



Présentation technique de Microsoft Identity Integration Server 2003 avec Service Pack 1

Microsoft Corporation

Publié : décembre 2004

Mis à jour : août 2005

Résumé

Microsoft Identity Integration Server 2003 (MIIS) permet l'intégration et la gestion des informations d'identité à travers plusieurs entrepôts de données, systèmes et plateformes. MIIS optimise Active Directory en fournissant une large gamme de fonctionnalités d'interopérabilité, parmi lesquelles : l'*intégration* avec une vaste gamme d'entrepôts de données d'identité ; la *gestion* et la *synchronisation* des informations d'identité, notamment la synchronisation et la gestion des mots de passe entre différents systèmes ; et la *diffusion* des modifications apportées aux informations d'identité par détection automatique des mises à jour et le partage des modifications entre les systèmes.

Ce livre blanc décrit les améliorations et les nombreuses nouvelles fonctionnalités qu'apporte MIIS 2003 ; elles en font un composant stratégique de toute implémentation de gestion des identités.

Les informations contenues dans ce document représentent l'opinion actuelle de Microsoft Corporation sur les points cités à la date de publication. Microsoft s'adapte aux conditions fluctuantes du marché et cette opinion ne doit pas être interprétée comme un engagement de la part de Microsoft ; de plus, Microsoft ne peut pas garantir la véracité de toute information présentée après la date de publication.

Ce document est fourni uniquement à titre indicatif. MICROSOFT EXCLUT TOUTE GARANTIE, EXPRESSE OU IMPLICITE, EN CE QUI CONCERNE LES INFORMATIONS DE CE DOCUMENT.

L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicable dans son pays. Aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de restitution, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre) sans la permission expresse et écrite de Microsoft Corporation.

Microsoft peut détenir des brevets, avoir déposé des demandes d'enregistrement de brevets ou être titulaire de marques, droits d'auteur ou autres droits de propriété intellectuelle portant sur tout ou partie des éléments qui font l'objet du présent document. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

Sauf mention contraire, les noms de sociétés, d'organisations, de produits, de personnes ou les événements mentionnés dans les exemples sont fictifs. Toute ressemblance avec des noms ou des événements réels est purement fortuite et involontaire.

© 2004 Microsoft Corporation. Tous droits réservés.

Microsoft, Active Directory, Visual Basic, Visual C++, Visual C#, Visual Studio, Windows, le logo Windows, Windows NT et Windows Server sont soit des marques de Microsoft Corporation, soit des marques déposées de Microsoft Corporation, aux États-Unis d'Amérique et/ou dans d'autres pays.

Les noms de sociétés et de produits mentionnés dans ce document sont des marques de leurs propriétaires respectifs.

Sommaire

Introduction à Microsoft Identity Integration Server 2003	1
Fonctionnalités	2
Identity Integration Feature Pack (IIFP) pour Microsoft Windows Server Active Directory	4
Enterprise Edition	4
Avantages	4
Vue d'ensemble de l'architecture	6
Sources de données connectées	6
Agents de gestion	6
Espace connecteur (EC).....	7
Connecteurs et déconnecteurs	7
Métaverse (MV)	8
Nouvelles fonctionnalités	9
Flux d'attribut et priorité	9
Extensions personnalisées	10
Visual Studio .NET	11
Solution de sécurité Microsoft .NET Framework.....	11
Outil de traçabilité des données	12
Base de données MIIS 2003	12
Haute disponibilité et service de cluster.....	13
Gestionnaire d'identité	14
Catégories de règles d'agent de gestion.....	15
Metaverse Search.....	16
Gestion de mots de passe	17
Mode Aperçu.....	18
Approvisionnement	19
Révocation	20
Infrastructure de gestion Windows (WMI, Windows Management Instrumentation).....	20
Résumé.....	21
Liens connexes.....	22

Introduction à Microsoft Identity Integration Server 2003

Aujourd'hui, dans la plupart des entreprises, chaque application ou système possède sa propre base de données ou son propre annuaire d'utilisateurs pour gérer les personnes autorisées à utiliser cette ressource. Les données d'identité et de contrôle d'accès résident dans des dizaines, voire des centaines, de répertoires différents, comme les répertoires de ressources réseau spécialisés, les serveurs de messagerie électronique, la gestion des ressources humaines, la messagerie vocale, la paie et de nombreuses autres applications.

Chaque application ou système possède sa propre définition de l'« identité » d'un utilisateur (nom, poste, numéros d'identification, rôles, appartenance à des groupes). De nombreux systèmes ou applications possèdent leur propre mot de passe et processus pour authentifier leurs utilisateurs. Chacun dispose de son propre outil pour la gestion des comptes d'utilisateur et a même parfois des administrateurs dédiés chargés de cette tâche. En outre, la plupart des entreprises possèdent plusieurs processus de demande de ressources ainsi que d'octroi et de modification des droits d'accès. Certains de ces processus sont automatisés, mais la plupart sont basés sur des documents papier. Beaucoup diffèrent d'un service de l'entreprise à un autre, même lorsqu'ils exécutent la même fonction.

L'administration et la mise en service de nouveaux comptes dans ces différents entrepôts de données prennent souvent du temps et se révèlent redondantes. Cela gêne les utilisateurs qui doivent se souvenir de plusieurs identifiants et mots de passe pour les différents systèmes et applications. Plus grande est l'organisation, plus le nombre des entrepôts de données ainsi que l'effort requis pour assurer leur mise à jour sont importants. Ce labyrinthe de processus inefficaces et de systèmes superposés peut avoir des conséquences importantes sur les points suivants :

Maîtrise des dépenses et efficacité

- Les nouveaux employés et sous-traitants patientent pendant plusieurs jours pour obtenir le droit d'accès aux applications dont ils ont besoin.
- Le personnel du service d'assistance technique, les responsables, le personnel informatique et celui des ressources humaines consacrent de nombreuses heures à remplir des formulaires, à entrer et mettre à jour des données d'utilisateur, à définir des comptes et à réinitialiser des mots de passe.

Sécurité

- Les employés, sous-traitants et partenaires commerciaux qui cessent leur activité avec l'entreprise conservent un accès aux systèmes pendant de longues périodes et les comptes d'utilisateur « orphelins » (non valides) prolifèrent.
- L'organisation ne peut satisfaire ni les exigences d'audit ni respecter les réglementations en vigueur.

Service client et chaîne logistique

- Des vues incomplètes sur les données des clients gênent le service client et empêchent des opportunités de vente croisée.
- Les initiatives Web en faveur des clients et les projets d'intégration de la chaîne logistique sont entravés, car les entreprises ne peuvent ouvrir leurs systèmes informatiques et leurs informations sensibles à des tiers externes, par manque de confiance.

Microsoft Identity Integration Server (MIIS) 2003 représente la solution pour sortir de ce chaos. MIIS est un système qui gère et coordonne des informations d'identité provenant de plusieurs sources de données. Il vous permet d'associer toutes ces informations dans une vue unique et logique.

Fonctionnalités

Les sections suivantes décrivent les fonctionnalités de MIIS 2003¹.

Centralisation des informations d'identité

Dans la plupart des organisations, les informations d'identité sont dispersées dans de nombreuses sources de données différentes. Ceci entraîne des risques importants de doublons et d'incompatibilité des formats de données et oblige les administrateurs à accéder à plusieurs sources de données pour gérer la même identité.

Afin de résoudre les problèmes liés aux données d'identité résidant dans plusieurs sources, MIIS peut :

- regrouper les données d'une personne ou d'une ressource spécifique en créant une entrée unique contenant tout ou partie des informations d'identité en provenance de chacune des sources de données ;
- présenter une seule vue unifiée de tout ou partie des attributs en provenance des différentes sources, que ces dernières soient compatibles ou pas ;
- fournir un emplacement unique à partir duquel les administrateurs, les applications et les utilisateurs peuvent accéder aux informations d'identité d'un objet spécifique ou les gérer.

Gestion des informations d'identité

Des annuaires distincts contiennent souvent des informations d'identité conflictuelles concernant une même personne ou ressource. En outre, le service qui possède et gère les données d'une source de d'informations spécifique pense généralement que ses données font autorité par rapport à celles résidant dans d'autres sources et refuse souvent d'abandonner son contrôle sur ces données.

