règle doit être défini sur `SUBTYPE_TASKSCHEDULE_REPETITION_RULE:`.

   ```
   <Rule subtype='SUBTYPE_TASKSCHEDULE_REPETITION_RULE'
   name='SCHEDULING_RULE_ACCEPT_ALL_DATES'>
   ```

   Comme nous l'avons fait remarquer précédemment, les règles Répétition TaskSchedule peuvent modifier la programmation de réconciliation par défaut.

   La variable `calculatedNextDate` peut soit accepter la date suivante, qui est calculée selon la méthode par défaut, soit retourner une autre date. Comme écrit dans l'exemple de règle, `calculatedNextDate` accepte sans condition la date par défaut, comme indiqué dans l'extrait suivant :

   ```
   <RuleArgument name='calculatedNextDate'/>
   <block>
     <ref>calculatedNextDate</ref>
   </block>
   ```

   Pour créer un programme personnalisé, remplacez la logique de règle entre les éléments `<block>`. Par exemple, pour remplacer l'heure de début de la réconciliation par 10h00 le samedi, incluez le JavaScript suivant entre les éléments `<block>` :

   ```
   <block>
     <script>
        var calculatedNextDate = env.get('calculatedNextDate');

       // Test to see if this task is scheduled for a Saturday
       // (Note that 6 is used to denote Saturday in JavaScript)
       if(calculatedNextDate.getDay() == 6) {
         // If so, set the time to 10:00:00
         calculatedNextDate.setHours(10);
         calculatedNextDate.setMinutes(0);
         calculatedNextDate.setSeconds(0);
       }
       // Return the modified date
       calculatedNextDate;
     </script>
   </block>
   ```

   Dans "Pour afficher l'exemple de règle Accepter toutes les dates" à la page 264, `calculatedNextDate` est au départ défini sur l'heure programmée par défaut. Si l'heure de la prochaine exécution est un samedi, la règle programme donc le début de la réconciliation pour 10h00. Si la date de la prochaine exécution programmée n'est pas un samedi, l'exemple de règle

"Pour afficher l'exemple de règle Accepter toutes les dates" à la page 264 retourne `calculatedNextDate` sans effectuer aucun ajustement d'heure et la programmation par défaut est utilisée.

Pour plus d'informations sur la création et l'utilisation de règles personnalisées dans Identity Manager, voir le Chapitre 4, "Working with Rules" du *Sun Identity Manager Deployment Reference*.

Adaptateurs Active Sync

La fonctionnalité Active Sync d'Identity Manager permet de synchroniser les informations stockées dans une *ressource externe faisant autorité* (par exemple une application ou une base de données) avec les données utilisateur d'Identity Manager. Configurer la synchronisation pour une ressource Identity Manager permet à celle-ci d'*écouter* ou effectuer des interrogations sur les changements à la ressource faisant autorité.

Vous pouvez configurer la façon dont les changements des attributs de la ressource confluent dans Identity Manager en spécifiant le formulaire d'entrée dans la stratégie de synchronisation de la ressource (pour le type d'objets cibles approprié).

Remarque – Les pages de ce chapitre sont consacrées à l'exécution de tâches Active Sync au moyen de l'interface administrateur. Pour des informations plus approfondies sur Active Sync, voir le Chapitre 3, "Data Loading and Synchronization" du *Sun Identity Manager Deployment Guide*.

Configuration de la synchronisation

Identity Manager utilise une stratégie de synchronisation pour activer la synchronisation pour les ressources.

▼ Pour éditer ou configurer la synchronisation

Chaque ressource a sa propre stratégie de synchronisation. Suivez les étapes ci-après pour configurer ou éditer une stratégie de synchronisation :

1. **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**
2. **Sélectionnez dans la Liste des ressources la ressource pour laquelle vous voulez configurer la synchronisation.**
3. **Dans la liste Actions de ressource, trouvez et sélectionnez Éditer la stratégie de synchronisation.**

   La page Éditer la stratégie de synchronisation correspondant à la ressource s'ouvre.

Spécifiez les options suivantes dans la page Éditer la stratégie de synchronisation pour configurer la synchronisation :

- **Type d'objet cible**. Sélectionnez le type d'utilisateurs auquel la stratégie s'applique, Utilisateurs Identity Manager ou Utilisateurs de Service Provider.

  Remarque – Dans une implémentation Service Provider, vous devez configurer une stratégie de synchronisation (avec Utilisateurs de Service Provider spécifié en tant que type d'objet) pour activer la synchronisation des données pour ces utilisateurs. Pour toute information sur les utilisateurs de Service Provider, voir le Chapitre 17, "Administration de Service Provider".

- **Paramètres de planification**. Cette section permet de spécifier la méthode de démarrage et la programmation des interrogations.

  Vous pouvez spécifier les types de démarrage suivants :

  - **Automatique ou Automatique avec basculement**. Démarre la source faisant autorité au démarrage d'Identity System.
  - **Manuel**. Requiert l'intervention d'un administrateur pour démarrer la source faisant autorité.
  - **Désactivé**. Désactive la ressource.

    Utilisez les options Date de début et Heure de début pour spécifier le début de l'interrogation. Spécifiez les cycles d'interrogation en sélectionnant un intervalle et en entrant une valeur pour ce dernier (secondes, minutes, heures, jours, semaines, mois).

    Remarque – Si vous changez la méthode de démarrage ou la programmation d'interrogation, vous devez redémarrer le serveur pour que les changements soient appliqués.

    Si vous définissez une date et une heure de début d'interrogation ultérieures à la date actuelle, l'interrogation commencera au moment indiqué. Si la date et l'heure de début d'interrogation que vous définissez sont antérieures à la date actuelle, Identity Manager détermine alors le moment à partir duquel effectuer l'interrogation en fonction de ces informations et de la fréquence d'interrogation.

    Par exemple :

    - Vous configurez une synchronisation active pour la ressource le 18 juillet 2005 (un mardi).
    - Vous définissez une interrogation hebdomadaire, avec une date et une heure de début définies au 4 juillet 2005 à 9h00 (un lundi).

  Dans ce cas, la ressource commencera l'interrogation le 25 juillet 2005 (le lundi suivant).

Si vous n'indiquez pas de date ni d'heure de début, l'interrogation est immédiatement exécutée. Si vous suivez cette approche, à chaque redémarrage du serveur d'application, toutes les ressources configurées pour la synchronisation active commenceront immédiatement l'interrogation. L'approche standard consiste à définir une date et une heure de début.

- **Serveurs de synchronisation**. Dans un environnement clustérisé, tout serveur peut exécuter la synchronisation. Sélectionnez une option pour spécifier les serveurs qui seront utilisés pour exécuter la synchronisation pour la ressource.
  - Sélectionnez tout serveur disponible si le serveur sur lequel la synchronisation s'exécute n'a pas d'importance. Un serveur sera choisi parmi l'ensemble des serveurs possibles au début de la synchronisation.
  - Sélectionnez Utiliser les paramètres de `waveset.properties` pour utiliser les serveurs spécifiés à cet emplacement pour exécuter la synchronisation (cette fonctionnalité est désapprouvée).
  - Sélectionnez Utiliser les serveurs spécifiés puis sélectionnez un ou plusieurs serveurs disponibles dans la liste des serveurs de synchronisation, pour sélectionner des serveurs spécifiques pour exécuter la synchronisation.
- **Paramètres spécifiques aux ressources**. Cette section permet de spécifier la façon dont la synchronisation déterminera les données à traiter pour la ressource.
- **Paramètres communs**. Spécifiez les paramètres généraux pour les activités de synchronisation des données.

  Ces paramètres sont les suivants :
  - **Administrateur mandataire**. Sélectionnez l'administrateur qui traitera les mises à jour. Toutes les actions seront autorisées par le biais des capacités assignées à cet administrateur. Vous devez sélectionner un administrateur mandataire avec un formulaire utilisateur vide.
  - **Formule de saisie des données**. Sélectionnez le formulaire de saisie qui traitera les mises à jour des données. Cet élément de configuration optionnel permet de transformer les attributs avant de les enregistrer sur des comptes.
  - **Règles** (*facultatif*). Sélectionnez les règles à utiliser pendant le processus de synchronisation des données.

Vous pouvez spécifier ce qui suit :

- **Règle de traitement**. Sélectionnez cette règle pour spécifier une règle de traitement à exécuter pour chaque compte entrant. Cette sélection prévaut sur toutes les autres options. Si vous spécifiez une règle de traitement, le processus sera exécuté pour chaque ligne, quels que soient les autres paramètres de cette ressource. Il peut s'agir d'un nom de processus ou d'une règle évaluant un nom de processus.
- **Règle de corrélation**. Sélectionnez une règle de corrélation pour ignorer la règle de corrélation spécifiée dans la stratégie de réconciliation de la ressource. Les règles de corrélation permettent d'établir une corrélation entre les comptes de ressource et les comptes Identity System.
- **Règle de confirmation**. Sélectionnez une règle de confirmation pour ignorer la règle de confirmation spécifiée dans la stratégie de réconciliation de la ressource.
- **Règle de traitement de résolution**. Sélectionnez cette règle pour spécifier le nom d'une définition de tâche à exécuter en cas de correspondances multiples pour un enregistrement dans la source de données. Il s'agit normalement d'un processus qui invite un administrateur à effectuer une action manuellement. Il peut être constitué d'un nom de processus ou d'une règle évaluant un nom de processus.
- **Règle de suppression**. Spécifiez une règle qui retourne true (vrai) ou false (faux) et qui sera évaluée pour chaque mise à jour d'utilisateur entrant pour déterminer si une suppression doit être effectuée.

- **Créer des comptes sans correspondance**. Lorsque cette option est activée (true), l'adaptateur tente de créer les comptes qu'il ne trouve pas dans le système Identity Manager. Si elle n'est pas activée, l'adaptateur soumet le compte au processus retourné par la Règle de traitement de résolution.
- **Paramètres de journalisation**. Saisissez une valeur pour les options de journalisation.

  Les options de journalisation sont les suivantes :

  - **Nombre maximum d'archives de consignation**. Si cette option est supérieure à zéro, les `N` derniers fichiers journaux sont conservés. Si elle est égale à zéro, alors un seul fichier journal est réutilisé. Si elle est égale à `-1`, les fichiers journaux ne sont jamais supprimés.
  - **Durée de consignation active maximum**. Une fois cette période écoulée, le journal actif est archivé. Si la valeur indiquée est zéro, aucun archivage en fonction du temps ne sera effectué. Si l'option Nombre maximum d'archives de consignation est définie sur zéro, le journal actif sera tronqué et réutilisé après cette période. Ce critère de durée est évalué indépendamment de ceux définis par la Taille maximale du fichier journal.

    Entrez un chiffre et sélectionnez l'unité de temps (jours, heures, minutes, mois, secondes ou semaines). L'unité par défaut est le jour.

- **Chemin d'accès du fichier journal**. Entrez le chemin d'accès au répertoire dans lequel créer les fichiers journaux actifs et archivés. Les noms des fichiers journaux doivent commencer par le nom de la ressource.
- **Dimension maximale du fichier journal**. Entrez la taille maximale, en octets, du fichier journal actif. Le fichier journal actif est archivé lorsqu'il atteint la taille maximale. Si l'option Nombre maximum d'archives de consignation est définie sur zéro, le journal actif sera tronqué et réutilisé après cette période. Ces critères de taille sont évalués indépendamment des critères d'âge spécifiés par la durée de consignation active maximum.
- **Niveau du journal**. Spécifiez un niveau de journalisation.

  Les niveaux de journalisation suivants sont disponibles :

  - **0**. Pas de journalisation
  - **1**. Erreur
  - **2**. Informations
  - **3**. Informations détaillées
  - **4**. Déboguer

4 Cliquez sur Enregistrer pour enregistrer les paramètres de stratégie pour la ressource.

Édition des adaptateurs Active Sync

Vous devez arrêter la synchronisation avant d'éditer l'adaptateur Active Sync.

▼ Pour arrêter la synchronisation

1 Ouvrez la page Éditer la synchronisation (pour les instructions, voir "Pour éditer ou configurer la synchronisation" à la page 266.)

2 Sous Paramètres de planification, localisez Type lancement et sélectionnez Désactivé.

Les utilisateurs de Service Provider désélectionneront quant à eux l'option Activer la synchronisation.

Un message d'avertissement s'affiche indiquant que la synchronisation active est désactivée.

3 Cliquez sur Enregistrer.

La désactivation de la synchronisation pour une ressource résulte en l'arrêt de la tâche de synchronisation quand les changements sont enregistrés.

Réglage des performances de l'adaptateur Active Sync

La synchronisation étant une tâche d'arrière-plan, la configuration de l'adaptateur Active Sync risque d'influer négativement sur les performances du serveur.

Le réglage des performances de l'adaptateur Active Sync consiste en les tâches suivantes :

Gérez les adaptateurs Active Sync par le biais de la liste des ressources. Sélectionnez un adaptateur Active Sync puis accédez aux actions de commande de démarrage, arrêt et actualisation du statut depuis la section *Synchronisation* de la liste Actions de ressource.

Modification de l'intervalle d'interrogation

L'intervalle d'interrogation détermine quand l'adaptateur Active Sync commence à traiter de nouvelles informations. Les intervalles d'interrogation doivent être déterminés sur la base du type de l'activité effectuée. Par exemple, si l'adaptateur lit dans une grande liste d'utilisateurs depuis une base de données et met à jour tous les utilisateurs dans Identity Manager à chaque fois, envisagez d'exécuter ce processus tous les jours au petit matin. Certains adaptateurs peuvent avoir un outil de recherche rapide pour les nouveaux éléments à traiter et être réglés pour s'exécuter toutes les minutes.

Spécification de l'hôte sur lequel l'adaptateur s'exécutera

Pour spécifier l'hôte sur lequel les adaptateurs s'exécuteront, vous devez éditer la propriété `sources.hosts` dans le fichier `waveset.properties`.

Spécifiez l'un des paramètres suivants :

- Définissez `sources.hosts=`*`nomhôte1,nomhôte2,nomhôte3`* . Ce paramètre liste les noms d'hôtes des machines qui exécuteront les adaptateurs Active Sync. L'adaptateur s'exécutera sur le premier hôte disponible listé dans ce champ.

  Remarque – Le *nomhôte* que vous saisissez doit correspondre à une entrée de la liste de serveurs d'Identity Manager. Affichez la liste des serveurs depuis l'onglet Configurer.

- Définissez `sources.hosts=localhost`. Avec ce paramètre, l'adaptateur s'exécutera sur le premier serveur Identity Manager qui tentera de démarrer Active Sync pour la ressource.

Remarque – Dans un cluster, vous devriez utiliser la première option si vous avez besoin de spécifier un serveur spécifique.

Ce paramétrage de la propriété ne s'applique qu'à la synchronisation des utilisateurs Identity Manager. La configuration de l'hôte pour la synchronisation des utilisateurs de Service Provider est déterminée par la Stratégie de synchronisation.

Les adaptateurs Active Sync qui ont besoin de davantage de mémoire et de cycles de CPU peuvent être configurés pour s'exécuter sur des serveurs dédiés pour faciliter l'équilibrage de charge des systèmes.

Démarrage et arrêt

Les adaptateurs Active Sync peuvent être désactivés, démarrés manuellement ou démarrés automatiquement. Vous devez avoir la capacité administrateur appropriée pour changer les ressources Active Sync pour démarrer ou arrêter les adaptateurs Active Sync. Pour toute information sur les capacités administrateur, voir "Catégories de capacités" à la page 217.

Lorsqu'un adaptateur est défini sur automatique, il redémarre avec le serveur d'application. Lorsque vous démarrez un adaptateur, il s'exécute immédiatement en suivant l'intervalle d'interrogation spécifié. Lorsque vous arrêtez un adaptateur, celui-ci s'arrête au premier contrôle d'indicateur d'arrêt suivant.

Journalisation de l'adaptateur

Les journaux d'adaptateur capturent des informations sur l'adaptateur actuellement en train d'effectuer le traitement. La quantité de détails capturée par le journal dépend du niveau de journalisation défini. Les journaux d'adaptateur sont utiles pour le débogage des problèmes et pour suivre la progression du processus de l'adaptateur.

Chaque adaptateur a son propre fichier journal, chemin et niveau de journalisation. Vous spécifiez ces valeurs dans la section Journalisation de la Stratégie de synchronisation pour le type d'utilisateurs approprié (Identity Manager ou Service Provider).

Ne supprimez les journaux d'un adaptateur que lorsque ce dernier a été arrêté. Dans la plupart des cas, il convient d'effectuer une copie à des fins d'archivage avant de supprimer un journal d'adaptateur.

◆ ◆ ◆ CHAPITRE 8

Génération de rapports

Identity Manager génère des rapports pour les activités système automatisées et manuelles. Un solide ensemble de fonctionnalités de génération de rapports permet de capturer et d'afficher à tout moment des informations et statistiques d'accès importantes sur les utilisateurs Identity Manager.

Ce chapitre présente les types de rapports générés par Identity Manager et explique la création, l'exécution des rapports, leur envoi sous forme d'e-mails ainsi que le téléchargement des informations qu'ils contiennent.

Ce chapitre se compose des rubriques suivantes :

Travailler avec les rapports

Dans Identity Manager, les rapports constituent une catégorie de tâches spéciale. Résultat, vous travaillez avec des rapports dans deux zones de l'interface administrateur d'Identity Manager :

- **Rapports (Exécuter des rapports)**. La zone Exécuter des rapports permet de définir, exécuter, supprimer et télécharger les rapports. Seuls les administrateurs ayant des capacités suffisantes peuvent définir, exécuter, supprimer et télécharger des rapports. Pour plus d'informations, voir l'Annexe D, “Définitions des capacités”.
- **Tâches du serveur**. Une fois que vous avez défini des rapports, allez à la zone Tâches programmées (Tâches du serveur → Gérer la planification) pour programmer et modifier les tâches de rapport. Les objets TaskDefinition doivent contenir `visibility=schedule` pour pouvoir être programmés. Utilisez les pages de débogage pour effectuer cette modification. Pour plus d'informations, voir “Édition des objets Configuration Identity Manager” à la page 118.

Types de rapports

Les rapports se classent en deux catégories :

- **Rapports d'Identity Manager**. Cette catégorie inclut tout un éventail de types de rapports, notamment les rapports en temps réel, récapitulatifs, de journal d'audit, de journal système et d'utilisation.
- **Rapports de l’auditeur**. Cette catégorie fournit des informations qui vous aideront à gérer la compatibilité des utilisateurs sur la base des critères définis dans les stratégies d'audit.

Au sein de ces deux catégories, les rapport se subdivisent en de nombreux types. Les différents types de rapports sont examinés plus en détail plus loin dans ce chapitre. Les rapports d'Identity Manager sont examinés à partir de la section “Rapports d'Identity Manager” à la page 280 et ceux de l'auditeur à partir de la section“Rapports de l’auditeur” à la page 289.

Pour les instructions à suivre pour afficher les rapports d'Identity Manager et de l'auditeur, voir “Affichage des rapports” à la page 276.

Exécution des rapports

▼ Pour exécuter un rapport

1 **Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.**

La page Exécuter des rapports s'ouvre.

2 **Pour afficher la liste des rapports d'Identity Manager disponibles, sélectionnez Rapports d'Identity Manager dans le menu déroulant Type du rapport (cette option est sélectionnée par défaut).**

Pour afficher la liste des rapports de l'auditeur disponibles, sélectionnez Rapports de l'auditeur dans le menu déroulant Type du rapport. Pour plus d'informations, voir "Travailler avec les rapports de l'auditeur" à la page 469 au Chapitre 15, "Audit : contrôler la conformité".

La Figure 8–1 représente un exemple de l'écran Exécuter des rapports. Les rapports de l'auditeur sont sélectionnés dans le menu déroulant Type du rapport.

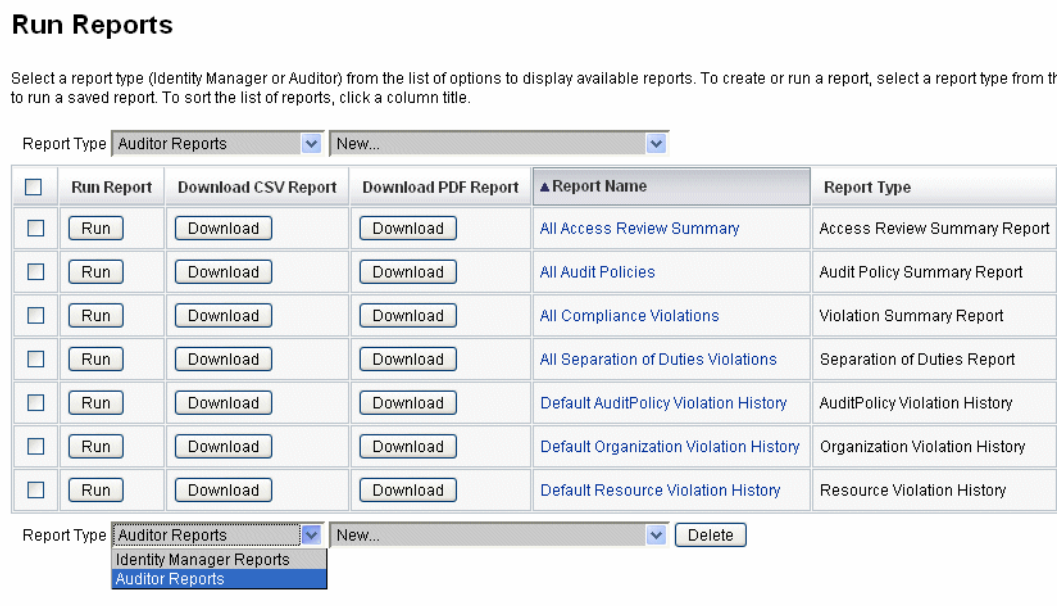


FIGURE 8–1 Sélection d'Exécuter des rapports

3 **Cliquez sur Exécuter pour lancer un rapport.**

Remarque – Pour permettre l'exécution simultanée de plusieurs instances du même rapport, éditez ce rapport et sélectionnez Autoriser l'exécution simultanée de rapports. L'activation de cette option permet à plusieurs administrateurs d'exécuter le même rapport en même temps.

Si deux instances ou plus d'un même rapport sont exécutées simultanément, le nom de chaque rapport sera complété de l'ID de son administrateur suivi d'un horodatage.

Affichage des rapports

Après avoir exécuté un rapport depuis la page Exécuter des rapports, vous pouvez en afficher la sortie immédiatement ou ultérieurement.

▼ Pour afficher un rapport

1. **Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.**
   La page Exécuter des rapports s'ouvre.
2. **Cliquez sur l'onglet Afficher les rapports.**
   La page Afficher les rapports s'ouvre.
3. **Cliquez sur un rapport pour l'afficher.**

Création de rapports

Cette section explique la création d'un nouveau rapport d'Identity Manager ou de l'auditeur qui n'est pas basé sur un rapport existant.

Remarque – Pour modifier un rapport existant et l'enregistrer sous un nouveau nom, reportez-vous à "Édition et clonage des rapports" à la page 277 dans la section suivante.

▼ Pour créer un nouveau rapport

1. **Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.**
   La page Exécuter des rapports s'ouvre.
2. **Utilisez le menu déroulant Type du rapport pour sélectionner une catégorie de rapports.**
   Il existe deux catégories de rapports :
   - les rapports d'Identity Manager,
   - les rapports d'Identity Auditor.
3. **Utilisez le menu déroulant suivant pour sélectionner un type de rapport spécifique à créer (ce menu commence par Nouveau).**
   Identity Manager affiche la page Définir un rapport, laquelle permet de choisir les options permettant de créer le rapport, de l'exécuter ou de l'enregistrer.

Après avoir entré et sélectionné les critères du rapport, vous pouvez :

- Exécuter le rapport sans l'enregistrer. Cliquez sur Exécuter pour lancer le rapport. Identity Manager n'enregistre pas le rapport (si vous avez défini un nouveau rapport) ni les critères de rapport modifiés (si vous avez édité un rapport existant).
- Enregistrer le rapport. Cliquez sur Enregistrer pour l'enregistrer. Une fois enregistré, vous pouvez exécuter le rapport depuis la page Exécuter des rapports (la liste des rapports).

Pour plus d'informations sur l'exécution des rapports, voir "Exécution des rapports" à la page 274.

Édition et clonage des rapports

Cette section explique comment modifier ou cloner un rapport existant et l'enregistrer sous un nouveau nom.

▼ Pour éditer ou cloner un rapport

1. **Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.**

   La page Exécuter des rapports s'ouvre.

2. **Utilisez le menu déroulant Type du rapport pour sélectionner une catégorie de rapports.**

   Il existe deux catégories de rapports :

   - Rapports d'Identity Manager,
   - Rapports de l'auditeur.

     Le tableau des rapports indique les rapports existants dans la catégorie sélectionnée.

3. **Cliquez sur le nom d'un rapport pour l'éditer.**

4. **Pour éditer un rapport, ajustez les paramètres comme requis et cliquez sur Enregistrer.**

   Pour cloner un rapport, entrez un nouveau nom de rapport. Ajustez les paramètres du rapport comme requis et cliquez sur Enregistrer pour l'enregistrer sous ce nouveau nom.

Envoi des rapports par e-mail

Lors de la création ou de la modification d'un rapport, vous pouvez sélectionner une option afin d'envoyer par e-mail les résultats de ce rapport à un ou plusieurs destinataires. Lorsque vous sélectionnez cette option, la page est actualisée et vous êtes invité à indiquer les destinataires de l'e-mail. Indiquez un ou plusieurs destinataires, en séparant leurs adresses par une virgule.

Vous pouvez aussi choisir l'un des formats suivants pour que le rapport soit joint à l'e-mail :

- **Joindre le rapport au format CSV**. Joint les résultats du rapport au format CSV (Comma-Separated Value, valeurs séparées par des virgules).
- **Joindre le rapport au format PDF**. Joint les résultats du rapport au format PDF (Portable Document Format).

Programmation des rapports

Vous pouvez exécuter un rapport immédiatement ou le programmer pour qu'il s'exécute à intervalles réguliers en choisissant l'une des sélections suivantes :

- Sélectionnez **Rapports → Exécuter des rapports** pour exécuter immédiatement les rapports enregistrés. Pour la liste des rapports, cliquez sur Exécuter. Identity Manager exécute le rapport puis en affiche les résultats dans les formats récapitulatif et détaillé.
- Sélectionnez **Tâches du serveur → Gérer la planification** pour programmer l'exécution des tâches de rapport. Une fois une tâche de rapport sélectionnée, vous pouvez en définir la fréquence et les options. Vous pouvez aussi ajuster des détails spécifiques au rapport (comme dans la page Définir un rapport de la zone Rapports).

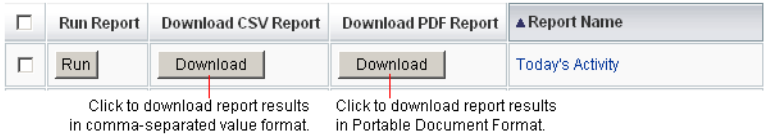
  Pour que la TaskDefinition d'un rapport figure dans la liste, vous devez définir l'attribut `visibility` sur `schedule` dans l'objet TaskDefinition.

Téléchargement des données des rapports

La page Exécuter des rapports permet de télécharger les informations des rapports pour les utiliser dans une autre application telle qu'Acrobat Reader ou StarOffice.

Ouvrez la page Exécuter des rapports et cliquez sur Télécharger dans l'une des colonnes suivantes :

- **Télécharger le rapport CSV**. Télécharge la sortie du rapport au format CSV. Une fois la sortie enregistrée, vous pouvez l'ouvrir et travailler avec le rapport dans une autre application telle que StarOffice.
- **Télécharger le rapport PDF**. Télécharge la sortie du rapport au format PDF qui peut être affiché avec Adobe Reader.



Configuration de la sortie des rapports

Pour configurer la sortie des rapports, cliquez sur Rapports puis sélectionnez Configurer les rapports.

Ces sélections sont disponibles sur la page Configurer les rapports :

- **Options des rapports PDF**

  Concernant les rapports générés au format PDF, vous pouvez effectuer des sélections pour déterminer les polices à utiliser dans le rapport, la taille des pages et leur orientation.

  - **Nom de la police PDF**. Sélectionnez la police à utiliser pour générer les rapports PDF. Par défaut, seules les polices disponibles pour tous les afficheurs de PDF sont indiquées. Cependant, des polices supplémentaires (telles que celles nécessaires pour prendre en charge les langues asiatiques) peuvent être ajoutées au système en copiant les fichiers de définition de polices dans le répertoire `fonts/` du produit et en redémarrant le serveur.

    Les formats de définition de police acceptés sont les suivants : `.ttf`, `.ttc`, `.otf` et `.afm`. Si vous sélectionnez une de ces polices, elle doit aussi être disponible sur le système informatique sur lequel le rapport est affiché. Sinon, sélectionnez l'option Polices incorporées dans les documents PDF.
  - **Polices incorporées dans les documents PDF**. Sélectionnez cette option pour incorporer la définition de la police dans le rapport PDF généré. Le rapport pourra ainsi être affiché dans n'importe quel afficheur PDF.

    Remarque – L'incorporation de la police peut considérablement augmenter la taille du document.

  - **Format de page**. Choisissez le format des pages PDF en sélectionnant lettre (8 ½ par 11 po) ou légal (8 ½ par 14 po) dans le menu (la valeur par défaut est *lettre*).

    Remarque – Vous pouvez ajouter d'autres tailles à ce menu en utilisant le champ pdfPageSize du formulaire Reports Config Library. La valeur pdfPageSize doit être une valeur connue à la classe `com.lowagie.text.Rectangle` dans le package `itext`.

  - **Orientation**. Choisissez l'orientation des pages PDF en sélectionnant portrait ou paysage dans le menu (la valeur par défaut est *portrait*).

- **Options du rapport CSV**. Sélectionnez l'option Nom du jeu de caractères pour spécifier un jeu de caractères à utiliser pour lors de la génération des rapports CSV. Toutes les applications qui importent les fichiers CSV ne prennent pas toutes en charge le codage UTF-8 par défaut. Sélectionnez un autre jeu de caractères si besoin est.
- **Configuration des événements suivis**. Sélectionnez l'option Activer la récupération des événements pour configurer des rapports pour le contrôle du système mais ne l'appliquez pas à la personnalisation du formatage des rapports (pour plus d'informations, voir "Configuration des événements suivis" à la page 298).

Cliquez sur Enregistrer pour enregistrer les options de configuration des rapports.

Rapports d'Identity Manager

Les types de rapports d'Identity Manager peuvent être regroupés dans les catégories suivantes :

Rapports AuditLog

Les rapports AuditLog sont basés sur les événements capturés dans le journal d'audit du système. Ces rapports fournissent des informations sur, entre autres, les comptes générés, les demandes approuvées, les tentatives d'accès ayant échoué, les changements et les réinitialisations de mot de passe, les activités d'auto-provisioning, les violations de stratégie et les utilisateurs de Service Provider (extranet).

Remarque – Avant d'exécuter les journaux d'audit, vous devez spécifier les types d'événements Identity Manager à capturer. Pour cela, sélectionnez Configurer dans la barre de menu puis sélectionnez Vérification informatique. Sélectionnez le ou les noms de un ou plusieurs groupes d'audit pour en enregistrer les événements (réussites et échecs). Pour plus d'informations sur la configuration de groupes de configuration d'audit, voir "Configuration de groupes et d'événements d'audit" à la page 111.

▼ Pour définir un rapport AuditLog

1 **Suivez les instructions de création d'un rapport dans "Création de rapports" à la page 276.**

Sélectionnez Rapports d'Identity Manager dans le premier menu Type du rapport et sélectionnez Rapport de liste de contrôle dans le second menu.

La page Définir un rapport s'ouvre.

2 **Remplissez le formulaire et cliquez sur Enregistrer.**

Cliquez sur Aide si vous avez besoin d'aide avec le formulaire.

Une fois que vous avez défini et enregistré les paramètres du rapport, exécutez ce dernier depuis la page Exécuter des rapports. Cliquez sur Exécuter pour produire un rapport de tous les résultats qui correspondent aux critères enregistrés. Le rapport inclura la date à laquelle un événement s'est produit, l'action effectuée et le résultat de celle-là.

Rapports AuditLog d'utilisateurs individuels

À l'instar des rapports AuditLog, le AuditLog utilisateur individuel est basé sur des événements capturés dans le journal d'audit du système. Toutefois, ce rapport vous invite à sélectionner l'utilisateur objet du rapport et retourne une liste de toutes les opérations effectuées sur cet utilisateur. Pour maximiser les résultats, ce rapport recherche dans les deux champs `AccountId` et `ObjectDesc` du journal d'audit le nom d'utilisateur correspondant.

Ce rapport peut retourner un ensemble fixe de colonnes ou un ensemble personnalisé que vous aurez sélectionné. Les colonnes sont définies dans `reporttasks.xml` et `defaultreports.xml`. Ces deux fichiers figurent dans le répertoire `sample` (situé sous le répertoire d'installation d'Identity Manager).

▼ Pour définir un rapport AuditLog utilisateur individuel

1 **Suivez les instructions de création d'un rapport dans "Création de rapports" à la page 276.**

Sélectionnez Rapports d'Identity Manager dans le premier menu Type du rapport et sélectionnez Rapport AuditLog utilisateur individuel dans le second menu.

La page Définir un rapport s'ouvre.

2 **Remplissez le formulaire et cliquez sur Enregistrer.**

Cliquez sur Aide si vous avez besoin d'aide avec le formulaire.

Rapports en temps réel

Les rapports en temps réel interrogent directement les ressources pour rapporter des informations en temps réel.

Les rapports en temps réel sont les suivants :

- **Rapport de groupe de ressources**. Résume les attributs du groupe, utilisateurs membres compris.
- **Rapport sur les statuts des ressources**. Teste l'état de la connexion d'une ou plusieurs ressources spécifiées en exécutant la méthode `testConnection` sur chaque ressource.
- **Rapport d'utilisateur de ressources**. Liste les comptes de ressources d'un utilisateur et ses attributs de compte.

▼ Pour définir un rapport en temps réel

1 **Suivez les instructions de création d'un rapport dans "Création de rapports" à la page 276.**

Sélectionnez Rapports d'Identity Manager dans le premier menu Type du rapport et sélectionnez Rapport de groupe de ressources, Rapport sur les statuts des ressources ou Rapport d'utilisateur de ressources dans le second menu.

La page Définir un rapport s'ouvre.

2 **Remplissez le formulaire et cliquez sur Enregistrer.**

Cliquez sur Aide si vous avez besoin d'aide avec le formulaire.

Une fois que vous avez défini et enregistré les paramètres du rapport, exécutez ce dernier depuis la page de liste Exécuter des rapports. Cliquez sur Exécuter pour produire un rapport de tous les résultats qui correspondent aux critères enregistrés.

Rapports récapitulatifs

Les types de rapports récapitulatifs comprennent les rapports suivants disponibles dans la liste Rapports d'Identity Manager :

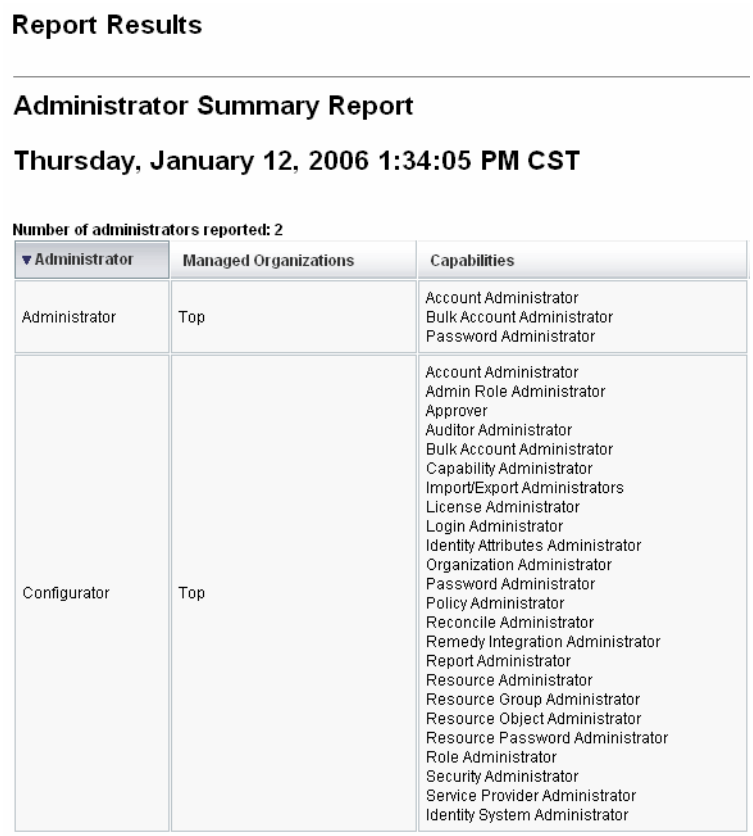
- **Rapport d'index de comptes**. Rapport sur des comptes de ressources sélectionnés en fonction de la situation de réconciliation.
- **Rapport d'administrateur**. Affiche les administrateurs Identity Manager, les organisations qu'ils gèrent et les capacités qui leur sont assignées. Quand vous définissez un rapport d'administrateur, vous pouvez sélectionner les administrateurs à inclure par organisation.
- **Rapport sur les rôles admin**. Répertorie les utilisateurs assignés à des rôles admin.
- **Rapport de rôle**. Rapport sur tous les aspects des rôles et des ressources associées.

- **Rapport de tâches**. Rapport sur les tâches en attente et terminées. Vous déterminez le détail des informations à inclure en effectuant des sélections dans une liste d'attributs (approbateur, description, date d'expiration, propriétaire, date de début et état).
- **Rapport d'utilisateur**. Affiche les utilisateurs, les rôles auxquels ils sont assignés et les ressources auxquelles ils peuvent accéder. Lorsque vous définissez un rapport utilisateur, vous pouvez sélectionner les utilisateurs à inclure par nom, responsable assigné, rôle, organisation ou assignation de ressources.
- **Rapport des questions utilisateur**. Permet aux administrateurs de rechercher les utilisateurs n'ayant pas répondu au nombre minimum de questions d'authentification, comme spécifié dans leurs conditions de stratégie de compte. Les résultats indiquent le nom de l'utilisateur, la stratégie de compte, l'interface associée à la stratégie et le nombre minimum de questions nécessitant des réponses.

Remarque – Par défaut, les rapports suivants sont automatiquement étendus à l'ensemble des organisations contrôlées par l'administrateur connecté, à moins que ce comportement ne soit explicitement réduit à une ou plusieurs organisations sélectionnées pour lesquelles le rapport doit être exécuté :

- les rapports récapitulatifs du rôle admin,
- les rapports récapitulatifs administrateur,
- les rapports récapitulatifs des rôles,
- les rapports récapitulatifs des questions utilisateur,
- les rapports récapitulatifs des utilisateurs.

Comme indiqué dans la figure suivante, le Rapport d'administrateur liste les administrateurs Identity Manager, les organisations que ceux-ci gèrent et les capacités et rôles qui leur sont assignés.



Report Results

Administrator Summary Report

Thursday, January 12, 2006 1:34:05 PM CST

Number of administrators reported: 2

▼Administrator	Managed Organizations	Capabilities
Administrator	Top	Account Administrator Bulk Account Administrator Password Administrator
Configurator	Top	Account Administrator Admin Role Administrator Approver Auditor Administrator Bulk Account Administrator Capability Administrator Import/Export Administrators License Administrator Login Administrator Identity Attributes Administrator Organization Administrator Password Administrator Policy Administrator Reconcile Administrator Remedy Integration Administrator Report Administrator Resource Administrator Resource Group Administrator Resource Object Administrator Resource Password Administrator Role Administrator Security Administrator Service Provider Administrator Identity System Administrator

▼ Pour définir un rapport récapitulatif

1. **Suivez les instructions de création d'un rapport dans "Création de rapports" à la page 276.**

   Sélectionnez un des types de rapports récapitulatifs (listés ci-dessus) dans le second menu.

   La page Définir un rapport s'ouvre.

2. **Remplissez le formulaire et cliquez sur Enregistrer.**

   Cliquez sur Aide si vous avez besoin d'aide avec le formulaire.

Rapports SystemLog

Un rapport SystemLog indique les messages et erreurs système qui sont enregistrés dans le référentiel.

Lorsque vous configurez ce rapport, vous pouvez spécifier si inclure ou exclure les éléments suivants :

- les composants du système (tels que l'approvisionneur, l'ordonnanceur ou le serveur) ;
- les codes d'erreur ;
- les niveaux de sécurité (erreur, erreur fatale ou avertissement).

Vous définissez également le nombre maximal d'enregistrements à afficher (par défaut, 3000) et si vous voulez les enregistrements les plus anciens ou les plus récents si le nombre des enregistrements disponibles dépasse le maximum spécifié.

Lorsque vous exécutez un rapport SystemLog, des entrées Syslog spécifiques peuvent être récupérées en spécifiant l'ID de syslog de l'entrée cible. Par exemple, pour afficher des entrées spécifiques dans le rapport Recent Systems Messages (Messages système récents), éditez le rapport et sélectionnez le champ Événement. Entrez ensuite l'ID de syslog requis et cliquez sur Exécuter.

Remarque – Vous pouvez aussi exécuter la commande `lh syslog` pour extraire des enregistrements du journal système. Pour le détail des options de commande, lisez "Commande `syslog`" à la page 576 dans l'Annexe A, "Références `lh`".

▼ Pour définir un rapport SystemLog

1 **Suivez les instructions de création d'un rapport dans "Création de rapports" à la page 276.**

Sélectionnez Rapports d'Identity Manager dans le premier menu Type du rapport et sélectionnez Rapport SystemLog dans le second menu.

La page Définir un rapport s'ouvre.

2 **Remplissez le formulaire et cliquez sur Enregistrer.**

Cliquez sur Aide si vous avez besoin d'aide avec le formulaire.

Une fois que vous avez défini et enregistré les paramètres du rapport, exécutez ce dernier depuis la page de liste Exécuter des rapports.

Rapports d'utilisation

Créez et exécutez des rapports pour afficher des récapitulatifs graphiques et/ou en tableaux des événements système liés aux objets Identity Manager tels que les administrateurs, les utilisateurs, les rôles ou les ressources. Vous pouvez afficher les données des rapports d'utilisation sous forme de tableaux, graphiques à barres, circulaire ou linéaires.

▼ Pour définir un rapport d'utilisation

1 **Suivez les instructions de création d'un rapport dans "Création de rapports" à la page 276.**

2 **Sélectionnez Rapports d'Identity Manager dans le premier menu Type du rapport et sélectionnez Rapport d'utilisation dans le second menu.**

La page Définir un rapport s'ouvre.

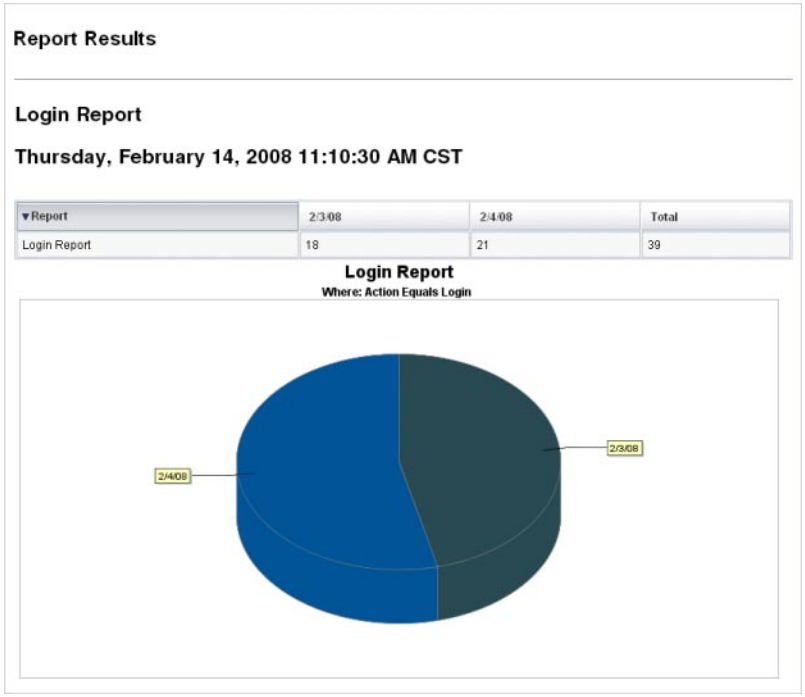
3 **Remplissez le formulaire et cliquez sur Enregistrer.**

Cliquez sur Aide si vous avez besoin d'aide avec le formulaire.

Une fois que vous avez défini et enregistré les paramètres du rapport, exécutez ce dernier depuis la page de liste Exécuter des rapports.

Exemple 8–1 Graphique d'un rapport d'utilisation (comptes utilisateur générés)

La figure suivante représente un exemple de rapport d'utilisation. Le tableau dans le haut du rapport affiche les événements constituant le rapport tandis que le graphique dans le bas représente les mêmes informations sous forme graphique.



Rapports de flux de travaux

Ce rapport liste les flux de travaux par nom et fournit les informations suivantes :

- la durée moyenne employée par chaque flux de travaux pour se terminer ;
- le nombre de fois où chaque flux de travaux a été demandé ;
- le nombre de demandes de flux de travaux qui ont été terminées.

De plus, cliquer sur le nom d'un flux de travaux ouvre une vue détaillée de ce flux détaillant les différentes activités qui ont été instrumentées au sein de ce flux de travaux ainsi que la durée moyenne employée par ce dernier pour s'exécuter complètement.

Les rapports de flux de travaux sont particulièrement utiles pour capturer des indicateurs de performance utiles pour établir si les objectifs de l'Accord de niveau de service (SLA) ont été atteints.

Identity Manager doit être configuré pour capturer les indicateurs de synchronisation de flux de travaux pour qu'il soit possible d'exécuter des rapports de flux de travaux. Pour plus d'informations, voir la section suivante.

Configuration de flux de travaux pour capturer les événements de synchronisation d'audit

Pour pouvoir exécuter des rapports de flux de travaux, vous devez d'abord activer l'audit des flux de travaux pour chacun des types de flux de travaux à inclure dans le rapport.

Remarque – L'audit des flux de travaux dégrade la performance. Par conséquent, vous devez uniquement activer l'audit des flux de travaux pour les flux de travaux que vous envisagez d'utiliser avec les Rapports de flux de travaux.

Activez l'audit des flux de travaux comme suit :

- Pour les flux de travaux que vous pouvez configurer dans l'interface administrateur en utilisant les modèles de tâches, sélectionnez la case à cocher Contrôler l'intégralité du flux de travaux sur l'onglet Vérification informatique du formulaire de configuration du modèle de tâche. Pour les instructions, voir "Configuration de l'onglet Vérification informatique " à la page 330.
- Pour les flux de travaux qui n'ont pas de modèle de tâches, voir "Modification des flux de travaux pour consigner les événements de synchronisation standard" à la page 345.

Spécification des attributs à stocker pour le rapport de flux de travaux

S'il n'est pas nécessaire de définir des attributs, il est important pour tirer au maximum parti des rapports de flux de travaux de stocker les attributs en fonction desquels vous envisagez de filtrer vos rapports par la suite.

Pour définir le jeu d'attributs à stocker pour chaque type de flux de travaux, utilisez le formulaire de configuration de modèle de tâches à onglets de l'interface administrateur. L'onglet Vérification informatique contient une section Attributs d'audit, qui se trouve sous la case à cocher Contrôler l'intégralité du flux de travaux. Pour les instructions, voir "Configuration de l'onglet Vérification informatique " à la page 330.

▼ Pour définir un rapport de flux de travaux

1 **Suivez les instructions de création d'un rapport dans "Création de rapports" à la page 276.**

Sélectionnez Rapports d'Identity Manager dans le premier menu Type du rapport et sélectionnez Rapport d'utilisation dans le second menu.

La page Définir un rapport s'ouvre.

2 **Remplissez le formulaire et cliquez sur Enregistrer. Vous pouvez définir les paramètres temporels ainsi qu'ajouter les attributs de votre choix pour les contrôler (voir "Spécification des attributs à stocker pour le rapport de flux de travaux" à la page 288 dans la section précédente).**

Pour affiner les résultats, spécifiez un nom d'attribut (par exemple, `user.global.state`), sélectionnez une condition puis entrez une valeur pour l'attribut. Vous pouvez entrer tous les attributs dont vous avez besoin.

Cliquez sur Aide si vous avez besoin d'aide avec le formulaire.

Une fois que vous avez défini et enregistré les paramètres du rapport, exécutez ce dernier depuis la page Exécuter des rapports. Cliquez sur Exécuter pour produire un rapport de tous les résultats qui correspondent aux critères enregistrés.

Le rapport retournera les flux de travaux par nom et précisera le temps moyen employé par un flux de travaux pour se terminer, le nombre de fois où un flux de travaux a été demandé et le nombre de ces demandes qui ont été complétées.

Cliquez sur le nom d'un flux de travaux pour ouvrir une vue détaillée de ce flux détaillant les différentes activités qui ont été instrumentées dans ce flux. Les processus pouvant avoir les mêmes activités nommées, les activités sont regroupées par processus.

Rapports de l'auditeur

Les rapports de l'auditeur fournissent des informations qui vous aideront à gérer la compatibilité des utilisateurs sur la base des critères définis dans les stratégies d'audit.

Identity Manager fournit les rapports d'auditeur suivants :

- rapports de couverture des examens d'accès,
- rapports détaillés de l'examen des accès,
- rapports récapitulatifs de l'examen des accès,
- rapports de couverture de l'étendue des utilisateurs du scannage d'accès,
- rapports récapitulatifs des stratégies d'audit,
- rapports des attributs audités,
- historique des violations de stratégie d'audit,
- rapports d'accès utilisateur,
- historique des violations par organisation,
- historique des violations par ressource,
- rapports de séparation des obligations,
- rapports récapitulatifs des violations.

Pour définir un rapport de l'auditeur, suivez les étapes de la section "Création de rapports" à la page 276.

Pour plus d'informations, voir "Travailler avec les rapports de l'auditeur" à la page 469 au Chapitre 15, "Audit : contrôler la conformité".

Travailler avec les graphes

Vous pouvez effectuer les opérations liées aux graphes suivantes :

Affichage des graphes définis

Identity Manager fournit quelques exemples de graphes. Certains utilisent des données d'exemple, d'autres non. Nous vous conseillons de créer des graphes supplémentaires applicables à votre déploiement.

Vous devez supprimer les exemples de graphes et de tableaux de bord avant de lancer la production d'un déploiement. Certains des exemples de graphes n'utilisant pas d'exemples de données peuvent apparaître vides si aucune donnée applicable n'a été collectée.

▼ Pour afficher un graphe défini

1. **Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.**
2. **Cliquez sur Graphes de tableau de bord dans le menu secondaire.**
3. **Sélectionnez une catégorie de graphes de tableau de bord dans la liste d'options Sélection du type de graphe de tableau de bord.**

   Tous les graphes de la catégorie sélectionnée s'affichent dans la liste des graphes.
4. **Cliquez sur le nom d'un graphe.**
5. **Le cas échéant, cliquez sur Interrompre l'actualisation pour interrompre le rafraîchissement du tableau de bord. Cliquez sur Reprendre pour renouveler la vue.**

   Remarque – Pour les tableaux de bord contenant de nombreux graphes, il est parfois utile d'interrompre l'actualisation jusqu'à ce que tous les graphes soient chargés initialement.
6. **Si vous le souhaitez, cliquez sur Actualiser maintenant pour forcer une régénération immédiate.**
7. **Cliquez sur Terminé pour revenir à la page de liste Graphes de tableau de bord.**

Remarque – Si l'un des graphes affiche un message d'erreur, ouvrez l'objet Configuration système pour l'éditer ("Édition des objets Configuration Identity Manager" à la page 118) et définissez `dashboard.debug=true`. Une fois cette propriété définie, retournez au graphe qui avait généré l'erreur et utilisez le lien Veuillez insérer le texte de ce script en cas de problème pour récupérer le script du graphe. Ce script de graphe doit être inclus lors de la signalisation du problème.

▼ Pour créer un graphe de tableau de bord

1. **Dans l'interface administrateur, sélectionnez Rapports → Graphes de tableau de bord.**

2. **Sélectionnez une catégorie de graphes de tableau de bord dans la liste d'options Sélection du type de graphe de tableau de bord.**

   Tous les graphes de la catégorie sélectionnée s'affichent dans la liste des graphes.

3. **Cliquez sur Nouveau pour afficher la page Créer le graphe du tableau de bord et entrez un nom pour le graphe.**

   Choisissez un nom explicite unique car les graphes sont ajoutés aux tableaux de bord en fonction de leur nom.

4. **Sélectionnez un registre : IDM ou SAMPLE.**

   Les données d'exemple fournies le sont pour vous permettre de vous familiariser avec le système. Il n'y a pas d'exemples de données pour tous les événements suivis ; la sélection proposée est surtout utile pour les démonstrations et lors de l'expérimentation des diverses options de graphes. Supprimez les données d'exemple avant de passer en environnement de production.

   Remarque – Les événements suivis utilisant des données d'exemple diffèrent des événements réellement suivis.

5. **Sélectionnez un type d'événement suivi dans la liste.**

   Un événement est une caractéristique système, par exemple l'utilisation de la mémoire ou une agrégation d'événements tels que des opérations sur les ressources, dont les valeurs historiques sont suivies et peuvent être affichées sous forme de graphes ou de diagrammes.

   Les événements suivis sélectionnables dans le registre IDM sont les suivants :

   - **Nombre d'exécutions de Provisioner**. Suit le nombre d'opérations d'approvisionneur réalisées (par type d'opérations).
   - **Durée de l'exécution de Provisioner**. Indique la durée de chaque opération d'approvisionneur (par type).

- **Nombre d'opérations portant sur les ressources**. Suit le nombre des opérations portant sur les ressources.
- **Durée de l'opération sur les ressources**. Suit la durée d'une opération portant sur les ressources.
- **Durée du flux de travaux**. Indique le temps employé pour exécuter un flux de travaux.
- **Nombre d'exécution du flux de travaux**. Suit le nombre de fois où un flux de travaux donné est exécuté.

6 Sélectionnez une Échelle de temps dans la liste.

Cette option détermine la fréquence à laquelle les données sont regroupées (par exemple, toutes les heures) et la durée de conservation de ces données (par exemple, un mois). Le système stocke les données des événement suivis durant des échelles de temps de plus en plus grandes pour offrir une vue actuelle détaillée du système et permettre de comprendre les tendances historiques.

7 Sélectionnez une mesure dans la liste.

Une mesure (nombre ou moyenne) sera sélectionnée par défaut, selon l'événement suivi sélectionné. Chaque graphe affiche une unique mesure. Les mesures disponibles dépendent de l'événement suivi sélectionné.

Les mesures possibles sont les suivantes :

- **Nombre**. Nombre total de fois où l'événement s'est produit dans l'intervalle de temps considéré.
- **Moyen**. Moyenne arithmétique des valeurs d'événements dans l'intervalle de temps considéré.
- **Maximum**. Valeur maximale de l'événement dans l'intervalle de temps considéré.
- **Minimum**. Valeur minimale de l'événement dans l'intervalle de temps considéré.
- **Histogramme**. Nombres séparés pour des plages discrètes de valeurs d'événement pour l'intervalle de temps considéré.

8 Sélectionnez Afficher le nombre comme dans la liste.

Le nombre figurant sur le graphe est affiché sous forme de total brut ou mis à l'échelle selon diverses échelles de temps.

9 Sélectionnez un Type de graphe dans la liste.

Cet élément détermine l'affichage des données de l'événement suivi. Les types de graphe disponibles dépendent de l'événement suivi sélectionné et peuvent comprendre des graphes en courbes, des graphes à barres et des graphes à secteurs.

10 Spécifiez une Dimension de base (*facultatif*).

Effectuez un choix dans la liste suivante :

- **Nom de la ressource**. Si cette option est sélectionnée, toutes les valeurs de la ou des dimensions sont incluses dans le graphe. Désélectionnez cette option pour choisir des valeurs individuelles de la dimension à inclure dans le graphe.
- **Instance du serveur**. Si cette option est sélectionnée, toutes les valeurs de la dimension sont incluses dans le graphe. Désélectionnez cette option pour choisir des valeurs individuelles de la dimension à inclure dans le graphe.
- **Type de l'opération**. Si cette option est sélectionnée, toutes les valeurs de la dimension sont incluses dans le graphe. Désélectionnez cette option pour choisir des valeurs individuelles de la dimension à inclure dans le graphe.

  Une fois la dimension sélectionnée, la page est actualisée pour afficher un graphe.

11 Entrez le texte dans le champ Options du graphe pour insérer un sous-titre sous le titre principal du graphe (*facultatif*).

12 Sélectionnez Options de graphe avancées (*optionnel*).

Utilisez cette option si vous voulez spécifier les éléments suivants :

- **Lignes de la grille**,
- **Police**,
- **Palette de couleurs**.

13 Cliquez sur Enregistrer pour créer le graphe.

▼ Pour éditer un graphe de tableau de bord

1 Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.

2 Cliquez sur Graphes de tableau de bord dans le menu secondaire.

La page Graphes de tableau de bord s'ouvre.

3 Sélectionnez une catégorie dans le menu déroulant Sélection du type de graphe de tableau de bord.

Un tableau listant les graphes de tableau de bord s'ouvre.

4 Cliquez sur le nom d'un graphe pour l'éditer.

Les attributs du graphe que vous pouvez éditer varient selon le graphe sélectionné.

Une ou plusieurs des caractéristiques suivantes peuvent être éditées :

- **Nom du graphe**. Les graphes sont ajoutés à un tableau de bord par nom.
- **Registre**. Spécifie la *Description de l'événement suivi* définie dans le registre. La sélection courante est la suivante : SAMPLE, Service Provider et IDM.
- **Événement suivi**. Caractéristique système, telle que l'utilisation de la mémoire, ou une agrégation d'événements, tels que des opérations sur les ressources, dont les valeurs historiques sont suivies et peuvent être visualisées sous forme de graphes ou de diagrammes.
- **Échelle de temps**. Contrôle la fréquence à laquelle les données sont regroupées et la durée de conservation de ces données.
- **Mesure**. Chaque graphe affiche une unique mesure. Les mesures disponibles dépendent de l'événement suivi sélectionné. Selon la mesure sélectionnée, d'autres options pourront être disponibles.
- **Type du graphe**. Contrôle la façon dont les données de l'événement suivi sont affichées (par exemple sous forme de graphe linéaire ou de diagramme à barres).
- **Valeurs des dimensions incluses**. Si cette option est activée, toutes les valeurs de la ou des dimensions sont incluses dans le graphe.
- **Sous-titre du graphe**. Si vous le souhaitez, saisissez un sous-titre sous le titre principal du graphe.
- **Options de graphe avancées**. Sélectionnez cette option si vous voulez définir les éléments suivants :
  - **Lignes de la grille**,
  - **Police**,
  - **Palette de couleurs**.

5 Cliquez sur Enregistrer.

▼ Pour supprimer un graphe défini

1 Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.

2 Cliquez sur Graphes de tableau de bord dans le menu secondaire.

3 Sélectionnez une catégorie de graphes de tableau de bord dans la liste d'options Sélection du type de graphe de tableau de bord.

Tous les graphes de la catégorie sélectionnée s'affichent dans la liste des graphes.

4 Utilisez les cases à cocher pour sélectionner les graphes à supprimer puis cliquez sur Supprimer.

Remarque – Les graphes sont supprimés sans avertissement de tous les tableaux de bord qui les contenaient.

Travailler avec les tableaux de bord

Un tableau de bord est un ensemble de graphes connexes qui sont affichés sur une même page. Comme avec les graphes, Identity Manager fournit un ensemble d'exemples de tableaux de bord que les administrateurs sont encouragés à personnaliser en fonction de leur déploiement. Pour les instructions, voir "Pour créer des tableaux de bord" à la page 295.

▼ Pour afficher les tableaux de bord

1 **Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.**

2 **Cliquez sur Afficher les tableaux de bord dans le menu secondaire pour afficher les tableaux de bord actuellement définis.**

La page Tableaux de bord s'ouvre.

3 **Sélectionnez Afficher en regard du tableau de bord à afficher.**

Remarque – Pour les tableaux de bord contenant de nombreux graphes, il est parfois utile d'interrompre l'actualisation jusqu'à ce que tous les graphes soient chargés initialement.

Si vous le souhaitez, cliquez sur Interrompre pour interrompre l'actualisation du tableau de bord ou sur Actualiser pour renouveler l'affichage.

Les sections suivantes contiennent des procédures permettant de travailler avec les tableaux de bord.

- "Pour créer des tableaux de bord" à la page 295 ;
- "Édition des tableaux de bord" à la page 296 ;
- "Suppression des tableaux de bord" à la page 297.

▼ Pour créer des tableaux de bord

1 **Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.**

2 **Cliquez sur Afficher les tableaux de bord dans le menu secondaire.**

3 **Cliquez sur Nouveau.**

4 **Saisissez le nom du nouveau tableau de bord.**

5 **Saisissez un résumé décrivant le nouveau tableau de bord.**

6 **Sélectionnez une fréquence d'actualisation en secondes, minutes ou heures, dans la liste.**

Remarque – Définir une fréquence d'actualisation inférieure à 30 secondes peut causer des problèmes avec les tableaux de bord contenant plusieurs graphes.

---

7 **Pour associer un style de graphe au tableau de bord, sélectionnez l'entrée appropriée dans la liste.**

Remarque – Un même graphe peut être utilisé dans plusieurs tableaux de bord.

---

8 **Pour supprimer un graphe de tableau de bord, sélectionnez l'entrée appropriée dans la liste et cliquez sur Supprimer le(s) graphe(s).**

9 **Cliquez sur Enregistrer.**

Édition des tableaux de bord

Pour éditer un tableau de bord, utilisez la procédure décrite dans "Pour créer des tableaux de bord" à la page 295 mais au lieu de sélectionner Nouveau, sélectionnez le tableau de bord que vous voulez modifier et éditez les attributs suivants :

- le nom du tableau de bord ;
- le résumé décrivant le nouveau tableau de bord ;
- la fréquence d'actualisation en secondes, minutes ou heures, à sélectionner dans la liste.
- ajoutez ou supprimez les graphes associés à un tableau de bord.

Remarque – Supprimer un graphe d'un tableau de bord ne supprime pas ce graphe. Le graphe continue à être utilisable dans d'autres tableaux de bord.

Un même graphe peut être utilisé dans plusieurs tableaux de bord.

La Figure 8–2 illustre un exemple de la page d'édition d'un tableau de bord.

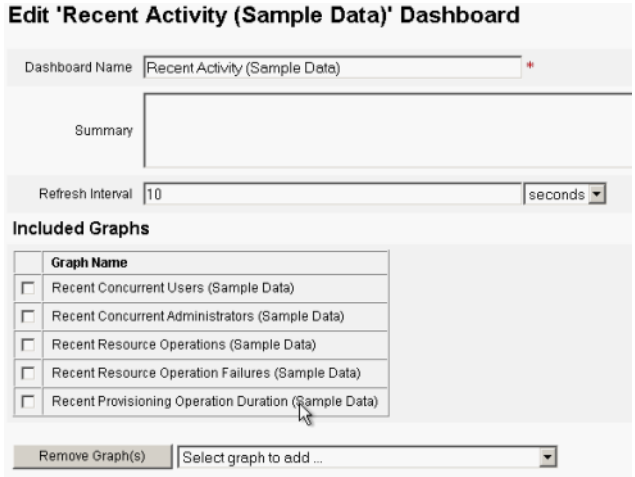


FIGURE 8–2 Édition des tableaux de bord

Suppression des tableaux de bord

Pour supprimer les tableaux de bord de Service Provider, cliquez dans la zone Service Provider sur Gestion du tableau de bord, puis sélectionnez le tableau de bord de votre choix et cliquez sur supprimer.

Remarque – Les graphes inclus dans le tableau de bord ne sont pas supprimés en utilisant cette procédure. Supprimez-les en utilisant la page Gérer les graphes des tableaux de bord (voir "Pour supprimer un graphe défini" à la page 294).

Contrôle du système

Vous pouvez paramétrer Identity Manager pour suivre les événements en temps réel et contrôler les événements en les affichant dans des graphes de tableau de bord. Les tableaux de bord permettent d'évaluer rapidement les ressources du système et de déceler les anomalies, de comprendre les tendances de performance historiques (en fonction de l'heure du jour, du jour de la semaine, etc.) et d'isoler de manière interactive les problèmes avant d'examiner les journaux d'audit. Ils ne fournissent pas autant de détails que ces derniers mais donnent des indices sur où rechercher les problèmes dans les journaux.

Vous pouvez créer des représentations graphiques des tableaux de bord pour suivre les activités automatiques et manuelles à un haut niveau. Identity Manager fournit des exemples de graphes de tableau de bord relatifs aux *opérations portant sur les ressources*. Les graphes de tableau de bord relatifs aux *opérations portant sur les ressources* permettent de contrôler rapidement les ressources du système pour maintenir un niveau de service acceptable.

Vous pouvez afficher les données d'exemple pour ces graphes dans le tableau Opérations sur les ressources. Pour plus d'informations sur l'utilisation des tableaux de bord, voir "Travailler avec les tableaux de bord" à la page 295.

Les statistiques sont recueillies et regroupées à divers niveaux pour présenter une vue en temps réel basée sur vos spécifications.

Configuration des événements suivis

La zone Configuration des événements suivis de la page Configurer les rapports permet de déterminer si la collecte de statistiques pour les événements suivis est actuellement activée et de l'activer. Cliquez sur Activer la récupération des événements pour activer la configuration des événements suivis.

Spécifiez les options suivantes pour la collecte des événements.

- **Fuseau horaire**. Cette option définit le fuseau horaire à utiliser pour enregistrer les événements suivis. Celui-ci détermine principalement les limites du jour.

  Vous pouvez aussi définir le fuseau horaire sur le fuseau horaire par défaut défini sur le serveur.
- **Périodes de récupération**. Cette option spécifie les intervalles de temps pour lesquels les données sont regroupées (en d'autres termes, la fréquence à laquelle elles sont collectées et la durée pendant laquelle elles sont conservées). Par exemple, si un intervalle de une minute est sélectionné, les données sont collectées toutes les minutes et conservées pendant une minute.

Le système stocke les données des événement suivis durant des périodes de plus en plus longues pour permettre une vue actuelle détaillée du système et faciliter la compréhension des tendances historiques.

Les périodes de temps suivantes sont disponibles et tous ces intervalles sont sélectionnés par défaut. Effacez les sélections correspondant aux intervalles que vous ne voulez pas inclure dans la collecte :

- intervalles de 10 secondes,
- intervalles de 1 minute,
- intervalles de 1 heure,
- intervalles de 1 jour,
- intervalles de 1 semaine,
- intervalles de 1 mois.

Une fois les événements suivis configurés, utilisez les tableaux de bord pour les contrôler. S'ils sont disponibles, utilisez les curseurs pour effectuer un zoom avant sur une section du graphe.

Analyse de risque

Les fonctionnalités d'analyse de risque d'Identity Manager permettent de générer des rapports sur des comptes utilisateur dont les profils ne rentrent pas dans certaines limites de sécurité. Les rapports d'analyse de risque balaient la ressource physique pour collecter des données et affichent, par ressource, les détails relatifs aux comptes désactivés, aux comptes verrouillés et aux comptes sans propriétaire. Ils fournissent également des détails sur les mots de passe expirés. Les détails des rapports varient en fonction du type de ressource.

Remarque – Des rapports standard sont disponibles pour les ressources AIX, HP, Solaris, NetWare NDS et Windows Active Directory.

Les pages d'analyse de risque sont contrôlées par un formulaire et peuvent être configurées pour votre environnement. Vous trouverez sous l'objet RiskReportTask sur la page `idm\debug` ("Page de débogage d'Identity Manager" à la page 45) une liste de formulaires que vous pourrez modifier en utilisant Identity Manager IDE. Pour plus d'informations sur la configuration des formulaires, voir le Chapitre 2, "Identity Manager Forms" du *Sun Identity Manager Deployment Reference*.

▼ Pour créer un rapport d'analyse de risque

1. **Dans l'interface administrateur, cliquez sur Rapports dans le menu principal.**
2. **Cliquez sur Exécuter des analyses des risques dans le menu secondaire.**
3. **Utilisez le menu déroulant Nouveau pour sélectionner un rapport à créer.**

   Une page Paramètres du rapport d'analyse de risque s'ouvre.
4. **Remplissez le formulaire.**

   Vous pouvez limiter le rapport au scannage des ressources sélectionnées et, selon le type des ressources, vous pouvez rechercher les comptes qui remplissent les critères suivants :

   - les comptes désactivés, expirés, inactifs ou verrouillés ;
   - les comptes qui n'ont jamais été utilisés ;
   - les comptes sans nom complet ou mot de passe ;
   - les comptes ne requerrant pas de mot de passe ;
   - les comptes dont les mots de passe ont expiré ou n'ont pas été modifiés pendant un nombre spécifié de jours.
5. **Cliquez sur Enregistrer.**

▼ Pour programmer un rapport d'analyse de risque

Une fois ces rapports définis, vous pouvez suivre les étapes suivantes pour programmer les rapports d'analyse de risque pour qu'ils s'exécutent à des intervalles spécifiés.

1 **Dans l'interface administrateur, cliquez sur Tâches du serveur dans le menu principal.**

2 **Cliquez sur Gérer la planification dans le menu secondaire.**

La page Tâches programmées s'ouvre.

3 **Sélectionnez un rapport d'analyse de risque à programmer.**

La page Créer un nouveau programme de tâches Analyse de risque s'ouvre.

4 **Saisissez un nom et les informations de programmation puis, en option, ajustez d'autres sélections relatives à l'analyse de risque.**

5 **Cliquez sur Enregistrer pour enregistrer la programmation.**

◆ ◆ ◆ CHAPITRE 9

Modèles de tâches

Les modèles de tâches d'Identity Manager permettent d'utiliser l'interface Administrateur pour configurer certains comportements de flux de travaux au lieu de devoir écrire des flux de travaux personnalisés.

Ce chapitre se compose des sections suivantes :

- "Activation des modèles de tâches" à la page 301. Explique comment rendre les modèles de tâches disponibles pour votre système.
- "Configuration des modèles de tâches" à la page 306. Explique l'utilisation des modèles de tâches pour configurer le comportement des flux de travaux.

Activation des modèles de tâches

Identity Manager fournit les modèles de tâches suivants que vous pouvez configurer :

- **Créer un modèle utilisateur**. Configure les propriétés de la tâche Créer un utilisateur.
- **Delete User Template**. Configure les propriétés de la tâche Supprimer l'utilisateur.
- **Mettre à jour le modèle utilisateur**. Configure les propriétés de la tâche Mettre à jour un utilisateur.

Avant d'utiliser ces modèles de tâches, vous devez mapper les processus des modèles de tâches.

▼ Pour mapper les types de processus

1 **Dans l'interface Administrateur, sélectionnez Tâche du serveur dans le menu puis sélectionnez Configurer les tâches.**

La Figure 9–1 illustre la page Configurer les tâches.

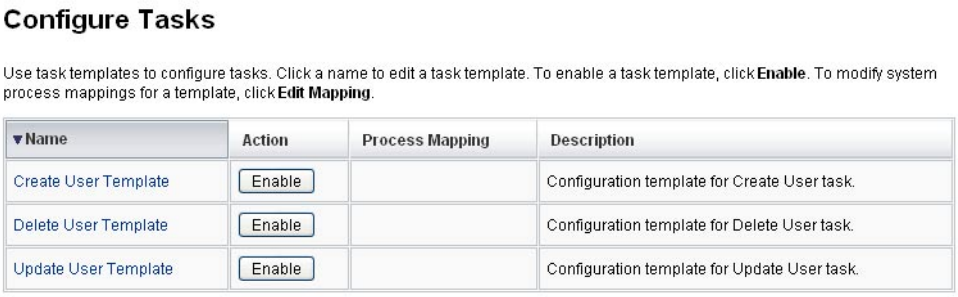


FIGURE 9–1 Page Configurer les tâches initiale

La page Configurer les tâches contient un tableau comportant les colonnes suivantes :

- **Nom**. Fournit des liens vers les modèles Créer un utilisateur, Supprimer un utilisateur et Mettre à jour un utilisateur.
- **Action**. Contient l'un des boutons suivants :
  - **Activer**. S'affiche si vous n'avez pas encore activé de modèle.
  - **Modifier un mappage**. S'affiche une fois que vous avez affiché un modèle.

    La procédure permettant d'activer et d'éditer les mappages de processus est la même.
- **Mappages des processus**. Liste le type de processus mappé pour chaque modèle.
- **Description**. Fournit une brève description de chaque modèle.

2 Cliquez sur Activer pour ouvrir la page Éditer les mappages de processus pour un modèle.

Par exemple, la page suivante (Figure 9–2) s'affiche pour le modèle Créer un modèle utilisateur.

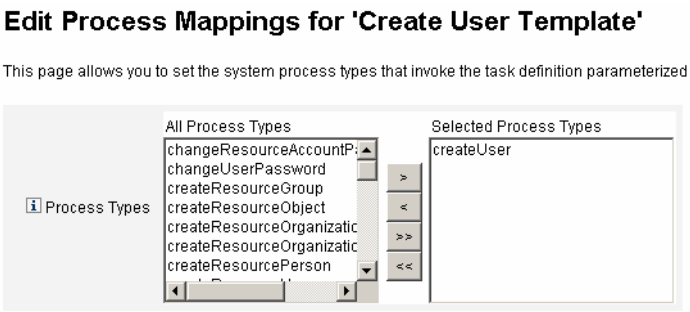
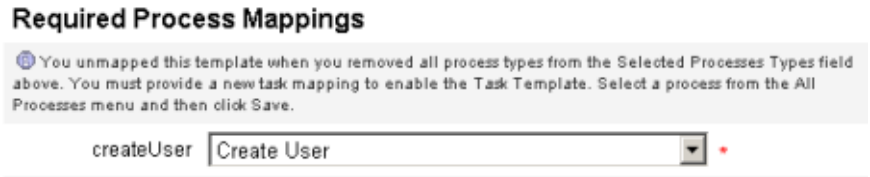


FIGURE 9–2 Page Modifier les mappages de processus

Remarque – Le type de processus par défaut (dans ce cas, `createUser`) s'affiche automatiquement dans la liste Types de processus sélectionnés. Si nécessaire, vous pouvez sélectionner un autre type de processus dans le menu.

- En règle générale, vous ne mapperez pas plus d'un type de processus par modèle.
- Si vous supprimez le type de processus de la liste Types de processus sélectionnés sans sélectionner de remplaçant, une section Mappages de processus obligatoires s'affiche vous demandant de sélectionner un nouveau mappage de tâche.



3 **Cliquez sur Enregistrer pour mapper le type de processus sélectionné et revenir à la page Configurer les tâches.**

Remarque – Lorsque la page Configurer les tâches se réaffiche, le bouton Modifier un mappage remplace le bouton Activer et le nom du processus est listé dans la colonne Mappage des processus.

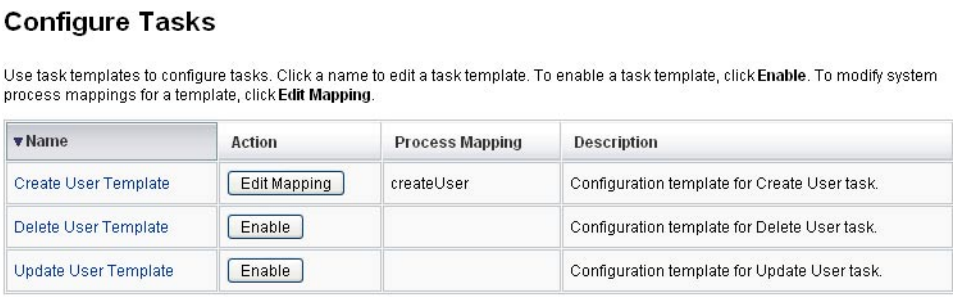


FIGURE 9–3 Tableau Configurer les tâches mis à jour

4 **Répétez le processus de mappage pour chacun des modèles restants.**

Informations supplémentaires

Vérification des mappages

- Vous pouvez vérifier les mappages en sélectionnant Configurer → Mappages des formulaires et processus. Lorsque la page Mappages des formulaires et processus s'affiche, faites défiler vers le bas le tableau Mappages des processus et vérifiez que les Types de processus suivants sont mappés vers les entrées Nom de processus mappé sur indiquées dans le tableau.

Type de processus	Nom de processus mappé sur
`createUser`	`Create User Template` (Créer un modèle utilisateur)
`deleteUser`	`Delete User Template`
`updateUser`	`Update User Template` (Mettre à jour le modèle utilisateur)

  Si les modèles ont été activés avec succès, les entrées Nom de processus mappé sur devraient toutes inclure le mot *Template* (Modèle).
- Vous pouvez aussi mapper les types de processus directement depuis la page Mappages des formulaires et processus si vous saisissez **`Template`** dans la colonne Nom de processus mappé sur comme indiqué dans le tableau.

▼ Pour configurer un modèle de tâche

Une fois les types de processus des modèles mappés ("Activation des modèles de tâches" à la page 301), vous pouvez configurer les modèles de tâches.

1 Dans l'interface administrateur, cliquez sur Tâches du serveur dans le menu principal puis sur Configurer les tâches.

La page Configurer les tâches s'ouvre.

2 Sélectionnez un lien dans la colonne Nom.

L'une des pages suivantes s'affiche :

- **Éditer le modèle de tâche 'Créer un modèle utilisateur'**. Ouvrez cette page pour éditer le modèle utilisé pour créer un nouveau compte utilisateur.
- **Éditer le modèle de tâche 'Delete User Template'**. Ouvrez cette page pour éditer le modèle utilisé pour supprimer ou suspendre un compte utilisateur.
- **Éditer le modèle de tâche 'Mettre à jour le modèle utilisateur'**. Ouvrez cette page pour éditer le modèle utilisé pour mettre à jour les informations d'un utilisateur existant.

Chaque page Éditer le modèle de tâche contient un ensemble d'onglets constituant une zone de configuration majeure pour le flux de travaux utilisateur.

Le tableau suivant détaille ces différents onglets, leur rôle et les modèles qui les utilisent.

Nom de l'onglet	Rôle	Modèle
Général (*onglet par défaut*)	Permet de définir la façon dont le nom d'une tâche s'affiche dans la barre des tâches située sur les pages Accueil et Comptes, et dans le tableau des instances de tâches sur la page Tâches.	Modèles de tâches Créer un utilisateur et Mettre à jour un utilisateur uniquement
	Permet de spécifier la façon dont les comptes utilisateur sont supprimés ou suspendus.	Modèle Delete User Template uniquement
Notification	Permet de configurer des e-mails de notification qui sont envoyés aux administrateurs et utilisateurs quand Identity Manager appelle un processus.	Tous les modèles
Approbations	Permet d'activer ou de désactiver les approbations par type, de désigner des approbateurs supplémentaires et de spécifier des attributs d'après les données de compte avant qu'Identity Manager n'exécute certaines tâches.	Tous les modèles
Vérification informatique	Permet d'activer et de configurer l'audit pour le flux de travail. Utilisez cet onglet pour configurer un flux de travaux pour capturer des informations pour les rapports de flux de travaux.	Tous les modèles
Provisioning	Permet d'exécuter une tâche en arrière-plan et d'autoriser Identity Manager à réessayer une tâche en cas d'échec de la première tentative.	Modèles de tâches Créer un utilisateur et Mettre à jour un utilisateur uniquement
Ouverture et clôture	Permet de suspendre une tâche de création jusqu'à une date/heure spécifiée (ouverture) ou de suspendre une tâche de suppression jusqu'à une date/heure spécifiée (clôture).	Modèle de tâche Créer un utilisateur
Transformations des données	Permet de configurer la façon dont les données de l'utilisateur sont transformées pendant le provisioning.	Modèles de tâches Créer un utilisateur et Mettre à jour un utilisateur uniquement

3 Sélectionnez l'un des onglets pour configurer les caractéristiques du flux de travaux pour le modèle.

Les instructions à suivre pour la configuration de ces onglets figurent dans les sections suivantes :

- "Pour mapper les types de processus" à la page 301 ;
- "Pour configurer un modèle de tâche" à la page 304.

4 **Une fois les modèles configurés, cliquez sur le bouton Enregistrer pour enregistrer vos modifications.**

Configuration des modèles de tâches

Cette section contient des informations et des instructions relatives à la configuration des modèles de tâches. Elle se compose des rubriques suivantes :

Configuration de l'onglet Général

Cette section contient les instructions à suivre pour configurer l'onglet Général, qui est disponible dans le cadre du processus de configuration des modèles de tâches. Pour les instructions relatives au démarrage du processus de configuration, voir "Configuration des modèles de tâches" à la page 306.

Remarque – Dans l'interface Administrateur, les pages permettant d'éditer les modèles de tâches de création et de mise à jour d'utilisateur sont identiques. Les instructions de configuration ne sont donc fournies que dans une section.

Pour les modèles de tâches Créer un utilisateur et Mettre à jour un utilisateur

Lorsque vous ouvrez le formulaire Éditer le modèle de tâche Créer un modèle utilisateur ou Éditer le modèle de tâche Mettre à jour le modèle utilisateur, la page de l'onglet Général s'affiche par défaut. Cette page se compose du champ de texte Nom de la tâche et d'un menu Insérer un attribut, comme indiqué à la Figure 9–4. Pour les instructions relatives au démarrage du processus de configuration, voir la section "Configuration des modèles de tâches" à la page 306.

FIGURE 9–4 L'onglet Général : Créer un modèle utilisateur

Les noms de tâches peuvent contenir des références à du texte littéral et/ou des attributs qui sont résolues pendant l'exécution de la tâche.

▼ Pour changer le nom de tâche par défaut

1 **Saisissez un nom dans le champ Nom de la tâche.**

Vous pouvez éditer ou remplacer complètement le nom de tâche par défaut.

2 **Le menu Nom de la tâche fournit la liste des attributs actuellement définis pour la vue associée à la tâche configurée par ce modèle. Sélectionnez un attribut dans le menu (*facultatif*).**

Identity Manager ajoute le nom de l'attribut à l'entrée dans le champ Nom de la tâche. Par exemple :

```
Créer un utilisateur $(accountId) $(user.global.email)
```

3 **Lorsque vous avez terminé, vous pouvez :**

- Sélectionner un autre onglet pour continuer à éditer les modèles.
- Cliquer sur Enregistrer pour enregistrer vos changements et revenir à la page Configurer les tâches.

  Le nouveau nom de tâche s'affiche dans la barre des tâches d'Identity Manager, située dans le bas des onglets Accueil et Comptes.
- Cliquez sur Annuler pour abandonner vos modifications et revenir à la page Configurer les tâches.

Pour le Delete User Template

Lorsque vous ouvrez le formulaire Éditer le modèle de tâche 'Delete User Template', la page de l'onglet Général s'affiche par défaut (pour les instructions relatives au démarrage du processus de configuration, voir "Configuration des modèles de tâches" à la page 306).

▼ Pour spécifier la façon dont les comptes utilisateur sont supprimés/suspendus

1 Utilisez lez boutons de Supprimer le compte Identity Manager pour spécifier si un compte Identity Manager peut être supprimé pendant une opération de suppression.

Ces boutons sont les suivants :

- **Jamais**. Sélectionnez ce bouton pour empêcher à jamais la suppression des comptes.
- **Uniquement s'il ne subsiste aucun compte lié à l'utilisateur après le deprovisioning**. Sélectionnez ce bouton pour autoriser les suppressions de comptes utilisateur uniquement s'il ne subsiste aucun compte de ressource lié après le deprovisioning.
- **Toujours**. Sélectionnez ce bouton pour toujours autoriser les suppressions de comptes utilisateur, même s'il subsiste des comptes de ressources assignés.

2 Utilisez les cases Deprovisioning des comptes de ressources pour contrôler le deprovisioning des comptes de ressources pour *tous* les comptes de ressources.

Remarque – L'annulation de l'assignation ou la suppression du lien d'une ressource *externe* d'un utilisateur ne génère pas de demande de provisioning ni d'élément de travail. Lorsque vous annulez l'assignation ou supprimez le lien d'une ressource externe, Identity Manager ne suspend pas ni ne supprime le compte de cette ressource, vous n'avez donc rien à faire.

Ces cases sont les suivantes :

- **Supprimer tout**. Cochez cette case pour supprimer tous les comptes représentant l'utilisateur sur toutes les ressources assignées.
- **Annuler toutes les assignations**. Cochez cette case pour annuler toutes les assignations de compte de ressources de l'utilisateur. Les comptes de ressources ne seront pas supprimés.
- **Supprimer tous les liens**. Cochez cette case pour interrompre tous les liens du système Identity Manager vers les comptes de ressources. Les utilisateurs auxquels des comptes sont assignés mais pas liés s'affichent accompagnés d'une indication stipulant qu'une mise à jour est nécessaire.

Ces options annulent les comportements du tableau Deprovisioning de comptes de ressources individuels.

3 Utilisez les cases Deprovisioning de comptes de ressources individuels pour autoriser une approche plus précise du deprovisioning des utilisateurs (par rapport à Deprovisioning des comptes de ressource).

Ces cases sont les suivantes :

- **Supprimer**. Activez cette case pour supprimer le compte qui représente l'utilisateur sur la ressource.
- **Annuler l'assignation**. Activez cette case pour que l'utilisateur ne soit plus assigné directement à la ressource. Le compte de ressource ne sera pas supprimé.
- **Annuler le lien**. Activez cette case pour interrompre le lien du système Identity Manager vers les comptes de ressources. Les utilisateurs auxquels des comptes sont assignés mais pas liés s'affichent accompagnés d'une indication stipulant qu'une mise à jour est nécessaire.

Les options **Deprovisioning de comptes de ressources individuels** sont utiles pour spécifier une stratégie de deprovisioning distincte pour différentes ressources. Par exemple, la plupart des clients ne veulent pas supprimer les utilisateurs Active Directory car chaque utilisateur a un identificateur qui ne pourra plus jamais être recréé après la suppression. Cependant, dans les environnements où de nouvelles ressources sont ajoutées, vous pouvez ne pas vouloir utiliser cette option car la configuration du deprovisioning doit être mise à jour à chaque fois qu'une nouvelle ressource est ajoutée.

Configuration de l'onglet Notification

Cette section contient les instructions à suivre pour configurer l'onglet Notification, qui est disponible dans le cadre du processus de configuration des modèles de tâches. Pour les instructions relatives au démarrage du processus de configuration, voir “Configuration des modèles de tâches” à la page 306.

Tous les Modèles de tâches prennent en charge l'envoi de notifications par e-mail aux administrateurs et utilisateurs quand Identity Manager appelle un processus (en général une fois le processus terminé). Vous pouvez utiliser l'onglet Notification pour configurer ces notifications.

Remarque – Identity Manager utilise des modèles d’e-mails pour envoyer des informations et des demandes d’actions aux administrateurs, approbateurs et utilisateurs. Pour plus d’informations sur les modèles d’e-mails d’Identity Manager, voir la section “Personnalisation des modèles d'e-mails” à la page 106 de ce guide.

La Figure 9–5 représente la page Notification pour le modèle Créer un modèle utilisateur.

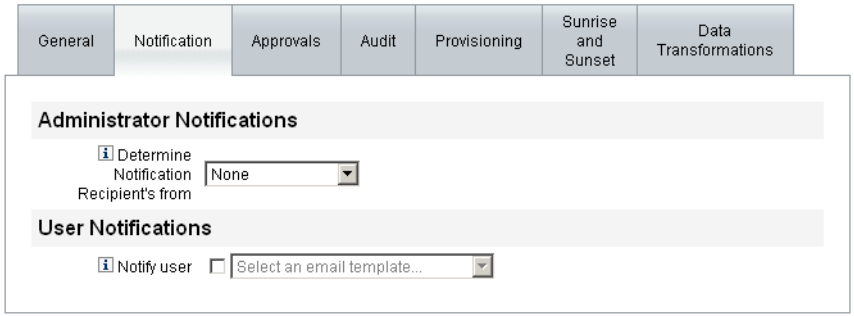


FIGURE 9–5 Onglet Notification : Créer un modèle utilisateur

Configuration des notifications utilisateur

Lorsque vous spécifiez les utilisateurs à avertir, vous devez aussi spécifier le nom d'un modèle d'e-mail qui sera utilisé pour générer l'e-mail utilisé pour la notification.

