Novell Pilote DirXML® pour Active Directory*

www.novell.com

GUIDE D'IMPLÉMENTATION

103-000261-001

Novell®

Notices légales

Novell exclut toute garantie relative au contenu ou à l'utilisation de cette documentation. En particulier, Novell ne garantit pas que cette documentation est exhaustive ni exempte d'erreurs. Novell se réserve en outre le droit de réviser cette publication à tout moment et sans préavis.

Par ailleurs, Novell exclut toute garantie relative à tout logiciel, notamment toute garantie, expresse ou implicite, que le logiciel présenterait des qualités spécifiques ou qu'il conviendrait à un usage particulier. Novell se réserve en outre le droit de modifier à tout moment tout ou partie des logiciels Novell, sans notification préalable de ces modifications à quiconque.

L'exportation ou la réexportation de ce produit est interdite dès lors qu'elle enfreint les lois et réglementations applicables, y compris, de façon non limitative, les réglementations des États-Unis en matière d'exportation ou la législation en vigueur dans votre pays de résidence.

Brevets en cours d'homologation.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Guide d'implémentation
Octobre 2002

Documentation en ligne : Pour accéder à la documentation en ligne de ce produit (et d'autres produits Novell) et obtenir les mises à jour, consultez le site www.novell.com/documentation.

Marques commerciales de Novell

ConsoleOne est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
DirXML est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
eDirectory est une marque de Novell, Inc.
NDS est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
NetWare est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
Novell est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
Novell Client est une marque de Novell, Inc.
Novell Directory Services est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
ZENworks est une marque de Novell, Inc.

Autres marques commerciales

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.

Tables des matières

À propos de ce guide **7**

1 Présentation du pilote DirXML pour Active Directory **9**

Présentation du pilote . . . 9
Nouvelles fonctionnalités . . . 9
Prise en charge d'Exchange 2000 . . . 10
Prise en charge de schéma . . . 10
Nouveau champ d'authentification sécurisée . . . 10
Configuration par défaut du pilote . . . 11
Flux de données . . . 11

2 Installation du pilote DirXML pour Active Directory **15**

Planification de l'installation . . . 15
Emplacements d'installation . . . 15
Options de sécurité . . . 18
Conditions préalables . . . 23
Installation et mise à niveau . . . 23
Installation du pilote Active Directory (installation locale) . . . 23
Installation du pilote de domaine Active Directory (installation du chargeur distant) . . . 23
Mise à niveau du pilote . . . 25
Configuration après installation . . . 25

3 Personnalisation du pilote DirXML pour Active Directory **33**

Configuration des paramètres du pilote . . . 33
Configuration de l'authentification et des mots de passe du pilote . . . 33
Configuration de la synchronisation des données . . . 34
Activation des boîtes aux lettres Exchange 2000 . . . 35
Gestion des noms de login . . . 37

À propos de ce guide

Ce guide explique comment installer et configurer le pilote DirXML® pour Active Directory.

Il contient les sections suivantes :

- Chapitre 1, « Présentation du pilote DirXML pour Active Directory », page 9

  Cette section décrit les nouvelles fonctionnalités et explique la configuration par défaut du pilote.

- Chapitre 2, « Installation du pilote DirXML pour Active Directory », page 15

  Cette section décrit les procédures d'installation et de mise à niveau, ainsi que les tâches de configuration à exécuter après l'installation.

- Chapitre 3, « Personnalisation du pilote DirXML pour Active Directory », page 33

  Cette section explique comment personnaliser les paramètres du pilote et la synchronisation des données. Elle fournit des exemples de personnalisations courantes.

Documentation supplémentaire

Pour obtenir une documentation sur l'utilisation de DirXML et des autres pilotes DirXML, accédez au (http://www.novell.com/documentation/french/dirxml11a/index.html) site Web de la documentation relative à DirXML.

Mises à jour de la documentation

Vous trouverez la version la plus récente de ce document sur le site Web de la documentation relative au pilote DirXML pour Active Directory. (http://www.novell.com/documentation/french/dirxml_AD/index.html)

Conventions utilisées dans la documentation

Dans la documentation Novell, le symbole « supérieur à » (>) est utilisé pour séparer deux opérations dans une étape de procédure ainsi que deux éléments dans un chemin de références croisées.

Le symbole de marque (®, ™, etc.) indique une marque de Novell. L'astérisque (*) indique une marque commerciale de fabricant tiers.

Commentaires des utilisateurs

Vos commentaires et suggestions sur le présent guide et sur les autres documents qui accompagnent Novell DirXML nous intéressent. Pour nous contacter, envoyez-nous un message électronique à l'adresse suivante : proddoc@novell.com.

1 Présentation du pilote DirXML pour Active Directory

Cette section comprend les rubriques suivantes :

- « Présentation du pilote », page 9
- « Nouvelles fonctionnalités », page 9
- « Configuration par défaut du pilote », page 11

Présentation du pilote

Le pilote DirXML® pour Active Directory* est conçu pour synchroniser les données entre Novell® eDirectory™ et le service Annuaire Microsoft* Active Directory*. La synchronisation est bidirectionnelle; c'est à vous de déterminer si les informations doivent être transmises depuis et vers les deux annuaires, ou si elles doivent être transmises uniquement d'un annuaire vers l'autre.

En outre, il est possible de configurer le pilote afin de synchroniser les données de la boîte aux lettres Microsoft Exchange 2000 dans Active Directory.

Nouvelles fonctionnalités

Le pilote mis à jour prend en charge Exchange 2000 et l'authentification sécurisée.

Prise en charge d'Exchange 2000

Le pilote prend désormais en charge les attributs suivants, qui permettent l'utilisation d'un objet Active Directory comme boîte aux lettres Microsoft Exchange 2000 :

- msExchHomeServerName
- mailNickname
- mail
- msExchMailboxSecurityDescriptor
- authOrig
- uauthOrig

Pour plus d'informations sur l'utilisation de DirXML pour configurer les boîtes aux lettres Exchange 2000, reportez-vous à la section « Activation des boîtes aux lettres Exchange 2000 », page 35.

Prise en charge de schéma

Les fichiers de pilotes préconfigurés sont livrés avec un schéma AD partiel de sorte que vous n'avez pas à lire le schéma AD au démarrage du pilote. Si le schéma partiel inclus n'est pas suffisant, cliquez sur Rafraîchir le schéma d'application dans la page Règle d'assignation de schéma.

