

Sun Java™ System Identity Synchronization pour Windows Notes de version

Version 1 2004Q3

Référence 817-7852

Ces notes de mise à jour contiennent des informations importantes disponibles au moment de la mise sur le marché de Sun Java™ System Identity Synchronization pour Windows 1 2004Q3. Vous y trouverez des renseignements sur les nouvelles fonctions, les améliorations, les restrictions et problèmes connus, les notes techniques, etc. Prenez connaissance de ce document avant de commencer à utiliser Sun Java System Identity Synchronization pour Windows 1 2004Q3 (Identity Synchronization pour Windows).

Ces notes de mise à jour comprennent les sections suivantes :

- [Historique des mises à jour](#)
- [À propos d' Identity Synchronization pour Windows 1 2004Q3](#)
- [Bogues résolus dans la présente version](#)
- [Informations importantes](#)
- [Problèmes connus et restrictions](#)
- [Fichiers redistribuables](#)
- [Comment signaler des problèmes et apporter des commentaires](#)
- [Ressources Sun supplémentaires](#)

Des adresses URL de sites tiers, qui renvoient à des informations complémentaires connexes, sont référencées dans ce document.

REMARQUE Sun décline toute responsabilité quant à la disponibilité des sites tiers mentionnés. Sun ne garantit pas le contenu, la publicité, les produits et autres matériaux disponibles sur ces sites ou dans ces ressources, ou accessibles par leur intermédiaire, et ne saurait en être tenu pour responsable. Par ailleurs, la responsabilité de Sun ne saurait être engagée en cas de dommages ou de pertes, réels ou supposés, occasionnés par, ou liés à, l'utilisation du contenu, des produits ou des services disponibles sur ces sites ou dans ces ressources, ou accessibles par leur biais, ou encore à la confiance qui a pu leur être accordée.

Historique des mises à jour

Tableau 1 Historique des mises à jour

Date	Description des modifications
30 septembre 2004	Version initiale des Notes de version.

À propos d' Identity Synchronization pour Windows 1 2004Q3

Identity Synchronization pour Windows assure une synchronisation bidirectionnelle des mots de passe entre les annuaires suivants :

- Sun Java™ System Directory Server et Microsoft Windows 2000/2003 Active Directory ;
- Sun Java System Directory Server et Windows NT SAM Registry.

Lors de la synchronisation de Sun Java System Directory Server (serveur d'annuaires) et de Windows 2000/2003 Active Directory, vous pouvez installer et exécuter tous les composants Identity Synchronization pour Windows dans les environnements des systèmes d'exploitation Solaris™ et Windows 2000 Server. Par contre, lors de la synchronisation entre Directory Server et Windows NT, vous devez exécuter les composants Windows NT dans l'environnement Windows NT.

Cette section inclut :

- Les [Nouveautés de cette version](#)
- Les [Configurations matérielles et logicielles requises](#)

Nouveautés de cette version

Nouvelles fonctionnalités

Identity Synchronization pour Windows 1 2004Q3 offre notamment les nouvelles fonctionnalités suivantes :

- **Suppression d'entrées utilisateur** : vous pouvez configurer et activer la synchronisation bidirectionnelle des suppressions d'entrées utilisateur entre Sun Java System Directory Server et Active Directory.
- **Basculement d'Active Directory** : cette fonctionnalité permet de spécifier des serveurs Active Directory supplémentaires pour le basculement pendant l'authentification sur demande. Le plug-in Identity Synchronization pour Windows de Directory Server utilise cette fonctionnalité pour authentifier les utilisateurs auprès d'Active Directory lorsque leur mot de passe a été modifié dans Active Directory. Dans la version 1.0, lorsque le serveur Active Directory principal était indisponible, l'authentification d'intercommunication auprès d'Active Directory à partir du plug-in Identity Synchronization pour Windows de Directory Server échouait et l'utilisateur ne pouvait pas s'authentifier auprès de Directory Server. Cette condition se produisait uniquement à la première tentative d'authentification auprès de Directory Server après la modification du mot de passe utilisateur correspondant sur Active Directory.
- **Classes d'objets utilisateur pour Active Directory** : vous pouvez utiliser n'importe quelle classe d'objets appropriée (Utilisateur ou une extension) pour les informations du schéma Active Directory. (Dans la version 1.0, vous ne pouviez utiliser que la classe d'objets Utilisateur.)
- **Prise en charge de Windows Server 2003 Active Directory** : vous pouvez désormais installer et configurer Identity Synchronization pour Windows 1 2004Q3, et synchroniser les mots de passe et les attributs avec l'Active Directory exécuté sur une plate-forme Windows Server 2003, Standard ou Enterprise Edition.
- **Prise en charge de classes d'objets supplémentaires pour la synchronisation utilisateur** : vous pouvez définir des mappages pour les attributs qui figurent dans les classes d'objets auxiliaires et structurelles. Dans Active Directory, les classes auxiliaires définies sont limitées par les classes d'objets principales/structurelles choisies. Dans Directory Server, vous pouvez utiliser n'importe quelle classe d'objets.
- **Migration** : permet de migrer de la version 1.0 ou 1.0 SP1 vers la version 1 2004Q3.
- **Prise en charge de la plate-forme Solaris 9 x86** : Identity Synchronization pour Windows prend totalement en charge la plate-forme Solaris 9 x86.

- **Fonctionnement de la ligne de commande linkusers et resync** : Les fonctionnalités de la commande linkusers sont désormais fusionnées avec la commande resync. La ligne de commande resync s'enrichit par conséquent de trois options. Les commandes sont les suivantes :
 - `-f <linkusers.cfg>` -- le fichier de liaison (utilisé auparavant dans la commande linkusers) ;
 - `-k` -- lier uniquement les utilisateurs ;
 - `-i NEW_LINKED_USERS` -- réinitialisation du mot de passe des utilisateurs récemment liés. Cette commande est identique aux commandes ALL_USERS et NEW_USERS, excepté pour les utilisateurs qui sont liés sur Directory Server.

Pour plus d'informations sur cette nouvelle fonctionnalité, reportez-vous au manuel *Identity Synchronization for Windows Installation and Configuration Guide*.

REMARQUE Microsoft ayant planifié la fin de vie de Windows NT pour décembre 2004, Identity Synchronization pour Windows 1 2004Q3 corrigera les bogues associés à ce système d'exploitation mais ne prendra pas en charge les nouvelles fonctionnalités pour cette plate-forme.

Pour plus d'informations, reportez-vous à la page Windows Life Cycle Support à l'adresse suivante :

[http://support.microsoft.com/default.aspx?scid=fh;\[ln\];LifeWin](http://support.microsoft.com/default.aspx?scid=fh;[ln];LifeWin)

Modifications apportées au produit

Les modifications apportées au produit pour la version 1 2004Q3 sont les suivantes :

- **Installation** : comme Sun Java Enterprise System 2 2004Q2 installe Sun Java System Message Queue Enterprise Edition et Sun Java System Directory Server (tous deux étant nécessaires pour Identity Synchronization pour Windows 1 2004Q3), vous devez installer Sun Java Enterprise System sur vos systèmes Solaris avant d'installer Identity Synchronization pour Windows 1 2004Q3.

Jusqu'ici, Identity Synchronization pour Windows version 1.0 installait Sun Java System Message Queue 3.0.1 (file d'attente des messages), ce qui n'est pas le cas avec la version 1 2004Q3.
- **Changement de nom des produits et de la documentation** : le produit *Sun ONE* Identity Synchronization pour Windows (et sa documentation) s'appelle désormais *Sun Java System Identity Synchronization pour Windows*.

Améliorations des performances

Les performances de la synchronisation ont été considérablement améliorées.

Modifications apportées à la documentation

Changement de nom des produits et de la documentation : le produit *Sun ONE Identity Synchronization pour Windows* (et sa documentation) s'appelle désormais *Sun Java System Identity Synchronization pour Windows*.

Configurations matérielles et logicielles requises

Configuration requise du système d'exploitation

Les tableaux suivants présentent la configuration requise du système d'exploitation de cette version d'Identity Synchronization pour Windows :

Tableau 2 Configuration requise pour Solaris

Composant	Configuration requise pour Solaris
Composants principaux	Solaris 8™ pour UltraSPARC® (32 et 64 bits) Solaris 9™ édition pour plate-forme SPARC® (32 et 64 bits)Système d'exploitation Solaris 9™ (édition pour plate-forme x86 pour Pentium II ou ultérieur) IA-32
Connecteurs pour Sun Java™ System Directory Server et Windows Active Directory	Solaris 8 pour UltraSPARC (32 et 64 bits) Solaris 9 pour plates-formes SPARC (32 et 64 bits)Système d'exploitation Solaris 9™ (édition pour plate-forme x86 pour Pentium II ou ultérieur) IA-32
Plug-in Sun Java™ System Directory Server	Solaris 8 pour UltraSPARC (32 et 64 bits) Solaris 9 pour plates-formes SPARC (32 et 64 bits)Système d'exploitation Solaris 9™ (édition pour plate-forme x86 pour Pentium II ou ultérieur) IA-32

Tableau 3 Configuration requise pour Windows

Composant	Configuration requise pour Windows
Noyau	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows Server 2003, Standard ou Enterprise Edition
Connecteurs pour Sun Java™ System Directory Server et Windows Active Directory	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4 Windows Server 2003, Standard ou Enterprise Edition
Plug-in Sun Java™ System Directory Server	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4 Windows Server 2003, Standard ou Enterprise Edition
Connecteurs et plug-ins NT (sous-composants)	Contrôleur de domaine principal Windows NT 4.0 Server SP 6A (pour x86 seulement)
Pour effectuer une synchronisation avec Active Directory sur Windows Server 2003, Standard et Enterprise Edition	Windows Server 2003 Standard Edition (avec les dernières mises à jour de sécurité) Windows Server 2003 Enterprise Edition (avec les dernières mises à jour de sécurité)

Configuration matérielle requise

Pour exécuter Identity Synchronization pour Windows, le matériel (quelle que soit la plate-forme) doit avoir la configuration minimale suivante :

- environ 400 Mo d’espace disque pour une installation minimale ;
- un minimum de 512 Mo de RAM pour les serveurs exécutant un composant Identity Synchronization pour Windows (1 Go de RAM de préférence).

Sun Java SystemConfiguration logicielle requise

Pour exécuter Identity Synchronization pour Windows, vous devez installer les composants logiciels Sun Java System suivants :

- Sun Java System Message Queue Enterprise Edition version 3.5 SP 1 (anciennement Sun ONE Message Queue)

Vous devez installer Message Queue Enterprise Edition version 3.5 SP 1 avant d’installer Identity Synchronization pour Windows. Il est également recommandé d’installer Message Queue Enterprise Edition version 3.5 SP 1 avant d’installer Sun Java System Directory Server 5 2004Q2.

Pour installer le noyau Identity Synchronization pour Windows sur une installation Sun Java System Message Queue *existante*, vous devez utiliser Message Queue Enterprise Edition 3.5 SP1. Si vous installez le noyau Identity Synchronization pour Windows sur une version incorrecte de Message Queue, la synchronisation échoue.

- Sun Java System Directory Server version 5 2004Q2 ou ultérieure

Pour installer Identity Synchronization pour Windows 1 2004Q3, vous devez exécuter Directory Server 5 2004Q2 (5.2 Patch 2).

Pour obtenir plus d'informations concernant l'installation du package Solaris ou les patches à appliquer, reportez-vous à la section [Informations importantes](#) du manuel [Notes de version de Sun Java System Directory Server 5 2004Q2](#).

Pour obtenir plus d'informations concernant l'installation d'une archive compressée (ZIP), l'application d'un patch et les bogues connus de la mise à niveau du fichier zip, reportez-vous aux [Notes relatives à l'installation](#) du manuel [Notes de version de Sun One Directory Server 5.2](#).

Pour obtenir une liste des bogues résolus par Directory Server 5.2 Patch 2, consultez les fichiers Lisezmoi des patches appliqués ou, pour les corrections de bogues importantes : [Notes de version de Sun Java System Directory Server 5 2004Q2](#).

Vous devez installer un plug-in Directory Server (sous-composant) sur chaque Directory Server déployé, qu'il soit maître, réplique ou hub.