Pour avertir l'utilisateur qui est créé, mis à jour ou supprimé, activez la case à cocher Avertir l'utilisateur, comme indiqué dans la Figure 9–6 et sélectionnez un modèle d'e-mail dans la liste.

FIGURE 9–6 Spécification d'un modèle d'e-mail

Configuration des notifications à l'administrateur

Pour spécifier la façon dont Identity Manager détermine les destinataires des notifications à l'administrateur, sélectionnez une option dans le menu Déterminer les destinataires de la notification à partir de.

Les options disponibles sont les suivantes :

- **Aucun(e)** (option par défaut). Aucun administrateur ne sera averti.
- **Attribut**. Sélectionnez cette option pour déduire les ID de compte des destinataires des notifications d'un attribut spécifié dans la vue des utilisateurs. Pour plus d'informations, voir "Spécification des destinataires des notifications à l'administrateur par attribut" à la page 311.
- **Règle**. Sélectionnez cette option pour déduire les ID de compte des destinataires des notifications en évaluant une règle spécifiée. Pour plus d'informations, voir "Spécification des destinataires des notifications à l'administrateur par règle" à la page 312.

- **Requête**. Sélectionnez cette option pour déduire les ID de compte des destinataires des notifications de l'interrogation d'une ressource particulière. Pour plus d'informations, voir "Spécification des destinataires des notifications à l'administrateur par interrogation" à la page 313.
- **Liste des administrateurs**. Sélectionnez cette option pour choisir explicitement les destinataires des notifications dans une liste. Pour plus d'informations, voir "Spécification des destinataires des notifications à l'administrateur par attribut" à la page 311.

Spécification des destinataires des notifications à l'administrateur par attribut

Remarque – La résolution de cet attribut doit fournir une chaîne représentant un ID de compte unique ou une liste d'ID de compte.

▼ Pour déduire les ID de compte des destinataires des notifications d'un attribut spécifié

1 **Sélectionnez Attribut dans le menu Déterminer les destinataires de la notification à partir de : de nouvelles options s'affichent comme indiqué dans la figure suivante.**

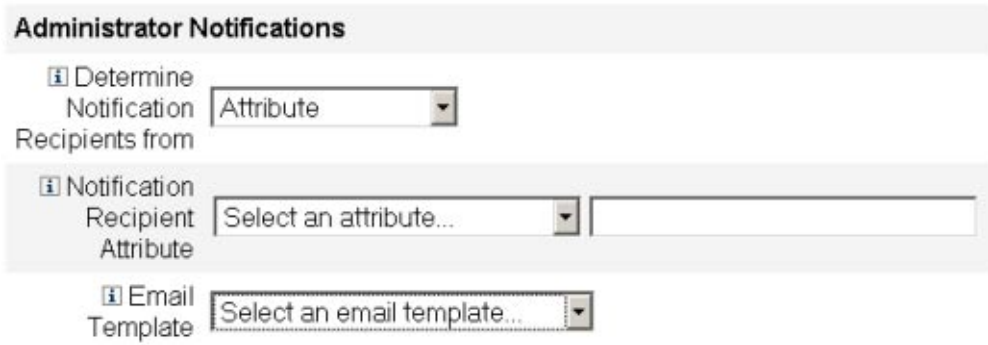


FIGURE 9–7 Notifications à l'administrateur : Attribut

Ces options sont les suivantes :

- **Attribut de destinataire de notification**. Fournit une liste d'attributs (actuellement définis pour la vue associée à la tâche configurée par ce modèle) utilisés pour déterminer les ID de compte des destinataires.
- **Modèle d'e-mail**. Fournit une liste de modèles d'e-mails.

2 **Sélectionnez un attribut dans le menu Attribut de destinataire de notification.**

Le nom de l'attribut s'affiche dans le champ de texte adjacent au menu.

3 **Sélectionnez un modèle dans le menu Modèle d'e-mail pour spécifier un format pour l'e-mail de notification des administrateurs.**

Spécification des destinataires des notifications à l'administrateur par règle

Remarque – La résolution de cette règle doit fournir une chaîne représentant un ID de compte unique ou une liste d'ID de compte.

▼ Pour déduire les ID de compte des destinataires des notifications d'une règle spécifiée

1 **Sélectionnez Règle dans le menu Déterminer les destinataires de la notification par. Les nouvelles options suivantes s'affichent dans le formulaire Notification.**

FIGURE 9–8 Notifications à l'administrateur : Règle

- **Règle du destinataire de notification**. Fournit une liste de règles (couramment définies pour votre système) qui, lors de l'évaluation, retourne les ID de compte des destinataires.
- **Modèle d'e-mail**. Fournit une liste de modèles d'e-mails.

2 **Sélectionnez une règle dans le menu Règle de destinataire de la notification.**

3 **Sélectionnez un modèle dans le menu Modèle d'e-mail pour spécifier un format pour l'e-mail de notification des administrateurs.**

Spécification des destinataires des notifications à l'administrateur par interrogation

Remarque – Pour l'instant, seules les interrogations de ressource LDAP et Active Directory sont prises en charge.

▼ Pour déduire les ID de compte des destinataires des notifications de l'interrogation d'une ressource spécifiée

1 **Sélectionnez Requête dans le menu Déterminer les destinataires de la notification à partir de : de nouvelles options s'affichent comme indiqué à la Figure 9–9.**

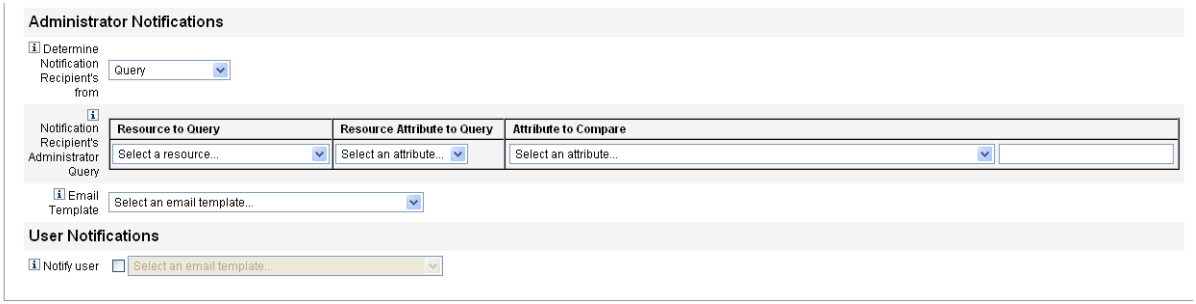


FIGURE 9–9 Notifications à l'administrateur : Requête

Le tableau Requête administrateur du destinataire de notification consiste en les menus suivants, que vous pouvez utiliser pour construire une interrogation :

- **Ressource à interroger**. Fournit une liste des ressources actuellement définies pour votre système.
- **Attribut de ressource à interroger**. Fournit une liste des attributs de ressource actuellement définis pour votre système.
- **Attribut à comparer**. Fournit une liste des attributs actuellement définis pour votre système.
- **Modèle d'e-mail**. Fournit une liste de modèles d'e-mails.

2 **Sélectionnez une ressource, un attribut de ressource et un attribut à comparer dans ces menus afin de construire l'interrogation.**

3 **Sélectionnez un modèle dans le menu Modèle d'e-mail pour spécifier un format pour l'e-mail de notification des administrateurs.**

▼ Pour spécifier les destinataires des notifications administrateur dans la Liste des administrateurs

1 **Sélectionnez Liste des administrateurs dans le menu Déterminer les destinataires de la notification à partir de : de nouvelles options s'affichent comme indiqué dans la figure suivante.**

FIGURE 9–10 Notifications à l'administrateur : Liste des administrateurs

Ces options sont les suivantes :

- **Administrateurs à notifier**. Fournit un outil de sélection avec la liste des administrateurs disponibles.
- **Modèle d'e-mail**. Fournit une liste de modèles d'e-mails.

2 **Sélectionnez un ou plusieurs administrateurs dans la liste Administrateurs disponibles et déplacez-les vers la liste Administrateurs sélectionnés.**

3 **Sélectionnez un modèle dans le menu Modèle d'e-mail pour spécifier un format pour l'e-mail de notification des administrateurs.**

Configuration de l'onglet Approbations

Cette section contient les instructions à suivre pour configurer l'onglet Approbations, qui est disponible dans le cadre du processus de configuration des modèles de tâches. Pour les instructions relatives au démarrage du processus de configuration, voir la section "Configuration des modèles de tâches" à la page 306.

Vous pouvez utiliser l'onglet Approbations pour désigner des approbateurs supplémentaires et pour spécifier les attributs pour le formulaire d'approbation des tâches avant qu'Identity Manager n'exécute des tâches de création, suppression ou mise à jour d'utilisateurs.

Traditionnellement, les administrateurs associés à une organisation, une ressource ou un rôle spécifique, doivent par défaut approuver certaines tâches avant leur exécution. Identity Manager vous permet également de désigner des *approbateurs supplémentaires*, qui sont des administrateurs supplémentaires auxquels il sera demandé d'approuver la tâche.

Remarque – Si vous configurez des Approbateurs supplémentaires pour un flux de travaux, vous demandez une approbation des approbateurs traditionnels *et* de tout approbateur supplémentaire spécifié dans le modèle.

La Figure 9–11 illustre la page Approbations initiale de l'interface utilisateur administrateur.

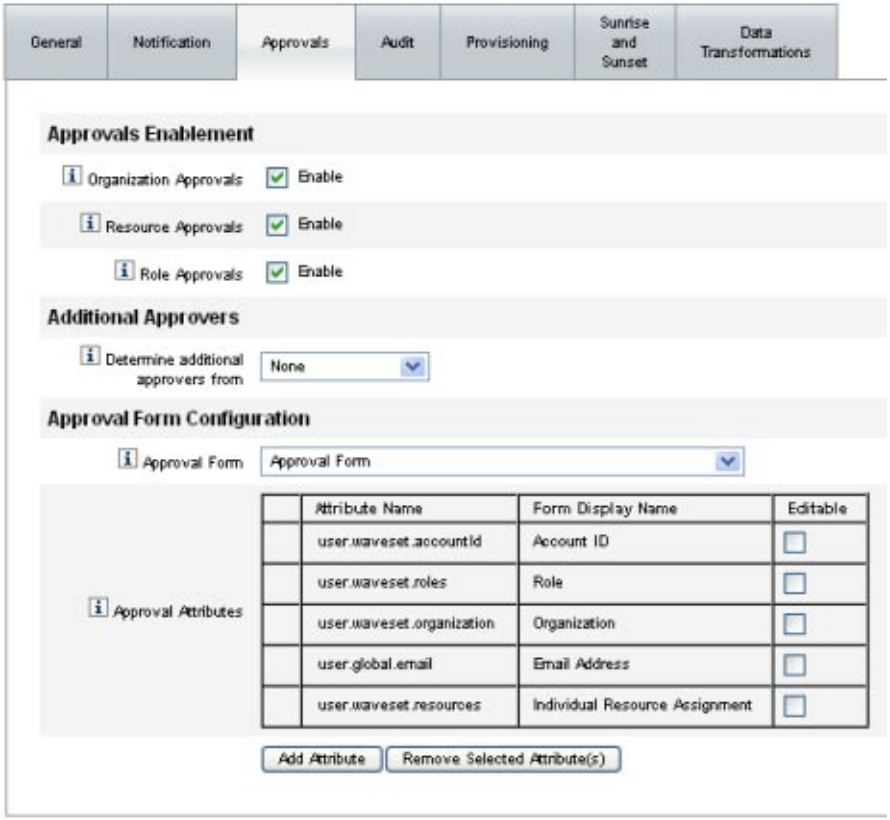


FIGURE 9–11 L'onglet Approbations : Créer un modèle utilisateur

▼ Pour configurer les approbations

1. **Complétez la section Activation des approbations (voir "Activation des approbations (onglet Approbations, section Activation des approbations)" à la page 317).**

2. **Complétez la section Activation des approbations (voir "Spécification d'approbateurs supplémentaires (onglet Approbations, section Approbateurs supplémentaires)" à la page 317).**

3. **Complétez la section Configuration du formulaire d'approbation uniquement pour les modèles Créer un utilisateur et Mettre à jour l'utilisateur (voir "Configuration du formulaire d'approbation (onglet Approbations, section Configuration du formulaire d'approbation) " à la page 327).**

4. **Lorsque vous avez terminé de configurer l'onglet Approbations, vous pouvez :**

- sélectionner un autre onglet pour continuer à éditer les modèles ;
- cliquer sur Enregistrer pour enregistrer vos modifications et revenir à la page Configurer les tâches ;
- cliquer sur Annuler pour abandonner vos modifications et revenir à la page Configurer les tâches.

Activation des approbations (onglet Approbations, section Activation des approbations)

Utilisez les cases à cocher Activation des approbations suivantes pour exiger des approbations avant de poursuivre les tâches de création, suppression ou mise à jour d'utilisateurs.

Remarque – Par défaut, ces cases à cocher sont activées pour les modèles Créer un utilisateur et Mettre à jour l'utilisateur, mais sont *désactivées* pour le modèle Supprimer l'utilisateur.

- **Approbations des organisations**. Sélectionnez cette case à cocher pour exiger des approbations de tout approbateur organisationnel configuré.
- **Approbations des ressources**. Sélectionnez cette case à cocher pour exiger des approbations de tout approbateur de ressource configuré.
- **Approbations des rôles**. Sélectionnez cette case à cocher pour exiger des approbations de tout approbateur de rôle configuré.

Spécification d'approbateurs supplémentaires (onglet Approbations, section Approbateurs supplémentaires)

Utilisez le menu Déterminer des approbateurs supplémentaires à partir de pour spécifier la façon dont Identity Manager déterminera les approbateurs supplémentaires pour les tâches de création, suppression ou mise à jour d'utilisateurs.

Les options de ce menu sont listées dans le Tableau 9–1.

TABLEAU 9–1 Options du menu Déterminer des approbateurs supplémentaires à partir de

Option	Description
Aucun(e) (option par défaut)	Aucun approbateur supplémentaire n'est requis pour l'exécution de cette tâche.
Attribut	Les ID de compte des approbateurs sont déduits d'un attribut spécifié dans la vue de l'utilisateur.
Règle	Les ID de compte des approbateurs sont déduits de l'évaluation d'une règle spécifiée.

TABLEAU 9–1 Options du menu Déterminer des approbateurs supplémentaires à partir de *(Suite)*

Option	Description
Requête	Les ID de compte des approbateurs sont déduits de l'interrogation d'une ressource particulière.
Liste des administrateurs	Les approbateurs sont choisis explicitement dans une liste.

Lorsque vous sélectionnez l'une de ces options (à l'exception de *Aucun(e)*), des options supplémentaires s'affichent dans l'interface utilisateur administrateur.

Utilisez les instructions fournies dans les sections suivantes pour spécifier une méthode pour déterminer des approbateurs supplémentaires.

▼ Pour déterminer des approbateurs supplémentaires à partir d'un attribut

Utilisez les étapes suivantes pour déterminer des approbateurs supplémentaires à partir d'un attribut.

1 Sélectionnez Attribut dans le menu Déterminer des approbateurs supplémentaires à partir de.

Remarque – La résolution de cet attribut doit fournir une chaîne représentant un ID de compte unique ou une liste d'ID de compte.

De nouvelles options s'affichent comme indiqué sur la figure suivante.

FIGURE 9–12 Approbateurs supplémentaires : Attribut

- **Attribut approbateur**. Fournit une liste d'attributs (actuellement définis pour la vue associée à la tâche configurée par ce modèle) utilisés pour déterminer les ID de compte des destinataires.

- **Délai d'expiration de l'approbation**. Fournit une méthode permettant de spécifier quand l'approbation expirera.

  Le paramètre Délai d'expiration de l'approbation s'applique aussi bien aux approbations initiales qu'aux approbations réassignées.

2 **Utilisez le menu Attribut approbateur pour sélectionner un attribut.**

L'attribut sélectionné s'affiche dans le champ de texte adjacent.

3 **Décidez si vous voulez que la demande d'approbation expire au bout d'un délai donné.**

- Pour spécifier un délai d'attente, reportez-vous aux instructions de la section "Pour configurer les délais d'expiration des approbations" à la page 322.
- Si vous ne voulez pas spécifier de délai d'attente, allez à "Configuration du formulaire d'approbation (onglet Approbations, section Configuration du formulaire d'approbation) " à la page 327 ou enregistrez vos changements et passez à la configuration d'un autre onglet.

▼ Pour déterminer des approbateurs supplémentaires à partir d'une règle

Utilisez les étapes suivantes pour déduire les ID de compte des approbateurs d'une règle spécifiée.

1 **Sélectionnez Règle dans le menu Déterminer des approbateurs supplémentaires à partir de.**

Remarque – La résolution de cette règle doit fournir une chaîne représentant un ID de compte unique ou une liste d'ID de compte.

De nouvelles options s'affichent comme indiqué sur la figure suivante.

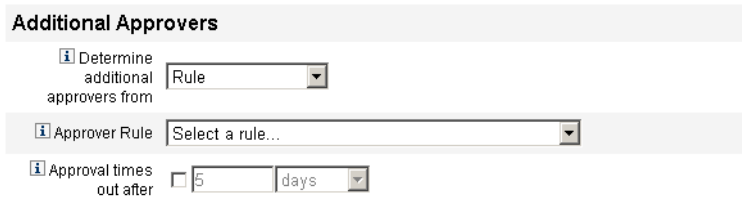


FIGURE 9–13 Approbateurs supplémentaires : Règle

- **Règle de l'approbateur**. Fournit une liste de règles (couramment définies pour votre système) qui, lors de l'évaluation, retourne les ID de compte des destinataires.

- **Délai d'expiration de l'approbation**. Fournit une méthode permettant de spécifier quand l'approbation expirera.

  Le paramètre Délai d'expiration de l'approbation s'applique aussi bien aux approbations initiales qu'aux approbations réassignées.

2 Sélectionnez une règle dans le menu Règle de l'approbateur.

3 Décidez si vous voulez que la demande d'approbation expire au bout d'un délai donné.

- Pour spécifier un délai d'attente, reportez-vous aux instructions de la section "Pour configurer les délais d'expiration des approbations" à la page 322.
- Si vous ne voulez pas spécifier de délai d'attente, allez à "Configuration du formulaire d'approbation (onglet Approbations, section Configuration du formulaire d'approbation) " à la page 327 ou enregistrez vos changements et passez à la configuration d'un autre onglet.

▼ Pour déterminer des approbateurs supplémentaires à partir d'une interrogation

Utilisez les étapes suivantes pour déduire les ID de compte des approbateurs de l'interrogation d'une ressource spécifiée.

Remarque – Pour l'instant, seules les interrogations de ressources LDAP et Active Directory sont prises en charge.

---

1 Sélectionnez Requête dans le menu Déterminer des approbateurs supplémentaires à partir de : de nouvelles options s'affichent comme indiqué dans la figure suivante.

FIGURE 9–14 Approbateurs supplémentaires : Requête

- **Requête d'administrateur d'approbation**. Fournit un tableau composé des menus suivants que vous pouvez utiliser pour construire une interrogation :
  - **Ressource à interroger**. Fournit une liste des ressources actuellement définies pour votre système.

- **Attribut de ressource à interroger**. Fournit une liste des attributs de ressource actuellement définis pour votre système.
- **Attribut à comparer**. Fournit une liste des attributs actuellement définis pour votre système.

- **Délai d'expiration de l'approbation**. Fournit une méthode permettant de spécifier quand l'approbation expirera.

Remarque – Le paramètre Délai d'expiration de l'approbation s'applique aussi bien aux approbations initiales qu'aux approbations réassignées.

---

2 Construisez une interrogation comme suit :

a. Sélectionnez une ressource dans le menu Ressource à interroger.

b. Sélectionnez des attributs dans les menus Attribut de ressource à interroger et Attribut à comparer.

3 Décidez si vous voulez que la demande d'approbation expire au bout d'un délai donné.

- Pour spécifier un délai d'attente, reportez-vous aux instructions de la section "Pour configurer les délais d'expiration des approbations" à la page 322.
- Si vous ne voulez pas spécifier de délai d'attente, allez à "Configuration du formulaire d'approbation (onglet Approbations, section Configuration du formulaire d'approbation) " à la page 327 ou enregistrez vos changements et passez à la configuration d'un autre onglet.

▼ Pour déterminer des approbateurs supplémentaires à partir de la liste des administrateurs

Utilisez les étapes suivantes pour choisir explicitement des approbateurs supplémentaires dans la liste des administrateurs.

1 Sélectionnez Liste des administrateurs dans le menu Déterminer des approbateurs supplémentaires à partir de : de nouvelles options s'affichent, comme indiqué dans la figure suivante.

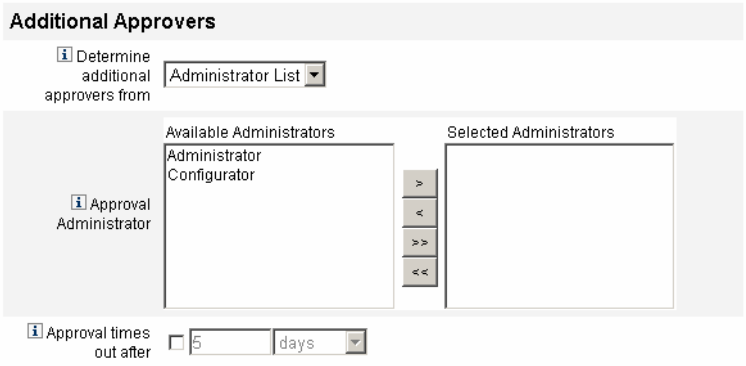


FIGURE 9–15 Approbateurs supplémentaire : Liste des administrateurs

- **Administrateurs à notifier**. Fournit un outil de sélection avec la liste des administrateurs disponibles.
- **Formulaire d'approbation**. Fournit une liste de formulaires utilisateur que les approbateurs supplémentaires peuvent utiliser pour approuver ou rejeter une demande d'approbation.
- **Délai d'expiration de l'approbation**. Fournit une méthode permettant de spécifier quand l'approbation expirera.

Le **Délai d'expiration de l'approbation** s'applique aussi bien aux approbations initiales qu'aux approbations réassignées.

2 Sélectionnez un ou plusieurs administrateurs dans la liste Administrateurs disponibles et déplacez les noms sélectionnés dans la liste Administrateurs sélectionnés.

3 Décidez si vous voulez que la demande d'approbation expire au bout d'un délai donné.

- Pour spécifier un délai d'attente, reportez-vous aux instructions de la section "Pour configurer les délais d'expiration des approbations" à la page 322.
- Si vous ne voulez pas spécifier de délai d'attente, vous pouvez continuer la "Configuration du formulaire d'approbation (onglet Approbations, section Configuration du formulaire d'approbation) " à la page 327.

▼ Pour configurer les délais d'expiration des approbations

Utilisez les étapes suivantes pour configurer les délais d'expiration des approbations dans la section Délai d'expiration de l'approbation.

1 Sélectionnez la case à cocher Délai d'expiration de l'approbation.

Le champ de texte adjacent et le menu sont activés et les options Action après délai d'attente s'affichent comme indiqué sur la figure suivante.

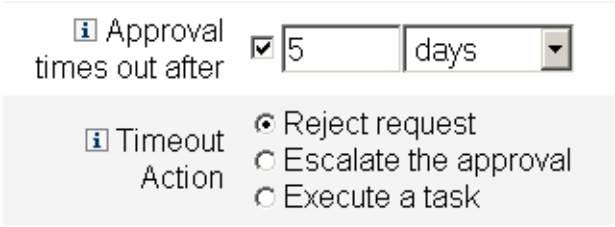


FIGURE 9–16 Options relatives au délai d'expiration des approbations

2 Utilisez le champ de texte Délai d'expiration de l'approbation et le menu pour spécifier un délai d'attente comme suit :

a. Sélectionnez secondes, minutes, heures ou jours dans le menu.

b. Saisissez un nombre dans le champ de texte pour indiquer le nombre de secondes, minutes, heures ou jours à spécifier pour le délai d'attente.

Remarque – Le paramètre Délai d'expiration de l'approbation s'applique aussi bien aux approbations initiales qu'aux approbations réassignées.

---

3 Utilisez les boutons Action après délai d'attente pour spécifier ce qui se passe à l'expiration de la demande d'approbation.

Cliquez sur l'un des éléments suivants :

- **Rejeter la demande**. Identity Manager rejette automatiquement la demande si elle n'est pas approuvée dans le délai d'expiration spécifié.
- **Réassigner l'approbation**. Identity Manager réassigne automatiquement la demande à un autre approbateur si elle n'est pas approuvée dans le délai d'expiration spécifié.

  Lorsque vous activez ce bouton, de nouvelles options s'affichent car vous devez indiquer la façon dont Identity Manager déterminera les approbateurs en cas d'approbation réassignée. Pour les instructions, allez à "Pour configurer la section Déterminer les approbateurs de signalisation" à la page 324.
- **Exécuter une tâche**. Identity Manager exécute automatiquement une tâche de remplacement si la demande d'approbation n'est pas approuvée dans le délai d'expiration spécifié.

  Activez ce bouton pour afficher le menu Tâche après expiration du délai d'approbation permettant de spécifier une tâche à exécuter en cas d'expiration du délai d'attente de l'approbation. Pour les instructions, allez à "Pour configurer la section Tâche après expiration du délai d'approbation" à la page 326.

▼ Pour configurer la section Déterminer les approbateurs de signalisation

Lorsque vous sélectionnez Réassigner l'approbation dans la section Action après délai d'attente ("Pour configurer les délais d'expiration des approbations" à la page 322), le menu Déterminer les approbateurs de signalisation s'affiche, comme indiqué sur la figure suivante.

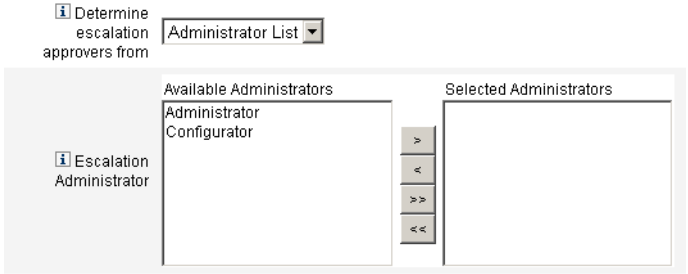
- **Choisissez une option dans ce menu pour spécifier la façon dont les approbateurs sont déterminés dans le cas d'une approbation réassignée.**

  Les options sont les suivantes :

  - **Attribut**. Détermine les ID de compte des approbateurs à l'aide d'un attribut spécifié dans la vue de l'utilisateur.

    Remarque – La résolution de cet attribut doit fournir une chaîne représentant un ID de compte unique ou une liste d'ID de compte.

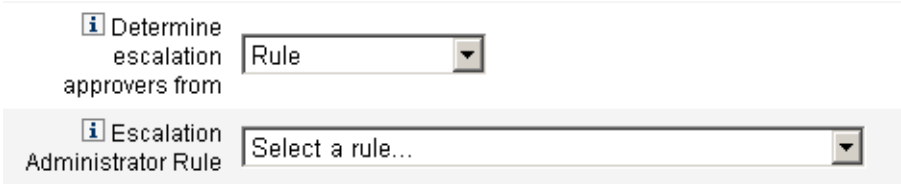
    Lorsque vous sélectionnez cette option, le menu Attribut de l'administrateur de signalisation s'affiche. Sélectionnez un attribut dans la liste. L'attribut sélectionné s'affiche dans le champ de texte adjacent, comme indiqué sur la figure suivante.



  - **Règle**. Détermine les ID de compte des approbateurs en évaluant une règle spécifiée.

Remarque – La résolution de cette règle doit fournir une chaîne représentant un ID de compte unique ou une liste d'ID de compte.

Lorsque vous sélectionnez cette option, le menu Règle de l'administrateur de signalisation s'affiche comme indiqué. Sélectionnez une règle dans la liste.

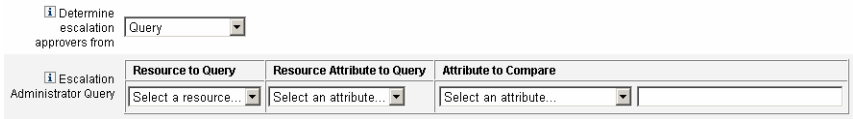


- **Requête**. Détermine les ID de compte des approbateurs en interrogeant une ressource particulière.

  Les menus Requête de l'administrateur de signalisation s'affichent comme indiqué sur la figure suivante.

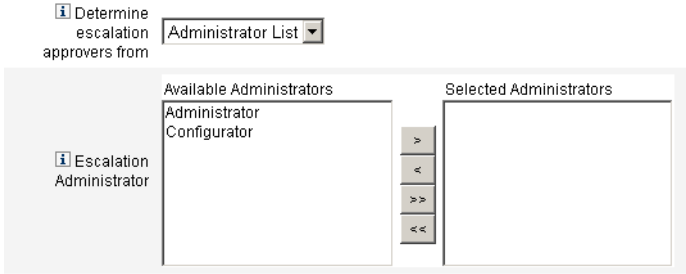
  Construisez votre interrogation comme suit :

  a. Sélectionnez une ressource dans le menu Ressource à interroger.
  b. Sélectionnez un attribut dans le menu Attribut de ressource à interroger.
  c. Sélectionnez un attribut dans le menu Attribut à comparer.



- **Liste des administrateurs** (*valeur par défaut*). Choisissez explicitement les approbateurs dans une liste.

  L'outil de sélection Administrateur de signalisation s'affiche comme illustré sur la figure suivante.



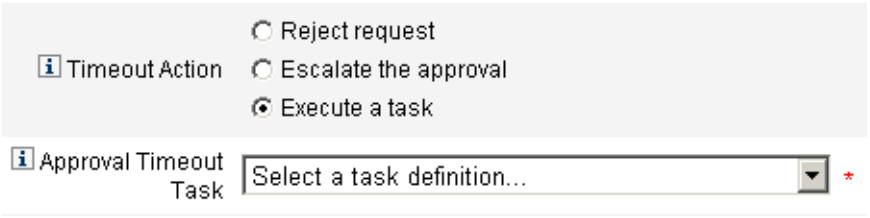
Sélectionnez les approbateurs comme suit :

a. Sélectionnez un ou plusieurs noms d'administrateurs dans la liste Administrateurs disponibles.

b. Amenez les noms sélectionnés dans la liste Administrateurs sélectionnés.

▼ Pour configurer la section Tâche après expiration du délai d'approbation

Lorsque vous sélectionnez l'option Exécuter une tâche dans la section Action après délai d'attente ("Pour configurer les délais d'expiration des approbations" à la page 322), le menu Tâche après expiration du délai d'approbation s'affiche, comme indiqué sur la figure suivante.



- **Choisissez une définition de tâche à exécuter en cas d'expiration du délai d'attente de la demande d'approbation.**

  Par exemple, vous pouvez autoriser le demandeur à soumettre une demande d'assistance ou à envoyer un rapport à l'administrateur.

Configuration du formulaire d'approbation (onglet Approbations, section Configuration du formulaire d'approbation)

Remarque – Le Delete User Template ne contient pas de section Configuration du formulaire d'approbation. Vous pouvez uniquement configurer cette section pour les modèles Créer un utilisateur et Mettre à jour l'utilisateur.

Vous pouvez utiliser les fonctionnalités de la section Configuration du formulaire d'approbation pour sélectionner un formulaire d'approbation et ajouter (ou supprimer) des attributs de ce formulaire d'approbation.

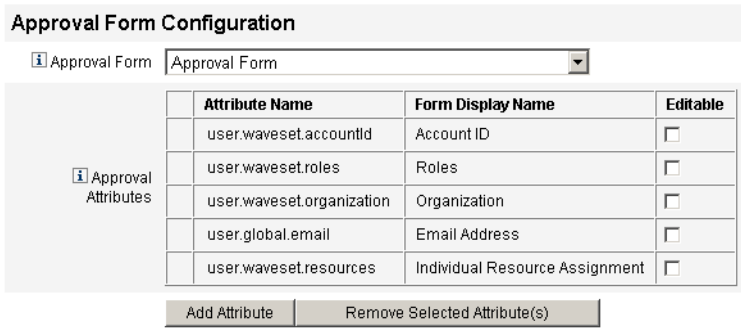


FIGURE 9–17 Configuration du formulaire d'approbation

Par défaut, le tableau Attributs d'approbation contient les attributs standard suivants :

- `user.waveset.accountId`
- `user.waveset.roles`
- `user.waveset.organization`
- `user.global.email`
- `user.waveset.resources`

Remarque – Le formulaire d'approbation par défaut a été instrumenté pour permettre l'affichage des attributs d'approbation. Si vous utilisez un formulaire d'approbation autre que celui par défaut, vous devez instrumenter ce formulaire pour afficher les attributs d'approbation spécifiés dans le tableau Attributs d'approbation.

▼ Pour configurer un formulaire d'approbation pour des approbateurs supplémentaires

1 **Sélectionnez un formulaire dans le menu Formulaire d'approbation.**

Les approbateurs utiliseront ce formulaire pour approuver ou rejeter une demande d'approbation.

2 **Sélectionnez les cases à cocher de la colonne Modifiable du tableau Attributs d'approbation pour éditer la valeur des attributs.**

Par exemple, si vous sélectionnez la case à cocher `user.waveset.accountId`, l'approbateur peut changer l'ID de compte de l'utilisateur.

Remarque – Si vous modifiez des valeurs d'attribut spécifiques à un compte dans le formulaire d'approbation, vous devrez aussi ignorer les valeurs d'attribut du même nom lorsque l'utilisateur sera effectivement provisionné. Par exemple, si la ressource `R1` existe sur votre système avec l'attribut de schéma `description` et que vous ajoutez l'attribut `user.accounts[R1].description` au formulaire d'approbation sous forme d'attribut modifiable, tous les changements apportés à la valeur de l'attribut `description` dans le formulaire d'approbation ignoreront la valeur propagée de `global.description` uniquement pour la ressource `R1`.

---

3 **Cliquez sur les bouton Ajouter un attribut ou** *Supprimer les attributs sélectionnés* **pour indiquer les attributs des données de compte du nouvel utilisateur à afficher dans le formulaire d'approbation.**

- Pour ajouter des attributs au formulaire, reportez-vous à "Pour ajouter des attributs au formulaire d'approbation" à la page 328.
- Pour supprimer des attributs du formulaire, voir "Suppression des attributs" à la page 329.

Vous ne pouvez pas supprimer les attributs par défaut d'un formulaire d'approbation sans modifier le fichier XML.

▼ Pour ajouter des attributs au formulaire d'approbation

1 **Cliquez sur le bouton Ajouter un attribut qui se trouve sous le tableau Attributs d'approbation.**

Le menu Nom d'attribut est activé dans le tableau Attributs d'approbation, comme indiqué sur la figure suivante.

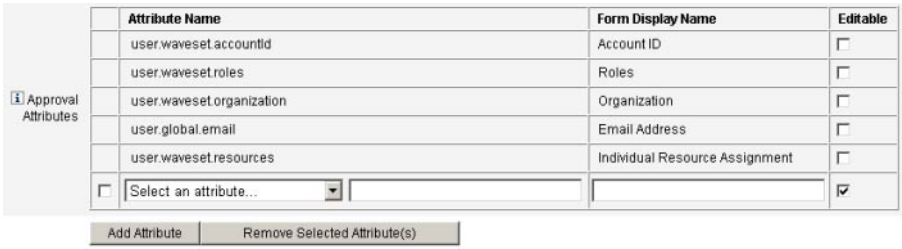


FIGURE 9–18 Ajout d'attributs d'approbation

2 Sélectionnez un attribut dans le menu.

Le nom d'attribut sélectionné s'affiche dans le champ de texte adjacent et le nom à afficher par défaut de l'attribut s'affiche dans la colonne Nom d'affichage du formulaire.

Par exemple, si vous sélectionnez l'attribut `user.waveset.organization`, vous pouvez :

- Changer si nécessaire le nom d'attribut par défaut ou le Nom d'affichage du formulaire en saisissant un nouveau nom dans le champ de texte approprié.
- Sélectionner la case à cocher Modifiable pour permettre à l'approbateur de changer la valeur de l'attribut.

  Par exemple, l'approbateur peut vouloir ignorer certaines informations telles que l'adresse e-mail de l'utilisateur.

3 Répétez ces étapes pour spécifier des attributs supplémentaires.

Suppression des attributs

Remarque – Vous ne pouvez pas supprimer les attributs par défaut d'un formulaire d'approbation sans modifier le fichier XML.

▼ Pour supprimer des attributs du formulaire d'approbation

1 Activez une ou plusieurs cases à cocher dans la colonne la plus à gauche du tableau Attributs d'approbation.

2 Cliquez sur le bouton Supprimer les attributs sélectionnés pour supprimer immédiatement les attributs sélectionnés de la table Attributs d'approbation.

Par exemple, `user.global.firstname` et `user.waveset.organization` seront supprimés du tableau suivant si vous cliquez sur le bouton Supprimer les attributs sélectionnés.

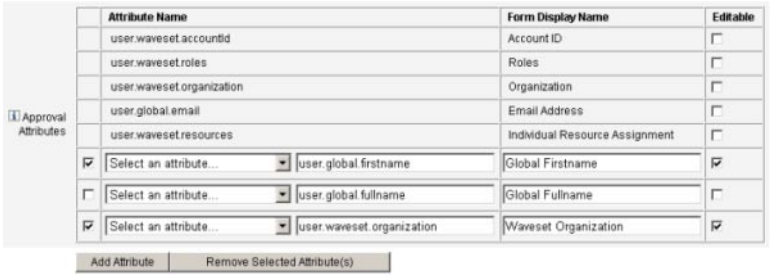


FIGURE 9–19 Suppression des attributs d'approbation

Configuration de l'onglet Vérification informatique

Cette section contient les instructions à suivre pour configurer l'onglet Vérification informatique, qui est disponible dans le cadre du processus de configuration des modèles de tâches. Pour les instructions relatives au démarrage du processus de configuration, voir "Configuration des modèles de tâches" à la page 306.

Tous les Modèles de tâches configurables prennent en charge la configuration de flux de travaux pour contrôler certaines tâches. Plus précisément, vous pouvez configurer l'onglet Vérification informatique pour contrôler si les événements de flux de travaux seront audités et spécifier les attributs qui seront stockés à des fins de génération de rapports.

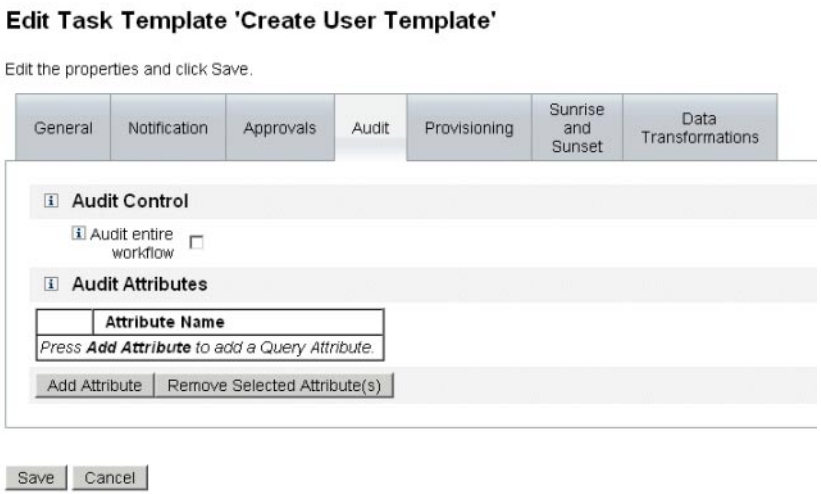


FIGURE 9–20 Audit du modèle Créer un utilisateur

Pour configurer l'audit

1. **Sélectionnez la case à cocher Contrôler l'intégralité du flux de travaux pour activer la fonctionnalité d'audit des flux de travaux.**

   Pour toute information sur l'audit des flux de travaux, voir "Création d'événements de contrôle à partir des flux de travaux" à la page 342. Sachez toutefois que l'audit des flux de travaux dégrade la performance.

2. **Cliquez sur le bouton Ajouter un attribut qui se trouve dans la section Attributs d'audit pour sélectionner les attributs que vous voulez contrôler à des fins de génération de rapports.**

3. **Lorsque le menu Sélectionner un attribut s'affiche dans le tableau Attributs d'audit, sélectionnez un attribut dans la liste.**

   Le nom de l'attribut sélectionné s'affiche dans le champ de texte adjacent.

FIGURE 9–21 Ajout d'un attribut

Pour supprimer des attributs

1. **Cochez la case en regard de l'attribut à supprimer.**

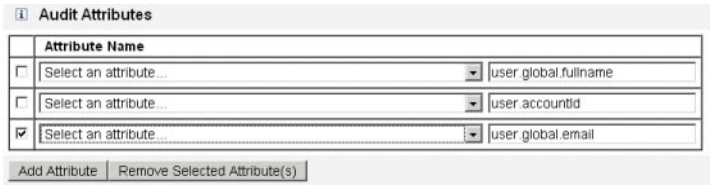


FIGURE 9–22 Suppression de l'attribut `user.global.email`

2. **Cliquez sur le bouton Supprimer les attributs sélectionnés.**

Configuration de l'onglet Provisioning

Cette section contient les instructions à suivre pour configurer l'onglet Provisioning, qui est disponible dans le cadre du processus de configuration des modèles de tâches. Pour les instructions relatives au démarrage du processus de configuration, voir "Configuration des modèles de tâches" à la page 306.

Remarque – Cet onglet est uniquement disponible pour les modèles Créer un utilisateur et Mettre à jour l'utilisateur.

FIGURE 9–23 Onglet Provisioning : Créer un modèle utilisateur

L'onglet Provisioning permet de configurer les options suivantes liées au provisioning :

- **Provisionner en arrière-plan**. Cochez cette case à cocher pour exécuter une tâche de création, suppression ou mise à jour en arrière-plan au lieu d'exécuter cette tâche de manière synchrone.

  Le provisioning en arrière-plan permet de continuer à travailler dans Identity Manager pendant l'exécution de la tâche.
- **Ajouter le lien Réessayer au résultat de la tâche**. Cochez cette case à cocher pour ajouter un lien Réessayer à l'interface utilisateur quand une erreur de provisioning est causée par l'exécution d'une tâche. Le lien Réessayer permet aux utilisateurs de relancer la tâche si la première tentative s'est soldée par un échec.

Configuration de l'onglet Ouverture et clôture

Cette section contient les instructions à suivre pour configurer l'onglet Ouverture et clôture, qui est disponible dans le cadre du processus de configuration des modèles de tâches. Pour les instructions relatives au démarrage du processus de configuration, voir "Configuration des modèles de tâches" à la page 306.

Remarque – Cet onglet est uniquement disponible pour le modèle Créer un utilisateur.

L'onglet Ouverture et clôture permet de sélectionner une méthode pour déterminer l'heure et la date auxquelles les actions suivantes se produiront :

- provisioning d'un nouvel utilisateur (*ouverture*),
- deprovisioning d'un nouvel utilisateur (*clôture*).

Par exemple, vous pouvez spécifier une date de clôture pour un employé intérimaire dont le contrat a une durée déterminée de six mois.

La Figure 9–24 illustre les paramètres de l'onglet Ouverture et clôture.

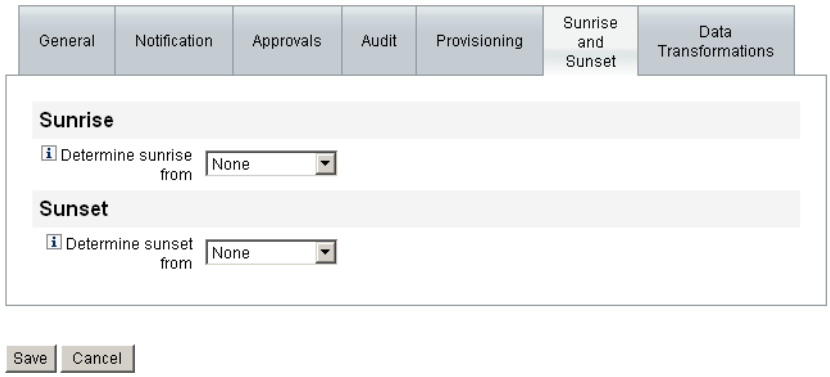


FIGURE 9–24 L'onglet Ouverture et clôture : Créer un modèle utilisateur

Les sections suivantes contiennent les instructions à suivre pour configurer l'onglet Ouverture et clôture.

Configuration des ouvertures

Configurez les paramètres d'ouverture pour spécifier la date et l'heure auxquelles le provisioning aura lieu pour un nouvel utilisateur et indiquer l'utilisateur qui sera le propriétaire de l'élément de travail pour l'ouverture.

▼ Pour configurer les ouvertures

1 **Sélectionnez l'une des options suivantes dans le menu Définir l'ouverture à partir de pour spécifier la façon dont Identity Manager déterminera la date et l'heure du provisioning.**

- **Spécification d'une heure**. Reporte le provisioning jusqu'à une heure future spécifiée. Pour les instructions, allez à "Pour reporter le provisioning jusqu'à une heure spécifiée" à la page 334.
- **Spécification d'une date**. Reporte le provisioning jusqu'à une date du calendrier future spécifiée. Pour les instructions, allez à "Pour reporter le provisioning jusqu'à une date du calendrier spécifiée" à la page 335.
- **Spécification d'un attribut**. Reporte le provisioning jusqu'à une date et une heure spécifiées qui sont fonction de la valeur de l'attribut dans la vue de l'utilisateur. L'attribut doit contenir une chaîne de date/heure. Lorsque vous spécifiez un attribut pour qu'il contienne une chaîne date/heure, vous pouvez spécifier un format de date auquel vous voudriez que les données se conforment.

  Pour les instructions, allez à "Pour déterminer la date et l'heure du provisioning en spécifiant un attribut" à la page 335.
- **Spécification d'une règle**. Reporte le provisioning en fonction d'une règle dont l'évaluation génère une chaîne date/heure. Comme lorsque vous spécifiez un attribut, vous pouvez spécifier un format de date auquel vous voudriez que les données se conforment.

  Pour les instructions, allez à "Pour déterminer la date et l'heure du provisioning en évaluant une règle" à la page 336.

Le menu Définir l'ouverture à partir de passe par défaut sur l'option Aucun(e), qui permet au provisioning d'être effectué immédiatement.

2 **Sélectionnez un utilisateur dans le menu Propriétaire de l'élément de travail pour spécifier qui sera le propriétaire de l'élément de travail de l'ouverture.**

Remarque – Les éléments de travail d'ouverture sont disponibles depuis l'onglet Approbations.

Spécification d'une heure

Cette section contient des instructions utiles pour reporter le provisioning jusqu'à une heure spécifique.

▼ Pour reporter le provisioning jusqu'à une heure spécifiée

1 **Sélectionnez Heure indiquée dans le menu Définir l'ouverture à partir de.**

2 **Lorsqu'un nouveau champ de texte et un menu s'affichent à droite du menu Définir l'ouverture à partir de, saisissez un nombre dans le champ de texte vide puis sélectionnez une unité de temps dans le menu.**

Par exemple, pour provisionner un nouvel utilisateur dans deux heures, spécifiez les informations indiquées dans la figure suivante.

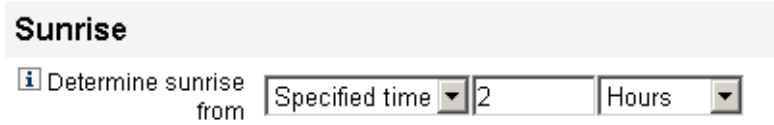


FIGURE 9–25 Provisioning d'un nouvel utilisateur dans deux heures

▼ Pour reporter le provisioning jusqu'à une date du calendrier spécifiée

Cette section contient des instructions utiles pour reporter le provisioning jusqu'à une date spécifique.

1 **Sélectionnez Jour indiqué dans le menu Définir l'ouverture à partir de.**

2 **Utilisez les options du menu qui s'affichent pour préciser la semaine du mois, le jour de la semaine et le mois de l'année auxquels le provisioning aura lieu.**

Par exemple, pour provisionner un nouvel utilisateur le deuxième lundi de septembre, spécifiez les informations indiquées dans la figure suivante.

FIGURE 9–26 Provisioning d'un nouvel utilisateur à une date donnée

▼ Pour déterminer la date et l'heure du provisioning en spécifiant un attribut

Les instructions de cette section vous permettront de déterminer la date et l'heure d'une opération de provisioning sur la base des valeurs des attributs dans les données de compte des utilisateurs.

1 **Sélectionnez Attribut dans le menu Définir l'ouverture à partir de.**

Les options suivantes sont activées :

- **Menu Attribut d'ouverture** Cette option fournit la liste des attributs actuellement définis pour la vue associée à la tâche configurée par ce modèle.
- **Case à cocher et menu Format spécifique de la date**. Cette option permet de spécifier une chaîne de format de date pour la valeur de l'attribut (le cas échéant).

Si vous ne cochez pas la case Format de date spécifique, les chaînes de date doivent être conformes à un format acceptable pour l'attribut `convertDateToString` de la méthode `FormUtil`. Consultez la documentation du produit pour la liste complète des formats de date pris en charge.

2 Sélectionnez un attribut dans le menu Attribut d'ouverture.

3 Si nécessaire, cochez la case à cocher Format de date spécifique et quand le champ Format de date spécifique devient actif, saisissez une chaîne de format de date.

Par exemple, pour provisionner un nouvel utilisateur sur la base de la valeur de son attribut `waveset.accountId` en utilisant le format jour, mois et année, spécifiez les informations indiquées dans la figure suivante.

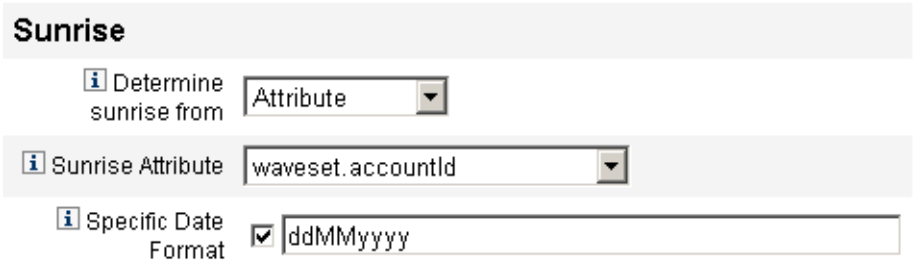


FIGURE 9–27 Provisioning d'un nouvel utilisateur par attribut

▼ Pour déterminer la date et l'heure du provisioning en évaluant une règle

Cette section contient des instructions utiles pour déterminer la date et l'heure de provisioning en évaluant une règle donnée.

1 Sélectionnez Règle dans le menu Définir l'ouverture à partir de.

Les options suivantes sont activées :

- Menu **Règle d'ouverture** Fournit la liste des règles actuellement définies pour votre système.
- Case à cocher et menu **Format spécifique de la date**. Cette option permet de spécifier une chaîne de format de date pour la valeur renvoyée par la règle (le cas échéant).

Si vous ne cochez pas la case Format de date spécifique, les chaînes de date doivent être conformes à un format acceptable pour l'attribut `FormUtil` de la méthode `convertDateToString`. Consultez la documentation du produit pour la liste complète des formats de date pris en charge.

2 **Sélectionnez une règle dans le menu Règle d'ouverture.**

3 **Si nécessaire, cochez la case à cocher Format de date spécifique et quand le champ Format de date spécifique devient actif, saisissez une chaîne de format de date.**

Par exemple, pour provisionner un nouvel utilisateur sur la base de la règle Email en utilisant le format année, mois, jour, heures, minutes et secondes, spécifiez les informations indiquées dans la figure suivante.

FIGURE 9–28 Provisioning d'un nouvel utilisateur en utilisant une règle

Configuration des clôtures

Les options et procédures de configuration de clôtures (deprovisioning) sont essentiellement identiques à celles présentées pour les ouvertures (provisioning) dans la section Configuration des ouvertures.

La seule différence réside dans le fait que la section Clôture fournit également un menu Tâche de clôture car vous devez spécifier une tâche pour suspendre l'utilisateur à la date et à l'heure indiquées.

▼ Pour configurer une clôture

1 **Utilisez le menu Définir la clôture à partir de pour spécifier la méthode employée pour déterminer quand aura lieu le deprovisioning.**

Remarque – Le menu Définir la clôture à partir de passe par défaut sur l'option Aucun(e), qui permet au deprovisioning d'être effectué immédiatement.

- **Heure indiquée**. Reporte le deprovisioning jusqu'à l'heure spécifiée dans le futur. Pour les instructions, allez à "Pour reporter le provisioning jusqu'à une heure spécifiée" à la page 334.
- **Date indiquée**. Reporte le deprovisioning jusqu'à une date du calendrier future spécifiée. Pour les instructions, allez à "Pour reporter le provisioning jusqu'à une date du calendrier spécifiée" à la page 335.
- **Attribut**. Reporte le deprovisioning jusqu'à une date et une heure spécifiées qui sont fonction de la valeur de l'attribut dans les données de compte des utilisateurs. L'attribut doit contenir une chaîne de date/heure. Lorsque vous spécifiez un attribut pour qu'il contienne une chaîne de date/heure, vous pouvez spécifier un format de date auquel vous voudriez que les données se conforment. Pour les instructions, consultez "Pour déterminer la date et l'heure du provisioning en spécifiant un attribut" à la page 335.
- **Règle**. Reporte le deprovisioning en fonction d'une règle dont l'évaluation génère une chaîne de date/heure. Comme lorsque vous spécifiez un attribut, vous pouvez spécifier un format de date que les données devraient respecter.

  Pour les instructions, voir "Pour déterminer la date et l'heure du provisioning en évaluant une règle" à la page 336.

2 **Utilisez le menu Tâche de clôture pour spécifier une tâche afin de suspendre l'utilisateur à la date et à l'heure indiquées.**

Configuration de l'onglet Transformations des données

Cette section contient les instructions à suivre pour configurer l'onglet Transformations des données, qui est disponible dans le cadre du processus de configuration des modèles de tâches. Pour les instructions relatives au démarrage du processus de configuration, voir "Configuration des modèles de tâches" à la page 306.

Remarque – Cet onglet est uniquement disponible pour les modèles Créer un utilisateur et Mettre à jour l'utilisateur.

Pour modifier les données d'un compte utilisateur pendant l'exécution du flux de travaux, vous pouvez utiliser l'onglet Transformations des données pour indiquer la façon dont Identity Manager devra transformer les données pendant le provisioning.

Par exemple, si vous voulez que les formulaires et les règles génèrent des adresses e-mail conformes à la stratégie de l'entreprise ou si vous voulez générer les dates d'ouverture ou de clôture.

Lorsque vous sélectionnez l'onglet Transformations des données, la page suivante s'affiche.

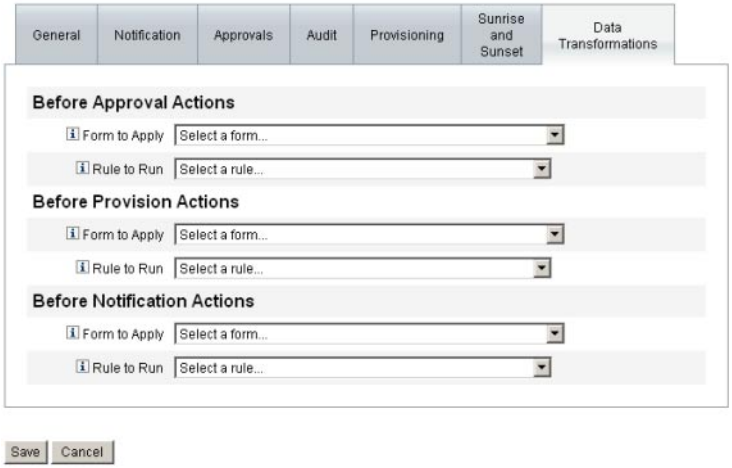


FIGURE 9–29 Onglet Transformations des données : Créer un modèle utilisateur

Cette page se compose des sections suivantes :

- **Actions avant approbation**. Configurez les options de cette section pour transformer les données d'un compte utilisateur avant d'envoyer des demandes d'approbation à des approbateurs spécifiés.
- **Actions avant provisioning**. Configurez les options de cette section pour transformer les données d'un compte utilisateur avant une action de provisioning.
- **Actions avant notification**. Configurez les options de cette section pour transformer les données d'un compte utilisateur avant l'envoi de notifications aux destinataires spécifiés.

Vous pouvez configurer les options suivantes dans chaque section :

- Menus **Formulaire à appliquer** Cette option fournit la liste des formulaires actuellement définis pour votre système. Ces menus permettent de spécifier les formulaires qui seront utilisés pour transformer les données des comptes utilisateur.
- Menus **Règle à appliquer**. Cette option fournit la liste des règles actuellement configurées pour votre système. Ces menus permettent de spécifier les règles qui seront utilisées pour transformer les données des comptes utilisateur.

◆ ◆ ◆ CHAPITRE 10

Journalisation d'audit

Ce chapitre explique la façon dont le système d'audit enregistre les événements.

Les informations sont organisées dans les rubriques suivantes :

Présentation de la journalisation d'audit

L'objectif de l'audit d'Identity Manager est d'enregistrer qui a fait quoi sur quel objet Identity Manager et pour quelle raison.

Les événements de contrôle ou d'audit sont gérés par un ou plusieurs éditeurs. Par défaut, Identity Manager enregistre les événements de contrôle dans le référentiel en utilisant l'éditeur du référentiel. Le filtrage, avec l'aide de groupes d'audit, permet à l'administrateur de sélectionner un sous-ensemble d'événements de contrôle pour les enregistrer. Chaque éditeur peut se voir assigner un ou plusieurs groupes d'audit activés au départ.

Remarque – Pour plus d'informations sur le contrôle et la gestion des violations commises par les utilisateurs, voir le Chapitre 13, "Audit des identités : principes de base".

Rôle de l'audit dans Identity Manager

La plupart de l'audit par défaut est effectué par les composants internes d'Identity Manager. Certaines interfaces permettent toutefois de générer des événements à partir de flux de travaux ou de code Java.

L'instrumentation d'audit par défaut d'Identity Manager est concentrée sur quatre zones principales :

- **L'approvisionneur**. Un composant interne connu sous le nom d'approvisionneur peut gérer des événements de contrôle.
- **Les gestionnaires de vues**. Dans l'architecture de type vue, le gestionnaire de vues génère des enregistrement d'audit. Un gestionnaire de vues doit toujours contrôler quand des objets sont créés ou modifiés.
- **La session**. Les méthodes de session (par exemple `checkinObject`, `createObject`, `runTask`, `login` et `logout`) créent un enregistrement d'audit après avoir terminé une opération auditable. La plupart de l'instrumentation est poussée dans les gestionnaires de vues.
- **Le flux de travaux**. Par défaut, seuls les flux de travaux d'approbation sont instrumentés pour générer des enregistrements d'audit. Ils génèrent un événement de contrôle lorsque les demandes sont approuvées ou rejetées. L'interfaçage avec la fonctionnalité de flux de travaux du journal d'audit se fait au travers de l'application `com.waveset.session.WorkflowServices`. Pour plus d'informations, voir la section suivante.

Création d'événements de contrôle à partir des flux de travaux

Par défaut, seuls les flux de travaux d'approbation sont instrumentés pour générer des enregistrements d'audit. Cette section décrit l'utilisation de l'application `com.waveset.session.WorkflowServices` pour générer des événements de contrôle supplémentaires à partir de tout processus de flux de travaux.

Des événements de contrôle supplémentaires peuvent être nécessaires si vous devez effectuer des rapports sur des flux de travaux personnalisés. Pour toute information sur l'ajout d'événements de contrôle aux flux de travaux, voir "Modification des flux de travaux pour consigner les événements de contrôle standard" à la page 344.

Des événements de contrôle spéciaux peuvent aussi être ajoutés aux flux de travaux en appui des rapports de flux de travaux ("Rapports de flux de travaux" à la page 287). Les rapports de flux de travaux rapportent le temps employé par les flux de travaux pour se compléter. Des événements de contrôle spéciaux sont requis pour stocker les données nécessaires au calcul de

cette durée. Pour toute information sur l'ajout d'événements de contrôle de synchronisation aux flux de travaux, voir "Modification des flux de travaux pour consigner les événements de synchronisation standard" à la page 345.

L'application `com.waveset.session.WorkflowServices`

L'application `com.waveset.session.WorkflowServices` génère des événements de contrôle à partir de tout processus de flux de travaux. Le Tableau 10–1 détaille les arguments disponibles pour cette application.

TABLEAU 10–1 Arguments de `com.waveset.session.WorkflowServices`

Argument	Type	Description
`op`	Chaîne	Opération pour WorkflowServices. Doit être défini sur `audit` ou `auditWorkflow`. Utilisez `audit` pour le contrôle de flux de travaux standard. Utilisez `auditWorkflow` pour stocker les événements de contrôle de synchronisation requis pour les calculs de durée. Obligatoire.
`type`	Chaîne	Nom du type d'objets en cours d'audit. Les types d'objets auditables sont listés dans le Tableau B–5. Obligatoire pour consigner les événements de contrôle standard.
`action`	Chaîne	Nom de l'action effectuée. Les actions auditables sont listées dans le Tableau B–6. Obligatoire.
`status`	Chaîne	Nom du statut pour l'action spécifiée. Le statut est listé dans le Tableau B–7 (dans la colonne Résultats). Obligatoire pour consigner les événements de contrôle standard.
`name`	Chaîne	Nom de l'objet concerné par l'action spécifiée. Obligatoire pour consigner les événements de contrôle standard.
`resource`	Chaîne	(*facultatif*) Nom de la ressource où réside l'objet qui est changé.
`accountId`	Chaîne	(*facultatif*) ID de compte modifié. Doit être un nom de compte de ressource natif.
`error`	Chaîne	(*facultatif*) Chaîne d'erreur localisée accompagnant toute défaillance.
`reason`	Chaîne	(*facultatif*) Nom de l'objet ReasonDenied, qui mappe vers un message internationalisé décrivant les causes des défaillances courantes.
`attributes`	Mappe	(*facultatif*) Mappe des noms et valeurs d'attribut qui ont été ajoutés ou modifiés.
`parameters`	Mappe	(*facultatif*) Mappe jusqu'à cinq noms ou valeurs supplémentaires pertinents pour un événement.

TABLEAU 10–1 Arguments de `com.waveset.session.WorkflowServices` *(Suite)*

Argument	Type	Description
`organizations`	Liste	(*facultatif*) Liste des noms ou ID d'organisation où cet événement sera placé. Cet argument est utilisé pour le calcul de l'étendue organisationnelle du journal d'audit. S'il est absent, le gestionnaire tentera de résoudre l'organisation sur la base du type et du nom. Si la résolution est impossible, l'événement est placé dans Haut (plus haut niveau de la hiérarchie des organisations).
`originalAttributes`	Mappe	(*facultatif*) Mappe des anciennes valeurs d'attribut. Les noms doivent correspondre à ceux listés dans l'argument attributes. Les valeurs seront les valeurs précédentes que vous voulez enregistrer dans le journal d'audit.

Modification des flux de travaux pour consigner les événements de contrôle standard

Pour créer un événement d'audit standard dans un flux de travaux, ajoutez l'élément `<Activity>` suivant à ce flux de travaux.

```
<Activity name='createEvent'>
```

Ensuite, imbriqué dans l'élément `<Activity>`, incluez un élément `<Action>` qui référencie l'application `com.waveset.session.WorkflowServices` :

```
<Action class='com.waveset.session.WorkflowServices'>
```

Imbriqué dans l'élément `<Action>`, incluez les éléments `<Argument>` obligatoires et optionnels. Pour la liste des arguments, voir le Tableau 10–1.

Pour consigner les événements de contrôle standard, l'argument `op` doit être sur défini sur `audit`.

Les "Exemples de flux de travaux" à la page 344 montrent le code minimum requis pour créer un événement de contrôle standard.

Exemples de flux de travaux

L'exemple suivant illustre une activité de flux de travaux simple et montre la génération d'un événement qui enregistrera une activité de suppression de ressource nommée `ADSIResource1`, effectuée par `ResourceAdministrator`.

EXEMPLE 10–1 Activité de flux de travaux simple

```
<Activity name='createEvent'> <Action class='com.waveset.session.WorkflowServices'>
<Argument name='op' value='audit'/> <Argument name='type' value='Resource'/>
<Argument name='action' value='Delete'/> <Argument name='status' value='Success'/>
<Argument name='subject' value='ResourceAdministrator'/>
<Argument name='name' value='ADSIResource1'/> </Action> <Transition to='end'/> </Activity>
```

Les exemples suivants illustrent la façon dont vous pouvez ajouter des attributs spécifiques à un flux de travaux qui suit les modifications appliquées par chaque utilisateur dans un processus d'approbation à un niveau granulaire. Cette addition suivra normalement une `ManualAction` sollicitant une saisie d'un utilisateur.

`ACTUAL_APPROVER` est défini dans le formulaire et dans le flux de travail (si l'approbation se fait depuis le tableau des approbations) sur la base de la personne qui a effectivement effectué l'approbation. `APPROVER` identifie la personne à qui l'approbation a été assignée.

EXEMPLE 10–2 Attributs ajoutés pour suivre les changements dans un processus d'approbation

```
<Action name='Audit the Approval' application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='audit'/> <Argument name='type' value='User'/>
<Argument name='name' value='$(CUSTOM_DESCRIPTION)'/> <Argument name='action' value='approve'/>
<Argument name='accountId' value='$(accountId)'/> <Argument name='status' value='success'/>
<Argument name='resource' value='$(RESOURCE_IF_APPLICABLE)'/>
<Argument name='loginApplication' value='$(loginApplication)'/>
<Argument name='attributes'> <map>
<s>fullname</s><ref>user.accounts[Lighthouse].fullname</ref>
<s>jobTitle</s><ref>user.accounts[Lighthouse].jobTitle</ref>
<s>location</s><ref>user.accounts[Lighthouse].location</ref>
<s>team</s><ref>user.waveset.organization</ref> <s>agency</s>
<ref>user.accounts[Lighthouse].agency</ref> </map> </Argument>
<Argument name='originalAttributes'> <map> <s>fullname</s> <s>User's previous fullname</s>
<s>jobTitle</s> <s>User's previous job title</s> <s>location</s> <s>User's previous location</s>
<s>team</s> <s>User's previous team</s> <s>agency</s> <s>User's previous agency</s> </map>
</Argument> <Argument name='attributes'> <map> <s>firstname</s> <s>Joe</s> <s>lastname</s>
<s>New</s> </map> </Argument> <Argument name='subject'> <or> <ref>ACTUAL_APPROVER</ref>
<ref>APPROVER</ref> </or>
</Argument> <Argument name='approver' value='$(APPROVER)'/> </Action>
```

Modification des flux de travaux pour consigner les événements de synchronisation standard

Les flux de travaux peuvent être modifiés pour consigner des événements de contrôle en appui des rapports de flux de travaux ("Rapports de flux de travaux" à la page 287). Les événements de contrôle standard se limitent à consigner qu'un événement s'est produit tandis que les

événements de contrôle de synchronisation consignent le démarrage et l'arrêt d'un événement ce qui permet d'effectuer des calculs de durée. En plus des données des événements de synchronisation, la plupart des informations enregistrées par les événements de contrôle standard sont également enregistrées. Pour plus d'informations, voir "Informations stockées par les événements de contrôle de synchronisation" à la page 347.

Remarque – Pour consigner les événements de contrôle de synchronisation, vous devez commencer par activer le contrôle du flux de travaux pour chacun des types de flux de travaux que vous envisagez de contrôler.

- Pour les flux de travaux que vous pouvez configurer dans l'interface Administrateur en utilisant les modèles de tâches, commencez par activer le modèle de tâche correspondant au flux de travaux à contrôler. Pour les instructions, voir "Activation des modèles de tâches" à la page 301.

  Activez ensuite le contrôle des flux de travaux en sélectionnant la case à cocher Contrôler l'intégralité du flux de travaux. Pour les instructions, voir "Configuration de l'onglet Vérification informatique " à la page 330.
- Pour les flux de travaux qui n'ont pas de modèles de tâches, définissez une variable nommée `auditWorkflow` et définissez-en la valeur sur `true`.

Sachez toutefois que l'audit des flux de travaux dégrade la performance.

L'Exemple 10–3 indique le code nécessaire pour créer des événements de contrôle de synchronisation. Pour consigner les événements de contrôle de synchronisation, l'argument `op` doit être sur défini sur `auditWorkflow`.

L'argument `action` est également obligatoire et doit être défini sur l'une des valeurs suivantes :

- `StartWorkflow`
- `EndWorkflow`
- `StartProcess`
- `EndProcess`
- `StartActivity`
- `EndActivity`

Des arguments d'action supplémentaires peuvent être définis dans `auditconfig.xml`.

Exemples : Démarrage et arrêt des événements de contrôle dans un flux de travail

L'Exemple 10–3 illustre l'activation des événements de contrôle de synchronisation dans un flux de travaux. Pour instrumenter un flux de travaux, les événements `auditWorkflow` doivent être ajoutés au début et à la fin des flux de travaux, processus et activités.

L'opération `auditWorkflow` est définie dans `com.waveset.session.WorkflowServices` . Pour plus d'informations, voir la section "L'application `com.waveset.session.WorkflowServices`" à la page 343.

EXEMPLE 10–3 Démarrage des événements de contrôle de synchronisation dans un flux de travaux

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/>
<Argument name='action' value='StartWorkflow'/>
</Action>
```

Pour arrêter la consignation des événements de contrôle de synchronisation dans un flux de travaux, ajoutez le code de l'Exemple 10–4 à une activité `pre-end` près de la conclusion du flux de travaux. Sachez que lors de l'instrumentation d'un flux de travaux ou d'un processus, vous n'êtes pas autorisé à mettre quoi que soit dans une activité `end`. Vous devez créer une activité `pre-end` qui effectue l'événement `auditWorkflow` final et passe sans conditions à l'événement `end`.

EXEMPLE 10–4 Arrêt des événements de contrôle de synchronisation dans un flux de travaux

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/> <Argument name='action' value='EndWorkflow'/>
</Action>
```

Informations stockées par les événements de contrôle de synchronisation

Par défaut, les événements de contrôle de synchronisation consignent la plupart des informations stockées par les événements de contrôle standard, notamment les attributs suivants :

Attribut	Description
`WORKFLOW`	Nom du flux de travaux en cours d'exécution
`PROCESS`	Nom du processus courant en cours d'exécution
`INSTANCEID`	ID d'instance unique du flux de travaux en cours d'exécution
`ACTIVITY`	Activité dans laquelle l'événement est consigné
`MATCH`	Identificateur unique au sein d'une instance de flux de travaux

Les attributs ci-dessus sont stockés dans le tableau `logattr` et sont issus de `auditableAttributesList`. Identity Manager vérifie également si l'attribut `workflowAuditAttrConds` est défini.

Il est possible d'appeler plusieurs fois certaines activités au sein d'une unique instance de processus ou flux de travaux. Pour faire correspondre les événements de contrôle pour une instance d'activité donnée, Identity Manager stocke un identificateur unique au sein d'une instance de flux de travaux dans le tableau `logattr`.

Pour stocker des attributs supplémentaires dans le tableau `logattr` d'un flux de travaux, vous devez définir une liste `workflowAuditAttrConds`, que l'on assume être une liste de `GenericObjects`. Si vous définissez un attribut `attrName` dans la liste `workflowAuditAttrConds`, Identity Manager extrait `attrName` de l'objet dans le code, d'abord en utilisant `attrName` en tant que clé puis en stockant la valeur d'`attrName`. L'ensemble des clés et valeurs sont stockées sous forme de valeurs en majuscules.

Configuration d'audit

La configuration d'audit est composée de un ou plusieurs éditeurs et de plusieurs groupes prédéfinis.

Un groupe d'audit définit un sous-ensemble des événements de contrôle sur la base des types d'objets, actions et résultats des actions. Chaque éditeur se voit assigner un ou plusieurs groupes d'audit. Par défaut, l'éditeur du référentiel est assigné à tous les groupes d'audit.

Un éditeur d'audit délivre des événements de contrôle à une destination d'audit particulière. L'éditeur de référentiel par défaut écrit les enregistrements d'audit dans le référentiel. Tout éditeur d'audit peut avoir des options spécifiques à l'implémentation. Les éditeurs d'audit peuvent avoir un programme de formatage assigné (les programmes de formatage assurent la représentation textuelle des événements de contrôle).

L'objet Configuration d'audit (`#ID#Configuration:AuditConfiguration`) est défini dans le fichier `sample/auditconfig.xml`. Cet objet Configuration a une extension qui est un objet générique.

Au niveau supérieur, cet objet Configuration a les attributs suivants :

- "Attribut `filterConfiguration`" à la page 348,
- "L'attribut `extendedTypes`" à la page 354,
- "L'attribut `extendedActions`" à la page 356,
- "L'attribut `extendedResults`" à la page 356,
- "L'attribut `publishers`" à la page 357.

Attribut `filterConfiguration`

L'attribut `filterConfiguration` liste les groupes d'événements, utilisés pour permettre à un ou plusieurs événements de passer à travers le filtre d'événements. Chacun des groupes listés dans l'attribut `filterConfiguration` contient les attributs listés dans le Tableau 10–2.

TABLEAU 10–2 Attributs de `filterConfiguration`

Attribut	Type	Description
`groupName`	Chaîne	Nom du groupe d'événements
`displayName`	Chaîne	Clé du catalogue de messages représentant le nom du groupe
`enabled`	Chaîne	Indicateur booléen indiquant si l'ensemble du groupe est activé ou désactivé. L'attribut est une optimisation pour l'objet de filtrage.
`enabledEvents`	Liste	Liste d'objets génériques décrivant les événements activés par un groupe. Un événement doit être listé pour en permettre la consignation. Chaque objet listé doit avoir les attributs suivants : ■ `objectType` (Chaîne) : nom`objectType` ; ■ `actions` (Liste) : liste d'une ou plusieurs actions ; ■ `results` (Liste) : liste d'un ou plusieurs résultats.

L'Exemple 10–5 illustre le groupe Gestion des ressources (Resource Management) par défaut.

EXEMPLE 10–5 Le groupe Gestion des ressources (Resource Management) par défaut

```
<Object name='Resource Management'> <Attribute name='enabled' value='true'/>
<Attribute name='displayName' value='UI_RESOURCE_MGMT_GROUP_DISPLAYNAME'/>
<Attribute name='enabledEvents'> <List> <Object> <Attribute name='objectType' value='Resource'/>
<Attribute name='actions' value='ALL'/> <Attribute name='results' value='ALL'/> </Object> <Object>
<Attribute name='objectType' value='ResourceObject'/> <Attribute name='actions' value='ALL'/>
<Attribute name='results' value='ALL'/> </Object> </List> </Attribute> </Object>
```

Identity Manager fournit des groupes d'événements de contrôle par défaut. Ces groupes et les événements qu'ils autorisent sont décrits dans les sections suivantes :

- “Groupe Gestion des comptes” à la page 350,
- “Groupe Modifications hors Identity System” à la page 350,
- “Groupe Gestion de la conformité” à la page 351,
- “Groupe Gestion de la configuration” à la page 351,
- “Groupe Gestion d'événement” à la page 352,
- “Groupe Connexions/Déconnexions” à la page 352,
- “Groupe Gestion des mots de passe” à la page 352,
- “Groupe Gestion des ressources” à la page 353,
- “Groupe Gestion des rôles” à la page 353,
- “Groupe Gestion de la sécurité” à la page 353,
- “Groupe Service Provider” à la page 354,
- “Groupe Gestion des tâches” à la page 354.

Vous pouvez configurer des groupes d'événements de contrôle à partir de la page Configuration d'audit de l'interface administrateur d'Identity Manager (Configurer > Vérification informatique). Pour les instructions, voir "Configuration de groupes et d'événements d'audit" à la page 111.

Vous pouvez aussi configurer les événements de type réussite et échec pour chaque groupe toujours à partir de la page Configuration d'audit. L'interface ne prend pas en charge l'ajout ou la modification d'événements pour les groupes, mais vous pouvez le faire en utilisant les pages de débogage d'Identity Manager ("Page de débogage d'Identity Manager" à la page 45).

Remarque – Certaines actions que vous pouvez choisir pour un audit ne génèrent pas d'enregistrement de journal.. De même, sélectionner l'option « All Actions » (Toutes les actions) ne signifie pas que toutes les actions listées sont disponibles ou possibles pour tous les groupes d'événements de contrôle.

Groupe Gestion des comptes

Ce groupe est activé par défaut.

TABLEAU 10–3 Groupes d'événements Gestion des comptes par défaut

Type	Actions
`Encryption Key` (Clé de chiffrement)	Toutes les actions.
`Identity System Account` (Compte Identity System)	Toutes les actions.
`Resource Account` (Compte de ressources)	Activer, Approuver, Créer, Désactiver, Déverrouiller, Modifier, Rejeter, Renommer, Supprimer
`Workflow Case` (Case flux de travaux)	Démarrer l'activité, Démarrer le flux de travaux, Démarrer le processus, Terminer l'activité, Terminer le flux de travaux, Terminer le processus
`User` (Utilisateur)	Activer, Approuver, Créer, Désactiver, Modifier, Rejeter, Renommer, Supprimer

Groupe Modifications hors Identity System

Ce groupe est désactivé par défaut.

TABLEAU 10–4 Groupes d'événements et événements de Modifications hors Identity Manager

Type	Actions
`ResourceAccount` (Compte de ressource)	`NativeChange`

Groupe Gestion de la conformité

Ce groupe est activé par défaut.

TABLEAU 10–5 Événements du groupe Gestion de la conformité par défaut

Type	Actions
`Audit Policy` (Stratégie d'audit)	Toutes les actions.
`AccessScan` (Scannage des accès)	Toutes les actions.
`ComplianceViolation` (ComplianceViolation)	Toutes les actions.
`Data Exporter` (Exportateur de données)	Toutes les actions.
`UserEntitlement` (UserEntitlement)	Approuvé par l'attestateur, Arrêter, Nouveau scannage requis, Rejeté par l'attestateur, Résolution demandée
`Access Review Workflow` (Flux de travaux de l'examen des accès)	Toutes les actions.
`Remediation Workflow` (Flux de travaux de résolution)	Toutes les actions.

Groupe Gestion de la configuration

Ce groupe est activé par défaut.

TABLEAU 10–6 Groupes d'événements de Gestion de la configuration par défaut

Type	Actions
`Configuration` (Configuration)	Toutes les actions.
`UserForm` (Formulaire utilisateur)	Toutes les actions.

TABLEAU 10–6 Groupes d'événements de Gestion de la configuration par défaut *(Suite)*

Type	Actions
`Rule` (Règle)	Toutes les actions.
`EmailTemplate` (Modèle d'e-mail)	Toutes les actions.
`LoginConfig` (Config. de connexion)	Toutes les actions.
`Policy` (Stratégie)	Toutes les actions.
`XmlData` (Données XML)	Importer
`Log` (Journal)	Toutes les actions.

Groupe Gestion d'événement

Ce groupe est activé par défaut.

TABLEAU 10–7 Groupes d'événements de Gestion d'événement par défaut

Type	Actions
`Email` (E-mail)	Notifier
`TestNotification` (Notification de test)	Notifier

Groupe Connexions/Déconnexions

Ce groupe est activé par défaut.

TABLEAU 10–8 Groupes d'événements de Connexions/Déconnexions d'Identity Manager par défaut

Type	Actions
`User` (Utilisateur)	Connexion, Déverrouiller, Fermer la session, Informations d'identification expirées, Récupération du nom d'utilisateur, Verrouiller

Groupe Gestion des mots de passe

Ce groupe est activé par défaut.

TABLEAU 10–9 Groupes d'événements et événements de Gestion des mots de passe par défaut

Type	Actions
Compte de ressources	Modifier le mot de passe, Réinitialiser le mot de passe

Groupe Gestion des ressources

Ce groupe est activé par défaut.

TABLEAU 10–10 Groupes d'événements et événements de Gestion des ressources par défaut

Type	Actions
`Resource` (Ressource)	Toutes les actions.
`Resource Object` (Objet de ressource)	Toutes les actions.
`ResourceForm` (Formulaire de ressource)	Toutes les actions.
`ResourceAction` (Action de ressource)	Toutes les actions.
`AttrParse` (AttrParse)	Toutes les actions.
`Workflow Case` (Case flux de travaux)	Démarrer l'activité, Démarrer le flux de travaux, Démarrer le processus, Terminer l'activité, Terminer le flux de travaux, Terminer le processus

Groupe Gestion des rôles

Ce groupe est désactivé par défaut.

TABLEAU 10–11 Groupes d'événements et événements de Gestion des rôles par défaut

Type	Actions
`Role` (Rôle)	Toutes les actions.

Groupe Gestion de la sécurité

Ce groupe est activé par défaut.

TABLEAU 10–12 Groupes d'événements et événements de Gestion de la sécurité par défaut

Type	Actions
`Capability` (Capacité)	Toutes les actions.
`EncryptionKey` (Clé de chiffrement)	Toutes les actions.
`Organization` (Organisation)	Toutes les actions.
`Admin Role` (Rôle Admin)	Toutes les actions.

Groupe Service Provider

Ce groupe est activé par défaut.

TABLEAU 10–13 Groupes d'événements et événements de Service Provider

Type	Actions
`Directory User` (Utilisateur du répertoire)	Créer, Légende post-opération, Légende pré-opération, Mettre à jour les réponses d'authentification, Modifier, Récupération du nom d'utilisateur, Réponse de repêchage, Supprimer

Groupe Gestion des tâches

Ce groupe est désactivé par défaut.

TABLEAU 10–14 Groupes d'événements et événement de Gestion des tâches par défaut

Type	Actions
`TaskInstance` (Instance de tâche)	Toutes les actions.
`TaskDefinition` (Définition de tâches)	Toutes les actions.
`TaskSchedule` (Planification de la tâche)	Toutes les actions.
`TaskResult` (Résultat de la tâche)	Toutes les actions.
`ProvisioningTask` (Tâche de provisioning)	Toutes les actions.

L'attribut `extendedTypes`

Tout nouveau type ajouté à la classe `com.waveset.object.Type` peut être contrôlé. Une clé de base de données unique composée de deux caractères et stockée dans la base de données doit être assignée à tout nouveau type. Tous les nouveaux types sont ajoutés aux diverses interfaces de génération de rapports d'audit. Tout nouveau type devant être consigné dans la base de données sans être filtré doit être ajouté à l'attribut `enabledEvents` d'un groupe d'événements de contrôle (comme décrit dans la section relative à l'attribut `enabledEvents`).

Vous pouvez dans certains cas vouloir contrôler un élément associé à aucun `com.waveset.object.Type` ou représenter un type existant avec une granularité plus poussée.

Par exemple, l'objet `WSUser` stocke l'ensemble des informations de compte de l'utilisateur dans le référentiel. Au lieu de marquer chaque événement comme de type `USER`, le processus d'audit

scinde l'objet `WSUser` en deux types d'audit différents (Compte de ressource et Compte Identity Manager). Scinder l'objet de cette façon facilite la recherche d'informations de compte spécifiques dans le journal d'audit.

Ajoutez des types d'audit étendus en les ajoutant à l'attribut `extendedObjects`. Chaque objet étendu doit avoir les attributs listés dans le tableau suivant.

TABLEAU 10–15 Attributs d'objet étendus

Argument	Type	Description
`name`	Chaîne	Nom du type, est utilisé lors de la construction d'AuditEvents et pendant le filtrage d'événements.
`displayName`	Chaîne	Clé du catalogue de messages représentant le nom du type.
`logDbKey`	Chaîne	Clé de base de données formée de deux caractères à utiliser pour stocker cet objet dans la table du journal. Pour les valeurs réservées, voir "Mappages de la base de données du journal d'audit" à la page 585.
`supportedActions`	Liste	Actions prises en charge par ce type d'objets. Cet attribut sera utilisé pour la création de requêtes d'audit depuis l'interface utilisateur. Si cette valeur est null, toutes les actions seront affichées comme des valeurs possibles à demander pour ce type d'objets.
`mapsToType`	Chaîne	(facultatif) Nom du `com.waveset.object.Type` mappant vers ce type, le cas échéant. Cet attribut est utilisé lors des tentatives de résolution de l'appartenance d'un objet à une organisation si cet élément n'est pas déjà spécifié sur l'événement.
`organizationalMembership`	Liste	(facultatif) Liste par défaut des ID des organisations où les événements de ce type doivent être placés s'ils n'ont pas déjà une appartenance à une organisation assignée.

Toutes les clés spécifiques au client doivent commencer par le symbole # pour éviter tout doublon en cas d'ajout de nouvelles clés internes.

L'Exemple 10–6 illustre le type étendu Compte Identity Manager.

EXEMPLE 10–6 Type étendu Compte Identity Manager

```
<Object name='LighthouseAccount'> <Attribute name='displayName' value='LG_LIGHTHOUSE_ACCOUNT'/>
<Attribute name='logDbKey' value='LA'/> <Attribute name='mapsToType' value='User'/>
<Attribute name='supportedActions'> <List> <String>Disable</String> <String>Enable</String>
<String>Create</String> <String>Modify</String> <String>Delete</String> <String>Rename</String>
</List> </Attribute> </Object>
```

L'attribut extendedActions

Les actions d'audit mappent normalement vers des objets com.waveset.security.Right. Lorsque vous ajoutez de nouveaux objets Right (droit), vous devez spécifier une logDbKey de deux caractères, qui sera stockée dans la base de données. Vous pouvez rencontrer des cas de figure dans lesquels il n'y a pas de droit correspondant à une action particulière devant être contrôlée. Vous pouvez étendre les actions en les ajoutant à la liste d'objets de l'attribut extendedActions.

Chaque objet extendedActions doit comprendre les attributs listés dans le Tableau 10–16.

TABLEAU 10–16 Attributs de extendedAction

Attribut	Type	Description
name	Chaîne	Nom de l'action, est utilisé lors de la construction d'AuditEvents et pendant le filtrage d'événements.
displayName	Chaîne	Clé du catalogue de messages représentant le nom de l'action.
logDbKey	Chaîne	Clé de base de données formée de deux caractères à utiliser pour stocker cette action dans le tableau du journal. Pour les valeurs réservées, voir "Mappages de la base de données du journal d'audit" à la page 585.

Toutes les clés spécifiques au client doivent commencer par le symbole # pour empêcher tout doublon en cas d'ajout de nouvelles clés internes.

Le Tableau 10–16 illustre l'ajout d'une action pour Fermer la session.

EXEMPLE 10–7 Ajout d'une action pour Fermer la session

```
<Object name='Logout'> <Attribute name='displayName' value='LG_LOGOUT'/>
<Attribute name='logDbKey' value='LO'/> </Object>
```

L'attribut extendedResults

En plus d'étendre les types et les actions d'audit, vous pouvez ajouter des résultats. Par défaut, il y a deux résultats : *Réussite* et *Échec*. Vous pouvez étendre les résultats en en ajoutant à la liste d'objets de l'attribut extendedResults.

Chaque objet extendedResults doit comprendre les attributs listés dans le Tableau 10–17.

TABLEAU 10–17 Attributs de `extendedResults`

Attribut	Type	Description
`name` (nom)	Chaîne	Nom du résultat, est utilisé lors de la définition du statut sur activé.
`displayName` (Nom à afficher)	Chaîne	Clé du catalogue de messages représentant le nom d'un résultat.
`logDbKey`	Chaîne	Clé de base de données formée de un caractère à utiliser pour stocker ce résultat dans le tableau du journal. Pour les valeurs réservées, voir la section intitulée Clés de la base de données.

Toutes les clés spécifiques au client doivent commencer par la plage 0–9 pour empêcher tout doublon en cas d'ajout de nouvelles clés internes.

L'attribut `publishers`

Tous les éléments de la liste `publishers` sont des objets génériques. Chaque objet `publishers` a les attributs suivants.