Nouveau champ d'authentification sécurisée

Le fichier de pilote préconfiguré comprend un nouveau champ de configuration qui spécifie l'utilisation de l'authentification sécurisée pour le pilote. Une fois que vous avez importé le fichier de pilote préconfiguré, le nouveau champ Utiliser une authentification sécurisée s'affiche dans l'onglet Paramètres du pilote de la page Propriétés du pilote.

Reportez-vous à la section « Options de sécurité », page 18 pour plus d'informations sur les paramètres de sécurité applicables en matière de synchronisation des données DirXML.

Configuration par défaut du pilote

Les notions de base de DirXML sont expliquées dans le manuel DirXML 1.1a Administration Guide (Guide d'administration de DirXML 1.1a). Le guide d'implémentation du pilote DirXML pour Active Directory décrit les mises en oeuvre, les ajouts et les exceptions spécifiques du pilote Active Directory.

Flux de données

Canaux Éditeur et Abonné

Le pilote prend en charge les canaux Éditeur et Abonné :

- Le canal Éditeur lit uniquement les événements d'Active Directory qui concernent les domaines hébergés sur le serveur que vous avez configuré, avant de les envoyer à l'annuaire eDirectory via le moteur DirXML.
- Le canal Abonné détecte les objets de l'annuaire eDirectory ajoutés ou modifiés et répercute ces modifications dans Active Directory.

Lorsque le pilote est configuré pour qu'Active Directory et eDirectory soient autorisés à mettre à jour un attribut spécifique, la modification la plus récente permet de déterminer la valeur de l'attribut.

Règles

Les règles permettent de contrôler la synchronisation des données entre le pilote et eDirectory. Le pilote Active Directory est livré avec un ensemble de règles préconfigurées détaillées dans le Tableau 1, « Règles pour le pilote Active Directory », page 11. Les règles peuvent être personnalisées par l'intermédiaire de Novell iManager, comme l'explique le Chapitre 3, « Personnalisation du pilote DirXML pour Active Directory », page 33.

Tableau 1 Règles pour le pilote Active Directory

Règle	Description
Création	Configurée sur l'objet Pilote. Indique que, pour qu'un objet Utilisateur Active Directory puisse être créé dans eDirectory, les attributs Internet EMail Address et Surname doivent être définis.

Règle	Description
Assignation de schéma	Configurée sur l'objet Pilote. Assigne les propriétés d'utilisateur et de groupe eDirectory suivantes aux attributs d'utilisateur et de groupe Active Directory : Description, description Facsimile Telephone Number, facsimile telephoneNumber Full name, displayName Given Name, givenName Initials, initials Internet EMail Address, mail L, physicalDeliveryOfficeName Member, member Physical Delivery Office Name, l Postal Code, PostalCode Postal Office Box, postOfficeBox S, st SA, streetAddress See Also, seeAlso Surname, sn Telephone Number, telephoneNumber Title, title CN, cn Group Membership, memberOf Owner, managedBy
Concordance	Configurée sur l'objet Pilote. Spécifie que dans eDirectory, un utilisateur est identique à l'utilisateur spécifié dans Active Directory lorsque la valeur de l'attribut Internet Email Address est la même aux deux endroits. Spécifie que dans eDirectory, un groupe est identique au groupe spécifié dans Active Directory lorsque la valeur de l'attribut Internet CN est la même aux deux endroits.

Règle	Description
Placement	Configurée sur les canaux Éditeur et Abonné. Indique que les nouveaux utilisateurs seront nommés d'après la valeur de la partie la plus à gauche du nom distinctif source et placés dans les conteneurs que vous avez définis à l'installation du pilote. Créez ces conteneurs avant de démarrer le pilote. Le placement par défaut crée une arborescence simple dans eDirectory et Active Directory. Pour obtenir un placement hiérarchique, vous devez créer une feuille de style.

2 Installation du pilote DirXML pour Active Directory

Le pilote DirXML® pour Active Directory peut être installé avec d'autres pilotes DirXML pendant l'installation du moteur DirXML. Cette méthode d'installation est décrite dans le manuel DirXML 1.1a Administration Guide (Guide d'administration de DirXML 1.1a) sur le site Web de la documentation relative à DirXML (http://www.novell.com/documentation/french/dirxml11a/index.html).

Le pilote peut également être installé séparément (comme l'explique cette section) en exécutant l'installation de DirXML et en sélectionnant uniquement le pilote Active Directory.

Ce chapitre contient les rubriques d'installation suivantes :

- « Planification de l'installation », page 15
- « Conditions préalables », page 23
- « Installation et mise à niveau », page 23

Planification de l'installation

Avant de démarrer l'installation du pilote, vous devez déterminer l'emplacement et les paramètres de sécurité de l'installation.

Emplacements d'installation

Le pilote doit être exécuté sous Windows* 2000. Toutefois, il n'est pas nécessaire d'installer le moteur DirXML sur la même machine. À l'aide du chargeur distant, vous pouvez séparer le moteur et le pilote, ce qui vous permet d'équilibrer la charge sur une seule machine ou de vous adapter aux instructions de la société.

Le pilote AD peut être exécuté conformément à l'un des scénarios suivants :

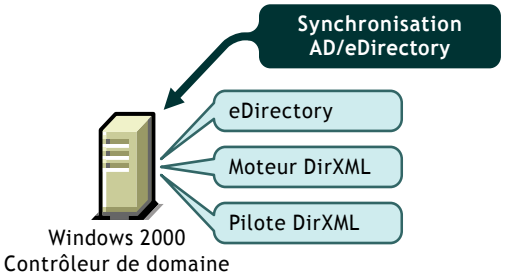
- Serveur unique

  Un contrôleur de domaine Windows 2000 unique héberge eDirectory, le moteur DirXML et le pilote.

  Cette configuration convient aux organisations qui souhaitent faire des économies sur le coût du matériel. Il s'agit également de la configuration la plus performante car le trafic réseau est inexistant entre DirXML et Active Directory.

  Toutefois, l'hébergement de eDirectory et de DirXML sur le contrôleur de domaine augmente la charge totale au niveau du contrôleur, et par conséquent le risque de défaillance de ce dernier. Les contrôleurs de domaine jouant un rôle crucial dans le réseau Microsoft, de nombreuses organisations sont davantage concernées par la rapidité d'authentification du domaine et par les risques associés à une panne du contrôleur de domaine que par le coût d'un matériel supplémentaire.