Pour obtenir les dernières informations concernant les patches nécessaires à l'installation de Directory Server 5 2004Q2 sur Solaris, reportez-vous aux manuels *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* et *Sun Java System Directory Server 5 2004Q2 Release Notes*, que vous trouverez sur le site Web suivant :

http://docs.sun.com/db/coll/DirectoryServer_04q2

- Patch du journal des modifications rétroactif de Sun Java System Directory Server 5 2004Q2

Pour corriger un problème relatif aux fonctionnalités de journal des modifications rétroactif de Directory Server et de suppression dans Identity Synchronization pour Windows 1 2004Q2, un patch doit être installé sur Sun Java System Directory Server 5 2004Q2. Les numéros de patch, selon votre environnement, sont les suivants :

- Pour le format de package Solaris SPARC : numéro de patch 117907-02 ou supérieur
- Pour les installations d'archives compressées Solaris SPARC : patch 5077789
- Pour le format de package Solaris x86 : numéro de patch 117908-02 ou supérieur
- Pour les installations d'archives compressées Solaris x86 : patch 5077789
- Pour les installations d'archives compressées Windows : patch 5077789

Pour plus d'informations sur ces patches et sur la façon de les mettre à jour dans l'environnement Directory Server, reportez-vous au fichier `README.patch` situé dans le répertoire de téléchargement d'Identity Synchronization pour Windows : `<racine_téléchargement>/patches/directory/README.patch`

- Java Runtime Environment

J2SE Java Runtime Environment (JRE) n'est pas fourni avec ce produit.

- Pour exécuter le programme d'installation d'Identity Synchronization pour Windows sur Solaris ou Windows Active Directory, vous devez installer JRE 1.4.2_04 (ou ultérieur) . Vous pouvez également installer J2SE version 1.4.2_04 SDK, dont les performances sont supérieures à celles de JRE.
- Sur Windows NT, vous devez installer JRE 1.4.1_03 (ou ultérieur).

Par ailleurs, sous Solaris, vous devez attribuer la valeur 1.4.2_04 JRE (ou ultérieur) à `JAVA_HOME` avant d'installer Identity Synchronization pour Windows ou bien le programme d'installation risque d'indiquer que `JAVA_HOME` n'est pas défini.

Bogues résolus dans la présente version

Le tableau suivant présente les bogues résolus dans Identity Synchronization pour Windows 1 2004Q3 :

Tableau 4 Bogues résolus dans Identity Synchronization pour Windows 1 2004Q3

Référence	Description
Installation/Désinstallation	
4881466	L'installation des composants principaux avec une instance Message Queue existante sur un port autre que 7676 échouait.
4829497	Le programme de désinstallation ne supprimait pas tous les fichiers et dossiers.
4820869	Sur Windows, il fallait relancer le système avant de réinstaller les composants principaux.
4916789	Des ID de plug-in Directory Server en double étaient générés pour les répliques installées sur la racine du serveur.
5035406	L'installation du noyau échouait sur les machines sous Solaris lorsque JRE était utilisé à la place de JDK.
4880807	<code>runInstaller.sh</code> et <code>runUninstaller.sh</code> ne prenaient pas en charge une option <code>-nodisplay</code> .

Tableau 4 Bogues résolus dans Identity Synchronization pour Windows 1 2004Q3 (*Suite*)

Référence	Description
5030928	Le programme d'installation ne prenait pas en charge différentes informations d'authentification pour les hôtes primaires et de basculement.
5037157	Le script de désinstallation n'existait pas après une installation du plug-in DS seulement.
5050554	Le démarrage du programme d'installation en mode « -nodisplay » exigeait un DISPLAY fiable.
4915192	L'installation du connecteur sur un serveur Directory Server uniquement SSL était impossible.
5052509	Le script de désinstallation en mode texte ne supprimait pas tous les packages associés à Identity Synchronization.
4937341	La désinstallation d'Identity Synchronization pour Windows à l'aide de l'option Ajout/Suppression de programmes sur les systèmes Windows ne fonctionnait pas.
5056685	Le programme de désinstallation des plug-ins NT ne supprimait pas la DLL de filtre de mot de passe (procédure requise pour que Windows ne charge pas la DLL au démarrage). Ce bogue provoquait des problèmes au cours de la réinstallation du composant.
4988901	Certains panneaux du programme d'installation ne s'affichaient pas correctement lorsque l'utilisateur cliquait sur le bouton « Précédent ».
5030567	Pendant l'installation du connecteur NT, le programme d'installation n'indiquait pas clairement que tous les sous-composants du connecteur NT étaient déjà installés.
5036330	Si la valeur par défaut du champ vous invitant à saisir un nom descriptif unique pour le domaine d'administration était modifiée pendant l'installation, la procédure échouait.
5041518	Le panneau de port du connecteur s'affichait par erreur lorsque l'utilisateur cliquait sur le bouton Précédent pendant l'installation des sous-composants.
5048953/ 5049733	Si la valeur JAVA_HOME contenait des guillemets, la désinstallation échouait.
5050691	Pendant l'installation du noyau, la fenêtre de configuration de Message Queue affichait un message incorrect concernant la version de Message Queue installée sur le système. Elle affichait la valeur « null ».
5057716	Même si le plug-in Directory Server était désinstallé, ni le package du plug-in ni ses entrées de registre n'étaient supprimés du système.
5071574	Le numéro de port valide (65535) n'était pas accepté pour le connecteur Directory Server.
5079602	L'entrée nt_dll_registrar ne forçait pas la clé de registre « Notification Packages » sur REG_MULTI_SZ.

Synchronisation des mots de passe

4845844	La commande <code>Idsync resync</code> ne pouvait pas créer d'utilisateurs sur NT à partir de Directory Server lors de la synchronisation.
4937502	Les connecteurs peuvent arrêter la synchronisation après une perte fréquente de connectivité du réseau.

Tableau 4 Bogues résolus dans Identity Synchronization pour Windows 1 2004Q3 (*Suite*)

Référence	Description
4939825	Le connecteur Directory Server ne supprimait pas l'attribut de détection de boucle pour les entrées modifiées.
4906752	Une création d'utilisateurs, suivie rapidement d'une opération modrdn sur Sun Directory Server, n'était pas synchronisée.
4933861	Le connecteur NT présentait une activité excessive lorsque la synchronisation démarrait après une opération « idsync resync -c -o Sun » et que des attributs synthétiques étaient utilisés.
4941200	Les entrées utilisateur renommées n'étaient pas synchronisées lorsque seule la casse était modifiée.
4893525	Les modifications d'attributs étaient perdues à la fermeture de la connexion réseau avec le serveur Active Directory.
5019327	Le connecteur Directory Server synchronise les utilisateurs avec la classe d'objets définie par rapport à la sous-classe du type de classe d'objets synchronisée.
4995351	Identity Synchronization pour Windows mappait un attribut incorrect.
5036025	Une modification des SUL, suivie d'une tentative de synchronisation des utilisateurs, entraînait une erreur NullPointerException (indiquée dans les fichiers journaux) et le connecteur cessait de répondre.
5054654	Les modifications de mot de passe sur NT étaient perdues en cas de réinitialisation ou d'arrêt inopiné du connecteur.

Sun Java System Message Queue

4881240	Sous Solaris, il était impossible d'utiliser une instance Message Queue existante lorsqu'elle était installée dans un répertoire utilisateur.
---------	-----------------------------------------------------------------------------------------------------------------------------------------------

Problèmes généraux

4943564 / 4939730	<i>Userpassword</i> n'était pas un attribut facultatif.
4994145	Le plug-in Directory Server testait trop fréquemment la connexion à des hôtes non disponibles.
5041435	La mise à jour sur demande des mots de passe empêchait Directory Server de répondre lorsque l'option « Password History » était activée.
4939859	Idsync linkusers/resync ignorait l'option de filtrage LDAP lorsque le connecteur source était Windows NT.
4987742	<i>resync</i> ne traitait pas toutes les entrées en raison d'une condition d'indétermination.
5048362	Des caractères de saut de ligne des messages journalisés n'étaient pas automatiquement supprimés.
4925575	Le programme d'installation du connecteur Active Directory ne vérifiait pas si le domaine correspondait au domaine de certification.
4901486	Auparavant, plusieurs forêts Active Directory n'étaient pas prises en charge par Identity Synchronization pour Windows 1 2004Q3.

Tableau 4 Bogues résolus dans Identity Synchronization pour Windows 1 2004Q3 (*Suite*)

Référence	Description
Problèmes généraux de la console	
5040094	« objectclass=<some oc> » indiquait une erreur de filtre incorrecte.
5030704	L'intervalle <code>resync</code> de la source Active Directory ne pouvait pas être modifié à partir de la console.
5026929	La valeur par défaut des attributs de création obligatoires ne pouvait pas être modifiée.
4941238	Le visionneur de journal n'analysait pas correctement l'enregistrement de journal.
5008697	La modification du mappage <code>cn</code> ajoutait un élément à la liste au lieu de mettre à jour l'élément existant.
50134407	Une source d'annuaires pouvait être créée avec le même nom qu'une source existante. Aucun message d'erreur ne s'affichait et la source d'annuaires ne pouvait pas être supprimée.
5026198	Des erreurs typographiques ont été corrigées dans la fenêtre Journal de la console.
5044529	La commande <code>prepds</code> de la console ne fonctionnait pas pour Directory Server en mode SSL uniquement.
5045350	Lorsqu'un attribut de création était modifié, sa valeur ne pouvait pas être définie sur <code><aucun></code> .
4921889	Lorsque l'option d'affichage de l'arborescence était de nouveau sélectionnée, la console ne retournait pas à la vue normale de l'arborescence.
Connecteur	
4988028	RTE (exception d'exécution) Java sur un attribut non modifié manquant.
Utilitaires de lignes de commande	
5015766	La transmission d'un mot de passe vide à <code>idsync changepw</code> rend impossible par la suite l'accès au registre de configuration.
4986303	L'interface de ligne de commande n'attribuait pas de valeur par défaut aux options <code>-h</code> , <code>-p</code> , <code>-D</code> et <code>-s</code> .
5038195	<code>resetconn</code> ne prévoyait pas de message d'erreur approprié lorsque le suffixe de configuration était incorrect.
5019543	<code>printstat</code> ne prévoyait pas de message d'erreur approprié lorsque le suffixe de configuration était incorrect.
5024148	<code>resetconn</code> ne supprimait pas les informations d'authentification de Message Queue du connecteur.
4941125	<code>resync</code> mettait à jour les utilisateurs synchronisés lorsque la source était Sun et que les attributs synthétiques étaient synchronisés.
4939484	Il était parfois impossible de quitter la commande <code>linkusers</code> .
5015575	L'opération de ligne de commande ne s'arrêtait pas malgré l'exécution de la commande « <code>c</code> » à l'invite de commande.
5062028	L'invite de ligne de commande cessait de répondre lorsque le noyau était installé avec SSL (la valeur de port par défaut sur la ligne de commande était le port SSL).

Informations importantes

Cette section comprend les dernières informations qui n'ont pas pu être incluses dans la documentation de base des produits. Elle aborde les sujets suivants :

- [Notes relatives à l'installation](#)
- [Problèmes de compatibilité](#)
- [Récupération de données en cas de panne du système ou d'application](#)
- [Mises à jour de la documentation d'Identity Synchronization pour Windows 1 2004Q3](#)
- [Exécution d'Identity Synchronization pour Windows dans un environnement protégé par un pare-feu](#)

Notes relatives à l'installation

Avant d'installer Identity Synchronization pour Windows 1 2004Q3, assurez-vous d'avoir lu le chapitre « Preparing for Installation » du manuel *Sun Java™ System Identity Synchronization pour Windows 1 2004Q3 Installation and Configuration Guide*.

Utilisation de Windows Server 2003

- Vous pouvez désormais utiliser Windows Server 2003, Standard ou Enterprise Edition comme plate-forme pour installer et configurer Identity Synchronization pour Windows 1 2004Q3.
- Sous Windows Server 2003, contrairement à Windows 2000, la stratégie par défaut pour les mots de passe impose des mots de passe stricts.

Problèmes relatifs à Windows Server 2003

La fonction obligeant l'utilisateur à modifier son mot de passe à la prochaine connexion diffère sous Windows Server 2003 et sous Windows 2000 (4997513).

Sous Windows 2003, l'indicateur L'utilisateur doit changer de mot de passe à la prochaine ouverture de session est à « 1 » par défaut, ce qui n'est pas le cas sous Windows 2000.

