Novell Identity Manager

3.0

www.novell.com

GUIDE D'ADMINISTRATION

13 décembre 2005

Novell®

Mentions 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.

Tous les produits ou informations techniques fournis dans le cadre de ce contrat peuvent être soumis à des contrôles d'exportation aux États-Unis et à la législation commerciale d'autres pays. Vous acceptez de vous conformer à toutes les réglementations de contrôle des exportations et à vous procurer les licences requises ou la classification permettant d'exporter, de réexporter ou d'importer des biens de consommation. Vous acceptez de ne pas procéder à des exportations ou à des réexportations vers des entités figurant sur les listes d'exclusion d'exportation en vigueur aux États-Unis ou vers des pays terroristes ou frappés d'embargo par la législation d'exportation des États-Unis. Vous acceptez de ne pas utiliser les produits livrables pour le développement prohibé d'armes nucléaires, de missiles ou d'armes chimiques et biologiques. Pour plus d'informations sur l'exportation du logiciel Novell, reportez-vous au site www.novell.com/info/exports/. Novell décline toute responsabilité pour toute autorisation d'exportation refusée.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
États-Unis
www.novell.com

Documentation en ligne : afin d'accéder à la documentation en ligne de ce produit et des autres produits Novell, ainsi que des mises à jour, visitez le site suivant : www.novell.com/documentation.

Marques Novell

eDirectory est une marque de Novell, Inc.
exteNd est une marque de Novell, Inc.
exteNd Director est une marque de Novell, Inc.
GroupWise est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
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.
NMAS est une marque de Novell, Inc.
Novell est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
Novell Certificate Server est une marque de Novell, Inc.
Novell Client est une marque de Novell, Inc.
SUSE est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.

Éléments tiers

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

Tables des matières

À propos de ce guide

Novell® Identity Manager 3, anciennement DirXML®, est un service de partage des données et de synchronisation qui permet à des applications, annuaires et bases de données de partager des informations. Il relie des informations dispersées et permet d'établir des stratégies qui régiront les mises à jour automatiques de certains systèmes en cas de changement d'identités. Identity Manager est à la base du provisioning des comptes, de la sécurité, du libre-service utilisateur, de l'authentification, des autorisations, des workflows automatisés et des services Web. Il permet d'intégrer, de gérer et de contrôler vos informations d'identité distribuées, de manière à proposer les bonnes ressources aux bonnes personnes.

Ce guide présente les technologies Identity Manager et en décrit les fonctions d'administration et de configuration.

Indication

Nous souhaiterions connaître vos commentaires et suggestions sur ce guide et les autres documentations fournies avec ce produit. Au bas de chaque page de la documentation en ligne figure une zone User Comments (Commentaires des utilisateurs) que vous pouvez utiliser à cet effet. Vous pouvez également accéder à http://www.novell.com/documentation/feedback.html et entrer vos commentaires à cet emplacement.

Mises à jour de la documentation

Vous trouverez la version la plus récente de ce document sur le site Web de la documentation relative à Identity Manager (http://www.novell.com/documentation).

Documentation complémentaire

Afin d'obtenir des instructions sur l'installation et la mise à niveau de Identity Manager, reportez-vous au *Identity Manager 3.0 Installation Guide (Guide d'installation Identity Manager 3.0)*.

Afin d'obtenir des informations sur les stratégies et sur les filtres Identity Manager, reportez-vous au *Policy Builder and Driver Customization Guide (Guide de création des stratégies et de personnalisation des pilotes)*.

Afin d'obtenir des informations sur la conception et les pratiques de déploiement, reportez-vous au *Designer for Identity Manager 3:Administration Guide (Guide d'administration de Designer pour Identity Manager 3)*.

Afin d'obtenir des informations sur les stratégies, le libre-service et la gestion des mots de passe, reportez-vous au Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe) (http://www.novell.com/documentation).

Pour savoir comment utiliser les pilotes Identity Manager, reportez-vous au site Web de la documentation des pilotes Identity Manager (http://www.novell.com/documentation/idmdrivers/index.html).

Conventions typographiques

Dans cette documentation, 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.

Un symbole de marque (®, ™, etc.) indique une marque de Novell. Un astérisque (*) indique qu'il s'agit d'une marque commerciale d'un fabricant tiers.

Présentation de l'architecture Identity Manager 3.0

1

Identity Manager se compose de trois éléments essentiels.

1.1 Changements terminologiques par rapport aux versions précédentes

Si vous n'avez jamais utilisé DirXML® 1.1a ou Identity Manager 2.0, il est inutile que vous consultiez cette section.

Sous DirXML 1.1a, le terme « règle » décrivait, selon le contexte, un ensemble de règles, chacune des règles composant cet ensemble et les conditions et opérations de chaque règle. Cette ambiguïté générait une certaine confusion lorsque le contexte n'était pas clair.

Dans Identity Manager 2, le terme « stratégie » remplace le terme « règle », et décrit désormais une transformation de haut niveau. À présent, vous définissez un ensemble de stratégies, dont chacune est composée d'une ou de plusieurs règles. Le terme « règle » décrit maintenant un jeu de conditions et d'opérations.

Le tableau suivant indique les changements terminologiques intervenus entre DirXML 1.1a et Identity Manager 2.x.

Tableau 1-1 *Changements terminologiques entre DirXML 1.1a et Identity Manager 2.x*

Élément décrit	Terminologie DirXML 1.1a	Terminologie Identity Manager 2.x
Ensemble de transformations	Règle	Ensemble de stratégies
Une transformation au sein d'un ensemble	Règle	Stratégies
Les conditions et opérations dans une transformation donnée	Règle	Règle

Le tableau suivant indique les changements terminologiques intervenus entre Identity Manager 2.x et Identity Manager 3.0.

Tableau 1-2 *Changements terminologiques entre Identity Manager 2.x et Identity Manager 3.0*

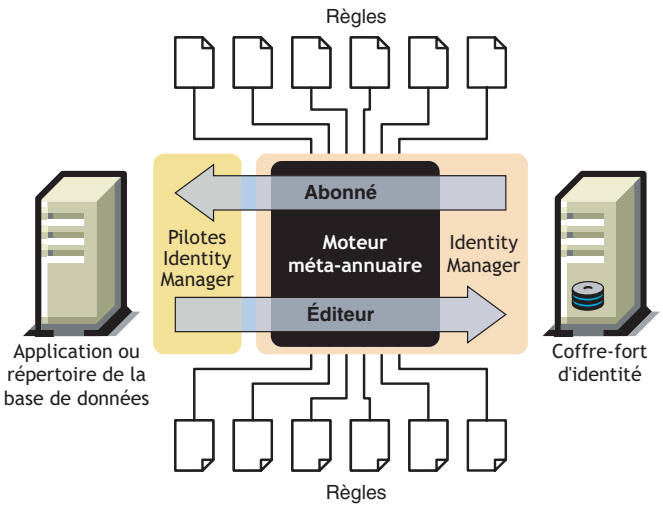
Élément décrit	Terminologie Identity Manager 2.x	Terminologie Identity Manager 3
Produit	DirXML	Identity Manager
Serveur sur lequel est installé le produit	Serveur DirXML	Serveur méta-annuaire
Serveur au sein de l'application ou de la base de données avec laquelle les données sont synchronisées	Serveur du système DirXML connecté	Serveur de système connecté
Emplacement de stockage des objets	eDirectory™	Coffre-fort d'identité
Composant de traitement	Moteur DirXML	Moteur méta-annuaire

1.2 Identity Manager

Identity Manager se charge de la synchronisation des données entre le coffre-fort d'identité et le système connecté, qui se compose d'applications, d'annuaires, de bases de données ou de fichiers.

Identity Manager comprend plusieurs composants. L'illustration ci-dessous présente les composants de base, ainsi que les relations qui existent entre eux :

Figure 1-1 *Composants Identity Manager*



Le moteur méta-annuaire est le module central de l'architecture Identity Manager. Il constitue l'interface permettant aux pilotes Identity Manager de synchroniser les informations avec le coffre-fort d'identité, et permet même la connexion et le partage des données entre des systèmes de données hétérogènes.

Le moteur méta-annuaire traite les données et les événements du coffre-fort d'identité au format XML. Il utilise un processeur de règles et un moteur de transformation de données pour manipuler les données passant d'un système à l'autre.

1. Il lit le filtre pour tous les pilotes Identity Manager.

2. Il enregistre les pilotes associés aux événements appropriés du coffre-fort d'identité.
3. Il filtre des données en fonction des spécifications de chaque pilote.
4. Il définit un cache pour les événements du coffre-fort d'identité transmis via chaque pilote.

Lors de son initialisation, le coffre-fort d'identité effectue les tâches suivantes.

- Une fois qu'un événement est mis en cache, le pilote qui possède le cache lit cet événement.
- Le pilote reçoit alors des données du coffre-fort d'identité au format eDirectory natif, les convertit au format XDS (vocabulaire XML utilisé par Identity Manager et pouvant être transformé par une stratégie), puis envoie l'événement au moteur méta-annuaire. Celui-ci lit toutes les stratégies du pilote du système connecté et crée des données au format XML conformes à ces stratégies avant de les envoyer au pilote du système connecté. Il envoie ensuite les données au système connecté. Pour plus d'informations sur les stratégies, reportez-vous à la section « Introduction to Policies (Introduction aux stratégies) » du *Policy Builder and Driver Customization Guide (Guide de création des stratégies et des personnalisation des pilotes)*.
- La partie Éditeur du pilote rassemble et envoie les mises à jour du système connecté au coffre-fort d'identité. Lorsque le pilote du système connecté est informé des modifications apportées aux informations partagées par les deux systèmes, il rassemble ces informations et vérifie qu'elles ont été filtrées pour donner l'ensemble de données voulu. Il convertit ensuite ces données au format XDS, puis les transmet au moteur.

1.2.1 Moteur méta-annuaire

Le moteur méta-annuaire se compose de deux éléments : l'interface eDirectory et le moteur de synchronisation.

Interface eDirectory

L'interface eDirectory (intégrée au moteur méta-annuaire) est utilisée pour la détection des événements qui se produisent dans eDirectory. Cette interface garantit la transmission d'événements à Identity Manager grâce à l'utilisation du cache d'événements. Elle prend en charge le chargement de plusieurs pilotes. Autrement dit, même si une seule instance Identity Manager s'exécute pour le serveur eDirectory concerné, elle peut communiquer avec plusieurs systèmes connectés. La détection de retour en boucle (loopback) est intégrée à cette interface afin d'éviter la survenue d'événements en boucle entre le coffre-fort d'identité et le système connecté. Malgré cette protection, les développeurs sont encouragés à créer également des systèmes de détection de retour en boucle dans chaque pilote de système connecté.

Moteur de synchronisation

Le moteur de synchronisation applique les stratégies Identity Manager à chacun des événements qui lui sont présentés. Les stratégies sont créées dans le Générateur de stratégies à partir du script DirXML. Le Générateur de stratégies permet de créer des stratégies dans l'interface graphique plutôt qu'avec des documents XML ou des feuilles de style au format XSLT. Vous pouvez toutefois utiliser des feuilles de style, mais le Générateur de stratégies est plus simple à utiliser. Pour plus d'informations sur le Générateur de stratégies ou le script DirXML, reportez-vous au *Policy Builder and Driver Customization Guide (Guide de création des stratégies et de personnalisation des pilotes)*.

Le moteur de synchronisation applique chaque type de stratégie au document source. La capacité à apporter ces modifications constitue l'un des atouts majeurs de Identity Manager. Les données sont

transformées en temps réel, à mesure qu'elles sont partagées entre le coffre-fort d'identité et les systèmes connectés.

1.2.2 Fichiers de configuration du pilote

Les configurations du pilote sont des fichiers XML préconfigurés, inclus dans Identity Manager. Vous pouvez utiliser les assistants de iManager et du Designer pour importer ces fichiers de configuration.

Ces configurations de pilote contiennent des exemples de stratégies. Elles ne sont pas destinées à être utilisées en production, mais elles peuvent vous servir de modèles à modifier.

1.2.3 Cache d'événements de Identity Manager

Tous les événements générés par l'intermédiaire de eDirectory sont conservés dans un cache d'événements jusqu'à ce qu'ils soient traités avec succès. Cela garantit qu'aucune donnée n'est perdue suite à une erreur de connexion, à une perte de ressources système, à la non-disponibilité d'un pilote ou à tout autre incident réseau.

1.2.4 Module d'interface (shim) pilote

Le module d'interface pilote est utilisé comme canal d'informations entre le système connecté et le coffre-fort d'identité. Il est écrit en langage Java, C ou C++.

La communication entre le moteur méta-annuaire et le module d'interface pilote se fait sous forme de documents XML dans lesquels sont décrits les événements, les requêtes et les résultats. Le module d'interface pilote est généralement appelé « pilote ». Il s'agit du canal permettant de transmettre les informations entre le coffre-fort d'identité et le système connecté.

Le module d'interface pilote prend en charge les événements suivants :

- Ajouter (création)
- Modifier
- Effacer
- Renommer
- Déplacer
- Interroger

Le module d'interface pilote doit également prendre en charge une fonction de requête définie qui permet à Identity Manager d'interroger le système connecté.

Lorsqu'un événement se produit dans le coffre-fort d'identité et qu'il génère une opération au niveau du système connecté, Identity Manager crée un document XML qui décrit l'événement et le soumet au module d'interface pilote via le canal Abonné.

Lorsqu'un événement survient au niveau du système connecté, le module d'interface pilote génère un document XML dans lequel cet événement est décrit. Il soumet ensuite le document XML à Identity Manager via le canal Éditeur. Une fois l'événement traité par les stratégies de l'Éditeur, Identity Manager demande au coffre-fort d'identité d'exécuter les opérations appropriées.

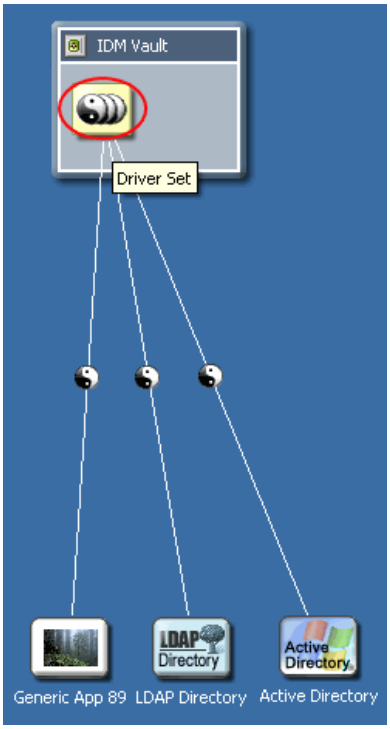
1.2.5 Ensemble de pilotes

Un ensemble de pilotes est un objet Conteneur qui regroupe les pilotes Identity Manager. Un ensemble de pilotes peut être associé à un serveur à la fois. Par conséquent, tous les pilotes en cours d'exécution doivent être regroupés au sein du même ensemble.

L'objet Ensemble de pilotes doit exister dans une réplique en lecture/écriture sur chacun des serveurs qui l'utilisent. Il est donc recommandé de créer des partitions pour l'ensemble de pilotes. Ainsi, lorsque des répliques d'utilisateurs sont déplacées vers un autre serveur, les objets Pilote ne le sont pas.

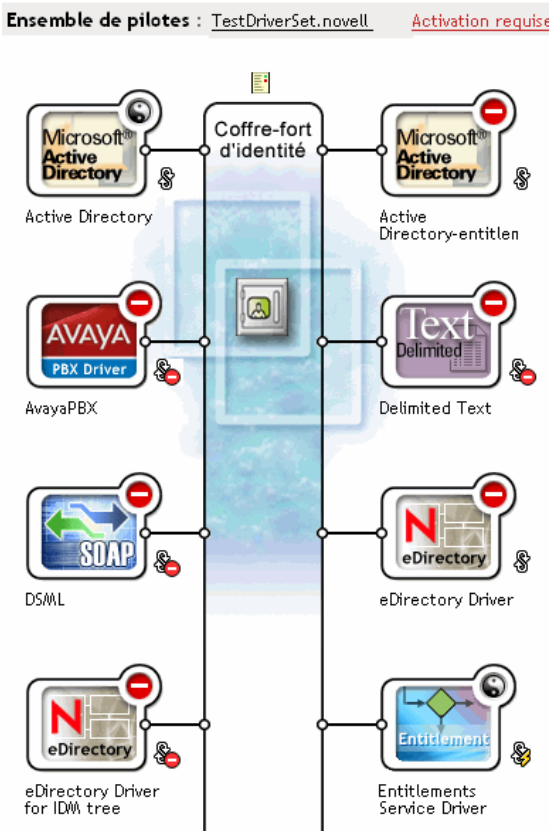
L'illustration suivante montre comment l'ensemble de pilotes apparaît dans Designer.

Figure 1-2 *Ensemble de pilotes dans Designer*



L'illustration suivante montre comment l'ensemble de pilotes apparaît dans iManager.

Figure 1-3 *Ensemble de pilotes dans iManager*



Depuis l'espace Modeler du Designer (reportez-vous à la Figure 1-2 page 13, plus haut) ou la page Présentation de iManager (reportez-vous à la Figure 1-3 page 14, plus haut), vous pouvez effectuer les opérations suivantes :

- Affichage et modification de l'ensemble de pilotes et de ses propriétés
- Affichage des pilotes au sein de l'ensemble de pilotes
- Modification de l'état d'un pilote
- Association d'un ensemble de pilotes à un serveur
- Ajout ou suppression de pilotes
- Affichage d'informations d'activation relatives à l'ensemble de pilotes
- Affichage du journal d'état de l'ensemble de pilotes

1.2.6 Objet Pilote

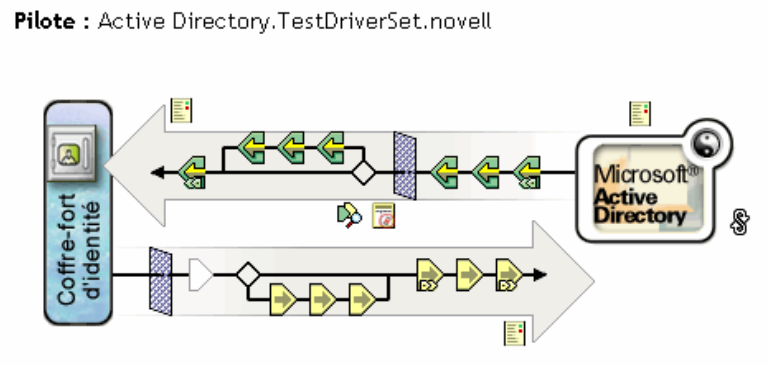
Un objet Pilote représente un pilote permettant la connexion au système connecté associé au coffre-fort d'identité. Les composants suivants contiennent l'objet Pilote et ses paramètres de configuration :

- Un objet Pilote de l'arborescence eDirectory contenu dans un objet Ensemble de pilotes.
- Un objet canal Abonné contenu dans l'objet Pilote.

- Un objet Éditeur contenu dans l'objet Pilote.
- Plusieurs objets de stratégies référencés par les objets Pilote, Abonné et Éditeur.
- Module d'interface de pilote exécutable référencé par l'objet Pilote.
- Paramètres propres au module d'interface configurés par l'administrateur.
- Mot de passe eDirectory pour l'objet Pilote. Le mot de passe peut être utilisé par le module d'interface pour authentifier une partie distante de ce dernier.
- Paramètres d'authentification utilisés lors de la connexion au système connecté et de l'authentification auprès de ce dernier.
- Droits, même si certains pilotes n'en comprennent pas. Les droits peuvent être activés au moment de la création du pilote ou ajoutés ultérieurement.
- une option de démarrage du pilote qui inclut les éléments suivants :
  - Activé : le pilote n'est pas exécuté.
  - Manuel : le démarrage du pilote doit se faire manuellement à l'aide de iManager.
  - Démarrage auto : le pilote est automatiquement lancé au démarrage du coffre-fort d'identité.
- Une référence à une stratégie d'assignation de schéma.
- Une représentation au format XML du schéma du système connecté. Elle est généralement obtenue automatiquement du système connecté par l'intermédiaire du module d'interface.

Dans iManager, vous pouvez accéder à la page Présentation du pilote Identity Manager et modifier les paramètres, les stratégies, les feuilles de style et les droits associés à un pilote existant. La présentation du pilote Identity Manager est illustrée ci-dessous.

Figure 1-4 *Présentation du pilote Identity Manager*



En outre, l'objet Pilote est utilisé pour le contrôle des droits eDirectory. L'objet Pilote doit posséder des droits eDirectory suffisants sur tout objet qu'il lit ou écrit. Pour cela, l'objet Pilote doit être un ayant droit des objets eDirectory avec lesquels le pilote se synchronise, ou des équivalences de sécurité doivent lui être accordées.

Pour plus d'informations sur l'attribution de droits, reportez-vous à la section « eDirectory Rights (Droits eDirectory) (http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbachifb.html) » du *Novell eDirectory 8.8 Administration Guide (Guide d'administration de Novell eDirectory 8.8)*.

1.2.7 Canaux Éditeur et Abonné

Les pilotes Identity Manager contiennent deux canaux de traitement des données : le canal Éditeur et le canal Abonné. Le canal Éditeur envoie les événements du système connecté au coffre-fort d'identité. Le canal Abonné envoie les événements du coffre-fort d'identité au système connecté. Chacun de ces canaux contient ses propres stratégies, qui définissent le traitement et la transformation des données.

Figure 1-5 *Canaux Éditeur et Abonné dans Designer*

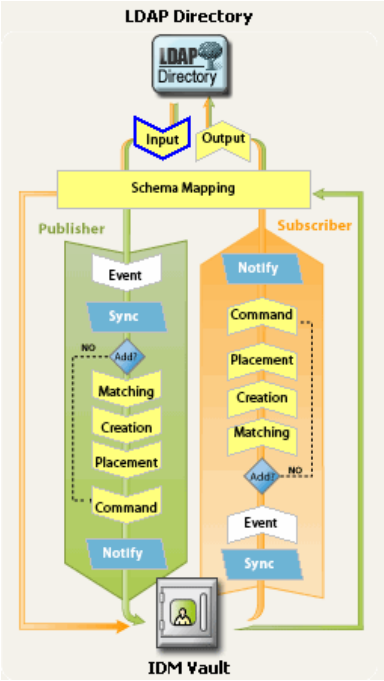
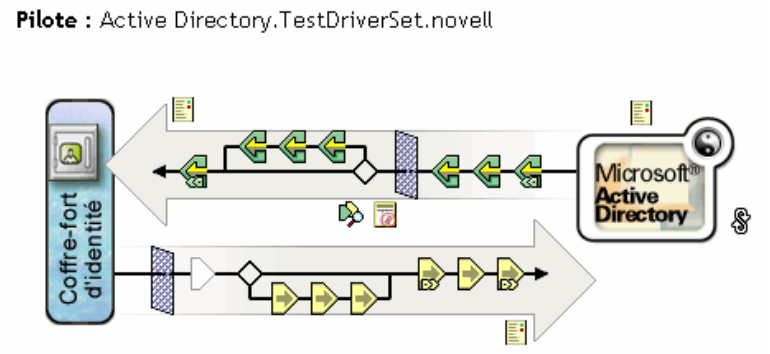


Figure 1-6 *Canaux Éditeur et Abonné dans iManager*



1.2.8 Événements et commandes

La distinction entre événements et commandes au sein de Identity Manager est importante. Si un événement est envoyé à un pilote, il s'agit d'une commande. S'il est envoyé à Identity Manager, il s'agit d'une notification. Lorsque le pilote envoie une notification d'événement à Identity Manager, il lui signale qu'une modification a été apportée au système connecté. Le moteur méta-annuaire

détermine ensuite, en fonction de règles configurables, les éventuelles commandes à envoyer au coffre-fort d'identité.

Lorsque Identity Manager envoie une commande au pilote, cela signifie qu'il a déjà accepté en entrée un événement du coffre-fort d'identité, appliqué les stratégies appropriées et déterminé que la modification du système connecté représentée par la commande était nécessaire.

1.2.9 Stratégies et filtres

Les stratégies et les filtres permettent de contrôler la façon dont les flux de données transitent entre les systèmes. Les règles contenues dans les stratégies permettent de définir la façon dont les classes, les attributs et les événements du coffre-fort d'identité sont convertis pour être utilisés dans le système connecté, et vice versa. Pour plus de détails sur les stratégies et les filtres, reportez-vous au *Policy Builder and Driver Customization Guide (Guide de création des stratégies et de personnalisation des pilotes)*.

1.2.10 Associations

Les autres produits de gestion des identités requièrent, pour la plupart, que le système connecté stocke un identificateur afin d'associer les objets du système connecté à l'annuaire. Grâce à Identity Manager, aucune modification du système connecté n'est requise. Chaque objet du coffre-fort d'identité contient une table d'association qui fait correspondre à l'objet un identificateur unique dans les systèmes connectés. Cette table est dotée d'un index inversé afin que le système connecté n'ait pas à fournir d'identificateur de coffre-fort d'identité (tel qu'un nom distinctif) au pilote d'intégration lors de la mise à jour du coffre-fort.

La création d'une association entre deux objets se produit lorsqu'un événement touche un objet qui n'a pas encore été associé à un autre objet du coffre-fort d'identité. Pour que cette association puisse être créée, l'ensemble minimal de critères définissables doit être rempli pour chaque objet. Par exemple, vous pouvez créer une stratégie indiquant que lorsque deux des quatre attributs sont concordants à plus de 90 % (nom, numéro de téléphone, ID d'employé et adresse électronique), l'objet est associé.

Les stratégies de concordance définissent les critères qui permettent de déterminer si deux objets sont identiques. Si aucune correspondance n'est trouvée pour l'objet modifié, un nouvel objet peut être créé. Pour que cela se produise, tous les critères minimaux de création doivent être remplis. Ces critères sont définis par une stratégie de création. Enfin, la stratégie de placement définit l'emplacement de création du nouvel objet dans la hiérarchie d'assignation de nom.

Les associations peuvent être créées de deux manières :

- En tant que correspondance entre deux objets
- En tant que nouvelle création d'objet à un emplacement donné

Une association créée entre deux objets reste active jusqu'à ce que les objets soient supprimés ou que l'association soit annulée par un administrateur.

Table d'association

Dans Identity Manager, les associations font référence à la concordance entre des objets eDirectory et des objets qui résident sur des systèmes connectés. Lors de la première installation de Identity Manager, le schéma eDirectory est étendu. Une partie de cette extension se compose d'un nouvel attribut lié à la classe de base de tous les objets eDirectory. Cet attribut est une table d'association.

Les tables d'association conservent une trace de tous les objets des systèmes connectés auxquels un objet eDirectory est lié. Cette table est créée et gérée automatiquement. Par conséquent, il est rarement nécessaire d'en modifier manuellement les informations. En revanche, il est souvent utile de les afficher.

L'attribut d'association de l'objet peut être affiché dans iManager.

1. Dans la barre d'outils de iManager, sélectionnez l'icône *Afficher les objets*.

2. Localisez l'objet et sélectionnez-le, puis sélectionnez *Modifier l'objet*.
3. Sélectionnez l'onglet Identity Manager.

L'attribut d'association apparaît sur cet onglet.

1.3 Application utilisateur

L'Application utilisateur est une solution de provisioning. Elle vient compléter Identity Manager 3 et intègre un puissant outil de workflow d'approbation à Identity Manager. Elle permet ainsi aux entreprises de prendre des décisions de provisioning qui s'appuient à la fois sur des saisies manuelles et sur des règles automatiques ne nécessitant aucune intervention manuelle. Pour plus d'informations, reportez-vous à la documentation de l'application utilisateur (http://www.novell.com/documentation/idm).

1.4 Designer

Designer est une application client autonome. Il se compose d'un espace Modeler, d'une palette, de vues, d'un Générateur de stratégies, d'un générateur de documents et d'autres fonctionnalités qui permettent de concevoir, tester, documenter et déployer des solutions Identity Manager dans un environnement hautement productif. Pour plus d'informations sur Designer, reportez-vous au document *Designer for Identity Manager 3: Administration Guide (Guide d'administration de Designer pour Identity Manager 3)*.

Gestion des pilotes Identity Manager

2

Cette section contient des informations qui vous aideront à créer et à gérer votre pilote Identity Manager. Les rubriques sont les suivantes :

2.1 Création et configuration d'un pilote

Pour chaque pilote Identity Manager que vous envisagez d'utiliser, créez un objet Pilote et importez une configuration. L'objet Pilote contient des paramètres et des stratégies de configuration pour ce pilote. Lors de la création d'un objet Pilote, vous importez un fichier de configuration spécifique au pilote. Les configurations de pilote contiennent un ensemble de stratégies par défaut. Il permet de commencer dans de bonnes conditions l'implémentation de votre modèle de partage de données. La plupart du temps, vous configurez un pilote à l'aide de la configuration par défaut, puis vous modifiez cette configuration en fonction des besoins de votre environnement.

Vous pouvez utiliser deux méthodes pour créer des objets Pilote.

- La tâche Créer un pilote permet de créer un seul pilote et d'importer sa configuration. Pour plus d'informations, reportez-vous à « Création d'un objet Pilote » page 20.
- La tâche Importer des pilotes permet de créer plusieurs pilotes simultanément et d'importer leurs configurations. Pour plus d'informations, reportez-vous à la Section 2.1.2, « Création de plusieurs pilotes », page 20.

2.1.1 Création d'un objet Pilote

Le fichier XML de configuration du pilote permet de créer et de configurer les objets nécessaires au bon fonctionnement du pilote. Il inclut également des stratégies de base que vous pouvez adapter à votre implémentation.

1. Dans iManager, sélectionnez *Utilitaires Identity Manager > Nouveau pilote*.
2. Sélectionnez l'ensemble de pilotes dans lequel vous souhaitez créer le pilote, puis cliquez sur *Suivant*.

   Si vous placez ce pilote dans un nouvel ensemble de pilotes, vous devez en préciser le nom, ainsi qu'un contexte et un serveur associé.
3. Activez l'option *Importer une configuration de pilote du serveur (fichier .XML)* et sélectionnez le fichier .xml, puis cliquez sur *Suivant*.

   Le fichier de configuration du pilote est installé sur le serveur Web au moment de la configuration de iManager.
4. Suivez les invites pour finir d'importer la configuration du pilote.

Les objets Identity Manager nécessaires sont créés. Si vous n'avez pas défini les équivalences de sécurité ou si vous avez exclu les utilisateurs dotés de privilèges administratifs pendant l'importation, vous pouvez exécuter ces tâches en modifiant les propriétés de l'objet Pilote.

Remarque : si vous n'activez pas l'option Droits pendant l'importation, les stratégies de droit ne sont pas créées. Si vous souhaitez utiliser les droits ultérieurement, vous devez créer un nouveau pilote avec l'option Droits activée.

2.1.2 Création de plusieurs pilotes

Identity Manager permet de créer simultanément plusieurs pilotes. Le processus est similaire à celui de la création d'un seul pilote ; en effet, les fichiers XML de configuration du pilote créent et configurent les objets nécessaires au bon fonctionnement des pilotes.

Pour importer simultanément plusieurs pilotes :

1. Dans iManager, sélectionnez *Utilitaires Identity Manager > Importer des pilotes*.
2. Sélectionnez l'ensemble de pilotes dans lequel vous voulez créer les nouveaux pilotes, puis cliquez sur *Suivant*.

   Si vous placez ces pilotes dans un nouvel ensemble, vous devez en préciser le nom, ainsi qu'un contexte et un serveur associé.
3. Sélectionnez les configurations d'application à ajouter à l'ensemble de pilotes, puis cliquez sur *Suivant*.
4. Répondez aux invites et spécifiez les données demandées, puis cliquez sur *Suivant*.

   Lorsque vous sélectionnez plusieurs configurations à importer simultanément, les pages de configuration des applications s'affichent l'une après l'autre.