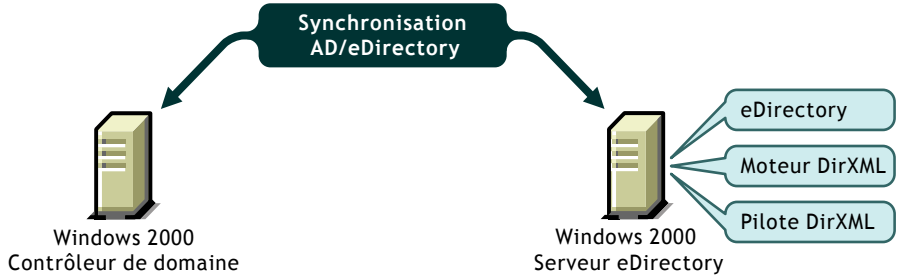
Figure 1 Serveur unique - Installation



- Double serveur

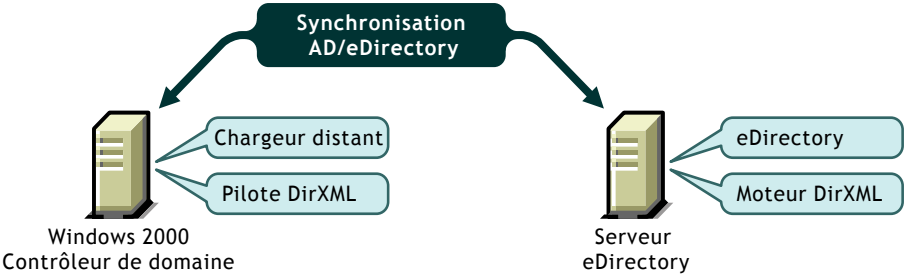
  Il existe deux méthodes d'installation des configurations à double serveur. Dans le cadre de la première configuration, eDirectory, le moteur DirXML et le pilote sont installés sur un ordinateur différent de celui sur lequel se trouve le contrôleur de domaine Active Directory.

Figure 2 Configuration à double serveur (1)



Dans le cadre de la seconde configuration, eDirectory et le moteur DirXML sont installés sur un ordinateur, le pilote et le chargeur distant étant installés sur le contrôleur de domaine Active Directory.

Figure 3 Configuration à double serveur (2)



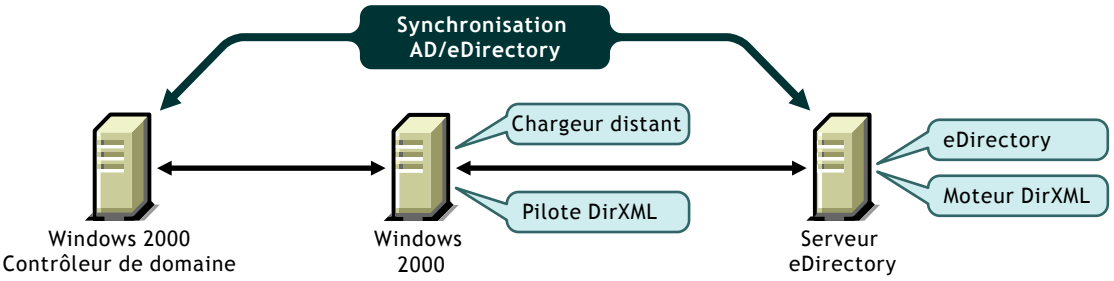
Ces deux configurations suppriment le problème de baisse de performance qu'est susceptible d'entraîner l'hébergement de eDirectory et du moteur DirXML sur le contrôleur de domaine. La première configuration est intéressante si les règles de votre entreprise n'autorisent pas l'exécution du pilote sur le contrôleur de domaine. La deuxième solution est intéressante en cas d'installation de eDirectory et de DirXML sur une plate-forme autre que Windows 2000.

- Triple serveur

  Une configuration à trois serveurs peut être utilisée si vous êtes obligé de recourir à des plates-formes spécifiques ou de respecter des limites de contrôleur de domaine. Cette configuration est plus difficile à mettre en oeuvre, mais elle permet de s'adapter aux contraintes de certaines organisations.

Elle implique d'exécuter eDirectory et DirXML sur un ordinateur, le chargeur distant et le pilote sur un deuxième ordinateur Windows 2000 et le contrôleur de domaine Active Directory sur une troisième machine.

Figure 4 Configuration à triple serveur



Options de sécurité

Le pilote peut être exécuté suivant plusieurs modes de sécurité. Les principaux facteurs à prendre en compte sont l'authentification, le codage et l'utilisation du chargeur distant DirXML. Si vous utilisez le chargeur distant, vous devez considérer les paramètres de sécurité applicables sur le canal Chargeur distant entre DirXML et le pilote, ainsi que les paramètres applicables entre le pilote et Active Directory. Si vous disposez d'une version récente de Windows 2000, vous pouvez également prendre en compte l'option de sécurité qu'est la signature.

En matière de gestion de la sécurité, une simple recommandation est impossible, car le profil de sécurité disponible avec Windows 2000 change en fonction du service pack, de l'infrastructure du serveur DNS, ainsi que des paramètres des règles du domaine et des règles locales sur les serveurs Windows 2000. Les sections suivantes expliquent les options de sécurité et suggèrent des configurations. Veillez attentivement à la sécurité lors de l'implémentation de votre pilote et de la mise à jour des composants.

Paramètres de sécurité

Vous pouvez définir les paramètres d'installation suivants pendant ou après l'installation, dans la page Paramètres du pilote. Pour garantir les meilleures conditions de sécurité en matière de synchronisation des données XML, vous devez comprendre comment les paramètres fonctionnent en relation les uns avec les autres et en relation avec le système d'exploitation.

- **ID d'authentification :** compte utilisé par le pilote pour accéder aux données du domaine. Les formats de nom d'utilisateur valides sont les suivants :

Nom d'utilisateur	Format
Nom de l'utilisateur principal	utilisateur@domaine.com
Nom du domaine	utilisateur
Nom de domaine complet	domaine\utilisateur

  Si vous ne définissez pas d'ID d'authentification, le pilote utilise son identité locale pour son authentification.

- **Mot de passe de l'application :** mot de passe du compte de l'ID d'authentification. Définissez un mot de passe lorsque vous utilisez un ID d'authentification.