Pour résoudre les problèmes concernant des informations d'identité conflictuelles, MIIS peut :

- gérer le flux des informations d'identité entre des sources de données connectées pour résoudre des conflits d'informations d'identité à travers l'organisation ;
- définir les informations d'identité spécifiques à importer depuis chaque source de données connectée ;
- établir des règles pour déterminer quel annuaire contient la valeur faisant autorité concernant un attribut spécifique, et permettre au serveur MIIS de mettre à jour les autres sources de données connectées avec cette valeur faisant autorité.

Gestion des modifications des informations d'identité

Les informations d'identité d'une organisation étant souvent contenues dans plusieurs sources de données, une modification apportée aux données dans l'une d'entre elles n'est pas automatiquement répercutée dans toutes les autres. Pour propager la modification dans l'ensemble de l'organisation, des

¹ Ce livre blanc est spécifique aux fonctions de MIIS 2003, Enterprise Edition avec le Service Pack 1 (SP1)

administrateurs doivent appliquer manuellement les modifications dans chaque source de données. Cela conduit généralement à des erreurs et à des désynchronisations au sein de l'organisation.

Pour résoudre les problèmes résultant des modifications des informations d'identité, MIIS peut :

- détecter toute modification des informations d'identité, quelle que soit sa provenance ;
- propager automatiquement les modifications, y compris les ajouts, les suppressions et les suspensions d'utilisateurs vers toutes les sources de données connectées ;
- garantir que les modifications apportées à un attribut ou à des objets sont appropriées, en fonction de la source faisant autorité.

Large connectivité

MIIS domine le marché grâce à ses capacités de connectivité. Une connectivité prête à l'emploi avec la plupart des systèmes d'exploitation réseau (NOS), la messagerie électronique, les bases de données, les annuaires, les applications et même un accès aux fichiers plats, vous permet de vous connecter à une pléthore de sources d'informations d'identité disparates dans votre entreprise. Tout cela sans devoir installer quelque logiciel que ce soit sur les systèmes cibles.

MIIS est livré avec des « agents de gestion » qui vous permettent d'effectuer ensuite une intégration avec de différents types de référentiels. Voici une liste de l'offre de connectivité du serveur MIIS :

• Type de système	• Exemples
• <i>Systèmes d'exploitation réseau et services d'annuaires</i>	• <i>Microsoft Windows NT®, Active Directory®, Active Directory Application Mode, IBM Tivoli Directory Server, Novell eDirectory, SunONE/iPlanet Directory, systèmes X.500 et autres produits de méta-annuaires</i>
• <i>Systèmes de messagerie</i>	• <i>Lotus Notes et Domino, Microsoft Exchange 5.5, 2000 et 2003</i>
• <i>Systèmes d'application</i>	• <i>PeopleSoft, SAP, ERP1, commutateurs téléphoniques et systèmes basés sur XML et DSML</i>
• <i>Systèmes de base de données</i>	• <i>Microsoft SQL Server™, Oracle, Informix, dBase, IBM DB2</i>
• <i>Systèmes basés sur des fichiers</i>	• <i>Fichiers DSMLv2, LDIF, CSV, de texte délimité, à largeur fixe, avec paire attribut-valeur</i> •

¹La connectivité aux systèmes PeopleSoft, SAP et ERP peut être obtenue par connexion aux bases de données sous-jacentes, ou par création d'une interface avec une exportation de fichier plat à partir de ces systèmes.

Les agents de gestion sont prêts à l'emploi dès leur installation. Les entreprises qui doivent étendre ou modifier un agent de gestion particulier le font facilement en utilisant un des nombreux langages supportés.

Microsoft Identity Integration Server 2003 est disponible en deux éditions (MIIS 2003 Enterprise Edition ou Identity Integration Feature Pack pour Microsoft Windows Server Active Directory). Vous pouvez choisir l'édition qui répond le mieux à vos besoins.

Identity Integration Feature Pack (IIFP) pour Microsoft Windows Server Active Directory

Ce Feature pack a été conçu de manière à intégrer des informations d'identité entre plusieurs forêts Active Directory ou entre Active Directory et ADAM (Active Directory Application Mode). IIFP permet à un client d'effectuer les opérations suivantes :

- synchroniser automatiquement les utilisateurs, et leurs informations associées, d'une forêt Active Directory avec des contacts dans d'autres forêts Active Directory ;
- synchroniser uniquement l'utilisateur ou l'unité d'organisation qui le nécessite ;
- synchroniser des groupes locaux, globaux ou universels de domaine entre plusieurs forêts ;
- synchroniser des listes d'adresses globales Exchange 2000 et Exchange 2003 entre plusieurs forêts ;
- synchroniser des informations d'identité entre Active Directory et des instances ADAM ;
- gérer des utilisateurs entre plusieurs forêts.

Le Identity Integration Feature Pack nécessite Microsoft SQL Server 2000 Standard Edition ou Enterprise Edition comme stockage principal, et doit être installé sur un serveur Microsoft Windows Server 2003, Enterprise Edition.

Enterprise Edition

Microsoft Identity Integration Server 2003, Enterprise Edition, fournit une fonctionnalité classique de synchronisation d'annuaires qui permet à un client de synchroniser et de gérer des informations d'identité sur une large gamme de sources de données et de systèmes.

MIIS 2003, Enterprise Edition, nécessite Microsoft SQL Server 2000 Enterprise Edition ou Standard Edition comme espace de stockage principal.

Avantages

Les clients qui déploient MIIS 2003 bénéficieront d'avantages dans différents domaines, dont les suivants :

Réduction des coûts d'administration. MIIS garantit la cohérence et l'intégrité des données dans votre entreprise, en propageant et en répartissant les modifications apportées aux informations d'identité dans vos différents systèmes. Des fortes capacités transactionnelles vous permettent de contrôler comment et quand ces modifications sont gérées et traitées. En transférant et en échangeant les informations d'identité entre des systèmes hétérogènes, vous pouvez dorénavant fournir à vos utilisateurs une représentation cohérente et précise des informations d'identité de votre entreprise.

Intégration des processus d'entreprise. MIIS inclut de puissantes fonctionnalités permettant l'alimentation automatique des comptes du système d'exploitation réseau (NOS), de la messagerie électronique ou d'autres applications dans l'entreprise. L'alimentation automatique des comptes basé sur un annuaire vous permet d'être très efficace, en réduisant le volume de traitement manuel à exécuter sur les différents systèmes lorsque, par exemple, vous recrutez un nouvel employé.

Amélioration de la cohérence et de l'intégrité des données. MIIS applique dans toute l'entreprise la notion de « propriétaire » des informations d'identité. Sans la possibilité d'affecter et de faire respecter cette notion de propriété, les données d'identité peuvent perdre leur intégrité. Par exemple, la définition du poste occupé par un employé est une information qui doit appartenir au système des ressources humaines sinon, l'employé pourrait lui-même modifier son titre à partir du carnet d'adresses de sa messagerie électronique. Lorsque l'entreprise possède plusieurs référentiels d'identité, cette notion de propriété des identités prend encore plus d'importance. MIIS garantit que les données qui ont été malencontreusement modifiées seront restaurées avec la valeur détenue par le système propriétaire de la donnée..

Sécurité accrue. MIIS vérifie que les informations dans l'entreprise sont cohérentes et à jour. Associez à l'intégration des règles métiers de l'entreprise et à la fonctionnalité d'approvisionnement, toute modification du statut d'un employé peut être propagée rapidement et de manière efficace à travers votre entreprise. Par exemple, lorsque des employés quittent l'entreprise, MIIS peut automatiquement suspendre leurs comptes et réduire ainsi les risques de violation de la sécurité.

Vue d'ensemble de l'architecture

L'environnement global de MIIS 2003 est constitué de plusieurs composants dont les principaux sont les sources de données connectées, les agents de gestion, l'espace connecteur et le métaverse.