Les objets Identity Manager nécessaires pour chaque pilote sont créés. Si vous n'avez pas défini les équivalences de sécurité ou si vous avez exclu les utilisateurs dotés de privilèges administratifs pendant l'importation, vous pouvez exécuter ces tâches en modifiant les propriétés de l'objet Pilote.

2.2 Gestion des pilotes DirXML 1.1a dans un environnement Identity Manager

Les pilotes existants créés pour DirXML 1.1a fonctionnent également sous Identity Manager.

Le moteur méta-annuaire livré avec Identity Manager 3.0 est compatible en amont avec les pilotes plus anciens (à condition que les mises à jours et correctifs les plus récents aient été appliqués aux modules d'interface et aux configurations de ces pilotes). Vous pouvez donc exécuter les pilotes DirXML 1.1a sur les serveurs Identity Manager aussi longtemps que vous le voulez, sans apporter de modification.

Toutefois, les plugs-in iManager n'ont qu'une compatibilité en amont limitée. Un pilote ancien peut être affiché sur la page Présentation d'un ensemble de pilotes, mais sa configuration ne peut être ni affichée, ni modifiée si le pilote n'est pas converti. Lorsque vous cliquez sur un pilote DirXML 1.1a dans la page Présentation de l'ensemble de pilotes, les plugs-in Identity Manager détectent qu'il est au format DirXML 1.1a et vous invitent à le convertir au format 3.0 à l'aide d'un assistant.

Si vous ne voulez pas encore apporter de modification à un pilote existant, vous pouvez quitter l'assistant.

Pour modifier un pilote au format 1.1a, vous devez utiliser les plugs-in DirXML 1.1a. Pour cela, utilisez un serveur Web iManager séparé sur lequel les plugs-in 1.1a sont installés. Vous ne pouvez pas utiliser les plugs-in Identity Manager livrés avec Identity Manager pour modifier la configuration d'un pilote sans le convertir au format Identity Manager 3.0.

2.3 Mise à niveau de la configuration d'un pilote du format DirXML 1.1a au format Identity Manager

Pour effectuer la mise à niveau de DirXML 1.1a à Identity Manager 3, vous devez passer par Identity Manager 2. Le programme d'installation Identity Manager 2 installe de nouveaux modules d'interface pilote mais ne modifie pas les objets ou les configurations des pilotes existants.

Les configurations des pilotes existants créés pour DirXML 1.1a fonctionnent également sous Identity Manager. Toutefois, les plugs-in Identity Manager ne permettent d'éditer que les pilotes au format Identity Manager.

Important : l'exécution d'une configuration ou d'un module d'interface pilote Identity Manager avec un moteur DirXML 1.1a n'est pas prise en charge.

Un assistant vous aide à convertir les pilotes DirXML 1.1a au format Identity Manager.

Pour démarrer l'assistant :

1. Dans iManager, cliquez sur *Identity Manager* > *Présentation de Identity Manager*.
2. Recherchez l'ensemble de pilotes qui contient le pilote à convertir, puis cliquez sur *Rechercher*.
3. Cliquez sur l'icône du pilote que vous voulez convertir.

   Une invite vous propose de convertir le pilote au nouveau format.
4. Suivez les étapes de l'assistant pour terminer la conversion.

2.4 Démarrage, arrêt ou redémarrage d'un pilote

1. Dans iManager, cliquez sur *Identity Manager > Présentation de Identity Manager*.
2. Localisez l'ensemble de pilotes contenant le pilote concerné, puis cliquez sur *Rechercher*.
3. Cliquez sur l'angle supérieur droit de l'icône du pilote dont vous souhaitez modifier l'état, puis cliquez sur *Démarrer le pilote* si le pilote est arrêté ou sur *Arrêter le pilote* s'il est en cours d'exécution.

2.5 Paramètres de pilote

Les paramètres de chaque pilote figurent dans les propriétés de celui-ci. Ces paramètres contiennent des informations spécifiques au pilote, notamment l'intervalle d'interrogation, la méthode d'authentification, l'utilisation de SSL ou la définition de la pulsation du pilote.

2.6 Utilisation de valeurs de configuration globale

Les valeurs de configuration globale sont des paramètres similaires aux paramètres du pilote. Ces valeurs peuvent être définies pour un ensemble de pilotes ou pour un pilote individuel. Si un pilote ne possède pas de valeur de configuration globale, il hérite de celle de l'ensemble de pilotes.

Les valeurs de configuration globale permettent de spécifier des paramètres pour les fonctions Identity Manager, telles que la synchronisation des mots de passe ou la pulsation de pilote, ainsi que des paramètres spécifiques à une configuration de pilote particulière. Certaines valeurs de configuration globale sont fournies avec les pilotes, mais vous pouvez ajouter vos propres valeurs. Vous pourrez utiliser ces valeurs dans les stratégies pour personnaliser la configuration de votre pilote.

Important : les paramètres de synchronisation des mots de passe sont des valeurs de configuration globale (GCV), mais il vaut mieux les modifier dans l'interface graphique fournie sur la page Variables de serveur pour le pilote, plutôt que sur la page GCV. La page Variables de serveur, qui affiche les paramètres de synchronisation des mots de passe, est accessible sous forme d'onglet, comme les autres paramètres du pilote, ou en cliquant sur *Gestion des mots de passe > Synchronisation de mot de passe*, en recherchant le pilote et en cliquant sur son nom. La page contient de l'aide en ligne pour chaque paramètre de synchronisation des mots de passe.

Pour ajouter, supprimer ou modifier des GCV qui ne sont pas liées à la synchronisation des mots de passe Identity Manager :

1. Dans iManager, cliquez sur *Identity Manager > Présentation de Identity Manager*.
2. Localisez l'objet Ensemble de pilotes ou Pilote, cliquez dessus, puis cliquez sur *Rechercher*.
3. Cliquez dans l'angle supérieur droit du pilote, puis cliquez sur *Éditer les propriétés*.
4. Sélectionnez *Valeurs de configuration globale*.
5. Modifiez les valeurs par défaut définies lors de la création du pilote.
6. Si vous souhaitez ajouter des informations supplémentaires, cliquez sur *Édition XML*.
7. Cliquez sur *Activer l'édition XML*.

8 Ajoutez, supprimez ou modifiez le fichier XML, puis cliquez sur *OK* pour appliquer les modifications.

2.7 Utilisation de l'utilitaire de ligne de commande DirXML

L'utilitaire de ligne de commande DirXML permet d'accéder aux verbes eDirectory spécifiques à Identity Manager. Cet utilitaire ne remplace ni iManager, ni Designer. Il est essentiellement utilisé pour les scripts. Reportez-vous à l'Annexe A, « Utilitaire de ligne de commande DirXML », page 251 pour plus de détails sur l'utilitaire de ligne de commande DirXML. Pour les tâches de routine, utilisez plutôt iManager ou Designer.

2.8 Affichage des informations de versions

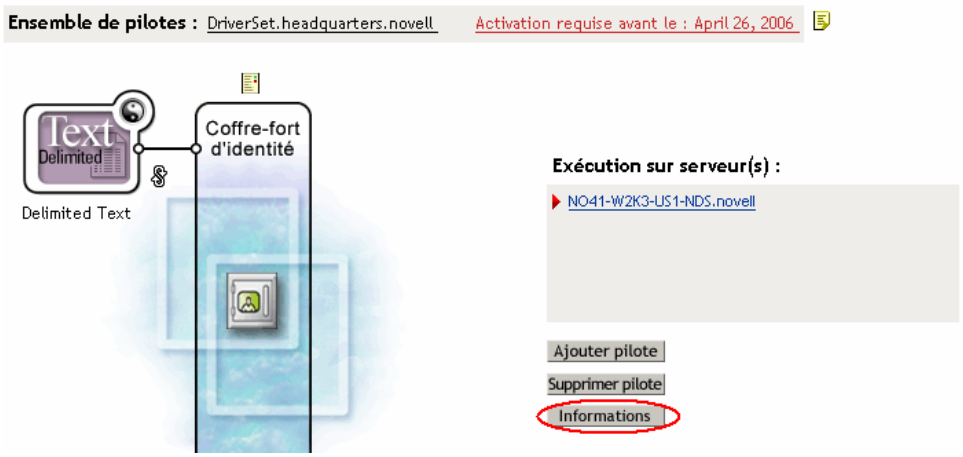
L'outil d'identification de version permet d'effectuer les tâches suivantes.

- Section 2.8.1, « Affichage d'une vue hiérarchique des informations de version », page 23
- Section 2.8.2, « Affichage des informations de version dans un fichier texte », page 25
- Section 2.8.3, « Enregistrement des informations de version », page 26

2.8.1 Affichage d'une vue hiérarchique des informations de version

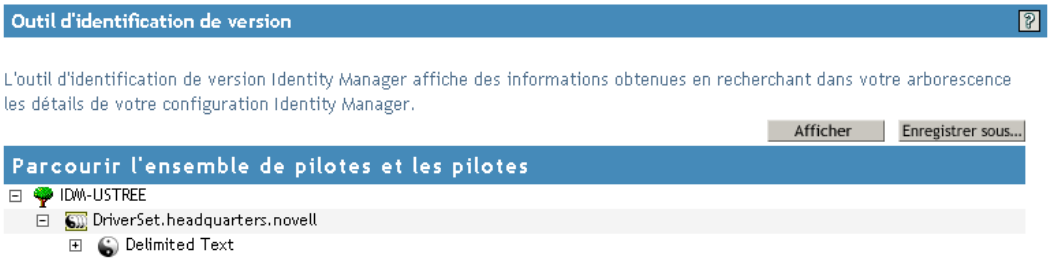
1 Dans iManager cliquez sur *Identity Manager* > *Présentation de Identity Manager*, puis sur *Rechercher* pour rechercher votre ensemble de pilotes.

2 Cliquez sur *Informations* dans l'écran Présentation de Identity Manager.



Vous pouvez également sélectionner *Utilitaires Identity Manager* > *Identification des versions*, puis naviguer jusqu'à l'ensemble de pilotes et le sélectionner avant de cliquer sur *OK*.

3 Affichez une vue globale ou non développée des informations de version.

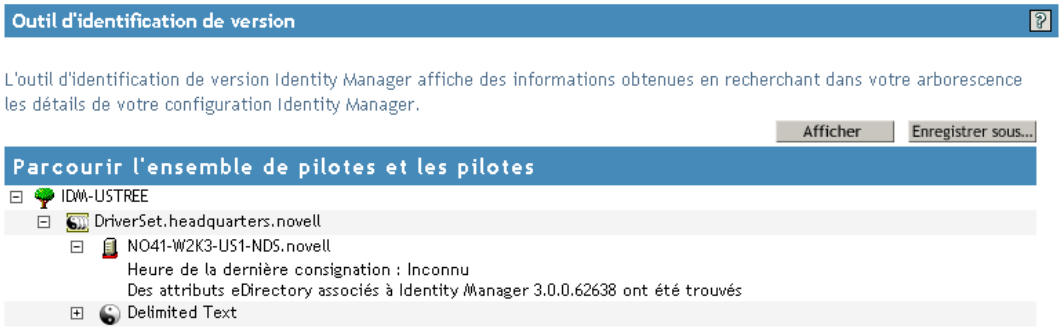


La vue hiérarchique non développée affiche les éléments suivants.

- L'arborescence eDirectory pour laquelle vous êtes authentifié.
- L'ensemble de pilotes que vous avez sélectionné.
- Les serveurs associés à l'ensemble de pilotes.

  Si l'ensemble de pilotes est associé à plusieurs serveurs, vous pouvez afficher les informations Identity Manager sur chaque serveur.
- Les pilotes.

4 Affichez les informations de version liées aux serveurs en développant l'icône du serveur.



La vue développée d'une icône de serveur de niveau supérieur affiche les informations suivantes.

- L'heure de la dernière consignation.
- La version Identity Manager exécutée sur le serveur.

5 Affichez des informations de version liées aux pilotes en développant l'icône de pilote.

La vue développée d'une icône de pilote de niveau supérieur affiche les informations suivantes.

- Le nom du pilote.
- Le module pilote (par exemple, com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver).

La vue développée d'une icône de serveur sous une icône de pilote affiche les informations suivantes.

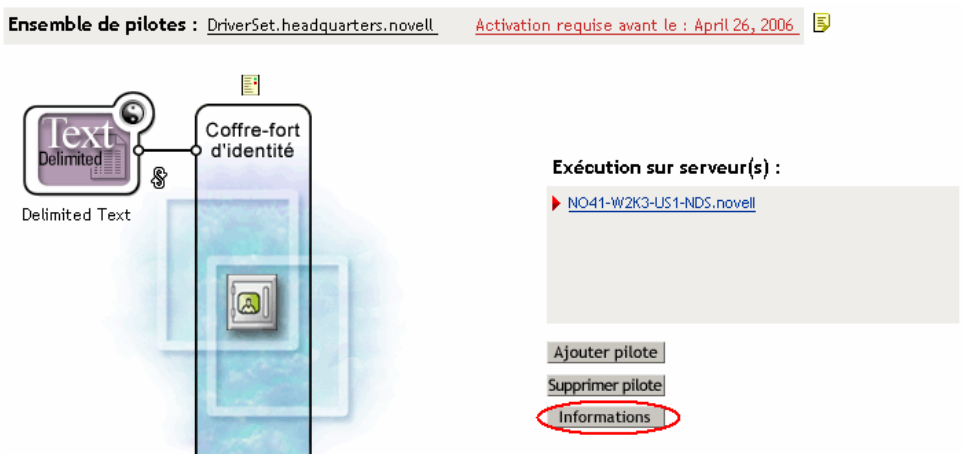
- L'ID du pilote.
- La version de l'instance du pilote exécutée sur ce serveur.

2.8.2 Affichage des informations de version dans un fichier texte

Identity Manager publie les informations de version dans un fichier. Vous pouvez afficher ces informations au format texte. La représentation textuelle contient les mêmes informations que la vue hiérarchique.

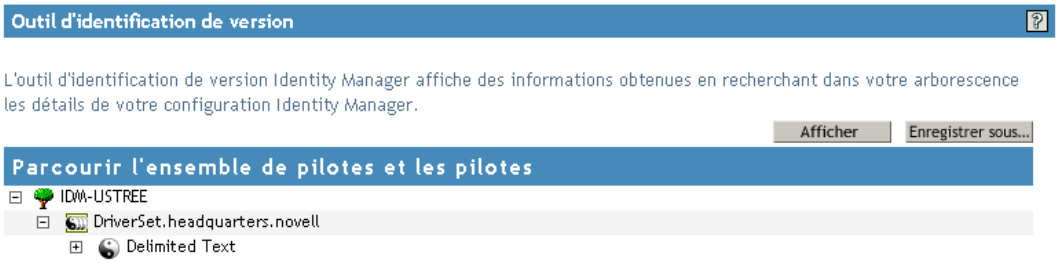
1 Dans iManager cliquez sur *Identity Manager* > *Présentation de Identity Manager*, puis sur *Rechercher* pour rechercher votre ensemble de pilotes.

2 Cliquez sur *Informations* dans l'écran Présentation de Identity Manager.

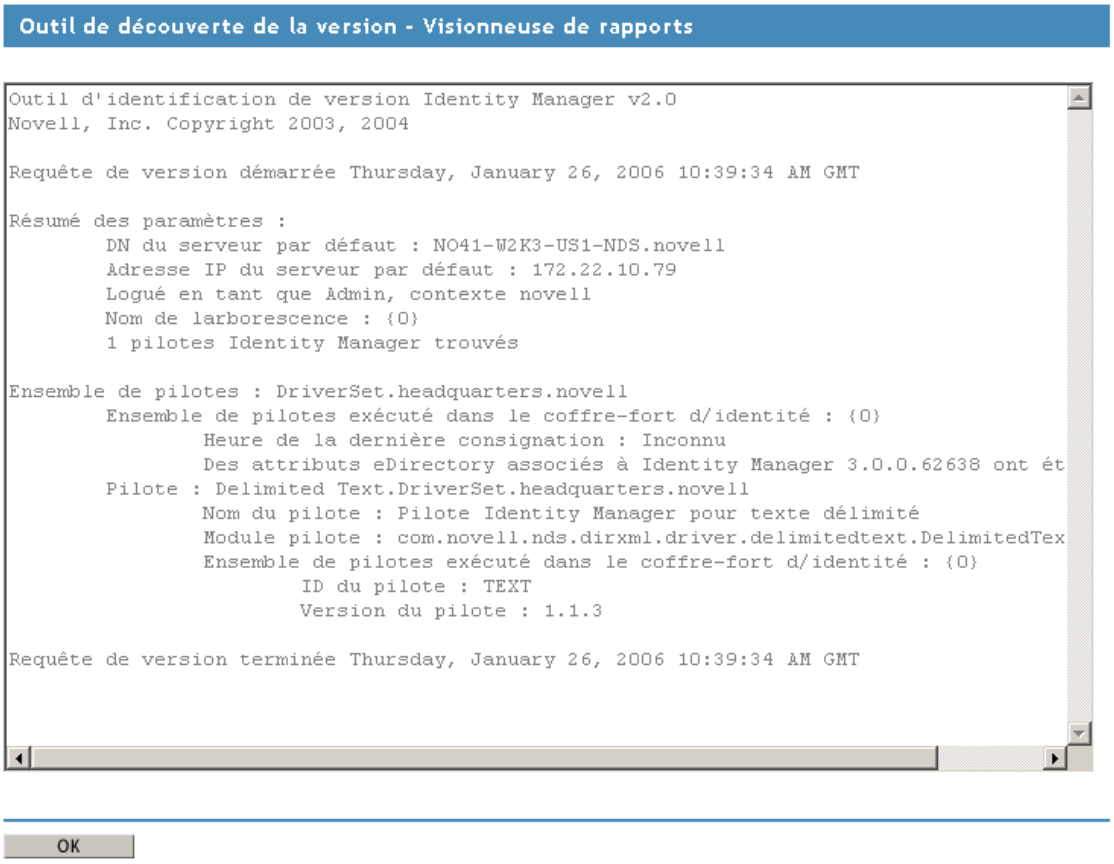


Vous pouvez également sélectionner *Utilitaires Identity Manager > Outil d'identification de version* , puis naviguez jusqu'à l'ensemble de pilotes et sélectionnez-le avant de cliquer sur *Informations*.

3 Dans la boîte de dialogue Outil d'identification de version, cliquez sur *Afficher*.



Les informations s'affichent dans un fichier texte, dans la fenêtre Visionneuse de rapports.

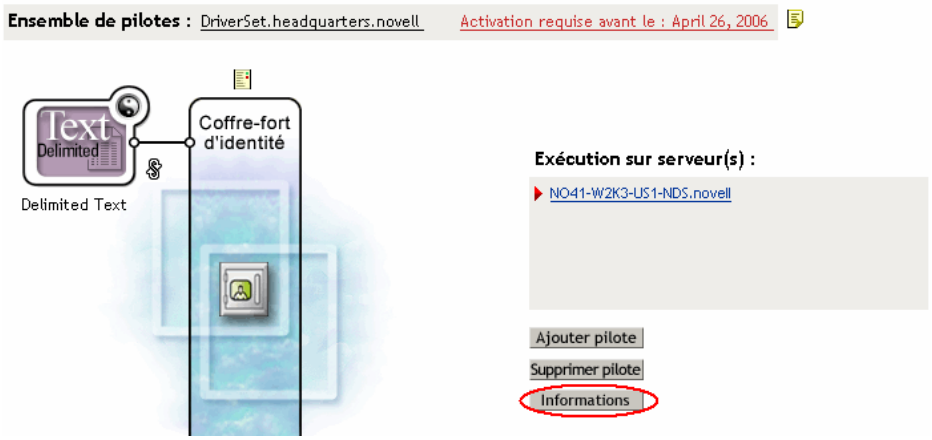


2.8.3 Enregistrement des informations de version

Vous pouvez enregistrer des informations de version dans un fichier texte de votre unité locale ou réseau.

1 Dans iManager cliquez sur *Identity Manager > Présentation de Identity Manager*, puis sur *Rechercher* pour rechercher votre ensemble de pilotes.

2 Cliquez sur *Informations* dans l'écran Présentation de Identity Manager.



Vous pouvez également sélectionner *Utilitaires Identity Manager* > *Outil d'identification de version* , puis naviguez jusqu'à l'ensemble de pilotes et sélectionnez-le avant de cliquer sur *Informations*.

3 Dans la boîte de dialogue Outil d'identification de version, cliquez sur *Enreg sous*.

4 Dans la boîte de dialogue Téléchargement de fichier, cliquez sur *Enregistrer*.

5 Recherchez le répertoire désiré, saisissez un nom de fichier, puis cliquez sur *Enregistrer*.

Identity Manager enregistre les données dans un fichier texte.

2.9 Utilisation de mots de passe nommés

Identity Manager permet de stocker plusieurs mots de passe de façon sécurisée pour un pilote donné. Cette fonctionnalité est appelée Mots de passe nommés. Chaque mot de passe différent est accessible par une clé ou un nom.

Vous pouvez aussi utiliser la fonctionnalité Mots de passe nommés pour mémoriser d'autres informations en toute sécurité, par exemple un nom d'utilisateur.

Pour utiliser un mot de passe nommé dans une stratégie de pilote, désignez-le par le nom du mot de passe plutôt que par le mot de passe proprement dit ; le moteur méta-annuaire envoie alors le mot de passe au pilote. Vous pouvez utiliser la méthode décrite dans cette section pour la mémorisation et la récupération des mots de passe nommés, avec n'importe quel pilote, sans apporter de modification au module d'interface pilote.

Remarque : les exemples de configuration fournis pour le pilote Identity Manager pour Lotus Notes incluent un exemple de cette utilisation des mots de passe nommés. Le module d'interface pilote Notes a également été personnalisé pour prendre en charge d'autres façons d'utiliser les mots de passe nommés ; des exemples de ces méthodes sont également inclus. Pour plus d'informations, reportez-vous à la section « Named Passwords (Mots de passe nommés) » du *Identity Manager Driver for Lotus Notes: Implementation Guide (Guide d'implémentation du pilote Identity Manager pour Lotus Notes)*.

Dans cette section :

2.9.1 Configuration des mots de passe nommés avec Designer

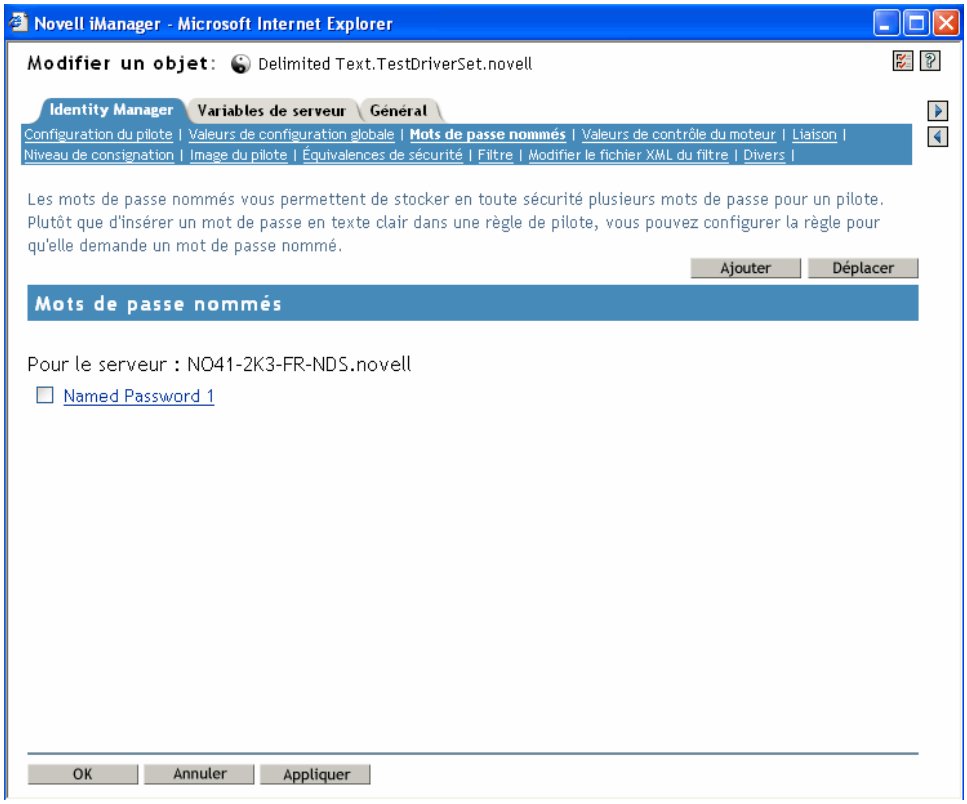
1. Sélectionnez l'objet Pilote, cliquez avec le bouton droit, puis sélectionnez *Propriétés*.
2. Sélectionnez *Mot de passe nommé* et cliquez sur *Nouveau*.

3. Indiquez le *Nom* du mot de passe nommé.
4. Indiquez le *Nom d'affichage* du mot de passe nommé.
5. Indiquez le mot de passe nommé, puis saisissez-le à nouveau.
6. Cliquez sur *OK* deux fois.

2.9.2 Configuration des mots de passe nommés avec iManager

1. Dans iManager, cliquez sur *Identity Manager* > *Présentation de Identity Manager*.
2. Recherchez l'ensemble de pilotes ou localisez et sélectionnez le conteneur dans lequel se trouve l'ensemble de pilotes. Une représentation graphique de l'ensemble de pilotes apparaît.
3. Dans l'écran Présentation de Identity Manager, cliquez sur l'angle supérieur droit de l'icône du pilote, puis sur *Éditer les propriétés*.
4. Dans la page de modification de l'objet de l'onglet Identity Manager, cliquez sur *Mots de passe nommés*.

   La page Mots de passe nommés apparaît, listant les Mots de passe nommés actuels pour ce pilote. Si vous n'avez pas configuré de mots de passe nommés, la liste est vide.



5 Pour ajouter un mot de passe nommé, cliquez sur *Ajouter*, remplissez les champs, puis cliquez sur *OK*.

6 Indiquez un nom, un nom d'affichage et un mot de passe, puis cliquez deux fois sur *OK*.

N'oubliez pas que vous pouvez utiliser cette fonction pour mémoriser de façon sûre d'autres informations, par exemple un nom d'utilisateur.

7 Le message suivant s'affiche : Voulez-vous redémarrer le pilote pour que vos modifications soient prises en compte ? (OK=Oui, Annuler=Non). Cliquez sur *OK*.

8 Pour supprimer un mot de passe nommé, cliquez sur *Supprimer*. Le mot de passe est supprimé sans invite vous demandant de confirmer l'opération.

2.9.3 Utilisation des mots de passe nommés dans les stratégies de pilotes

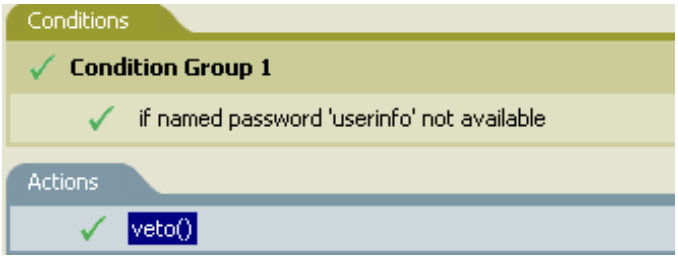
- « Utilisation du Générateur de stratégies » page 30
- « Utilisation de XSLT » page 31

Utilisation du Générateur de stratégies

Le Générateur de stratégies permet d'appeler un mot de passe nommé. Créez une nouvelle règle et sélectionnez un mot de passe nommé comme condition. Vous pouvez définir une opération qui

dépend de la disponibilité de ce mot de passe. L'exemple suivant montre que si le mot de passe nommé userinfo n'est pas disponible, l'opération se heurte à un veto.

Figure 2-1 *Stratégie utilisant un mot de passe nommé*



Utilisation de XSLT

L'exemple suivant montre comment un mot de passe nommé peut être référencé dans une stratégie de pilote sur le canal Abonné dans XSLT :

```
<xsl:value-of
select="query:getNamedPassword($srcQueryProcessor,'mynamedpassword')"
xmlns:query="http://www.novell.com/java/
com.novell.nds.dirxml.driver.XdsQueryProcessor/>
```

2.9.4 Configuration des mots de passe nommés avec l'utilitaire de ligne de commande DirXML

- « Création d'un mot de passe nommé dans l'utilitaire de ligne de commande DirXML » page 31
- « Suppression d'un mot de passe nommé dans l'utilitaire de ligne de commande DirXML » page 33

Création d'un mot de passe nommé dans l'utilitaire de ligne de commande DirXML

1. Exécutez l'utilitaire de ligne de commande DirXML.

   Pour plus d'informations, reportez-vous à l'Annexe A, « Utilitaire de ligne de commande DirXML », page 251.

2. Saisissez votre nom d'utilisateur et votre mot de passe.

   La liste d'options suivante apparaît.

```
DirXML commands

 1: Start driver
 2: Stop driver
 3: Driver operations...
 4: Driver set operations...
 5: Log events operations...
 6: Get DirXML version
99: Quit
```

```
Enter choice:
```

3 Saisissez 3 pour les opérations du pilote.

Une liste numérotée de pilotes apparaît.

4 Saisissez le numéro du pilote auquel vous voulez ajouter un mot de passe nommé.

La liste d'options suivante apparaît.

```
Select a driver operation for:driver_name

 1: Start driver
 2: Stop driver
 3: Get driver state
 4: Get driver start option
 5: Set driver start option
 6: Resync driver
 7: Migrate from application into DirXML
 8: Submit XDS command document to driver
 9: Check object password
10: Initialize new driver object
11: Passwords operations
12: Cache operations
99: Exit

Enter choice:
```

5 Saisissez 11 pour les opérations de mot de passe.

La liste d'options suivante apparaît.

```
Select a password operation

 1: Set shim password
 2: Reset shim password
 3: Set named password
 4: Clear named password(s)
 5: List named passwords
99: Exit

Enter choice:
```

6 Saisissez 3 pour définir un nouveau mot de passe nommé.

L'invite suivante apparaît :

```
Enter password name:
```

7 Saisissez le nom par lequel vous voulez désigner le mot de passe nommé.

8 Saisissez le mot de passe que vous voulez sécuriser à l'invite suivante :

```
Enter password:
```

Les caractères que vous saisissez pour le mot de passe ne s'affichent pas.

9 Confirmez le mot de passe en le saisissant de nouveau à l'invite suivante :

```
Confirm password:
```

10 Lorsque vous avez entré et confirmé le mot de passe, vous revenez au menu des opérations de mot de passe.

Une fois cette procédure terminée, vous pouvez utiliser l'option 99 deux fois pour quitter le menu et l'utilitaire de ligne de commande DirXML.

Suppression d'un mot de passe nommé dans l'utilitaire de ligne de commande DirXML

Cette option est particulièrement utile si vous n'avez plus besoin des mots de passe nommés que vous avez précédemment créés.

1 Exécutez l'utilitaire de ligne de commande DirXML.

Pour plus d'informations, reportez-vous à l'Annexe A, « Utilitaire de ligne de commande DirXML », page 251.

2 Saisissez votre nom d'utilisateur et votre mot de passe.

La liste d'options suivante apparaît.

```
DirXML commands

 1: Start driver
 2: Stop driver
 3: Driver operations...
 4: Driver set operations...
 5: Log events operations...
 6: Get DirXML version
99: Quit

Enter choice:
```

3 Saisissez 3 pour les opérations du pilote.

Une liste numérotée de pilotes apparaît.