- **Contexte d'authentification :** URL LDAP qui code le nom DNS du contrôleur de domaine Active Directory. Par exemple : LDAP://moncontrôleur.mondomaine.com. Vous pouvez utiliser une adresse IP à la place d'un nom DNS, mais ce choix entraîne le retrait du pilote de Kerberos et l'authentification peut échouer.

  Pour configurer une communication sécurisée SSL, ajoutez le numéro de port SSL LDAP au nom d'hôte du serveur DNS (par exemple : LDAP://moncontrôleur.mondomaine.com:636). Sachez que la technologie SSL fonctionne uniquement si vous avez défini une infrastructure à base de certificats et que vous avez importé les certificats sur vos serveurs Windows 2000. Pour plus d'informations, consultez la documentation Microsoft sur les services de certificats.

  Si vous ne spécifiez aucun contexte, le pilote adresse sa connexion à la machine locale.

- **Utiliser une authentification sécurisée :** lorsque la valeur de cette option est Yes, le pilote négocie l'authentification Kerberos ou NTLM vers Active Directory.

  Lorsque la valeur de cette option est No, le pilote utilise une liaison simple LDAP. Une liaison simple n'est généralement pas acceptable car elle transmet les mots de passe en texte clair sur le réseau. Toutefois, si vous avez configuré une communication sécurisée SSL, le mot de passe est envoyé sur un canal codé SSL et est donc sécurisé.

- **Utiliser SSL :** ce paramètre contrôle le codage si vous vous connectez à Active Directory à l'aide du numéro de port SSL LDAP. Par défaut, la valeur du paramètre est No, ce qui signifie que la communication sécurisée SSL est abandonnée lorsque l'authentification de la liaison simple est terminée. Une fois l'authentification effectuée, la communication s'effectue en texte clair.

  Si vous définissez la valeur Yes, le canal SSL est codé pendant toute la conversation. Un canal codé est préférable car le pilote synchronise généralement les informations sensibles. Cependant, le codage ralentit les performances générales de vos serveurs.

  Ce paramètre peut être configuré à la page Paramètres du pilote après l'importation du pilote.

- **Utiliser la signature/le sceau :** cet indicateur active la signature et le sceau de la connexion Active Directory si vous n'utilisez pas le port SSL LDAP. La signature permet de s'assurer que les données ne sont pas interceptées par un ordinateur malveillant. Le sceau code les données de sorte qu'elles ne puissent pas s'afficher sur un moniteur réseau.

  Ce paramètre fonctionne *uniquement* si vous exécutez Windows 2000 SRP1 (Security Rollout Package SP1) ou Windows 2000 SP3, avec Internet Explorer 5.5 SP2 installé sur les deux serveurs Windows 2000. Il active la signature et le codage sur une connexion authentifiée Kerberos ou NTLM.

  Comme pour le mode SSL, ce paramètre n'est pas disponible lors de l'importation initiale; il est défini via la page Paramètres du pilote une fois l'installation terminée.

- **Conserver les références :** ce paramètre indique au pilote d'utiliser une méthode d'authentification mise à jour pour conserver sa connexion à Active Directory. La méthode mise à jour est importante sur les systèmes qui ont été mis à niveau vers Windows 2000 SRP1 (Security Rollout Package 1) ou Windows 2000 SP3. Si vous utilisez une version antérieure de Windows et que vous êtes satisfait du mécanisme d'authentification existant, définissez la valeur No pour ce paramètre.

Options d'authentification

Les trois méthodes d'authentification utilisées par le pilote sont listées ci-dessous. Si vous avez installé un progiciel de sécurité différent dans l'infrastructure SSPI Microsoft, vous disposez d'options supplémentaires.

- **Utiliser l'identité du processus :** ce mode est sélectionné lorsque vous laissez le champ ID d'authentification vide. En général, eDirectory s'exécute en tant que service et vous recevez les droits LSA (Local Service Account) pour Active Directory. Ce niveau de droits fonctionne lorsque vous exécutez le pilote sur votre serveur Active Directory, sauf si une règle ou les paramètres de sécurité Active Directory locaux n'autorisent pas l'accès pour le LSA. Il fonctionne pour les configurations sur un seul serveur.
- **Liaison simple :** transmet le nom d'utilisateur et le mot de passe en texte clair. Cette option doit être utilisée uniquement avec SSL.
- **Authentification Kerberos / NTLM :** NTLM est l'authentification de domaine standard utilisée par Windows NT 4. Cette méthode est moins performante que Kerberos (les clés sont moins longues et l'authentification mutuelle n'est pas prise en charge). Toutefois, l'authentification NTLM, qui a été utilisée pendant des années avec l'authentification de domaine, est acceptable pour la plupart des utilisations.

  Kerberos est la nouvelle authentification Windows 2000 et la méthode préférée pour les futures authentifications avec Microsoft. Elle met en oeuvre un schéma d'authentification mutuelle tiers et est généralement plus performante que NTLM. Le pilote n'est pas averti du schéma d'authentification utilisé.

Configurations recommandées en matière de sécurité

Utilisation du chargeur distant

Étant donné que l'authentification dépend de plusieurs paramètres tels que le support pack Windows 2000, votre infrastructure DNS, les paramètres des règles et de registre, la méthode d'authentification la plus fiable consiste à installer le pilote sur l'ordinateur qui héberge Active Directory, puis d'utiliser le chargeur distant DirXML pour connecter le moteur DirXML, comme illustré dans la Figure 3, « Configuration à double serveur (2) », page 17. Cette configuration sera encore plus performante si vous définissez les paramètres du pilote comme suit.

Contexte d'authentification : Vide

ID d'authentification : Nom de l'utilisateur principal

Mot de passe : Mot de passe pour l'ID d'authentification spécifié

Utiliser une authentification sécurisée : Yes

Utiliser SSL : No

Signature : No

Sceau : No

Conserver les références : Yes

Isolement du contrôleur de domaine

Si vous ne souhaitez pas exécuter le pilote sur votre contrôleur de domaine Active Directory, comme illustré dans la Figure 2, « Configuration à double serveur (1) », page 17 et dans la Figure 4, « Configuration à triple serveur », page 18, définissez les paramètres du pilote comme suit :

Contexte d'authentification : LDAP:// *nomd'hôte*

ID d'authentification : Nom de l'utilisateur principal

Mot de passe : Mot de passe pour l'ID d'authentification spécifié

Utiliser une authentification sécurisée : Yes

Utiliser SSL : No

Signature : No, sauf si vous avez installé le dernier support pack Windows 2000 et Internet Explorer 5.5 SP2 sur les deux serveurs.