Sources de données connectées

Une source de données connectée est un annuaire, une base de données ou tout autre entrepôt de données contenant des données d'identité à intégrer au serveur MIIS. Les sources de données connectées peuvent être des annuaires d'entreprise, des annuaires de messagerie électronique, des annuaires de systèmes d'exploitation réseau, des bases de données de ressources humaines ou des données de fichiers plats, tels que LDIF, XML ou du texte délimité.

Agents de gestion

Un agent de gestion relie une source de données connectée spécifique au serveur MIIS. Cet agent de gestion est responsable du déplacement de données entre la source de données connectée et MIIS. Lorsque des données sont modifiées sur MIIS, l'agent de gestion peut aussi exporter les données vers la source de données connectée, de manière à assurer la synchronisation entre cette source et MIIS. En règle générale, il existe au moins un agent de gestion pour chaque annuaire connecté. MIIS 2003, Enterprise Edition, inclut des agents de gestion pour les entrepôts de données d'identité suivants :

- Active Directory
- ADAM (Active Directory Application Mode)
- Fichiers texte de type paires attribut-valeur
- Fichiers de valeurs séparées par des virgules
- Fichiers texte délimités
- DSML (Directory Services Markup Language) 2.0
- Exchange 5.5, « tête de pont » Exchange 5.5
- Synchronisation des listes d'adresses globales Exchange 2000 et Exchange 2003
- Fichiers texte de longueur fixe
- IBM DB2, IBM Tivoli Directory Server
- Format LDIF (LDAP Data Interchange Format)
- Lotus Notes/Domino 4.6/5.0/6.0
- Novell eDirectory
- Annuaire Sun/iPlanet/Netscape 4.x/5.x (avec prise en charge du « journal des modifications »)
- Microsoft SQL Server 2000, SQL Server 7.0
- Domaines Microsoft Windows NT 4
- Oracle 8i/9i
- Prise en charge d'Informix, dBase, ODBC et OLE DB via SQL Server DTS (Data Transformation Services)

Les agents de gestion contiennent des règles qui régissent la façon dont les attributs d'un objet sont mappés, dont des objets d'annuaire connectés sont recherchés dans la base consolidée (métaverse), ainsi que le moment où des objets doivent être créés ou supprimés dans les annuaires connectés.

L'un des principaux avantages de l'implémentation d'agents de gestion de MIIS est qu'aucun logiciel supplémentaire n'a besoin d'être déployé sur les systèmes connectés. Cela entraîne une diminution du coût total de possession, car les composants logiciels supplémentaires n'ont pas besoin d'être gérés sur les différentes plateformes.

Les données d'identité collectées par les agents de gestion sont stockées au sein de MIIS, dans deux espaces de noms logiques : l'espace connecteur et le métaverse.

Espace connecteur (EC)

L'espace connecteur est une zone de stockage, ou zone de mise en attente, utilisée par les agents de gestion pour déplacer des données vers et à partir d'une source de données connectée. Chaque source de données connectée possède sa propre zone logique dans l'espace connecteur, gérée par son agent de gestion correspondant. L'EC est par essence un miroir de la source de données connectée, chaque objet de la source de données connectée disposant d'une entrée correspondante dans l'espace connecteur. L'espace connecteur ne contient pas l'objet de l'annuaire connecté proprement dit, mais un sous-ensemble des attributs de l'objet, tel que défini par les règles de l'agent de gestion.

L'espace connecteur a été conçu de manière à fournir plusieurs avantages qui ne sont pas disponibles sur d'autres solutions.

Il contient l'ensemble des attributs utiles provenant d'un annuaire, d'une base de données ou d'un fichier connecté. Puisque ces données d'identité sont disponibles dans l'espace connecteur, une entreprise peut aisément les analyser sans devoir interroger les sources d'origine. Cela facilite l'accès aux données et élimine le besoin d'un programme entre les différents systèmes d'où proviennent ces informations d'identité, surtout lorsque ces systèmes sont utilisés en production, avec des charges de travail bien définies qui accepteraient mal des requêtes à périodicité aléatoire.

L'espace connecteur assure aussi le suivi de l'« état » d'un objet et de ses attributs. Plus particulièrement, après synchronisation avec le système connecté, l'EC contient l'état en cours de l'objet/attribut, ainsi que le nouvel état (s'il a changé), et tout autre ajout ou suppression s'étant produit dans le système connecté. Cet état étant disponible dans l'EC, il est possible de vérifier la modification et de la confirmer ou de l'infirmer via un programme. Selon les règles métiers qui régissent la façon dont MIIS effectue l'approvisionnement, ces modifications d'état (par exemple suppression d'un employé dans la base de données des ressources humaines) peuvent amener MIIS à exécuter des actions sur les autres systèmes connectés, comme la désactivation d'un compte de messagerie ou d'un compte réseau. MIIS s'assure que ces modifications sont répercutées sur les objets appropriés de l'EC.

L'espace connecteur assure une transparence complète de toutes les opérations concernant un objet, qu'il s'agisse d'ajouts, de suppressions ou d'attributions de nouveaux noms, ou d'opérations au niveau de l'attribut, comme la modification ou la suppression d'une valeur. Un administrateur peut ainsi inspecter, créer un rapport ou envoyer un message électronique sur toute modification, avant qu'elle ne soit vraiment traitée.

Connecteurs et déconnecteurs

Au sein de l'espace connecteur existent deux types d'objets : les objets connecteurs et les objets déconnecteurs.

- Un objet connecteur est lié à un objet dans la métaverse.
- Un objet déconnecteur n'est lié à aucun objet dans la métaverse.

Lorsque vous propagez un nouvel objet à partir d'une source de données connectée vers l'espace connecteur, un objet déconnecteur est automatiquement créé (car il n'est pas encore lié à un objet dans la métaverse). Les règles de projection et de jointure présentes dans l'agent de gestion déterminent si l'objet peut être créé dans la métaverse et s'il peut donc devenir un objet connecteur. En général, nous vous recommandons de projeter des objets dans la métaverse, puis de créer une liaison. Cependant, il est possible que vous ne souhaitiez pas la présence dans la métaverse de certains objets, tels que des comptes administrateur. Si vous désignez ces derniers comme objets déconnecteurs dans l'EC ceux-ci ne peuvent pas être créés dans la métaverse. Par conséquent, ils ne sont pas synchronisés avec les autres annuaires connectés.

L'avantage des objets déconnecteurs est qu'il suffit à un administrateur de marquer un compte comme déconnecteur pour qu'il ne soit plus synchronisé avec d'autres sources connectées. Sans écrire une seule ligne de code, l'administrateur utilise simplement l'interface de gestion MIIS pour transformer un objet connecteur en objet déconnecteur. D'autres solutions nécessitent le codage manuel de chaque exception.

Métaverse (MV)

La métaverse est un ensemble de tables au sein du serveur MIIS, qui contiennent les informations d'identité intégrées (« jointes ») provenant de plusieurs sources connectées. Toutes les informations d'identité concernant une personne spécifique, qui sont stockées dans différentes sources connectées, sont synthétisées dans une entrée unique au sein de la métaverse.