4 Saisissez le numéro du pilote pour lequel vous voulez supprimer des mots de passe nommés.

La liste d'options suivante apparaît.

```
Select a driver operation for:driver_name

 1: Start driver
 2: Stop driver
 3: Get driver state
 4: Get driver start option
 5: Set driver start option
 6: Resync driver
 7: Migrate from application into DirXML
 8: Submit XDS command document to driver
 9: Check object password
```

```
10: Initialize new driver object
11: Passwords operations
12: Cache operations
99: Exit

Enter choice:
```

5 Saisissez 11 pour les opérations de mot de passe.

La liste d'options suivante apparaît.

```
Select a password operation

 1: Set shim password
 2: Reset shim password
 3: Set named password
 4: Clear named password(s)
 5: List named passwords
99: Exit

Enter choice:
```

6 (Facultatif) Saisissez 5 pour afficher la liste des mots de passe nommés existants.

La liste des mots de passe nommés existants s'affiche.

Cette étape peut vous aider à vérifier que vous supprimez le bon mot de passe.

7 Saisissez 4 pour supprimer un ou plusieurs mots de passe nommés.

8 Saisissez No pour supprimer un seul mot de passe nommé à l'invite suivante :

```
Do you want to clear all named passwords? (yes/no):
```

9 Saisissez le nom du mot de passe nommé que vous voulez supprimer à l'invite suivante :

```
Enter password name:
```

Lorsque vous saisissez le nom du mot de passe nommé que vous voulez supprimer, vous revenez au menu des opérations de mot de passe :

```
Select a password operation

 1: Set shim password
 2: Reset shim password
 3: Set named password
 4: Clear named password(s)
 5: List named passwords
99: Exit

Enter choice:
```

10 (Facultatif) Saisissez 5 pour afficher la liste des mots de passe nommés existants.

La liste des mots de passe nommés existants s'affiche.

Cette étape permet de vérifier que vous avez supprimé le bon mot de passe.

Une fois cette procédure terminée, vous pouvez utiliser l'option 99 deux fois pour quitter le menu et l'utilitaire de ligne de commande DirXML.

2.10 Réassociation d'un objet Pilote à un serveur

Un objet Pilote est associé à un serveur.

Si l'association devient invalide pour une raison quelconque, cela est indiqué de la façon suivante :

- Lorsque vous mettez à niveau eDirectory sur votre serveur Identity Manager, vous obtenez l'erreur « UniqueSPIException error -783 ».
- Aucun serveur ne figure en regard du pilote, dans l'écran Présentation de Identity Manager.
- Le nom d'un serveur figure en regard du pilote dans l'écran Présentation de Identity Manager, mais il est tronqué.

Pour résoudre ce problème, dissociez l'objet Pilote et le serveur puis réassociez-les.

Connectez-vous à iManager et localisez l'objet Pilote dans l'écran Présentation de Identity Manager. Utilisez les icônes pour supprimer puis ajouter un serveur à la liste des noms de serveurs près de l'icône du pilote. La suppression puis l'ajout réassocie le serveur et l'objet Pilote.

2.11 Ajout de la pulsation du pilote

La pulsation du pilote est une fonction des pilotes Identity Manager disponible depuis la version 2. Son utilisation est facultative. La pulsation du pilote est configurée par le biais d'un paramètre de pilote, en spécifiant un intervalle de temps. S'il existe un paramètre de pulsation de pilote et si son intervalle a une valeur différente de 0, le pilote envoie un document de pulsation au moteur méta-annuaire s'il n'y a aucune communication sur le canal Éditeur pendant l'intervalle de temps spécifié.

L'objectif de la pulsation est de fournir un déclencheur qui permet d'initier une opération à des intervalles réguliers, si le pilote ne communique pas sur le canal Éditeur aussi souvent que vous voulez que l'opération se produise. Personnalisez la configuration de votre pilote ou d'autres outils si vous voulez profiter de la pulsation. Le moteur méta-annuaire accepte le document de pulsation mais n'effectue aucune opération en conséquence.

Pour la plupart des pilotes, aucun paramètre n'est utilisé pour la pulsation dans les exemples de configuration, mais vous pouvez l'ajouter.

Un pilote personnalisé non livré avec Identity Manager peut aussi fournir un document de pulsation si son développeur a écrit le pilote pour qu'il le prenne en charge.

Pour configurer la pulsation, procédez comme suit :

1. Dans iManager, cliquez sur *Identity Manager* > *Présentation de Identity Manager*.
2. Recherchez et sélectionnez l'ensemble de pilotes, puis cliquez sur *Rechercher*.
3. Dans l'écran Présentation de Identity Manager, cliquez sur l'angle supérieur droit de l'icône du pilote, puis sur *Éditer les propriétés*.
4. Dans l'onglet Identity Manager, cliquez sur *Configuration du pilote*, défilez jusqu'à Paramètres de pilote et recherchez Pulsation ou un nom similaire.

   Si un paramètre de pilote existe déjà pour la pulsation, vous pouvez modifier l'intervalle et enregistrer les modifications ; la configuration est alors terminée.

La valeur de l'intervalle ne peut pas être inférieure à 1. Une valeur de 0 signifie que la fonctionnalité est désactivée.

Les minutes sont en général l'unité de temps ; toutefois, certains pilotes peuvent choisir de l'implémenter différemment, par exemple en utilisant des secondes.

5 Si aucun paramètre de pilote n'existe pour la pulsation, cliquez sur Édition XML.

6 Ajoutez un paramètre de pilote comme dans l'exemple suivant, en tant qu'enfant de <publisher-options>. Pour un pilote AD, faites-en un enfant de <driver-options>.

```
<pub-heartbeat-interval display-name="Heart Beat">10</pub-
heartbeat-interval>
```

Suggestion : Si le pilote ne produit pas de document de pulsation après redémarrage, vérifiez le placement du paramètre de pilote dans le XML.

7 Enregistrez les modifications et vérifiez que le pilote est arrêté et redémarré.

Une fois que vous avez ajouté le paramètre de pilote, vous pouvez modifier l'intervalle en utilisant la vue graphique. Une autre option consiste à créer une référence vers une valeur de configuration globale pour l'intervalle. Comme d'autres valeurs de configuration globale, vous pouvez régler la pulsation du pilote au niveau de l'ensemble de pilotes plutôt que pour chaque objet Pilote. Si un pilote n'a pas de valeur de configuration globale et si l'ensemble de pilotes en a une, le pilote hérite de cette dernière.

Voici un exemple de document d'état de pulsation envoyé par le pilote Notes :

```
<nds dtdversion="2.0" ndsversion="8.x">
  <source>
    <product build="20031112_1037" instance="blackcap"
version="2.0">DirXML Driver for Lotus Notes</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <status level="success" type="heartbeat"/>
  </input>
</nds>
```

2.12 Affichage des processus Identity Manager

Pour afficher les événements de traitement Identity Manager, servez-vous de la fonction DSTRACE. Cette fonction ne sert que pour les tests et le dépannage de Identity Manager. Si vous exécutez DSTRACE alors que les pilotes sont en phase de production, le taux d'utilisation du serveur Identity Manager augmente et le traitement des événements risque d'en être très ralenti.

Pour que les processus Identity Manager soient affichés dans DSTRACE, des valeurs sont ajoutées aux objets Ensemble de pilotes et Pilote. Cela peut être fait dans Designer et dans iManager.

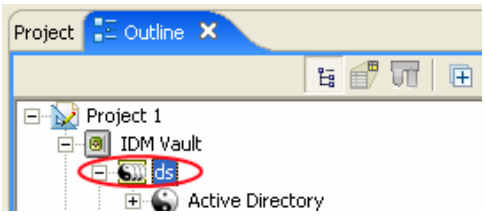
- Section 2.12.1, « Ajout de niveaux de trace dans Designer », page 37
- Section 2.12.2, « Ajout de niveaux de trace dans iManager », page 39
- Section 2.12.3, « Enregistrement des processus Identity Manager dans un fichier », page 40

2.12.1 Ajout de niveaux de trace dans Designer

Vous pouvez ajouter des niveaux de trace à l'objet Ensemble de pilotes ou à chaque objet Pilote.

Ensemble de pilotes

1 Dans un projet ouvert dans Designer, sélectionnez l'objet Ensemble de pilotes dans la vue Aperçu.



2 Cliquez avec le bouton droit de la souris et cliquez sur *Propriétés*, puis cliquez sur *5. Trace*.

3 Définissez les paramètres de trace, puis cliquez sur *OK*. Pour plus d'informations sur les paramètres de trace de l'ensemble de pilotes, reportez-vous au Tableau 2-1 page 37.

Si vous définissez le niveau de trace sur l'objet Ensemble de pilotes, tous les pilotes apparaissent dans les journaux DSTRACE.

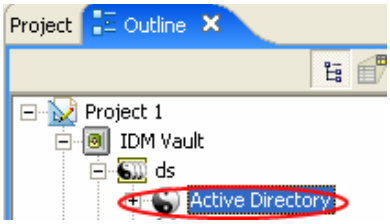
Tableau 2-1 *Paramètres de trace de l'ensemble de pilotes*

Paramètre	Description
Niveau de trace du pilote	Alors que le niveau de trace de l'objet Pilote augmente, la quantité d'informations qui s'affichent dans DSTRACE augmente. Le niveau de trace Un affiche les erreurs, mais pas leur cause. Pour afficher les informations de synchronisation du mot de passe, définissez le niveau de trace sur cinq.
Niveau de trace XSL	DSTRACE affiche les événements XSL. Ne définissez ce niveau de trace que lorsque vous corrigez les feuilles de style XSL. Si vous ne souhaitez pas afficher les informations XSL, définissez le niveau sur zéro.
Port de débogage Java	Permet aux développeurs de joindre un débogueur Java.
Fichier de trace Java	Lorsque ce champ contient une valeur, toutes les informations Java relatives à l'objet Ensemble de pilotes sont copiées dans un fichier. La valeur du champ correspond au correctif du fichier. Si le fichier est spécifié, les informations Java y sont copiées. Si vous n'avez pas besoin de déboguer Java, laissez ce champ vide.

Paramètre	Description
Taille maximum du fichier de trace	Permet de définir une limite pour le fichier de trace Java. Si vous définissez la limite de fichier sur Illimitée, la taille du fichier augmente jusqu'à ce qu'il n'y ait plus de place sur le disque.

Pilote

1 Dans un projet ouvert dans Designer, sélectionnez l'objet Pilote dans la vue Aperçu.



2 Cliquez avec le bouton droit de la souris et cliquez sur *Propriétés*, puis cliquez sur *8. Trace*.

3 Définissez les paramètres de trace, puis cliquez sur *OK*. Pour plus d'informations sur ces paramètres, reportez-vous au Tableau 2-2 page 38.

Si vous définissez les paramètres uniquement sur l'objet Pilote, seules les informations relatives à ce pilote apparaissent dans le journal DSTRACE.

Tableau 2-2 *Paramètres de trace du pilote*

Paramètre	Description
Niveau de trace	Alors que le niveau de trace de l'objet Pilote augmente, la quantité d'informations qui s'affichent dans DSTRACE augmente. Le niveau de trace Un affiche les erreurs, mais pas leur cause. Pour afficher les informations de synchronisation du mot de passe, définissez le niveau de trace sur cinq. Si vous sélectionnez *Use setting from Driver Set (Utiliser le paramètre de l'ensemble de pilotes)*, la valeur associée à l'objet Ensemble de pilotes est utilisée.
Fichier de trace	Spécifiez le nom et l'emplacement du fichier dans lequel sont copiées les informations Identity Manager pour le pilote sélectionné. Si vous sélectionnez *Use setting from Driver Set (Utiliser le paramètre de l'ensemble de pilotes)*, la valeur associée à l'objet Ensemble de pilotes est utilisée.

Paramètre	Description
Taille maximum du fichier de trace	Permet de définir une limite pour le fichier de trace Java. Si vous définissez la limite de fichier sur Illimitée, la taille du fichier augmente jusqu'à ce qu'il n'y ait plus de place sur le disque. Si vous sélectionnez *Use setting from Driver Set (Utiliser le paramètre de l'ensemble de pilotes)*, la valeur associée à l'objet Ensemble de pilotes est utilisée.
Nom de la trace	En préfixe des messages de trace du pilote, figure la valeur saisie et non le nom du pilote. Utilisez ce paramètre si le nom du pilote est particulièrement long.

2.12.2 Ajout de niveaux de trace dans iManager

Vous pouvez ajouter des niveaux de trace à l'objet Ensemble de pilotes ou à chaque objet Pilote.

Ensemble de pilotes

1. Dans iManager, sélectionnez *Identity Manager* > *Présentation de Identity Manager*.
2. Recherchez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.
3. Cliquez sur le nom de l'ensemble de pilotes.

4. Sélectionnez l'onglet *Divers* correspondant à l'objet Ensemble de pilotes.
5. Définissez les paramètres de trace, puis cliquez sur *OK*. Pour plus d'informations sur ces paramètres, reportez-vous au Tableau 2-1 page 37.

Pilote

1. Dans iManager, sélectionnez *Identity Manager* > *Présentation de Identity Manager*.
2. Recherchez l'objet Ensemble de pilotes dans lequel se trouve le pilote, puis cliquez sur *Rechercher*.
3. Cliquez dans l'angle supérieur droit de l'objet Pilote, puis cliquez sur *Éditer les propriétés*.
4. Sélectionnez l'onglet *Divers* correspondant à l'objet Pilote.
5. Définissez les paramètres de trace, puis cliquez sur *OK*. Pour plus d'informations, reportez-vous au Tableau 2-2 page 38.

Remarque : l'option *Use setting from Driver Set (Utiliser le paramètre de l'ensemble de pilotes)* n'existe pas dans iManager.

2.12.3 Enregistrement des processus Identity Manager dans un fichier

L'enregistrement des processus Identity Manager dans un fichier se fait par le biais du paramètre de l'objet Pilote ou de DSTRACE. Le paramètre de l'objet Pilote est le paramètre Fichier de trace.

Les méthodes suivantes permettront de capturer et d'enregistrer les processus Identity Manager sous différents systèmes d'exploitation avec DSTRACE.

NetWare

Utilisez `DSTRACE.NLM` pour afficher les messages de trace sur la console du système ou dans un fichier (`SYS:\SYSTEM\DSTRACE.LOG`). `DSTRACE.NLM` affiche les messages de trace dans l'écran DSTRACE Console (Console DSTRACE).

1. Saisissez `DSTRACE.NLM` sur la console du serveur.

   Le fichier `DSTRACE.NLM` est alors chargé dans la mémoire.
2. Saisissez `DSTRACE SCREEN ON` sur la console du serveur.

   Affiche les messages de trace dans l'écran de la console DSTRACE.
3. Saisissez `DSTRACE FILE ON` sur la console du serveur.

   Enregistre les messages de trace envoyés à la console DSTRACE dans le fichier `DSTRACE.LOG`.
4. Saisissez `DSTRACE -ALL` sur la console du serveur.

   Désactive tous les drapeaux de trace.
5. Saisissez `DSTRACE +DXML DSTRACE +DVRS` sur la console du serveur.

   Affiche les événements Identity Manager.
6. Saisissez `DSTRACE+TAGS DSTRACE +TIME` sur la console du serveur.

   Affiche les balises et les tampons horaires des messages.
7. Basculez vers l'écran de la console DSTRACE et attendez que l'événement soit passé.
8. Revenez à la console du serveur.
9. Saisissez `DSTRACE FILE OFF` sur la console du serveur.

   Arrête la capture des messages de trace dans le fichier-journal. Arrête également la consignation des informations dans le fichier.
10. Ouvrez le fichier `DSTRACE.LOG` dans un éditeur de texte et recherchez l'événement ou l'objet que vous avez modifié.

Fenêtres

1. Sélectionnez Panneau de configuration > NDS Services > dstrace.dlm, puis cliquez sur *Démarrer*.

   La fenêtre NDS Server Trace Utility (Utilitaire de trace du serveur NDS) s'ouvre.

2 Sélectionnez *Éditer* > *Options*, puis cliquez sur *Effacer tout*.

   Tous les drapeaux par défaut sont effacés.

3 Sélectionnez *DirXML* et *DirXML Drivers (Pilotes DirXML)*.

4 Cliquez sur OK.

5 Sélectionnez *Fichier* > *Nouveau*.

6 Indiquez le nom de fichier et l'emplacement dans lequel vous souhaitez enregistrer les informations DSTRACE, puis cliquez sur Ouvrir.

7 Attendez que l'événement se produise.

8 Sélectionnez *Fichier* > *Fermer*.

   Cela arrête la copie des informations dans le fichier-journal.

9 Ouvrez le fichier dans un éditeur de texte et recherchez l'événement ou l'objet que vous avez modifié.

UNIX

1 Saisissez `ndstrace` pour lancer l'utilitaire ndstrace.

2 Saisissez `set ndstrace=nodebug`

   Désactive tous les drapeaux de trace définis.

3 Saisissez `set ndstrace on`

   Affiche les messages de trace sur la console.

4 Saisissez `set ndstrace file on`

   Capture les messages de trace dans le fichier `ndstrace.log` situé dans le répertoire d'installation de eDirectory. Par défaut, il s'agit du répertoire `/var/nds`.

5 Saisissez `set ndstrace=+dxml`

   Affiche les événements Identity Manager.

6 Saisissez `set ndstrace=+dvrs`

   Affiche les événements du pilote Identity Manager.

7 Attendez que l'événement se produise.

8 Saisissez `set ndstrace file off`

   Arrête la consignation des informations dans le fichier.

9 Saisissez `exit` pour quitter l'utilitaire ndstrace.

10 Ouvrez le fichier dans un éditeur de texte. Recherchez l'événement ou l'objet qui a été modifié.

iMonitor

iMonitor permet d'obtenir les informations DSTRACE depuis un navigateur Web. Peu importe l'emplacement dans lequel s'exécute Identity Manager. Ces fichiers permettent l'exécution d'iMonitor :

- `NDSIMON.NLM`, pour une exécution sur NetWare.
- `NDSIMON.DLM`, pour une exécution sous Windows.

- `ndsimonitor`, pour une exécution sous UNIX.

1. Accédez à iMonitor depuis l'adresse http://*server_ip*:8008/nds.

   Le port 8008 est le port par défaut.
2. Saisissez le nom et le mot de passe d'un utilisateur doté de droits administratifs, puis cliquez sur *Login*.
3. À gauche, sélectionnez *Configuration de Trace*.
4. Cliquez sur *Effacer tout*.
5. Sélectionnez DirXML et les pilotes DirXML.
6. Cliquez sur *Trace activée*.
7. À gauche, sélectionnez *Historique de trace*.
8. Cliquez sur le document dont la date de la dernière modification est Actuel pour afficher la trace instantanément.
9. Modifiez l'*Intervalle de rafraîchissement* si vous souhaitez afficher les informations plus souvent.
10. À gauche, sélectionnez *Configuration de Trace* puis cliquez sur *Trace désactivée* pour désactiver le suivi.
11. Pour afficher l'historique du suivi, sélectionnez Historique de trace. Les fichiers sont différenciés par leur tampon horaire.

S'il vous faut une copie du fichier HTML, son emplacement par défaut est le suivant :

- NetWare : `SYS:\SYSTEM\ndsimon\DSTRACE*.htm`
- Windows : *`Drive_letter`*`:\Novell\NDS\ndsimon\dstrace\*.htm`
- UNIX : `/var/nds/dstrace/*.htm`

Configuration d'un système connecté

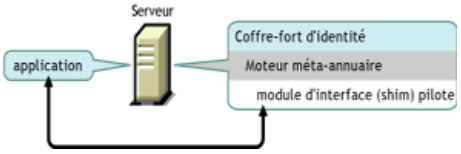
3

Cette section présente des renseignements sur les éléments suivants :

3.1 Présentation

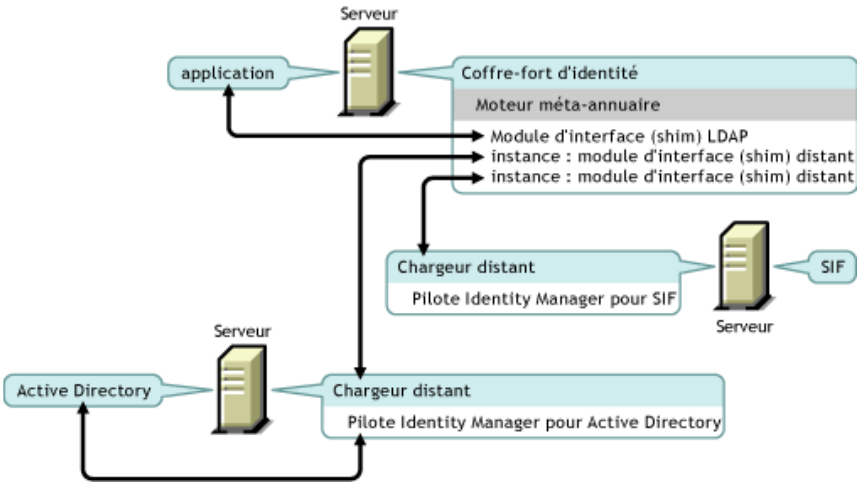
Comme le montre l'illustration suivante, le moteur méta-annuaire s'exécute sur un serveur, dans eDirectory. Le module d'interface pilote Identity Manager et le pilote configuré correspondant communiquent avec une application et avec le moteur méta-annuaire.

Figure 3-1 *Moteur méta-annuaire intégré à eDirectory*



Comme le montre l'illustration suivante, le système connecté étend les fonctionnalités Identity Manager sur diverses applications :

Figure 3-2 *Système connecté avec chargeur distant*



Le système connecté exige un chargeur distant. Ce service permet au moteur méta-annuaire d'échanger des données avec les pilotes Identity Manager qui s'exécutent sous forme de processus différents et à des emplacements différents, notamment :

- Comme processus séparés sur le serveur sur lequel le moteur méta-annuaire s'exécute

  Le moteur méta-annuaire est intégré au processus eDirectory. Les pilotes Identity Manager peuvent s'exécuter sur le même serveur que le moteur méta-annuaire. En fait, ils peuvent faire partie du même processus que ce moteur.

  Toutefois, pour des raisons stratégiques, vous voudrez peut-être que le pilote Identity Manager s'exécute en tant que processus séparé sur le serveur. En général, les pilotes Identity Manager peuvent toutefois s'exécuter sur des serveurs distincts.

  Si le pilote s'exécute en tant que processus séparé, le chargeur distant fournit un canal de communication entre le moteur méta-annuaire et le pilote.

- Sur des serveurs autres que celui sur lequel le moteur méta-annuaire s'exécute

  Certains pilotes Identity Manager ne peuvent pas s'exécuter sur le même serveur que le moteur méta-annuaire. Le chargeur distant permet d'exécuter le moteur méta-annuaire dans un environnement tout en exécutant un pilote Identity Manager sur un serveur dont l'environnement est différent. Par exemple, vous ne pouvez pas exécuter un pilote Active Directory sur un serveur NetWare. Le moteur méta-annuaire peut s'exécuter sur le serveur NetWare tandis que le chargeur distant s'exécute sur un serveur Active Directory.

  Scénario : serveurs séparés. Le moteur méta-annuaire s'exécute sur un serveur NetWare. Exécutez le pilote Identity Manager pour Active Directory. Ce pilote ne peut pas s'exécuter sur un serveur NetWare car il doit s'exécuter dans un environnement Active Directory. Installez et exécutez le chargeur distant sur un serveur Windows 2003. Le chargeur distant constitue un canal de communication entre le pilote Active Directory et le moteur méta-annuaire.

  Scénario : non-Hôte. Le moteur méta-annuaire s'exécute sous Solaris. Communiquez avec le système NIS sur lequel vous voulez provisionner les comptes utilisateur. Ce système n'héberge généralement pas le moteur méta-annuaire. Installez le chargeur distant et le pilote Identity Manager pour NIS sur le système NIS. Le chargeur distant sur le système NIS exécute le pilote NIS et permet au moteur méta-annuaire et au pilote NIS d'échanger des données.

Identity Manager 3 offre des fonctionnalités de serveur distant via dirxml_remote, rdxml ou dirxml_jremote.

Dirxml_remote

Dirxml_remote est un exécutable qui permet au moteur méta-annuaire de communiquer avec les pilotes Identity Manager qui s'exécutent sous Windows.

La console du chargeur distant utilise `dirxml_remote.exe`. Si, dans la ligne de commande, vous spécifiez `dirxml_remote.exe` sans aucun paramètre, l'assistant d'application du chargeur distant est lancé. Si vous saisissez `dirxml_remote.exe` et si vous spécifiez des paramètres, le chargeur distant démarre.

Rdxml

Rdxml est un exécutable qui permet au moteur méta-annuaire de communiquer avec les pilotes Identity Manager qui s'exécutent dans les environnements Solaris, Linux ou AIX.

Rdxml prend en charge les pilotes natifs ou Java.

Dirxml_jremote

Dirxml_jremote est un chargeur distant Java pur. Il permet d'échanger des données entre le moteur méta-annuaire qui s'exécute sur un serveur et les pilotes Identity Manager qui s'exécutent à un autre emplacement dans lequel rdxml et Dirxml_jremote ne fonctionnent pas. Il devrait fonctionner sur n'importe quel système doté d'un JRE compatible (1.4.0 au minimum, 1.4.2 ou supérieur recommandé) et de sockets Java, mais il n'est officiellement pris en charge que sur les systèmes suivants :

- HP-UX
- AS/400
- OS/390
- z/OS

Présentation : tâches principales

Pour utiliser le chargeur distant, vous devez accomplir les tâches suivantes :

- Si vous prévoyez d'utiliser SSL (Secure Socket Layer), fournissez des certificats pour garantir le transfert sécurisé des données.
- Installez, configurez et exécutez le chargeur distant.
- Importez, configurez et lancez le pilote Identity Manager.

Certains administrateurs préfèrent importer et configurer le pilote Identity Manager avant de configurer le chargeur distant. Par exemple, si le pilote est déjà en cours d'exécution, vous pouvez souhaiter l'activer à distance.

D'un autre côté, si le chargeur distant est en cours d'exécution, vous pouvez importer, configurer et lancer le pilote, puis vérifier immédiatement si la communication se fait correctement entre le moteur méta-annuaire, le chargeur distant et le pilote Identity Manager.

3.2 Sécurisation du transfert des données

Si vous envisagez d'utiliser SSL (Secure Socket Layer) pour sécuriser le transfert des données, effectuez les tâches suivantes :

1. Créez un certificat de serveur.

   Si vous n'avez pas l'habitude des certificats, créez-en un.

   Toutefois, s'il existe déjà un certificat de serveur SSL et si vous avez l'habitude d'utiliser les certificats SSL, vous pouvez utiliser le certificat existant sans en créer un nouveau.

   Lorsqu'un serveur est intégré à une arborescence, eDirectory crée les certificats par défaut suivants :

   - SSL CertificateIP
   - SSL CertificateDNS
2. Exportez un certificat signé automatiquement.

3.2.1 Création d'un certificat de serveur

1 Dans Novell iManager, cliquez sur *Serveur de certificats Novell* > *Créer un certificat de serveur*.

2 Sélectionnez le serveur qui détiendra le certificat et donnez un surnom à ce dernier (par exemple, remotecert).

Important : il est préférable de ne pas utiliser d'espaces dans le surnom du certificat. Par exemple, utiliser remotecert plutôt que remote cert.

N'oubliez pas de noter le surnom. Vous l'utiliserez pour le nom KMO dans les paramètres de connexion distants du pilote.

---

3 Laissez la valeur de la méthode de création sur *Standard*, puis cliquez sur *Suivant*.

4 Vérifiez l'écran Résumé, cliquez sur *Terminer*, puis sur *Fermer*.

Vous avez créé un certificat de serveur. Passez à la Section 3.2.2, « Exportation d'un certificat signé automatiquement », page 46.

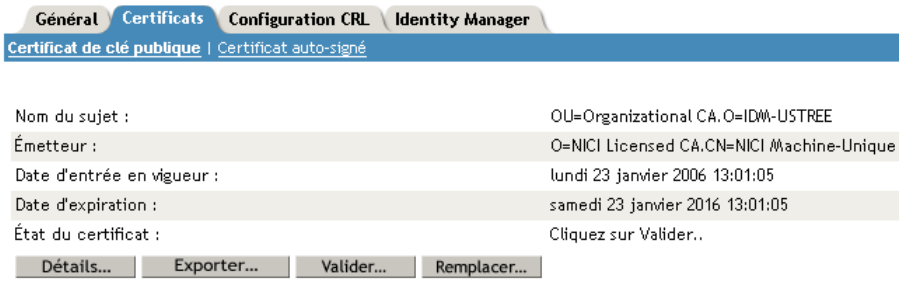
3.2.2 Exportation d'un certificat signé automatiquement

1 Dans iManager, cliquez sur *Administration eDirectory* > *Modifier l'objet*.

2 Recherchez et sélectionnez l'autorité de certification dans le conteneur Sécurité, puis cliquez sur *OK*.

Le nom de l'autorité de certification (CA) provient du nom de l'arborescence (Treename-CA.Security).

3 Dans l'onglet *Certificat*, cliquez sur *Certificat signé automatiquement*, puis sur *Exporter*.



4 Dans l'assistant d'exportation du certificat, cliquez sur *Non*, puis sur *Suivant*.

Vous ne devez pas exporter la clé privée avec le certificat.

5 Sélectionnez un *fichier au format Base64* (par exemple, akranes-tree CA.b64), puis cliquez sur *Suivant*.

6 Cliquez sur le lien permettant d'*enregistrer le certificat exporté dans un fichier*, spécifiez un nom de fichier et un emplacement, puis cliquez sur *Enregistrer*.

Les noms Rootfile doivent être suivis de l'extension .pem.

7 Dans la boîte de dialogue Enregistrer sous, copiez ce fichier dans un répertoire local.

8 Cliquez sur *Fermer*.

3.3 Installation des chargeurs à distance

Cette section présente des renseignements sur les éléments suivants :

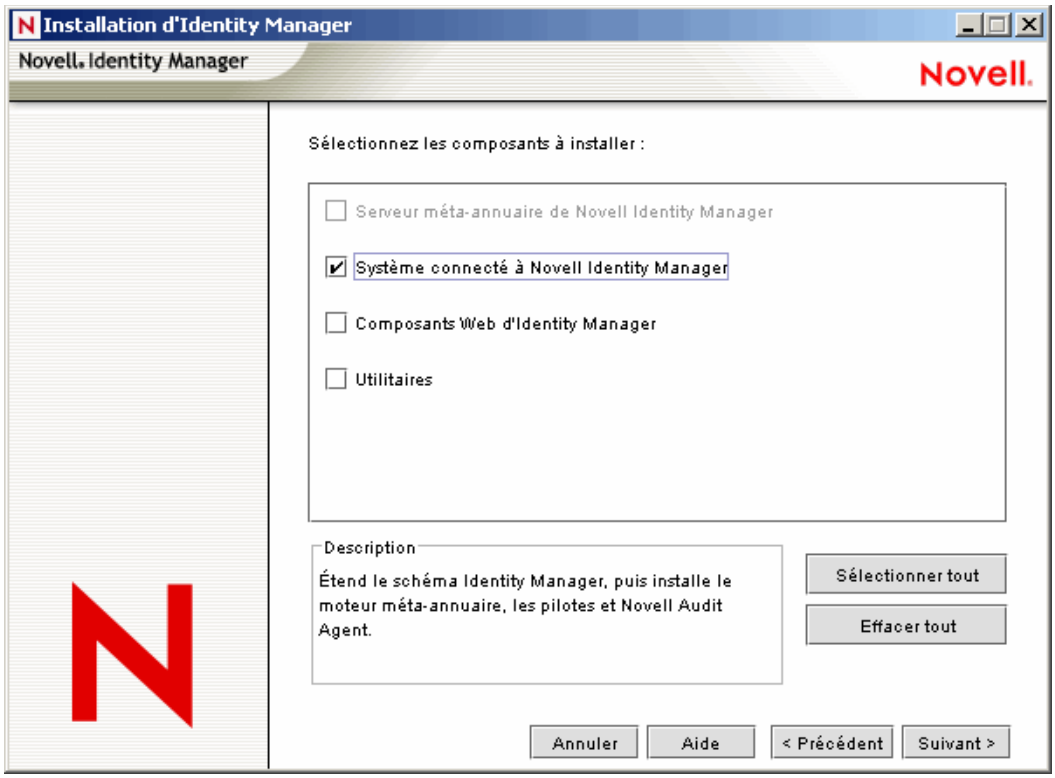
3.3.1 Installation des chargeurs distants

Cette section présente des renseignements sur les éléments suivants :

- « Installation d'un chargeur distant sur un serveur Windows » page 48
- « Installation d'un chargeur distant sous Solaris, Linux ou AIX » page 49
- « Installation d'un chargeur distant sur HP-UX, AS/400, OS/390 ou z/OS » page 50

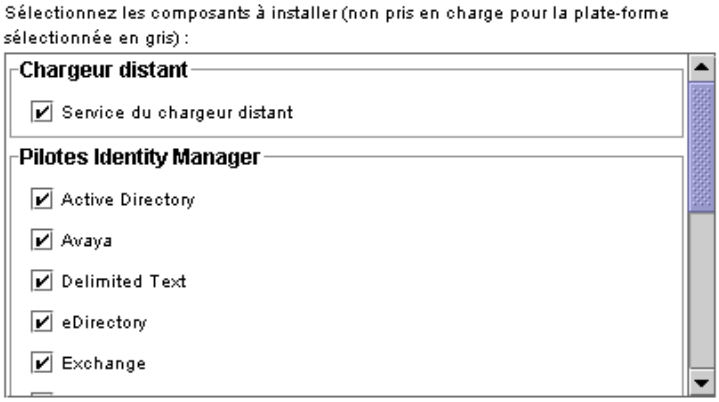
Installation d'un chargeur distant sur un serveur Windows

1. Exécutez le programme d'installation Identity Manager 3 (par exemple, \nt\install.exe).
2. Affichez la page de bienvenue, acceptez l'accord de licence, puis affichez les deux pages Présentation.
3. Dans la boîte de dialogue Installation Identity Manager, désélectionnez tous les composants à l'exception de *Système connecté*, puis cliquez sur *Suivant*.