Sceau : No, sauf si vous avez installé le dernier support pack Windows 2000 et Internet Explorer 5.5 SP2 sur les deux serveurs.

Conserver les références : Yes

Utilisation de SSL

SSL est une option intéressante si vous avez déjà créé une infrastructure de services de certificats et que vous avez importé les certificats adéquats. Il n'est pas nécessaire d'installer les services de certificats uniquement pour la synchronisation des données DirXML, car les options précédentes garantissent des communications sécurisées.

Contexte d'authentification : LDAP:// *nomd'hôte*:636

ID d'authentification : Nom de l'utilisateur principal

Mot de passe : Mot de passe pour l'ID d'authentification spécifié

Utiliser une authentification sécurisée : No

Utiliser SSL : Yes ou No, selon le niveau de codage souhaité. Choisissez Yes pour l'authentification et les communications sécurisées, No pour l'authentification sécurisée uniquement.

Signature : No
Sceau : No
Conserver les références : Yes

Conditions préalables

- Novell DirXML 1.1a ou version ultérieure
- Windows 2000 Professionnel ou Server avec Service Pack 1 ou 2
- Le serveur doit être un membre du domaine AD
- Internet Explorer 5.5 ou version ultérieure
- Nom DNS du contrôleur de domaine Active Directory
- Novell iManager

  Pour plus d'informations sur l'installation d'iManager, reportez-vous au manuel DirXML 1.1a Administration Guide (Guide d'administration de DirXML 1.1a).

  Remarque : La gestion de DirXML à l'aide de ConsoleOne est expliquée dans la documentation de DirXML1.1 (http://www.novell.com/documentation/french/dirxml11/index.html).

Installation et mise à niveau

Installation du pilote Active Directory (installation locale)

Dans le cadre d'une configuration locale, le pilote est installé sur le même ordinateur que le moteur DirXML. Pour installer le pilote en local, exécutez le programme d'installation de DirXML 1.1 et sélectionnez Moteur et pilotes DirXML > Pilote DirXML pour Active Directory.

Après l'installation, vous devez configurer le pilote comme indiqué à la section « Configuration après installation », page 25.

Installation du pilote de domaine Active Directory (installation du chargeur distant)

Dans le cadre d'une configuration distante, le pilote et le service du chargeur distant sont installés sur un autre ordinateur que celui qui héberge le moteur DirXML. Pour installer une configuration distante :

1. Insérez le CD-ROM de DirXML et cliquez sur Suivant dans l'écran Bienvenue.
2. Dans la page de licence, cliquez sur J'accepte.
3. Dans la boîte de dialogue Composants, sélectionnez Service du chargeur distant de DirXML puis cliquez sur Suivant.
4. Acceptez le chemin d'installation par défaut du chargeur distant, puis cliquez sur Suivant.
5. Sélectionnez les éléments suivants, puis cliquez sur Suivant.
   - Service du chargeur distant DirXML
   - Pilote DirXML pour Active Directory
6. Lisez le résumé du produit, puis cliquez sur Terminer pour installer les fichiers du chargeur distant.
7. Lorsque vous y êtes invité, créez un raccourci.
8. Exécutez l'assistant de configuration du chargeur distant de DirXML à partir de votre bureau.
9. Dans la page Bienvenue, cliquez sur Suivant.
10. Conservez le numéro de port de commande par défaut, puis cliquez sur Suivant.
11. Conservez le nom de fichier de configuration par défaut, puis cliquez sur Suivant.
12. Dans la boîte de dialogue Pilote DirXML, sélectionnez Natif, puis cliquez sur Suivant.
13. Dans la boîte de dialogue Connexion à DirXML, conservez les paramètres de port par défaut.

    Notez le numéro de port pour l'utiliser ultérieurement au cours de la configuration du pilote.
14. Configurez le niveau de trace à 3 afin d'obtenir des données de suivi minimales pour le dépannage, indiquez l'emplacement et le nom du fichier de trace, puis cliquez sur Suivant.
15. Sélectionnez Installer cette instance du chargeur distant comme un service, puis cliquez sur Suivant.
16. Définissez les mots de passe du chargeur distant et de l'objet Pilote.

    Notez les mots de passe pour les utiliser ultérieurement au cours de la configuration du pilote.

17 Lisez le résumé puis cliquez sur Terminer.

18 Lorsque vous y êtes invité, démarrez le service.

Continuez de configurer le pilote comme expliqué à la section « Configuration après installation », page 25.

Mise à niveau du pilote

Pour mettre à niveau le pilote DirXML pour Active Directory, exécutez le programme d'installation de DirXML et sélectionnez Moteur et pilotes DirXML > Pilote DirXML pour Active Directory. Vous pouvez effectuer cette opération pendant l'installation du moteur, ou une fois celui-ci installé.

Le nouveau pilote vient remplacer le précédent tout en conservant sa configuration. Il suffit de confirmer les paramètres lus par le fichier d'importation du pilote.

Aucune configuration n'est nécessaire après l'installation si vous mettez à niveau le pilote. Vous devez toutefois redémarrer le pilote. Pour ce faire, dans Novell iManager, sélectionnez Gestion DirXML > Présentation. Cliquez ensuite sur l'indicateur d'état du pilote dans l'angle supérieur droit de l'icône du pilote, puis cliquez sur Démarrer le pilote.

Configuration après installation

Aucune configuration n'est nécessaire si vous mettez à niveau un pilote existant.

Si vous utilisez le pilote Active Directory pour la première fois, vous devez effectuer les tâches post-installation décrites dans les sections suivantes :

- « Création d'un utilisateur admin », page 26
- « Configuration du pilote », page 27
- « Configuration du pilote pour le chargeur distant », page 29
- « Démarrage du pilote », page 30
- « Migration et resynchronisation des données », page 30
- « Activation du pilote », page 31