Lorsque vous exécutez un agent de gestion, les modifications apportées aux objets dans les sources connectées sont inscrites dans l'EC, les règles et filtres de déconnecteurs sont ensuite appliqués, puis les données obtenues sont inscrites dans la métaverse si les règles de flux d'importation détectent que ces données doivent être ajoutées au métaverse. La métaverse envoie ensuite ces modifications vers l'EC des annuaires avec lesquels l'objet est synchronisé. Ensuite, leurs agents de gestion respectifs propagent ces modifications vers les annuaires connectés, en fonction des règles définies dans chacun de ces agents

Nouvelles fonctionnalités

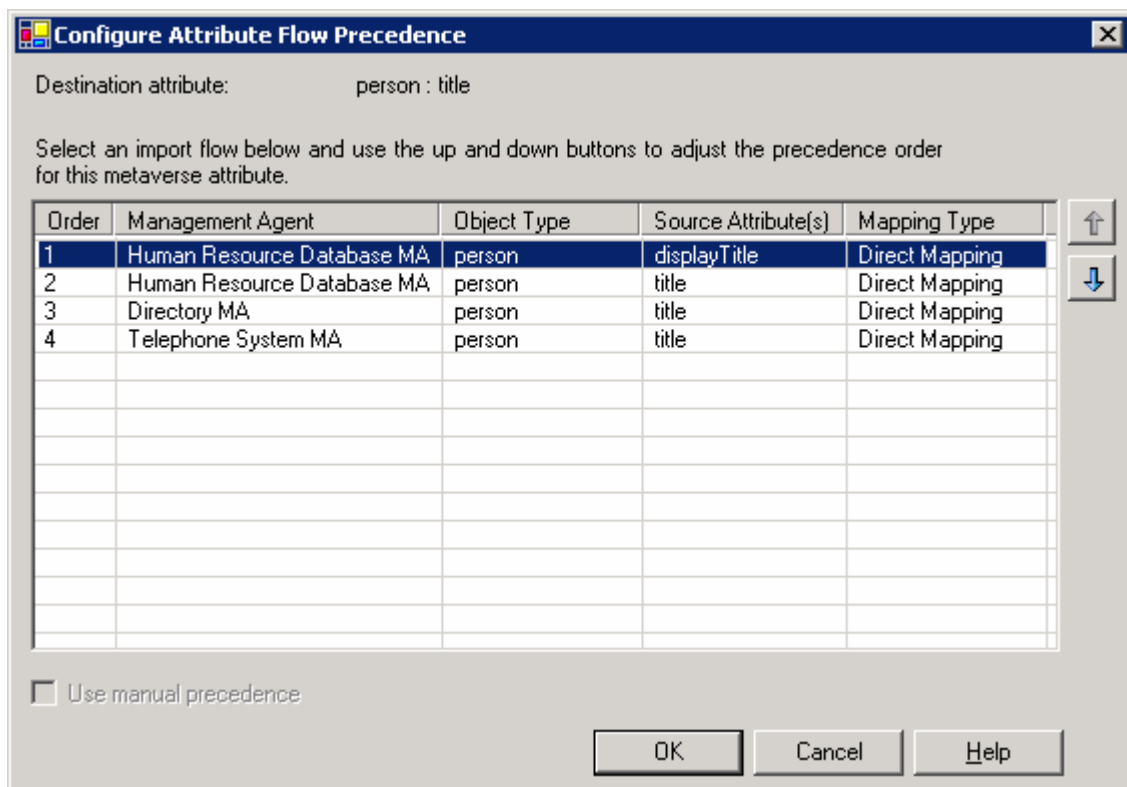
Les sections suivantes fournissent un bref aperçu de certaines des nouvelles fonctionnalités de MIIS 2003.

Flux d'attribut et priorité

Le flux d'attribut est le processus d'envoi des modifications concernant les attributs d'un objet à destination ou en provenance de la métaverse. Les règles de flux d'attribut sont définies par les mappages d'attributs dans l'agent de gestion. Lorsque des modifications apportées aux attributs d'un objet sont détectées dans l'espace connecteur ou dans la métaverse, les attributs sont propagés en fonction des règles de mappage et de leur priorité.

Le flux d'attribut d'importation (de l'espace connecteur vers la métaverse) est défini au niveau de la métaverse et appliqué lors de la réception d'une modification de l'espace connecteur. Le flux d'attribut d'exportation (de la métaverse vers l'espace connecteur) est défini au niveau de l'agent de gestion et appliqué lors de la réception d'une modification dans la métaverse.

Les règles de flux d'attribut sont gérées par ordre de priorité ou de classement d'attribut. Lorsque plusieurs agents de gestion ou sources de données définissent des mappages d'attributs pour le même attribut cible de la métaverse, il convient de définir une source de données prioritaire, afin de maintenir l'intégrité des données.



Dans la capture d'écran ci-dessous, vous voyez que l'attribut « title » sera obtenu via le champ « display title » de l'agent de gestion de la base de données Ressources humaines, et si ce champ est vide, il sera obtenu à partir de l'attribut « title ». Si celui-ci est aussi vide, il sera obtenu de l'attribut « title » de l'agent de gestion de l'annuaire et enfin de l'attribut « title » de l'agent de gestion du système téléphonique. La priorité d'attribut permet aussi à une source de priorité plus élevée de remplacer une source de priorité inférieure. Ainsi, dans cet exemple, bien que le titre puisse être obtenu à partir de l'agent de gestion du système téléphonique, si une valeur apparaît dans l'agent de gestion des

ressources humaines ou de l'annuaire, elle remplacera celle obtenue auprès du système téléphonique. C'est également le cas si le titre affiché dans l'agent de gestion de la base de données des ressources humaines est toujours présent ; il est alors prioritaire sur les autres sources concernant cet attribut.

La priorité d'attribut vous offre la flexibilité de définir plusieurs sources pour un attribut, et de définir une priorité entre ces sources.

La priorité d'attribut ne requiert aucune programmation. Les solutions concurrentes nécessitent une programmation personnalisée pour gérer ce cas courant.

Extensions personnalisées

Si la plupart des tâches d'administration peuvent être accomplies avec le Gestionnaire d'identité, les administrateurs de Microsoft Identity Integration Server 2003 peuvent personnaliser le fonctionnement des agents de gestion et de la métaverse en créant des extensions personnalisées. Les extensions personnalisées se créent à l'aide d'un langage de programmation, tel que Microsoft Visual Basic® .NET, Visual C++®.NET ou Visual C#® .NET. Elles sont implémentées sous forme d'une bibliothèque de classes Microsoft .NET Framework, ou d'une DLL (dynamic link library), puis stockées dans le dossier des extensions du répertoire racine du serveur MIIS.

MIIS 2003 prend en charge les types suivants d'extensions personnalisées :

Extension de règle	Description
Agent de gestion	Une extension personnalisée d'agent de gestion est appliquée aux données lors du transfert vers et à partir d'une source de données connectée à l'espace connecteur. Chaque agent de gestion ne peut posséder qu'un seul jeu d'extension de règles, dans un assemblage unique.
Métaverse	Une extension personnalisée de la métaverse est appliquée aux données pendant leur traitement, lorsqu'un événement provoque une modification en entrée de la métaverse. La métaverse ne peut posséder qu'une extension.

Une extension personnalisée peut être utilisée pour effectuer des actions spéciales, telles que :

Intercepter des exceptions. Certaines exceptions sont autorisées au cours de la synchronisation, tandis que d'autres peuvent entraîner l'abandon de la synchronisation. Vous pouvez utiliser une extension personnalisée pour décider de continuer ou d'abandonner la synchronisation lorsqu'une exception se produit.

Vérifier les valeurs d'attribut. Vous pouvez utiliser une extension personnalisée pour vérifier la valeur d'un attribut.

Créer un nom unique. Lorsqu'une modification intervient sur un objet dans la métaverse, un annuaire connecté peut nécessiter un nouveau nom unique. Vous pouvez utiliser une extension personnalisée afin de créer un nom unique pour un annuaire connecté.

Créer un attribut de nom unique dans la métaverse. Chaque objet dans la métaverse peut nécessiter un attribut de nom unique. Vous pouvez utiliser une extension personnalisée pour vérifier qu'une valeur proposée pour un attribut de nom est unique et pour créer des attributs de nom unique.

Créer une nouvelle entrée d'espace connecteur. Dans le cadre de l'ajout de nouveaux objets à la métaverse, une extension personnalisée peut automatiquement créer de nouvelles entrées dans l'espace connecteur pour les systèmes connectés.

Activer ou désactiver un compte d'utilisateur dans Active Directory. Lorsque le statut d'une personne associée à un compte utilisateur change, les modifications correspondantes doivent être répercutées dans Active Directory. Une extension personnalisée peut activer ou désactiver un compte utilisateur dans Active Directory après une modification dans un système connecté.

Définir un mot de passe initial dans Active Directory. Lorsque vous ajoutez un nouvel utilisateur à la métaverse, vous devez éventuellement définir un mot de passe initial. Vous pouvez définir un mot de passe initial pour un utilisateur via une extension personnalisée.

Il ne s'agit que de quelques exemples de ce que peuvent accomplir des extensions de règles personnalisées.