Lorsque vous créez des utilisateurs sous Windows 2000/2003 avec l'indicateur « L'utilisateur doit changer de mot de passe à la prochaine ouverture de session » à « 1 », sur Directory Server les utilisateurs sont créés sans mot de passe. A la prochaine connexion à Active Directory, les utilisateurs sont contraints de modifier leur mot de passe, ce qui invalide leur mot de passe sur Directory Server et force une synchronisation sur demande la prochaine fois qu'ils s'authentifient auprès de Directory Server.

Les utilisateurs ne peuvent pas s'authentifier auprès de Directory Server tant qu'ils n'ont pas modifié leur mot de passe sur Active Directory.

Problèmes de compatibilité

Problèmes de compatibilité lors de l'utilisation de certains produits de la console distante pour accéder à la console Identity Synchronization pour Windows (5077227)

Des problèmes peuvent se produire si vous essayez d'afficher la console Identity Synchronization pour Windows à l'aide de PCAnywhere 10.x ou Remote Administration 2.1 (cependant, PCAnywhere 9.2 ne provoque pas d'erreurs). Si les problèmes persistent, supprimez le logiciel d'administration distante. Vous pouvez également utiliser VNC. Aucun problème d'affichage de la console Identity Synchronization pour Windows n'a été signalé avec cet outil.

Récupération de données en cas de panne du système ou d'application

En cas de panne matérielle ou logicielle, il peut être nécessaire de restaurer les données à partir d'une copie de sauvegarde dans certaines sources d'annuaires synchronisées.

Après la récupération des données proprement dit, une procédure supplémentaire est nécessaire pour garantir l'exécution correcte de la synchronisation.

En général, les connecteurs conservent les informations sur la dernière modification propagée à la file d'attente des messages.

Ces données, qui désignent l'état des connecteurs, permettent de déterminer la modification suivante que le connecteur doit lire à partir de sa source d'annuaires. Si la base de données d'une source d'annuaires synchronisée est restaurée à partir d'une sauvegarde, l'état des connecteurs risque de ne plus être valide.

Les connecteurs Windows (Active Directory ou Windows NT) gèrent également une base de données interne. Cette base de données est une copie de la source de données synchronisée et permet d'identifier les modifications dans la source de données connectée. La base de données interne n'est naturellement plus valide lorsque la source Active Directory connectée ou que le système Windows NT sont restaurés à partir d'une copie de sauvegarde.

En général, la commande `idsync resync` peut être utilisée pour renseigner de nouveau la source de données récupérée.

REMARQUE La resynchronisation ne peut pas être utilisée pour synchroniser des mots de passe à une exception près. L'option `-i ALL_USERS` permet d'invalidier des mots de passe dans des systèmes Sun Java System Directory Server si la source de données de resynchronisation est Windows (et si la liste SUL comprend uniquement des systèmes Active Directory).

L'utilisation de la commande `idsync resync` ne constitue cependant peut-être pas une solution acceptable dans tous les cas.

ATTENTION Avant d'exécuter l'une des étapes détaillées ci-dessous, vérifiez que la synchronisation est arrêtée.

Synchronisation bidirectionnelle

La procédure recommandée est d'utiliser la commande `idsync resync` avec les paramètres de modificateur appropriés (conformément aux paramètres de synchronisation). La cible de l'opération de resynchronisation doit être la source d'annuaires récupérée.

Synchronisation unidirectionnelle

Si la source de données récupérée est la destination d'une synchronisation, vous pouvez suivre la même procédure que pour la synchronisation bidirectionnelle.

Si la source de données récupérée est une source de synchronisation, la commande `idsync resync` peut être utilisée pour renseigner de nouveau la source d'annuaires récupérée. Il n'est pas nécessaire de modifier les paramètres de flux de synchronisation dans la configuration d'Identity Synchronization pour Windows. La commande `idsync resync` permet de définir le flux de synchronisation indépendamment des flux configurés à l'aide de l'option `-o <Windows|Sun>`.

Considérez l'exemple de scénario suivant :

Une synchronisation bidirectionnelle est configurée entre un serveur Sun Java System Directory Server et Active Directory

- La base de données d'un serveur Microsoft Active Directory doit être récupérée à partir d'une sauvegarde.
 - Dans Identity Synchronization pour Windows, cette source Active Directory est configurée pour la liste d'utilisateurs de synchronisation « AD ».
 - Une synchronisation bidirectionnelle est configurée pour les modifications, les créations et les suppressions entre cette source Active Directory et une source Sun Directory Server.
1. Arrêtez la synchronisation : `idsync stopsync -w - -q -`
 2. Resynchronisez la source Active Directory, ainsi que les modifications, les créations et les suppressions : `idsync resync -c -x -o Sun -l AD -w - -q -`
 3. Redémarrez la synchronisation : `idsync startsync -w - -q --`

Procédures de récupération propres aux différentes sources d'annuaires

Microsoft Active Directory

Si Active Directory peut être restauré à partir d'une sauvegarde, suivez les procédures décrites dans les sections Synchronisation bidirectionnelle ou Synchronisation unidirectionnelle.

Vous devrez cependant peut-être utiliser un autre contrôleur de domaine après une erreur critique. Le cas échéant, exécutez la procédure suivante pour mettre à jour la configuration du connecteur Active Directory :

1. Démarrez la console de gestion Identity Synchronization pour Windows.
2. Sélectionnez l'onglet Configuration.
3. Développez le nœud Sources d'annuaires.
4. Sélectionnez la source Active Directory appropriée.
5. Cliquez sur Modifier le contrôleur...
6. Sélectionnez le nouveau contrôleur de domaine.

Il est recommandé de faire du contrôleur de domaine sélectionné le propriétaire du rôle NT PDC FSMO du domaine

7. Enregistrez la configuration.
8. Arrêtez le service Identity Synchronization sur l'hôte sur lequel s'exécute le connecteur Active Directory.

9. Supprimez tous les fichiers (mais pas les répertoires) sous `<racineserveur>/isw-<nomhôte>/persist/ADPxxx`, où xxx représente la partie numérique de l'identificateur du connecteur Active Directory (par exemple, 100 si l'identificateur du connecteur Active Directory est CNN100).
10. Démarrez le service Identity Synchronization sur l'hôte sur lequel s'exécute le connecteur Active Directory.
11. Suivez la procédure des sections Synchronisation unidirectionnelle ou Synchronisation bidirectionnelle, selon votre flux de synchronisation.

Sun Java System Directory Server

La base de données du journal des modifications rétroactif ou la base de données des utilisateurs synchronisés (ou les deux) peuvent être affectées par une erreur critique.

1. Base de données du journal des modifications rétroactif.

La base de données du journal des modifications rétroactif peut contenir des modifications que le connecteur Directory Server n'a pas pu traiter. La restauration de cette base de données n'a d'intérêt que si la copie de sauvegarde contient des modifications non traitées. Pour le savoir, comparez la dernière entrée du fichier

`<racineserveur>/isw-<nomhôte>/ADPxxx/accessor.state` avec le dernier numéro de modification dans la copie de sauvegarde. Si la valeur dans le fichier `accessor.state` est supérieure ou égale au numéro de modification, il n'est pas nécessaire de restaurer la base de données, mais vous devez la recréer.

Une fois la base de données du journal des modifications rétroactif recréée, n'oubliez pas d'exécuter la commande `idsync prepds` ou de cliquer sur Préparer Directory Server dans la fenêtre Source d'annuaires Sun de la console de gestion d'Identity Synchronization pour Windows.

Le connecteur Directory Server détecte la création de la base de données du journal des modifications rétroactif et consigne un message d'avertissement. Vous pouvez ignorer ce message sans risque.

2. Base de données synchronisée.

Si aucune sauvegarde de la base de données synchronisée n'est disponible, le connecteur Directory Server doit être réinstallé.

Si la base de données synchronisée peut être restaurée à partir d'une copie de sauvegarde, suivez les procédures décrites dans les sections Synchronisation bidirectionnelle ou Synchronisation unidirectionnelle.

Mises à jour de la documentation d'Identity Synchronization pour Windows 1 2004Q3

Vous pouvez accéder à la documentation en ligne d'Identity Synchronization pour Windows à l'aide d'un navigateur. En outre, vous pouvez télécharger l'ensemble de la documentation au format HTML.

Après avoir téléchargé ce fichier, extrayez-le à l'emplacement suivant:

```
<RacineServeur>/manual/fr/isw
```

La racine du serveur est l'emplacement du serveur d'administration Sun Java System. Le chemin d'accès de la racine du serveur dépend de la plate-forme, de l'installation et de la configuration. Le répertoire RacineServeur contient le programme `startconsole`.

Vous pouvez ensuite accéder à l'ensemble de la documentation directement à partir de l'adresse `<RacineServeur>/manual/fr/isw/index.html` ou de la console du serveur en sélectionnant Accueil documentation dans le menu Aide.

Exécution d'Identity Synchronization pour Windows dans un environnement protégé par un pare-feu

Vous pouvez exécuter Identity Synchronization pour Windows dans un environnement protégé par un pare-feu. Cette section décrit les ports du serveur qui doivent être visibles au travers du pare-feu :

- [Configuration requise pour Message Queue](#)
- [Configuration requise pour le programme d'installation](#)
- [Configuration requise pour les composants principaux](#)
- [Configuration requise pour la console](#)
- [Configuration requise pour les connecteurs](#)
- [Configuration requise pour le plug-in Directory Server](#)

Configuration requise pour Message Queue

Par défaut, Message Queue utilise des ports dynamiques pour tous les services à l'exception de son mappeur de ports. Pour accéder au courtier Message Queue malgré la présence d'un pare-feu, le courtier doit utiliser des ports fixes pour tous les services.

Après avoir installé le noyau, vous devez définir les propriétés de configuration du courtier `imq.<nom_service>.<type_protocole>.port`. En particulier, vous devez définir l'option `imq.ssljms.tls.port`. Pour plus d'informations, reportez-vous au manuel *Sun Java™ System Message Queue Administrator's Guide*.

Configuration requise pour le programme d'installation

Le programme d'installation d'Identity Synchronization pour Windows doit pouvoir communiquer avec le serveur Directory Server faisant office d'annuaire de configuration.

- Si vous installez un connecteur Active Directory, le programme d'installation doit pouvoir joindre le port LDAP (port 389) d'Active Directory.
- Si vous installez un connecteur Directory Server ou un plug-in Directory Server (sous-composant), le programme d'installation doit pouvoir joindre le port LDAP (port 389 par défaut) de Directory Server.

Configuration requise pour les composants principaux

Message Queue, le gestionnaire système et l'interface de ligne de commande doivent pouvoir joindre le serveur d'annuaires sur lequel est stockée la configuration d'Identity Synchronization pour Windows.

Configuration requise pour la console

La console Identity Synchronization pour Windows doit pouvoir joindre les composants suivants :

- Active Directory sur LDAP (port 389) ou LDAPS (port 636) ;
- le catalogue global Active Directory sur LDAP (port 3268) ou LDAPS (port 3269) ;
- chacun des serveurs d'annuaires sur LDAP ou LDAPS ;
- Sun Java System Administration Server ;
- Message Queue.

Configuration requise pour les connecteurs

Tous les connecteurs doivent pouvoir communiquer avec Message Queue. En outre :

- Le connecteur Active Directory doit pouvoir accéder au contrôleur de domaine Active Directory via LDAP (port 389) ou LDAPS (port 636).
- Le connecteur Directory Server doit pouvoir accéder au(x) serveur(s) d'annuaires via LDAP (port 389 par défaut) ou LDAPS (port 636 par défaut).

Configuration requise pour le plug-in Directory Server

Chaque plug-in Directory Server doit pouvoir joindre le port de serveur du connecteur Directory Server, sélectionné à l'installation du connecteur. Les plug-ins exécutés sur les répliques maîtres de Directory Server doivent pouvoir se connecter au port LDAP (port 389) ou LDAPS (port 636) d'Active Directory. Les plug-ins exécutés sur d'autres répliques de Directory Server doivent pouvoir joindre les ports LDAP ou LDAPS Directory Server du maître.