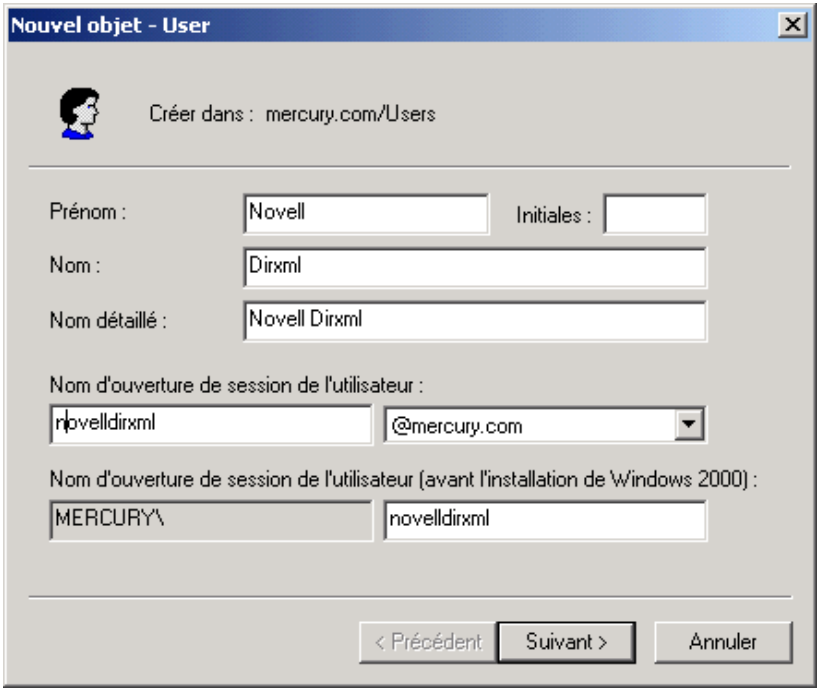
Création d'un utilisateur admin

Nous vous recommandons de créer un utilisateur doté de droits d'administrateur, qui sera utilisé exclusivement par le pilote pour son authentification auprès d'Active Directory. Cela permet de protéger le compte administrateur DirXML de toute modification apportée à d'autres comptes administrateur.

Pour créer un utilisateur admin, procédez comme suit :

1. Cliquez sur Démarrer > Programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory.
2. Dans l'écran Utilisateurs et ordinateurs Active Directory, sélectionnez le conteneur dans lequel vous souhaitez ajouter l'utilisateur, puis cliquez sur Créer un nouvel utilisateur.
3. Entrez le nom complet (qui correspond au nom d'objet Active Directory) et entrez le nom de login (qui correspond au nom d'authentification Active Directory).

Figure 5 Création d'un utilisateur Active Directory pour le pilote



Notez le nom de login avec le domaine pour les utiliser ultérieurement au cours de la configuration du pilote. Par exemple, notez novelldirxml@mercury.com.

4. Cliquez sur Suivant puis définissez le mot de passe pour le nouvel utilisateur. Sélectionnez l'option Le mot de passe n'expire jamais pour qu'aucune règle de mot de passe ne puisse désactiver le pilote de façon inopinée.
5. Cliquez sur Suivant, lisez le résumé, puis cliquez sur Terminer.

Configuration du pilote

L'assistant de création de pilote vous permet d'importer un fichier de pilote Active Directory préconfiguré. Ce fichier crée et configure les objets nécessaires au fonctionnement du pilote.

1. Dans Novell iManager, sélectionnez Gestion DirXML > Créer un pilote.
2. Sélectionnez un ensemble de pilotes.

   Si vous placez ce pilote dans un nouvel ensemble de pilotes, vous devez spécifier un nom d'ensemble de pilotes, ainsi qu'un contexte et un serveur associé.
3. Sélectionnez Importer un pilote préconfiguré à partir du serveur puis sélectionnez le fichier ADDriver.xml.

   Le fichier de pilote préconfiguré est installé sur le serveur Web lorsque vous installez iManager.
4. Au cours de l'importation, vous êtes invité à entrer les informations suivantes :

Champ	Description
Nom du pilote	Nom de l'objet eDirectory à assigner à ce pilote. Étant donné que chaque domaine Active Directory requiert un pilote distinct, vous devez inclure le nom du domaine dans le nom de votre pilote.
ID d'authentification	Utilisez le nom de l'utilisateur principal ou le nom complet de domaine NT. Si vous ne spécifiez aucun utilisateur pour l'authentification, vous devrez utiliser l'identité locale pour négocier l'accès aux données.

Champ	Description
Mot de passe	Entrez le mot de passe pour le compte utilisateur spécifié dans ID d'authentification.
Serveur d'authentification	Laissez le champ Serveur vide pour utiliser la machine locale. Si vous indiquez le port 636 pour l'URL LDAP, vous spécifiez LDAP sur SSL. Cela fonctionne uniquement si une autorité de certification et des certificats sont installés sur votre système local.
Nom du domaine (au format LDAP)	Le pilote requiert des noms de domaine au format LDAP et DNS.
Nom DNS du domaine (au format DNS)	Le pilote requiert des noms de domaine au format LDAP et DNS.
Intervalle d'interrogation	eDirectory envoie les modifications à Active Directory au fur et à mesure qu'elles sont effectuées. La fréquence d'envoi des modifications d'Active Directory vers eDirectory dépend toutefois uniquement de l'intervalle d'interrogation configuré. L'intervalle par défaut est de 15 minutes. **Important :** L'intervalle d'interrogation diminue les performances du système. Nous vous recommandons de définir un intervalle de 1 minute. Vous pourrez l'augmenter par la suite, si les performances du système sont diminuées.
Authentification sécurisée	Si cette option a la valeur Yes, le pilote choisit une négociation pour l'authentification Kerberos ou NTLM entre les serveurs Windows 2000. Si cette option a la valeur No, le pilote utilise une liaison simple LDAP. Relisez la section « Options de sécurité », page 18 pour vous assurer que les paramètres de sécurité que vous configurez répondent à vos besoins.
Conteneur de base dans eDirectory	Indiquez le conteneur en utilisant le format à barres obliques, par exemple acmearbo\est\utilisateurs Si ce conteneur n'existe pas, vous devez le créer avant de démarrer le pilote.

Champ	Description
Conteneur de base dans AD	Indiquez le conteneur à l'aide de noms LDAP séparés par des virgules, par exemple CN=Utilisateurs,DC=MonDomaine,DC=com Vérifiez l'attribut d'assignation de nom utilisé par votre organisation : CN ou UI. Si le conteneur cible n'existe pas, vous devez le créer avant de démarrer le pilote.

5 Une fois l'importation terminée, cliquez sur Oui pour définir des équivalences de sécurité sur le pilote importé.

5a Cliquez sur Ajouter > sélectionnez un objet qui dispose de droits d'administrateur.

5b Cliquez sur Appliquer > Fermer.

6 Cliquez sur Oui pour spécifier des utilisateurs exclus :

6a Cliquez sur Ajouter > sélectionnez les utilisateurs à exclure (l'utilisateur admin, par exemple).

