Sun Java™ System

Notes de version d'Identity Installation Pack 2005Q4M3

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

N° de référence : 820-4369-10

Table des matières

Ajouts et corrections de la documentation

API désapprouvées

Notes relatives à Identity Installation Pack 2005Q4M3 SP4

Avant d'installer ou de mettre à niveau le logiciel Sun Java™ System Identity Installation Pack, parcourez la section « Remarques sur l'installation et la mise à jour », page 69.

Installation

Utilisez Identity Installation Pack 2005Q4M3 pour installer Sun Java™ System Identity Manager, Sun Java™ System Identity Auditor et Sun Java™ System Identity Manager Service Provider Edition (SPE) dans un nouvel environnement ou en tant que mise à jour.

Vous pouvez mettre à jour Identity Manager, Identity Auditor et Identity Manager SPE à partir d'Identity Manager v5.0 ou de l'un quelconque de ses service packs jusqu'au 5.0 SP6. Si votre version d'Identity Manager est plus ancienne, vous devez commencer par effectuer une mise à jour vers Identity Manager v5.0.

Pour des instructions d'installation du produit détaillées, reportez-vous à *Identity Manager Upgrade* et *Identity Install Pack Installation*.

Remarque La version minimum de Java prise en charge est 1.4.2.

Logiciels et environnements pris en charge

Cette section répertorie les logiciels et les environnements compatibles avec le produit logiciel Identity :

- Systèmes d'exploitation
- Serveurs d'application
- Navigateurs
- Serveurs de bases de données
- Java Runtime Environment
- Sun Identity Manager Gateway
- Ressources prises en charge
- Serveurs Web

Remarque Les développeurs de produits logiciels mettant au point fréquemment de nouvelles versions, des mises à jour et des correctifs pour leurs logiciels, les informations publiées ici changent souvent. Consultez les notes de version pour connaître les nouveautés avant de vous lancer dans l'installation.

Systèmes d'exploitation

- AIX 4.3.3, 5.2, 5L v5.3
- HP-UX 11i v1, 11i v2
- Microsoft Windows 2000 SP3 ou version ultérieure
- Microsoft Windows 2003
- Solaris 8, 9, 10 Sparc et x86d
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Novell SuSE Linux Enterprise Server 9 SP1

Serveurs d'application

Le serveur d'application utilisé avec Identity Manager doit être conforme Servlet 2.2 et installé avec la plate-forme Java incluse (sauf spécification autre ci-après) :

- Apache Tomcat
  - Version 4,1.x (avec JDK 1.4.2)
  - Version 5.0.x (avec JDK 1.4.2)
- BEA WebLogic® Express 8.1 (avec JDK 1.4.2)
- BEA WebLogic® Server™ 8.1 (avec JDK 1.4.2)
- IBM WebSphere® 6.0
- IBM WebSphere® Application Server - Express Version 5.1.1 (avec JDK 1.4.2)
- Sun™ ONE Application Server 7
- Sun Java™ System Application Server Platform Edition 8
- Sun Java™ System Application Server Platform Edition et Enterprise Edition 8.1

Remarque Si votre serveur d'application actuel ne prend pas en charge JDK 1.4.2, consultez le constructeur pour examiner les implications d'une mise à niveau vers un serveur compatible avant d'installer Identity Installation Pack 2005Q4M3 SP4.

Navigateurs

- Microsoft Internet Explorer 5.x et versions ultérieures
- Safari v2.0 (et ultérieures) pour Mac OS X 10.4.2 (et ultérieures)
- Mozilla 1.78 (avec JRE 1.5)
- Firefox 1.04, 1.05, 1.06 (avec JRE 1.5)

Serveurs de bases de données de référentiel

- IBM® DB2® Universal Database pour Linux, UNIX® et Windows® (version 7.x, 8.1, 8.2)
- Microsoft SQL Server™ 2000
- MySQL™ 4.1
- Oracle 9i® et Oracle Database 10g, 10gR1 et 10gR2®

Sun Identity Manager Gateway

Si vous envisagez de configurer des ressources Windows Active Directory, Novell NetWare, Novell GroupWise, Exchange 5.5, Remedy, Lotus Domino ou RSA ACE/Server, installez Sun Identity Manager Gateway.

Ressources prises en charge

Le logiciel d'identité prend en charge les ressources suivantes.

Customer Relationship Management (CRM)

- Siebel 6.2, 7.0.4, 7.7, 7.8

Bases de données

- IBM® DB2® Universal Database pour Linux, UNIX® et Windows® (7.x, 8.1, 8.2)
- Microsoft® Identity Integration Server (MIIS) 2003
- Microsoft SQL Server 2000
- MySQL™ 4.1.x, 5.x
- Oracle® 8i, 9i, 10g Release 1, 10g Release 2
- Sybase Adaptive Server® 12.x

Annuaires

- LDAP v3
- Microsoft® Active Directory® 2000, 2003
- Novell® eDirectory on Novell NetWare 5.1, 6.0
- Open LDAP
- Sun™ ONE Directory Server 4.x
- Sun Java™ System Directory Server 5 2004Q2, 2005Q1

Remarques

- Bien qu'Identity Manager soit testé sur Sun™ ONE Directory Server et Open LDAP, les serveurs LDAP compatibles v3 devraient fonctionner sans changement au niveau de l'adaptateur de ressources.
- Sun Java™ System Directory Server 5 2005Q1 nécessite l'installation d'un patch pour le plug-in Directory Server retro changelog si vous utilisez Active Sync. Ce patch est requis pour la réplication « normale » uniquement (pas pour la réplication MMR).

ERP (Enterprise Resource Planning - planification des ressources)

- Oracle Financials on Oracle Applications 11.5.9, 11.5.10, 12
- Peoplesoft® PeopleTools 8.1 à 8.4.2 avec HRMS 8.0 à 8.8
- SAP® R/3 v4.5, v4.6
- SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
- SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
- SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)
- mySAP ERP ECC 5.0 (SAP 5.0)

Assistance

- Remedy® Help Desk 4.5, 5.0

Plates-formes de messages

- Blackberry RIM Enterprise Server 4+ (utilise un adaptateur de scripts Windows générique)
- Sun Java System Messaging and Calender Service
- Lotus Notes® 5.0, 6.5, 6.5.4 (Domino)
- Microsoft® Exchange 5.5, 2000, 2003
- Novell® GroupWise 5.x, 6.0

Remarque Microsoft Exchange 2000 et 2003 sont gérés par le biais des ressources de Microsoft Windows Active Directory 2000 et 2003.

File de messages

- JMS Message Queue Listener

Systèmes d'exploitation

- HP OpenVMS 7.2
- HP-UX 11.0, 11i v1, 11i v2
- IBM AIX® 4.3.3, 5.2, 5L v5.3
- IBM OS/400® V4r3, V4r5, V5r1, V5r2, V5r3, V5r4
- Microsoft Windows® NT® 4.0
- Microsoft Windows® 2000, 2003
- Generic Windows Script Adapter (utilise Gateway
- Red Hat Linux 8.0, 9.0
- Red Hat Linux Advanced Server 2.1
- Red Hat Linux Enterprise Server 3.0, 4.0
- Sun Solaris™ 8, 9, 10
- SuSE Enterprise 9

Gestionnaires de sécurité

- ActivCard® 5.0
- eTrust CA-ACF2® Security
- Natural
- IBM RACF®
- Scripted Host
- INISafe Nexess 1.1.5
- RSA® SecurID® 5.0, 6.0
- RSA® SecurID® 5.1, 6.0 pour UNIX
- eTrust CA-Top Secret® Security 5.3

Contrôle des accès au Web

- IBM Tivoli® Access Manager 4.x, 5.1
- Netegrity® Siteminder® 5.5
- RSA® ClearTrust® 5.0.1
- Sun™ ONE Identity Server 6.0, 6.1, 6.2
- Sun™ Java System Identity Server 2004Q2
- Sun™ Java System Access Manager 6 2005Q1, 7 2005Q4

Serveurs Web

Remarque L'intégration entre un serveur d'application et un serveur Web n'est pas nécessaire pour Identity Manager. Vous pouvez choisir d'utiliser un serveur Web pour un meilleur équilibrage de charge et une sécurité accrue (par le biais du protocole HTTPS).

- Apache 1.3.19
- iPlanet 4.1
- Microsoft Internet Information Server (IIS) 4.0, 5.0
- Sun™ ONE Web Server 6

Logiciels obsolètes

La prise en charge des packages logiciels suivants, utilisés en tant que serveurs d'application, référentiels de bases de données et ressources gérées finira avec la prochaine version majeure d'Identity Manager. Le support continuera jusqu'à la prochaine version majeure d'Identity Manager. Contactez votre représentant du support client ou le support technique pour toute question relative à la migration vers des versions plus récentes de ces packages.

Serveurs de bases de données

- Oracle 8*i*
- IBM DB2 Universal Database pour Linux, UNIX et Windows 7.0

Systèmes d'exploitation

- Solaris 7

Ressources

- Microsoft Exchange 5.5
- IBM DB2 7.0

Support officiel de l'adaptateur de ressources NT4

Parce que nous nous efforçons continuellement de doter nos dernières versions de fonctionnalités nouvelles ou améliorées, nous devons faire passer en fin de vie (EOL, End-of-life) les versions plus anciennes. Les plans de produits en fin de vie sont liés à l'abandon par Microsoft du support au système d'exploitation NT4. Sun met fin au

support du système d'exploitation NT mais pas au reste des fonctionnalités de l'adaptateur NT. Sun s'engage à continuer à assister les clients utilisant encore le système d'exploitation NT jusqu'à fin 2006.

Prise en charge des API

L'API (Application Programming Interface, interface de programmation d'application)Identity Manager v6.0 inclut toutes les classes publiques (et tout champ ou méthode public ou protégé d'une classe publique) listés dans le tableau suivant.

Type d'API	Noms des classes
Session	com.waveset.msgcat.* com.waveset.util.* com.waveset.object.* com.waveset.exception.* com.waveset.expression.* com.waveset.config.* com.waveset.session.SessionUtil com.waveset.session.ScriptSession com.waveset.session.SessionFactory com.waveset.session.Session com.waveset.session.UserViewConstants
Adaptateur	com.waveset.adapter.* com.waveset.util.Trace
Stratégie	com.waveset.policy.PolicyImplementation com.waveset.policy.StringQualityPolicy
Tâches	com.waveset.task.Executor com.waveset.task.TaskContext
IG	com.waveset.ui.FormUtil com.waveset.ui.util.RequestState com.waveset.ui.util.html.*
Flux de travaux	com.waveset.provision.WorkflowServices com.waveset.session.WorkflowServices com.waveset.workflow.WorkflowApplication com.waveset.workflow.WorkflowContext

Identity Manager SPE inclut en plus les classes publiques indiquées dans le tableau suivant.

Type d'API	Noms des classes
SPE	com.sun.idm.idmx.api.IDMXContext com.sun.idm.idmx.api.IDMXContextFactory com.sun.idm.idmx.auditor.* com.sun.idm.idmx.txn.TransactionPersistentStore com.sun.idm.idmx.txn.TransactionQuery com.sun.idm.idmx.txn.TransactionSummary

Ces classes sont les seules à être officiellement prises en charge. Si vous utilisez des classes qui ne figurent pas dans ces tableaux, contactez le support technique pour savoir s'il est nécessaire de migrer vers une classe prise en charge.

API désapprouvées

La section « API désapprouvées », page 151, dresse la liste de toutes les API d'Identity Manager désapprouvées dans cette version et leurs substituts (le cas échéant).

Fin de vie

Nous nous efforçons de faire évoluer nos produits pour satisfaire aux normes de qualité qu'exigent nos clients. Doter continuellement la dernière version, Identity Manager v6, de fonctionnalités nouvelles ou améliorées, nous oblige amène à donner ici des avis de fin de vie (EOL) pour les versions plus anciennes. Nous vous conseillons d'implémenter sans attendre vos plans de migration pour éviter de travailler sur des versions qui ne font plus l'objet d'un plan de maintenance.

Fin de vie utile (EOSL) pour l'assistance sur le logiciel

Au cours de la période de fin de vie utile, l'assistance est proposée selon deux phases : assistance complète et assistance limitée. La durée de la phase d'assistance complète est variable en fonction du produit. Voir le Tableau 1 ci-dessous pour consulter la liste des phases complètes et limitées par produit.

Phase de support complet

Pendant la phase d'assistance complète, Sun offrira à ses clients l'assistance correspondant au contrat d'assistance entre le client et Sun (y compris la liste de service applicable), comme défini à l'adresse suivante : `http://www.sun.com/service/servicelist/`. Toutefois, dès l'annonce de fin de vie d'un produit logiciel, les clients n'auront plus accès aux mises à jour et aux mises à niveau de ce produit.

Phase de support limité

Pendant la phase d'assistance limitée, Sun offrira à ses clients l'assistance correspondant au contrat d'assistance entre le client et Sun (y compris la liste de service applicable), comme défini à l'adresse suivante : `http://www.sun.com/service/servicelist/`. Toutefois, les clients ne pourront plus soumettre de bogues ni recevoir de nouveaux correctifs de Sun. Comme pendant la phase d'assistance complète, dès l'annonce de fin de vie d'un produit logiciel, les clients n'auront plus accès aux mises à jour et aux mises à niveau de ce produit.

Notes de fin de vie utile pour les produits Identity Manager

Des dates spécifiques sont indiquées ci-après. Veuillez contacter le représentant du support client ou le support technique pour toute assistance pour la planification d'une mise à niveau vers Identity Manager 6.0 (2005Q4M3).

- Identity Manger 2005Q4M3 sera entièrement pris en charge jusqu'au 25 mai 2008, avec un support limité jusqu'au 25 mai 2012.
- Identity Manager 2005Q3M1, qui intègre Identity Manager 5.5 et Identity Auditor 1.5, (et tous les packs de service) bénéficiera d'une assistance complète jusqu'au 11 août 2007, et d'une assistance limitée jusqu'au 11 août 2011.
- Identity Manager 5.0 (et tous les packs de service) bénéficiera d'une assistance complète jusqu'au 11 août 2007, et d'une assistance limitée jusqu'au 11 août 2011.
- Identity Manager 2005Q3M3 sera pris en charge jusqu'en octobre 2006, sans service pack supplémentaire.
- Identity Manager 2005Q1M3 sera pris en charge jusqu'en mars 2006, sans service pack supplémentaire.
- Lighthouse 4.1 (tous service packs inclus) sera pris en charge jusqu'en mars 2006, sans service pack supplémentaire.
- Lighthouse 4.0, SP1 compris, fin du support en septembre 2004.

- Lighthouse 3.1 (tous service packs inclus) fin du support en septembre 2005.
- Lighthouse 2,0 (tous niveaux de patchs inclus) fin du support en mai 2004.
- Lighthouse 1.x (version 1.6 incluse) fin du support en mai 2004.

Identity Installation Pack 2005Q4M3 SP4 - Fonctions

Avant d'installer ou de mettre à niveau le logiciel Sun Java™ System Identity Installation Pack, consultez la section « Remarques sur l'installation et la mise à jour » ainsi que toute la documentation fournie avec le service pack Identity Manager 2005Q4M3 le plus récent.

Nouveautés et défauts corrigés dans cette version

Cette section résume puis détaille les nouveautés d'Identity Installation Pack 2005Q4M3 SP4. Pour de plus amples détails, reportez-vous aux différentes sections de ce chapitre.

Interface administrateur

- Lorsque vous affichez **Tâches du serveur**, la colonne **Heure de début** sous l'onglet **Toutes les tâches** permet dorénavant de trier les éléments selon un ordre chronologique correct. Dans les versions antérieures, la colonne **Heure de début** triait mal les éléments. (ID-16783)
- Lors d'une recherche d'utilisateurs effectuée sur l'onglet **Liste des comptes** (Comptes > Liste des comptes), la fonction de recherche affiche désormais les utilisateurs une seule fois par organisation. Dans les versions antérieures, le même utilisateur figurait à plusieurs reprises dans les résultats de la recherche par organisation. (ID-16795)

  Voir également : la section *Problèmes connus* à la page 24 concernant un problème distinct relatif à la table de l'arborescence des comptes disponible sous l'onglet Liste des comptes.
- Lors des recherches par utilisateur effectuées dans la table de l'arborescence des comptes, l'attribut du responsable de l'utilisateur retourné affiche désormais le nom complet de la personne. Dans les versions antérieures, seul l'ID du responsable de l'employé s'affichait. (ID-14645)
- La colonne **Statut** de la page **Résultats du changement de mot de passe utilisateur** a été supprimée. Elle a également été supprimée des pages suivantes : **Changer les résultats des réponses**, **Changer tous les résultats** et **Résultats du changement de mot de passe**. La colonne **Statut** n'affichait pas de données et n'avait pas d'intérêt particulier. (ID-16889)
- Vous pouvez désormais effacer la valeur de type de champ **DatePicker** sur les formulaires. (ID-17022)

- Le tri de la table **Approbation en cours** fonctionne à présent. Dans les versions antérieures, un utilisateur doté d'approbations en attente ne pouvait pas trier cette table. Le message « Impossible de formater la page des résultats, aucune ID et aucun résultat de tâche » s'affichait à la place. (ID-17304)
- Le composant d'affichage de texte permet dorénavant de générer le rendu `autocomplete="off"` sur des champs d'entrée pour lesquels la propriété d'affichage `autocomplete` a été définie sur `off`. (La définition de la propriété `autocomplete` sur `off` empêche les navigateurs de proposer le stockage des informations d'identification de l'utilisateur sur leur ordinateur.)

  Vous pouvez effectuer cette personnalisation dans XPRESS en ajoutant la propriété d'affichage. L'utilisation de toute autre valeur que `off` empêche la génération de l'attribut de remplissage automatique (autocomplete) (ce qui revient à ne pas définir du tout la propriété). (ID-17045)
- Une vulnérabilité de script intersite a été identifiée et corrigée dans les pages suivantes (ID-17241) :
  - task/taskLaunch.jsp
  - user/processLaunch.jsp
  - user/requestLaunch.jsp

Audit

- Les enregistrements d'audit relatifs à la création de rôles fournissent désormais des informations sur le rôle (dont les ressources assignées, les sous-rôles, les super rôles et les attributs de rôle) dans la section réservée aux **modifications** du rapport d'audit. (ID-16327)

Synchronisation des mots de passe

- Un changement de comportement introduit dans Microsoft Windows Server 2003 SP2 a nécessité la modification de la DLL PasswordSync d'Identity Manager (`lhpwic.dll`). Dans SP2, les notifications de changement de mot de passe envoyées par Windows à PasswordSync peuvent contenir des données de comptes d'ordinateur mal formatées. Cela peut entraîner PasswordSync à émettre une exception. Enfin, cela peut provoquer le blocage du composant LSASS (Local Security Authority Subsystem) de Microsoft, ce qui entraîne le redémarrage du contrôleur de domaine.

Comme les données de comptes d'ordinateur ne sont pas traitées par PasswordSync (seuls les comptes utilisateur sont traités), la DLL PasswordSync a été mise à jour de manière à ignorer toutes les notifications de changement de comptes d'ordinateur dès leur réception.

Les comptes d'ordinateur Windows se terminent par un symbole de dollar américain ($). Par conséquent, vous noterez que PasswordSync ne traitera aucun compte se terminant par un signe $, y compris les comptes utilisateur qui le feraient. (ID-17245)

- Le journal de suivi de PasswordSync a été mis à jour. Lorsque PasswordSync/JMS transmet à Identity Manager une notification de changement de mot de passe provenant de Windows Active Directory et que l'utilisateur n'existe pas dans Identity Manager, le journal de suivi enregistre maintenant un message approprié. Dans les versions antérieures, dans les mêmes circonstances, PasswordSync émettait une exception de pointeur nul sans fournir d'explication. (ID-16920)
- L'initialisation d'un contrôleur de domaine Active Directory en mode « Directory Service Restore » n'entraîne plus de cycle de réinitialisation continu en cas de blocage de PasswordSync (`lhpwic.dll`). (ID-16695)
- PasswordSync a été mis à jour de manière à empêcher les erreurs « ingérables » survenant sur les contrôleurs de domaine Active Directory exécutant PasswordSync (`lhpwic.dll`). Lorsque des comptes d'ordinateur sont mis à jour dans un domaine, le contrôleur de domaine envoie de manière erronée une notification de mise à jour de mot de passe à la DLL PasswordSync d'Identity Manager. Par conséquent, la DLL ne ferme pas correctement les identificateurs de recherche. (ID-16495)

  Voir également : un autre problème relatif à PasswordSync causant des fuites d'identificateurs a été résolu. (ID-16827)

- Une nouvelle entrée de registre Windows génère un fichier de vidage (dump) si la DLL PasswordSync émet une exception.

  Nom de la clé : `dumpFilebase`

  Type : `REG_SZ`

  Cette clé devrait être ajoutée aux contrôleurs de domaine Windows exécutant PasswordSync. Normalement, la clé de registre doit être définie sur le chemin d'accès complet au répertoire où le vidage de la mémoire sera écrit, par exemple : `c:\temp`.

  Si la valeur du registre est définie, chaque fois qu'une exception est détectée lors du traitement des mots de passe, le vidage de mémoire est écrit.

  Remarque : sur le serveur Windows 2000 (avec n'importe quel Service Pack), vous devez également procéder à l'installation dans le répertoire configuré `DbgHelp.dll`, disponible auprès de Microsoft. La version minimale requise de ce fichier est la 5.1. Téléchargez ce fichier à l'adresse :

  `http://www.microsoft.com/whdc/DevTools/Debugging/default.mspx`

  Si le fichier DbgHelp.dll n'est pas installé, aucun vidage ne sera généré sous Windows 2000.

  Les fichiers dump sont nommés suivant ce format :

  `lhpwic-AAAAMMJJ-HHmm-xxxxx.dmp`

  Dans ce nom, `AAAAMMJJ` correspond à la date du fichier dump, `HHmm` à l'heure du fichier dump (au format 24 h) et `xxxxx` au numéro de thread de l'application.

  Vous noterez que les fichiers dump doivent être supprimés manuellement. La taille de ces fichiers peut aller de 20 Mo à plus de 100 Mo, selon la taille du processus LSASS Windows. Au fil du temps, les systèmes dotés d'un espace disque limité peuvent saturer si vous ne supprimez jamais ces fichiers dump. (ID-17552)

Réconciliation

- Lors de la réconciliation, une exception de pointeur nul peut survenir au cours d'une recherche d'ID de compte. Ce problème a été résolu. (ID-17186)

Rapports

- Les événements suivants seront désormais inclus dans les rapports du journal d'audit, notamment le rapport d'activité du jour :
  - Tentatives de création d'un utilisateur doté d'un ID utilisateur ou d'un mot de passe manquant
  - Tentatives de création d'un utilisateur doté d'un rôle inexistant (de même que les tentatives d'assignation d'un rôle inexistant à un utilisateur existant)
  - Tentatives de création d'un utilisateur violant la stratégie d'ID de compte
  - Tentatives de création d'un utilisateur auquel une ressource non accessible est assignée (de même que les tentatives d'assignation d'une ressource non accessible à un utilisateur existant)
  - Tentatives de suppression d'utilisateurs inexistants

  Ces événements seront également consignés dans le journal système.

  Dans les versions antérieures, les tentatives infructueuses de création et de suppression d'utilisateurs étaient uniquement consignées dans le journal système. (ID-13284)

- Identity Manager prend désormais en charge le type de données CLOB pour acctAttrChanges lorsqu'une base de données Oracle est utilisée comme référentiel d'Identity Manager.

  L'avantage de l'utilisation de CLOB (à la place du type de données par défaut VARCHAR(4000)) est que cette solution autorise la consignation d'un ensemble de changements bien plus important ; cela rend cependant cette colonne plus difficile à interroger à cause de la nature propriétaire des routines d'accès de CLOB.

  Pour autoriser un ensemble de changements plus important, vous devez remplacer le type de colonne log.acctAttrChanges par CLOB (depuis VARCHAR(4000)) et ajuster en conséquence l'attribut maxLogAcctAttrChangesLength de l'objet de configuration RepositoryConfiguration. (ID-15326)

Ressources

- L'adaptateur de ressources Solaris oblige dorénavant les utilisateurs à changer leurs mots de passe lors de la connexion suivante. Pour activer cette fonction, ajoutez `expirePassword` à la colonne Attribut utilisateur Identity System de la carte schématique et `force_change` à la colonne Attribut d'utilisateur de ressources. Cet attribut doit être défini sur le type chaîne. (ID-17032, ID-17146)
- L'adaptateur de ressources Oracle a été mis à jour afin de fournir un message d'erreur plus détaillé dans l'éventualité où il pourrait pas ajouter, modifier ou supprimer une responsabilité utilisateur. L'adaptateur dresse désormais la liste des responsabilités qu'il n'a pas pu mettre à jour. (ID-16656)
- L'adaptateur de ressources Sun Access Manager peut désormais se connecter à Access Manager en mode SSL. Dans les versions antérieures, lors du test de la configuration de l'adaptateur de ressources, les administrateurs recevaient une erreur du type « Impossible de créer AuthContext ». (ID-16454)
- La passerelle Microsoft ADSI a été mise à jour. Si une ressource Active Directory est utilisée pour authentifier un utilisateur se connectant à Identity Manager, l'interface graphique d'Identity Manager invite désormais l'utilisateur à changer de mot de passe si son mot de passe Windows a expiré. Dans les versions antérieures, l'utilisateur recevait simplement un message d'erreur l'informant que son mot de passe était arrivé à échéance. (ID-16681)
- La prise en charge de l'accès aux serveurs Remedy a changé. La passerelle ne dépend plus de la version 4.5 des bibliothèques d'API Remedy. Les clients sont désormais obligés de placer les bibliothèques Remedy dans le répertoire de la passerelle. Ces bibliothèques sont disponibles sur le serveur Remedy. (ID-17361, ID-16551)
- Avec ce Service Pack, Identity Manager prend en charge les versions 6.3 et 7.0 de Remedy. Il existe toutefois de nombreuses différences conséquentes entre ces versions au niveau des exemples de données, des valeurs par défaut et de la configuration initiale. Par exemple, le nom du schéma « ticket » est HPD:HelpDesk dans la version 6.3 et HPD:Help Desk dans la 7.0. (ID-17361, ID-14611)
- Lors de la configuration d'une ressource Active Directory, il est désormais possible de spécifier un domaine dans la section des propriétés d'authentification des ressources. Les administrateurs doivent indiquer un domaine dans les environnements multidomaine ou forêts de sorte que seuls les identifiants de connexion soient authentifiés auprès du domaine Active Directory approprié. Si aucun domaine n'est spécifié, un utilisateur peut être bloqué après une seule tentative de connexion échouée. Cela s'explique par le fait que l'utilisateur peut recevoir un échec de mot de passe pour chacun des domaines partageant une relation de confiance avec le domaine principal. (ID-16603)

- Un problème relatif à l'adaptateur de ressources Unix SecurId a été résolu. Avant cette correction, une modification apportée au prénom ou au nom de famille d'un utilisateur entraînait la suppression des groupes auxquels appartenait l'utilisateur au sein de la ressource SecurId. (ID-16914)

Ordonnanceur

- L'ordonnanceur a été mis à jour de manière à masquer la sortie de l'entrée SystemLog (syslog) `'EVNT00', LockedByAnother`. Dans les environnements clusterisés, ce message d'erreur était consigné dans le journal un nombre de fois trop élevé. (ID-15714)
- L'ordonnanceur a été mis à jour de manière à réduire les risques de voir deux instances d'Identity Manager exécutant simultanément le même flux de travaux. Avant cette mise à jour, les environnements clusterisés dotés de plusieurs ordonnanceurs utilisant le même référentiel étaient fragilisés par ce problème. (ID-16500)

Autres défauts corrigés

16382

Problèmes connus

- La table de l'arborescence des comptes disponible via l'onglet **Liste des comptes** (Comptes > Liste des comptes) n'affiche pas la colonne **Responsable**. (Seules les colonnes **Nom**, **Nom de famille** et **Prénom** sont visibles.)

  Pour corriger ce problème, utilisez l'Éditeur de processus métier afin d'éditer l'objet de configuration UserUIConfig.

  Localisez l'élément `<AppletColumns>` et insérez les lignes XML suivantes à la fin de la liste :

  ```
  <Object name='idmManager'>
    <Attribute name='label' value='UI_ATTR_MANAGER'/>
  </Object>
  ```

  Enregistrez vos modifications et redémarrez le serveur d'application. (ID-17710)

- Dans l'interface administrateur, le seul moyen d'annuler une délégation envoyée (**Approbations** > **Déléguer mes approbations**) consiste à définir une date de fin identique à la date de début (ou à une date dépassée). (ID-16790, ID-16799)

- TaskScheduleViewer ne formate pas la date de début selon le format requis pour cette entrée. De ce fait, vous devez corriger la date de début lors de l'édition d'une programmation de tâche. (ID-5675)

- Par défaut, lorsqu'un utilisateur tape la réponse à une question d'authentification, les caractères sont remplacés par des astérisques (*). Toutefois, cette pratique désactive la capacité de certains éditeurs de méthode d'entrée (IME) de créer des caractères complexes, comme ceux utilisés en japonais kanji.

  Pour permettre l'utilisation d'un IME pour répondre aux questions d'authentification, utilisez la page de débogage afin de modifier la valeur de la propriété `secret` sur `false` dans le formulaire utilisateur Question Login Form.

  ```
  <Property name='secret' value='false'/>
  ```

  Remarque : la définition de cette valeur sur false présente un risque de sécurité, car les réponses aux questions d'authentification son désormais lisibles à l'écran. Les réponses sont toujours stockées sous forme chiffrée. (ID-7424)

- Certaines options de configuration disponibles dans l'interface administrateur d'Identity Manager ne sont pas utilisées avec Identity Manager SPE. (ID-10843). Il s'agit entre autres des suivantes :

  - Options de configuration de l'assistant de ressource : exclure les règles de comptes, les approbateurs et les organisations
  - Attributs de rôle

- FireFox 1.5 n'affiche pas correctement certains formulaires d'Identity Manager. Par exemple, dans le formulaire Tabbed User, le navigateur n'intègre pas les étiquettes, ce qui a pour effet de décaler le tout vers la droite. (ID-13109)
- La case « Rapporter seulement les utilisateurs dont nom d'utilisateur » figure deux fois dans les rapports d'utilisateur et des questions utilisateur. L'une des cases possède I-help, mais pas l'autre. Les deux cases, utilisées individuellement, retournent les données correctes. (ID-13155)
- Si la journalisation dans les pages utilisateur final SPE produit une erreur HTTP Status 500, cela peut indiquer qu'il existe plusieurs clés de chiffrement dans la configuration SPE. Ceci peut être provoqué par la création d'une nouvelle dans Identity Manager pendant le processus de mise à niveau.

  La solution consiste à supprimer les clés de chiffrement du répertoire de configuration SPE et de procéder à une nouvelle exportation à partir d'Identity Manager. (ID-13162)
- Lorsqu'une valeur a été définie pour un attribut email d'un utilisateur, elle ne peut pas être supprimée. Il est possible de changer la valeur, mais pas de la redéfinir comme nulle. (ID-13164)
- Si vous modifiez un formulaire de rôle en vue de changer la variable showSuperAndSubRoles de 0 à 1, puis vous importez un fichier de définition d'objet de super rôle contenant des sous-rôles existants à partir de l'onglet Configurer, ces sous-rôles ne contiendront pas la section <SuperRoles>. En revanche, si vous créez un super rôle via l'interface graphique d'Identity Manager, les sous-rôles référencés par ce super rôle seront mis à jour. (ID-15053)

  Ce problème peut se produire avec des rôles créés en dehors d'Identity Manager et disposant de références à des rôles existants (des sous-rôles ou des super rôles) déjà présents sur le système.

  Lors de l'importation de ces rôles, les rôles déjà présents sur le système ne sont pas mis à jour de manière à refléter les nouvelles relations. Ainsi, l'intégrité référentielle n'est pas conservée. Faites appel à la fonction RoleUpdater pour vérifier et corriger l'intégrité référentielle lorsque les rôles sont importés de cette manière.

  Solution : voir ID-15482 décrit à la section « Rôles ».
- Les attributs de verrouillage de Microsoft SQL Server 2000 peuvent provoquer des erreurs d'interblocage dans des conditions de charge extrêmes dans Identity Manager. (ID-16068)

  Solution : mettez à niveau Microsoft SQLServer de la version 2000 vers la version 2005 en mode natif.

  Microsoft SQL Server 2005 (qui dispose d'une nouvelle fonctionnalité appelée *Isolement de captures instantanées*) a été testé avec Identity Manager sous

une charge importante et ne présente pas les mêmes problèmes d'interblocage que SQL Server 2000.

Certains clients ont également trouvé qu'il était pratique de modifier leur base de données de manière à utiliser `READ_COMMITTED_SNAPSHOT` de la manière suivante :

```
ALTER DATABASE dbname SET READ_COMMITTED_SNAPSHOT ON
</quote>
```

- À cause de problèmes d'interopérabilité entre les sources de données WebSphere et les pilotes JDBC Oracle, les clients d'Oracle qui veulent utiliser une source de données WebSphere avec Identity Manager doivent utiliser Oracle 10g R2 et le pilote JDBC correspondant (le pilote JDBC Oracle 9 ne fonctionnera pas avec une source de données WebSphere et Identity Manager). Si vous avez une version d'Oracle antérieure à la version 10g R2 et ne pouvez pas mettre à niveau Oracle vers 10g R2, configurez alors le référentiel d'Identity Manager de sorte qu'il se connecte à la base de données d'Oracle en utilisant le JDBC Driver Manager d'Oracle (et non pas une source de données WebSphere). (ID-16167)

  Pour plus d'informations, reportez-vous à l'URL suivant :

  `http://www-1.ibm.com/support/docview.wss?uid=swg21225859`

- Certains mots de l'onglet de l'écran Édition d'un utilisateur risquent de mal s'afficher en mode plurilingue. (ID-16054)

  Solution : pour vous assurer que les mots des onglets s'affichent correctement, ajoutez ce qui suit à `$WSHOME/styles/customStyle.css` :

```
table.Tab2TblNew td {
background-image:url(../images/tabs/level2_deselect.jpg);
background-repeat:repeat-x;background-position:left top;
background-color:#C4CBD1;
border:solid 1px #8f989f;
white-space:nowrap;
}

table.Tab2TblNew td.Tab2TblSelTd {
border-bottom:none;
background-image:url(../images/tabs/level3_selected.jpg);
background-repeat:repeat-x;background-position:left bottom;
background-color:#F2F4F3;
border-left:solid 1px #8f989f;
border-right:solid 1px #8f989f;
border-top:solid 1px #8f989f;
white-space:nowrap;
}
```

Fonctions précédentes et correction des bogues

Fonctions précédentes

Cette section décrit les fonctions ajoutées aux Service Packs précédents d'Identity Installation Pack 2005Q4M3.