4. Sélectionnez un emplacement pour le système connecté (le chargeur distant et les modules d'interface pilote distants), puis cliquez sur *Suivant*.

5 Sélectionnez *Service du chargeur distant* et les modules d'interface pilote du chargeur distant, puis cliquez sur *Suivant*.



6 Accusez réception de la contrainte d'activation, affichez les produits à installer, puis cliquez sur *Terminer*.

7 Indiquez si vous voulez placer l'icône de la console du chargeur distant sur votre bureau.

Installation d'un chargeur distant sous Solaris, Linux ou AIX

Avant de suivre les instructions de cette section, vous devez avoir téléchargé et décompressé Identity Manager 3. Si vous devez télécharger Identity Manager, rendez-vous sur le site Web de téléchargement de Novell (http://download.novell.com).

Une fois que vous avez décompressé le fichier Identity Manager 3 que vous avez téléchargé du site Web Novell, procédez aux étapes suivantes :

1 Exécutez un des fichiers d'installation suivants, selon votre plate-forme :

- dirxml_solaris.bin
- dirxml_linux.bin
- dirxml_aix.bin

2 Après avoir accepté l'accord de licence, appuyez sur Entrée pour arriver à la page de sélection des paramètres d'installation.

```
===============================================================================
Choose Install Set
------------------

Please choose the Install Set to be installed by this installer.

  ->1- Metadirectory Server
    2- Connected System Server
    3- Web-based Administrative Server

    4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
   :
```

3 Sélectionnez Serveur pour système connecté en saisissant 2, puis appuyez sur Entrée.

4 Dans l'écran Résumé avant installation, revoyez les composants que vous avez sélectionnés pour installation, puis appuyez sur Entrée.

```
================================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Install Set
    Connected System Server

Product Components:
    LDAP Driver,
    SAP Driver,
    JDBC Driver,
    Delimited Text Driver,
    Notes Driver,
    Remote Loader,
    Groupwise Driver,
    AVAYA Driver,
    SOAP Driver,
    REMEDY Driver


PRESS <ENTER> TO CONTINUE:
```

Installation d'un chargeur distant sur HP-UX, AS/400, OS/390 ou z/OS

Les plates-formes HP-UX, AS/400, OS/390 et z/OS exigent le chargeur distant Java.

1 Créez un répertoire sur le système cible sur lequel vous voulez exécuter le chargeur distant Java.

2 À partir du CD Identity Manager 3 ou de l'image téléchargée, copiez le fichier approprié dans le sous-répertoire `/java_remoteloader` du répertoire créé à l'étape 1 :

Plate-forme	Fichier
HP-UX AS/400	dirxml_jremote.tar.gz dirxml_jremote.tar.gz dirxml_jremote_mvs.tar
z/OS OS/390	dirxml_jremote_mvs.tar

3 Pour HP-UX, AS/400 ou z/OS, décompressez le fichier dirxml_jremote.

4 Décompressez le fichier que vous venez de copier.

Le chargeur distant Java est désormais prêt à être configuré. Le fichier .tar ne comportant pas de pilote, vous devez copier manuellement les pilotes dans le répertoire lib. Ce répertoire se trouve sous le répertoire dans lequel la décompression a été effectuée.

Pour plus d'informations sur MVS, décompressez le fichier dirxml_jremote_mvs.tar. Reportez-vous ensuite au document usage.html.

3.3.2 Configuration du chargeur distant

Le chargeur distant peut héberger les modules d'interface pilote de l'application Identity Manager contenus dans les fichiers .dll, .so ou .jar. Le chargeur distant Java héberge les modules d'interface pilote Java. Il ne charge ni n'héberge les modules d'interface pilote natifs (C++).

• « Configuration du chargeur distant sous Windows » page 51

- « Configuration du chargeur distant à l'aide des options de ligne de commande » page 56
- « Démarrage du chargeur distant » page 62
- « Arrêt du chargeur distant » page 64

Configuration du chargeur distant sous Windows

- « Utilisation de l'utilitaire Console du chargeur distant » page 51
- « Ajout d'une instance du chargeur distant » page 52
- « Modification d'une instance du chargeur distant » page 56

Utilisation de l'utilitaire Console du chargeur distant

La console du chargeur distant ne fonctionne que sous Windows. Elle permet de gérer tous les pilotes Identity Manager qui s'exécutent sous le chargeur distant sur l'ordinateur en question :

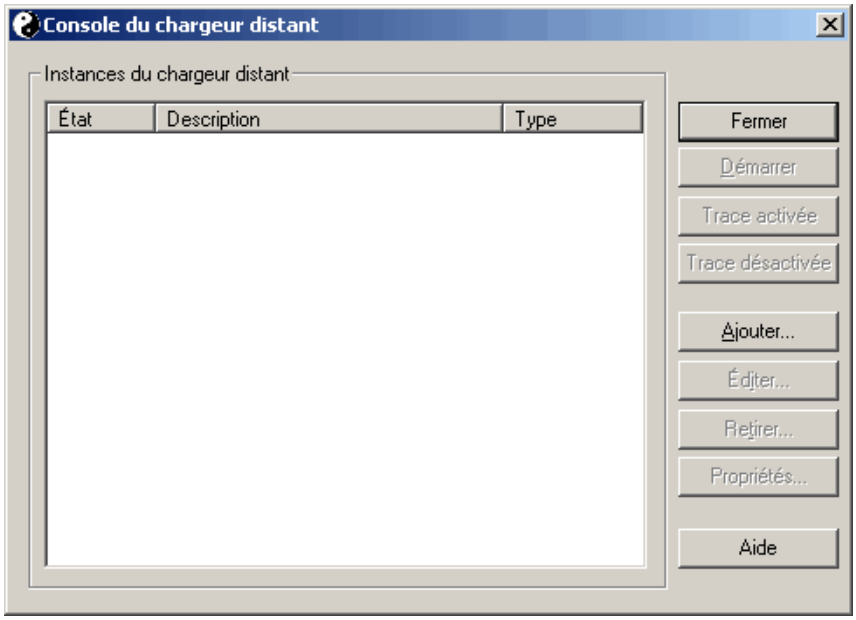
Si vous mettez à niveau vers Identity Manager 3, la console détecte et importe les instances existantes du chargeur distant. Pour être automatiquement importées, les configurations du pilote doivent être stockées dans le répertoire du chargeur distant, en général `c:\novell\remoteloader`. Vous pouvez ensuite utiliser la console pour gérer les pilotes distants.

Pour lancer la console du chargeur distant, cliquez sur l'icône correspondante sur le Bureau.

Figure 3-3 *Icône de la console du chargeur distant*

La console du chargeur distant permet de lancer, arrêter, ajouter, supprimer et modifier chaque instance d'un service du chargeur distant.

Figure 3-4 *Console du chargeur distant*



Si, dans la ligne de commande, vous saisissez `dirxml_remote.exe` sans aucun paramètre, l'assistant d'application du chargeur distant est lancé.

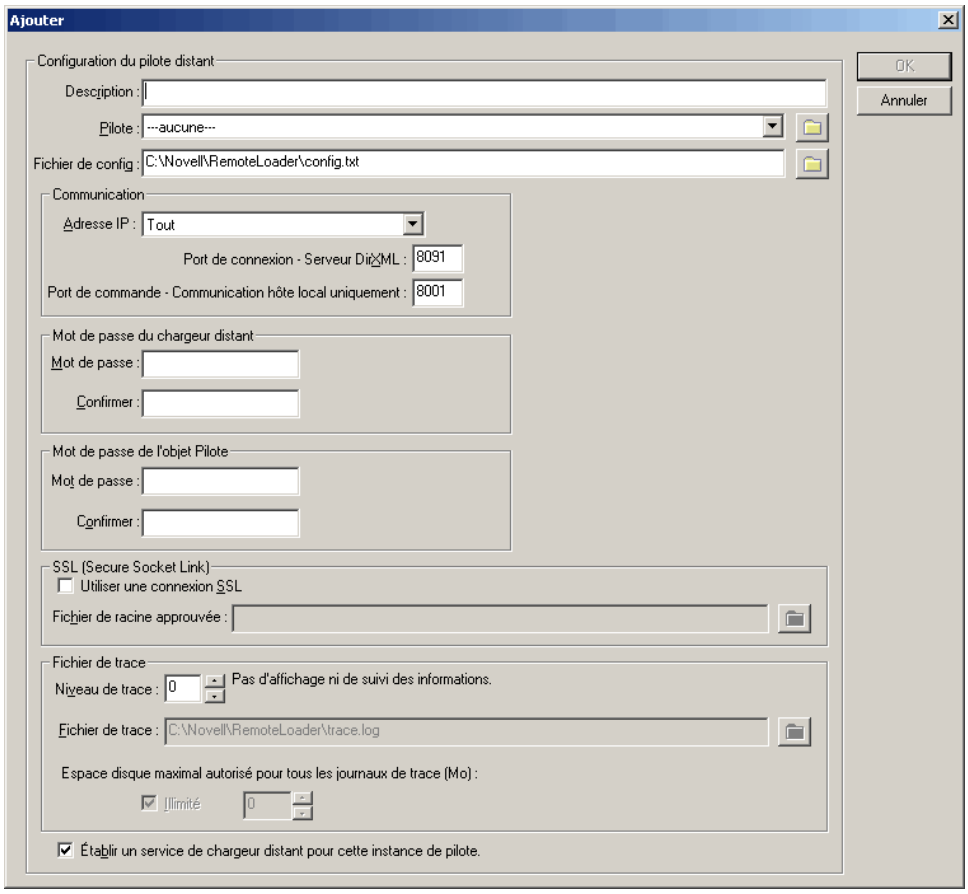
Remarque : l'utilisation conjointe de la console et de l'assistant peut avoir des effets inattendus. Nous vous recommandons donc d'utiliser la console en avançant et de mettre à niveau vos configurations existantes dans la console.

Ajout d'une instance du chargeur distant

Pour ajouter une instance du chargeur distant, cliquez sur Ajouter, puis donnez les informations suivantes :

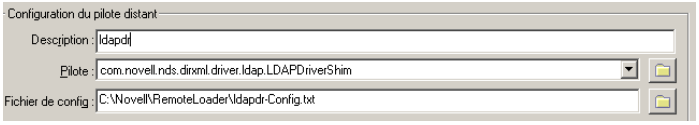
- « Configuration du pilote distant » page 53
- « Paramètres de communication » page 54
- « Mot de passe du chargeur distant » page 54
- « Mot de passe de l'objet Pilote » page 55
- « SSL (Secure Socket Layer) » page 55
- « Fichier de trace » page 55
- « Établissement d'un service de chargeur distant pour cette instance de pilote » page 56

Figure 3-5 *Paramètres de configuration du chargeur distant*



Configuration du pilote distant

Figure 3-6 *Configuration du pilote distant*

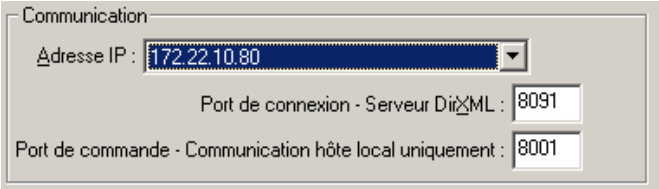


- Description : spécifiez une description pour identifier l'instance du chargeur distant.
- Pilote : recherchez et sélectionnez le module d'interface pilote.
- Fichier de config : indiquez le nom du fichier de configuration.

  La console du chargeur distant place les paramètres de configuration dans ce fichier texte et utilise ces paramètres lorsqu'elle s'exécute.

Paramètres de communication

Figure 3-7 *Paramètres de communication*



- Adresse IP : spécifiez l'adresse IP sur laquelle le chargeur distant écoute les connexions à partir du serveur méta-annuaire.
- Port de connexion - serveur méta-annuaire Spécifiez le port TCP sur lequel le chargeur distant écoute les connexions à partir du serveur méta-annuaire.

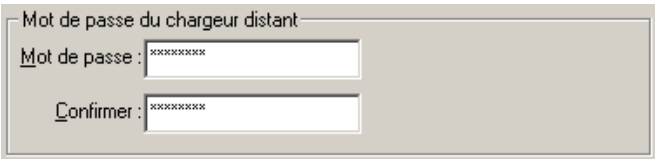
  Le port TCP/IP par défaut pour cette connexion est le port 8090. Avec chaque nouvelle instance créée, le numéro du port par défaut passe automatiquement au numéro supérieur.
- Port de commande - Communication hôte local uniquement : spécifiez le numéro du port TCP sur lequel un chargeur distant écoute les commandes telles que l'arrêt et la modification du niveau de trace.

  Chaque instance du chargeur distant qui s'exécute sur cette machine doit avoir un numéro de port de commande différent. Le port de commande par défaut est 8000. Avec chaque nouvelle instance que vous créez, le numéro du port par défaut passe automatiquement au numéro supérieur.

Remarque : plusieurs instances du chargeur distant peuvent être exécutées sur le serveur qui héberge les différentes instances de pilote ; il suffit pour cela de spécifier des ports de connexion et des ports de commande différents.

Mot de passe du chargeur distant

Figure 3-8 *Mot de passe du chargeur distant*

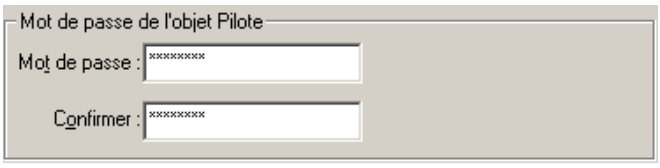


- Mot de passe : ce mot de passe permet de contrôler l'accès à une instance du chargeur distant pour un pilote.

  Le mot de passe doit être identique (y compris la casse) au mot de passe saisi au moment de la configuration du pilote dans la zone de texte Saisissez le mot de passe du chargeur distant, à la section « Authentification » de la page « Configuration Identity Manager ».
- Confirmez : ressaisissez le mot de passe.

Mot de passe de l'objet Pilote

Figure 3-9 *Mot de passe de l'objet Pilote*

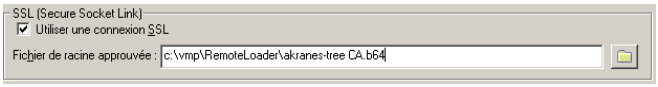


- Mot de passe : le chargeur distant utilise ce mot de passe pour s'authentifier auprès du serveur méta-annuaire.

  Le mot de passe doit être identique au mot de passe saisi au moment de la configuration du pilote dans la zone de texte Mot de passe de l'objet Pilote de la page Configuration du pilote.
- Confirmer : ressaisissez le mot de passe.

SSL (Secure Socket Layer)

Figure 3-10 *SSL (Secure Socket Layer)*

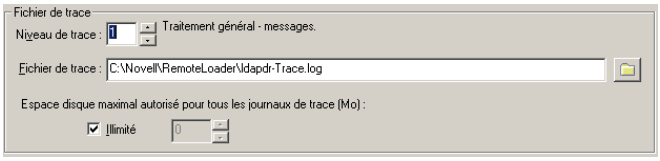


- Utiliser une connexion SSL : sélectionnez cette option pour spécifier une connexion SSL.
- Fichier de racine approuvée : localisez et sélectionnez un fichier de racine approuvée.

  Il s'agit du certificat signé automatiquement issu de l'autorité de certification organisationnelle de l'arborescence eDirectory. Reportez-vous à la Section 3.2.2, « Exportation d'un certificat signé automatiquement », page 46.

Fichier de trace

Figure 3-11 *Fichier de trace*



- Niveau de trace : définissez un niveau de trace supérieur à zéro pour afficher une fenêtre de trace contenant les messages d'information émis par le chargeur distant et par le pilote. Le paramètre de niveau de trace le plus fréquent est le niveau 3.

  Si le niveau de trace est défini sur 0, la fenêtre de trace ne s'ouvre pas et n'affiche pas de message.
- Ficher de trace : spécifiez le nom du fichier de trace dans lequel écrire les messages de trace.

  Chaque instance du chargeur distant exécutée sur une machine spécifique doit utiliser un fichier de trace différent. Les messages de trace ne sont consignés dans le fichier de trace que si le niveau de trace est supérieur à zéro.

- Espace disque maximal autorisé pour tous les journaux de trace (Mo) : spécifiez la taille maximum que les données du fichier de trace peuvent occuper sur le disque pour l'instance en question.

Établissement d'un service de chargeur distant pour cette instance de pilote

Figure 3-12 *Établissement d'un service de chargeur distant pour cette instance de pilote*

- Pour configurer en tant que service l'instance du chargeur distant, sélectionnez cette option. Lorsqu'elle est activée, le système d'exploitation démarre automatiquement le chargeur distant au démarrage de l'ordinateur.

Modification d'une instance du chargeur distant

1. Dans la colonne Description, sélectionnez l'instance du chargeur distant.
2. Cliquez sur *Arrêter*, saisissez le mot de passe du chargeur distant puis cliquez sur *OK*.
3. Cliquez sur *Éditer*, puis modifiez les informations de configuration. Les champs sont les mêmes que pour l'ajout d'une instance du chargeur distant.

Configuration du chargeur distant à l'aide des options de ligne de commande

Pour exécuter le chargeur distant, toutes les plates-formes utilisent un fichier de configuration (par exemple, LDAPShim.txt). Vous pouvez créer ou modifier un fichier de configuration à l'aide des options de ligne de commande. Les instructions suivantes donnent des informations sur les principaux paramètres du fichier de configuration. Afin d'obtenir des informations sur d'autres paramètres, reportez-vous à l'Annexe B, « Options de configuration d'un chargeur distant », page 263.

1. Ouvrez un éditeur de texte.
2. Facultatif : spécifiez une description à l'aide de l'option -description.

Option	Autre nom	Paramètre	Description
-description	-desc	brève description	Spécifiez une chaîne de description abrégée (par exemple, SAP) pour le titre de la fenêtre de trace et pour la consignation de Nsure Audit. Exemple : -description SAP -desc SAP La console du chargeur distant place les formes longues des options dans les fichiers de configuration. Vous pouvez utiliser soit la forme longue (par exemple, -description), soit la forme abrégée (par exemple, -desc).

3. Spécifiez le port TCP/IP que doit utiliser l'instance du chargeur distant à l'aide de l'option -commandport.

Option	Autre nom	Paramètre	Description
-commandport	-cp	Numéro de port	Spécifie le port TCP/IP utilisé par l'instance du chargeur distant à des fins de contrôle. Si l'instance du chargeur distant héberge un module d'interface pilote de l'application, le port de commande est un port utilisé par une autre instance du chargeur distant pour communiquer avec l'instance qui héberge le module d'interface pilote. Si l'instance du chargeur distant envoie une commande à une instance qui héberge un module d'interface d'application, le port de commande est le port utilisé par cette dernière instance. Si le port de commande n'est pas spécifié, le port 8000 est utilisé par défaut. Plusieurs instances du chargeur distant peuvent être exécutées sur le même serveur qui héberge différentes instances de pilote ; il suffit de spécifier des ports de connexion et des ports de commande différents. Exemple : -commandport 8001 -cp 8001

4 Spécifiez les paramètres de connexion au serveur méta-annuaire sur lequel s'exécute le module d'interface pilote distant Identity Manager à l'aide de l'option -connection.

Saisissez -connection "*parameter* [parameter] [parameter]".

Par exemple, saisissez un des éléments suivants :

```
-connection "port=8091 rootfile=server1.pem"
-conn "port=8091 rootfile=server1.pem"
```

Tous les paramètres doivent être entre guillemets. Voici quelques paramètres possibles :

Option	Autre nom	Paramètre	Description
-connection	-conn	Chaîne de configuration de connexion	Spécifie les paramètres de connexion à utiliser pour la connexion au serveur méta-annuaire sur lequel est exécuté le module d'interface pilote distant Identity Manager. Par défaut, la méthode de connexion utilisée pour le chargeur distant est TCP/IP avec SSL. Le port TCP/IP par défaut pour cette connexion est 8090. Plusieurs instances du chargeur distant peuvent s'exécuter sur le même serveur. Chaque instance du chargeur distant héberge une instance du module d'interface pilote de l'application Identity Manager. Différenciez les multiples instances du chargeur distant en spécifiant des ports de connexion et des ports de commande différents pour chaque instance du chargeur distant. Exemple : -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"

Option	Autre nom	Paramètre	Description
port		Numéro de port décimal	Un paramètre requis. Il spécifie le port TCP/IP sur lequel le chargeur distant écoute des connexions du module d'interface pilote distant. Exemple : port=8090
adresse		adresse IP	Un paramètre facultatif. Spécifie que le chargeur distant écoute à partir d'une adresse IP locale spécifique. Cette information est utile si le serveur qui héberge le chargeur distant possède plusieurs adresses IP et si ce dernier doit utiliser une seule adresse. Vous disposez de trois options : address=*address number* address='localhost' Don't use this parameter. Si vous n'utilisez pas l'option -address, le chargeur distant écoute sur toutes les adresses IP locales. Exemple : address=137.65.134.83
rootfile			Un paramètre conditionnel. Si vous exécutez SSL et si vous souhaitez que le chargeur distant communique avec un pilote natif, saisissez `rootfile='trusted certname'`

keystore			Paramètres conditionnels. Cette option est utilisée uniquement pour les modules d'interface d'application Identity Manager contenus dans les fichiers .JAR.
			
			Spécifie le nom du fichier keystore Java qui contient le certificat de racine approuvée de l'émetteur du certificat utilisé par le module d'interface distant. Il s'agit en général de l'autorité de certification de l'arborescence eDirectory qui héberge le module d'interface pilote distant.
			
			Si vous exécutez SSL et si vous souhaitez que le chargeur distant communique avec un pilote Java, saisissez une paire clé-valeur :
			
			`keystore='keystorename'`
			`storepass='password'`

-storepass		storepass	Cette option est utilisée uniquement pour les modules d'interface d'application Identity Manager contenus dans les fichiers .JAR. Spécifie le mot de passe du fichier keystore Java indiqué par le paramètre keystore. Exemple : storepass=mypassword Cette option ne s'applique qu'au chargeur distant Java.

5 Facultatif : spécifiez un paramètre de trace à l'aide de l'option -trace.

Option	Autre nom	Paramètre	Description
-trace	-t	Nombre entier	Spécifie le niveau de trace. Cette option est utilisée uniquement lorsqu'un module d'interface d'application est hébergé. Les niveaux de trace correspondent à ceux utilisés sur le serveur de méta-annuaire. Exemple : -trace 3 -t 3

6 Facultatif : spécifiez un fichier de trace à l'aide de l'option -tracefile.

Option	Autre nom	Paramètre	Description
-tracefile	tf	nom_fichier	Spécifie le fichier dans lequel consigner les messages de trace. Les messages de trace sont consignés si le niveau de trace est supérieur à zéro, que la fenêtre de trace soit ouverte ou non. Exemple : -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt

7 Facultatif : limitez la taille du fichier de trace à l'aide de l'option -tracefilemax.

Par exemple, saisissez un des éléments suivants :

```
-tracefilemax 1000M
-tfm 1000M
```

Dans cet exemple, le fichier de trace ne peut pas dépasser 1 Go.

Option	Autre nom	Paramètre	Description
-tracefilemax	-tfm	taille	Spécifie la taille maximum que les données du fichier de trace peuvent occuper sur le disque. Si vous spécifiez cette option, il y aura un fichier de trace avec le nom spécifié via l'option tracefile et jusqu'à 9 fichiers de purge supplémentaires. Ces fichiers sont nommés en utilisant la base du nom de fichier de trace principal plus "_*n*", avec n allant de 1 à 9. Le paramètre de taille est le nombre d'octets. Spécifiez la taille en utilisant les suffixes K, M ou G pour kilo-octets, mégaoctets ou gigaoctets. Si la taille des données du fichier de trace est supérieure au maximum spécifié lorsque le chargeur distant est démarré, les données du fichier de trace restent supérieures au maximum spécifié jusqu'à ce que la purge soit terminée sur les 10 fichiers Exemple : -tracefilemax 1000M -tfm 1000M Dans cet exemple, le fichier de trace ne peut pas dépasser 1 Go.

8 Spécifiez la classe ou le module à l'aide des options -class ou -module.

Option	Autre nom	Paramètre	Description
-class	-cl	Nom de la classe Java	Spécifie le nom de la classe Java du module d'interface d'application Identity Manager à héberger. Par exemple, pour un pilote Java, saisissez un des éléments suivants : -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java utilise un keystore pour lire les certificats. L'option -class et l'option -module s'excluent mutuellement. Pour afficher la liste des noms de classe Java, reportez-vous au Tableau B-2 page 270 de l'Annexe B, « Options de configuration d'un chargeur distant », page 263.

Option	Autre nom	Paramètre	Description
-module	-m	Nom de module	Spécifie le module qui contient le module d'interface d'application Identity Manager à héberger. Par exemple, pour un pilote natif, saisissez un des éléments suivants : -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" ou -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" L'option -module utilise un certificat rootfile. L'option -module et l'option -class s'excluent mutuellement.

9 Nommez et enregistrez le fichier.

Vous pouvez modifier certains paramètres pendant que le chargeur distant s'exécute. Pour plus d'informations sur ces paramètres, reportez-vous à l'Annexe B, « Options de configuration d'un chargeur distant », page 263.

Paramètre	Description
-commandport	Spécifie une instance du chargeur distant.
-config	Spécifie un fichier de configuration.
-javadebugport	Spécifie que l'instance du chargeur distant doit activer le débogage Java sur le port spécifié.
-password	Permet d'envoyer des commandes.
-service	Installe une instance en tant que service. Windows uniquement.
-tracechange	Change le niveau de trace.
-tracefilechange	Change le nom du fichier de trace dans lequel sont copiées les données.
-unload	Décharge l'instance du chargeur distant.
-window	Active ou désactive la fenêtre de trace d'une instance du chargeur distant. Windows uniquement.

Paramétrage des variables d'environnement sous Solaris, Linux ou AIX

Après l'installation du chargeur distant, vous pouvez définir la variable d'environnement `RDXML_PATH` qui remplace le répertoire courant par rdxml. Ce répertoire sert ensuite de chemin

d'accès de base aux fichiers créés ultérieurement. Pour définir la valeur de la variable `RDXML_PATH`, saisissez les commandes suivantes :

- set RDXML_PATH=*path*
- export RDXML_PATH

Démarrage du chargeur distant

- « Démarrage du chargeur distant sous Windows » page 62
- « Démarrage du chargeur distant à partir de la ligne de commande » page 63

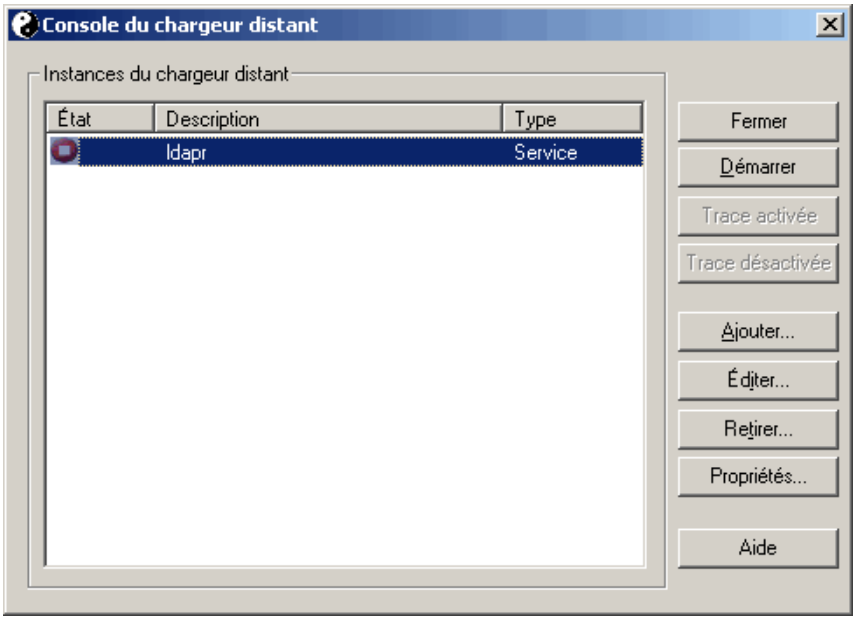
Démarrage du chargeur distant sous Windows

Pour exécuter le chargeur distant sous Windows :

Figure 3-13 *Icône de la console du chargeur distant*

1. Sur le Bureau, cliquez sur l'icône de la console du chargeur distant.

   Figure 3-14 *Console du chargeur distant*

2. Sélectionnez une instance de pilote, puis cliquez sur *Démarrer*.

Démarrage du chargeur distant à partir de la ligne de commande

Sous Solaris, Linux ou AIX, le composant binaire rdxml contient la fonctionnalité chargeur distant. Ce composant se trouve dans le répertoire `/usr/bin/`. Sous Windows, le chargeur distant se trouve par défaut dans le répertorie c:\novell\RemoteLoader.