TABLEAU 10–18 Attributs de `publishers`

Attribut	Type	Description
`class` (Classe)	Chaîne	Nom de la classe de l'éditeur.
`displayName` (Nom à afficher)	Chaîne	Clé du catalogue de messages représentant le nom de l'éditeur.
`description` (Description)	Chaîne	Description de l'éditeur.
`filters` (Filtres)	Liste	Liste des groupes d'audit assignés à cet éditeur.
`formatter` (Programme de formatage)	Chaîne	Nom du programme de formatage (le cas échéant).
`options` (Options)	Liste	Liste des options de l'éditeur. Ces options sont spécifiques à l'éditeur ; chaque élément de la liste est une représentation de mappe de `PublisherOption`. Voir exemples dans `sample/auditconfig.xml`.

Schéma de la base de données

Deux tables du référentiel d'Identity Manager sont utilisées pour stocker les données d'audit :

- `waveset.log` stocke les détails des événements ;
- `waveset.logattr` stocke les ID des organisations auxquelles appartiennent les différents événements.

Ces tables sont examinées au début de cette section.

Lorsque les données du journal d'audit dépassent les limites de longueur de colonne spécifiées pour les tables ci-dessus, Identity Manager tronque les données pour respecter ces limites. La troncature du journal d'audit fait l'objet de la section "Troncation du journal d'audit" à la page 361.

Certaines colonnes du journal d'audit ont des limites de longueur configurables. Pour savoir quelles sont ces colonnes et apprendre à en changer la longueur limite, voir "Configuration du journal d'audit" à la page 361.

Table `waveset.log`

Cette section décrit les différents noms de colonnes et types de données figurant dans la table `waveset.log`. Les types de données sont issus de la définition de la base de données Oracle et varient légèrement d'une base de données à l'autre. Pour la liste des valeurs de schéma pour toutes les bases de données prises en charge, voir l'Annexe B, "Schéma de la base de données du journal d'audit"

Quelques-unes des valeurs des colonnes sont stockées sous forme de clés dans la base de données pour optimiser l'espace. Pour la définition des clés, voir la section intitulée "Mappages de la base de données du journal d'audit" à la page 585.

- `objectType CHAR(2)` : clé de deux caractères représentant le type d'objets qui est contrôlé.
- `action CHAR(2)` : clé de deux caractères représentant l'action qui a été effectuée.
- `actionStatus CHAR(1)` : clé de un caractère représentant le résultat de l'action qui a été effectuée.
- `reason CHAR(2)` : clé de deux caractères décrivant l'objet `ReasonDenied` en cas d'échec. `ReasonDenied` est une classe qui enveloppe une entrée du catalogue de messages et est utilisée pour les échecs courants tels que des informations d'authentification non valables et des privilèges insuffisants.
- `actionDateTimeVARCHAR(21)` : date et heure auxquelles l'action ci-dessus a eu lieu. La valeur est stockée en heure GMT.
- `objectName VARCHAR(128)` : nom de l'objet qui fait l'objet d'une action pendant une opération.

- `resourceName VARCHAR(128)` : nom de la ressource qui a été utilisée pendant une opération, le cas échéant. Certains événements ne référencient pas les ressources ; cependant, dans de nombreux cas, cet élément donne davantage de détails pour consigner la ressource où une opération a été effectuée.
- `accountName VARCHAR(255)` : ID du compte objet de l'action en cours, le cas échéant.
- `server VARCHAR(128)` : serveur sur lequel l'action a été effectuée (automatiquement assigné par le journal d'événements).
- `message VARCHAR(255*)` ou `CLOB` : tout message localisé associé à une action incluant des éléments tels que des messages d'erreur. Le texte est stocké localisé et ne sera donc pas internationalisé. La limite de longueur de cette colonne est configurable. Le type de données par défaut est `VARCHAR` et la limite de taille par défaut est 255. Pour plus d'informations sur le réglage de la taille limite, voir "Configuration du journal d'audit" à la page 361.
- `interface VARCHAR(50)` : interface d'Identity Manager (par exemple l'interface administrateur, utilisateur, IVR ou SOAP) depuis laquelle l'opération a été effectuée.
- `acctAttrChanges VARCHAR(4000)` à `CLOB` : stocke les attributs de compte qui ont changé au cours d'une création et d'une mise à jour. Le champ des changements d'attributs est toujours rempli lors d'une création ou d'une mise à jour pour un objet compte de ressource ou compte Identity Manager. Tous les attributs modifiés pendant une action sont stockés dans ce champ sous la forme d'une chaîne. Les données adoptent le format `NAME=VALUE NAME2=VALUE2`. Ce champ peut être interrogé en exécutant des instructions SQL « `contains` » (contient) portant sur le nom ou la valeur.

  L'exemple de code suivant illustre une valeur dans la colonne `acctAttrChanges`.

```
COMPANY="COMPANY" DEPARTMENT="DEPT" DESCRIPTION="DSMITH DESCRIPTION"
FAX NUMBER="5122222222" HOME ADDRESS="12282 MOCKINGBIRD LANE" HOME CITY="AUSTIN"
HOME PHONE="5122495555" HOME STATE="TX" HOME ZIP="78729" JOB TITLE="DEVELOPER"
MOBILE PHONE="5125551212" WORK PHONE="5126855555" EMAIL="someone@somecompany.COM"
EXPIREPASSWORD="TRUE" FIRSTNAME="DANIEL" FULLNAME="DANIEL SMITH" LASTNAME="SMITH"
```

Remarque – Si votre installation d'Identity Manager utilise un référentiel Oracle et que vous remarquez des erreurs de troncature dans le journal d'audit, vous pouvez convertir le champ `accountAttrChanges` de la table du journal d'audit de `VARCHAR(4000)` à `CLOB`. Identity Manager fournit un exemple de script DDL, dans le répertoire `/web/sample` , qui convertit `log.acctAttrChanges` de `VARCHAR(4000)` en `CLOB`. Le script `convert_log_acctAttrChangesCHAR2CLOB.oracle.sql` préserve les données existantes et autorise plus de 4000 caractères dans le champ `accountAttrChanges`.

Cette conversion est optionnelle et ne doit être effectuée que si vous remarquez des erreurs de troncature. Veillez par ailleurs à sauvegarder les tables concernées avant de lancer le script de conversion.

Après avoir exécuté le script de conversion, arrêtez et redémarrez votre serveur d'application Web. Tout nouveau rapport exécuté devrait s'afficher correctement.

- `acctAttr01label-acctAttr05label VARCHAR(50)` : ces cinq emplacements `NAME` supplémentaires sont des colonnes pouvant promouvoir jusqu'à cinq noms d'attributs stockés chacun dans une colonne propre au lieu de l'être dans le grand blob. Vous pouvez promouvoir un attribut depuis la page Resource Schema Configuration (Configuration du schéma des ressources) en utilisant le réglage « `Vérification informatique ?` » : l'attribut sera alors disponible pour l'exploration de données.
- `acctAttr01value-acctAttr05value VARCHAR(128)` : ces cinq emplacements `VALUE` supplémentaires peuvent promouvoir jusqu'à cinq valeurs d'attributs stockées chacune dans une colonne propre au lieu de l'être dans le grand blob.
- `parm01label-parm05label VARCHAR(50)` : cinq emplacements utilisés pour stocker des paramètres associés à un événement. Des exemples de ces paramètres sont les noms IP du client et ID de la session.
- `parm01value-parm05value VARCHAR(128*)` ou `CLOB` : cinq emplacements utilisés pour stocker les paramètres associés à un événement. Par exemple, les valeurs d'IP du client et ID de la session. La limite de longueur de ces colonnes est configurable. Le type de données par défaut est `VARCHAR` et la limite de taille par défaut est 128. Pour plus d'informations sur le réglage de la taille limite, voir “Configuration du journal d'audit” à la page 361.
- `id VARCHAR(50)` : ID unique assigné à chaque enregistrement par le référentiel référencé dans la table `waveset.logattr`.
- `name VARCHAR(128)` : nom généré assigné à chaque enregistrement.
- `xml BLOB` : est utilisé en interne par Identity Manager.

La table waveset.logattr

La table waveset.logattr est utilisée pour stocker les ID d'appartenance organisationnelle pour chaque événement, élément utilisé pour établir l'étendue du journal d'audit par organisation.

- id VARCHAR(50) : ID de l'enregistrement waveset.log.
- attrname VARCHAR(50) : actuellement, toujours MEMBEROBJECTGROUPS.
- attrval VARCHAR(255) : ID du groupe MemberObject auquel l'événement appartient.

Troncation du journal d'audit

Lorsqu'une ou plusieurs colonnes de données du journal d'audit dépassent les limites de longueur de colonne spécifiées, les données de la ou des colonnes concernées sont tronquées. Plus précisément, les données sont tronquées à la limite indiquée moins trois caractères. Une ellipse (...) est ensuite ajoutée aux données de la colonne pour indiquer qu'une troncature a été effectuée.

De plus, la colonne NAME de l'enregistrement d'audit en question est précédée de la chaîne #TRUNCATED# pour faciliter l'interrogation des enregistrements tronqués.

Remarque – Identity Manager part du principe que le codage UTF–8 est employé lorsqu'il calcule où tronquer les messages. Si votre configuration utilise un codage autre que l'UTF–8, il est possible que les données tronquées dépassent encore la taille de colonne effective dans votre base de données. Si tel est le cas, le message tronqué ne s'affiche pas dans le journal d'audit et une erreur est écrite dans le journal système.

Configuration du journal d'audit

Certaines colonnes du journal d'audit peuvent être configurées pour stocker de grandes quantités de données dans le référentiel.

Redimensionnement des limites de longueur des colonnes

Plusieurs colonnes du journal d'audit ont des limites de longueur configurables. Ces colonnes sont les suivantes :

- la colonne message ;
- les colonnes parmNNvalue (où NN = 01, 02, 03, 04 ou 05) ;

- la colonne `xml`.

Remarque – Pour la description des colonnes du journal d'audit, voir "Schéma de la base de données" à la page 358.

Les limites de longueur des colonnes peuvent être modifiées en éditant l'objet `RepositoryConfiguration`. Pour les instructions à suivre pour éditer l'objet `RepositoryConfiguration`, voir "Édition des objets Configuration Identity Manager" à la page 118.

- Pour changer la limite de longueur de la colonne `message`, modifiez la valeur `maxLogMessageLength`.
- Pour changer la limite de longueur de la colonne `parmNNvalue`, modifiez la valeur `maxLogParmValueLength`. La même valeur limite s'applique à l'ensemble des cinq colonnes (il n'est pas possible de définir de valeurs de longueur de colonne individuelles).
- Pour changer la limite de longueur de la colonne `xml`, modifiez la valeur `maxLogXmlLength`.

Un redémarrage du serveur est nécessaire pour que les nouvelles valeurs soient appliquées.

Les paramètres de limite de longueur des colonnes figurant dans l'objet `RepositoryConfiguration` déterminent la quantité maximale de données pouvant être stockée dans une colonne. Si les données à stocker dépassent ces paramètres, Identity Manager tronque les premières. Pour plus d'informations, voir "Troncation du journal d'audit" à la page 361.

Si vous augmentez un paramètre de longueur de colonne dans l'objet `RepositoryConfiguration`, vérifiez également que le paramètre de taille de colonne de votre base de données est supérieur ou égal à la taille configurée dans l'objet `RepositoryConfiguration`.

Suppression d'enregistrements dans le journal d'audit

Le journal système doit être tronqué régulièrement afin de ne pas trop devenir trop volumineux. Utilisez la Tâche de maintenance AuditLog pour programmer une tâche qui supprime les anciens enregistrements du journal d'audit.

1. **Dans l'interface administrateur, cliquez sur Tâches du serveur → Gérer la planification.**
2. **Dans la section Tâches disponibles pour planification, cliquez sur Tâche de maintenance AuditLog.**

   La page Créer un nouveau programme de tâches Tâche de maintenance AuditLog s'ouvre.
3. **Remplissez le formulaire et cliquez sur Enregistrer.**

Utilisation d'éditeurs d'audit personnalisés

Identity Manager peut envoyer des événements de contrôle à des éditeurs d'audit personnalisés.

Les éditeurs personnalisés suivants sont fournis :

- **Console**. Imprime les événements de contrôle sur la sortie ou l'erreur standard.
- **Fichier**. Écrit les événements de contrôle dans un fichier simple.
- **JDBC**. Enregistre les événements de contrôle dans un magasin de données JDBC.
- **JMS**. Enregistre les événements de contrôle dans une file d'attente ou une rubrique JMS.
- **JMX**. Publie les événements de contrôle de sorte qu'un client JMX (Java Management Extensions) peut contrôler l'activité du journal d'audit d'Identity Manager.
- **Scripté**. Permet aux scripts personnalisés de stocker les événements de contrôle.

Pour créer votre propre éditeur, voir "Développement d'éditeurs d'audit personnalisés" à la page 371.

Cette section se compose des rubriques suivantes :

▼ Pour activer les éditeurs d'audit personnalisés

Les éditeurs d'audit personnalisés s'activent depuis la page Configuration d'audit.

1. **Dans l'interface administrateur, cliquez sur Tâches du serveur dans le menu principal puis sur Audit dans le menu secondaire.**

   La page Configuration d'audit s'ouvre.

2. **Sélectionnez l'option Utiliser un éditeur personnalisé au bas de la page.**

   Un tableau listant les éditeurs d'audit actuellement configurés s'ouvre.

3. **Pour configurer un nouvel éditeur personnalisé, sélectionnez le type éditeur personnalisé dans le menu déroulant Nouvel éditeur.**

   Complétez le formulaire Configurer le nouvel éditeur d'audit. Cliquez sur OK.

4. **Important ! Cliquez sur Enregistrer pour enregistrer le nouvel éditeur.**

Types d'éditeurs Console, Fichier, JDBC et Scripté

Pour activer les éditeurs d'audit Console, Fichier, JDBC ou Scripté, suivez les étapes de la section "Pour activer les éditeurs d'audit personnalisés" à la page 363. Sélectionnez le type d'éditeur approprié dans le menu déroulant Nouvel éditeur.

Complétez le formulaire Configurer le nouvel éditeur d'audit. Pour toute question sur le formulaire, consultez les i-Helps et l'aide en ligne.

- L'éditeur d'audit Console imprime les événements de contrôle sur la sortie ou l'erreur standard.
- L'éditeur d'audit Fichier écrit les événements de contrôle dans un fichier simple.
- L'éditeur d'audit JDBC enregistre les événements de contrôle dans un magasin de données JDBC.
- L'éditeur d'audit Scripté autorise les scripts personnalisés écrits en JavaScript ou en BeanShell pour stocker les événements de contrôle.

Type d'éditeur JMS

Les éditeurs personnalisés de journal d'audit JMS permettent de publier des enregistrements d'événements de contrôle dans une file d'attente ou une rubrique JMS (Java Message Service).

Avantages de l'utilisation de JMS

Publier sur JMS augmente la flexibilité en matière de corrélation dans les environnements présentant plusieurs serveurs Identity Manager. De plus, JMS peut être utilisé dans des situations caractérisées par des restrictions concernant d'utilisation de l'éditeur de fichier d'audit Fichier, par exemple dans les environnements Windows où le journal peut ne pas être accessible à un outil de génération de rapports client pendant l'exécution du serveur.

JMS offre plusieurs avantages pour les environnements multiserveurs :

- Le magasin des messages JMS centralise (et simplifie) le stockage des messages et leur récupération.
- L'architecture JMS n'impose pas de restrictions quant au nombre de clients pouvant accéder au service.
- Le protocole JMS est facile à envoyer à travers les pare-feu et autres infrastructures réseau.

Point à point ou publication/inscription ?

Java Message System propose deux modèles pour la messagerie : le modèle point à point ou de mise en attente et le modèle publication/inscription ou à rubriques. Identity Manager prend en charge ces deux modèles.

Dans le modèle point à point, un producteur poste les messages dans une file d'attente donnée et un consommateur lit les messages dans cette file d'attente. Ici, le producteur connaît la destination du message qu'il poste directement dans la file d'attente du consommateur.

Le modèle point à point présente les caractéristiques suivantes :

- Un seul consommateur obtient le message.
- Le producteur n'a pas à être en cours d'exécution au moment où le récepteur consomme le message et le récepteur n'a besoin d'être en cours d'exécution au moment où le message est envoyé.
- Le récepteur accuse réception de tout message traité avec succès.

Le modèle publication/inscription, d'autre part, prend en charge la publication de messages dans une rubrique de messages donnée. Zéro abonnés ou plus peuvent se révéler intéressés par recevoir des messages sur une rubrique de messages donnée. Dans ce modèle, l'éditeur et l'abonné ignorent tout l'un de l'autre. Une bonne métaphore pour ce modèle est le panneau d'affichage anonyme.

Le modèle publication/inscription présente les caractéristiques suivantes :

- Plusieurs consommateurs peuvent recevoir les messages.
- Une dépendance de synchronisation existe entre éditeurs et abonnés. L'éditeur doit créer un abonnement pour que les clients puissent s'abonner. Une fois inscrits, les abonnés doivent rester actifs en permanence pour recevoir les messages à moins d'un abonnement durable n'ait été établi. Dans le cas d'un abonnement durable, les messages publiés alors que l'abonné n'est pas connecté sont distribués de nouveau quand ce dernier se reconnecte.

Remarque – Pour plus d'informations sur JMS, voir `http://www.sun.com/software/products/message_queue/index.xml`

Configuration du type d'éditeur JMS

L'éditeur JMS formate les événements de contrôle en messages de texte TextMessages JMS. Ces TextMessages sont ensuite envoyés à une file d'attente ou une rubrique selon la configuration. Les messages de texte peuvent être formatés au format XML ou ULF (Universal Logging Format) selon la configuration.

Pour activer le type d'éditeur JMS, suivez les étapes de la section “Pour activer les éditeurs d'audit personnalisés” à la page 363 et sélectionnez JMS dans le menu déroulant Nouvel éditeur.

Pour configurer le type d'éditeur JMS, complétez le formulaire Configurer le nouvel éditeur d’audit. Pour toute question sur le formulaire, consultez les i-Helps et l'aide en ligne.

Type d'éditeur JMX

L'éditeur de journal d'audit JMX publie les événements de contrôle de sorte qu'un client JMX (Java Management Extensions) peut contrôler l'activité du journal d'audit d'Identity Manager.

Définition de JMX

Java Management Extensions (JMX) est une technologie Java qui permet la gestion et/ou le contrôle des applications, objets système, périphériques et réseaux orientés services. L'entité gérée/contrôlée est représentée par des objets appelés des MBeans (pour Managed Bean, bean géré).

Implémentation de l'éditeur JMX d'Identity Manager

L'éditeur de journal d'audit JMX d'Identity Manager contrôle le journal d'audit à la recherche d'événements. Lorsqu'un événement est détecté, l'éditeur JMX enveloppe l'enregistrement de l'événement de contrôle avec un MBean et met à jour un historique temporaire (qui est conservé en mémoire). Pour chaque événement, une petite notification séparée est envoyée au client JMX. Si l'événement est digne d'intérêt, le client JMX peut interroger le MBean enveloppant l'événement de contrôle pour obtenir des informations supplémentaires.

Remarque – Pour toute information sur les enregistrements d'événements de contrôle, voir la javadoc `com.waveset.object.AuditEvent`. La javadoc est disponible dans le kit REF présenté dans la section "Développement d'éditeurs d'audit personnalisés" à la page 371.

Pour récupérer les informations du MBean approprié, un numéro de séquence d'historique est nécessaire. Ce numéro figure dans la notification de l'événement.

Chaque notification d'événement inclut les informations suivantes :

- **Type** (Type). Chaîne décrivant le type de l'événement. Cette chaîne adopte le format `AuditEvent.<ObjectType>.<Action>` où `ObjectType` et `Action` sont retournés de `com.waveset.AuditEvent`. Par exemple, si un événement de déverrouillage est envoyé, le type est `AuditEvent.LighthouseAccount.Unlock`.
- **SequenceNumber** (Numéro de séquence). Clé du tampon d'historique utilisée pour demander des informations au MBean.

▼ Pour configurer le type d'éditeur JMX

1 **Pour activer le type d'éditeur JMX, suivez les étapes de la section "Pour activer les éditeurs d'audit personnalisés" à la page 363 et sélectionnez JMX dans le menu déroulant Nouvel éditeur.**

2. **Pour configurer le type d'éditeur JMX, complétez le formulaire Configurer le nouvel éditeur d'audit. Pour toute question sur le formulaire, consultez les i-Helps et l'aide en ligne.**
   - **Nom de l'éditeur**. Saisissez un nom unique pour l'éditeur d'événements de contrôle JMX.
   - **Limite de l'historique**. Changez la valeur par défaut comme requis pour spécifier le nombre d'éléments événement que l'éditeur doit conserver en mémoire (la valeur par défaut est 100).
3. **Cliquez sur Essai pour vérifier que le Nom de l'éditeur est acceptable.**
4. **Cliquez sur OK. Le formulaire Configurer le nouvel éditeur d'audit se ferme.**
5. **Important ! Cliquez sur Enregistrer.**

Affichage des événements de contrôle avec un client JMX

Utilisez un client JMX pour afficher l'éditeur JMX. JConsole, qui est inclus dans le JDK 1.5, a été utilisé pour créer les captures d'écran suivantes.

Si vous utilisez JConsole, choisissez attach to process (joindre au processus) pour afficher le MBean `IDM:type=AuditLog`. Pour toute information sur la configuration de JConsole en vue de l'utiliser en tant que client JMX, voir "Viewing JMX Data" du *Sun Identity Manager 8.1 System Administrator's Guide*.

Dans JConsole, cliquez sur l'onglet Notifications pour afficher les événements de contrôle. Notez le numéro de séquence figurant dans la notification. Un numéro de séquence est requis pour interroger le MBean afin d'obtenir des informations supplémentaires.

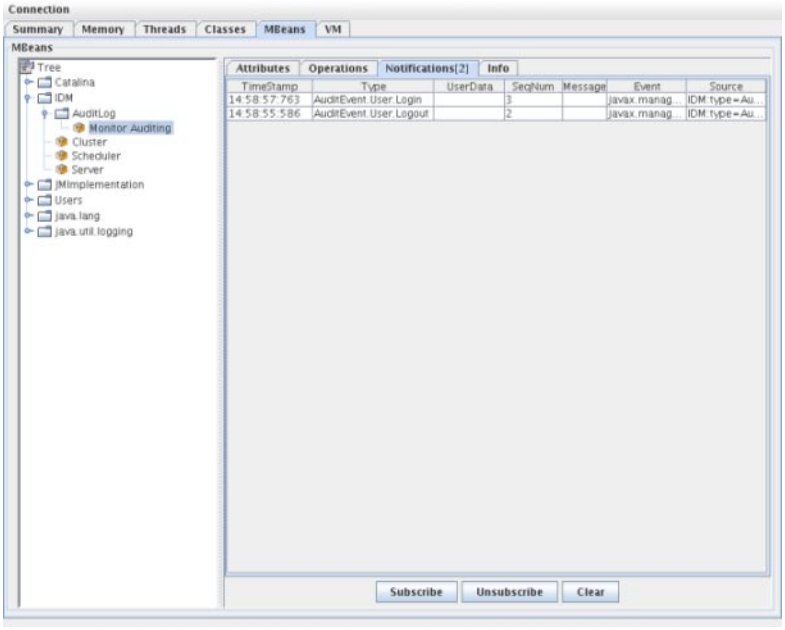


FIGURE 10–1 Affichage des notifications d'événement de contrôle de JMX dans JConsole

Interrogation du MBean afin d'obtenir des informations supplémentaires

Dans JConsole, cliquez sur l'onglet Operations (Opérations). Utilisez le numéro de séquence figurant dans la notification pour interroger le MBean afin d'obtenir les détails de l'événement. Toutes les opérations présentent le préfixe « get » et le seul paramètre est le numéro « sequence ».

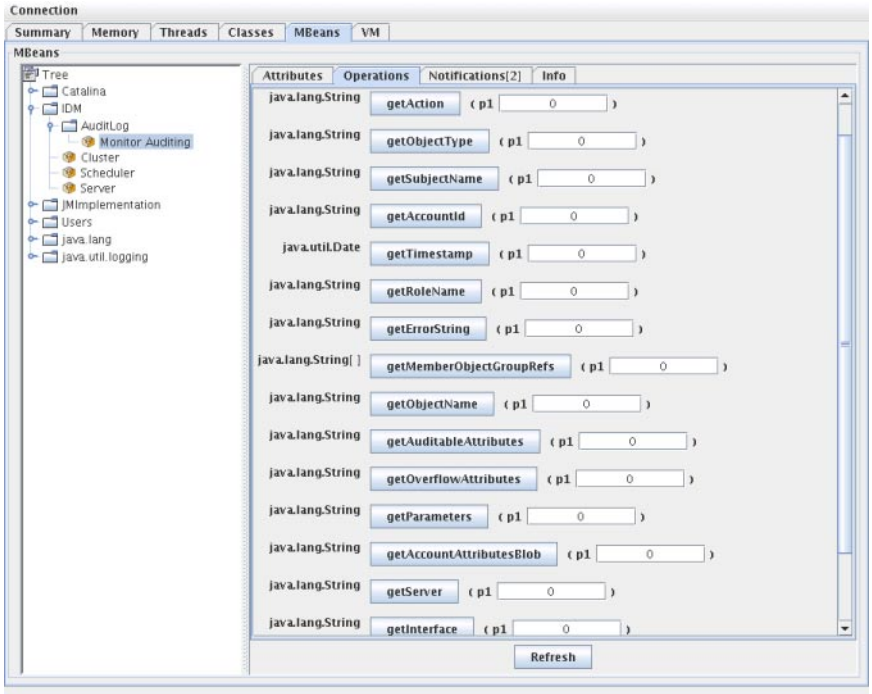


FIGURE 10–2 Interrogation du MBean afin d'obtenir des informations supplémentaires dans JConsole

Le MBean est pratiquement un mappage biunivoque vers la classe `com.waveset.object.AuditEvent` . Le Tableau 10–19 contient la description des différentes paires attribut/opération fournies par MBean.

TABLEAU 10–19 Description des paires attribut/opération MBeanInfo

Attribut / Opération	Description
`AccountAttributesBlob`	Liste des attributs modifiés
`AccountId`	ID de compte associé à l'événement
`Action`	Action entreprise pendant l'événement
`AuditableAttributes`	Attributs auditables
`ErrorString`	Toute chaîne d'erreur
`Interface`	L'interface d'audit
`MemberObjectGroupRefs`	Références du groupe des objets membres
`ObjectName`	Nom de l'objet

TABLEAU 10–19 Description des paires attribut/opération MBeanInfo *(Suite)*

Attribut / Opération	Description
`ObjectType`	Type de l'objet
`OverflowAttributes`	Tous les attributs de dépassement
`Parameters`	Tous les paramètres
`Reason`	Raison de l'événement
`ResourceName`	Ressource associée à l'événement
`RoleName`	Rôle associé à l'événement
`SubjectName`	Utilisateur ou service associé à l'événement
`Server`	Nom du serveur depuis lequel l'événement a été déclenché
`Status`	Statut de l'événement de contrôle
`Timestamp`	Date et heure de l'événement de contrôle

Dans JConsole, cliquez sur l'onglet Attributes (Attributs). Les attributs comportent le préfixe `Current` indiquant qu'ils contiennent le dernier événement de contrôle en date envoyé par le système.

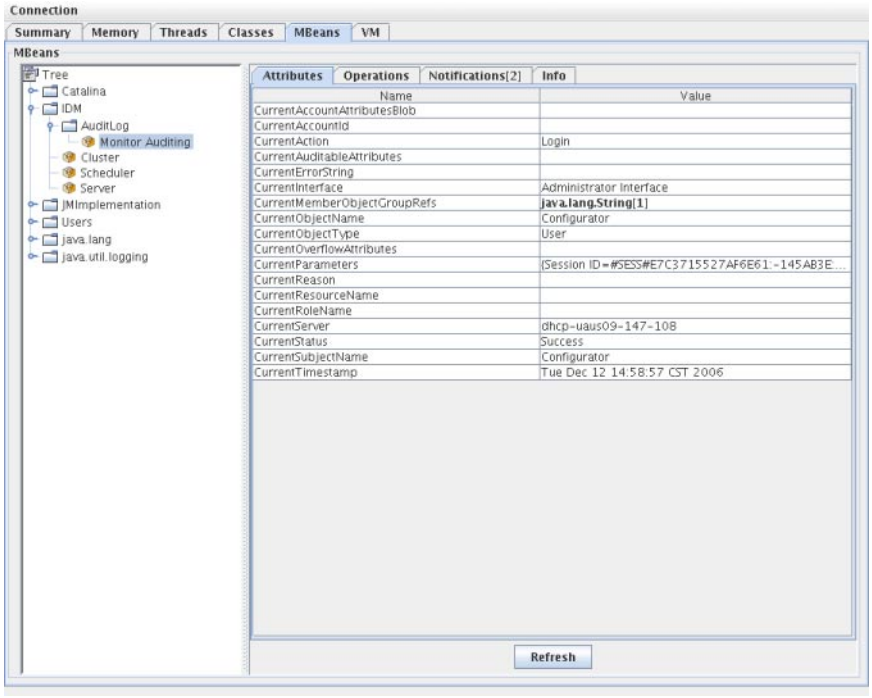


FIGURE 10–3 Affichage des attributs de Mbeans dans JConsole

Développement d'éditeurs d'audit personnalisés

Cette section explique la création d'un nouvel éditeur d'audit personnalisé en Java.

Les éditeurs personnalisés de type Console, Fichier ou JDBC fournis avec Identity Manager implémentent l'interface `AuditLogPublisher`. Le code source de ces éditeurs figure dans le kit REF. La documentation des interfaces est également disponible dans le kit REF, au format javadoc (voir la javadoc pour les détails de l'interface).

Remarque – Le kit REF (Resource Extension Facility) figure dans le répertoire `/REF` du CD de votre produit ou a été fourni avec votre image d'installation.

Les développeurs sont encouragés à étendre la classe `AbstractAuditLogPublisher`. Cette classe analyse la configuration et contrôle que toutes les options obligatoires ont été fournies à l'éditeur (voir les exemples d'éditeurs du kit REF).

Les éditeurs doivent avoir un constructeur `no-arg`.

Cycle de vie des éditeurs

Les étapes suivantes illustrent le cycle de vie d'un éditeur.

1. L'objet est généré.
2. Le programme de formatage (le cas échéant) est défini en utilisant la méthode `setFormatter()`.
3. Les options sont fournies en utilisant la méthode `configure(`*Mappe*`)`.
4. Les événements sont publiés en utilisant la méthode `publish(`*Mappe, GestionnaireErreursJournalisation*`)`.
5. L'éditeur est terminé en utilisant la méthode `shutdown()`.

Les étapes 1 à 3 sont exécutées lorsqu'Identity Manager démarre et à chaque fois que la configuration d'audit est mise à jour. L'étape 4 n'a pas lieu si aucun événement de contrôle n'est généré avant l'appel de shutdown.

`configure(`*Mappe* `)` n'est appelé qu'une fois sur le même objet d'éditeur (un éditeur n'a aucune préparation à effectuer pour les changements de configuration à la volée). Une fois la configuration d'audit mise à jour, les éditeurs courants sont arrêtés puis les nouveaux éditeurs sont créés.

La méthode `configure()` mentionnée à l'étape 3 peut émettre une `WavesetException`. Dans ce cas, l'éditeur sera ignoré et aucun autre appel ne sera effectué à l'adresse de l'éditeur.

Configuration des éditeurs

Les éditeurs peuvent avoir zéro options ou plus. La méthode `getConfigurationOptions()` retourne la liste des options prises en charge par l'éditeur. Les options sont encapsulées en utilisant la classe `PublisherOption` (voir la javadoc pour les détails de cette classe). L'afficheur de la configuration d'audit appelle cette méthode quand il compile l'interface de configuration pour l'éditeur.

Identity Manager configure l'éditeur en utilisant la méthode `configure(` *Mappe*`)` au démarrage du serveur et après les changements de configuration d'audit.

Développement de programmes de formatage

Le kit REF comprend le code source des programmes de formatage suivants :

- `XmlFormatter`. Formate les événements de contrôle sous forme de chaînes XML.
- `UlfFormatter`. Formate les événements de contrôle conformément au format ULF (Universal Logging Format, Format de journalisation universel). Il s'agit du format utilisé par Sun Application Server.

Les programmes de formatage doivent implémenter l'interface `AuditRecordFormatter`. De plus, ces programmes doivent avoir un constructeur `no-arg`. Pour de plus amples détails, consultez la javadoc incluse dans le kit REF.

Enregistrement des éditeurs/programmes de formatage

L'attribut d'audit de l'objet `#ID#Configuration:SystemConfiguration` liste l'ensemble des éditeurs et programmes de formatage enregistrés. Ces éditeurs et programmes de formatage sont les seuls disponibles dans l'interface utilisateur de configuration d'audit.

◆ ◆ ◆ CHAPITRE 11

PasswordSync

PasswordSync détecte les changements de mot de passe d'utilisateur amorcés sur les domaines Windows et les transfère dans Identity Manager. Identity Manager synchronise ensuite ces changements de mots de passe avec les autres ressources définies dans Identity Manager.

Ce chapitre se compose des rubriques suivantes :

Présentation de PasswordSync

La fonctionnalité PasswordSync assure la synchronisation des changements de mot de passe effectués dans des domaines Windows Active Directory avec les autres ressources définies dans Identity Manager. PasswordSync doit être installé sur chacun des contrôleurs de domaine dans les domaines qui seront synchronisés avec Identity Manager. PasswordSync doit être installé séparément d'Identity Manager.

PasswordSync se compose d'un DLL (`lhpwic.dll`) qui réside sur chaque contrôleur de domaine. Ce DLL reçoit les notifications de mise à jour de mot de passe de Windows, les chiffre et les envoie via HTTPS à la servlet PasswordSync. La servlet PasswordSync se trouve sur le serveur d'application exécutant Identity Manager.

Remarque – L'utilisation de HTTP est prise en charge mais celle de HTTPS reste préférable.

La servlet PasswordSync convertit la notification en un format compréhensible par Identity Manager. La servlet envoie ensuite le changement de mot de passe (toujours chiffré) à Identity Manager en utilisant l'une des méthodes suivantes :

- **Méthode directe**. La servlet communique directement le changement de passe à Identity Manager en utilisant les classes Identity Manager natives (voir "Présentation de PasswordSync" à la page 375).

  La méthode de connexion directe est uniquement recommandée pour les environnement de petite taille peu complexes qui requièrent seulement la livraison de messages à un unique système et n'ont pas besoin que la livraison des messages soit garantie. Si, pour une raison quelconque, la livraison directe d'un message échoue, ce dernier est perdu. Il n'y a pas de livraison de secours.

- **Méthode JMS**. La servlet envoie les informations de mot de passe à Identity Manager en utilisant JMS (Java Message Service). Avec JMS, la servlet envoie les changements de mot de passe à la file d'attente de messages de JMS. De son côté, l'adaptateur de ressources Listener JMS d'Identity Manager contrôle s'il n'y a pas de nouveaux messages dans la file d'attente. S'il détecte un message de changement de mot de passe en attente dans la file d'attente, l'adaptateur Listener JMS prélève le message de la file d'attente et l'importe dans Identity Manager (voir Figure 11–2).

  La méthode JMS est recommandée pour les environnements complexes caractérisés par de grands volumes, la nécessité de délivrer des messages à plusieurs systèmes et requerrant une livraison garantie des messages. La file d'attente de messages de JMS peut être rendue hautement disponible. Du moment qu'un message est inséré dans la file d'attente, si sa livraison à Identity Manager échoue, la file d'attente conserve le changement jusqu'à ce que le message puisse être délivré à Identity Manager.

  Vous devez installer et configurer JMS séparément.

La Figure 11–1 schématise une connexion directe. Dans cette configuration, la servlet PasswordSync envoie directement les messages de mise à jour à Identity Manager.

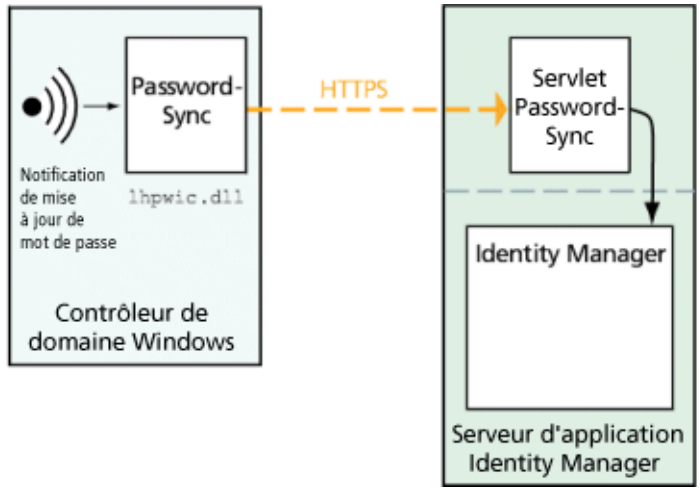


FIGURE 11–1 Diagramme logique de PasswordSync (connexion directe)

La Figure 11–2 schématise une connexion JMS. Dans cette configuration, la servlet PasswordSync envoie les messages de mise à jour à la file d'attente de messages de JMS. L'adaptateur de ressources Listener JMS d'Identity Manager contrôle périodiquement si la file d'attente (action indiquée par la flèche bleu clair sur le schéma) ne contient pas de nouveaux messages. La file d'attente répond en envoyant les messages à Identity Manager (action indiquée par la flèche bleu foncé).

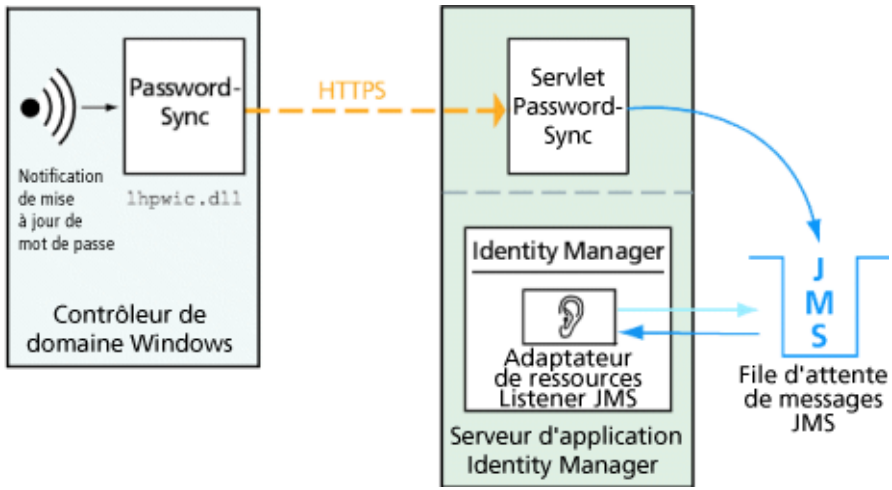


FIGURE 11–2 Diagramme logique de PasswordSync (connexion JMS)

Lorsqu'Identity Manager reçoit une notification de changement de mot de passe, il la déchiffre et traite le changement en utilisant une tâche de flux de travaux. Le mot de passe est mis à jour sur toutes les ressources assignées de l'utilisateur et un serveur SMTP envoie un e-mail à l'utilisateur l'avertissant du statut du changement de mot de passe.

Remarque – Windows se limite à envoyer une notification de mise à jour en cas de réussite du changement de mot de passe. Si une demande de changement de mot de passe ne respecte pas la stratégie de mot de passe du domaine, Windows la rejette et aucune donnée de synchronisation n'est envoyée à Identity Manager.

La Figure 11–3 montre Identity Manager amorçant un flux de travaux et envoyant un e-mail à l'utilisateur après avoir reçu une notification de mise à jour de mot de passe.

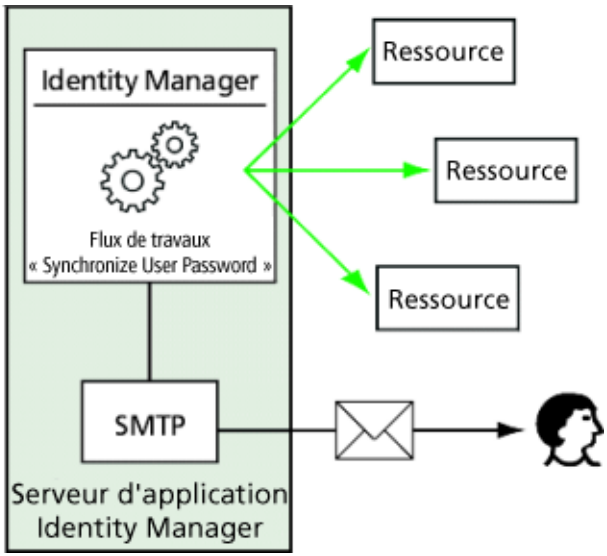


FIGURE 11–3 PasswordSync déclenche un flux de travaux

Remarque – PasswordSync rejette toutes les notifications de changement de compte relatives à des noms de compte se terminant par $ (signe des dollars). Les noms de compte se terminant par $ sont supposés être des comptes d'ordinateur Windows. Aucun nom de compte utilisateur se terminant par le signe des dollars ne sera transmis à Identity Manager.

Avant de commencer l'installation

La fonctionnalité PasswordSync peut uniquement être installée sur les contrôleurs de domaine Windows 2008, Windows 2003 et Windows 2000 (la prise en charge des contrôleurs de domaine Windows NT a été arrêtée dans la version 8.0 d'Identity Manager). Vous devez installer PasswordSync sur chacun des contrôleurs de domaine principaux et de sauvegarde qui seront synchronisés avec Identity Manager. Configurer PasswordSync pour HTTPS est vivement recommandé.

Remarque – Les versions de PasswordSync antérieures à la version 7.1.1 doivent être mises à jour vers la version 7.1.1 minimum sur tous les contrôleurs de domaine.

La prise en charge de la servlet rpcrouter2 a été désapprouvée dans la version 8.0 et sera supprimée dans une version future. Les versions 7.1.1 et suivantes de PasswordSync prennent en charge le nouveau protocole.

Si JMS est utilisé, PasswordSync doit être connecté à un serveur JMS. Pour plus d'informations sur les exigences concernant le système JMS, voir la section consacrée à l'adaptateur de ressources Listener JMS dans le guide *Sun Identity Manager 8.1 Resources Reference*.

De plus, pour PasswordSync, vous devez :

- installer Microsoft .NET 1.1 minimum sur chaque contrôleur de domaine ;
- supprimer les versions précédentes de PasswordSync.

Ces exigences sont examinées plus en détail dans les sections suivantes.

Installation de Microsoft .NET 1.1

Pour utiliser PasswordSync, vous devez installer au minimum Microsoft .NET 1.1 Framework. Microsoft .NET 1.1 Framework est installé par défaut si vous utilisez un contrôleur de domaine Windows 2003. Microsoft .NET 2.0 Framework est installé par défaut sur les contrôleurs de domaine Windows 2008. Si vous utilisez un contrôleur de domaine Windows 2000, aucun Framework n'est installé par défaut. Vous pouvez télécharger la boîte à outils du Centre de téléchargement de Microsoft à l'URL suivant :

`http://www.microsoft.com/downloads`

Remarque –

- Saisissez **`.NET Framework Redistributable`** dans les mots-clés du champ de recherche pour localiser rapidement la boîte à outils Framework.
- La boîte à outils installe .NET Framework.

Configuration de PasswordSync pour SSL

Bien que les données sensibles soient chiffrées avant d'être envoyées au serveur Identity Manager, Sun Microsystems recommande de configurer PasswordSync afin d'utiliser une connexion SSL sécurisée (c'est-à-dire une connexion HTTPS).

Pour toute information sur l'installation des certificats SSL importés, lisez l'article suivant de la base de connaissances Comment faire de Microsoft :

`http://support.microsoft.com/kb/816794`

Une fois PasswordSync installé, vous pouvez vérifier que votre connexion SSL est correctement configurée en indiquant un URL HTTPS dans la boîte de dialogue Configuration de PasswordSync Configuration. Pour les instructions, voir "Test de la configuration" à la page 405.

Désinstallation des versions précédentes de PasswordSync

Vous *devez* supprimer toutes les instances de PasswordSync installées au préalable avant d'installer une version plus récente.

- Si la version de PasswordSync installée au préalable prend en charge le programme d'installation `IdmPwSync.msi`, vous pouvez utiliser l'utilitaire Ajout/Suppression de programmes standard de Windows pour supprimer le programme.
- Si la version de PasswordSync installée au préalable *ne prend pas en charge* le programme d'installation `IdmPwSync.msi`, utilisez le programme de désinstallation InstallAnywhere pour supprimer le programme.

Installation et configuration de PasswordSync sous Windows

Cette section contient des informations et des instructions relatives à l'installation et à la configuration de PasswordSync.

Ces informations sont organisées comme suit :

- "Pour installer l'application de configuration de PasswordSync" à la page 381 ;
- "Pour configurer PasswordSync" à la page 382.

▼ Pour installer l'application de configuration de PasswordSync

La procédure suivante détaille l'installation de l'application de configuration de PasswordSync.

Remarque – Vous devez installer PasswordSync sur chaque contrôleur de domaine dans les domaines qui seront synchronisés avec Identity Manager.

Veillez à désinstaller toutes les versions installées au préalable de PasswordSync avant d'aller plus loin.

---

1 **Depuis le support d'installation d'Identity Manager,**

- Si vous effectuez l'installation sur une version 32 bits de Windows, double-cliquez sur `pwsync\IdmPwSync_x86.msi`.
- Si vous effectuez l'installation sur une version 64 bits de Windows, double-cliquez sur `pwsync\IdmPwSync_x64.msi`.

L'assistant d'installation s'ouvre et la fenêtre Welcome (Bienvenue) comportant les boutons de navigation suivants s'affiche :

- **Cancel** (Annuler). Cliquez sur ce bouton pour quitter l'assistant à tout moment sans enregistrer aucune de vos modifications.
- **Back** (Welcome). Cliquez sur ce bouton pour revenir à une boîte de dialogue précédente.
- **Next** (Suivant). Cliquez sur ce bouton pour passer à la boîte de dialogue suivante.

2 **Lisez les informations indiquées sur l'écran Welcome (Bienvenue) puis cliquez sur Next (Suivant) pour afficher la fenêtre Choose Setup Type (Choix du type d'installation).**

3 **Cliquez au choix sur Typical (Typique) ou Complete (Complète) pour installer l'intégralité du package PasswordSync, ou cliquez sur Custom (Personnalisée) pour contrôler les parties du package qui seront installées. Cliquez sur Next (Suivant) pour continuer.**

4 **Lorsque la fenêtre Ready to Install (Prêt pour l'installation) s'affiche, cliquez sur Install (Installer) pour installer le produit.**

5 **Une dernière fenêtre s'affiche. Activez la zone Launch Configuration Application (Lancer l'application de configuration) pour pouvoir commencer à configurer Password Sync puis cliquez sur Finish (Terminer) pour compléter le processus d'installation.**

Les instructions à suivre pour configurer PasswordSync figurent au Chapitre 11, “PasswordSync”.

Remarque – Une boîte de dialogue s'affiche indiquant que vous devez redémarrer le système pour que les changements soient appliqués. Il n'est pas nécessaire de redémarrer avant de configurer PasswordSync, mais vous devez redémarrer le contrôleur de domaine avant d'implémenter PasswordSync.

“Installation et configuration de PasswordSync sous Windows” à la page 381 décrit les fichiers qui sont installés sur chaque contrôleur de domaine.

Composant installé	Description
`%$INSTALL_DIR$%\configure.exe`	Programme de configuration PasswordSync
`%$INSTALL_DIR$%\configure.exe.manifest`	Fichiers de données pour le programme de configuration
`%$INSTALL_DIR$%\passwordsyncmsgs.dll`	DLL gérant les messages de PasswordSync
`%SYSTEMROOT%\SYSTEM32\lhpwic.dll`	DLL de notification de mot de passe implémentant la fonction DLL `PasswordChangeNotify()` de Windows.

▼ Pour configurer PasswordSync

Si vous exécutez l'application de configuration à partir du programme d'installation, l'application affiche les écrans de configuration sous la forme d'un assistant. Une fois l'assistant complété, toutes les fois que vous exécuterez l'application de configuration de PasswordSync, vous pourrez naviguer dans les écrans en sélectionnant un onglet.

1 **Démarrez l'application de configuration de PasswordSync (si elle n'est pas déjà en cours d'exécution).**

Par défaut, l'application de configuration est installées dans Program Files → Sun Identity Manager PasswordSync → Configuration.

Remarque – Si vous ne projetez pas d'utiliser JMS, lancez l'application de configuration depuis une ligne de commande en veillant à inclure l'indicateur `-direct` comme suit :

```
C:\InstallDir\Configure.exe -direct
```

La boîte de dialogue de l'assistant PasswordSync Configuration (Configuration de PasswordSync) s'affiche (voir Figure 11–4).

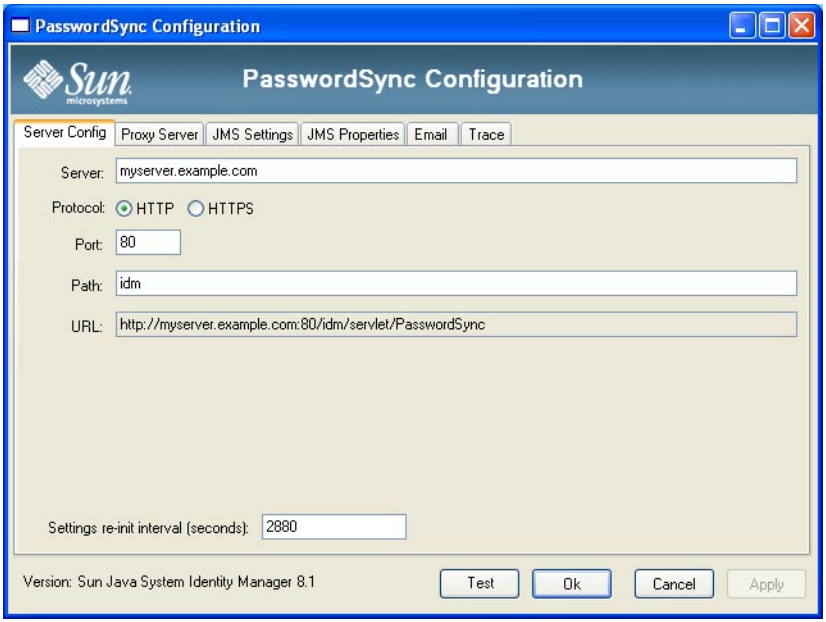


FIGURE 11–4 Assistant de configuration de PasswordSync

2 Éditez les champs de cette boîte de dialogue comme requis.

Ces champs sont les suivants :

- **Server** (Serveur) doit être remplacé par le nom complet de l'hôte ou l'adresse IP où Identity Manager est installé.
- **Protocol** (Protocole) indique si établir des connexions sécurisées avec Identity Manager.

PasswordSync prend en charge la configuration d'un comportement de contrôle de certificats pour les connexions HTTPS. Lorsque vous activez HTTPS, les options suivantes s'affichent :

- **Allow revoked certificates** (Autoriser les certificats révoqués). Ce paramètre mappe vers la valeur de registre `securityIgnoreCertRevoke` sur la connexion. Par défaut, PasswordSync n'ignore pas les problèmes de révocation et la valeur de registre `securityIgnoreCertRevoke` est définie sur 0.

  Si vous voulez que PasswordSync ignore les messages relatifs aux certificats révoqués, cochez cette case (ou définissez la valeur de registre `SECURITY_FLAG_IGNORE_REVOCATION` sur 1).

- **Allow invalid certificates** (Autoriser les certificats non valides). Ce paramètre s'applique aux options `SECURITY_FLAG_IGNORE_CERT_CN_INVALID`, `SECURITY_FLAG_IGNORE_CERT_DATE_INVALID` et `SECURITY_FLAG_IGNORE_UNKNOWN_CA` sur la connexion. Par défaut, PasswordSync n'autorise pas les certificats non valides et les valeurs de registre sont définies sur 0.

  Cocher cette case ou définir la valeur de registre `securityAllowInvalidCert` sur 1 permet à PasswordSync d'utiliser des certificats qui échouent à un certain nombre de contrôles de sécurité. L'activation de cette option n'est *pas recommandée* pour un environnement de production.

Remarque – Ces paramètres ne sont pas affichés pour le type de protocole HTTP et sont sans effet sur les paramètres HTTP.

- **Port** (Port). Spécifiez un port disponible pour le serveur. Pour HTTP, le port par défaut est le 80. Pour HTTPS, le port par défaut est le 443.
- **Path** (Chemin). Spécifiez le chemin d'Identity Manager sur le serveur d'application.
- L'**URL** est généré en concaténant ensemble les autres champs. La valeur contenue dans le champ URL ne peut pas être éditée dans ce champ.
- **Settings re-init interval (seconds)** (Intervalle de réinitialisation des paramètres (en secondes) précise la fréquence à laquelle le fichier `dll` de PasswordSync doit relire les paramètres dans le registre. La valeur par défaut est 2880 secondes ou 8 heures.

Remarque – Cet assistant de configuration de PasswordSync affiche la valeur en secondes, mais la valeur du registre est effectivement stockée en millisecondes.

Le fichier `dll` de PasswordSync lit les paramètres de configuration dans le registre pendant que le `dll` est actif. Cette valeur d'intervalle est stockée dans la valeur de registre `reinitIntervalMilli`.

Les mots de passe ne peuvent pas être synchronisés pendant la mise à jour des paramètres, ce qui peut entraîner un petit délai dans le traitement d'un changement de mot de passe. En général, ce délai ne dépasse pas une seconde. PasswordSync traite tous les changements de mot de passe reçus pendant une mise à jour dès que celle-ci est terminée. Par ailleurs, PasswordSync ne traite pas les mises à jour des paramètres pendant qu'une synchronisation de mot de passe est en cours. La mise à jour sera reprogrammée et effectuée à un moment ultérieur.

3 **Cliquez sur Next (Suivant) pour afficher la page Proxy Server Configuration (Configuration du serveur proxy) (Figure 11–5) et éditez les champs comme requis.**

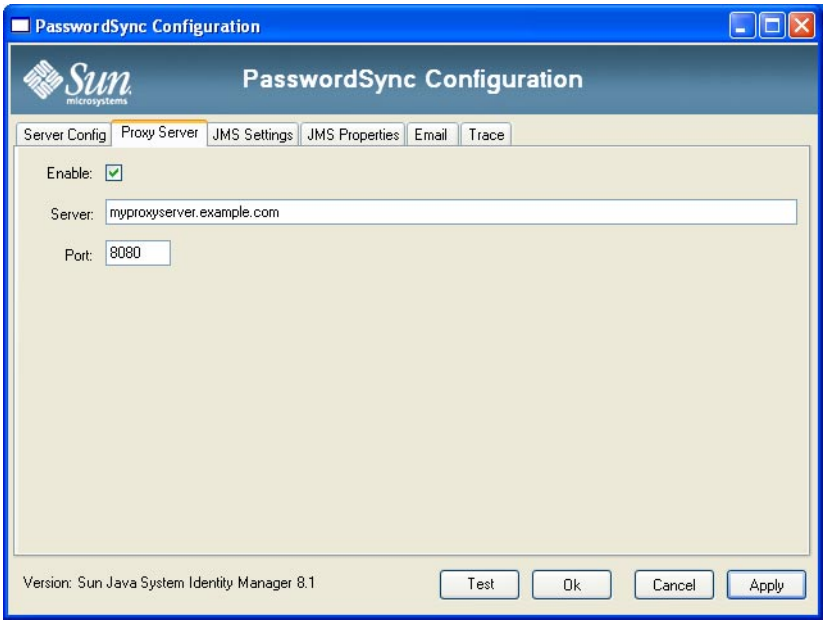


FIGURE 11–5 La boîte de dialogue du serveur proxy de l'assistant de PasswordSync

Ces champs sont les suivants :

- **Enable** (Activer). Sélectionnez ce champ si un serveur proxy est nécessaire.
- **Server** (Serveur). Vous devez saisir ici le nom d'hôte complet ou l'adresse IP du serveur proxy.
- **Port** (Port). Spécifiez un numéro de port disponible pour le serveur (le port de proxy par défaut est le 8080 tandis que le port HTTPS par défaut est le 443).

4 **Cliquez sur Next (Suivant).**

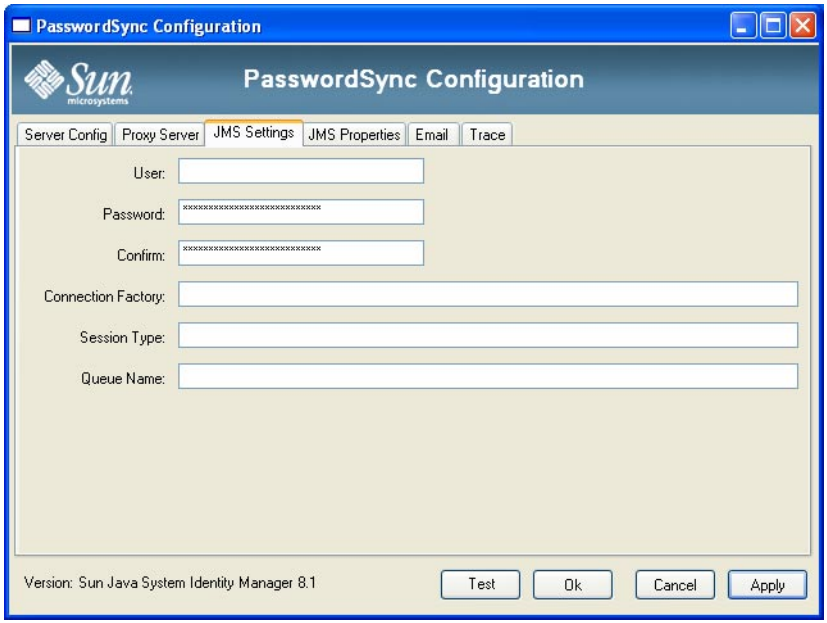


FIGURE 11–6 La boîte de dialogue des paramètres JMS de l'assistant de PasswordSync

Lorsque la boîte de dialogue des paramètres de JMS (Figure 11–6) s'affiche, effectuez l'une des actions suivantes :

- Éditez les champs suivants comme nécessaire :
  - **User** (Utilisateur) indique le nom d'utilisateur JMS qui place les nouveaux messages dans la file d'attente.
  - **Password** (Mot de passe) et **Confirm** (Confirmer) spécifient le mot de passe de l'utilisateur JMS.
  - **Connection Factory** (Fabrique de connexion) indique le nom de la fabrique de connexion JMS à utiliser. Cette fabrique doit déjà exister sur le système JMS.
  - Dans la plupart des cas, **Session Type** (Type de session) doit être défini sur `LOCAL`, qui indique qu'une transaction de session locale sera utilisée. La session sera validée après la réception de chaque message. D'autres valeurs possibles sont `AUTO`, `CLIENT` et `DUPS_OK`.
  - **Queue Name** (Nom de la file) spécifie le nom de recherche de destination pour les événements de synchronisation de mot de passe.
- Si vous ne projetez pas d'utiliser JMS et que vous avez lancé l'assistant de configuration avec l'indicateur `-direct`, cliquez sur Next (Suivant) pour afficher la boîte de dialogue User (Utilisateur). Allez directement à l'étape Figure 11–7.

5 Cliquez sur Next (suivant) pour afficher la boîte de dialogue des propriétés de JMS (Figure 11–7).

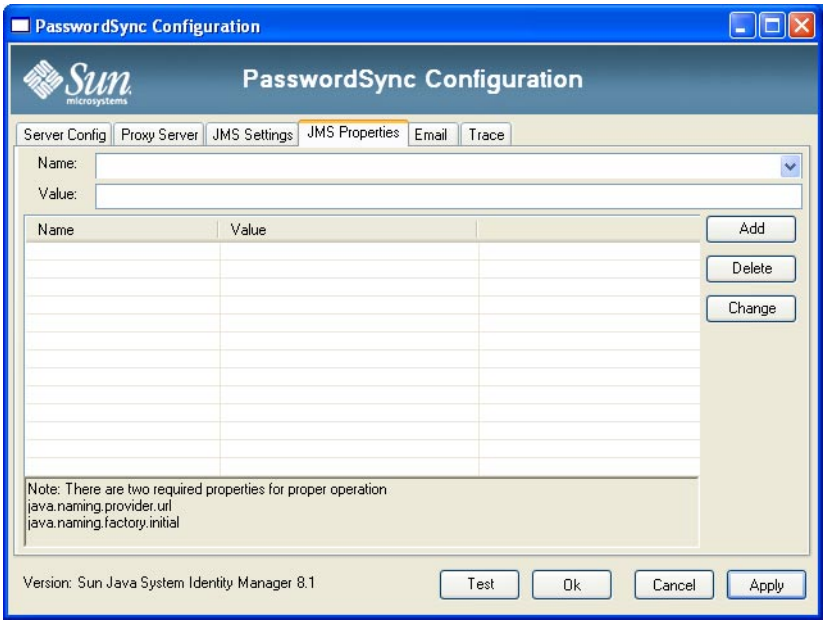


FIGURE 11–7 La boîte de dialogue des propriétés JMS de l'assistant de PasswordSync

La boîte de dialogue des propriétés JMS permet de définir l'ensemble des propriétés qui sont utilisées pour construire le contexte JNDI initial. Vous devez définir les paires nom/valeur suivantes :

- `java.naming.provider.url` : spécifiez l'URL de la machine exécutant le service JNDI.
- `java.naming.factory.initial` : spécifiez le nom de la classe (package compris) de l'Initial Context Factory (Fabrique de contexte initiale) pour le Service Provider JNDI.

  Le menu déroulant Name (Nom) contient une liste de classes du package `java.naming`. Sélectionnez une classe ou saisissez-en le nom puis entrez la valeur correspondante dans le champ Value (Valeur).

6 Si vous ne projetez pas d'utiliser JMS et que vous avez lancé l'assistant de configuration avec l'indicateur `-direct`, configurez l'onglet User (Utilisateur). Sinon, ignorez cette étape et passez directement à la suivante.

Pour configurer l'onglet User (Utilisateur), éditez les champs qui doivent l'être.

- **Account ID** (ID de compte). Spécifiez le nom d'utilisateur que vous utiliserez pour vous connecter à Identity Manager.
- **Password** (Mot de passe). Indiquez le mot de passe qui vous utiliserez pour vous connecter à Identity Manager.

7 Cliquez sur Next (Suivant) pour afficher la boîte de dialogue Email (E-mail) (Figure 11–8) et éditez les champs qui doivent l'être.

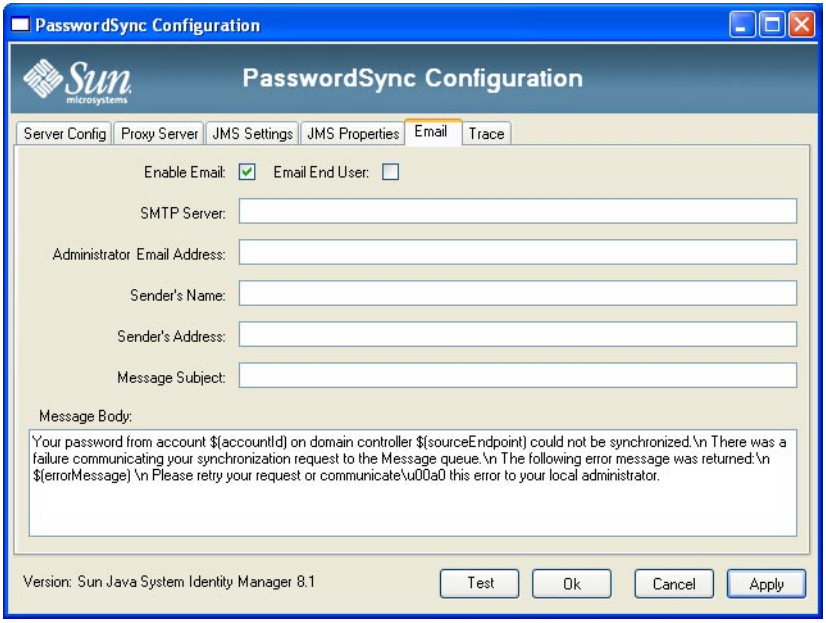


FIGURE 11–8 La boîte de dialogue d'e-mail de l'assistant de PasswordSync

Pour envoyer une notification par e-mail lorsque la synchronisation d'un changement de mot de passe échoue à cause d'une erreur de communication ou d'une autre erreur externe à Identity Manager, utilisez les options suivantes de la boîte de dialogue Email (E-mail) pour paramétrer la notification et configurer l'e-mail.

- **Enable Email** (Activer l'e-mail). Sélectionnez cette option pour activer cette fonctionnalité.
- **Email End User** (E-mail à l'utilisateur final). Sélectionnez cette option pour que l'utilisateur reçoive des notifications. Sinon, seul l'administrateur sera averti.
- **SMTP Server** (Serveur SMTP). Saisissez le nom complet ou l'adresse IP du serveur SMTP qui devra être utilisé pour envoyer les notifications d'échec.
- **Administrator Email Address** (Adresse e-mail de l'administrateur). Saisissez l'adresse e-mail à laquelle vous voulez envoyer les notifications.
- **Sender's Name** (Nom de l'expéditeur). Saisissez le « nom convivial » de l'expéditeur.
- **Sender's Address** (Adresse de l'expéditeur). Saisissez l'adresse e-mail de l'expéditeur.
- **Message Subject** (Objet du message). Saisissez la ligne d'objet qui sera utilisée pour toutes les notifications.
- **Message Body** (Corps du message). Saisissez le texte de la notification.

Le corps du message peut contenir les variables suivantes :

- `$(accountId)` : ID de compte de l'utilisateur tentant de changer son mot de passe.
- `$(sourceEndpoint)` : nom d'hôte du contrôleur de domaine sur lequel le notificateur de mot de passe est installé, pour faciliter la localisation des machines défectueuses.
- `$(errorMessage)` : message d'erreur décrivant l'erreur qui s'est produite.

8 Cliquez sur l'onglet Trace (Tracer) Figure 11–9.

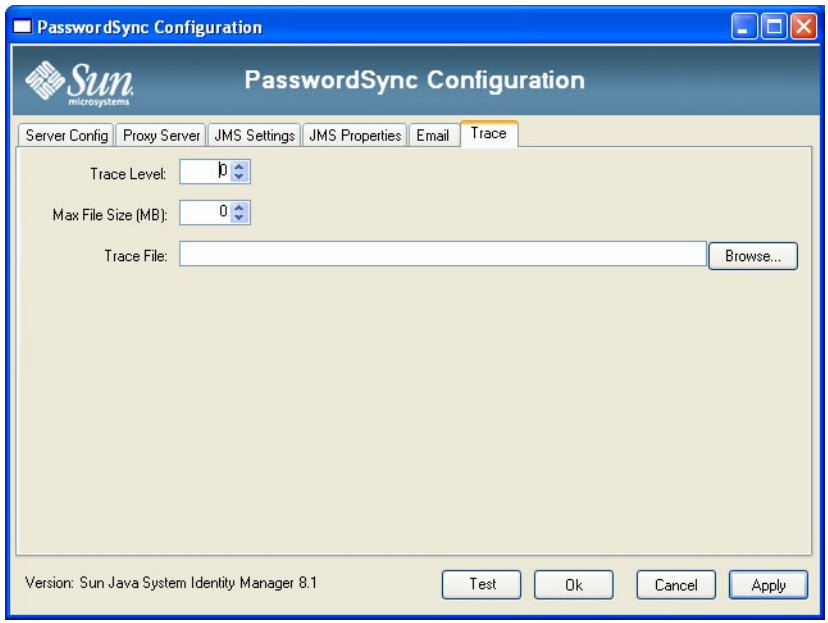


FIGURE 11–9 L'onglet Trace (Tracer).

Définissez les champs suivants :

- **Trace Level** (Niveau de suivi),
- **Max File Size (MB)** (Taille de fichier max. (en Mo)),
- **Trace File** (Fichier de suivi).

9 Cliquez sur Finish (Terminer) pour enregistrer vos modifications.

Si vous exécutez de nouveau l'application de configuration, un ensemble d'onglets s'affiche à la place de l'assistant. Pour afficher cette application sous la forme d'un assistant, saisissez la ligne de commande suivante sur la ligne de commande :

`C:\`*InstallDir*`\Configure.exe -wizard`

Pour tester votre configuration PasswordSync, voir "Test de la configuration" à la page 405.

Installation silencieuse de PasswordSync

Vous pouvez configurer le programme d'installation de PasswordSync pour une installation silencieuse. Pour utiliser cette fonctionnalité, vous devez commencer par enregistrer les paramètres de configuration dans un fichier pendant que vous installez PasswordSync. Les futures installations référenceront ce fichier et réutiliseront les paramètres de configuration.

Remarque – Pour utiliser la procédure d'installation silencieuse, vous devez installer le produit dans son intégralité sur chacun des serveurs qui l'utiliseront. L'enregistrement et la réutilisation des paramètres de configuration dépendent de l'application de configuration qui sera installée sur le système.

Le processus d'installation silencieuse utilise un utilitaire Windows appelé `msiexec` qui installe les fichiers `.msi` depuis la ligne de commande.

Saisissez `msiexec /?` à une invite de commande pour afficher les informations d'utilisation relatives à cet utilitaire.

De la documentation est également disponible sur le site Web de Microsoft. Par exemple, pour obtenir de la documentation sur l'utilisation de `msiexec` sous Windows Server 2003, reportez-vous à `http://technet.microsoft.com/en-us/library/cc759262.aspx`.

▼ Pour capturer les paramètres d'installation dans un fichier de configuration

Suivez les instructions ci-après pour installer PasswordSync en utilisant l'assistant d'installation. L'utilitaire de configuration capture les paramètres de configuration et les écrit dans un fichier XML.

Avant de commencer Supprimez les versions plus anciennes de PasswordSync avant l'installation.

1. **Allez au répertoire contenant le fichier d'installation de PasswordSync (`.msi`).**

   Pour plus d'informations, voir "Pour installer l'application de configuration de PasswordSync" à la page 381.

2. **Saisissez ce qui suit à une invite de commande : Les arguments et les valeurs sont sensibles à la casse.**

   `msiexec /i` *pwSyncInstallFile* `CONFIGARGS="-writexml` *fullPathToFile*`"`

   Où :

   - **pwSyncInstallFile** est le fichier d'installation de PasswordSync (`IdmPwSync_86.msi` ou `IdmPwSync_x64.msi`).
   - **fullPathToFile** spécifie où écrire le fichier XML.

Par exemple :

```
msiexec /i IdmPwSync_x86.msi CONFIGARGS="-writexml c:\tmp\myconfig.xml"
```

3 **Installez le produit.**

▼ Pour installer PasswordSync en silence

Avant de commencer

- Vous devez avoir créé un fichier XML de configuration d'installation. Pour les instructions, voir "Pour capturer les paramètres d'installation dans un fichier de configuration" à la page 390.
- Supprimez les versions plus anciennes de PasswordSync avant l'installation.

1 **Copiez votre fichier XML de configuration d'installation dans un emplacement où il peut être lu par le programme d'installation.**

2 **Saisissez ce qui suit à une invite de commande. Les arguments et les valeurs sont sensibles à la casse.**

```
msiexec /i pwSyncInstallFile ADDLOCAL="installFeature" CONFIGARGS="-readxml fullPathToFile"
 INSTALLDIR="installDir" /q
```

Où :

- **pwSyncInstallFile** est le fichier d'installation de PasswordSync (`IdmPwSync_86.msi` ou `IdmPwSync_x64.msi`).
- **installFeature** indique les fonctionnalités de PasswordSync à installer. Choisissez l'une des options suivantes :
  - `MainProgram` : installe seulement le fichier `.dll` intercepteur.
  - `Configuration` : installe seulement l'application de configuration.
  - `ALL` : installe l'intégralité du produit.

  Si aucune option n'est spécifiée, `MainProgram` est utilisé par défaut si l'option `/q` est fournie.
- **fullPathToFile** spécifie le chemin du fichier XML de configuration.
- **installDir** précise le chemin complet d'un répertoire d'installation personnalisé. Facultatif.
- **/q** spécifie une installation sans IG qui redémarre automatiquement le serveur une fois terminée. S'il n'est pas inclus, l'assistant d'installation s'affichera mais la configuration s'exécutera avec les paramètres prédéfinis. Facultatif.

Exemples :

```
msiexec /i IdmPwSync_x86.msi CONFIGARGS="-readxml c:\tmp\myconfig.xml"

msiexec /i IdmPwSync_x86.msi ADDLOCAL="MainProgram"
CONFIGARGS="-readxml c:\tmp\myconfig.xml" /q

msiexec /i IdmPwSync_x64.msi ADDLOCAL="Complete"
CONFIGARGS="-readxml c:\tmp\myconfig.xml"
INSTALLDIR="C:\Program Files\Sun Microsystems\MyCustomInstallDirectory" /q
```

Déploiement de PasswordSync sur le serveur d'application

Une fois PasswordSync installé sur vos contrôleurs de domaine Windows, vous devez effectuer les étapes supplémentaires suivantes sur le serveur d'application exécutant Identity Manager.

Vous n'avez pas à installer la servlet PasswordSync sur le serveur d'application. Elle a été installée automatiquement quand vous avez installé Identity Manager.

Pour terminer de déployer PasswordSync toutefois, vous devez effectuer les actions suivantes dans Identity Manager :

- ajouter et configurer l'adaptateur Listener JMS (si vous utilisez JMS) ;
- implémenter le flux de travaux « Synchronize User Password » (Synchroniser le mot de passe de l'utilisateur) ;
- paramétrer les notifications.

Ajout et configuration d'un adaptateur Listener JMS

Si la servlet PasswordSync utilise JMS pour envoyer des messages à Identity Manager, vous devez ajouter l'adaptateur de ressource Listener JMS d'Identity Manager. L'adaptateur de ressource Listener JMS contrôle régulièrement si des messages n'ont pas été placés dans la file d'attente de messages de JMS par la servlet de PasswordSync. Si la file d'attente contient un nouveau message, l'adaptateur l'envoie à Identity Manager qui le traite.

▼ Pour ajouter l'adaptateur de ressource Listener JMS

1 **Connectez-vous à l'interface administrateur d'Identity Manager ("Interface administrateur d'Identity Manager" à la page 37).**

2 **Sélectionnez Ressources → Configurer les types dans le menu principal.**

La Page Configurer les ressources gérées s'ouvre comme indiqué à la Figure 11–10.

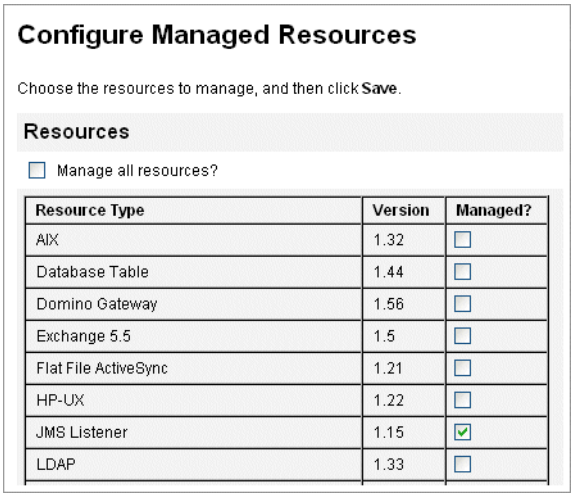


FIGURE 11–10 Page Configurer les ressources gérées

3 **Vérifiez que la case à cocher Listener JMS dans la colonne Gérés ? est cochée comme indiqué à la Figure 11–10.**

Si cette case n'est pas sélectionnée, cochez-la et cliquez sur Enregistrer.

4 **Cliquez sur Lister les ressources dans le menu secondaire.**

5 **Localisez le menu déroulant Actions du type de ressources et sélectionnez Nouvelle ressource.**

La page Nouvelle ressource s'affiche.

6 **Pour ajouter l'adaptateur Listener JMS, sélectionnez Listener JMS dans le menu déroulant (comme indiqué à la Figure 11–11) et cliquez sur Nouveau.**

FIGURE 11–11 L'assistant Nouvelle ressource

7 Configurez les paramètres suivants sur la page Paramètres de ressource puis cliquez sur suivant.

- **Type de destination**. Cette valeur est en général définie sur File d'attente (les rubriques ne sont en général pas applicables car il y a un abonné et, potentiellement, plusieurs éditeurs).
- **Propriétés JNDI du contexte initial**. Définissez l'ensemble des propriétés qui sont utilisées pour construire le contexte JNDI initial.

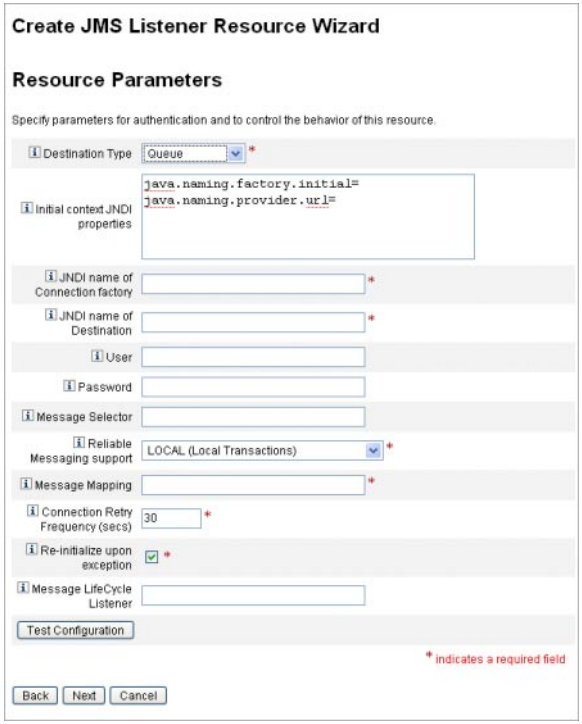
  Vous devez définir les paires nom/valeur suivantes :

  - `java.naming.factory.initial`. Spécifiez le nom de la classe (package compris) de l'Initial Context Factory (Fabrique de contexte initiale) pour le Service Provider JNDI.
  - `java.naming.provider.url`. Spécifiez l'URL de la machine exécutant le service JNDI.

    Vous pouvez avoir à définir des propriétés supplémentaires. La liste des propriétés et valeurs doit correspondre à celles indiquées sur la page des paramètres JMS sur le serveur JMS. Par exemple, pour fournir les informations d'authentification et la méthode de liaison, il est possible que vous deviez spécifier les propriétés d'exemple suivantes :

    - `java.naming.security.principal` : DN de liaison (par exemple, cn=Directory manager).
    - `java.naming.security.authentication` : méthode de liaison (par exemple, simple).
    - `java.naming.security.credentials` : mot de passe.
- **Nom JNDI de la fabrique de connexion**. Saisissez le nom d'une fabrique de connexion tel que défini sur le serveur JMS.
- **Nom JNDI de destination**. Saisissez le nom d'une destination tel que défini sur le serveur JMS.
- **Utilisateur** et **Mot de passe**. Saisissez le nom et le mot de passe du compte de l'administrateur qui demande de nouveaux événements de la file d'attente.

- **Support de messagerie fiable**. Sélectionnez `LOCAL (transactions locales)`. Les autres options ne sont pas applicables pour la synchronisation des mots de passe.
- **Mappage des messages**. Entrez `java:com.waveset.adapter.jms.PasswordSyncMessageMapper`. Cette classe convertit les messages provenant du serveur JMS en un format pouvant être utilisé par le flux de travaux Synchronize User Password.



8 **Sur la page de l'assistant Attributs de compte (Figure 11–12), cliquez sur Ajouter un attribut et mappez les attributs suivants, qui sont mis à la disposition de l'adaptateur Listener JMS par `PasswordSyncMessageMapper`.**

- `IDMAccountId` : cet attribut est résolu par `PasswordSyncMessageMapper`, sur la base des attributs `resourceAccountId` et `resourceAccountGUID` transmis dans le message JMS.
- `password`: mot de passe chiffré transféré dans le message JMS.

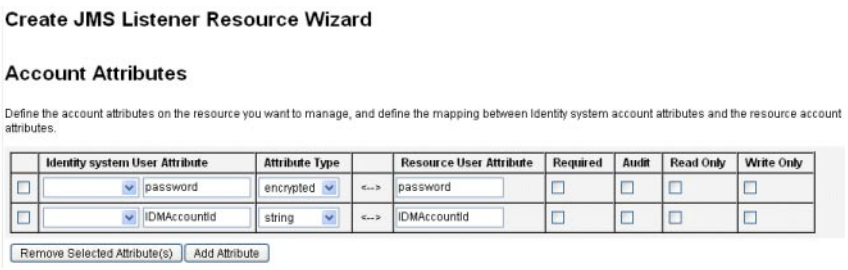


FIGURE 11–12 Page Attributs de compte de l'assistant de création de la ressource Listener JMS

9 Cliquez sur Suivant.

La page de l'assistant Modèle d'identité s'ouvre comme indiqué à la Figure 11–13. Vous remarquerez que les attributs que vous avez ajoutés à l'étape précédente sont disponibles dans la section des mappages d'attributs de l'assistant Ressources (Figure 11–13).

FIGURE 11–13 Mappages d'attributs de l'assistant Ressources du Listener JMS

10 Cliquez sur Suivant et configurez les options de la page Paramètres du système d'identité qui doivent l'être.

Pour plus d'informations sur le paramétrage de l'adaptateur de ressources Listener JMS, voir le guide *Sun Identity Manager 8.1 Resources Reference*.

Implémentation du flux de travaux « Synchronize User Password »

À la réception d'une notification de changement de mot de passe, Identity Manager lance le flux de travaux Synchronize User Password (Synchroniser le mot de passe de l'utilisateur). Le flux de travaux Synchronize User Password par défaut contrôle l'afficheur ChangeUserPassword puis

l'enregistre de nouveau. Le flux de travaux traite ensuite tous les comptes de ressource (à l'exception de la ressource Windows qui a envoyé la notification de changement de mot de passe initiale). Pour finir, Identity Manager envoie à l'utilisateur un e-mail indiquant si le changement de mot de passe a réussi sur toutes les ressources.

Pour utiliser l'implémentation par défaut du flux de travaux Synchronize User Password, assignez-le en tant que règle de traitement pour l'instance d'adaptateur Listener JMS en question. Les règles de traitement peuvent être assignées quand vous configurez le Listener JMS pour la synchronisation (voir "Configuration d'Active Sync" à la page 404).

Pour modifier le flux de travaux, copiez le fichier `$WSHOME/sample/wfpwsync.xml` et effectuez les modifications de votre choix. Importez ensuite le flux de travaux modifié dans Identity Manager.

Les modifications susceptibles d'être apportées au flux de travaux par défaut peuvent porter sur :

- les entités qui sont averties lorsqu'un mot de passe est changé ;
- ce qui se passe si un compte Identity Manager est introuvable ;
- la façon dont les ressources sont sélectionnées dans le flux de travaux ;
- si autoriser les changements de mot de passe depuis Identity Manager.

Pour des informations détaillées sur l'utilisation des flux de travaux, voir le Chapitre 1, "Workflow" du *Sun Identity Manager Deployment Reference*.

Paramétrage des notifications

Identity Manager fournit deux modèles d'e-mails pouvant informer les utilisateurs de l'issue d'un changement de mot de passe sur les différentes ressources.

Ces modèles sont les suivants :

- Avis de synchronisation du mot de passe,
- Avis d'échec de la synchronisation du mot de passe.

Ces deux modèles doivent être mis à jour pour fournir des informations spécifiques à l'entreprise sur ce que doivent faire les utilisateurs quand ils ont besoin d'assistance supplémentaire. Pour plus d'informations, voir "Personnalisation des modèles d'e-mails" à la page 106 au Chapitre 4, "Configuration des objets d'administration d'entreprise".

Configuration de PasswordSync avec un serveur JMS Sun

Identity Manager peut utiliser Java Message Service (JMS) pour recevoir les notifications de changement de mot de passe de la servlet PasswordSync. En plus de garantir la livraison, JMS est en mesure de délivrer les messages à plusieurs systèmes.

Remarque – Pour plus d'informations sur cet adaptateur, voir *Sun Identity Manager 8.1 Resources Reference*.

Cette section précise, en utilisant un exemple de scénario, les instructions à suivre pour configurer PasswordSync avec un serveur JMS Sun.

Ces informations sont organisées comme suit :

- "Scénario d'exemple" à la page 398 ;
- "Création et stockage d'objets administrés" à la page 399 ;
- "Configuration de l'adaptateur Listener JMS pour ce scénario" à la page 403 ;
- "Configuration d'Active Sync" à la page 404.

Scénario d'exemple

Un cas d'utilisation typique (simple) de la configuration de PasswordSync avec un serveur JMS est celui dans lequel les utilisateurs sont autorisés à changer leurs mots de passe sous Windows et où Identity Manager prélève les nouveaux mots de passe et met à jour les comptes utilisateur avec les nouveaux mots de passe sur un serveur Sun Directory.

L'environnement suivant a été configuré pour ce scénario :

- Windows Server 2003 Enterprise Edition– Active Directory ;
- Sun Java™ System Identity Manager 6.0 2005Q4M3 ;
- MySQL exécuté sous SUSE Linux 10.0 ;
- Tomcat 5.0.28 exécuté sous SUSE Linux 10.0 ;
- Sun Java System Message Queue 3.6 SP3 2005Q4 exécuté sous SUSE Linux 10.0 ;
- Sun Java System Directory Server 5.2 SP4 exécuté sous SUSE Linux 10.0 ;
- Java 1.5 (Java 5.0).

Les fichiers suivants ont été copiés du répertoire `common/lib` de Tomcat pour activer JMS et JNDI :

- `jms.jar` (de la file d'attente de messages Sun),
- `fscontext.jar` (de la file d'attente de messages Sun),
- `imq.jar` (de la file d'attente de messages Sun),
- `jndi.jar` (du SDK Java).

Création et stockage d'objets administrés

Cette section contient les instructions à suivre pour créer et stocker les objets administrés suivants, indispensables pour que le scénario d'exemple fonctionne correctement :

- les objets Fabrique de connexion,
- les objets Destination.

Vous pouvez stocker les objets administrés dans un annuaire LDAP ou dans un fichier. Si vous utilisez un fichier, toutes les instances de ce fichier doivent être identiques.

Pour les instructions, voir

- "Stockage des objets administrés dans un annuaire LDAP" à la page 399 ;
- "Stockage des objets administrés dans un fichier" à la page 401.

Remarque –

- Les instructions de cette section supposent que vous avez installé la file d'attente de messages Sun Java System Message Queue (les outils nécessaires figurent dans le répertoire `bin/` de votre installation de Message Queue).
- Vous pouvez utiliser l'interface graphique administrative de Message Queue administrative `imqadmin`) ou l'outil de ligne de commande `imqobjmgr`) pour créer ces objets administrés. Les instructions suivantes utilisent l'outil de ligne de commande.

Stockage des objets administrés dans un annuaire LDAP

PasswordSync et le Listener JMS peuvent être configurés pour utiliser les objets administrés stockés dans un annuaire LDAP. La Figure 11–14 illustre le processus. La servlet PasswordSync et le listener JMS doivent tout deux récupérer les paramètres de fabrique de connexion et de destination de l'annuaire LDAP pour envoyer et recevoir des messages.

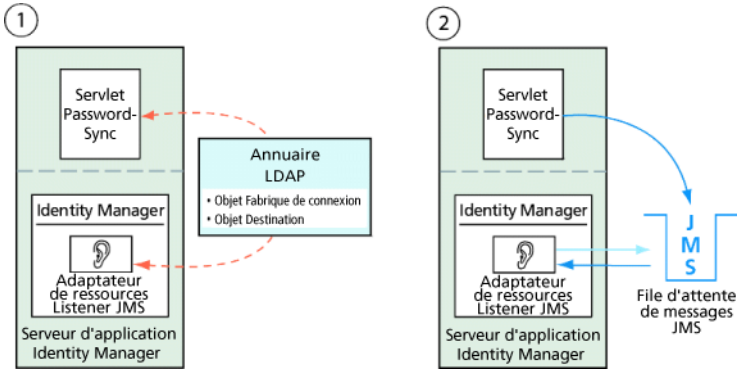


FIGURE 11–14 Récupération des objets Fabrique de connexion et Destination de l'annuaire LDAP

Utilisation de l'outil de ligne de commande de Message Queue

Cette section explique l'utilisation de l'outil de ligne de commande de Message Queue (`imqobjmgr`) pour stocker les objets administrés dans un annuaire LDAP.