Installation et mise à jour

- Si vous utilisez SQL Server 2000 SP4 comme référentiel et un pilote JDBC de Microsoft, vous devez utiliser le pilote SQL Server 2000 pour JDBC SP3. (ID-9917)
- L'attribut système `waveset.serverId` a été ajouté. Utilisez cet attribut pour définir des noms de serveurs uniques lorsque votre déploiement comprend plusieurs exemplaires d' Identity Manager pointant vers un seul référentiel sur un seul serveur physique. (ID-11578)
- Identity Manager prend désormais en charge Oracle Database 10g Release2® comme référentiel. (ID-12908)
- Le programme d'installation prend dorénavant en charge la mise à niveau d'installations ayant renommé, supprimé ou désactivé le compte Configurator par défaut. Le programme d'installation demande maintenant le nom d'utilisateur et le mot de passe permettant d'importer le fichier update.xml lors du post-traitement. Si le nom d'utilisateur ou le mot de passe saisi est erroné, vous êtes à nouveau invité à le taper (à trois reprises au maximum). L'erreur doit être affichée dans la zone de texte en arrière-plan. (ID-13006)

  Pour effectuer une installation manuelle, vous devez spécifier les indicateurs `-U <nom-utilisateur > -P <mot-de-passe >`afin de passer les informations d'identification à la procédure UpgradePostProcess.
- Identity Manager s'installe correctement sur les machines sans carte graphique. (ID-14258)

Interfaces administrateur et utilisateur

- Les panneaux **Configurer > Serveurs > Modifier les paramètres de serveur/Modifier les paramètres par défaut du serveur** comprennent désormais un onglet Modèles de courrier électronique. Cet onglet contient la variable d'hôte SMTP par défaut/par serveur que tous les modèles d'e-mail possédant la variable `$(smtpHost)` utilisent par défaut. Cet onglet utilise également la variable de configuration de serveur lorsque le champ de l'hôte SMTP est vide. (ID-3574)
- Lorsque vous cliquez sur Réinitialiser la requête dans l'écran Rechercher Utilisateurs, la liste déroulante du nom et la limite des résultats sont dorénavant restaurées dans leur état initial. (ID-8961)
- Les pages Changer le mot de passe d'utilisateur et Réinitialiser mot de passe d'utilisateur dans l'interface administrateur d'Identity Manager contiennent désormais des options de menu pour le type de recherche. Ces options déroulantes comprennent les opérandes **commence avec**, **contient** et **est** pour rechercher les utilisateurs dont le mot de passe doit être changé ou réinitialisé. (ID-8965)
- La page de débogage offre dorénavant les options **export default** et **export all**. Ces options fonctionnent de façon similaire aux options de console, mis à part que celles de la page de débogage n'offrent pas la possibilité de choisir le nom du fichier exporté. Au lieu de cela, Identity Manager crée un fichier intitulé `export<`***`date`***`>.xml` que vous pouvez enregistrer à partir de la page de débogage. (ID-9270)
- L'importation d'un modèle d'e-mail contenant une adresse « cc » est maintenant prise en charge. (ID-9768)
- La page Attributs d'identité comprend désormais une section Mots de passe, laquelle présente le statut de la génération des mots de passe par rapport aux attributs d'identité. Vous pouvez configurer Identity Manager de sorte qu'il assigne des mots de passe aux nouveaux utilisateurs à partir d'une valeur par défaut ou d'une règle, ou au moyen d'une stratégie de comptes du système d'identité générant des mots de passe. (ID-10274, 12560)
- Messages d'erreur révisés associés à l'édition de stratégie. (ID-12187)
- Identity Manager comprend à présent un attribut de responsable par défaut, lequel assure la prise en charge d'une relation responsable-subordonné construite. Ces informations sont stockées sur l'objet utilisateur Identity Manager. Pour plus d'informations à ce sujet, reportez-vous à la section *Ajouts et corrections de la documentation* de ces notes de version. (ID-12416)

- Vous pouvez maintenant configurer des attributs d'identité basés sur les récents changements des ressources (opérations d'édition ou de création). (ID-12678) Si les ressources ont changé depuis le dernier enregistrement des attributs d'identité dans l'interface administrateur d'Identity Manager, la page Attributs d'identité affiche ce message : « Une ou plusieurs ressources ont été modifiées depuis le dernier enregistrement des attributs d'identité. Si ces modifications influent sur les attributs d'identité, elles doivent alors être assimilées via la page Configurer les attributs d'identité à partir des modifications apportées aux ressources. ». Identity Manager fournit un lien vers la page Configurer les attributs d'identité à partir des modifications apportées aux ressources permettant de sélectionner les attributs des cartes schématiques des ressources modifiées devant être utilisés comme source ou cible des attributs d'identité.

  Après l'enregistrement d'une ressource depuis la page de l'assistant Ressources ou Attributs de compte, Identity Manager affiche une page demandant si vous souhaitez configurer les attributs d'identité basés sur les récents changements des ressources. Choisissez **Oui** pour accéder à la page Configurer les attributs d'identité à partir des modifications apportées aux ressources. Choisissez **Non** pour revenir à la liste des ressources.

  Pour désactiver cette page, choisissez **Ne plus me poser cette question**. La page est désactivée en définissant la propriété `idm_showMetaViewFromResourceChangesPage` sur l'utilisateur connecté sur false.
- Les objets à sélection multiple trient à présent les valeurs disponibles lorsque les propriétés `noApplet=true` et `sorted=true` sont définies. (ID-12823)
- Les modifications d'un objet de configuration contenant une liste statique n'ont pas été supprimés par l'arborescence des comptes. Par exemple, les organisation contrôlées par un administrateur ont été déterminées par une règle qui a récupéré une liste statique d'un objet de configuration. Auparavant, le serveur aurait redémarré pour détecter les modifications de l'objet de configuration. Dorénavant, l'arborescence passe en objets de configuration lorsque vous fermez la session avant de vous reconnecter. (ID-14442)
- Il est possible de définir une plage de dates pour le sélecteur de date afin de permettre le choix de certaines dates seulement dans le calendrier. (ID-10100)
- Les modèles de configuration serveur et de modification d'e-mail ont été changés pour permettre à l'administrateur de déterminer si les opérations SSL ou d'authentification doivent être effectuées sur le serveur SMTP. (ID-12465)
- La page continueLogin.jsp affiche le message correctement à présent. (ID-13193)

- Les modifications suivantes ont été apportées à l'EDI (environnement de développement intégré Identity Manager) Identity Manager 7.1 afin d'assurer la prise en charge d'Identity Manager version 2005Q4M3 SP3 : (ID-14089, 15211)
  - Le débogueur d' Identity Manager est maintenant activé par défaut.

    Si vous déployez un environnement de production, il est recommandé de définir la propriété de configuration système sur `serverSettings.default.debugger.enabled=`**`false`**.
  - Le débogueur d'Identity Manager prend dorénavant en charge la définition des points d'arrêt dans les bibliothèques de règles.
  - La synchronisation des mots de passe en mode direct nécessite la configuration de `SimpleRpcHandler` dans le fichier `web.xml`. `SimpleRpcHandler` interfère avec certains appels `RemoteSession`. Si vous n'utilisez pas la synchronisation des mots de passe en mode direct et si vous rencontrez des problèmes avec les appels de type `RemoteSession`, supprimez la configuration `SimpleRpcHandler` du servlet `rpcrouter2` afin de résoudre les problèmes de session distante.

    Modifiez les entrées suivantes dans le fichier `web.xml` ;

    ```
    <init-param>
    <param-name>handlers</param-name>
    <param-
    value>com.waveset.rpc.SimpleRpcHandler,com.waveset.rpc.Passwor
    dSyncHandler</param-value>
    </init-param>
    ```

    en les remplaçant par les suivantes :

    ```
    <init-param>
    <param-name>handlers</param-name>
    <param-value>com.waveset.rpc.PasswordSyncHandler</param-value>
    </init-param>
    ```

    Si vous souhaitez utiliser `RemoteSession` et la synchronisation des mots de passe en mode direct, configurez un servlet distinct pour la gestion des appels `RemoteSession`.
- Un problème qui empêchait le déverrouillage d'un objet d'organisation lorsqu'un utilisateur ayant des droits insuffisants tentait de le supprimer a été résolu. (ID-14942)

Formulaires

- Dans un formulaire, l'utilisation de `<set>` au sein d'`<Expansion>` fonctionne normalement à présent. (ID-9617)
- Les messages relatifs aux règles de vérification s'affichent à présent dans la langue du client et non plus celle du serveur. (ID-12780)

Passerelle

- La passerelle fonctionne désormais sous Windows 2000 SP4 et images vmware Windows 2003 SP1. (ID-12826)

Composants d'affichage HTML

- La classe d'affichage DatePicker possède la nouvelle propriété `strict`. Lorsqu'elle est définie, cette propriété permet la validation des dates entrées manuellement. (ID-11037)
- Vous pouvez maintenant désactiver la régénération forcée du menu Utilisateur final en ajoutant la propriété `doNotRegenerateEndUserMenu` au formulaire End User Menu. (ID-11327)
- Le composant SortingTable respecte à présent les propriétés `align`, `valign` et `width` des composants enfant constituant le tableau lors de la conversion au format HTML. Un composant InlineAlert est également disponible pour afficher des messages d'erreur, d'avertissement, de réussite et d'information dans les formulaires. (ID-12560)
- Le composant treetable prend désormais en charge les colonnes ajustables. Vous pouvez ainsi définir la largeur des colonnes dans les tableaux Liste des utilisateurs et Liste des ressources sur une valeur fixe (exprimée sous forme de pixels ou de pourcentage) au moyen de feuilles de style CSS. Vous avez également la possibilité de redimensionner les colonnes à l'aide de la souris en cliquant et en déplaçant la bordure droite de l'en-tête de colonne voulu. (ID-11474)

Remarque Dans Firefox/Mozilla et autres navigateurs Gecko, redimensionner une colonne peut provoquer la sélection de texte du navigateur. Ceci ne se produit pas avec Internet Explorer ni Safari, car le comportement onselectstart DHTML peut être supprimé.

Identity Auditor

- Il est à présent possible de configurer une stratégie d'audit en vue d'analyser un ensemble limité de ressources. (ID-9127)
- Database Table et Microsoft Identity Information Server utilisent maintenant les formulaires personnalisés spécifiés pour ces deux ressources. (ID-10302)
- Le titre Rapport d'accès utilisateur s'affiche correctement. (ID-11538)
- La tâche de balayage d'accès fonctionne maintenant sur les organisations dynamiques. (ID-12437)

- Vous pouvez définir l'option d'affichage utilisateur CallViewValidators (UserViewConstants.OP_CALL_VIEW_VALIDATORS) sur « true » ou sur false » pour activer ou désactiver respectivement le contrôle de stratégie d'audit pendant le provisioning. (ID-12757)
- Le processus de mise à niveau n'efface plus le modèle d'e-mail Avis de vérification d'accès (ID-13216)

Identity Manager SPE

Identity Manager SPE 2005Q4M3 SP1 introduit les nouvelles fonctions suivantes. Pour des informations détaillées sur ces fonctions, voir *Identity Manager Service Provider Edition Administration Addendum* et *Identity Manager SPE Deployment*.

Amélioration des pages de l'utilisateur final

Des pages de l'utilisateur final améliorées sont désormais disponibles. Les pages d'exemple comprennent les fonctions suivantes :

- Connexion (et déconnexion) incluant l'authentification via des questions de repêchage
- Enregistrement et inscription
- Changement de mot de passe et de nom d'utilisateur
- Édition des questions de repêchage et de l'adresse de notification
- Traitement des mots de passe et noms d'utilisateur oubliés
- Notification par e-mail
- Audit

Les pages peuvent être personnalisées pour votre déploiement. Vous pouvez personnaliser les éléments suivants :

- Marquage
- Options de configuration (par exemple, le nombre de tentatives de connexion ayant échoué)
- Ajout et suppression de pages

Stratégie relative au mot de passe et à l'ID de compte

Il existe maintenant des stratégies d'ID de compte et de mot de passe pour Identity Manager SPE et les comptes de ressources. Ces stratégies sont implémentées avec la même infrastructure stratégique qu'Identity Manager. (ID-12556)

Coexistence d'Active Sync et d'Identity Manager SPE Sync

Vous pouvez à présent exécuter Active Sync et SPE Synchronization sur le même serveur Identity Manager. Cependant, n'exécutez pas les deux sur la même ressource. (ID-12178)

Répertoires utilisateur LDAP et Configuration séparés

Les informations relatives à l'utilisateur et à la configuration peuvent maintenant être stockées dans des instances distinctes de LDAP. Ces instances sont sélectionnées au cours de la configuration initiale. (ID-12548)

Intégration d'Access Manager

Vous pouvez désormais utiliser Sun Java System Access Manager 7 2005Q4 pour l'authentification dans les pages utilisateur final d'Identity Manager SPE. Access Manager vérifie que seuls les utilisateurs authentifiés peuvent accéder aux pages utilisateur final.

Autres corrections

- Identity Manager SPE reprend à présent le traitement des transactions après l'arrêt brutal du service (par exemple, lorsque le serveur d'application se ferme suite à un manque de mémoire). (ID-14579)
- Les transactions Identity Manager SPE prennent désormais en charge les niveaux de cohérence des mises à jour d'utilisateurs configurables. Les bases de données de stockage des transactions existantes doivent être modifiées et comprendre une colonne supplémentaire, `userId VARCHAR(N)` où `N` est suffisamment grand pour contenir la longueur maximale attendue pour un DN utilisateur Identity Manager SPE, suivi de 8 caractères supplémentaires. Ce changement apporté à la base de données ne se produit pas automatiquement lors de l'exécution des scripts de mise à niveau. (ID-13830)

Localisation

- Les clés de message servant de questions d'authentification s'affichent correctement à présent sur la page des résultats. (ID-13076)

Journalisation

- Les événements Active Sync sont maintenant enregistrés dans le journal système. (ID-12446)
- Les changements de questions d'authentification de l'utilisateur sont maintenant enregistrés dans les journaux d'audit. (ID-13082)
- Les sous-appels par méthode directe ou indirecte peuvent désormais être suivis. (ID-13436) Cette fonction peut être utile pour déboguer des problèmes connus pour survenir à un niveau inférieur à une méthode d'entrée spécifique. Pour activer cette fonction, définissez le niveau pour une étendue avec le modificateur`subcalls`, comme dans l'exemple suivant :

  ```
  trace 4,subcalls=2
  com.waveset.recon.ReconTask$WorkerThread#reconcileAccount
  ```

  La méthode `reconcileAccount()` est ainsi suivie au niveau 4 et tous les sous-appels au niveau 2.
- Les erreurs qui surviennent dans Scheduler sont maintenant écrites dans le journal système, au lieu d'être conservées dans l'objet TaskSchedule. (ID-14261)

Réconciliation

- La définition de la tâche de fin de notification de réconciliation se termine correctement lorsqu'elle est spécifiée comme flux de travaux de post-réconciliation (ID-9259)
- Lorsqu'il existe un grand nombre d'objets Compte (dont la création résulte des réconciliations et des provisions), les performances de réconciliation et de provisioning peuvent diminuer considérablement.

  Pour corriger ce problème, un index doit être créé dans la colonne du nom de la table du compte dans le référentiel. Certains scripts qui y contribuent sont fournis dans le répertoire d'exemples. Le `account_index.sqlserver` s'applique à Microsoft SQL Server, le `account_index.sql` à toutes les autres bases de données. (ID-14478)

Rapports

- Identity Manager crée dorénavant des événements d'audit lorsque des capacités sont créées et modifiées. (ID-9734).
- Identity Manager offre maintenant une nouvelle option de rôles nommée dans le champ **Select which Identity Manager attributes you would like to display for each user**. La sélection de cette option pour les rapports nouveaux et existants a pour effet d'afficher une liste séparée par des virgules des rôles du rapport. (ID-9777)
- Vous pouvez maintenant spécifier la liste des attributs à afficher dans leur propre colonne dans les rapports CSV et PDF. Si vous ne spécifiez pas de liste, tous les attributs sont affichés dans une seule colonne intitulée Attributs auditables. (ID-10468)
- Par défaut, les rapports suivants sont automatiquement étendus à l'ensemble des organisations contrôlées par l'administrateur connecté, à moins que ce comportement soit explicitement réduit à une ou plusieurs organisations spécifiques pour lesquelles le rapport doit être exécuté : (ID-12116)
  - Récapitulatif de rôle admin
  - Récapitulatif administrateur
  - Récapitulatif de rôle
  - Récapitulatif des questions utilisateur
  - Récapitulatif utilisateur

  Pour prendre cette fonction en charge, le composant d'étendue de l'organisation, qui était un simple composant de `sélection` est devenu un composant `à sélection multiple`.
- Deux nouveaux rapport soutiennent l'introduction de l'assistance intégrée pour les relations responsable-employé : Résumé de mes subordonnés directs, Résumé de mes employés directs, Résumé de mes employés directs et indirects et Mes subordonnés directs. (ID-12416, ID-12689)
- Le rapport d'utilisateur de ressources génère maintenant les fichiers CSV et PDF correctement. (ID12509, 13701)
- La consignation dans des journaux d'audit est désormais prise en charge pour la création, la modification et la suppression de rôles admin. (ID-12514)
- Le rapport utilisateur contient maintenant un attribut de recherche pour faciliter l'exécution d'un rapport en fonction du responsable de l'utilisateur. (ID-12689)

- Les rapports utilisateur indiquent maintenant l'ID de compte de tous les comptes de la ressource dans une liste séparée par des points-virgules. (ID-12820). Les comptes et les ressources indirectement assignés, via un rôle ou un groupe de ressources, sont également indiqués. Lorsqu'il n'existe qu'un seul compte de ressource, l'ID de compte n'est affiché que s'il diffère de celui d'Identity Manager.
- Les noms des colonnes sont maintenant correctement affichés dans les rapports PDF. (ID-12794)
- La génération de noms `TaskTemplate` trop longs (dépassant la valeur MAX_NAME_LENGTH) a été corrigée. (ID-13790)

Référentiel

- Identity Manager prend désormais en charge Oracle Database 10g Release2® comme référentiel. (ID-12908)
- SQL Server 2005 est désormais pris en charge en tant que référentiel. (ID-14755). Pour utiliser cette version de SQL Server, procédez comme suit :
  1. Téléchargez le pilote JDBC de SQLServer 2005 (version 1.2) à partir du site Web de Microsoft.
  2. Archivez la version antérieure du pilote, située dans le répertoire `$WSHOME/WEB-INF/lib`. Remplacez ensuite l'ancienne version par le pilote `sqljdbc.jar` dans le même répertoire.
  3. Vérifiez le script de création de la base de données. Lors de la création de la base de données, vous pouvez ne plus placer lignes dans un commentaire :

```
ALTER DATABASE dbname SET READ_COMMITTED_SNAPSHOT ON
GO
```

     Pour plus d'informations sur ce paramètre, consultez la documentation de SQLServer 2005.

  4. Lors de la définition du référentiel avec la commande lh setup ou lh setRepo, utilisez les paramètres suivants :

```
type = SQLServer
jdbc driver = com.microsoft.sqlserver.jdbc.SQLServerDriver
url = jdbc:sqlserver://NomMachine:Port;DatabaseName=waveset
```

     Remplacez le nom de la machine et le port par des paramètres valables dans l'URL.
- Le référentiel IDM s'initialise plus rapidement à présent. (ID-14937)

Ressources

Nouvelles ressources

La prise en charge des ressources suivantes a été ajoutée depuis Identity Manager 2005Q4M3 : Pour plus de détails, voir *Addenda aux références des ressources d'Identity Manager*.

- HP OpenVMS (ID-8556)
- BridgeStream SmartRoles (ID-12262)
- SE/400 v4r5, v5r2, v5r3, et v5r4 (5.2, 5.3, et 5.4).
- Shell Script (ID-11906, ID-9866)
- JDBC sous forme de script (ID-7540)
- Siebel 7.8
- Prise en charge de domaines par Sun Java System Access Manager (ID-12414)

Généralités

- Identity Manager prend désormais en charge le stockage d'attributs de comptes binaires. Les adaptateur suivants prennent cette fonction en charge : (ID-8851, 12665)
  - Active Directory
  - LDAP
  - Active Sync fichier plat
  - Database Table
  - JDBC sous forme de script
  - Services de communications Sun Java System

  Active Directory prend désormais en charge les attributs binaires `thumbnailPhoto` (Windows 2000 Server et supérieur) et `jpegPhoto` (Windows 2003). Les autres adaptateurs prennent en charge des attributs tels que `jpegPhoto`, `audio` et `userCertificate`.

  Identity Manager émet une exception lorsque vous tentez d'envoyer des attributs binaires ou complexes à une ressource qui ne les prend pas en charge.

  Les attributs binaires doivent être aussi petits que possible. Si vous chargez un attribut binaire trop grand (par exemple 200 Ko), vous pouvez rencontrer un message d'erreur indiquant que vous avez dépassé la taille maximale de paquet autorisée. Contactez le support client si vous souhaitez des recommandations pour gérer des attributs de grande taille.

- Les agents adaptateurs de ressources offrent désormais une ressource optionnelle qui prend en charge la rétention des connexions pendant les opérations de bloc : RA_HANGTIMEOUT. Cet attribut spécifie la valeur du délai d'attente, en secondes, avant qu'une demande vers la passerelle arrive à échéance et soit considérée comme bloquée. La valeur par défaut est 0, et indique de ne pas rechercher les connexions bloquées. (ID-12455)
- Les modifications d'objets AttrParse peuvent à présent prendre effet sans redémarrer Identity Manager. (ID-12516)
- Les performances d'`AttrParse` ont été améliorées. L'analyse standard n'émet plus ni ne saisit d'exception pour chaque caractère compris dans un tampon analysé. (ID-13384)
- Identity Manager prend désormais en charge les connexions aux ressources de mainframe via la bibliothèque Attachmate Reflection for the Web Emulator Class Library. Pour plus d'informations sur la configuration de cette fonction, reportez-vous à la section *Ajouts et corrections de la documentation* de ces notes de version. (ID-14815)

Active Sync

- L'assistant Active Sync est plus complètement internationalisé à présent. (ID-10504)
- Le système prend désormais en charge les tentatives répétées d'Active Sync sur une ressource. Pour activer cette fonction, mettez à jour le fichier XML de la ressource de sorte qu'il comprenne deux attributs de ressource supplémentaires du formulaire :

  ```
  <ResourceAttribute name='syncRetryCountLimit' type='string'
  multi='false' facets='activesync' value='180'/>
  <ResourceAttribute name='syncRetryInterval' type='string'
  multi='false' facets='activesync' value='10000'/>
  ```

  `syncRetryCountLimit` correspond au nombre tentatives répétées de mise à jour et `syncRetryInterval` désigne l'intervalle de temps à attendre (en millisecondes) entre deux tentatives. Ces valeurs s'afficheront comme paramètres de ressource personnalisés lors de la configuration d'Active Sync. Il est conseillé de spécifier un nom d'affichage au moyen d'une clé de catalogue personnalisée si la localisation est voulue. (ID-11255)
- Le nombre maximum de journaux Active Sync configurés sur une ressource Active Sync est désormais reconnu correctement. (ID-11848)

Domino

- Vous pouvez créer un utilisateur Domino sans fichier ID ni adresse e-mail, mais avec une entrée seulement dans le répertoire Domino. (ID-11201)
- Vous pouvez désormais désactiver les comptes sans fournir de liste des groupes refusés dans les ressources Domino 6.x. Lorsqu'aucun groupe refusé n'est spécifié, Identity Manager utilise l'attribut CheckPassword pour activer et désactiver sur la ressource Domino. La valeur 2 désactive le compte. (ID-12088)
- Pour l'adaptateur de ressources Domino, les mises à jour simultanées de HTTPPassword pour plusieurs utilisateurs disposant de l'appel d'API `NSFNoteComputeWithForm()` ne génèrent plus d'erreur de passerelle de type -551. (ID-12466)

Annuaire

- Identity Manager offre désormais un mécanisme plus évolutif pour éditer les grands attributs d'objet ressource à liste de valeurs. Des exemples de formulaire pour utiliser cette approche pour gérer les groupes LDAP sont fournis dans `sample/forms/LDAPgroupScalable.xml`. (ID-9882)
- L'adaptateur de ressource LDAP utilise désormais directement JSSE Provider. (ID-9958) La version minimale de Java prise en charge dans Identity Manager est désormais 1.3, ce qui permet d'utiliser les prestataires de services de sécurité extérieurs pour la communication SSL dans le cas des adaptateurs de ressources Domino, LDAP et NDS SecretStore. Vous pouvez enregistrer des bibliothèques de prestataires de services de sécurité extérieurs à l'aide du fichier java.security standard.

  Pour plus d'informations, voir http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html#ProviderInstalling
- Vous pouvez désormais éditer les groupes LDAP dont les noms contiennent des barres obliques avant. (ID-9872)

  L'attribut de configuration `ldapJndiConnectionFactory.alwaysUseNames` a été ajouté au fichier `Waveset.properties`.

  Cette propriété est activée par défaut. Lorsqu'elle est activée, tous les noms de chaîne sont analysés dans un nom utilisant le NameParser du contexte. Ceci contribue à éviter les problèmes d'échappement JNDI. Cette option n'est utile que si l'option `ldapJndiConnectionFactory.wrapUnpooledConnections` est définie sur true.

Le relais sur la valeur par défaut (true) ou la définition explicite de cette valeur sur true nécessite la version 1.4 ou supérieure de JVM. En raison d'un problème avec JNDI, certaines opérations Renommer peuvent échouer dans des versions antérieures de machines virtuelles JVM lorsque cette option est activée.

- L'adaptateur LDAP ne crée plus de nom distinctif (DN) erroné pour les nouveaux comptes. (ID-10951)

  La méthode d'échappement de `com.sun.idm.util.ldap.DnUtil` est également applicable aux formulaires pour neutraliser les valeurs à insérer dans les modèles d'identité des adaptateurs de ressources au format DN LDAP. Autre solution possible, l'utilisation d'une stratégie accountId avec l'option « Requérir le format DN LDAP » cochée pour valider les noms distinctifs LDAP insérés dans Identity Manager par entrée (entrée utilisateur, ActiveSync et réconciliation, par exemple).

- La valeur par défaut de l'attribut **Objectclasses to synchronize** d'Active Sync sur les ressources LDAP est désormais définie sur inetorgperson. (ID-11644)

- Le filtre de recherche `LDAPActiveSync` destiné à détecter les modifications dans le journal changelog a été optimisé au niveau des performances. La partie filtre (`objectClass=changelogEntry`) a été supprimée du filtre de recherche par défaut. (ID-11722)

  Vous avez la possibilité de restaurer l'ancien comportement en ajoutant directement l'attribut de ressource **Remove objectClass from Search Params Filter** à la définition de la ressource en utilisant la valeur false de la manière suivante :

  ```
  <ResourceAttribute name='Remove objectClass from Search Params
  Filter' displayName='Remove objectClass from Search Params
  Filter' facets='activesync' value='false'>
  </ResourceAttribute>
  ```

  Remarque : il est impossible de modifier ce paramètre depuis l'interface graphique (IG).

- Le changement d'appartenance à un groupe LDAP utilise à présent des ajouts et retraits individuels au lieu de réécrire intégralement le groupe (c.-à-d., remplacer entièrement l'attribut uniqueMember). (ID-13035)

- Il est possible de configurer l'adaptateur LDAP de sorte qu'un tri VLV est effectué sur une valeur autre que `uid`. (ID-13321). Pour modifier cette valeur, ajoutez ce qui suit à la définition de la ressource :

  ```
  <ResourceAttribute name='vlvSortAttribute' displayName='VLV Sort
  Attribute' description='VLV Sort Attribute'
  value='myValue'></ResourceAttribute>
  ```

- L'attribut `PasswordNeverExpires` d'Active Directory peut désormais être défini lors d'une mise à jour. (ID-13710)

- L'adaptateur NDS Active Sync n'interroge plus les changements fondés sur lastModifiedTimeStamp de l'objet utilisateur. Cet attribut était auparavant mis à jour dès qu'un utilisateur se connectait ou se déconnectait. Pour surmonter ce problème, la dernière valeur modifiée est maintenant calculée sur la base lastModifiedTimestamp des attributs d'un utilisateur définis dans la carte schématique. Lorsque la valeur lastModifiedTimestamp d'un attribut est supérieure à la marque maximale présentée par l'adaptateur, la passerelle renvoie cet utilisateur au serveur comme modifié.(ID-13896)
- Un problème qui empêchait les utilisateurs NDS récemment créés d'accéder à leur répertoires de base a été corrigé. (ID-14208)
- Les délais d'attente de récupération des données Active Directory ne provoquent plus la fin prématurée des réconciliations.(ID-14564)
- Un problème qui provoquait le blocage de l'adaptateur Active Directory Active Sync en raison des connexions à la passerelle restant ouvertes a été corrigé. (ID-14597)
- L'adaptateur LDAP permet au raccourci d'activation `nsaccountlock` d'utiliser une logique basée sur la présence/absence d'une valeur pour déterminer si un utilisateur LDAP est désactivé. (ID-14925) Consultez la section *Ajouts et corrections de la documentation* de ces notes de version pour des informations plus détaillées.

Oracle ERP

- Plusieurs attributs ont été ajoutés à l'adaptateur Oracle ERP afin de prendre en charge les fonctions d'audit. (ID-11725) Consultez la section *Ajouts et corrections de la documentation* de ces notes de version pour des informations plus détaillées.
- L'adaptateur Oracle ERP n'échoue plus pour fermer les curseurs de base de données Oracle. Auparavant, ce défaut provoquait l'erreur suivante : (ID-12222)
- Dans les formulaires pour les adaptateurs Oracle ERP, la méthode `listResourceObjects` dans la classe `com.waveset.ui.FormUtil` peut maintenant retourner les responsabilités spécifiques d'un utilisateur et être filtrée pour retourner toutes les responsabilités ou seulement les responsabilités actives. (ID-12629)

  Les options intégrées sont :

  - `key id` - (chaîne) Identifie l'identité de la ressource dont les responsabilités sont retournées.
  - `activeRespsOnly` - (chaîne) true ou false. Cette valeur est fausse par défaut lorsqu'elle n'est pas envoyée.

- L'adaptateur Oracle ERP offre maintenant un mot-clé `sysdate` ou `SYSDATE`. Vous pouvez utiliser ce mot clé avec `to_date` pour spécifier une date d'expiration pour une responsabilité avec l'heure locale d'un serveur Oracle E-Business Suite (EBS). (ID-12709)
- L'adaptateur Oracle ERP d'Identity Manager offre maintenant un nouvel attribut de compte `employee_number`. Cet attribut représente un `employee_number` issu du tableau `per_people_f`. Consultez la section *Ajouts et corrections de la documentation* de ces notes de version pour des informations plus détaillées. (ID-12710).
- La mise à jour d'une responsabilité de compte Oracle ERP en utilisant l'adaptateur Oracle ERP n'entraîne plus la mise à jour des autres responsabilités associées au compte. (ID-13889) Par conséquent, seul l'horodatage d'audit Oracle ERP de la responsabilité modifiée est mis à jour. Les horodatages d'audit Oracle ERP des autres responsabilités du compte demeurent inchangées.
- L'attribut de compte person_fullname a été ajouté à la carte schématique pour l'adaptateur Oracle ERP. Dans le formulaire utilisateur Oracle ERP, cet attribut sert à afficher le champ indiquant le nom de la personne. Ce champ est en lecture seule et affiche le nom complet de l'utilisateur lorsqu'un compte Oracle ERP est lié au système Oracle HR utilisant le numéro d'employé. (ID-14675)
- L'adaptateur Oracle ERP empêche dorénavant de supprimer les liens des comptes de ressource si la ressource Oracle ERP est inaccessible lors de la réconciliation complète. (ID-14960) (La ressource peut être inaccessible pour de nombreuses raisons, notamment une configuration de connexion incorrecte.)
- L'adaptateur Oracle ERP prend désormais en charge Oracle E-Business Suite 12. Pour plus d'informations à ce sujet, reportez-vous à la section *Ajouts et corrections de la documentation* de ces notes de version. (ID-15062, 16705)
- L'attribut de compte `npw_number` a été ajouté à l'adaptateur Oracle ERP afin de prendre en charge les comptes de travailleurs contingents. (ID-16507)

SAP et SAP HR

- Vous pouvez maintenant configurer l'adaptateur SAP HR pour traiter les IDOC de tout type de message. Précédemment, seuls les IDOC de type HRMD_A pouvaient être traités. (ID-12120)

  ```
  ORA-01000: nombre maximum de curseurs ouverts dépassé
  ```

- Les adaptateurs SAP et SAPHR offrent à présent trois nouveaux attributs de ressources dotés des paramètres permettant d'effectuer une nouvelle tentative d'opération SAP suite à une panne de réseau. (ID-12579) Il s'agit des attributs :
  - SAP BAPI Retry Count – Nombre de nouvelles tentatives de l'opération

  - SAP Connection Retry Count - nombre de nouvelles tentatives de reconnexion au serveur SAP.
  - SAP Connection Retry Wait Time - nombre de millisecondes d'attente avant de tenter une reconnexion au serveur SAP.
- Les mots de passe peuvent maintenant être définis comme non expirés en utilisant le mode CUA sur une ressource SAP. (ID-13355)
- L'adaptateur SAP n'émet plus une exception JCO_ERROR_FUNCTION_NOT_FOUND lorsque le système SAP ne contient pas le module de fonction PASSWORD_FORMAL_CHECK. (ID-14663)
- L'adaptateur SAP rapporte correctement à présent l'état des comptes désactivés. (ID-14834)
- Les profils et les groupes (rôles) d'activité faisant partie d'un environnement peuvent désormais être mis à jour avec une date de début et une date de fin. (ID-15613)

  En ce qui concerne les rôles, mappez l'attribut `activityGroups` de l'adaptateur à :

  `CUA->directLocalActivityGroupObjects`

  En ce qui concerne les profils, mappez « `profiles` » à :

  `CUA->directLocalProfileObjects`
- L'adaptateur SAP prend maintenant en charge la mise à jour du champ ALIAS dans SAP. Le mappage des attributs dans la configuration schématique est ALIAS->USERALIAS. (ID-16320)

UNIX

- Les adaptateurs UNIX contiennent maintenant un attribut de ressource Répertoire de base. Lorsqu'il est présent, cet attribut remplace le paramètre du répertoire de base de la ressource native pour le compte en cours de création. Ce paramètre est la valeur définie pour cet attribut annexée à `accountID`. Si vous définissez le répertoire de base de l'utilisateur dans les attributs du compte, ce paramètre prend le pas sur le répertoire de base. (ID-8587)
- Vous pouvez maintenant définir des valeurs de délai d'attente par défaut via la stratégie de type de ressources. En outre, vous pouvez aussi utiliser la propriété `maxWaitMilliseconds` pour contrôler la fréquence d'interrogation que l'adaptateur sous forme de script d'Identity Manager utilise en attendant que la ressource termine une tâche. (ID-11906)
- Les adaptateurs Solaris et Linux renvoient désormais des informations sur la dernière connexion remontant à une année. (ID-12182)

- Lors de l'affichage des informations de compte depuis une ressource Solaris configurée avec NIS, les informations d'appartenance à un groupe sont affichées avec le nom du groupe, au lieu de l'ID numérique du groupe. (ID-12667)
- Deux attributs de ressources, Groupe principal par défaut et Shell de connexion, ont été ajoutés aux adaptateurs de ressources Solaris, AIX, HP-UX, Red Had Linux et SuSE Linux. (ID-15034)

Autres adaptateurs

- L'adaptateur de ressources RACF vous permet désormais de contrôler directement les règles des jeux de données au lieu de laisser Identity Manager les administrer. Cela vous permet de créer des règles de jeux de données différentes des règles natives d'Identity Manager. (ID-10446)

  L'exemple de règle « après création » suivant définit une règle de jeu de données `<ID utilisateur>.test1.**` à la place de la valeur par défaut d'Identity Manager (`<ID utilisateur>.**`).