Pour exécuter le chargeur distant :

1. Définissez le mot de passe.

Plate-forme	Commande
Fenêtres	`dirxml_remote` -config *path_to_config_file* -sp *password password*
Solaris Linux AIX	`rdxml` -config *path_to_config_file* -sp *password password*
HP-UX AS/400 OS/390 z/OS	`dirxml_jremote` -config *path_to_config_file* -sp *password password*

Option	Autre nom	Paramètre	Description
-password	-p	password	Spécifie le mot de passe d'authentification des commandes. Ce mot de passe doit être identique au premier mot de passe spécifié dans **setpasswords** pour l'instance de chargeur qui fait l'objet de la commande. Si une option de commande (déchargement, modification du niveau de trace, etc.) est spécifiée et si l'option **mot de passe** ne l'est pas, l'utilisateur est invité à entrer le mot de passe du chargeur représentant la cible de la commande. Exemple : -password novell4 -p novell4
-setpasswords	-sp	Mot de passe Mot de passe	Spécifie le mot de passe de l'instance du chargeur distant et celui de l'objet Pilote Identity Manager du module d'interface pilote distant avec lequel le chargeur distant va communiquer. Le premier mot de passe de l'argument est celui du chargeur distant. Le deuxième est celui de l'objet Pilote Identity Manager associé au module d'interface pilote distant sur le serveur méta-annuaire. Aucun mot de passe ne doit être spécifié ou les deux doivent l'être. Si aucun mot de passe n'est spécifié, le chargeur distant demande les mots de passe. Il s'agit d'une option de configuration. Elle permet de configurer l'instance du chargeur distant à l'aide des mots de passe spécifiés, mais ne permet pas de charger le module d'interface pilote de l'application Identity Manager ni de communiquer avec une autre instance du chargeur. Exemple : -setpasswords novell4 staccato3 -sp novell4 staccato3

2 Démarrez le chargeur distant.

Plate-forme	Commande
Fenêtres	`dirxml_remote` -config *path_to_config_file*
Solaris Linux AIX	`rdxml` -config *path_to_config_file*
HP-UX AS/400 OS/390 z/OS	`dirxml_jremote` -config *path_to_config_file*

3 Avec iManager, démarrez le pilote.

4 Vérifiez que le chargeur distant fonctionne correctement.

Le chargeur distant ne charge le module d'interface pilote de l'application Identity Manager que lorsque le chargeur distant est en communication avec le module d'interface pilote distant du serveur méta-annuaire. Cela signifie notamment que le module d'interface d'application est fermé dès que la communication est rompue entre le chargeur et le serveur méta-annuaire.

Pour Linux, Solaris ou AIX, utilisez la commande ps ou un fichier de trace pour savoir si la commande et les ports de connexion écoutent.

Pour les plates-formes HP-UX ou similaires, surveillez le chargeur distant Java à l'aide de la commande tail du fichier de trace :

```
tail -f trace filename
```

Si la dernière ligne du journal affiche ce qui suit, cela signifie que le chargeur s'exécute correctement et qu'il attend la connexion du module d'interface pilote distant Identity Manager :

```
TRACE: Remote Loader: Entering listener accept()
```

Pour configurer le chargeur distant (rdxml) afin qu'il démarre automatiquement sous UNIX, reportez-vous au document TID 10097249 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097249.htm).

Arrêt du chargeur distant

Plate-forme	Commande
Fenêtres	Utilisez la console du chargeur distant pour arrêter une instance du pilote.
Solaris Linux AIX	`rdxml` -config *path_to_config_file* -u
HP-UX AS/400 OS/390 z/OS	`dirxml_jremote` -config *path_to_config_file* -u

Si plusieurs instances du chargeur distant s'exécutent sur l'ordinateur, spécifiez l'option –cp *port de commande* pour que le chargeur distant puisse arrêter l'instance appropriée.

Pour arrêter le chargeur distant, vous devez disposer des droits nécessaires ou saisir le mot de passe du chargeur distant.

Scénario : droits suffisants. Le chargeur distant s'exécute en tant que service Windows. Vous avez des droits suffisants pour l'arrêter. Vous saisissez un mot de passe, mais vous vous rendez compte qu'il est incorrect. Le chargeur distant s'arrête tout de même.

Le chargeur distant « n'accepte pas » le mot de passe. En fait, il l'ignore puisqu'il est superflu dans ce cas. Si vous exécutez le chargeur distant comme application et non comme service, le mot de passe est utilisé.

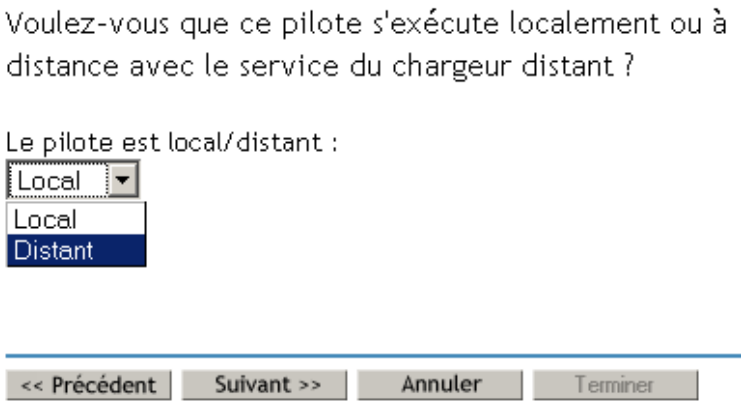
3.4 Configuration des pilotes Identity Manager pour une utilisation avec les chargeurs distants

Vous pouvez configurer un nouveau pilote ou activer un pilote existant pour qu'il communique avec le chargeur distant. Vous trouverez dans cette section des informations générales sur la configuration des pilotes pour qu'ils communiquent avec le chargeur distant. Afin d'obtenir des informations complémentaires et spécifiques aux pilotes, reportez-vous au guide d'implémentation du pilote en question.

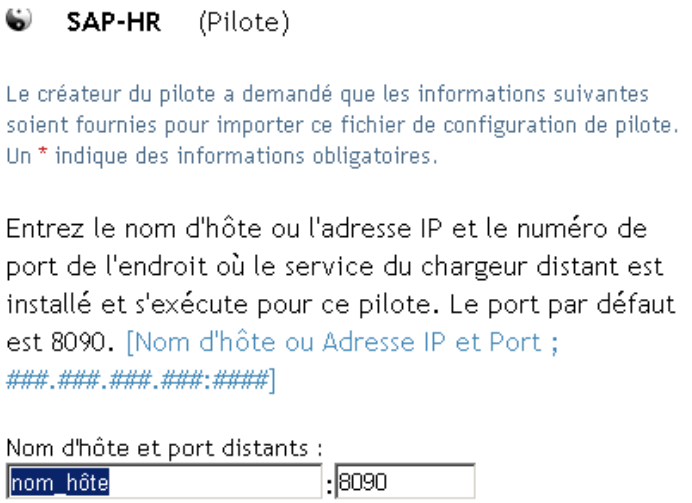
- Section 3.4.1, « Importation et configuration d'un nouveau pilote », page 65
- Section 3.4.2, « Configuration d'un pilote existant », page 67
- Section 3.4.3, « Création d'un fichier Keystore », page 68

3.4.1 Importation et configuration d'un nouveau pilote

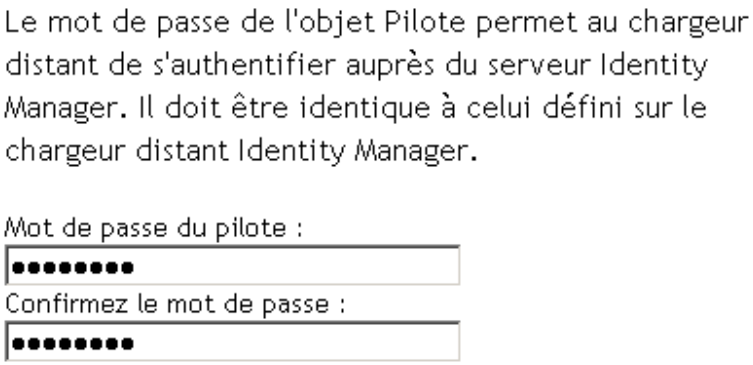
1. Dans Novell iManager, importez ou créez et configurez un nouveau pilote.
2. Faites défiler les options de configuration jusqu'à la dernière, sélectionnez Distant dans la liste déroulante, puis cliquez sur *Suivant*.



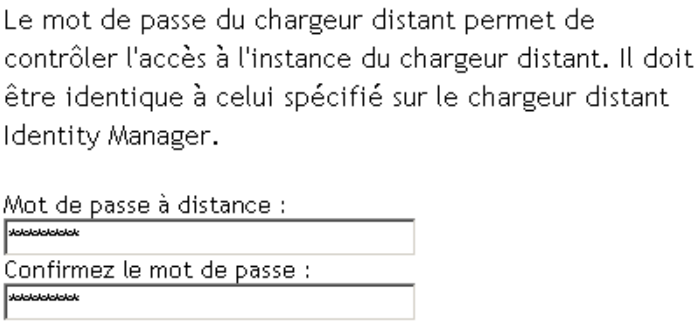
3 Saisissez un nom d'hôte et un port.



4 Saisissez deux fois le mot de passe de l'objet Pilote.



5 Saisissez deux fois le mot de passe du chargeur distant, puis cliquez sur *Suivant*.

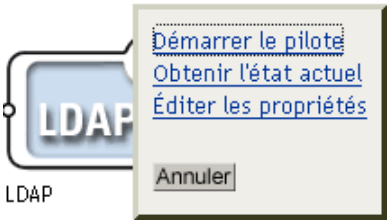


6 Définissez un utilisateur de même sécurité, cliquez sur *Suivant*, puis sur *Terminer*.

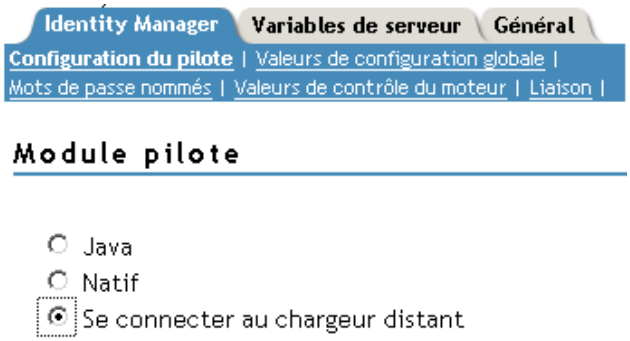
3.4.2 Configuration d'un pilote existant

Spécifiez les paramètres de l'objet Pilote permettant de le connecter au chargeur distant.

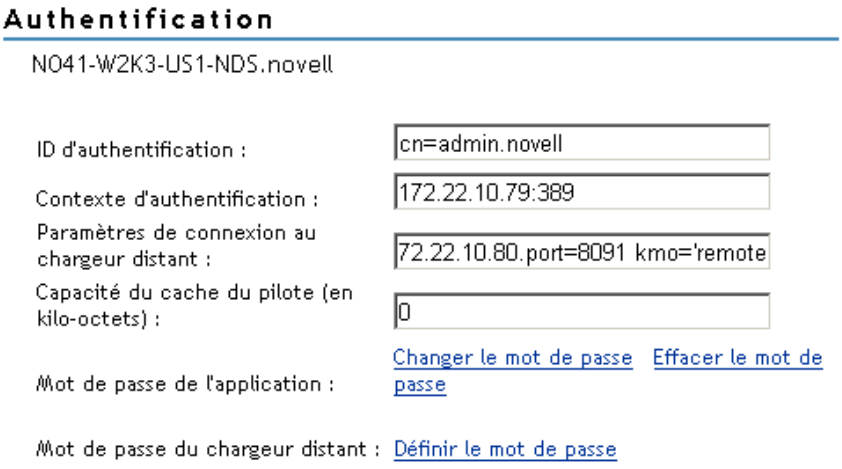
1. Dans Novell iManager, cliquez sur *Identity Manager* > *Présentation de Identity Manager*.
2. Localisez et sélectionnez le pilote que vous voulez modifier.



3. Cliquez sur l'icône d'état du pilote, puis cliquez sur *Éditer les propriétés*.
4. Dans la zone Module pilote, sélectionnez Se connecter au chargeur distant.



5. Dans la zone Authentification, saisissez les paramètres du chargeur distant.



- Paramètres de connexion au chargeur distant

Vous avez précédemment exporté le certificat signé automatiquement. Reportez-vous à la Section 3.2.2, « Exportation d'un certificat signé automatiquement », page 46. Pour SSL, vous devez connaître le surnom du certificat signé automatiquement.

Dans la zone de texte Paramètres de connexion au chargeur distant, saisissez les paramètres par paires clé-valeur. Par exemple, saisissez

```
hostname=192.168.0.1 port=8090 kmo=remotecert
hostname=192.168.0.1 port=8090 kmo='remote cert'
```

- nom d'hôte

  Nom ou adresse IP de l'hôte (par exemple, 190.162.0.1). Spécifie l'adresse ou le nom de l'ordinateur sur lequel le chargeur distant s'exécute. Si vous ne spécifiez pas l'adresse IP ou le nom du serveur, la valeur localhost est utilisée par défaut.

- port

  Endroit dans lequel le chargeur distant accepte les connexions en provenance du module d'interface pilote distant. Si vous ne saisissez pas ce paramètre de communication, il prend par défaut la valeur 8090.

- kmo

  Spécifie le nom de clé (par exemple, kmo=remotecert) de l'objet Matériel clé (KMO) contenant les clés et le certificat utilisés pour SSL.

  Si vous avez utilisé des espaces dans le nom de certificat, mettez le surnom de l'objet KMO entre guillemets simples.

  Suggestion : Le nom de l'objet KMO est la valeur du surnom spécifiée à l'étape 2 de la Section 3.2.1, « Création d'un certificat de serveur », page 46.

- Saisissez le mot de passe de l'application

  Spécifiez le mot de passe de l'utilisateur de l'application. En général, le module d'interface pilote a besoin de ce mot de passe pour que le pilote se connecte à l'application.

- Saisissez le mot de passe du chargeur distant

  Spécifiez le mot de passe pour le chargeur distant. Le module d'interface pilote distant utilise ce mot de passe pour s'authentifier auprès du chargeur distant.

  Remarque : définissez ou redéfinissez simultanément le mot de passe de l'application et le mot de passe du chargeur distant.

6 Cliquez sur *OK*.

3.4.3 Création d'un fichier Keystore

Un keystore est un fichier Java qui contient des clés de codage et, le cas échéant, des certificats. Si vous voulez utiliser SSL entre le chargeur distant et le moteur méta-annuaire et si vous utilisez un module d'interface pilote Java, vous devez créer un fichier keystore.

- « Keystore sous Windows » page 69
- « Keystore sous Solaris, Linux ou AIX » page 69
- « Keystore sur toutes les plates-formes » page 69

Keystore sous Windows

Sous Windows, exécutez l'utilitaire Keytool qui se trouve généralement dans le répertoire `c:\novell\remoteloader\jre\bin`.

Keystore sous Solaris, Linux ou AIX

Dans les environnements Solaris, Linux ou AIX, utilisez le fichier create_keystore. Ce fichier est installé avec rdxml et figure également dans le fichier dirxml_jremote.tar.gz, dans le répertoire `\dirxml\java_remoteloader`. Le fichier create_keystore est un script de shell qui appelle l'utilitaire Keytool.

Sous UNIX, dans lequel le fichier keystore est créé à partir du certificat signé automatiquement, ce certificat peut être exporté au format .der binaire ou Base64.

Saisissez la commande suivante sur la ligne de commande :

`create_keystore` *self-signed_certificate_name keystorename*

Par exemple, saisissez une des commandes suivantes :

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

Le script create_keystore spécifie un mot de passe codé en dur, “dirxml”, pour le mot de passe keystore. Cela ne pose pas de risque de sécurité ; en effet, seuls un certificat public et une clé publique sont mémorisés dans le keystore.

Keystore sur toutes les plates-formes

Pour créer un keystore sur n'importe quelle plate-forme, vous pouvez entrer ce qui suit à l'invite de la ligne de commande :

`keytool` -import -alias trustedroot -file *self-signed_certificate_name* -keystore *filename* -storepass

Filename peut être n'importe quel nom (par exemple, rdev_keystore).

Création de stratégies

4

Les stratégies permettent de personnaliser le flux d'informations entrant et sortant du coffre-fort d'identité pour un environnement particulier.

Par exemple, une société peut utiliser inetorgperson en tant que classe d'utilisateur principal, et une autre société peut utiliser Utilisateur. Pour cela, une stratégie doit être créée afin d'indiquer au moteur méta-annuaire comment est appelé l'utilisateur dans chacun des systèmes. Chaque fois que des opérations affectant les utilisateurs circulent entre les systèmes connectés, Identity Manager applique la stratégie permettant cette modification.

Les stratégies créent aussi de nouveaux objets, mettent à jour des valeurs d'attributs, apportent des transformations aux schémas, définissent des critères de correspondance, gèrent des associations Identity Manager, etc.

Vous trouverez des instructions détaillées sur les stratégies dans le *Policy Builder and Driver Customization Guide (Guide de création des stratégies et de personnalisation des pilotes)*. Ce guide contient :

- une description détaillée de chaque stratégie disponible ;
- un guide et des références approfondis pour le Générateur de stratégies, y compris des exemples et une syntaxe pour chaque situation, opération, nom et verbe ;
- des informations relatives à la création de stratégies via les feuilles de style XSLT.

Pour plus d'informations sur les stratégies, reportez-vous au *Policy Builder and Driver Customization Guide (Guide de création des stratégies et de personnalisation des pilotes)*.

Synchronisation de mot de passe sur des systèmes connectés

5

5.1 Présentation

Identity Manager propose la synchronisation bidirectionnelle des mots de passe, rendue possible par les mots de passe universels et la prise en charge des systèmes connectés pour l'abonnement aux mots de passe ou leur publication.

Comme pour d'autres attributs d'un compte utilisateur, vous avez le choix entre plusieurs sources de données expertes.

5.1.1 Présentation des mots de passe

Les mots de passe NDS®, simples, de distribution et universels ont des usages différents. Dans les versions précédentes de eDirectory™ et Identity Manager, les systèmes connectés ne pouvaient actualiser que le mot de passe NDS, à travers une synchronisation unilatérale.

Identity Manager utilise un mot de passe universel, qui est réversible et peut être synchronisé avec les autres mots de passe du coffre-fort d'identité. Le mot de passe universel existe depuis la version 8.7.1 de eDirectory. Il est protégé par trois niveaux de codage.

NMAS™ contrôle le lien qui unit le mot de passe universel aux autres mots de passe du coffre-fort d'identité. Par exemple, il contrôle si le mot de passe universel reste synchronisé avec les mots de passe NDS, simple ou de distribution. Il intercepte les requêtes de changement de mot de passe entrantes et les gère conformément aux paramètres des stratégies de mot de passe NMAS.

Identity Manager contrôle la relation entre les mots de passe du coffre-fort d'identité et ceux des systèmes connectés. Il utilise pour cela le mot de passe de distribution, c'est-à-dire le mot de passe présent dans le coffre-fort d'identité qui peut être fourni aux systèmes connectés. À l'instar du mot de passe universel, le mot de passe de distribution est protégé par trois niveaux de codage et il est réversible.

Dans la stratégie de mot de passe NMAS, vous pouvez préciser si le mot de passe de distribution doit être identique au mot de passe universel en définissant le paramètre *Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel*. Si le mot de passe de distribution est identique au mot de passe universel et si vous choisissez d'utiliser la synchronisation bidirectionnelle des mots de passe avec les systèmes connectés, n'oubliez pas que vous utilisez Identity Manager pour extraire le mot de passe universel de eDirectory et l'envoyer à d'autres systèmes connectés. Vous devez sécuriser le transport du mot de passe, de même que les systèmes connectés sur lesquels il sera stocké. Reportez-vous au Chapitre 7, « Sécurité : meilleures pratiques », page 201.

Si le mot de passe de distribution n'est pas identique au mot de passe universel, parce que vous avez désactivé le paramètre dans la stratégie de mot de passe NMAS, vous pouvez « tunnelliser » les mots de passe entre les systèmes connectés qui utilisent le mot de passe de distribution, sans utiliser ni affecter le mot de passe universel ou le mot de passe NDS. N'oubliez pas que la tunnellisation permet uniquement de synchroniser les mots de passe entre systèmes connectés. Si elle est activée, la tunnellisation ne définit pas le mot de passe du coffre-fort d'identité/universel.

Pour plus d'informations sur les différents mots de passe eDirectory, reportez-vous au *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de Novell Modular Authentication Services (NMAS) 2.3)* (http://www.novell.com/documentation/nmas23/index.html). Afin d'obtenir différents exemples d'utilisation de la synchronisation des mots de passe avec Identity Manager, reportez-vous à la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111.

5.1.2 Définition de la synchronisation bidirectionnelle des mots de passe

La synchronisation bidirectionnelle des mots de passe est la combinaison de l'acceptation par Identity Manager des mots de passe des systèmes connectés que vous spécifiez et de la distribution des mots de passe aux systèmes connectés que vous choisissez.

La disponibilité de la synchronisation bidirectionnelle des mots de passe sur un système connecté particulier dépend de ce que ce système prend en charge.

Certains systèmes connectés peuvent accepter des mots de passe nouveaux ou modifiés de la part de Identity Manager et peuvent aussi lui fournir le mot de passe de l'utilisateur. Ces systèmes connectés prennent en charge la synchronisation bidirectionnelle des mots de passe avec Identity Manager :

- Active Directory
- Novell® eDirectory
- NIS (Network Information Services - services d'informations réseau)
- NT Domain

Pour ces systèmes connectés, l'utilisateur peut modifier un mot de passe dans l'un des systèmes et procéder à la synchronisation de ce mot de passe avec les autres systèmes via Identity Manager. Toutefois, si vous utilisez les stratégies de mots de passe NMAS avancées, il vaut mieux que les utilisateurs modifient leurs mots de passe dans la console en libre-service de iManager, qui reste le meilleur endroit pour modifier les mots de passe car toutes les stratégies auxquels le mot de passe utilisateur doit se soumettre y sont répertoriés.

Les autres systèmes connectés ne peuvent pas fournir le mot de passe de l'utilisateur et ne prennent donc pas en charge la synchronisation bidirectionnelle des mots de passe. Ils peuvent toutefois fournir des données qui serviront à créer des mots de passe et les envoyer à Identity Manager, en définissant des stratégies au sein même de la configuration du pilote.

Plusieurs autres systèmes peuvent accepter des mots de passe Identity Manager, y compris définir un mot de passe initial pour un nouvel utilisateur ou modifier un mot de passe, voire les deux. Reportez-vous à la Section 5.2, « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 84.

5.1.3 Comparaison entre la version 1.0 de la synchronisation des mots de passe et la version fournie avec Identity Manager

Tableau 5-1 *Comparaison : version 1.0 de la synchronisation des mots de passe et version fournie avec Identity Manager*

	Version 1.0 de la synchronisation des mots de passe	Version de la synchronisation des mots de passe fournie avec Identity Manager 2 et 3
Version du produit	Produit distinct Identity Manager.	Fourni avec Identity Manager, non vendu séparément.

	Version 1.0 de la synchronisation des mots de passe	Version de la synchronisation des mots de passe fournie avec Identity Manager 2 et 3
Plates-formes	• Active Directory • NT Domain • eDirectory	Ces plates-formes prennent entièrement en charge la synchronisation bidirectionnelle des mots de passe : • Active Directory • eDirectory • NIS • NT Domain Ces systèmes connectés prennent en charge la publication des mots de passe sur Identity Manager. Le mot de passe universel et le mot de passe de distribution sont réversibles ; Identity Manager peut donc les distribuer aux systèmes connectés. Tout système connecté prenant en charge l'élément de mot de passe Abonné peut souscrire à des mots de passe Identity Manager. Reportez-vous à la Section 5.2, « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 84.
Mot de passe utilisé dans un coffre-fort d'identité	Mot de passe NDS (non réversible)	Mot de passe universel (réversible) ou mot de passe de distribution (réversible également). Si on le souhaite, le mot de passe NDS peut rester synchronisé. Pour consulter des exemples de scénarios, reportez-vous à la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111.
Fonctionnalité principale pour les systèmes Windows connectés	Envoi de mots de passe à Identity Manager afin que le mot de passe du coffre fort d'identité soit synchronisé avec le mot de passe Windows. Les mots de passe n'ont pas été renvoyés à NT ou AD parce que le mot de passe NDS n'est pas réversible.	Pour assurer la synchronisation bidirectionnelle des mots de passe. Les mots de passe peuvent être synchronisés dans les deux sens car le mot de passe universel et le mot de passe de distribution sont réversibles.
Modifications de LDAP	Non pris en charge.	Pris en charge
Client™ Novell®	Obligatoire.	Non obligatoire.
Attribut nadLoginName	Utilisé pour garantir la mise à jour des mots de passe.	Non utilisé.

	Version 1.0 de la synchronisation des mots de passe	Version de la synchronisation des mots de passe fournie avec Identity Manager 2 et 3
Composant contenant la fonctionnalité de synchronisation des mots de passe	Le pilote Identity Manager contenait la fonctionnalité destinée à la mise à jour de nadLoginName.	Les stratégies Identity Manager de la configuration du pilote proposent la fonctionnalité de synchronisation des mots de passe. Le pilote ne fait que mener à bien les tâches qui lui ont été confiées par le moteur méta-annuaire, et qui sont issues de la logique des stratégies. Le manifeste du pilote, les valeurs de configuration globale (GCV) et les paramètres de filtre du pilote doivent également prendre en charge la synchronisation des mots de passe. Ces éléments sont compris dans les exemples de configuration du pilote ou peuvent être ajoutés à un pilote existant. Reportez-vous à la Section 5.7, « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe », page 101.
Agents	Partie distincte du logiciel.	Aucun agent n'est installé : la fonctionnalité fait maintenant partie intégrante du pilote.

5.1.4 Fonctionnalités de la synchronisation des mots de passe Identity Manager

La synchronisation des mots de passe Identity Manager se fait dans les deux sens. Les mots de passe peuvent être envoyés par des systèmes connectés et acceptés par Identity Manager, ou distribués par Identity Manager et acceptés par les systèmes connectés.

Acceptation de mots de passe provenant des systèmes connectés

Comme dans les versions précédentes de DirXML® et Identity Manager, tout système connecté peut publier un mot de passe dans le coffre-fort d'identité.

Vous pouvez préciser les applications des systèmes connectés dont Identity Manager accepte les mots de passe. Vous pouvez même choisir si Identity Manager doit mettre à jour le mot de passe des utilisateurs dans le coffre-fort d'identité dans lequel s'exécute Identity Manager ou s'il doit simplement agir à la manière d'une conduite ou d'un « tunnel », en synchronisant les mots de passe uniquement entre les systèmes connectés. Cela implique qu'il est possible de distinguer le mot de passe du coffre-fort d'identité de celui distribué par Identity Manager aux systèmes connectés, si on le souhaite.

Certains systèmes connectés (AD, autres coffres-forts d'identité, NT et NIS) peuvent fournir le mot de passe de l'utilisateur. Dès lors, lorsqu'un utilisateur change de mot de passe sur un système connecté, la modification peut être synchronisée avec Identity Manager et avec les autres systèmes connectés.

D'autres systèmes connectés ne peuvent pas fournir le mot de passe de l'utilisateur ; ils peuvent toutefois être configurés pour fournir à Identity Manager un mot de passe créé à partir d'une feuille de style, par exemple un mot de passe initial basé sur le nom de famille ou l'ID du salarié.

Distribution des mots de passe aux systèmes connectés

La synchronisation des mots de passe Identity Manager permet de distribuer un mot de passe commun aux systèmes connectés.

Dans les versions précédentes Identity Manager, un pilote pouvait envoyer des mots de passe à Identity Manager depuis un compte utilisateur sur un système connecté. Le mot de passe pouvait être utilisé pour mettre à jour l'utilisateur correspondant dans eDirectory. Toutefois, le mot de passe NDS de eDirectory n'étant pas réversible, il était impossible de transférer un mot de passe du coffre-fort d'identité central Identity Manager vers plusieurs systèmes connectés. Pour se procurer le mot de passe eDirectory, il fallait le capturer avant qu'il ne soit stocké dans eDirectory, par exemple à travers le client Novell.

Le mot de passe universel fourni par eDirectory 8.7.3 est réversible. Il peut être distribué.

Identity Manager peut accepter un mot de passe d'un système connecté. Comme le mot de passe universel est réversible, Identity Manager peut le distribuer du coffre-fort d'identité aux systèmes connectés qui prennent en charge la définition initiale des mots de passe pour les nouveaux comptes, ainsi que leur modification.

Quelle que soit l'origine du mot de passe, Identity Manager utilise le mot de passe de distribution en tant que référentiel à partir duquel distribuer les mots de passe aux systèmes connectés. Le mot de passe de distribution, comme le mot de passe universel, permet d'appliquer les stratégies de mot de passe.

Pour plus d'informations sur l'utilisation du mot de passe universel et du mot de passe de distribution dans la synchronisation des mots de passe, reportez-vous à « Implémentation de la synchronisation des mots de passe » page 111.

Comme pour tous les autres attributs des utilisateurs, vous pouvez décider quels sont les systèmes qui constituent des sources de mots de passe expertes. Identity Manager distribue les mots de passe de cette source aux autres systèmes connectés.

Vous pouvez établir la synchronisation bidirectionnelle des mots de passe entre des systèmes connectés qui la prennent en charge.

Application des stratégies de mot de passe dans la zone de stockage et sur les systèmes connectés

En appelant NMAS, Identity Manager peut appliquer les stratégies de mot de passe sur les mots de passe entrants. Si le mot de passe publié depuis un système connecté vers Identity Manager ne respecte pas les stratégies, vous pouvez paramétrer Identity Manager de sorte qu'il n'accepte pas le mot de passe dans le coffre-fort d'identité. Cela signifie aussi que les mots de passe non conformes aux stratégies ne seront pas distribués aux autres systèmes connectés.

De plus, Identity Manager peut appliquer les stratégies de mot de passe sur les systèmes connectés. Si le mot de passe publié vers Identity Manager ne respecte pas les règles de la stratégie, vous pouvez paramétrer Identity Manager de sorte qu'il n'accepte pas de distribuer le mot de passe et même qu'il réinitialise le mot de passe non conforme sur le système connecté à l'aide du mot de passe de distribution actuel présent dans le coffre-fort d'identité.

Supposons que vous souhaitiez que les mots de passe comprennent au moins un caractère numérique. Le système connecté, lui, n'a pas la capacité d'appliquer cette stratégie. Vous pouvez demander que Identity Manager réinitialise les mots de passe provenant du système connecté qui ne respectent pas les règles de la stratégie.

Si vous utilisez les règles de mots de passe avancées, ainsi que la synchronisation des mots de passe dans Identity Manager, nous vous conseillons de rechercher les stratégies de mot de passe de tous les systèmes connectés afin de vérifier que les règles avancées définies dans la stratégie de mot de passe eDirectory sont compatibles. Cette recherche garantit le bon déroulement de la synchronisation des mots de passe.

N'oubliez pas de vérifier que tous les utilisateurs à qui vous avez assigné des stratégies de mot de passe NMAS correspondent aux utilisateurs qui doivent participer à la synchronisation des mots de passe entre les systèmes connectés.

Les stratégies de mot de passe NMAS sont assignées dans une perspective centrée sur l'arborescence. La synchronisation des mots de passe, en revanche, est définie pilote par pilote. Par ailleurs, les pilotes sont installés pour chaque serveur et ne peuvent gérer que les utilisateurs se trouvant sur une réplique principale ou en lecture/écriture. Pour que la synchronisation des mots de passe donne les résultats escomptés, vérifiez que les conteneurs situés dans une réplique principale ou en lecture/écriture sur le serveur sur lequel s'exécutent les pilotes auxquels s'applique la synchronisation correspondent aux conteneurs pour lesquels vous avez assigné des stratégies de mot de passe avec le mot de passe universel activé. L'assignation d'une stratégie de mot de passe au conteneur racine d'une partition garantit que cette stratégie s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

Pour plus d'informations sur l'assignation des stratégies de mot de passe NMAS aux utilisateurs, reportez-vous à la section « Assigning Password Policies to Users (Assignation de stratégies de mot de passe aux utilisateurs) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html).

Scénarios de synchronisation des mots de passe

Identity Manager permet de spécifier quels sont les systèmes qui constituent des sources de mots de passe expertes. Vous pouvez également décider du flux des mots de passe.

La plupart des fonctionnalités de la synchronisation des mots de passe dans Identity Manager repose sur le mot de passe universel, la fonction de mot de passe réversible du coffre-fort d'identité. Toutefois, certains scénarios fonctionnent sans déploiement du mot de passe universel.