Stockage des objets Fabrique de connexion

Ouvrez l'outil de ligne de commande de Message Queue (`imqobjmgr`) et saisissez les commandes de "Stockage des objets Fabrique de connexion" à la page 400 pour stocker les objets Fabrique de connexion.

EXEMPLE 11–1 Stockage des objets Fabrique de connexion

```
#> ./imqobjmgr add -l "cn=mytestFactory"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t qf -o "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements] ...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name: cn=mytestFactory The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url
ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication
simple java.naming.security.credentials netscape
java.naming.security.principal
cn=directory manager Object successfully added.
```

Dans les "Stockage des objets Fabrique de connexion" à la page 400 `imqAddressList` définit le nom d'hôte du serveur/courtier JMS (`gwenig.coopsrc.com`), le port (`7676`) et la méthode d'accès (`jms`).

Stockage des objets Destination

Dans l'outil de ligne de commande de Message Queue (`imqobjmgr`), saisissez les commandes de "Stockage des objets Destination" à la page 401 pour stocker les objets Destination.

EXEMPLE 11–2 Stockage des objets Destination

```
#> ./imqobjmgr add -l "cn=mytestDestination"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t q -o "imqDestinationName=mytestDestination"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description]
A Description for the Destination Object imqDestinationName [Destination Name]
mytestDestination Using the following lookup name: cn=mytestDestination
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/ ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager Object successfully added.
```

Vous pouvez contrôler l'objet nouvellement créé avec une `ldapsearch` ou un navigateur LDAP.

La section consacrée au stockage des objets administrés sur un serveur LDAP est terminée. Ignorez la section suivante, qui explique comment stocker les objets administrés dans un fichier et allez directement à la section consacrée à la "Configuration de l'adaptateur Listener JMS pour ce scénario" à la page 403.

Stockage des objets administrés dans un fichier

PasswordSync et le Listener JMS peuvent être configurés pour utiliser les objets administrés stockés dans un fichier. Si vous ne stockez pas les objets administrés sur un serveur LDAP ("Stockage des objets administrés dans un annuaire LDAP" à la page 399), suivez les instructions de cette section.

Stockage des objets Fabrique de connexion

Ouvrez l'outil de ligne de commande de Message Queue (`imqobjmgr`) et saisissez les commandes de "Stockage des objets Fabrique de connexion" à la page 402 pour stocker les objets Fabrique de connexion et indiquer un nom de recherche.

EXEMPLE 11–3 Stockage des objets Fabrique de connexion et spécification de noms de recherche

```
#> ./imqobjmgr add -l "mytestFactory" -j
"java.naming.factory.initial= com.sun.jndi.fscontext.RefFSContextFactory"
 -j "java.naming.provider.url=file:///home/gael/tmp" -t qf -o
 "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name:
mytestFactory
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
To specify a destination:
#> ./imqobjmgr add -l "mytestQueue" -j
"java.naming.factory.initial=com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t q -o
"imqDestinationName=myTestQueue"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination
Object imqDestinationName [Destination Name] myTestQueue
Using the following lookup name:
mytestQueue
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
```

Création de la destination sur le courtier

Par défaut, le courtier Sun Message Queue permet de créer automatiquement la destination de la file d'attente (voir `config.properties`, où la valeur par défaut de `imq.autocreate.queue` est `true`).

Si la destination de la file d'attente n'est pas créée automatiquement, vous devez créer l'objet Destination sur le courtier en utilisant la commande indiquée dans "Création de la destination sur le courtier" à la page 402 (où *myTestQueue* est la destination).

EXEMPLE 11–4 Création d'un objet Destination sur le courtier

```
name (Queue name):
#> cd /opt/sun/mq/bin
#>./imqcmd create dst -t q -n mytestQueue
Username: <admin>
Password: <admin>
Creating a destination with the following attributes:
Destination Name mytestQueue
Destination Type Queue On the broker specified by:
------------------------
Host Primary Port
------------------------ localhost 7676
Successfully created the destination.
```

Vous pouvez stocker les objets administrés dans un annuaire ou dans un fichier :

- **Dans un annuaire :** utiliser un annuaire permet de stocker les objets Fabrique de connexion et Destination de manière centralisée.

  Quand vous utilisez un annuaire, ces objets administrés sont stockés sous la forme d'entrées d'annuaire.

  Remarque – Si la servlet PasswordSync d'Identity Manager et le serveur d'Identity Manager ne sont pas la même machine, chacune des machines doit pouvoir accéder au fichier `.bindings`. Vous pouvez répéter deux fois (une par machine) la création des objets administrés ou copier le fichier `.bindings` dans l'emplacement approprié sur chaque machine.

- **Dans un fichier :** si la servlet PasswordSync d'Identity Manager et le serveur d'Identity Manager sont exécutés sur le même serveur (ou si vous n'avez pas d'annuaire disponible), vous pouvez stocker les objets administratifs dans un fichier.

  Lorsque vous utilisez un fichier, les deux objets administrés sont stockés dans un unique fichier (appelé `.bindings` sous à la fois Windows et UNIX), sous le répertoire que vous spécifiez pour le java.naming.provider.url (par exemple, `file:///c:/temp` sous Windows ou `file:///tmp` sous UNIX).

Configuration de l'adaptateur Listener JMS pour ce scénario

Configurez l'adaptateur Listener JMS sur le serveur d'application. Suivez les instructions de la section “Ajout et configuration d'un adaptateur Listener JMS” à la page 392.

Configuration d'Active Sync

Configurez ensuite le listener JMS pour la synchronisation. Active Sync est requis si vous utilisez JMS, mais n'est pas utilisé pour les connexions directes.

▼ Pour configurer le listener JMS pour la synchronisation

1. **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**
2. **Dans la Liste des ressources, cochez la case à cocher Listener JMS.**
3. **Dans la liste Actions de ressource, sélectionnez Éditer la stratégie de synchronisation.**

   La page Éditer la stratégie de synchronisation relative à la ressource Listener JMS s'ouvre (Figure 11–15).

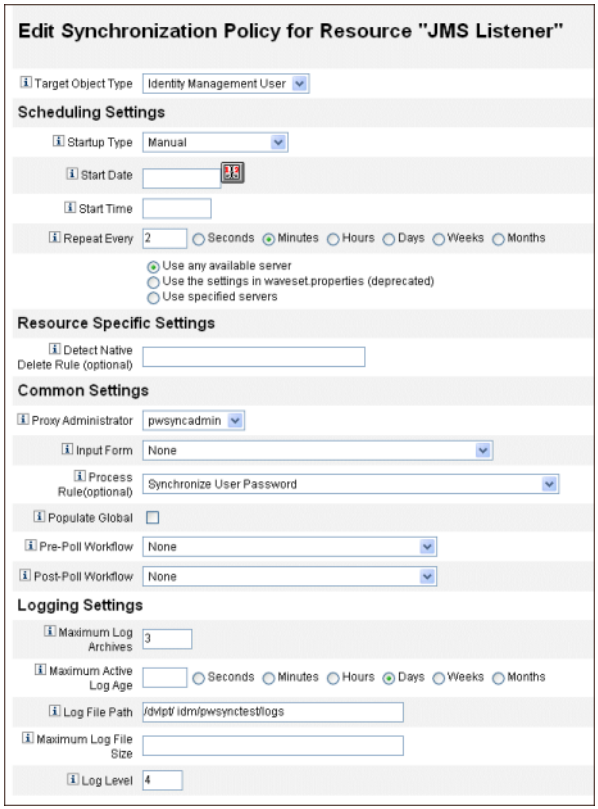


FIGURE 11–15 Configuration d'Active Sync pour le listener JMS

4. **Sous Paramètres communs, localisez Administrateur mandataire et sélectionnez** `pwsyncadmin` **(cet administrateur est associé à un formulaire vide).**

5. **Sous Paramètres communs, localisez Règle de traitement et sélectionnez Synchronize User Password (Synchroniser le mot de passe de l'utilisateur) dans la liste. Le flux de travaux Synchronize User Password par défaut accepte chaque demande provenant de l'adaptateur Listener JMS, contrôle l'afficheur ChangeUserPassword puis enregistre de nouveau l'afficheur ChangeUserPassword.**

6. **Indiquez dans la zone Chemin d'accès du fichier le chemin du répertoire dans lequel les fichiers journaux actif et archivés doivent être créés.**

7. **À des fins de débogage, définissez le Niveau du journal sur 4 pour générer un journal détaillé.**

8. **Cliquez sur Enregistrer.**

Test de la configuration

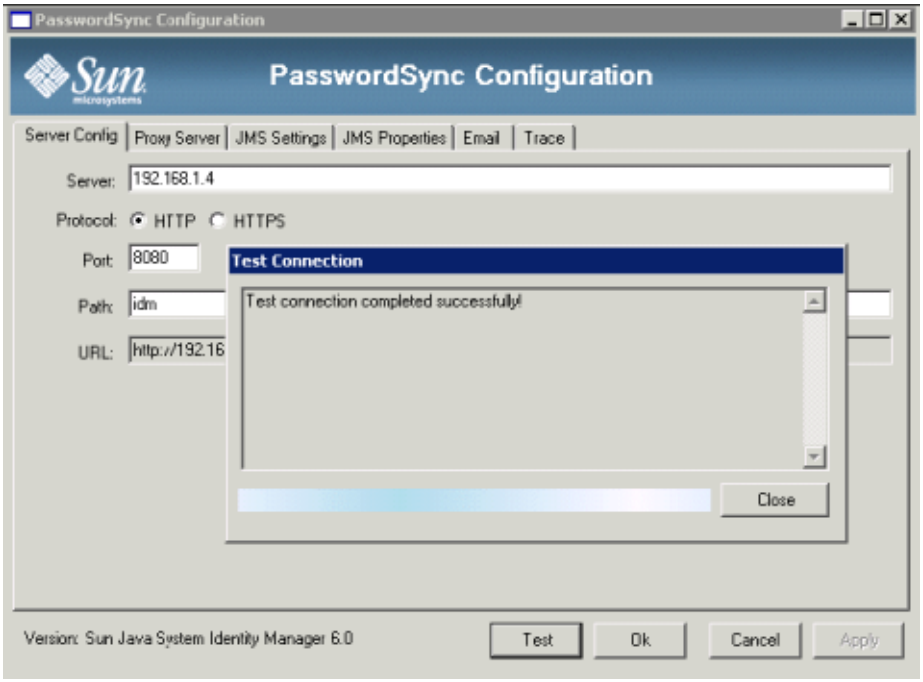
Vous pouvez utiliser l'application Windows PasswordSync Configuration pour déboguer le côté Windows de votre configuration.

1. **Démarrez l'application de configuration de PasswordSync si elle n'est pas déjà en cours d'exécution.**

   Par défaut, l'application de configuration est installée dans Program Files → Sun Java System Identity Manager PasswordSync → Configuration.

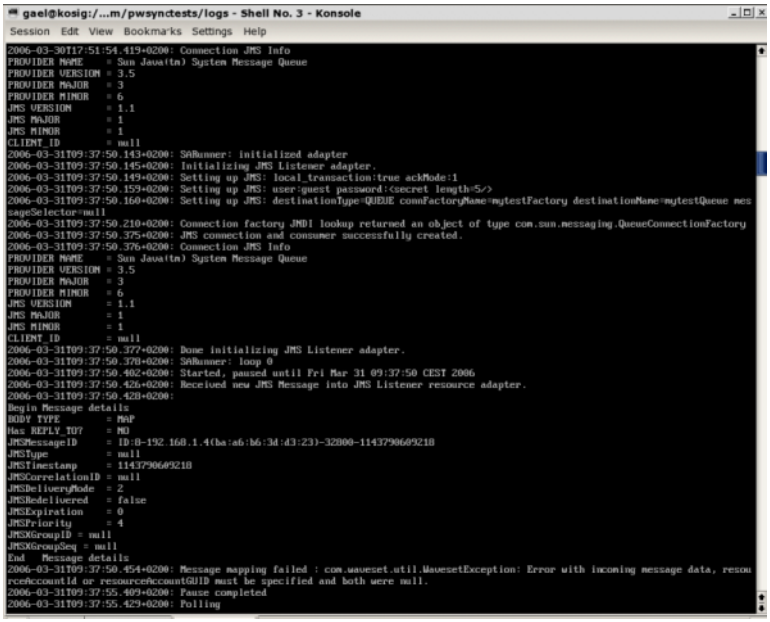
2. **Quand la boîte de dialogue de configuration de PasswordSync s'affiche, cliquez sur le bouton Essai.**

3. **Si vous utilisez JMS, la boîte de dialogue Vérifier la connexion s'affiche avec un message indiquant si la vérification de la connexion s'est terminée avec succès.**



4. Cliquez sur Fermer pour fermer la boîte de dialogue Vérifier la connexion.
5. Cliquez sur OK pour fermer la boîte de dialogue de configuration de PasswordSync.

   L'adaptateur Listener JMS s'exécute ensuite en mode débogage et génère des informations de débogage dans un fichier, similaire à celui de la figure suivante.



Débogage de PasswordSync sous Windows

PasswordSync écrit tous les échecs dans l'Observateur d'événements de Windows (si vous avez besoin d'aide pour utiliser l'Observateur d'événements, reportez-vous à l'aide de Windows). Le nom de la source pour les entrées du journal des erreurs est *PasswordSync*.

Pour toute information sur le dépannage de PasswordSync sous Windows, voir le *Sun Identity Manager 8.1 System Administrator's Guide*.

Désinstallation de PasswordSync sous Windows

Pou désinstaller l'application PasswordSync, allez au Panneau de configuration de Windows et sélectionnez Ajout/Suppression de programmes. Sélectionnez ensuite Sun Java System Identity Manager PasswordSync et cliquez sur Supprimer.

Remarque – PasswordSync peut aussi être désinstallé (ou réinstallé) en chargeant le support d'installation d'Identity Manager et en cliquant sur l'icône `pwsync\IdmPwSync.msi`.

Vous devez redémarrer votre système pour compléter le processus.

Foire Aux Questions relative à PasswordSync

Cette section répond à certaines questions fréquemment posées sur PasswordSync.

Question : PasswordSync peut-il être implémenté sans Java Messaging Service ?

Réponse : Oui, mais procéder de la sorte élimine les avantages découlant de l'utilisation d'un JMS pour suivre les événements de changement de mot de passe.

Pour implémenter PasswordSync sans JMS, lancez l'application de configuration avec l'indicateur suivant :

```
Configure.exe -direct
```

Lorsque l'indicateur `-direct` est spécifié, l'application de configuration affiche l'onglet User (Utilisateur).

Si vous implémentez PasswordSync sans JMS, il est inutile de créer un adaptateur Listener JMS. Vous pouvez par conséquent ignorer les procédures listées dans la section "Déploiement de PasswordSync sur le serveur d'application" à la page 392. Si vous souhaitez configurer des notifications, vous devrez peut être modifier le flux de travaux Change User Password (Changer le mot de passe utilisateur).

Remarque – Si vous exécutez ensuite l'application de configuration sans spécifier l'indicateur `-direct`, PasswordSync aura besoin d'un JMS pour être configuré. Relancez l'application avec l'indicateur `-direct` pour éviter de nouveau le JMS.

Question : PasswordSync peut-il être utilisé en conjonction avec d'autres filtres de mots de passe Windows utilisés pour appliquer les stratégies de mot de passe personnalisées ?

Réponse : Oui, vous pouvez utiliser PasswordSync en conjonction avec d'autres filtres de mots de passe `_WINDOWS_`. PasswordSync devra toutefois être le dernier filtre de mots de passe listé dans la valeur de registre Notification Package (Package de notification).

Vous devez utiliser le chemin de registre suivant :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages (value of type REG_MULTI_SZ)
```

Par défaut, le programme d'installation place l'intercepteur de mots de passe Identity Manager en fin de liste, mais si vous avez installé le filtre de mots de passe personnalisé après l'installation, vous devrez déplacer `lhpwic` à la fin de la liste Notification Packages (Packages de notification).

Vous pouvez utiliser PasswordSync en conjonction avec d'autres stratégies de mot de passe Identity Manager. Lorsque les stratégies sont contrôlées sur le côté serveur d'Identity Manager, toutes les stratégies de mot de passe de ressource doivent réussir pour que la synchronisation du mot de passe soit transmise à d'autres ressources. C'est pourquoi vous devez rendre la stratégie de mot de passe Windows native aussi restrictive que la plus restrictive des stratégies de mot de passe définies dans Identity Manager.

Remarque – Le DLL intercepteur de mots de passe ne met pas en œuvre de stratégies de mot de passe.

Question : La servlet PasswordSync peut-elle être installée sur un serveur d'application autre qu'Identity Manager ?

Réponse : Oui. La servlet PasswordSync a besoin des fichiers `jar` `spml.jar` et `idmcommon.jar` en plus de tous les fichiers `jar` requis par l'application JMS.

Question : Le service PasswordSync envoie-t-il les mots de passe au serveur `lh` en texte clair ?

Réponse : Même si les pratiques recommandées préconisent d'exécuter PasswordSync sur SSL, toutes les données sensibles sont chiffrées avant d'être envoyées au serveur Identity Manager.

Pour toute information, voir "Configuration de PasswordSync pour SSL" à la page 380.

Question : Pourquoi certains changements de mot de passe résultent-ils en `com.waveset.exception.ItemNotLocked` ?

Réponse : Si vous activez PasswordSync, un changement de mot de passe (même initié depuis l'interface utilisateur) se traduit par un changement de mot de passe sur la ressource, ce qui fait que la ressource contacte Identity Manager.

Si vous configurez correctement la variable de flux de travaux `passwordSyncThreshold`, Identity Manager examine l'objet Utilisateur et décide qu'il a déjà géré le changement de mot de passe. Cependant, si l'utilisateur ou l'administrateur effectue un autre changement de mot de passe pour le même utilisateur au même moment, l'objet Utilisateur peut être verrouillé.

◆ ◆ ◆ CHAPITRE 12

Sécurité

Ce chapitre contient des informations sur les fonctionnalités de sécurité d'Identity Manager et détaille les étapes à suivre pour réduire encore les risques.

Lisez les rubriques suivantes pour en savoir plus sur la gestion de la sécurité des systèmes avec Identity Manager.

Fonctionnalités de sécurité

Identity Manager favorise une diminution des risques de sécurité grâce aux fonctionnalités suivantes :

- **Désactivation instantanée de l'accès aux comptes**. Identity Manager permet de désactiver les droits d'accès des organisations ou des individus en une unique opération.
- **Limitation des sessions de connexion**. Vous pouvez définir des limites concernant les sessions de connexion simultanées.
- **Analyse de risque active**. Identity Manager scanne sans interruption le système pour détecter les éléments constituant des risques pour la sécurité tels que les comptes inactifs et les manipulations de mot de passe suspectes.

- **Gestion complète des mots de passe**. Des capacités de gestion de mots de passe complètes et flexibles assurent un contrôle d'accès total.
- **L'audit et la génération de rapports permettent de contrôler les activités d'accès** Vous pouvez exécuter un vaste éventail de rapports pour fournir des informations ciblées sur les activités d'accès (pour plus d'informations sur les fonctionnalités de génération de rapports, voir le Chapitre 8, “Génération de rapports”).
- **Contrôle granulaire des privilèges administratifs**. Vous pouvez accorder et gérer le contrôle administratif dans Identity Manager en assignant une unique Capacité à un utilisateur ou une gamme d'obligations administratives définie par le biais de rôles admin.
- **Chiffrement des clés du serveur**. Identity Manager permet de créer et de gérer des clés de chiffrement du serveur par le biais de la zone Tâches.

De plus, l'architecture du système cherche à réduire dès que possible les risques de sécurité. Par exemple, une fois déconnecté, vous ne pouvez plus accéder aux pages visitées au préalable en utilisant la fonctionnalité *Précédent* de votre navigateur.

Limitation des sessions de connexion simultanées

Par défaut, un utilisateur Identity Manager peut avoir plusieurs sessions de connexion simultanées. Vous pouvez limiter les sessions simultanées à une session par application de connexion en ouvrant l'objet Configuration système pour le modifier (“Édition des objets Configuration Identity Manager” à la page 118) et en éditant la valeur de l'attribut Configuration `security.authn.singleLoginSessionPerApp`. Cet attribut est un objet qui contient un attribut pour chaque nom d'application de connexion (par exemple, l'interface administrateur, l'interface utilisateur ou Identity Manager IDE). Remplacer sa valeur par `true` impose une unique session de connexion pour chaque utilisateur.

Dans ce cas, un utilisateur peut se connecter à plus d'une seule session, mais seule la dernière session de connexion demeure active et valide. Si l'utilisateur exécute une action dans une session invalide, il est automatiquement déconnecté de la session et celle-ci se termine.

Gestion des mots de passe

Identity Manager propose plusieurs niveaux de gestion de mots de passe :

- **Gestion des changements administratifs**
  - Vous pouvez changer le mot de passe d'un utilisateur depuis plusieurs emplacements (les pages Éditer l'utilisateur, Rechercher des utilisateurs ou Changement du mot de passe).
  - Permet de changer les mots de passe sur n'importe laquelle des ressources d'un utilisateur grâce à la sélection granulaire des ressources.

- **Réinitialisation des mots de passe administratifs**
  - Permet de générer des mots de passe aléatoires.
  - Permet d'afficher les mots de passe pour l'utilisateur final ou l'administrateur.
- **Mot de passe de changement utilisateur**
  - Fournit un service de changement de mot de passe en libre-service pour l'utilisateur final sur

    http://*localhost*:8080/idm/user
  - En option, permet de personnaliser la page du libre-service pour qu'elle corresponde à l'environnement de l'utilisateur final.
- **Données de mise à jour des utilisateurs**

  Permet de paramétrer tout attribut de schéma utilisateur devant être géré par l'utilisateur final.
- **Récupération d'accès utilisateur**.
  - Utilise les réponses d'authentification pour accorder à un utilisateur le droit d'accès nécessaire pour changer son mot de passe.
  - Utilise l'authentification d'intercommunication pour accorder un droit d'accès à un utilisateur en utilisant l'un de plusieurs mots de passe
- **Stratégies de mot de passe**

  Utilisent des règles pour définir les paramètres des mots de passe.

Authentification d'intercommunication

L'authentification d'intercommunication permet d'accorder des droits d'accès utilisateur et administrateur par le biais de un ou plusieurs mots de passe différents.

Identity Manager gère l'authentification à travers l'implémentation des éléments suivants :

- *applications de connexion* (ensemble de groupes de modules de connexion),
- *groupes de modules de connexion* (ensemble ordonné de modules de connexion),
- *modules de connexion* (définissez l'authentification pour chaque ressource assignée et spécifiez une exigence de réussite parmi plusieurs pour l'authentification).

À propos des applications de connexion

Les applications de connexion définissent un ensemble de groupes de modules de connexion, qui définissent eux-mêmes l'ensemble et l'ordre des modules de connexion utilisés lorsqu'un utilisateur se connecte à Identity Manager. Chaque application de connexion comprend un ou plusieurs groupes de modules de connexion.

Au moment de la connexion, l'application de connexion vérifie son ensemble de groupes de modules de connexion. Si seul un groupe de modules de connexion est défini, il est utilisé et les modules de connexion qu'il contient sont traités dans l'ordre défini à l'intérieur du groupe. Si l'application de connexion comporte plusieurs groupes de modules de connexion définis, Identity Manager vérifie les *règles de contrainte de connexion* appliquées à chaque groupe de modules pour déterminer celui à traiter.

Règles de contrainte de connexion

Les règles de contrainte de connexion sont appliquées aux groupes de modules de connexion. Dans chacun des ensembles de groupes de modules d'une application de connexion, seul un groupe peut ne pas se voir appliquer de règle de contrainte de connexion.

Pour déterminer, dans un ensemble, celui des groupes de modules de connexion qui doit être traité, Identity Manager évalue la compatibilité du premier groupe de modules de connexion avec la règle de contrainte. Si ce premier groupe de modules de connexion respecte la règle, il est traité par Identity Manager. Si ce groupe ne respecte pas la règle, Identity Manager évalue tous les groupes de modules de connexion les uns après les autres jusqu'à ce que l'un des groupes soit conforme à la règle, ou qu'un groupe de modules de connexion auquel aucune règle de contrainte n'est appliquée soit évalué (et donc utilisé).

Remarque – Si une application de connexion contient plus d'un groupe de modules de connexion, le groupe auquel aucune règle de contrainte n'est appliquée doit être placé en dernière position dans l'ensemble des groupes.

Exemple de règle de contrainte de connexion

L'exemple suivant est un exemple de règle de contrainte de connexion basée sur l'emplacement. La règle récupère l'adresse IP du demandeur dans l'en-tête HTTP, puis vérifie si elle se trouve sur le réseau 192.168. Si l'adresse IP contient la valeur 192.168, la règle retourne la valeur true et le groupe de modules de connexion est sélectionné.

EXEMPLE 12–1 Règle de contrainte de connexion basée sur l'emplacement

```
<Rule authType='LoginConstraintRule' name='Sample On Local Network'>
<match> <ref>remoteAddr</ref> <s>192.168.</s> </match>
<MemberObjectGroups> <ObjectRef type='ObjectGroup' name='All'/> </MemberObjectGroups>
</Rule>
```

Édition des applications de connexion

Dans la barre de menu, sélectionnez Sécurité → Connexion pour accéder à la page Connexion.

La liste des applications de connexion affiche les éléments suivants :

- les différentes applications de connexion à Identity Manager (interfaces) définies ;
- les groupes de modules de connexion constituant l'application de connexion ;
- les limites de délai d'attente de la session Identity Manager définies pour chaque application de connexion.

Depuis la page Connexion, vous pouvez :

- créer des applications de connexion personnalisées ;
- supprimer des applications de connexion personnalisées ;
- gérer les groupes de modules de connexion.

Pour éditer une application de connexion, sélectionnez-la dans la liste.

Définition des limites des sessions Identity Manager

La page Modifier une application de connexion vous permet de définir un délai d'attente (limite) pour chaque session de connexion à Identity Manager. Sélectionnez les heures, minutes et secondes, puis cliquez sur Enregistrer. Les limites établies s'affichent dans la liste des applications de connexion.

Vous pouvez définir des délais d'attente de session pour chaque application de connexion à Identity Manager. Lorsqu'un utilisateur se connecte à une application Identity Manager, la valeur de délai d'attente de session actuellement configurée est utilisée pour calculer la date et l'heure à venir auxquelles la session de l'utilisateur expirera pour être restée inactive. La date calculée est ensuite stockée avec la session Identity Manager de l'utilisateur de sorte à pouvoir être contrôlée à chaque fois qu'une demande est formulée.

Si un administrateur de connexion modifie la valeur du délai d'attente de session d'une application de connexion, la nouvelle valeur sera appliquée pour toutes les connexions futures. Les sessions existantes expireront sur la base de la valeur en vigueur au moment de la connexion de l'utilisateur.

Les valeurs définies pour le délai d'attente HTTP s'appliquent à toutes les applications Identity Manager et ont la priorité sur la valeur de délai d'attente de session de l'application de connexion.

Désactivation de l'accès aux applications

Dans les pages Créer une application de connexion et Modifier une application de connexion, vous pouvez sélectionner l'option Désactiver pour désactiver une application de connexion et empêcher par là les utilisateurs de se connecter. Si un utilisateur essaie de se connecter à une

application désactivée, l'utilisateur est réacheminé sur une autre page indiquant que l'application est actuellement désactivée. Vous pouvez éditer le message qui s'affiche sur cette page en éditant le catalogue personnalisé.

Les applications de connexion restent désactivées jusqu'à ce que vous désélectionniez l'option. À titre de protection, vous ne pouvez pas désactiver la connexion de l'administrateur.

Édition des groupes de modules de connexion

La liste des groupes de modules de connexion affiche les éléments suivants :

- les différents groupes de modules de connexion ;
- les modules de connexion individuels qui constituent un groupe de modules de connexion ;
- si un groupe de modules de connexion contient des règles de contrainte.

Vous pouvez créer, éditer et supprimer des groupes de modules de connexion depuis la page Groupes de modules de connexion. Sélectionnez un groupe de modules de connexion dans la liste pour l'éditer.

Édition des modules de connexion

Saisissez les détails ou effectuez des sélections pour les modules de connexion comme indiqué ci-après (les options ne sont pas toutes disponibles pour tous les modules de connexion).

- **Exigence de réussite de connexion**. Sélectionnez une exigence applicable à ce module. Les sélections sont les suivantes :
  - **requis**. Le module de connexion doit réussir. Qu'il réussisse ou non, l'authentification passe au module de connexion suivant de la liste. S'il n'y a pas d'autre module de connexion, l'ouverture de session administrateur réussit.
  - **exigence**. Le module de connexion est requis pour la réussite de l'opération. En cas de réussite, l'authentification passe au module de connexion suivant de la liste. Dans le cas contraire, l'authentification s'arrête.
  - **suffisant**. Le module de connexion n'est pas requis pour la réussite de l'opération. En cas de réussite, l'authentification ne passe pas au module de connexion suivant et l'administrateur est connecté. Dans le cas contraire, l'authentification passe au module de connexion suivant de la liste.
  - **en option**. Le module de connexion n'est pas requis pour la réussite de l'opération. Que l'opération réussisse ou non, l'authentification passe au module de connexion suivant de la liste.

- **Attributs de recherche de connexion**. (LDAP uniquement). Indiquez une liste ordonnée de noms d'attributs utilisateur LDAP à utiliser lors des tentatives de liaison (connexion) au serveur LDAP associé. Chacun des attributs utilisateur LDAP indiqués, ainsi que le nom de connexion spécifié par l'utilisateur, est utilisé, en respectant l'ordre, pour rechercher un utilisateur LDAP correspondant. Ceci permet à un utilisateur de se connecter à Identity Manager en utilisant un cn LDAP ou une adresse e-mail (quand Identity Manager est configuré pour l'intercommunication avec LDAP).

  Par exemple, si vous indiquez ce qui suit et que l'utilisateur tente de se connecter sous le nom `gwilson`, la ressource LDAP va d'abord rechercher un utilisateur LDAP répondant au critère `cn=gwilson`.

  ```
  cn
  ```

  ```
  mail
  ```

  Si une correspondance est trouvée, une tentative de connexion est lancée avec le mot de passe indiqué par l'utilisateur. Si aucune correspondance n'est trouvée, la ressource LDAP va rechercher un utilisateur LDAP correspondant au critère `mail=gwilson`. Si cette opération se solde également par un échec, la connexion échoue.

  Si vous n'indiquez aucune valeur, les attributs de recherche LDAP par défaut sont les suivants :

  ```
  uid
  ```

  ```
  cn
  ```

- **Règle de corrélation de connexion**. Sélectionnez une règle de corrélation à utiliser pour mapper les informations de connexion fournies par l'utilisateur vers un utilisateur Identity Manager. Cette règle permet de rechercher un utilisateur Identity Manager à l'aide de la logique qui y est spécifiée. Cette règle doit retourner une liste d'une ou plusieurs conditions `AttributeConditions` qui serviront à rechercher un utilisateur Identity Manager concordant. La règle sélectionnée doit avoir l'authType `LoginCorrelationRule`. Pour la description des étapes suivies par Identity Manager pour mapper un ID utilisateur authentifié vers un utilisateur Identity Manager, voir l'Exemple 12–2.
- **Règle de nom de nouvel utilisateur**. Sélectionnez une règle de nom de nouvel utilisateur à utiliser lors de la création automatique de nouveaux utilisateurs Identity Manager dans le cadre de la connexion.

Cliquez sur Enregistrer pour enregistrer un module de connexion. Une fois le module enregistré, vous pouvez en choisir la position par rapport aux autres modules de connexion du groupe.

Attention – Si la configuration de connexion d'Identity Manager permet de s'authentifier sur plusieurs systèmes, il est recommandé d'utiliser les mêmes ID utilisateur et mot de passe de compte sur tous les systèmes cibles de l'authentification Identity Manager.

Si les combinaisons ID utilisateur/mot de passe diffèrent, la connexion échoue sur tous les systèmes dont l'ID utilisateur et le mot de passe ne correspondent pas à ceux saisis dans le formulaire Identity Manager User Login.

Certains de ces systèmes peuvent avoir une stratégie de blocage qui impose un nombre limite d'échecs de connexion au-delà duquel le compte est verrouillé. Pour ces systèmes, les comptes utilisateur peuvent être verrouillés même si la connexion de l'utilisateur à travers Identity Manager continue à fonctionner.

L'Exemple 12–2 contient un pseudocode qui décrit les étapes suivies par Identity Manager pour mapper les ID utilisateur authentifiés vers les utilisateurs Identity Manager.

EXEMPLE 12–2 Logique de traitement des modules de connexion

```
if an existing IDM user's ID is the same as the specified user ID

   if that IDM user has a linked resource whose resource name matches the
   resource that was authenticated and whose accountId matches the resource
   accountId returned by successful authentication (e.g. dn), then we have
   found the right IDM user

   otherwise if there is a LoginCorrelationRule associated with the
   configured login module

      evaluate it to see if it maps the login credentials to a single IDM
      user

      otherwise login fails

   otherwise login fails

if the specified userID does not match an existing IDM user's ID

   try to find an IDM user that has a linked resource whose resource
   name matches the resource accountID returned by successful authentication

     if found, then we have found the right IDM user

     otherwise if there is a LoginCorrelationRule associated with the
     configured login module
```

EXEMPLE 12–2 Logique de traitement des modules de connexion *(Suite)*

```
        evaluate it to see if it maps the login credentials to a single
        IDM user

        otherwise login fails

    otherwise login fails
```

Dans l'Exemple 12–2, le système essaie de trouver un utilisateur Identity Manager correspondant en utilisant les ressources reliées de l'utilisateur (informations sur les ressources). Si l'approche basée sur les informations sur les ressources échoue et qu'une règle loginCorrelationRule est configurée, le système essaie de trouver un utilisateur correspondant en utilisant cette règle.

Configuration de l'authentification pour les ressources communes

Si vous avez plusieurs ressources identiques sur le plan logique (par exemple, plusieurs serveurs de domaine Active Directory partageant une relation de confiance) ou plusieurs ressources résidant toutes sur le même hôte physique, vous pouvez spécifier que ces ressources sont des *ressources communes*.

Vous avez intérêt à déclarer les ressources communes car Identity Manager sait ainsi qu'il n'a à essayer et à s'authentifier qu'une fois auprès d'un groupe de ressources. Sinon, si un utilisateur saisit un mot de passe erroné, Identity Manager essaie le même mot de passe sur chaque ressource. Ceci peut entraîner le blocage du compte de l'utilisateur suite à de trop nombreux échecs de connexion, même si l'utilisateur n'a saisi qu'une fois le mot de passe erroné.

Avec les ressources communes, si un utilisateur s'authentifie auprès d'une ressource commune, Identity Manager essaie automatiquement et mappe l'utilisateur vers les ressources restantes du groupe de ressources communes. Par exemple, un compte utilisateur Identity Manager peut être lié à un compte de ressource pour la ressource AD-1. Le groupe de modules de connexion, cependant, peut définir que les utilisateurs doivent s'authentifier auprès de la ressource AD-2.

Si AD-1 et AD-2 sont définies comme des ressources communes (dans ce cas, dans le même domaine de confiance), si l'utilisateur réussit à s'authentifier auprès d'AD-2, Identity Manager peut mapper également l'utilisateur vers AD-1 en trouvant le même ID de compte utilisateur sur la ressource AD-1.

Attention – Toutes les ressources listées dans un groupe de ressources communes doivent également être incluses dans la définition du module de connexion. Si une liste complète des ressources communes ne figure pas dans la définition du module de connexion, cette fonctionnalité ne se comportera pas correctement.

Les ressources communes peuvent être définies dans l'objet Configuration système ("Édition des objets Configuration Identity Manager" à la page 118) en utilisant le format suivant.

EXEMPLE 12–3 Configuration de l'authentification pour les ressources communes

```
<Attribute name='common resources'>
<Attribute name='Common Resource Group Name'>
<List>
<String>Common Resource Name</String>
<String>Common Resource Name</String>
</List
</Attribute> </Attribute>
```

Configuration de l'authentification des certificats X509

Utilisez les informations et procédures suivantes pour configurer l'authentification des certificats X509 pour Identity Manager.

Prérequis pour la configuration

Pour prendre en charge l'authentification basée sur les certificats X509 dans Identity Manager, assurez-vous que l'authentification SSL bidirectionnelle (client et serveur) est configurée correctement. Du point de vue du client, cela signifie qu'un certificat d'utilisateur conforme X509 doit avoir été importé dans le navigateur (ou être disponible par le biais d'un lecteur de cartes à puce) et que le certificat de confiance doit être importé dans le keystore de certificats de confiance du serveur d'application Web.

Par ailleurs, le certificat client utilisé doit être activé pour l'authentification client.

▼ Pour vérifier que l'option authentification client du certificat client utilisé est sélectionnée

1. **En utilisant Internet Explorer, sélectionnez Outils puis Options Internet.**
2. **Sélectionnez l'onglet Contenu.**
3. **Dans la zone Certificats, cliquez sur Certificats.**

4 **Sélectionnez le certificat client puis cliquez sur Avancé.**

5 **Dans la zone réservée au but du certificat, vérifiez que l'option Authentification client est sélectionnée.**

Configuration de l'authentification basée sur les certificats X509 dans Identity Manager

▼ Pour configurer l'authentification basée sur les certificats X509

1 **Connectez-vous à l'interface administrateur en tant que Configurator (ou avec des permissions équivalentes).**

2 **Sélectionnez Configurer puis Connexion pour afficher la page Connexion.**

3 **Cliquez sur Gérer les groupes de modules de connexion pour afficher la page Groupes de modules de connexion.**

4 **Sélectionnez un groupe de modules de connexion dans la liste.**

5 **Sélectionnez Module de connexion Certification X509 Identity Manager dans la liste Assigner le module de connexion. Identity Manager affiche la page Modifier un module de connexion.**

6 **Définissez l'exigence de réussite de connexion.**

Les valeurs suivantes sont acceptables :

- **requis**. Le module de connexion est requis pour la réussite de l'opération. Que l'opération réussisse ou non, l'authentification passe au module de connexion suivant de la liste. S'il n'y a pas d'autre module de connexion, l'ouverture de session administrateur réussit.
- **exigence**. Le module de connexion est requis pour la réussite de l'opération. En cas de réussite, l'authentification passe au module de connexion suivant de la liste. Dans le cas contraire, l'authentification s'arrête.
- **suffisant**. Le module de connexion n'est pas requis pour la réussite de l'opération. En cas de réussite, l'authentification ne passe pas au module de connexion suivant et l'administrateur est connecté. Dans le cas contraire, l'authentification passe au module de connexion suivant de la liste.
- **en option**. Le module de connexion n'est pas requis pour la réussite de l'opération. Que l'opération réussisse ou non, l'authentification passe au module de connexion suivant de la liste.

7. **Sélectionnez une règle de corrélation de connexion. Il peut s'agir indifféremment d'une règle intégrée ou d'une règle de corrélation personnalisée (pour toute information sur la création de règles de corrélation personnalisées, voir la section suivante).**

8. **Cliquez sur Enregistrer pour revenir à la page Modifier un groupe de modules de connexion.**

9. **En option, triez de nouveau les modules de connexion (si plus d'un module de connexion est assigné au groupe de modules de connexion) et cliquez sur Enregistrer.**

10. **Assignez le groupe de modules de connexion à une application de connexion s'il ne l'est pas déjà. Dans la page Groupes de modules de connexion, cliquez sur Revenir aux applications de connexion puis sélectionnez une application de connexion. Après avoir assigné un groupe de modules de connexion à l'application, cliquez sur Enregistrer.**

Remarque – Si l'option `allowLoginWithNoPreexistingUser` est définie sur la valeur `true` dans le fichier `waveset.properties`, vous serez invité lorsque vous configurerez le Module de connexion Certification X509Identity Manager à sélectionner une Règle de nom de nouvel utilisateur. Cette règle permettra de déterminer la façon dont seront nommés les nouveaux utilisateurs créés lorsqu'ils ne seront pas trouvés par la `Règle de corrélation de connexion` associée. La règle de nom de nouvel utilisateur a les mêmes arguments d'entrée disponibles que la Règle de corrélation de connexion. Elle retourne une unique chaîne constituée du `nom d'utilisateur utilisé pour créer le nouveau compte utilisateur Identity Manager.` Un exemple de règle de nom de nouvel utilisateur figure dans `idm/sample/rules`, sous le nom `NewUserNameRules.xml`.

Création et importation d'une règle de corrélation de connexion

Le Module de connexion Certification X509 d'Identity Manager utilise une règle de corrélation pour déterminer comment mapper les données de certificat vers l'utilisateur Identity Manager approprié. Identity Manager inclut une règle de corrélation intégrée, nommée Corréler via X509 Certificate SubjectDN.

Vous pouvez aussi ajouter vos propres règles de corrélation. À titre d'exemple, consultez `LoginCorrelationRules.xml` dans le répertoire `idm/sample/rules`.

Toute règle de corrélation doit respecter les directives suivantes :

- Son attribut `authType` doit être défini sur `LoginCorrelationRule`.
- Elle doit retourner une instance de liste d'`AttributeConditions` qui sera utilisée par le module de connexion pour rechercher l'utilisateur Identity Manager associé. Par exemple, la règle de corrélation peur retourner une `AttributeCondition` qui recherche l'utilisateur Identity Manager associé par son adresse e-mail.

Les arguments transmis aux règles de corrélation de connexion sont les suivants :

- les champs des certificats X509 standard (par exemple `subjectDN`, `issuerDN` et les dates de validité) ;
- les propriétés d'extensions critiques et non critiques.

La convention de nommage pour les arguments de certificat transmis à la règle de corrélation de connexion est :

```
cert.field name.subfield name
```

Voici quelques exemples de noms d'arguments disponibles pour la règle :

- `cert.subjectDN`,
- `cert.issuerDN`,
- `cert.notValidAfter`,
- `cert.notValidBefore`,
- `cert.serialNumber`.

La règle de corrélation de connexion, en utilisant les arguments transmis, retourne une liste de une ou plusieurs `AttributeConditions`. Celles-ci sont utilisées par le Module de connexion Certification X509Identity Manager pour trouver l'utilisateur Identity Manager associé.

Une exemple de règle de corrélation de connexion nommé `LoginCorrelationRules.xml` est inclus dans `idm/sample/rules`.

Après avoir créé une règle de corrélation personnalisée, vous devez l'importer dans Identity Manager. Depuis l'interface administrateur, sélectionnez Configurer puis Importer le fichier d'échange pour utiliser l'utilitaire d'importation de fichiers.

Test de la connexion SSL

Pour tester la connexion SSL, allez à l'URL de l'interface de l'application configurée en utilisant SSL (par exemple, `https://idm007:7002/idm/user/login.jsp`). Vous êtes averti que vous entrez dans un site sécurisé et êtes invité à préciser quel certificat personnel envoyer au serveur Web.

Diagnostic des problèmes

Signalez tous les problèmes liés à l'authentification utilisant des certificats X509 comme des messages d'erreur sur le formulaire de connexion.

Pour des diagnostics plus complets, activez le suivi sur le serveur Identity Manager pour les classes et niveaux suivants :

- `com.waveset.session.SessionFactory 1`,
- `com.waveset.security.authn.WSX509CertLoginModule 1`,
- `com.waveset.security.authn.LoginModule 1`.

Si l'attribut de certificat client n'est pas nommé `javaxservlet.request.X509Certificate` dans la requête HTTP, vous recevrez un message indiquant que cet attribut est introuvable dans la requête HTTP.

▼ Pour corriger un nom d'attribut de certificat client dans une requête HTTP

1. **Activez le suivi pour `SessionFactory` pour afficher la liste complète des attributs HTTP et déterminer le nom du certificat X509.**
2. **Utilisez l'utilitaire de débogage d'Identity Manager ("Page de débogage d'Identity Manager" à la page 45) pour éditer l'objet `LoginConfig`.**
3. **Remplacez le nom de `<AuthnProperty>` dans `<LoginConfigEntry>` pour le Module de connexion Certification X509 Identity Manager par le nom correct.**
4. **Enregistrez puis réessayez.**

   Il est également possible que vous deviez supprimer puis ajouter de nouveau le Module de connexion Certification X509 Identity Manager dans l'application de connexion.

Utilisation et gestion du chiffrement

Le chiffrement est utilisé pour assurer la confidentialité et l'intégrité des données du serveur en mémoire et dans le référentiel, ainsi que celles de toutes les données transmises entre le serveur Identity Manager et la passerelle.

Les sections suivantes fournissent des informations supplémentaires sur l'utilisation et la gestion du chiffrement dans le serveur Identity Manager et la passerelle, et répondent aux questions relatives aux clés de chiffrement du serveur et de la passerelle.

Données protégées par chiffrement

Le tableau suivant indique les types de données qui sont protégés par chiffrement dans le produit Identity Manager ainsi que les codes utilisés pour protéger chaque type de données.

TABLEAU 12–1 Types de données protégés par chiffrement

Type de données	RSAMD5	Clé NIST Triple DES 168 bits (DESede/ECB/NoPadding)	Clé PKCS#5 basée sur des mots de passe Crypto 56 bits (PBEwithMD5andDES)
Clés de chiffrement du serveur		Valeur par défaut	Option de configuration
Clés de chiffrement de la passerelle		Valeur par défaut	Option de configuration
Mots du dictionnaire des stratégies	Oui		
Mots de passe utilisateur		Oui	
Historique des mots de passe utilisateur		Oui	
Réponses de l'utilisateur		Oui	
Mots de passe des ressources		Oui	
Historique des mots de passe des ressources	Oui		
Toute la charge utile entre le serveur et les passerelles		Oui	

Foire Aux Questions relative aux clés de chiffrement du serveur

Vous trouverez dans les sections suivantes les réponses aux questions fréquemment posées sur la source, l'emplacement, la maintenance et l'utilisation des clés de chiffrement du serveur.

Question : D'où viennent les clés de chiffrement du serveur ?

Réponse : Les clés de chiffrement du serveur sont des clés Triple-DES symétriques de 168 bits.

Le serveur prend en charge les deux types de clés suivants :

- **Clé par défaut**. Cette clé est compilée dans le code du serveur.
- **Clé générée de manière aléatoire**. Cette clé peut être générée au démarrage initial du serveur ou à tout moment où la sécurité de la clé actuelle est en question.

Question : Où les clés de chiffrement du serveur sont-elles conservées ?

Réponse : Les clés de chiffrement du serveur sont des objets conservés dans le référentiel. Il peut y avoir de nombreuses clés de chiffrement de données dans tout référentiel.

Question : Comment le serveur sait-il quelles clés utiliser pour le chiffrement et le rechiffrement des données chiffrées ?

Réponse : Toute donnée chiffrée stockée dans le référentiel comporte un préfixe qui est l'ID de la clé de chiffrement du serveur qui a été utilisée pour la chiffrer. Lorsqu'un objet contenant des données chiffrées est lu en mémoire, Identity Manager utilise la clé de chiffrement de serveur associée au préfixe ID des données chiffrées à déchiffrer puis les rechiffre avec la même clé si les données sont modifiées.

Question : Comment puis-je mettre à jour les clés de chiffrement du serveur ?

Réponse : Identity Manager fournit une tâche appelée Gérer le chiffrement du serveur.

Cette tâche permet à un administrateur de sécurité autorisé d'effectuer plusieurs tâches de gestion de clés, notamment :

- générer une nouvelle clé de serveur « actuelle » ;
- re-chiffrer des objets existants, par type, contenant des données chiffrées avec la clé de serveur « actuelle ».

Pour plus d'informations sur l'utilisation de cette tâche, voir "Gestion du chiffrement du serveur" à la page 429 dans ce même chapitre.

Question : Qu'arrive-t-il aux données chiffrées existantes si la clé de serveur « actuelle » est changée ?

Réponse : Rien. Les données chiffrées existantes continueront à être déchiffrées ou rechiffrées avec la clé référencée par le préfixe ID des données chiffrées. Si une nouvelle clé de chiffrement du serveur est générée et définie comme étant la clé « actuelle », toutes les nouvelles données à chiffrer utiliseront cette nouvelle clé du serveur.

Pour éviter les problèmes liés à la cœxistence de plusieurs clés tout en maintenant un haut niveau d'intégrité des données, utilisez la tâche Gérer le chiffrement du serveur pour rechiffrer toutes les données chiffrées existantes avec la clé de chiffrement de serveur « actuelle ».

Question : Que se passe-t-il quand vous importez des données chiffrées pour lesquelles aucune clé de chiffrement n'est disponible ?

Réponse : Si vous importez un objet contenant des données chiffrées, mais que ces données ont été chiffrées avec une clé qui ne figure pas dans le référentiel dans lequel elles sont importées, ces données seront importées mais pas déchiffrées.

Question : Comment les clés du serveur sont-elles protégées ?

Réponse : Si le serveur n'est pas configuré pour utiliser le chiffrement basé sur les mots de passe (PBE) - PKCS#5 (défini dans l'objet Configuration système en utilisant l'attribut `pbeEncrypt` ou la tâche Gérer le chiffrement du serveur), la clé par défaut est utilisée pour chiffrer les clés du serveur. La clé par défaut est la même pour toutes les installations d'Identity Manager.

Si le serveur est configuré pour utiliser le chiffrement PBE, une clé PBE est générée à chaque fois que le serveur est démarré. La clé PBE est générée en fournissant un mot de passe, généré à

partir d'un secret spécifique au serveur, au chiffrement PBEwithMD5andDES. La clé PBE est uniquement conservée dans la mémoire et n'est jamais persistante. De plus, la clé PBE est la même pour tous les serveurs partageant le même référentiel.

Pour activer le chiffrement PBE des clés du serveur, le chiffrement PBEwithMD5andDES doit être disponible. Identity Manager n'inclut pas par défaut ce chiffrement dans ses packages mais il s'agit d'un standard PKCS#5 disponible dans de nombreuses implémentations de fournisseurs JCE tels que ceux fournis par Sun et IBM.

Question : Puis-je exporter les clés du serveur pour les stocker de manière sûre à l'extérieur ?

Réponse : Oui. Si les clés du serveur sont chiffrées avec PBE, elle seront déchiffrées puis rechiffrées avec la clé par défaut avant d'être exportées. Ceci permettra de les importer sur le même ou sur un autre serveur à une date ultérieure, indépendamment de la clé PBE du serveur local. Si les clés du serveur sont chiffrées avec la clé par défaut, aucun traitement ne sera effectué avant leur exportation.

Lorsqu'elles sont importées sur un serveur configuré pour les clés PBE, les clés sont déchiffrées puis rechiffrées avec la clé PBE du serveur local si ce serveur est configuré pour le chiffrement par clés PBE.

Question : Quelles sont les données chiffrées entre le serveur et la passerelle ?

Réponse : Toutes les données (la charge utile) transmises entre le serveur et la passerelle sont chiffrées avec Triple-DES avec une clé symétrique par session serveur-passerelle générée de manière aléatoire de 168 bits.

Foire Aux Questions relative aux clés de passerelle

Vous trouverez dans les sections suivantes les réponses aux questions fréquemment posées sur la source, le stockage, la maintenance et la protection des clés de passerelle.

Question : Quelle est la source des clés de passerelle employées pour chiffrer ou déchiffrer les données ?

Réponse : À chaque fois qu'un serveur Identity Manager se connecte à une passerelle, le handshake initial génère une nouvelle clé Triple-DES aléatoire de 168 bits. Cette clé est utilisée pour chiffrer ou déchiffrer toutes les données transmises par la suite entre le serveur et cette passerelle. Une clé de session unique est générée pour chaque paire serveur/passerelle.

Question : Comment les clés sont-elles distribuées aux passerelles ?

Réponse : Les clés de session sont générées de manière aléatoire par le serveur puis échangées de manière sécurisée entre le serveur et la passerelle en étant chiffrées avec la clé maîtresse secrète partagée dans le cadre de l'handshake serveur-passerelle initial.

Lors du handshake initial, le serveur interroge la passerelle pour déterminer le mode que celle-ci prend en charge. La passerelle peut fonctionner dans les deux modes suivants :

- **Mode par défaut** . Le handshake de protocole serveur-passerelle initial est chiffré avec la clé Triple-DES de 168 bits par défaut, qui est compilée dans le code du serveur.
- **Mode sécurisé**. Une clé de passerelle Triple-DES aléatoire par référentiel partagé de 168 bits est générée et communiquée du serveur à la passerelle dans la cadre du protocole de handshake initial. Cette clé de passerelle est stockée dans le référentiel du serveur à l'instar des autres clés de chiffrement et l'est également par la passerelle dans le registre local de cette dernière.

  Lorsqu'une passerelle en mode sécurisé est contactée par un serveur, le serveur chiffre les données de test avec la clé de la passerelle et les envoie à la passerelle. La passerelle tente alors de déchiffrer les données de test, d'ajouter des données propres aux données de test, de rechiffrer le tout puis de renvoyer les données au serveur. Si le serveur réussit à déchiffrer les données de test et les données propres à la passerelle, il génère une clé de session serveur-passerelle unique qu'il chiffre avec la clé de la passerelle et l'envoie à cette dernière. À la réception, la passerelle déchiffre la clé de session et la conserve pour l'utiliser pendant la vie de la session serveur-à-passerelle. Si le serveur ne réussit pas à déchiffrer les données de test et les données propres à la passerelle, il chiffre la clé de la passerelle en utilisant la clé par défaut et les envoie à la passerelle. La passerelle déchiffre la clé de passerelle en utilisant sa clé par défaut compilée et stocke la clé de passerelle dans son registre. Le serveur chiffre ensuite la clé de session serveur-passerelle unique avec la clé de la passerelle puis l'envoie à la passerelle qui l'utilisera pendant la vie de la session serveur-à-passerelle.

  À partir de ce moment, la passerelle n'acceptera plus que les demandes émanant de serveurs ayant chiffré la clé de session avec sa clé de passerelle. Au démarrage, la passerelle contrôle s'il y a une clé dans le registre. S'il y en a une, elle l'utilise. S'il n'y en a pas, elle utilise celle par défaut. Une fois qu'elle a une clé définie dans le registre, la passerelle n'autorise plus l'établissement des sessions avec la clé par défaut, ce qui empêche des tiers de configurer un serveur indésirable et d'établir une connexion avec la passerelle.

Question : Puis-je mettre à jour les clés de passerelle utilisées pour chiffrer ou déchiffrer la charge utile serveur-à-passerelle ?

Réponse : Identity Manager fournit une tâche appelée Gérer le chiffrement du serveur qui permet à un administrateur de sécurité autorisé d'effectuer plusieurs tâches de gestion de clés et notamment de générer une nouvelle clé de passerelle « actuelle » et de mettre à jour toutes les passerelles avec cette clé de passerelle « actuelle ». Cette clé est celle utilisée pour chiffrer la clé par session utilisée pour protéger l'ensemble de la charge utile transmise entre le serveur et la passerelle. La clé de passerelle nouvellement générée sera chiffrée avec au choix la clé par défaut ou la clé PBE, selon la valeur de l'attribut `pbeEncrypt` dans l'objet Configuration système (“Édition des objets Configuration Identity Manager” à la page 118).

Question : Où les clés de passerelle sont-elles stockées sur le serveur, sur la passerelle ?

Réponse : Sur le serveur, la clé de la passerelle est stockée dans le référentiel comme les clés du serveur. Sur la passerelle, la clé de la passerelle est stockée dans une clé de registre locale.

Question : Comment les clés de la passerelle sont-elles protégées ?

Réponse : La clé de la passerelle est protégée de la même façon que les clés du serveur. Si le serveur est configuré pour utiliser le chiffrement PBE, la clé de la passerelle sera chiffrée avec une clé générée par PBE. Si l'option est false, elle sera chiffrée avec la clé par défaut. Pour plus d'informations, voir "Foire Aux Questions relative aux clés de chiffrement du serveur" à la page 425 .

Question : Puis-je exporter les clés de la passerelle pour les stocker de manière sûre à l'extérieur ?

Réponse : La clé de la passerelle peut être exportée en utilisant la tâche Gérer le chiffrement du serveur comme les clés du serveur. Pour plus d'informations, voir "Foire Aux Questions relative aux clés de chiffrement du serveur" à la page 425 .

Question : Comment les clés du serveur et de la passerelle sont-elles détruites ?

Réponse : Pour détruire les clés du serveur et de la passerelle, vous devez les supprimer du référentiel du serveur. Vous remarquerez qu'aucune clé ne doit être supprimée tant qu'il reste des données du serveur chiffrées avec cette clé ou une passerelle reposant sur cette clé. Utilisez la tâche Gérer le chiffrement du serveur pour rechiffrer toutes les données du serveur avec la clé actuelle du serveur et pour synchroniser la clé actuelle de la passerelle avec toutes les passerelles pour assurer qu'aucune clé obsolète n'est encore utilisée avant sa suppression.

Gestion du chiffrement du serveur

La fonctionnalité de chiffrement du serveur d'Identity Manager permet de créer de nouvelles clés de chiffrement de serveur 3DES et de les chiffrer en utilisant le chiffrement 3DES, PKCS#5 ou AES (Advanced Encryption Standard). Seuls les utilisateurs ayant des capacités Administrateur de la sécurité peuvent exécuter la tâche Gérer le chiffrement du serveur, qui est configurée depuis la page Gérer le chiffrement du serveur.

▼ Pour accéder à la page Gérer le chiffrement du serveur

Pour ouvrir la page Gérer le chiffrement du serveur :

1. **Sélectionnez Tâches du serveur > Exécuter des tâches.**
2. **Dans la page Tâches disponibles qui s'affiche, cliquez sur Gérer le chiffrement du serveur pour ouvrir la page éponyme.**

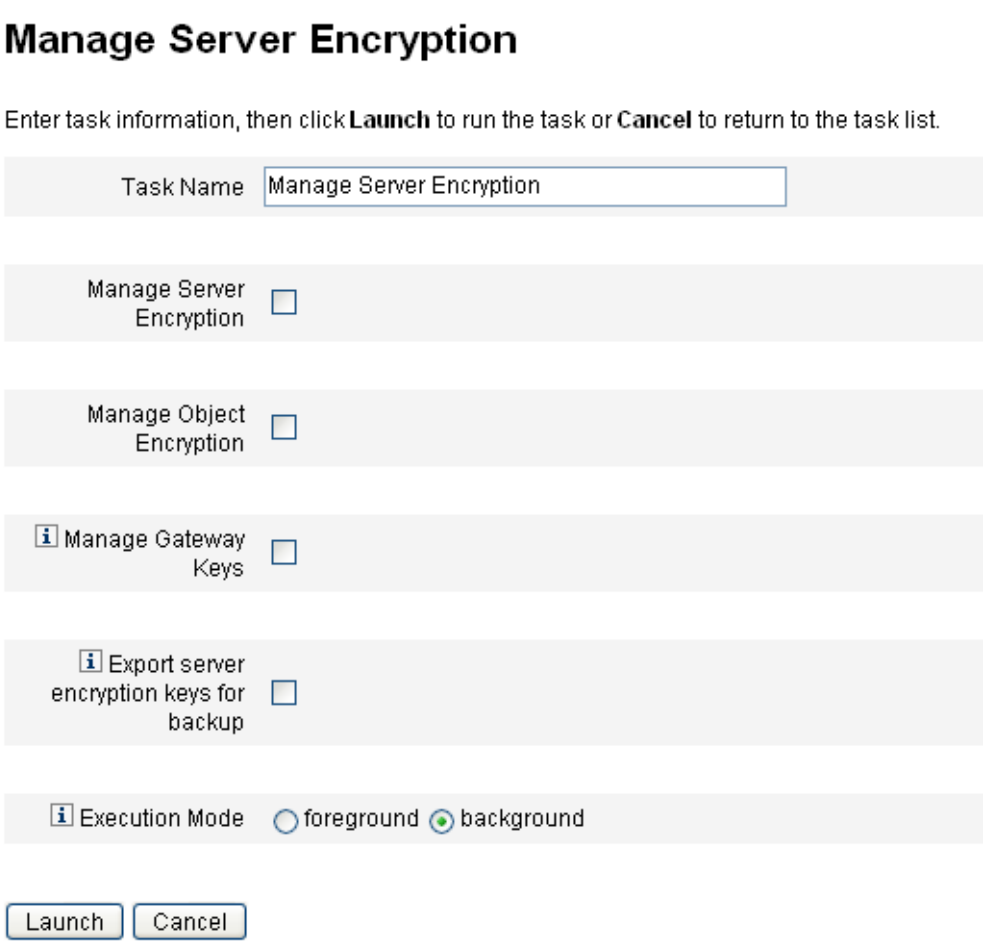


FIGURE 12–1 Page Gérer le chiffrement du serveur

▼ Pour configurer le chiffrement du serveur

Utilisez cette page pour configurer le chiffrement du serveur et des objets, les clés de passerelle, les options de sauvegarde et le mode d'exécution.

1 **Saisissez un nom dans Nom de la tâche.**

Ce champ est par défaut *Gérer le chiffrement du serveur*. Vous pouvez entrer un autre nom de tâche si vous ne voulez pas utiliser le paramètre par défaut.

2 **Choisissez une ou plusieurs des options suivantes.**

Pour faire votre sélection :

- **Gérer le chiffrement du serveur**. Choisissez cette option pour configurer le chiffrement du serveur.

  Les options supplémentaires suivantes s'affichent :

  - **Chiffrement des clés de chiffrement serveur**. Vous devez indiquer une méthode pour le chiffrement des clés de chiffrement du serveur. Les types de chiffrement peuvent être : Triple DES, PKCS#5 (DES), ou PKCS#5 (AES).

    Remarque –

    - Seuls les types de chiffrement instantiables sur votre système s'afficheront sur cette page. Par exemple, si votre système ne prend pas en charge PKCS#5 (AES), seuls Triple DES et PKCS#5 (DES) seront affichés.
    - Pour PKCS#5 (AES), vous devez télécharger et configurer les « Unlimited Strength Jurisdiction Policy Files » pour la JVM exécutant Identity Manager. Pour de plus amples détails, consultez la documentation de votre fournisseur Java.

      De plus, PKCS#5 (AES) requiert que vous installiez et configuriez le fichier `jar` `Bouncy Castle JCE provider` en fournisseur JCE pour la JVM exécutant Identity Manager. Ce fichier `jar` est packagé dans l'image d'installation d'Identity Manager et figure dans le répertoire *wshome*`/WEB-INF/lib`. Deux fichiers `jar`, `bcprov-jdk15-137.jar` et `bcprov-jdk16-137.jar`, sont fournis pour être utilisés avec les versions correspondantes de Java. Pour de plus amples détails, consultez la documentation de votre fournisseur Java et celle de Bouncy Castle.

  - **Générer une nouvelle clé de chiffrement serveur et la définir en tant que clé de chiffrement serveur actuelle**. Sélectionnez cette option pour générer une nouvelle clé de chiffrement de serveur. Toute donnée chiffrée générée après cette sélection sera chiffrée avec cette clé. La génération d'une nouvelle clé de chiffrement du serveur est sans effet sur la clé appliquée aux données chiffrées existantes.
  - **Générez un nouveau mot de passe PBE aléatoire sécurisé**. Sélectionnez cette option pour générer un nouveau mot de passe, basé sur un secret spécifique au serveur, à chaque fois que le serveur est démarré. Si vous ne sélectionnez pas cette option ou si votre serveur n'est pas configuré pour utiliser le chiffrement basé sur des mots de passe, Identity Manager utilisera la clé par défaut pour chiffrer les clés du serveur.
- **Gérer le chiffrement des objets**. Choisissez cette option pour indiquer les types d'objets qui doivent être rechiffrés et la méthode de chiffrement à utiliser.
  - **Chiffrement des types d'objets**. Choisissez l'un des types de chiffrement affichés, au choix Triple DES (valeur par défaut), Clé de 256 bits AES, Clé de 192 bits AES ou Clé de 128 bits AES.

Remarque – Pour AES avec des clés de 192 ou 256 bits, vous devez télécharger et configurer les « Unlimited Strength Jurisdiction Policy Files » pour la JVM exécutant Identity Manager. Pour de plus amples détails, consultez la documentation de votre fournisseur Java.

Seuls les types de chiffrement instantiables sur votre système s'afficheront sur cette page. Par exemple, si votre système ne prend pas en charge les clés AES de 192 ou 256 bits utilisant les « Unlimited Strength Jurisdiction Policy Files », seules les options Triple DES et Clé de 128 bits AES sont affichées.

- **Sélectionnez les types d'objets à rechiffrer à l'aide de la clé de chiffrement serveur actuelle**. Choisissez un ou plusieurs des types d'objets Identity Manager listés dans le tableau.

- **Gérer les clés de passerelle**. Choisissez cette option pour spécifier le chiffrement de la passerelle.

  Les options suivantes s'affichent :

  - **Sélectionner l'option de clé de passerelle**. Choisissez l'une des options suivantes :
    - **Générer une nouvelle clé et synchroniser toutes les passerelles**. Choisissez cette option quand vous commencez à activer un environnement de passerelle sécurisé. Une nouvelle clé de passerelle est créée et communiquée à toutes les passerelles.
    - **Synchroniser toutes les passerelles avec la clé de passerelle en cours**. Sélectionnez cette option pour synchroniser toute nouvelle passerelle ou les passerelles qui n'ont pas communiqué la nouvelle clé de passerelle. Utilisez cette option si une passerelle ne fonctionnait pas lors de la synchronisation de toutes les passerelles avec la clé actuelle ou pour imposer une mise à jour de clé pour une nouvelle passerelle.
  - **Type de clé de passerelle**. Choisissez l'un des types de chiffrement affichés, qui peuvent être Triple DES, Clé de 256 bits AES, Clé de 192 bits AES ou Clé de 128 bits AES.

    Remarque – Pour AES avec des clés de 192 ou 256 bits, vous devez télécharger et configurer les « Unlimited Strength Jurisdiction Policy Files » pour la JVM exécutant Identity Manager. Pour de plus amples détails, consultez la documentation de votre fournisseur Java.

    Seuls les types de chiffrement instantiables sur votre système s'afficheront sur cette page. Par exemple, si votre système ne prend pas en charge les clés AES de 192 ou 256 bits en utilisant les « Unlimited Strength Jurisdiction Policy Files », seules les options Triple DES et Clé de 128 bits AES sont affichées.

- **Exporter les clés de chiffrement serveur pour sauvegarde**. Choisissez cette option pour exporter les clés de chiffrement de serveur existantes dans un fichier formaté XML. Lorsque vous sélectionnez cette option, Identity Manager affiche un champ supplémentaire permettant de spécifier un chemin et un nom de fichier afin d'exporter les clés.

Remarque – Sélectionnez cette option si vous utilisez le chiffrement PKCS#5 et choisissez de générer et définir une nouvelle clé de chiffrement de serveur. Il est également recommandé de stocker les clés exportées sur un support amovible qui sera conservé dans un endroit sécurisé (et non sur un réseau).

---

3 **Choisissez le Mode d'exécution.**

Vous pouvez exécuter cette tâche au premier ou en arrière-plan (paramètre par défaut).

Remarque – Si vous choisissez de rechiffrer un ou plusieurs types d'objets avec une nouvelle clé, l'exécution de cette tâche peut être longue et il est préférable qu'elle s'exécute en arrière-plan.

---

4 **Lorsque vous avez terminé de configurer les options de cette page, cliquez sur Lancer.**

Utilisation des types d'autorisations pour sécuriser les objets

En règle générale, vous utiliserez les permissions spécifiées dans une capacité `AdminGroup` pour accorder l'accès à un `objectType` Identity Manager tel qu'une configuration, une règle ou une `TaskDefinition`. Cependant, accorder l'accès à tous les objets d'un `objectType` Identity Manager au sein d'une ou plusieurs organisations contrôlées est parfois trop étendu.

L'utilisation de types d'autorisations (`AuthType`) permet de mieux définir ou restreindre l'accès à un sous-ensemble d'objets pour un `objectType` Identity Manager donné. Vous pouvez, par exemple, ne pas vouloir accorder aux utilisateurs l'accès à toutes les règles rentrant dans leur étendue de contrôle lors du remplissage des règles pour la sélection dans un formulaire utilisateur.

Pour définir un nouveau type d'autorisation, éditez l'objet Configuration `AuthorizationTypes` dans le référentiel d'Identity Manager et ajoutez un nouvel élément `<AuthType>`.

Cet élément requiert les deux propriétés suivantes :

- le nom du nouveau type d'autorisations ;
- le type d'autorisation existant ou `objectType` que le nouvel élément étend ou définit.

Par exemple, pour ajouter un nouveau type d'autorisations Règle appelé `Marketing Rule`, qui étend `Rule`, vous devez définir ce qui suit :

```
<AuthType name='Marketing Rule' extends='Rule'/>
```

Ensuite, pour activer le type d'autorisations à utiliser, vous devez le référencer dans deux endroits :

- Au sein d'une capacité `AdminGroup` personnalisée qui accorde un ou plusieurs droits au nouveau type d'autorisations.
- Au sein des objets qui devraient être de ce type.

Voici des exemples de ces deux références. Dans le premier, une définition de capacité `AdminGroup` accorde l'accès à `Marketing Rules`.

EXEMPLE 12–4 Définition de capacité `AdminGroup`

```
<AdminGroup name='Marketing Admin'>
  <Permissions>
    <Permission type='Marketing Rule' rights='View,List,Connect,Disconnect/>
  </Permissions>
  <AdminGroups>
    <ObjectRef type='AdminGroup' id='#ID#Account Administrator'/>
  </AdminGroups>
</AdminGroup>
```

Dans l'exemple suivant, une définition `Rule` permet aux utilisateurs d'accéder à l'objet puisqu'ils se sont vus octroyer l'accès à `Rule` ou `Marketing Rule`.

EXEMPLE 12–5 Définition de `Rule`

```
<Rule name='Competitive Analysis Info' authType='Marketing Rule'>
 ...
</Rule>
```

Remarque – Tous les utilisateurs auxquels des droits d'accès à un type d'autorisations ou à un type statique étendu par un type d'autorisations, ont été accordés, auront les mêmes droits sur les types d'autorisations enfants. Ainsi, en utilisant l'exemple précédent, tout utilisateur auquel des droits d'accès à `Rule` auront été accordé bénéficiera des mêmes droits d'accès pour `Marketing Rule`. L'inverse toutefois n'est pas vrai.

Pratiques de sécurité

En tant qu'administrateur Identity Manager, vous pouvez réduire encore les risques de sécurité pour vos comptes et données protégés en suivant les recommandations ci-après, lors de l'installation et par la suite.

Lors de l'installation

Pour réduire les risques de sécurité pendant l'installation :

- Accédez à Identity Manager via un serveur Web sécurisé utilisant HTTPS.
- Réinitialisez les mots de passe des comptes administrateur Identity Manager par défaut (Administrator et Configurator). Pour renforcer encore la sécurité de ces comptes, vous pouvez les renommer.
- Limitez l'accès au compte Configurator.
- Limitez les ensembles de capacités des administrateurs aux seules actions nécessaires dans le cadre de leurs fonctions et limitez les capacités administrateur en configurant des hiérarchies organisationnelles.
- Changez le mot de passe par défaut du référentiel d'index d'Identity Manager.
- Activez l'audit pour suivre les activités dans l'application Identity Manager.
- Éditez les permissions sur les fichiers dans le répertoire d'Identity Manager.
- Personnalisez les flux de travaux pour insérer des approbations ou d'autres points de contrôle.
- Développez une procédure de récupération qui explique comment récupérer votre environnement Identity Manager en cas d'urgence.

Pendant l'utilisation

Pour diminuer les risques de sécurité pendant l'utilisation :

- Changez régulièrement les mots de passe des comptes administrateur Identity Manager par défaut (Administrator et Configurator).
- Déconnectez-vous d'Identity Manager lorsque vous n'utilisez pas le système de manière active.
- Définissez le délai d'attente par défaut d'une session Identity Manager. Les valeurs de délai d'attente des sessions peuvent varier car elles peuvent être définies indépendamment pour chaque application de connexion.

Si votre serveur d'application est conforme Servlet 2.2, le processus d'installation d'Identity Manager définit le délai d'attente des sessions HTTP sur une valeur par défaut de 30 minutes.

Vous pouvez changer cette valeur en éditant la propriété. Il convient d'ailleurs de la définir sur une valeur inférieure pour renforcer la sécurité. Ne la définissez pas sur une valeur supérieure à 30 minutes.

▼ Pour changer la valeur de délai d'attente des sessions

1. **Éditez le fichier `web.xml`, qui se trouve dans le répertoire `idm/WEB-INF` de la structure de répertoires de votre serveur d'application.**

2. **Changez la valeur numérique dans les lignes suivantes :**