Problèmes connus et restrictions

Cette section contient une liste des problèmes connus relatifs à Identity Synchronization pour Windows 1 2004Q3. Les domaines suivants du produit sont abordés :

- [Installation et désinstallation](#)
- [Connecteurs et plug-Ins](#)
- [Console et ligne de commande](#)
- [Synchronisation des mots de passe](#)
- [Sun Java System Message Queue](#)
- [Problèmes d'ordre général](#)

Installation et désinstallation

Instructions de nettoyage manuel du registre du produit (5050004)

Si vous devez supprimer des références à Identity Synchronization pour Windows dans le registre du produit, suivez les procédures décrites pour les plates-formes Windows NT et Windows 2000 dans le chapitre 7, section « *What to Do if the 1.0 Uninstallation Fails* » du manuel *Identity Synchronization for Windows Installation and Configuration Guide*.

Les scripts Solaris ne fonctionnent pas si le noyau est installé dans un répertoire dont le nom comporte des espaces (4801643)

Les scripts de ligne de commande Solaris ne fonctionnent pas si vous installez le noyau Identity Synchronization pour Windows dans un répertoire dont le chemin d'accès comporte un espace.

Le courtier Message Queue ne peut pas démarrer si le DN de base contient des espaces (4892332 et 4892490).

L'authentification du courtier Message Queue échoue si vous installez le noyau sur un suffixe contenant des espaces.

Effets secondaires de l'installation du noyau avec une instance Message Queue existante (4882194)

L'installation du noyau avec une instance existante du courtier Message Queue peut compromettre cette instance. Prenons, par exemple, une configuration existante modifiée comme suit :

- Le fichier `/etc/imag/imagbrokerd.conf` a été modifié pour lancer automatiquement le courtier au démarrage, ce qui empêchait à la réinitialisation le lancement d'autres instances du courtier, lancées à partir du script `/etc/init.d/imag`.

Le courtier Message Queue exige un minimum de 512 Mo de mémoire (4819519)

Le courtier Message Queue exige un minimum de 512 Mo de mémoire. Comme le courtier installé fait partie du noyau, la machine sur laquelle le noyau est installé doit avoir un minimum de 1 Go de RAM.

Impossible de désinstaller des plug-ins car l'installation d'une instance de multi-serveur d'annuaires supprime le programme de désinstallation (4916035)

Vous ne pouvez pas désinstaller plusieurs plug-ins si deux instances de Directory Server ont la même racine d'installation dans un système de fichiers (par exemple, `/usr/sunone/servers/slapd-foxhead` et `/usr/sunone/servers/slapd-foxhead2`).

Solution :

1. Ouvrez la console du Directory Server où vous avez installé le plug-in.
2. Cliquez sur l'onglet Configuration.
3. Double-cliquez sur le dossier `Plugins` pour développer l'arborescence des plug-ins.
4. Cliquez sur `pswsync` et décochez la case Activer les plug-ins.
5. Redémarrez Directory Server.

Le comportement du connecteur Active Directory est indéterminé si l'installation en cours est annulée et qu'une nouvelle tentative de réinstallation est effectuée (5038905)

Si vous annulez le programme d'installation pendant la configuration du connecteur, l'option Connecteur n'est plus proposée à l'installation .

Solution

Exécutez la commande `idsync resetconn` à partir de l'invite de ligne de commande pour réinitialiser la configuration du connecteur, puis relancez le programme d'installation pour réinstaller le connecteur. Pour plus d'informations sur l'exécution de la commande `idsync resetconn`, reportez-vous au manuel *Sun Java System Identity Synchronization pour Windows Installation and Configuration Guide*.

Des clés du registre associées au produit ne sont pas supprimées lors de la désinstallation du produit (5045237)

Après la désinstallation du noyau, les nœuds Sun Java System Identity Synchronization pour Windows correspondants dans le fichier registre du produit ne sont pas supprimés. Pour réussir la réinstallation du produit, vous devez supprimer manuellement les nœuds des clés du registre produit. Pour plus d'informations sur la suppression de ces clés de registre du produit, reportez-vous au manuel *Identity Synchronization pour Windows Installation and Configuration Guide*. Cette situation ne se produit que sur Solaris 8.

Des références associées à Identity Synchronization pour Windows s'affichent sur la console lorsque le noyau est désinstallé sans connexion au registre de configuration (5049700)

Un message d'erreur s'affiche lorsque vous démarrez la console après avoir effectué une désinstallation en aveugle (sans connexion au registre de configuration) d'Identity Synchronization pour Windows.

Le répertoire « temp », où les journaux d'installation sont enregistrés, pouvait devenir un dossier caché (5051905)

Le dossier sous `C:\ Documents and Settings > Administrateur > Local Settings` pouvait être un dossier caché sur certains systèmes Windows.

Solution

Pour afficher le dossier `Local Setting` et le sous-dossier `Temp`, vous devez sélectionner l'option de l'Explorateur Windows `Afficher les fichiers et dossiers cachés`. Une autre solution consiste à taper `cd %TEMP` ou `cd %TMP` à l'invite de commande pour afficher les fichiers journaux associés à l'installation dans le répertoire. Vous pouvez afficher les journaux à l'aide du Bloc-notes.

Échec de l'authentification auprès du courtier Message Queue si le suffixe racine contient des espaces (4892903)

La configuration d'Identity Synchronization pour Windows doit être stockée dans le suffixe racine, sans espace, en raison d'une limitation de Message Queue.

Solution

Créez un suffixe racine pour stocker la configuration d'Identity Synchronization pour Windows avant d'installer le noyau.

Après un échec de l'installation du plug-in Directory Server, la liste des tâches indique que l'installation du plug-in est terminée (5081912)

Dans certains cas, la liste des tâches indique que le plug-in Directory Server a été installé bien que son installation ait échoué.

Au cours de la désinstallation d'un connecteur, le programme de désinstallation n'indique pas l'espace disque récupéré avec précision (5081823)

Lors de la désinstallation d'un connecteur, le programme de désinstallation indique de façon incorrecte 0 octets (comme nombre d'octets qui seront récupérés après la désinstallation). Si les propriétés de l'espace disque sont affichées, l'espace disque effectivement récupéré diffère de zéro.

Le programme d'installation ne vous demande pas d'installer les composants dans le même répertoire que celui dans lequel est installé le plug-in Directory Server (5080178)

Si le plug-in Directory Server est le premier composant installé sur une machine, tous les composants installés par la suite sur cette machine doivent l'être dans le même répertoire d'installation. Cependant, le programme d'installation n'impose pas cette condition pendant l'installation.

Le programme de désinstallation peut afficher des informations incorrectes lors de la désinstallation des composants (5079489)

Si un connecteur est désinstallé sur une machine sur laquelle le noyau n'est pas installé, le programme d'installation indique de manière erronée qu'il désinstalle le noyau. Vous pouvez ignorer ce message. Les références à la console Identity Synchronization pour Windows ne sont pas supprimées si une désinstallation est exécutée alors que l'annuaire de configuration n'existe pas (5077156)

Si vous sélectionnez l'option de désinstallation du produit sans annuaire de configuration, la console Sun Server conserve toutes les références à la console Identity Synchronization pour Windows. Après la désinstallation du produit, l'icône correspondant à Identity Synchronization pour Windows existe toujours dans l'arborescence de topologie. Une erreur se produit lorsque vous essayez d'afficher la console. Pour plus d'informations sur la suppression des références à la console, reportez-vous au chapitre 8, section « Uninstalling the Console Manually » du manuel *Identity Synchronization for Windows Installation and Configuration Guide*.

La désinstallation ne supprime pas le répertoire « racine-du-serveur/isw-*/lib » ni les fichiers jar (5038284)

La désinstallation ne supprime pas le répertoire lib, qui contient les fichiers *.jar. Ces fichiers ainsi que le répertoire doivent être supprimés manuellement.

Comportement indéterminé du connecteur Active Directory après annulation de l'installation, puis réinstallation (5038905)

Lors de l'installation du connecteur Active Directory, si l'opération d'installation est annulée inopinément, puis que vous tentez de réinstaller le connecteur, le connecteur Active Directory indique un état « Installé » incorrect. L'état ne change pas et l'opération de synchronisation ne s'effectue pas. Toute réinstallation du connecteur Active Directory échoue.

Solution

Vous devez exécuter la commande `idsync resetconn` pour réinstaller le connecteur. Pour plus d'informations sur l'exécution de la commande `idsync resetconn`, reportez-vous au manuel *Identity Synchronization for Windows Installation and Configuration Guide*.

Échec de l'installation d'Identity Synchronization pour Windows sur Directory Server 5.2p3 installé avec Sun Java Enterprise System 3 (5092530)

Vous ne pouvez pas installer le produit Identity Synchronization pour Windows de base sur Directory Server 5.2 P3 ou supérieur. Identity Synchronization pour Windows 1 2004Q3 ne prendra en charge Sun Java Enterprise System 3 (Directory Server 5.2 P3) que comme source de synchronisation de données.

La liste d'installation vous invite à installer le plug-in Directory Server sur le maître secondaire même après l'installation (5096593)

La liste des tâches est presque toujours exacte, mais il arrive néanmoins qu'elle n'indique pas toutes les étapes requises ou qu'elle ne détecte pas que certaines étapes ont déjà été effectuées. Par exemple, elle n'indique pas toujours quels plug-ins Directory Server ont déjà été installés ou ont besoin de l'être.

Absence de liste ACL lors de l'installation d'Identity Synchronization pour Windows sur un système FAT32 (5097751)

Après avoir installé Identity Synchronization pour Windows sur un disque formaté en FAT32, les ACL n'existent pas au niveau des dossiers et des fichiers. Il est conseillé d'éviter d'installer le logiciel sur des partitions non NTFS.

Échec de la désinstallation du plug-in seul lors de l'utilisation de la version compressée de Directory Server (5101589)

Lorsque vous tentez d'effectuer une désinstallation de plug-in seul, l'opération échoue si vous utilisez le package d'archive compressée de Directory Server.

Échec de l'installation si un nom d'administrateur multioctet est utilisé à l'invite (5109332)

Si vous saisissez un nom d'administrateur LDAP multioctet à l'invite lors de l'installation du noyau, l'opération échoue. Le message d'erreur suivant s'affiche : « Le programme d'installation ne peut pas télécharger le fichier de schéma /var/opt/isw/SUNWisw/misc/40so-psw.out.ldif. Vérifiez le fichier journal du programme d'installation pour plus de détails. » Le processus d'installation s'interrompt et la boîte de dialogue se ferme inopinément.

Solution

Pour éviter ce problème, veillez à utiliser le nom d'administration LDAP par défaut « admin » pour l'installation. En cas d'échec d'une installation précédente, relancez le programme d'installation et réinstallez le noyau en utilisant le nom admin par défaut. Un message peut apparaître, indiquant que des fichiers du noyau ont été trouvés sur la machine. Vous pouvez ignorer ce message et continuer pour terminer l'opération d'installation.

Connecteurs et plug-Ins

La suppression d'une entrée pré-existante démarre la synchronisation du connecteur NT (4864009)

Les installations effectuées avec des utilisateurs Windows existants (Active Directory ou NT) doivent exécuter une commande `idsync resync` avant de démarrer la synchronisation pour éviter des comportements non définis (tels que la synchronisation inattendue d'utilisateurs Windows existants sur Directory Server).

Redémarrez les connecteurs s'ils sont inactifs (4938309)

Si le journal des erreurs central a enregistré un message de type `No response from connector [CNN100] for 10 minutes`, vous devrez sans doute arrêter puis redémarrer le démon/service Identity Synchronization pour Windows où le connecteur est exécuté.

Solution

- Sur Solaris, saisissez la commande `/etc/init.d/isw stop`, puis la commande `/etc/init.d/isw start`.
- Sur Windows, redémarrez le service Sun Java System Identity Synchronization pour Windows.

Redémarrage de Directory Server une fois le protocole SSL (Secure Sockets Layer) du plug-in Directory Server activé (4944804).

Vous devez redémarrer Directory Server après avoir activé le protocole SSL du plug-in Directory Server (sous-composant) et ajouté le certificat de l'autorité de certification (CA) d'Active Directory à la base de données des certificats de Directory Server, ou bien la synchronisation sur demande risque de ne pas authentifier un utilisateur dont le mot de passe a changé sur Active Directory (voir les exemples de messages journalisés).