6b Cliquez sur Appliquer > Fermer.

7 Cliquez sur Terminer.

Les objets DirXML nécessaires pour la synchronisation avec Active Directory sont créés.

Configuration du pilote pour le chargeur distant

Si vous avez installé le pilote et le service du chargeur distant sur un ordinateur différent de celui sur lequel est installé le serveur qui héberge le moteur DirXML, vous devez procéder comme suit pour connecter le pilote et le chargeur distant.

1 Dans iManager, cliquez sur Gestion DirXML > Présentation.

2 Localisez le pilote dans son ensemble de pilotes.

3 Cliquez sur l'icône du pilote pour ouvrir la page Présentation du pilote.

4 Cliquez de nouveau sur l'icône du pilote pour ouvrir la page Modifier l'objet.

5 Entrez dans les champs suivants les informations spécifiques à votre environnement :

- Mot de passe de l'objet Pilote
- Paramètres de connexion au chargeur distant
- Mot de passe du chargeur distant

6 Cliquez sur Appliquer.

Démarrage du pilote

1 Dans iManager, sélectionnez Gestion DirXML > Présentation.

2 Localisez le pilote dans son ensemble de pilotes.

3 Cliquez sur l'indicateur d'état du pilote dans l'angle supérieur droit de l'icône du pilote, puis cliquez sur Démarrer le pilote.

La synchronisation s'effectue objet après objet au fur et à mesure des modifications apportées à chacun des objets. Si vous souhaitez une synchronisation immédiate, vous devez lancer cette procédure comme indiqué dans la section suivante, « Migration et resynchronisation des données », page 30.

Migration et resynchronisation des données

DirXML synchronise les données au fur et à mesure des modifications effectuées. Si vous souhaitez synchroniser immédiatement toutes les données, choisissez l'un des scénarios suivants :

- **Migration des données depuis eDirectory :** permet de sélectionner les conteneurs ou les objets que vous souhaitez utiliser pour migrer les données depuis eDirectory vers une application. Lorsque vous migrez des données à partir d'un objet, le moteur DirXML applique à celui-ci toutes les règles de concordance, de placement et de création, ainsi que le filtre Abonné.
- **Migration des données vers eDirectory :** permet de définir les critères utilisés par DirXML pour migrer les données d'un objet depuis une application vers Novell eDirectory. Lorsque vous migrez des données à partir d'un objet, le moteur DirXML applique à celui-ci toutes les règles de concordance, de placement et de création, ainsi que le filtre Éditeur.

- **Synchronisation :** DirXML recherche dans eDirectory et dans l'application cible les objets associés qui ont été modifiés depuis le dernier traitement du pilote, puis génère des événements pour les modifications non traitées. La fonction de synchronisation ne traite pas les objets qui ne comportent pas d'association.

Pour utiliser l'une des options décrites ci-dessus :

1. Dans iManager, sélectionnez Gestion DirXML > Présentation.
2. Recherchez l'ensemble de pilotes qui contient le pilote Active Directory, puis double-cliquez sur son icône.
3. Cliquez sur le bouton de migration approprié.

Activation du pilote

DirXML et les pilotes DirXML doivent être activés dans les 90 jours qui suivent l'installation. S'ils ne le sont pas, ils seront arrêtés. Pendant ou après cette période de 90 jours, vous pouvez activer les produits DirXML dans le cadre d'une licence complète.

Pour activer le pilote, vous devez :

- acquérir des licences DirXML ;
- créer une requête d'activation de produit ;
- soumettre la requête d'activation de produit ;
- installer la référence d'activation de produit envoyée par Novell.

Pour plus d'informations sur l'exécution de ces tâches, reportez-vous à Activation de produit DirXML (http://www.novell.com/documentation/french/dirxml11a/index.html).

3 Personnalisation du pilote DirXML pour Active Directory

Le pilote DirXML® pour Active Directory inclut un exemple de configuration que vous pouvez utiliser comme point de départ de votre déploiement.

La plupart des déploiements DirXML nécessitent de modifier ces exemples. Par exemple, vous devez personnaliser le pilote si vous souhaitez une synchronisation des données dans une seule direction, ou si les attributs que vous synchronisez sont différents de ceux fournis dans l'exemple.

Cette section comprend les rubriques de personnalisation suivantes :

- « Configuration des paramètres du pilote », page 33
- « Configuration de la synchronisation des données », page 34

Configuration des paramètres du pilote

Lorsque vous modifiez les paramètres du pilote, vous adaptez le comportement de celui-ci à votre environnement réseau. Ainsi, il se peut que l'intervalle d'interrogation par défaut du canal Éditeur soit trop court pour la synchronisation. Le rallongement de cet intervalle permettrait d'améliorer les performances réseau tout en assurant une synchronisation appropriée.

Configuration de l'authentification et des mots de passe du pilote

L'authentification donne au pilote les privilèges d'administrateur nécessaires pour mettre les données à jour. Au cours de l'installation du pilote, vous avez été invité à spécifier un utilisateur pour l'authentification. Pensez à utiliser un compte autre qu'Administrateur pour faciliter la gestion des modifications de mots de passe.

Remarque : Aucun équivalent administratif n'est nécessaire si le pilote Active Directory s'exécute sur l'ordinateur sur lequel Active Directory est installé et si les droits sur le contexte de sécurité local sont accordés.

La configuration d'un mot de passe a pour effet de générer une paire de clés publique/privée pour le pilote. Cette paire de clés est requise uniquement en cas d'utilisation du chargeur distant.

1. Dans iManager, cliquez sur Gestion DirXML > Présentation.
2. Localisez le pilote dans son ensemble de pilotes.
3. Cliquez sur l'icône du pilote pour afficher la page de présentation correspondante.
4. Cliquez de nouveau sur l'icône pour afficher la page Modifier l'objet.
5. Recherchez le champ Authentification et entrez les informations d'authentification suivantes :
   - Nom de l'utilisateur principal, dans le champ ID d'authentification (par exemple, entrez Administrateur@domaine.com)
   - Contrôleur de domaine avec lequel vous effectuez la synchronisation, dans le champ Contexte d'authentification (par exemple, entrez LDAP://Contrôleur domaine.domaine.com)

     Vous pouvez choisir de ne pas entrer le contexte et l'ID d'authentification si vous exécutez le module d'interface ADDRIVER.DLL sur la machine qui héberge votre domaine Active Directory.
   - Mot de passe d'authentification

     Vous devez modifier le mot de passe de ce champ chaque fois que votre mot de passe administrateur change.
6. Cliquez sur Appliquer.