```
<session-config>  <session-timeout>30</session-timeout></session-config>
```

◆ ◆ ◆ CHAPITRE 13

Audit des identités : principes de base

Ce chapitre présente les principes sur lesquels reposent l'audit des identités et les contrôles d'audit. Les contrôles d'audit peuvent être utilisés pour contrôler et gérer le contrôle et la compatibilité des systèmes et applications informatiques de l'entreprise.

Ce chapitre présente les principes et tâches suivants :

À propos de l'audit des identités

Identity Manager définit l'*audit* comme la capture, l'analyse, la réponse systématiques des/aux données d'identité à travers l'entreprise afin d'assurer la compatibilité avec les stratégies et réglementations internes et externes.

La conformité à la législation en matière de comptabilité et de confidentialité des données n'est pas une tâche aisée. Les fonctionnalités d'audit d'Identity Manager offrent une approche flexible vous permettant d'implémenter une solution de compatibilité qui fonctionne pour votre entreprise.

Dans la plupart des environnements, différents groupes sont concernés par la compatibilité : les équipes d'audit internes et externes (dont l'audit est le principal centre d'intérêt) et le personnel non lié à l'audit (qui peut percevoir l'audit comme une perte de temps). L'informatique est également souvent concernée par la compatibilité et facilite la transformation des exigences de l'équipe d'audit interne en l'implémentation de la solution choisie. La clé de l'implémentation réussie d'une solution d'audit est une capture précise des connaissances, contrôles et processus du personnel non lié à l'audit et l'automatisation de l'application de ces informations.

Objectifs de l'audit des identités

L'audit des identités améliore la performance d'audit comme suit :

- *L'audit des identités détecte automatiquement les violations de compatibilité et en facilite la résolution rapide grâce à une notification immédiate.*

  Les fonctionnalités de stratégie d'audit d'Identity Manager permettent de définir des *règles* (c'est-à-dire des critères) pour les violations. Une fois celles-ci définies, le système effectue un scannage à la recherche de conditions qui violent les stratégies établies, par exemple des changements d'accès non autorisés ou des privilèges d'accès erronés. Lorsqu'il détecte une de ces conditions, le système avertit les personnes appropriées conformément à une chaîne de signalisation définie. Les tâches appelées par les utilisateurs ou les flux de travaux automatiquement appelés par les violations de stratégie peuvent ensuite résoudre (corriger) la violation.

- *Il fournit des informations-clés, à la demande sur l'efficacité des contrôles d'audit internes*

  Les Rapports de l'auditeur fournissent des informations d'état sur les violations et les exceptions pour une analyse rapide de l'état de risque. L'onglet Rapports fournit également des rapports graphiques sur les violations. Vous pouvez afficher les violations par ressource, organisation ou stratégie, en personnalisant chaque diagramme en fonction de caractéristiques de rapport que vous définissez.

- *Il automatise les examens de certification des contrôles d'identité pour réduire le risque opérationnel.*

  Les capacités de flux de travaux activent la notification automatisée des violations de stratégie et d'accès à des examinateurs spécialisés.

- *Il prépare des rapports exhaustifs qui détaillent les activités des utilisateurs et satisfont les exigences règlementaires.*

  La zone Rapports permet de définir des rapports et des diagrammes détaillés fournissant des informations sur l'historique des accès et les privilèges et d'autres violations de stratégie. Le système conserve une piste d'audit d'identité sécurisée et complète qui peut être explorée par le biais des fonctionnalités de génération de rapports, pour les mises à jour des données d'accès et des profils des utilisateurs.

- *Il simplifie le processus des examens périodiques visant à maintenir la sécurité et la conformité aux réglementations.*

  Des examens d'accès périodiques peuvent être effectués pour collecter les enregistrements des habilitations des utilisateurs et déterminer les habilitations nécessitant un examen. Le processus avertit ensuite les attestateurs désignés des demandes en attente d'examen et met à jour le statut ou les demandes en attente une fois les actions de l'attestateur sur les demandes complétées.

- *Il identifie les capacités susceptibles de donner lieu à des conflits d'intérêt pour les comptes utilisateur*

Identity Manager fournit un Rapport de séparation des obligations qui identifie les utilisateurs ayant des capacités ou privilèges spécifiques susceptibles de donner lieu à un conflit d'intérêt potentiel.

Comprendre l'audit des identités

Identity Manager fournit une fonctionnalité permettant l'audit des privilèges et droits d'accès des comptes utilisateur ainsi qu'une fonctionnalité distincte pour le maintien et la certification de la compatibilité. Ces fonctionnalités sont la compatibilité basée sur des stratégies et les examens des accès périodiques.

Compatibilité basée sur des stratégies

Identity Manager emploie un système de stratégie d'audit qui permet aux administrateurs de maintenir la compatibilité des exigences établies par l'entreprise pour tous les comptes utilisateur.

Vous pouvez utiliser les stratégies d'audit pour assurer la compatibilité de deux manières à la fois différentes et complémentaires : la compatibilité continue et la compatibilité périodique.

Ces deux techniques sont particulièrement complémentaires dans un environnement dans lequel les opérations de provisioning peuvent être effectuées en dehors d'Identity Manager. Lorsqu'un compte peut être changé par un processus qui n'exécute pas ou ne respecte pas les stratégies d'audit existantes, la compatibilité périodique est nécessaire.

Compatibilité continue

Avec la compatibilité continue, une stratégie d'audit est appliquée à toutes les opérations de provisioning, de sorte qu'un compte ne peut pas être modifié d'une façon non conforme à la stratégie en cours.

Vous pouvez activer la compatibilité continue en assignant une stratégie d'audit à une organisation, un utilisateur ou ces deux éléments. Toutes les opérations de provisioning effectuées sur un utilisateur entraîneront une évaluation des stratégies assignées à l'utilisateur. Tout échec de stratégie résultant interrompra l'opération de provisioning.

Une stratégie *basée sur les organisations* est définie de manière hiérarchique. Il n'y a qu'un ensemble de stratégies d'organisation en vigueur pour un utilisateur donné. L'ensemble de stratégies appliqué est celui assigné à l'organisation de plus bas niveau. Par exemple :

Organisation	Ensemble de stratégies directement assigné	Stratégie effective
Austin	Stratégies A1, A2	Stratégies A1, A2
Marketing		Stratégies A1, A2
Développement	Stratégies B, C2	Stratégies B, C2
Assistance		Stratégies B, C2
Test	Stratégies D, E5	Stratégies D, E5
Finance		Stratégies A1, A2
Houston		<aucun(e)>

Compatibilité périodique

Dans le cadre de la *compatibilité périodique*, Identity Manager évalue la stratégie à la demande. Toute condition non conforme est capturée comme une violation de compatibilité.

Lors de l'exécution des scannages de compatibilité périodique, vous pouvez sélectionner les stratégies à inclure dans le scannage. Le processus de scannage mélange les stratégies directement assignées (c'est-à-dire celles assignées aux utilisateurs et aux organisations) et un ensemble arbitraire de stratégies sélectionnées.

Les utilisateurs Identity Manager ayant des capacités Administrateur Auditor peuvent créer des stratégies d'audit et contrôler la compatibilité avec ces stratégies en exécutant périodiquement des scannages de stratégie et des examens de violations de stratégie. Les violations peuvent être gérées par le biais des procédures de résolution et d'atténuation.

Pour plus d'informations sur les capacités Administrateur Auditor, voir "Comprendre et gérer les capacités" à la page 216 au Chapitre 6, "Administration".

L'audit d'Identity Manager permet des scannages d'utilisateurs réguliers. Ces scannages exécutent des stratégies d'audit pour détecter toute déviation par rapport aux limites de compte fixées. Lorsqu'une violation est détectée, les opérations de résolution sont lancées. Les règles peuvent être des règles de stratégie d'audit standard fournies par Identity Manager, ou des règles personnalisées définies par l'utilisateur.

Flux de tâches logiques pour la compatibilité basée sur les stratégies

La Figure 13–1 représente le flux de tâches suivi pour établir des contrôles d'audit basés sur des stratégies.

Examens d'accès périodiques

Identity Manager fournit des examens d'accès périodiques qui permettent aux directeurs et autres parties en charge d'examiner et de vérifier les privilèges d'accès des utilisateurs à une fréquence ad hoc ou périodique. Pour plus d'informations sur cette fonctionnalité, voir "Examens d'accès périodiques et attestations" à la page 484.

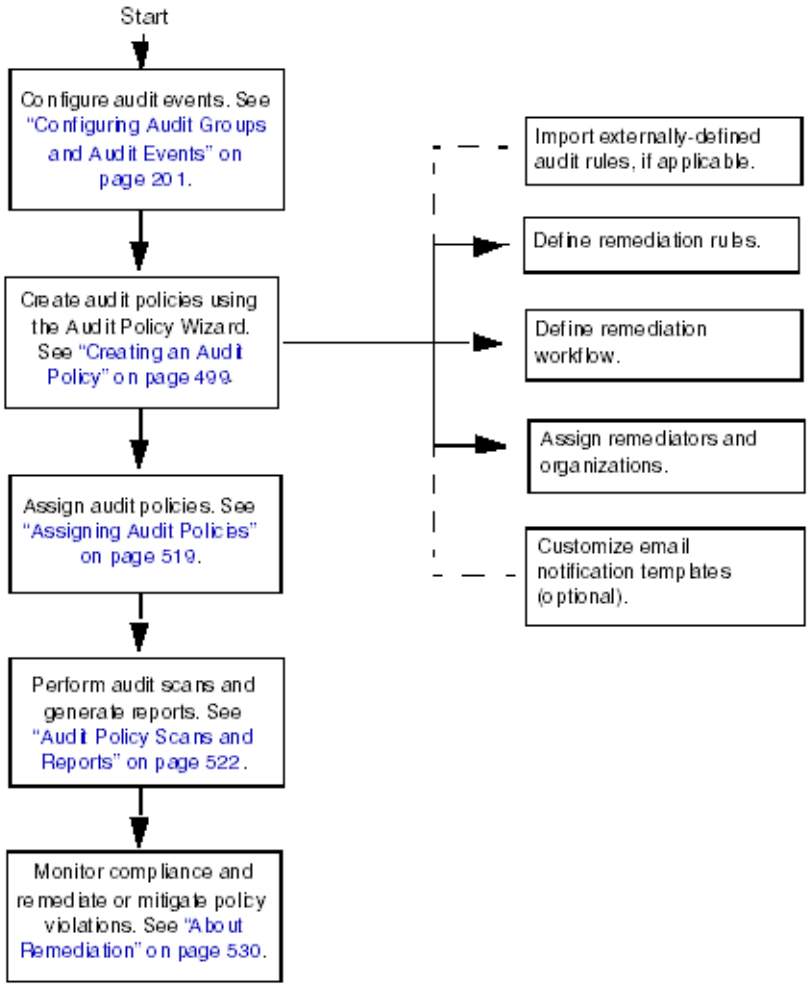


FIGURE 13–1 Flux de tâches logique pour l'établissement de la compatibilité basée sur les stratégies

Travailler avec l'audit des identités dans l'interface administrateur

Cette section explique comment accéder aux fonctionnalités d'audit des identités dans l'interface administrateur. Les modèles de notification par e-mail utilisés pour l'audit des identités sont également examinés.

Utilisation de la section Conformité de l'interface

Pour créer et gérer des stratégies d'audit, utilisez la section Conformité de l'interface administrateur d'Identity Manager.

▼ Pour utiliser la section Conformité pour créer et gérer des stratégies d'audit

1 **Connectez-vous à l'interface administrateur ("Connexion à l'interface utilisateur final d'Identity Manager" à la page 43).**

2 **Cliquez sur Conformité dans la barre de menu.**

Les sous-onglets (ou options de menu) suivants sont disponibles dans la section Conformité :

- Gérer les stratégies,
- Gérer les scannages d'accès,
- Examens des accès.

Gérer les stratégies

La page Gérer les stratégies liste les stratégies que vous êtes autorisé à afficher et éditer. Vous pouvez aussi gérer les scannages d'accès depuis cette zone.

La page Gérer les stratégies permet de travailler avec les stratégies d'audit pour accomplir les tâches suivantes :

- créer une stratégie d'audit ;
- sélectionner une stratégie à afficher ou éditer ;
- supprimer une stratégie.

Des informations détaillées sur ces tâches figurent plus loin dans la section "Exemple de scénario de stratégie d'audit " à la page 446.

Gérer les scannages d'accès

L'onglet Gérer les scannages d'accès permet de créer, modifier et supprimer des scannages d'accès. Vous pouvez définir sur cet onglet des scannages à exécuter ou programmer pour des examens d'accès périodiques. Pour plus d'informations sur cette fonctionnalité, voir "Examens d'accès périodiques et attestations" à la page 484.

Examens des accès

L'onglet Examens des accès permet de lancer, terminer, supprimer et contrôler la progression des examens des accès. Il affiche un rapport récapitulatif des résultats de scannage comportant des liens d'information permettant d'accéder à des informations plus détaillées sur l'état des examens et les activités en attente.

Pour plus d'informations sur cette fonctionnalité, voir "Gestion des examens d'accès" à la page 495.

Guide de référence rapide de l'interface des tâches d'audit des identités

Pour savoir comment effectuer d'autres tâches d'audit des identités dans l'interface administrateur, voir le Tableau B–8. Ce tableau de référence rapide indique où aller pour commencer tout un éventail de tâches d'audit.

Modèles d'e-mails

L'audit des identités utilise la notification par e-mail pour un certain nombre d'opérations. Un objet Modèle d'e-mail est utilisé pour chacune de ces notifications. Les en-têtes et le corps des messages e-mail basés sur ces modèles d'e-mail peuvent être personnalisés.

TABLEAU 13–1 Modèles d'e-mails d'audit des identités

Nom du modèle	Objectif
Avis de résolution de l'examen des accès	Est envoyé aux solutionneurs par un examen des accès lorsque les habilitations de l'utilisateur sont créées au départ dans l'état de résolution.
Avis d'attestation en masse	Est envoyé aux attestateurs par un examen des accès lorsqu'ils ont des attestations en attente.
Avis de violation de stratégie	Est envoyé aux solutionneurs par un scannage de stratégie d'audit en cas de violation.

TABLEAU 13–1 Modèles d'e-mails d'audit des identités *(Suite)*

Nom du modèle	Objectif
Avis de début du scannage d'accès	Est envoyé au propriétaire d'un scannage d'accès quand un examen des accès commence un scannage.
Avis de fin du scannage d'accès	Est envoyé au propriétaire d'un scannage d'accès à la fin d'un scannage d'accès.

Activation de la journalisation d'audit

Pour que vous puissiez commencer à gérer les examens de compatibilité et d'accès, le système de journalisation d'audit d'Identity Manager doit être activé et configuré pour collecter les évènements de contrôle. Par défaut, le système d'audit est activé. Un administrateur Identity Manager ayant la capacité Configurer l'audit peut configurer l'audit.

Identity Manager fournit le groupe de configuration d'audit Gestion de la conformité.

Suivez les étapes ci-après pour afficher ou modifier les événements stockés par le groupe Gestion de la conformité :

1. **Connectez-vous à l'interface administrateur** ("Connexion à l'interface utilisateur final d'Identity Manager" à la page 43).
2. **Sélectionnez Configurer dans la barre de menu puis cliquez sur Vérification informatique.**
3. **Sur la page Configuration d'audit, sélectionnez le nom de groupe d'audit Gestion de la conformité.**

Remarque –

- Pour plus d'informations sur le paramétrage des groupes de configuration d'audit, voir "Configuration de groupes et d'événements d'audit" à la page 111.
- Pour plus d'informations sur l'enregistrement des événements par le système d'audit, voir le Chapitre 10, "Journalisation d'audit".

À propos des stratégies d'audit

Une *stratégie d'audit* définit les limites des comptes pour un ensemble d'utilisateurs d'une ou plusieurs ressources. Elle comprend les *règles* qui définissent les limites d'une stratégie et les *flux de travaux* permettant de traiter les violations qui se produisent. Les scannages d'audit utilisent les critères définis dans une stratégie d'audit afin de déterminer si des violations se sont produites dans l'organisation.

Une stratégie d'audit est constituée des composants suivants :

- Les **Règles de stratégie** définissent des violations spécifiques. Les règles de stratégie peuvent contenir des fonctions écrites dans les langages XPRESS, XML Object ou JavaScript.
- Un **Flux de travaux de résolution** (en option) est lancé lorsqu'un scannage d'audit identifie une violation des règles de stratégie.
- Les **Solutionneurs** sont des utilisateurs désignés qui sont autorisés à répondre aux violations de stratégie. Les solutionneurs peuvent être des utilisateurs individuels ou des groupes d'utilisateurs.

Création d'une stratégie avec les règles de stratégie d'audit

Les règles définissent les conflits potentiels en fonction des attributs au sein d'une stratégie d'audit. Une stratégie d'audit peut contenir des centaines de règles qui référencient un vaste éventail de ressources. Pendant l'évaluation d'une règle, celle-ci a accès aux données de compte utilisateur depuis une ou plusieurs ressources. La stratégie d'audit peut limiter les ressources disponibles pour la règle.

Il est possible d'avoir une règle qui contrôle un unique attribut sur une unique ressource tout comme il est possible d'avoir une règle qui contrôle plusieurs attributs sur plusieurs ressources.

Réponse aux violations de stratégie avec les flux de travaux de résolution

Une fois que vous avez créé des règles pour définir des violations de stratégie, vous sélectionnez le flux de travaux qui sera lancé à chaque fois qu'une violation sera détectée pendant un scannage d'audit. Identity Manager fournit le flux de travaux Standard Remediation (Résolution standard) par défaut, qui assure le traitement de résolution par défaut pour les scannages de stratégie d'audit. Entre autres actions, ce flux de travaux de résolution par défaut génère les e-mails de notification à destination de chacun des Solutionneurs de niveau 1 (et, le cas échéant, des solutionneurs des niveaux suivants).

Remarque – Contrairement aux processus de flux de travaux d'Identity Manager, les flux de travaux de résolution doivent se voir assigner l'`AuthType=AuditorAdminTask` et le sous-type `SUBTYPE_REMEDIATION_WORKFLOW`. Si vous importez un flux de travaux pour l'utiliser dans les scannages d'audit, vous devez ajouter cet attribut manuellement. Pour plus d'informations, voir "(facultatif) Importation des règles de séparation des obligations dans Identity Manager" à la page 449.

Désignation des solutionneurs

Si vous assignez un flux de travaux de résolution, vous devez désigner au minimum un solutionneur. Vous pouvez désigner jusqu'à trois niveaux de solutionneurs pour une stratégie d'audit. Pour plus d'informations sur la résolution, voir "Résolution et atténuation des violations de conformité" à la page 474.

Vous devez assigner un flux de travaux de résolution pour pouvoir assigner des solutionneurs.

Exemple de scénario de stratégie d'audit

Supposez que vous soyez responsable des comptes fournisseurs et des comptes clients et deviez implémenter des procédures visant à empêcher tout cumul de responsabilités dangereux chez les employés du service comptabilité. La stratégie choisie devra garantir que le personnel ayant des responsabilités concernant les comptes fournisseurs n'en aura pas pour les comptes clients.

La stratégie d'audit contiendra les éléments suivants :

- Un ensemble de règles. Chaque règle spécifiera une condition constituant une violation de stratégie
- Un flux de travaux lançant des tâches de résolution.
- Un groupe d'administrateurs désignés, ou solutionneurs, ayant des permissions leur permettant d'afficher et de répondre aux violations de stratégie créées par des règles précédentes.

Une fois que les règles ont identifié des violations de stratégie (dans ce scénario, des utilisateurs cumulant trop de responsabilités), le flux de travaux associé peut lancer des tâches de résolution spécifiques, notamment des notifications automatiques à l'adresse de solutionneurs sélectionnés.

Les solutionneurs de niveau 1 sont les premiers solutionneurs contactés lorsqu'un scannage d'audit identifie une violation de stratégie. Lorsque la période de signalisation identifiée dans cette zone est dépassée, Identity Manager avertit les solutionneurs du niveau suivant (si plus d'un niveau est spécifié pour la stratégie d'audit).

La section suivante « Travailler avec les stratégies d'audit », explique l'utilisation de l'assistant Stratégie d'audit pour créer une stratégie d'audit.

◆ ◆ ◆ CHAPITRE 14

Audit : stratégies d'audit

Ce chapitre explique la création, l'édition, la suppression et l'assignation de stratégies d'audit en utilisant l'Assistant Stratégie d'audit.

Ce chapitre présente les principes et tâches suivants :

Travailler avec les stratégies d'audit

Pour créer une stratégie d'audit, utilisez l'assistant Stratégie d'audit d'Identity Manager. Après avoir défini une stratégie d'audit, vous pouvez effectuer dessus des actions variées, par exemple la modifier ou la supprimer.

Règles des stratégies d'audit

Les règles de stratégie d'audit définissent des violations spécifiques. Les règles de stratégie peuvent contenir des fonctions écrites dans les langages XPRESS, XML Object ou JavaScript.

Vous pouvez utiliser l'assistant Stratégie d'audit pour créer des règles simples ou l'Identity Manager IDE ou un éditeur XML pour en créer de plus puissantes.

- Les règles doivent être du sous-type `SUBTYPE_AUDIT_POLICY_RULE`. Les règles générées par l'Assistant Stratégie d'audit se voient automatiquement assigner ce sous-type.
- Les règles doivent être du type authType `AuditPolicyRule`. Les règles générées par l'Assistant Stratégie d'audit se voient automatiquement assigner cet authType.

Les règles créées en utilisant l'Assistant Stratégie d'audit renverront la valeur `true` ou `false`. Les règles de stratégie qui retournent la valeur `true` résultent en une violation de stratégie. En utilisant Identity Manager IDE, cependant, vous pouvez créer une règle qui ignorera un utilisateur pendant un scannage d'audit ou un examen des accès. Les règles de stratégie d'audit qui retournent la valeur `ignore` arrêteront le traitement des règles pour l'utilisateur en question et ignoreront ce dernier pour passer directement au prochain utilisateur cible.

Pour plus d'informations sur la création de règles de stratégie d'audit, voir le Chapitre 4, "Working with Rules" du *Sun Identity Manager Deployment Reference*.

Création d'une stratégie d'audit

Pour créer une stratégie d'audit, utilisez l'Assistant Stratégie d'audit.

▼ Pour ouvrir l'Assistant Stratégie d'audit

L'Assistant Stratégie d'audit vous guide dans le processus de création d'une stratégie d'audit. Suivez les étapes ci-après pour accéder à cet assistant.

1. **Connectez-vous à l'interface administrateur ("Connexion à l'interface utilisateur final d'Identity Manager" à la page 43).**
2. **Cliquez sur l'onglet Conformité.**

   Le sous-onglet ou menu Gérer les stratégies s'ouvre.
3. **Pour créer une nouvelle stratégie d'audit, cliquez sur Nouvelle.**

Création d'une stratégie d'audit : Présentation

En utilisant l'assistant, vous exécuterez les tâches suivantes pour créer une stratégie d'audit :

- sélectionner ou créer les règles à utiliser pour définir les limites de la stratégie ;
- assigner des approbateurs et établir des limites de signalisation ;
- assigner un flux de travaux de résolution.

Après avoir effectué les tâches présentées dans chacun des écrans de l'assistant, cliquez sur Suivant pour passer à l'étape suivante.

Avant de commencer

Créer une stratégie d'audit ne s'improvise pas. Avant de commencer, vérifiez que vous avez bien effectué les tâches suivantes :

- Identifié les règles que vous utiliserez pour créer la stratégie dans l'Assistant Stratégie d'audit. Les règles choisies dépendent du type de la stratégie créée et des limites spécifiques que vous voulez définir. Pour plus d'informations, voir "Pour identifier les règles dont vous avez besoin" à la page 449 dans la section suivante.
- Importé tout flux de travaux de résolution ou règle à inclure dans la nouvelle stratégie. Pour plus d'informations, voir "(facultatif) Importation des règles de séparation des obligations dans Identity Manager" à la page 449.
- Vérifié que vous avez les capacités requises pour créer des stratégies d'audit. Pour les capacités requises, voir la section "Comprendre et gérer les capacités" à la page 216 au Chapitre 6, "Administration".

▼ Pour identifier les règles dont vous avez besoin

Les contraintes que vous indiquez dans la stratégie sont implémentées dans un ensemble de règles que vous créez ou importez. Lorsque vous utilisez l'Assistant Stratégie d'audit pour créer une règle, suivez les étapes ci-après :

1. **Identifiez la ressource spécifique avec laquelle vous travaillez.**
2. **Sélectionnez un attribut de compte dans la liste des attributs valides pour cette ressource.**
3. **Sélectionnez une condition à imposer sur l'attribut.**
4. **Saisissez une valeur pour la comparaison.**

   Pour toute information sur la création de règles de stratégie d'audit sans l'assistant Stratégie d'audit, voir le Chapitre 4, "Working with Rules" du *Sun Identity Manager Deployment Reference*.

(facultatif) Importation des règles de séparation des obligations dans Identity Manager

L'Assistant Stratégie d'audit ne peut pas créer de règles de séparation des obligations. Vous devez élaborer ces règles hors d'Identity Manager puis les importer en utilisant l'option Importer le fichier d'échange de l'onglet Configurer.

(facultatif) Importation d'un flux de travaux dans Identity Manager

▼ Pour importer un flux de travaux externe

Pour utiliser un flux de travaux de résolution qui n'est pas actuellement disponible dans Identity Manager, importez le flux de travaux externe. Vous pouvez créer des flux de travaux personnalisés en utilisant un éditeur XML ou l'Identity Manager IDE.

1. **Définissez** `authType='AuditorAdminTask' et ajoutez subtype='SUBTYPE_REMEDIATION_WORKFLOW'` **. Vous pouvez utiliser Identity Manager IDE ou l'éditeur XML de votre choix pour définir ces objets Configuration.**

2. **Importez le flux de travaux en utilisant l'option Importer le fichier d'échange.**

   a. **Connectez-vous à l'interface administrateur ("Connexion à l'interface utilisateur final d'Identity Manager" à la page 43).**

   b. **Cliquez sur l'onglet Configurer puis sur le sous-onglet ou le menu Importer le fichier d'échange.**

      La page Importer le fichier d'échange s'ouvre.

   c. **Parcourez la structure de répertoires jusqu'au fichier de flux de travaux à télécharger puis cliquez sur Importer.**

      Après avoir réussi à importer le flux de travaux, ce dernier s'affiche dans la liste d'options Flux de travaux de résolution de l'Assistant Stratégie d'audit ("Création d'une stratégie d'audit" à la page 448).

Nommage et description de la stratégie d'audit

Saisissez le nom de la nouvelle stratégie et une brève description dans l'Assistant Stratégie d'audit (représenté à la Figure 14–1).

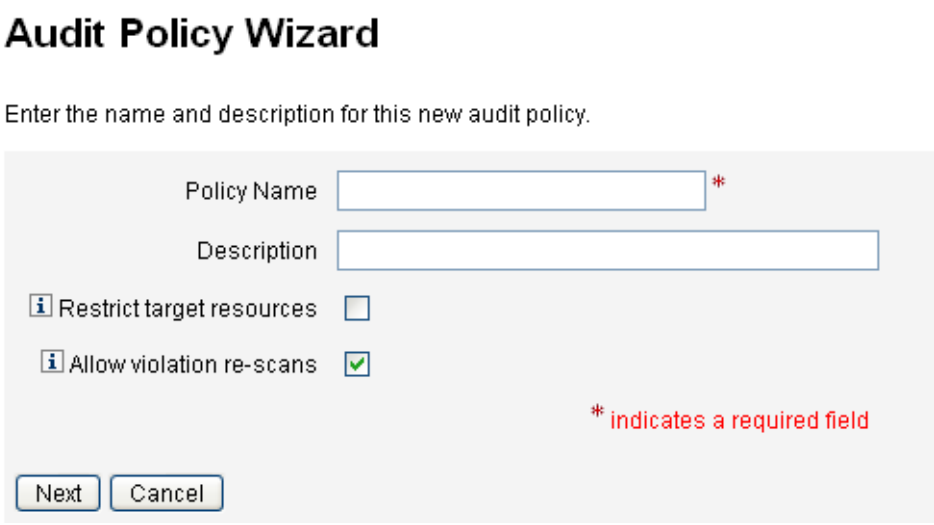


FIGURE 14–1 Assistant Stratégie d'audit: écran de saisie du nom et de la description

---

Remarque – Les noms de stratégies d'audit ne peuvent pas contenir les caractères suivants : ' (apostrophe), . (point), | (barre verticale), [(crochet gauche),] (crochet droit), , (virgule), : (deux points), $ (symbole du dollar), " (guillemets doubles), \ (backslash) ou = (signe égal).

Vous devez aussi éviter d'utiliser les caractères suivants : _ (trait de soulignement), % (signe du pourcentage), ^ (caret) et * (astérisque).

Si vous voulez que seules des ressources sélectionnées fassent l'objet d'accès lors de l'exécution du scannage, sélectionnez l'option Restreindre les ressources cible.

Si vous voulez que la résolution d'une violation entraîne le rescannage immédiat de l'utilisateur, sélectionnez l'option Autorisation de nouveaux scannages de violations.

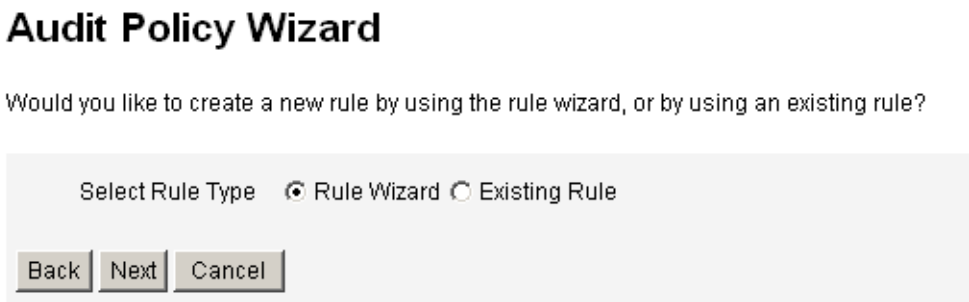
Remarque – Si la stratégie d'audit ne restreint pas les ressources, toutes les ressources pour lesquelles un utilisateur a des comptes feront l'objet d'accès pendant le scannage. Si les règles n'utilisent que quelques ressources, il est plus efficace de restreindre la stratégie à ces ressources.

Cliquez sur Suivant pour passer à la page suivante.

▼ Pour sélectionner un type de règle

Utilisez cette page pour lancer le processus consistant à définir ou inclure des règles dans votre stratégie (le gros du travail quand vous créez une stratégie consiste justement à définir et créer des règles).

Comme indiqué sur la figure suivante, vous pouvez choisir de créer votre propre règle en utilisant l'Assistant Règle d'Identity Manager ou d'incorporer une règle existante. L'Assistant Règle ne permet d'utiliser qu'une ressource dans une règle tandis que les règles importées peuvent en référencer autant que nécessaire.



1 **Décidez si créer une nouvelle règle ou utiliser une règle existante.**

Choisissez l'une des options suivantes :

- Pour créer une nouvelle règle, choisissez l'option Assistant Règle (paramètre par défaut).
- Pour incorporer une règle existante que vous avez créée en utilisant l'Identity Manager IDE, choisissez l'option Règle existante.

2 **Cliquez sur Suivant.**

3 **Selon la sélection effectuée à l'étape 1, continuez par l'une ou l'autre des sections suivantes :**

- Si vous avez sélectionné Assistant Règle, allez à la section "Pour utiliser l'Assistant Règle pour créer une nouvelle règle" à la page 453 et suivez les instructions fournies.
- Si vous avez sélectionné Règle existante, allez à la section "Pour sélectionner une règle existante" à la page 452 et suivez les instructions fournies.

Pour sélectionner une règle existante

Pour inclure une règle existante dans la nouvelle stratégie, sélectionnez Règle existante sur l'écran Sélectionnez un type de règle puis cliquez sur Suivant. Sélectionnez ensuite une règle de stratégie d'audit existante dans le menu déroulant Sélectionner une règle existante.

Remarque – Si vous ne voyez pas le nom d'une règle que vous avez importée au préalable dans Identity Manager, vérifiez si vous avez bien ajouté à cette règle les attributs supplémentaires décrits dans "Création d'une stratégie avec les règles de stratégie d'audit" à la page 445.

Cliquez sur Suivant.

Allez directement à la section "Ajout de règles" à la page 456.

Pour utiliser l'Assistant Règle pour créer une nouvelle règle

Si vous choisissez de créer une règle en utilisant la sélection Assistant Règle dans l'Assistant Stratégie d'audit, précédez en saisissant les informations requises dans les pages examinées dans les sections suivantes.

Pour nommer et décrire une règle

Vous pouvez, en option, donner un nom à la nouvelle règle et la décrire. Utilisez cette page pour entrer le texte de la description qui s'affichera à proximité du nom de la règle à chaque fois qu'Identity Manager affichera la règle. Entrez une description concise et claire qui ait un sens pour décrire la règle. Cette description s'affichera dans Identity Manager sur la page Examen de la violation de stratégie.

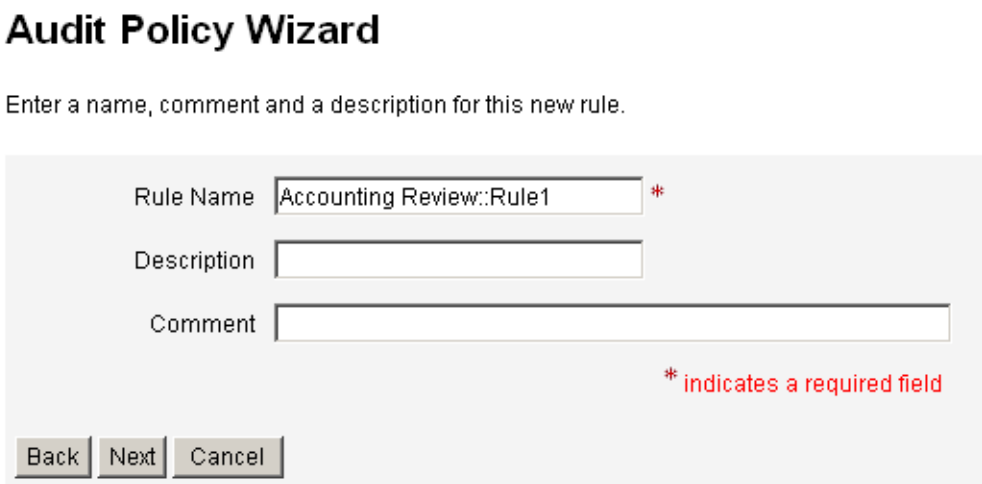


FIGURE 14–2 Assistant Stratégie d'audit : écran de saisie de la description de la règle

Par exemple, pour créer une règle identifiant les utilisateurs ayant les deux valeurs d'attribut Oracle ERP responsibilityKey `Payable User` et `Receivable User`, vous pouvez entrer le texte

suivant dans le champ Description : **`Identifie les utilisateurs responsables à la fois des comptes fournisseurs et des comptes clients`**.

Utilisez le champ Commentaires pour indiquer des informations supplémentaires sur la règle.

Sélectionnez la ressource référencée par la règle

Utilisez cette page pour sélectionner la ressource que la règle référencera. Toute variable de la règle doit correspondre à un attribut sur cette ressource. Toutes les ressources auxquelles vous avez accès en consultation s'afficheront dans cette liste d'options. Dans cet exemple, Oracle ERP est sélectionné.

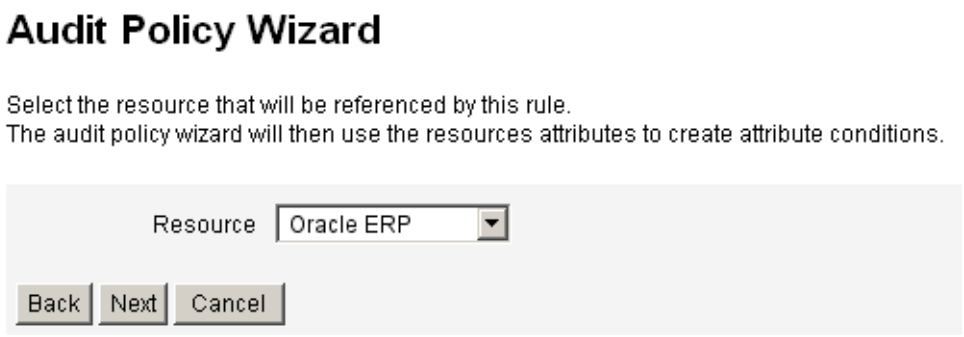


FIGURE 14–3 Assistant Stratégie d'audit : écran Sélectionner ressource

---

Remarque – La plupart mais pas tous les attributs de chacun des adaptateurs de ressources disponibles sont pris en charge. Pour toute information sur les attributs spécifiques disponibles, voir le guide *Sun Identity Manager 8.1 Resources Reference*.

Cliquez sur Suivant pour passer à la page suivante.

Création de l'expression de la règle

Cet écran permet d'entrer l'expression de votre nouvelle règle. Cet exemple crée une règle dans laquelle un utilisateur ayant la valeur d'attribut Oracle ERP `responsibilityKey` `Payable User` ne peut pas aussi avoir la valeur d'attribut `Receivable User`.

▼ Pour créer une expression de règle

1 **Sélectionnez un attribut d'utilisateur dans la liste des attributs disponibles. Cet attribut correspondra directement à une variable de règle.**

2. **Sélectionnez une condition logique dans la liste. Les conditions valides sont les suivantes : = (égal à), != (différent de), < (inférieur à), <= (inférieur ou égal à), > (supérieur à), >= (supérieur ou égal à), is true (est vrai), is null (est null), is not null (non null) et contains (contient). Aux fins de cet exemple, vous pouvez sélectionner `contains` dans la liste des conditions d'attribut possibles.**

3. **Saisissez une valeur pour l'expression. Par exemple, si vous entrez `Payable user`, vous spécifiez un utilisateur Oracle ERP ayant la valeur `Payable user` dans l'attribut `responsibilityKeys`.**

4. **(facultatif) Cliquez sur l'un des opérateurs `AND` (ET) ou `OR` (OU) pour ajouter une ligne et créer une nouvelle expression.**

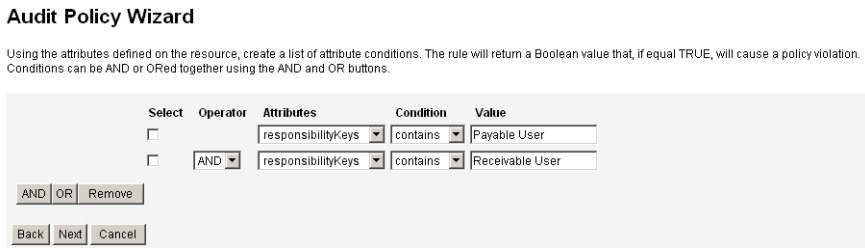


FIGURE 14–4 Assistant Stratégie d'audit : écran de sélection de l'expression de la règle

Cette règle retourne une valeur booléenne. Si les deux instructions sont vraies, la règle de stratégie retourne la valeur TRUE, qui entraîne une violation de stratégie.

Remarque – Identity Manager ne prend pas en charge le contrôle d'imbrication de règles. De plus, utiliser l'Assistant Stratégie d'audit pour créer des stratégies avec différents opérateurs booléens entre les règles peut produire des résultats imprévisibles car l'ordre d'évaluation n'est pas précisé.

Pour les expressions de règle complexes, créez les règles en utilisant un éditeur XML au lieu d'utiliser l'Assistant Stratégie d'audit. Utiliser un éditeur XML permet d'utiliser l'inversion quand cela est nécessaire afin d'utiliser seulement un unique opérateur booléen entre les règles.

L'exemple de code suivant montre le XML de la règle que vous avez créée dans cet écran :

```
<Description>Payable User/Receivable User</Description>
  <RuleArgument name='resource' value='Oracle ERP'>
    <Comments>Resource specified when  audit policy was created.</Comments>
    <String>Oracle ERP</String>
  </RuleArgument>
    <and>
```

```
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Receivable User</s>
      </contains>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Payables User</s>
      </contains>
    </and>
    <MemberObjectGroups>
      <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
    </MemberObjectGroups>
</Rule>
```

Pour supprimer une expression de la règle, sélectionnez la condition d'attribut et cliquez sur Supprimer.

Cliquez sur Suivant pour poursuivre avec l'Assistant Stratégie d'audit. Vous aurez la possibilité d'ajouter davantage de règles soit en ajoutant des règles existantes soit en utilisant de nouveau l'assistant.

Ajout de règles

Vous pouvez créer des règles supplémentaires en important des règles existantes ou en utilisant l'assistant (pour plus d'informations, voir "Pour sélectionner un type de règle" à la page 451).

Cliquez sur les opérateurs `AND` (ET) ou `OR` (OU) pour ajouter les règles comme requis. Pour supprimer une règle, sélectionnez-la et cliquez sur Supprimer.

Des violations de stratégie n'ont lieu que si l'expression booléenne de *toutes* les règles donne true. En regroupant les règles avec les opérateurs AND/OR, la stratégie peut se solder par true, même si ce n'est pas le cas de toutes les règles. Identity Manager crée des violations uniquement pour les règles dont l'évaluation se solde par true et uniquement si l'évaluation de l'expression de la stratégie donne true.

Remarque – Identity Manager ne prend pas en charge la commande d'imbrication de règles. De plus, utiliser l'Assistant Stratégie d'audit pour créer des stratégies avec différents opérateurs booléens entre les règles peut produire des résultats imprévisibles car l'ordre d'évaluation n'est pas précisé.

Pour les expressions de règle complexes, créez les règles en utilisant un éditeur XML au lieu d'utiliser l'Assistant Stratégie d'audit. Utiliser un éditeur XML permet d'utiliser l'inversion quand cela est nécessaire afin d'utiliser seulement un unique opérateur booléen entre les règles.

Sélection d'un flux de travaux de résolution

Utilisez cet écran pour sélectionner un flux de travaux de résolution à associer à cette stratégie. Le flux de travaux ici assigné détermine les actions lancées au sein d'Identity Manager lorsqu'une violation d'audit est détectée.

Remarque – Un flux de travaux est démarré pour chaque stratégie d'audit occasionnant un échec. Chaque flux de travaux contiendra un ou plusieurs éléments de travail pour chaque violation de compatibilité créée par le scannage de stratégie pour la stratégie spécifique.

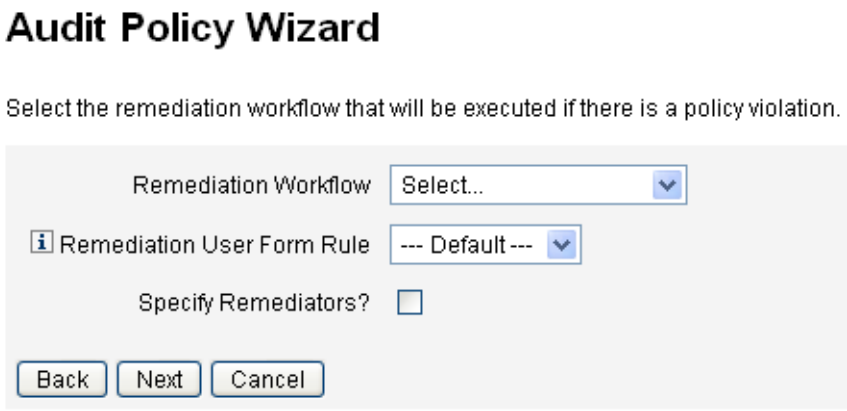


FIGURE 14–5 Assistant Stratégie d'audit : écran de sélection du flux de travaux de résolution

---

Remarque – Pour toute information sur l'importation d'un flux de travaux que vous avez créé en utilisant un éditeur XML ou l'Identity Manager IDE, voir "(facultatif) Importation des règles de séparation des obligations dans Identity Manager" à la page 449.

Utilisez le menu déroulant Règle de formulaire utilisateur de résolution pour sélectionner une règle qui calculera le formulaire utilisateur à appliquer lors de l'édition d'un utilisateur par le biais de la résolution. Par défaut, un solutionneur qui édite un utilisateur en réponse à un élément de travail de résolution utilisera le formulaire utilisateur assigné au solutionneur. Si en revanche une stratégie d'audit spécifie un formulaire utilisateur de résolution, ce dernier formulaire sera utilisé. Cela permet l'utilisation d'un formulaire très spécifique quand une stratégie d'audit indique un problème spécifique correspondant.

Pour spécifier les solutionneurs à associer à ce flux de travaux de résolution, sélectionnez la case à cocher Définir les solutionneurs ?. Si vous sélectionnez cette option, cliquer sur Suivant affichera la page Assign Remediators (Assigner les solutionneurs). Si vous ne sélectionnez pas cette option, l'assistant affichera ensuite l'écran Assigner organisation de l'Assistant Stratégie d'audit.

Sélection des solutionneurs et des délais pour les résolutions

Si vous spécifiez des solutionneurs, les solutionneurs assignés à cette stratégie seront avertis en cas de détection de violation de cette stratégie. Par ailleurs, le flux de travaux par défaut leur assigne un élément de travail de résolution. Tout utilisateur Identity Manager peut être un solutionneur.

Vous pouvez choisir d'assigner au moins un solutionneur de niveau 1 ou un utilisateur désigné. Les solutionneurs de niveau 1 sont les premiers contactés au moyen d'un e-mail lancé par le flux de travaux de résolution en cas de détection d'un flux de travaux. Si le délai d'attente de signalisation désigné est atteint sans qu'un solutionneur de niveau 1 ait répondu, Identity Manager contacte ensuite le solutionneur de niveau 2 indiqué ici. Identity Manager ne contacte les solutionneurs de niveau 3 qui si aucun solutionneur, de niveau 1 ou 2, n'a répondu avant l'expiration du délai d'attente de signalisation.

Remarque – Si vous indiquez une valeur de délai de signalisation pour le plus haut niveau de solutionneur sélectionné, l'élément de travail est supprimé de la liste lorsque la signalisation expire. Par défaut, le délai de signalisation est défini sur la valeur 0. Dans ce cas, l'élément de travail n'expire pas et reste dans la liste du solutionneur.

L'assignation de solutionneurs est facultative. Si vous sélectionnez cette option, cliquez ensuite sur Suivant pour passer à l'écran suivant après avoir spécifié les paramètres.

Pour ajouter des utilisateurs à la liste disponible des solutionneurs, entrez un ID utilisateur puis cliquez sur Ajouter. Une autre solution consiste à cliquer sur le bouton **...** (Autres) afin de rechercher un ID utilisateur. Entrez un ou plusieurs caractères dans le champ commence par puis cliquez sur Trouver. Après avoir sélectionné un utilisateur dans la liste de recherche, cliquez sur Ajouter pour l'ajouter à la liste des solutionneurs. Cliquez sur Abandonner pour fermer la zone de recherche.

Pour supprimer un ID de la liste des solutionneurs, sélectionnez-le dans la liste puis cliquez sur Supprimer.

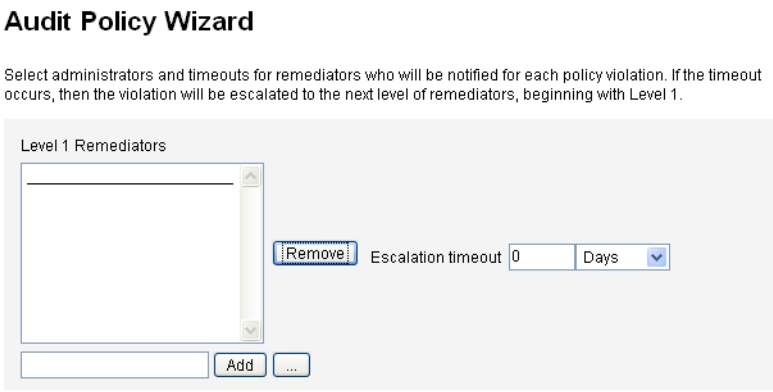


FIGURE 14–6 Assistant Stratégie d'audit : zone de sélection des solutionneurs de niveau 1

Sélection d'organisations pouvant accéder à la stratégie

Utilisez l'écran illustré à la Figure 14–7 pour sélectionner les organisations qui peuvent afficher et éditer cette stratégie.

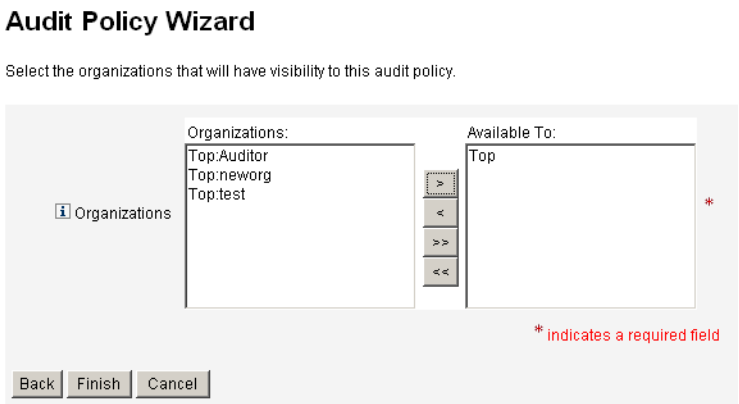


FIGURE 14–7 Assistant Stratégie d'audit : écran d'assignation de visibilité aux organisations

Après avoir effectué les sélections d'organisations, cliquez sur Terminer pour créer la stratégie d'audit et revenir à la page Gérer les stratégies. La stratégie qui vient d'être créée est maintenant visible dans cette liste.

Édition d'une stratégie d'audit

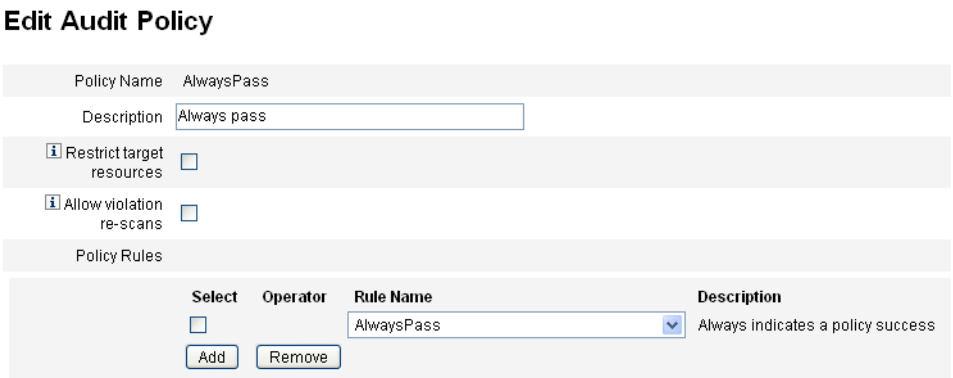
Les tâches d'édition courantes ayant pour objet des stratégies d'audit sont les suivantes :

- l'ajout ou la suppression de règles ;
- le changement des ressources cibles ;
- l'ajustement de la liste des organisations qui ont accès à la stratégie ;
- la modification du délai d'attente de signalisation associé à chaque niveau de résolution ;
- la modification du flux de travaux de résolution associé à la stratégie.

Page Éditer la stratégie

Cliquez sur le nom d'une stratégie dans la colonne de nom de la stratégie d'audit pour ouvrir la page Éditer la stratégie. Cette page contient les informations d'audit classées dans les zones suivantes :

- une zone consacrée à l'identification et aux règles,
- une zone dédiée au délai d'attente de signalisation et aux solutionneurs,
- une zone réservée aux flux de travaux et organisations.



Cette zone de la page permet de :

- éditer la description de la stratégie ;
- ajouter ou supprimer une règle.

Remarque – Vous ne pouvez pas utiliser ce produit pour éditer directement une règle existante. Utilisez l'Identity Manager IDE ou un éditeur XML pour éditer la règle puis importez-la dans Identity Manager. Vous pouvez ensuite supprimer l'ancienne version puis ajouter la nouvelle version revue et corrigée.

Édition de la description de la stratégie d'audit

Éditez la description de la stratégie d'audit en sélectionnant le texte du champ Description puis en entrant le nouveau texte.

Édition des options

En option, sélectionnez ou désélectionnez les options Restreindre les ressources cible ou Autorisation de nouveaux scannages de violations.

Suppression d'une règle de la stratégie

Pour supprimer une règle de la stratégie, cliquez sur le bouton Sélectionner qui précède le nom de cette règle puis cliquez sur Supprimer.

Ajout d'une règle à la stratégie

Cliquez sur Ajouter pour ajouter un nouveau champ que vous pourrez utiliser pour sélectionner une règle à ajouter.

Changement d'une règle utilisée par la stratégie

Dans la colonne Nom de la règle, sélectionnez une autre règle dans la liste de sélection.

Zone Solutionneurs

La Figure 14–8 illustre une partie de la zone Solutionneurs, laquelle permet d'assigner des solutionneurs de niveau 1, 2 et 3 pour une stratégie.

FIGURE 14–8 Page Édition de la stratégie d'audit : assignation des solutionneurs

Cette zone de la page permet de :

- supprimer ou assigner des solutionneurs à une stratégie ;
- régler les délais d'attente de signalisation.

Suppression ou assignation de solutionneurs

Sélectionnez un solutionneur pour un niveau de résolution ou plus en entrant un ID utilisateur et en cliquant sur Ajouter. Pour rechercher un ID utilisateur, cliquez sur **...** (Autres). Vous devez sélectionner au minimum un solutionneur.

Pour supprimer un solutionneur, sélectionnez un ID utilisateur puis cliquez sur Supprimer.

Réglage des délais d'attente de signalisation

Sélectionnez la valeur de délai d'attente puis entrez la nouvelle valeur. Par défaut, aucune valeur de délai d'attente n'est définie.

Remarque – Si vous indiquez une valeur de délai de signalisation pour le plus haut niveau de solutionneur sélectionné, l'élément de travail est supprimé de la liste lorsque la signalisation expire.

Zone Flux de travaux de résolution et Organisations

La Figure 14–9 illustre la zone dans laquelle vous indiquez le flux de travaux de résolution et les organisations pour une stratégie d'audit.

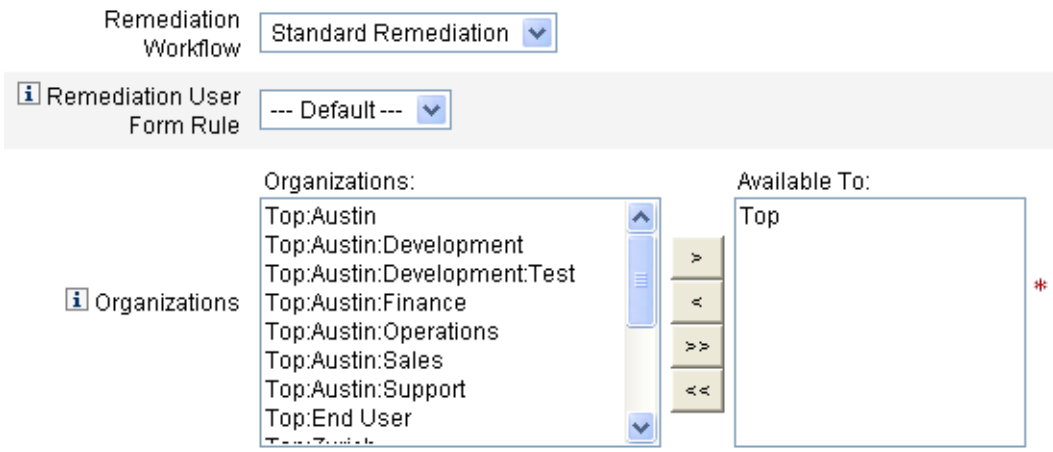


FIGURE 14–9 Page Édition de la stratégie d'audit: Flux de travaux de résolution et Organisations

Cette zone de la page permet de :

- changer le flux de travaux de résolution qui est lancé lorsqu'une violation de stratégie a lieu ;
- sélectionner une règle de formulaire utilisateur de résolution ;
- choisir les organisations qui ont accès à cette stratégie.

Changement du flux de travaux de résolution

Pour changer le flux de travaux de résolution assigné à une stratégie, vous pouvez sélectionner un flux de travaux de remplacement dans la liste des options. Par défaut, aucun flux de travaux n'est assigné à une stratégie d'audit.

Remarque – Si aucun flux de travaux n'est assigné à la stratégie d'audit, les violations ne seront pas assignées à un solutionneur.

Sélectionnez un flux de travaux de résolution dans la liste, puis cliquez sur Enregistrer.

Sélection d'une règle de formulaire utilisateur de résolution

En option, vous pouvez sélectionner une règle permettant de calculer le formulaire utilisateur appliqué lors de l'édition d'un utilisateur par le biais d'une résolution.

Assignation ou suppression de visibilité pour les organisations

Définissez les organisations pour lesquelles cette stratégie d'audit sera disponible et cliquez sur Enregistrer.

Exemples de stratégies

Identity Manager contient les exemples de stratégies suivants, accessibles depuis la liste Stratégies d'audit :

- la stratégie IDM Role Comparison,
- la stratégie IDM Account Accumulation.

La stratégie IDM Role Comparison

Cet exemple de stratégie permet de comparer les droits d'accès actuels d'un utilisateur à ceux spécifiés par les rôles Identity Manager. Cette stratégie garantit que tous les attributs de ressource spécifiés par les rôles sont définis pour l'utilisateur.

Cette stratégie échoue si :

- certains des attributs de ressource spécifiés par les rôles manquent à l'utilisateur ;
- les attributs de ressource de l'utilisateur diffèrent de ceux spécifiés par les rôles.

Stratégie IDM Account Accumulation

Cet exemple de stratégie vérifie que tous les comptes détenus par l'utilisateur sont référencés par au moins un rôle également détenu par l'utilisateur.

Cette stratégie échoue si l'utilisateur a des comptes sur des ressources non explicitement référencées par un rôle assigné à l'utilisateur.

Suppression d'une stratégie d'audit

Lorsqu'une stratégie d'audit est supprimée d'Identity Manager, toutes les violations qui référencient cette stratégie sont également supprimées.

Les stratégies peuvent être supprimées de la zone Conformité de l'interface, quand vous cliquez sur Gérer les stratégies pour afficher les stratégies. Pour supprimer une stratégie d'audit, sélectionnez le nom de cette stratégie dans la vue des stratégies puis cliquez sur Supprimer.

Dépannage des stratégies d'audit

De manière générale, il convient de résoudre les problèmes associés à une stratégie d'audit en déboguant les règles de cette stratégie.

Pour déboguer une règle, ajoutez les éléments de suivi suivants au code de la règle.

```
<block trace='true'>
<and>
    <contains>
```

```
        <ref>accounts[AD].firstname</ref>
        <s>Sam</s>
    </contains>
    <contains>
        <ref>accounts[AD].lastname</ref>
        <s>Smith</s>
    </contains>
</and>
</block>
```

- Si vous ne parvenez pas à voir votre flux de travaux dans l'interface d'Identity Manager, vérifiez que :
  - Vous avez ajouté l'attribut `subtype='SUBTYPE_REMEDIATION_WORKFLOW'` à votre flux de travaux. Les flux de travaux dénués de ce sous-type ne sont pas visibles dans l'interface administrateur d'Identity Manager.
  - Vous avez la capacité correspondant à l'authType `AuditorAdminTask`.
  - Vous contrôlez l'organisation contenant le flux de travaux.
- Si vous avez importé des règles mais ne les voyez pas dans l'Assistant Stratégie d'audit, vérifiez que :
  - Chaque règle est de `subtype="SUBTYPE_AUDIT_POLICY_RULE'` ou `subtype="SUBTYPE_AUDIT_POLICY_SOD_RULE'`.
  - Vous avez la capacité relative à l'authType `AuditPolicyRule`.
  - Vous contrôlez l'organisation contenant le flux de travaux.

Assignation des stratégies d'audit

Pour assigner une stratégie d'audit à une organisation, l'utilisateur doit avoir (au minimum) la capacité Assignation des stratégies d'audit aux organisations. Pour assigner une stratégie d'audit à un utilisateur, l'utilisateur doit avoir la capacité Assignation des stratégies d'audit aux utilisateurs. Un utilisateur ayant la capacité Assignation de stratégies d'audit a ces deux capacités.

Pour assigner une stratégie au niveau organisation, sélectionnez Organisation sur l'onglet Comptes puis sélectionnez les stratégies dans la listes Stratégies d'audit assignées.

▼ Pour assigner une stratégie au niveau utilisateur

1 Cliquez sur l'utilisateur dans la zone Comptes.

2 Sélectionnez Conformité dans le formulaire utilisateur.

3 **Sélectionnez des stratégies dans la liste Stratégies d'audit assignées.**

Remarque – Les stratégies d'audit directement assignées à un utilisateur (c.-à-d., assignées via l'assignation d'une organisation ou d'un compte utilisateur) sont toujours réévaluées lorsqu'une violation est résolue pour l'utilisateur en question.

Résolution des limites de capacités de l'auditeur

Par défaut, les capacités nécessaires pour effectuer les tâches d'audit sont contenues dans l'organisation Haut (groupe d'objets). Résultat, seuls les administrateurs qui contrôlent Haut peuvent assigner ces capacités à d'autres administrateurs.

Vous pouvez résoudre ce problème en ajoutant les capacités à une autre organisation. Identity Manager fournit deux utilitaires, situés dans le répertoire `sample/scripts`, qui facilitent cette tâche.

▼ Pour ajouter des capacités

Pour ajouter les capacités nécessaires pour effectuer des tâches d'audit pour une organisation autre que Haut, suivez les étapes ci-après :

1 **Exécutez la commande suivante pour lister toutes les capacités (AdminGroups) et leurs organisations associées (groupes d'objets) :**

```
beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
```

Cette commande capture la sortie dans un fichier CSV.

2 **Éditez ce fichier CSV pour ajuster les emplacements organisationnels des capacités comme voulu.**

3 **Exécutez cette commande pour mettre à jour Identity Manager.**

```
beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
```

◆ ◆ ◆ CHAPITRE 15

Audit : contrôler la conformité

Ce chapitre explique comment réaliser des audits et mettre en œuvre des procédures qui facilitent la gestion de la conformité aux réglementations fédérales applicables.

Sa lecture vous permettra de vous familiariser avec les principes et tâches suivants :

Scannages et rapports des stratégies d'audit

Cette section contient des informations sur les scannages de stratégies d'audit et explique comment exécuter et gérer les scannages d'audit.

Scannage d'utilisateurs et d'organisations

Un scannage exécute des stratégies d'audit sélectionnées sur des utilisateurs individuels ou des organisations. Vous pouvez scanner un utilisateur ou une organisation afin de rechercher une violation spécifique ou mettre en œuvre des stratégies non assignées à l'utilisateur ou à l'organisation. Lancez les scannages depuis la zone Comptes de l'interface.

Remarque – Vous pouvez également lancer ou programmer une stratégie d'audit sous l'onglet Tâches du serveur.

▼ Pour scanner un compte utilisateur ou une organisation

1 **Cliquez sur Comptes dans le menu principal de l'interface administrateur.**

2 **Dans la liste des comptes, vous pouvez :**

a. **Sélectionner un ou plusieurs utilisateurs, puis Scannage dans la liste d'options Actions de l'utilisateur.**

b. **Sélectionner une ou plusieurs organisations, puis l'option Scannage dans la liste Actions d'organisation.**

La boîte de dialogue Lancer une tâche s'affiche. La Figure 15–1 donne un exemple de page Lancer une tâche pour le scannage d'un utilisateur de stratégie d'audit.

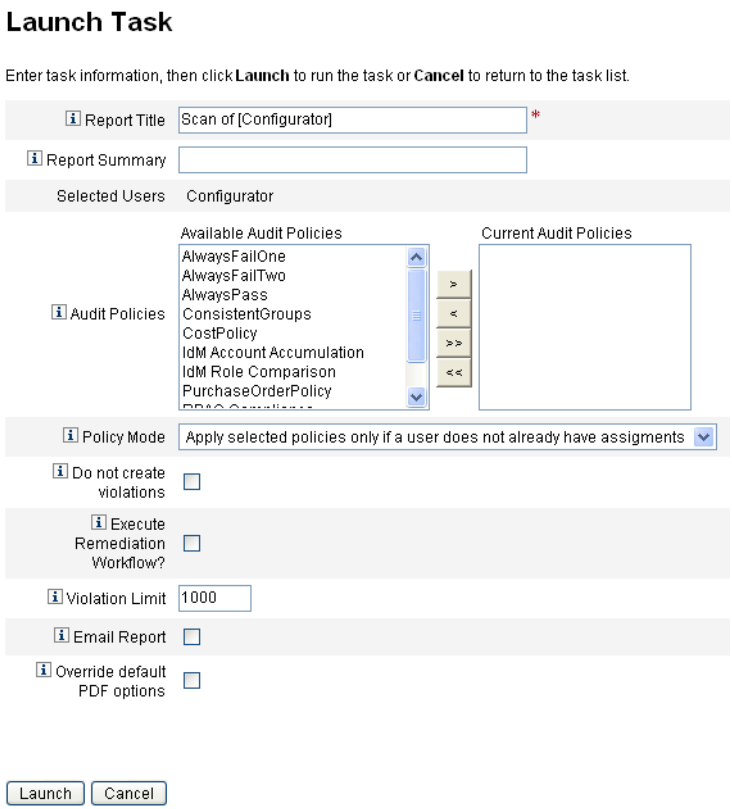


FIGURE 15–1 La boîte de dialogue Lancer une tâche

3 **Entrez un titre pour le scannage dans le champ Titre du rapport (*obligatoire*).**

4 **Spécifiez les autres options.**

Ces options sont les suivantes :

- **Récapitulatif du rapport** : entrez une description pour le scannage.
- **Add Policies (Ajouter des stratégies)** : sélectionnez une ou plusieurs stratégies d'audit à exécuter. Vous devez sélectionner au moins une stratégie.
- **Mode de stratégie** : sélectionnez un mode de stratégie, qui détermine le mode d'interaction entre les stratégies sélectionnées et les stratégies déjà assignées aux utilisateurs. Les assignations peuvent provenir directement de l'utilisateur ou de l'organisation à laquelle l'utilisateur est assigné.
- **Ne pas créer de violations** : cochez cette case si vous voulez que les stratégies d'audit soient évaluées et les violations consignées, mais ne voulez pas que les violations de conformité soient créées ou mises à jour ni que les flux des travaux de résolution soient exécutés. Les résultats des tâches résultant du scannage indiquent les violations qui auraient été créées, ce qui rend cette option particulièrement utile pour tester les stratégies d'audit.
- **Exécuter le flux de travaux de résolution ?** : cochez cette case pour exécuter le flux des travaux de résolution assignés dans la stratégie d'audit. Si la stratégie d'audit ne définit pas de flux de travaux de résolution, aucun flux de travaux de résolution ne sera exécuté.
- **Limite de violations** : éditez cette case pour définir le nombre maximum de violations de conformité pouvant être émises par ce scannage avant son abandon. Il s'agit d'une mesure de protection permettant de limiter les risques d'exécution d'une stratégie d'audit trop ouvertement agressive dans ses vérifications. Une case vide (sans valeur) signifie qu'aucune limite n'a été définie.
- **Envoyer le rapport par e-mail** : cochez cette case pour indiquer les destinataires du rapport. Identity Manager peut également joindre un fichier contenant un rapport au format CSV (valeurs séparées par une virgule).
- **Ignorer les options PDF par défaut** : cochez cette case pour ignorer les options PDF par défaut.

5 **Cliquez sur Lancer pour commencer le scannage.**

Pour voir les rapports d'un scannage d'audit, affichez les Rapports de l'auditeur.

Travailler avec les rapports de l'auditeur

Identity Manager fournit des rapports d'auditeur. Le tableau suivant décrit ces rapports.

TABLEAU 15–1 Description des rapports de l'auditeur

Type de rapport de l'auditeur	Description
Rapport de couverture des examens d'accès	Affiche les chevauchements ou les différences entre les utilisateurs ayant un rapport avec les examens d'accès sélectionnés. Vu que la plupart des examens d'accès se réfèrent aux utilisateurs spécifiés par une requête ou une opération d'appartenance, la liste exacte des utilisateurs peut varier avec le temps. Ce rapport peut montrer un chevauchement, des différences, ou les deux, entre les utilisateurs spécifiés dans deux examens des accès différents (pour voir si les examens seront efficaces) ; entre des habilitations générées par deux examens des accès différents (pour voir si la couverture change avec le temps) ; ou entre des utilisateurs et des habilitations (pour voir si des habilitations ont été générées pour tous les utilisateurs du même examen).
Détails de l'examen des accès	Affiche le statut de tous les enregistrements d'habilitation d'un utilisateur. Ce rapport peut être filtré en fonction de l'organisation d'un utilisateur, d'un examen des accès, d'une instance d'examen des accès, de l'état d'un enregistrement d'habilitation et d'un attestateur.
Récapitulatif de l'examen des accès	Fournit un récapitulatif de tous les examens des accès. Ce récapitulatif résume le statut des utilisateurs scannés, des stratégies scannées et des activités d'attestation relatives à chaque scannage d'examen d'accès listé.
Couverture de l'étendue des utilisateurs du balayage d'accès	Compare des scannages sélectionnés pour déterminer les utilisateurs inclus dans l'étendue du scannage. Indique les chevauchements (utilisateurs inclus dans tous les scannages) ou les différences (utilisateurs non compris dans tous les scannages, mais inclus dans plusieurs d'entre eux). Ce rapport s'avère pratique lorsque vous tentez d'organiser plusieurs scannages d'accès devant englober des utilisateurs identiques ou différents selon les besoins de l'opération.
Récapitulatif des stratégies d'audit	Récapitule les points essentiels de toutes les stratégies d'audit, y compris les règles, les solutionneurs et le flux des travaux de chacune.
Attribut audité	Affiche tous les rapports audités faisant état d'une modification d'un attribut de compte de ressource spécifié. Ce rapport explore les données d'audit pour tous les attributs auditables précédemment sauvegardés. Il explorera les données en fonction de tous les attributs étendus pouvant être spécifiés depuis WorkflowServices ou les attributs de ressources marqués comme auditables. Pour toute information sur la configuration de ce rapport, voir la section "Configuration du Rapport des attributs audités" à la page 473.
Historique des violations de stratégies d'audit	Représentation graphique de toutes les violations de conformité aux stratégies créées pendant un laps de temps spécifié. Ce rapport peut être filtré par stratégie et groupé par jour, semaine, mois ou trimestre.
Accès utilisateur	Affiche l'enregistrement d'audit et les attributs utilisateur d'un utilisateur spécifié.

TABLEAU 15–1 Description des rapports de l'auditeur *(Suite)*

Type de rapport de l'auditeur	Description
Historique des violations d'organisations	Représentation graphique de toutes les violations de conformité aux ressources créées pendant un laps de temps spécifié. Ce rapport peut être filtré par organisation et groupé par jour, semaine, mois ou trimestre.
Historique des violations de ressources	Représentation graphique de toutes les violations de conformité par ressource, créées pendant un laps de temps spécifié.
Séparation des obligations	Affiche les violations de séparation des obligations dans un tableau de conflits. En utilisant une interface Web, vous pouvez cliquer sur les liens et avoir accès à des informations supplémentaires. Ce rapport peut être filtré par organisation et groupé par jour, semaine, mois ou trimestre.
Récapitulatif des violations	Affiche toutes les violations de conformité actuelles. Ce rapport peut être filtré par solutionneur, ressource, règle, utilisateur ou stratégie

Les rapports sont disponibles sous l'onglet Rapports de l'interface d'Identity Manager

---

Remarque – La valeur `RULE_EVAL_COUNT` représente le nombre de règles évaluées au cours d'un scannage de stratégies. Cette valeur est parfois incluse dans les rapports.

Identity Manager calcule la valeur `RULE_EVAL_COUNT` comme suit :

```
nb d'utilisateurs scannés x (nb de règles dans la stratégie + 1)
```

Le +1 est inclus dans le calcul parce que Identity Manager compte également la *règle de stratégie*, à savoir la règle qui détermine si une stratégie a été violée. La règle de stratégie inspecte les résultats de la règle d'audit et effectue une opération booléenne pour obtenir un résultat de stratégie.

Par exemple, si vous avez une stratégie A avec trois règles et une stratégie B avec deux règles, et que vous explorez dix utilisateurs, la valeur `RULE_EVAL_COUNT` sera égale à 70 parce que

```
10 utilisateurs x (3 + 1 + 2 + 1 règles)
```

Création d'un rapport de l'auditeur

Pour exécuter un rapport, vous devez d'abord créer un modèle de rapport. Vous pouvez définir plusieurs critères pour ce rapport, y compris des destinataires auxquels envoyer les résultats du rapport par e-mail. Après la création et l'enregistrement d'un modèle de rapport, ce modèle est disponible sur la page Exécuter des rapports.

La figure ci-dessous donne un exemple de la page Exécuter des rapports avec une liste de rapports d'auditeur définis.

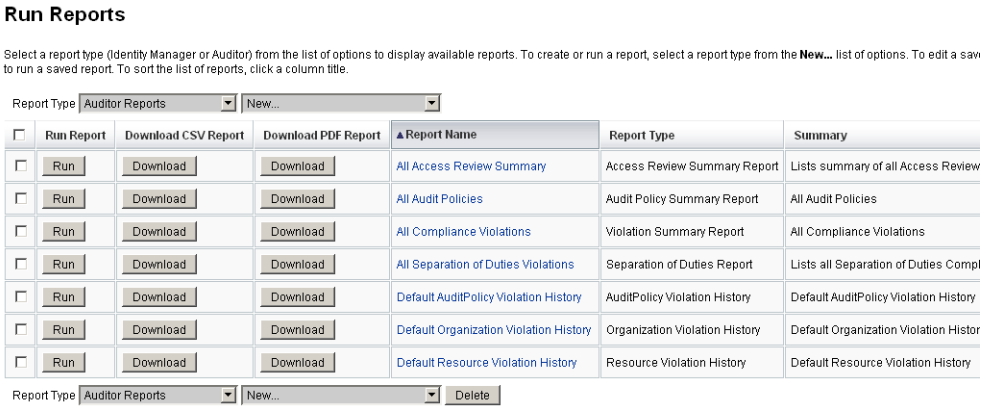


FIGURE 15–2 Sélections de la page Exécuter des rapports.

▼ Pour créer un rapport d'auditeur

1 Cliquez sur Rapports dans le menu principal de l'interface administrateur.

La page Exécuter des rapports s'ouvre.

2 Sélectionnez Rapports de l'auditeur pour le type de rapport.

3 Sélectionnez un rapport dans la liste de rapports Nouveau.

La page Définir un rapport s'ouvre. Les champs et la présentation de la boîte de dialogue changent en fonction du type du rapport. Accédez à l'Aide d'Identity Manager pour plus de détails sur la spécification des critères des rapports.

Après avoir entré et sélectionné les critères du rapport, vous pouvez :

- Exécuter le rapport sans l'enregistrer.

  Cliquez sur Exécuter pour lancer le rapport. Identity Manager n'enregistre pas le rapport (si vous avez défini un nouveau rapport) ni les critères du rapport modifiés (si vous avez modifié un rapport existant).

- Enregistrer le rapport.

  Cliquez sur Enregistrer pour enregistrer le rapport. Après l'enregistrement, vous pouvez exécuter le rapport depuis la page Exécuter des rapports (liste des rapports). Après avoir exécuté un rapport depuis la page Exécuter des rapports, vous pouvez en afficher la sortie immédiatement ou ultérieurement depuis l'onglet Afficher les rapports.

Pour plus de détails sur la planification d'un rapport, voir la section "Programmation des rapports" à la page 278.

Configuration du Rapport des attributs audités

Le Rapport des attributs audités (voir Tableau 15–1) peut contenir les modifications d'attributs apportées aux utilisateurs et comptes Identity Manager. Toutefois, la journalisation d'audit standard ne génère pas de journal d'audit suffisamment riche en données pour prendre en charge une expression de requête complète.

La journalisation d'audit standard *écrit* les attributs modifiés dans le champ `acctAttrChanges` du journal d'audit, mais ces attributs modifiés sont écrits de telle manière que la requête de rapports ne recherche les enregistrements correspondants qu'en fonction du nom des attributs modifiés. La requête de rapports ne peut pas trouver de correspondance précise en fonction de la valeur des attributs.

Vous pouvez configurer ce rapport pour trouver les enregistrements contenant des changements ayant porté sur l'attribut `lastname`, en configurant les paramètres suivants :

```
Attribute Name = 'acctAttrChanges'
Condition = 'contains'
Value = 'lastname'
```

Remarque – Il est nécessaire d'utiliser `Condition='contains'` en raison de la façon dont sont stockées les données dans le champ `acctAttrChanges`. Ce champ n'est pas multivalué. Il s'agit essentiellement d'une structure de données contenant les valeurs `before/after` (avant/après) de tous les attributs modifiés sous la forme `nomattr=valeur` Par conséquent, les paramètres précédents permettent à la requête de rapports de trouver toutes les instances de `lastname=` *xxx*.

Il est impossible de capturer uniquement les enregistrements d'audit ayant un attribut spécifique avec une valeur spécifique. Pour cela, procédez comme décrit dans la section "Configuration de l'onglet Vérification informatique " à la page 330. Cochez la case Contrôler l'intégralité du flux de travaux, cliquez sur le bouton Ajouter un attribut pour sélectionner les attributs à enregistrer à des fins de génération de rapports, puis cliquez sur Enregistrer.

Activez ensuite la configuration du modèle de tâche (si elle n'est pas déjà activée). Pour cela, procédez comme décrit à la section "Activation des modèles de tâches" à la page 301. Ne modifiez pas la valeur par défaut dans la liste des Types de processus sélectionnés ; cliquez uniquement sur Enregistrer.

Le flux des travaux peut maintenant fournir des enregistrements d'audit dont à la fois le nom et la valeur de l'attribut correspondent. Bien que l'activation de ce niveau d'audit fournisse bien plus d'informations, vous devez savoir qu'elle réduit significativement les performances et que vos flux de travail en seront ralentis.

Résolution et atténuation des violations de conformité

Cette section explique comment utiliser la fonction de résolution d'Identity Manager pour protéger le matériel critique.

Elle comprend les rubriques suivantes :

À propos de la résolution

Quand Identity Manager détecte une violation de la compatibilité avec la stratégie d'audit irrésolue (non atténuée), il crée une demande de résolution, qui doit être résolue par un *solutionneur*. Un solutionneur est un utilisateur désigné, autorisé à évaluer violations de stratégie d'audit et à y répondre.

Signalisation des solutionneurs

Identity Manager permet de définir trois niveaux de solutionneurs. Les demandes de résolution sont d'abord envoyées aux solutionneurs de niveau 1. Si aucun solutionneur de niveau 1 ne répond à une demande de résolution dans le délai d'attente imparti, Identity Manager signale la violation aux solutionneurs de niveau 2 et le compte à rebours du nouveau délai d'attente commence. Si aucun solutionneur de niveau 2 ne répond dans le délai d'attente imparti, la demande de résolution est signalée aux solutionneurs de niveau 3.

Pour la résolution, vous devez nommer au moins un solutionneur dans votre entreprise. La désignation de plusieurs solutionneurs pour chaque niveau est facultative, mais conseillée. Plusieurs solutionneurs aident à ne pas retarder ni arrêter le flux des travaux.

Sécurisation de l'accès aux résolutions

Les options d'autorisation suivantes se réfèrent aux éléments de travail d'authType `RemediationWorkItem`.

- Le propriétaire de l'élément de travail de résolution.
- Un responsable direct ou indirect du propriétaire de l'élément de travail de résolution.

- Un administrateur qui contrôle une organisation à laquelle appartient le propriétaire de l'élément de travail de résolution.

Par défaut, les contrôles d'autorisation se comportent de l'une des façons suivantes :

- Le propriétaire est l'utilisateur qui tente l'action.
- Le propriétaire est une organisation contrôlée par l'utilisateur tentant l'action.
- Le propriétaire est un subordonné de l'utilisateur tentant l'action.

Les second et troisième contrôles peuvent être configurés de manière indépendante en modifiant les options suivantes :

- **controlOrg**. Les valeurs valides sont true ou false.
- **subordinate**. Les valeurs valides sont true ou false.
- **lastLevel**. Le dernier niveau de subordonné à inclure dans le résultat ; -1 signifie tous les niveaux. La valeur par défaut de lastLevel est -1, ce qui correspond à subordonnés directs et indirects.

Ces options peuvent être ajoutées ou modifiées dans les éléments suivants :

```
UserForm: Remediation List
```

Processus de flux de travaux de résolution

Identity Manager fournit le Standard Remediation Workflow (flux de travaux de résolution standard) qui assure le traitement de résolution pour les scannages de stratégie d'audit.

Le flux de travaux de résolution standard génère une demande de résolution (élément de travail de type examen) contenant des informations sur la violation de conformité et envoie une notification par e-mail à chaque solutionneur de niveau 1 désigné dans la stratégie d'audit. Quand un solutionneur atténue la violation, le flux de travail change l'état de l'objet Violation de conformité existant et lui assigne une date d'expiration.

Une violation de conformité est identifiée de manière univoque par la combinaison utilisateur, nom de stratégie et nom de règle. Une stratégie d'audit évaluée comme true détermine la création d'une nouvelle violation de conformité pour chaque combinaison utilisateur/stratégie/règle, s'il n'existe pas déjà de violation correspondant à cette combinaison. Si aucune violation n'existe pour cette combinaison et que la violation et en état d'atténuation, le traitement du flux de travail ne prend aucune mesure. Si la violation existante n'est pas atténuée, sa numérotation récurrente est augmentée d'une unité.

Pour plus d'informations sur les flux de travaux de résolution, voir la section “À propos des stratégies d'audit” à la page 444.

Réponse aux demandes de résolution

Par défaut, chaque solutionneur dispose de trois types de réponses :

- **Résoudre**. Un solutionneur indique qu'une mesure corrective a été prise pour résoudre le problème sur la ressource.

  En cas de modification d'une violation de conformité, Identity Manager crée un événement d'audit pour consigner la résolution. De plus, Identity Manager garde en mémoire le nom du solutionneur ainsi que les commentaires éventuels.

  Remarque – Une fois résolue, une violation n'est supprimée qu'au scannage d'audit suivant. Si une stratégie d'audit a été configurée pour permettre de nouveaux scannages, l'utilisateur sera rescanné dès la résolution de la violation.

- **Atténuer**. Un solutionneur autorise la violation et accorde à l'utilisateur une dispense de violation pour un certain laps de temps.

  Si la violation est volontaire (par exemple, un dossier commercial relevant de deux groupes), vous pouvez atténuer la violation pendant une longue période. Vous pouvez aussi atténuer la violation pendant une courte période de temps (par exemple, si l'administrateur système des ressources est en congé et que vous ne savez pas comment résoudre le problème).

  Identity Manager garde en mémoire le nom du solutionneur qui a atténué la violation, ainsi que la date d'expiration de la dispense et tout commentaire associé.

  Remarque – Quand Identity Manager détecte une dispense arrivée à expiration, il change l'état de la violation de « atténué » à « en attente ».

- **Transférer**. Un solutionneur réassigne la responsabilité de la résolution de la violation à un autre utilisateur.

Exemple de résolution

Votre entreprise établit une règle selon laquelle un utilisateur ne peut pas être à la fois responsable des comptes fournisseurs et des comptes clients et vous recevez une notification signalant qu'un utilisateur a violé cette règle.

- Si l'utilisateur est un superviseur ayant la responsabilité des deux rôles le temps que l'entreprise embauche une seconde personne pour le poste, vous pouvez atténuer la violation et émettre une dispense d'une durée maximale de six mois.
- Si l'utilisateur viole la règle, vous pouvez demander à votre Administrateur ERP Oracle de corriger le conflit puis de résoudre la violation une fois le problème réglé pour cette ressource. Sinon, vous pouvez transmettre la demande de résolution à votre Administrateur ERP Oracle.

Modèle d'e-mail de résolution

Identity Manager contient le modèle d'e-mail Avis de violation de stratégie (disponible en sélectionnant l'onglet Configuration puis le sous-onglet Modèles d'e-mails). Vous pouvez configurer ce modèle pour avertir les solutionneurs des violations en attente. Pour plus d'informations, voir la section "Personnalisation des modèles d'e-mails" à la page 106 du Chapitre 4, "Configuration des objets d'administration d'entreprise".

Utilisation de la page Résolutions

Sélectionnez Éléments de travail → Résolutions pour accéder à la page Résolutions.

Vous pouvez utiliser cette page pour :

- afficher les violations en attente ;
- hiérarchiser les violations de stratégies ;
- atténuer une ou plusieurs violations de stratégies ;
- résoudre une ou plusieurs violations de stratégies ;
- transférer une ou plusieurs violations ;
- éditer des utilisateurs à partir d'un élément de travail de résolution.

Affichage des violations de stratégies

Vous pouvez utiliser la page Résolutions pour afficher les détails des violations avant de prendre des mesures adéquates.

Selon vos capacités ou votre place dans la hiérarchie des capacités d'Identity Manager, vous aurez la possibilité d'afficher et de prendre des mesures en cas de violation pour d'autres solutionneurs.

Les rubriques suivantes sont relatives à l'affichage des violations :

- "Affichage des demandes en attente" à la page 477 ;
- "Affichage des demandes terminées" à la page 478 ;
- "Mise à jour du tableau" à la page 479.

Affichage des demandes en attente

Les demandes en attente qui vous ont été assignées sont affichées, par défaut, dans le tableau Résolutions.

Vous pouvez utiliser l'option Lister les résolutions pour afficher les demandes de résolution en attente pour un autre solutionneur.

- Sélectionnez Mes rapports directs pour afficher les demandes en attente d'utilisateurs de votre organisation qui dépendent directement de vous.
- Sélectionnez Rechercher des utilisateurs pour entrer ou localiser un ou plusieurs utilisateurs dont vous voulez afficher les demandes en attente. Entrez un ID d'utilisateur, puis cliquez sur Appliquer pour afficher les demandes en attente de cet utilisateur. Sinon, cliquez sur **...** (Autres) pour rechercher un utilisateur. Après avoir trouvé et sélectionné un utilisateur, cliquez sur Abandonner pour fermer la zone de recherche.

Le tableau obtenu donne les informations suivantes pour chaque demande :

- **Solutionneur**. Nom du solutionneur assigné. Cette colonne s'affiche uniquement quand vous visualisez les demandes de résolution d'autres solutionneurs.
- **Utilisateur**. Utilisateur pour lequel la demande est faite.
- **Stratégie d'audit/Demande**. Action requise du solutionneur.
- **Règle d'audit/Description**. Commentaires de la résolution pour la demande.
- **État de la violation**. État courant de la violation.
- **Gravité**. Gravité attribuée à la demande (Aucune, Faible, Moyenne, Élevée ou Critique).
- **Priorité**. Priorité attribuée à la demande (Aucune, Faible, Moyenne, Élevée ou Urgente).
- **Date de la demande**. Date et heure auxquelles la demande de résolution a été émise.

Remarque – Tout utilisateur peut choisir un formulaire personnalisé contenant les données de résolution relatives à ce solutionneur particulier. Pour assigner un formulaire personnalisé, sélectionnez l'onglet Conformité dans le formulaire utilisateur.

Affichage des demandes terminées

Pour afficher vos demandes de résolution terminées, cliquez sur l'onglet Mes éléments de travail puis sur l'onglet Historique. La liste des éléments de travail précédemment résolus s'affiche.

Le tableau obtenu (qui est généré par un rapport`AuditLog`) contient les informations suivantes sur chaque demande de résolution :

- **Horodatage**. Date et heure auxquelles la demande a été résolue.
- **Objet**. Nom du solutionneur qui a traité la demande.
- **Action**. Indique si le solutionneur a atténué ou résolu la demande.
- **Type**. `ComplianceViolation` ou `Habilitation de l'utilisateur`.
- **Nom de l'objet**. Nom de la stratégie d'audit qui a été violée.
- **Resource**. Indique l'ID de compte du solutionneur (peut également indiquer Non applicable)

- **ID**. ID de compte relatif à la violation de stratégie.
- **Résultat**. Indique toujours `Réussite`.

En cliquant sur un horodatage dans le tableau, vous ouvrez une page Détails d'événement d'audit.

La page Détails d'événement d'audit donne des informations sur la demande terminée, y compris des informations sur sa résolution ou son atténuation, les paramètres de l'événement (le cas échéant) et les attributs auditables.

Mise à jour du tableau

Pour mettre à jour les informations contenues dans le tableau Résolutions, cliquez sur Actualiser. La page Résolution met le tableau à jour avec les nouvelles demandes de résolution éventuelles.

Hiérarchisation des violations de stratégie

Vous pouvez hiérarchiser les violations de stratégies en leur assignant une priorité, une gravité ou ces deux éléments. Hiérarchisez les violations à partir de la page Résolutions.

▼ Pour éditer la priorité ou la gravité des violations

1. **Sélectionnez une ou plusieurs violations dans la liste.**
2. **Cliquez sur Hiérarchiser**

   La page Hiérarchiser les violations de stratégie s'affiche.
3. **Vous pouvez définir un niveau de gravité pour la violation (facultatif). Les choix sont Aucune, Faible, Moyenne, Élevée ou Critique.**
4. **Vous pouvez définir un niveau de priorité pour la violation (facultatif). Les choix sont Aucune, Faible, Moyenne, Élevée ou Urgente.**
5. **Cliquez sur OK quand vous avez terminé de faire des sélections. Identity Manager retourne à la liste des résolutions.**

Remarque – Les niveaux de gravité et de priorité peuvent uniquement être définis pour les résolutions de type VC (violation de conformité).

Atténuation des violations de stratégies

Vous pouvez atténuer les violations de stratégies à partir des pages Résolutions et Examens des violations de stratégies.

Depuis la page Résolutions

▼ Pour atténuer des violations de stratégies en attente à partir de la page Résolutions

1 Sélectionnez des lignes dans le tableau pour indiquer les demandes à atténuer.

- Activez une ou plusieurs options pour spécifier les demandes à atténuer.
- Activez l'option dans l'en-tête du tableau pour atténuer toutes les demandes listées dans le tableau.

Identity Manager permet d'entrer un seul groupe de commentaires pour décrire une action d'atténuation. Vous pouvez ne pas vouloir effectuer de résolution en masse sauf si les violations ont un rapport entre elles et qu'un seul commentaire suffira.

Vous pouvez atténuer uniquement les demandes incluant des violations de stratégies. Les autres demandes de résolution ne peuvent pas être atténuées.

2 Cliquez sur Atténuer.

La page Atténuation de la violation de stratégie (ou Atténuation de plusieurs violations de stratégie) s'affiche.

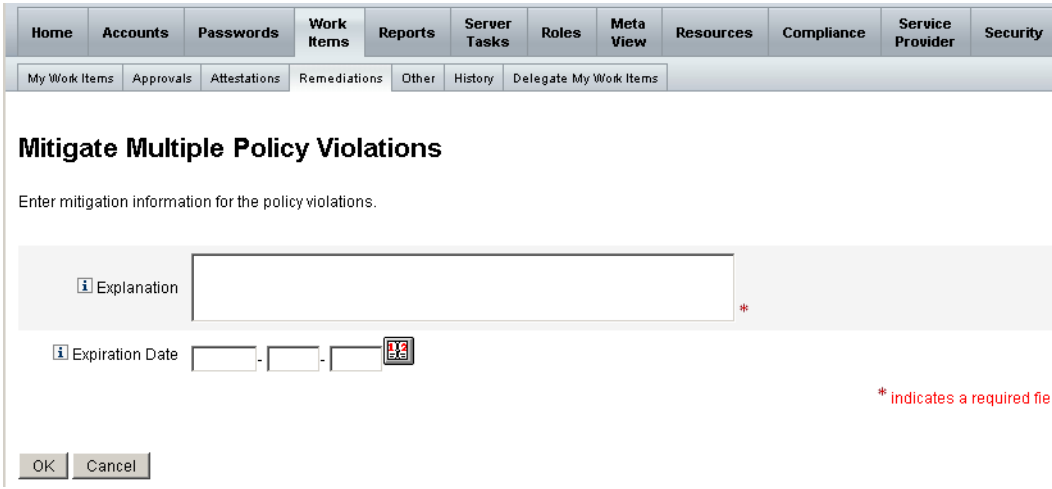


FIGURE 15–3 Page Atténuation de la violation de stratégie

3 **Entrez des commentaires sur la résolution dans le champ Explication.** (*obligatoire*)

Vos commentaires constituent une piste d'audit pour cette action ; veillez, par conséquent, à entrer des informations exhaustives et utiles. Par exemple, précisez la raison de l'atténuation de la violation, la date et la raison du choix d'une période de dispense.

4 **Entrez une date d'expiration pour la période de dispense (format `AAAA-MM-JJ`) directement dans le champ Date d'expiration ou en cliquant sur le bouton Date d'expiration et en sélectionnant une date dans le calendrier.**

Remarque – Si vous n'entrez pas de date, la durée de validité de la dispense est infinie.

---

5 **Cliquez sur OK pour enregistrer vos modifications et revenir à la page Résolutions.**

Résolution des violations de stratégies

▼ Pour résoudre une ou plusieurs violations de stratégies

1 **Utilisez les cases à cocher du tableau pour spécifier quelles demandes résoudre.**

- Cochez une ou plusieurs cases du tableau pour spécifier les demandes à résoudre.
- Cochez la case à cocher de l'en-tête du tableau pour résoudre toutes les demandes listées dans le tableau.

Si vous sélectionnez plusieurs demandes, n'oubliez pas que Identity Manager vous permet d'entrer un unique groupe de commentaires pour décrire l'action de résolution. Vous pouvez ne pas vouloir effectuer de résolution en masse sauf si les violations ont un rapport entre elles et qu'un seul commentaire suffira.

2 Cliquez sur Résoudre.

3 La page Résolution d'une violation de stratégie (ou Résolution de plusieurs violations de stratégie) s'affiche.

4 Entrez des commentaires sur la résolution dans le champ Commentaires.

5 Cliquez sur OK pour enregistrer vos modifications et revenir à la page Résolutions.

Remarque – Les stratégies d'audit directement assignées à un utilisateur (c.-à-d., assignées via l'assignation de l'organisation ou le compte utilisateur) sont toujours réévaluées lorsqu'une violation relative à cet utilisateur est résolue.

Transfert des requêtes de résolution

Vous pouvez transférer une ou plusieurs demandes de résolution à un autre solutionneur.

▼ Pour transférer des requêtes de résolution

1 Utilisez les cases à cocher du tableau pour spécifier quelles demandes transférer.

- Cochez la case à cocher de l'en-tête du tableau pour transférer toutes les demandes listées dans le tableau.
- Cochez une ou plusieurs cases du tableau pour transférer une ou plusieurs demandes.

2 Cliquez sur Transférer.

La page Sélectionner et Confirmer le transfert s'affiche.

FIGURE 15–4 Page Sélectionner et Confirmer le transfert

3 **Entrez le nom du solutionneur dans le champ Transmettre à, puis cliquez sur OK. Sinon, vous pouvez cliquer sur le bouton . . . (Autres) pour rechercher un nom de solutionneur. Sélectionnez un nom dans la liste de recherche puis cliquez sur Définir pour entrer un nom dans le champ Transmettre à. Cliquez sur Abandonner pour fermer la zone de recherche.**

Quand la page Résolutions réapparaît, le nom du nouveau solutionneur s'affiche dans la colonne Solutionneur du tableau.

Édition d'un utilisateur à partir d'un élément de travail de résolution

À partir d'un élément de travail de résolution, vous pouvez (si vous bénéficiez des droits de modification d'un utilisateur) éditer un utilisateur pour résoudre les problèmes (comme décrit dans l'historique des habilitations associé).

Pour éditer un utilisateur, cliquez sur Éditer l'utilisateur sur la page Demande de résolution d'examen. La page Éditer l'utilisateur affichée montre :

- l'historique des habilitations associé à l'utilisateur pour cet élément de travail ;
- les attributs relatifs à l'utilisateur.

  Les options qui s'affichent sur cette page sont les mêmes que dans le formulaire Éditer l'utilisateur disponible dans la zone des Comptes.

Après la modification de l'utilisateur, cliquez sur Enregistrer.

Remarque – L'enregistrement des modifications apportées à l'utilisateur entraîne l'exécution du flux des travaux de mise à jour de l'utilisateur. Vu que ce flux de travaux peut être associé à des approbations, il se peut que les modifications apportées aux comptes utilisateur restent sans effet pendant une certaine période de temps après l'enregistrement. Si la stratégie d'audit permet de répéter le scannage et que le flux de travaux de mise à jour de l'utilisateur n'est pas terminé, le scannage de stratégie suivant pourra détecter la même violation.

Examens d'accès périodiques et attestations

Identity Manager fournit des examens d'accès périodiques, qui permettent aux responsables et autres supérieurs d'examiner et de vérifier les privilèges d'accès des utilisateurs. Ceci permet d'identifier et de gérer l'accumulation, avec le temps, de privilèges par les utilisateurs et aide à maintenir la conformité avec les lois Sarbanes-Oxley, GLBA et autres lois fédérales.

Les examens d'accès peuvent être réalisés ponctuellement en fonction des besoins ou planifiés à des fréquences périodiques, par exemple, tous les trimestres. Vous pouvez ainsi effectuer des examens d'accès périodiques pour que les utilisateurs aient toujours un niveau de privilèges adéquat. Un examen d'accès peut facultativement comporter des scannages de stratégie d'audit.

À propos des examens d'accès périodiques

Un *Examen d'accès périodique* est un processus consistant à certifier qu'un utilisateur donné bénéficie des privilèges appropriés sur les ressources appropriées à un moment particulier.

Un examen d'accès périodique comporte les activités suivantes :

- **Scannages d'examen des accès**. Scannages utilisant certaines règles pour l'évaluation des *habilitations utilisateur* pour déterminer si une attestation est nécessaire.
- **Attestation**. Processus consistant à réponse aux demandes d'attestation en approuvant ou en rejetant les habilitations utilisateur.

Une *habilitation utilisateur* est un enregistrement détaillé des comptes d'un utilisateur sur un ensemble spécifique de ressources.

Scannages d'examen des accès

Pour commencer un examen des accès périodique, vous devez d'abord définir au moins un scannage des accès.

Le scannage des accès définit les personnes faisant l'objet du scannage, les ressources prises en compte, les stratégies d'audit optionnelles évaluées et les règles utilisées pour déterminer les enregistrements d'habilitation qui seront attestés manuellement et par qui.

Processus du flux de travaux d'examen des accès

En général, le flux de travaux d'examen d'accès d'Identity Manager :

- Construit une liste d'utilisateurs, récupère les informations de compte de chaque utilisateur et évalue les stratégies d'audit optionnelles.
- Crée des enregistrements d'habilitation utilisateur.
- Détermine si chaque enregistrement d'habilitation utilisateur doit faire l'objet d'une attestation.

- Assigne des éléments de travail à chaque attestateur.
- Attend l'approbation de tous les attestateurs ou le premier refus.
- Réassigne la demande à l'attestateur suivant, s'il ne reçoit pas de réponse dans le délai d'attente spécifié.
- Actualise les enregistrements d'habilitation utilisateur avec les résolutions.

Pour la description des capacités de résolution, voir la section "Résolution de l'examen des accès" à la page 504.

Capacités d'administrateur requises

Pour réaliser un examen périodique des accès et gérer les processus d'examen, un utilisateur doit bénéficier de la capacité Administrateur d'examens d'accès périodiques de l'auditeur. Un utilisateur ayant la capacité Administrateur des scannages d'accès d'audit peut créer et gérer les scannages des accès.

Pour assigner ces capacités, vous devez intervenir sur le compte utilisateur et modifier les attributs de sécurité. Pour plus d'informations sur les capacités, voir la section "Comprendre et gérer les capacités" à la page 216 au Chapitre 6, "Administration".

Processus d'attestation

L'*Attestation* est un processus de certification effectué par un ou plusieurs attestateurs désignés pour confirmer une habilitation utilisateur telle qu'elle se présente à une date donnée. Pendant un examen des accès, l'attestateur (ou les attestateurs) reçoit un e-mail de notification des demandes d'attestation des examens d'accès. Un attestateur peut être un utilisateur Identity Manager, mais ne doit pas nécessairement être un administrateur Identity Manager.

Flux de travail d'attestation

Identity Manager utilise un flux de travail d'attestation qui est lancé quand un scannage d'accès détecte des enregistrements d'habilitation nécessitant un examen. Pour cela, le scannage des accès se base sur les règles définies dans le scannage des accès.

Une règle évaluée par le scannage des accès détermine si l'enregistrement d'habilitation de l'utilisateur doit être attesté manuellement ou s'il peut être approuvé ou rejeté automatiquement. Si l'enregistrement d'habilitation de l'utilisateur doit être attesté manuellement, le scannage des accès utilise une deuxième règle pour déterminer quels sont les attestateurs appropriés.

Tout enregistrement d'habilitation utilisateur devant être attesté manuellement est assigné à un flux de travaux, avec un élément de travail par attestateur. Il est possible d'envoyer la notification de ces éléments de travail à l'attestateur en utilisant un flux de travaux ScanNotification regroupant tous les éléments dans une notification, par attestateur et par scannage. La notification sera effectuée par habilitation utilisateur, sauf si le flux de travaux

ScanNotification est sélectionné. Un attestateur peut donc recevoir plusieurs notifications par scannage, même en grand nombre, en fonction du nombre d'utilisateurs scannés.

Sécurisation de l'accès aux attestations

Ces options d'autorisation sont relatives aux éléments de travail d'authType `RemediationWorkItem`.

- Le propriétaire de l'élément de travail.
- Un responsable direct ou indirect du propriétaire de l'élément de travail.
- Un administrateur qui contrôle une organisation à laquelle appartient le propriétaire de l'élément de travail.
- Les utilisateurs qui ont été validés suite à des contrôles d'authentification.

Par défaut, les contrôles d'autorisations se comportent de *l'une* des façons suivantes :

- Le propriétaire est l'utilisateur qui tente l'action.
- Le propriétaire est une organisation contrôlée par l'utilisateur tentant l'action.
- Le propriétaire est un subordonné de l'utilisateur tentant l'action.

Les second et troisième contrôles peuvent être configurés de manière indépendante en modifiant les propriétés suivantes du formulaire :

- `controlOrg` — Les valeurs admises sont true ou false.
- `subordinate` — Les valeurs admises sont true ou false.
- `lastLevel` — Le dernier niveau de subordonné à inclure dans le résultat ; `-1` signifie tous les niveaux.

La valeur entière par défaut de `lastLevel` est `-1`, indiquant des subordonnés directs et indirects.

Vous pouvez ajouter ou modifier ces options de la façon suivante :