Si les recherches Active Directory dépassent le délai d'expiration, les administrateurs doivent augmenter la limite de recherche (4881182)

Si le journal des erreurs d'Active Directory indique une erreur de dépassement du délai d'expiration d'un connecteur, utilisez la commande `ntdsutil` du kit de ressources Windows 2000 pour augmenter le délai d'expiration de recherche en procédant comme suit :

```
C: dif>ntdsutil
ntdsutil: ldap policies
ldap policy: connections
server connections: set creds example.sun.com administrator password
server connections: connect to server matar
Binding to matar as user(administrator) in domain(example.sun.com) ...
Connected to matar as user(administrator) in domain(example.sun.com) ...

server connections: quit
ldap policy: show values
```

Policy	Current (New)
MaxPoolThreads	4
MaxDatagramRecv	1024
MaxReceiveBuffer	10485760
InitRecvTimeout	120
MaxConnections	5000
MaxConnIdleTime	900
MaxActiveQueries	20
MaxPageSize	1000
MaxQueryDuration	120
MaxTempTableSize	10000
MaxResultSetSize	262144
MaxNotificationPerConn	5

```
ldap policy: Set InitRecvTimeout to 2400
```

```
ldap policy: Commit Changes
```

Sun Java System Directory Server ne prend pas en charge le traitement de certains attributs à valeur binaire créés sans le sous-type ;binary (5029226)

Certains attributs, tels que `userCertificate` exigent l'option `;binary` au niveau de l'instance de création. Identity Synchronization pour Windows peut synchroniser les valeurs de ces attributs mais ne peut pas définir l'option `;binary` au moment de la création. Cela peut provoquer des problèmes pour les clients qui communiquent avec Sun Java System Directory Server. Sun Java System Directory Server ne renvoie pas cet attribut s'il a été créé sans l'option `;binary` alors que le client le demande.

Identity Synchronization pour Windows ne valide pas le nombre de caractères utilisés lors de la création de l'attribut `nom_utilisateur` (5021886)

NT SAM a une limite de 20 caractères pour l'attribut `nom_utilisateur`. Sun Java Directory Server n'a pas de restriction. L'entrée mappée sur l'attribut `nom_utilisateur` sur NT SAM ne peut pas être utilisée, même si le flux aboutit entre NT SAM et Sun Java Directory Server. Un message d'erreur s'affiche lorsque les propriétés de l'entrée sont éditées ou affichées sur NT SAM.

Console et ligne de commande

Exécution de la commande `idsync prepds` en cas de recréation, de corruption ou d'absence des fichiers de base de données du journal des modifications rétroactif (4921114 et 4832355)

Si la base de données du journal des modifications rétroactif (RCL) a été supprimée ou corrompue, Directory Server ou son connecteur émettent des messages d'avertissement. Lorsque ces messages s'affichent, vous devez recréer le journal des modifications rétroactif et réexécuter la commande `idsync prepds` avant la reprise de la synchronisation.

Les options du bouton **Parcourir pour le DN de base peuvent ne pas changer après le choix d'un nouveau contexte d'attribution de nom (4944711)**

Si vous configurez Identity Synchronization pour Windows à partir de la console pour utiliser plus d'une source Directory Server et plus de deux sources Active Directory (AD), lorsque vous configurez une nouvelle liste d'utilisateurs synchronisés (SUL), il se peut que les options du bouton **Parcourir** du DN de base ne reflètent pas exactement les sources Directory Server ou Active Directory.

Solution

Entrez manuellement le nom du DN de base dans le champ correspondant.

L'hôte de schéma de la console devrait pointer vers l'annuaire de configuration (4877996)

Lorsque vous spécifiez un hôte de schéma, il est recommandé d'utiliser uniquement l'annuaire de configuration de base. Vous ne devez pas utiliser de serveur d'annuaires autonome ou tout autre annuaire de configuration distant.

La fenêtre d'état de la console n'offre pas l'option d'accessibilité 508 pour la visualisation des fichiers journaux (4874361)

Avec le visionneur du fichier journal dans la fenêtre d'état de la console, vous ne pouvez pas utiliser d'interface sans souris pour visualiser les fichiers journaux.

Solution

Pour visualiser les fichiers journaux, copiez-les dans votre éditeur de texte habituel (en dehors du visionneur de journaux de la console).

L'état de la console pour Message Queue n'indique pas correctement l'état réel des composants du système (4937312)

En cas d'interruption de la connectivité du réseau entre la console et le courtier de message, la console peut indiquer de manière incorrecte l'état des composants système.

Solution

Si vous constatez des problèmes réseau, redémarrez la console. Vous pouvez également exécuter la commande `idsync printstat` pour recevoir une vue plus exacte de l'état de Message Queue.

Lors de l'ajout d'une nouvelle source de données Directory Server, un message demande que Directory Server soit préparé alors qu'il l'est déjà (5029558)

Chaque fois que vous créez une source Sun Java System Directory Server, vous êtes invité à préparer la source Directory Server. Si vous avez déjà préparé la source de l'annuaire, vous pouvez sans risque cliquer sur l'option Non.

Un message s'affiche, indiquant que la réinitialisation est en cours, dès que vous exécutez la commande CLI `resetconn`. La réinitialisation des mots de passe échoue et toutes les informations sur la source Directory Server, la configuration, etc., sont supprimées (5039655)

La console ne doit pas être active au moment de l'exécution de la fonction de ligne de commande `resetconn`. Si vous ne quittez pas la console avant d'exécuter cette commande, un message s'affiche, indiquant que la réinitialisation est en cours. Quittez à présent la console et redémarrez-la.

Échec de l'exécution de la commande « `startsync` ». Le message d'erreur « Échec de démarrage de la synchronisation pour certaines des sources d'annuaires demandées » s'affiche (5050443)

Dans certaines conditions (une mémoire insuffisante, par exemple), il est possible que la ligne de commande ou la console de gestion indique que le démarrage de la synchronisation a réussi même si certains composants n'ont pu démarrer la synchronisation. Si vous rencontrez des problèmes de synchronisation, vérifiez si le journal des erreurs contient des messages associés à la mémoire.

Échec de l'attribut paramétré s'il existe plusieurs valeurs pour des attributs à valeur unique (5069907)

La synchronisation échoue si plusieurs valeurs sont indiquées au lieu d'une seule pour les attributs à valeur unique. Aucun message d'erreur ni d'avertissement ne s'affiche si les valeurs sont enregistrées sur Directory Server.

Lorsque la commande idsync est exécutée, les mots de passe s'affichent en texte clair à l'écran (4900126)

Lorsque la commande `idsync` demande les mots de passe de liaison et de configuration, ils s'affichent en texte clair et non crypté lorsque vous les saisissez.

Solution

Pour éviter l'affichage des mots de passe à l'écran, stockez chaque mot de passe dans un fichier protégé, puis redirigez celui-ci vers la ligne de commande. Si l'option « - » est fournie pour un argument de mot de passe, la commande `idsync` demande les valeurs de mot de passe dans l'ordre d'apparition des options sur la ligne de commande. Par exemple, si le mot de passe de l'administrateur est `Mpadmin` et celui de configuration `Mpconfig`, créez un fichier (`mots_passe.txt`) avec le contenu suivant :

`Mpadmin`

`Mpconfig`

Exécutez ensuite la commande `idsync printstat -w - -q - <mots_passe.txt`.

Erreur lors du chargement des fichiers journaux (5091787)

Dans certains cas, lors du chargement du fichier `audit.log` dans l'onglet État de la console, le message d'erreur suivant peut apparaître : « Impossible d'extraire les entrées de journal en raison d'une erreur inconnue. Il est possible que vous deviez redémarrer le serveur d'administration.

Solution

Le fichier `audit.log` sera chargé suite à la demande d'accès, lors des tentatives de chargement suivantes.

Affichage d'un message d'erreur de Prepds dans la configuration MMR lors d'une migration (5093124)

Pendant la migration d'un environnement répliqué, `idsync prepds` peut indiquer à tort que la réplication du schéma a échoué, avec, par exemple, un message d'erreur du type : « Échec de la réplication des changements de schéma du serveur Sun Java System Directory Server par défaut `ldap://exemple.pardefaut.com:389` au serveur Sun Java(TM) System Directory Server secondaire à `ldap://exemple.secondaire.com:389`. Vérifiez les paramètres de réplication. » Dans ce cas, exécutez à nouveau `idsync prepds` avec les mêmes arguments. N'examinez les paramètres de réplication que si la deuxième exécution d'`idsync prepds` entraîne le même message d'erreur.

Impossible d'utiliser Reflection X 10.0 pour accéder à la console (5095013)

Certaines des boîtes de dialogue sont inutilisables car les boutons ou les zones de texte ne sont pas visualisables et les boîtes de dialogue ne peuvent pas être redimensionnées.

Affichage de messages journalisés avec des caractères multioctets corrompus dans la console (6174184)

Des caractères multioctets peuvent être enregistrés dans le journal si vous utilisez un nom multioctet de liste d'utilisateurs de synchronisation ou si un suffixe multioctet est actuellement en cours de synchronisation. Pour afficher correctement les messages journalisés, ouvrez le fichier journal (/var/opt/SUNWsw/logs/central/error.log) dans un visionneur capable d'afficher des documents codés au format UTF-8.

Les commandes startsync et stopsync ne fonctionnent pas correctement lorsque le mot de passe de configuration a été modifié. Un message d'erreur s'affiche (6175396).

Si vous modifiez le mot de passe de configuration d'Identity Synchronization pour Windows à l'aide de la commande `idsync changepw` sans redémarrer ensuite la machine, les commandes `idsync startsync` et `idsync stopsync` ne fonctionnent pas correctement. Les commandes affichent un message tel que : « Le message reçu n'était pas chiffré. » et retournent un code de sortie de 1.

Bien que le message d'erreur s'affiche, l'opération de démarrage ou d'arrêt de la synchronisation s'effectue. Vous pouvez le vérifier en exécutant la commande `idsync printstat`. Cependant, pour éviter ce problème, assurez-vous que vous redémarrez la machine à chaque changement du mot de passe de configuration.

Synchronisation des mots de passe

Problèmes de stratégie des mots de passe (4834865 et 4811572)

Des erreurs de synchronisation peuvent se produire lorsque des stratégies de mot de passe sont utilisées sur différents annuaires. C'est le cas, par exemple, de la longueur du mot de passe et du nombre minimum et maximum de caractères exigés. Les administrateurs sont contraints de modifier manuellement la stratégie de mot de passe pour qu'elle soit compatible avec celle d'autres systèmes.

Les attributs ou mots de passe correspondants qui sont modifiés simultanément risquent de ne pas se synchroniser correctement (4854183 et 4808601).

Lorsqu'une entrée se synchronise entre deux sources d'annuaires et que des modifications sont appliquées en même temps à un attribut, ce dernier risque de ne pas se synchroniser correctement. Prenons, par exemple, la séquence d'événements suivante :

- Jean Dupont modifie son numéro de téléphone en 555-1111 dans Active Directory.
- Cette modification se propage à Directory Server, mais avant qu'elle n'arrive, un administrateur attribue par erreur à Jean Dupont le numéro 555-1112 dans Directory Server.

- La modification introduite dans Active Directory est ensuite appliquée à Directory Server et le numéro 555-1111 attribué à Jean Dupont.
- De la même manière, la modification introduite dans Directory Server se propage à Active Directory, où le numéro de Jean Dupont devient le 555-1112.

Les deux sources d'annuaires ont échangé leur valeur et se sont désynchronisées.

Pareillement, un mot de passe risque, dans certains cas, de ne pas se synchroniser correctement lorsqu'il est modifié presque simultanément sur Active Directory et Directory Server.

Sur les systèmes peu chargés, une désynchronisation n'est possible que si les modifications de mot de passe sont effectuées dans un intervalle de quelques secondes. Bien que cette situation puisse se produire même si le mot de passe AD est modifié *après* avoir pris la valeur Directory Server, c'est improbable car il faudrait alors que la modification du mot de passe AD survienne dans les quelques millisecondes qui suivent sa définition sur la valeur Directory Server.

Utilisation de la fonction obligeant l'utilisateur de modifier son mot de passe à la prochaine connexion (4827180)

Lorsqu'un administrateur modifie le mot de passe d'un utilisateur sur Active Directory et spécifie que celui-ci doit le modifier à la prochaine connexion, la modification n'est pas synchronisée sur Directory Server avant que l'utilisateur ne se connecte et modifie son mot de passe.