La synchronisation des mots de passe dans Identity Manager s'appuie également sur le mot de passe de distribution. Comme pour le mot de passe universel, une stratégie peut être appliquée au mot de passe de distribution.

Pour les principales méthodes d'implémentation de la synchronisation des mots de passe, reportez-vous à « Implémentation de la synchronisation des mots de passe » page 111. Ces scénarios peuvent être associés pour répondre aux besoins de votre environnement.

Synchronisation des mots de passe sous Windows sans le client Novell

Un client Novell n'est plus nécessaire pour synchroniser les mots de passe avec Active Directory et NT Domain.

Notification des utilisateurs en cas d'échec de la synchronisation des mots de passe

Application des stratégies de mot de passe dans la zone de stockage et sur les systèmes connectés explique comment Identity Manager peut appliquer les stratégies de mot de passe en refusant les mots de passe non conformes en provenance des systèmes connectés.

Grâce à la fonctionnalité de notification par message électronique, vous pouvez demander à Identity Manager d'avertir l'utilisateur en cas d'échec d'une modification du mot de passe.

Scénario. Vous avez configuré Identity Manager pour qu'il refuse les mots de passe entrants de NT Domain s'ils ne respectent pas vos stratégies de mots de passe. Vous avez activé la notification par message électronique. L'une des règles de votre stratégie de mots de passe NMAS spécifie que le nom de la société ne peut servir de mot de passe. Un utilisateur remplace le mot de passe du système connecté de NT Domain par le nom de la société. NMAS n'accepte pas le mot de passe et Identity Manager envoie un message électronique à l'utilisateur indiquant que le nouveau mot de passe n'a pas été synchronisé.

Vous devez configurer le serveur de messagerie et les modèles avant d'utiliser cette fonctionnalité. Vous pouvez personnaliser les éléments suivants :

- Texte des messages envoyés par Identity Manager
- Notification, pour en envoyer une copie à l'administrateur

Pour plus d'informations, reportez-vous à « Configuration de la notification par message électronique » page 147.

Vérification de l'état de synchronisation du mot de passe pour un utilisateur

Identity Manager permet d'interroger les systèmes connectés pour vérifier l'état de synchronisation des mots de passe d'un utilisateur. Si le système connecté prend en charge la vérification du mot de passe, vous saurez si la synchronisation des mots de passe a réussi.

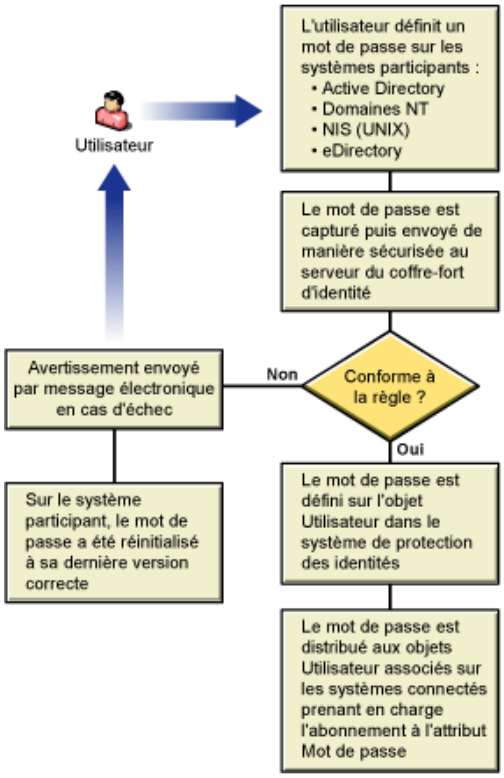
Pour plus d'informations sur la vérification des mots de passe, reportez-vous à « Vérification de l'état de synchronisation du mot de passe pour un utilisateur » page 146.

Afin d'obtenir une liste des systèmes qui prennent en charge la vérification des mots de passe, reportez-vous à « Prise en charge par les systèmes connectés de la synchronisation des mots de passe » page 84.

5.1.5 Diagramme de présentation du déroulement de la synchronisation des mots de passe

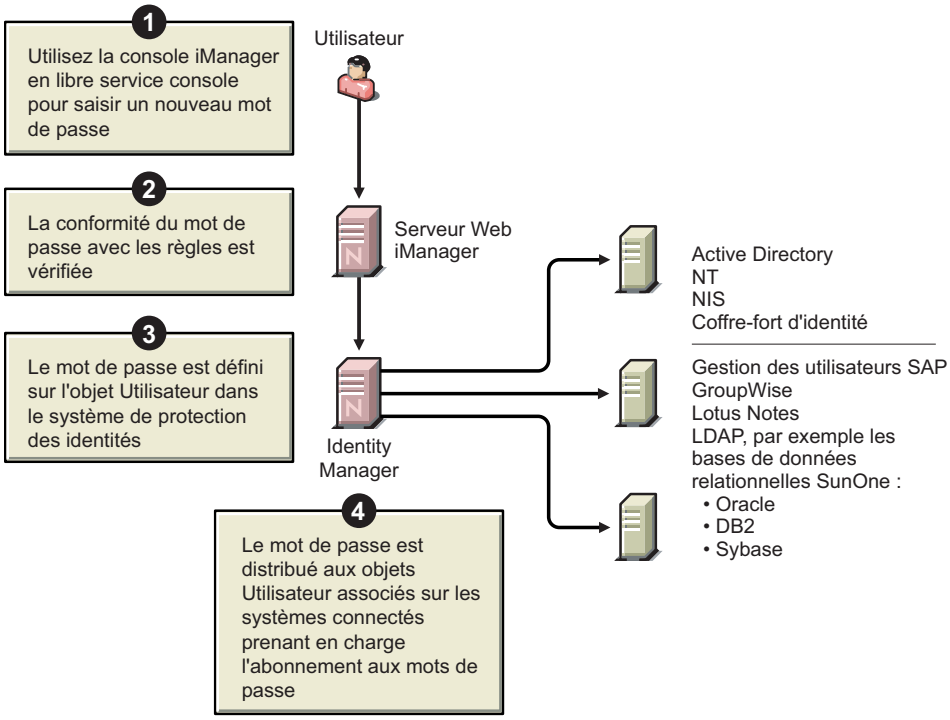
Le diagramme suivant décrit la publication de mots de passe vers Identity Manager par les systèmes connectés.

Figure 5-1 *Publication de mots de passe vers Identity Manager par les systèmes connectés.*



Le diagramme suivant décrit la distribution de mots de passe aux systèmes connectés par Identity Manager.

Figure 5-2 *Distribution de mots de passe aux systèmes connectés par Identity Manager*

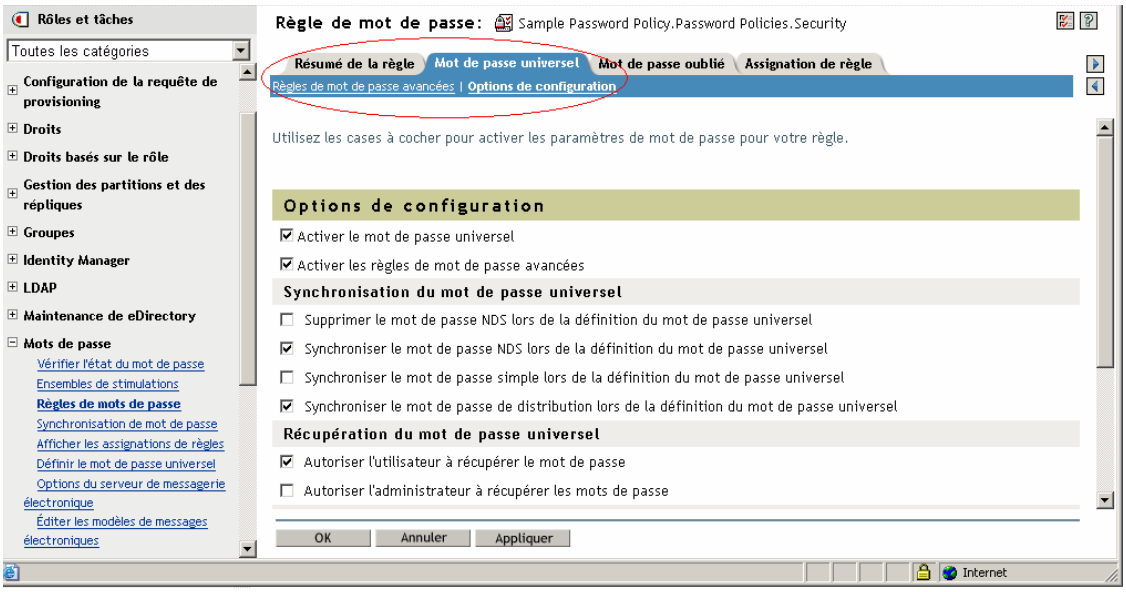


5.1.6 Affichage des illustrations

Dans cette documentation, des illustrations accompagnent fréquemment les procédures pour décrire les options de iManager. La façon dont ces options s'affichent sur votre ordinateur dépend de votre navigateur.

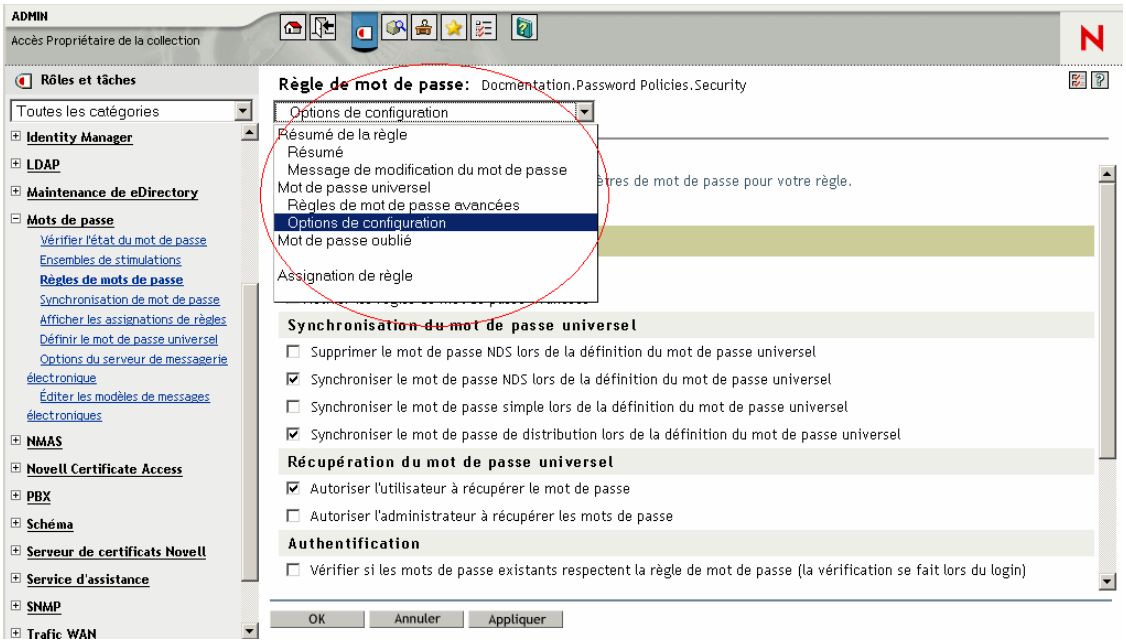
Par exemple, Internet Explorer affiche les options iManager sous forme d'onglets.

Figure 5-3 *Onglets dans iManager*



En revanche, le navigateur Firefox affiche les options iManager dans une liste déroulante.

Figure 5-4 *Liste déroulante dans iManager*



Dans cette documentation, les illustrations représentent les options telles qu'elles apparaissent dans le navigateur Firefox.

5.2 Prise en charge par les systèmes connectés de la synchronisation des mots de passe

Lorsqu'un objet Utilisateur est créé, Identity Manager peut toujours accepter un mot de passe d'un système connecté, même si ce dernier ne prend pas en charge la fourniture du mot de passe de l'utilisateur à partir de ce système.

AD, NT, eDirectory et NIS acceptent les mots de passe envoyés par Identity Manager et prennent en charge l'envoi du mot de passe de l'utilisateur à Identity Manager. Ils acceptent donc totalement la synchronisation bidirectionnelle des mots de passe.

Lorsque vous définissez une stratégie lors de la configuration du pilote sur le canal Éditeur, les autres systèmes peuvent fournir des données utilisables pour la création des mots de passe. L'exemple de configuration de la plupart des pilotes comprend un modèle de stratégie proposant un mot de passe par défaut basé sur le nom de famille.

Les systèmes connectés peuvent, de diverses manières, accepter un mot de passe de la part de Identity Manager. Certains prennent en charge la définition d'un ensemble initial de mots de passe pour les nouveaux comptes, mais pas les événements de modification des mots de passe.

Les fonctionnalités des exemples de configuration de pilotes sont notées dans le manifeste du pilote. Les tableaux suivants fournissent des informations complémentaires qui ne figurent pas dans le manifeste du pilote. Ils indiquent si l'application accepte l'ensemble initial de mots de passe pour les nouveaux comptes, ou si elle accepte plutôt la modification des mots de passe existants. Le manifeste indique si le système connecté peut accepter un mot de passe, mais ne fait pas cette distinction.

Les pilotes sont regroupés : vous voyez ainsi les exemples de configuration de pilotes dotés de fonctionnalités similaires.

5.2.1 Systèmes prenant en charge la synchronisation bidirectionnelle des mots de passe

Les systèmes connectés suivants prennent en charge la synchronisation bidirectionnelle des mots de passe. Ils peuvent fournir le mot de passe de l'utilisateur et accepter des mots de passe Identity Manager.

Tableau 5-2 *Systèmes prenant en charge la synchronisation bidirectionnelle des mots de passe*

Pilote de système connecté	Canal Abonné	Canal Abonné	Canal Abonné	Canal Éditeur
	L'application accepte la définition du mot de passe initial	**L'application accepte la modification du mot de passe**	**L'application prend en charge la vérification du mot de passe**	**L'application peut fournir (synchroniser) un mot de passe**
Active Directory	Oui	Oui	Oui	Oui
eDirectory[1]	Oui	Oui	Oui	Oui
NT Domain	Oui	Oui	Non	Oui
NIS	Oui	Oui	Oui	Oui

Pilote de système connecté	Canal Abonné	Canal Abonné	Canal Abonné	Canal Éditeur
	L'application accepte la définition du mot de passe initial	L'application accepte la modification du mot de passe	L'application prend en charge la vérification du mot de passe	L'application peut fournir (synchroniser) un mot de passe
SIF	Oui	Oui	Non	Oui

[1]La synchronisation bidirectionnelle des mots de passe est disponible pour les utilisateurs entre les arborescences de coffres-forts d'identité, même si le mot de passe universel n'est pas activé pour ces utilisateurs. Reportez-vous à la Section 5.8.2, « Scénario 1 : utilisation du mot de passe NDS pour la synchronisation entre deux coffres-forts d'identité », page 112.

5.2.2 Systèmes acceptant les mots de passe en provenance de Identity Manager

Les systèmes connectés suivants acceptent, à un certain degré, des mots de passe provenant de Identity Manager. Ils ne peuvent pas fournir le mot de passe d'un utilisateur sur le système connecté à Identity Manager.

Même s'ils ne peuvent pas fournir ce mot de passe, ils peuvent être configurés pour créer un mot de passe sur le canal Éditeur à partir d'une stratégie, en fonction des autres données utilisateur présentes sur le système connecté. Les exemples de configuration de pilotes proposent un mot de passe par défaut basé sur le nom de famille.

Tableau 5-3 *Systèmes acceptant les mots de passe en provenance de Identity Manager*

Pilote de système connecté	Canal Abonné	Canal Abonné	Canal Abonné	Canal Éditeur
	L'application accepte la définition du mot de passe initial	L'application accepte la modification du mot de passe	L'application prend en charge la vérification du mot de passe	L'application peut fournir (synchroniser) un mot de passe
GroupWise®	Oui	Oui	Non	Non[2]
JDBC	Oui[3]	No4	Non	Non[5]
LDAP	Oui[6]	Oui[6]	Oui	Non
Notes	Oui	Oui[7]	Oui[7]	Non
SAP User Management	Oui	Oui	Non	Non

[2]GroupWise prend en charge deux méthodes d'authentification :

- GroupWise fournit sa propre authentification et gère les mots de passe utilisateur.
- GroupWise utilise LDAP pour procéder à l'authentification par rapport à eDirectory et ne gère pas les mots de passe.

  Lorsque vous utilisez cette option, GroupWise ignore les mots de passe synchronisés par le pilote.

[3]La définition du mot de passe initial est possible sur toutes les bases de données sur lesquelles le compte utilisateur du système d'exploitation diffère du compte utilisateur de la base de données, comme Oracle*, MS SQL, MySQL* et Sybase*.

[4]Le pilote Identity Manager pour JDBC peut servir à modifier un mot de passe sur le système connecté, mais cette fonctionnalité n'est pas présentée dans l'exemple de configuration du pilote.

[5]Les mots de passe peuvent être synchronisés sous forme de données lorsqu'ils sont stockés dans une table.

[6]Si le serveur LDAP cible autorise la définition de l'attribut userpassword.

[7]Le pilote Notes accepte la modification du mot de passe et ne vérifie les mots de passe que pour le champ HTTPPassword dans Lotus Notes.

5.2.3 Systèmes n'acceptant et ne fournissant pas de mots de passe

Les systèmes connectés suivants n'acceptent pas les mots de passe et n'en fournissent pas à partir de l'exemple de configuration du pilote.

Même s'ils ne peuvent pas fournir le mot de passe de l'utilisateur à Identity Manager, ils peuvent être configurés pour créer un mot de passe sur le canal Éditeur à partir d'une stratégie, en fonction des autres données utilisateur présentes sur le systèmes connecté. Les exemples de configuration de pilotes montrent le mot de passe par défaut basé sur le nom de famille.

Tableau 5-4 *Systèmes n'acceptant et ne fournissant pas de mots de passe*

Pilote de système connecté	Canal Abonné	Canal Abonné	Canal Abonné	Canal Éditeur
	L'application accepte la définition du mot de passe initial	L'application accepte la modification du mot de passe	L'application prend en charge la vérification du mot de passe	L'application peut fournir (synchroniser) un mot de passe
Texte délimité	Non[8]	Non[8]	Non[8]	Non[8]
Exchange 5.5	Non	Non	Non	Non
PeopleSoft 3.6	Non	Non	Non	Non
PeopleSoft 4.0	Non	Non	Non	Non
SAP HR	Non	Non	Non	Non

[8]Le pilote Identity Manager pour le texte délimité ne possède pas de fonction dans le module d'interface pilote prenant directement en charge la synchronisation des mots de passe. Toutefois, selon le système connecté avec lequel vous effectuez la synchronisation, le pilote peut être configuré pour gérer les mots de passe.

5.2.4 Systèmes ne prenant pas en charge la synchronisation des mots de passe

Les systèmes connectés suivants n'ont pas pour objet d'être utilisés avec la synchronisation des mots de passe.

Tableau 5-5 *Systèmes ne prenant pas en charge la synchronisation des mots de passe*

Pilote de système connecté	Canal Abonné	Canal Abonné	Canal Abonné	Canal Éditeur
	L'application accepte la définition du mot de passe initial	L'application accepte la modification du mot de passe	L'application prend en charge la vérification du mot de passe	L'application peut fournir (synchroniser) un mot de passe
Avaya* PBX	Non	Non	Non	Non
Pilote de service de droits	Non	Non	Non	Non
Pilote de service de boucle	Non	Non	Non	Non
Pilote de service de tâches manuelles	Non	Non	Non	Non

5.3 Conditions préalables à la synchronisation des mots de passe

La synchronisation des mots de passe dépend de l'implémentation des éléments suivants :

- « Prise en charge du mot de passe universel » page 87
- « Capacités de synchronisation des mots de passe déclarées dans le manifeste du pilote » page 88
- « Contrôle de la synchronisation des mots de passe à l'aide des valeurs de configuration globale » page 88
- « Stratégies requises pour la configuration du pilote » page 91
- « Filtres que vous installez sur le système connecté pour capturer les mots de passe » page 95
- « Stratégies de mots de passe NMAS créées pour les utilisateurs » page 95
- « Méthodes de login NMAS » page 95

5.3.1 Prise en charge du mot de passe universel

Pour permettre la synchronisation des mots de passe entre les systèmes connectés, Identity Manager nécessite un mot de passe universel. Reportez-vous aux rubriques suivantes :

- “Deploying Universal Password (Déploiement du mot de passe universel)”, dans le *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html)
- Section 5.4.3, « Préparation à l'utilisation du mot de passe universel », page 97

5.3.2 Capacités de synchronisation des mots de passe déclarées dans le manifeste du pilote

Le manifeste du pilote déclare si un système connecté prend en charge les fonctions suivantes pour la synchronisation des mots de passe :

- Publication du mot de passe de l'utilisateur vers Identity Manager
- Acceptation d'un mot de passe Identity Manager

  Le manifeste ne distingue pas l'acceptation de la création d'un mot de passe initial de l'acceptation de modifications.
- Autorisation donnée à Identity Manager de vérifier le mot de passe sur le système connecté, pour déterminer l'état de la synchronisation des mots de passe d'un utilisateur

---

Remarque : le manifeste du pilote est rédigé par le développeur du pilote ou par l'expert Identity Manager qui en crée la configuration. Il n'a pas pour objet d'être modifié par un administrateur réseau. Le manifeste du pilote représente les véritables fonctionnalités du module d'interface pilote et sa configuration. Il ne suffit pas de modifier le manifeste pour changer les fonctionnalités. Pour ajouter des fonctionnalités, il faut améliorer le module d'interface pilote, le système connecté ou la configuration du pilote.

Les exemples de configurations de pilote fournies avec Identity Manager contiennent des entrées de manifeste de pilote. Pour les ajouter à un pilote existant, reportez-vous à la Section 5.7, « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe », page 101.

5.3.3 Contrôle de la synchronisation des mots de passe à l'aide des valeurs de configuration globale

Les valeurs de configuration globale permettent de définir une valeur constante qui peut figurer dans une stratégie. On les appelle parfois variables de serveurs, car elles sont contenues dans un attribut défini pour chaque réplique.

Pour la synchronisation des mots de passe, ces valeurs permettent de créer les paramètres du flux de mots de passe de et vers Identity Manager. Dans la configuration du pilote, les stratégies de synchronisation des mots de passe Identity Manager étant écrites de manière à se comporter différemment selon vos paramètres de valeur de configuration globale, il est facile de changer le flux des mots de passe sans modifier les stratégies.

Grâce aux valeurs de configuration globale, vous contrôlez les paramètres suivants séparément pour chaque système connecté.

Tableau 5-6 *Paramètres des systèmes connectés*

Paramètre	Description
Acceptation ou non par Identity Manager des mots de passe en provenance du système connecté	Ce paramètre s'applique à un mot de passe fourni par le système connecté, ainsi qu'à un mot de passe qui pourrait être créé par les stratégies Identity Manager lors de la configuration de pilotes sur le canal Éditeur. Si vous le désactivez, les deux types de mots de passe sont effacés, et ils n'atteignent pas Identity Manager.

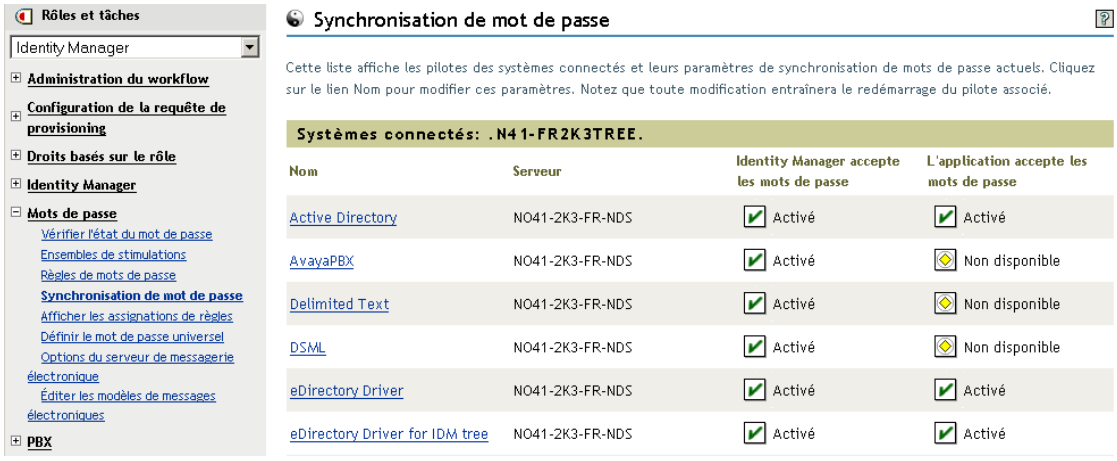
Paramètre	Description
Méthode de synchronisation utilisée par Identity Manager : mise à jour directe du mot de passe universel ou du mot de passe de distribution	Identity Manager contrôle le point d'entrée (le mot de passe qu'il met à jour). NMAS contrôle le flux entre chaque type de mot de passe, en fonction des paramètres définis dans la stratégie de mot de passe NMAS. Pour afficher une stratégie de mot de passe NMAS : 1. Dans iManager, sélectionnez *Mots de passe* > *Stratégies de mots de passe*. 2. Dans la *Liste des stratégies de mots de passe*, sélectionnez une stratégie. 3. Cliquez sur *Éditer*. 4. Sélectionnez une option dans la liste déroulante ou un onglet (selon la version de iManager utilisée). À la section 5.8, « Implémentation de la synchronisation des mots de passe », vous trouverez des scénarios utilisant ces méthodes.
Application ou non des stratégies de mot de passe NMAS sur les mots de passe entrant dans Identity Manager depuis un système connecté	Si ces stratégies sont appliquées, les mots de passe entrants qui ne les respectent pas ne sont pas copiés dans la zone de stockage Identity Manager.
Utilisation ou non par Identity Manager du mot de passe Identity Manager pour appliquer les stratégies de mot de passe NMAS sur un système connecté, par la réinitialisation des mots de passe qui ne respectent pas ces stratégies	Cette option est grisée dans l'interface NMAS si le système connecté ne la prend pas en charge (comme indiqué dans le manifeste du pilote). Le mot de passe n'est réinitialisé que si une opération le concernant échoue sur le canal Éditeur.
Acceptation ou non des mots de passe par le système connecté	Ce paramètre s'applique aussi bien aux mots de passe distribués par Identity Manager qu'aux mots de passe susceptibles d'être créés par les stratégies Identity Manager dans la configuration de pilotes sur le canal Éditeur. Si vous désactivez ce paramètre, les deux types de mots de passe sont effacés, de sorte qu'ils n'atteignent pas le système connecté. Cette option est grisée dans l'interface si le système connecté ne la prend pas en charge (comme indiqué dans le manifeste du pilote).
Si les utilisateurs sont avertis par message électronique lorsqu'un mot de passe n'est pas synchronisé.	Envoie automatiquement des messages électroniques aux utilisateurs concernés.

Les configurations de pilote fournies avec Identity Manager contiennent des entrées de manifeste de pilote. Pour les ajouter à un pilote existant, reportez-vous à la Section 5.7, « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe », page 101.

Pour modifier les valeurs de configuration globale :

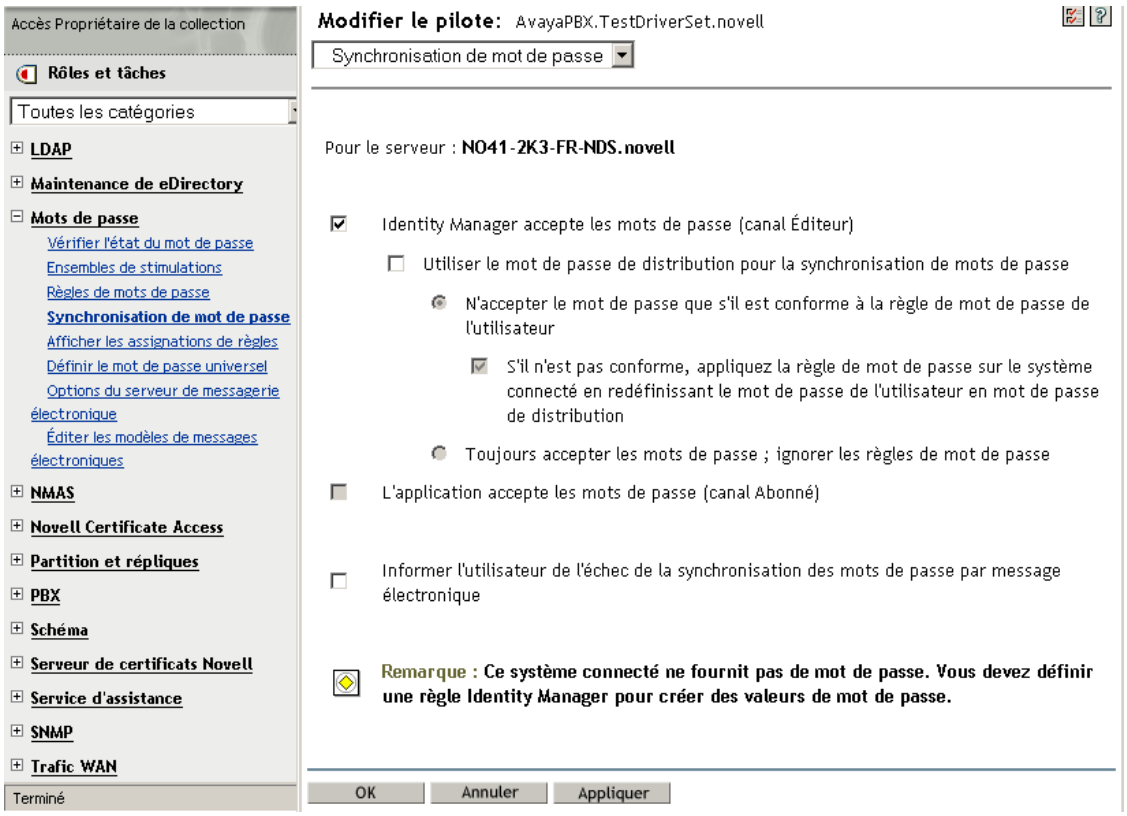
1. Dans iManager, sélectionnez *Mots de passe* > *Synchronisation de mot de passe*.
2. Recherchez un pilote.

Une fois que vous avez spécifié l'emplacement dans lequel vous souhaitez rechercher les pilotes des systèmes connectés, iManager affiche une présentation des paramètres de flux de mot de passe pour tous les pilotes de systèmes connectés qu'il trouve.



3 Pour afficher les paramètres, cliquez sur le nom d'un pilote.

La page Modifier le pilote affiche les valeurs de configuration globale pour la synchronisation des mots de passe.



Lorsqu'une option de cette page est grisée, le manifeste du pilote indique que le système connecté ne la prend pas en charge.

4 Apportez vos modifications puis cliquez sur *OK*.

Remarque : vous pouvez définir les valeurs de configuration globale séparément sur chaque pilote. Les valeurs de configuration globale définies pour un pilote remplacent les valeurs définies pour l'ensemble de pilotes. En définissant les valeurs pour un pilote particulier, vous bénéficiez d'un contrôle plus précis. Cette page n'affiche que les valeurs de configuration globale présentes sur le pilote concerné.

Si vous définissez les valeurs de configuration globale pour un objet Ensemble de pilotes, elles s'appliquent aux pilotes de cet ensemble qui ne disposent pas de valeurs propres. Si un pilote ne possède pas de paramètres propres et s'il hérite des valeurs de configuration globale de l'ensemble de pilotes, iManager ne les affiche pas. Les valeurs héritées seront malgré tout honorées par les stratégies de synchronisation des mots de passe.