```
UserForm: AccessApprovalList.
```

Remarque – Si vous paramétrez la sécurité sur attestations à des organisations contrôlées, la capacité Attestateur Auditeur est également requise pour modifier d'autres attestations de l'utilisateur.

Attestation déléguée

Par défaut, le flux des travaux de scannage des accès respecte les délégations, pour les éléments de travail de type Attestation d'examen des accès et Résolution de l'examen des accès, créées par les utilisateurs pour les éléments de travail d'attestation et les notifications. L'administrateur des

scannages d'accès peut désélectionner l'option Suivre la délégation pour ignorer les paramètres de délégation. Si un attestateur a délégué tous les éléments de travail à un autre utilisateur mais que l'option Suivre la délégation n'est pas paramétrée pour un scannage d'examen des accès, l'attestateur - et *pas* l'utilisateur à qui les délégations ont été assignées - recevra les notifications des demandes d'attestation et les éléments de travail.

Planification d'examens d'accès périodiques

Un examen d'accès peut être un processus long et laborieux pour toute entreprise. L'examen d'accès périodique d'Identity Manager permet de gagner du temps et de l'argent en automatisant une grande partie du processus. Toutefois, certaines tâches du processus restent chronophages. Par exemple, la recherche des données d'un compte utilisateur parmi des milliers d'utilisateurs peut prendre un temps considérable. L'attestation manuelle des enregistrements peut également prendre beaucoup de temps. Une bonne planification améliore l'efficacité du processus et réduit considérablement les efforts nécessaires.

La planification d'examens d'accès périodiques mérite quelques considérations :

- La durée du scannage peut varier considérablement en fonction du nombre d'utilisateurs et des ressources concernées.

  Un seul examen d'accès périodique peut prendre un ou plusieurs jours dans une organisation de grande taille et une attestation manuelle peut prendre une ou plusieurs semaines.

  Par exemple, pour une organisation comptant 50 000 utilisateurs et dix ressources, un scannage des accès peut prendre approximativement une journée, si on se base sur le calcul suivant :

  1 s/ressource * 50K utilisateurs * 10 ressources / 5 connexions simultanées = 28 heures

  Si les ressources sont disséminées dans plusieurs régions géographiques, ce temps augmente encore à cause des temps de latence du réseau.
- L'utilisation de plusieurs serveurs Identity Manager pour un traitement parallèle des données peut accélérer le processus d'examen des accès.

  L'exécution de plusieurs scannages en parallèle est plus efficace quand les ressources ne sont pas communes à tous les scannages. Lors de la définition d'un examen d'accès, vous devez créer plusieurs scannages et limiter les ressources à un ensemble de ressources spécifiques, en utilisant différentes ressources pour chaque scannage. Ensuite, quand vous lancerez la tâche, vous devrez sélectionner plusieurs scannages et programmer leur exécution immédiate.
- La personnalisation du flux des travaux d'attestation et des règles vous offre un meilleur contrôle du processus et davantage d'efficacité.

  Par exemple, vous pouvez personnaliser la règle de l'Attestateur pour étendre les obligations d'attestation à plusieurs attestateurs. Le processus d'attestation affecte des éléments de travail et envoie les notifications en conséquence.

- L'utilisation des Règles de signalisation des attestateurs permet de réduire le temps de réponse pour les demandes d'attestation.

  Définissez la règle de signalisation de l'attestateur ou utilisez une règle personnalisée pour configurer une chaîne de signalisation d'attestateurs. Vous devez également spécifier les délais de signalisation.
- Bien comprendre le mécanisme des Règles de détermination de l'examen permet un gain de temps en déterminant automatiquement les enregistrements d'habilitation qui nécessitent un examen manuel.
- Effectuez une notification groupée des demandes d'attestation pour un scannage en spécifiant un flux de travaux de notification au niveau du scannage.

Réglage des tâches de scannage

Lors d'un processus de scannage, plusieurs threads accèdent à la vue de l'utilisateur, permettant un accès potentiel aux ressources pour lesquelles l'utilisateur possède des comptes. L'accès à cette vue détermine l'évaluation de plusieurs stratégies d'audit et règles qui peut entraîner la création de violations de conformité.

Pour éviter que deux threads n'actualisent simultanément la même vue utilisateur, le processus établit un verrouillage à l'intérieur de la mémoire sur le nom d'utilisateur. Si le verrouillage n'a pas été établi (par défaut) dans un délai de cinq secondes, une erreur est associée au scannage et l'utilisateur est ignoré, ce qui assure ainsi une protection contre les scannages simultanés sur un même groupe d'utilisateurs.

Vous pouvez entrer les valeurs de plusieurs "paramètres réglables" fournis comme arguments de tâche dans la tâche de scannage :

- `clearUserLocks` (Booléenne). Si la condition est "true", tous les verrous utilisateur actuels sont libérés avant le démarrage du scannage.
- `userLock` (nombre entier). Délai d'attente (en millisecondes) lors d'une tentative de verrouillage d'un utilisateur. La valeur par défaut est 5 secondes. Une valeur négative désactive le verrouillage pour ce scannage.
- `scanDelay` (nombre entier). Temps de pause (en millisecondes) entre les distributions des threads de scannage. La valeur par défaut est 0 (pas de pause). Si vous entrez une valeur pour cet argument, le scannage sera plus lent, mais le système sera plus réactif à d'autres opérations.
- `maxThreads` (nombre entier). Nombre de threads simultanés utilisés pour traiter un scannage. La valeur par défaut est 5. Si la réponse des ressources est très lente, l'augmentation de ce chiffre peut accélérer le scannage.

Pour modifier les valeurs de ces paramètres, éditez le formulaire de Définition des tâches correspondant. Pour plus d'informations, voir le Chapitre 2, "Identity Manager Forms" du *Sun Identity Manager Deployment Reference*.

Création d'un scannage d'accès

▼ Pour définir le scannage d'examen des accès

1 **Sélectionnez Conformité→ Gérer les scannages d'accès**

2 **Cliquez sur Nouveau pour afficher la Création d'un nouveau scannage des accès.**

3 **Attribuez un nom au scannage d'accès.**

Remarque – Les noms des scannages des accès ne doivent pas contenir les caractères suivants :

' (apostrophe), . (point), | (barre verticale), [(crochet gauche),] (crochet droit), , (virgule), : (deux points), $ (symbole du dollar), " (guillemets doubles) et = (signe égal).

Évitez également d'utiliser ces caractères : _ (soulignement), % (pourcent), ^ (circonflexe) et * (astérisque)

---

4 **Ajoutez une description compréhensible pour l'identification du scannage (** *facultatif***).**

5 **Activez l'option Habilitations dynamiques pour donner des options supplémentaires aux attestateurs.**

Ces options sont les suivantes :

- Une attestation en attente peut faire l'objet d'un nouveau scannage immédiat pour actualiser les données d'habilitation et réévaluer le besoin d'une attestation.
- Une attestation en attente peut être dirigée vers un autre utilisateur pour sa résolution. Après la résolution, les données d'habilitation sont actualisées et réévaluées pour déterminer le besoin d'une attestation.

6 **Spécifiez le Type d'étendue de l'utilisateur (***obligatoire***).**

Choisissez l'une des options suivantes :

- **Règle Selon la condition de l'attribut**. Scanne les utilisateurs en fonction de la règle de Type d'étendue de l'utilisateur sélectionnée.

  Identity Manager fournit les règles par défaut suivantes :

  - Tous les administrateurs,

Remarque – Vous pouvez ajouter des règles définissant l'étendue de l'utilisateur en utilisant Identity Manager IDE Pour toute information sur Identity Manager IDE, allez sur `https://identitymanageride.dev.java.net/`.

- Tous mes subordonnés,
- Tous les non-administrateurs,
- Mes subordonnés directs,
- Utilisateur sans responsable.

- **Assigné aux ressources**. Scanne tous les utilisateurs qui ont un compte sur une ou plusieurs ressources sélectionnées. Si vous choisissez cette option, la page affiche les Ressources de l'étendue de l'utilisateur, qui permettent de spécifier des ressources.
- **Selon un rôle spécifique**. Scanne tous les membres qui ont au moins un rôle, ou tous les rôles, que vous spécifiez.
- **Membres d'organisations**. Choisissez cette option pour scanner tous les membres d'une ou plusieurs organisations sélectionnées.
- **Rapports aux responsables**. Scanne tous les utilisateurs qui dépendent des responsables sélectionnés. La hiérarchie est déterminée par l'attribut Identity Manager du compte Lighthouse de l'utilisateur.

  Si l'étendue de l'utilisateur est *organisation* ou *responsable*, l'option Étendue récursive est disponible. Cette option permet une sélection récursive de l'utilisateur dans la chaîne des membres contrôlés.

7 Si vous décidez également d'explorer les stratégies d'audit pour détecter les violations lors du scannage d'examen des accès, sélectionnez les stratégies d'audit à appliquer à ce scannage en déplaçant vos sélections de la liste des Stratégies d'audit disponibles à la liste des Stratégies d'audit en cours.

L'ajout de stratégies d'audit à un scannage d'accès détermine le même comportement que l'exécution d'un scannage d'audit sur le même groupe d'utilisateurs. Toutefois, toute violation détectée par les stratégies d'audit est stockée dans l'enregistrement d'habilitation de l'utilisateur. Cette information peut faciliter l'approbation et le rejet automatique, parce que la règle peut utiliser, comme partie intégrante de sa logique, la présence ou l'absence de violations dans l'enregistrement d'habilitation utilisateur.

8 Si vous avez scanné les stratégies d'audit lors de l'étape précédente, vous pouvez utiliser l'option Mode de stratégie pour spécifier comment le scannage des accès détermine les stratégies d'audit à exécuter pour un utilisateur donné. Un utilisateur peut avoir des stratégies assignées au niveau utilisateur et/ou au niveau de son organisation. Le comportement de

scannage des accès par défaut consiste à appliquer les stratégies pour le scannage des accès uniquement si l'utilisateur n'a pas encore de stratégies assignées.

a. Appliquer les stratégies sélectionnées et ignorer les autres assignations.

b. Appliquer les stratégies sélectionnées seulement si l'utilisateur n'a pas encore d'assignations.

c. Appliquer les stratégies sélectionnées en plus des assignations de l'utilisateur.

9 (Facultatif) Spécifiez le Propriétaire du processus d'examen. Utilisez cette option pour indiquer un propriétaire de la tâche d'examen des accès en cours de définition. Si un Propriétaire du processus d'examen est spécifié, un attestateur, qui rencontre un conflit potentiel en répondant à une demande d'attestation, peut *s'abstenir* au lieu d'approuver ou de rejeter une habilitation utilisateur ; dans ce cas, la demande d'attestation est transférée au Propriétaire du processus d'examen. Cliquez sur la boîte de sélection (ellipse) pour rechercher des comptes utilisateur et faire votre sélection.

10 Suivre la délégation. Sélectionnez cette option pour activer la délégation pour le scannage des accès. Le scannage des accès ne tiendra compte des paramètres de la délégation que si cette option est cochée. Suivre la délégation est activé par défaut.

11 Restreindre les ressources cible. Sélectionnez cette option pour limiter le scannage aux ressources cible.

Ce paramètre a un impact direct sur l'efficacité du scannage des accès. Si les ressources cible ne sont pas restreintes, chaque enregistrement d'habilitation utilisateur contiendra les informations de compte pour chacune des ressources auxquelles l'utilisateur est relié. Par conséquent, chaque ressource assignée est interrogée pour chaque utilisateur pendant le scannage. En utilisant cette option pour spécifier un sous-ensemble de ressources, vous pouvez réduire considérablement les temps de traitement d'Identity Manager pour la création d'enregistrements d'habilitation utilisateur.

12 Exécuter la résolution de violation. Sélectionnez cette option pour activer le flux de travaux de résolution des stratégies d'audit quand une violation est détectée.

Si cette option est sélectionnée, une violation détectée sur l'une des stratégies d'audit assignées entraînera l'exécution du flux de travaux de résolution des stratégies d'audit respectives.

Cette option doit normalement être sélectionnée, sauf pour les cas avancés.

13 Flux de travaux de l'approbation de l'accès. Sélectionnez le flux de travaux d'attestation standard par défaut ou un flux de travaux personnalisé (si disponible).

Ce flux de travaux s'utilise pour présenter à des attestateurs appropriés l'enregistrement d'habilitation de l'utilisateur pour son examen (selon la règle de l'attestateur). Le flux de travaux des attestations standard par défaut crée un seul élément de travail pour chaque attestateur. Si le

scannage des accès spécifie une signalisation, ce flux de travaux doit signaliser les éléments de travail restés trop longtemps en sommeil. Si aucun flux de travaux n'est spécifié, l'attestation de l'utilisateur restera indéfiniment

en attente.

Remarque – Pour plus d'informations sur la création et l'utilisation des règles Identity Auditor mentionnées dans cette étape et les suivantes, voir le Chapitre 4, "Working with Rules" du *Sun Identity Manager Deployment Reference*.

---

14 Règle de l'attestateur. Sélectionnez la règle d'attestateur par défaut ou sélectionnez une règle d'attestateur personnalisée (si disponible).

La règle de l'attestateur reçoit l'enregistrement d'habilitation utilisateur en tant qu'entrée et retourne une liste de noms d'attestateurs. Si vous avez sélectionné Suivre la délégation, le scannage des accès transforme la liste des noms en y laissant uniquement les noms des utilisateurs appropriés selon les informations de délégation configurées par chaque utilisateur dans la liste de noms d'origine. Si la délégation d'un utilisateur Identity Manager donne comme résultat un cycle de routine, les informations de délégation sont rejetées tandis que l'élément de travail est envoyé à l'attestateur initial. La règle `Default Attestor` indique que l'attestateur doit être le responsable (idmManager) de l'utilisateur auquel l'enregistrement d'habilitation se réfère ou bien le Compte Configurateur si l'`idmManager` de cet utilisateur est null. Si l'attestation doit impliquer des propriétaires de ressources ainsi que des responsables, vous devez utiliser une règle personnalisée.

15 Règle de signalisation à l'attestateur. Utilisez cette option pour spécifier la règle de signalisation à l'attestateur ou sélectionnez une règle personnalisée (si disponible). Vous pouvez aussi indiquer un délai de signalisation pour cette règle. Le délai de signalisation par défaut est 0 jour.

Cette règle spécifie la chaîne de signalisation pour un élément de travail qui a franchi le délai de signalisation. La règle de signalisation à l'attestateur par défaut transmet une requête d'attestation au responsable de l'attestateur (`idmManager`) ou au configurateur si la valeur `idmManager` de l'attestateur est null.

Vous pouvez entrer un délai de signalisation en minutes, heures ou jours.

L'ouvrage contient des informations supplémentaires sur la règle de signalisation à l'attestateur.

16 Règle de détermination de l'examen. (*obligatoire*)

Sélectionnez l'une des règles suivantes pour spécifier comment le processus de scannage déterminera la disposition d'un enregistrement d'habilitation :

- **Reject Changed Users** (Rejeter utilisateurs modifiés). Rejette automatiquement l'enregistrement d'habilitation utilisateur s'il diffère de la dernière habilitation utilisateur issue de la même définition de scannage des accès et si la dernière habilitation utilisateur avait été approuvée. Sinon, cette règle force l'attestation manuelle et approuve toutes les habilitations utilisateur restées inchangées depuis l'habilitation utilisateur approuvée au préalable. Par défaut, seule la portion « comptes » de la vue de l'utilisateur est prise en considération pour cette règle.
- **Review Changed Users** (Examiner utilisateurs modifiés). Cette règle force l'attestation manuelle de tout enregistrement d'habilitation utilisateur si celui-ci diffère de la dernière habilitation utilisateur issue de la même définition de scannage des accès et si la dernière habilitation utilisateur avait été approuvée. Approuve toutes les habilitations utilisateur restées inchangées depuis la dernière habilitation utilisateur approuvée. Par défaut, seule la portion « comptes » de la vue de l'utilisateur est prise en considération pour cette règle.
- **Review Everyone** (Examiner tous). Cette règle force l'attestation manuelle de tous les enregistrements d'habilitation utilisateur.

Les règles Reject Changed Users et Review Changed Users comparent l'habilitation utilisateur avec la dernière instance du même scannage des accès dans lequel l'enregistrement d'habilitation avait été approuvé.

Vous pouvez modifier ce comportement en copiant et en modifiant les règles pour limiter la comparaison à toute partie sélectionnée de la vue de l'utilisateur.

Cette règle peut retourner les valeurs suivantes :

- **-1**. Aucune attestation n'est requise.
- **0**. Rejette automatiquement l'attestation.
- **1**. Attestation manuelle requise.
- **2**. Approuve automatiquement l'attestation.
- **3**. Résout automatiquement l'attestation (résolution automatique).

  Cet ouvrage contient des informations supplémentaires sur la Règle de détermination de l'examen.

17 **Remediator Rule (Règle du solutionneur). Sélectionnez la règle à utiliser pour déterminer la personne devant résoudre l'habilitation d'un utilisateur spécifique dans le cas d'une résolution automatique. Cette règle peut examiner l'habilitation et les violations actuelles de l'utilisateur, et doit renvoyer une liste d'utilisateurs pour la résolution. Si aucun règle n'est spécifiée, aucune résolution n'aura lieu. Le plus souvent, cette règle s'applique quand l'habilitation comporte des violations de conformité.**

18 **Règle de formulaire utilisateur de résolution. Sélectionnez une règle à utiliser pour le choix d'un formulaire adapté pour les solutionneurs d'attestation pendant l'édition des utilisateurs. Les solutionneurs peuvent définir leur propre formulaire, qui remplacera celui-ci. Cette règle de formulaire doit être définie si le scannage détecte des données très spécifiques qui correspondent à un formulaire personnalisé.**

19 **Flux de travaux de notification.**

Sélectionnez l'une des options suivantes pour spécifier le comportement de la notification pour chaque élément de travail :

- **Aucun**. Il s'agit de la valeur par défaut. La sélection de cette option détermine l'envoi à l'attestateur d'un e-mail de notification pour chaque habilitation utilisateur individuelle qu'il doit attester.
- **ScanNotification**. La sélection de cette option regroupe les demandes d'attestation dans une même notification. La notification indique le nombre de demandes d'attestation qui ont été assignées au destinataire.

  Si un Propriétaire du processus d'examen a été spécifié dans le scannage des accès, le flux des travaux de ScanNotification enverra une notification au propriétaire du processus d'examen au début et à la fin du scannage. Voir "Création d'un scannage d'accès" à la page 489.

  Le flux des travaux ScanNotification utilise le modèle d'e-mail suivant :

  - Avis de début du scannage d'accès
  - Avis de fin du scannage d'accès
  - Avis d'attestation en masse

    Vous pouvez personnaliser le flux des travaux ScanNotification.

20 **Limite des violations. Utilisez cette option pour indiquer le nombre maximum de violations de conformité pouvant être émis par ce scannage avant son abandon. Par défaut, la limite est fixée à 1 000. Si le champ est vide, aucune limite n'est fixée.**

Bien qu'au cours d'un scannage d'audit ou d'un scannage des accès, le nombre des violations de stratégie est généralement faible par rapport au nombre des utilisateurs, le paramétrage de cette valeur peut servir de protection contre l'impact d'une stratégie défectueuse qui augmenterait significativement le nombre des violations. Par exemple, supposons :

qu'un scannage des accès portant sur 50 000 utilisateurs génère deux ou trois violations par utilisateur : les coûts de résolution pour chaque violation de conformité peuvent avoir des conséquences néfastes sur le système Identity Manager.

21 **Organisations. Sélectionnez les organisations pour lesquelles l'objet de ce scannage d'accès est disponible. Ce champ est obligatoire.**

Cliquez sur Enregistrer pour enregistrer la définition du scannage.

Suppression d'un scannage d'accès

Vous pouvez supprimer un ou plusieurs scannages d'accès. Pour supprimer un scannage d'accès, sélectionnez Gérer les scannages d'accès sous l'onglet Conformité, puis sélectionnez le nom du scannage et cliquez sur Supprimer.

Gestion des examens d'accès

Après la définition d'un scannage d'accès, vous pouvez l'utiliser ou le programmer comme faisant partie d'un examen d'accès. Après le lancement d'un examen d'accès, vous disposez de plusieurs options vous permettant de gérer le processus d'examen.

Dans les sections ci-après, vous trouverez des informations plus détaillées sur les questions suivantes :

Lancement d'un examen d'accès

Pour lancer un examen d'accès à partir de l'interface administrateur, vous avez le choix entre les méthodes suivantes :

- Cliquez sur Lancer l'examen depuis la page Conformité → Examens des accès.
- Sélectionnez la tâche d'examen des accès depuis la page Tâches du serveur → Exécuter des tâches.

Sur la page Lancer une tâche qui s'affiche, entrez un nom pour l'examen d'accès. Sélectionnez les scannages dans la liste Scannages d'accès disponibles et déplacez-les dans la liste Scannages d'accès sélectionnés.

Si vous sélectionnez plusieurs scannages, vous pouvez choisir l'une des options de lancement suivantes :

- **immédiatement**. Cette option lance immédiatement le scannage, dès que vous cliquez sur le bouton Lancer. Si vous sélectionnez cette option pour plusieurs scannages dans le lancement de la tâche, les scannages seront effectués en parallèle.
- **après une attente**. Cette option vous permet d'indiquer un délai d'attente avant de démarrer le scannage, relatif au lancement de la tâche d'examen des accès.

Remarque – Vous pouvez démarrer plusieurs scannages pendant une session d'examen des accès. Toutefois, vu que chaque scannage porte sur un nombre élevé d'utilisateurs, le processus complet peut prendre plusieurs heures avant d'arriver à son terme. Il est donc vivement conseillé de gérer vos scannages en conséquence. Par exemple, vous pouvez lancer un scannage qui s'exécutera immédiatement et en planifier d'autres à des horaires échelonnés.

Cliquez sur Lancer pour commencer le processus d'examen des accès.

Remarque – Le nom que vous assignez à un examen d'accès est important. Certains rapports peuvent établir une comparaison entre les examens d'accès de même nom exécutés périodiquement.

Quand vous lancez un examen d'accès, le schéma de progression du flux des travaux s'affiche en vous montrant l'avancement du processus.

Planification des tâches d'examen des accès

Il est possible de planifier une tâche d'examen des accès depuis la zone Tâche du serveur. Par exemple, pour configurer l'exécution périodique des examens des accès, sélectionnez Gérer la planification puis définissez la périodicité. Vous pouvez par exemple planifier l'exécution de la tâche à une fréquence mensuelle ou trimestrielle.

Pour planifier la périodicité, sélectionnez la tâche Examen d'accès sur la page Planifier tâches, puis complétez les informations sur la page Créer un programme de tâches.

Cliquez sur Enregistrer pour enregistrer la tâche planifiée.

Remarque – Par défaut, Identity Manager garde en mémoire les résultats des tâches d'examen des accès pendant une semaine. Si vous décidez de planifier un examen plus fréquemment, configurez les Options de résultats sur supprimer. Si les Options de résultats ne sont pas définies sur supprimer, le nouvel examen ne sera pas exécuté parce que les résultats de la tâche précédente seront encore présents.

Gestion de la progression des examens d'accès

Utilisez l'onglet Examens des accès pour contrôler la progression d'un examen des accès. Cette fonction est accessible sous l'onglet Conformité.

Sous l'onglet Examens des accès, vous pouvez afficher un récapitulatif de tous les examens d'accès actifs et traités précédemment. Pour chaque examen d'accès de la liste, vous disposez des informations suivantes :

- **Statut**. Statut courant du processus d'examen : en cours d'initialisation, en cours d'arrêt, arrêté, nombre de scannages en cours, nombre de scannages planifiés, en attente des attestations, ou terminé.
- **Date de lancement**. La date (horodatage) à laquelle la tâche d'examen des accès a commencé.
- **Total des utilisateurs**. Nombre total des utilisateurs à explorer.
- **Détails des habilitations**. Des colonnes supplémentaires du tableau fournissent les totaux des habilitations par statut. Elles précisent les habilitations en attente, approuvées, rejetées, arrêtées ou résolues, ainsi que le nombre total des habilitations.

  La colonne Résolu indique le nombre d'habilitations qui sont EN COURS DE RÉSOLUTION. Après la résolution d'une habilitation, son état devient EN ATTENTE ; par conséquent, à la conclusion d'un examen d'accès, la valeur de cette colonne est 0 (zéro).

Pour obtenir des informations plus détaillées sur l'examen, sélectionnez l'examen pour ouvrir un rapport récapitulatif.

La Figure 15–5 donne un exemple de rapport récapitulatif d'un examen des accès.

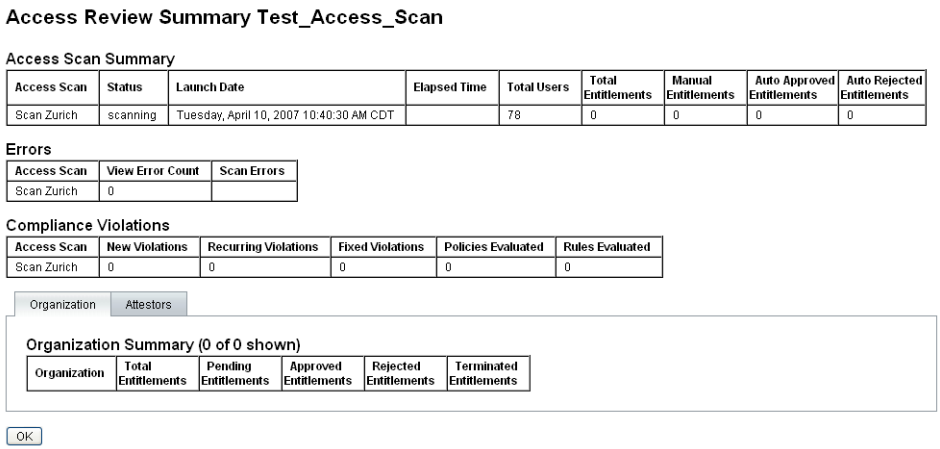


FIGURE 15–5 Page de Rapport récapitulatif d'un examen des accès

Cliquez sur l'onglet de formulaire Organisation ou Attestateurs pour afficher les informations de scannage classées selon ces objets.

Vous pouvez également voir et télécharger ces informations dans un rapport en exécutant le Rapport récapitulatif de l'examen des accès.

Modification des attributs des scannages

Après la configuration d'un scannage des accès, vous pouvez ajouter de nouvelles options au scannage en indiquant, par exemple, des ressources cible à explorer ou des stratégies d'audit à explorer pour détecter des violations pendant l'exécution du scannage des accès.

Pour définir un scannage, sélectionnez-le dans la liste des scannages des accès, puis modifiez ses attributs dans la page Éditer un scannage d'examen des accès.

Vous devez cliquer sur Enregistrer pour enregistrer les modifications apportées à la définition du scannage.

Remarque – Le changement de l'étendue d'un scannage des accès peut entraîner la modification des informations dans les enregistrements d'habilitation utilisateur récemment acquis, à cause de son impact sur la règle de détermination de l'examen, si cette règle compare les habilitations utilisateur avec des enregistrements d'habilitation plus anciens.

Annulation d'un examen d'accès

Dans la page Examens d'accès, cliquez sur Arrêter pour arrêter un examen sélectionné en cours.

L'arrêt d'un examen a les conséquences suivantes:

- Tous les scannages planifiés sont déplanifiés.
- Tous les scannages actifs sont arrêtés.
- Tous les flux de travaux et les éléments de travail en attente sont supprimés.
- Toutes les attestations en attente sont marquées comme annulées.
- Toutes les attestations que les utilisateurs ont terminées restent inchangées.

Suppression d'un examen d'accès

Dans la page Examens d'accès, cliquez sur Supprimer pour supprimer un examen sélectionné.

Vous pouvez supprimer un examen d'accès si le statut de la tâche est *arrêtée* ou *terminée*. Une tâche d'examen des accès en cours ne peut pas être supprimée si elle n'a pas d'abord été arrêtée.

La suppression d'un examen d'accès supprime tous les enregistrements d'habilitation utilisateur qui avaient été générés par cet examen. L'action de suppression est enregistrée dans le journal de l'audit.

Pour supprimer un examen d'accès, cliquez sur Supprimer dans la page Examen des accès.

Remarque – L'annulation et la suppression d'un examen des accès peut entraîner la mise à jour d'un grand nombre d'objets et de tâches Identity Manager, et peut donc prendre plusieurs minutes. Vous pouvez contrôler la progression de l'opération en affichant les résultats des tâches dans Tâches du serveur → Toutes tâches.

Gestion des obligations d'attestation

Vous pouvez gérer les demandes d'attestation depuis l'interface Administrateur ou Utilisateur d'Identity Manager. Cette section fournit des informations sur la réponse aux demandes d'attestations et les obligations liées aux attestations.

Notification des examens des accès

Au cours d'un scannage, Identity Manager envoie une notification aux attestateurs lorsque les demandes d'attestations nécessitent leur approbation. Si les responsabilités de l'attestateur ont été déléguées, les demandes d'attestations sont envoyées au délégué. Si plusieurs attestateurs ont été définis, chaque attestateur recevra un e-mail de notification.

Ces demandes apparaissent comme des éléments de travail d'attestation dans l'interface d'Identity Manager. Les éléments de travail d'attestation en attente sont affichés quand l'attestateur assigné se connecte à Identity Manager.

Affichage des demandes d'attestation en attente

Affichez les éléments de travail d'attestation depuis la zone Éléments de travail de l'interface d'Identity Manager. En ouvrant l'onglet Attestation dans la zone Éléments de travail, vous obtenez la liste de tous les enregistrements d'habilitation nécessitant une approbation. Dans la page Attestations, vous pouvez également afficher la liste des enregistrements d'habilitation pour tous vos rapports directs et pour les utilisateurs spécifiés que vous contrôlez directement ou indirectement.

Action sur les enregistrements d'habilitation

Les éléments de travail d'attestation contiennent les enregistrements d'habilitation utilisateur qui doivent être examinés. Les enregistrements d'habilitation fournissent des informations sur les privilèges d'accès des utilisateurs, les ressources assignées et les violations de stratégies.

Les réponses possibles à une demande d'attestation sont les suivantes :

- **Approuver**. Atteste que l'habilitation est appropriée pour ce qui est de la date indiquée dans l'enregistrement d'habilitation.
- **Rejeter**. L'enregistrement d'habilitation fait état de non-conformités possibles qui ne peuvent pas être validées ni résolues.

- **Nouveau scannage**. Demande un nouveau scannage pour réévaluer l'habilitation utilisateur.
- **Transférer**. Vous permet d'indiquer un autre destinataire pour l'examen.
- **S'abstenir**. L'attestation pour cet enregistrement n'est pas appropriée et on ne connaît pas d'attestateur plus approprié. L'élément de travail d'attestation est transféré au propriétaire du processus d'examen. Cette option n'est disponible que si un propriétaire du processus d'examen a été défini dans la tâche d'examen des accès.

Si un attestateur ne répond pas à une demande par l'une de ces actions avant la fin du délai de signalisation spécifié, un avis est envoyé à l'attestateur suivant de la chaîne de signalisation. Le processus de notification continue jusqu'à ce qu'une réponse soit consignée.

Le statut d'une attestation peut être contrôlé sous l'onglet Conformité → Examens des accès.

Résolution en boucle fermée

Vous pouvez éviter de rejeter des habilitations utilisateur :

- En marquant une habilitation comme « à corriger » en demandant sa correction par un autre utilisateur (Demande de résolution). Dans ce cas, un nouvel élément de travail de résolution est créé et assigné à un ou plusieurs solutionneurs spécifiés.

  Le nouveau solutionneur peut alors décider d'éditer l'utilisateur, soit en utilisant Identity Manager soit indépendamment, puis, une fois satisfait, de marquer l'élément de travail comme résolu. Dans ce cas, l'habilitation utilisateur est à nouveau scannée et évaluée.
- En demandant une réévaluation de l'habilitation (Nouveau scannage). Dans ce cas, l'habilitation utilisateur est à nouveau explorée et évaluée. L'élément de travail d'attestation d'origine est fermé. Un nouvel élément de travail d'attestation est créé si l'habilitation requiert encore une attestation selon les règles définies dans le scannage des accès.

Demande de résolution

Si une attestation en attente est définie par le scannage·des accès, vous pouvez l'acheminer vers un autre utilisateur à des fins de résolution.

Remarque – L'option Habilitations dynamiques sur les pages Créer un scannage d'accès ou Édition du scannage des accès active cette fonction.

▼ Pour demander une résolution depuis un autre utilisateur

1 Sélectionnez une ou plusieurs habilitations dans la liste des attestations, puis cliquez sur Demander la résolution.

La page Sélectionner et confirmer la demande de résolution s'affiche.

2. **Entrez un nom d'utilisateur, puis cliquez sur Ajouter pour ajouter l'utilisateur dans le champ Transmettre à. Sinon, cliquez sur ... (Autres) pour rechercher un nom d'utilisateur. Sélectionnez l'utilisateur dans la liste de recherche, puis cliquez sur Ajouter pour ajouter l'utilisateur dans la liste Transmettre à. Cliquez sur Abandonner pour fermer la zone de recherche.**

3. **Entrez des commentaires dans le champ Commentaires, puis cliquez sur Poursuivre.**

   Identity Manager renvoie la liste des attestations.

Remarque – Des informations détaillées sur la demande de résolution s'affichent dans la zone Historique de l'habilitation utilisateur en question.

Nouveau scannage des attestations

Si une attestation en attente est définie par le scannage·des accès, vous pouvez répéter le scannage et la réévaluer.

Remarque – L'option Habilitations dynamiques sur les pages Créer un scannage d'accès ou Édition du scannage des accès active cette fonction.

▼ Pour répéter le scannage d'une attestation en attente

1. **Sélectionnez une ou plusieurs habilitations dans la liste des attestations, puis cliquez sur Nouveau scannage.**

   La page Nouveau scannage des habilitations d'utilisateurs s'affiche.

2. **Entrez des commentaires sur le nouveau scannage dans la zone Commentaires, puis cliquez sur Poursuivre.**

Transfert d'éléments de travail d'attestation

Vous pouvez transférer un ou plusieurs éléments de travail d'attestation vers un autre utilisateur.

▼ Pour transférer des attestations

1. **Entrez un ou plusieurs éléments de travail dans la liste des attestations, puis cliquez sur Transférer.**

   La page Sélectionner et Confirmer le transfert s'affiche.

2. **Entrez un nom d'utilisateur dans le champ Transmettre à. Une autre solution consiste à cliquer sur le bouton ... (Autres) afin de rechercher un nom d'utilisateur.**

3 **Entrez des commentaires sur le transfert dans le champ Commentaires.**

4 **Cliquez sur Poursuivre.**

Identity Manager retourne la liste des attestations.

Remarque – La zone Historique de l'habilitation utilisateur en question affiche des informations détaillées sur le transfert.

Signature numérique des actions d'examen des accès

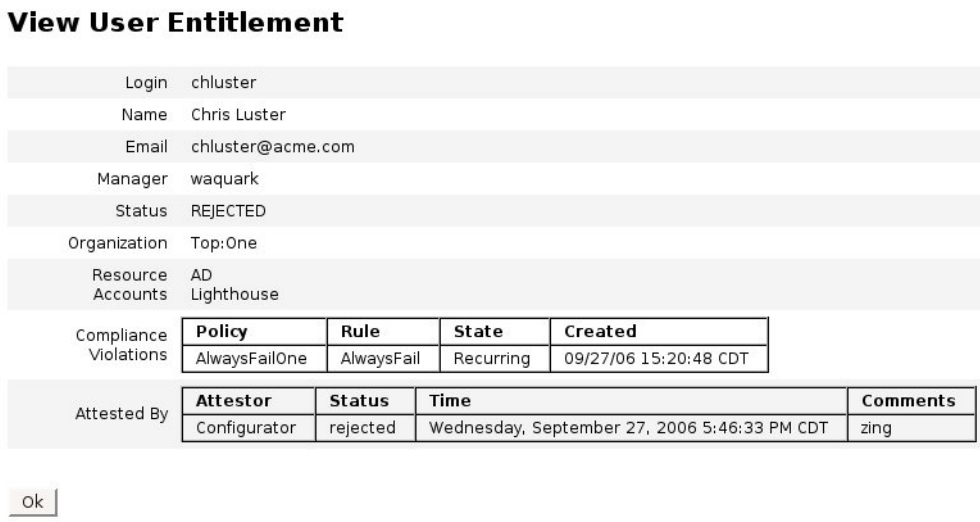
Vous pouvez définir une signature numérique pour la gestion des actions d'examen des accès. Pour toute information sur la configuration des signatures numériques, voir la section "Signature des approbations" à la page 240. Les sujets traités dans cette section expliquent la configuration requise côté serveur et côté client pour ajouter le certificat et la LRC à Identity Manager pour les approbations signées.

Rapports des examens des accès

Identity Manager fournit les rapports suivants, que vous pouvez utiliser pour évaluer les résultats d'un examen des accès :

- **Rapport de couverture des examens d'accès**. Fournit une liste d'utilisateurs précisant les chevauchements des habilitations utilisateur, les différences ou ces deux éléments sous forme de tableau, selon le mode de définition du rapport. Ce rapport peut également comporter des colonnes supplémentaires avec les examens d'accès qui contiennent des chevauchement et/ou des différences.
- **Rapport détaillé de l'examen des accès**. Ce rapport fournit les informations suivantes sous forme de tableau :
  - **Nom**. Nom de l'enregistrement d'habilitation utilisateur
  - **Statut**. Statut courant du processus d'examen : en cours d'initialisation, en cours d'arrêt, arrêté, nombre de scannages en cours, nombre de scannages planifiés, en attente des attestations, ou terminé.
  - **Attestateur**. Les utilisateurs Identity Manager désignés comme attestateurs pour l'enregistrement.
  - **Date de balayage**. Horodatage enregistré au moment du scannage.
  - **Date de disposition**. Date (horodatage) de l'attestation de l'enregistrement d'habilitation.
  - **Organisation**. Organisation de l'utilisateur dans les enregistrements d'habilitation.
  - **Responsable**. Supérieur d'un utilisateur qui a fait l'objet d'un scannage.
  - **Ressources**. Ressources sur lesquelles l'utilisateur a des comptes, qui ont été capturées dans cette habilitation utilisateur.

- **Violations**. Nombre de violations détectées au cours de l'examen.
- Cliquez sur un nom dans le rapport pour ouvrir l'enregistrement d'habilitation utilisateur. "Rapports des examens des accès" à la page 502 affiche un échantillon des informations fournies dans la vue de l'enregistrement d'habilitation utilisateur.



View User Entitlement

Login	chluster
Name	Chris Luster
Email	chluster@acme.com
Manager	waquark
Status	REJECTED
Organization	Top:One
Resource Accounts	AD Lighthouse

Compliance Violations

Policy	Rule	State	Created
AlwaysFailOne	AlwaysFail	Recurring	09/27/06 15:20:48 CDT

Attested By

Attestor	Status	Time	Comments
Configurator	rejected	Wednesday, September 27, 2006 5:46:33 PM CDT	zing

Ok

- **Rapport récapitulatif de l'examen des accès**.

  Ce rapport, également décrit à la section "Gestion de la progression des examens d'accès" à la page 496 et illustré à la Figure 15–5, présente les informations récapitulatives suivantes sur les scannages d'accès que vous avez sélectionnés pour le rapport :

  - **Nom de l'examen**. Nom du scannage des accès
  - **Date**. Horodatage du moment où l'examen a été lancé
  - **Nombre d'utilisateurs**. Nombre d'utilisateurs scannés pour l'examen
  - **Nombre d'habilitations**. Nombre d'enregistrements d'habilitation générés
  - **Approuvé**. Nombre d'enregistrements d'habilitation approuvés
  - **Rejeté**. Nombre d'enregistrements d'habilitation rejetés
  - **En attente**. Nombre d'enregistrements d'habilitation encore en attente
  - **Annulé**. Nombre d'enregistrements d'habilitation annulés

  Ces rapports peuvent être téléchargés au format PDF (Portable Document Format) ou CSV (Comma-Separated Value) depuis la page Exécuter des rapports.

Résolution de l'examen des accès

La résolution des violations de conformité et la résolution des examens des accès sont gérées dans la zone Résolutions sous l'onglet Éléments de travail. Il existe toutefois des différences entre les deux types de résolution. Cette section décrit le comportement unique de la résolution des examens des accès et montre comment ce comportement diffère des tâches de résolution et des informations fournies dans "Résolution et atténuation des violations de conformité" à la page 474.

À propos de la résolution de l'examen des accès

Quand un attestateur demande la résolution d'une habilitation utilisateur, le flux de travaux d'attestation standard crée une demande de résolution, qui doit être résolue par un solutionneur (un solutionneur est un utilisateur désigné, autorisé à évaluer les demandes de résolution et à y répondre).

Le problème peut uniquement être résolu ; il ne peut pas être atténué. L'attestation ne peut pas continuer tant que le problème n'est pas résolu.

Lorsque les résolutions sont le résultat d'un examen des accès, le tableau de bord des examens des accès suit tous les attestateurs et solutionneurs qui ont participé à l'examen.

Signalisation des demandes de résolution de l'examen des accès

Les demandes de résolution de l'examen des accès ne sont pas réassignées au-delà du solutionneur initial.

Le processus de flux de travaux de résolution

La logique de résolution des examens d'accès est définie dans le flux de travaux de résolution standard.

Lorsqu'un attestateur demande la résolution d'une habilitation utilisateur, le flux de travaux de résolution standard :

- génère une demande de résolution (de type `accessReviewRemediation`), contenant des informations sur l'habilitation utilisateur qui doit être résolue ;
- envoie un e-mail au solutionneur requis.

Le nouveau solutionneur peut alors décider d'éditer l'utilisateur, soit en utilisant Identity Manager soit indépendamment, puis, une fois satisfait, de marquer l'élément de travail comme résolu. Dans ce cas, l'habilitation utilisateur est à nouveau scannée et évaluée.

Réponse aux demandes de résolution d'examens d'accès

Par défaut, le solutionneur des examens d'accès a le choix entre trois réponses :

- **Résoudre**. Un solutionneur indique qu'une mesure corrective a été prise pour résoudre le problème.

  Dans ce cas, l'habilitation utilisateur est à nouveau scannée et évaluée. Si l'habilitation utilisateur est encore marquée comme nécessitant une attestation, l'attestateur d'origine continue à la voir dans la liste des éléments de travail Attestations.

  Des informations détaillées sur l'action de la demande de résolution s'affichent dans la zone Historique de l'habilitation utilisateur en question.
- **Transférer**. Un solutionneur réassigne la responsabilité de la résolution de la demande de résolution à un tiers.

  Des informations détaillées sur l'action de transfert s'affichent dans la zone Historique de l'habilitation utilisateur en question.
- **Éditer l'utilisateur**. Un solutionneur choisit d'éditer directement l'utilisateur pour remédier au problème.

  Ce bouton ne s'affiche que si le solutionneur est autorisé à modifier les utilisateurs. Après avoir apporté des modifications à l'utilisateur et cliqué sur Enregistrer, le solutionneur accède à la page de confirmation de la résolution pour entrer une description de la modification apportée à l'utilisateur.

  Dans ce cas, l'habilitation utilisateur est à nouveau scannée et évaluée. Si l'habilitation utilisateur est encore marquée comme nécessitant une attestation, l'attestateur d'origine continue la voir dans la liste des éléments de travail Attestations.

  Des informations détaillées sur l'édition s'affichent pour l'action de demande de résolution dans la zone Historique de l'habilitation utilisateur en question.

Page Résolutions

La colonne Type contient l'acronyme UE (User Entitlement, habilitation utilisateur) pour tous les éléments de travail de résolution qui sont des éléments de travail de résolution d'examens des accès.

Actions de résolution d'examen des accès non prises en charge

Les fonctionnalités de hiérarchisation et d'atténuation ne sont pas prises en charge pour la résolution des examens des accès.

◆ ◆ ◆ CHAPITRE 16

Exportateur de données

La fonction Exportateur de données permet de consigner des informations sur les utilisateurs, les rôles et d'autres types d'objets dans un entrepôt de données externe.

Ce chapitre contient les informations et procédures à suivre pour paramétrer et mettre à jour l'exportateur de données. Pour des informations détaillées sur la planification et l'implémentation de l'exportateur de données, voir le Chapitre 5, "Data Exporter" du *Sun Identity Manager Deployment Guide*.

Ce chapitre se compose des rubriques suivantes :

Présentation de l'exportateur de données

Identity Manager contient et traite les données pertinentes pour la gestion des identités à travers les systèmes et applications distribués. Pour améliorer la performance d'ensemble, Identity Manager ne conserve pas toutes les données qu'il génère pendant le provisioning normal et les autres activités quotidiennes. Par exemple, Identity Manager par défaut ne conserve pas les activités de flux de travaux ni les instances de tâches d'état intermédiaire. S'il est nécessaire de capturer tout ou partie des données qu'Identity Manager abandonne d'habitude, vous pouvez activer la fonctionnalité Exportateur de données.

Lorsque l'exportateur de données est activé, Identity Manager stocke tout changement apporté à un objet spécifié (type de données) détecté sous la forme d'un enregistrement dans une table du référentiel. Ces événements sont mis en file d'attente jusqu'à ce qu'une tâche les écrive dans un entrepôt de données externe (vous pouvez configurer la fréquence à laquelle chaque type de

données est exporté). Les données exportées peuvent être encore traitées ou utilisées comme point de départ pour des interrogations et transformations à l'aide d'outils de transformation commerciale, de génération de rapports et d'analyse.

L'exportation des données dans un entrepôt a un impact négatif sur les performances du serveur Identity Manager et cette fonctionnalité doit être désactivée, sauf si l'entreprise a réellement besoin d'exporter les données.

Identity Manager permet également de créer et d'exécuter des requêtes sur attributs. Une requête sur attributs explore l'entrepôt de données pour identifier les objets Utilisateur ou Rôle qui satisfont les critères spécifiés. Pour plus d'informations, voir "Configuration des requêtes sur attributs" à la page 521.

Planification de l'implémentation de l'exportateur de données

L'exportateur de données étant désactivé par défaut, vous devez le configurer pour qu'il devienne opérationnel. Plusieurs décisions préliminaires doivent être prises pour la configuration de l'exportateur de données.

- Quels seront les types de données exportés ?
- Quelles seront les techniques employées pour capturer les données pour chaque type de données ?
- Quelle sera la fréquence d'exportation des différents types de données ?
- Que contiendra le schéma exporté pour chaque type de données ?
- Une classe de fabrique WIC (Warehouse Interface Code) sera-t-elle nécessaire ?

Lorsque l'exportateur de données est activé, la configuration par défaut exporte tous les attributs de tous les types de données. Cela peut causer des charges de traitement inutiles sur Identity Manager et l'entrepôt en consommant sur ce dernier un espace de stockage qui ne sera jamais utilisé. L'entreposage des données a tendance à être conservateur et à capturer les données lorsqu'il y a une chance qu'elles soient utilisées ultérieurement. Vous n'avez pas à exporter toutes les données qui peuvent être exportées. Vous pouvez configurer les types de données à exporter et empêcher l'exportation de certains événements.

Une fois les décisions ci-dessus prises, suivez les étapes ci-après pour implémenter l'exportateur de données.

▼ Pour implémenter l'exportateur de données

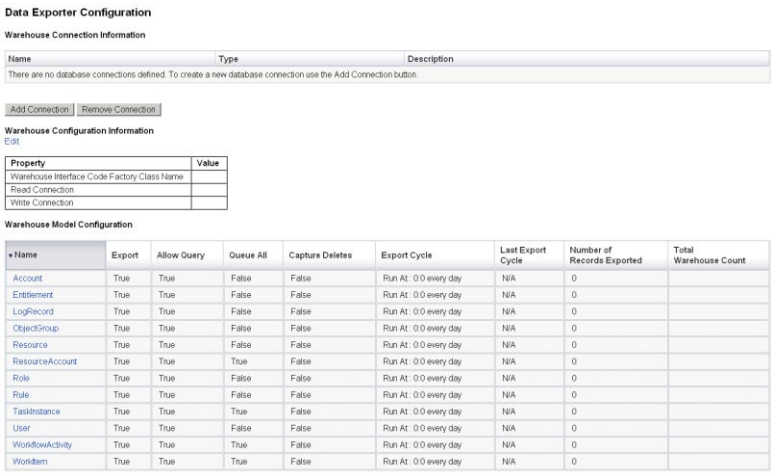
1. **(facultatif) Personnalisez le schéma d'exportation pour les types sélectionnés et régénérez la LDD de l'entrepôt. Pour plus d'informations, reportez-vous à "Customizing Data Exporter" du *Sun Identity Manager Deployment Guide*.**
2. **Créez un compte utilisateur sur le RDBMS de l'entrepôt et chargez la LDD de l'entrepôt sur ce système. Pour plus d'informations, voir "Customizing Data Exporter" du *Sun Identity Manager Deployment Guide*.**
3. **Configurez l'exportateur de données, comme décrit à la section "Configuration de l'exportateur de données" à la page 509.**
4. **Testez l'exportateur de données pour vérifier qu'il est configuré correctement. Pour plus d'informations, voir "Test de l'exportateur de données" à la page 520.**
5. **(facultatif) Créez des requêtes sur attributs qui explorent les données écrites dans l'entrepôt de données. Pour plus d'informations, voir "Configuration des requêtes sur attributs" à la page 521.**
6. **Mettez à jour l'exportateur de données en utilisant JMX et en contrôlant les fichiers journaux. Pour plus d'informations, voir "Mise à jour de l'exportateur de données" à la page 525.**

Configuration de l'exportateur de données

La page Configuration de l'exportateur de données permet de définir les types de données à conserver, de spécifier les attributs à exporter et de programmer l'exportation des données. Chaque type de données peut être configuré séparément.

▼ Pour configurer l'exportateur de données

1. **Dans l'interface administrateur, cliquez sur Configurer dans le menu principal. Cliquez ensuite sur l'onglet secondaire Entrepôt. La page Configuration de l'exportateur de données s'ouvre.**



Data Exporter Configuration

Warehouse Connection Information

Name	Type	Description
There are no database connections defined. To create a new database connection use the Add Connection button.		

Add Connection | Remove Connection

Warehouse Configuration Information
Edit

Property	Value
Warehouse Interface Code Factory Class Name	
Read Connection	
Write Connection	

Warehouse Model Configuration

Name	Export	Allow Query	Queue All	Capture Deletes	Export Cycle	Last Export Cycle	Number of Records Exported	Total Warehouse Count
Account	True	True	False	False	Run At : 0:0 every day	N/A	0	
Entitlement	True	True	False	False	Run At : 0:0 every day	N/A	0	
LogRecord	True	True	False	False	Run At : 0:0 every day	N/A	0	
ObjectGroup	True	True	False	False	Run At : 0:0 every day	N/A	0	
Resource	True	True	False	False	Run At : 0:0 every day	N/A	0	
ResourceAccount	True	True	True	False	Run At : 0:0 every day	N/A	0	
Role	True	True	False	False	Run At : 0:0 every day	N/A	0	
Rule	True	True	False	False	Run At : 0:0 every day	N/A	0	
TaskInstance	True	True	True	False	Run At : 0:0 every day	N/A	0	
User	True	True	False	False	Run At : 0:0 every day	N/A	0	
WorkflowActivity	True	True	True	False	Run At : 0:0 every day	N/A	0	
WorkItem	True	True	True	False	Run At : 0:0 every day	N/A	0	

FIGURE 16–1 Configuration de l'exportateur de données

2 **Pour définir et écrire des connexions, cliquez sur le bouton Ajouter la connexion. La page Éditer la connexion de base de données s'ouvre.**

Complétez les champs de cette page et cliquez sur Enregistrer pour revenir à la page Configuration de l'exportateur de données. Pour plus d'informations, voir "Définition de connexions en lecture et en écriture" à la page 511.

3 **Pour assigner la classe WIC et les connexions de base de données, cliquez sur le lien Éditer qui figure dans la section Informations de configuration de l'entrepôt. La page Configuration de l'entrepôt de l'exportateur de données s'ouvre.**

Complétez les champs de cette page et cliquez sur Enregistrer pour revenir à la page Configuration de l'exportateur de données. Pour plus d'informations, voir "Définition des informations de configuration de l'entrepôt" à la page 513.

4 **Cliquez sur le lien d'un type de données dans la table Configuration de modèle d'entrepôt. La page Configuration du type d'exportateur de données s'ouvre.**

Complétez les onglets Exporter, Attributs et Planifier de cette page et cliquez sur Enregistrer pour revenir à la page Configuration de l'exportateur de données. Pour plus d'informations, voir "Configuration des modèles d'entrepôts " à la page 514.

Répétez cette étape pour chaque type de données.

5 **Pour configurer le flux de travaux qui sera exécuté avant et après toute exportation d'un type de données, cliquez sur le lien Éditer dans la section Automatisation de l'exportateur. La page Configuration de l'automatisation de l'exportateur de données s'ouvre.**

Complétez les champs de cette page et cliquez sur Enregistrer pour revenir à la page Configuration de l'exportateur de données. Pour plus d'informations, voir la section appropriée.

6 **Pour configurer le démon de la tâche d'exportation, cliquez sur le lien Éditer qui figure dans la section Configuration de tâche d'entrepôt. La page Configuration de l'entrepôt de l'exportateur de données s'ouvre.**

Complétez les champs de cette page et cliquez sur Enregistrer pour revenir à la page Configuration de l'exportateur de données. Pour plus d'informations, voir "Configuration de la tâche d'entrepôt" à la page 517.

Remarque – Une fois ces étapes effectuées, l'exportation est entièrement opérationnelle. Lorsque l'exportation est activée, les enregistrements de données commencent à se mettre en file d'attente pour l'exportation. Si vous n'activez pas la tâche d'exportation, les tables des files se remplissent et la mise en file d'attente est suspendue. Il est en général plus efficace d'exporter des petits lots (plus fréquents) que des gros, mais l'exportation dépend de la disponibilité d'écriture de l'entrepôt lui-même, qui peut être limitée pour d'autres raisons.

---

7 **En option, définissez la taille de file d'attente maximale. Pour plus d'informations, voir "Modification de l'objet Configuration" à la page 519.**

Définition de connexions en lecture et en écriture

Identity Manager utilise une connexion en écriture pendant les cycles d'exportation. Il utilise la connexion en lecture pour indiquer le nombre d'enregistrements figurant actuellement dans l'entrepôt (pendant la configuration de l'entrepôt) et pour servir l'interface des requêtes sur attributs.

Les connexions à l'entrepôt peuvent être définies comme une DataSource de serveur d'application, une connexion JDBC ou une référence à une ressource de données. Si une connexion JDBC ou une ressource de base de données est définie, l'exportation des données utilise de manière extensive un petit nombre de connexions pendant les opérations d'écriture puis ferme toutes les connexions. L'exportateur de données utilise uniquement la connexion en lecture pendant la configuration de l'entrepôt et l'exécution des requêtes sur attributs, et ferme ces connexions dès la fin de l'opération.

L'exportateur utilise le même schéma pour les connexions en écriture et en lecture, et vous pouvez utiliser les mêmes informations de connexion pour ces deux connexions. Cependant, si vous avez des connexions séparées, le déploiement peut écrire dans un ensemble de tables d'activation de l'entrepôt, faire de ces tables l'entrepôt réel puis transformer les tables de l'entrepôt en un mini-entrepôt de données dans lequel Identity Manager lira.

Vous pouvez éditer le formulaire Data Export Configuration (Configuration de l'exportation des données) pour empêcher Identity Manager de lire dans l'entrepôt. Ce formulaire contient la propriété `includeWarehouseCount`, suivant laquelle Identity Manager interroge l'entrepôt et affiche le nombre d'enregistrements de chaque type de données. Pour désactiver cette fonctionnalité, copiez le formulaire Data Export Configuration, remplacez la valeur de la propriété `includeWarehouseCount` par `true` et importez votre formulaire personnalisé.

▼ Pour définir des connexions en lecture et en écriture

1 Dans la page Configuration de l'exportateur de données, cliquez sur le bouton Ajouter la connexion.

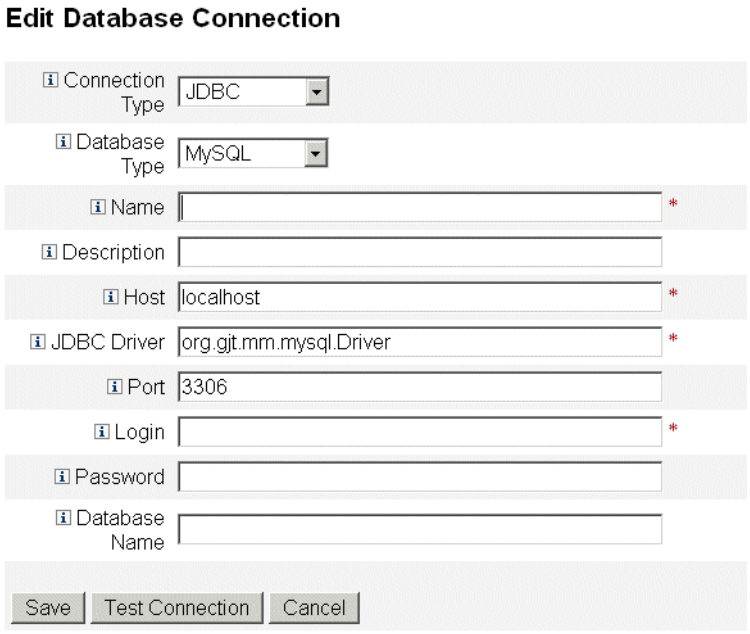


FIGURE 16–2 Configuration de l'exportateur de données

2 Indiquez la façon dont Identity Manager établira les connexions en lecture ou en écriture avec l'entrepôt de données en sélectionnant une option dans le menu déroulant Type de connexion.

- **JDBC**. Cette option connecte à une base de données en utilisant l'interface de programmation d'applications JDBC (Java Database Connectivity). Le groupement des connexions est assuré par le Warehouse Interface Code.
- **Ressource**. Cette option utilise les informations définies dans une ressource. Le groupement des connexions est assuré par le Warehouse Interface Code.
- **Source de données**. Cette option utilise le serveur d'application sous-jacent pour la gestion des connexions et le groupement. Ce type de connexion requiert des connexions depuis le serveur d'application.

  Les champs qui s'affichent sur la page varient selon l'option que vous avez sélectionnée dans le menu déroulant **Type de connexion**. Pour des informations détaillées sur la configuration de la connexion avec la base de données, consultez l'aide en ligne.

3 **Cliquez sur Enregistrer pour enregistrer vos changements de configuration et revenir à la page Configuration de l'exportateur de données.**

Répétez cette procédure si vous utiliserez des connexions en lecture et en écriture séparées.

Définition des informations de configuration de l'entrepôt

Pour configurer l'entrepôt, vous devez sélectionner une connexion en lecture, une connexion en écriture et indiquer une classe de fabrique WIC (Warehouse Interface Code). La classe de fabrique WIC assure l'interface entre Identity Manager et l'entrepôt. Identity Manager fournit une implémentation par défaut du code mais vous pouvez compiler la vôtre. Pour plus d'informations sur la création de classes de fabrique personnalisées, voir le Chapitre 5, "Data Exporter" du *Sun Identity Manager Deployment Guide*.

Le fichier `jar` contenant la classe de fabrique et tous les fichiers `jar` de support doivent être présents dans le répertoire `$WSHOME/exporter` sur le serveur Identity Manager qui exécute la tâche d'exportation et sur tout serveur configurant l'exportateur de données. Un seul serveur Identity Manager peut exporter des données à tout instant t.

▼ Pour définir les informations de configuration de l'entrepôt

1 **Dans la page Configuration de l'exportateur de données, cliquez sur le lien Éditer qui figure dans la section Informations de configuration de l'entrepôt.**

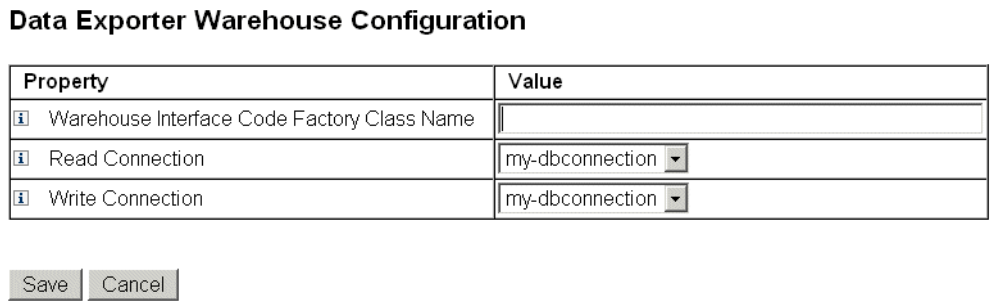


FIGURE 16–3 Configuration de l'exportateur de données

2 **Spécifiez une valeur dans le champ Nom de la classe de fabrique du code de l'interface d'entrepôt. Si votre intégrateur n'a pas créé de classe personnalisée, entrez la valeur** `com.sun.idm.warehouse.base.Factory`**.**

3 **Spécifiez les connexions en sélectionnant une option dans les deux menus déroulants Lire la connexion et Écrire la connexion.**

4 **Cliquez sur Enregistrer pour enregistrer vos changements de configuration et revenir à la page Configuration de l'exportateur de données.**

Configuration des modèles d'entrepôts

Tout type de données exportable possède une série d'options permettant de contrôler si, comment et quand exporter ce type de données. Étant donné qu'exporter les données augmente la charge pesant sur les serveurs Identity Manager, l'exportation ne doit être activée que pour les types de données présentant un intérêt réel pour l'entreprise.

Le tableau suivant décrit les différentes types de données qui peuvent être exportés.

TABLEAU 16–1 Types de données pris en charge

Type de données	Description
`Account`	Enregistrement contenant la liaison entre un utilisateur et un compte de ressource.
`AdminGroup`	Groupe de permissions Identity Manager disponibles sur tous les groupes d'objets.
`AdminRole`	Permissions assignées à un ou plusieurs groupes d'objets.
AuditPolicy	Collection de règles évaluées pour un objet Identity Manager afin d'en déterminer la compatibilité avec une stratégie d'entreprise.
`ComplianceViolation`	Enregistrement contenant une non compatibilité d'un utilisateur avec une stratégie d'audit.
`Entitlement`	Enregistrement contenant la liste des attestations d'un utilisateur spécifique.
`LogRecord`	Enregistrement contenant un unique enregistrement d'audit.
`ObjectGroup`	Conteneur de sécurité modélisé sous la forme d'une organisation.
`Resource`	Système/application sur lequel les comptes sont provisionnés.
`ResourceAccount`	Ensemble d'attributs constituant un compte sur une ressource spécifique.
`Role`	Conteneur logique pour l'accès.
`Rule`	Bloc de logique qui peut être exécuté par Identity Manager.
`TaskInstance`	Enregistrement indiquant un processus en cours d'exécution ou terminé.
`User` (Utilisateur)	Utilisateur logique incluant zéro compte ou plus.

TABLEAU 16–1 Types de données pris en charge *(Suite)*

Type de données	Description
`WorkflowActivity`	Activité unique d'un flux de travaux Identity Manager.
`WorkItem`	Action manuelle d'un flux de travaux Identity Manager.

▼ Pour configurer des modèles d'entrepôts

1 **Dans la page Configuration de l'exportateur de données, cliquez sur un lien de type de données.**

2 **Dans l'onglet Exporter, indiquez si exporter ce type de données. Si vous ne voulez pas l'exporter, désélectionnez la case à cocher Exporter et cliquez sur Enregistrer. Sinon, sélectionnez les options restantes de l'onglet Exporter.**

- **Autoriser la requête**. Contrôle si le modèle peut être interrogé.
- **File d'attente, tout**. Capture tous les changements apportés aux objets de ce type. Cocher cette option peut ajouter des coûts de traitement considérables à l'Exportateur. Utilisez cette option avec parcimonie.
- **Capture des suppressions**. Enregistre tous les objets supprimés de ce type. Cocher cette option peut ajouter des coûts de traitement considérables à l'Exportateur. Utilisez cette option avec parcimonie.

3 **L'onglet Attributs permet de sélectionner les attributs qui peuvent être spécifiés dans le cadre d'une requête sur attributs et ceux qui peuvent être affichés dans les résultats des requêtes. Vous ne pouvez pas supprimer les attributs par défaut depuis l'interface administrateur. Pour plus d'informations sur la modification des attributs par défaut, voir le Chapitre 1, "Working with Attributes" du *Sun Identity Manager Deployment Guide*.**

Les noms des nouveaux attributs ont les caractéristiques suivantes :

- `attrName` : l'attribut est de premier niveau et scalaire.
- `attrName[]` : l'attribut est un attribut de premier niveau avec valeur de liste, où les éléments de la liste ont une valeur scalaire.
- `attrName['`*clé*`']` : l'attribut contient une valeur de mappe et la valeur de la mappe avec la clé spécifiée est désirée.
- `attrName[].`*nom2* : l'attribut est un attribut de premier niveau avec valeur de liste, où les éléments de la liste sont des structures. *nom2* est l'attribut auquel accéder dans la structure.

Remarque – Si vous voulez exporter des attributs vers le tableau `EXT_RESOURCEACCOUNT_ACCTATTR`, vous devez contrôler la case Audit de chaque attribut à exporter.

---

4 **Spécifiez la fréquence à laquelle exporter les informations associées avec le type de données sur l'onglet Planifier. Les cycles sont relatifs à la minuit sur le serveur. Un cycle devrait avoir lieu toutes les 20 minutes en commençant à l'heure pile, puis 20 et 40 minutes plus tard. Si une tentative d'exportation prend plus longtemps qu'un cycle programmé, le cycle suivant sera ignoré. Par exemple si un cycle est défini toutes les 20 minutes et commence à minuit et qu'il faut 25 minutes pour terminer l'exportation, la prochaine exportation commencera à 00h40. L'exportation programmée à l'origine pour 00h20 n'aura pas lieu.**

Configuration de l'automatisation de l'exportateur

Identity Manager permet de spécifier des flux de travaux qui s'exécutent avant et après l'exportation des données.

Le flux de travaux Cycle Start (Début de cycle) peut, par exemple, être utilisé pour empêcher une exportation si un événement justifiant une annulation se produit. Par exemple, si une application qui lit ou écrit dans les tables d'activation a besoin d'un accès exclusif à ces tables au moment où une exportation est programmée, l'exportation doit être annulée. Le flux de travaux doit retourner la valeur 1 pour annuler l'exportation. Identity Manager crée un enregistrement d'audit qui indique que l'exportation a été ignorée et fournit les résultats d'erreur. Si le flux de travaux retourne 0 et qu'aucune erreur ne se produit, le type de données sera exporté.

Le flux de travaux Cycle Complete (Cycle complet) s'exécute une fois que tous les enregistrements ont été exportés. Ce flux de travaux déclenche en général une autre application pour le traitement des données exportées. Une fois ce flux de travaux terminé, l'exportateur contrôle s'il n'y a pas un autre type de données à exporter.

Des exemples de flux de travaux figurent dans le fichier `$WSHOME/sample/web/exporter.xml`. Le `subtype` d'un flux de travaux de l'exportateur est `DATA_EXPORT_AUTOMATION` et son `authType` `WarehouseConfig`.

▼ Pour configurer l'automatisation de l'exportateur

1 **Dans la page Configuration de l'exportateur de données, cliquez sur le lien Éditer qui figure dans la section Automatisation de l'exportateur.**

2 **En option, sélectionnez un flux de travaux à exécuter avant une exportation à partir du menu déroulant Flux de travaux de début de cycle.**

3 **En option, sélectionnez un flux de travaux à exécuter après une exportation à partir du menu déroulant Flux de travaux de début de cycle.**

Configuration de la tâche d'entrepôt

Il n'est pas obligatoire d'exécuter la tâche d'exportation sur un serveur dédié, mais vous devez l'envisager si vous pensez exporter une quantité de données importante. La tâche d'exportation est efficace pour transférer les données d'Identity Manager dans l'entrepôt et consommera autant de CPU que possible pendant l'opération. Si vous n'utilisez pas de serveur dédié, vous devez empêcher ce serveur de gérer le trafic interactif car le temps de réponse augmente considérablement pendant une exportation de grande ampleur.

▼ Pour configurer les informations de configuration de l'entrepôt

1 **Dans la page Configuration de l'exportateur de données, cliquez sur le lien Éditer qui figure dans la section Configuration de tâche d'entrepôt.**

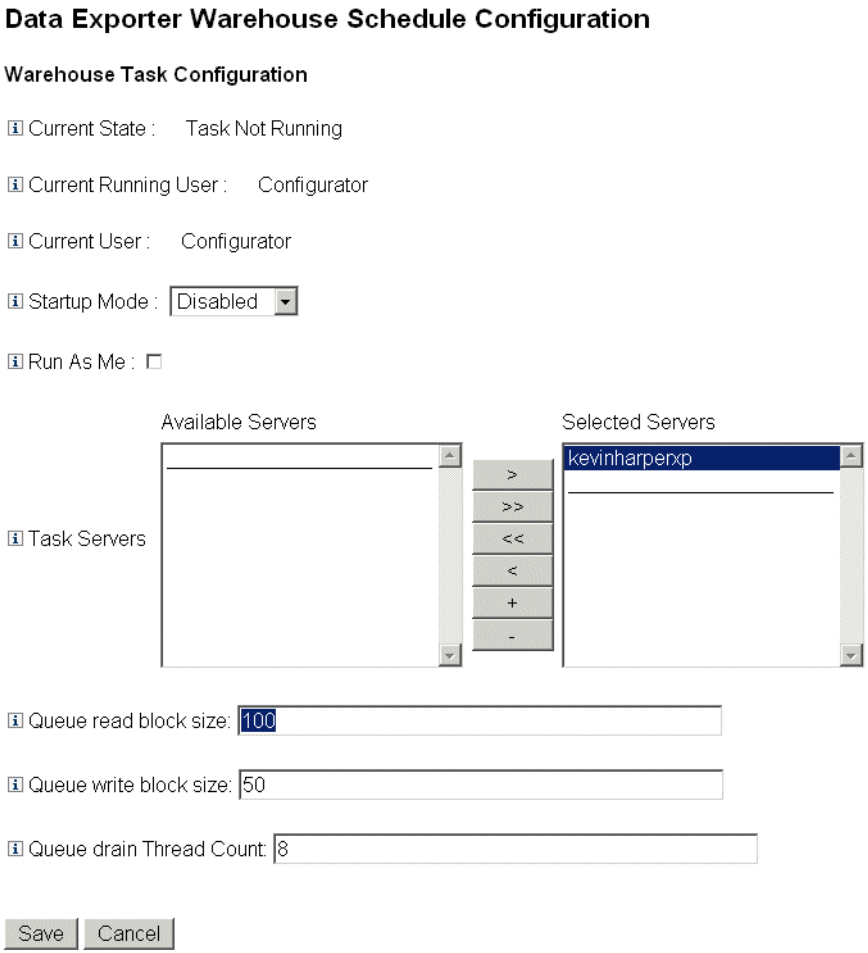


FIGURE 16–4 Configuration du programme de l'entrepôt de données

2 **Sélectionnez une option dans le menu déroulant Mode de démarrage pour déterminer si la tâche d'entrepôt commence immédiatement au démarrage d'Identity Manager. Sélectionner Désactivé signifie que la tâche doit être lancée manuellement.**

3 **Cochez la case à cocher Exécuter comme moi pour que la tâche d'entrepôt s'exécute sous votre compte administratif.**

4 **Sélectionnez les serveurs sur lesquels la tâche peut s'exécuter. Vous pouvez spécifier plusieurs serveurs, mais seule une tâche d'entrepôt peut s'exécuter à un instant t donné. Si le serveur exécutant la tâche est arrêté, l'ordonnanceur redémarre automatiquement la tâche sur un autre serveur de la liste (si disponible).**

5 **Indiquez le nombre d'enregistrements lus de la file d'attente dans un tampon de mémoire avant d'écrire dans le champ Taille des blocs de lecture dans la file d'attente. La valeur par défaut de ce champ convient pour la plupart des exportations. Augmentez cette valeur si le serveur du référentiel d'Identity Manager est lent par rapport au serveur de l'entrepôt.**

6 **Indiquez le nombre d'enregistrements écrits dans l'entrepôt au cours d'une unique transaction dans le champ Taille des blocs d'écriture dans la file d'attente.**

7 **Indiquez le nombre de threads Identity Manager à utiliser pour lire les enregistrements mis en file d'attente dans le champ Nombre de threads utilisés pour la file d'attente. Augmentez ce nombre si la table de file d'attente contient un grand nombre d'enregistrements de types différents. Diminuez ce nombre si la table de file d'attente ne contient que quelques types de données.**

8 **Cliquez sur Enregistrer pour enregistrer vos changements de configuration et revenir à la page Configuration de l'exportateur de données.**

Modification de l'objet Configuration

Lorsque l'exportateur de données est configuré et opérationnel, tous les types de données qui sont configurés pour être mis en file d'attente sont capturés dans la table de file d'attente interne. Par défaut, cette table n'a pas de limite supérieure mais il est possible d'en configurer une en éditant l'objet Configuration `Data Warehouse Configuration` (Configuration de l'entrepôt de données). Cet objet a un objet imbriqué nommé `warehouseConfig`. Ajoutez la ligne suivante à l'objet `warehouseConfig` :

```
<Attribute name='maxQueueSize' value='YourValue'/>
```

La valeur de `maxQueueSize` peut être tout entier positif inférieur à 2^{31}. L'exportateur de données désactive la mise en file d'attente quand cette limite est atteinte. Les données générées ne peuvent alors plus être exportées tant que la file n'est pas vidée.

Dans le cadre d'un fonctionnement normal, Identity Manager peut générer plusieurs milliers d'enregistrements modifiés à l'heure et la table de mise en file d'attente peut croître très rapidement. Étant donné que la table de file d'attente se trouve dans le référentiel d'Identity Manager, cette croissance consommera du tablespace dans le RDBMS, voire risque d'épuiser le tablespace. Définir un plafond pour la file d'attente peut être nécessaire si vous disposez d'un tablespace limité.

Utilisez le Mbean Data Queue JMX pour contrôler la taille de la table de file d'attente. Pour plus d'informations, voir "Contrôle de l'exportateur de données" à la page 525.

Test de l'exportateur de données

Une fois l'exportateur de données dûment configuré, celui-ci se comporte comme un processus d'arrière-plan, en envoyant des données à l'entrepôt aux intervalles configurés. Pour exécuter l'exportateur de données à la demande, utilisez la tâche Lanceur d'exportateur d'entrepôt de données.

▼ Pour démarrer le lanceur d'exportateur d'entrepôt de données

1. **Désactivez la tâche d'entrepôt. Pour plus d'informations, voir "Configuration de la tâche d'entrepôt" à la page 517.**
2. **Cliquez sur Tâches du serveur dans le menu principal. Cliquez ensuite sur l'onglet secondaire Exécuter des tâches. La page Tâches disponibles s'ouvre.**
3. **Cliquez sur le lien Lanceur d'exportateur d'entrepôt de données. La page Lancer une tâche s'ouvre.**
4. **Sélectionnez la case à cocher Options de débogage pour afficher des options supplémentaires.**
5. **Sélectionnez la case à cocher Ignorer les attributs LastMod d'origine pour que l'exportateur de données ignore l'horodatage « last polled » qu'il utilise pour déterminer les enregistrements du référentiel Identity Manager qui ont déjà été exportés. Lorsque cette option est sélectionnée, tous les enregistrements du référentiel Identity Manager des types sélectionnés sont exportés.**
6. **Choisissez les types de données à exporter dans la liste Exporter une fois. Si vous ne choisissez pas de type dans la liste Exporter une fois, la tâche d'exportation s'exécute comme un démon et procède à l'exportation sur la base de la programmation définie au préalable. Si vous sélectionnez un ou plusieurs types de données, Identity Manager les exporte immédiatement puis la tâche d'exportation se termine.**
7. **Définissez les valeurs des autres champs de la page comme requis.**
8. **Cliquez sur Lancer pour commencer la tâche.**

Configuration des requêtes sur attributs

Les requêtes sur attributs permettent à Identity Manager de lire les données qui ont été stockées dans l'entrepôt de données. Elles peuvent identifier des utilisateurs ou des rôles sur la base des valeurs actuelles ou historiques des types de données utilisateur, rôle ou connexes. Une requête sur attributs s'apparente à un rapport Rechercher des utilisateurs ou Rechercher un rôle, à la différence que les critères de correspondance peuvent être évalués sur les données d'historique et que la requête sur attributs permet de rechercher des attributs qui sont de types de données autres que l'utilisateur ou le rôle interrogé.

L'objectif d'une requête sur attribut est d'entreprendre une action sur les résultats en utilisant Identity Manager. La requête sur attributs n'est pas un outil de génération de rapports universel.

Une requête sur attributs peut poser des questions similaires aux suivantes :

- Qui a accédé au système X entre les heures A et B et qui a approuvé l'accès en question ?
- Combien de demandes de provisioning ont-elles été traitées dans les dernières 48 heures et quelle a été la durée des différentes requêtes ?

Les résultats d'une requête sur attributs ne peuvent pas être enregistrés. Pour préparer un rapport général sur les données de l'entrepôt, vous devez utiliser des outils de création de rapports en vente dans le commerce.

Création d'une requête

Une requête sur attributs peut rechercher des objets Utilisateur ou Rôle. La requête peut être extrêmement complexe, en permettant à son auteur de sélectionner une ou plusieurs conditions d'attribut sur des types de données connexes. Les requêtes sur attributs d'utilisateur peuvent rechercher des attributs avec les types de données User (Utilisateur), Account (Compte), ResourceAccount (Compte de ressource), Role (Rôle), Entitlement (Habilitation) et WorkItem (Élément de travail). Les requêtes sur attributs de rôle peuvent rechercher des attributs avec les types de données Role (Rôle), User (Utilisateur) et WorkItem (Élément de travail).

Au sein d'un même type de données, toutes les conditions d'attribut sont logiquement liées par l'opérateur ET, ce qui signifie que toutes les conditions doivent être remplies pour permettre une correspondance. Par défaut, toutes les correspondances sont liées par l'opérateur ET tous types de données confondus, mais si vous sélectionnez la case à cocher Utiliser OR, les correspondances de types de données divers sont reliées par un OU logique.

L'entrepôt peut contenir plusieurs enregistrements pour un même objet Utilisateur ou Rôle, de sorte qu'une unique requête peut retourner plusieurs correspondances pour le même utilisateur ou rôle. Pour faciliter la différenciation des correspondances, chaque type de données peut être limité à une période de façon à ne prendre en compte que les enregistrements entrant dans la période spécifiée. Chaque type de données connexe peut être limité à une période en permettant, ce qui permet d'émettre une requête de la forme suivante :

```
find all Users with Resource Account on ERP1 between May and July 2005
who were attested by Fred Jones between June and August 2005
```

Plage de dates de minuit à minuit. Par exemple, du 3 mai 2007 au 5 mai 2007, soit 48 heures. Les enregistrements du 5 mai 2007 ne seront pas inclus.

Les opérandes (valeurs à comparer à) pour chaque condition d'attribut doivent être indiqués dans la définition de la requête. Le schéma limite certains attributs à un ensemble limité de valeurs potentielles tandis que d'autres n'ont pas de restrictions. Par exemple, la plupart des champs de date doivent être entrés au format `AAAA-MM-JJ HH:mm:ss`.

Remarque – Compte tenu de la quantité des données contenues dans l'entrepôt et de la complexité de la requête, il faut parfois attendre longtemps pour obtenir les résultats. Si vous naviguez en vous éloignant de la page de la requête alors qu'une requête sur attributs est en cours, vous ne pourrez pas voir les résultats de la requête.

▼ Pour créer une requête sur attributs

1 **Dans l'interface administrateur, cliquez sur Conformité dans le menu principal.**

La page Stratégies d'audit (onglet Gérer les stratégies) s'ouvre.

2 **Cliquez sur l'onglet secondaire Requête sur attributs.**

La page Rechercher dans l'entrepôt de données s'ouvre.

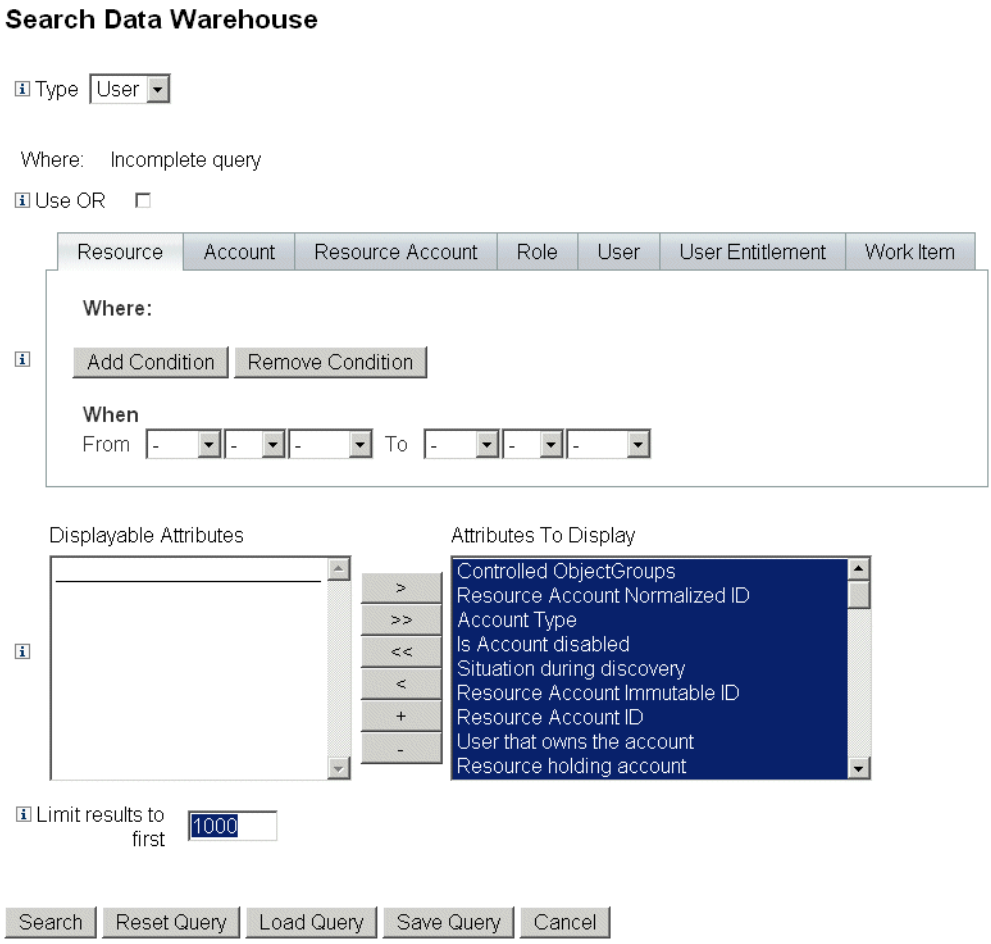


FIGURE 16–5 Rechercher dans l'entrepôt de données

3 Sélectionnez si explorer des enregistrements d'utilisateur ou de rôle dans le menu déroulant Type.

4 Sélectionnez la case à cocher Utiliser OR pour qu'Identity Manager lie par un OU logique les résultats de chaque type de données interrogé. Par défaut, le système effectue un ET logique sur les résultats.

5 Sélectionnez un onglet qui représente un type de données qui figurera dans la requête sur attributs.

a. Cliquez sur Ajouter une condition. Un ensemble de menus déroulants s'affiche.

b. **Sélectionnez un opérande (condition à contrôler) dans le menu déroulant de gauche et le type de comparaison à effectuer dans celui de droite. Entrez ensuite une chaîne ou un entier à rechercher. La liste des opérandes possibles est définie dans le schéma externe. Pour la description des différents opérandes, reportez-vous à l'aide en ligne.**

c. **En option, sélectionnez une plage de dates pour restreindre la portée de la requête.**

   Ajoutez les conditions supplémentaires requises au type de données actuellement sélectionné. Répétez cette étape pour tous les types de données qui feront partie de la définition de la requête sur attributs.

6 **Parmi les attributs disponibles, sélectionnez ceux que vous souhaitez afficher dans les résultats de la requête sur attributs.**

7 **Indiquez ensuite une valeur dans le champ Limiter les résultats aux premiers. Lorsque des conditions de plusieurs types de données sont utilisées, la limite est appliquée à la sous-requête pour chaque type et le résultat final est l'intersection de toutes les sous-requêtes. Ainsi, le résultat final peut exclure certains enregistrements à cause de la limite posée sur les sous-requêtes.**

8 **Cliquez sur Recherche pour exécuter la requête sur attributs immédiatement ou sur Enregistrer la requête pour la réutiliser. Pour toute information sur la réutilisation des requêtes sur attributs, voir "Enregistrement d'une requête sur attributs" à la page 524.**

Enregistrement d'une requête sur attributs

Après la configuration d'une requête (et son exécution éventuelle pour s'assurer qu'elle produit les résultats escomptés), vous pouvez l'enregistrer afin de pouvoir l'exécuter plus tard.

▼ Pour enregistrer une requête sur attributs

1 **Dans la page Rechercher dans l'entrepôt de données, cliquez sur Enregistrer la requête. La page Enregistrer la requête sur attributs s'ouvre.**

2 **Indiquez un nom et une description pour la requête.**

3 **Sélectionnez la case à cocher Enregistrer les valeurs de condition pour enregistrer les valeurs des conditions (chaînes et entiers) que vous avez entrées sur la page Rechercher dans l'entrepôt de donnée. Si vous ne sélectionnez pas cette case à cocher, la requête sur attributs enregistrée fera office de modèle et vous devrez entrer les valeurs à chaque fois que vous l'exécuterez.**

4 **Quiconque peut exécuter une requête enregistrée, mais, par défaut, seul l'auteur d'une requête peut la modifier. Pour permettre à d'autres utilisateurs de modifier votre requête, vous devez cocher la case Autoriser un tiers à modifier cette requête.**

5 **Vu que la requête retourne des objets Utilisateur ou Rôle, vous pouvez choisir les attributs des objets à afficher dans les résultats. Si vous souhaitez afficher des attributs qui ne sont pas inclus dans la liste Attributs à afficher, vous pouvez aller à la page Configuration de l'exportateur de données et ajouter de nouveaux attributs affichables au type Utilisateur ou Rôle.**

Chargement d'une requête

Vous pouvez charger toute requête enregistrée par tout utilisateur, mais ne pouvez modifier que les requêtes que vous avez créées ou que vos collègues ont marquées comme étant modifiables par un tiers.

▼ Pour charger une requête sur attributs

1 **Dans la page Rechercher dans l'entrepôt de données, cliquez sur Charger la requête. La page Charger la requête sur attributs s'ouvre. La colonne Résumé de la requête indique Requête incomplète si la requête a été enregistrée sous la forme d'un modèle.**

2 **Sélectionnez la case à cocher à gauche de la requête et cliquez sur Charger la requête.**

Mise à jour de l'exportateur de données

Cette section explique comment suivre le statut de l'exportateur de données. Les informations sont organisées dans les rubriques suivantes :

- "Contrôle de l'exportateur de données" à la page 525 ;
- "Contrôle de la journalisation" à la page 526.

Contrôle de l'exportateur de données

Une fois l'exportateur configuré et opérationnel, vous pouvez décider de le contrôler pour en assurer le fonctionnement continu. L'exportateur a plusieurs beans JMX qui sont utiles pour en déterminer le comportement. Les beans JMX incluent des statistiques sur les débits de lecture/écriture moyens de l'exportateur, la taille actuelle/maximale de la file d'attente de la mémoire interne et la taille de la file d'attente persistante. L'exportateur produit également des enregistrements d'audit pendant l'exportation, plus précisément un enregistrement pour chaque cycle de chaque type de données. Ces enregistrements d'audit incluent le nombre d'enregistrements du type concerné qui ont été exportés et la durée de l'exportation.

L'exportateur de données fournit les beans de gestion JMX suivants qui contrôlent l'exportateur.

TABLEAU 16–2 Beans de gestion JMX

Nom du bean	Description
DataExporter	Contient le nombre d'exportations actuellement en file d'attente et la limite supérieure de la file d'attente.
DataQueue	Contient le nombre d'exportations en file d'attente actuellement mises en cache et le débit d'arrivée dans le cache.
ExporterTask	Contient le nombre de lecture d'exportation (depuis Identity Manager), écritures (dans l'entrepôt), les débits (enregistrements/seconde) de lecture et d'écriture et le nombre d'erreurs.

L'exportateur de données peut être configuré pour mettre en file d'attente les enregistrements d'exportation dans une table de mise en file d'attente dans le cadre du fonctionnement normal d'Identity Manager. Étant donné que la file d'attente doit potentiellement pouvoir croître jusqu'à un grand nombre d'enregistrements et survivre à un redémarrage du serveur, la file d'attente est sauvegardée dans une table dans le référentiel d'Identity Manager. Or, les écritures dans le référentiel ralentissant en général le fonctionnement normal d'Identity Manager, la file d'attente utilise un petit cache de mémoire pour mettre en tampon les enregistrements jusqu'à ce qu'ils puissent être conservés dans le référentiel.

Les attributs du MBean DataQueue peuvent être représentés graphiquement pour indiquer le plus grand nombre d'enregistrements mis en file d'attente en mémoire (sur un unique serveur Identity Manager). Sur un système équilibré, le nombre d'enregistrements en mémoire cache doit être réduit et tendre rapidement vers zéro. Si vous remarquez que ce chiffre augmente (de l'ordre de plusieurs milliers) ou ne revient pas à zéro au bout de quelques secondes, vous devez enquêter sur la performance d'écriture du référentiel.

Le Mbean ExportTask contient deux nombres d'erreurs, un pour la lecture, l'autre pour l'écriture. Ces nombres devraient être nuls mais il est possible que pour plusieurs raisons des erreurs se produisent, spécialement pendant l'écriture. L'erreur d'écriture la plus courante est celle due au fait que les données exportées ne tiennent pas dans les colonnes de la table de l'entrepôt, ce qui correspondant à un dépassement. Certaines données de chaîne exportées sont sans limite tandis que les colonnes de la table doivent avoir une limite supérieure.

Contrôle de la journalisation

Identity Manager a deux ensembles d'objets qui croissent sans limite : le journal d'audit et le journal système. L'exportateur de données résout certains des problèmes de maintenance associés aux tables de ces journaux.

Journaux d'audit

Identity Manager écrit des enregistrements d'audit inaltérables dans le journal d'audit qui font office de piste d'audit historique des opérations effectuées. Identity Manager utilise ces enregistrements dans certains rapports et les données des enregistrements peuvent être affichées dans l'interface administrateur. Cependant, étant donné que le journal d'audit croît sans limite et qu'il le fait à une vitesse raisonnable, le déployeur doit déterminer quand tronquer ce journal. Avant l'exportateur de données, si vous vouliez préserver les enregistrements antérieurs à la troncature, vous étiez obligé de vider les tables depuis le référentiel. Si l'exportateur de données est activé et configuré pour exporter les enregistrements de journal, les anciens enregistrements sont conservés dans l'entrepôt et Identity Manager peut tronquer les tables d'audit comme requis.

Journaux système

Les journaux systèmes ont la même propriété d'inaltération que les journaux d'audit, mais ne sont en général pas générés aussi fréquemment. L'exportateur de données n'exporte pas les journaux système. Pour tronquer le journal système et préserver les anciens enregistrements, vous devez vider les tables dans le référentiel.

◆ ◆ ◆ CHAPITRE 17

Administration de Service Provider

Ce chapitre contient les informations à connaître pour administrer la fonctionnalité Service Provider dans Sun Identity Manager. Pour utiliser ces informations, la maîtrise des annuaires LDAP (Lightweight Directory Access Protocol) et de la gestion fédérée sera utile. Pour un examen plus vaste de l'implémentation de Sun Identity Manager Service Provider (Service Provider), voir le guide *Sun Identity Manager Service Provider 8.1 Deployment*.

Ce chapitre se compose des rubriques suivantes :

Présentation des fonctionnalités de Service Provider

Dans un environnement fournisseur de services, vous devez avoir la possibilité de gérer le provisioning utilisateur pour tous les utilisateurs finaux, utilisateurs de l'extranet et de l'intranet inclus. Les fonctionnalités de Service Provider permettent aux administrateurs d'entreprise de classer les comptes d'identité en deux types distincts : les utilisateurs Identity Manager et les utilisateurs Service Provider. Les utilisateurs Service Provider dans Identity Manager sont des comptes utilisateur qui ont été configurés en tant que type Utilisateur de Service Provider.

Les capacités de provisioning utilisateur et d'audit d'Identity Manager s'étendent aux implémentations de fournisseur de services en assurant les fonctionnalités suivantes.

Pages utilisateur final améliorées

Des pages utilisateur final qui sont personnalisables pour une implémentation de Service Provider sont fournies.

Stratégie d'ID de compte et de mot de passe

Vous pouvez définir des stratégies d'ID de compte et de mot de passe pour les utilisateurs et comptes de ressources de Service Provider, comme avec d'autres utilisateurs Identity Manager.

Le code de contrôle de stratégie est activé pour les utilisateurs Service Provider avec la Stratégie de compte système de Service Provider, qui a été ajoutée à la table Stratégies principale.

Synchronisation d'Identity Manager et Service Provider

La synchronisation des comptes d'Identity Manager et de Service Provider peut être configurée pour s'exécuter sur tout serveur Identity Manager ou limitée à des serveurs sélectionnés.

La synchronisation de Service Provider, à l'instar de celle d'Identity Manager, peut facilement être arrêtée et démarrée depuis les options Actions de ressource de la page Ressources. Voir "Démarrage et arrêt de la synchronisation" à la page 570.

Les formulaires de saisie ne sont pas les mêmes pour la synchronisation des utilisateurs Identity Manager que pour celle des utilisateurs Service Provider. Voir "Interface utilisateur final" à la page 565.

Intégration d'Access Manager

Vous pouvez utiliser Sun Access Manager 7 2005Q4 pour l'authentification sur les pages utilisateur final de Service Provider. Si l'intégration avec Access Manager est configurée, Access Manager assure que seuls des utilisateurs authentifiés peuvent accéder aux pages utilisateur final.

Service Provider requiert le nom de l'utilisateur à des fins d'audit. Mettez à jour le fichier `AMAgent.properties` pour ajouter l'ID de l'utilisateur aux en-têtes HTTP, par exemple :