L'authentification d'un utilisateur échoue dans les circonstances suivantes :

1. Un utilisateur modifie son mot de passe sur AD (le mot de passe se propage à Directory Server et le mot de passe sur Directory Server est invalidé).
2. L'administrateur réinitialise le mot de passe de l'utilisateur et met à « 1 » l'indicateur obligeant l'utilisateur à modifier son mot de passe à la prochaine connexion.
3. Si l'utilisateur tente de se connecter à Directory Server en utilisant le mot de passe du point 1 ou 2, la tentative de connexion échoue. La modification du mot de passe sur AD ou Directory Server met à jour la valeur du mot de passe sur Directory Server.

La spécification d'un mot de passe non ASCII dans NT ou Active Directory avec le plug-in de contrôle 7 bits activé empêche la synchronisation du mot de passe sur Directory Server (4817344)

Sur Directory Server, le plug-in de contrôle 7 bits (sous-composant) est activé par défaut pour les valeurs d'attribut du mot de passe utilisateur. Reportez-vous à :

<http://docs.sun.com/source/816-6699-10/plugattr.html>

Si vous synchronisez des mots de passe entre Windows et Directory Server qui ne soient pas exclusivement 7 bits et qu'ensuite vous activez et configurez ce plug-in pour les valeurs d'attribut du mot de passe utilisateur, la synchronisation échoue.

Vous devez prendre garde lorsque vous synchronisez des mots de passe avec des caractères non ASCII car le codage de caractères de la valeur du mot de passe n'est pas conservé. Par conséquent, les clients Windows et les clients Directory Server doivent utiliser le même codage de caractères lorsqu'ils changent de mot de passe et, dans certains cas, d'authentification, car l'opération échoue.

Pas de prise en charge des valeurs de mot de passe multiples (4807350)

Les valeurs de mot de passe multiples ne sont pas prises en charge.

La resynchronisation ne reprend pas automatiquement au redémarrage du gestionnaire système (5077660)

Lorsque la commande resync est exécutée et le gestionnaire système redémarré, la resynchronisation ne reprend pas automatiquement là où elle s'était arrêtée et recommence depuis le début.

Risque de suppression des attributs de création lors de la resynchronisation (5085134)

Pas de synchronisation des mises à jour simultanées d'un attribut (5077760)

Ce problème se produit si une valeur est ajoutée à un attribut alors qu'à peu près au même moment, une autre valeur est ajoutée à l'attribut dans une entrée correspondante de l'annuaire distant. L'attribut risque de ne pas être synchronisé.

Lors de la resynchronisation, les actions de liaison ne sont pas reçues par le connecteur Directory Server même si l'opération de resynchronisation a été abandonnée (4985505)

Lors de l'exécution de la commande `resync -c -o Sun`, les actions LINK sont envoyées à Directory Server après la création des nouveaux utilisateurs dans Active Directory. Ces actions LINK ne sont pas reçues par le connecteur Directory Server bien que l'opération de resynchronisation ait été abandonnée. Ces actions LINK sont actuellement publiées dans la même rubrique MQ temporaire que toutes les actions resync/linkusers.

En raison d'un problème connu du plug-in du journal des modifications rétroactif de Directory Server, les entrées supprimées peuvent ne pas être synchronisées de Directory Server vers Active Directory (5077814).

Parfois le plug-in du journal des modifications rétroactif de Directory Server ne parvient pas à stocker l'entrée `dspswuserlink` pour une entrée supprimée. Dans ce cas, la synchronisation de l'entrée Directory Server vers Active Directory n'a pas lieu pour l'entrée supprimée.

Solution

Pour résoudre ce problème, mettez à jour Directory Server avec le patch approprié. Pour plus d'informations sur les patchs requis pour résoudre ce problème, reportez-vous à la section « [Patch du journal des modifications rétroactif de Sun Java System Directory Server 5 2004Q2](#) ».

Sun Java System Message Queue

Pas de connexion du gestionnaire système à Message Queue (4907711)

Le gestionnaire système ne peut pas se connecter à Message Queue alors que ce dernier est activé.

Solution

Redémarrez le service/démon Identity Synchronization pour Windows où le noyau est installé.

Augmentez la mémoire maximale du courtier Message Queue pour les déploiements de 100 000 utilisateurs et plus (4924939)

Identity Synchronization pour Windows configure le courtier Message Queue afin qu'il utilise un maximum de 512 Mo de mémoire par défaut, ce qui est suffisant pour la plupart des installations. Cependant, pour les installations de plus de 100 000 utilisateurs, vous devez augmenter la mémoire maximale à au moins 1 Go pour obtenir des performances optimales. Pour les déploiements de plus de 200 000 utilisateurs, portez la mémoire à 2 Go.

Si le noyau Identity Synchronization pour Windows est installé sur *Solaris*, utilisez la procédure suivante pour augmenter la mémoire limite du courtier Message Queue :

1. Exécutez la commande suivante pour arrêter le courtier Message Queue :
`/etc/init.d/imq stop`
2. Dans le fichier `/etc/imq/imqbrokerd.conf`, modifiez le paramètre de la mémoire par défaut actuelle de `-Xmx512m` pour lui donner une valeur de `-Xmx1024m` pour 1 Go de mémoire, ou de `-Xmx2048m` pour 2 Go.
3. Exécutez la commande suivante pour démarrer le courtier Message Queue :
`/etc/init.d/imq start`

Si le noyau Identity Synchronization pour Windows est installé sur *Windows 2000*, utilisez la procédure suivante pour augmenter la mémoire maximale du courtier Message Queue :

1. À partir de la console de gestion des services Windows, arrêtez le service de courtier Message Queue.

2. Dans le répertoire `<racine-installation>/isw-<nom-machine>/imq/bin`, exécutez la commande `imqsvcadmin query` à partir de la ligne de commande. Le résultat sera semblable à celui présenté ci-après :

```
Service iMQ Broker is installed.

Display name: iMQ Broker

Start Type: Automatic

Binary location: C:\sunone\servers\isw-example\imq\in\imqbrokersvc

JREHome: c:/j2sdk1.4.2/jre/

VM Args: -Xmx512m

Broker Args: -passfile
"C:/sunone/servers/isw-example/imq/etc/passfile.properties"

-DimqConnectionType=TLS -port 7676 -name psw-broker
```

3. Enregistrez le résultat de cette commande dans un fichier.
4. Désinstallez le service du courtier Message Queue en exécutant la commande `imqsvcadmin remove`.
5. Avant de pouvoir continuer, vous devez redémarrer la machine Windows 2000 sur laquelle le noyau est installé.
6. Dans le répertoire `<racine-installation>/isw-<nom-machine>/imq/bin`, exécutez la commande suivante en utilisant le résultat enregistré de la commande `imqsvcadmin query` que vous venez d'exécuter. Par exemple :

```
imqsvcadmin install -jrehome c:/j2sdk1.4.2/jre/ -vmargs -Xmx1024m -args
"-passfile C:/sunone/servers/isw-example/imq/etc/passfile.properties
-DimqConnectionType=TLS -port 7676 -name psw-broker"
```

Où :

- L'argument `-args` est rempli d'après le champ `Broker Args` .
- L'argument `-jrehome` est rempli d'après le champ `JREHome`.
- Pour avoir 1 Go de mémoire, utilisez `-vmargs -Xmx1024m`.
- Pour la Java VM 64 bits uniquement : pour passer à 2 Go de mémoire, utilisez la commande `-vmargs -Xmx2048m`.
La taille de mémoire maximale pour la Java VM 32 bits est `-Xmx1750m`.

7. À partir de la console de gestion des services Windows, démarrez le service de courtier Message Queue.

Démarrage et arrêt du courtier Message Queue (4809493)

Sous Windows, les administrateurs peuvent contrôler le courtier Message Queue, exécuté en tant que service, en accédant au poste de travail.

Pour démarrer et arrêter le courtier sous Windows, redémarrez la machine après avoir installé le noyau de sorte que le gestionnaire de services prenne en compte la variable d'environnement `IMQ_JAVAHOME`. Cette situation s'applique uniquement si vous avez installé Message Queue avec le noyau (autrement dit, aucun Message Queue n'était déjà installé).

Utilisez les commandes suivantes :

```
/etc/init.d/imq (stop ou start)
```

L'utilisation de Message Queue sur une machine où le noyau n'est pas installé n'est pas prise en charge (4943576)

Les composants clés d'Identity Synchronization pour Windows et de Message Queue doivent être installés sur le même hôte.

Problèmes d'ordre général

Des erreurs peuvent encore exister même si le démarrage de la synchronisation a réussi (4814324)

Même si `idsync startsync` indique le succès du démarrage de la synchronisation, vous devez vérifier dans le journal des erreurs central que les connecteurs ont pu se connecter à leurs sources d'annuaires.

Il est fortement recommandé de placer l'annuaire de configuration et la source d'annuaires dans des instances Directory Server séparées dans le cas d'une configuration MMR (réplication multimaître) (4943470 et 4943480).

Dans une configuration MMR, Sun recommande de placer l'annuaire de configuration et la source d'annuaires dans des instances Directory Server séparées et de configurer les accords de réplication *avant* d'installer Identity Synchronization pour Windows.

Lorsque vous désignez la même instance Directory Server comme annuaire de configuration et comme Directory Server par défaut (données utilisateur) et créez des accords de réplication après avoir installé Identity Synchronization pour Windows, les éléments de schéma créés lors de l'installation du noyau Identity Synchronization pour Windows peuvent être supprimés. Dans cette situation, Identity Synchronization pour Windows n'est pas exécuté.

Solution

Pour mettre à jour le schéma que vous auriez effacé accidentellement :

1. Copiez le fichier 40so-psw.ldif (qui contient les objets de schéma du registre de configuration du package d'installation seulement) dans le répertoire du schéma de l'instance Directory Server.

2. Modifiez le nom du fichier 40so-psw.ldif.

Certaines références dans le schéma ne sont pas chargées lors du traitement de 40so-psw.ldif au démarrage (conséquence : le serveur ne démarre pas).

3. Copiez le fichier renommé dans le répertoire du schéma des deux maîtres (du point de vue du serveur, le schéma n'a pas été modifié sur le protocole car le numéro de séquence de modification de l'entrée du schéma reste inchangé).

Les attributs utilisés pendant l'opération de liaison doivent être indexés dans Directory Server (4814412)

Lors de la liaison d'utilisateurs à l'aide de la commande idsync resync (option -f <nomfichier>), la commande recherche dans Directory Server les utilisateurs qui correspondent aux utilisateurs Active Directory ou Windows NT. Chaque attribut Directory Server utilisé dans une opération idsync resync doit être indexé pour l'égalité.

Impossible de désactiver le journal central (4945507 et 4933217)

Bien que le journal central d'Identity Synchronization pour Windows (qui journalise dans les fichiers, le journal système ou les deux) autorise apparemment sa désactivation, il continue d'effectuer la journalisation dans l'emplacement spécifié précédemment.

Par exemple, si après avoir spécifié la journalisation du journal système (syslog) à partir de la console (avec journalisation des fichiers désactivée), vous décidez de la désactiver, le programme continue la journalisation du journal système. Si après avoir spécifié la journalisation des fichiers à partir de la console (avec journalisation du journal système désactivée), vous décidez de la désactiver, le programme continue la journalisation des fichiers.

Le même comportement se produit lorsque l'option « Écrire les journaux dans un fichier » est décochée et que le journal système n'a jamais été utilisé. Dans ce cas, le programme continue d'écrire des journaux dans le répertoire.

Le redémarrage du service Identity Synchronization pour Windows n'a aucun effet : la journalisation continue.

Le bouton Parcourir de la liste d'utilisateurs de synchronisation ne fonctionne pas dans certains cas (4944348)

Lorsque vous recherchez un DN de base dans la liste d'utilisateurs synchronisés (SUL), l'assistant de création ou l'écran d'édition, il est recommandé de vérifier le DN de base dérivé à l'aide du bouton Parcourir. Dans certains cas, le bouton ne parcourt pas le bon répertoire et fournit un DN de base incorrect.

Désactivation des comptes utilisateur sur Active Directory (4943785)

Lorsqu'un utilisateur invalide un compte et modifie le mot de passe sur Active Directory (AD), il ne peut plus s'authentifier via AD en utilisant le nouveau mot de passe. Par contre, après avoir désactivé un compte utilisateur sur AD, il peut toujours se connecter au moyen de Sun Java System Directory Server.