Visual Studio .NET

Visual Studio® .NET est un ensemble complet d'outils de développement pour la création d'applications Web ASP, de services Web XML, d'applications de bureau et nomades. Il permet aussi de créer des extensions personnalisées pour Microsoft Identity Integration Server 2003. Visual Basic .NET, Visual C++ .NET et Visual C# .NET utilisent tous le même environnement de développement intégré, qui leur permet de partager des outils et facilite la création de solutions en langage mixte. En outre, Visual Studio .NET prend en charge .NET Framework, qui fournit le Common Language Runtime et des classes de programmation unifiées.

Plutôt que de concevoir des extensions à l'aide d'un seul langage (Perl, par exemple) ou par des transformations XSLT/XML complexes, un administrateur MIIS 2003 peut désormais étendre MIIS avec tout langage Visual Studio .NET. En outre, de nombreux partenaires Visual Studio .NET prennent en charge des langages supplémentaires pour les administrateurs qui préfèrent programmer avec Visual Perl, Visual Python, Pascal ou même COBOL. L'environnement de développement intégré de Visual Studio .NET fournit un modèle d'objet facile à comprendre, avec des outils de débogage performants. Un développeur peut aisément définir des points d'arrêt, déboguer des règles, réévaluer des règles, etc.

Solution de sécurité Microsoft .NET Framework

L'extension de MIIS 2003 via l'utilisation de Visual Studio .NET bénéficie automatiquement de l'architecture de sécurité Microsoft .NET Framework. La solution de sécurité .NET Framework est basée sur le concept de code géré, avec des règles de sécurité renforcées par le Common Language Runtime (CLR). La majeure partie du code géré est vérifiée, afin de garantir la sûreté du type et la bonne définition du comportement d'autres propriétés. Dans le code vérifié, une méthode déclarée comme acceptant une valeur de 4 octets, par exemple, rejette une tentative d'accès avec un paramètre de 8 octets, pour cause de type non sûr. La vérification garantit aussi que le flux d'exécution est dirigé uniquement vers des emplacements connus, tels que les points d'entrée de méthode - processus qui supprime l'éventualité que l'exécution saute vers un emplacement arbitraire.

La vérification empêche l'exécution de tout code de type non sûr et permet de repérer de nombreuses erreurs de programmation courantes, avant qu'elles ne posent problème. Les vulnérabilités courantes, telles que les dépassements de mémoire tampon, la lecture de mémoire arbitraire ou la mémoire non initialisée et le transfert arbitraire du contrôle, ne sont plus possibles. Ceci est précieux pour l'administrateur du serveur MIIS, car le code est vérifié avant son exécution. Les développeurs en bénéficient également, car bon nombre des bogues courants qui gênaient jusqu'à présent le développement sont maintenant identifiés et ne peuvent plus causer de dégâts.

Le CLR permet aussi l'exécution de code non géré, mais ce dernier ne bénéficie pas de ces mesures de sécurité. Des autorisations spécifiques sont associées à la possibilité d'appeler du code non géré. En outre, une solide stratégie de sécurité garantit que ces autorisations sont accordées avec prudence. La

charge enrichie du langage XML (Extensible Markup Language), un accès Web simple aux informations de base de données, et des outils d'analyse performants, associés à une disponibilité élevée et à une sécurité stricte, aident les entreprises innovantes à réécrire leurs règles et à se doter de la flexibilité requise pour répondre rapidement aux futurs changements. Les outils qui fournissent des fonctionnalités de développement extrêmement rapides offrent aux entreprises de nouveaux niveaux de flexibilité, ce qui réduit considérablement les délais nécessaires au développement d'applications.

SQL Server 2000 peut être indexé pour effectuer des recherches très rapides, il possède son propre jeu d'outils d'analyse et de maintenance, et il est parfaitement intégré à Windows Server 2003, Enterprise Edition. Vous pouvez installer SQL Server 2000 sur un serveur distant ou sur le serveur qui exécute MIIS.

SQL Server 2000 est utilisé pour stocker toutes sortes d'informations et données MIIS, telles que :

- les données d'attribut à valeurs multiples ;
- les agents de gestion ;
- les extensions personnalisées ;
- les données de l'espace connecteur ;
- les données de la métaverse ;
- les données de liaison entre la métaverse et l'espace connecteur ;
- les profils d'exécution d'agent de gestion ;
- l'historique d'exécution d'agent de gestion ;
- le journal des jointures d'objets.

Haute disponibilité et service de cluster

Outre les performances et l'adaptabilité, les entreprises exigent que les applications qu'elles utilisent soient disponibles. Pour offrir de la haute disponibilité, une solution doit être complète et posséder un service de basculement de type cluster SQL Server 2000.

Le service de cluster à basculement est un processus au cours duquel le système d'exploitation et SQL Server 2000 s'associent pour assurer la disponibilité en cas de panne d'application, de matériel ou d'erreur du système d'exploitation. Le service de cluster à basculement fournit une redondance matérielle, les ressources stratégiques étant automatiquement transférées depuis un ordinateur défaillant vers un serveur de même configuration. Ce service de cluster à basculement permet aussi d'effectuer la maintenance système d'un ordinateur, pendant qu'un autre nœud effectue la tâche. Cet avantage permet aussi de limiter l'immobilisation du système lors d'une maintenance normale.

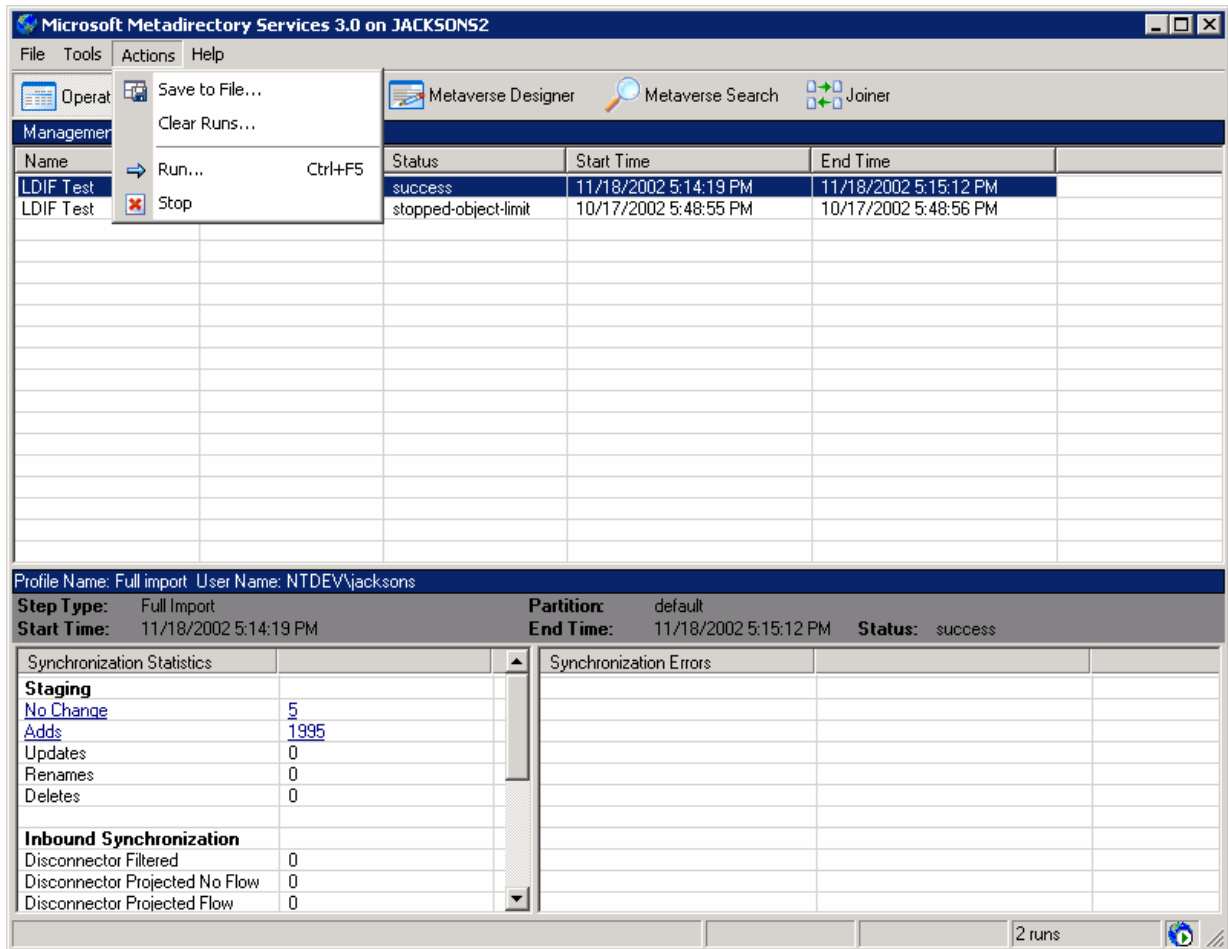
Pour plus d'informations sur SQL Server 2000, visitez <http://www.microsoft.com/sql>.