```
com.sun.identity.agents.config.response.attribute.mapping[uid] = HEADER_speuid
```

Le filtre d'authentification des pages utilisateur final met la valeur d'en-tête HTTP dans la session HTTP où le reste du code s'attend à ce qu'elle figure.

Configuration initiale

Pour configurer les fonctionnalités de Service Provider, utilisez les procédures suivantes pour éditer les objets Configuration d'Identity Manager vers le serveur d'annuaire :

- Édition de la configuration principale ;
- Édition de la configuration de recherche d'utilisateurs.

Remarque –

Avant d'aller plus loin, vérifiez les points suivants :

- Contrôlez si vous avez défini votre ressource LDAP. Une ressource d'exemple nommée Service Provider End-User Directory (Annuaire utilisateur final de Service Provider) est importée par défaut. Vous pouvez configurer plusieurs ressources si les informations des utilisateurs et de configuration sont stockées dans des annuaires différents.
- Le schéma doit inclure les mappages pour un objet XML.

  Si désiré, configurez votre stratégie de compte Service Provider.
- Le contexte Base configuré pour la ressource d'annuaire ne s'applique qu'aux utilisateurs stockés dans l'annuaire.

Édition de la configuration principale

▼ Pour éditer des objets Configuration pour une implémentation de Service Provider

1. **Dans l'interface administrateur, cliquez sur Service Provider dans le menu.**
2. **Cliquez sur Éditer la configuration principale.**

   La page Configuration de Service Provider s'ouvre.
3. **Complétez le formulaire Configuration de Service Provider.**

   Utilisez les instructions fournies dans les sections suivantes :

   - “Configuration de l'annuaire” à la page 532 ;
   - “Formulaires utilisateur et stratégie” à la page 535 ;
   - “Base de données des transactions” à la page 536 ;
   - “Configuration des configurations des événements suivis” à la page 537 ;
   - “Index de compte de synchronisation” à la page 538 ;
   - “Configuration des légendes” à la page 540

Configuration de l'annuaire

Dans la section Configuration du répertoire, indiquez les informations permettant de configurer l'annuaire LDAP et spécifiez les attributs d'Identity Manager pour les utilisateurs de fournisseur de services.

La Figure 17–1 illustre cette zone de la page Configuration de Service Provider, ainsi que la zone Formulaires utilisateur et stratégie qui fait l'objet de la section suivante.

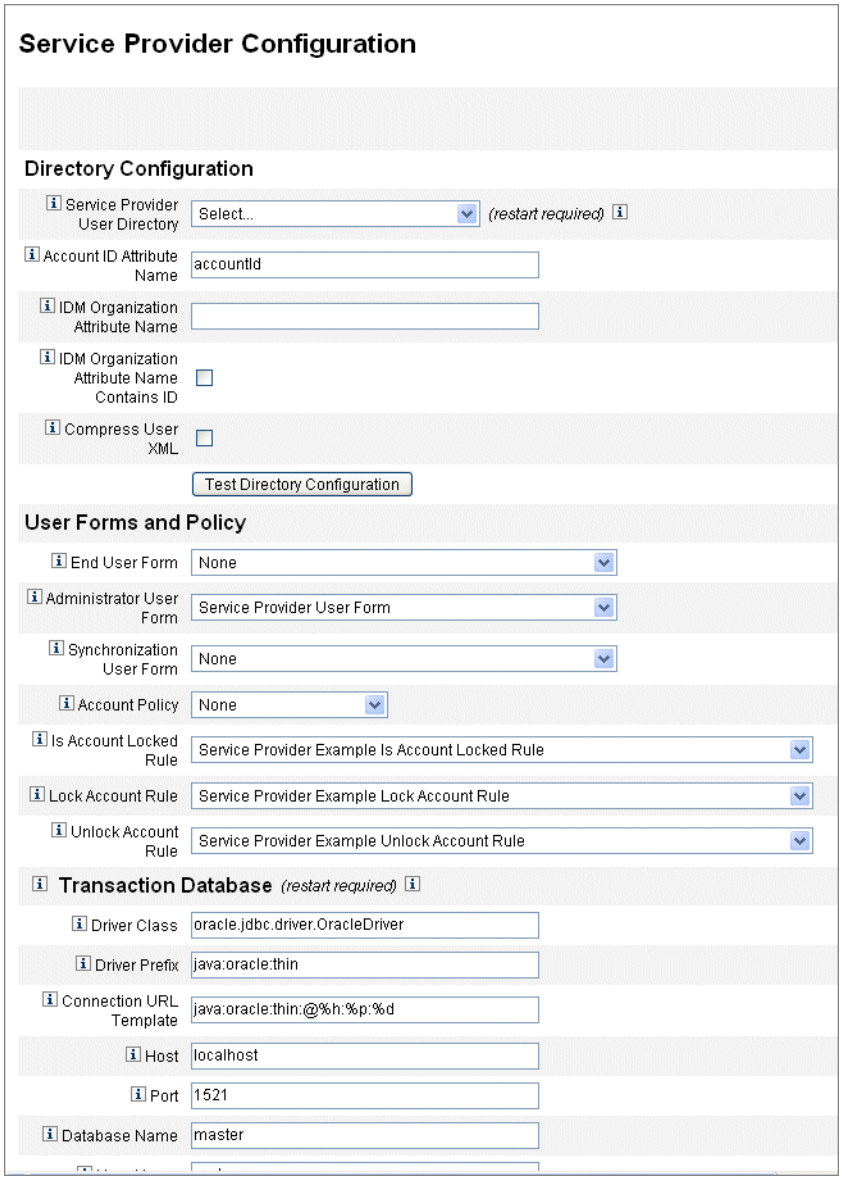


FIGURE 17–1 Configuration de Service Provider (Annuaire, Formulaires utilisateur et stratégie)

▼ Pour compléter le formulaire Configuration du répertoire

1 Sélectionnez le Service Provider End-User Directory dans la liste.

Sélectionnez la ressource d'annuaire LDAP où toutes les données utilisateur de Service Provider sont stockées.

2 Saisissez le Nom de l'attribut d'ID de compte.

Il s'agit du nom de l'attribut de compte LDAP qui contient un identificateur court unique pour le compte. Ce nom est considéré comme le nom de l'utilisateur pour l'authentification et l'accès au compte par l'intermédiaire de l'API. Le nom d'attribut doit être défini dans la carte schématique.

3 Indiquez un Nom de l'attribut de l'organisation IDM.

Cette option spécifie le nom de l'attribut de compte LDAP qui contient le nom ou l'ID d'une organisation d'Identity Manager à laquelle le compte LDAP appartient. Elle est utilisée pour l'administration déléguée des comptes LDAP. Le nom de l'attribut doit être défini dans la carte schématique de la ressource LDAP et correspond au nom de l'attribut système d'Identity Manager (le nom figurant dans la partie gauche de la carte schématique).

Remarque – Spécifiez le Nom de l'attribut de l'organisation Identity Manager (et Le nom de l'attribut de l'organisation IDM contient l'ID, si nécessaire) si vous voulez activer l'administration déléguée par le biais de l'autorisation de l'organisation.

---

4 Si vous choisissez de sélectionner Le nom de l'attribut de l'organisation IDM contient l'ID, activez cette option.

Sélectionnez cette option si l'attribut de ressource LDAP qui fait référence à l'organisation d'Identity Manager à laquelle le compte LDAP appartient contient l'ID de l'organisation Identity Manager et non pas son nom.

5 Si vous choisissez de sélectionner Compresser l'XML de l'utilisateur, activez cette option.

Sélectionnez cette option, si vous choisissez de compresser l'XML de l'utilisateur stocké dans l'annuaire.

6 Cliquez sur Tester la configuration de l'annuaire pour vérifier les entrées effectuées pour la configuration.

Remarque – Vous pouvez tester les configurations d'annuaire, de transaction et d'audit en fonction de vos besoins. Pour les tester complètement toutes les trois, cliquez sur tous les boutons de test de configuration.

Formulaires utilisateur et stratégie

Dans la zone Formulaires utilisateur et stratégie, illustrée à la Figure 17–1 ci-dessus, indiquez les formulaires et les stratégies à utiliser pour la gestion des utilisateurs de fournisseur de services.

▼ Pour spécifier des formulaires et des stratégies pour la gestion des utilisateurs de Service Provider

1. **Sélectionnez le Formulaire utilisateur final dans la liste.**

   Ce formulaire est utilisé partout sauf sur les pages Administrateur délégué et au cours de la synchronisation. Si la valeur Aucun est sélectionnée, aucun formulaire utilisateur par défaut n'est utilisé.

2. **Sélectionnez le Formulaire administrateur dans la liste.**

   Il s'agit du formulaire utilisateur par défaut qui est utilisé dans les contextes Administrateur. Cela inclut les pages d'édition des comptes Service Provider. Si la valeur Aucun est sélectionnée, aucun formulaire utilisateur par défaut n'est utilisé.

   Remarque – Si vous ne choisissez pas de Formulaire administrateur, les administrateurs seront dans l'impossibilité de créer ou d'éditer des utilisateurs de Service Provider depuis Identity Manager.

   ---

3. **Sélectionnez un Formulaire utilisateur de synchronisation dans la liste.**

   Le Formulaire utilisateur de synchronisation est le formulaire par défaut utilisé si aucun formulaire n'est spécifié pour une ressource exécutant la synchronisation de Service Provider. Si un formulaire d'entrée est spécifié dans la stratégie de synchronisation d'une ressource, c'est ce dernier qui sera utilisé. Les ressources nécessitent généralement des formulaires d'entrée de synchronisation différents. Dans ce cas, vous devez définir le formulaire utilisateur de synchronisation sur chaque ressource au lieu d'en sélectionner un dans la liste.

4. **Sélectionnez une Stratégie de compte dans la liste.**

   Les choix incluent toute stratégie de compte d'identité définie par le biais de Configurer > Stratégies.

5. **Sélectionnez une Règle Le compte est-il verrouillé dans la liste.**

   Sélectionnez une règle à exécuter sur la vue Utilisateur de Service Provider à même de déterminer si un compte est verrouillé.

6. **Sélectionnez une Règle Verrouiller le compte.**

   Sélectionnez une règle à exécuter sur la vue Utilisateur de Service Provider à même de définir les attributs, dans la vue, qui sont à l'origine du verrouillage du compte.

7 **Sélectionnez une Règle Déverrouiller le compte.**

Sélectionnez une règle à exécuter sur la vue Utilisateur de Service Provider à même de définir les attributs, dans la vue, qui sont à l'origine du déverrouillage du compte.

Base de données des transactions

Utilisez cette section de la page Configuration de Service Provider, illustrée à la Figure 17–2, pour configurer une base de données de transactions. Ces options ne sont requises que lorsque vous utilisez le magasin de transactions persistant de JDBC. Vous devez redémarrer le serveur pour que les changements apportés aux valeurs soient appliqués.

La table de la base de données destinée aux transactions doit être configurée conformément au schéma figurant dans les scripts de LDD `create_spe_tables` (situés dans le répertoire `sample` de votre installation d'Identity Manager). Il peut s'avérer nécessaire de personnaliser le script approprié en fonction de l'environnement cible.

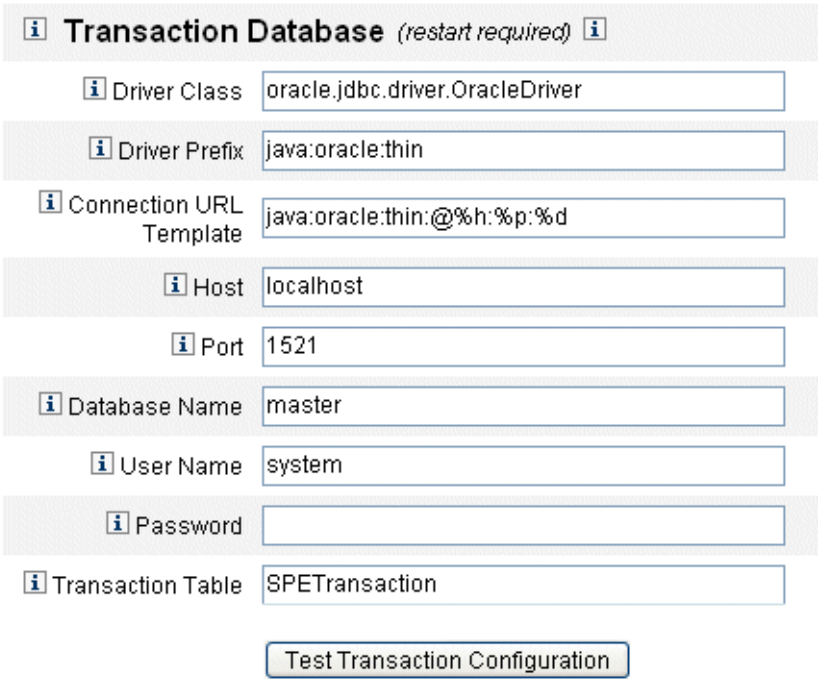


FIGURE 17–2 Configuration de Service Provider (Base de données des transactions)

▼ Pour configurer une base de données des transactions

1 **Entrez les informations de base de données suivantes :**

- **Classe de pilote**. Spécifiez le nom de classe du pilote JDBC.
- **Préfixe du pilote**. Ce champ est optionnel. Si ce champ est renseigné, le gestionnaire de pilote JDBC est interrogé avant l'enregistrement d'un nouveau pilote.
- **Modèle d'URL de connexion**. Ce champ est optionnel. Si ce champ est renseigné, le gestionnaire de pilote JDBC est interrogé avant l'enregistrement d'un nouveau pilote.
- **Hôte**. Entrez le nom de l'hôte sur lequel la base de données est exécutée.
- **Port**. Saisissez le numéro de port sur lequel le serveur de base de données écoute.
- **Nom de la base de données**. Entrez le nom de la base de données à utiliser.
- **Nom de l'utilisateur**. Saisissez l'ID d'un utilisateur de la base de données autorisé à lire, mettre à jour et supprimer des lignes dans les tables de transactions et d'audit de la base de données sélectionnée.
- **Mot de passe**. Saisissez le mot de passe de l'utilisateur de base de données.
- **Tableau des transactions**. Entrez le nom de la table de la base de données sélectionnée à utiliser pour le stockage des transactions en attente.

2 **Le cas échéant, cliquez sur Tester la configuration des transactions pour vérifier vos entrées.**

Passez à la section suivante de la page Configuration de Service Provider pour configurer les événements suivis.

Configuration des configurations des événements suivis

Lorsqu'il est activé, la récupération des événements permet de suivre les statistiques en temps réel pour faciliter la mise à jour des niveaux de services attendus et concordés. La récupération des événements est activé par défaut comme illustré à la Figure 17–3. Désélectionner la case à cocher Activer la récupération des événements désactive la récupération.

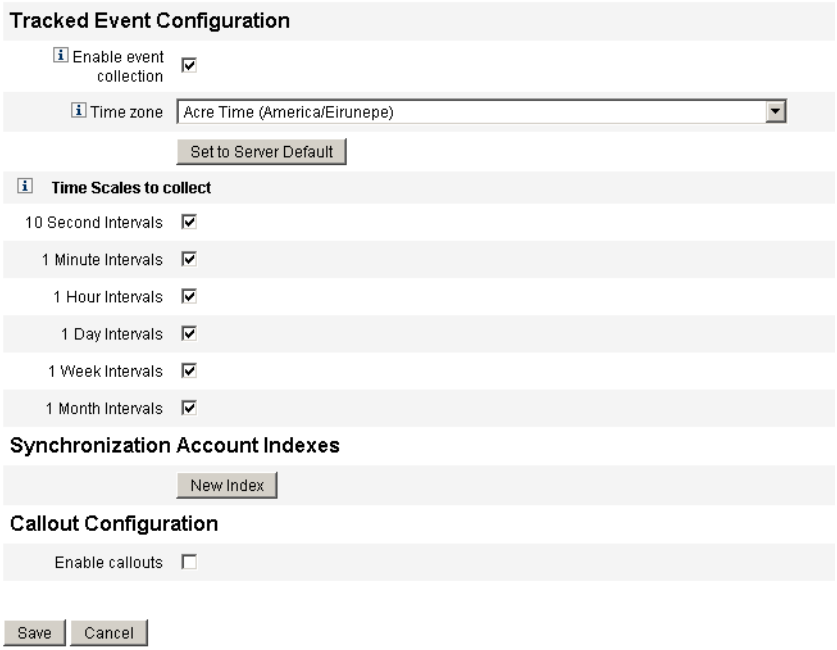


FIGURE 17–3 Configuration de Service Provider Configuration (Configuration des événements suivis, index de compte et légendes)

▼ Pour spécifier un fuseau horaire et des intervalles de récupération pour les événements suivis de Service Provider

1 Sélectionnez le Fuseau horaire dans la liste.

Sélectionnez le fuseau horaire à utiliser lors de l'enregistrement des événements suivis ou sélectionnez Définir sur la valeur par défaut du serveur pour utiliser le fuseau horaire défini sur le serveur.

2 Sélectionnez les options Périodes de récupération.

Les opérations de récupération sont regroupées en fonction des intervalles de temps suivants : toutes les 10 secondes, toutes les minutes, toutes les heures, tous les jours, toutes les semaines et tous les mois. Désactivez les intervalles auxquelles vous ne voulez pas que la récupération ait lieu.

Index de compte de synchronisation

Lorsque vous synchronisez des ressources dans une implémentation Service Provider, il peut être nécessaire de définir des index de compte pour corréler correctement les événements envoyés par la ressource aux utilisateurs dans l'annuaire de Service Provider.

Par défaut, les événements de ressource doivent contenir pour l'attribut accountId une valeur qui correspond à l'attribut accountId contenu dans l'annuaire. Dans certaines ressources, l'ID de compte n'est pas envoyé de manière cohérente. Par exemple, les événements de suppression d'ActiveDirectory ne contiennent que le GUID de compte généré par ActiveDirectory.

Les ressources qui n'incluent pas l'attribut accountId doivent inclure une valeur pour l'un ou l'autre des attributs suivants.

- **guid**. Cet attribut contient normalement un identificateur unique généré par le système.
- **identity**. Cet attribut est normalement le même qu'accountId pour toutes les ressources à l'exception des ressources LDAP où identity contient le DN complet de l'objet.

Si vous devez effectuer une corrélation en utilisant guid ou identity, vous devez définir un index de compte pour ces attributs. Un index est simplement la sélection de un ou plusieurs attributs d'utilisateur d'annuaire pouvant être utilisés pour stocker des identités spécifiques des ressources. Une fois les identités stockées dans l'annuaire, elles peuvent être utilisées dans les filtres de recherche pour corréler les événements de synchronisation.

Pour définir des index de compte, commencez par déterminer les ressources qui seront utilisées pour la synchronisation et celles de celles-ci qui requièrent un index. Éditez ensuite la définition Resource pour l'annuaire Service Provider et ajoutez les attributs dans la carte schématique pour les attributs GUID ou identity pour chacune des ressources Active Sync. Par exemple, si vous effectuez une synchronisation depuis ActiveDirectory, vous pouvez définir un attribut nommé AD-GUID mappé vers un attribut d'annuaire inutilisé tel que manager.

▼ Pour définir des attributs d'index pour une ressource

Après avoir défini tous les attributs d'index dans la ressource Service Provider. effectuez les étapes suivantes :

1. **Dans la zone Index de compte de synchronisation de la page de configuration, cliquez sur le bouton Nouvel index.**

   Le formulaire s'étend pour contenir un champ de sélection de ressource, suivi de deux champs de sélection d'attributs. Les champs de sélection d'attributs restent vides jusqu'à ce qu'une ressource soit sélectionnée.

2. **Sélectionnez une ressource dans la liste.**

   Les champs de sélection d'attributs contiennent maintenant les valeurs définies dans la carte schématique pour la ressource sélectionnée.

3. **Sélectionnez l'attribut d'index approprié pour l'Attribut GUID ou l'Attribut d'identité complet.**

   Il est en général inutile de les définir tous les deux. Si ces deux attributs sont définis, le logiciel tente d'abord une corrélation en utilisant GUID puis utilise l'identité complète.

4 **Vous pouvez cliquer de nouveau sur Nouvel index pour définir les attributs d'index pour d'autres ressources.**

5 **Pour supprimer un index, cliquez sur le bouton Supprimer à droite du champ de sélection Ressource.**

Supprimer un index supprime uniquement cet index de la configuration, cela ne modifie pas tous les utilisateurs d'annuaire existants pouvant avoir des valeurs stockées dans les attributs d'index.

Remarque – Supprimer un index supprime uniquement cet index de la configuration, cela ne modifie pas tous les utilisateurs d'annuaire existants pouvant avoir des valeurs stockées dans les attributs d'index.

Configuration des légendes

Sélectionnez cette option dans la section Configuration des légendes pour activer les légendes. Lorsque les légendes sont activées, les mappages des légendes s'affichent vous permettant de sélectionner des options pré-opération et post-opération pour chaque type de transaction listé.

Par défaut, les options pré- et post-opération sont définies sur Aucun(e).

Si vous spécifiez les légendes post-opération, utilisez l'option Attendre la légende post-opération pour spécifier que la transaction doit attendre que le traitement de la légende post-opération soit complet pour se terminer. Ainsi, toute transaction dépendante ne sera exécutée qu'après la réussite de la légende post-opération.

Remarque – Après avoir complété vos sélections pour toutes les sections sur la page Configuration de Service Provider, cliquez sur Enregistrer pour compléter la configuration.

Édition de la configuration de recherche d'utilisateurs

Utilisez cette page, illustrée à la Figure 17–4, pour configurer les paramètres de recherche par défaut pour les recherches effectuées par les administrateurs délégués sur la page Gérez les utilisateurs de Service Provider. Ces paramètres par défaut s'appliquent à tous les utilisateurs de la page Gérez les utilisateurs de Service Provider, mais peuvent être ignorés session par session.

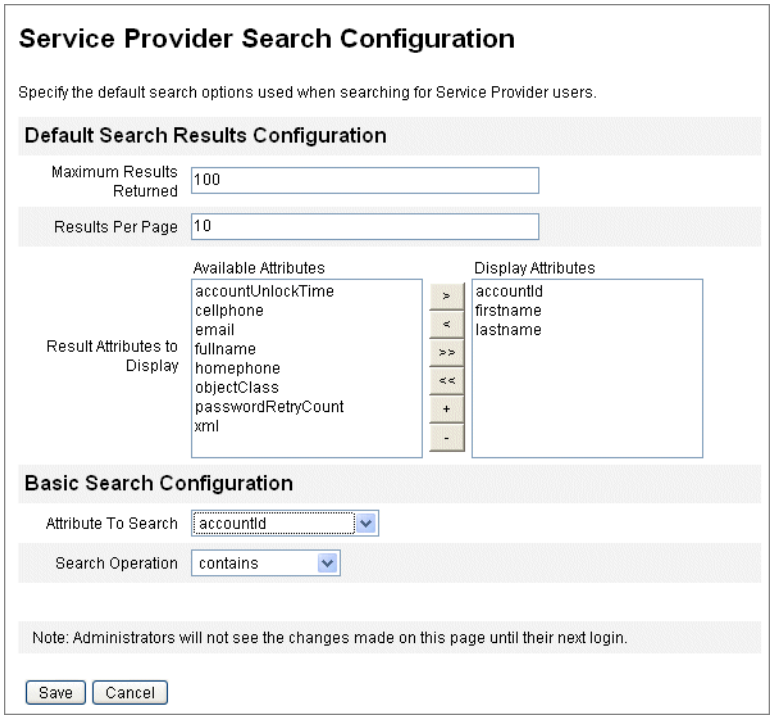


FIGURE 17–4 Configuration de recherche

▼ Pour configurer les paramètres de recherche par défaut pour la recherche d'utilisateurs de Service Provider

1. **Cliquez sur Service Provider dans la barre de menu.**
2. **Cliquez sur Éditer la configuration de recherche d'utilisateurs.**
3. **Saisissez un nombre dans Nombre maximal de résultats retournés (100 par défaut).**
4. **Saisissez un nombre dans Résultats par page (10 par défaut).**
5. **Sélectionnez les Attributs disponibles à côté des Attributs de résultat à afficher en utilisant les flèches de direction.**
6. **Sélectionnez l'Attribut à rechercher dans la liste.**
7. **Choisissez l'Opération de recherche dans la liste.**

8 **Cliquez sur Enregistrer.**

Remarque – Les modifications apportées à la configuration de recherche ne prennent effet qu'après une déconnexion et une reconnexion.

Ces objets Configuration ne sont pas disponibles si le Répertoire de Service Provider n'a pas été configuré.

Gestion des transactions

Une transaction encapsule une unique opération de provisioning, par exemple la création d'un utilisateur ou l'assignation de nouvelles ressources. Pour pouvoir être réalisées lorsque les ressources sont indisponibles, les transactions sont écrites dans le magasin de transactions persistant.

Les rubriques suivantes de cette section contiennent les procédures de gestion des transaction de fournisseur de services.

- "Paramétrage des options d'exécution par défaut des transactions" à la page 542 ;
- "Paramétrage du magasin de transactions persistant" à la page 545 ;
- "Définition des paramètres avancés de traitement des transactions" à la page 546 ;
- "Contrôle des transactions" à la page 549.

Paramétrage des options d'exécution par défaut des transactions

Ces options déterminent la manière dont sont exécutées les transactions, y compris le traitement synchrone/asynchrone, ainsi que le moment auquel elles sont stockées dans le magasin de transactions persistant. Ces options peuvent être remplacées dans l'affichage IDMXUser ou par l'intermédiaire du formulaire utilisé pour le traitement. Pour plus d'informations, voir le guide *Sun Identity Manager Service Provider 8.1 Deployment*.

▼ Pour configurer les transactions de Service Provider

1 **Cliquez sur Service Provider → Éditer la configuration de la transaction.**

La page Configuration de transaction Service Provider s'affiche.

La Figure 17–5 illustre la zone Options d'exécution des transactions par défaut.

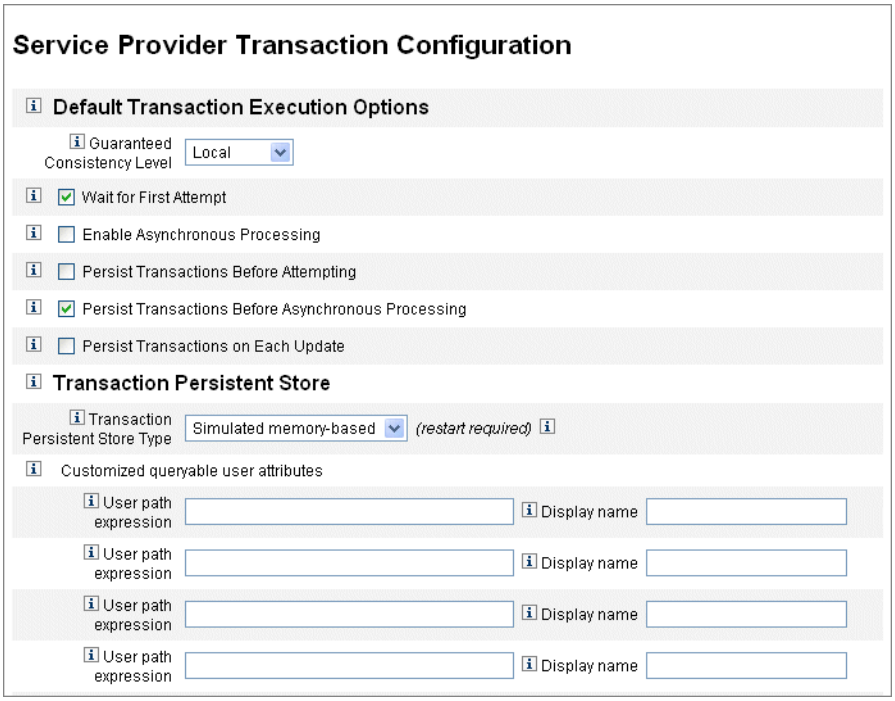


FIGURE 17–5 Configuration des transactions

2 **Sélectionnez les options de Niveau de cohérence garanti pour indiquer le niveau de cohérence des transactions pour les mises à jour d'utilisateurs.**

Ces options sont les suivantes :

- **Aucun**. L'exécution dans l'ordre des mises à jour des ressources d'un utilisateur n'est pas garantie.
- **Locale**. Les mises à jour des ressources d'un utilisateur traitées par un même serveur sont assurées de l'être dans l'ordre.
- **Terminer**. Toutes les mises à jour des ressources d'un utilisateur sont assurées d'être effectuées dans l'ordre sur tous les serveurs. Cette option implique le maintien de l'ensemble des transactions avant toute tentative ou avant un traitement asynchrone.

3 **Activez les Options d'exécution des transactions par défaut en fonction de vos besoins.**

Ces options sont les suivantes :

- **Attendre la première tentative**. Cette option indique la manière dont le contrôle retourne le résultat à l'appelant lorsqu'un objet Vue IDMXUser est archivé. Si elle est activée, l'opération d'archivage est bloquée jusqu'à ce que la transaction de provisioning ait effectué une seule tentative. Si le traitement asynchrone est désactivé, la transaction réussit ou échoue au retour du contrôle. Si le traitement asynchrone est activé, la transaction continue d'être retentée en arrière-plan. Si cette option est désactivée, l'opération d'archivage redonne le contrôle à l'appelant avant de tenter la transaction de provisioning. Envisagez d'activer cette option.
- **Activer le traitement asynchrone**. Cette option contrôle si le traitement des transactions de provisioning continue après les retours d'appel d'archivage.

  L'activation du traitement asynchrone permet au système de retenter des transactions. Elle améliore également le débit en permettant l'exécution asynchrone des threads travailleur configurés dans "Définition des paramètres avancés de traitement des transactions" à la page 546. Si vous sélectionnez cette option, configurez les intervalles de nouvelle tentative et les tentatives pour les ressources en cours de provisioning ou mises à jour par le biais du formulaire d'entrée de synchronisation.

  Entrez un Délai de nouvelle tentative quand vous sélectionnez Activer le traitement asynchrone. Cette limite supérieure exprimée en millisecondes fixe la durée pendant laquelle le serveur retente un transaction de provisioning qui a échoué. Ce paramètre complète les paramètres de relance définis sur les ressources individuelles, annuaire LDAP des utilisateurs de Service Provider compris. Par exemple, si cette limite est atteinte avant les seuils de nouvelle tentative de ressource, la transaction est abandonnée. Si la valeur est négative, le nombre de nouvelles tentatives est limité par les seuls paramètres des ressources individuelles.
- **Rendre les transactions persistantes avant d'essayer**. Si cette option est activée, les transactions de provisioning sont écrites dans le magasin de transactions persistant avant d'être tentées. L'activation de cette option peut mobiliser de manière inutile des ressources système dans la mesure où la plupart des transactions de provisioning réussissent à la première tentative. Envisagez de désactiver cette option à moins que l'option Attendre la première tentative ne soit désactivée. Cette option n'est pas disponible si le niveau de cohérence complet est sélectionné.
- **Rendre les transactions persistantes avant le traitement asynchrone**(*Sélection par défaut*). Si cette option est activée, les transactions de provisioning sont écrites dans le magasin de transactions persistant avant d'être traitées de façon asynchrone. Si l'option Attendre la première tentative est activée, les transactions nécessitant une tentative supplémentaire sont conservées avant que le contrôle ne soit renvoyé à l'appelant. Si l'option Attendre la première tentative est désactivée, les transactions sont toujours maintenues avant d'être tentées. Il est recommandé d'activer cette option. Cette option n'est pas disponible si le niveau de cohérence complet est sélectionné.

- **Rendre les transactions persistantes à chaque mise à jour**. Si cette option est activée, les transactions de provisioning sont maintenues après toute tentative de relance. Cela peut faciliter l'isolement des problèmes car le magasin de transactions persistant, qui est explorable depuis la page Recherche de transaction, est toujours à jour.

Paramétrage du magasin de transactions persistant

Les options de la page Configuration de transaction Service Provider s'appliquent au magasin de transactions persistant. Le type du magasin peut être configuré ainsi que des attributs interrogeables supplémentaires à exposer dans le magasin, comme illustré sur la figure suivante.

FIGURE 17–6 Configuration du magasin de transactions persistant de Service Provider

▼ Pour définir les options de la page Configuration de transaction de Service Provider

1 Sélectionnez le Type du magasin de transactions persistant de votre choix dans la liste.

Si l'option Base de données est sélectionnée, alors les SGBDR configurés dans la page de configuration principale de Service Provider sont utilisés pour maintenir les transactions de provisioning. Cela garantit que les transactions devant être relancées ne seront pas perdues en cas de redémarrage d'un serveur. La sélection de cette option requiert la configuration du RDBMS sur la page principale de configuration de Service Provider. Si l'option Basés sur la mémoire simulée est sélectionnée, les transactions nécessitant une nouvelle tentative sont uniquement stockées en mémoire et sont perdues au redémarrage du serveur. Activez l'option Base de données pour les environnements de production.

Remarque – L'utilisation du magasin de transactions persistant basé sur la mémoire n'est pas adaptée aux environnement clustérisés.

En cas de changement du Type du magasin de transactions persistant, vous devez redémarrer toutes les instances d'Identity Manager en cours d'exécution pour que le changement soit appliqué.

2 **Vous pouvez entrer des Attributs utilisateur interrogeables personnalisés.**

Sélectionnez des attributs supplémentaires de l'objet IDMXUser à exposer dans les récapitulatifs des transactions. Ces attributs sont interrogeables à partir de la page de recherche des transactions et s'affichent dans les résultats de la recherche.

Ces attributs sont les suivants :

- **Expression du chemin utilisateur**. Entrez une expression de chemin dans l'objet IDMXUser .
- **Nom d'affichage**. Choisissez un nom à afficher correspondant à l'expression de chemin. Le nom d'affichage est indiqué sur la page de recherche des transactions.

Définition des paramètres avancés de traitement des transactions

Ces options avancées déterminent le fonctionnement interne du gestionnaire des transactions. Ne modifiez pas les valeurs par défaut fournies à moins que l'analyse de performance n'indique qu'elles ne sont pas idéales. Toutes les entrées sont obligatoires.

La Figure 17–5 illustre la zone Paramètres avancés de traitement des transactions sur la page Éditer la configuration de la transaction.

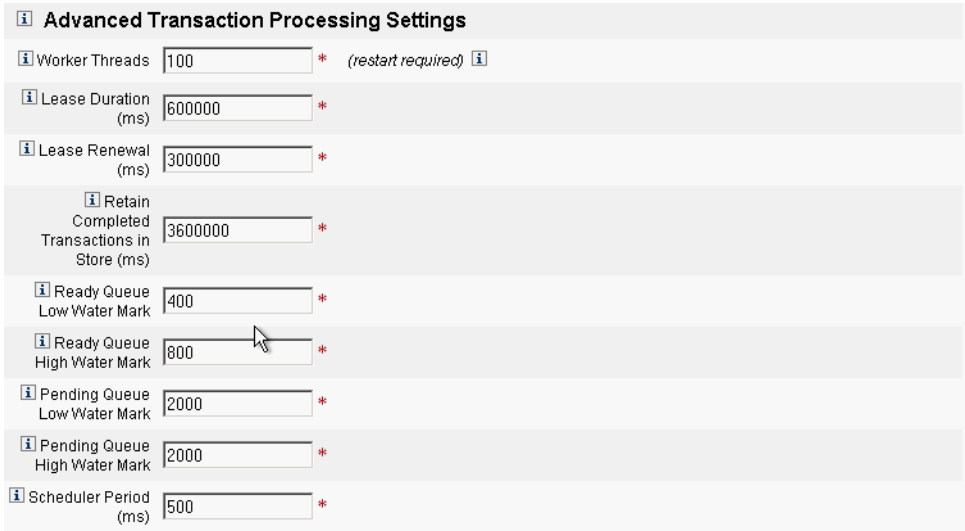


FIGURE 17–7 Paramètres avancés de traitement des transactions

▼ Pour définir les paramètres avancés de traitement des transactions

1 **Saisissez le nombre souhaité de Threads travailleur (100 par défaut).**

Il s'agit du nombre de threads utilisés pour traiter les transactions. Cette valeur limite le nombre de transaction traitées simultanément. Ces threads sont alloués statiquement au démarrage.

Remarque – En cas de changement du paramètre Threads travailleur, vous devez redémarrer toutes les instances d'Identity Manager en cours d'exécution pour que le changement soit appliqué.

---

2 **Saisissez la Durée du bail (ms) de votre choix (600 000 par défaut).**

Ce paramètre détermine le délai pendant lequel un serveur verrouille une transaction relancée. Ce bail est renouvelé selon les besoins. Toutefois, si le serveur ne s'arrête pas correctement, un autre serveur ne pourra pas verrouiller la transaction tant que le bail du serveur initial n'expirera pas. Cette valeur devrait être de une minute minimum. La sélection d'une valeur inférieure à une minute peut affecter la charge sur le magasin de transactions persistant.

3 **Entrez le moment du Renouvellement du bail (ms) (300 000 par défaut).**

Cette option détermine le moment où le bail d'une transaction verrouillée est renouvelé. Le bail est renouvelé lorsque la durée restante du bail atteint cette valeur en millisecondes.

4 **Entrez la durée pendant laquelle Conserver les transactions terminées dans le magasin (ms) (360 000 par défaut).**

Ce paramètre détermine le délai, en millisecondes, après lequel les transactions terminées sont supprimées du magasin de transactions persistant. Si les transactions ne sont pas configurées pour être immédiatement persistantes, le magasin de transactions persistant ne contient pas toutes les transactions terminées.

5 **Entrez le Seuil inférieur de la file d'attente des transactions prêtes (400 par défaut).**

Lorsque la file d'attente de l'ordonnanceur de transactions contenant les transactions prêtes à être exécutées descend en dessous de ce seuil, l'ordonnanceur complète la file d'attente avec des transactions prêtes disponibles à hauteur du seuil supérieur.

6 **Entrez le Seuil supérieur de la file d'attente des transactions prêtes (800 par défaut).**

Lorsque la file d'attente de l'ordonnanceur de transactions contenant les transactions prêtes à être exécutées descend en dessous du seuil inférieur, l'ordonnanceur complète la file d'attente avec des transactions prêtes disponibles à hauteur de ce seuil.

7 **Entrez le Seuil inférieur de la file d'attente des transactions en attente (2000 par défaut).**

La file d'attente de l'ordonnanceur de transactions conserve les transactions qui ont échoué et sont en attente d'une relance. Si la taille de cette file d'attente dépasse le seuil supérieur, toutes les transactions au-delà du seuil inférieur sont transférées dans le magasin de transactions persistant.

8 **Entrez le Seuil supérieur de la file d'attente des transactions en attente (2000 par défaut).**

La file d'attente de l'ordonnanceur de transactions conserve les transactions qui ont échoué et sont en attente d'une relance. Si la taille de cette file d'attente dépasse le seuil supérieur, toutes les transactions au-delà du seuil inférieur sont transférées dans le magasin de transactions persistant.

9 **Entrez la Fréquence d'exécution de l'ordonnanceur (ms) (500 par défaut).**

Cette valeur précise le nombre de fois où l'ordonnanceur sera exécuté. Lorsqu'il s'exécute, l'ordonnanceur des transactions transfère les transactions prêtes à être exécutées de la file d'attente des transactions en attente vers la file d'attente des transactions prêtes, et effectue d'autres tâches périodiques telles que le transfert de transactions persistantes vers le magasin de transactions persistant.

10 **Cliquez sur Enregistrer pour accepter les paramètres.**

Contrôle des transactions

Les transactions de Service Provider sont écrites dans le magasin de transactions persistant. Vous pouvez rechercher des transactions dans le Magasin de transactions persistant pour afficher le statut de ces transactions.

Remarque – En utilisant la page Éditer la configuration de la transaction, l'administrateur peut contrôler si les transactions sont maintenues. Par exemple, elles peuvent être maintenues immédiatement, avant même d'avoir été tentées pour la première fois.

La page Recherche de transaction permet de spécifier des conditions de recherche permettant de filtrer les transactions à afficher en fonction de critères spécifiques liés à l'événement de transaction, tels que l'utilisateur, le type, le statut, l'ID de transaction, l'état actuel et la réussite ou l'échec de la transaction. Cela inclut les transactions qui sont encore tentées, ainsi que celles déjà terminées. Les transactions non terminées peuvent être annulées afin d'empêcher toute tentative ultérieure.

▼ Pour rechercher des transactions

1 **Dans l'interface administrateur, cliquez sur Tâches du serveur → Transactions du Service Provider.**

La page Recherche de transaction Service Provider s'ouvre, vous permettant de spécifier les conditions de recherche.

Remarque – La recherche retourne uniquement les transactions correspondant à *toutes* les conditions sélectionnées plus bas. Cela est similaire à la page Comptes → Rechercher des utilisateurs.

---

2 **Configurez votre recherche.**

Choisissez une ou plusieurs des options suivantes :

- **Nom de l'utilisateur**. Activez cette option pour rechercher des transactions qui s'appliquent uniquement aux utilisateurs possédant l'ID de compte entré.

  Remarque – Si vous avez configuré des Attributs utilisateur interrogeables personnalisés sur la page Configuration de transaction Service Provider, ceux-ci s'affichent ici. Par exemple, vous pouvez choisir d'effectuer une recherche en fonction du Nom ou du Nom complet si ces attributs ont été configurés en tant qu'attributs utilisateur interrogeables personnalisés.

- **Type** Activez cette option pour rechercher des transactions du ou des types sélectionnés.

- **État**. Activez cette option pour rechercher des transactions possédant le ou les états sélectionnés suivants :
  - Les transactions ayant l'état **Non tentée** n'ont pas encore été tentées.
  - Les transactions ayant l'état **Relance en attente** ont été tentées une fois ou plus, ont subi une ou plusieurs erreurs et sont planifiées pour être retentées dans les limites de nouvelles tentatives configurées pour les ressources individuelles.
  - Les transactions ayant l'état **Réussite** ont été effectuées avec succès.
  - Les transactions ayant l'état **Échec** se sont soldées par un ou plusieurs échecs.
- **Tentatives**. Activez cette option pour rechercher des transactions en fonction de leur nombre de tentatives d'exécution. Les transactions ayant échoué sont relancées à hauteur des limites de nouvelles tentatives configurées pour les ressources individuelles.
- **Envoi**. Activez cette option pour rechercher des transactions en fonction du moment où elles ont été soumises pour la première fois (en heures, minutes ou jours).
- **Terminé(e)**. Activez cette option pour rechercher des transactions en fonction du moment où elles se sont terminées (en heures, minutes ou jours).
- **Statut annulé**. Activez cette option pour rechercher des transactions en fonction de si elles ont été ou non annulées.
- **ID de transaction**. Activez cette option pour rechercher des transactions en fonction de leur ID unique. Cette option permet de trouver une transaction en fonction de son ID, qui figure dans tous les enregistrement du journal d'audit.
- **Exécution sur**. Activez cette option pour rechercher des transactions en fonction du serveur Service Provider sur lequel elles s'exécutent. L'identificateur du serveur est basé sur son nom de machine sauf s'il a été remplacé dans le fichier `Waveset.properties`.
- **Limiter les résultats aux premiers**. Seuls les résultats antérieurs à la limite spécifiée sont retournés. En cas de résultats supplémentaires, aucune indication n'est fournie.

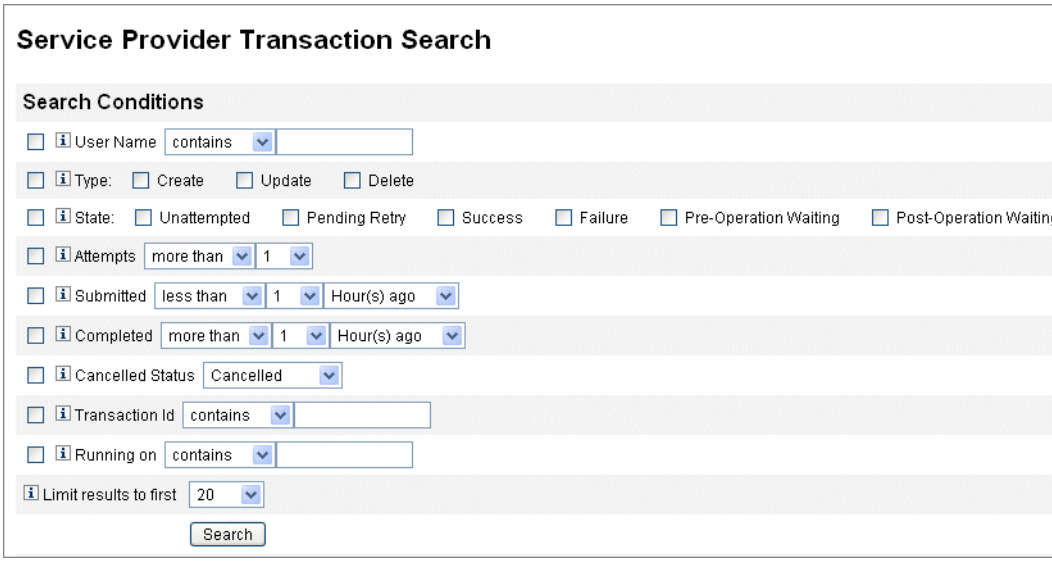


FIGURE 17–8 Rechercher des transactions

3 **Cliquez sur Recherche.**

Les résultats de la recherche s'affichent.

4 **Vous pouvez cliquer sur Téléchargez toutes les transactions correspondantes dans le bas de la page de résultats pour enregistrer les résultats dans un fichier au format XML.**

Remarque – Pour annuler les transactions retournées dans les résultats de recherche, sélectionnez une transaction dans le tableau des résultats et cliquez sur Annuler a été sélectionné. Vous pouvez pas annuler de transactions terminées ou déjà annulées.

Administration déléguée pour les utilisateurs de Service Provider

L'administration déléguée pour les utilisateurs de Service Provider est activée par l'utilisation des *rôles admin* d'Identity Manager ou par le biais du modèle d'autorisation basé sur les organisations.

Délégation par autorisation basée sur les organisations

Identity Manager assure, par défaut, la délégation des obligations administratives par le biais du modèle d'autorisation basé sur les organisations.

Gardez à l'esprit les points suivants lorsque vous créez des administrateurs délégués dans un modèle d'autorisation basé sur les organisations :

- Les administrateurs Service provider sont des utilisateurs Identity Manager ayant des capacités et des organisations contrôlées spécifiques.
- Les valeurs des attributs d'organisation des utilisateurs peuvent être le nom de l'organisation Identity Manager ou l'ID de l'objet. Cela dépend du paramétrage du champ Le nom de l'attribut de l'organisation Identity Manager contient l'ID dans l'écran de configuration principale d'Identity Manager.
- Vous pouvez créer une hiérarchie Identity Manager et y placer les organisations en reflétant la manière dont vous voulez en déléguer l'administration. Utilisez l'identification spécifique des organisations et non pas leur nom simple.
- Les organisations des utilisateurs de Service Provider sont reprises des attributs utilisateur du serveur d'annuaire.
  - Vous devez définir les attributs dans la carte schématique pour la ressource serveur d'annuaire.
  - La comparaison des attributs se fait par *correspondance exacte* par rapport à la liste des organisations contrôlées d'un administrateur. La valeur stockée dans l'annuaire doit correspondre au nom de l'organisation, pas à l'ensemble de la hiérarchie. Si un administrateur contrôle `Haut:orgA:sub1`, la valeur `sub1` doit être stockée dans l'attribut d'organisation pour l'utilisateur de Service Provider.
  - Si l'attribut n'est pas défini ou ne correspond pas à une organisation Identity Manager, l'utilisateur Service Provider est traité comme un membre de l'organisation Haut. Les administrateurs Service Provider doivent avoir les capacités utilisateur Service Provider dans `Haut` pour gérer ces utilisateurs.

  Les paramètres d'attribut déterminent l'étendue des recherches effectuées par les administrateurs Service Provider.
- Pour créer un compte administrateur délégué, vous devez d'abord créer un administrateur Identity Manager puis ajouter les capacités d'administrateur Service Provider. Il y a des capacités spécifiques aux tâches de Service Provider qui peuvent être assignées à l'utilisateur (sur l'onglet Sécurité de la page Éditer l'utilisateur). Les organisations contrôlées spécifient les utilisateurs Service Provider que l'administrateur peut modifier. Toutes les ressources disponibles pour les utilisateurs Service Provider le sont également pour les administrateurs Identity Manager.

Remarque – Pour plus d'informations sur l'administration déléguée d'Identity Manager, voir "Administration déléguée" à la page 202 au Chapitre 6, "Administration"

Délégation par assignation de rôle admin

Pour accorder des capacités et des étendues de contrôle précises aux utilisateurs Service Provider, utilisez un rôle admin d'utilisateurs Service Provider. Les rôles admin peuvent être configurés pour être assignés de manière dynamique à un ou plusieurs utilisateurs Identity Manager ou Service Provider au moment de la connexion.

Des règles peuvent être définies et assignées aux rôles admin qui spécifient les capacités (par exemple `Créer les utilisateurs de Service Provider`) accordées aux utilisateurs auxquels le rôle admin a été assigné.

Pour utiliser la délégation de rôle admin pour les utilisateurs de Service Provider, vous devez l'activer dans l'objet Configuration système d'Identity Manager ("Édition des objets Configuration Identity Manager" à la page 118).

Si la délégation par assignation de rôle admin est activée, le Nom de l'attribut de l'organisation IDM dans Configuration de Service Provider n'est pas requis.

Activation de la délégation de rôles admin de Service Provider

Pour activer la délégation de rôles admin de Service Provider (l'administration déléguée de Service Provider), ouvrez l'objet Configuration système pour le modifier ("Édition des objets Configuration Identity Manager" à la page 118) et définissez la propriété suivante sur `true`:

`security.authz.external.`*app name*`.`*object type*

Où *app name* est l'application Identity Manager (par exemple l'interface administrateur) et *object type* `Service Provider Users`.

Cette propriété peut être activée par application Identity Manager (par exemple, pour l'interface administrateur ou l'interface utilisateur) et par type d'objet. Actuellement, le seul type d'objet pris en charge est `Service Provider Users`. La valeur par défaut est `false`.

Par exemple, pour activer l'administration déléguée de Service Provider pour les administrateurs Identity Manager, définissez l'attribut suivant dans l'objet Configuration System Configuration (Configuration système) sur « true » :

```
security.authz.external.Administrator Interface.Service Provider Users
```

Si l'administration déléguée de Service Provider est désactivée (définie sur false) pour une application Identity Manager ou Service Provider donnée, le modèle d'autorisation basé sur les organisations est utilisé.

Lorsque l'administration déléguée de Service Provider est activée, les événements suivis capturent des informations sur le nombre et la durée des règles d'autorisation exécutées. Ces statistiques sont disponibles dans le tableau de bord.

Configuration d'un rôle admin d'utilisateurs de Service Provider

Pour configurer rôle admin d'utilisateurs de Service Provider, créez un rôle admin et précisez l'étendue de contrôle, les capacités et la personne à qui ce rôle doit être assigné.

Remarque – Avant de créer un rôle admin d'utilisateurs de Service Provider, définissez le contexte et le filtre de recherche, le filtre post-recherche, les capacités et les règles d'assignation d'utilisateurs de ce rôle admin.

Pour utiliser les règles suivantes, vous devez en indiquer l'`authType` :

- SPEUsersSearchContextRule,
- SPEUsersSearchFilterRule,
- SPEUsersAfterSearchFilterRule,
- CapabilitiesOnSPEUserRule,
- UserIsAssignedAdminRoleRule,
- SPEUserIsAssignedAdminRoleRule.

Identity Manager fournit des exemples de règles que vous pouvez utiliser pour créer ces règles pour les rôles admin d'utilisateurs de Service Provider. Ces règles sont disponibles dans `sample/adminRoleRules.xml` dans le répertoire d'installation d'Identity Manager.

Pour plus d'informations sur la création de ces règles pour votre environnement, voir le guide *Sun Identity Manager Service Provider 8.1 Deployment*.

▼ Pour configurer un rôle admin d'utilisateurs de Service Provider

1. **Dans l'interface administrateur, cliquez sur Sécurité dans le menu puis sur Rôles admin.**

   La page Rôles admin s'ouvre.

2. **Cliquez sur Nouveau.**

   La page Créer un rôle Admin s'ouvre.

3. **Indiquez un nom pour le rôle admin et sélectionnez Utilisateurs de Service Provider pour le type.**

4. **Indiquez les options Portée du contrôle, Capacités et Assigner aux utilisateurs, comme décrit dans les sections suivantes.**

Spécification de l'étendue du contrôle

La portée ou étendue de contrôle d'un rôle admin d'utilisateurs Service Provider précise les utilisateurs Service Provider qu'un administrateur Identity Manager, un utilisateur final Identity Manager ou un utilisateur final Service Provider Identity Manager donné, est autorisé à voir. L'étendue est imposée lorsqu'une demande visant à lister les utilisateurs de Service Provider Users dans l'annuaire est effectuée.

Vous pouvez spécifier un ou plusieurs des paramètres suivants pour l'étendue de contrôle du rôle admin d'utilisateurs Service Provider :

- **Contexte de la recherche utilisateur**. Indiquez si une règle ou une chaîne de texte doit être utilisée pour commencer une recherche.

  Si Aucun(e) est indiqué, le contexte de recherche par défaut sera le contexte de base spécifié dans la ressource Identity Manager configurée en tant qu'annuaire des utilisateurs de Service Provider .
- **Filtre de recherche des utilisateurs**. Indiquez si une règle ou une chaîne de texte doit être appliquée pour le filtre de recherche.

  La chaîne de texte spécifiée ou retournée par la règle sélectionnée doit être une chaîne de filtre de recherche conforme LDAP qui représente l'ensemble des utilisateurs, au sein du contexte de recherche, qui sera contrôlé par les utilisateurs assignés à ce rôle Admin. Le filtre indiqué sera combiné au filtre de recherche spécifié par l'utilisateur afin de garantir que les utilisateurs retournés par la recherche n'incluent aucun utilisateur que les utilisateurs auxquels ce rôle admin est assigné ne sont pas autorisés à lister.
- **Règle de filtre post-recherche des utilisateurs**. Sélectionnez une règle qui sera appliquée après l'application du filtre de recherche d'utilisateurs.

  Cette règle sera utilisée après l'exécution de la recherche LDAP initiale sur l'annuaire des utilisateurs de Service Provider et les résultats de son évaluation permettront de déterminer les noms distinctifs (dn) auxquels l'utilisateur demandant est autorisé à accéder.

  Ce type de règle peut être utilisé quand vous devez déterminer si un utilisateur doit figurer dans l'étendue de contrôle de l'utilisateur demandant en utilisant des attributs d'utilisateur non LDAP (par exemple, l'appartenance au groupe) ou quand la décision du filtre doit être faite en utilisant un référentiel autre que l'annuaire des utilisateurs de Service Provider (par exemple, une base de données Oracle ou RACF).

Spécification de capacités

Les capacités du rôle admin d'utilisateurs Service Provider spécifient les capacités et les droits que l'utilisateur demandant a sur l'utilisateur de Service Provider pour lequel l'accès est demandé. Elles sont imposées quand une demande d'affichage, création, modification ou suppression d'un utilisateur de Service Provider, est formulée.

Sur l'onglet Capacités, sélectionnez la Règle de capacités pour ce rôle admin.

Assignation des rôles admin aux utilisateurs

Les rôles admin d'utilisateurs Service Provider peuvent être assignés dynamiquement aux utilisateurs de fournisseur de services en indiquant une règle qui sera évaluée au moment de la connexion pour déterminer si assigner le rôle admin en question à l'utilisateur qui s'authentifie.

Cliquez sur l'onglet Assigner aux utilisateurs et sélectionnez la règle à appliquer pour l'assignation.

Remarque – L'assignation dynamique de rôles admin aux utilisateurs doit être activée pour chaque interface de connexion (par exemple, pour l'interface utilisateur et l'interface administrateur) en définissant l'objet Configuration système suivant ("Édition des objets Configuration Identity Manager" à la page 118) sur `true`:

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.` *logininterface*

La valeur par défaut pour toutes les interfaces est `false`.

Délégation des rôles admin d'utilisateurs Service Provider

Par défaut, les utilisateurs de Service Provider peuvent assigner (ou *déléguer*) les rôles admin d'utilisateurs Service Provider qui leurs sont assignés à d'autres utilisateurs Service Provider de leur étendue de contrôle.

En effet, tout utilisateur Identity Manager ayant des capacités permettant d'éditer les utilisateurs de Service Provider peut assigner les rôles admin d'utilisateurs Service Provider qui lui sont assignés à d'autres utilisateurs de Service Provider de son étendue de contrôle.

Un rôle admin d'utilisateurs Service Provider peut aussi inclure une liste d'*Assignataires* qui peuvent assigner ce rôle admin indifféremment de l'étendue de contrôle. Ces assignations directes permettent d'assurer qu'au moins un compte utilisateur connu peut assigner le rôle admin.

Gestion des utilisateurs de Service Provider

Cette section explique les procédures et informations à suivre pour gérer les utilisateurs de Service Provider par le biais d'Identity Manager.

Cette section se compose des rubriques suivantes :

- "Recherche d'utilisateurs Service Provider" à la page 560 ;
- "Interface utilisateur final" à la page 565.

Organisations d'utilisateurs

Avec Service Provider, la valeur d'un attribut sur l'utilisateur détermine l'organisation à laquelle cet utilisateur est assigné. Cela est spécifié par le champ Nom de l'attribut de l'organisation Identity Manager dans la configuration principale de Service Provider (voir "Configuration initiale" à la page 531). Cependant, les noms de ces organisations doivent correspondre à la valeur d'un attribut utilisateur assigné dans le serveur d'annuaire.

Si le Nom de l'attribut de l'organisation Identity Manager est défini, une liste à plusieurs sélections des organisations disponibles s'affiche sur les pages Créer un utilisateur et Éditer l'utilisateur. Par défaut, les noms courts des organisations sont affichés. Vous pouvez modifier le Formulaire utilisateur de Service Provider pour afficher le chemin complet de l'organisation.

Vous pouvez choisir l'attribut qui deviendra l'attribut de nom de l'organisation. L'attribut de nom de l'organisation est ensuite utilisé dans les pages de gestion des utilisateurs de Service Provider pour limiter les administrateurs qui peuvent rechercher et gérer cet utilisateur.

Remarque – Il existe maintenant des stratégies d'ID de compte et de mot de passe pour les comptes Service Provider et de ressources.

La Stratégie de compte système de Service Provider est disponible dans le principal tableau Stratégies.

Création d'utilisateurs et de comptes

Tous les utilisateurs de fournisseur de services doivent avoir un compte dans l'annuaire de Service Provider. Si un utilisateur a des comptes sur d'autres ressources, alors les liens vers ces comptes sont stockés dans l'entrée d'annuaire de l'utilisateur, de sorte que les informations relatives à ces comptes sont disponibles lorsque l'utilisateur est affiché.

Remarque – Un exemple de formulaire utilisateur de Service Provider est fourni pour créer et éditer des utilisateurs. Personnalisez ce formulaire pour satisfaire les exigences de gestion d'utilisateurs dans votre environnement Service Provider. Pour plus d'informations, voir le Chapitre 2, "Identity Manager Forms" du *Sun Identity Manager Deployment Reference*.

▼ Pour créer un compte Service Provider

1 Dans l'interface administrateur, cliquez sur Comptes dans la barre de menu.

2 Cliquez sur l'onglet Gérez les utilisateurs de Service Provider.

3 Cliquez sur Créer un utilisateur.

Remarque – Dans le cadre de l'utilisation du formulaire utilisateur de Service Provider par défaut, les champs effectifs qui s'affichent dépendent des attributs configurés dans la table Attributs de compte (la carte schématique) de la ressource annuaire de Service Provider. Par ailleurs, lorsque vous assignez des ressources à l'utilisateur (par exemple en tant qu'administrateur délégué), de nouvelles sections s'ajoutent à l'écran : vous pouvez y spécifier les valeurs d'attributs de ces ressources. Vous pouvez aussi personnaliser les champs.

---

4 Indiquez les valeurs d'attributs pour ces ressources comme requis.

Ces valeurs d'attributs sont les suivantes :

- **accountid** (ID de compte, *obligatoire*),
- **password** (mot de passe),
- **confirmation** (confirmation du mot de passe),
- **firstname** (prénom, *obligatoire*),
- **lastname** (nom, *obligatoire*),
- **fullname** (nom complet),
- **email** (e-mail),
- **home phone** (téléphone domicile),
- **cell phone** (téléphone portable),
- **password retry count** (nombre de tentatives de mot de passe),
- **account unlock time** (heure de déverrouillage du compte).

5 Assignez toutes les ressources souhaitées depuis la liste Disponible en utilisant les boutons de direction.

6 Le Statut du compte affiche si le compte est verrouillé ou déverrouillé. Cliquez sur cette option pour verrouiller ou déverrouiller le compte.

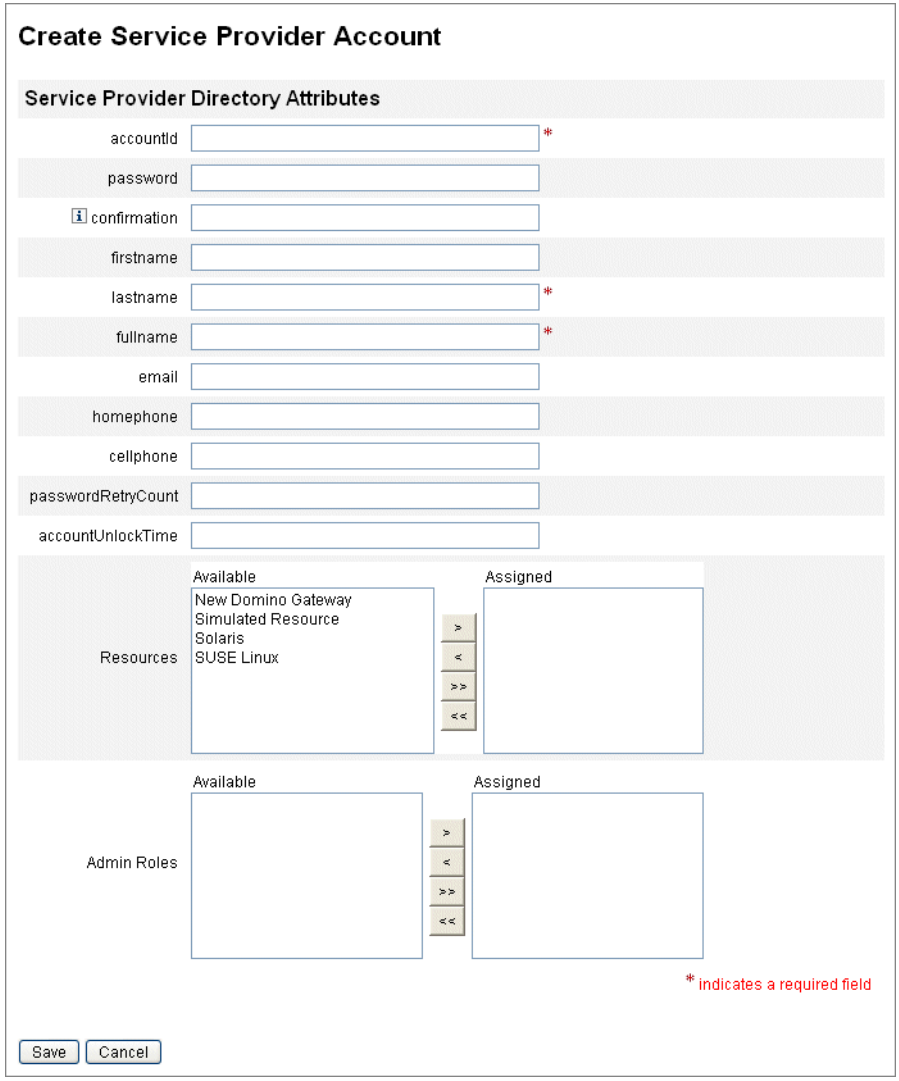


FIGURE 17–9 Création d'utilisateurs et de comptes Service Provider

---

Remarque – Ce formulaire remplit automatiquement les valeurs des attributs de compte de ressource en fonction des attributs définis pour le compte de l'annuaire (au sommet). Par exemple, si la ressource définit `firstName`, le produit indique dans le formulaire la valeur `firstName` du compte de l'annuaire. Cependant, passé ce remplissage initial, les modifications apportées à ces attributs ne sont pas propagées aux comptes de ressources. Le cas échéant, personnalisez l'exemple de Formulaire utilisateur de Service Provider fourni.

---

7 Cliquez sur Enregistrer pour créer le compte utilisateur.

Recherche d'utilisateurs Service Provider

Service Provider inclut une fonctionnalité de recherche configurable visant à faciliter la gestion des comptes utilisateur. Seules les utilisateurs rentrant dans votre étendue (telle que définie par votre organisation et, éventuellement, d'autres facteurs) sont retournés dans le cadre d'une recherche.

Pour effectuer une recherche de base d'utilisateurs de fournisseur de services, cliquez dans la zone Comptes de l'interface d'Identity Manager sur Gérez les utilisateurs de Service Provider puis entrez la valeur à rechercher avant de cliquer sur Recherche.

Les rubriques suivantes examinent les fonctionnalités de recherche de Service Provider :

Recherche avancée

Utilisez les instructions suivantes pour effectuer une recherche avancée d'utilisateurs Service Provider.

▼ Pour effectuer une recherche avancée d'utilisateurs Service Provider

1 Dans la page de recherche d'utilisateurs de Service Provider, cliquez sur Avancé.

2 Choisissez l'attribut souhaité dans la liste.

3 Choisissez l'opération souhaitée dans la liste.

Vous définissez un ensemble de conditions afin de filtrer les utilisateurs obtenus après recherche et précisez que ces derniers doivent répondre à toutes les conditions spécifiées.

4 Entrez la valeur de recherche souhaitée puis cliquez sur Recherche.

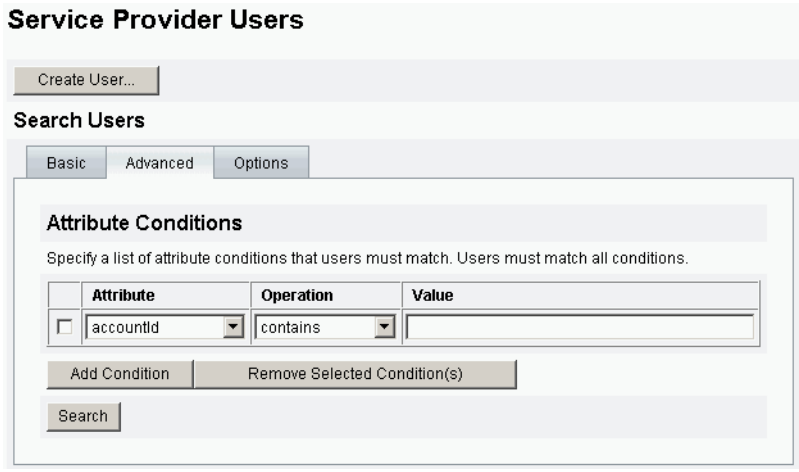


FIGURE 17–10 Recherche d'utilisateurs

Vous pouvez ajouter ou supprimer des Conditions d'attribut, en utilisant les options suivantes :

- Cliquez sur Ajouter une condition et indiquez les nouveaux attributs.
- Sélectionnez l'élément et cliquez sur Supprimer la ou les conditions sélectionnées.

Résultats de la recherche

Les résultats de recherche de Service Provider s'affichent dans un tableau comme illustré à la Figure 17–11. Les résultats peuvent être triés en fonction de n'importe quel attribut en cliquant sur l'en-tête de colonne correspondant à cet attribut. Les résultats affichés dépendent des attributs sélectionnés.

Les flèches naviguent vers la première et la dernière pages ainsi que vers les pages précédente et suivante. Vous pouvez aller directement à une page spécifique en en entrant le numéro dans la zone de texte et en appuyant sur Entrée.

Pour éditer un utilisateur, cliquez sur son nom dans le tableau.

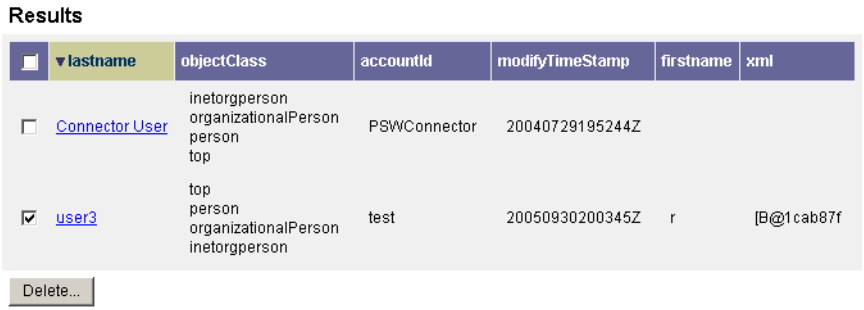


FIGURE 17–11 Exemple de résultats de recherche

Les pages de résultats de recherche vous permettent de supprimer des utilisateurs ou de supprimer les liens de comptes de ressources, en sélectionnant un ou plusieurs utilisateurs et en cliquant sur le bouton Supprimer. Cette action active une page de suppression d'utilisateur et présente des options supplémentaires (voir "Suppression, annulation des assignations et suppression des liens de comptes" à la page 563)

Liaison des comptes

Service Provider peut être installé dans des environnements dans lesquels les utilisateurs ont des comptes sur plusieurs ressources. La fonction de liaison de compte de Service Provider permet d'assigner des comptes de ressources existants à des utilisateurs de Service Provider de manière incrémentielle. Le processus de liaison de compte est contrôlé par la stratégie de liaison de Service Provider, qui définit une règle de corrélation de liens et une option de vérification des liens.

▼ Pour lier les comptes utilisateur

1. **Dans l'interface administrateur, cliquez sur Ressources dans la barre de menu.**
2. **Sélectionnez la ressource de votre choix.**
3. **Sélectionnez Éditer la stratégie de liaison Service Provider dans le menu Actions de ressource.**
4. **Sélectionnez une règle de corrélation de liens. Cette règle recherche sur la ressource les comptes dont l'utilisateur peut être le propriétaire.**
5. **Sélectionnez une règle de confirmation de lien. Cette règle élimine tout compte de ressource de la liste de comptes potentiels que la règle de corrélation de liens sélectionne.**

Remarque – Si la règle de corrélation de liens ne sélectionne pas plus d'un compte, la règle de confirmation de lien n'est pas nécessaire.

6 **Sélectionnez Vérification des liens requise pour lier le compte de ressource à l'utilisateur de Service Provider.**

Suppression, annulation des assignations et suppression des liens de comptes

▼ Pour supprimer des comptes utilisateur, annuler leur assignation ou supprimer leurs liens

1 **Cliquez sur Comptes dans la barre de menu.**

2 **Cliquez sur Gérez les utilisateurs de Service Provider.**

3 **Effectuez une recherche de base ou avancée.**

4 **Sélectionnez le ou les utilisateurs de votre choix.**

5 **Cliquez sur le bouton Supprimer.**

6 **Sélectionnez l'une des options globales facultatives suivantes.**

Ces options sont les suivantes :

- **Supprimer tous les comptes de ressources**

  Remarque – La suppression d'une ressource entraîne celle du compte, mais l'assignation de la ressource est conservée. Le compte sera recréé lors d'une mise à jour ultérieure de l'utilisateur. La suppression implique donc forcément la suppression du lien du compte de ressource.

- **Annuler l'assignation de tous les comptes de ressources**

  Remarque – L'annulation de l'assignation d'une ressource entraîne la suppression de cette assignation et implique la suppression du lien du compte de ressource. Lorsque vous annulez l'assignation d'une ressource, le compte de ressources n'est pas supprimé.

- **Supprimer les liens de tous les comptes de ressources**

Remarque – La suppression du lien entre un utilisateur et un compte de ressources n'entraîne pas la suppression du compte. L'assignation de ressource n'est pas non plus supprimée et une mise à jour ultérieure de l'utilisateur permettra de lier de nouveau le compte ou de créer un nouveau compte sur la ressource.

7 Vous pouvez également sélectionner une action pour un ou plusieurs comptes de ressources dans les colonnes Supprimer, Annuler l'assignation ou Supprimer le lien.

8 Après avoir sélectionné les comptes utilisateur souhaités, cliquez sur OK.

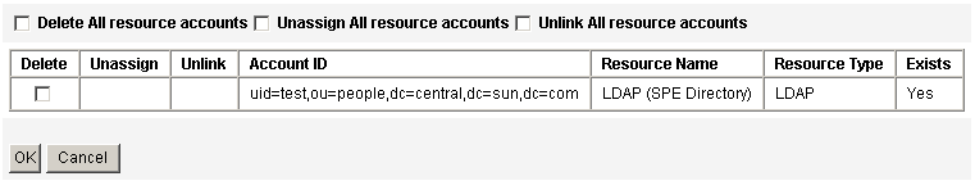


FIGURE 17–12 Suppression, annulation des assignations et suppression des liens de comptes

Définition des options de recherche

▼ Pour définir les options de recherche d'utilisateurs Service Provider :

1 Dans l'interface administrateur, cliquez sur Comptes dans la barre de menu.

2 Cliquez sur Service Provider.

3 Cliquez sur Options.

Remarque – Ces options ne sont valides que pour la session en cours. Les options déterminent le mode d'affichage des résultats, agissent tant sur les résultats de la recherche élémentaire que sur ceux de la recherche avancée. Certains paramètres agissent uniquement sur les nouvelles recherches.

4 Entrez le Nombre maximal de résultats retournés.

5 Entrez le Nombre de résultats par page.

6 À l'aide des touches de direction, choisissez les Attributs d'affichage dans la liste Attributs disponibles.

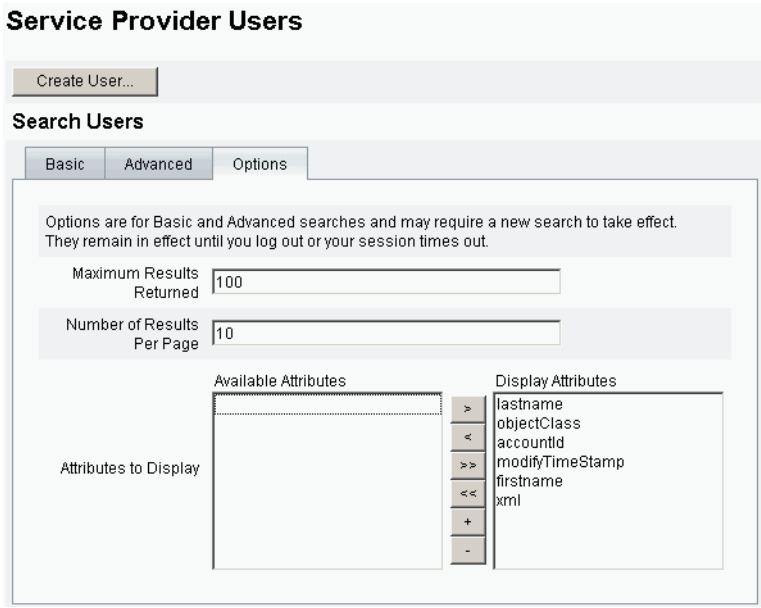


FIGURE 17–13 Définition des options de recherche pour les utilisateurs de Service Provider

Interface utilisateur final

Les exemples de pages utilisateur final intégrées fournissent des exemples d'enregistrement et de libre-service typiques des environnements xSP. Les exemples sont extensibles et peuvent être personnalisés. Vous pouvez changer l'apparence, modifier les règles de navigation entre les pages ou encore afficher des messages spécifiques à l'environnement linguistique de votre déploiement. Pour toute information sur la personnalisation des pages utilisateur final, voir le guide *Sun Identity Manager Service Provider 8.1 Deployment*.

En plus de contrôler les événements de libre-service et d'enregistrement, il est possible d'envoyer une notification à l'utilisateur concerné en utilisant des modèles d'e-mails. Des exemples d'utilisation des stratégies d'ID de compte et de mot de passe, ainsi que de verrouillage des comptes, sont également fournis. Les développeurs d'applications peuvent aussi tirer parti des formulaires d'Identity Manager. Le service d'authentification modulaire implémenté en tant que filtre de servlet peut être étendu ou remplacé si besoin est. Cela permet l'intégration avec des systèmes de gestion d'accès comme Sun Access Manager.

Exemples de pages utilisateur final

Les exemples de pages utilisateur final fournis permettent à l'utilisateur d'enregistrer et de mettre à jour des informations utilisateur de base par le biais d'une série d'écrans de navigation aisée et de recevoir des notifications par e-mail de leurs actions.

Les pages d'exemple comprennent les fonctionnalités suivantes :

- connexion (et déconnexion) incluant l'authentification au moyen de questions/réponses,
- enregistrement et inscription,
- changement de mot de passe,
- changement de nom d'utilisateur,
- changement des questions/réponses,
- changement d'adresse pour les notifications,
- gestion des noms d'utilisateur oubliés,
- gestion des mots de passe oubliés,
- notification par e-mail,
- audit.

Remarque – Identity Manager utilise une table de validation pour l'enregistrement. Seuls les utilisateurs figurant dans cette table sont autorisés à s'enregistrer. Ainsi, lorsque l'utilisateur Sophie Enfant s'enregistre, le système trouve l'entrée correspondant à Sophie Enfant comportant l'adresse e-mail senfant@exemple.com, dans la table de validation et l'enregistrement est accepté.

Ces pages sont simples à personnaliser pour votre déploiement.

Vous pouvez facilement les personnaliser pour votre déploiement en :

- changeant la marque ;
- modifiant les options de configuration (par exemple, le nombre de tentatives de connexion ayant échoué) ;
- ajoutant ou supprimant des pages.

Pour plus d'informations sur la personnalisation de ces pages, voir le guide *Sun Identity Manager Service Provider 8.1 Deployment*.

Enregistrement d'un nouvel utilisateur

Les nouveaux utilisateurs sont invités à s'enregistrer. Lors de l'enregistrement, ils peuvent définir leurs données de connexion, questions/réponses et informations de notification.

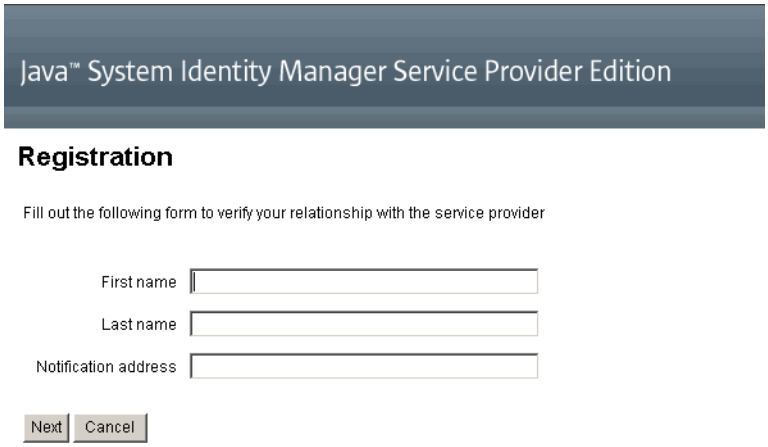


FIGURE 17–14 Page Enregistrement

Écrans Accueil et Mon profil

La Figure 17–15 illustre l'onglet Accueil et la page Mon profil des utilisateurs finaux. Un utilisateur peut changer son ID et son mot de passe de connexion, gérer la notification et créer des questions/réponses.

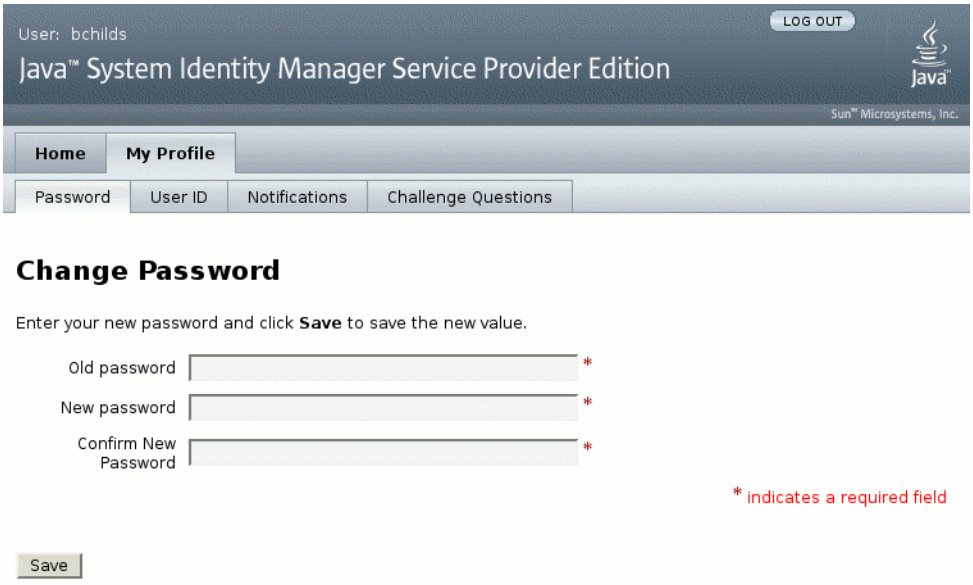


FIGURE 17–15 Page Mon profil

Synchronisation des utilisateurs Service Provider

Pour les utilisateurs de Service Provider, la synchronisation est activée par le biais de la stratégie de synchronisation. Pour synchroniser les changements apportés aux attributs sur les ressources avec Identity Manager pour les utilisateurs de fournisseur de services, vous devez configurer la synchronisation de Service Provider.

Les rubriques suivantes expliquent comment activer la synchronisation dans une implémentation de fournisseur de services :

- “Configuration de la synchronisation” à la page 569 ;
- “Contrôle de la synchronisation” à la page 569 ;
- “Démarrage et arrêt de la synchronisation” à la page 570 ;
- “Migration des utilisateurs” à la page 570.

Remarque – La synchronisation de Service Provider est configurée depuis la liste de ressources de la zone Ressources d'Identity Manager.

Configuration de la synchronisation

Pour configurer la synchronisation de Service Provider, vous devez éditer la stratégie de synchronisation pour les ressources comme décrit dans "Pour éditer ou configurer la synchronisation" à la page 266.

Lorsque vous éditez la stratégie de synchronisation, les options suivantes doivent être spécifiées pour activer les processus de synchronisation pour les utilisateurs de fournisseur de services.

- Sélectionnez Utilisateur Service Provider en tant que Type d'objet cible.
- Dans la section Paramètres de planification, sélectionnez Activer la synchronisation.

Suivez les instructions de la section "Pour éditer ou configurer la synchronisation" à la page 266 pour indiquer d'autres options comme approprié pour votre environnement. L'intervalle de synchronisation par défaut pour les tâches de synchronisation de Service Provider est par défaut de 1 minute.

Remarque – La règle de confirmation et le formulaire doivent utiliser la vue IDMXUser et non pas la vue utilisateur d'entrée d'Identity Manager (pour plus d'informations, voir le guide *Sun Identity Manager Service Provider 8.1 Deployment*).

Cela est nécessaire dans la mesure où les règles de confirmation accèdent à une vue utilisateur pour chaque utilisateur identifié dans la règle de corrélation, ce qui a un impact sur la performance de synchronisation.

Cliquez sur Enregistrer pour enregistrer la définition de stratégie. Si la synchronisation n'est pas désactivée dans la stratégie, elle sera planifiée comme indiqué. Si la désactivation de la synchronisation est spécifiée, le service de synchronisation est arrêté s'il est en cours d'exécution. Si elle est activée, la synchronisation sera démarrée au redémarrage du serveur Identity Manager ou lors de la sélection de Démarrer pour le Service Provider sous l'action de ressource Synchronisation.

Contrôle de la synchronisation

Identity Manager fournit les méthodes suivantes pour contrôler la synchronisation de Service Provider.

- Afficher le statut de la synchronisation dans le champ de description dans la liste Ressource.
- Utiliser l'interface JMX pour contrôler les indicateurs de synchronisation.

Démarrage et arrêt de la synchronisation

La synchronisation de Service Provider est activée par défaut lorsque vous configurez Identity Manager pour une implémentation de fournisseur de services.

▼ Pour désactiver Service Provider Active Sync

1. **Dans l'interface administrateur, cliquez sur Ressources dans le menu.**

   La page Lister les ressources s'ouvre.

2. **Dans la zone Service Provider, sélectionnez la ressource et cliquez sur Éditer la stratégie de synchronisation pour éditer la stratégie.**

3. **Désélectionnez la case à cocher Activer la synchronisation.**

4. **Cliquez sur Enregistrer.**

   La synchronisation s'arrête lorsque la stratégie est enregistrée.

   Pour arrêter la synchronisation sans la désactiver, sélectionnez Arrêter pour Service Provider depuis l'action de ressource Synchronisation.

Remarque – Si vous arrêtez la synchronisation en utilisant l'action de ressource, sans désactiver la synchronisation, celle-ci redémarrera au démarrage du serveur d'Identity Manager.

Migration des utilisateurs

La fonctionnalité Service Provider contient un exemple de tâche de migration d'utilisateurs et des scripts associés. Cette tâche migre les utilisateurs Identity Manager existants ver l'annuaire des utilisateurs de Service Provider. Cette section explique comment utiliser la tâche de migration d'exemple. Nous vous recommandons de modifier cet exemple pour l'utiliser dans votre cas de figure.

▼ Pour migrer des utilisateurs Identity Manager existants

1. **Dans l'interface administrateur, cliquez sur Tâches du serveur dans le menu.**

   La page Rechercher tâches s'ouvre.

2. **Cliquez sur Exécuter des tâches dans le menu secondaire.**

3. **Cliquez sur Migration SPE.**

4. **Entrez un nom unique dans Nom de la tâche.**

5 **Sélectionnez une Ressource dans la liste.**

Il s'agit d'une ressource dans Identity Manager qui représente le serveur d'annuaire Service Provider. Les liens vers cette ressource trouvés dans les utilisateurs Identity Manager ne sont pas migrés.

6 **Entrez un attribut d'identité.**

Ceci est l'attribut d'utilisateur Identity Manager contenant l'identité unique courte de l'utilisateur de l'annuaire.

7 **Sélectionnez une Règle d'identité dans la liste.**

Ceci est une règle facultative pouvant calculer le nom de l'utilisateur de l'annuaire à partir des attributs de l'utilisateur Identity Manager. La règle d'identité peut calculer un nom simple (en général un UID) qui est ensuite traité à travers le modèle d'identité de la ressource pour former le nom distinctif (DN) du serveur d'annuaire. La règle peut aussi retourner un DN entièrement spécifié qui évite le modèle d'ID.

8 **Cliquez sur Lancer pour démarrer la tâche de migration en arrière-plan.**

Configuration des événements d'audit de Service Provider

Dans une implémentation de Service Provider, le système de journalisation d'audit d'Identity Manager contrôle les événements liés aux activités des utilisateurs de l'extranet. Identity Manager fournit le groupe de configuration d'audit de Service Provider (activé par défaut) qui spécifie les événements de contrôle consignés pour les utilisateurs de Service Provider. Voir la Figure 17–16.

Pour plus d'informations sur la journalisation et la modification des événements dans le groupe de configuration d'audit de Service Provider, voir le Chapitre 10, “Journalisation d'audit”

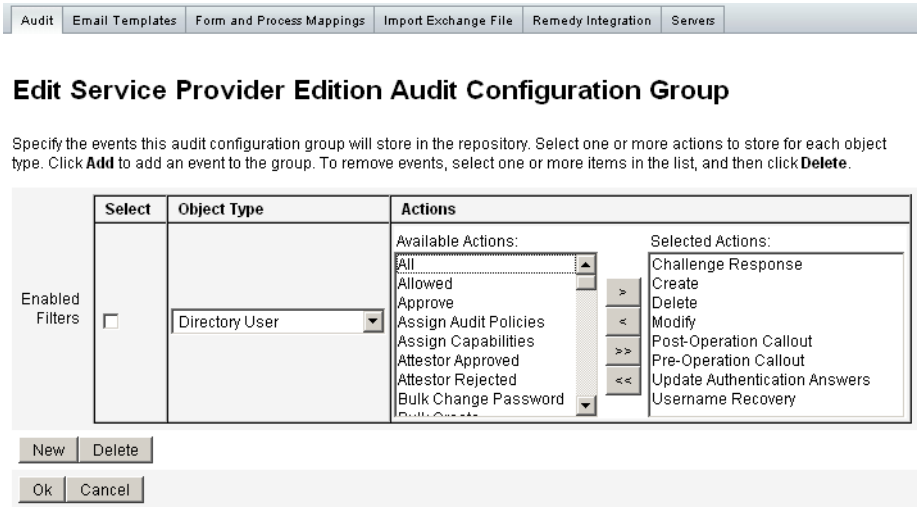


FIGURE 17–16 Page Éditer le groupe de configuration d'audit Service Provider

◆ ◆ ◆ ANNEXE A

Références `lh`

Cette annexe contient des informations qui vous aideront à utiliser l'interface de ligne de commande d'Identity Manager et à exécuter des commandes Identity Manager.

Ces informations sont organisées comme suit :

Syntaxe de la commande `lh`

Utilisez la syntaxe suivante pour appeler l'interface de ligne de commande d'Identity Manager et exécuter des commandes Identity Manager :