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE ResourceAction PUBLIC 'waveset.dtd' 'waveset.dtd'>
<ResourceAction name='create after action'>
  <ResTypeAction restype='RACF'>
    <act>
      var TSO_PROMPT = " READY";
      var TSO_MORE = " ***";
      var cmd1 = "addsd '"+identity+".test1.**'
owner('"+identity+"')[enter]";
      var result1 = hostAccess.doCmd(cmd1, TSO_PROMPT, TSO_MORE);
    </act>
  </ResTypeAction>
</ResourceAction>
```

- L'adaptateur RACF prend maintenant en charge les filtres de recherche pour `listAllObjects`. (ID-10895)
- Vous pouvez désormais créer et mettre à jour des objets qui nécessitent une navigation dans le composant professionnel parent/enfant dans Siebel. Reportez-vous à la section *Ajouts et corrections de la documentation* dans ces notes de version pour des informations plus détaillées. (ID-11427)
- La méthode `isPickListAttribute` de l'adaptateur Siebel n'est plus mal identifiée comme `isMVGAttribute` dans le système de suivi. (ID-11471)
- Pour les ressources SecurId, l'attribut du client est maintenant traité comme un attribut optionnel. (ID-11509)
- L'adaptateur Active Sync fichier plat fournit à présent un message d'avertissement dans le journal Active Sync (si activé) chaque fois qu'une erreur empêchant l'exécution d'une action `diff` à des fins de synchronisation se produit. (ID-12484)

- Si vous configurez Identity Manager pour provisionner vers une ressource RSA Clear Trust 5.5.2, aucune bibliothèque supplémentaire n'est nécessaire pour les communications SSL comme avec les versions précédentes de Clear Trust. (ID-12499)
- L'assistant Database Table ne permet plus de configurer des tables inaccessibles. (ID-12643)
- L'adaptateur LDAP Siteminder effectue à présent correctement les opérations suivantes, même lorsque l'utilisateur Siteminder est verrouillé suite à l'échec de ses tentatives de connexion :
  (ID-12824)
  - activer
  - désactiver
  - expiration du mot de passe (avec activation/désactivation)
  - non expiration du mot de passe (avec activation/désactivation)
- L'adaptateur RACF ne recherche plus une chaîne longue pour chaque utilisateur récupéré dans `listAllObjects`, ce qui augmente généralement les performances de cette fonction dans le cas d'un nombre important d'utilisateurs. (ID-12829)
- Les tablespaces temporaires ne respectent pas les paramètres de quota et génèrent une exception SQL s'ils sont tentés à partir d'Oracle 10gR2. (ID-12843)

  Jusqu'à présent, l'adaptateur de ressources définissait un quota sur un tablespace temporaire, même lorsque l'attribut de compte oracleTempTSQuota n'était pas mappé. Ce comportement a changé. Dorénavant, si vous mappez l'attribut oracleTempTSQuota, l'ancien comportement est conservé (pas de changement), mais si vous supprimez le mappage, aucun quota n'est plus défini pour le tablespace temporaire.

  Sur les ressources Oracle 10gR2, supprimez l'attribut oracleTempTSQuota de l'adaptateur de ressources.
- Le cas échéant, Identity Manager efface les privilèges admin avant de tenter de supprimer un utilisateur à ID sécurisé. (ID-13053)
- Un problème rencontré en effectuant une réconciliation sur VMS a été corrigé. (ID-13425)
- Le SecurID de l'adaptateur UNIX effectue désormais le codage et le décodage de caractères UTF-8 lors d'opérations avec RSA. (ID-13451)
- L'adaptateur Shell Script peut maintenant détecter les erreurs générées depuis une ResourceAction au cours des fonctions de création et de mise à jour utilisateur.(ID-13465)

- Lors de la création d'un compte sur une ressource Windows NT via l'adaptateur de ressources Windows NT, un message d'erreur du type suivant ne s'affiche plus sur la page des résultats de la création d'un utilisateur : « Erreur lors de la requête de mot de passe : put_PasswordRequired(): 0X80004005:E_FAIL ». (ID-13618)
- Un nouveau paramètre de configuration de ressource, enableEmptyString, a été ajouté à l'adaptateur Database Table pour permettre l'écriture d'une chaîne vide, au lieu d'une valeur NULLE, dans les colonnes de caractères définies comme non nulles dans le schéma du tableau. Cette option n'influence pas la façon dont les chaînes sont écrites pour les tableaux Oracle. (ID-13737)
- L'adaptateur Shell Script prend maintenant en charge les fonctions renommer, désactiver et activer. (ID-14472)
- L'adaptateur JDBC sous forme de script met à jour correctement un attribut dans lequel la valeur d'origine était nulle mais qui est définie comme une valeur non nulle. (ID-14655)

Rôles

- Les rôles et groupes de ressources offrent désormais la possibilité (seuls ou à plusieurs) d'assigner à des utilisateurs plusieurs comptes sur une ressource. Consultez la section *Ajouts et corrections de la documentation* de ces notes de version pour des informations plus détaillées. (ID-6684)
- Lorsque vous importez des rôles contenant des liens pointant vers des super rôles existants, Identity Manager met dorénavant à jour les rôles existants avec des liens renvoyant aux rôles que vous venez d'importer. (ID-15482)

  Identity Manager détecte et crée des liens à partir de super rôles existants jusqu'aux sous-rôles qui y font référence. Lors des mises à niveau, Identity Manager appelle la classe RoleUpdater utilisée pour réparer les rôles.

  Vous pouvez mettre à jour les rôles en dehors du processus de mise à niveau en important un nouveau fichier RoleUpdater.xml disponible dans sample/forms/RoleUpdater.xml. Par défaut, Identity Manager ajoute les liens de sous-rôles lors de la mise à niveau ou lors de l'importation du fichier RoleUpdater.xml.

  Pour désactiver cette nouvelle fonctionnalité, définissez l'attribut `nofixsubrolelinks` de RoleUpdater sur true. Par exemple :

  ```
  <MapEntry key='nofixsubrolelinks' value='true' />
  ```

  Pour des informations connexes sur la mise à jour automatique des rôles lors de l'importation, consultez le bogue ID-15053 décrit à la section « Problèmes connus ».

Sécurité

- Les utilisateurs dotés de capacités d'approbateur peuvent désormais déléguer leurs futures demandes d'approbation à un ou plusieurs autres utilisateurs qui ne sont pas des approbateurs Identity Manager pendant une période spécifique. La délégation est possible à partir de trois interfaces : (ID-8485)
  - Menu principal Utilisateur final – lien Déléguer les approbations
  - Onglet Approbations admin - sous-onglet Déléguer mes approbations
  - (Admin) Créer/Éditer/Afficher l'utilisateur - section Sécurité
- La génération de mot de passe fonctionne désormais correctement, et échoue normalement lorsque les mots de passe ne sont pas générés correctement. (ID-12275)
- Identity Manager offre dorénavant le type d'autorisation (authType) utilisateur final EndUserLibrary . La capacité EndUser (AdminGroup) offre désormais un accès Liste et Vue aux bibliothèques dont le type d'authentification est EndUserLibrary. (ID-12469)

  Pour permettre l'accès au contenu d'une bibliothèque à l'utilisateur final, définissez `authType=EndUserLibrary` et vérifiez que l'attribut MemberObjectGroup de la bibliothèque est défini sur Tous.
- Un utilisateur d'Identity Manager peut disposer de sessions de connexion simultanées. Vous pouvez toutefois limiter les sessions simultanées à une par application de connexion en changeant la valeur de l'attribut de configuration security.authn.singleLoginSessionPerApp dans l'objet configuration système. 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 BPE). Changer la valeur de cet attribut pour true impose une session à connexion unique à chaque utilisateur. (ID-12778)

  Dans ce cas, un utilisateur ne peut se connecter qu'à une seule session. Toutefois, seule la dernière session de connexion demeure active et valide. Si l'utilisateur exécute une action dans une session invalide, il est automatiquement forcé hors de la session et celle-ci se termine.
- Les changements de mot de passe utilisateur initiés par les administrateurs, via SPML ou autre, ne sont pas ajoutés à l'historique du mot de passe. Il existe à présent deux moyens de configurer l'application afin d'enregistrer un mot de passe dans l'historique des utilisateurs. Une seule méthode est nécessaire. (ID-13029)

- Option d'affichage (prioritaire si présente ou définie sur vrai) : définissez l'attribut savePasswordHistory sur le formulaire cible. Par exemple :

```
<Field name='savePasswordHistory'>
  <Default>
    <Boolean>true</Boolean>
  </Default>
</Field>
```

- Appliquez les paramètres de configuration système suivants et basculez le comportement sur l'interface souhaitée. Cela devra être ajouté à l'objet de configuration système si cela n'est pas déjà fait.

```
<Attribute name='security'>
  <Object>
    <Attribute name='admin'>
      <Object>
        <Attribute name='changePassword'>
          <Object>
            <Attribute name='Administrator Interface'>
              <Object>
                <Attribute name='savePasswordHistory'>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
            <Attribute name='Command Line Interface'>
              <Object>
                <Attribute name='savePasswordHistory'>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
            <Attribute name='IVR Interface'>
              <Object>
                <Attribute name='savePasswordHistory'>
                  <Boolean>false</Boolean>
                </Attribute>
              </Object>
            </Attribute>
            <Attribute name='SOAP Interface'>
              <Object>
                <Attribute name='savePasswordHistory'>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
            <Attribute name='User Interface'>
              <Object>
                <Attribute name='savePasswordHistory'>
```

```
                    <Boolean>false</Boolean>
                  </Attribute>
                </Object>
              </Attribute>
            </Object>
          </Attribute>
        </Object>
      </Attribute>
....
```

Serveur

- Les sous-objets TaskInstance tels que les approbations sont désormais supprimés correctement à la fin d'une tâche. (ID-3258)
- Identity Manager a maintenant besoin d'accéder au répertoire `tmp`. (ID-7804) Pour cela, si votre serveur d'application utilise une stratégie de sécurité, vous devez ajouter la permission suivante :

```
permission java.io.FilePermission "$(java.io.tmpdir)$(/)*",
"read,write,delete";
```

- La page Rechercher Utilisateurs traite désormais les hiérarchies profondément imbriquées de nombreuses organisations. (ID-10352)
- Dans un environnement clusterisé, un échec de connexion sur les pages de l'utilisateur final n'entraîne plus d'exception liée à la sérialisation. (ID-10556)
- Un serveur ne déclenche plus de mécanisme de basculement sur lui-même et termine ses propres tâches si le serveur prend trop longtemps pour traiter les informations de tâche. (ID-10920)
- Les attributs utilisateur étendus sont désormais supprimés correctement des objets utilisateur. (ID-11721)
- Le ResourceConnectionManager est dorénavant avisé des arrêts à venir. Par conséquent, le serveur n'a plus à attendre l'expiration des connexions SSH pour quitter. (ID-12214)
- La condition qui provoquait une erreur de type « pas de cache » sur la page Toutes les tâches pour les utilisateurs des sous-organisations ne possédant pas d'accès admin aux organisations parentes a été corrigée. (ID-12288)
- Le traitement des séparateurs est désormais supprimé entre crochets. De ce fait, tous les caractères compris entre les deux crochets sont traités comme un index ou un filtre. Remarque : il n'existe actuellement aucun mécanisme pour neutraliser le crochet de fermeture]. (ID-12384)
- Les fins d'instances de tâches sont désormais auditées en tant qu'actions de type Terminer et non plus de type Modifier. (ID-12791)
- Les actions utilisateur peuvent être effectuées sur les utilisateurs après suppression d'une ressource leur étant directement assignée. (ID-14806)

SOAP

- La prise en charge SPML a été étendue pour couvrir les rôles et les groupes de ressources en plus des personnes. (ID-8850)
- La nouvelle capacité SPMLAccess permet aux administrateurs de comptes d'accéder à l'interface SPML. (ID-10854)
- Le serveur SPML retourne désormais des erreurs pour les demandes qui contiennent des filtres utilisant des opérateurs qui ne sont pas encore implémentés. (ID-11343)
- L'interface SPML d'Identity Manager offre une `login` ExtendedRequest qui permet aux appelants de se connecter comme administrateur. A partir de cette version, l'interface SPML offre également une `loginUser` ExtendedRequest qui permet à l'appelant d'obtenir une session d'auto-provisioning utilisateur. Cette `loginUser` ExtendedRequest prend en charge la connexion avec un mot de passe ou des réponses à des questions de sécurité. (ID-12103)

Vues

- La vue Utilisateur offre désormais l'attribut de contrôle suivant : (ID-4383)

  `accounts[`***resname***`].waveset.forceUpdate`

  où ***resname*** représente le nom de la ressource. La valeur de cet attribut est une liste d'attributs du compte de ressource qui est toujours envoyée à la ressource pour mise à jour lorsqu'un utilisateur est modifié.
- Les vues de compte de ressource (DeprovisionViewer, DisableViewer, EnableViewer, PasswordViewer, RenameUserViewer, ReprovisionViewer et UnlockViewer) prennent désormais en charge deux nouvelles options pour récupérer les attributs de compte de ressource pour l'utilisateur : (ID-10176)
  - `fetchAccounts` - un Booléen qui provoque l'inclusion dans la vue des attributs de compte pour les ressources assignées à l'utilisateur
  - `fetchAccountResources` - une liste de noms de ressources parmi laquelle les extraire. Sinon, Identity Manager utilise toutes les ressources assignées.

Flux de travaux

- Les avertissements Invalid checkReference ne sont plus retournés lors de l'exécution des flux de travaux. (ID-10802)
- Si vous utilisez `notification.rediret` pour rediriger les messages vers un fichier, ce dernier est désormais écrit à l'aide de `emailNotifier.contentCharset`, comme le serait le message s'il était envoyé par e-mail. Cela permet au fichier de contenir des caractères non-ISO-8859-1. (ID-10331, 14984)
- Des informations supplémentaires sont ajoutées à un message de flux de travaux lorsqu'un approbateur tente d'approuver ou de rejeter un élément de travail déjà approuvé ou rejeté. (ID-11045)
- Identity Manager offre désormais le service de flux de travaux `auditPolicyScan`. Vous pouvez utiliser ce service de flux de travaux pour analyser les violations de stratégie d'audit de l'utilisateur en fonction des stratégies qui lui ont été assignées. Lorsqu'il n'y a pas de stratégie assignée à l'utilisateur, une stratégie assignée à l'organisation est utilisée, le cas échéant. Consultez la section *Ajouts et corrections de la documentation* de ces notes de version pour des informations plus détaillées. (ID-12589)
- RoleAdminTask authType a été assigné à Manage Role TaskDefinition et ResourceAdminTask authType à Manage Resource TaskDefinition. (ID-12768)

Défauts corrigés dans les versions précédentes

Cette section détaille des défauts corrigés depuis Identity Installation Pack 2005Q4M3.

Installation et mise à jour

- Le processus de mise à niveau n'efface plus le modèle d'e-mail Examen des accès. (ID-13216)

Interface administrateur

- Lorsque vous configurez une nouvelle action utilisateur pour le menu applet de l'utilisateur, les touches de texte sont désormais affichées correctement. (ID-8400)
- Identity Manager traite désormais correctement les affichages de l'aide qui déclenchaient des erreurs lorsqu'ils contenaient des caractères spéciaux. (ID-8747)
- Lorsque l'attribut singleLoginSessionPerApp d'une application de connexion est défini sur true, Identity Manager se comporte comme suit : un utilisateur peut se connecter plusieurs fois à la même application. Toutefois, la dernière session de connexion de l'utilisateur est la seule active et valide. Si l'utilisateur essaie d'exécuter une tâche pendant une autre session de connexion en tant que même utilisateur d'Identity Manager, il est automatiquement forcé hors connexion et celle-ci se termine. (ID-9543)
- Lorsqu'un utilisateur est directement assigné à une organisation, et qu'une UserMemberRule l'assigne également à la même organisation, l'utilisateur n'est plus dupliqué dans la liste. (ID-10410)
- La page de délai d'attente de session peut désormais être localisée et sera affichée dans la langue spécifiée par la localisation de l'utilisateur. (ID-10571)
- L'exemple de formulaire LDAP Password Sync (sample/forms/LDAPPasswordActiveSyncForm.xml) définit dorénavant le champ `waveset.password` au lieu de `password.password` et `password.confirmpassword`. (ID-11660)
- L'interface administrateur d'Identity Manager ne génère plus d'erreurs lorsque les résultats de recherche incluent un nom d'utilisateur contenant une apostrophe, et que ce nom est utilisé dans un lien pour une commande ultérieure. (ID-11123)

- Les composants MultiSelect affichent désormais correctement les chaînes uniques. (ID-11979)
- Identity Manager affiche maintenant le message d'erreur correct lorsque vous tentez d'éditer un type d'objet de ressource qui ne prend pas les mises à jour en charge. (ID-12242)
- Lorsque vous utilisez l'arborescence pour lister les ressources, les noeuds dont les noms contiennent des caractères de soulignement se développent correctement à présent. (ID-12478)
- L'aide en ligne affiche dorénavant les pages d'aide correctes lorsque des options sont sélectionnées hors assistant dans le sous-menu de configuration ActiveSync. (ID-12597)
- Vous pouvez maintenant supprimer des utilisateurs lorsque vous utilisez la localisation en français. (ID-12642)
- L'arborescence, la page Compte, et la page des résultats de la recherche affichent maintenant un attribut Responsable non résolu comme nom du responsable d'Identity Manager placé entre parenthèses. A chaque mise à jour de l'utilisateur, Identity Manager tente de résoudre l'attribut responsable non résolu. S'il résout l'attribut, Identity Manager retire les parenthèses et exécute un contrôle de contrainte sur la valeur suivante. (ID-12726)
- Le lien de boîte de réception disponible lors de la connexion d'un utilisateur anonyme pointe à présent vers le nouveau tableau répertoriant les éléments de travail de l'utilisateur final. (ID-12816)
- Vous pouvez maintenant positionner les boutons du composant TabPanel. (ID-12797)
- Identity Manager convertit désormais les modèles d'e-mail mail.example.com par défaut vers la nouvelle fonctionnalité de variable de configuration du serveur. (ID-12720)
- Les champs de mot de passe sont désormais affichés conditionnellement lorsque l'interface utilisateur d'Identity Manager ne comprend pas le module de connexion LH et qu'un AdminRole est assigné à l'utilisateur. (ID-12692)
- Identity Manager affiche désormais des listes de groupes de ressources accessibles via l'onglet Ressources présentées dans l'ordre d'enregistrement des listes. (Dans les versions antérieures, les ressources étaient triées.) (ID-14117)
- Vous pouvez dorénavant rechercher des rôles avec de nombreuses organisations à partir de la page Rechercher des rôles sans qu'une erreur relative au groupe d'objet s'affiche. (ID-15303)
- Lorsque vous annulez l'assignation de comptes de ressources à un utilisateur en utilisant la fonctionnalité Éditer l'utilisateur, la SITUATION des comptes dans l'index des comptes est désormais mise à jour correctement dans tous les cas de figure. (ID-15310)

- Le menu sous l'onglet Rôles > Rechercher des rôles > Approbateurs peut désormais présenter des utilisateurs dotés de la capacité Approbateur de rôles. (ID-15373)
- Un problème relatif à l'échec d'Internet Explorer en présence d'un URL comptant plus de 2 000 caractères a été résolu. (ID-15801)
- Les utilisateurs d'Internet Explorer 6 ou 7 doté de la mise à jour de sécurité 912812 n'ont plus besoin de double-cliquer sur une case de sélection multiple pour mettre en surbrillance la case ou de double-cliquer sur un élément pour le déplacer. (ID-15824)
- Lorsque vous spécifiez le paramètre `true` pour `IAPI.cancel` (lequel annule toutes les mises à jour en attente détectées pour l'utilisateur en cours de traitement) sur le formulaire ActiveSync Input, la vue de l'utilisateur ne reste plus verrouillée après son traitement. (ID-15912)
- Lorsque vous effectuez une recherche d'utilisateurs pour laquelle vous sélectionnez l'option Organisation des utilisateurs en plus d'autres critères de recherche, vous recevez des résultats pertinents. (ID-16076)
- Sur la page Rechercher rôle, la liste des approbateurs est maintenant triée. (ID-16392)
- Le composant DatePicker fonctionne normalement quel que soit le fuseau horaire. (ID-16618)

Éditeur de processus métier

- Vous pouvez afficher et éditer les valeurs négatives (en secondes) pour les délais d'attente d'action manuelle. (ID-9715)
- La sélection de **Stocker l'attribut dans le référentiel d'Identity Manager** lors de l'édition d'un attribut MetaView fonctionne désormais normalement. (ID-12396)

Formulaires

- Identity Manager offre de nouveaux exemples de formulaires de création et de mise à jour de groupe LDAP autorisant les noms de membres non uniques. (ID-8831)
- Les composants MultiSelect traitent désormais correctement les éléments dont les étiquettes sont identiques (noms d'affichage). (ID-10964)
- La valeur maxlength par défaut du composant texte est dorénavant illimitée (elle était auparavant de 256 caractères) (ID-11995).
- Les champs de groupes NTForm et NDSUserForm implémentent désormais correctement la règle ListObjects. (ID-12301)

- Les assistants de ressource d'adaptateur hôte gèrent maintenant mieux les champs affinityAdmin, en empêchant les duplications et les entrées nulles. (ID-12024)
- Le formulaire de mise à jour de groupe LDAP n'ignore plus les modifications lorsque les appartenances au réseau demeurent identiques. (ID-12162)
- La méthode `listResourceObjects` de `com.waveset.ui.FormUtil` exécute à présent correctement les filtres définis. Consultez les JavaDocs pour obtenir plus d'informations concernant cette méthode. (ID-14422)

Identity Auditor

- Le contrôle de stratégie pendant la création d'un utilisateur ne crée plus d'instances de tâche supplémentaires. (ID-10489)

Identity Manager SPE

- Lors de la création d'un compte de ressource, lorsqu'une ressource est indisponible, Identity Manager SPE mémorise les valeurs de l'attribut de ressource. Lors de la prochaine édition de cet utilisateur dans Identity Manager SPE, le compte est créé sur la ressource si cette dernière est disponible. (ID-11168)
- Vous pouvez maintenant désactiver les événements suivis dans SPE en désélectionnant l'option Activer le recueil des événements sur la page **Service Provider > Modifier la configuration principale**. Vous pouvez aussi désactiver de façon sélective sur la même page l'option de collecte des données d'événement suivies pour chaque échelle de temps. Comme tous les paramètres de cette page, les objets de configuration modifiés doivent être exportés vers le répertoire SPE principal pour prendre effet. (ID-12033)
- La méthode SPE IDMXContext deleteObjects supprime désormais correctement les objets du stockage du répertoire. (ID-11251)
- Le sous-système d'audit de Service Provider Edition n'émet plus d'exception de pointeur nul à la fermeture d'un conteneur. (ID-12845)
- IDMXUserViewer émettait une exception de pointeur nul si le formulaire associé aux propriétés spécifiques de la vue autres qu'inclure, ou cibles et le mappage d'option passé aux les méthodes de traitement de vue (create/checkin/checkout/refresh) était nul. (ID-12861)
- Les attributs LDAP supprimés sont désormais propagés après la remise à disposition d'une ressource temporairement hors service. (ID-15471)

Connexion

- Le lancement d'une tâche personnalisée pendant la connexion ne la ralentit plus excessivement. (ID-12377)
- Identity Manager enregistre désormais correctement les tentatives de connexion administrateur des utilisateurs sans capacités, organisations ou capacités/organisations. (ID-12497)

Synchronisation des mots de passe

- L'application de configuration de synchronisation des mots de passe (Configure.exe) ne tronque plus les propriétés JMS en présence d'un signe d'égalité (=) lors de la lecture à partir du référentiel. (ID-12658)
- Le fichier `passwordsync.dll` retourne désormais les messages d'erreur appropriés en cas d'échec de connexion. Ce changement corrige aussi les possibles fuites de gestion survenant pendant les échecs de connexion. (ID-15451)
- Les mots de passe interceptés avec des caractères situés en dehors de la plage ASCII de 7 bits sont désormais codés correctement au format UTF-8 avant leur chiffrement. (ID-15829)

Réconciliation

- Les réconciliations ne s'arrêtent plus lorsque les ressources comportent des utilisateurs en double. (ID-14949)
- Certaines correspondances de comptes ambiguës lors de réconciliations sont désormais interprétées comme une correspondance préférée afin d'éviter des erreurs de réconciliation inutiles. (ID-14965)
- Les réconciliations ne s'arrêtent plus lorsque les normalisations d'utilisateurs suppriment d'un utilisateur toutes les informations sur les ressources. (ID-15028)

Rapports

- Windows 2000 Active Directory Inactive Account Scan (une tâche située sous la barre de menu supérieure Analyse du risque) se termine désormais correctement. (ID-11148)
- Vous pouvez dorénavant utiliser le rapport Utilisateur de la ressource avec plusieurs utilisateurs. (ID-11420)
- Lorsqu'un administrateur délégué exécute un rapport utilisateur, les utilisateurs membres d'une organisation en raison d'une UserMembersRule sont désormais inclus. (ID-11871)

- Lorsqu'un nom de ressource est sélectionné pour l'axe y d'un rapport d'utilisation, la valeur est désormais utilisée dans la requête. (ID-12035)
- Par défaut, les rapports suivants sont automatiquement étendus à l'ensemble des organisations contrôlées par l'administrateur connecté, à moins que ce comportement soit explicitement réduit à une ou plusieurs organisations spécifiques pour lesquelles le rapport doit être exécuté. Pour prendre cette fonction en charge, le composant d'étendue de l'organisation, qui était un simple composant de sélection est devenu un composant à sélection multiple. (ID-12116)
- Identity Manager audite désormais correctement les modifications d'appartenance au groupe LDAP. (Il inclut maintenant les valeurs anciennes et nouvelles.) (ID-12163)
- Il est à présent possible de personnaliser un rapport CSV codé avec le jeu de caractères UTF-8 en texte multioctet de manière à l'afficher dans des applications ne prenant pas en charge le codage UTF-8 (comme Microsoft Excel). (ID-13574, 15407)
- Les rapports PDF envoyés par e-mail respectent désormais les paramètres de polices et de polices incorporées définis à n'importe quel niveau. (ID-15328)
- Les balises ont été supprimées des rapports PDF suivants : (ID-15408)
  - Tous les rôles admin
  - Tous les administrateurs
  - Tous les rôles
- Les formulaires des rapports d'utilisation sont désormais obligatoires pour spécifier une valeur d'attribut d'axe X. (ID-15777)

Référentiel

- Le référentiel d'Identity Manager effectue maintenant la gestion propriétaire Oracle pour les colonnes BLOB. Les scripts d'exemple pour Oracle définissent désormais la colonne xml comme BLOB de type de données (au lieu de LONG VARCHAR). Tous les tableaux des nouvelles installations seront créés avec des colonnes xml BLOB. Au cours d'une mise à niveau, seuls les nouveaux tableaux auront une colonne xml BLOB, mais les autres tableaux peuvent être convertis en BLOB en effectuant les modifications indiquées dans le script de mise à niveau (dans les cas de grands déploiements, ce processus de mise à niveau peut prendre plusieurs heures). Vous devez effectuer une mise à niveau vers le pilote JDBC Oracle le plus récent pour obtenir les meilleures performances des BLOB. (ID-11999)

- Le référentiel d'Identity Manager a été modifié pour éviter une impasse spécifique à Microsoft SQL Server 2000. Le référentiel utilise désormais l'ID (au lieu du nom) de LAST_MOD_ITEM lorsqu'il sélectionne la dernière valeur modifiée comme type. (ID-12297)
- Les systèmes de base de données Oracle lents n'entraînent plus l'exécution de tâches suspendues sur plus d'un ordonnanceur à la fois. (ID-15372)
- La suppression d'un rôle pour un utilisateur au sein d'un groupe d'utilisateurs similaires n'a plus d'incidence sur les entrées des autres utilisateurs dans le référentiel. Par ailleurs, cette action ne vous empêche plus de rechercher ces utilisateurs par le critère du rôle. (ID-15584)

Ressources

Passerelle

- La passerelle ne s'arrête plus brutalement en utilisant directement les API d'Identity Manager sans passer par l'interface d'Identity Manager. (ID-12481)

Généralités

- Vous pouvez utiliser les apostrophes en toute sécurité dans les mots de passe. (ID-10043)
- Les assistants de ressource d'adaptateur hôte gèrent maintenant les champs affinityAdmin, qui empêchent les duplications et les entrées nulles. (ID-12024)
- Les processus Active Sync exécutés sur un cluster Websphere utilisant un démarrage "automatique avec basculement" ne se bloquent plus. (ID-12540)
- Pour certains adaptateurs de ressources, les règles d'exclusion sont maintenant appliquées avant que les utilisateurs soient extraits lors d'une réconciliation, ce qui permet d'exclure des utilisateurs spécifiques, d'éviter des erreurs générées par la ressource et d'améliorer les performances pour un grand nombre d'utilisateurs. (ID-14436)
- Identity Manager respecte à présent le paramètre de combinaison deny, ignore des fonctions prises en charge pour une ressource. Si vous sélectionnez **`ignore`**, l'action n'est pas exécutée, mais elle peut apparaître sous forme de message dans l'IG dans certaines situations. (ID-14948)

- Si des ressources communes sont configurées dans l'objet Configuration système à des fins d'utilisation lors de la connexion et si une connexion de ressource commune échoue, les connexions n'aboutissent plus à des échecs s'il existe une autre ressource dans la pile du module de connexion qui n'est pas une ressource commune et qui requiert des propriétés d'authentification différentes de celles des ressources de module de connexion précédentes. (ID-15047)
- L'exécution d'Active Sync ne se poursuit pas lorsque l'option Créer des comptes sans correspondance est définie sur true et que la valeur de l'option Nombre d'erreurs autorisées est dépassée. (ID-15662)

Annuaires

- L'adaptateur de ressource Active Directory émet désormais une exception lorsqu'un type de chiffrement incorrect est spécifié. Les valeurs admises sont (vide), "none", "kerberos" and "ssl". (ID-9011)
- Identity Manager interroge dorénavant les connexions LDAP. (ID-10219)
- Les attributs de gestion Out of Office d'un utilisateur Active Directory (Exchange) avec e-mail n'échouent plus lorsque `msExchHideFromAddressLists` est défini sur true. En outre, le formulaire utilisateur d'exemple Active Directory a été mis à jour pour empêcher Identity Manager d'afficher des attributs Out of Office lorsque `msExchHideFromAddressLists` est activé. (ID-12231)
- Le traitement Active Sync LDAP Changelog traite maintenant le type de changement MODIFY sans valeur. (ID-12298)
- L'adaptateur ADSIResourceAdapter ferme dorénavant les connexions lors des demandes d'objets de ressources. (ID-15098)
- Identity Manager ne lit plus les attributs de comptes en écriture seule à partir d'un annuaire LDAP ou d'Active Directory. (ID-15838)

Mainframe

- Dans l'adaptateur RACF, en changement pour DFLTGRP produit désormais l'ajout (au besoin) de DFLTGRP aux GROUPES pour garantir que DFLTGRP puisse être défini comme le nouveau groupe par défaut. (ID-9987)
- Les connexions d'adaptateur de ressource Mainframe sont correctement interrogées et ne bloquent plus les opérations mainframe. (ID-12388)
- L'émulation de terminal utilisé à présent pour créer un compte NaturalResourceAdapter autorise un nom d'utilisateur de 8 caractères qui n'utilise pas d'onglet pour sélectionner l'attribut de copie de liens. (ID-12503)

- Le mécanisme par défaut AttrParse de la liste d'utilisateurs RACF a été étendu en vue de gérer les nombres importants d'« AUTORISATIONS DE CLASSES » et les utilisateurs de modèles dotés d'entrées de groupe telles que « GROUP SYS1 CONNEXION UTILISATEUR NON INDIQUÉE ». (ID-15021)
- Si un compte Resource Affinity (Affinité de la ressource) sur une ressource RACF dispose de privilèges insuffisants pour lister un utilisateur, Identity Manager génère désormais un message d'erreur approprié. (ID-15331)
- Lors de la suppression de comptes RACF, le système demande à présent, par le biais d'un masque de la recherche, les profils des jeux de données de l'utilisateur, énumère ces profils et supprime les jeux de données individuellement (au lieu de tenter de tous les effacer via un DELDSD .**). (ID-15413)
- L'effacement d'un attribut RACF dans un formulaire n'entraînait pas de la part d'Identity Manager celui de l'attribut sur l'utilisateur suite à l'envoi du formulaire. Identity Manager efface à présent l'attribut. (ID-15971)
- L'adaptateur de ressources Top Secret gère à présent correctement `ASUSPEND`, `PSUSPEND`, `VSUSPEND` et `XSUSPEND` lors de l'activation et de la désactivation des utilisateurs. (ID-16295)
- Un problème relatif à l'adaptateur Top Secret qui provoquait le chargement incomplet des attributs utilisateur a été corrigé. (ID-16334)

Oracle et Oracle ERP

- Au cours d'une session avec l'adaptateur de ressource Oracle, tous les curseurs Oracle sont fermés, même lorsque des exceptions se produisent. (ID-10357)
- Utilisez le format suivant pour les adaptateurs de ressource Oracle et Oracle ERP qui se connectent aux environnements Oracle RAC utilisant un pilote léger : (ID-10875)

  jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=host01)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host02)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host03)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=PROD)))
- L'ERP Oracle peut facultativement limiter les comptes retournés par le répétiteur de compte et les interfaces listObjects en définissant l'attribut de ressource `activeAccountsOnly` sur TRUE. La valeur par défaut est FALSE. Lorsqu'il est défini sur FALSE, tous les comptes de la ressource sont retournés. Lorsqu'il est TRUE, seuls les comptes dont START_DATE and END_DATE couvrant SYSDATE (maintenant) sont retournés. (ID-12303)
- Les adaptateurs Oracle ERP ont été mis à jour pour fermer PreparedStatements de façon plus homogène, réduisant ainsi le nombre de curseurs ouverts. (ID-12564)

SAP

- L'adaptateur SAP traite maintenant les cas où des groupes d'activité dupliqués sont retournés par listAllObjects(). (ID-7776)
- L'adaptateur SAP offre la possibilité de retourner le mot de passe temporaire généré dans l'objet WavesetResult lorsque l'adaptateur n'a pas été en mesure de définir un mot de passe comme non expiré. Cette situation se produit uniquement dans les conditions suivantes :
  - ❍ un changement de mot de passe administrateur est demandé et expirePassword = false
  - ❍ le mot de passe souhaité ne satisfait pas la stratégie de mot de passe SAP

  L'échec intervient le plus souvent lorsque le mot de passe souhaité se trouve déjà dans l'historique des mots de passe SAP.

  L'attribut de ressource `Retourner des mots de passe SAP temporaires en cas d'échec` a été créé pour offrir cette possibilité, mais il ne fonctionne pas à l'heure actuelle. (ID-12185)
- L'adaptateur SAP vérifie désormais plus solidement le mot de passe d'un utilisateur par rapport à son mot de passe actuel lorsque la requête est un changement de mot de passe administrateur et que l'indicateur `expirePassword` est false. Ceci évite une condition d'erreur lorsque le mot de passe souhaité et le mot de passe actuel de l'utilisateur sont identiques. (ID-12447)
- L'écriture de profils et de groupes d'activités SAP dans un environnement CUA (Central User Administration) ne divise plus en deux une nouvelle ligne de tableau lorsque les informations sont séparées par deux-points. (ID-14371)

UNIX

- Les adaptateurs UNIX offre la fonctionnalité de base d'initialisation et de réinitialisation `sudo`. Toutefois, lorsqu'une action de ressource est définie et contient une commande dans le script exigeant une autorisation `sudo` vous devez spécifier la commande `sudo` avec la commande UNIX. (Par exemple, vous devez spécifier `sudo useradd` au lieu de simplement `useradd`.) Les commandes qui nécessitent `sudo` doivent être enregistrées dans la ressource native. Utilisez `visudo` pour enregistrer ces commandes. (ID-10206)

- Les adaptateurs Red Hat Linux et SuSE Linux occupent dorénavant le groupe principal, le groupe secondaire et les derniers champs de connexion pendant les processus de traitement des listes en masse tels que Charger de la Ressource and Extraire vers fichier. (ID-11627)

  Si la carte schématique indique que le dernier champ de connexion doit être suivi, le processus de listes en masse peut être considérablement ralenti, car l'adaptateur doit demander individuellement les dernières informations de connexion de chaque utilisateur.
- Vous pouvez maintenant mapper l'attribut `time_last_login resource` sur les adaptateurs Solaris, HP-UX et Linux selon un nom d'attribut différent de celui par défaut (heure de la dernière connexion). (ID-11692)
- Si vous effectuez une opération Créer un objet ressource pour une ressource de serveur Solaris NIS, sélectionnez plusieurs comptes sous Utilisateurs, puis cliquez sur Enregistrer. Tous les comptes sont alors ajoutés au fichier du groupe dans le répertoire source de mots de passe NIS sur le serveur NIS géré. Dans les versions antérieures, cette opération fonctionnait uniquement lorsqu'un compte était sélectionné. (ID-15085)
- Pour Solaris NIS, Identity Manager n'ajoute plus la cible `netid`, laquelle était inutile et générait des messages d'erreur dans les suivis. (ID-15503)
- Pour Solaris NIS, Identity Manager n'empêche plus l'utilisation de la commande `sudo` si le répertoire contenant les fichiers de modèle `passwd`, `shadow` et `group` de Solaris NIS est protégé en lecture contre l'utilisateur admin. (ID-15505)
- Pour Solaris NIS, un compte n'est plus partiellement créé si le groupe principal par défaut est totalement absent ou s'il correspond à un nom ne figurant pas dans le fichier de groupe. (ID-15509)
- Un problème entraînant l'échec de la génération de l'ID d'un utilisateur ou d'un groupe Solaris NIS dans un environnement sans utilisateur ni groupe au départ a été corrigé. De plus, les fichiers de modèle `passwd` et `group` se trouvent dans un répertoire autre que `/etc`. (ID-15510)
- Pour Solaris NIS, si deux comptes sont créés sur une ligne et si un shell est spécifié pour le premier compte mais pas pour le second (soit il n'est pas défini dans le fichier `defadduser` soit le fichier `defadduser` n'existe pas), le second compte n'est plus créé avec le shell du premier. (ID-15511)
- Sous Solaris NIS, le fichier `/usr/sadm/defadduser` est utilisé comme source optionnelle pour les valeurs par défaut des nouveaux comptes. Dans les versions antérieures d'Identity Manager, le système utilisait un élément incorrect de ce fichier afin de définir le groupe principal par défaut d'un nouvel utilisateur Identity Manager. À présent, il s'agit effectivement de l'élément `defgname` qui est chargé de cette tâche. La valeur de ce groupe principal par défaut est remplacée par l'attribut de ressource **Groupe principal par défaut**, lequel est lui-même remplacé par l'attribut de compte du même nom. (ID-15512)

- Identity Manager ne stocke plus les mots de passe chiffrés Solaris NIS et HP-UX NIS dans les deux fichiers de modèle NIS `passwd` et `shadow` lorsqu'un compte est mis à jour. La valeur de paramètre substituable x est stockée dans le fichier `passwd`. (ID-15593)
- Un problème selon lequel vous pouviez créer un groupe sur une ressource Solaris NIS portant le nom ou l'ID d'un groupe existant a été corrigé. (ID-15755)
- Lors de la suppression d'un utilisateur d'une ressource Solaris, Identity Manager ne produit plus de résultat positif erroné si l'utilisateur est connecté à la ressource et que la suppression échoue. (ID-15761)

Autres problèmes

- L'adaptateur UNIX SecurID traite correctement les attributs Compte utilisateur Identity System lorsque les noms par défaut sont modifiés. (ID-10521)
- Si vous avez une ressource Active Sync PeopleSoft Component qui utilise l'interface de composant LH_AUDIT_RANGE_COMP_INTF, vous devez effectuer les changements de la ressource si vous souhaitez continuer à utiliser l'interface de composant LH_AUDIT_RANGE_COMP_INTF. (ID-11226)

  Vérifiez que votre ressource possède un attribut de ressource `auditLegacyGetUpdateRows` défini sur true.