Gestionnaire d'identité

Le Gestionnaire d'identité (Identity Manager) est l'interface d'administration de MIIS 2003. Il comprend plusieurs composants.

Operations

Utilisez Operations pour suivre l'historique d'exécution de tous les agents de gestion, notamment leur état, leurs erreurs et les statistiques de synchronisation. Vous pouvez aussi déclencher des agents de gestion, modifier la liste d'historiques d'exécution d'un agent de gestion, enregistrer ces historiques dans un fichier et afficher les propriétés d'un objet dans l'espace connecteur.



Le graphique ci-dessus représente une capture d'écran du Gestionnaire d'identité. Remarquez la facilité avec laquelle il est possible d'exécuter ou d'arrêter un agent de gestion. Le volet inférieur gauche signale que lors de la dernière exécution de l'agent de gestion, cinq enregistrements n'ont pas été modifiés et 1995 ont été ajoutés. En cliquant sur les liens « No change » ou « Adds », il vous est facile de voir quels enregistrements n'ont pas été modifiés, ou lesquels ont été ajoutés. L'accès aux informations opérationnelles est très simple dans MIIS 2003.

Management Agents (MA ou Agents de gestion)

Utilisez la vue « Management Agents » pour créer et modifier des agents de gestion, configurer des profils d'exécution pour chaque agent, ou importer et exporter des agents de gestion. Vous pouvez également afficher les statistiques d'importation et les erreurs de la dernière exécution d'un agent de gestion.

Metaverse Designer

Utilisez la vue « Métaverse Designer » pour créer de nouveaux types d'objet ou supprimer des types d'objet de la métaverse. En outre, vous pouvez ajouter, modifier ou supprimer des attributs de n'importe quel type d'objet dans la métaverse. C'est aussi à partir de cet outil que vous spécifiez la priorité du flux d'attribut pour un type d'objet.

Metaverse Search

Utilisez « Métaverse Search » pour créer et modifier des requêtes de recherche en fonction du type d'objet et des valeurs d'attribut. Vous pouvez également importer et exporter des requêtes. À partir des résultats de la recherche, vous pouvez afficher les propriétés d'un objet dans la métaverse.

Joiner

Utilisez la vue « Joiner » pour afficher les objets déconnectés d'un agent de gestion. Joiner vous permet d'associer manuellement un objet déconnecté de l'espace connecteur à un objet de la métaverse, ou pour projeter un objet de l'espace connecteur dans la métaverse. Vous pouvez aussi utiliser Joiner pour déconnecter un objet de la métaverse.

Règles d'agent de gestion

Les agents de gestion peuvent contenir différents types de règles et de filtres qui déterminent la manière dont des objets et leurs attributs sont traités lors de l'exécution de l'agent. Vous pouvez définir ces règles dans l'interface utilisateur ou à l'aide d'une extension personnalisée. Un agent de gestion peut contenir les catégories de règles suivantes.

Catégories de règles d'agent de gestion

Les **mappages d'attributs** définissent les relations entre les attributs d'objets de connecteur et les attributs d'objets de la métaverse. Vous utilisez des mappages d'attributs pour le flux des attributs de l'espace connecteur vers la métaverse, ou pour joindre un objet connecteur à un objet de la métaverse. Vous pouvez spécifier les types de mappages suivants.

Type de mappage	Définition
Mappage direct	Définit une relation directe (une mise en correspondance) entre un attribut source unique et un attribut destination unique. La valeur de l'attribut source est affectée à l'attribut destination qui ne peut pas être modifié par une extension personnalisée. Exemple : le mappage d'employeeID avec userID.
Extension personnalisée	Définit une relation directe entre plusieurs attributs source et un attribut destination unique. Exemple : le mappage de firstName et lastName avec fullName.
Constante	Définit un attribut destination unique et la valeur constante que possédera cet attribut.

Les **règles de jointure** déterminent l'association entre un objet connecteur et un objet de la métaverse. Ces règles sont composées de deux parties vont toujours de pair : critères de recherche et résolution. Les critères de recherche sont toujours constitués d'attributs de la métaverse, classés par priorité. Lorsque vous exécutez un agent de gestion, une recherche de jointure est appliquée à chaque objet de l'espace connecteur qui tente de trouver un objet correspondant dans la métaverse. Lorsqu'une recherche renvoie des résultats, les règles de résolution déterminent si :

- aucun des objets n'est acceptable, auquel cas les critères de recherche suivants sont évalués ;
- un seul des objets est acceptable, auquel cas il est joint à l'objet connecteur ;
- plus d'un des objets est acceptable, auquel cas l'opération de jointure échoue.

Les **règles de projection** sont exécutées après les règles de jointure et déterminent si un agent de gestion projette un objet de l'espace connecteur dans la métaverse, et de quelle manière. Les agents de gestion appliquent les règles de projection aux objets, lorsqu'une jointure a échoué ou n'a pas été configurée. Les règles de projection configurent uniquement la classe d'objet de l'objet projeté. Les attributs sont configurés à l'aide de règles de flux d'attribut. Il existe une règle de projection pour chaque type d'objet de l'espace connecteur ; ce peut être une règle de déclaration ou une règle d'extension personnalisée.

Les **règles déclaratives** définissent un mappage élémentaire des classes d'objets, où les classes sources et cibles sont sélectionnées à partir de l'espace connecteur disponible et des types de classes de la métaverse.

Les **règles d'extension personnalisées** permettent aux utilisateurs d'écrire une extension personnalisée pouvant examiner l'objet source et déterminer s'il est projeté dans la métaverse et, le cas échéant, avec quelle classe d'objet.

Le **filtre de maintien du déconnecteur** (Stay disconnecter filter) détermine si l'agent de gestion tente de joindre ou de projeter un objet déconnecteur de l'espace connecteur dans la métaverse. Il s'agit de la première règle appliquée à un objet de l'espace connecteur. Une fois que vous avez exécuté un agent de gestion, tous les objets présents dans l'annuaire connecté sont représentés dans l'espace connecteur. Cependant, il peut exister certains types d'objets, tels que les comptes d'administration ou les utilisateurs d'un service spécifique de l'entreprise, qu'un administrateur MIIS veut empêcher de se joindre à un objet de la métaverse. Vous pouvez configurer le filtre maintien du déconnecteur pour qu'il bloque la liaison de ces objets avec la métaverse.

Les **règles de révocation** déterminent ce qui arrive à un objet de l'espace connecteur après sa déconnexion d'un objet de la métaverse. Vous pouvez effectuer n'importe laquelle des opérations suivantes :

- transformer l'objet connecteur en objet déconnecteur normal ;
- transformer l'objet connecteur en objet déconnecteur explicite ;
- supprimer l'objet de la métaverse ;
- appeler une extension personnalisée. Cela vous permet d'évaluer l'objet de l'espace connecteur avant de le transformer en déconnecteur ou de le supprimer. En outre, vous pouvez modifier les attributs de l'objet, par exemple définir un compte d'utilisateur comme désactivé.