```
lh { $class | $command } [ $arg [$arg... ] ]
```

Où :

- `class` doit être un nom de classe complet, par exemple `com.waveset.session.WavesetConsole`.
- `command` doit être l'une des commandes suivantes :
  - `assessment` peut être utilisé pendant les mises à niveau. Supporte les sous-commandes qui effectuent des rapports sur tous les objets modifiés et sur toutes les versions installées d'Identity Manager. Pour de plus amples détails, voir le guide *Sun Identity Manager 8.1 Upgrade*.
  - `config` démarre le Business Process Editor.
  - `console` démarre la console d'Identity Manager.
  - `genReports` génère un ensemble de données aléatoires pouvant être utilisé pour faire une démonstration de la fonctionnalité de génération de rapports d'Identity Manager.

- import importe un objet Identity Manager. Spécifiez l'option -s pour le mode strict. Lorsque le mode strict est activé, le contrôle des références pendant l'importation est moins permissif.
- js appelle un programme JavaScript.
- javascript appelle aussi un programme JavaScript.
- msgtool génère un catalogue de messages personnalisé basé sur WPMessages.properties. Ce catalogue peut être manipulé pour apporter des changements personnalisés au texte ou aux langues.
- script exécute JavaScript ou BeanShell.
- setRepo définit le référentiel d'index d'Identity Manager.
- setup démarre le processus d'installation d'Identity Manager, qui permet de définir la clé de licence et le référentiel d'index d'Identity Manager, et d'importer les fichiers de configuration.
- spml lance le navigateur SPML.
- syslog [options] extrait des enregistrements du journal système. Pour plus de détails, voir "Commande syslog" à la page 576.
- waveset est un alias de la commande console. Voir console ci-dessus.
- xmlparse valide XML pour les objets Identity Manager.
- xpress [options] *nomFichier* évalue une expression. Une option valide est -trace (active la sortie de suivi).

Remarques sur l'utilisation

Lorsque vous travaillez avec les commandes lh, tenez compte des remarques suivantes :

- Pour afficher l'aide relative à l'utilisation d'une commande, saisissez lh sans aucun argument.
- Lorsque vous définissez les variables d'environnement de chemin pour la commande lh :
  - Définissez l'emplacement JAVA_HOME sur le répertoire JRE qui contient un répertoire bin contenant l'exécutable Java. Cet emplacement varie selon l'installation.

    Su vous avez un JRE Sun standard (sans JDK), un emplacement de répertoire typique est C:\Program Files\Java\jre1.5.0_14 (ou similaire). Ce répertoire contient le répertoire bin contenant l'exécutable Java. Dans ce cas, définissez JAVA_HOME sur C:\Program Files\Java\jre1.5.0_14.

    Une installation JDK complète a plusieurs exécutables Java. Dans ce cas, définissez JAVA_HOME sur le répertoire jre imbriqué contenant le fichier bin/java.exe approprié. Pour une installation typique, définissez JAVA_HOME sur C:\java\jdk1.5.0_14\jre.
  - Définissez la variable WSHOME sur le répertoire d'installation d'Identity Manager, comme suit :

```
set WSHOME=<path_to_identity_manager_directory>
```

Par exemple, pour définir la variable sur le répertoire d'installation par défaut, saisissez :

```
set WSHOME=C:\Program Files\tomcat\webapps\idm
```

Remarque – La valeur de la variable `WSHOME` ne doit *pas* contenir les caractères suivants :

- Guillemets anglo-saxons (“ “)

  N'utilisez pas de guillemets anglo-saxons, pas même si le chemin du répertoire de déploiement de l'application contient des espaces.
- Un backslash à la fin du chemin (\)

Sur les systèmes UNIX, vous devez aussi exporter les variables de chemin en saisissant ce qui suit :

```
export WSHOME
export JAVA_HOME
```

- Pour exécuter la commande en mode 64 bits, annulez la mise en commentaire de la ligne `FLAGS="$FLAGS -d64"` dans le script `lh`.
- Pour démarrer l'interface de ligne de commande d'Identity Manager
  - Sous Windows, saisissez ce qui suit à une invite de commande :

    ```
    %WSHOME%\bin\lh
    ```
  - Sous UNIX, Saisissez ce qui suit à une invite de commande :

    ```
    $WSHOME/bin/lh
    ```

Exemples de commandes `lh`

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console– u $user– p` *CheminVersMotPasse*`.txt`
- `lh setup -U` *Administrateur* `-P` *CheminVersMotPasse*`.txt`
- `lh setRepo– c -A` *Administrateur* `-C` *CheminVersMotPasse* `.txt`
- `lh setRepo– t` *FichiersLocaux* `– f $WSHOME`

Commande syslog

Cette section contient les informations suivantes sur la commande syslog :

Utilisation de la commande syslog

Utilisez la syntaxe suivante pour appeler la commande syslog :

```
syslog [options]
```

Options de la commande syslog

Utilisez les options suivantes pour inclure ou exclure des informations.

TABLEAU A–1 Options de la commande syslog

Option	Description
-d *Nombre*	Affiche les enregistrements des *Nombre* jours précédents (par défaut=1).
-E	Affiche uniquement les enregistrements de niveau de gravité erreur ou supérieur.
-F	Affiche uniquement les enregistrements de niveau de gravité fatal.
-i *IDJournal*	Affiche uniquement les enregistrements ayant un ID syslog donné. Les ID de syslog sont affichés sur certains messages d'erreur et référencient une entrée de journal système spécifique.
-W	Affiche uniquement les enregistrements de niveau de gravité avertissement ou supérieur (option par défaut).
-X	Inclut la cause rapportée de l'erreur, si disponible.

◆ ◆ ◆ ANNEXE B

Schéma de la base de données du journal d'audit

Cette annexe contient des informations sur les valeurs du schéma des données d'audit pour les types de bases de données pris en charge et les mappages de la base de données du journal d'audit.

Type de base de données Oracle

Le Tableau B–4 liste les valeurs du schéma de données pour le type de base de données Oracle.

TABLEAU B–1 Valeurs du schéma de données pour le type de base de données Oracle

Colonne de la base de données	Valeur
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)

TABLEAU B–1 Valeurs du schéma de données pour le type de base de données Oracle *(Suite)*

Colonne de la base de données	Valeur
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) ou CLOB (voir la remarque [1] à la fin du tableau)
acctAttrChanges	VARCHAR(4000) ou CLOB
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)

TABLEAU B–1 Valeurs du schéma de données pour le type de base de données Oracle *(Suite)*

Colonne de la base de données	Valeur
sequence	CHAR(19)
xmlSize	NUMBER(19,0)
xml	BLOB

Remarque – La limite de longueur de ces colonnes est configurable. Le type de données par défaut est VARCHAR et la limite de taille par défaut est indiquée entre parenthèses. Pour plus d'informations sur le réglage de la taille limite, voir "Configuration du journal d'audit" à la page 361.

Type de base de données DB2

Le Tableau B–2 liste les valeurs du schéma de données pour le type de base de données DB2.

TABLEAU B–2 Valeurs du schéma de données pour le type de base de donnée DB2

Colonne de la base de données	Valeur
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)

TABLEAU B–2 Valeurs du schéma de données pour le type de base de donnée DB2 *(Suite)*

Colonne de la base de données	Valeur
message	VARCHAR(255) ou CLOB (voir la remarque [1] à la fin du tableau)
acctAttrChanges	CLOB(16M)
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
sequence	CHAR(19)
xmlSize	DECIMAL(19,0)
xml	CLOB(16M)

Remarque – La limite de longueur de ces colonnes est configurable. Le type de données par défaut est VARCHAR et la limite de taille par défaut est indiquée entre parenthèses. Pour plus d'informations sur le réglage de la taille limite, voir "Configuration du journal d'audit" à la page 361.

Type de base de données MySQL

Le Tableau B–3 liste les valeurs du schéma de données pour le type de base de données MySQL.

TABLEAU B–3 Valeurs du schéma de données pour le type de base de données MySQL

Colonne de la base de données	Valeur
id	VARCHAR(50) BINARY NOT NULL
name	VARCHAR(128) BINARY NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(255)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) ou CLOB (voir la remarque [1] à la fin du tableau)
acctAttrChanges	TEXT
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)

TABLEAU B–3 Valeurs du schéma de données pour le type de base de données MySQL *(Suite)*

Colonne de la base de données	Valeur
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
sequence	CHAR(19)
xmlSize	BIGINT
xml	MEDIUMTEXT

Remarque – La limite de longueur de ces colonnes est configurable. Le type de données par défaut est VARCHAR et la limite de taille par défaut est indiquée entre parenthèses. Pour plus d'informations sur le réglage de la taille limite, voir "Configuration du journal d'audit" à la page 361.

Type de base de données SQL Server

Le Tableau B–4 liste les valeurs du schéma de données pour le type de base de données SQL Server.

TABLEAU B–4 Valeurs du schéma de données pour le type de base de données SQL Server

Colonne de la base de données	Valeur
id	NVARCHAR(50) NOT NULL
name	NVARCHAR(128) NOT NULL
repomod	DATETIME NOT NULL CURRENT_TIMESTAMP
resourceName	NVARCHAR(128)
accountName	NVARCHAR(255)
objectType	NCHAR(2)
objectName	NVARCHAR(128)
action	NCHAR(2)
actionDateTime	NCHAR(21)
actionStatus	NCHAR(1)
interface	NVARCHAR(50)
server	NVARCHAR(128)
subject	NVARCHAR(128)
reason	NCHAR(2)
message	NVARCHAR(255) ou CLOB (voir la remarque [1] à la fin du tableau)
acctAttrChanges	NTEXT
acctAttr01label	NVARCHAR(50)
acctAttr01value	NVARCHAR(128)
acctAttr02label	NVARCHAR(50)
acctAttr02value	NVARCHAR(128)
acctAttr03label	NVARCHAR(50)
acctAttr03value	NVARCHAR(128)
acctAttr04label	NVARCHAR(50)

TABLEAU B–4 Valeurs du schéma de données pour le type de base de données SQL Server *(Suite)*

Colonne de la base de données	Valeur
acctAttr04value	NVARCHAR(128)
acctAttr05label	NVARCHAR(50)
acctAttr05value	NVARCHAR(128)
parm01label	NVARCHAR(50)
parm01value	NVARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm02label	NVARCHAR(50)
parm02value	NVARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm03label	NVARCHAR(50)
parm03value	NVARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm04label	NVARCHAR(50)
parm04value	NVARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
parm05label	NVARCHAR(50)
parm05value	NVARCHAR(128) ou CLOB (voir la remarque [1] à la fin du tableau)
sequence	NTEXT
xmlSize	NUMERIC(19,0)
xml	NTEXT

Remarque – La limite de longueur de ces colonnes est configurable. Le type de données par défaut est VARCHAR et la limite de taille par défaut est indiquée entre parenthèses. Pour plus d'informations sur le réglage de la taille limite, voir "Configuration du journal d'audit" à la page 361.

Mappages de la base de données du journal d'audit

Le Tableau B–5 contient les mappages entre les clés stockées de la base de données du journal d'audit et la chaîne affichée vers laquelle elles mappent dans la sortie des rapports d'audit. Identity Manager stocke les éléments qui sont utilisés en tant que constantes sous la forme de clés de base de données courtes pour économiser l'espace du référentiel. L'interface du produit n'affiche pas ces mappages. De fait, vous les voyez uniquement lorsque vous examinez la sortie d'un vidage des résultats de rapport d'audit.

Le Tableau B–6 contient les clés de la base de données des actions auditables, le Tableau B–7 les clés de statut des actions et le Tableau B–8 les codes de raison qui sont stockés dans la base de données sous forme de clés.

TABLEAU B–5 Clés de la base de données de types/Clés d'objet

Nom du type	Texte anglais	DbKey
`AccessReview`	`AccessReview` (Examen des accès)	`AV`
`AccessReviewWorkflow*`	`Access Review Workflow` (Flux de travaux de l'examen des accès)	`AW`
`AccessScan`	`AccessScan` (Scannage des accès)	`AS`
`Account`	`Account` (Compte)	`AN`
`AdminGroup`	`Capability` (Capacité)	`AG`
`Administrator`	`Administrator` (Administrateur)	`AD`
`AdminRole`	`Admin Role` (Rôle admin)	`AR`
`Application`	`Resource Group` (Groupe de ressources)	`AP`
`AttributeDefinition`	`AttributeDefinition` (Définition d'attributs)	`AF`
`AttrParse`	`AttrParse` (AttrParse)	`AT`
`AuditConfig`	`AuditConfig` (Config. contrôle)	`AC`
`AuditPolicy`	`AuditPolicy` (AuditPolicy)	`CP`
`BeanPod`	`Bean Pod` (Bean Pod)	`BP`
`ComplianceViolation`	`ComplianceViolation` (ComplianceViolation)	`CV`
`Configuration`	`Configuration` (Configuration)	`CN`
`DataExporter`	`Data Exporter` (Exportateur de données)	`DE`
`Discovery`	`Discovery` (Détection)	`DS`

TABLEAU B–5 Clés de la base de données de types/Clés d'objet *(Suite)*

Nom du type	Texte anglais	DbKey
`Email*`	`Email` (E-mail)	`EM`
`EmailTemplate`	`EmailTemplate` (Modèle d'e-mail)	`ET`
`EncryptionKey`	`EncryptionKey` (Clé de chiffrement)	`KY`
`Event`	`Event` (Événement)	`EV`
`Extract`	`Extract` (Extraire)	`ER`
`ExtractTask`	`ExtractTask` (Tâche d'extraction)	`EX`
`IDMXUser*`	`Directory User` (Utilisateur du répertoire)	`UX`
`LighthouseAccount*`	`Identity System Account` (Compte Identity System)	`LA`
`LoadConfig`	`LoadConfig` (Config. de chargement)	`LD`
`LoadTask`	`LoadTask` (Tâche de chargement)	`LT`
`Log`	`Log` (Connexion)	`LG`
`LoginApp`	`LoginApp` (LoginApp)	`LP`
`LoginConfig`	`LoginConfig` (Config. de connexion)	`LC`
`LoginModGroup`	`LoginModGroup` (LoginModGroup)	`LF`
`MetaView`	`Meta View` (Vue méta)	`MV`
`ObjectGroup`	`Organization` (Organisation)	`OG`
`Policy`	`Policy` (Stratégie)	`PO`
`ProvisioningTask`	`ProvisioningTask` (Tâche de provisioning)	`PT`
`RemediationWorkflow*`	`Remediation Workflow` (Flux de travaux de résolution)	`RW`
`RemedyConfig`	`RemedyConfig` (Config. Remedy)	`RC`
`Resource`	`Resource` (Ressource)	`RS`
`ResourceAccount*`	`Resource Account` (Compte de ressources)	`RA`
`ResourceAction`	`ResourceAction` (Action de ressource)	`RN`
`ResourceForm`	`ResourceForm` (Formulaire de ressource)	`RF`
`ResourceObject`	`ResourceObject` (Objet ressource)	`RE`

TABLEAU B–5 Clés de la base de données de types/Clés d'objet *(Suite)*

Nom du type	Texte anglais	DbKey
RiskReportTask	RiskReportTask (Tâche de rapport de risque)	RR
Role	Role (Rôle)	RL
Rule	Rule (Règle)	RU
SnapShot	SnapShot (Instantané)	SS
ServerObject	ServerObject (Objet Serveur)	SV
SysLog	SysLog (Syslog)	SL
System	System (Système)	SY
TaskDefinition	TaskDefinition (Définition de tâches)	TD
TaskInstance	TaskInstance (Instance de tâche)	TI
TaskResult	TaskResult (Résultat de la tâche)	TR
TaskResultPage	ResultPage (Page de résultats)	TP
TaskSchedule	TaskSchedule (Planification de la tâche)	TS
TaskTemplate	TaskTemplate (Tâche modèle)	TT
TestNotification*	Test Notification (Notification de test)	TN
User (Utilisateur)	User (Utilisateur)	US
UserEntitlement	UserEntitlement (Habilitation de l'utilisateur)	UE
UserForm	UserForm (Formulaire utilisateur)	UF
WorkflowCase*	Workflow Case (Case flux de travaux)	WC
WorkItem	WorkItem (Élément de travail)	WI
XmlData	XmlData (Données XML)	XD

[1]

TABLEAU B–6 Clés de la base de données des actions

Nom de l'action	Texte anglais	DbKey
Allowed*	Allowed (Autorisé)	AL

[1] * Types étendus

TABLEAU B–6 Clés de la base de données des actions *(Suite)*

Nom de l'action	Texte anglais	DbKey
`Approve`	`Approve` (Approuver)	`AP`
`Assign Audit Policies`	`Assign Audit Policies` (Assignation de stratégies d'audit)	`AA`
`Assign Capabilities`	`Assign Capabilities` (Assigner les capacités)	`AC`
`AttestorApproved*`	`Attestor Approved` (Approuvé par l'attestateur)	`TA`
`AttestorRejected*`	`Attestor Rejected` (Rejeté par l'attestateur)	`AR`
`AttestorRemediate*`	`Remediation Requested` (Résolution demandée)	`AF`
`AttestorRescan*`	`Rescan Requested` (Nouveau scannage requis)	`AN`
`Bulk Change Password`	`Bulk Change Password` (Changement de mot de passe en masse)	`BW`
`Bulk Create`	`Bulk Create` (Création en masse)	`BC`
`Bulk Delete`	`Bulk Delete` (Suppression en masse)	`BD`
`Bulk Deprovision`	`Bulk Deprovision` (Deprovisioning en masse)	`BP`
`Bulk Disable`	`Bulk Disable` (Désactivation en masse)	`BF`
`Bulk Enable`	`Bulk Enable` (Activation en masse)	`BE`
`Bulk Modify`	`Bulk Modify` (Modification en masse)	`BM`
`Bulk Reset Password`	`Bulk Reset Password` (Cliquez sur Réinitialiser mot de passe)	`BR`
`Bulk Unassign`	`Bulk Unassign` (Annuler les affectations en masse)	`BU`
`Bulk Unlink`	`Bulk Unlink` (Supprimer les liens en masse)	`BL`
`Bypass Verify`	`Bypass Verify` (Ignorer la vérification)	`BV`
`CancelReconcile*`	`Cancel Reconcile` (Annuler la réconciliation)	`CR`
`challengeResponse*`	`Challenge Response` (Réponse de repêchage)	`CD`

TABLEAU B–6 Clés de la base de données des actions *(Suite)*

Nom de l'action	Texte anglais	DbKey
`Change Password`	`Change Password` (Modifier le mot de passe)	`CP`
`Connect`	`Connect` (Connecter)	`CN`
`Control Active Sync`	`Control Active Sync` (Contrôler Active Sync)	`CA`
`Create`	`Create` (Créer)	`CT`
`CredentialsExpired*`	`Credentials Expired` (Informations d'identification expirées)	`CE`
`Debug`	`Debug` (Déboguer)	`DB`
`Delegate`	`Delegate` (Déléguer)	`DG`
`Delete`	`Delete` (Supprimer)	`DL`
`Deprovision`	`Deprovision` (Suspendre)	`DP`
`Disable`	`Disable` (Désactiver)	`DS`
`Disconnect`	`Déconnecter` (Déconnecter)	`DC`
`Enable`	`Enable` (Activer)	`EN`
`End Activity`	`End Activity` (Terminer l'activité)	`EA`
`End Process`	`End Process` (Terminer le processus)	`PE`
`End Workflow`	`End Workflow` (Terminer le flux de travaux)	`EW`
`Execute`	`Execute` (Exécuter)	`LN`
`Expired*`	`Expired` (Expiré)	`EX`
`Export`	`Export` (Exporter)	`EP`
`Fixed*`	`Fixed` (Résolu)	`FX`
`Import`	`Import` (Importer)	`IM`
`List`	`List` (Liste)	`LI`
`Lock`	`Lock` (Verrouiller)	`LK`
`Login`	`Login` (Connexion)	`LG`
`Logout*`	`Logout` (Fermer la session)	`LO`
`Mitigated*`	`Mitigated` (Atténué)	`VM`

TABLEAU B–6 Clés de la base de données des actions *(Suite)*

Nom de l'action	Texte anglais	DbKey
Modify	Modify (Modifier)	MO
Modify Active Sync	Modify Active Sync (Modifier Active Sync)	MA
NativeChange*	Native Change (Modification native)	NC
Notify*	Notify (Notifier)	NO
PostOperation*	Post-Operation Callout (Légende post-opération)	PT
PreOperation*	Pre-Operation Callout (Légende pré-opération)	PP
Prioritize*	Prioritize (Hiérarchiser)	PR
Provision	Provision (Provisionner)	PV
Recurring*	Recurring (Récurrent)	RC
Reject	Reject (Rejeter)	RJ
Remediated*	Remediated (Résolu)	VR
Rename	Rename (Renommer)	RE
RequestReconcile*	Request Reconcile (Demander la réconciliation)	RR
ResetPassword	ResetPassword (Réinitialiser le mot de passe)	RP
Run Debugger	Run Debugger (Exécuter le débogueur)	RD
ScanBegin*	Scan Begin (Début du scannage)	SB
ScanEnd*	Scan End (Fin du scannage)	SE
StartActivity*	Start Activity (Démarrer l'activité)	SA
StartProcess*	Start Process (Démarrer le processus)	SP
StartWorkflow*	Start Workflow (Démarrer le flux de travaux)	SW
Terminate*	Terminate (Arrêter)	TR
Unassign	Unassign (Annuler l'assignation)	UA
Unlink	Unlink (Annuler le lien)	UN
Unlock	Unlock (Déverrouiller)	UL

TABLEAU B–6 Clés de la base de données des actions *(Suite)*

Nom de l'action	Texte anglais	DbKey
`updateAuthenticationAnswers*`	`Update Authentication Answers` (Mettre à jour les réponses d'authentification)	`AQ`
`usernameRecovery*`	`Username Recovery` (Récupération du nom d'utilisateur)	`UR`
`View`	`View` (Afficher)	`VW`
`View Only`	`View Only` (Afficher uniquement)	`VO`

[2]

TABLEAU B–7 Clés de la base de données de statut des actions

Résultat	DbKey
`Success` (Réussite)	`S`
`Failure` (Échec)	`F`

TABLEAU B–8 Raisons stockées sous forme de clés

Nom de la raison	Texte anglais	DbKey
`PolicyViolation`	Violation of policy {0}: {1} (Violation de stratégie {0} : {1})	`PV`
`InvalidCredentials`	Invalid Credentials (Identification invalide)	`CR`
`InsufficientPrivileges`	Insufficient Privileges (Privilèges insuffisants)	`IP`
`DatabaseAccessFailed`	Database Access Failed (Échec de l'accès à la base de données)	`DA`
`AccountDisabled`	Account Disabled (Compte désactivé)	`DI`

[2] `*` `Actions étendues`

◆ ◆ ◆ ANNEXE C

Guide de référence rapide de l'interface utilisateur

Le Tableau C–1 est un guide de référence rapide des onglets les plus fréquemment utilisés d'Identity Manager. Ce tableau indique le principal emplacement de l'interface d'Identity Manager d'où vous pouvez commencer chaque tâche, ainsi que, le cas échéant, des points de départs et méthodes de remplacement utilisables pour effectuer la même tâche.

Guide de référence rapide des tâches de l'interface d'Identity Manager

TABLEAU C–1 Tâche de référence

Pour effectuer cette tâche	Allez à	Ou à
Gérer les utilisateurs Identity Manager :		
Créer et éditer des utilisateurs	Onglet Comptes, sélection Lister les comptes	Onglet Comptes, sélection Rechercher des utilisateurs (page Résultats de recherche de compte utilisateur)
Approuver la création des comptes utilisateur	Onglet Éléments de travail, onglet Approbations	
Configurer l'authentification des utilisateurs (stratégies)	Onglet Sécurité, sélection Stratégies	

TABLEAU C–1 Tâche de référence *(Suite)*

Pour effectuer cette tâche	Allez à	Ou à
Changer les mots de passe des utilisateurs	Onglet Mots de passe, sélection Changer le mot de passe de l'utilisateur	Onglet Comptes, sélection Lister les comptes Onglet Comptes, sélection Rechercher des utilisateurs (page Résultats de recherche de compte utilisateur) Interface utilisateur d'Identity Manager
Réinitialiser les mots de passe des utilisateurs	Onglet Mots de passe, sélection Réinitialiser le mot de passe de l'utilisateur	Onglet Comptes, sélection Lister les comptes Onglet Comptes, sélection Rechercher des utilisateurs (page Résultats de recherche de compte utilisateur)
Rechercher des utilisateurs	Onglet Comptes, sélection Rechercher des utilisateurs	Onglet Mots de passe, sélection Changer le mot de passe de l'utilisateur
Activer ou désactiver des utilisateurs	Onglet Comptes, sélection Lister les comptes	Onglet Comptes, sélection Rechercher des utilisateurs (page Résultats de recherche de compte utilisateur)
Déverrouiller des utilisateurs	Onglet Comptes, sélection Lister les comptes	Onglet Comptes, sélection Rechercher des utilisateurs (page Résultats de recherche de compte utilisateur)
Gérer les administrateurs Identity Manager :		
Paramétrer l'administration déléguée (par le biais d'organisations)	Onglet Comptes, sélection Lister les comptes, page Créer un utilisateur	
Assigner des capacités	Onglet Comptes, sélection Lister les comptes, page Créer un utilisateur ou Éditer l'utilisateur, onglet Sécurité	
Assigner des capacités (par le biais de rôles d'administration)	Onglet Comptes, sélection Lister les comptes, page Créer un utilisateur ou Éditer l'utilisateur, onglet Sécurité	
Paramétrer des approbateurs (pour valider la création des comptes)	Onglet Comptes, sélection Lister les comptes, page Créer une organisation Onglet Rôles, page Créer un rôle	

TABLEAU C–1 Tâche de référence *(Suite)*

Pour effectuer cette tâche	Allez à	Ou à
Configurer Identity Manager :		
Créer et gérer des ressources (Assistant Ressource)	Onglet Ressources	
Gérer des groupes de ressources	Onglet Ressources, sélection Lister les groupes de ressources	
Créer et gérer des rôles	Onglet Rôles	
Rechercher des rôles	Onglet Rôles, sélection Rechercher des rôles	
Éditer des capacités	Onglet Sécurité, sélection Capacités	
Créer et éditer des rôles admin	Onglet Sécurité, sélection Rôles admin, page Créer/Éditer un rôle admin	
Paramétrer des modèles d'e-mails	Onglet Configuration, sélection Modèles d'e-mail	
Configurer des stratégies de mot de passe, de compte et de nommage ; assigner des stratégies aux organisations	Onglet Sécurité, sélection Stratégies	
Charger et synchroniser des comptes et des données :		
Importer des fichiers de données (par exemple des formulaires au format XML)	Onglet Configuration, sélection Importer le fichier d'échange	
Charger des comptes de ressources	Onglet Comptes, sélection Charger à partir de la ressource	
Charger des comptes à partir d'un fichier	Onglet Comptes, sélection Charger à partir du fichier	
Comparer les utilisateurs Identity Manager avec les comptes de ressources	Onglet Ressources, sélection Réconcilier avec les ressources	
Contrôler et gérer la compatibilité :		
Désactiver ou activer l'audit	Onglet Configuration, sélection Vérification informatique	

TABLEAU C–1 Tâche de référence *(Suite)*

Pour effectuer cette tâche	Allez à	Ou à
Configurer les événements d'audit à capturer	Onglet Configuration, sélection Vérification informatique	
Définir des stratégies d'audit (créer, éditer, supprimer)	Onglet Conformité, sélection Gérer les stratégies	
Assigner des stratégies d'audit	Onglet Comptes, sélection Conformité	
Définir des solutionneurs et assigner des flux de travaux de résolution pour une stratégie d'audit	Onglet Conformité, onglet Gérer les stratégies	
Répondre aux demandes de résolution de violations de stratégie	Onglet Mes éléments de travail, sélection Résolutions	
Atténuer les violations de stratégie	Onglet Éléments de travail, onglet Résolutions	
Examiner les violations de stratégie résolues	Onglet Éléments de travail, onglet Résolutions	
Générer des rapports de stratégie d'audit	Onglet Rapports, onglet Exécuter des rapports	
Effectuer un scannage d'audit sur un ou plusieurs utilisateurs ou organisations	Onglet Comptes, sélectionnez Scanner dans la liste Actions de l'utilisateur ou Actions d'organisation	
Configurer des examens d'accès périodiques	Onglet Conformité, sélection Gérer les scannages d'accès	
Contrôler les examens d'accès périodiques	Onglet Conformité, sélection Examens des accès	
Affichage des rapports d'audit	Onglet Rapports, sélection du type Rapports de l'auditeur	
Éditer les capacités d'audit des administrateurs	Onglet Sécurité, onglet Capacités	
Paramétrer des modèles d'e-mails pour la notification de l'audit	Onglet Configuration, onglet Modèles d'e-mail	
Importer des fichiers de données/règles (par exemple des formulaires au format XML)	Onglet Configuration, onglet Importer le fichier d'échange	

TABLEAU C–1 Tâche de référence *(Suite)*

Pour effectuer cette tâche	Allez à	Ou à
Définir un scannage d'examen des accès	Onglet Conformité, onglet Gérer les scannages d'accès	
Exécuter un examen des accès	Onglet Conformité, onglet Examens des accès	
Terminer un examen des accès	Onglet Conformité, onglet Examens des accès	
Programmer un examen des accès	Onglet Tâches du serveur, onglet Gérer la planification	
Définir des examens d'accès périodiques	Onglet Conformité, onglet Gérer les scannages d'accès	
Contrôler le statut des examens d'accès	Onglet Conformité, onglet Examens des accès	
Configurer des attestateurs	Onglet Conformité, onglet Gérer les scannages d'accès	
Effectuer les tâches des attestateurs (examiner et certifier les habilitations des utilisateurs)	Onglet Éléments de travail, onglet Mes éléments de travail, onglet Attestation	
Analyse de risque et génération de rapports :		
Exécuter et gérer des rapports	Onglet Rapports, sélection Exécuter des rapports pour créer, exécuter et télécharger des rapports ; Afficher les rapports pour afficher les résultats des rapports.	
Définir et exécuter des rapports d'analyse de risque	Onglet Rapports, sélection Analyse de risque	
Afficher des rapports graphiques	Onglet Rapports, sélection Afficher les tableaux de bord	
Examiner un rapport de séparation des obligations	Onglet Rapports, onglet Exécuter des rapports	
Gérer les tâches Identity Manager :		
Exécuter une tâche définie (ou un processus)	Onglet Tâches du serveur, sélection Exécuter des tâches	

TABLEAU C–1 Tâche de référence *(Suite)*

Pour effectuer cette tâche	Allez à	Ou à
Planifier une tâche	Onglet Tâches du serveur, sélection Gérer la planification	
Afficher les résultats des tâches	Onglet Tâches du serveur, sélection Rechercher tâches ou Toutes tâches	
Suspendre ou terminer une tâche	Onglet Tâches du serveur, sélection Toutes tâches	
Gérer les utilisateurs Service Provider :		
Gérer les utilisateurs Service Provider	Onglet Comptes, sélection Gérez les utilisateurs de Service Provider	
Gérer les transactions de Service Provider	Onglet Tâches du serveur, sélection Transactions du Service Provider	
Configurer les fonctionnalités de Service Provider	Onglet Service Provider, sélection Éditer la configuration principale	
Configurer les paramètres par défaut des transactions	Onglet Service Provider, sélection Éditer la configuration de la transaction	
Créer ou éditer des stratégies Service Provider	Onglet Sécurité, sélection Stratégies	

◆ ◆ ◆ ANNEXE D

Définitions des capacités

Cette annexe contient les définitions des différentes capacités utilisées dans Identity Manager.

Elle se compose des rubriques suivantes :

- “Définitions des capacités basées sur des tâches” à la page 599 ;
- “Définitions des capacités fonctionnelles” à la page 622 ;

Pour toute information d'ordre général sur les capacités, voir la section “Comprendre et gérer les capacités” à la page 216.

Remarque – Toutes les capacités accordent un accès utilisateur ou administrateur aux onglets Mots de passe → Changer mon mot de passe et Changer mes réponses.

Définitions des capacités basées sur des tâches

Cette section décrit une à une les différentes capacités basées sur des tâches pouvant être assignées aux utilisateurs. Elle répertorie également les onglets et sous-onglets auxquels chaque capacité permet d'accéder. Les capacités sont classées par nom en ordre alphabétique.

Remarque – Ce tableau ne contient pas d'informations sur les onglets et sous-onglets par défaut disponibles pour tous les utilisateurs tels que l'onglet Changer mon mot de passe.

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de rapports détaillés d'examen d'accès	Créer, éditer, supprimer et exécuter des rapport détaillés d'examen des accès, rapports de couverture des examens d'accès et des rapports de couverture de l'étendue des utilisateurs du scannage d'accès	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Administrateur du rapport récapitulatif de l'examen des accès	Créer, éditer, supprimer et exécuter des rapports récapitulatifs d'examen des accès	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Administrateur de comptes	Réaliser toutes les opérations sur les utilisateurs, notamment assigner des capacités. Ne comprend pas les opérations en masse.	Comptes → onglets Lister les comptes, Rechercher des utilisateurs, Extraire vers le fichier, Charger à partir du fichier et Charger à partir de la ressource Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de rapports admin	Créer, éditer, supprimer et exécuter des rapports d'administrateur et des rapports de rôles admin.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports (rapports d'administrateur et sur les rôles admin uniquement)
Administrateur de rôles admin	Créer, éditer et supprimer des rôles admin.	Sécurité → onglet Rôles admin
Administrateur des applications	Créer, éditer et supprimer des rôles d'application.	Tâches du serveur → onglet Rechercher tâches, Toutes tâches, Exécuter des tâches(synchroniser les rôles) Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur du matériel	Créer, éditer et supprimer des rôles Matériel.	Tâches du serveur → onglet Rechercher tâches, Toutes tâches, Exécuter des tâches(synchroniser les rôles) Rôles → onglet Lister les rôles et onglet Rechercher des rôles

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de l'assignation de stratégies d'audit	Assigner des stratégies d'audit aux comptes utilisateur et aux organisations. Éditer la stratégie d'audit utilisateur depuis la liste Actions de l'utilisateur et éditer la stratégie d'audit d'organisation depuis la liste Actions d'organisation.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs.
Administrateur de l'assignation des stratégies d'audit aux organisations	Assigner des stratégies d'audit aux organisations uniquement. Éditer la stratégie d'audit d'organisation depuis la liste Actions d'organisation.	Comptes → onglet Lister les comptes
Administrateur de l'assignation des stratégies d'audit aux utilisateurs	Assigner des stratégies d'audit aux utilisateurs uniquement. Éditer la stratégie d'audit utilisateur depuis la liste Actions de l'utilisateur.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs
Assigner des capacités d'utilisateur	Modifier les attributions de capacités utilisateur (assigner et annuler l'assignation). Doit être assignée avec une autre capacité d'administrateur (par exemple, Créer un utilisateur ou Activer un utilisateur).	Comptes → onglets Lister les comptes (éditer uniquement) et Rechercher des utilisateurs.
Administrateur de stratégies d'audit	Créer, modifier et supprimer des stratégies d'audit.	Conformité → onglet Gérer les stratégies
Administrateur de rapport de scannage des stratégies d'audit	Exécuter ou planifier les tâches de scannage de stratégies d'audit.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches, Exécuter des tâches et Gérer la planification
Administrateur de rapports d'audit	Créer, modifier, supprimer et exécuter des rapports d'audit. Accéder aux rapports de liste de contrôle, d'historique des changements de l'utilisateur, AuditLog utilisateur individuel et d'utilisation uniquement.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports.
Administrateur de rapport AuditLog	Créer, modifier, supprimer et exécuter le rapport de liste de contrôler.	Rapports → onglet Exécuter des rapports
Administrateur de rapport des attributs audités	Créer, modifier, supprimer et exécuter le rapport des attributs audités.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur des scannages d'accès d'audit	Créer, éditer et supprimer des scannages Examen des accès périodique	Conformité → onglet Gérer les scannages d'accès
Administrateur Auditor	Paramétrer, gérer et contrôler les stratégies d'audit, les scannages d'audit et la compatibilité des utilisateurs.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches, Exécuter des tâches et Gérer la planification Rapports → onglet Exécuter des rapports et onglet Afficher les rapports Conformité → onglets Gérer les stratégies, Gérer les scannages d'accès et Examens des accès
Attestateur Auditor	Requis pour attester les attestations d'autres utilisateurs lorsque la sécurité de l'organisation est activée.	Onglets Mots de passe et Éléments de travail par défaut uniquement
Administrateurs d'examens d'accès périodiques de l'auditeur	Gérer les examens des accès périodiques (PAR), gérer les scannages des accès, gérer les attestations, gérer les rapports PAR.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Conformité → onglet Gérer les scannages d'accès et onglet Examen des accès
Solutionneur Auditor	Résoudre, atténuer et transférer les violations de stratégies d'audit.	Onglets Mots de passe et Éléments de travail par défaut uniquement
Administrateur de rapports Auditor	Créer, modifier, supprimer et exécuter tout rapport de l'auditeur.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches, Exécuter des tâches et Gérer la planification Rapports → toutes actions sur les rapports de l'auditeur
Utilisateur d'affichage Auditor	Afficher les informations de compatibilité associées à l'utilisateur.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs
Administrateur de l'historique des violations par stratégie d'audit	Créer, modifier, supprimer et exécuter le rapport sur l'historique des violations par stratégie d'audit.	Rapports → onglet Exécuter des rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de comptes en masse	Réaliser des opérations régulières et en masse sur les utilisateurs, assignations de capacités comprises.	Comptes → onglets Lister les comptes, Rechercher des utilisateurs, Lancer des actions en masse, Extraire vers le fichier, Charger à partir du fichier et Charger à partir de la ressource Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de modifications de comptes en masse	Réaliser des opérations régulières et en masse à l'exception des suppressions sur les utilisateurs, assignations de capacités comprises. Ne peut pas créer ni supprimer d'utilisateurs.	Comptes → onglets Lister les comptes, Rechercher des utilisateurs et Lancer des actions en masse. Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de changements de mots de passe de ressources en masse	Changer le mot de passe pour le compte de connexion de ressource spécifié sur les ressources indiquées.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglet Lister les ressources et onglet Lancer des actions en masse

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de modifications de comptes d'utilisateurs en masse	Réaliser des opérations régulières et en masse, à l'exception des suppressions, sur les utilisateurs existants. Impossible de créer, supprimer ou assigner des capacités aux utilisateurs.	Comptes → onglets Lister les comptes, Rechercher des utilisateurs et Lancer des actions en masse. Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Création d'utilisateurs en masse	Assigner des ressources et émettre des requêtes de création d'utilisateurs (sur des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes (Créer uniquement), Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Suppression d'utilisateurs en masse	Supprimer les comptes utilisateur Identity Manager suspendre, annuler l'assignation et supprimer les liens des comptes de ressources (pour des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes, Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Suppression d'utilisateurs IDM en masse	Supprimer des comptes utilisateur Identity Manager existants (pour des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes (Supprimer uniquement), Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Deprovisionning en masse de l'utilisateur	Supprimer des comptes de ressources existants et en supprimer les liens (pour des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes (Suspendre uniquement), Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Désactivation d'utilisateurs en masse	Désactiver des utilisateurs et des comptes de ressources existants (sur des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes (Désactiver uniquement), Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Activation d'utilisateurs en masse	Activer des utilisateurs et des comptes de ressources existants (sur des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes (Activer uniquement), Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de réinitialisation des mots de passe de ressources en masse	Réinitialiser le mot de passe pour le compte de connexion de ressource spécifié sur les ressources indiquées.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglet Lister les ressources et onglet Lancer des actions en masse

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Annuler en masse les affectations d'utilisateurs	Annuler les assignations et supprimer les liens de comptes de ressources existants (pour des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes (Annuler l'assignation uniquement), Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Supprimer en masse les liens des utilisateurs	Supprimer les liens de comptes de ressources existants (pour des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes (Supprimer le lien uniquement), Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Mise à jour d'utilisateurs en masse	Éditer, déplacer et mettre à jour des utilisateurs et des comptes de ressources existants (sur des utilisateurs individuels et en utilisant des opérations en masse).	Comptes → onglets Lister les comptes (éditer, déplacer et mettre à jour uniquement), Rechercher des utilisateurs et Lancer des actions en masse Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de comptes utilisateur en masse	Réaliser toutes les opérations, y compris les opérations en masse, sur les utilisateurs existants.	Comptes → onglets Lister les comptes, Rechercher des utilisateurs, Lancer des actions en masse, Extraire vers le fichier, Charger à partir du fichier et Charger à partir de la ressource Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur des rôles professionnels	Créer, éditer et supprimer des rôles professionnels.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches (synchroniser les rôles) Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de capacités	Créer, éditer et supprimer des capacités.	Sécurité → onglet Capacités
Administrateur de modifications de comptes	Réaliser toutes les opérations, à l'exception de la suppression, sur les utilisateurs existants, assignation de capacités incluse. Ne comprend pas les opérations en masse Créer des rapports admin et d'utilisateur, exécuter et éditer des rapports admin, exécuter des rapports AuditLog dans l'étendue. Ne peut pas exécuter des rapports admin ou d'utilisateur sur des organisations ne faisant pas partie de l'étendue. Ne pas supprimer les utilisateurs.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de modifications Active Sync de ressources	Changer les paramètres des ressources Active Sync.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglet Lister les ressources

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de modifications de mots de passe	Changer les mots de passe de compte de ressources et d'utilisateur. Accéder à la tâche Exporter les scannages de mots de passe seulement (depuis l'onglet Exécuter des tâches)	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Mots de passe → Changer le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches. Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de modifications de mots de passe (vérification requise)	Changer les mots de passe des comptes de ressources et utilisateur suite à la validation des réponses aux questions d'authentification de l'utilisateur. Accéder à la tâche Exporter les scannages de mots de passe seulement (depuis l'onglet Exécuter des tâches)	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Mots de passe → onglet Changer le mot de passe de l'utilisateur (vérification requise avant l'action) Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de modifications de mots de passe de ressources	Changer les mots de passe des comptes administrateur de ressources. Changer les mots de passe des ressources uniquement (depuis Gérer une connexion → Changement du mot de passe dans le menu des actions)	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglet Lister les ressources.
Administrateur de modifications de comptes d'utilisateurs	Effectuer toutes les opérations sur les utilisateurs existants à l'exception des suppressions et des opérations en masse. Impossible de créer, supprimer ou assigner des capacités aux utilisateurs.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Configurer l'audit	Configuration des événements et groupes de configuration contrôlés dans le système.	Configurer → Onglet Vérification informatique

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Configurer les certificats	Configuration des certificats de confiance et des LRC.	Sécurité → onglet Certificats
Contrôler administrateur de ressource de synchronisation active	Contrôler l'état des ressources Active Sync (démarrage, arrêt ou actualisation, par ex.).	Ressources → onglet Lister les ressources Pour les ressources Active Sync : menu d'actions Active Sync
Créer un utilisateur	Assigner des ressources et lancer des demandes de création d'utilisateur. Ne comprend pas les opérations en masse	Comptes → onglet Lister les comptes (Créer uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur d'entrepôt de données	Configurer l'exportateur de données et exécuter la tâche Lanceur d'exportateur d'entrepôt de données.	Rapports → onglet Graphes de tableau de bord et onglet Afficher les tableaux de bord Ressources → onglet Lister les ressources Configurer → onglet Entrepôt
Requête d'entrepôt de données	Configurer et exécuter des requêtes sur attributs	Rapports → onglet Graphes de tableau de bord et onglet Afficher les tableaux de bord Ressources → onglet Lister les ressources Conformité → Requête sur attributs
Supprimer l'utilisateur	Supprimer des comptes utilisateur Identity Manager ; suspendre, annuler les assignations et supprimer les liens de comptes de ressources. Ne comprend pas les opérations en masse.	Comptes → onglet Lister les comptes (Supprimer uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Supprimer l'utilisateur IDM	Supprimer des comptes utilisateur Identity Manager. Ne comprend pas les opérations en masse.	Comptes → onglet Lister les comptes (Supprimer uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Deprovisionning de l'utilisateur	Supprimer des comptes de ressources existants et en supprimer les liens. Ne comprend pas les opérations en masse.	Comptes → onglet Lister les comptes (Suspendre uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Désactiver un utilisateur	Désactiver les comptes de ressources et d'utilisateur existants. Ne comprend pas les opérations en masse	Comptes → onglet Lister les comptes (Désactiver uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Activer un utilisateur	Activer des comptes de ressources et d'utilisateur existants. Ne comprend pas les opérations en masse	Comptes → onglet Lister les comptes (Activer uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur des utilisateurs finaux	Visualiser et modifier les droits portant sur les types d'objets spécifiés dans la capacité Utilisateur final et définis par la règle d'organisations contrôlées par les utilisateurs finaux.	Tous les onglets par défaut

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur des ressources externes	Afficher et configurer les ressources externes uniquement. Ne peut pas créer de nouvelles ressources.	Configurer → onglet Ressources externes
Configurer le schéma d'Identity Manager	Afficher et configurer le schéma effectif pour les utilisateurs ou rôles en utilisant l'objet Configuration Identity Manager `IDM Schema Configuration`.	Tous les onglets par défaut
Importer un utilisateur	Importer des utilisateurs depuis des ressources définies.	Comptes → onglets Lister les comptes, Rechercher des utilisateurs, Extraire vers le fichier, Charger à partir du fichier et Charger à partir de la ressource Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateurs d'import/export	Importer et exporter tous les types d'objets.	Configurer → onglet Importer le fichier d'échange
Administrateur des rôles informatiques	Créer, éditer et supprimer des rôles informatiques.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches (synchroniser les rôles) Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de connexion	Éditer l'ensemble des modules de connexion pour une interface de connexion donnée.	Sécurité → onglet Connexion
Administrateur d'organisations	Créer et éditer des organisations et des jonctions d'annuaires. Supprimer uniquement des organisations.	Comptes → onglet Lister les comptes
Approbateur d'organisation	Approuver les demandes de nouvelles organisations.	Onglets Mots de passe et Éléments de travail par défaut uniquement
Administrateur d'historique des violations par organisation	Créer, éditer, supprimer et exécuter les rapports d'historique des violations par organisation uniquement.	Rapports → onglet Exécuter des rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de mots de passe	Lister, changer et réinitialiser les mots de passe de compte de ressources et d'utilisateur.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de mots de passe (vérification requise)	Lister, changer et réinitialiser les mots de passe de compte de ressources et d'utilisateur uniquement. Validation réussie des réponses aux questions d'authentification de l'utilisateur requise pour la réussite de l'action.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Exécuter le débogage	Accéder aux et exécuter des opérations depuis les pages de débogage d'Identity Manager. **Remarque –** Les pages de débogage d'Identity Manager ne sont pas accessibles depuis le menu. Pour accéder aux pages de débogage, saisissez l'URL suivant dans votre navigateur : `http://<`*`HôteServeurApp`*`>:<`*`Port`*`>/idm/debug`	Tous les onglets par défaut
Administrateur de stratégies	Créer, éditer et supprimer des stratégies.	Sécurité → onglet Stratégies
Administrateur de rapport récapitulatif des stratégies	Créer, éditer, supprimer et exécuter des rapports récapitulatifs de stratégies.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Enregistrement du composant du produit Identity Manager	Enregistrer une installation d'Identity Manager auprès de Sun Microsystems ou créer une étiquette de service locale.	Configurer → onglet Enregistrement du produit
Administrateur de réconciliation	Éditer les stratégies de réconciliation et contrôler les tâches de réconciliation.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches (afficher la tâche de réconciliation). Ressources → onglet Lister les ressources et onglet Examiner index de compte
Administrateur de rapports de réconciliation	Créer, éditer, supprimer et exécuter des rapports de réconciliation.	Rapports → onglet Exécuter des rapports (Rapport d'index de comptes uniquement) et onglet Afficher les rapports
Administrateur des demandes de réconciliation	Gérer les demandes de réconciliation.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglet Lister les ressources (fonctionnalités de liste et réconciliation uniquement) et onglet Afficher les rapports
Administrateur de l'intégration de Remedy	Éditer la configuration de l'intégration Remedy (afficher les tâches, exécuter la synchronisation des rôles).	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Configurer → onglet Intégration Remedy
Renommer des utilisateurs	Renommer des utilisateurs et des comptes de ressources existants (lister tous les comptes de l'étendue, renommer les utilisateurs).	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de rapports	Configurer les paramètres d'audit et exécuter tous les types de rapports (afficher les tâches, exécuter la synchronisation des rôles).	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rapports → onglets Exécuter des rapports Afficher les rapports, Exécuter une analyse de risque et Afficher les analyses des risques Rôles → onglet Lister les rôles et onglet Rechercher des rôles Configurer → Onglet Vérification informatique
Administrateur de réinitialisations de mots de passe	Réinitialiser les mots de passe de compte de ressources et d'utilisateur.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs (réinitialiser le mot de passe uniquement) Mots de passe → Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches (aucune tâche n'est disponible pour les utilisateurs avec cette capacité) Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de réinitialisations de mots de passe (vérification requise)	Réinitialiser les mots de passe de compte de ressources et d'utilisateur. Validation réussie des réponses de l'utilisateur aux questions d'authentification requise pour la réussite de l'action.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Mots de passe → Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches (aucune tâche n'est disponible pour les utilisateurs avec cette capacité) Rôles → onglet Lister les rôles et onglet Rechercher des rôles

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de réinitialisations de mots de passe des ressources	Réinitialiser les mots de passe de compte administrateur (depuis Gérer une connexion → Réinitialisation du mot de passe dans le menu des actions).	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglet Lister les ressources
Administrateur de ressources	Créer, éditer et supprimer des ressources. Le Rapport d'utilisateur de ressources et le de groupe de ressources retournent une erreur avec les ressources situées hors de l'étendue. Éditer les stratégies globales, les paramètres et les groupes de ressources. Ne peut pas gérer les connexions ni les objets Ressource.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglets Lister les ressources, Lister les groupes de ressources et Examiner index de compte Configurer → Serveurs de connecteurs
Approbateur de ressources	Approuver les assignations de ressources	Tous les onglets Mots de passe et Éléments de travail par défaut
Administrateur de groupes de ressources	Créer, éditer et supprimer des groupes de ressources.	Ressources → onglet Lister les groupes de ressources
Administrateur d'objets ressources	Afficher, créer, modifier et supprimer des objets Ressource.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglet Lister les ressources
Administrateur de mots de passe de ressources	Changer et réinitialiser les mots de passe de compte proxy de ressources.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Ressources → onglet Lister les ressources (Changer un mot de passe de ressource uniquement depuis Gérer une connexion → Changement du mot de passe dans le menu des actions)
Administrateur de rapports de ressources	Créer, éditer, supprimer et exécuter des rapports de ressources.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Administrateur d'historique des violations par ressource	Créer, éditer, supprimer et exécuter des rapports d'historique des violations par ressource.	Rapports → onglet Exécuter des rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur d'analyses de risques	Créer, éditer, supprimer et exécuter des analyses de risque.	Rapports → onglet Analyse de risque et onglet Afficher les analyses des risques
Administrateur de rôles	Créer, éditer, synchroniser et supprimer des rôles.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches
		Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Approbateur de rôles	Approuver les assignations de rôles	Tous les onglets Mots de passe et Éléments de travail par défaut
Administrateur de rapports de rôle	Créer, éditer, supprimer et exécuter des rapports de ressources.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
		Rôles → onglet Lister les rôles
Exécuter le rapport détaillé de l'examen des accès	Exécuter le rapport détaillé de l'examen des accès	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter le rapport récapitulatif de l'examen des accès	Exécuter le rapport récapitulatif de l'examen des accès	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter un rapport admin	Exécuter des rapports d'administrateur.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter le rapport de scannage des stratégies d'audit	Exécuter le rapport de scannage des stratégies d'audit.	Tâches du serveur → Toutes tâches, Rechercher tâches et Exécuter des tâches uniquement
Exécuter un rapport d'audit	Exécuter des rapports d'audit, AuditLog, historique des changements de l'utilisateur, AuditLog utilisateur individuel et d'utilisation uniquement.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter le rapport des attributs audités	Exécuter et afficher le rapport des attributs audités.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter le rapport Auditor	Exécuter tous les rapports du type Rapport AuditLog.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches
		Rapports → onglet Exécuter des rapports et onglet Afficher les rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Exécuter le rapport AuditLog	Exécuter et afficher les rapports auditLog, Activité d'aujourd'hui et Activité hebdomadaire.	Rapports → onglet Exécuter des rapports
Exécuter l'historique des violations par stratégie d'audit	Exécuter et afficher les rapports d'historique des violations par organisation, Activité d'aujourd'hui et Activité hebdomadaire.	Rapports → onglet Exécuter des rapports
Exécuter le rapport récapitulatif des stratégies	Exécuter et afficher le rapport récapitulatif des stratégies.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter l'historique des violations par organisation	Exécuter le rapport d'historique des violations par organisation.	Rapports → onglet Exécuter des rapports
Exécuter les rapports de réconciliation	Exécuter et afficher les rapports d'index de comptes.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter un rapport de ressource	Exécuter et afficher les rapports d'utilisateur de ressources et de groupe de ressources.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter l'historique des violations par ressource	Exécuter les rapports d' historique des violations par ressource.	Rapports → onglet Exécuter des rapports
Exécuter une analyse de risque	Exécuter et afficher des analyses de risque.	Rapports → onglet Exécuter des analyses de risque et onglet Afficher les analyses des risques
Exécuter un rapport de rôle	Exécuter et afficher des rapports de rôle.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports Rôles → onglet Lister les rôles
Exécuter un rapport de séparation des obligations	Exécuter et afficher des rapports de séparation des obligations.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter les rapports de tâches	Exécuter et afficher des rapports de tâches.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter le rapport d'accès utilisateur	Exécuter et afficher des rapports d'utilisateur détaillés et des rapports d'accès utilisateur.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Exécuter un rapport d'utilisateur	Exécuter et afficher des rapports d'utilisateur.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Exécuter le rapport récapitulatif des violations	Exécuter le rapport récapitulatif des violations.	Rapports → onglet Exécuter des rapports
Administrateur de la sécurité	Créer des utilisateurs avec des capacités ; activer et désactiver des utilisateurs, lister et contrôler les objets Ressource, gérer les clés de chiffrement, gérer les configurations de connexion et d'audit et gérer les stratégies.	Comptes → onglet Lister les comptes (certaines actions) et onglet Rechercher des utilisateurs (rapport d'audit) Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches, Exécuter des tâches et Configurer les tâches Rapports → onglets Exécuter des rapports Afficher les rapports, Graphes de tableau de bord, Afficher les tableaux de bord et Configurer les rapports Ressources → Lister les ressources Configurer → onglets Vérification informatique et Entrepôt Sécurité → onglets Certificats, Connexion et Stratégies Service Provider → Éditer la configuration de recherche d'utilisateurs
Administrateur de rapports de séparation des obligations	Créer, éditer, exécuter, afficher et supprimer des rapports de séparation des obligations.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Administrateur des rôles admin Service Provider	Gérer les rôles admin de Service Provider et les règles associées.	Sécurité → onglet Rôles admin

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de Service Provider	Créer, éditer et gérer les utilisateurs et transactions de fournisseur de services ; configurer la base de données des transactions et les événements suivis.	Comptes → onglet Gérez les utilisateurs de Service Provider Tâches du serveur → onglet Transactions du Service Provider Rapports → onglet Graphes de tableau de bord Rapports → onglet Afficher les tableaux de bord Service Provider → onglets Éditer la configuration principale, Éditer la configuration de la transaction et Éditer la configuration de recherche d'utilisateurs
Créer les utilisateurs de Service Provider	Créer des comptes utilisateur pour les utilisateurs (extranet) de Service Provider.	Comptes → onglet Gérez les utilisateurs de Service Provider
Supprimer les utilisateurs de Service Provider	Supprimer un compte utilisateur de Service Provider.	Comptes → onglet Gérez les utilisateurs de Service Provider
Mettre à jour les utilisateurs de Service Provider	Mettre à jour un compte utilisateur de Service Provider.	Comptes → onglet Gérez les utilisateurs de Service Provider
Administrateur d'utilisateurs de Service Provider	Gérer les utilisateurs (extranet) de Service Provider.	Comptes → onglet Gérez les utilisateurs de Service Provider
Afficher les utilisateurs de Service Provider	Afficher les informations des comptes utilisateur (extranet) de Service Provider.	Comptes → onglet Gérez les utilisateurs de Service Provider
Administrateur de rapports de tâches	Créer, éditer, supprimer et afficher des rapports de tâche.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Annuler les affectations de l'utilisateur	Annuler les assignations de comptes de ressources existants et en supprimer les liens. Ne comprend pas les opérations en masse.	Comptes → onglet Lister les comptes (Annuler l'assignation uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Supprimer les liens de l'utilisateur	Supprimer les liens des comptes de ressources existants. Ne comprend pas les opérations en masse.	Comptes → onglet Lister les comptes (Supprimer le lien uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Déverrouiller un utilisateur	Déverrouiller les comptes de ressources d'un utilisateur existant qui prennent en charge le déverrouillage. Ne comprend pas les opérations en masse.	Comptes → onglet Lister les comptes (Déverrouiller uniquement) et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches, Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Mettre à jour un utilisateur	Éditer les utilisateurs existants et lancer les demandes de mise à jour de l'utilisateur. Gérer les tâches de serveur existantes.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs Tâches du serveur → onglets Rechercher tâches, Toutes tâches, Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de rapport d'accès utilisateur	Créer, éditer, supprimer et afficher des rapports d'accès utilisateur.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur de comptes d'utilisateurs	Toutes les opérations sur les utilisateurs sauf assigner des capacités aux utilisateurs.	Comptes → onglets Lister les comptes, Rechercher des utilisateurs, Extraire vers le fichier, Charger à partir du fichier et Charger à partir de la ressource Mots de passe → onglet Changer le mot de passe de l'utilisateur et onglet Réinitialiser le mot de passe de l'utilisateur Tâches du serveur → onglets Rechercher tâches, Toutes tâches et Exécuter des tâches Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Administrateur de rapports d'utilisateur	Créer, éditer, supprimer et afficher des rapports d'utilisateur.	Rapports → onglet Exécuter des rapports et onglet Afficher les rapports
Afficher les applications	Lister les rôles de type Application et en afficher les informations. Aucune action de modification n'est autorisée.	Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Afficher le matériel	Lister les rôles de type Matériel et en afficher les informations. Aucune action de modification n'est autorisée.	Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Afficher les rôles professionnels	Lister les rôles professionnels et en afficher les informations. Aucune action de modification n'est autorisée.	Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Afficher les rôles informatiques	Lister les rôles informatiques et en afficher les informations. Aucune action de modification n'est autorisée.	Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Afficher les rôles	Lister tous les types de rôles et afficher les informations de tous les rôles. Aucune action de modification n'est autorisée.	Rôles → onglet Lister les rôles et onglet Rechercher des rôles
Afficher l'utilisateur	Afficher les détails d'un utilisateur individuel. Aucune action de modification n'est autorisée.	Comptes → onglet Lister les comptes et onglet Rechercher des utilisateurs
Administrateur de rapport récapitulatif des violations	Créer, éditer, supprimer et exécuter des rapports récapitulatif de violations.	Rapports → onglet Exécuter des rapports

TABLEAU D–1 Définitions des capacités basées sur des tâches d'Identity Manager *(Suite)*

Capacité	Permet à l'administrateur/utilisateur de	Peut accéder aux onglets et sous-onglets suivants
Administrateur Identity System	Effectuer des tâches à l'échelle du système, par exemple éditer des objets Configuration système, synchroniser les rôles, éditer des modèles d'adaptateur de ressources et exécuter des rapports.	Tâches du serveur → onglets Rechercher tâches, Toutes tâches, Exécuter des tâches , Gérer la planification et Configurer les tâches Rapports → onglets Exécuter des rapports, Afficher les rapports, Graphes de tableau de bord, Afficher les tableaux de bord et Configurer les rapports Ressources → Lister les ressources Configurer → onglets Vérification informatique, Entrepôt, Modèles d'e-mail, Mappages des formulaires et processus, Serveurs, Interface utilisateur et Enregistrement du produit Conformité → Examens des accès Sécurité → Certificats

Définitions des capacités fonctionnelles

Les capacités fonctionnelles comprennent les capacités basées sur des tâches ainsi que d'autres capacités fonctionnelles.

- **Administrateur de comptes**
  - Administrateur des approbateurs
    - Approbateur d'organisation
    - Approbateur de ressources
    - Approbateur de rôles
  - Assigner des capacités d'utilisateur
  - Accès SPML
  - Administrateur de comptes d'utilisateurs
    - Créer un utilisateur
    - Supprimer l'utilisateur
      - Supprimer l'utilisateur IDM
      - Deprovisionning de l'utilisateur
      - Annuler les affectations de l'utilisateur
      - Supprimer les liens de l'utilisateur
    - Désactiver un utilisateur

- Activer un utilisateur
- Administrateur de mots de passe
  - Administrateur de modifications de mots de passe
  - Administrateur de réinitialisations de mots de passe
- Renommer des utilisateurs
- Déverrouiller un utilisateur
- Mettre à jour un utilisateur
- Afficher l'utilisateur
- Importer un utilisateur

- **Administrateur des rôles admin**
- **Administrateur Auditor**
  - Assignation de stratégies d'audit
    - Assigner des stratégies d'audit aux organisations
    - Assigner des stratégies d'audit aux utilisateurs
  - Administrateur de stratégies d'audit

    Utilisateur d'affichage Auditor
  - Administrateurs d'examens d'accès périodiques de l'auditeur

    Administrateur des scannages d'accès d'audit
  - Administrateur de rapports Auditor
  - Administrateur de mots de passe
  - Administrateur de comptes d'utilisateurs
  - Assigner des capacités d'utilisateur
- **Administrateur de rapports Auditor**
  - Administrateur de rapports détaillés d'examen d'accès

    Exécuter le rapport détaillé de l'examen des accès
  - Administrateur du rapport récapitulatif de l'examen des accès

    Exécuter le rapport récapitulatif de l'examen des accès
  - Administrateur de rapport de scannage des stratégies d'audit

    Exécuter le rapport de scannage des stratégies d'audit
  - Administrateur de rapport des attributs audités

    Exécuter le rapport des attributs audités
  - Administrateur de l'historique des violations par stratégie d'audit

    Exécuter le rapport d'historique des violations de stratégie d'audit
  - Administrateur d'historique des violations par organisation

Exécuter le rapport d'historique des violations par organisation

- Administrateur de rapport récapitulatif des stratégies
- Administrateur d'historique des violations par ressource

  Exécuter le rapport d'historique des violations par ressource
- Exécuter le rapport Auditor
- Administrateur de rapports de séparation des obligations

  Exécuter un rapport de séparation des obligations
- Administrateur de rapport d'accès utilisateur

  Exécuter le rapport d'accès utilisateur
- Administrateur de rapport récapitulatif des violations

- **Utilisateur d'affichage Auditor**

  Afficher l'utilisateur
- **Administrateur de comptes en masse**
  - Administrateur des approbateurs
  - Assigner des capacités d'utilisateur
  - Administrateur de comptes utilisateur en masse
    - Création d'utilisateurs en masse
    - Suppression d'utilisateurs en masse
      - Suppression d'utilisateurs IDM en masse
      - Deprovisionning en masse de l'utilisateur
      - Annuler en masse les affectations d'utilisateurs
      - Supprimer en masse les liens des utilisateurs
    - Désactivation d'utilisateurs en masse
    - Activation d'utilisateurs en masse
    - Administrateur de mots de passe
    - Renommer des utilisateurs
    - Déverrouiller un utilisateur
    - Afficher l'utilisateur
    - Importer un utilisateur
- **Administrateur de modifications de comptes en masse**
  - Administrateur des approbateurs
  - Assigner des capacités d'utilisateur
  - Administrateur de modifications de comptes d'utilisateurs en masse
    - Désactivation d'utilisateurs en masse

- Activation d'utilisateurs en masse
- Mise à jour d'utilisateurs en masse
- Administrateur de mots de passe
- Renommer des utilisateurs
- Déverrouiller un utilisateur
- Afficher l'utilisateur

- **Administrateur de ressources en masse**
  - Changer administrateur de ressource de synchronisation active
  - Contrôler administrateur de ressource de synchronisation active
  - Administrateur de groupes de ressources
- **Administrateur des mots de passe de ressources en masse**
  - Administrateur de changements de mots de passe de ressources en masse
  - Administrateur de réinitialisation des mots de passe de ressources en masse
- **Administrateur de capacités**
- **Administrateur de modifications de comptes**
  - Administrateur des approbateurs
  - Assigner des capacités d'utilisateur
  - Administrateur de modifications de comptes d'utilisateurs
    - Administrateur de mots de passe
      - Administrateur de modifications de mots de passe
      - Administrateur de réinitialisations de mots de passe
    - Désactiver un utilisateur
    - Activer un utilisateur
    - Renommer des utilisateurs
    - Déverrouiller un utilisateur
    - Mettre à jour un utilisateur
    - Afficher l'utilisateur
- **Configurer les certificats**
- **Administrateur d'entrepôt de données**
- **Requête d'entrepôt de données**
- **Déboguer**
- **Administrateur des utilisateurs finaux**
- **Configuration du schéma IDM**
- **Administrateurs d'import/export**
- **Administrateur de licences**
- **Administrateur de connexion**

- **Administrateur de métavues**
- **Administrateur d'organisations**
- **Administrateur de mots de passe (vérification requise)**
  - Administrateur de modifications de mots de passe (vérification requise)
  - Administrateur de réinitialisations de mots de passe (vérification requise)
- **Administrateur de stratégies**
- **Administrateur du produit**
- **Administrateur de réconciliation**

  Administrateur des demandes de réconciliation
- **Administrateur de l'intégration de Remedy**
- **Administrateur de rapports**
  - Administrateur de rapports admin

    Exécuter un rapport admin
  - Administrateur de rapports d'audit

    Exécuter un rapport d'audit
  - Administrateur de rapports Auditor
    - Administrateur de rapports détaillés d'examen d'accès

      Exécuter le rapport détaillé de l'examen des accès
    - Administrateur du rapport récapitulatif de l'examen des accès

      Exécuter le rapport récapitulatif de l'examen des accès
    - Administrateur de rapport de scannage des stratégies d'audit

      Exécuter le rapport de scannage des stratégies d'audit
    - Administrateur de rapport des attributs audités

      Exécuter le rapport des attributs audités
    - Administrateur de rapport AuditLog

      Exécuter le rapport AuditLog
    - Administrateur de l'historique des violations par stratégie d'audit

      Exécuter l'historique des violations par stratégie d'audit
    - Administrateur d'historique des violations par organisation

      Exécuter l'historique des violations par organisation
    - Administrateur de rapport récapitulatif des stratégies

      Exécuter le rapport récapitulatif des stratégies
    - Administrateur de rapports de réconciliation

      Exécuter les rapports de réconciliation

- Administrateur d'historique des violations par ressource

  Exécuter l'historique des violations par ressource
- Exécuter le rapport Auditor
  - Exécuter le rapport détaillé de l'examen des accès
  - Exécuter le rapport récapitulatif de l'examen des accès
  - Exécuter le rapport de scannage des stratégies d'audit
  - Exécuter le rapport des attributs audités
  - Exécuter le rapport AuditLog
  - Exécuter l'historique des violations par stratégie d'audit
  - Exécuter l'historique des violations par organisation
  - Exécuter le rapport récapitulatif des stratégies
  - Exécuter l'historique des violations par ressource
  - Exécuter un rapport de séparation des obligations
  - Exécuter le rapport d'accès utilisateur
  - Exécuter le rapport récapitulatif des violations
- Administrateur de rapports de séparation des obligations

  Exécuter un rapport de séparation des obligations
- Administrateur de rapport d'accès utilisateur

  Exécuter le rapport d'accès utilisateur
- Administrateur de rapport récapitulatif des violations

  Exécuter le rapport récapitulatif des violations

- Administrateur de rapports de réconciliation

  Exécuter les rapports de réconciliation
- Administrateur de rapports de ressources

  Exécuter un rapport de ressource
- Administrateur d'analyses de risques

  Exécuter une analyse de risque
- Administrateur de rapports de rôle

  Exécuter un rapport de rôle
- Administrateur de rapports de tâches

  Exécuter les rapports de tâches
- Administrateur de rapports d'utilisateur

  Exécuter un rapport d'utilisateur
- Configurer l'audit

- **Administrateur de ressources**
  - Changer administrateur de ressource de synchronisation active

- Contrôler administrateur de ressource de synchronisation active
- Administrateur de groupes de ressources

- **Administrateur d'objets ressources**
- **Administrateur des mots de passe des ressources**
  - Administrateur de modifications de mots de passe de ressources
  - Administrateur de réinitialisations de mots de passe des ressources
- **Administrateur de rôles**
  - Administrateur des applications
  - Administrateur du matériel
  - Administrateur des rôles professionnels
  - Administrateur des rôles informatiques
- **Administrateur de la sécurité**
- **Administrateur de Service Provider**
  - Administrateur d'utilisateurs de Service Provider
  - Créer les utilisateurs de Service Provider
  - Supprimer les utilisateurs de Service Provider
  - Mettre à jour les utilisateurs de Service Provider
  - Afficher les utilisateurs de Service Provider
- **Administrateur des rôles admin Service Provider**
- **Administrateur Waveset**

Glossaire

Adaptateur de ressources

Composant d'Identity Manager qui fournit un lien entre le moteur Identity Manager et la ressource.

Ce composant permet à Identity Manager de gérer les comptes d'utilisateur sur une ressource donnée (notamment la création, la mise à jour, la suppression, l'authentification et le scannage des droits), ainsi que d'utiliser cette ressource pour l'authentification d'intercommunication.

Administrateur

Personne configurant Identity Manager ou étant responsable de tâches opérationnelles, telles que la création d'utilisateurs et la gestion de l'accès aux ressources.

Application (rôle)

L'un des quatre types de rôle disponibles dans Identity Manager, le type Application rassemble des ressources et/ou des groupes de ressources et/ou des applications spécifiques sur des ressources, dont les utilisateurs ont besoin pour s'acquitter de leurs tâches. Les rôles de type Application ne peuvent pas être assignés directement à des utilisateurs, mais peuvent l'être à des rôles informatiques et professionnels.

Approbateur

Utilisateur disposant de droits d'administration et responsable de l'approbation et du rejet des demandes d'accès.

Approbation

Processus consistant à accepter ou à refuser à un utilisateur une demande d'accès à un rôle, une ressource ou une organisation. Un administrateur Identity Manager autorisé à visualiser et à répondre à un élément de travail d'approbation est un *approbateur*.

Assistant Ressources

Outil d'Identity Manager qui guide l'utilisateur à travers les processus de création et de modification des ressources, notamment la définition et la configuration des paramètres des ressources, des attributs de compte, du modèle d'identification et des paramètres Identity Manager.

Attestateur

Utilisateur qui accepte la responsabilité consistant à certifier (*attester*) que l'habilitation d'un utilisateur est appropriée. Un attestateur a des privilèges étendus dans Identity Manager, nécessaires pour gérer les habilitations utilisateur nécessitant une attestation.

Attestation

Processus consistant à certifier qu'un utilisateur donné est doté des privilèges appropriés sur les ressources appropriées à un instant t. Un utilisateur Identity Manager autorisé à visualiser et à répondre à un élément de travail de type attestation est un *attestateur*. Les règles d'Identity Manager déterminent si un enregistrement d'habilitation utilisateur doit être attesté manuellement ou s'il peut être approuvé ou rejeté automatiquement.

Attester

Action effectuée par un attestateur pendant un examen des accès pour confirmer qu'une habilitation utilisateur est appropriée.

Attribut de compte Les attributs de compte offrent aux administrateurs Identity Manager un moyen de créer un jeu standard de noms mappant vers des attributs sur les ressources gérées. Par exemple, un attribut Identity Manager nommé *fullname* peut être mappé vers l'attribut *displayName* sur les ressources Active Directory et vers l'attribut *cn* sur les ressources LDAP. Tout changement apporté à l'attribut *fullname* de l'utilisateur dans Identity Manager, est transmis aux attributs *displayName* et *cn* de l'utilisateur sur les comptes de ressource distants de l'utilisateur.

Capacité Groupe de droits d'accès associé aux comptes utilisateur qui régit les actions exécutées dans Identity Manager ; contrôle d'accès de bas niveau au sein d'Identity Manager.

Carte schématique Associe les attributs de compte de ressources aux attributs de compte Identity Manager d'une ressource.

Les attributs de compte Identity Manager créent un lien commun vers différentes ressources ; ils sont référencés par les formulaires.

Compte d'adaptateur de ressources Données d'identification utilisées par un adaptateur de ressources d'Identity Manager pour accéder à une ressource gérée.

Compte utilisateur Compte créé à l'aide d'Identity Manager.

Peut faire référence à un compte Identity Manager ou à un compte situé sur une ressource distante gérée par Identity Manager. La configuration de comptes utilisateur est un processus dynamique. Les informations à fournir ou les champs à renseigner varient en fonction des ressources fournies à l'utilisateur de manière directe ou indirecte via l'assignation de rôles.

Délai de signalisation Période de temps spécifiée pour une demande d'élément de travail pendant laquelle le propriétaire assigné de l'élément de travail doit répondre avant que le processus Identity Manager ne l'envoie au prochain répondeur assigné.

Délégation Processus consistant à assigner de manière temporaire les futurs éléments de travail à un ou plusieurs utilisateurs pendant une période donnée.

Éditeur de processus métier Représentation graphique des formulaires, règles et flux de travaux d'Identity Manager fournie avec les versions d'Identity Manager antérieures à la 7.0. L'éditeur de processus métier a été remplacé par l'Identity Manager IDE dans les versions actuelles d'Identity Manager. Voir Glossaire.

Élément de travail Demande d'action générée par un flux de travaux, un formulaire ou une procédure d'Identity Manager. Les approbations, les approbations de changement, les attestations et les résolutions constituent quatre types d'élément de travail.

Examen d'accès périodique Examen d'accès qui est effectué à intervalles réguliers, par exemple tous les trimestres.

Examen des accès Processus contrôlé permettant aux responsables ou autres supérieurs hiérarchiques d'examiner et de certifier les privilèges d'accès des utilisateurs. Les enregistrements d'habilitation utilisateur peuvent être approuvés ou rejetés automatiquement, ou attestés manuellement. Voir aussi *Attestation*.

Flux de travaux Processus logique renouvelé au cours duquel les documents, les informations ou les tâches sont transmises d'un participant à un autre. Les flux de travaux Identity Manager comprennent plusieurs processus contrôlant la création, la mise à jour, l'activation, la désactivation et la suppression des comptes utilisateur.

Formulaire	Objet associé à une page Web contenant les règles d'affichage que le navigateur doit adopter sur cette page concernant les attributs d'affichage des utilisateurs. Les formulaires peuvent intégrer des logiques d'entreprise et sont souvent utilisés pour manipuler des données d'affichage avant qu'elles ne soient présentées à l'utilisateur.
Groupe de ressources	Ensemble de ressources utilisées pour ordonner la création, la suppression et la mise à jour des comptes de ressources d'utilisateur.
Habilitation	Voir *Habilitation utilisateur*
Habilitation utilisateur	Dans Identity Manager, privilège d'accès contrôlable octroyé à un utilisateur sur une ressource ou un système et permettant d'appliquer les restrictions d'accès.
Identity Manager IDE	L'environnement de développement intégré Identity Manager (Identity Manager IDE) est une application qui permet d'afficher, personnaliser et déboguer les objets Identity Manager dans votre déploiement. L'Identity Manager IDE est disponible sous la forme d'un plug-in NetBeans.
Interface administrateur	Interface utilisateur permettant aux administrateurs de configurer et de gérer Identity Manager.
Interface utilisateur	Dans Identity Manager, l'interface utilisateur permet aux utilisateurs dépourvus de capacités administratives d'exécuter un éventail de tâches « en libre service », telles que la modification de leur mot de passe et la définition des réponses aux questions d'authentification. Est également appelée *interface utilisateur final*.
Jonction d'annuaires	Ensemble d'organisations reliées hiérarchiquement qui reflète l'ensemble de conteneurs hiérarchiques effectif d'une ressource d'annuaire. Toute organisation contenue dans une jonction d'annuaires est une *organisation virtuelle*.
Matériel (rôle)	L'un des quatre types de rôle disponibles dans Identity Manager, le type Matériel est (généralement) réservé aux ressources non connectées et/ou non numériques nécessitant un provisioning manuel comme, par exemple, les téléphones et ordinateurs portables. Les rôles de type Matériel ne peuvent pas être assignés directement à des utilisateurs, mais peuvent l'être à des rôles informatiques et à des rôles professionnels.
Modèle d'identité	Définit le nom du compte de ressources de l'utilisateur.
Organisation	Conteneur Identity Manager utilisé pour activer la délégation administrative. Les organisations définissent l'étendue des entités (telles que les comptes d'utilisateur, les ressources et les comptes d'administrateur) qu'un administrateur contrôle ou gère. Les organisations fournissent un contexte « où », essentiellement pour des objectifs administratifs d'Identity Manager.
Organisation virtuelle	Organisation définie au sein d'une jonction d'annuaires. *Voir* Jonction d'annuaires.
Réconciliation	Fonctionnalité d'Identity Manager qui compare régulièrement les comptes de ressources d'Identity Manager avec ceux résidant sur les ressources proprement dites. La réconciliation corrèle les données des comptes et fait ressortir les différences.

Règle Objet du référentiel Identity Manager contenant une fonction écrite en langage XPRESS, XML Object ou JavaScript. Les règles fournissent un mécanisme pour le stockage des variables logiques ou statiques fréquemment utilisées, pour qu'elles puissent être réutilisées dans des formulaires, des flux de travaux et des rôles.

Résolution Processus consistant à corriger les violations de conformité détectées par la fonction d'audit d'Identity Manager. Identity Manager contrôle les données à l'échelle de l'entreprise afin de s'assurer de leur conformité aux réglementations et stratégies internes et externes. Un administrateur autorisé à visualiser et à répondre aux violations de stratégies est un *solutionneur*.

Ressource Dans Identity Manager, une ressource stocke des informations sur la procédure de connexion à la ressource ou au système sur lesquels sont créés les comptes. Les ressources distantes auxquelles Identity Manager fournit un accès incluent notamment les gestionnaires de sécurité des systèmes mainframe, bases de données, services d'annuaire, applications, systèmes d'exploitation, systèmes ERP (planification des ressources) et plates-formes de messagerie.

Rôle Un rôle est un objet Identity Manager permettant de regrouper des droits d'accès aux ressources en vue de les assigner efficacement à des utilisateurs. Les rôles sont organisés en quatre types : les rôles professionnels, informatiques, Application et Matériel. Les rôles informatiques, Application et Matériel permettent d'organiser les habilitations de ressources en groupes. Ces trois groupes sont ensuite assignés à des rôles professionnels de manière à permettre aux utilisateurs d'accéder aux ressources nécessaires pour exécuter leurs tâches.

Rôle admin Ensemble unique de capacités pour chaque ensemble d'organisations assigné à un utilisateur administratif.

Rôle informatique L'un des quatre types de rôle disponibles dans Identity Manager, le type Informatique regroupe plusieurs rôles (Matériel, Application et/ou d'autres rôles informatiques imbriqués), de même que des ressources et/ou des groupes de ressources. Dans certaines configurations, les rôles informatiques peuvent être assignés directement à des utilisateurs, mais ils sont généralement attribués à des rôles professionnels, lesquels sont assignés·à des utilisateurs.

Rôle professionnel L'un des quatre types de rôle disponibles dans Identity Manager, le type Professionnel permet d'organiser les droits d'accès en groupes dont se servent les personnes effectuant des tâches semblables au sein d'une organisation. Ce type de rôle se compose d'un ou de plusieurs rôles de type Matériel, rôles de type Application et/ou rôles informatiques. Les rôles professionnels sont conçus pour être assignés directement aux utilisateurs.

Schéma Liste des attributs de compte utilisateur d'une ressource.

Solutionneur Utilisateur Identity Manager spécifié en tant que solutionneur assigné pour une stratégie d'audit.

Lorsqu'Identity Manager détecte une violation de conformité qui requiert une résolution, il crée un élément de travail de résolution qu'il envoie à la liste d'éléments de travail du solutionneur.

Stratégie Établit des limites pour les comptes Identity Manager.

Les stratégies Identity Manager établissent les options relatives aux utilisateurs, aux mots de passe et à l'authentification ; elles sont liées à des organisations ou à des utilisateurs. Les stratégies de mot de passe de ressource et d'ID de compte définissent des règles, des mots autorisés et des valeurs d'attribut ; elles sont liées à des ressources individuelles.

Tâche d'attestation	Collecte logique des examens d'habilitation utilisateur nécessitant une attestation. Les habilitations utilisateur sont regroupées dans une même tâche d'attestation si elles sont assignées au même attestateur et produites à partir de la même instance d'examen d'accès.
Utilisateur	Personne qui possède un compte sur le système Identity Manager. Les utilisateurs peuvent détenir un éventail de capacités dans Identity Manager. Les personnes dotées de capacités étendues sont les *administrateurs* Identity Manager.
Utilisateurs de Service Provider	Utilisateurs de l'extranet ou clients d'un fournisseur de services que l'on distingue du personnel de l'entreprise fournisseur de services ou des utilisateurs de l'intranet.

Index

B

C

D

E

F

G

I

J

L

M

Q

R

S

T

U

V

W

X

Z