```
<ResourceAttribute name='auditLegacyGetUpdateRows'
    value='true'
    displayName='Use Legacy Get Update Rows'
    type='boolean'
    multi='false'
    facets='activesync' >
</ResourceAttribute>
```

- Vous pouvez désormais supprimer les objets d'organisation Sun Access Manager de l'applet de ressources d'Identity Manager. (Identity Manager supprime ensuite tous les objets enfant sans confirmation.) (ID-11516)
- Pour gérer les utilisateurs SecurId, Identity Manager prend désormais en charge trois jetons par utilisateur. (ID-11723)
- Pour l'adaptateur Database Table, les connexions de la base de données sont maintenant fermées le plus tôt possible pendant l'itération et l'interrogation, empêchant toute poursuite inutile des connexions inutilisées. (ID-11986)
- L'adaptateur JMS Listener n'échoue plus sur Websphere 6.0. Un changement de traitement asynchrone pour synchrone des messages permet désormais à JMS Listener de fonctionner sur les serveurs J2EE qui interdisent le traitement asynchrone des messages JMS au sein d'une application web. La fréquence d'interrogation doit maintenant être définie pour les ressources JMS Listener. (ID-12654)

- Les adaptateurs SecurID appliquent l'exigence RSA selon laquelle l'attribut de connexion par défaut doit comprendre exclusivement des caractères anglophones d'un seul octet.(ID-13805)
- Les mots de passe dotés de caractères situés en dehors de la plage ASCII de 7 bits sont désormais définis correctement par la passerelle (pour la création et la mise à jour) lorsqu'Identity Manager est déployé avec Tivoli Access Manager et Active Directory. (ID-15006)
- L'adaptateur Shell Script « piège » et signale désormais la sortie des scripts de suppression qui renvoient ouvertement une erreur. (ID-15340)
- L'adaptateur de table de base de données vous permet de spécifier le paramètre de ressource **Jeter de nouveau toutes les exceptions SQL**. Lorsque cette option n'est pas cochée, les exceptions SQL émises par les instructions SQL et dotées d'un code d'erreur égal à 0 sont détectées et supprimées. (ID-15390)
- Un problème qui provoquait des interblocages lors de l'utilisation d'Active Sync et de la ressource PeopleSoft a été résolu. (ID-16109)

Réconciliation

- Le paramétrage de ControlledOrganizationRule sur User AdminRole n'empêche plus le démarrage du démon de réconciliation. (ID-12695)

Référentiel

- Les messages d'erreur du formulaire, `com.waveset.util.InternalError : La longueur de la chaîne de récapitulatif (2185) dépasse le maximum (2048)` ne se produisent plus lors de l'enregistrement d'utilisateurs ou d'autres objets. (ID-12492)

Rôles

- Les noms de rôle qui contiennent des apostrophes ne sont plus tronqués lors de l'édition du rôle. (ID-8806)
- Identity Manager traite désormais correctement l'ajout et la soustraction de groupes assignés par l'intermédiaire des attributs de rôle. (ID-10832)
- Les rôles qui sont créés dans Identity Manager 5.0 et les sous-rôles d'autres rôles contiennent maintenant des liens vers leurs super rôles. (ID-11477)
- Lorsqu'une ressource est renommée, les attributs de rôle continuent désormais à référencer correctement la ressource appropriée. (ID-11689)

- Les actions en masse peuvent supprimer le rôle de waveset.roles lorsque celui-ci ne contient qu'un seul rôle. (ID-14568)
- Le système met désormais à jour correctement les sous/super rôles pendant les actions d'enregistrement sous. (ID-16010)

Sécurité

- Vous pouvez supprimer les informations de débogage détaillées qui sont masquées dans les commentaires HTML en définissant la propriété `ui.web.disableStackTraceComments` dans le fichier `Waveset.properties` sur true. Si vous effectuez une mise à niveau à partir d'une version précédente d'Identity Manager, vous devrez ajouter cette propriété à config/Waveset.properties. La propriété est ignorée (ce qui revient à la définir sur false) si elle est absente du fichier des propriétés.(ID-10499)
- Les utilisateurs anonymes peuvent désormais accéder à différents types d'objets, notamment les règles, sans définir l'attribut abandonné `endUserAccess` dans l'objet Configuration système. (ID-11248)
- Pour configurer cette version afin de provisionner vers une ressource Clear Trust 5.5.2, vous devez installer `ct_admin_api.jar` depuis le CD d'installation de Clear Trust 5.5.2. Vous n'avez pas besoin de bibliothèques supplémentaires pour la communication SSL. (ID-12449)
- Pendant la création d'AdminRole, Identity Manager traite désormais correctement l'inclusion et l'exclusion de tous les types d'objet. (ID-12491)
- Les administrateurs possédant les capacités suivantes ont désormais accès à la page Lister ressources : (ID-12647)
  - Administrateur des mots de passe des ressources
  - Changer administrateur des mots de passe de ressources
  - Réinitialiser administrateur des mots de passe des ressources
  - Changer administrateur de ressource de synchronisation active
  - Contrôler administrateur de ressource de synchronisation active
  - Administrateur de réconciliation
  - Administrateur des demandes de réconciliation
- Vous avez dorénavant la possibilité d'ajouter des mots de passe à l'historique des mots de passe d'un utilisateur lors de la création d'un utilisateur. (ID-15179)
- Un approbateur ne contrôlant pas l'organisation supérieure peut désormais afficher les approbations précédemment approuvées/rejetées. (ID-15271)

- Si un utilisateur détenant des éléments de travail en attente est supprimé, Identity Manager s'assure à présent que ces éléments ne sont pas perdus, en procédant comme suit : (ID-15868)
  - Si un élément de travail en attente a été délégué alors que le délégant n'a pas été supprimé, il est renvoyé à ce dernier, qui devient alors le nouveau propriétaire de l'élément de travail.
  - Si un élément de travail a été délégué et que le délégant a été supprimé ou si l'élément de travail en attente n'a pas été délégué, la tentative de suppression échoue tant que l'élément n'est pas résolu ou transmis à un autre utilisateur.

Serveur

- Le serveur d'application ne s'arrête plus brutalement en utilisant les pilotes Oracle OCI avec SSL (ID-7109)
- Vous ne recevez plus d'exception de pointeur nul lorsque vous tentez une connexion au menu Utilisateur final si l'utilisateur Identity Manager est doté d'un rôle sur une ressource dans laquelle il n'existe pas. (ID-12379)
- La session est maintenant correctement définie pendant les extensions et la dérivation pendant le traitement de créations de comptes de ressources dans le cadre d'une action en masse. (ID-16181)
- Sous certaines conditions, il était possible qu'une tâche planifiée soit traitée par plusieurs serveurs à une heure de début programmée. Cela n'est plus possible. (ID-16318)

SOAP

Vous pouvez dorénavant contrôler les appels SPML 1.0 par l'intermédiaire de la fonction `debug/callTimer.jsp`. Lorsque l'appel est éloigné, la méthode `doRequest()` de com.waveset.rpc.SpmlHandler est très utile pour déterminer la performance SOAP/SPML. Les méthodes SPML individuelles (par exemple, `addRequest`) sont également réglées pour une surveillance pratique. (ID-8463)

Flux de travaux

- Sous certaines conditions, un élément de travail arrivé à échéance pouvait être édité sans générer d'erreur. Une erreur indique à présent que cet élément de travail est erroné. (ID-15439)
- La variable de flux de travaux WF_ACTION_ERROR est maintenant définie lorsqu'une erreur se produit dans l'adaptateur de ressources Remedy. (ID-16360)
- Un modèle d'e-mail personnalisé peut désormais être utilisé pour les approbations transférées. Vous devez spécifier le modèle d'e-mail dans les sous-processus d'approbation, par ID. (ID-16468)

Autres défauts corrigés

6496, 8586, 8739, 8958, 8960, 9936, 10235, 10475, 10483, 10832, 11232, 11642, 11767, 11979,12135, 12203, 12234, 12274, 12368, 12377, 12464,12483, 12510, 12585, 12611, 12614, 12673, 12967, 13054, 13338, 13434, 13965, 14044, 14178, 14334, 14792, 14874, 14893, 14899, 15036, 15073, 15219, 15474, 16107, 16282, 16389, 16395, 16610, 17346

Remarques sur l'installation et la mise à jour

Remarques sur l'installation

- Vous devez installer manuellement Identity Install Pack sous HP-UX.
- Pour exécuter Identity Manager sous Tomcat 4.1.x, téléchargez les fichiers jar JSSE à partir du site Web de Sun (à l'adresse `http://java.sun.com/products/jsse/index-103.html`) et placez-les dans le répertoire `idm\WEB-INF\lib`.
- L'exécution de Sun Identity Manager Gateway sur un système Windows NT nécessite l'extension Microsoft Active Directory Client. Le DSClient se trouve à l'adresse `http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288358`.
- Les fichiers jar suivants ont été supprimés à cause de problème de licence. (ID-9338) Ces fichiers jar sont requis pour l'adaptateur de ressources suivant. Chacun d'entre eux est indiqué ci-dessous, avec les informations pour se les procurer auprès de leurs fournisseurs respectifs.

  Adaptateur : OS400ResourceAdapter

  URL : `http://jt400.sourceforge.net`

  Projet : JTOpen

  JAR : jt400.jar

  Version : 2.03

  Adaptateur : ONTDirectorySmartAdapter

  URL : `http://my.opennetwork.com`

  Projet : Directory Smart

  JAR : dsclass.jar, DSUtils.jar

  Version : N/D

Remarques sur la mise à jour

Lors de la mise à jour d'Identity Manager, pensez à consulter la section du chapitre d'installation relative à votre serveur d'application. Cette section contient un résumé des tâches de mise à niveau depuis la version 6.0 vers la version 6.0 SP4 d'Identity Manager. Pour plus d'informations, reportez-vous au manuel *Identity Manager 6.0 Upgrade*.

Identity Install Pack 2005Q4M3 SP4 peut être mis à jour à partir des versions suivantes :

- Identity Manager 6.0 (tous niveaux de pack de service)
- Identity Auditor 1.7 (tous niveaux de pack de service)

Remarque Si l'installation actuelle d'Identity Manager nécessite une personnalisation importante, contactez Sun Professional Services qui vous assistera dans la planification et l'exécution de la mise à niveau.

Utilisez les informations et les procédures ci-après pour mettre Identity Manager à jour.

Remarque Dans certains environnements, y compris HP-UX, vous devez (ou préférerez peut-être) suivre les procédures de mise à jour manuelles. Dans ce cas, passez à la section intitulée *Mise à jour manuelle d'Identity Manager.*

Remarque Identity Manager 6.0 introduit un changement de schéma qui fournit de nouveaux tableaux pour les tâches, les groupes, les organisations et le tableau du journal syslog. Vous devez créer ces nouvelles structures de tableaux et déplacer les données existantes. Voir *Etape 2 : Mettre à jour le schéma de la base de données référentielle* dans la section *Ajouts et corrections de la documentation* de ce document.

Remarque Si vous avez modifié le modèle Access Review Notice dans la version 6.0 d'Identity Manager vous devez enregistrer le modèle avant la mise à niveau Identity Manager ou le modifier après. (Le processus de mise à niveau efface le modèle et les valeurs par défaut.) (ID-13216)

Étape 1 : Mettez à jour le logiciel Identity Manager.

Utilisez les informations et les procédures ci-après pour mettre Identity Manager à jour.

Remarques :

- Dans certains environnements, y compris HP-UX, vous devez (ou souhaiterez peut-être) suivre les procédures de mise à jour manuelles. Dans ce cas, passez à la section intitulée *Mise à jour manuelle d'Identity Manager.*
- Dans les environnements UNIX, assurez-vous que le répertoire `/var/opt/sun/install` existe et que vous pouvez y écrire.
- Lors de la mise à jour, vous devrez connaître l'emplacement d'installation du serveur d'application.
- Les correctifs installés auparavant sont archivés dans le répertoire `$WSHOME/patches/`*`HotfixName`*.
- Les commandes présentées dans les étapes suivantes sont propres à une installation Windows et à un serveur d'application Tomcat. Les commandes que vous utilisez peuvent être différentes suivant l'environnement dans lequel vous travaillez.

Pour mettre à jour Identity Manager :

1. Arrêtez le serveur d'application.
2. Si vous exécutez Sun Identity Manager Gateway sur le serveur Identity Manager arrêtez le service de passerelle avec cette commande :

   ```
   gateway -k
   ```
3. Exécutez la commande `install` pour démarrer le processus d'installation.

   Identity Manager affiche le panneau de bienvenue.
4. Cliquez sur **Next**. Identity Manager affiche le panneau de sélection du répertoire d'installation. Choisissez Upgrade et cliquez sur Next.
5. Entrez un emplacement pour le répertoire d'installation (ou cliquez sur **Browse** pour le rechercher) d'Identity Manager et cliquez sur **Next**.
6. Cliquez sur **Next** pour commencer la mise à jour.

   Identity Manager affiche le panneau récapitulatif de l'installation.

Remarque Cliquez sur **Details** pour obtenir des informations plus détaillées sur l'installation. En fonction de la quantité d'informations acquises pendant le processus d'installation, l'ensemble des messages peut ne pas être affiché ici. Affichez le fichier journal (identifié dans les détails) pour des informations plus détaillées. Lorsque vous avez terminé, cliquez sur **Close** pour quitter l'installateur.

7. Supprimez tous les fichiers Identity Manager compilés du répertoire de travail du serveur d'application.
8. Si le processus de mise à niveau ne l'a pas déjà fait, déplacez les fichiers de classe de correctifs du répertoire `WEB-INF/classes` vers le répertoire `patches/`*`HotfixName`*.

Étape 2 : Mettez à jour Sun Identity Manager Gateway

Si vous exécutez la Sun Identity Manager Gateway sur un système distant, procédez comme suit :

1. Connectez-vous au système Windows 2000 où la Sun Identity Manager Gateway est installée.
2. Accédez au répertoire où la passerelle est installée.
3. Arrêtez le service de la passerelle en exécutant la commande :

   ```
   gateway -k
   ```
4. Sous Windows 2000 ou version ultérieure, quittez toutes les instances du plug-in Services MMC.
5. Supprimez les fichiers de passerelle existants.
6. Si la passerelle juste mise à jour est installée sur un système qui n'est pas le serveur d'Identity Manager, copiez le fichier `gateway.zip` depuis l'emplacement où l'image d'installation a été décompressée.
7. Décompressez le fichier `gateway.zip` dans le répertoire d'installation de la passerelle.
8. Démarrez le service de passerelle en exécutant la commande suivante :

   ```
   gateway -s
   ```

Vous pouvez aussi démarrer et arrêter la passerelle comme suit :

1. Ouvrez le panneau de configuration de Windows.
2. Ouvrez Services. (Dans Windows 2000, Services se trouve dans les Outils administratifs.)
3. Sélectionnez Sun Identity Manager Gateway.
4. Cliquez sur **Démarrer** ou **Arrêter**.

Mise à niveau manuelle d'Identity Manager

Dans certains environnements, il est nécessaire de procéder à la mise à jour manuelle au lieu de recourir au programme d'installation et de mise à niveau d'Identity Manager.

Remarques :

- Assurez-vous de définir la variable d'environnement `JAVA_HOME`.
- Assurez-vous que le répertoire `bin` situé au sein du répertoire `JAVA_HOME` se trouve dans le chemin.
- Les correctifs installés auparavant sont archivés dans le répertoire `$WSHOME/patches/`*`NomCorrectif`*.
- Avant la mise à niveau, restaurez le compte Configurator intégré afin qu'il se nomme Configurator et dispose de la capacité d'importation. En outre, le mot de passe pour ce compte doit être configurator. Après la mise à niveau, rétablissez le compte Configurator dans son état préalable à la mise à niveau. Au besoin, renommez ce compte et changez le mot de passe avant déploiement dans votre environnement de production.

Procédez comme suit pour mettre Identity Manager à jour manuellement :

1. Arrêtez le serveur d'application et Sun Identity Manager Gateway.
2. Entrez la suite de commandes suivante :

   Sur les plates-formes Windows prises en charge

   a. Définissez votre environnement :

   ```
   set SPPATH=Chemin d'accès aux fichiers du pack de service
   set WSHOME=Chemin de l'installation d'Identity Manager
   OU Répertoire de transfert
   set TEMP=Chemin d'accès au répertoire temporaire
   ```

   b. Exécutez le prétraitement :

   ```
   mkdir %TEMP%
   cd /d %TEMP%
   jar -xvf %SPPATH%\IDPAK2005Q4M3_SP4.jar \
   WEB-INF\lib\idm.jar \ WEB-INF\lib\idmcommon.jar \
   WEB-INF\lib\idmformui.jar
   set TMPLIBPTH=%TEMP%\WEB-INF\lib
   set CLASSPATH=%TMPLIBPTH%\idm.jar;\
   %TMPLIBPTH%\idmcommon.jar;%TMPLIBPTH%\idmformui.jar
   java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
      com.waveset.install.UpgradePreProcess
   ```

c. Installez le logiciel :

```
cd %WSHOME%
jar -xvf %SPPATH%\IDM.jar
```

d. Exécutez le post-traitement :

```
java -classpath %CLASSPATH% -Dwaveset.home=%WSHOME%
  com.waveset.install.UpgradePostProcess
```

Sur les plates-formes UNIX prises en charge

a. Définissez votre environnement :

`export SPPATH=`***Chemin d'accès aux fichiers extraits du pack de service***
`export WSHOME=`***Chemin d'installation d'Identity Manager***
`OU` ***Répertoire de transfert***
`export TEMP=`***Chemin d'accès au répertoire temporaire***

b. Exécutez le prétraitement :

```
mkdir $TEMP
cd $TEMP
jar -xvf $SPPATH/IDPAK2005Q4M3_SP4.jar \
WEB-INF/lib/idm.jar WEB-INF/lib/idmcommon.jar \
WEB-INF/lib/idmformui.jar
CLASSPATH=$TEMP/WEB-INF/lib/idm.jar:\
$TEMP/WEB-INF/lib/idmcommon.jar:\
$TEMP/WEB-INF/lib/idmformui.jar
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME \
com.waveset.install.UpgradePreProcess
```

c. Installez le logiciel :

```
cd $WSHOME
jar -xvf $SPPATH/IDM.jar
```

d. Exécutez le post-traitement :

```
java -classpath $CLASSPATH -Dwaveset.home=$WSHOME
  com.waveset.install.UpgradePostProcess
```

3. Passez au répertoire `$WSHOME/bin/solaris` ou `$WSHOME/bin/linux`, puis définissez les autorisations sur les fichiers du répertoire de manière à les rendre exécutables.
4. Si vous avez procédé à une installation dans un répertoire de transfert, créez un fichier `.war` à des fins de déploiement vers le serveur d'application.

Remarque Consultez le chapitre correspondant dans *Sun Java™ System Identity Manager Installation* pour des instructions spécifiques au serveur.

5. Supprimez les fichiers d'Identity Manager du répertoire de travail du serveur d'application.

6. Si le processus de mise à niveau ne l'a pas déjà fait, déplacez les fichiers de classe de correctifs du répertoire `WEB-INF/classes` vers le répertoire `patches/`*`HotfixName`*.
7. Démarrez le serveur d'application.
8. Mettez à jour la base de données d'Identity Manager. Consultez la section précédente *Étape 2 : Mettez à jour Sun Identity Manager Gateway* pour des instructions détaillées.
9. Procédez à la mise à jour, puis redémarrez Sun Identity Manager Gateway. Consultez la section précédente *Étape 2 : Mettez à jour Sun Identity Manager Gateway* pour des instructions détaillées.

Ajouts et corrections de la documentation

À propos des guides du logiciel de système d'identité

La documentation du logiciel de système d'identité est organisée en plusieurs guides, qui sont fournis au format Acrobat (`.pdf`) sur le CD Identity Install Pack. La version inclut les guides suivants.

Logiciel de système d'identité

Installation du package d'installation (`Identity_Install_Pack_Installation_2005Q4M3.pdf`) — Décrit l'installation et la mise à jour du logiciel de système d'identité.

Identity Manager

- *Identity Manager Administration* (`IDM_Administration_2005Q4M3.pdf`) — Présente les interfaces administrateur et utilisateur d' Identity Manager.
- *Identity Manager Upgrade* (`IDM_Upgrade_2005Q4M3.pdf`) — Fournit des informations facilitant la planification et l'exécution des mises à niveau.

Remarque Pour cette version, les publications *Identity Manager Technical Deployment* et *Identity Manager Technical Reference* ont été réorganisés en plusieurs ouvrages, à savoir :

- *Identity Manager Technical Deployment Overview* (`IDM_Deployment_Overview_2005Q4M3.pdf`) — Présentation conceptuelle du produit Identity Manager (architectures des objets comprise) avec une introduction aux composants de base du produit.
- *Identity Manager Workflows, Forms, and Views* (`IDM_Workflows_Forms_Views_2005Q4M3.pdf`) — Informations de référence et procédurales décrivant l'utilisation des flux de travaux, formulaires et vues d' Identity Manager — inclut des informations sur les outils dont vous avez besoin pour personnaliser ces objets.
- *Identity Manager Deployment Tools* (`IDM_Deployment_Tools_2005Q4M3.pdf`) — Informations de référence et procédurales décrivant l'utilisation des différents outils de déploiement d'Identity Manager et notamment des règles et des bibliothèques de règles, des tâches et processus communs, du support des dictionnaires et de l'interface du service Web basée sur SOAP fournie par le serveur Identity Manager.

- *Identity Manager Resources Reference* (`IDM_Resources_Reference_2005Q4M3.pdf`)— Informations de référence et procédurales décrivant le chargement et la synchronisation des informations de compte d'une ressource dans Sun Java™ System Identity Manager. Les adaptateurs supplémentaires sont documentés dans `ResourcesRef_Addendum_2005Q4M3SP1.pdf`
- *Identity Manager Audit Logging* (`IDM_Audit_Logging_2005Q4M3.pdf`) — Informations de référence et procédurales décrivant le chargement et la synchronisation des informations de compte d'une ressource dans Sun Java™ System Identity Manager.
- *Identity Manager Tuning, Troubleshooting, and Error Messages* (`IDM_Troubleshooting_2005Q4M3.pdf`) — Informations de référence et procédurales décrivant les messages d'erreur et les exceptions d' Identity Manager, fournit des instructions pour le suivi et le dépannage des problèmes auxquels vous risquez de vous heurter en travaillant.

Identity Auditor

Identity Auditor Administration (`IDA_Administration_2005Q4M3.pdf`) : contient la présentation de l'interface administrateur d'Identity Auditor.

Identity Manager Service Provider Edition

- *Identity Manager Service Provider Edition Administration Addendum* (`SPE_Administration_Addendum_2005Q4M3SP1.pdf`) : présente les fonctions d'Identity Manager SPE.
- *Identity Manager Service Provider Edition Deployment* (`SPE_Deployment_2005Q4M3_SP1.pdf`) : fournit des informations sur le déploiement d'Identity Manager SPE.

Navigation dans les guides en ligne

Utilisez la fonction Signets d'Acrobat pour naviguer dans les guides. Cliquez sur le nom d'une session dans le panneau des signets pour aller directement à son emplacement dans le document.

L'ensemble de documentation d'Identity Manager peut être visualisé depuis toute installation d'Identity Manager en navigant vers `idm/doc` dans un navigateur Web.

Installation du package d'installation

Corrections

Préface

La référence croisée erronée à l'Annexe H dans Comment trouver les informations dans ce guide a été supprimée. (ID-12369)

Chapitre 1 : Opérations préliminaires à l'installation

- Microsoft Exchange 5.5 a été supprimé du tableau des ressources prises en charge. Il a été désapprouvé. (ID-12682)
- Lotus Notes® 6.5.4 (Domino) a été ajouté au tableau des ressources prises en charge. (ID-12226)
- JDK 1.5 a été ajouté comme version de Java prise en charge à plusieurs reprises. (ID-12984)
- Les informations SAP des systèmes ERP dans le tableau des ressources prises en charge ont été modifiées comme suit : (ID-12635)
  - SAP® R/3 v4.5, v4.6
  - SAP® R/3 Enterprise 4.7 (SAP BASIS 6.20)
  - SAP® NetWeaver Enterprise Portal 2004 (SAP BASIS 6.40)
  - SAP® NetWeaver Enterprise Portal 2004s (SAP BASIS 7.00)
- Les informations Red Hat dans le tableau des ressources prises en charge ont été modifiées comme suit :
  - Red Hat Linux Advanced Server 2.1
  - Red Hat Linux Enterprise Server 3.0, 4.0
- La section Serveurs de bases de données de référentiel et les informations ci-après ont été ajoutées dans Logiciels et environnements pris en charge : (ID-12425)
  - IBM® DB2® Universal Database pour Linux, UNIX® et Windows® (version 7.x, 8.1, 8.2)
  - Microsoft SQL Server™ 2000
  - MySQL™ 4.1
  - Oracle 9i® et Oracle Database 10g, 10gR1 et 10gR2®

Chapitre 2 : Installation d'Identity Install Pack pour Tomcat

Le chapitre couvre désormais le serveur d'application Apache Tomcat, Versions 4.1.x ou 5.0.x.

Chapitre 4 : Installation d'Identity Install Pack pour Websphere

- Le chapitre traite maintenant de l'installation de Websphere 5.1 express et 6.0. (ID-12655, 12656) Les remarques et informations suivantes ont été ajoutées aux points indiqués :

Remarque L'étape suivante n'est pas nécessaire pour installer Identity Install Pack 6.0 ou version ultérieure.

4. Passez au répertoire de transfert et supprimez les fichiers suivants, au besoin :

```
WEB-INF\lib\cryptix-jce-provider.jar
WEB-INF\lib\cryptix-jce-api.jar
```

25. Téléchargez le plus récent `jlog package` de WebSphere à l'adresse :

```
http://www.alphaworks.ibm.com/tech/loggingtoolkit4j
```

Remarque Le `jlog package` est dorénavant intégré à WebSphere'6.0. Ne le téléchargez que pour les versions antérieures.

- Étant donné que vous devez installer JDK 1.4.2 pour cette version, la section *Pour JDK 1.3.x :* n'est plus applicable. Dans le même chapitre, la section *Pour JDK 1.4* doit être remplacée par *Pour JDK 1.4.2*.

Chapitres 7 et 8 : Installation d'Identity Install Pack pour Sun ONE/Sun Java System Application Server 7/8

- Les informations corrigées suivantes ont été ajoutés dans les Étapes d'installation > Étape 5 : Edit the server.policy File > exemples de permission : (ID-12292)

```
permission java.io.FilePermission
"/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/
idm/config/trace1.log", "read,write,delete";

permission java.io.FilePermission "$(java.io.tmpdir)$(/)*",
"read,write,delete";
```

- Les informations suivantes ont été ajoutés dans les Étapes d'installation > Étape 5 : Edit the server.policy File > exemples de permission :

  Pour exécution avec Identity Manager Service Provider Edition, ajoutez la permission suivante aux entrées de fichier server.policy ci-dessus.