Metaverse Search

Utilisez la vue « Métaverse Search » pour rechercher les entrées qui existent dans votre métaverse et analyser les valeurs d'attribut fournies par les règles de flux d'attribut en importation configurées dans

les agents de gestion. En plus des attributs, types d'objets et informations d'attribution de nom élémentaire, vous pouvez aisément afficher les entrées liées dans tous les espaces connecteurs pour lesquels l'entrée de la métaverse possède un connecteur. Avec chacune de ces entrées liées, vous pouvez afficher la manière dont le lien a été créé (par exemple via des règles de jointure, des règles de projection, des règles de mise en service, ou en utilisant manuellement l'outil de jointure). Nous l'avons vu, chaque modification apportée à une entrée de la métaverse est tracée et, dans cette vue, il est possible de savoir ce qui a été modifié, par quel agent de gestion, à quelle date et à quelle heure.

Ces actions peuvent être réalisées non seulement via la vue « Métaverse Search » du Gestionnaire d'identité, mais aussi au moyen de l'interface d'automatisation WMI (Windows Management Instrumentation). Ceci permet la création de scripts ou d'applications capables de déterminer l'état de n'importe quelle entrée de la métaverse et de renvoyer l'ensemble des informations utiles sur ces connecteurs. Le scénario intégré de gestion des mots de passe en constitue un excellent exemple. Des applications tierces de gestion de mots de passe peuvent utiliser cette interface WMI pour interroger la métaverse et obtenir une liste des connecteurs associés à un utilisateur. Ainsi, ces applications n'ont pas à gérer des données de jointure distinctes, ce qui représente des coûts et un effort important pour l'utilisateur final.

Gestion de mots de passe

La gestion des mots de passe représente l'un des coûts informatiques les plus importants pour les entreprises. Dans certaines organisations, le coût de la gestion de mots de passe par un service d'assistance technique dépasse 50 % de l'ensemble des coûts d'assistance, d'autres entreprises font état d'un coût encore plus élevé. Il s'agit ici des coûts directs, sans tenir compte de la perte d'efficacité des utilisateurs imputable aux temps morts ou à la nécessité d'aider des collègues, chacun pouvant représenter le double des coûts directs supportés par le service informatique.

MIIS a toujours visé à réduire les coûts associés à l'administration de comptes utilisateur. MIIS 2003 y contribue par l'introduction de nouvelles fonctionnalités de gestion des mots de passe. Ces fonctionnalités incluent :

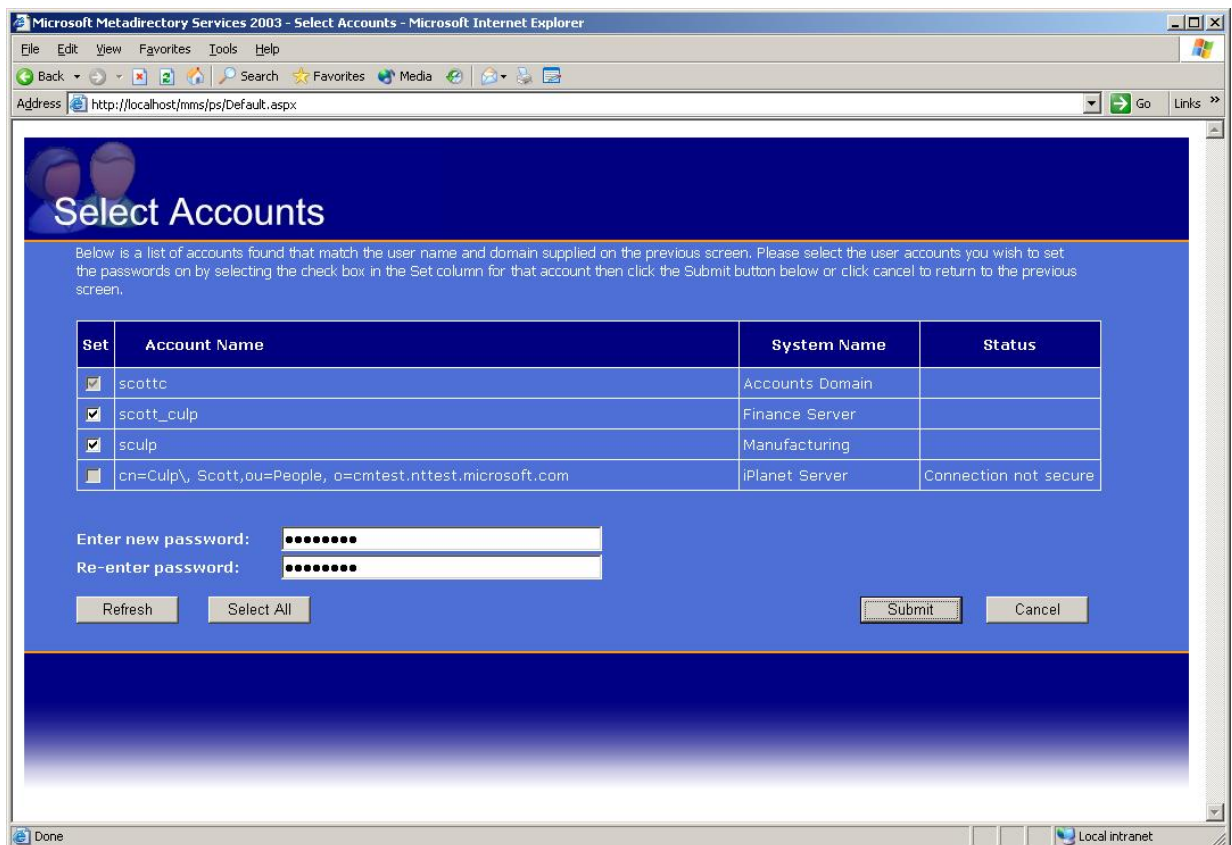
- Un point unique d'administration des mots de passe via une application de services Web qui permet la réinitialisation des mots de passe par le service d'assistance technique ou par l'utilisateur.
- Une API qui fournit des fonctions de gestion des mots de passe.
- L'assistance à la mise en œuvre d'une stratégie de mot de passe et la vérification de la stratégie en cas d'utilisation avec Active Directory.
- Des informations d'audit et d'état claires, via les entrées du journal des événements.
- Des points d'intégration pour des solutions tierces de gestion de mots de passe leur permettant de réduire considérablement, voire de supprimer, les besoins en données d'enregistrement fournies par l'utilisateur.

Dans MIIS 2003, la gestion des mots de passe est effectuée via une API exposée par le fournisseur WMI installé avec MIIS. Les fonctions de cette API serveur permettent à un développeur d'applications de rechercher dans MIIS des entrées spécifiques et de définir ou de modifier, en tant qu'administrateur, le mot de passe des comptes.

Cependant, l'API seule ne résout pas tout. Il existe deux problèmes spécifiques à résoudre : d'abord, le cas où une personne appelle le service d'assistance technique pour la réinitialisation des mots de passe de tous les systèmes gérés par MIIS dans lesquels il possède des comptes ; ensuite, le cas où un utilisateur veut modifier son mot de passe de tous ses comptes système gérés par MIIS. Dans MIIS 2003, deux applications fournissent les fonctions requises pour résoudre ces deux problèmes.

Ce sont des applications Web développées avec ASP.NET et Visual Studio .NET ; elles nécessitent Windows Server et IIS 6.0 pour fonctionner. Visual Studio .NET est nécessaire pour l'ajout de code, mais pas pour le déploiement. Ces applications Web utilisent l'API pour rechercher des comptes d'utilisateur particuliers dans MIIS 2003 et permettent de définir ou de modifier le mot de passe de ces comptes, selon un ensemble de paramètres de configuration modifiables via un fichier de paramètres XML lors du déploiement de l'application. En outre, du code source est fourni pour illustrer l'utilisation de l'API.

En plus du fichier XML avec les paramètres de configuration, MIIS 2003 définit des zones d'appel dans lesquelles les administrateurs peuvent ajouter leur propre logique de post-traitement pour chaque compte concerné et pour l'ensemble du processus. Ainsi, si la définition d'un mot de passe dans un système spécifique échoue, les administrateurs peuvent étendre les fonctions de l'application et entreprendre une action spécifique pour laquelle ils auraient développée un code. De même, une fois les demandes d'initialisation ou de modification satisfaites pour l'ensemble des comptes, les administrateurs peuvent créer du code supplémentaire pour envoyer des confirmations par messagerie électronique, générer des entrées de journal des événements ou définir des mots de passe dans des systèmes qui ne sont pas gérés par MIIS.