Modification du port de l'annuaire de configuration (4941271)

Lorsque vous modifiez le port d'un serveur Sun Java System Directory Server utilisé comme annuaire de configuration Identity Synchronization pour Windows, vous devez également modifier la configuration d'Identity Synchronization pour Windows afin que le logiciel reconnaisse le changement de port. Dans le cas contraire, le gestionnaire système et le courtier Message Queue ne fonctionnent pas.

Solution

1. Modifiez le port dans
`<img_installroot>\img\var\instances\psw-broker\props\config.properties.`
Par exemple, `img.user_repository.ldap.server=<hôte>\:<port>`
2. Modifiez le port dans `<isw_installroot>\resources\SystemManagerBootParams.cfg`
Par exemple, `<Nom_paramètre="manager.configReg.hostPort" value="<port>" />`
3. Redémarrez le service/démon du courtier Message Queue.
4. Redémarrez le démon/service Identity Synchronization pour Windows.

Prise en charge restreinte des attributs différents à valeurs multiples (4987930 et 4807260)

Identity Synchronization pour Windows fournit seulement une prise en charge restreinte pour la synchronisation d'attributs différents à valeurs multiples, car les résultats ne sont pas définis. Les restrictions appliquées sont les suivantes :

- Les valeurs d'un attribut à valeur multiple sont synchronisées en tant qu'unité. Par exemple, si vous ajoutez une valeur unique à un attribut à valeur multiple qui possède déjà quatre valeurs, les cinq valeurs sont synchronisées en tant qu'unité, et les valeurs de l'attribut distant correspondant sont définies sur ces cinq valeurs.
- Lorsque des utilisateurs pré-existants sont liés, leurs attributs ne sont pas automatiquement synchronisés. Lorsqu'un attribut à valeur multiple change, les valeurs de l'attribut sur la source d'annuaires distante sont écrasées par les valeurs de la source d'annuaires locale. Par exemple, si vous ajoutez un numéro de téléphone à l'attribut `telephoneNumber`, précédemment vide, d'une entrée dans Active Directory, l'attribut `telephoneNumber` de l'entrée correspondante dans Directory Server prend cette nouvelle valeur, écrasant celles existantes.

- Des mises à jour simultanées d'un attribut à valeur multiple risquent de ne pas se synchroniser. Si vous ajoutez une valeur à un attribut à valeur multiple alors qu'une valeur différente est ajoutée quasi simultanément à l'attribut à valeur multiple dans l'entrée d'annuaire distant correspondante, l'attribut risque de se désynchroniser. Cette situation se produit également pour les attributs à valeur unique.
- Lorsque vous modifiez ou renommez l'attribut `cn`, le `cn` est un attribut de type valeur multiple sur Directory Server, mais de type valeur unique sur AD. AD utilise ce type d'attribut (et sa valeur) pour générer de nouveaux DN pour les entrées de personnes à renommer ou modifier. Comme le connecteur ne connaît pas la valeur à utiliser dans un attribut `cn` à valeur multiple pour créer le nouveau DN, il envoie, par défaut, la première valeur. La première valeur n'étant pas généralement la valeur correcte, la modification ou le changement de nom échoue sur Active Directory.

Si vous spécifiez `renames (ldap modrdns)` avec l'indicateur `deleteoldrdn` à 0 et sélectionnez `cn` pour le type d'attribut des composants `rdn`, l'opération échoue côté AD. Par exemple, si l'entrée suivante existe et qu'elle est synchronisée à la fois sur Directory Server et AD,

```
cn=ancien rdn, ou=exemple,com
cn=ancien rdn
```

et vous renommez l'entrée sur Directory Server et mettez l'indicateur `deleteoldrdn` à 0, Identity Synchronization pour Windows modifie l'entrée côté Directory Server, qui devient

```
cn=nouveau rdn, ou=exemple,com
cn= ancien rdn
cn= nouveau rdn
```

mais la modification du nom échoue côté AD car l'entrée créée sera :

```
cn=ancien rdn, ou=exemple.com (et non pas cn=nouveau rdn, ou=exemple.com)
```

provoquant un message d'erreur (enregistré dans le journal d'audit), semblable à celui présenté ci-après :

```
[30/Jan/2004:16:41:14.831 -0600] WARNING 16 CNN100 dragon "The action does not have a
single value for attribute cn. The corresponding user at the remote repository might not
have been created with a corresponding attribute value, the attribute might have
multiple values, or cn is not a significant or creation attribute for this directory
source. See audit log for more information" (Action ID=CNN101-FA6784B526-787, SN=1) %%
```

Pour que l'opération réussisse, vous devez mettre à « 1 » l'indicateur `deleteoldrdn`. Utilisez l'exemple d'instructions de modification LDAP suivant pour exécuter correctement le changement de nom :

```
dn: cn=ancien rdn, ou=exemple.com
changetype: modrdn
newrdn: cn=nouveau rdn
deleteoldrdn: 0
```

- Lorsque vous modifiez un attribut `cn` en utilisant le type de modification `modify` et le mode `add`, si vous ajoutez plusieurs attributs de type `cn` ou s'il existe déjà un attribut de ce type et que vous en ajoutez un, l'opération `modify` échoue. Par exemple, si l'entrée `cn` suivante existe à la fois sur Directory Server et Active Directory,

```
cn=exemple1, ou=exemple.com
cn=exemple1
```

Vous appliquez à l'entrée les instructions de modification LDAP suivantes,

```
dn: cn=exemple1, ou=exemple.com
changetype: modify
add: cn
cn: nouvelle valeur
```

l'entrée sur Directory Server devient

```
cn=exemple1, ou=exemple.com
cn=exemple1
cn=nouvelle valeur
```

Cependant, l'opération `modify` échoue côté AD, car AD est à valeur unique. Le même message d'erreur que celui du cas précédent apparaît dans le journal d'audit car le connecteur ne peut pas faire la distinction entre un changement de nom et une modification.

Active Directory traite les attributs de description comme des attributs à valeur unique même si le schéma AD les décrit comme étant à valeur multiple (4938940)

Lorsque vous ajoutez des entrées à Directory Server à l'aide d'un attribut de description à valeur multiple, l'erreur DSID-031D0809 suivante est enregistrée dans le journal d'audit du connecteur Active Directory (AD) :

```
[16/Oct/2003:10:02:54.998 -0500] SEVERE 29 CNN101 dragon "Unable to create user
"cn=Aaccf Amar1072,cn=users,dc=example,dc=sun,dc=com" at
ldaps://starlingvm0.example.sun.com:636. LDAP add operation failed. Error code: 19,
reason: 00002081: AtrErr: DSID-031D0809, #1: 0: 00002081: DSID-031D0809, problem 1005
(CONSTRAINT_ATT_TYPE), data 0, Att d (description)
" (Action ID=CNN100-F841CDBF2A-2568, SN=8)
```

L'entrée existe sur Directory Server mais pas sur AD.

Ce problème serait un défaut d'Active Directory. Pour plus d'informations, reportez-vous à l'article suivant de la Base de connaissances Microsoft (286760) :

<http://support.microsoft.com/default.aspx?scid=kb;en-us;286760&Product=win2000>

Solution

Supprimez l'entrée de Directory Server, créez l'attribut de description à valeur unique et ajoutez de nouveau l'entrée.

Il convient également de ne pas initialiser plusieurs attributs pour la description dans la boîte de dialogue Définir les mappages et valeurs des attributs de création.

Pas de message d'erreur du plug-in lorsque le certificat SSL (Secure Sockets Layer) n'est pas de confiance (4924027 et 4924705)

Dans une configuration de réplication multimaître (MMR), lorsqu'un plug-in (sous-composant) Identity Synchronization pour Windows communique en utilisant le protocole SSL et qu'un problème SSL provoque une défaillance, si le plug-in n'envoie pas de messages d'erreur, il est probable qu'un certificat CA du certificat du serveur *homologue* (qui peut être un maître par défaut, un maître secondaire ou une instance Active Directory) manque dans la base de données du Directory Server qui exécute le plug-in.

Vous pouvez utiliser l'utilitaire de ligne de commande `idsync certinfo` pour identifier les certificats manquants. Cet utilitaire identifie quels certificats sont obligatoires et dans quelle base de données (les certificats attendus par le produit).

Les utilisateurs créés dans Sun Java System doivent inclure tous les attributs des filtres de la liste d'utilisateurs synchronisés (4900568)

Si vous synchronisez une création d'entrée vers Windows à partir de Sun Java System Directory Server avec des filtres dans les définitions de la liste SUL de Directory Server, essayez de créer une entrée comportant des valeurs d'attribut qui ne correspondent pas au filtre SUL. La création de l'entrée n'est pas propagée car les attributs ne figurent pas dans la liste SUL. Du fait que la création d'origine ne s'est pas propagée, l'entrée sur Directory Server ne se retrouve pas côté Windows.

Solution

Dans cette situation, un message d'avertissement est journalisé et l'administrateur doit exécuter `idsync resync -c -o Sun` pour créer l'entrée Directory Server sur Windows.

Si vous modifiez l'entrée pour que les attributs correspondent au filtre SUL, les modifications apportées à l'entrée se propagent côté Windows.

Retard de la synchronisation sur demande provoqué par NetBIOS (4876741)

Une tentative de synchronisation de deux domaines Active Directory (AD) en utilisant une configuration composée d'un Directory Server et de composants principaux sur Windows 2000 a provoqué un retard lorsque la fonction de synchronisation sur demande du plug-in Directory Server communiquait avec AD. Normalement, la plupart des requêtes faites à AD durent quelques millisecondes. Un suivi de paquets a identifié des paquets NBNS (NetBIOS Name Service) suspects.

Solution

Pour résoudre le problème, accédez aux paramètres TCP/IP de la machine Directory Server et désactivez NetBIOS sur TCP/IP.

Espaces de noms (rubriques) Identity Synchronization pour Windows utilisés par le bus de message (4827081)

- ConConfig_100
- CntrlLog_100
- SysMgr_100
- PSW_AuditLoggingTopic
- PSW_ErrorLoggingTopic
- PSW_LinkAuditLoggingTopic

En outre :

- Pour chaque connecteur du système, il existera une rubrique CNN1XX_100 (telle que CNN100_100, CNN101_100 et CNN102_100).
- Pour chaque liste SUL du système, il existera une rubrique basée sur le nom SUL (par exemple, une SUL nommée *people* comportera une rubrique appelée *people_100*.)

La spécification d'un hôte à partir de la boîte de dialogue Catalogue global ou annuaire de configuration peut durer un certain temps (4826109 et 4812651).

Lorsque vous spécifiez un hôte qui ne peut être résolu, aucun indicateur de progression (tel qu'un curseur occupé ou une barre d'état) ne s'affiche pour indiquer une quelconque opération.

Les noms d'utilisateur NT doivent être uniques (4825636)

Lorsque vous créez un utilisateur dans Directory Server à propager vers NT, vérifiez que l'attribut Directory Server mappé sur NOM_UTILISATEUR comporte des valeurs uniques.

Recommandez aux utilisateurs de sécuriser les fichiers de configuration XML en utilisant des listes de contrôle d'accès (ACL) (4812824)

Utilisez la protection au niveau fichier pour les fichiers de configuration XML. Ces fichiers peuvent contenir des valeurs de mot de passe en clair. C'est pourquoi vous devez les sécuriser en utilisant les fonctions offertes par le système, telles que des ACL au niveau fichier.

Relation entre listes SUL et base de données (4811577)

Identity Synchronization pour Windows ne prend en charge qu'une base de données Directory Server unique. Vous devez inclure toutes les listes SUL dans une base de données Directory Server unique.

Croissance illimitée du nombre de journaux (4807451)

À moins de sauvegarder ou de supprimer les anciens journaux, le nombre de journaux de chaque type dans Identity Synchronization pour Windows est incrémenté d'un chaque jour.

Le nom des journaux a le format suivant :

- audit_AAAA_MM_JJ.log
- error_AAAA_MM_JJ.log

Les journaux conservés sont les suivants :

- audit
- error

Ces journaux se trouvent aux emplacements suivants :

- **Sous Solaris** : /var/opt/SUNWisw/logs
- **Sous Windows** : <racine-installation>/isw-<nom-machine>/logs

Pas de synchronisation des entrées à caractères spéciaux entre Directory Server et Active Directory (4816867)

Identity Synchronization pour Windows ne peut pas résoudre les caractères spéciaux (du fait de restrictions de mappage) ou bien Active Directory ne peut pas créer l'utilisateur car son uid comporte un ou plusieurs caractères spéciaux.