```
permission java.lang.RuntimePermission "shutdownHooks";
```

Chapitre 14 : Désinstallation des applications

*Version* a été supprimé de l'exemple de syntaxe dans Supprimer le logiciel > sous UNIX > Étape 3. (ID-7762)

Chapitre 15 : Installation des applications (installation manuelle)

L'exemple de syntaxe a été corrigé dans Étapes d'installation > Étape 3: Configuration de l'identité `Pack d'installation Connexion à la base de données index > Environnements non-Xwindows > Étape 3 à :` (ID-5821)

3. Définissez votre clé de licence avec les commandes suivantes :

```
cd idm/bin
./lh license set -f LicenseKeyFile
```

Annexe A : Référence de la base de données index

La ligne décrivant le serveur SQL a été modifiée de la manière suivante :

Sélection	Saisie
Serveur SQL **Valeurs par défaut à utiliser avec le pilote JDBC de Microsoft SQL Server 2005 :** • **URL :** « jdbc:sqlserver://host.your.com:1433;DatabaseName=dbname » • **Pilote JDBC :** com.microsoft.sqlserver.jdbc.SQLServerDriver • **Connexion comme utilisateur :** waveset Utilisez les valeurs suivantes avec le pilote JDBC de Microsoft SQL Server 2000 : • **URL :** « jdbc:microsoft:sqlserver://host.your.com:1433;DatabaseName=dbname;SelectMethod=Cursor » • **Pilote JDBC :** com.microsoft.jdbc.sqlserver.SQLServerDriver • **Connexion comme utilisateur :** waveset	Indiquez l'emplacement de la base de données d'index et le mot de passe sélectionné lors de la configuration de la base de données. **Remarque :** toutes les connexions au serveur SQL doivent être effectuées au moyen de la même version du pilote JDBC. Cela inclut le référentiel de même que l'ensemble des adaptateurs de ressources gérant ou nécessitant des comptes ou tables SQL Server, notamment ceux de Microsoft SQL, de Microsoft Identity Integration Server, de Database Table, de Scripted JDBC et tout autre adaptateur personnalisé basé sur ces modèles. Des erreurs de conflit se produisent si vous tentez d'utiliser des versions différentes du pilote.

Annexe C : Configuration des sources de données pour Identity Manager

- Plusieurs URL IIOP ne sont pas prises en charge. (ID-12499) Les informations erronées suivantes ont été supprimées de Configuration d'une source de données WebSphere pour Identity Manager > Configuration d'une source de données Websphere 5> Configuration d'une source de données dans un cluster Websphere :

  Lorsque les serveurs d'application n'ont pas le même port spécifié dans la propriété **BOOTSTRAP_ADDRESS**, java.naming.provider.url peut spécifier plusieurs URL, par exemple :

  `iiop://localhost:9812,iiop://localhost:9813.`

- Toutes les propriétés j2c.qui étaient utilisées dans la version 5 de WebSphere font maintenant partie du fichier resources.xml dans WebSphere version 6. Des informations relatives à Configuration d'une source de données Websphere 5.1/6.x et à Configuration des données d'authentification 6.x ont été ajoutées. Les informations relatives à Configuration d'une source de données Websphere 4.x ont été supprimées. (ID-12767) Modifications concernées dans les sections suivantes :

Configuration d'un fournisseur JDBC

Utilisez la console d'administration de WebSphere pour configurer un nouveau fournisseur JDBC.

1. Cliquez sur l'onglet **Resources** dans le panneau de gauche pour afficher la liste des types de ressources.
2. Cliquez sur **JDBC Providers** pour afficher un tableau des fournisseurs JDBC configurés.
3. Cliquez sur le bouton **New** au-dessus du tableau des fournisseurs JDBC configurés.
4. Choisissez le type jdbc et le type d'implémentation dans la liste des types de bases de données JDBC. Cliquez sur Next.

   Oracle, Oracle JDBC Drive, et Connection pool Data Source sont utilisés dans cet exemple.
5. Continuez la configuration des propriétés générales.
   - Spécifiez le nom.
   - Spécifiez le chemin d'accès au JAR qui contient le pilote JDBC dans le champ **Classpath**. Par exemple, pour spécifier le pilote léger Oracle, spécifiez un chemin d'accès similaire au suivant :

   ```
   /usr/WebSphere/AppServer/installedApps/idm/idm.ear/idm.war/WEB-INF/lib/oraclejdbc.jar
   ```

   Remarque Vous pouvez utiliser la console d'administration pour spécifier le chemin d'accès au JAR qui contient le pilote JDBC. Dans le menu intitulé **Environment**, sélectionnez l'option **WebSphere Variable.** Dans ce panneau, choisissez d'abord le **noeud**, **de cellule** et le **serveur** pour lesquels définir cette variable d'environnement. Spécifiez ensuite le chemin d'accès au JAR comme valeur de cette variable.

   - Spécifiez le nom entièrement qualifié de la classe JDBC Driver dans le champ **Implementation ClassName**.
     - Pour le pilote léger Oracle, cette valeur est`oracle.jdbc.pool.OracleConnectionPoolDataSource`.
     - Pour le pilote db2 jcc, cette valeur est com.ibm.db2.jcc.DB2ConnectionPoolDataSource
   - Vous pouvez aussi changer le nom ou la description du fournisseur à votre guise.

     Un fois terminé, cliquez sur le bouton **OK** en bas du tableau. Le panneau de droite doit afficher le fournisseur que vous avez ajouté.

Pour configurer une source de données qui utilise ce fournisseur JDBC, consultez « Pointer le référentiel Identity Manager vers la source de données ».

Configuration d'une source de données JDBC Websphere

1. Utilisez la console administrative de WebSphere pour définir une source de données avec un fournisseur JDBC existant. Si vous devez définir un nouveau fournisseur JDBC pour utilisation avec Identity Install Pack, reportez-vous à la section « Configuration d'un fournisseur JDBC ».

Avant de terminer la configuration de la source de données, vous devez configurer les données d'authentification. Les alias contiennent les informations d'identification utilisées pour connexion aux DBMS.

Configurez les données d'authentification 5.1

1. Cliquez sur l'onglet **Security** dans le panneau de gauche pour afficher la liste des types de configuration de sécurité.
2. Cliquez sur l'onglet **JAAS Configuration** dans le panneau de gauche pour afficher la liste des types de configuration JAAS.
3. Cliquez sur l'onglet **J2C Authentication Data** dans le panneau de gauche. Le panneau de droite affiche le tableau des entrées de données d'authentification.
4. Cliquez sur le bouton **New** au-dessus du tableau des entrées de données d'authentification. Le panneau de droite affiche le tableau des propriétés générales qui peuvent être configurées.
5. Configurez les propriétés générales de la nouvelle entrée de données d'authentification. Notez ce qui suit :
   - **Alias** est le nom qui figurera dans la liste de sélection en cas de configuration des informations d'identification DBMS pour une source de données.
   - **UserID** est le nom utilisé pour connexion au DBMS.
   - **Password** est le mot de passe utilisé pour connexion au DBMS.

Configurez ensuite la source de données.

Configurez les données d'authentification 6.x

1. Cliquez sur **Security > Global security**.
2. Sous Authentication, cliquez sur **JAAS configuration > J2C authentication data**. Le panneau **J2C Authentication Data Entries** est affiché.
3. Cliquez sur **New**.
4. Entrez un alias unique, une ID utilisateur valide, un mot de passe valide et une courte description (facultative).
5. Cliquez sur **OK** ou sur **Apply**. Aucune validation de l'ID et du mot de passe utilisateur n'est requise.

6. Cliquez sur **Save**.

Remarque L'entrée juste créée est visible sans redémarrer le processus du serveur d'application pour utilisation dans la définition de source de données. Toutefois l'entrée ne prend effet qu'après redémarrage du serveur.

Configurez la source de données

Remarque Si vous configurez une source de données dans un cluster Websphere 5.x, consultez "Configurer la source de données dans un cluster Websphere" pour des informations plus détaillées.

1. Cliquez sur l'onglet **Resources** dans le panneau de gauche pour afficher la liste des types de ressources.
2. Cliquez sur **JDBC Providers** pour afficher un tableau des fournisseurs JDBC configurés.
3. Cliquez sur le nom d'un fournisseur JDBC dans le tableau. Le panneau de droite affiche le tableau des propriétés générales configurées pour le fournisseur JDBC sélectionné.
4. Faites défiler jusqu'au tableau de propriétés supplémentaires. Cliquez sur **Data Sources**. Le panneau de droite affiche le tableau des sources de données configurées pour utilisation avec ce fournisseur JDBC.

Remarque Notez le champ **Scope** en haut du cadre dans la console d'administration de WebSphere. Vérifiez que **Node** et **Server** sont vides que sorte que les informations de cellule soient présentées pour configuration sous les boutons **New** et **Delete**.

5. Cliquez sur le bouton **New** au-dessus du tableau des sources de données. Le panneau de droite affiche le tableau des propriétés générales à configurer.
6. Configurez les propriétés générales de la nouvelle source de données. Notez ce qui suit :
   - **JNDI Name** est le chemin d'accès à l'objet source de données dans le service de répertoire.
     Vous devez spécifier cette même valeur comme argument `-f` dans `setRepo -t`*`dbms`* `-i`*`initCtxFac`* `-f`*`filepath`*.
   - **Container-managed persistence** ne doit pas être coché. Identity Install Pack n'utilise pas les Enterprise Java Beans (EJB).
   - **Component-managed Authentication Alias** pointe vers les informations d'identification utilisées pour accéder au DBMS (vers lequel cette source de données pointe).
   - Sélectionnez dansla liste déroulante l'alias qui contient l'ensemble d'informations d'identification DBMS approprié. Pour plus d'informations, voir *Configurez les données d'authentification 5.1*.

- **Container-managed Authentication Alias** n'est pas utilisé Définissez cette valeur sur `(none)`. Identity Install Pack établit sa propre connexion au DBMS (vers lequel cette source de données pointe).
- Cliquez sur **OK** une fois panneau configuré. La page Data Sources est affichée.

7. Cliquez sur la source de données que vous avez créée. Faites ensuite défiler jusqu'au tableau des propriétés supplémentaire près du bas. Cliquez sur le lien **Custom Properties**.

   Le panneau de droite affiche le tableau des propriétés DBMS spécifiques.

8. Configurez les propriétés personnalisées pour cette source de données. Cliquez sur le lien de chaque propriété pour définir sa valeur. Notez ce qui suit :
   - **URL** est la seule propriété obligatoire. Cette URL de base de données identifie l'instance de base de données qui contient driverType, serverName, portNumber et databaseName. Vous pouvez aussi spécifier certaines de ces propriétés individuelles.
   - dans cet exemple, **driverType** est léger.
   - **serverName** est un nom d'hôte (ou une adresse IP).
   - **databaseName** est généralement un nom de base de données court.
   - **portNumber** est 1521 par défaut pour Oracle.
   - **preTestSQLString** peut être configuré sur une valeur comme SELECT 1 FROM USEROBJ. La demande SQL confirme que le tableau USERJOB existe et qu'il est accessible.
9. Depuis le tableau des propriétés supplémentaires, vous pouvez aussi cliquer sur le lien **Connection Pool** si vous souhaitez configurer ces propriétés pour le réglage des performances.

Annexe E : Configuration JCE

La remarque suivante doit figurer :

Remarque Étant donné que vous devez installer JDK 1.4.2 pour cette version, tous les environnements pris en charge devraient disposer de JCE 1.2 et les informations contenues dans cette annexe ne sont plus applicables.

Ajouts

Chapitre 1 : Opérations préliminaires à l'installation

- La remarque suivante a été ajoutée sous Configuration du flux de tâches > Puce Installer et configurer le logiciel Identity Install Pack : (ID-8431)

Remarque Sur les systèmes Unix ou Linux :

- Lors de l'installation des versions 5.0 – 5.0 SP1 d'Identity Install Pack, `/var/tmp` doit exister et être inscriptible par l'utilisateur qui exécute le programme d'installation.
- Lors de l'installation des versions 5.0 SP2 et supérieures d'Identity Install Pack, `/var/opt/sun/install` doit exister et être inscriptible par l'utilisateur qui exécute le programme d'installation.

- Les notes suivantes ont été ajoutées aux tâches préalables > Configurer une base de données index > Configurer un serveur SQL > étape 3b : (ID-11835)

Remarque Les fichiers suivants doivent se trouver dans le répertoire `$WSHOME/WEB-INF/lib` :

```
db2jcc
db2jcc_license_cisuz.jar or db2jcc_license_cu.jar
```

- La note suivante a été ajoutée sous Logiciels et environnements pris en charge > Serveurs d'application : (ID-12385)

Remarque Votre conteneur de serveur d'application actuel doit prendre UTF-8 en charge.

Chapitre 2 : Installation d'Identity Install Pack pour Tomcat

- L'étape suivante a été ajoutés dans les Étapes d'installation > Étape 1 : Installer le logiciel Tomcat > Installation sur UNIX : (ID-12487)

  2. Ajoutez les fichiers Java `mail.jar` et `activation.jar` au répertoire `./tomcat/common/lib`. Les fichiers jar mail et activation se trouvent à l'adresse :

```
http://java.sun.com/products/javamail
http://java.sun.com/products/beans/glasgow/jaf.html
```

- Les étapes suivantes ont été ajoutées dans les Étapes d'installation > Étape 1 : Installer le logiciel Tomcat > Installation sur UNIX : (ID-12462)

  3. Lorsque vous configurez Tomcat pour la prise en charge UTF-8, ajoutez l'attribut `URIEncoding="UTF-8"` à l'élément *connector* dans le fichier *`TOMCAT_DIR`*`conf/server.xml`, par exemple :

```
<!—Définissez un connecteur Coyote HTTP/1.1 non SSL sur le port
spécifié pendant l'installation -->
<Connector port="8080"
           maxThreads="150"
           minSpareThreads="25"
           maxSpareThreads="75"
           enableLookups="false" redirectPort="8443"
           acceptCount="100" debug="0" connectionTimeout="20000"
           disableUploadTimeout="true"
           URIEncoding="UTF-8" />
```

  4. Lorsque vous configurez Tomcat pour la prise en charge UTF-8, ajoutez également `-Dfile.encoding=UTF-8` dans vos options de machine virtuelle Java.

Chapitre 13 : Mise à jour d'Identity Manager

Une référence croisée vers la mise à niveau d'Identity Manager pour aider les utilisateurs à trouver les informations de mise à niveau complètes a été ajoutée. (ID-12366)

Chapitre 15 : Installation des applications (installation manuelle)

La remarque suivante a été ajoutée dans les Étapes d'installation > Étape 2 : Installer le logiciel d'application : (ID-8344)

Remarque À partir de la version 5.0 SP3, les classes d'adaptateur sont contenues dans le fichier `idmadapter.jar`. Si vous disposez d'un adaptateur personnalisé, vous devez peut-être mettre à jour votre chemin de classe.

Annexe B : Configuration de MySQL

Les informations suivantes ont été ajoutées sous Configuration de MySQL > étape 3 Démarrage du processus MySql : (ID-12461)

Si ce processus n'a pas été démarré, procédez comme suit pour enregistrer et démarrer MySQL.
Sous Windows, si vous installez un autre répertoire que `c:\mysql`créez un fichier appelé `c:\my.cnf` avec le contenu suivant :

```
[mysqld]
basedir=d:/mysql/
default-character-set=utf8
default-collation=utf8_bin
```

Sous Windows, installez et démarrez le service :

```
cd <MySQL_Install_Dir>/bin
mysqld-nt --install
net start mysql
```

Annexe C : Configuration des sources de données pour Identity Manager

Les informations suivantes ont été ajoutées sous Configurer une source de données Websphere pour Identity Manager > Pointer le référentiel Identity Manager vers la source de données : (ID-12071)

8. Pointez le référentiel vers le nouvel emplacement. Par exemple :

```
lh -Djava.ext.dirs=$JAVA_HOME/jre/lib/ext:$WAS_HOME/lib setRepo
-tdbms -iinitCtxFac
-ffilepath -uiiop://localhost:bootstrap_port
-Uusername
-Ppassword
-toracle icom.ibm.websphere.naming.WsnInitialContextFactory -
fDataSourcePath
```

Dans l'exemple ci-dessus, *DataSourcePath* peut être `jdbc/jndiname`. `bootstrap_port` est le port d'adresse de démarrage du serveur WebSphere.

L'option `-Djava.ext.dirs` ajoute tous les fichiers JAR dans les répertoires WebSphere `lib/` et `java/jre/lib/ext/` à CLASSPATH. Cela est nécessaire pour que la commande setrepo fonctionne normalement.

Changez l'option `-f` pour qu'elle corresponde à la valeur spécifiée pour le champ **JNDI Name** lors de la configuration de la source de données. Voir Référence setrepo pour plus d'informations sur cette commande.

Guide Identity Manager Upgrade

Ajouts

Chapitre 1 : Vue d'ensemble de la mise à niveau

L'élément suivant a été ajouté dans la section *Exemple de mise à niveau*: (ID-12467)

Soyez prudent lorsque vous éditez le champ de super rôle dans le formulaire de rôle. Le super rôle peut-être lui même un rôle imbriqué. Les super et sous-rôles indiquent une imbrication des rôles et de leurs ressources ou groupes de ressources associés. Lorsqu'il est appliqué à un utilisateur, le super rôle inclut les ressources associées à tout sous-rôle désigné. Le champ de super rôle est affiché pour indiquer les rôles qui contiennent le rôle affiché.

Chapitre 3 : Développer le plan de mise à niveau

Ce qui suit a été ajouté à la section Mise à niveau de l'environnement d'Identity Manager 5.x vers 6.x. (ID-12361)

Etape 2 : Mettre à jour le schéma de la base de données référentielle

Identity Manager 6.0 introduit un changement de schéma qui fournit de nouveaux tableaux pour les tâches, les groupes, les organisations et le tableau du journal syslog. Vous devez créer ces nouvelles structures de tableaux et déplacer les données existantes.

Remarque Avant de mettre à jour le schéma du référentiel, effectuez une sauvegarde complète des tableaux de référentiel.

1. Identity Manager utilise deux tableaux pour stocker les objets utilisateur. Les exemples de script (dans le répertoire `sample`) peuvent servir à effectuer les modifications de schéma.

   Reportez-vous au script `sample/upgradeto2005Q4M3.`*`DatabaseName`* pour mettre à jour vos tableaux de référentiel.

Remarque La mise à niveau des bases de données MySQL est très intense. Pour plus d'informations à ce sujet, reportez-vous au fichier `sample/upgradeto2005Q4M3.mysql`.

Guide Identity Manager Administration

Ajouts

- Si l'ouverture est configurée, créer un utilisateur crée un élément de travail qui peut être affiché depuis l'onglet **Approbations**. Approuver cet élément remplace la date d'ouverture et crée le compte, rejeter l'élément annule la création du compte.
- Lors de la planification de la réconciliation, vous pouvez fournir le nom d'une règle pour qu'elle soit utilisée pour personnaliser la planification. Par exemple, une règle pourra repousser les réconciliations prévues pour un samedi au lundi suivant. (ID-11391)

Chapitre 4 : Administration

- Des informations sur la fonction de délégation des approbations ont été ajoutées. (ID-12754)

Délégation des approbations

Si vous avez des capacités d'approbateur, vous pouvez déléguer vos futures demandes d'approbation à un ou plusieurs utilisateurs (délégués) pendant une durée spécifique. Il n'est pas nécessaire que les utilisateurs possèdent des capacités d'approbateur pour être délégués.

La fonction de délégation ne s'applique qu'aux demandes d'approbation à venir. Les demandes existantes (qui figurent dans l'onglet En attente d'approbation) sont transmises par la fonction de transfert.

Pour configurer la délégation, sélectionnez l'onglet**Delegate My Approvals** dans la zone **Approvals.**

Remarques

- L'accès à la fonction délégation est disponible si vous possédez une capacité qui vous octroie le droit d'accès à WorkItem ou toute extension authType de WorkItem, notamment Approval, OrganizationApproval, ResourceApproval et RoleApproval ; ou tout sous-type personnalisé qui étend WorkItem ou l'un de ses authTypes.
- Vous pouvez aussi déléguer les approbations depuis l'onglet de formulaire Security des pages Create/Edit/View User et depuis le menu principal de l'interface utilisateur.

Les délégués peuvent approuver pour votre compte toutes les demandes pendant la période de délégation effective. Les demandes d'approbation déléguées contiennent le nom du délégué.

Entrées du journal d'audit pour les demandes

Les entrés du journal d'audit pour les demandes d'approbation approuvées et rejetées contiennent votre nom (le délégataire) si la demande est déléguée. Les modifications des informations d'approbateur délégué d'un utilisateur sont journalisées dans la section des modifications détaillées de l'entrée du journal d'audit lorsqu'un utilisateur est créé ou modifié.

Chapitre 5 : Configuration

- Des informations relatives à la configuration des attributs d'identité lorsqu'une ressource est créée ou mise à jour ont été ajoutées. (ID-12606)

Configuration des attributs d'identité à partir des changements de ressource

Les attributs d'identité définissent la relation mutuelle des attributs sur les ressources. Lorsque vous créez ou modifiez une ressource, les relations de ces attributs peuvent être affectées.

Lorsque vous enregistrez une ressource, Identity Manager affiche la page Configurer les attributs d'identité ? Dès lors, vous pouvez choisir parmi les possibilités suivantes :

- Continuer vers la page Configurer les attributs d'identité à partir des modifications apportées aux ressources et configurer les attributs. Cliquez sur **Oui** pour continuer.
- Revenir à la liste de ressources. Cliquez sur **Non** pour revenir.
- Désactiver cette page pour les prochaines mises à jour de la ressource. Cliquez sur **Ne plus me poser cette question** pour désactiver cette page.

Remarque Le bouton **Ne plus me poser cette question** n'est visible que pour les utilisateurs qui ont la capacité de modifier la métavue.

Page Réactiver la configuration des attributs d'identité ?

Lorsque cette page est désactivée, utilisez l'une des méthodes suivantes pour la réactiver :

- Utilisez la fonction de débogage d'Identity Manager pour éditer l'objet WSUser de l'utilisateur connecté. Changez la valeur de la propriété `idm_showMetaViewFromResourceChangesPage` pour `vrai`.

- Ajoutez un champ similaire à l'exemple suivant au formulaire utilisateur (par exemple, le Tabbed User Form) puis utilisez la page Edit User pour changer la valeur de ce paramètre :

```
<Field name='accounts[Lighthouse].properties.displayMetaViewPage'>
  <Display class='Checkbox'>
    <Property name='label' value='Display Meta View?'/>
  </Display>
</Field>
```

Configuration des attributs

Utilisez Configurer les attributs d'identité de la page des modifications apportées aux ressources afin de sélectionner les attributs dans les cartes schématiques des ressources modifiées à utiliser comme sources et cibles des attributs d'identité. Dans certains cas, vous ne pouvez pas sélectionner d'attributs dans les colonnes Source et Cible. Vous ne pouvez pas sélectionner un attribut comme source dans les cas suivants :

- Il est marqué comme crypté dans la carte schématique.
- Il est marqué en écriture seule dans la carte schématique.

Vous ne pouvez pas sélectionner un attribut comme cible dans les cas suivants :

- Un attribut d'identité est stocké de façon globale sous le même nom. Par exemple, s'il existe un attribut d'identité global intitulé « firstname », l'option cible de firstname est sélectionnée et ne peut pas être désélectionnée.
- L'attribut est marqué en lecture seule dans la carte schématique.
- Les fonctions de création et de mise à jour de la ressource sont désactivées et ne sont pas prises en charge par la ressource.

Chapitre 7 : Sécurité

- La remarque suivante a été insérée dans la section « Configuring Authentication for Common Resources » (Configuration de l'authentification des ressources communes). (ID-16805)

  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 non plus dans la définition du module de connexion, cette fonctionnalité ne se comportera pas correctement.

- Des informations relatives aux limitations de session de connexion simultanée ont été ajoutées. (ID-12778)

Limitation des sessions de connexion simultanées

Par défaut, un utilisateur d'Identity Manager peut disposer de sessions de connexion simultanées. Vous pouvez toutefois limiter les sessions simultanées à une par application de connexion en changeant la valeur de l'attribut de configuration `security.authn.singleLoginSessionPerApp` dans l'objet configuration système. 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 BPE). Changer la valeur de cet attribut pour `vrai` impose une session à connexion unique à chaque utilisateur.

Dans ce cas, un utilisateur ne peut se connecter qu'à une seule session ; toutefois, seule la dernière session de connexion demeure active et valide. Si l'utilisateur exécute une action dans une session invalide, il est automatiquement forcé hors de la session et celle-ci se termine.

Chapitre 8 : Génération de rapports

Dans la section intitulée Rapports récapitulatifs, la description du rapport utilisateur contient désormais la capacité de rechercher les utilisateurs par responsable : (ID-12690)

- **User** – 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.

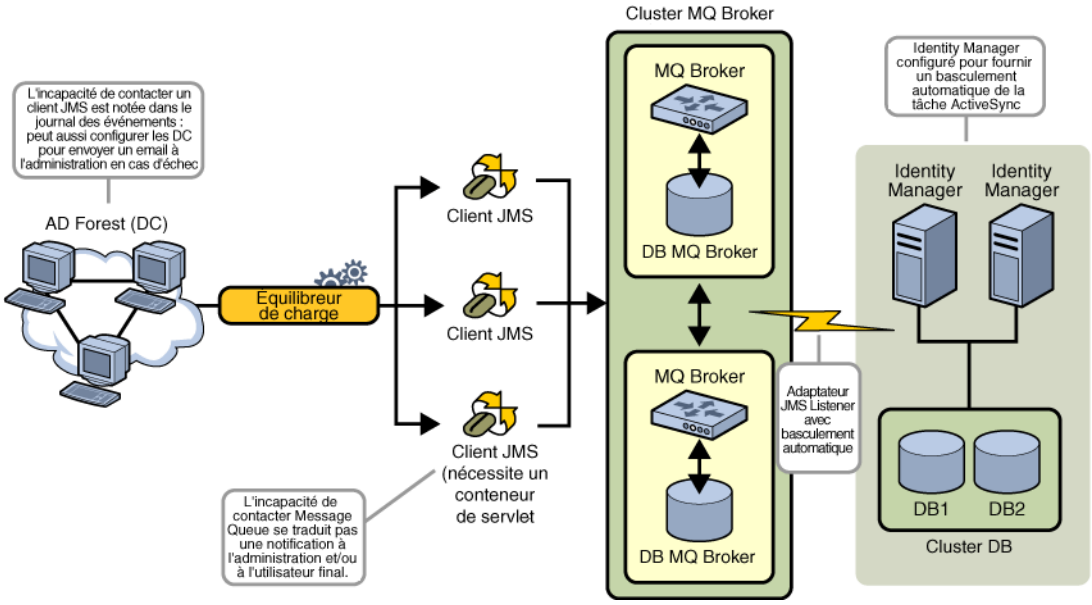
Chapitre 10 : PasswordSync

- Des instructions de configuration de Windows PasswordSync avec un serveur Sun JMS ont été ajoutées. Voir le document *Configuration de PasswordSync avec un serveur Sun JMS* qui accompagne ces notes de version. (ID-11788)
- La nouvelle section suivante sur la description de l'architecture haute disponibilité avec un basculement pour PasswordSync a été ajoutée. (ID-12634)
- Une section qui décrit comment implémenter PasswordSync sans utiliser de serveur de messagerie Java a été ajoutée. (ID-14974)

Déploiement de basculement pour Windows PasswordSync

L'architecture de PasswordSync permet l'élimination d'un tous les points d'échec individuels du déploiement de la synchronisation de mot de passe Windows pour Identity Manager.

Si vous configurez chaque Active Directory Domain Controller (ADC) pour se connecter à l'un parmi une série de clients JMS par l'intermédiaire d'un équilibrage de charge (voir la figure ci-après), les clients JMS peuvent envoyer des messages à un cluster Message Queue Broker, qui assure qu'aucun message n'est perdu en cas de défaillance d'une file d'attente de messages.



Remarque Votre cluster Message Queue nécessitera probablement une base de données pour la permanence des messages. (Les instructions de configuration d'un cluster Message Queue broker doivent être fournies dans la documentation de votre fournisseur.)

Le serveur Identity Manager qui exécute l'adaptateur JMS Listener configuré pour basculement automatique contactera le cluster Message Queue broker. Bien que l'adaptateur ne s'exécute que sur un seul Identity Manager à la fois, en cas de défaillance du serveur ActiveSync principal, l'adaptateur commence à rechercher les messages relatifs à un mot de passe sur un serveur Identity Manager secondaire et à propager les changements de mot de passe vers les ressources en aval.

Implémentation de PasswordSync sans service de messagerie Java

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. Configurez PasswordSync à l'aide des procédures décrites dans « Configuration de PasswordSync », avec les exceptions suivantes :

- Ne configurez pas les onglets de paramètres et de propriétés du JMS.
- Sous l'onglet Utilisateur, spécifiez l'ID de compte et le mot de passe à utiliser pour connexion à Identity Manager.

Si vous implémentez PasswordSync sans JMS, il est inutile de créer un adaptateur JMS Listener. Par conséquent, omettez les procédures indiquées dans « Déploiement de PasswordSync ». Si vous souhaitez configurer des notifications, vous devrez peut être modifier le flux de travaux Changer le mot de passe utilisateur.

Remarque Si vous exécutez ultérieurement l'application de configuration sans spécifier l'indicateur `-direct`, la configuration de PasswordSync nécessite un JMS. Relancez l'application avec l'indicateur `-direct` pour contourner à nouveau le JMS.

Corrections

Chapitre 5 : Ressources

Dans le tableau de classes de ressources personnalisées, la classe de ressource personnalisée pour l'adaptateur ClearTrust a été corrigée comme suit : (ID-12681)

```
com.waveset.adapter.ClearTrustResourceAdapter
```

Chapitre 10 : PasswordSync

Dans la section intitulée Configuration de PasswordSync, sous Boîte de dialogue des paramètres JMS, la description suivante Queue Name a été corrigée comme suit :

- **Queue Name** spécifie le nom de recherche de destination pour les événements de synchronisation de mot de passe. (ID-12621)

lh Reference

La syntaxe de commande a été mise à jour pour indiquer correctement un espace après les options spécifiées. (ID-12798)

Lorsque vous utilisez l'option -p, pour des raisons de sécurité, *Password* doit être spécifié sous forme de chemin d'accès à un fichier texte contenant un mot de passe, plutôt que directement au niveau de la ligne de commande.

Exemples

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console –u $user –p PathtoPassword.txt`
- `lh setup -U Administrator -P PathtoPassword.txt`
- `lh setup -U Administrator -P PathtoPassword.txt`
- `lh setRepo –t LocalFiles –f $WSHOME`

Commande license

Utilisation

```
license [options] { status | set {paramètres} }
```

Options

- `-U username` (si le compte Configurator est renommé)
- `-P PathtoPassword.txt` (si le mot de passe Configurator a changé)

Les paramètres de l'option `set` doivent adopter la forme `-f File`.

Identity Manager Workflows, Forms, and Views

Chapitre 1 : Flux de travaux

La présentation des actions manuelles dans ce chapitre doit contenir les informations suivantes :

Si le type `itemType` d'un élément de travail est défini sur l'assistant, l'élément de travail contournera par défaut l'obtention d'approbateurs de transfert lors de l'extraction de la vue Élément de travail. Si le type d'élément (itemType) est différent de l'assistant, Identity Manager extrait toujours les approbateurs de transfert à moins que la liste `CustomUserList` soit définie sur true (vrai) en tant que propriété du formulaire utilisée avec l'action manuelle. (ID-10777)

Pour cela, incluez le code suivant dans le formulaire:

```
<Form>
   <Properties>
      Property name='CustomUserLists' value='true'/>
   </Properties>
```

Chapitre 2 : Services de flux de travaux

- Le tableau Arguments du service de flux de travaux de session `createView` est inexact. Le tableau suivant décrit les arguments disponibles dans ce service.

Nom	Obligatoire	Valeurs correctes	Description
op	oui	`createView`	
viewid	oui		Spécifie le type d'affichage à créer.
options	non		Spécifie les options spécifiques de l'affichage. Les valeurs que vous pouvez passer sont spécifiques à la vue utilisée. La vue la plus courante est la vue Utilisateur. Les options figurent dans `session.UserViewConstants`. Les vues les plus simples devraient déclarer leurs constantes optionnelles dans le fichier `Viewer.java`. La deuxième vue la plus utilisée depuis le flux de travaux est très probablement ProcessViewer, suivie de PasswordViewer, DisableViewer, EnableViewer et RenameViewer. Elles ont par comparaison peu d'options.

- Identity Manager offre la méthode de service de flux de travaux `checkStringQualityPolicy`, qui contrôle la valeur d'une chaîne désignée par rapport à la stratégie associée à la chaîne. (ID-12428, 12440)

Nom	Obligatoire	Valeurs correctes	Description
policy	oui		Identifie la stratégie (chaîne)
mappage	non		Fournit un mappage des données que la chaîne ne doit pas contenir (mappage). `returnNull` -- (Facultatif) Défini sur vrai, la méthode retourne un objet nul après réussite.
value	oui		Spécifie la valeur de la chaîne à contrôler (objet).
pwdhistory	non		Liste les mots de passe précédents de l'utilisateur au format chiffré et en majuscules.
owner	oui		Identifie l'utilisateur dont la valeur de chaîne est en cours de contrôle.

  La méthode retourne un objet `checkPolicyResult`. Une valeur `true` indique que la chaîne passe le test de la stratégie. Si la chaîne ne passe pas le test de la stratégie, la méthode retourne un message d'erreur. Si vous avez défini l'option `returnNull` sur true dans le paramètre `map`, la méthode retourne un objet nul après réussite.

- Identity Manager propose désormais le service de flux de travaux auditPolicyScan (ID-12615). Faites appel à ce service de flux de travaux pour analyser les violations de stratégie d'audit de l'utilisateur en fonction des stratégies qui lui ont été assignées. Lorsqu'aucune stratégie n'est assignée à l'utilisateur, Identity Manager utilise une stratégie assignée à l'organisation, le cas échéant.

  Cette méthode admet un argument, *view*, qui spécifie la vue Utilisateur de l'utilisateur indiqué. Elle retourne la variable de flux de travaux checkPolicyResult. Cette variable contient l'une de ces valeurs :

  - la liste des violations ;
  - une valeur nulle en l'absence de violation.

Chapitre 3 : Formulaires

Identity Manager peut déterminer dans l'affichage si un attribut dans une carte schématique de ressource est requis. Le formulaire Éditer l'utilisateur indique ces attributs par un * (astérisque). Par défaut, Identity Manager affiche cet astérisque après le champ de texte qui suit le nom de l'attribut. (ID-10662)

Pour personnaliser l'emplacement de l'astérisque, procédez comme suit :

1. À l'aide de l'éditeur BPE ou XML d'Identity Manager de votre choix, ouvrez l'objet de configuration Component Properties.
2. Ajoutez `EditForm.defaultRequiredAnnotationLocation=left` à l'indicateur `<SimpleProperties>`.

   La valeurs correctes pour `defaultRequiredAnnotationLocation` comprennent left, right, et none.
3. Enregistrez vos modifications et redémarrez votre serveur d'application.

Chapitre 4 : Méthodes FormUtil

- Identity Manager offre la nouvelle méthode FormUtil `checkStringQualityPolicy`, qui contrôle la valeur d'une chaîne désignée par rapport à la stratégie associée à la chaîne. (ID-12428, 12440)

  checkStringQualityPolicy(LighthouseContext s, String policy, Object value, Map map, List pwdhistory, String owner)

Paramètre	Description
LighthouseContext	Spécifie le contexte Lighthouse de l'utilisateur actuel.
policy	(Obligatoire) Spécifie le nom de la stratégie par rapport à laquelle la chaîne sera testée.
value	(Obligatoire) Identifie la valeur de la chaîne à contrôler.
map	(Facultatif) Offre un mappage des données que la chaîne ne doit pas contenir. `returnNull` -- (Facultatif) Défini sur `true`, la méthode retourne un objet nul après réussite.
pwdhistory	(Facultatif) Liste les mots de passe précédents de l'utilisateur en format crypté et en majuscules.
owner	(Obligatoire) Identifie l'utilisateur dont la valeur de chaîne est en cours de contrôle.

Cette méthode retourne une valeur true pour indiquer que la chaîne passe le test de la stratégie. Si la chaîne ne passe pas le test de la stratégie, la méthode retourne un message d'erreur. Si vous avez défini l'option `returnNull` sur true dans le paramètre `map`, la méthode retourne un objet nul après réussite.

- Identity Manager offre désormais la méthode FormUtil `controlsAtLeastOneOrganization`. (ID-9260)

  controlsAtLeastOneOrganization(LighthouseContext s, List organizations)

  throws WavesetException {

  Détermine si un utilisateur actuellement authentifié contrôle les organisations spécifiées sur une liste d'un ou plusieurs noms d'organisation (ObjectGroup). La liste des organisations prises en charge comprend celles retournées en listant tous les objets de type ObjectGroup.

Paramètre	Description
s	Spécifie le contexte Lighthouse de l'utilisateur actuel (session).
organizations	Spécifie une liste d'un ou plusieurs noms d'organisation. La liste des organisations prises en charge comprend celles retournées en listant tous les objets de type ObjectGroup.

Cette méthode retourne :

`true` – Indique que l'utilisateur actuellement authentifié d'Identity Manager contrôle l'une des organisations de la liste.

`false` – Indique que l'utilisateur actuellement authentifié d'Identity Manager ne contrôle aucune des organisations de la liste.

Chapitre 5 : Vues

Types de compte

Cette version d'Identity Manager offre une aide pour assigner plusieurs comptes aux utilisateurs sur une ressource contenant des *types de compte*. (ID-12697) Vous pouvez désormais assigner facultativement un type de compte à une ressource lorsque vous assignez des ressources à un utilisateur, avec les limitations suivantes :

- Chaque compte d'une ressource ne peut être que d'un seul type.
- Les utilisateurs ont généralement un seul compte d'un type donné.

Un administrateur doit préalablement définir un type de compte sur une ressource avant de pouvoir l'associer à une ressource. Une IdentityRule doit aussi être définie. (Voir samples/identityRules.xml pour des exemples de règles d'identité.)

Identity Manager utilise le sous-type IdentityRule pour associer une règle à un type de compte. Cette règle génère les `accountIds` selon les besoins. (Ces règles fonctionnent de façon similaire au modèle d'identité, mais sont implémentées dans XPRESS et peuvent accéder à l'API LighthouseContext).

Consultez *Identity Manager Administration* pour le mode d'emploi de l'interface administrateur d'Identity Manager pour assigner des types de comptes aux ressources.

Omission du type de compte

Si vous omettez le type de compte d'une ressource, Identity Manager assigne le type de compte par défaut, qui offre une compatibilité ascendante. Toutefois, lorsqu'une ressource n'a pas de type de compte défini, cette fonction est désactivée.

Le type de compte par défaut utilise le modèle d'identité. Toutefois, vous pouvez aussi spécifier que le type par défaut utilise une règle spécifiée au lieu du modèle d'identité.

Le type de compte par défaut est unique en ce sens qu'un utilisateur peut assigner plusieurs comptes de ce type. Toutefois, la meilleure pratique suggère de ne pas assigner plusieurs comptes du même type.

Modifications liées à la vue

Les changements suivants des vues d'Identity Manager prennent en charge les types de compte.

- La vue Resource possède désormais un attribut `accountType` (Liste). Chaque entrée est un objet avec un attribut `identityRule`, qui nomme la règle utilisée pour générer les `accountIds` pour ce type.

- L'attribut `resources` des vues Role et Application permettent désormais d'utiliser des assignations de ressource qualifiées. La syntaxe de ces assignations qualifiées est `<resource name>|<account type>`.

- La vue User contient désormais l'attribut `waveset.resourceAssignments`, qui prend les assignations de ressource qualifiées. (`waveset.resources` contient uniquement des références non qualifiées). Vous pouvez changer l'un ou l'autre des attributs, mais la meilleure pratique suggère d'utiliser uniquement `waveset.resourceAssignment` pour les mises à jour et `waveset.resources` pour la lecture seule.)

  La façon d'accéder aux objets dans l'attribut `accounts` de la vue User n'a pas changé avec l'ajout de cette nouvelle fonction. Utilisez des noms de ressource qualifiés pour indexer la liste`accounts` (par exemple, `accounts[resource|type]` sélectionne le compte de ressource pour cette combinaison de ressource et de type. Si vous ne spécifiez pas de type, vous pouvez quand même accéder à ces objets via `accounts[resource]`.)
- Les vues associées, notamment Deprovision et Change Password, utilisent aussi ce type d'adressage. Les objets de cette liste ont également un nouvel attribut `accountType`, qui spécifie le type de compte du compte de ressource.

Vue Approbateurs délégués

Utilisez cette vue pour assigner un ou plusieurs utilisateurs Identity Manager comme approbateurs délégués d'un approbateur existant. Ceci permet à un approbateur de déléguer ses capacités d'approbation pendant une période de temps spécifiée à des utilisateurs qui ne sont pas obligatoirement approbateurs. Les attributs de haut niveau comprennent : (ID-12754)

Remarque La vue User contient ces mêmes attributs, (sauf l'attribut de nom). Ces nouveaux attributs sont contenus dans les comptes [Lighthouse]. namespace.

name

Identifie l'utilisateur qui délègue les approbations.

delegateApproversTo

Spécifie à qui l'utilisateur délègue les approbations, les valeurs correctes incluant manager, selectedUsers, ou delegateApproversRule.

delegateApproversSelected

- Si `selectedUsers` est la valeur de `delegateApproversRule`, liste les noms des utilisateurs sélectionnés.
- Si `delegatedApproversRule` est la valeur de `delegateApproversTo`, identifie la règle sélectionnée.
- Si `manager` est la valeur de `delegateApproversTo`, cet attribut n'a pas de valeur.

delegateApproversStartDate

Spécifie la date de début de la délégation des approbations. Par défaut, l'heure et les minutes de la date de début sont 12 :01 de ce jour.

delegateApproversEndDate

Spécifie la date de fin de la délégation des approbations. Par défaut, l'heure et les minutes de la date de fin sélectionnée sont 11 :59 de ce jour.

La documentation de la vue Role a été mise à jour comme suit. (ID-12390)

Vue Rôle

Utilisée pour définir les objets de rôle d'Identity Manager.

Lorsqu'elle est archivée, cette vue lance le flux de travaux Manage Role. Par défaut, ce flux de travaux enregistre simplement les changements de la vue dans le référentiel, et fournit des points d'ancrage pour les approbations et les autres personnalisations.

Le table suivant liste les attributs de haut niveau de cette vue.

Attribut	Modifiable ?	Type de données	Obligatoire
`name`	Lecture/écriture	Chaîne	Oui
`resources`	Lecture/écriture	Liste	Non
`applications`	Lecture/écriture	Liste	Non
`roles`	Lecture/écriture	List	Non
`assignedResources`	Lecture/écriture	List	Non
`notifications`	Lecture/écriture	Liste	Non
`approvers`	Lecture/écriture	Liste	Non
`properties`	Lecture/écriture	Liste	
`organizations`	Lecture/écriture	Liste	Oui

Tableau 1. Attributs de la vue Role

name

Identifie le nom du rôle. Ceci correspond au nom de l'objet Role dans le référentiel d'Identity Manager.

resources

Spécifie les noms de ressources assignées localement.

applications

Spécifie les noms des applications assignées localement (Groupes de ressources).

roles

Spécifie les noms des rôles assignés localement.

assignedResources

Liste à plat de toutes les ressources assignées via les ressources, les applications et les rôles.

Attribut	Modifiable ?	Type de données
resourceName		Chaîne
name		Chaîne
attributes		Objet

resourceName

Identifie le nom de la ressource assignée.

name

Identifie le nom ou l'ID de la ressource (de préférence l'ID).

attributes

Identifie les caractéristiques de la ressource. Tous les sous-attributs sont des chaînes modifiables.

Attribut	Description
name	Nom de l'attribut de ressource
valueType	Type de valeur défini pour cet attribut. Les valeurs admises comprennent Rule, text ou none.
requirement	Type de valeur définie par cet attribut. Les valeurs admises comprennent Rule, Text, None, Value, Merge with Value, Remove with Value, Merge with Value clear existing, Authoritative set to value. Authoritative merge with value, Authoritative merge with value clear existing.
rule	Spécifie le nom de la règle si le type de valeur est Rule.
value	Spécifie la valeur si le type de règle est Text.

Tableau 2. Options des attributs (Vue Rôle)

- `notifications` -- Liste les noms des administrateurs qui doivent approuver l'assignation de ce rôle à un utilisateur.
- `approvers` -- Spécifie les noms des approbateurs qui doivent approuver l'assignation de ce rôle à un utilisateur.
- `properties` -- Identifie les propriétés définies par l'utilisateur qui sont stockées dans ce rôle.
- `organizations` -- Liste les organisations dont ce rôle est un membre.
- Les vues Resource Account (Deprovision, Disable, Enable, Password, Rename User, Reprovision, et Unlock) prennent désormais en charge deux nouvelles options de vue que vous pouvez utiliser pour récupérer les attributs de compte de ressource pour l'utilisateur. (ID-12482)
  - `fetchAccounts` - (Booléen) Provoque l'inclusion dans la vue des attributs de compte pour les ressources assignées à l'utilisateur.
  - `fetchAccountResources` - Liste les noms de ressources parmi lesquelles extraire. Sans spécification, toutes les ressources sont utilisées.

  Vous pouvez très facilement définir ces options comme propriétés de formulaire. (Pour plus d'informations, voir la discussion de la vue WorkItem List dans le chapitre Vues de ce guide).

Chapitre 6 : Langage XPRESS

- La fonction `instanceOf` n'est pas actuellement documentée dans le chapitre langage XPRESS. Cette fonction détermine si un objet est une instance du type spécifié dans le paramètre `name`. (ID-12700)

  `name` – identifie le type d'objet par rapport auquel vous vérifiez.

  Cette fonction retourne 1 ou 0 (vrai ou faux) selon que l'objet de sous-expression est une instance du type spécifié dans le paramètre `name`.

  L'expression suivante retourne 1 car ArrayList est une liste

```
<instanceof name='List'>
   <new class='java.util.ArrayList'/>
</instanceof>
```

Chapitre 8 : HTML Display Components

- La description du composant SortingTable a été révisée comme suit :

  Utilisez-le pour créer un tableau dont le contenu peut être trié par titre de colonne. Les composants enfant déterminent le contenu de ce tableau. Créez un composant enfant par colonne (définie par la propriété `columns`). Les colonnes sont généralement contenues dans un FieldLoop.

  Ce composant respecte les propriétés `align`, `valign` et `width` des composants enfant lors de la conversion des cellules du tableau. (ID-12606)

- Identity Manager offre désormais le composant d'affichage InlineAlert. (ID-12606)

  Affiche une boîte d'alerte d'erreur, d'avertissement, de réussite ou informative. Ce composant est généralement situé en haut d'une page. Vous pouvez afficher plusieurs alertes dans une seule boîte en définissant des composants enfant de type`InlineAlert$AlertItem`.

  Les propriétés de ce composant d'affichage comprennent :

  - `alertType` – Spécifie le type d'alerte à afficher. Cette propriété détermine les styles et les images à utiliser. Les valeurs correctes sont error, warning, success et info. La valeur par défaut de cette propriété est info. Cette propriété n'est valable que pour `InlineAlert`.
  - `header` – Spécifie le de la boîte d'alerte à afficher. Ce peut être une chaîne ou un objet de message. Cette propriété est valable pour `InlineAlert` ou `InlineAlert$AlertItem`.
  - `alertType` – Spécifie le message d'alerte à afficher. Cette valeur peut être une chaîne ou un objet de message. Cette propriété est valable pour `InlineAlert` ou `InlineAlert$AlertItem`.
  - `linkURL` – Spécifie une URL facultative à afficher en bas de l'alerte. Cette propriété est valable pour `InlineAlert` ou `InlineAlert$AlertItem`.
  - `linkText` – Spécifie le texte de `linkURL`. Ce peut être une chaîne ou un objet de message. Cette propriété est valable pour `InlineAlert` ou `InlineAlert$AlertItem`.
  - `linkText` – Spécifie le titre de `linkURL`. Ce peut être une chaîne ou un objet de message. Cette propriété est valable pour `InlineAlert` ou `InlineAlert$AlertItem`.

Exemples

Message d'alerte unique

```
<Field>
   <Display class='InlineAlert'>
      <Property name='alertType' value='warning'/>
      <Property name='header' value='Data not Saved'/>
      <Property name='value' value='The data entered is not yet saved.
          Please click Save to save the information.'/>
   </Display>
</Field>
```

Messages d'alertes multiples

Définissez `alertType` uniquement dans la propriété `InlineAlert`. Vous pouvez définir d'autres propriétés dans `InlineAlert$AlertItems`.

```
<Field>
   <Display class='InlineAlert'>
      <Property name='alertType' value='error'/>
   </Display>
   <Field>
     <Display class='InlineAlert$AlertItem'>
        <Property name='header' value='Server Unreachable'/>
        <Property name='value' value='The specified server could not
       be contacted. Please view the logs for more information.'/>
        <Property name='linkURL' value='viewLogs.jsp'/>
        <Property name='linkText' value='View logs'/>
        <Property name='linkTitle' value='Open a new window with
           the server logs'/>
     </Display>
  </Field>
  <Field>
     <Display class='InlineAlert$AlertItem'>
        <Property name='header' value='Invalid IP Address'/>
        <Property name='value' value='The IP address entered is
       in an invalid subnet. Please use the 192.168.0.x subnet.'/>
     </Display>
  </Field>
</Field>
```

- Identity Manager offre désormais le composant d'affichage Selector. (ID-12729)

  Offre un champ à une ou plusieurs valeurs (similaire aux composants Text ou ListEditor, respectivement) avec les champs de recherche ci-dessous. Après l'exécution d'une recherche, Identity Manager affiche les résultats sous les champs de recherche et insère les résultats dans le champ de valeur.

  Contrairement aux autres composants de conteneur, `Selector` a une valeur (le champ où les `résultats` de recherche sont insérés). Les champs contenus sont généralement des champs de critère de recherche. `Selector` implémente une propriété pour afficher le contenu des résultats de recherche.

  Les propriété comprennent :

  - `fixedWidth` – Spécifie si le composant doit avoir une largeur fixe (même comportement que Multiselect). (Booléen)
  - `multivalued` – Indique si la valeur est une liste ou une chaîne. (La valeur de cette propriété détermine si un champ ListEditor ou Text est produit pour la valeur). (Booléen)
  - `allowTextEntry` – Indique si les valeurs doivent être sélectionnées dans la liste fournie ou entrées manuellement. (Booléen)
  - `valueTitle` – Spécifie l'étiquette à utiliser sur le composant `value`. (Chaîne)
  - `valueTitle` – Spécifie l'étiquette à utiliser sur le composant `picklist`. (Chaîne)
  - `pickValues` – les valeurs disponibles dans le composant liste de sélection (si elles sont nulles, la liste de sélection n'est pas affichée). (Liste)
  - `pickValueMap` – mappage des étiquettes d'affichage pour les valeurs de la liste de sélection. (mappage ou liste)
  - `sorted` – Indique que les valeurs doivent être triées dans la liste de sélection (en cas de valeurs multiples non ordonnées, la liste de valeurs est également triée). (booléen)
  - `clearFields` – Liste les champs qui doivent être réinitialisés lorsque le bouton Effacer est sélectionné. (liste)

  Les propriétés suivantes ne sont valables que dans un composant à plusieurs valeurs :

  - `ordered` – Indique que l'ordre des valeurs importe. (booléen)
  - `allowDuplicates` – Indique si la liste des valeurs peut contenir des doublons. (booléen)
  - `ValueMap` – offre un mappage des étiquettes d'affichage pour les valeurs de la liste. (mappage)

Ces propriétés ne sont valables que dans un composant à valeur unique :

- `nullLabel` – Spécifie une étiquette à utiliser pour indiquer une valeur nulle. (chaîne)

- Les descriptions des composants `Select` et `MultiSelect` ont été révisées comme suit pour inclure les discussions relatives à la propriété `caseInsensitive`. (ID-13364)

Composant MultiSelect

Affiche un objet à sélection multiple, qu'Identity Manager affiche sous forme de deux touches de sélection de texte côte à côte dans lesquelles un ensemble de valeurs défini dans une boîte peut être déplacé dans une autre. Les valeurs dans la boîte de gauche sont définies par la propriété `allowedValues`, les valeurs sont souvent obtenues dynamiquement en appelant une méthode Java comme `FormUtil.getResources`. Les valeurs affichées dans la boîte à sélection multiple de droite sont remplies à partir de la valeur actuelle de l'attribut de vue associé, qui est identifié par le nom de champ.

Vous pouvez définir les titres de formulaire pour chacune des boîtes de cet objet à sélection multiple par l'intermédiaire des propriétés `availabletitle` et `selectedtitle`.

Si vous voulez un composant `MultiSelect` qui n'utilise pas d'applet, définissez la propriété `noApplet` sur true.

Remarque Si vous exécutez Identity Manager sur un système qui exécute le navigateur Safari, vous devez personnaliser tous les formulaires contenant des composants MultiSelect pour définir l'option noApplet. Définissez cette option comme suit :

```
<Display class='MultiSelect'>
      <Property name='noApplet' value='true'/>
 ...
```

Les propriétés de ce composant d'affichage comprennent :

- `availableTitle` – Spécifie le titre de la boîte disponible.
- `selectedTitle` – Spécifie le titre de la boîte sélectionnée.
- `ordered` – Définit si les éléments sélectionnés peuvent être déplacés vers le haut ou le bas dans la liste d'éléments de la boîte de texte. Une valeur `true` indique que d'autres boutons seront produits pour permettre de monter ou descendre les éléments sélectionnés.
- `allowedValues` – Spécifie les valeurs associoées à la boîte de gauche de l'objet à sélection multiple. Cette valeur doit être une liste de chaînes. **Remarque** : L'élément `<Constraints>` peut servir à remplir cette boîte, mais son utilisation a été désapprouvée.

- `sorted` – Spécifie que les valeurs des deux boîtes seront triées alphabétiquement.
- `noApplet` – Spécifie si le composant MultiSelect sera implémenté avant un applet ou avec une paire de boîtes de sélection HTML standard. Un applet est utilisé par défaut, ce qui est préférable pour traiter les longues listes de valeurs. Voir la remarque précédente pour des informations sur l'utilisation de cette option sur les systèmes exécutant le navigateur Safari.
- `typeSelectThreshold` – (Disponible uniquement lorsque la propriété `noApplet` est réglée sur true.) Contrôle si une boîte de sélection pré-saisie apparaît sous
  la liste `allowedValue`. Lorsque le nombre d'entrées dans la boîte de sélection
  de gauche atteint le seuil défini par cette propriété, un champ de saisie de texte supplémentaire apparaît sous la boîte de sélection. A mesure que vous tapez des caracatères dans ce champ de texte, la boîte défile pour afficher l'entrée correspondante si elle existe. Par exemple, si vous entrez **w**, la boîte de sélection défile jusqu'à la première entrée qui commence par **w**.
- `width` – Spécifie la largeur de la boîte sélectionnée en pixels. La valeur par défaut est 150.
- `height` – Spécifie la hauteur de la boîte sélectionnée en pixels. La valeur par défaut est 400.
- `caseInsensitive` -- A utiliser pour effectuer des comparaisons insensibles à la casse.

Composant Select

Affiche un objet à sélection unique. Les valeurs de la boîte de liste doivent être fournies par la propriété `allowedValues`.

Les propriétés de ce composant d'affichage sont les suivantes :

- `allowedValues` – Spécifie la liste des valeurs sélectionnables pour affichage dans la boîte de liste.
- `allowedOthers` – spécifie que les valeurs initiales qui ne figuraient pas dans la liste `allowedValues` doivent être tolérées et ajoutées silencieusement à la liste.
- `autoSelect` – Définie sur `true`, cette propriété provoque la sélection automatique de la première valeur dans `allowedValues` si la valeur initiale du champ est nulle.
- `caseInsensitive` -- A utiliser pour effectuer des comparaisons insensibles à la casse.
- `multiple` – Définie sur `true`, permet de sélectionner plusieurs valeurs.

- `nullLabel` – Spécifie le texte affiché en haut de la boîte de liste lorsqu'aucune valeur n'est sélectionnée.
- `optionGroupMap` – Permet au sélecteur de produire des options dans les groupes utilisant l'indicateur `<optgroup>`. Formatez le mappage de sorte que les clés des mappages correspondent aux étiquettes de groupes, et que les élements désignent les listes d'éléments sélectionnables. (Les valeurs doivent être membres de `allowedValues` pour pouvoir être générées.)
- `size` – (Facultatif) Spécifie le nombre maximal de lignes à afficher. Si le nombre de lignes dépasse cette taille, une barre de défilement est ajoutée.
- `sorted` – Définie sur `true`, provoque le tri des valeurs de la liste.
- `valueMap` – Mappe les valeurs brutes aux valeurs affichées.

Le composant prend en charge les propriétés `command` et `onChange`.

- La discussion du composant `DatePicker` doit décrire les nouvelles propriétés suivantes. (ID-14802)

  Le composant HTML `DatePicker` permet désormais de sélectionner des dates discrètes. Vous pouvez spécifier une plage de dates qui permettent de sélectionner des dates particulières dans le calendrier.

  `DatePicker` implémente les deux propriétés nouvelles suivantes :

  `SelectAfter` -- Limite les dates sélectionnables affichées dans le calendrier aux dates égales ou supérieures à la date entrée. La valeur de cette propriété peut être une chaîne de date ou un objet Java Date.

```
<Property name='SelectAfter' value='**/**/****'/>
```

  `SelectBefore` -- Limite les dates sélectionnables affichées dans le calendrier aux dates égales ou inférieures à la date entrée. La valeur de cette propriété peut être une chaîne de date ou un objet Java Date.

```
<Property name='SelectBefore' value='**/**/****'/>
```

  Lorsque vous utilisez un formulaire qui implémente l'indicateur `<Display class='DatePicker'>`, ajoutez ces variables au formulaire pour définir la plage de dates. Si vous ne définissez pas ces propriétés, les dates sélectionnables dans le calendrier seront illimitées.

Identity Manager Technical Deployment Overview

La discussion suivante consacrée aux flux de travaux, formulaires et JSP fait partie de la présentation de l'architecture de *Identity Manager Technical Deployment Overview* (ID-7332).

Exécution du processus

Lorsqu'un utilisateur entre des données dans un champ d'une page et clique sur Save, les composants vue, flux de travaux et formulaire travaillent ensemble pour exécuter les processus nécessaires au traitement des données.

Chaque page d'Identity Manager a une vue, un flux de travaux et un formulaire associé qui effectue le traitement des données nécessaire. Ces associations de flux de travaux, vue et formulaire sont indiquées dans les deux tableaux ci-après.

Processus de l'interface utilisateur d'Identity Manager

Les tableaux suivants indique les formulaires, les vues et les flux de travaux impliqués dans les processus initiés à partir des pages de l'interface utilisateur d'Identity Manager suivantes :

Page de l'interface	Formulaire	Vue	Flux de travaux
Main menu	• endUserMenu • Menu End User par défaut	User La vue est en lecture seule. Cette page n'est pas modifiable	aucun
Change Password	• endUserChangePassword • formulaire Change Password par défaut	Password	• changeUserPassword • Change User Password par défaut
Change Other Account Attributes	• endUserForm • formulaire End User par défaut	User	Update User

Page de l'interface	Formulaire	Vue	Flux de travaux
Check Process Status	• endUserTaskList • liste End User Task par défaut	List La vue contient des informations sur les objets TaskInstance lancés par l'utilisateur	aucun
Process Status La page est générée par la classe TaskViewResults	aucun	aucune	aucun
Available Processes	• endUserLaunchList • liste End User Launch par défaut	List La vue comprend des informations sur les objets TaskDefinition accessibles pour l'utilisateur	aucun
Launch Process Lance une TaskDefinition sélectionnée	Défini par TaskDefinition	Process	aucun
Change Answers to Authentication Questions	• changeAnswers • formulaire Change User Answers par défaut	ChangeUserAnswers	aucun
Self Discovery Lien vers les comptes de ressource existants seulement	• selfDiscovery • Self Discovery par défaut	User	Update User
Inbox	• endUserWorkItemList • liste End User Work Item par défaut	List La vue contient des informations sur les WorkItems directement détenus par l'utilisateur actuel	aucun
Inbox Item Edit	Spécifié par WorkItem ou généré automatiquement	WorkItem	aucun

Processus de l'interface administrateur

Les tableaux suivants identifient les formulaires, les vues, les flux de travaux et les JSP impliqués dans les processus initiés depuis ces pages de l'interface administrateur d'Identity Manager :

Page de l'interface administrateur	Formulaire	Vue	Flux de travaux
Create Organization and Edit Organization	System Configuration mapping Selon le contexte, peut être un formulaire parmi plusieurs, notamment : • Organization Form • Organization Rename Form • Directory Junction Form • Virtual Organization Form • Virtual Organization Refresh Form	Org	aucun
Create User	• userForm • formulaire Tabbed User par défaut	User	• createUser • default Create User
Update User	• userForm • formulaire Tabbed User par défaut	User	• updateUser • Update User par défaut
Disable User's Resource Accounts	• disableUser • Disable User par défaut	Disable	• disableUser • Disable User par défaut
Rename User	• renameUser • formulaire Rename User par défaut	RenameUser	• renameUser • Rename User par défaut
Update User's Resource Accounts	• reprovisionUser • formulaire Reprovision par défaut	Reprovision	• updateUser • Update User par défaut

Page de l'interface administrateur	Formulaire	Vue	Flux de travaux
Unlock User's Resource Accounts	• unlockUser • Unlock User par défaut	Unlock	• unlockUser • Unlock User par défaut
Delete User's Resource Accounts	• deprovisionUser • formulaire Deprovision par défaut	Deprovision	• deleteUser • Delete User par défaut
Change User Password Utilise le même flux de travaux que l'interface graphique utilisateur, mais sous une forme différente	• changePassword • formulaire Change User Password par défaut	ChangeUserPassword	• changeUserPassword • Change User Password par défaut
Reset User Password	• resetPassword • formulaire Reset User Password par défaut	ResetUserPassword	• changeUserPassword • Change User Password par défaut
Change My Password Même vue, formulaire et flux de travaux que End-User Change Password mais JSP différent	• endUserChangePassword • formulaire Change Password par défaut	Password	• changeUserPassword • Change User Password par défaut
Change My Answers Même vue, formulaire que End-User Change Answers mais JSP différent	• changeAnswers • formulaire Change User Answers par défaut	ChangeUserAnswers	aucun
Approvals	• workItemList • liste Work Item par défaut • le formulaire par défaut inclut Work Item Confirmation	WorkItemList	aucun

Page de l'interface administrateur	Formulaire	Vue	Flux de travaux
Edit WorkItem Archivage des résultats de la vue WorkItem dans la reprise du flux de travaux qui les ont créés, mais aucun flux de travaux n'est créé juste pour traiter l'archivage de l'élément de travail	Spécifié par WorkItem, ou généré automatiquement	WorkItem	aucun
Launch Task Lance une TaskDefinition sélectionnée	Défini par TaskDefinition	Process	aucun
Create and Update Scheduled Tasks	pas de mappage de System Configuration, formulaire Task Schedule par défaut, fusionné avec le formulaire TaskDefinition Ce formulaire est généré par la combinaison du formulaire TaskDefinition avec le formulaire Task Schedule comme inclusion	TaskSchedule	aucun

Page de l'interface administrateur	Formulaire	Vue	Flux de travaux
Create Role and Edit Role	pas de mappage System Configuration Les formulaires Role Form et Role Rename dépendent du contexte	Role	• manageRole • Manage Role par défaut
Edit Resource	pas de mappage System Configuration, dépend du contexte, les formulaires comprennent : • Change Resource Account Password Form • Reset Resource Account Password Form • Edit Resource Policy Form • Resource Rename Form • Resource Wizard <resource type> • Resource Wizard. Autorise les formulaires d'assistant spécifiques au type, Resource Wizard par défaut	Resource	• manageResource • Manage Resource par défaut
Edit Capability	changeCapabilities, formulaire Change User Capabilities par défaut	ChangeUser Capabilities	aucun

Les pages Java Server (JSP) et leur rôle dans Identity Manager

Les tableaux suivants décrivent les JSP qui sont expédiés avec le système ainsi que leurs pages administrateur et interface utilisateur

JSP pour l'interface utilisateur d'Identity Manager

	JSP associée
Main Menu	user/main.jsp
Change Password	user/changePassword.jsp
Change Other Account Attributes	user/changeAll.jsp
Check Process Status	user/processStatusList.jsp
Process Status	user/processStatus.jsp
Available Processes	user/processList.jsp
Launch Process	user/processLaunch.jsp
Change Answers to Authentication Questions	user/changeAnswers.jsp
Self Discovery	user/selfDiscover.jsp
Inbox	user/workItemList.jsp
Inbox Item Edit	user/workItemEdit.jsp

JSPs for Admin Interface

	JSP associée
Create Organization and Edit Organization	security/orgedit.jsp
Create User	account/modify.jsp
Update User	account/modify.jsp
Disable User's Resource Accounts	account/resourceDisable.jsp
Rename User	account/renameUser.jsp
Update User's Resource Accounts	account/resourceReprovision.jsp
Unlock User's Resource Accounts	admin/resourceUnlock.jsp
Delete User's Resource Accounts	account/resourceDeprovision.jsp
Change User Password	admin/changeUserPassword.jsp

	JSP associée
Reset User Password	admin/resetUserPassword.jsp
Change My Password	admin/changeself.jsp
Change My Answers	admin/changeAnswers.jsp
Approvals	approval/approval.jsp
Edit WorkItem	approval/itemEdit.jsp
Launch Tasks	task/taskLaunch.jsp
Create and Update Scheduled Tasks	task/editSchedule.jsp
Create Role and Edit Role	roles/applicationmodify.jsp
Edit Resource	resources/modify.jsp
Edit Capability	account/modifyCapabilities.jsp

Annexe A, Modification des objets Configuration

À la page A-4, la liste de noms QueryableAttrNames par défaut devrait également inclure `idmManager`.

Référence des ressources d'Identity Manager 6.0

- La liste des attributs de compte pris en charge dans Resources Reference > Active Directory > Account Attributes > Account Attribute Support est plus actuelle dans la version PDF du document que dans la version HTML. Reportez-vous à la version PDF. (ID-12630)
- Le nœud supérieur d'Identity Manager 6.0 Resources Reference 2005Q4M3 de l'URL suivante ne contient pas de lien vers la section intitulée Domino : (ID-12636)

`http://docs.sun.com/app/docs/doc/819-4520`

Recherchez la section Domino en ouvrant Contents sur ce noeud à l'URL suivante :

`http://docs.sun.com/source/819-4520/Domino_Exchange.html#wp999317`

Adaptateur Access Manager

L'étape 5 de la procédure « Configuration générale » doit indiquer :

5. Ajoutez les lignes suivantes au fichier `java.security` si elles n'y sont pas déjà :