5.3.4 Stratégies requises pour la configuration du pilote

Ce sont les stratégies Identity Manager, sur les canaux Éditeur et Abonné de chaque pilote, qui gèrent le flux de mots de passe en fonction des valeurs de configuration globale décrites plus haut. Ces stratégies sont intégrées aux configurations de pilotes, dans Identity Manager.

Si, au lieu de la remplacer, vous mettez à niveau la configuration de pilote existante, vous devrez y ajouter certaines stratégies. Reportez-vous à la Section 5.7, « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe », page 101. Pour que la synchronisation des mots de passe fonctionne, ces stratégies doivent se trouver dans la configuration de votre pilote, au bon emplacement.

Stratégies requises dans l'ensemble de stratégies de transformation de la commande du canal Éditeur

Les stratégies répertoriées dans la colonne Nom de la stratégie de synchronisation des mots de passe doivent figurer dans le même ordre. Par ailleurs, elles doivent apparaître en dernier dans l'ensemble de stratégies de transformation de la commande du canal Éditeur.

Tableau 5-7 *Stratégies requises dans l'ensemble de stratégies de transformation de la commande du canal Éditeur*

Emplacement dans la configuration de pilote	Nom de la stratégie de synchronisation des mots de passe	Action de la stratégie
Stratégie de transformation de commande du canal Éditeur	Password(Pub)-Default Password Policy	Ajoute un mot de passe par défaut à un objet d'ajout si cet objet n'en contient pas encore. Cette stratégie et la stratégie Password(Sub)-Default Password Policy sont les seules que vous pouvez modifier ou supprimer. Pour que la fonction de synchronisation des mots de passe fonctionne correctement, les autres stratégies ne doivent pas être modifiées.
	Password(Pub)-Check Password GCV	Vérifie les GCV pour savoir si vous avez demandé à Identity Manager d'accepter les mots de passe de ce système connecté. Si ce n'est pas le cas, elle efface tous les éléments de mot de passe. La GCV a pour nom enable-password-publish ; le nom affiché est *Identity Manager accepte les mots de passe de l'application*.
	Password(Pub)-Publish Distribution Password	Transforme l'élément <password> pour permettre la mise à jour du mot de passe universel. Cette stratégie référence les GCV suivantes : • publish-password-to-dp • enforce-password-policy
	Password(Pub)-Publish NDS Password	Autorise l'élément <password> à traverser si vous avez spécifié que le mot de passe NDS doit être mis à jour. Dans le cas contraire, elle efface l'élément <password>. Cette stratégie référence la GCV nommée publish-password-to-nds.
	Password(Pub)-Add Password Payload	Intègre des données de charge transférées dans le moteur, à des fins de notification par message électronique.

Emplacement dans la configuration de pilote	Nom de la stratégie de synchronisation des mots de passe	Action de la stratégie
	Password(Sub)-Add Password Payload	Intègre des données de charge transférées dans le moteur, à des fins de notification par message électronique.

Stratégies requises dans l'ensemble de stratégies de transformation de l'entrée du canal Éditeur

Nous vous recommandons de répertorier la stratégie Password(Pub)-Sub Email Notifications en dernier s'il existe plusieurs stratégies dans la transformation de l'entrée.

Tableau 5-8 *Stratégies requises dans l'ensemble de stratégies de transformation de l'entrée du canal Éditeur*

Emplacement dans la configuration de pilote	Nom de la stratégie de synchronisation des mots de passe	Action de la stratégie
Stratégie de transformation de l'entrée du canal Éditeur	Password(Pub)-Sub Email Notifications	Si les informations de charge de mot de passe sont traitées et si l'état indique un problème, il envoie un message électronique à l'utilisateur. à l'adresse électronique indiquée dans l'attribut Adresse de messagerie Internet, dans eDirectory. Cette stratégie référence la GCV nommée notify-user-on-password-dist-failure pour déterminer s'il faut envoyer les messages électroniques de notification.

Stratégies requises dans l'ensemble de stratégies de transformation de la commande du canal Abonné

Les stratégies répertoriées dans la colonne Nom de la stratégie de synchronisation des mots de passe doivent figurer dans le même ordre. Par ailleurs, elles doivent apparaître en dernier dans l'ensemble de stratégies de transformation de la commande du canal Abonné.

Tableau 5-9 *Stratégies requises dans l'ensemble de stratégies de transformation de la commande du canal Abonné*

Emplacement dans la configuration de pilote	Nom de la stratégie de synchronisation des mots de passe	Action de la stratégie
Transformation de commande du canal Abonné	Password(Sub)-Transform Distribution Password	Transforme le mot de passe universel en élément <password>.
	Password(Sub)-Default Password Policy	Ajoute un mot de passe par défaut à un objet d'ajout si cet objet n'en contient pas encore. Cette stratégie et la stratégie Password(Pub)-Default Password Policy sont les seules que vous pouvez modifier ou supprimer. Pour que la fonction de synchronisation des mots de passe fonctionne correctement, les autres stratégies ne doivent pas être modifiées.
	Password(Sub)-Check Password GCV	Vérifie les GCV pour savoir si vous avez demandé au système connecté d'accepter les mots de passe. Si ce n'est pas le cas, elle efface tous les éléments de mot de passe. La GCV a pour nom enable-password-subscribe ; le nom affiché est *L'application accepte les mots de passe de la zone de stockage Identity Manager*.
	Password(Sub)-Add Password Payload	Intègre des données de charge de mot de passe transférées dans le moteur, à des fins de notification par message électronique.

Stratégies requises dans l'ensemble de stratégies de transformation de la sortie du canal Abonné

Nous vous recommandons de répertorier la stratégie Password(Sub)-Pub Email Notifications en dernier s'il existe plusieurs stratégies dans la transformation de la sortie.

Tableau 5-10 *Stratégies requises dans l'ensemble de stratégies de transformation de la sortie du canal Abonné*

Emplacement dans la configuration de pilote	Nom de la stratégie de synchronisation des mots de passe	Action de la stratégie
Transformation de la sortie du canal Abonné	Password(Sub)-Pub Email Notifications	Si les informations de charge de mot de passe sont traitées et si l'état indique un problème, il envoie un message électronique à l'utilisateur. Cette stratégie référence la GCV nommée notify-user-on-password-dist-failure pour déterminer s'il faut envoyer les messages électroniques de notification.

5.3.5 Filtres que vous installez sur le système connecté pour capturer les mots de passe

Pour AD, NT Domain et NIS, des filtres doivent être installés pour capturer le mot de passe de l'utilisateur.

Reportez-vous à la Section 5.9, « Définition des filtres de mots de passe », page 143.

5.3.6 Stratégies de mots de passe NMAS créées pour les utilisateurs

Même si certaines fonctions de la synchronisation des mots de passe sont utilisables en l'absence de mot de passe universel, les stratégies de mots de passe NMAS sont nécessaires pour activer le mot de passe universel pour vos utilisateurs. La stratégie de mot de passe permet également de spécifier des règles de mot de passe avancées et d'indiquer si la conformité des mots de passe existants des utilisateurs avec les règles est vérifiée.

Pour utiliser la synchronisation des mots de passe dans Identity Manager, vous devez bien comprendre les stratégies de mot de passe. Ces stratégies sont décrites à la section « Managing Passwords by Using Password Policies (Gestion des mots de passe à l'aide des stratégies de mot de passe) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html).

5.3.7 Méthodes de login NMAS

Dans certains cas, vous devez avoir installé la méthode de login à mot de passe simple pour profiter des fonctions de mots de passe. LDAP l'exige, par exemple.

Pour plus d'informations sur les méthodes de login, reportez-vous au *Novell Modular Authentication Services (NMAS) 3.0 Administration Guide (Guide d'administration de Novell Modular Authentication Services (NMAS) 3.0)* (http://www.novell.com/documentation/nmas30/index.html).

5.4 Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager

5.4.1 Commutation des utilisateurs du mot de passe NDS au mot de passe universel

Lorsque vous activez le mot de passe universel pour un groupe d'utilisateurs à l'aide d'une stratégie de mot de passe, le mot de passe doit être spécifié.

Si vous avez déjà utilisé la synchronisation des mots de passe pour mettre à jour le mot de passe NDS, vous devez planifier la transition des mots de passe des utilisateurs. Vous pouvez effectuer l'une des opérations suivantes pour que vos utilisateurs créent un mot de passe universel :

- Si vous utilisez le client Novell, transférez le client Novell prenant en charge le mot de passe universel.

  Le client Novell n'est pas requis pour la synchronisation des mots de passe dans Identity Manager.

  Après ce transfert, à la prochaine connexion des utilisateurs à l'aide du client Novell, le client capture le mot de passe NDS avant qu'il ne soit haché et l'utilise pour renseigner le mot de passe universel. Reportez-vous à la section « Planning Login and Change Password Methods for your Users (Planification des méthodes de login et de modification des mots de passe pour les utilisateurs) » du guide de gestion des mots de passe.
- Si vous n'utilisez pas le client Novell, demandez aux utilisateurs de se connecter à la console en libre-service de iManager. Cette méthode de connexion renseigne le mot de passe universel. Pour accéder à la console en libre-service de iManager, accédez au répertoire /nps sur votre serveur iManager. Par exemple, https://www.myiManager.com/nps.
- Demandez aux utilisateurs de se connecter en utilisant tout service qui s'authentifie à l'aide d'un serveur LDAP avec activation du mot de passe universel, le portail d'une société, par exemple.

5.4.2 Comment aider les utilisateurs à changer de mot de passe

Lorsqu'un utilisateur modifie son mot de passe dans iManager, la console en libre-service de iManager ou le client Novell, les stratégies de mot de passe NMAS avancées s'affichent. L'utilisateur peut ainsi créer un mot de passe conforme, sans avoir à deviner les règles.

Selon la configuration du flux de mots de passe, l'utilisateur peut modifier un mot de passe sur un système connecté ; ce mot de passe est alors synchronisé avec Identity Manager et avec les autres systèmes connectés. Toutefois, les systèmes connectés n'affichent pas les règles de mot de passe avancées lorsque l'utilisateur modifie un mot de passe.

Si vous souhaitez appliquer les règles de mot de passe avancées et éviter des mots de passe non conformes, il est recommandé de demander aux utilisateurs de ne modifier le mot de passe que dans la console en libre-service de iManager ou dans le client Novell, ou au moins de s'assurer que les règles de mot de passe avancées sont bien communiquées aux utilisateurs.

Sur un système connecté, l'utilisateur est autorisé à changer le mot de passe sans afficher les stratégies. Il peut donc en avoir un souvenir erroné. Seules les stratégies du système connecté lui-même sont appliquées lorsque l'utilisateur procède à la modification pour la première fois. L'utilisateur risque de rencontrer les problèmes suivants lorsqu'il crée un mot de passe incompatible sur un système connecté, selon les paramètres inscrits dans Identity Manager :

- Si vous avez activé le paramètre qui applique la stratégie sur les mots de passe entrant dans Identity Manager depuis les systèmes connectés, le nouveau mot de passe de l'utilisateur ne sera pas synchronisé sur le coffre-fort d'identité. Si vous avez défini Identity Manager pour qu'il avertisse les utilisateurs de l'échec, ils recevront un message électronique indiquant que leur mot de passe ne s'est pas synchronisé.
- Si vous avez également paramétré Identity Manager pour qu'il remplace les mots de passe non conformes sur les systèmes connectés, l'utilisateur ne pourra pas se connecter au système connecté avec le nouveau mot de passe choisi.

  Identity Manager réinitialise le mot de passe sur le système connecté avec le mot de passe de distribution, qui est probablement le dernier mot de passe conforme créé par l'utilisateur.

5.4.3 Préparation à l'utilisation du mot de passe universel

Pour vous préparer à utiliser le mot de passe universel, reportez-vous à la section « Deploying Universal Password (Déploiement du mot de passe universel) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html). Vous y trouverez la plupart des informations nécessaires.

Vous devez en outre vous souvenir que :

- eDirectory 8.7.1 ou une version supérieure est nécessaire à l'utilisation du mot de passe universel. NetWare® 6.5 n'est pas requis.
- La synchronisation des mots de passe dans Identity Manager s'appuie à la fois sur le mot de passe universel et sur le mot de passe de distribution. Le mot de passe de distribution est le référentiel à partir duquel Identity Manager distribue les mots de passe aux systèmes connectés. Comme pour le mot de passe universel, les stratégies NMAS peuvent être appliquées au mot de passe de distribution.
- Les plugs-in iManager fournis avec Identity Manager comprennent les plugs-in de gestion des mots de passe. Ils permettent de créer des stratégies de mot de passe et de déterminer la méthode de synchronisation entre le mot de passe universel et le mot de passe NDS, le mot de passe simple et le mot de passe de distribution.

  Ils remplacent les plugs-in du mot de passe universel qui étaient livrés avec NetWare 6.5. Ils sont décrits à la section « Managing Passwords by Using Password Policies (Gestion des mots de passe à l'aide des stratégies de mot de passe) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html).
- eDirectory 8.6. 2 ne peut pas être utilisé pour l'arborescence dont se sert Identity Manager. En revanche, eDirectory 8.6.2 est pris en charge pour un sous-ensemble de fonctions de

synchronisation des mots de passe. Vous pouvez donc utiliser eDirectory 8.6.2 pour d'autres arborescences si vous n'êtes pas encore prêt à mettre à niveau la totalité de votre environnement.

- Lors de la mise à niveau du logiciel, l'une des manières de réduire l'impact du déploiement du mot de passe universel consiste à créer une arborescence séparée pour Identity Manager, fonctionnant en tant que coffre-fort d'identité. De nombreux environnements utilisent déjà un coffre-fort d'identité pour Identity Manager et les pilotes.
- Le mot de passe universel apporte des fonctionnalités qui n'étaient pas prises en charge par les précédents outils de gestion des mots de passe, comme l'application des stratégies de mot de passe et la possibilité d'utiliser des caractères spéciaux.
- Il est très important de mettre à jour le client Novell et d'autres utilitaires, de manière à éviter une désynchronisation entre le mot de passe NDS et le mot de passe universel, parfois appelée « dérive du mot de passe ». Reportez-vous à la section « Planning Login and Change Password Methods for your Users (Planification des méthodes de login et de modification des mots de passe pour les utilisateurs) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html).
- La version la plus récente du client Novell prend en charge le mot de passe universel, peut renseigner le champ à la place de l'utilisateur lorsque vous activez le mot de passe universel pour la première fois pour cet utilisateur, et peut afficher et appliquer les stratégies de mot de passe NMAS lorsque les utilisateurs modifient leurs mots de passe.
- Un système connecté n'affiche pas les règles avancées créés dans une stratégie de mot de passe. Pour l'heure, le client Novell, même s'il les applique, est également concerné.

  Il est préférable de demander aux utilisateurs de ne modifier le mot de passe que dans la console en libre-service de iManager.

  Si vous les autorisez à modifier leurs mots de passe sur un système connecté ou en utilisant la dernière version du client Novell, aidez-les à créer un mot de passe conforme en vérifiant que les règles de la stratégie de mot de passe leur ont bien été communiqués.
- Assurez-vous que les administrateurs et les techniciens du service d'assistance savent que ConsoleOne® ne prend en charge le mot de passe universel que s'il est utilisé sur un serveur NetWare® 6.5 ou une version ultérieure ou sur une machine disposant de la dernière version du client Novell.
- Vérifiez que les administrateurs et les utilisateurs du service d'assistance comprennent les implications liées à l'utilisation d'utilitaires ne prenant en charge que le mot de passe NDS. Ces utilitaires peuvent être utilisés pour se connecter, mais pas pour modifier les mots de passe. Cette mesure évite le problème de dérive du mot de passe.

  Le *Novell Modular Authentication Services (NMAS) 3.0 Administration Guide (Guide d'administration de Novell Modular Authentication Services (NMAS) 3.0)* (http://www.novell.com/documentation/nmas30/index.html) contient la référence d'un document TID qui répertorie les utilitaires prenant en charge le mot de passe universel.

5.4.4 Mise en correspondance des conteneurs

Les stratégies de mot de passe NMAS sont assignées dans une perspective centrée sur l'arborescence. La synchronisation des mots de passe, en revanche, est définie pilote par pilote. Les pilotes sont installés pour chaque serveur et ne peuvent gérer que les utilisateurs se trouvant sur une réplique principale ou en lecture/écriture.

Pour que la synchronisation des mots de passe donne les résultats escomptés, vérifiez que les conteneurs d'une réplique principale ou en lecture/écriture sur le serveur, exécutant les pilotes et auxquels s'applique la synchronisation, correspondent aux conteneurs pour lesquels vous avez assigné des stratégies de mot de passe en activant le mot de passe universel. L'assignation d'une stratégie de mot de passe au conteneur racine d'une partition garantit que cette stratégie s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

5.4.5 Configuration de la notification par message électronique

Pour utiliser la fonction de notification par message électronique :

- Utilisez la tâche Configuration de la notification dans iManager pour configurer le serveur de messagerie.
- Le cas échéant, utilisez la tâche Configuration de la notification dans iManager pour personnaliser les modèles de message électronique.
- Vérifiez que les utilisateurs du coffre-fort d'identité ont rempli l'attribut Adresse de messagerie Internet.

Suivez les instructions de la Section 5.12, « Configuration de la notification par message électronique », page 147.

5.5 Configuration et synchronisation d'un nouveau pilote

Si vous n'avez pas utilisé la version 1.0 de la synchronisation des mots de passe dans votre environnement et si vous créez un pilote ou remplacez une configuration Identity Manager existante par une nouvelle configuration, configurez la fonctionnalité de synchronisation des mots de passe dans Identity Manager.

1. Vérifiez que votre environnement est prêt à utiliser le mot de passe universel.

   Reportez-vous à la Section 5.4, « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 96.

2. Créez un pilote ou remplacez la configuration de pilote existante par la configuration Identity Manager 3.

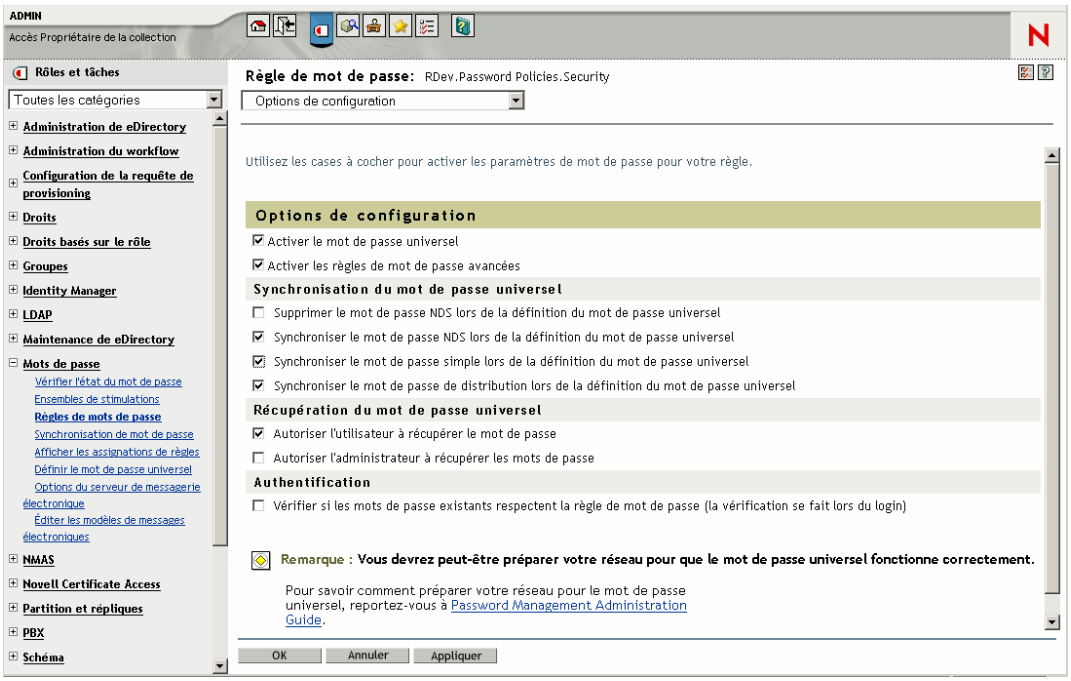
   Les configurations de Identity Manager contiennent les stratégies Identity Manager et les autres éléments nécessaires à la synchronisation des mots de passe dans Identity Manager. Pour plus d'informations sur l'importation des nouveaux exemples de configuration des pilotes, reportez-vous au Identity Manager Driver Guide (Guide de pilote Identity Manager) (http://www.novell.com/documentation/beta/dirxmldrivers) concerné.

3. Activez le mot de passe universel pour les utilisateurs en créant des stratégies de mot de passe NMAS, l'option Mot de passe universel étant activée.

   Reportez-vous à la section « Creating Password Policies (Création de stratégies de mot de passe) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html). Si vous avez déjà utilisé le mot de passe universel avec NetWare 6.5, des étapes supplémentaires sont décrites à la section « (NetWare 6.5 Only) Re-Creating Universal Password Assignments (Nouvelle création d'assignation de mot de passe universel - NetWare 6.5 uniquement) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)*.

Nous vous recommandons d'assigner des stratégies de mot de passe au niveau le plus élevé possible de l'arborescence.

La page Options de configuration permet de choisir comment NMAS doit assurer la synchronisation des différents types de mots de passe.



Vous trouverez des scénarios sur l'utilisation de la synchronisation des mots de passe et sur le rôle des stratégies de mot de passe Identity Manager à la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111. Reportez-vous également à l'aide en ligne.

4 Active Directory, NIS ou NT Domain uniquement : si vous voulez que les systèmes connectés fournissent des mots de passe utilisateur à Identity Manager, installez de nouveaux filtres de synchronisation des mots de passe et configurez-les.

Pour plus d'informations, reportez-vous au guide d'implémentation de chacun de ces pilotes, disponible à la page Identity Manager Drivers (Pilotes Identity Manager) (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

5 Pour chaque système connecté, assurez-vous que le flux de mots de passe est défini comme vous le souhaitez.

5a Dans iManager, cliquez sur *Gestion des mots de passe* > *Synchronisation de mot de passe*, puis recherchez les pilotes pour les systèmes connectés à gérer.

5b Reportez-vous aux paramètres actuels pour le flux de mots de passe.

Il s'agit d'une interface graphique permettant de définir les valeurs de configuration globale (GCV). Modifiez-les en cliquant sur le nom d'un pilote. Vous pouvez modifier les paramètres afin d'indiquer :

- si Identity Manager accepte les mots de passe de ce système.
- Le mot de passe que Identity Manager doit mettre à jour : directement le mot de passe universel ou directement le mot de passe de distribution.

Identity Manager contrôle le point d'entrée, et donc l'identité du mot de passe qu'il met à jour. NMAS contrôle le flux entre chaque type de mot de passe, en fonction des paramètres définis dans les options de configuration de la stratégie de mot de passe. Reportez-vous à l'illustration de l'Étape 3 page 99.

- Si la stratégie de mot de passe pour l'utilisateur est appliquée aux modifications de mots de passe entrant dans Identity Manager.
- Si la stratégie de mot de passe pour l'utilisateur est appliquée sur le système connecté, en réinitialisant les mots de passe non conformes.
- Si les mots de passe sont acceptés par ce système connecté.
- Si les notifications par message électronique sont envoyées en cas d'échec de la synchronisation des mots de passe.

6 Testez la synchronisation des mots de passe.

- Vérifiez que le mot de passe Identity Manager est distribué sur les systèmes spécifiés.
- Vérifiez que les systèmes connectés spécifiés publient les mots de passe vers Identity Manager.

Afin d'obtenir des astuces de dépannage, reportez-vous à la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111.

5.6 Mise à niveau depuis la version 1.0 de la synchronisation des mots de passe

Cette tâche ne s'applique qu'aux pilotes Identity Manager existants pour Active Directory et NT Domain utilisés avec la version 1.0 de la synchronisation des mots de passe.

Il est très important de bien suivre la procédure adéquate lorsque vous effectuez une mise à niveau depuis la version 1.0 de la synchronisation des mots de passe.

Pour plus d'informations, reportez-vous aux guides d'implémentation de chaque pilote Identity Manager pour Active Directory et NT Domain, disponibles sur la page Identity Manager Drivers (Pilotes Identity Manager) (http://www.novell.com/documentation/dirxmldrivers/index.html).

5.7 Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe

Cette section explique comment ajouter la prise en charge de la synchronisation des mots de passe sous Identity Manager à une configuration de pilote existante, au lieu de remplacer les configurations existantes par les exemples de configuration fournis avec Identity Manager.

Cette prise en charge doit être ajoutée à chaque pilote devant participer à la synchronisation des mots de passe. Pour ce faire, importez un fichier de configuration de type « support pack intégré » pour ajouter à la fois les stratégies, le manifeste de pilote et les valeurs de configuration globale.

Après l'ajout des stratégies, du manifeste du pilote et des valeurs de configuration globale, vous devez également ajouter l'attribut nspmDistributionPassword au filtre du pilote.

Important : si vous mettez à niveau un pilote Identity Manager pour AD ou NT Domain, et si ce pilote est utilisé avec la version 1.0 de la synchronisation des mots de passe, suivez les instructions

de mise à niveau proposées dans les guides d'implémentation des pilotes Identity Manager pour Active Directory et NT Domain, disponibles à la page Identity Manager Drivers (Pilotes Identity Manager) (http://www.novell.com/documentation/dirxmldrivers/index.html).

Les stratégies ajoutées dans cette procédure sont destinées à la prise en charge de la synchronisation des mots de passe à l'aide du mot de passe universel et du mot de passe de distribution. Si vous utilisez le pilote Identity Manager pour ne synchroniser que le mot de passe NDS, il est recommandé de ne pas utiliser les stratégies de la configuration de pilote Identity Manager. Le mot de passe NDS est synchronisé à l'aide des attributs Clé publique et Clé privée et non à l'aide de ces stratégies, comme cela est décrit à la Section 5.8.2, « Scénario 1 : utilisation du mot de passe NDS pour la synchronisation entre deux coffres-forts d'identité », page 112.

Conditions préalables

- ❑ Créez un enregistrement du pilote existant à l'aide de l'assistant d'exportation des pilotes.
- ❑ Vérifiez que vous avez bien installé le nouveau module d'interface pilote.

  Certaines fonctionnalités de synchronisation des mots de passe (par exemple, la fonction Vérifier l'état des mots de passe) ne fonctionnent qu'avec le nouveau module d'interface pilote Identity Manager.

  Important : si vous mettez à niveau un pilote Identity Manager pour AD ou NT Domain, et si ce pilote est utilisé avec la version 1.0 de la synchronisation des mots de passe, n'installez pas le module d'interface pilote avant d'avoir consulté les instructions de mise à niveau. Suivez les instructions de mise à niveau que vous trouverez dans les guides d'implémentation de chaque pilote Identity Manager pour Active Directory et NT Domain, disponibles à la page Identity Manager Drivers (Pilotes Identity Manager) (http://www.novell.com/documentation/dirxmldrivers/index.html).

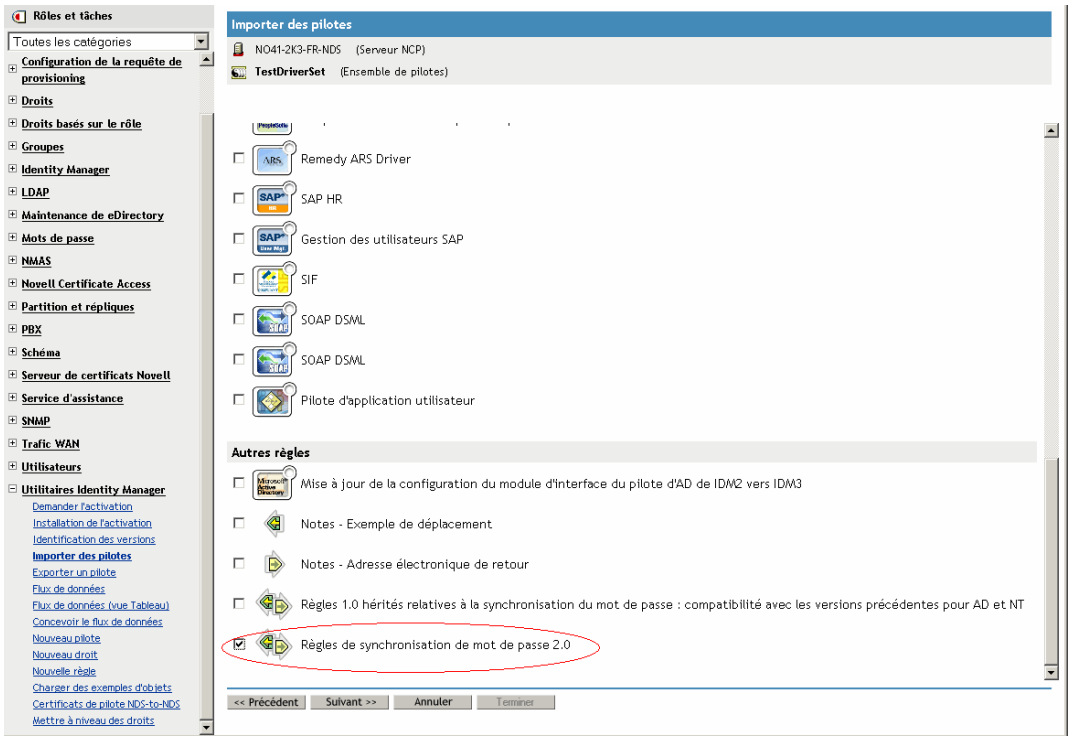
5.7.1 Étape 1 : convertissez le pilote au format Identity Manager 3.

1. Vérifiez que votre environnement est prêt à utiliser le mot de passe universel.

   Reportez-vous à la Section 5.4, « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 96.

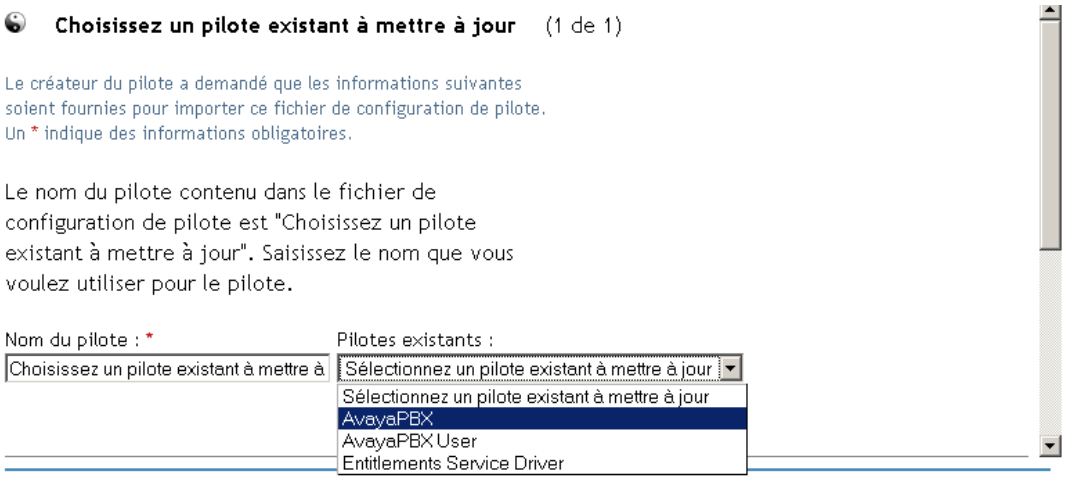
   Si vous utilisez la version 1.1a de DirXML®, reportez-vous à la Section 2.3, « Mise à niveau de la configuration d'un pilote du format DirXML 1.1a au format Identity Manager », page 21.
2. Dans iManager, cliquez sur *Utilitaires Identity Manager* > *Importer des pilotes*.
3. Sélectionnez l'ensemble de pilotes dans lequel se trouve le pilote existant, puis cliquez sur *Suivant*.