La console AD n'autorise pas la création d'un « nom de connexion utilisateur » qui

- comporte l'un des caractères spéciaux suivants : " / [] : | < > ; ? % \$ ^ & * () ! @ # - + = ~ `
- dépasse 20 caractères ;
- se termine par un point ou inclut des virgules ;
- inclut des caractères dans la plage 1 à 31, qui sont des caractères non imprimables.

La valeur par défaut de l'attribut useraccountcontrol empêche la création d'une classe d'objets Active Directory non utilisateur (5043156)

Il est impossible de créer des utilisateurs dans Active Directory si la classe d'objets sélectionnée des nouveaux utilisateurs n'autorise pas l'attribut useraccountcontrol. Cette restriction ne s'applique pas aux situations où la classe d'objets de l'utilisateur ou toute autre classe d'objets dérivée de l'utilisateur autorise l'attribut useraccountcontrol dans Active Directory.

Solution

Éditez l'utilisateur de configuration à partir de la console Directory Server. Recherchez et supprimez l'attribut useraccountcontrol.

Par exemple :

```
dn: cn=130,ou=AttributeDescriptions,cn=active[2],ou=GlobalConfig,ou=1.1,ou=IdentitySynchronization,ou=Services,dc=central,dc=sun,dc=com
pswVersion: 2
pswName: useraccountcontrol
pswSyntax: 1.3.6.1.4.1.1466.115.121.1.5
pswValue: 512
pswPreferCreationAttributeDefaultToAction: false
cn: 130
objectClass: pswattributedescription
objectClass: top
```

Éditez également toutes les références faites à l'attribut useraccountcontrol, en particulier dans l'attribut pswCreationAttributeDefaultRef du schéma global Active Directory.

Par exemple :

```
dn: cn=127,ou=ActiveDirectory,ou=Globals,cn=active[2],ou=GlobalConfig,ou=1.1,ou=IdentitySynchronization,ou=Services,dc=central,dc=sun,dc=com
```

Aucune validation des valeurs par défaut (5051725)

Il est possible de spécifier des valeurs par défaut pour les attributs et de les appliquer aux entrées d'annuaire au moment de la création des attributs (reportez-vous à la section « Creation Attributes » du manuel *Sun Java System Identity Synchronization pour Windows Installation and Configuration Guide*). À l'heure actuelle, aucune validation n'est effectuée pour les valeurs d'attribut spécifiées. La spécification de valeurs multiples pour les attributs à valeur unique provoque l'échec de la création de l'objet lors de la synchronisation des entrées. Lorsque vous spécifiez des valeurs d'attribut, assurez-vous que ces valeurs respectent le schéma LDAP de votre entreprise.

Traitement incohérent des modifications lorsque l'utilisateur figure dans la liste SUL (4970664)

Lorsqu'un utilisateur relève d'une liste SUL à la suite d'une modification (par exemple, la liste SUL comporte un filtre « l=Austin » et l'attribut l de l'utilisateur est modifié avec la valeur Austin), Sun Java System Identity Synchronization pour Windows applique un traitement différent à la mise à jour de l'utilisateur dans Active Directory et dans Sun Java System Directory Server :

- Si la mise à jour de l'utilisateur s'est produite dans Active Directory, le connecteur Identity Synchronization Directory Server crée l'utilisateur correspondant.
- Si la mise à jour de l'utilisateur s'est produite dans Sun Java System Directory Server, l'utilisateur correspondant n'est pas créé dans Active Directory. L'exécution de la commande `resync -c -o` Sun peut aider à résoudre ce problème.

Les entrées dont la classe d'objets structurelle hérite de la classe d'objets sélectionnée pour la synchronisation sont également synchronisées (5046861)

Par exemple, si la classe d'objets sélectionnée est `organizationalperson`, les utilisateurs dont la classe d'objets est `inetorgperson` sont également synchronisés car `inetorgperson` est une sous-classe de `organizationalperson`.

Pour éviter que cela ne se produise, la liste SUL doit comporter un filtre qui exclut la sous-classe :
(!(objectclass=inetorgperson))

Normalement, cela pose un problème lorsque vous utilisez la commande `resync` pour synchroniser des entrées supprimées, les sous-classes étant également supprimées. Par exemple, avec Active Directory, la classe d'objets `computer` hérite de l'utilisateur, et les entrées `computer` risquent d'être effacées car elles n'ont pas d'entrée Directory Server correspondante. Pour éviter la synchronisation des entrées `computer`, ajoutez un filtre dans la liste SUL de manière à les exclure :
(!(objectclass=computer))

Pas de suppression automatique des fichiers journaux après leur date d'expiration (5069020)

Les fichiers journaux ayant atteint la date d'expiration à partir de laquelle ils doivent être supprimés ne sont pas effacés.

Possibilité de configuration incorrecte ou d'échec de validation des valeurs d'attribut de création par défaut (5066657)

Si le nom d'un attribut de création est identique pour Directory Server et la source de données Active Directory, ajouter des valeurs par défaut à une source ajoute automatiquement les mêmes valeurs par défaut à l'autre source.

Solution

Supprimez les attributs de création et leur mappage dans la console, puis ajoutez-les à nouveau.

Avant d'enregistrer, procédez de la façon suivante :

Si les noms des attributs mappés sont identiques et si les syntaxes (OID) de ces attributs sont identiques dans les schémas Active Directory et Directory Server :

- Vérifiez que les valeurs par défaut que vous ajoutez pour les attributs ne sont pas les mêmes. L'absence de valeur peut également entraîner ce problème.

REMARQUE Si les valeurs par défaut sont identiques, ce problème ne se produit pas, car vous ne pouvez pas les séparer sans supprimer, puis rajouter les attributs de création et leur mappage.

La valeur par défaut de l'attribut useraccountcontrol empêche la création d'une classe d'objets Active Directory non utilisateur (5043156)

Il est impossible de créer des utilisateurs dans Active Directory si la classe d'objets sélectionnée pour les nouveaux utilisateurs n'autorise pas l'attribut useraccountcontrol. La classe d'objets de l'utilisateur ou toute autre classe d'objets dérivée de l'utilisateur autorise l'attribut useraccountcontrol dans Active Directory et ne sera pas affectée par cette limitation.

Impossible de mapper InetOrgperson avec une classe étendue contenant un attribut obligatoire (5091959)

Par exemple, un message d'erreur similaire au suivant s'affiche : « Aucun mappage ou valeur Sun n'est spécifié pour l'attribut Active Directory mail », où mail est un attribut obligatoire mappé à l'attribut mail de Sun.

Le manuel Identity Synchronization for Windows Installation and Configuration Guide ne mentionne pas le bouton Suivant ni le panneau Résumé (5104768)

Le manuel *Identity Synchronization for Windows Installation and Configuration Guide* indique qu'à la fin de chaque appel de l'assistant, vous devez quitter celui-ci en utilisant le bouton Fermer sur le panneau Résumé de l'installation. Cependant, aucun bouton Fermer n'apparaît sur le panneau. À partir du panneau Résumé de l'installation, vous devez cliquer sur le bouton Suivant afin d'afficher un autre panneau qui décrit les étapes d'installation et de configuration restantes. Pour toutes les installations sauf l'installation de base (Core), ce panneau contient un bouton Terminé qui permet de quitter l'assistant. Pour l'installation de base (Core), il contient un bouton Suivant qui affiche un panneau vous invitant à préciser si vous souhaitez démarrer la console. Vous pouvez quitter le programme d'installation à partir de ce dernier panneau en cliquant sur le bouton Terminé.

Limites de la prise en charge WAN (réseau étendu) (5097751)

Identity Synchronization pour Windows peut être déployé dans un environnement WAN, avec cependant certaines restrictions.

À l'exception du plug-in Directory Server, tous les composants d'Identity Synchronization pour Windows doivent être installés sur le même réseau local (par exemple sur la même machine). Autrement dit, aucun trafic Message Queue ne doit transiter par le réseau étendu. Cependant, ces composants peuvent communiquer sur un WAN avec des serveurs Directory Server ou des contrôleurs de domaine Active Directory.

Les performances obtenues avec un WAN dépendent des temps de latence et des vitesses des liaisons. Il est conseillé d'utiliser au minimum une connexion T1 (1,544 Mbit/s) avec des temps de latence inférieurs à 300 ms entre chaque connecteur et l'annuaire qu'il gère. Dans un déploiement où Active Directory et Directory Server sont séparés par un WAN, il est possible d'améliorer les performances en installant le connecteur Directory Server sur le même réseau local que Directory Server, et en forçant le connecteur Active Directory à communiquer avec Active Directory par l'intermédiaire du WAN.

Fichiers redistribuables

Sun Java System Identity Synchronization pour Windows 1 2004Q3 ne contient aucun fichier pouvant être redistribué.

Comment signaler des problèmes et apporter des commentaires

Si vous rencontrez des problèmes avec Sun Java System Identity Synchronization pour Windows, contactez le service clientèle Sun d'une des manières suivantes :

- En faisant appel aux services d'assistance logicielle Sun en ligne à l'adresse suivante :

<http://www.sun.com/service/sunone/software>

Ce site contient des liens vers la base de connaissances, le centre d'assistance en ligne et ProductTracker, ainsi que vers des programmes de maintenance et des coordonnées pour l'assistance.

- le numéro de téléphone associé à votre contrat de maintenance.

Afin de vous aider à résoudre votre problème, pensez à réunir les informations suivantes lorsque vous contactez l'assistance technique :

- description du problème, y compris l'endroit où il se produit et son impact sur l'exploitation ;
- type de machine, versions du système d'exploitation et du produit, y compris les correctifs et autres logiciels pouvant avoir un lien avec le problème ;
- procédure détaillée des méthodes utilisées pour reproduire le problème ;
- tous les journaux d'erreur ou vidages de la mémoire.

Sun attend vos commentaires

Afin d'améliorer sa documentation, Sun vous encourage à faire des commentaires et à apporter des suggestions. Pour ce faire, utilisez le formulaire électronique disponible à l'adresse suivante :

<http://www.sun.com/hwdocs/feedback/>

Veuillez indiquer le titre complet du document ainsi que sa référence dans les champs appropriés. Le numéro du document se trouve sur la page de titre du manuel ou en haut du document. Il s'agit généralement d'un nombre à 7 ou 9 chiffres. Par exemple, le numéro de référence du présent manuel Identity Synchronization pour Windows Version 1 2004Q3 Notes de version est 817-7852.

Ressources Sun supplémentaires

Vous pouvez obtenir des informations utiles concernant Sun Java System sur les sites Internet suivants :

- Documentation de Sun Java System Identity Synchronization pour Windows
http://docs.sun.com/coll/S1_IdSyncForWin_1.0
- Sun Java System Documentation
<http://docs.sun.com/prod/sunone>
- Services professionnels de Sun Java System
<http://www.sun.com/service/sunps/sunone>
- Produits et services logiciels de Sun Java System
<http://www.sun.com/software>

- Services d'assistance logicielle Sun Java System
<http://www.sun.com/service/sunone/software>
- Base de connaissances et d'assistance Sun Java System
<http://www.sun.com/service/support/software>
- Services de formation et d'assistance Sun
<http://training.sun.com>
- Services professionnels et de conseil Sun Java System
<http://www.sun.com/service/sunps/sunone>
- Informations pour les développeurs Sun Java System
<http://sunonedev.sun.com>
- Services d'assistance pour développeurs Sun
<http://www.sun.com/developers/support>
- Formation sur les logiciels Sun Java System
<http://www.sun.com/software/training>
- Fiches techniques sur les logiciels Sun
<http://www.sun.com/software>

Copyright © 2004 Sun Microsystems, Inc. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs des brevets américains répertoriés à l'adresse <http://www.sun.com/patents> et un ou plusieurs des brevets supplémentaires ou demandes de brevet en attente aux États-Unis et dans d'autres pays.

Propriété de SUN/CONFIDENTIEL.

L'utilisation est soumise aux termes du contrat de licence.

La distribution du logiciel peut s'accompagner de celle de composants mis au point par des tiers.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD sous contrat de licence par l'Université de Californie.

Sun, Sun Microsystems, le logo Sun, Java et Solaris sont des marques ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées dans le cadre d'un contrat de licence et sont des marques ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays.