```
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.net.ssl.internal.ssl.Provider
```

Le nombre qui suit security.provider sur chaque ligne spécifie l'ordre dans lequel Java consulte les classes de fournisseurs de sécurité et doit être unique. La numérotation peut varier en fonction de votre environnement. Si vous avez déjà plusieurs fournisseurs de sécurité dans le fichier java.security, insérez les nouveaux dans l'ordre indiqué ci-dessus et renumérotez les fournisseurs de securité existants. Ne supprimez pas les fournisseurs de sécurité existants et ne les dupliquez pas. (ID-12044)

Adaptateur Active Directory

Active Directory prend désormais en charge les attributs binaires `thumbnailPhoto` (Windows 2000 Server et supérieur) et `jpegPhoto` (Windows 2003).

Adaptateur BridgeStream SmartRoles

Identity Manager offre désormais un adaptateur de ressources BridgeStream SmartRoles qui provisionne les utilisateurs dans les SmartRoles. Cet adaptateur place les utilisateurs dans les organisations appropriées au sein des SmartRoles afin que ces derniers puissent déterminer de quels rôles professionnels ces utilisateurs doivent disposer.

En retirant un utilisateur des SmartRoles, l'adaptateur retire les rôles professionnels de l'utilisateur. Ces rôles professionnels peuvent être utilisés dans Identity Manager pour déterminer les rôles, les ressources, les attributs et l'accès qui doivent être assignés à l'utilisateur.

De plus, les SmartRoles peuvent être une source de changements des utilisateurs utilisant Active Sync. Vous pouvez charger les utilisateurs SmartRoles dans Identity Manager et les réconcilier.

Pour des informations détaillées sur cet adaptateur, consultez l'addenda *Sun Java™ System Identity Manager Resources Reference*. (ID-12714)

Adaptateur ClearTrust

- L'adaptateur de ressources ClearTrust prend désormais en charge la version 5.5.2 de ClearTrust.
- Les étapes 2 et 3 de la procédure Installation Notes d'Identity Manager doivent indiquer (ID-12906) :

1. Copiez le fichier `ct_admin_api.jar` depuis votre CD d'installation Clear Trust dans le répertoire `WEB-INF\lib`.
2. Si vous utilisez SSL, copiez les fichiers suivants dans le répertoire `WEB-INF\lib`.

Remarque Si vous provisionnez vers une ressource RSA Clear Trust 5.5.2, les bibliothèques supplémentaires ne sont pas nécessaires pour la communication SSL.

- `asn1.jar`
- `certj.jar`
- `jce1_2-do.jar`
- `jcert.jar`
- `jnet.jar`
- `jsafe.jar`
- `jsaveJCE.jar`
- `jsse.jar`
- `rsajsse.jar`
- `sslj.jar`

Adaptateur Database Table

Cet adaptateur prend en charge les types de données binaires, y compris les BLOB dans Oracle. Les attributs correspondants doivent être marqué comme binaires sur la carte schématique. Les exemples d'attributs binaires comprennent les fichiers graphiques, les fichiers audio et les certificats.

Adaptateur Active Sync fichier plat

- L'utilisateur administratif doit disposer de droits d'accès en lecture et écriture au répertoire qui contient le fichier plat. Cet utilisateur doit aussi disposer d'un accès en suppression si le paramètre Active Sync **Process Differences Only** est activé.

  En outre, le compte administrateur doit disposer d'autorisations de lecture, écriture et suppression sur le répertoire spécifié dans le champ Active Sync **Log File Path**. (ID-12477)
- Si le format de fichier est LDIF, les attributs binaires tels que les fichiers graphiques, les fichiers audio et les certificats peuvent être spécifiés. Les attributs binaires ne sont pas pris en charge pour les fichiers CSV et délimités par pipe.

Adaptateur HP OpenVMS

Identity Manager offre désormais un adaptateur de ressources HP OpenVMS qui prend en charge les version 7.0 et supérieures de VMS. Pour des informations détaillées sur cet adaptateur, consultez l'addenda *Sun Java™ System Identity Manager Resources Reference*. (ID-8556)

Adaptateur JMS Listener

L'adaptateur JMS Listener prend désormais en charge le traitement synchrone des message au lieu du traitement asynchrone. Par conséquent, le deuxième paragraphe de la section Connexions des Notes d'usage doit indiquer :

L'adaptateur JMS Listener fonctionne en mode synchrone. Il établit un consommateur de message synchrone sur la file d'attente ou la destination du sujet spécifiée par le champ **JNDI name of Destination**. Pendant chaque intervalle d'interrogation, l'adaptateur reçoit et traite tous les messages disponibles. Les messages peuvent être en outre (facultativement) qualifiés en définissant une chaîne de sélecteur de message JMS valide pour le champ **Message Selector**.

La section Mappage des messages doit contenir :

Lorsque l'adapateur traite un message qualifié, le message JMS reçu est d'abord converti en mappage de valeurs nommées en utilisant le mécanisme spécifié par le champ **Message Mapping**. Ce mappage est appelé *mappage de valeur* du message.

Le mappage de valeur du message est ensuite converti en mappage ActiveSync à l'aide de la carte schématique des attributs de compte. Si des attributs de compte sont spécifiés pour l'adaptateur, celui-ci recherche des noms clés dans le mappage de valeur du message qui figurent également comme attribut utilisateur de la ressource

dans la carte schématique. Si elle est présente, la valeur est copiée dans le mappage ActiveSync, mais le nom d'entrée figurant dans le mappage ActiveSync est converti selon le nom spécifié dans la colonne d'attribut utilisateur Identity System d'identité dans la carte schématique.

Si le mappage de valeur du message contient une entrée non convertible à l'aide de la carte schématique des attributs de compte, cette entrée est copiée sans modification dans le mappage ActiveSync.

Adaptateur LDAP

Prise en charge de l'attribut de compte binaire

Les attributs de compte binaire suivants de la classe d'objet inetOrgPerson sont désormais pris en charge :

Attribut Resource User	Syntaxe LDAP	Description
audio	Audio	Un fichier audio.
jpegPhoto	JPEG	Une image au format JPEG.
userCertificate	certificate	Un certificat au format binaire.

D'autres comptes binaires peuvent être pris en charge, mais ils n'ont pas été testés.

Désactivation et activation des comptes

L'adaptateur LDAP offre plusieurs méthodes pour désactiver les comptes sur une ressource LDAP. Utilisez l'une des techniques suivantes pour désactiver les comptes.

Changer le mot de passe pour une valeur inconnue

Pour désactiver les comptes en changeant le mot de passe pour une valeur de comptes inconnue, laissez les champs **Méthode d'activation LDAP** et **Paramètre d'activation LDAP** vides. Il s'agit de la méthode de désactivation des comptes par défaut. Le compte peut être réactivé en assignant un nouveau mot de passe.

Assigner le rôle `nsmanageddisabledrole`

Pour utiliser le rôle LDAP `nsmanageddisabledrole` pour désactiver et activer les comptes, configurez la ressource LDAP comme suit :

1. Sur la page Paramètres de ressource, définissez le champ **Méthode d'activation LDAP** sur `nsmanageddisabledrole`.
2. Définissez le champ **Paramètre d'activation LDAP** sur *`IDMAttribute`*`=CN=nsmanageddisabledrole,`*`baseContext`*. (*`IDMAttribute`* sera spécifié sur le schéma à l'étape suivante.)
3. Sur la page Attributs de compte, ajoutez *IDMAttribute* comme attribut utilisateur d'Identity System. Définissez l'attribut Utilisateur de la ressource sur `nsroledn`. Cet attribut doit être de type chaîne.
4. Créez un groupe nommé nsAccountInactivationTmp sur la ressource LDAP et assignez `CN=nsdisabledrole,`*`baseContext`* comme membre.

Les comptes LDAP peuvent maintenant être désactivés. Pour vérifier à l'aide de la console LDAP, contrôlez la valeur de l'attribut `nsaccountlock`. Une valeur `true` indique que le compte est verrouillé.

Si le compte est réactivé ultérieurement, il est supprimé du rôle.

Définissez l'attribut `nsAccountLock`

Pour utiliser l'attribut `nsAccountLock` pour désactiver et activer les comptes, configurez la ressource LDAP comme suit :

1. Sur la page Paramètres de ressource, définissez le champ **Méthode d'activation LDAP** sur `nsaccountlock`.
2. Définissez le champ **Paramètre d'activation LDAP** sur *`IDMAttribute`*`=true`. (*`IDMAttribute`* sera spécifié sur le schéma à l'étape suivante.) Par exemple, `accountLockAttr=true`.
3. Sur la page Attributs de compte, ajoutez la valeur spécifiée dans le champ **Paramètre d'activation** comme attribut utilisateur d'Identity System. Définissez l'attribut Utilisateur de la ressource sur `nsaccountlock`. Cet attribut doit être de type chaîne.
4. Définissez l'attribut LDAP `nsAccountLock` de la ressource sur `true`.

   Identity Manager définit `nsaccountlock` sur true lors de la désactivation d'un compte. Il présuppose également que les utilisateurs LDAP existants dont `nsaccountlock` est défini sur true sont désactivés. Si `nsaccountlock` est défini sur une autre valeur que true (null compris), le système en déduit que l'utilisateur est activé.

Désactiver les comptes sans les attributs `nsmanageddisabledrole` **et** `nsAccountLock`

Si les attributs `nsmanageddisabledrole` et `nsAccountLock` ne sont pas disponibles sur votre serveur d'annuaire, mais que ce dernier dispose d'une méthode similaire de désactivation des comptes, entrez l'un des noms de classe suivantes dans le champ **Méthode d'activation LDAP**. La valeur à entrer dans le champ **Paramètre d'activation LDAP** varie en fonction de la classe.

Nom de classe	Quand l'utiliser :
com.waveset.adapter.util. ActivationByAttributeEnableFalse	Le serveur de répertoire active un compte en définissant un attribut sur false, et désactive un compte en définissant l'attribut sur true. Ajoutez l'attribut à la carte schématique. Entrez ensuite le nom Identity Manager de l'attribut (défini sur le côté gauche de la carte schématique) dans le champ **Paramètre d'activation LDAP**.
com.waveset.adapter.util. ActivationByAttributeEnableTrue	Le serveur de répertoire active un compte en définissant un attribut sur true, et désactive un compte en définissant l'attribut sur false. Ajoutez l'attribut à la carte schématique. Entrez ensuite le nom Identity Manager de l'attribut (défini sur le côté gauche de la carte schématique) dans le champ **Paramètre d'activation LDAP**.
com.waveset.adapter.util. ActivationByAttributePullDisable PushEnable	Identity Manager doit désactiver les comptes en tirant une paire attribut/valeur de LDAP et les activer en poussant une paire attribut/valeur vers LDAP. Ajoutez l'attribut à la carte schématique. Entrez ensuite la paire attribut/valeur dans le champ **Paramètre d'activation LDAP**. Utilisez le nom Identity Manager pour l'attribut, tel qu'il est défini du côté gauche de la carte schématique.

Nom de classe	Quand l'utiliser :
com.waveset.adapter.util.ActivationByAttributePushDisablePullEnable	Identity Manager doit désactiver les comptes en poussant une paire attribut/valeur de LDAP et les activer en tirant une paire attribut/valeur vers LDAP. Ajoutez l'attribut à la carte schématique. Entrez ensuite la paire attribut/valeur dans le champ **Paramètre d'activation LDAP**. Utilisez le nom Identity Manager pour l'attribut, tel qu'il est défini du côté gauche de la carte schématique.
com.waveset.adapter.util.ActivationNsManagedDisabledRole	Le répertoire utilise un rôle spécifique pour déterminer l'état du compte. Lorsqu'un compte est assigné à ce rôle, le compte est désactivé. Ajoutez le nom du rôle à la carte schématique. Entrez ensuite une valeur dans le champ **Paramètre d'activation LDAP** en utilisant le format suivant : *IDMAttribute*=CN=*roleName*,*baseContext* *IDMAttribute* est le nom Identity Manager du rôle, tel qu'il est défini du côté gauche de la carte schématique.

Adaptateurs de mainframe (ACF2, Natural, RACF, Top Secret)

Vous pouvez utiliser Attachmate Reflection pour Web Emulator Class Library (Reflection ECL) afin de vous connecter à une ressource mainframe. Cette bibliothèque est compatible avec l'API IBM Host on Demand. Suivez la totalité des instructions d'installation fournies avec le produit. Effectuez ensuite les procédures décrites dans les sections « Remarques sur l'installation » et « Configuration SSL ».

Remarques sur l'installation

Effectuez les étapes ci-dessous pour configurer des connexions à l'aide d'Attachmate Reflection ECL :

1. Ajoutez la ressource à la liste des ressources d'Identity Manager, comme décrit dans *Identity Manager Resources Reference*.
2. Copiez les fichiers JAR pertinents dans le répertoire `WEB-INF/lib` de votre installation d'Identity Manager.
   - `RWebSDK.jar`
   - `wrqtls12.jar`
   - `profile.jar`
3. Ajoutez les définitions suivantes au fichier `Waveset.properties` afin de définir le service chargé de gérer la session de terminal :

   `serverSettings.`*`serverId`*`.mainframeSessionType=`*`Valeur`*
   `serverSettings.default.mainframeSessionType=`*`Valeur`*

   Vous pouvez définir la *Valeur* de la manière suivante :
   - 1 — IBM Host On--Demand (HOD)
   - 3 — Attachmate WRQ

   Si ces propriétés ne sont pas définies de manière explicite, Identity Manager tente d'utiliser WRQ avant HOD.
4. Une fois les bibliothèques Attachmate installées dans un WebSphere Application Server, ajoutez la propriété `com.wrq.profile.dir=`*`LibraryDirectory`* au fichier `WebSphere/AppServer/configuration/config.ini`.

   Cette opération permet au code Attachmate de trouver le fichier de licence.
5. Redémarrez le serveur d'application afin de prendre en compte les modifications apportées au fichier `Waveset.properties`.

Effectuez les étapes décrites à la section *Configuration SSL*.

Configuration SSL

Attachmate Reflection pour Web Emulator Class Library (Reflection ECL) est compatible avec IBM Host sur l'API Demand. Suivez la totalité des instructions d'installation fournies avec le produit. Effectuez ensuite les étapes ci-dessous dans Identity Manager.

1. Si un attribut de ressource nommé Propriétés de session n'existe pas encore pour la ressource, utilisez l'EDI Identity Manager ou déboguer les pages afin d'ajouter l'attribut à l'objet ressource. Insérez la définition suivante dans la section `<ResourceAttributes>` :

   ```
   <ResourceAttribute name='Session Properties' displayName='Session
   Properties' description='Session Properties' multi='true'>
   </ResourceAttribute>
   ```

2. Allez à la page Paramètres de ressource pertinente et ajoutez les valeurs suivantes à l'attribut de ressource Propriétés de la session :

   ```
   encryptStream
   true
   hostURL
   tn3270://nom-hôte:SSLport
   keystoreLocation
   Path_To_Trusted_ps.pfx_file
   ```

Adaptateurs Oracle/Oracle ERP

Le chapitre Oracle/Oracle ERP dans *Identity Manager Resources Reference* a été divisé en deux chapitres distincts pour cette version. Voir l'addenda *Sun Java™ System Identity Manager Resources Reference* pour afficher ces deux chapitres. (ID-12758)

Adaptateur Oracle

- La prise en charge d'Oracle 8i a été supprimée par erreur du tableau des adaptateurs et de la section adaptateur Oracle au chapitre 1 de Référence des ressources Identity Manager. Identity Manager prend toujours en charge Oracle 8*i* comme ressource. (ID-13078)
- Le nom de section `updateableAttributes` a été corrigé pour *`updatableAttributes`* dans la première étape de la Suppressions Cascade de ce chapitre, comme suit (ID-13075) :

- L'attribut de compte noCascade indique s'il convient d'effectuer des abandons en cascade lors de la suppression des utilisateurs. Par défaut, les abandons en cascade sont effectués. Afin de désactiver les abandons en cascade, ajoutez une entrée à la section `updatableAttributes` de l'objet Configuration système.
- La description du compte `oracleTempTSQuota` devrait être la suivante :

  Quantité maximale de tablespace temporaire que l'utilisateur peut allouer. Si l'attribut figure dans la carte schématique, le quota est toujours défini sur le tablespace temporaire. Si l'attribut est supprimé de la carte schématique, aucun quota ne sera défini sur le tablespace temporaire. L'attribut doit être supprimé pour les adaptateurs qui communiquent avec les ressources Oracle 10gR2. (ID-12843)

Adaptateur Oracle ERP

- L'adaptateur Oracle ERP offre désormais un attribut de compte `employee_number` qui représente un `employee_number` du tableau `per_people_f` (ID-12796):
  - Lorsque vous entrez une valeur à la création, l'adaptateur tente de rechercher un enregistrement utilisateur dans le tableau `per_people_f`, de récupérer `person_id` *dans* l'API de création et d'insérer `person_id` dans la colonne `employee_id` du tableau `fnd_user`.
  - Si aucun `employee_number` n'est entré à la création, aucune tentative n'est faite pour établir le lien.
  - Si vous entrez un `employee_number` à la création et que ce numéro est introuvable, l'adaptateur émet une exception.
  - L'adaptateur tente de retourner `employee_number` sur un `getUser`, si `employee_number` se trouve dans le schéma de l'adaptateur.
- L'attribut de compte `npw_number` prend en charge les travailleurs contingents. Il fonctionne de la même manière que `employee_number`. Les attributs `employee_number` et `npw_number` s'excluent mutuellement. Si vous les saisissez tous les deux à la création, `employee_number` a la priorité. (ID-16507)

Responsabilités d'audit

Plusieurs attributs ont été ajoutés à l'adaptateur Oracle ERP afin de prendre en charge les fonctions d'audit. (ID-11725)

Pour auditer les sous-éléments (comme les formulaires et les fonctions) de responsabilités assignées aux utilisateurs, ajoutez `auditorObject` à la carte schématique. `auditorObject` est un attribut complexe qui contient un ensemble d'objets de responsabilité. Les attributs suivants sont toujours retournés dans un objet de responsabilité :

- responsibility
- userMenuNames
- menuIds
- userFunctionNames
- functionIds
- formIds
- formNames
- userFormNames
- readOnlyFormIds
- readWriteOnlyFormIds
- readOnlyFormNames
- readOnlyUserFormNames
- readWriteOnlyFormNames
- readWriteOnlyUserFormNames
- functionNames
- readOnlyFunctionNames
- readWriteOnlyFunctionNames

Remarque les attributs readOnly et ReadWrite sont identifiés en interrogeant la colonne PARAMETERS dans le tableau fnd_form_functions pour l'un des suivants :

- QUERY_ONLY=YES
- QUERY_ONLY="YES"
- QUERY_ONLY = YES
- QUERY_ONLY = "YES"
- QUERY_ONLY=Y
- QUERY_ONLY="Y"

- QUERY_ONLY = Y
- QUERY_ONLY = "Y"

Si le paramètre de ressource **Return Set of Books and/or Organization** est défini sur TRUE, les attributs suivants sont également retournés :

- setOfBooksName
- setOfBooksId
- organizationalUnitName
- organizationalUnitId

À l'exception des attributs responsibility, setOfBooksName, setOfBooksId, organizationalUnitId et organizationalUnitName, les noms d'attribut correspondent aux noms d'attribut de compte pouvant être ajoutés à la carte schématique.
Les attributs de compte contiennent un ensemble global de valeurs assignées à l'utilisateur. Les attributs contenus dans les objets `responsibility` sont spécifiques à la responsabilité.

La vue auditorResps[] permet d'accéder aux attributs de responsabilité. Le fragment de formulaire suivant retourne toutes les responsabilités actives (et leurs attributs) assignées à un utilisateur.

```
<defvar name='audObj'>
   <invoke name='get'>
      <ref>accounts[Oracle ERP 11i VIS].auditorObject</ref>
   </invoke>
</defvar>
<!—ceci retourne la liste des objets de responsabilité -->
<defvar name='respList'>
   <invoke name='get'>
      <ref>audObj</ref>
      <s>auditorResps[*]</s>
   </invoke>
</defvar>
```

Par exemple :

- `auditorResps[0].responsibility` retourne le nom du premier objet de responsabilité.
- `auditorResps[0].responsibility` retourne les formNames nom du premier objet de responsabilité.

Prise en charge d'Oracle EBS 12

L'adaptateur Oracle ERP prend en charge Oracle E-Business Suite (EBS) version 12. Il n'est plus nécessaire d'éditer ou de mettre en commentaires des sections du OracleERPUserForm, selon la version d'ERP installée comme décrit dans l'*Identity Manager Resources Reference*.

L'attribut FormRef prend maintenant en charge les propriétés suivantes :

- RESOURCE_NAME — Spécifie le nom de la ressource ERP
- VERSION - Spécifie la version de la ressource ERP Les valeurs autorisées sont 11.5.9, 11.5.10, 12.
- RESP_DESCR_COL_EXISTS — Définit la présence de la colonne de description dans le tableau fnd_user_resp_groups_direct. Cette propriété est nécessaire si la version est 11.5.10 ou 12. Les valeurs admises sont TRUE et FALSE.

Ces propriétés doivent être saisies à chaque fois qu'il est fait référence au formulaire de l'utilisateur. Par exemple, le formulaire Tabbed User Form peut avoir besoin de lignes telles que les suivantes pour assurer la prise en charge de la version 12.

```
<FormRef name='Oracle ERP User Form'>
   <Property name='RESOURCE_NAME' value='Oracle ERP R12'/>
   <Property name='VERSION' value='12'/>
   <Property name='RESP_DESCR_COL_EXISTS' value='TRUE'/>
</FormRef>
```

Adaptateur SAP

- Dans la section Attributs de compte, le tableau qui décrit les infotypes iDoc par défaut pris en charge par l'adaptateur Active Sync SAP HR a été corrigé. Le sous-type pris en charge indiqué pour l'infotype 0105 Communication a été changé de EMAIL pour *MAIL* comme suit (ID-12880) :

  Par défaut, les infotypes suivants sont pris en charge :

Infotype	Nom	Sous-types pris en charge
0000	Actions	Non applicable
0001	Organizational Assignment	Non applicable
0002	Personal Data	Non applicable
0006	Addresses	01 (résidence permanente), 03 (résidence d'origine)
0105	Communication	MAIL (adresse email), 0010 (adresse internet)

SAPHRActiveSyncAdapter prend désormais en charge mySAP ERP ECC 5.0 (SAP 5.0).
Les changements suivants ont par conséquent été apportés aux notes de configuration de la ressource (ID-12769) :

Adaptateur de ressources SAP

Les notes de configuration de ressources suivantes s'appliquent uniquement à l'adaptateur de ressources SAP.

Procédez comme suit pour activer la capacité d'un utilisateur à changer son propre mot de passe SAP :

1. Définissez l'attribut de ressource **User Provides Password On Change**.
2. Ajoutez **`WS_USER_PASSWORD`** des deux côtés de la carte schématique. Il est inutile de modifier le formulaire utilisateur ou les autres formulaires.

Adaptateur Active Sync SAP HR

Les notes de configuration de ressources suivantes s'appliquent uniquement à l'adaptateur de ressources Active Sync SAP HR.

La technologie SAP Application Link Enabling (ALE) permet la communication entre les systèmes SAP et externes tels qu'Identity Manager. L'adaptateur Active Sync SAP HR utilise une interface de sortie ALE. Dans une interface de sortie ALE, le système logique de base devient l'expéditeur des messages sortants et le récepteur des messages entrants. Un utilisateur SAP sera probablement connecté au système/client logique de base lors de changements dans la base de données (par exemple, embauche d'un employé, mise à jour de données de position, fin de contrat d'un employé, etc.). Un système/client logique doit aussi être défini pour le client destinataire. Ce système logique sert de récepteur des messages sortants. En ce qui concerne le type de message entre les deux systèmes, l'adaptateur Active Sync utilise un type de message `HRMD_A`. Un type de message caractérise les données envoyées par les systèmes et se rapporte à la structure des données, également appelée type IDoc (par exemple, `HRMD_A05`).

Les étapes suivantes fournissent les configurations nécessaires sur SAP pour que l'adaptateur Active Sync reçoive les alimentations d'autorisation provenant de SAP HR :

Remarque Vous devez configurer les paramètres système SAP pour permettre le traitement Application Link Enabling (ALE) des IDocs `HRMD_A`. Ceci permet de distribuer les données entre deux systèmes d'application, également appelé *messagerie*.

Création d'un système logique

En fonction de votre environnement SAP actuel, il ne sera peut-être pas nécessaire de créer un système logique. Il suffira peut-être de modifier un modèle de distribution en ajoutant le type de message `HRMD_A` à une vue de modèle précédemment configurée. Il importe toutefois de respecter les recommandations SAP pour les systèmes logiques et la configuration de votre réseau ALE. Les instructions suivantes supposent que vous créez de nouveaux systèmes logiques et une nouvelle vue de modèle.

1. Entrez le code de transaction **SPRO**, puis affichez SAP Reference IMGproject (ou le projet applicable à votre organisation).
2. Sur la base de la version SAP que vous utilisez, effectuez l'une des opérations suivantes :
   - Pour SAP 4.6, cliquez sur **Basis Components > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Define Logical System**.
   - Pour SAP 4.7, cliquez sur **SAP Web Application Server > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Define Logical System**.
   - Pour SAP 5.0, cliquez sur **SAP Netweaver > SAP Web Application Server > IDOC Interface/Application Link Enabling (ALE) > Basic Settings > Logical Systems > Define Logical System**.
3. Cliquez sur **Edit** > `New Entries`.
4. Entrez un nom et une description pour le système logique que vous souhaitez créer (IDMGR).
5. Enregistrez votre entrée.

Assignation d'un client au système logique

1. Entrez le code de transaction SPRO, puis affichez SAP Reference IMGproject (ou le projet applicable à votre organisation).
2. Sur la base de la version SAP que vous utilisez, effectuez l'une des opérations suivantes :
   - Pour SAP 4.6, cliquez sur **Basis Components > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Assign Client to Logical System**.
   - Pour SAP 4.7, cliquez sur **SAP Web Application Server > Application Link Enabling (ALE) > Sending and Receiving Systems > Logical Systems > Assign Client to Logical System**.

- Pour SAP 5.0, cliquez sur **SAP Netweaver > SAP Web Application Server > IDOC Interface/Application Link Enabling (ALE) > Basic Settings > Logical Systems > Assign Client to Logical System**.

3. Sélectionnez le client.
4. Cliquez sur **GOTO > Details** pour afficher la boîte de dialogue Client Details.
5. Dans le champ Logical System, entrez le système logique que vous souhaitez assigner à ce client.
6. Dans la section Changes and Transports for Clients, cliquez sur **Automatic Recording of Changes**.
7. Enregistrez votre entrée.

Création d'un modèle de distribution

Pour créer un modèle de distribution :

1. Vérifiez que vous êtes connecté au système/client expéditeur.
2. Entrez le code de transaction **BD64**. Vérifiez que vous êtes en mode Change.
3. Cliquez sur **Edit > Model View > Create**.
4. Entrez le nom abrégé et technique de votre vue, ainsi que la date de début et de fin, puis cliquez sur **Continue**.
5. Sélectionnez la vue que vous avez créée, et cliquez sur **Add Message Type**.
6. Définissez le nom du système expéditeur/logique.
7. Définissez le nom du récepteur/serveur.
8. Dans la section Protection Client Copier and Comparison Tool, cliquez sur **Protection Level: No Restriction**.
9. Définissez le type de message que vous souhaitez utiliser (HRMD_A) et cliquez sur **Continue**.
10. Cliquez sur **Save**.

Enregistrement du module RFC Server avec la passerelle SAP

Lors de l'initialisation, l'adaptateur Active Sync s'enregistre avec la passerelle SAP. Il utilise l'ID "IDMRFC". Cette valeur doit correspondre à la valeur définie dans l'application SAP. Vous devez configurer l'application SAP de sorte que le module RFC Server puisse créer un identificateur vers elle. Pour enregistrer le module RFC Server comme destination RFC :

1. Dans l'application SAP, accédez à la transaction SM59.
2. Développez le répertoire de connexions TCP/IP.
3. Cliquez sur **Create (F8)**.
4. Dans le champ de destination RFC, entrez le nom du système de destination RFC. (IDMRFC).
5. Définissez le type de connexion sur **`T`** (Démarrer un programme externe via TCP/IP).
6. Entrez une description pour la nouvelle destination RFC et cliquez sur **Save**.
7. Cliquez sur le bouton d'enregistrement pour le type d'activation.
8. Définissez l'ID du programme. Nous vous recommandons d'utiliser la même valeur que la destination RFC (IDMRFC), puis de cliquer sur Entrée.
9. Si le système SAP est un système Unicode, le port doit être configuré pour Unicode. Cliquez sur l'onglet **Special Options** et recherchez la section Character Width In Target System. Il existe un paramètre pour unicode et non-unicode.
10. A l'aide des boutons supérieurs - **Test Connection** et **Unicode Test** - testez la connexion d'Identity Manager à la ressource. L'adaptateur doit être démarré pour passer le test.

Création d'une définition de port

Le port est le canal de communication auquel les IDocs sont envoyés. Le port décrit le lien technique entre les systèmes d'envoi et de réception. Vous devez configurer un port RFC pour cette solution. Pour créer une définition de port :

1. Entrez le code de transaction **`WE21`**.
2. Sélectionnez Transactional RFC, puis cliquez sur l'icône **Create**. Entrez la destination RFC **`IDMRFC`**.
3. Enregistrez vos modifications.

Modification de définition de port

Lors de la génération d'un profil partenaire, la définition de port peut avoir été entrée incorrectement. Pour que votre système fonctionne correctement, vous devez modifier la définition de port.

1. Entrez le code de transaction **`WE20`**.
2. Sélectionnez **Partner Type LS**.
3. Sélectionnez le profil de votre partenaire récepteur.
4. Sélectionnez **Outbound Parameters** puis cliquez sur **Display**.
5. Sélectionnez le type de message **`HRMD_A`**.
6. Cliquez sur **Outbound Options** puis modifiez le port récepteur afin qu'il ait le nom du port RFC que vous avez créé (IDMGR).
7. En mode Output, sélectionnez **Transfer IDoc Immediately** pour envoyer les IDocs immédiatement après leur création.
8. Depuis la section IDoc Type, sélectionnez un type de base :
   - Pour SAP 4.6, sélectionnez **HRMD_A05**
   - Pour SAP 4.7, sélectionnez **HRMD_A06**
9. Cliquez sur **Continue**/**Save**.

Adaptateur JDBC sous forme de script

Identity Manager Offre désormais un adaptateur de ressources JDBC sous forme de script pour prendre en charge la gestion de tous les schémas de base de données dans toutes les bases de données accessibles à JDBC. Cet adaptateur prend également Active Sync en charge pour interroger les modifications de compte dans la base de données. Pour des informations détaillées sur cet adaptateur, consultez l'addenda Sun Java™ System *Identity Manager Resources Reference*. (ID-12506)

Adaptateur Shell Script

Identity Manager offre désormais un adaptateur de ressources Shell Script pour prendre en charge la gestion des ressources contrôlées par scripts de shell exécutés sur le système hôte de la ressource. Cet adaptateur, qui est à usage général, est très hautement configurable.

Adaptateur Siebel CRM

Les objets Siebel qui nécessitent une navigation dans le composant professionnel parent/enfant peuvent désormais être créés et mis à jour. Il s'agit d'une fonction avancée qui n'est généralement pas implémentée dans Identity Manager.

La fonction de navigation avancée vous permet de spécifier facultativement les informations suivantes nécessaires pour créer et mettre à jours les composants professionnel enfant:

- nom d'objet professionnel
- nom de composant professionnel parent
- attribut de recherche parent
- composant professionnel cible
- attribut de recherche cible
- dans les attributs d'étendue (quels attributs du composant professionnel doivent être définis/mis à jour)
- co-action facultative

Une règle de navigation avancée peut être utilisée au cours des actions de création et de mise à jour. Elle ne peut pas être utilisée pour d'autres types d'actions.

Pour implémenter la fonction de navigation avancée de l'adaptateur Siebel CRM, procédez comme suit :

- Ajoutez un attribut à la carte schématique dans laquelle l'attribut Resource User (côté droit) s'intitule PARENT_COMP_ID.
- Utilisez la page de débogage pour ajouter manuellement l'attribut de ressource suivant à l'XML de votre ressource

```
<ResourceAttribute name='AdvancedNavRule'
   displayName='Advanced Nav Rule'
   value='MY_SIEBEL_NAV_RULE'>
</ResourceAttribute>
```

  Remplacez *MY_SIEBEL_NAV_RULE* par un nom de règle valide.

- Écrivez la règle de navigation avancée. La règle doit attendre la présence de deux variables :

  `resource.action` — La valeur doit être `create` ou `update`.

  `resource.objectType` — Pour la maintenance de compte normale, cette valeur sera `account`.

La règle doit retourner un mappage avec une ou plusieurs des paires nom/valeur suivantes :

Attribut	Définition
busObj	Nom de l'objet professionnel.
parentBusComp	Nom du composant professionnel parent pour busObj. Le contexte de l'objet professionnel est mis à jour en passant au premier enregistrement qualifié (voir parentSearchAttr) de ce composant professionnel
parentSearchAttr	Attribut à utiliser comme champ de recherche dans parentBusComp. La présence de la valeur à rechercher est attendue sous forme de valeur pour l'attribut dont le nom d'attribut de ressource utilisateur est PARENT_COMP_ID.
busComp	Nom du composant professionnel final à créer ou à mettre à jour. En cas de création, un nouvel enregistrement de ce composant professionnel est créé dans l'objet professionnel. En cas de mise à jour, l'enregistrement de composant professionnel à mettre à jour est sélectionné en passant au premier enregistrement qualifié (voir searchAttr) de ce composant professionnel.
searchAttr	Attribut à utiliser comme champ de recherche dans busComp. La valeur à rechercher est l'ID de compte de l'utilisateur.
attributes	Liste de chaînes qui spécifient l'ensemble de champs dans busComp qui sera défini ou mis à jour. Cette liste remplace les attributs définis dans la carte schématique de la ressource pour l'action effectuée.
coAction	Si l'action requise (resource.action) est create, spécifiez une valeur coAction de update pour indiquer à l'adaptateur d'effectuer également une mise à jour immédiatement après la création. Cela peut être nécessaire si la création n'est pas en mesure de créer tous les champs nécessaires, ce qui exige une mise à jour pour compléter logiquement la création. Cet attribut est ignoré sauf si resource.action est create et coAction défini sur update.

Un exemple de règle de navigation est fourni dans $WSHOME/sample/rules/SiebelNavigationRule.xml.

Adaptateur Sun Java System Access Manager

- Cet adaptateur prend en charge le mode legacy uniquement pour Access Manager 7 et supérieur. Les domaines ne sont pas pris en charge.

Installation et configuration d'Sun Java System Access Manager (Versions antérieures à Access Manager 7.0)

Les étapes 4 et 8 de la procédure « Installation et configuration de Sun Java System Access Manager » doivent indiquer (ID-13087) :

1. Créez un répertoire pour y placer les fichiers qui seront copiés depuis le serveur Sun Java System Access Manager. Ce répertoire est intitulé *CfgDir* dans cette procédure. L'emplacement de Sun Java System Access Manager sera appelé *AccessMgrHome*.
2. Copiez les fichiers suivants depuis *AccessMgrHome* vers *CfgDir*. Ne copiez pas la structure du répertoire.
   - `lib/*.*`
   - `locale/*.properties`
   - `config/serverconfig.xml`
   - `config/SSOConfig.properties` (Identity Server 2004Q2 et supérieur)
   - `config/ums/ums.xml`
3. Sous UNIX, vous devrez peut-être modifier les permissions des fichiers jar dans *CfgDir* pour permettre un accès universel en lecture. Exécutez la commande suivante pour changer les permissions

   `chmod a+r CfgDir/*.jar`
4. Faites précéder le chemin de classe JAVA des éléments suivants :
   - **Windows**: *CfgDir*`;`*CfgDir*`/am_sdk.jar;`*CfgDir*`/am_services.jar;`*CfgDir*`/am_logging.jar`
   - **UNIX**: *CfgDir*`:`*CfgDir*`/am_sdk.jar:`*CfgDir*`/am_services.jar:`*CfgDir*`/am_logging.jar`
5. Si vous utilisez la version 6.0, définissez la propriété système de Java afin qu'elle pointe vers votre*CfgDir*. Utilisez une commande similaire à la suivante :

   ```
   java -Dcom.iplanet.coreservices.configpath=CfgDir
   ```

6. Si vous utilisez la version 6.1 ou supérieure, ajoutez ou modifiez les lignes suivantes dans le fichier *CfgDir*/AMConfig.properties :

   ```
   com.iplanet.services.configpath=CfgDircom.iplanet.security.
   SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFact
   oryImpl

   com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.
   factory.JSSESocketFactory

   com.iplanet.security.encryptor=com.iplanet.services.util.
   JCEEncryption
   ```

   La première ligne définit le chemin `configpath`. Les trois dernières lignes changent les paramètres de sécurité.

7. Copiez les fichiers *CfgDir*/am_*.jar dans $WSHOME/WEB-INF/lib. Si vous utilisez la version 6.0, copiez aussi le fichier jss311.jar dans le répertoire $WSHOME/WEB-INF/lib.

8. Si Identity Manager est exécuté sous Windows et que vous utilisez Identity Server 6.0, copiez *IdServer*\lib\jss*.dll dans *CfgDir* et ajoutez *CfgDir* à votre chemin système.

Remarque Dans un environnement où Identity Manager est installé sur un autre système que Sun Java System Access Manager, contrôlez les conditions d'erreur suivantes. Si une erreur java.lang.ExceptionInInitializerError, suivie de java.lang.NoClassDefFoundError, lors de tentatives successives, est retournée en essayant de vous connecter à la ressource Sun Java System Access Manager, recherchez des données de configuration incorrectes ou manquantes.

Vérifiez également que la classe du fichier jar est celle indiquée par `java.lang.NoClassDefFoundError`. Faites précéder le chemin de classe du fichier jar contenant la classe du chemin de classe JAVA sur le serveur d'application.

Installation et configuration de Sun Java System Access Manager (Versions 7.0 et supérieures en mode Legacy)

Utilisez les étapes suivantes pour installer et configurer l'adaptateur de ressources au mode legacy.

1. Suivez les instructions fournies dans le *Sun Java™ System* Guide du développeur Access Manager 7 2005Q4 pour construire le SDK client depuis l'installation Sun Access Manager.
2. Extrayez les fichiers AMConfig.properties et amclientsdk.jar du fichier war produit.

3. Placez une copie de `AMConfig.properties` dans le répertoire suivant :

   InstallDir`/WEB-INF/classes`

4. Placez une copie de `amclientsdk.jar` dans le répertoire suivant :

   InstallDir`/WEB-INF/lib`

Adaptateur de Services de communications Sun Java System

- L'exemple de script qui peut être exécuté sur la ressource proxy après la création d'un utilisateur est indiqué de façon incorrecte. Le script ci-après peut être utilisé à la place : (ID-12536)

```
SET PATH=c:\Sun\Server-Root\lib
SET SYSTEMROOT=c:\winnt
SET CONFIGROOT=C:/Sun/Server-Root/Config
mboxutil -c -P user/%WSUSER_accountId%.*
```

- Les attributs de compte binaire suivants de la classe d'objet inetOrgPerson sont désormais pris en charge :

Attribut Resource User	Syntaxe LDAP	Description
audio	Audio	Un fichier audio.
jpegPhoto	JPEG	Une image au format JPEG.
userCertificate	certificate	Un certificat au format binaire.

D'autres comptes binaires peuvent être pris en charge, mais ils n'ont pas été testés.

Adaptateur Top Secret

Identity Manager Resources Reference indique de façon erronée que l'adaptateur Top Secret prend en charge la fonction renommer les comptes. L'adaptateur ne prend pas cette fonction en charge pour les comptes Top Secret.

Chapitre 3 : Adding Actions to Resources

Dans la section « Exemples sous Windows NT », les noms des champs (`Field`) des trois exemples sont mal définis. Remplacez toutes les instances de `accounts[NT].attributes.` par `resourceAccounts.currentResourceAccounts[NT].attributes.` Par exemple, à la section « Exemple 3 : Action that Follows the Deletion of a User », le nom `Field` à l'étape 4 devrait êtr rectifié de la sorte :

```
<Field name=
'resourceAccounts.currentResourceAccounts[NT].attributes.delete after
action'>
```

Messages de réglage, de dépannage et d'erreur d'Identity Manager

Ajouts

- Vous pouvez maintenant utiliser l'utilitaire de suivi standard sur com.waveset.task.Scheduler pour suivre l'ordonnanceur de tâches si une tâche pose problème.

  Pour plus d'informations, voir *Tracing the Identity Manager Server* dans *Sun Java™ System Identity Manager Messages de réglage, de dépannage et d'erreur*.

- Pour déboguer un problème qui survient à un niveau inférieur à une méthode d'entrée spécifique, envisagez le suivi au niveau de la méthode. Identity Manager offre désormais la possibilité de suivre uniquement une méthode et ses sous-appels directs et indirects. (ID-14967)

  Pour activer cette fonction, définissez le niveau de suivi pour une étendue avec le modificateur`subcalls`, comme dans l'exemple suivant :

```
trace 4,subcalls=2
com.waveset.recon.ReconTask$WorkerThread#reconcileAccount
```

  La méthode `reconcileAccount()` est ainsi suivie au niveau 4 et tous les sous-appels au niveau 2.

  Voir *Définition d'une configuration de suivi* dans Messages de réglage, de dépannage et d'erreur de *Sun Java™ System Identity Manager* pour des informations plus détaillées.

Corrections

Étant donné que vous devez installer JDK 1.4.2 pour cette version, les instructions indiquant de supprimer les fichiers jar Cryptix (`cryptix-jceapi.jar` et `cryptix-jce-provider.jar`) du répertoire `idm\WEB-INF\lib` dans le chapitre 1: *Réglage de performance, optimisation de l'environnement J2EE,* ne s'appliquent plus (sauf si vous effectuez une mise à niveau depuis une version précédente d'Identity Manager).

Outils de déploiement d'Identity Manager

Corrections

Chapitre 7 : Utilisation des services web d'Identity Manager

L'exemple launchProcess fourni dans la section Exemples ExtendedRequest a été corrigé comme suit (ID-13044) :

launchProcess

L'exemple qui suit affiche un format type pour une demande `launchProcess`. (Vue — Vue processus).