Dans l'exemple ci-dessus, l'utilisateur « Scott Culp » utilise un navigateur Web pour modifier son mot de passe sur plusieurs systèmes de son choix.

Mode Aperçu

Tout objet de l'espace connecteur peut être sélectionné et exécuté en mode Aperçu pour vérifier les règles appliquées et savoir comment s'effectue la synchronisation avec les autres annuaires ou sources connectées. Cela ne nécessite aucune modification des informations d'identité. Le mode Aperçu simule simplement les règles à appliquer et la synchronisation avec les différents systèmes. Le mode

Aperçu est particulièrement précieux lors des tests, du développement ou du débogage. D'autres solutions concurrentes laissent à l'administrateur le soin de déboguer du code ou des programmes complexes pour déterminer ce qui se déroule en arrière-plan.

Approvisionnement

L'approvisionnement est le processus de création, de connexion et de déconnexion des objets dans l'espace connecteur, sur la base des modifications apportées à ces objets. L'approvisionnement effectue des actions au niveau de l'objet, telles que :

- la création d'un nouvel objet dans l'espace connecteur et la définition des valeurs initiales d'attribut ne faisant pas partie du flux d'attributs en export;
- la déconnexion de la métaverse des objets de l'espace connecteur ;
- l'attribution d'un nouveau nom et le déplacement de connecteurs existants, c'est-à-dire la modification de l'attribut de nom unique.

L'approvisionnement est implémenté par la création d'une extension personnalisée et son activation. L'extension personnalisée est exécutée dès qu'un objet de la métaverse est modifié.

L'approvisionnement peut être activé ou désactivé à l'aide de la boîte de dialogue Configure Rules Extensions du menu Tools. Une fois les règles d'approvisionnement activées, elles affectent tous les objets de la métaverse. Les règles sont invoquées chaque fois que :

- un attribut a été ajouté, modifié ou supprimé par des règles de flux d'attribut en import ;
- un objet de l'espace connecteur a été joint à un objet de la métaverse ;
- un objet de l'espace connecteur a été projeté dans la métaverse ;
- un objet de l'espace connecteur a été déconnecté ou connecté à l'aide de la vue « Joiner » ;
- un objet de l'espace connecteur a été déconnecté d'un objet de la métaverse, et ce dernier n'a pas été supprimé ;
- les règles sont réévaluées au cours de l'exécution d'un agent de gestion.

L'extension personnalisée de règles d'approvisionnement peut bénéficier des capacités transactionnelles de MIIS 2003. Si un objet de l'espace connecteur est synchronisé avec plusieurs sources de données connectées et que l'une des liaisons échoue, la totalité de l'opération de synchronisation échoue par défaut. L'extension personnalisée peut être rédigée de façon à intercepter les erreurs et à les gérer via un agent de gestion, en :

- appelant une routine pour gérer l'erreur et poursuivre ensuite la synchronisation ; dans ce cas, la synchronisation réussira ;
- envoyant un rapport d'erreur vers MIIS ; dans ce cas, la synchronisation de cet objet échouera ;
- ignorant l'erreur ; dans ce cas, la synchronisation de cet objet échouera.

Si vous effectuez une synchronisation avec une source de données connectée qui utilise une structure hiérarchique, sachez que MIIS 2003 ne gère pas les opérations de conteneur. Par exemple, si vous approvisionnez un objet enfant, MIIS 2003 ne crée pas automatiquement de parent. La gestion d'annuaires hiérarchiques doit être intégralement effectuée dans la source de données connectée.

Révocation

Des règles de révocation sont définies pour chaque agent de gestion ; elles sont appelées lorsqu'un objet de l'espace connecteur est déconnecté d'un objet de la métaverse. Les règles de révocation peuvent être sélectionnées au moyen des propriétés d'agent de gestion dans le Gestionnaire d'identité, ou bien définies à l'aide d'une extension personnalisée.

Les options disponibles dans le Gestionnaire d'identités sont :

- transformer l'objet de l'espace connecteur en déconnecteur ;
- transformer l'objet de l'espace connecteur en déconnecteur explicite ; il s'agit du comportement par défaut.
- supprimer l'objet de l'espace connecteur.

Avec une extension personnalisée, lorsqu'un objet de l'espace connecteur est déconnecté de la métaverse, vous pouvez spécifier différentes actions, telles que :

- spécifier un état de déconnecteur (normal ou explicite) ;
- renommer ou déplacer l'objet de l'espace connecteur (ce qui revient à modifier l'attribut de nom unique) ;
- définir les attributs sur l'objet de l'espace connecteur qui seront exportés (par exemple, vous pouvez définir l'indicateur AccountDisabled sur n'importe quel compte d'utilisateur ayant été déconnecté.)

Les règles de révocation ne sont pas appelées lors de la déconnexion d'un objet à l'aide de la vue Joiner ou du « Connector filter ». Elles le sont lorsque les règles d'approvisionnement déconnectent un objet.

Infrastructure de gestion Windows (WMI, Windows Management Instrumentation)

MIIS 2003 continue à être très largement intégré au journal des événements et à l'Analyseur de performances (PerfMon) de Windows. En outre, dans MIIS 2003, nous avons intégré une interface WMI (Windows Management Instrumentation permettant de relier MIIS 2003 avec des consoles de gestion telles que MOM (Microsoft Operations Manager), HP OpenView, Tivoli et autres consoles tierces. Avec les interfaces de script WMI, un administrateur peut aisément développer des scripts opérationnels et des applications à l'aide de VBS, ou d'autres langages, capables de démarrer, arrêter ou lancer des agents de gestion, de vérifier l'état ou les erreurs ou de générer des rapports de statistiques.

Résumé

Microsoft Identity Integration Server 2003 est la troisième version majeure du produit de gestion du cycle de vie des identités de Microsoft. Cette version reflète plus de cinq années d'expérience en matière de déploiement, chez des centaines de clients représentant des millions d'identités. Fort de cette expérience Microsoft, avec MIIS 2003, a élevé la gestion du cycle de vie des identités jusqu'à des niveaux inégalés, qui la rendent :

- extensible et évolutive, afin de répondre aux exigences les plus contraignantes ;
- plus simple à concevoir, à déployer et à utiliser en minimisant l'intervention de services d'assistance
- utile pour les organisations de toute taille.

L'intégration de MIIS 2003 avec Windows Server 2003 Enterprise Edition, SQL Server 2000 et Visual Studio .NET, permet à une entreprise de bénéficier des dernières avancées en matière de systèmes d'exploitation, d'environnements de programmation, de bases de données évolutives et de sécurité. Qu'il soit intégré à Active Directory ou pas, MIIS 2003 constitue un excellent choix pour les entreprises à la recherche d'un système de gestion du cycle de vie des identités évolutif et fiable.

Liens connexes

Pour plus d'informations, voir les ressources suivantes :

- Microsoft Identity Integration Server 2003 Partners (Partenaires de MIIS 2003, en anglais) à l'adresse <http://www.microsoft.com/windowsserversystem/miis2003/partners/default.aspx>.
- Microsoft Identity Integration Server 2003 Password Management (Gestion des mots de passe dans MIIS 2003, en anglais) à l'adresse <http://www.microsoft.com/windowsserversystem/miis2003/techinfo/planning/miisspass.aspx>.
- Microsoft Identity Integration Server 2003 High Availability Planning (Planification de haute disponibilité de MIIS 2003, en anglais) à l'adresse <http://www.microsoft.com/windowsserversystem/miis2003/techinfo/planning/highavail.aspx>.
- Microsoft Identity Integration Server 2003 home page (Page d'accueil de MIIS 2003, en anglais) à l'adresse <http://www.microsoft.com/miis>.

Pour obtenir les dernières informations sur Windows Server 2003, consultez le site Web de Windows Server 2003, à l'adresse <http://www.microsoft.com/france/windows/windowsserver2003/default.aspx>.