Configuration de la synchronisation des données

La puissance de DirXML réside essentiellement dans la gestion des données partagées. Cette section décrit certaines personnalisations courantes du pilote Active Directory, notamment

- « Activation des boîtes aux lettres Exchange 2000 », page 35
- « Gestion des noms de login », page 37

Activation des boîtes aux lettres Exchange 2000

Vous pouvez activer les boîtes aux lettres Exchange 2000 pour un objet Active Directory. Pour ce faire, ajoutez plusieurs attributs pour définir le serveur Exchange destiné à héberger la boîte aux lettres, le nom de la boîte aux lettres et les personnes habilitées à l'afficher. Vous pouvez également configurer la boîte aux lettres de façon à limiter la réception à un ensemble connu d'expéditeurs de messages et à rejeter automatiquement les messages provenant d'autres expéditeurs. Le pilote prend en charge les syntaxes d'attributs correspondantes, mais ne crée pas automatiquement les attributs à votre place. Vous devez créer ces attributs dans vos propres feuilles de style.

Attributs Exchange

Vous pouvez générer des attributs Exchange pour les événements d'ajout sur le canal Abonné. Il est en revanche plus difficile d'autoriser un utilisateur à utiliser Exchange sur le canal Abonné ou de générer des boîtes aux lettres pour des objets déjà associés. Cette section liste les attributs Exchange pris en charge par le pilote DirXML pour Active Directory.

La façon dont vous générez les attributs de la boîte aux lettres Exchange et les feuilles de style que vous utilisez dépendent de vos propres règles de déploiement. Les attributs définis dans cette section se trouvent dans l'espace de nom de l'application. La règle d'assignation de schéma DirXML convertit les attributs que vous spécifiez entre l'espace de nom de l'application et l'espace de nom eDirectory et passe outre tout autre attribut qui n'a pas été modifié.

msExchHomeServerName

Nom du serveur Exchange destiné à héberger la boîte aux lettres. Le nom du serveur se présente au format Exchange hérité sous la forme d'un nom distinctif complet avec des barres obliques. Par exemple : /O=Hyperion/OU=Premier groupe administratif/CN=Configuration/CN=serveurs/CN=TIMS-DELL

Pour rechercher le nom hérité :

1. Exécutez la commande suivante pour obtenir le nom de votre domaine et d'autres informations racine :

```
ldifde -f domain.txt -d "" -r "(objectClass=*)" -
p Base -l
"defaultNamingContext,configurationNamingContext,
rootDomainNamingContext,dnsHostName" -s
```

```
myserver.mydomain.com -a
administrator@mydomain.com mypassword
```

Le résultat obtenu doit ressembler à ce qui suit :

```
dn:

changetype: add

defaultNamingContext: DC=td,DC=provo,DC=novell,DC=com

configurationNamingContext:
CN=Configuration,DC=td,DC=provo,DC=novell,DC=com

rootDomainNamingContext: DC=td,DC=provo,DC=novell,DC=com

dnsHostName: tims-dell.td.provo.novell.com
```

2. Remplacez le chemin dans l'option -d par la valeur de configurationNamingContext listée dans les résultats.

   Par exemple :

   ```
   ldifde -f exchservers.txt -d
   "cn=configuration,dc=mydomain,dc=com" -r
   "(objectClass=msExchExchangeServer)" -p Subtree -l
   "legacyExchangeDN" -s myserver.mydomain.com -a
   administrator@mydomain.com mypassword
   ```

   Le résultat obtenu doit ressembler à ce qui suit :

   ```
   dn: CN=TIMS-DELL,CN=Servers,CN=First Administrative
   Group,CN=Administrative Groups,CN=Hyperion,CN=Microsoft
   Exchange,CN=Services,CN=Configuration,DC=td,DC=provo,DC=
   novell,DC=com
   changetype: add
   legacyExchangeDN:
    /o=Hyperion/ou=First Administrative Group/
   cn=Configuration/cn=Servers/cn=TIMS- DELL
   ```

3. Utilisez les informations de legacyExchangeDN pour l'attribut msExchHomeServerName.

mailNickname

Nom local de l'utilisateur. Vous pouvez choisir l'attribut CN de l'utilisateur.

mail

Nom complet de l'utilisateur, qui comprend le domaine tel que utilisateur@domaine.com.

msExchMailboxSecurityDescriptor

Attribut qui contrôle l'accès à la boîte aux lettres. Il s'agit d'une liste de contrôle d'accès Active Directory standard. Le module d'interface ADDRIVER.DLL actuel ne traite pas la syntaxe ACL en général, mais a été mis à jour pour traiter spécifiquement cet attribut. Vous pouvez considérer cet attribut comme étant de type « état » (booléen); le fichier DLL génère alors une liste de contrôle d'accès qui accorde les droits appropriés à l'utilisateur.

authOrig

Liste des expéditeurs autorisés à envoyer des messages vers cette boîte aux lettres. Si vous définissez cet attribut, les expéditeurs qui ne se trouvent pas dans cette liste sont rejetés.

unauthOrig

Liste des expéditeurs qui ne sont pas autorisés à envoyer des messages vers cette boîte aux lettres.

Gestion des noms de login

Dans eDirectory, votre nom de login est votre nom distinctif complet tel que jbrun.ventes.ny.acme. Dans Active Directory, vous disposez de deux noms de login : votre nom de domaine NT, tel que jbrun, et votre nom d'utilisateur principal, tel que jbrun@acme.com.Vous pouvez utiliser l'un ou l'autre pour vous loguer. Dans Active Directory, vous êtes également identifié par un RDN (Relative Distinguised Name - nom distinctif relatif) généré par l'application utilisée pour créer votre compte.

Dans la configuration par défaut du pilote Active Directory, les valeurs de RDN sont synchronisées. Cela peut être gênant si vous utilisez la console MMC (Microsoft Management Console) pour créer ou pour gérer des comptes dans Active Directory. La console MMC génère des RDN sous la forme Nom, Prénom. Votre nom de login eDirectory devient alors *nom\, prénom.contexte*, c'est-à-dire un nom complexe qui peut poser problème. Pour éviter d'assigner un nom de login aussi complexe, créez une transformation d'événement du canal Éditeur qui supprime les événements de réassignation de nom.