```
ExtendedRequest req = new ExtendedRequest();
req.setOperationIdentifier("launchProcess");
req.setAsynchronous(false);
req.setAttribute("process", "Custom Process Name");
req.setAttribute("taskName", "Custom Process Display Name");
SpmlResponse res = client.request(req);
```

Utilisation de helpTool

Dans la version Identity Manager 6.0, une nouvelle fonction vous permettant d'effectuer des recherches dans l'aide en ligne et les fichiers de documentation, dont le format est HTML, a été ajoutée. Le moteur de recherche est basé sur la technologie de moteur de recherche « Nova » de SunLabs.

L'utilisation du moteur Nova se fait en deux phases : l'*indexation* et la *récupération*. Pendant la phase d'indexation, les documents d'entrée sont analysés et un index, qui sera utilisé en phase de récupération, est créé. Lors de la récupération, il est possible d'extraire des « passages » constituant le contexte dans lequel les termes demandés ont été trouvés. Le processus de récupération des passages requiert la présence des fichiers HTML d'origine, qui doivent donc figurer à un emplacement accessible au moteur de recherche dans le système de fichiers.

helpTool est un programme Java qui effectue deux fonctions de base :

- Il copie les fichiers sources HTML dans un emplacement connu du moteur de recherche.
- Il crée l'index utilisé pendant la phase de récupération.

Vous exécutez helpTool à partir de la ligne de commande en procédant comme suit :

```
$ java -jar helpTool.jar
usage: HelpTool
 -d    Répertoire de destination
 -h    Ces informations d'aide
 -i    Répertoire ou JAR contenant les fichiers d'entrée, sans
caractères génériques
 -n    Répertoire de l'index Nova
 -o    Nom du fichier de sortie
 -p    Fichier des propriétés d'indexation
```

Reconstruction/Recréation de l'index de l'aide en ligne

Les fichiers HTML de l'aide en ligne sont compressés dans un fichier JAR. Vous devez les extraire dans un répertoire pour le moteur de recherche. Utilisez la procédure suivante :

1. Décompressez la distribution de helpTool dans un répertoire temporaire. (Details TBD)

   Dans cet exemple, nous allons extraire les fichiers dans `/tmp/helpTool`.

2. Dans un shell UNIX ou une fenêtre de commande Windows, passez au répertoire dans lequel l'application Identity Manager a été déployée dans votre conteneur Web.

   Par exemple, un répertoire pour Sun Java System Application Server ressemble à celui-ci :

   ```
   /opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm
   ```

3. Faites du répertoire `help/` votre répertoire de travail courant.

Remarque Il est important d'exécuter helpTool depuis ce répertoire, sinon l'index risque de ne pas être compilé correctement. En outre, vous devez supprimer les anciens fichiers d'index en effaçant le contenu du sous-répertoire `index/help/`.

4. Rassemblez les informations suivantes pour les arguments de ligne de commande :

• **Répertoire de destination :**	`html/help/en_US` **Remarque** : Utilisez la chaîne locale appropriée pour votre installation.
• **Fichiers d'entrée** :	`../WEB-INF/lib/idm.jar`
• **Répertoire de l'index Nova** :	`index/help`
• **Nom du fichier de sortie** :	`index_files_help.txt` **Remarque** : Le nom de ce fichier n'est pas important, mais l'outil se fermera si ce fichier existe déjà.
• **Fichier des propriétés d'indexation** :	`index/index.properties`

5. Exécutez la commande suivante :

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/help/en_US -i ../
WEB-INF/lib/idm.jar -n index/help -o help_files_help.txt -p
index/index.properties
Extracted 475 files.
[15/Dec/2005:13:11:38] PM Init index/help AWord 1085803878
[15/Dec/2005:13:11:38] PM Making meta file: index/help/MF: 0
[15/Dec/2005:13:11:38] PM Created active file: index/help/AL
[15/Dec/2005:13:11:40] MP Partition: 1, 475 documents, 5496 terms.
[15/Dec/2005:13:11:40] MP Finished dumping: 1 index/help 0.266
[15/Dec/2005:13:11:40] IS 475 documents, 6,56 MB, 2,11 s, 11166,66
MB/h
[15/Dec/2005:13:11:40] PM Waiting for housekeeper to finish
[15/Dec/2005:13:11:41] PM Shutdown index/help AWord 1085803878
```

Reconstruction/Recréation de l'index de la documentation

Utilisez la procédure suivante pour reconstruire ou recréer l'index de la documentation :

1. Décompressez la distribution de helpTool dans un répertoire temporaire. (Details TBD)

   Dans cet exemple, nous allons extraire les fichiers dans `/tmp/helpTool`.

2. Dans un shell UNIX ou une fenêtre de commande Windows, passez au répertoire dans lequel l'application Identity Manager a été déployée dans votre conteneur Web.

   Par exemple, un répertoire pour Sun Java System Application Server ressemble à celui-ci :

   ```
   /opt/SUNWappserver/domains/domain1/applications/j2ee-modules/idm
   ```

3. Faites du répertoire `help/` votre répertoire de travail courant.

Remarque Il est important d'exécuter helpTool depuis ce répertoire, sinon l'index risque de ne pas être compilé correctement. En outre, vous devez supprimer les anciens fichiers d'index en effaçant le contenu du sous-répertoire `index/docs/`.

4. Rassemblez les informations suivantes pour les arguments de ligne de commande :

• **Répertoire de destination :**	`html/docs`
• **Fichiers d'entrée** :	`../doc/HTML/en_US` **Remarque** : L'outil copie le répertoire `en_US/` et les sous-répertoires dans la destination.
• **Répertoire de l'index Nova** :	`index/docs`
• **Nom du fichier de sortie** :	`index_files_docs.txt` **Remarque** : Le nom de ce fichier n'est pas important, mais l'outil se fermera si ce fichier existe déjà.
• **Fichier des propriétés d'indexation** :	`index/index.properties`

5. Exécutez la commande suivante :

```
$ java -jar /tmp/helpTool/helpTool.jar -d html/docs -i
../doc/HTML/en_US -n index/docs -o help_files_docs.txt -p
index/index.properties
Copied 84 files.
Copied 105 files.
Copied 1 files.
Copied 15 files.
Copied 1 files.
Copied 58 files.
Copied 134 files.
Copied 156 files.
Copied 116 files.
Copied 136 files.
Copied 21 files.
Copied 37 files.
Copied 1 files.
Copied 13 files.
Copied 2 files.
Copied 19 files.
Copied 20 files.
Copied 52 files.
Copied 3 files.
Copied 14 files.
Copied 3 files.
Copied 3 files.
Copied 608 files.
[15/Dec/2005:13:24:25] PM Init index/docs AWord 1252155067
[15/Dec/2005:13:24:25] PM Making meta file: index/docs/MF: 0
[15/Dec/2005:13:24:25] PM Created active file: index/docs/AL
[15/Dec/2005:13:24:28] MP Partition: 1, 192 documents, 38488 terms.
[15/Dec/2005:13:24:29] MP Finished dumping: 1 index/docs 0.617
[15/Dec/2005:13:24:29] IS 192 documents, 14.70 MB, 3.81 s, 13900.78
MB/h
[15/Dec/2005:13:24:29] PM Waiting for housekeeper to finish
[15/Dec/2005:13:24:30] PM Shutdown index/docs AWord 1252155067
```

API désapprouvées

Ce chapitre indique toutes les API d'Identity Manager désapprouvées dans Identity Manager 6.0 2005Q4M3 et leurs substituts (le cas échéant). Il se compose des sections suivantes :

- Constructeurs désapprouvés
- Méthodes et champs désapprouvés

Constructeurs désapprouvés

Le tableau suivant recense les constructeurs désapprouvés et, le cas échéant, les constructeurs de substitution correspondants.

Constructeur désapprouvé	Substitut
com.waveset.adapter.ActiveDirectoryActiveSyncAdapter	com.waveset.adapter.ADSIResourceAdapter
com.waveset.adapter.AD_LDAPResourceAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.AttrParse	com.waveset.object.AttrParse
com.waveset.adapter.ConfirmedSync	
com.waveset.adapter.DblBufIterator	com.waveset.util.BufferedIterator com.waveset.util.BlockIterator com.waveset.adapter.AccountIteratorWrapper
com.waveset.adapter.DominoActiveSyncAdapter	com.waveset.adapter.DominoResourceAdapter
com.waveset.adapter.LDAPChangeLogActiveSyncAdapter	com.waveset.adapter.LDAPResourceAdapter
com.waveset.adapter.NDSActiveSyncAdapter	com.waveset.adapter.NDSResourceAdapter
com.waveset.adapter.PeopleSoftResourceAdapter	
com.waveset.adapter.RemedyActiveSyncResourceAdapter	com.waveset.adapter.RemedyResourceAdapter
com.waveset.adapter.TopSecretActiveSyncAdapter	com.waveset.adapter.TopSecretResourceAdapter
com.waveset.exception.ConfigurationError	com.waveset.util.ConfigurationError

Constructeur désapprouvé	Substitut
com.waveset.exception.IOException	com.waveset.util.IOException
com.waveset.exception.XmlParseException	com.waveset.util.XmlParseException
com.waveset.object.IAPI	com.waveset.adapter.iapi.IAPI
com.waveset.object.IAPIProcess	com.waveset.adapter.iapi.IAPIFactory
com.waveset.object.IAPIUser	com.waveset.adapter.iapi.IAPIUser
com.waveset.object.RemedyTemplate	
com.waveset.object.ReportCounter	
com.waveset.object.SourceManager	com.waveset.view.SourceAdapterManageView
com.waveset.security.authn.LoginInfo	com.waveset.object.LoginInfo
com.waveset.security.authn.SignedString	com.waveset.util.SignedString
com.waveset.security.authn.Subject	com.waveset.object.Subject
com.waveset.security.authz.Permission	com.waveset.object.Permission
com.waveset.security.authz.Right	com.waveset.object.Right
com.waveset.util.Debug	com.sun.idm.logging.Trace
com.waveset.util.HtmlUtil	com.waveset.ui.util.html.HtmlUtil
com.waveset.util.ITrace	com.sun.idm.logging.Trace

Méthodes et champs désapprouvés

Les tableaux de cette section répertorient l'ensemble des méthodes et champs désapprouvés dans cette version. Les méthodes et les champs sont triés par nom de classe.

Les données de la colonne **Substitut** peuvent contenir les types d'information suivants :

- Si la colonne est vide, cela signifie qu'aucun substitut n'est disponible pour la méthode ou le champ en question.
- L'absence de nom de classe indique que la méthode ou le champ de substitution sont définis dans la même classe que l'élément désapprouvé.

- Si la méthode ou le champ de substitution sont définis dans une autre classe que celle de l'élément désapprouvé, le substitut est indiqué suivant la syntaxe Javadoc. Par exemple, la méthode `getBaseContextAttrName()` dans la classe com.waveset.adapter.ADSIResourceAdapter ayant été désapprouvée, elle a été remplacée par `com.waveset.adapter.ResourceAdapter#ResourceAdapter()`

  où :

  - `com.waveset.adapter` est le nom du package.
  - `ResourceAdapter` est le nom de la classe.
  - `ResourceAdapter()` correspond à la liste des méthodes et des arguments.

com.waveset.adapter.AccessManagerResourceAdapter

Méthode désapprouvée	Substitut
handlePDException(Exception)	handlePDException(PDException)

com.waveset.adapter.ACF2ResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.ActiveSync

Champ désapprouvé	Substitut
RA_UPDATE_IF_DELETE	

com.waveset.adapter.ActiveSyncUtil

Méthode désapprouvée	Substitut
getLogFileFullPath()	

com.waveset.adapter.ADSIResourceAdapter

Méthode ou champ désapprouvé(e)	Substitut
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map,Map,ResourceAdapterBase)
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

com.waveset.adapter.AgentResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.AIXResourceAdapter.BlockAcctIter

Méthode désapprouvée	Substitut
BlockAcctIter(AIXResourceAdapter,CaptureList)	BlockAcctIter(CaptureList)
BlockAcctIter(int,CaptureList)	BlockAcctIter(CaptureList)

com.waveset.adapter.AuthSSOResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.ClearTrustResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.DatabaseTableResourceAdapter

Champ désapprouvé	Substitut
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.DB2ResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.DominoResourceAdapter

Méthode ou champ désapprouvé(e)	Substitut
buildEvent(UpdateRow)	com.waveset.adapter.iapi.IAPIFactory#getIAPI(Map,Map,ResourceAdapterBase)
RA_UPDATE_IF_DELETE	com.waveset.adapter.ActiveSync#RA_DELETE_RULE

com.waveset.adapter.DominoResourceAdapterBase

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.ExampleTableResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.GenericScriptResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.GetAccessResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.HostConnectionPool

Méthode désapprouvée	Substitut
getConnection(HostAccessLogin)	com.waveset.adapter.HostConnPool#getAffinityConnection(HostAccessLogin)
releaseConnection(HostAccess)	com.waveset.adapter.HostConnPool#releaseConnection(HostAccess)

com.waveset.adapter.HostConnPool

Méthode désapprouvée	Substitut
getConnection(HostAccessLogin)	getAffinityConnection(HostAccessLogin)
putFree()	

com.waveset.adapter.iapi.IAPIFactory

Méthode désapprouvée	Substitut
getIAPIProcess(Map,Map,String,Resource)	getIAPI(Map,Map,String,ResourceAdapterBase)
getIAPIProcess(Element)	
getIAPIUser(Element)	
getIAPIUser(Map,Map,String,Map)	getIAPI(Map,Map,String,ResourceAdapterBase)
getIAPIUser(Map,Map,String,Resource)	getIAPI(Map,Map,String,ResourceAdapterBase)

com.waveset.adapter.IDMResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.INISafeNexessResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.LDAPResourceAdapterBase

Méthode ou champ désapprouvé(e)	Substitut
addUserToGroup(LDAPObject,String,String)	addUserToGroup(String,String,String)
buildBaseUrl()	
buildBaseUrl(String)	
buildEvent(UpdateRow)	
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()
getGroups(Name,String,Vector,Vector)	getGroups(String,String,Vector,Vector)
getLDAPAttributes(String,DirContext[],String)	getLDAPAttributes(String,DirContext,String,String[])
getLDAPAttributes(String,DirContext[])	getLDAPAttributes(String,DirContext,String,String[])
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE
removeNameFromAttribute(DirContext,Name,Attribute)	removeNameFromAttribute(DirContext,String,boolean,Attribute)
removeUserFromAllGroups(Name,String,WavesetResult)	removeUserFromAllGroups(String,boolean,String,WavesetResult)
removeUserFromGroup(DirContext,Name,String,String,Attributes)	removeUserFromGroup(DirContext,String,boolean,String,String,Attributes)
removeUserFromGroups(Name,Vector,String,WavesetResult)	removeUserFromGroups(String,boolean,Vector,String,WavesetResult)

com.waveset.adapter.MySQLResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.NaturalResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.NDSResourceAdapter

Méthode désapprouvée	Substitut
buildEvent(UpdateRow)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.ONTDirectorySmartResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.OS400ResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter

Méthode ou champ désapprouvé(e)	Substitut
DEFAULT_AUDIT_STAMP_FORMAT	
DEFAULT_AUDIT_STAMP_START_DATE	
getAccountAttributes(String)	
getUpdateRows(UpdateRow)	getUpdateRows(UpdateRow)
RA_AUDIT_STAMP_FORMAT	

com.waveset.adapter.RACFResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.RASecureConnection

Méthode désapprouvée	Substitut
ExchangeAuth(boolean)	ExchangeAuth(boolean,byte[])

com.waveset.adapter.RedHatLinuxResourceAdapter.BlockAcctIter

Méthode désapprouvée	Substitut
BlockAcctIter(int,CaptureList)	BlockAcctIter(SVIDResourceAdapter,CaptureList)

com.waveset.adapter.RequestResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.ResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceAdapterBase

Méthode désapprouvée	Substitut
getAccountAttributes(String)	
getAdapter(Resource,LighthouseContext)	getAdapterProxy(Resource,LighthouseContext)
getAdapter(Resource,ObjectCache,WSUser)	getAdapterProxy(Resource,ObjectCache)
getAdapter(Resource,ObjectCache)	getAdapterProxy(Resource,LighthouseContext)
getBaseContextAttrName()	getBaseContexts()
isExcludedAccount(String,Rule)	com.waveset.adapter.ResourceAdapterProxy#isExcludedAccount(String, Map,ResourceOperation,Rule)
isExcludedAccount(String)	com.waveset.adapter.ResourceAdapterProxy#isExcludedAccount(String, Map,ResourceOperation,Rule)

com.waveset.adapter.ResourceAdapterProxy

Méthode désapprouvée	Substitut
getAccountAttributes(String)	
getBaseContextAttrName()	getBaseContexts()

com.waveset.adapter.ResourceManager

Méthode désapprouvée	Substitut
getResourceTypes()	getResourcePrototypes() getResourcePrototypes(ObjectCache,boolean)
getResourceTypeStrings()	getResourcePrototypeNames(ObjectCache)

com.waveset.adapter.SAPHRActiveSyncAdapter

Champ désapprouvé	Substitut
RA_PROCESS_NAME	com.waveset.adapter.ActiveSync#RA_PROCESS_RULE

com.waveset.adapter.SAPResourceAdapter

Méthode désapprouvée	Substitut
unexpirePassword(String,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)
unexpirePassword(WSUser,WavesetResult)	unexpirePassword(String, String,String,WavesetResult)

com.waveset.adapter.ScriptedConnection

Sous-classe	Méthode désapprouvée	Substitut
Script	hasNextToken()	
Script	nextToken()	
ScriptedConnection	disConnect()	com.waveset.adapter.ResourceConnection#disconnect()
ScriptedConnectionFactory	getScriptedConnection(String,HashMap)	com.waveset.adapter.ScriptedConnectionPool#getConnection(HashMap,String,long,boolean)
SSHConnection	disConnect()	disconnect()
TelnetConnection	disConnect()	disconnect()

com.waveset.adapter.ScriptedHostResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.SkeletonResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.SMEResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.SQLServerResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.SunAccessManagerResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	
getBaseContextAttrName()	com.waveset.adapter.ResourceAdapter#getBaseContexts()

com.waveset.adapter.SVIDResourceAdapter.BlockAcctIter

Méthode ou champ désapprouvé(e)	Substitut
BlockAcctIter(int,CaptureList)	BlockAcctIter(CaptureList)
BlockAcctIter(SVIDResourceAdapter,CaptureList)	BlockAcctIter(CaptureList)

com.waveset.adapter.SybaseResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.TestResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.TopSecretResourceAdapter

Méthode désapprouvée	Substitut
hasError(String,String)	hasError(String,String,String)
login(HostAccess hostAccess)	login(HostAccess,ServerAffinity)

com.waveset.adapter.VerityResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.adapter.XMLResourceAdapter

Méthode désapprouvée	Substitut
getAccountAttributes(String)	

com.waveset.msgcat.Catalog

Méthode désapprouvée	Substitut
getMessage(String,Object[],Locale)	format (Locale,String,Object[])
getMessage(Locale,String,Object[])	format (Locale,String,Object[])

Méthode désapprouvée	Substitut
getMessage(Locale,String)	format (Locale,String)
getMessage(String,Locale)	format (Locale,String)
getMessage(String,Object[])	format (Locale,String,Object[])

com.waveset.object.Account

Méthode désapprouvée	Substitut
getUnowned()	hasOwner()
setUnowned(boolean)	setOwner(WSUser)

com.waveset.object.AccountAttributeType

Méthode désapprouvée	Substitut
getAttrType()	getSyntax()
setAttrType(String)	setSyntax(String) setSyntax(Syntax)

com.waveset.object.Attribute

Méthode ou champ désapprouvé(e)	Substitut
BLOCK_SIZE	BLOCK_ROWS_GET BLOCK_ROWS_LIST
EVENTDATE	EVENT_DATETIME
EVENTTIME	EVENT_DATETIME
getDbColumnLength()	
getDbColumnName()	

Méthode ou champ désapprouvé(e)	Substitut
STARTUP_TYPE_AUTO	com.waveset.object.Resource#STARTUP_TYPE_AUTO
STARTUP_TYPE_AUTO_FAILOVER	com.waveset.object.Resource#STARTUP_TYPE_AUTO_FAILOVER
STARTUP_TYPE_DISABLED	com.waveset.object.Resource#STARTUP_TYPE_DISABLED
STARTUP_TYPE_MANUAL	com.waveset.object.Resource#STARTUP_TYPE_MANUAL
STARTUP_TYPES	com.waveset.object.Resource#STARTUP_TYPES
STARTUP_TYPES_DISPLAY_NAMES	com.waveset.object.Resource#STARTUP_TYPES_DISPLAY_NAMES

com.waveset.object.AttributeDefinition

Méthode désapprouvée	Substitut
AttributeDefinition(String,String)	AttributeDefinition(String,Syntax)
setAttrType(String)	setSyntax(Syntax)

com.waveset.object.AuditEvent

Méthode désapprouvée	Substitut
setAttributeMap(Map)	setAuditableAttributes(Map)
addAuditableAttributes(AccountAttributeType[],WSAttributes)	setAuditableAttributes(Map)
getAttributeMap()	getAuditableAttributes()
getAttributeValue(String)	getAuditableAttributes()
setAccountAttributesBlob(Map)	setAccountAttributesBlob(Map,Map)
setAccountAttributesBlob(WSAttributes,List)	setAccountAttributesBlob(WSAttributes,WSAttributes,List)

com.waveset.object.CacheManager

Méthode désapprouvée	Substitut
getAllObjects(Type,AttributeCondition[])	listObjects(Type,AttributeCondition[])
getAllObjects(Type,WSAttributes)	listObjects(Type,WSAttributes)
getAllObjects(Type)	listObjects(Type)

com.waveset.object.Constants

Champ désapprouvé	Substitut
MAX_SUMMARY_STRING_LENGTH	

com.waveset.object.EmailTemplate

Méthode ou champ désapprouvé(e)	Substitut
setToAddress(String)	setTo(String)
getFromAddress()	getFrom()
getToAddress()	getTo()
setFromAddress(String)	setFrom(String)
VAR_FROM_ADDRESS	VAR_FROM
VAR_TO_ADDRESS	VAR_TO

com.waveset.object.Form

Méthode ou champ désapprouvé(e)	Substitut
EL_HELP	com.waveset.object.GenericObject#toMap(int)
getDefaultDataType()	getDefaultSyntax()
getType()	getSyntax()
setType(String)	setSyntax(Syntax)

com.waveset.object.GenericObject

Méthode désapprouvée	Substitut
toMap(boolean)	toMap(String,int)
toMap(String,boolean)	

com.waveset.object.LoginConfig

Méthode désapprouvée	Substitut
getApp(String)	getLoginApp(String)

com.waveset.object.MessageUtil

Méthode désapprouvée	Substitut
getActionDisplayKey(String)	
getEventParmDisplayKey(String)	
getResultDisplayKey(String)	
getTypeDisplayKey(String)	com.waveset.ui.FormUtil#getTypeDisplayName(LighthouseContext,String)

com.waveset.object.RepositoryResult

Méthode désapprouvée	Substitut
get(int)	next()
getId(int)	
getName(int)	
getObject(int)	
getRowCount()	
getRows()	
seek(int)	hasNext() next()
sort()	

com.waveset.object.RepositoryResult.Row

Méthode désapprouvée	Substitut
getSummaryAttributes()	getAttributes()

com.waveset.object.ResourceAttribute

Méthode désapprouvée	Substitut
setType(String)	setSyntax(Syntax)

com.waveset.object.TaskInstance

Champ désapprouvé	Substitut
DATE_FORMAT	com.waveset.util.Util#stringToDate(String,String) com.waveset.util.Util#getCanonicalDate(Date) com.waveset.util.Util#getCanonicalDate(Date,TimeZone) com.waveset.util.Util#getCanonicalDate(long)
VAR_RESULT_LIMIT	setResultLimit(int) getResultLimit()
VAR_TASK_STATUS	

com.waveset.object.TaskTemplate

Méthode désapprouvée	Substitut
setMode(String)	setExecMode(String)
setMode(TaskDefinition.ExecMode)	setExecMode(TaskDefinition,ExecMode)

com.waveset.object.Type

Méthode ou champ désapprouvé(e)	Substitut
AUDIT_CONFIG	
AUDIT_PRUNER_TASK	
AUDIT_QUERY	
DISCOVERY	
getSubtypes()	getLegacyTypes()
NOTIFY_CONFIG	
REPORT_COUNTER	

Méthode ou champ désapprouvé(e)	Substitut
SUMMARY_REPORT_TASK	
USAGE_REPORT	
USAGE_REPORT_TASK	

com.waveset.object.UserUIConfig

Méthode désapprouvée	Substitut
getCapabilityGroups()	
getAppletColumns()	getAppletColumnDefs()
getCapabilityGroup(String)	
getCapabilityGroupNames()	
getFindMatchOperatorDisplayNameKeys()	
getFindMatchOperators()	
getFindResultsColumns()	
getFindResultsSortColumn()	
getFindUserDefaultSearchAttribute()	
getFindUserSearchAttributes()	
getFindUserShowAttribute(int)	
getFindUserShowCapabilitiesSearch(int)	
getFindUserShowDisabled(int)	
getFindUserShowOrganizationSearch(int)	
getFindUserShowProvisioningSearch(int)	
getFindUserShowResourcesSearch(int)	
getFindUserShowRoleSearch(int)	

com.waveset.object.ViewMaster

Méthode désapprouvée	Substitut
ViewMaster()	ViewMaster(LighthouseContext)
ViewMaster(String,String)	ViewMaster(LighthouseContext)
ViewMaster(Subject,String)	ViewMaster(LighthouseContext)

com.waveset.session

Sous-classe	Méthode ou champ désapprouvé(e)	Substitut
Session	listApprovers()	getAdministrators(Map)
	listControlledApprovers()	getAdministrators(Map)
	listSimilarApprovers(String adminName)	getAdministrators(Map)
SessionFactory	getApp(String)	getLoginApp(String)
	getApps()	getLoginApps()
WorkflowServices	ARG_TASK_DATE	com.waveset.object.Attribute#DATE

com.waveset.task.TaskContext

Méthode désapprouvée	Substitut
getAccessPolicy()	
getRepository()	

com.waveset.ui.util.FormUtil

Méthode désapprouvée	Substitut
getAdministrators(Session,List)	getUsers(LighthouseContext,Map)
getAdministrators(Session,Map)	getUsers(LighthouseContext,Map)
getApplications(LighthouseContext,List)	getApplications(LighthouseContext,Map)
getApplications(LighthouseContext)	getApplications(LighthouseContext,Map)
getApproverNames(Session,List)	getUsers(LighthouseContext,Map)
getApproverNames(Session)	getUsers(LighthouseContext,Map)
getApprovers(Session,List)	getUsers(LighthouseContext,Map)
getApprovers(Session)	getUsers(LighthouseContext,Map)
getCapabilities(LighthouseContext,List,Map)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,List)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext,String,String)	getCapabilities(LighthouseContext,Map)
getCapabilities(LighthouseContext)	getCapabilities(LighthouseContext,Map)
getObjectNames(LighthouseContext,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String, String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,String,String,String,List)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String,List,Map)	getObjectNames(LighthouseContext,String,Map)
getObjectNames(LighthouseContext,Type,String,String,List)	getObjectNames(LighthouseContext,String,Map)
getOrganizations(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)

Méthode désapprouvée	Substitut
getOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext,boolean,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext,boolean)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getSimilarApproverNames(Session,String)	getUsers(LighthouseContext,Map)
getSimilarApproverNames(Session)	getUsers(LighthouseContext,Map)
getSimilarApprovers(Session,String)	getUsers(LighthouseContext,Map)
getSimilarApprovers(Session)	getUsers(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizations(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext,Map)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNames(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)

Méthode désapprouvée	Substitut
getUnassignedOrganizationsDisplayNamesWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext,List)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedOrganizationsWithPrefixes(LighthouseContext)	getOrganizationsDisplayNames(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,List,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String,List)	getUnassignedResources(LighthouseContext,Map)
getUnassignedResources(LighthouseContext,String)	getUnassignedResources(LighthouseContext,Map)

com.waveset.ui.util.html

Sous-classe	Méthode ou champ désapprouvé(e)	Substitut
Composant	isNoWrap()	
	setHelpKey(String)	
	setNoWrap(boolean)	
HtmlHeader	NORMAL_BODY	
MultiSelect	isLockhart()	
	setLockhart(boolean)	
WizardPanel	setPreviousLabel(String)	setPrevLabel(String)

com.waveset.util.JSSE

Méthode désapprouvée	Substitut
installIfAvailable()	

com.waveset.util.PdfReportRenderer

Méthode désapprouvée	Substitut
render(Element,boolean,String,OutputStream)	render(Element,boolean,String,OutputStream,String,boolean)
render(Element,boolean,String)	render(Element,boolean,String,String,boolean)
render(Report,boolean,String,OutputStream)	render(Report,boolean,String,OutputStream,String,boolean)
render(Report,boolean,String)	render(String,boolean,String,String,boolean)

com.waveset.util.Quota

Méthode désapprouvée	Substitut
getQuota()	

com.waveset.util.ReportRenderer

Méthode ou champ désapprouvé(e)	Substitut
renderToPdf(Report,boolean,String,OutputStream)	renderToPdf(Report,boolean,String,OutputStream,String,boolean)
renderToPdf(Report,boolean,String)	renderToPdf(Report,boolean,String,String,boolean)

com.waveset.util.Trace

Méthode désapprouvée	Substitut
data(long,Object,String,byte[])	com.sun.idm.logging.trace.Trace#data(long,String,byte[])
entry(long,Object,String,Object[])	com.sun.idm.logging.trace.Trace#entry(long,String,Object[])
entry(long,Object,String,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
entry(long,Object,String)	com.sun.idm.logging.trace.Trace#entry(long,String)
exception(long,Object,String,t)	com.sun.idm.logging.trace.Trace#throwing(long,String,Throwable) com.sun.idm.logging.trace.Trace#caught(long,String,Throwable)
exit(long,Object,String,boolean)	com.sun.idm.logging.trace.Trace#exit(long,String,boolean)
exit(long,Object,String,int)	com.sun.idm.logging.trace.Trace#exit(long,String,int)
exit(long,Object,String,long)	com.sun.idm.logging.trace.Trace#exit(long,String,long)
exit(long,Object,String,Object)	com.sun.idm.logging.trace.Trace#exit(long,String,Object)
exit(long,Object,String)	com.sun.idm.logging.trace.Trace#exit(long,String)
getTrace()	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(Class)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
getTrace(String)	com.sun.idm.logging.trace.TraceManager#getTrace(String)
level1(Class,String)	com.sun.idm.logging.trace.Trace#level1(String)
level1(Object,String)	com.sun.idm.logging.trace.Trace#level1(String)
level2(Class,String)	com.sun.idm.logging.trace.Trace#level2(String)
level2(Object,String)	com.sun.idm.logging.trace.Trace#level2(String)
level3(Class,String)	com.sun.idm.logging.trace.Trace#level3(String)
level3(Object,String)	com.sun.idm.logging.trace.Trace#level3(String)

Méthode désapprouvée	Substitut
level4(Class,String)	com.sun.idm.logging.trace.Trace#level4(String)
level4(Object,String)	com.sun.idm.logging.trace.Trace#level4(String)
variable(long,Object,String,String,boolean)	com.sun.idm.logging.trace.Trace#variable(long,String,String,boolean)
variable(long,Object,String,String,int)	com.sun.idm.logging.trace.Trace#variable(long,String,String,int)
variable(long,Object,String,String,long)	com.sun.idm.logging.trace.Trace#variable(long,String,String,long)
variable(long,Object,String,String,Object)	com.sun.idm.logging.trace.Trace#variable(long,String,String,Object)
void info(long,Object,String,String)	com.sun.idm.logging.trace.Trace#info(long,String,String)

com.waveset.util.Util

Méthode ou champ désapprouvé(e)	Substitut
DATE_FORMAT_CANONICAL	stringToDate(String,String) getCanonicalDate(Date) getCanonicalDate(Date,TimeZone) getCanonicalDate(long)
debug(Object)	
getCanonicalDateFormat()	stringToDate(String,String) getCanonicalDate(Date) getCanonicalDate(Date,TimeZone) getCanonicalDate(long)
getOldCanonicalDateString(Date,boolean)	getCanonicalDateString(Date)
rfc2396URLPieceEncode(String,String)	com.waveset.util.RFC2396URLPieceEncode#encode(String,String)
rfc2396URLPieceEncode(String)	com.waveset.util.RFC2396URLPieceEncode#encode(String)

com.waveset.workflow.WorkflowContext

Champ désapprouvé	Substitut
VAR_CASE_TERMINATED	com.waveset.object.WFProcess#VAR_CASE_TERMINATED