4 Déroulez la liste des configurations de pilotes jusqu'à *Autres stratégies* et sélectionnez uniquement *Stratégies de synchronisation de mot de passe 2.0*.



5 Cliquez sur *Suivant*.

6 Dans la liste déroulante *Pilotes existants*, sélectionnez le pilote à mettre à jour.



7 Dans la liste déroulante *Système connecté*, sélectionnez le type de système connecté.

Si le nom du pilote ne s'affiche pas dans la liste déroulante, sélectionnez *Autres systèmes*.

En fonction du type du pilote, l'assistant d'importation crée des entrées dans le manifeste du pilote pour préciser les capacités de configuration et le système connecté :

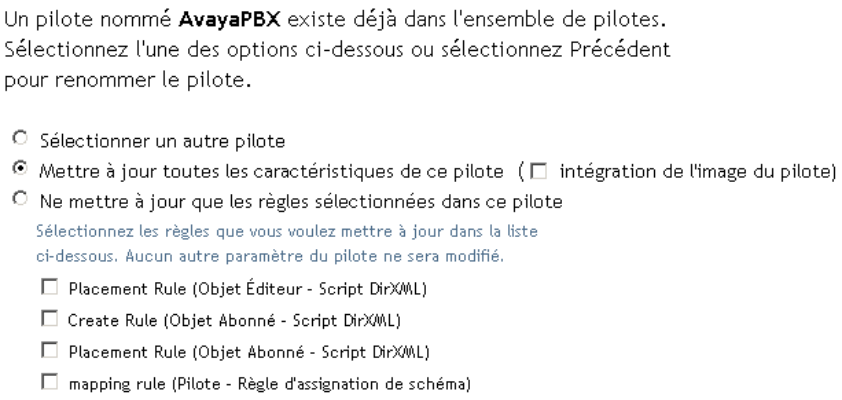
- Le système connecté peut-il fournir des mots de passe à Identity Manager ?

  Cela fait référence au mot de passe de l'utilisateur sur le système connecté, et non à un mot de passe qui peut être créé à l'aide d'une feuille de style. Seuls AD, eDirectory et NIS peuvent le faire.

- Le système connecté peut-il accepter des mots de passe venant de Identity Manager ?
- Le système connecté peut-il vérifier si le mot de passe correspond à celui de Identity Manager ?

Les entrées du manifeste du pilote doivent être correctes pour que les stratégies de synchronisation des mots de passe fonctionnent. Le manifeste du pilote indique la capacité combinée du système connecté, du module d'interface pilote Identity Manager et des stratégies de configuration des pilotes ; il ne doit généralement pas être modifié par l'administrateur réseau.

8 Cliquez sur *Suivant*.



9 Si vous n'avez pas de manifeste de pilote ni de valeurs de configuration globale à enregistrer, sélectionnez *Mettre à jour toutes les caractéristiques de ce pilote*.

Cette option fournit le manifeste du pilote, les valeurs de configuration globale et les stratégies Identity Manager nécessaires à la synchronisation des mots de passe.

Le manifeste et les valeurs de configuration globale remplacent toutes les valeurs existantes. Comme les paramètres de ce type n'existent que depuis Identity Manager 2, les pilotes DirXML 1.*x* ne devraient comporter aucune valeur existante susceptible d'être remplacée.

Les stratégies de synchronisation des mots de passe n'écrasent pas les objets Stratégie existants. Elles sont simplement ajoutées à l'objet Pilote.

Remarque : si vous devez enregistrer un manifeste de pilote ou des valeurs de configuration globale, sélectionnez *Ne mettre à jour que les stratégies sélectionnées dans ce pilote*, puis cochez les cases correspondant à ces stratégies. Cette option importe les stratégies de mot de passe mais ne modifie ni le manifeste de pilote ni les valeurs de configuration globale. Vous devez coller manuellement toute valeur supplémentaire.

---

10 Cliquez sur *Suivant*, puis sur *Terminer* pour mettre fin à l'utilisation de l'assistant.

À ce moment de la procédure, les nouvelles stratégies ont été créées en tant qu'objets Stratégie de l'objet Pilote ; cependant, elles ne font pas encore partie de la configuration du pilote. Vous

devez pour cela insérer chacune d'entre elles manuellement, au bon endroit dans la configuration du pilote sur les canaux Abonné et Éditeur.

5.7.2 Étape 2 : ajoutez les stratégies à la configuration du pilote

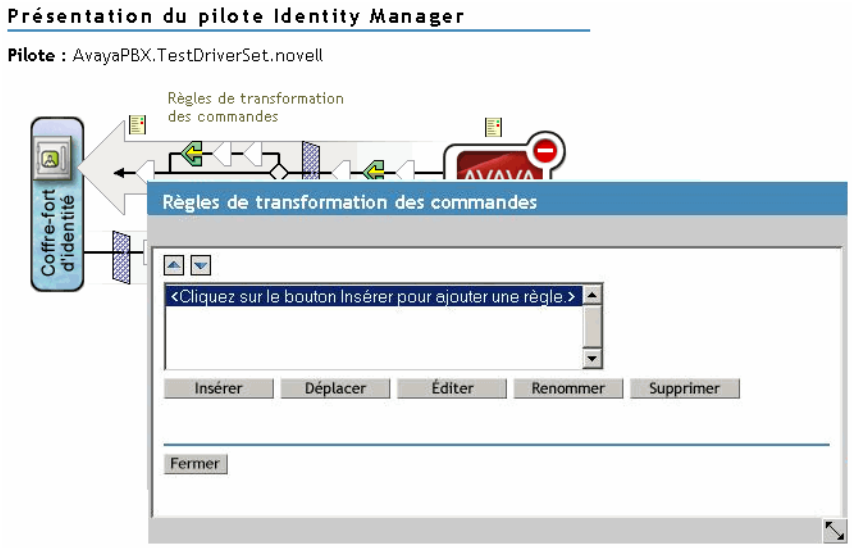
Pour connaître la liste des stratégies à ajouter et l'emplacement recommandé, reportez-vous à la Section 5.3.4, « Stratégies requises pour la configuration du pilote », page 91.

Insérez chacune des nouvelles stratégies à l'endroit qui convient dans la configuration du pilote existante.

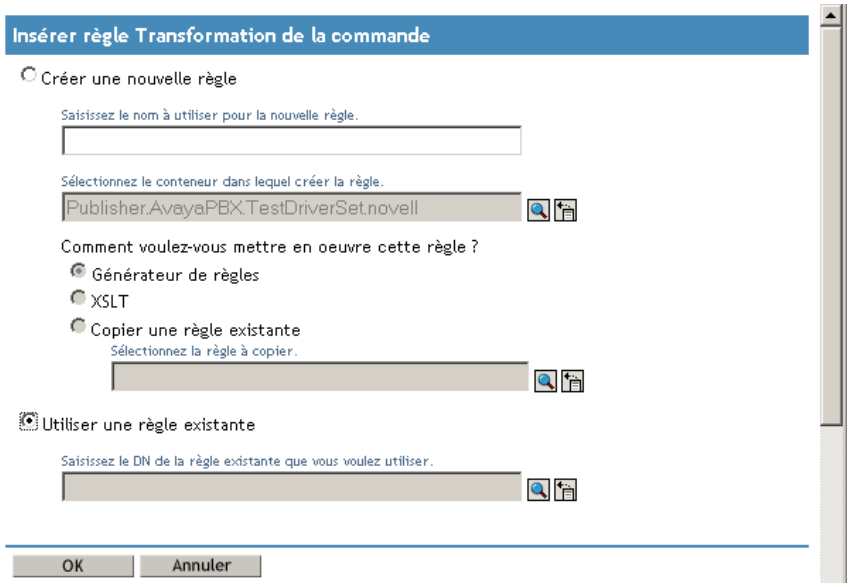
Si l'ensemble comprend plusieurs stratégies, vérifiez que ces stratégies de synchronisation de mot de passe Identity Manager apparaissent au bas de la liste.

Répétez ces étapes pour chaque stratégie.

1. Sélectionnez *Identity Manager > Présentation de Identity Manager*, puis recherchez l'ensemble de pilotes contenant le pilote dont vous effectuez la mise à jour.
2. Cliquez sur le pilote que vous venez de mettre à jour (par exemple, AvayaPBX).
3. Cliquez sur l'icône correspondant à l'endroit où vous devez ajouter l'une des nouvelles stratégies (par exemple, Stratégies de transformation de la commande sur le canal Éditeur).



4 Cliquez sur Insérer pour ajouter la nouvelle stratégie.



5 Cliquez sur *Utiliser une stratégie existante*, localisez le nouvel objet Stratégie, puis cliquez sur *OK*.

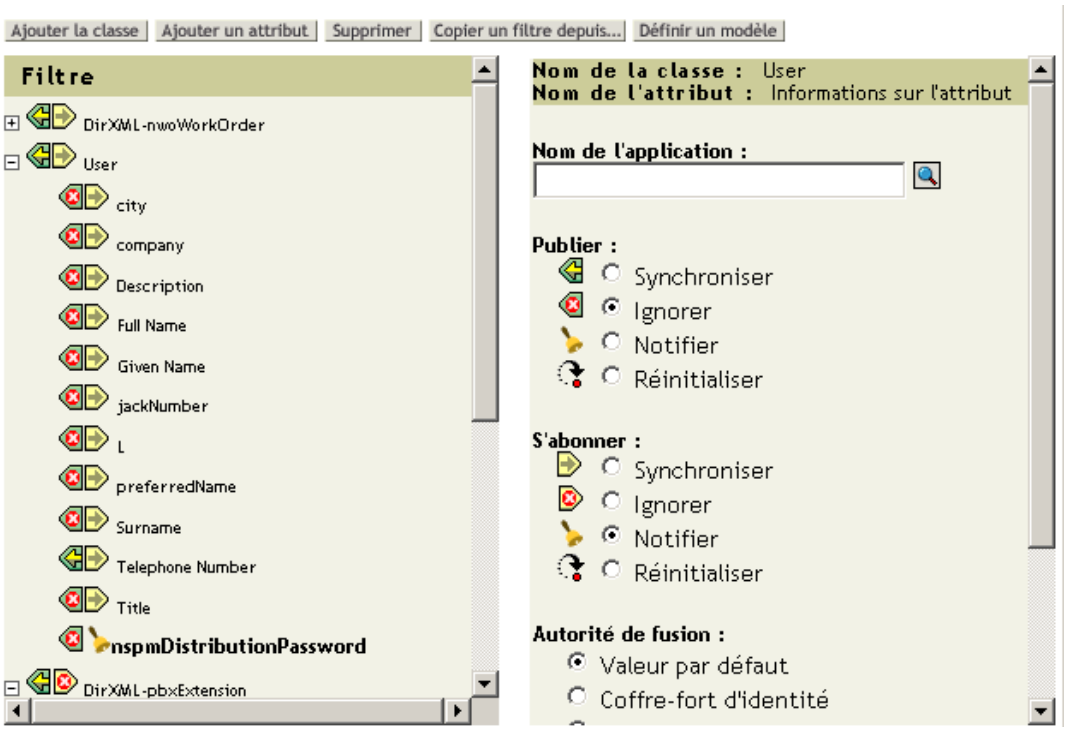
6 Si la liste des nouvelles stratégies contient plusieurs stratégies, utilisez les flèches pour amener les nouvelles stratégies à l'endroit correct dans la liste.

Vérifiez que les stratégies sont bien dans l'ordre indiqué à la Section 5.3.4, « Stratégies requises pour la configuration du pilote », page 91.

5.7.3 Étape 3 : changez les paramètres de filtre

1 Pour les classes d'objets pour lesquelles vous voulez synchroniser les mots de passe (Utilisateur, par exemple), vérifiez que l'attribut nspmDistributionPassword se trouve dans le filtre et qu'il possède les paramètres suivants :

- Pour le canal Éditeur, définissez le filtre sur *Ignorer* pour l'attribut *nspmDistributionPassword*.
- Pour le canal Abonné, définissez le filtre sur *Notifier* pour l'attribut *nspmDistribution Password*.



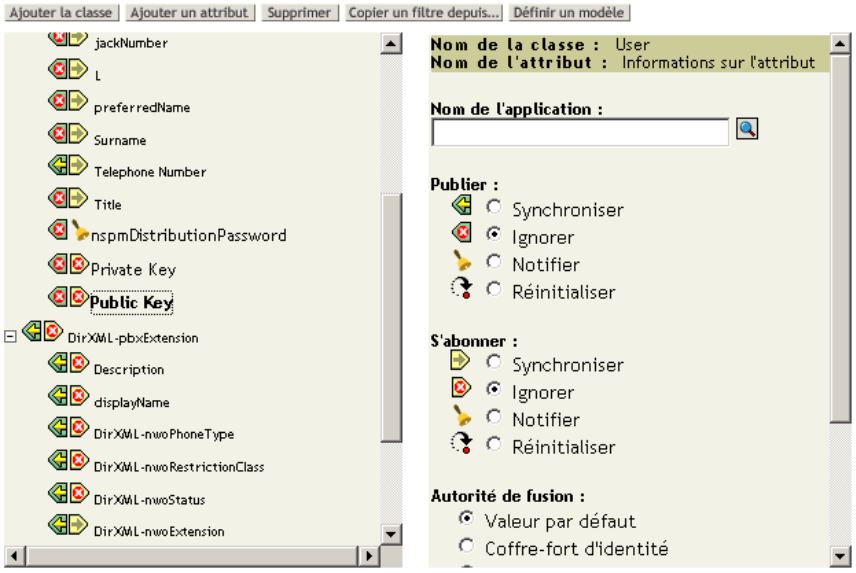
Pour afficher l'attribut, vous devrez peut-être faire défiler les classes et en sélectionner une (par exemple, Utilisateur), puis faire défiler les attributs.

Si l'attribut nspmDistributionPassword ne figure pas dans la liste :

1a Vérifiez que la classe est bien sélectionnée, puis cliquez sur *Ajouter un attribut*.

1b Recherchez et sélectionnez nspmDistributionPassword, puis cliquez sur OK.

2 Pour tous les objets pour lesquels l'attribut *nspmDistributionPassword* est défini sur *Notifier*, définissez les attributs Clé publique et Clé privée sur Ignorer.



3 Pour chacun des pilotes à mettre à niveau pour qu'il participe à la synchronisation des mots de passe, recommencez de l'Étape 2 page 102 (dans « Convertissez le pilote au format Identity Manager 3 ») à l'Étape 2 de cette section (« Changez les paramètres de filtre »).

À ce moment de la procédure, le pilote dispose d'un nouveau module d'interface pilote et des autres éléments nécessaires à la prise en charge de la synchronisation des mots de passe dans la configuration du pilote. De plus, il est au format Identity Manager, et il possède le manifeste de pilote, les GCV, les stratégies de synchronisation de mot de passe et les paramètres de filtre.

4 Vérifiez le guide d'implémentation de chaque pilote concerné pour connaître les éventuelles étapes ou informations complémentaires sur la configuration de la synchronisation des mots de passe dans Identity Manager. Reportez-vous à la page Identity Manager Drivers (Pilotes Identity Manager) (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

5 Activez le mot de passe universel pour les utilisateurs en créant les stratégies de mot de passe, l'option Mot de passe universel étant activée.

Reportez-vous à la section « Creating Password Policies (Création de stratégies de mot de passe) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html). Si vous avez déjà utilisé le mot de passe universel avec NetWare 6.5, des étapes supplémentaires sont décrites à la section « (NetWare 6.5 Only) Re-Creating Universal Password Assignments (Nouvelle création d'assignation de mot de passe universel - NetWare 6.5 uniquement) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)*.

Nous vous recommandons d'assigner des stratégies de mot de passe au niveau le plus élevé possible de l'arborescence.

La page Options de configuration permet de choisir comment NMAS doit assurer la synchronisation des différents types de mots de passe. Les paramètres par défaut doivent convenir à la plupart des implémentations. Pour plus d'informations, reportez-vous à l'aide en ligne sur cette page.

Vous trouverez des scénarios sur l'utilisation de la synchronisation des mots de passe et sur le rôle des stratégies de mot de passe à la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111.

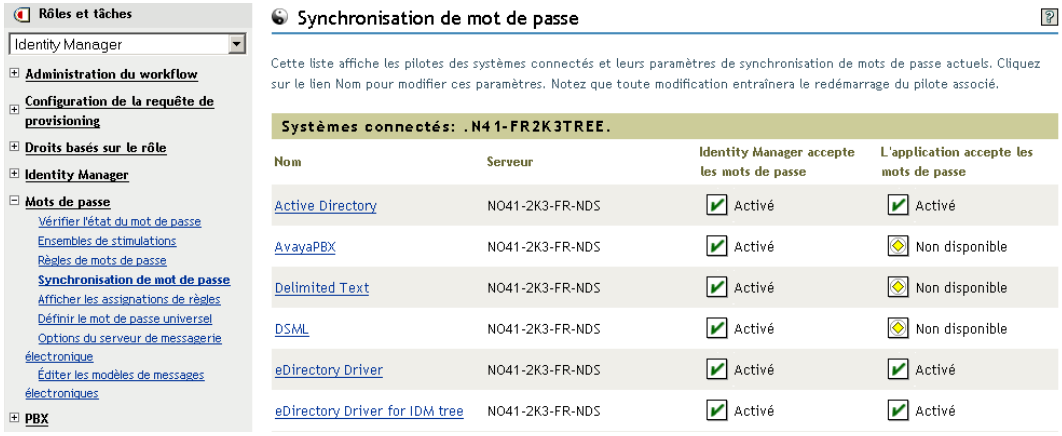
Les stratégies de mot de passe NMAS sont assignées dans une perspective centrée sur l'arborescence. La synchronisation des mots de passe, en revanche, est définie pilote par pilote. Les pilotes sont installés pour chaque serveur et ne peuvent gérer que les utilisateurs se trouvant sur une réplique principale ou en lecture/écriture.

Pour que la synchronisation des mots de passe donne les résultats escomptés, vérifiez que les conteneurs situés dans une réplique principale ou en lecture/écriture sur le serveur sur lequel s'exécutent les pilotes auxquels s'applique la synchronisation correspondent aux conteneurs pour lesquels vous avez assigné des stratégies de mot de passe avec le mot de passe universel activé. L'assignation d'une stratégie de mot de passe au conteneur racine d'une partition garantit que cette stratégie s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

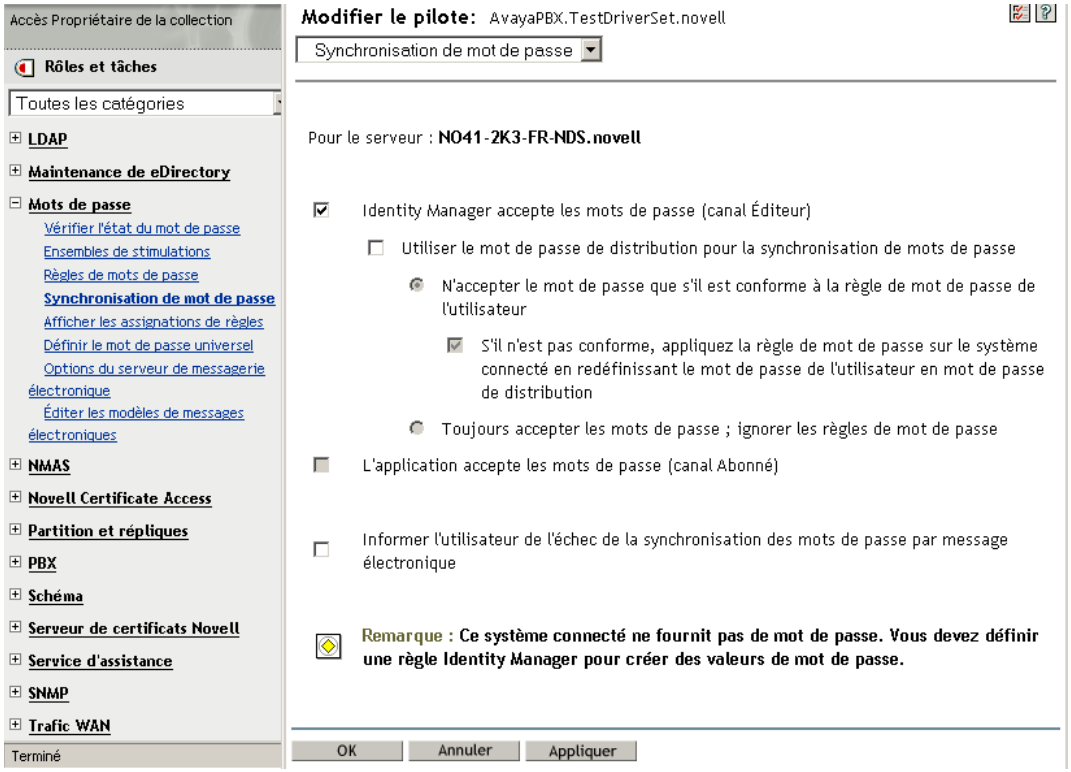
5.7.4 Étape 4 : définissez le flux de synchronisation des mots de passe

Vérifiez que votre flux de mots de passe est défini comme vous le souhaitez pour chaque système connecté.

1. Dans iManager, sélectionnez *Mots de passe* > *Synchronisation de mot de passe*.
2. Recherchez, dans l'arborescence ou le conteneur, les pilotes correspondant aux systèmes connectés que vous souhaitez gérer.



3 Sélectionnez un pilote pour afficher les paramètres actuels du flux de mots de passe.



Cette page répertorie les valeurs de configuration globale (GCV). Vous pouvez les modifier à l'aide des options.

Identity Manager contrôle le point d'entrée (le mot de passe qu'il met à jour). NMAS contrôle le flux entre chaque type de mot de passe, en fonction des options définies dans les options de configuration (l'Étape 3 page 90 permet d'afficher la page Options de configuration). Si vous sélectionnez *Utiliser le mot de passe de distribution pour la synchronisation de mots de passe*, Identity Manager utilise directement le mot de passe de distribution. Si vous désactivez cette option, il utilise directement le mot de passe universel.

Pour plus d'informations (et des illustrations) sur ces options, reportez-vous à la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111. Reportez-vous également à l'aide en ligne.

4 Testez la synchronisation des mots de passe.

Vérifiez que le mot de passe Identity Manager est distribué sur les systèmes spécifiés.

Vérifiez que les systèmes connectés spécifiés publient les mots de passe vers Identity Manager.

Afin d'obtenir des astuces de dépannage, reportez-vous à la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111.

5.8 Implémentation de la synchronisation des mots de passe

La fonctionnalité de synchronisation des mots de passe fournie dans Identity Manager permet d'implémenter plusieurs scénarios différents. Cette section décrit des scénarios de base, qui vous aideront à comprendre en quoi les paramètres de synchronisation des mots de passe Identity Manager et les stratégies de mot de passe NMAS affectent la synchronisation des mots de passe. Ces scénarios peuvent être associés pour répondre aux besoins de votre environnement.

5.8.1 Présentation de la relation entre Identity Manager et NMAS

Utilitaires et NMAS

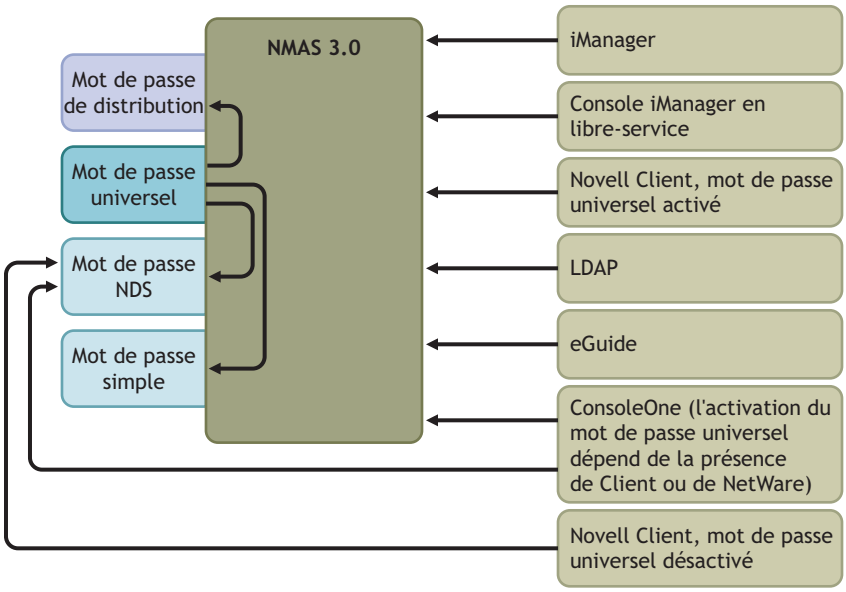
Certains utilitaires tels que iManager et le client Novell communiquent avec NMAS à la place de mettre à jour directement le mot de passe. NMAS est l'entité chargée de déterminer quels mots de passe seront mis à jour.

NMAS synchronise les mots de passe dans un coffre-fort d'identité, en fonction des paramètres configurés dans les stratégies de mot de passe NMAS.

Les utilitaires existants qui ne prennent pas en charge le mot de passe universel mettent directement à jour le mot de passe NDS, au lieu de communiquer avec NMAS pour déterminer les mots de passe mis à jour. Vous devez savoir comment les utilisateurs et les administrateurs du service d'assistance se servent des utilitaires hérités dans votre environnement. Ces utilitaires hérités mettent à jour directement le mot de passe NDS sans passer par NMAS. Il y a donc un risque de dérive du mot de passe (désynchronisation du mot de passe universel et du mot de passe NDS) si vous utilisez le mot de passe universel avec NMAS 2.3.

Vous devrez par exemple, pour assurer la prise en charge du mot de passe universel, vérifier que les utilisateurs mettent à jour le client Novell et que les utilisateurs du service d'assistance n'utilisent ConsoleOne qu'avec la dernière version du client Novell ou de NetWare.

Figure 5-5 *Synchronisation des mots de passe avec NMAS*



Identity Manager et NMAS

Identity Manager contrôle le point d'entrée (en mettant directement à jour le mot de passe universel ou le mot de passe de distribution). NMAS contrôle le flux de synchronisation des mots de passe dans le coffre-fort d'identité.

Dans le scénario 1, le pilote Identity Manager pour eDirectory peut mettre directement à jour le mot de passe NDS. Ce scénario est pratiquement le même que celui fourni dans DirXML 1.*x*.

Dans le scénario 2, le scénario 3 et le scénario 4, Identity Manager met à jour soit le mot de passe universel, soit le mot de passe de distribution. Identity Manager effectue les modifications par le biais de NMAS. Cela permet à NMAS de mettre à jour d'autres mots de passe du coffre-fort d'identité, en fonction des paramètres des stratégies de mot de passe NMAS, et d'appliquer les stratégies de mot de passe NMAS avancées pour les mots de passe synchronisés avec les systèmes connectés. Dans ces scénarios, le mot de passe distribué par Identity Manager aux systèmes connectés est toujours le mot de passe de distribution.

La différence entre les scénarios 2, 3 et 4 réside dans les différentes combinaisons de paramètres des stratégies de mot de passe NMAS et de paramètres de synchronisation de mot de passe Identity Manager pour chaque pilote de système connecté.

5.8.2 Scénario 1 : utilisation du mot de passe NDS pour la synchronisation entre deux coffres-forts d'identité

Comme dans la version 1.0 de la synchronisation des mots de passe, vous pouvez synchroniser le mot de passe NDS entre deux coffres-forts d'identité à l'aide du pilote eDirectory. Ce scénario n'exige pas l'implémentation du mot de passe universel et peut être utilisé avec eDirectory 8.6. 2ou

une version ultérieure. Ce type de synchronisation de mot de passe est aussi appelé synchronisation de la paire clé privée/clé publique.

Cette méthode ne doit être utilisée que pour la synchronisation de mots de passe entre deux coffres-forts d'identité. Elle ne fait pas appel à NMAS et ne peut donc pas être utilisée pour synchroniser les mots de passe avec les applications connectées.

- « Avantages et inconvénients du scénario 1 » page 113
- « Implémentation du scénario 1 » page 114
- « Dépannage du scénario 1 » page 115

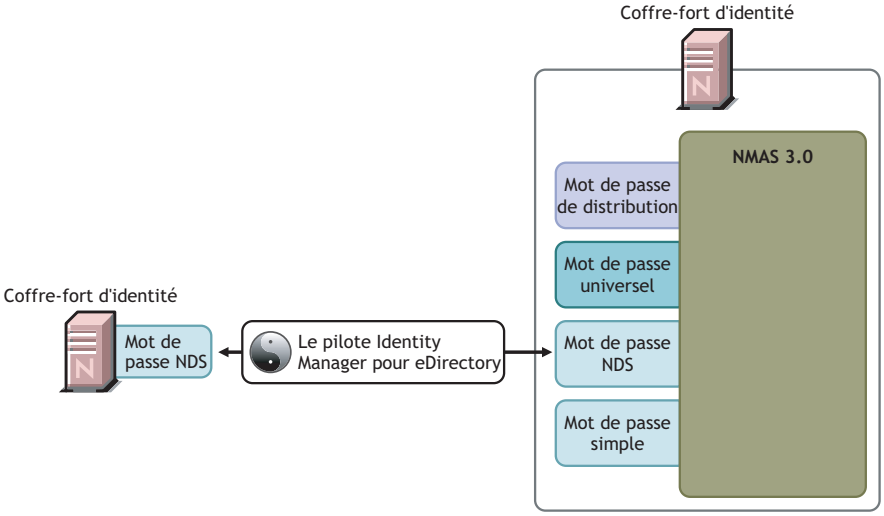
Avantages et inconvénients du scénario 1

Tableau 5-11 *Avantages : synchronisation des mots de passe dans eDirectory à l'aide du mot de passe NDS*

Avantages	Inconvénients
Simplicité de la configuration. N'inclut que les attributs adéquats dans le filtre de pilote. Si vous déployez Identity Manager 3 et eDirectory 8.7.3 par étapes, cette méthode peut vous aider à effectuer un déploiement graduel. • Il n'est pas nécessaire d'ajouter les nouvelles stratégies de synchronisation des mots de passe aux configurations de pilote. • N'exige pas que le mot de passe universel soit implémenté dans le coffre-fort d'identité. • Peut être utilisé avec les coffres-forts connectés exécutant eDirectory version 8.6.2 ou ultérieure. • N'exige pas NMAS 2.3. Applique les restrictions de base sur les mots de passe que vous définissez pour le mot de passe NDS.	Cette méthode permet de synchroniser les mots de passe entre deux coffres-forts d'identité. Ils ne peuvent pas être synchronisés vers d'autres systèmes connectés. N'actualise ni le mot de passe universel ni le mot de passe de distribution. Cette méthode n'utilisant pas NMAS, vous ne pouvez pas valider les mots de passe provenant d'un autre coffre-fort d'identité en fonction des règles de mot de passe avancées. Cette méthode n'utilisant pas NMAS, vous ne pouvez pas réinitialiser les mots de passe sur le coffre-fort d'identité connecté s'ils ne se conforment pas à la stratégie de mot de passe NMAS. Aucune notification par message électronique n'est fournie en cas d'échec de synchronisation des mots de passe Les opérations Vérifier l'état du mot de passe depuis iManager ne sont pas prises en charge (pour cette fonction, le mot de passe de distribution est exigé).

Le diagramme suivant montre que, comme dans DirXML 1.*x*, le pilote Identity Manager pour eDirectory peut être utilisé pour synchroniser le mot de passe NDS entre deux coffres-forts d'identité. Ce scénario ne passe pas par NMAS.

Figure 5-6 *Utilisation du mot de passe NDS pour la synchronisation entre deux coffres-forts d'identité*



Implémentation du scénario 1

Pour implémenter ce type de synchronisation des mots de passe, configurez le pilote.

Déploiement du mot de passe universel

Inutile.

Configuration de la stratégie de mot de passe

Aucun.

Paramètres de la synchronisation des mots de passe

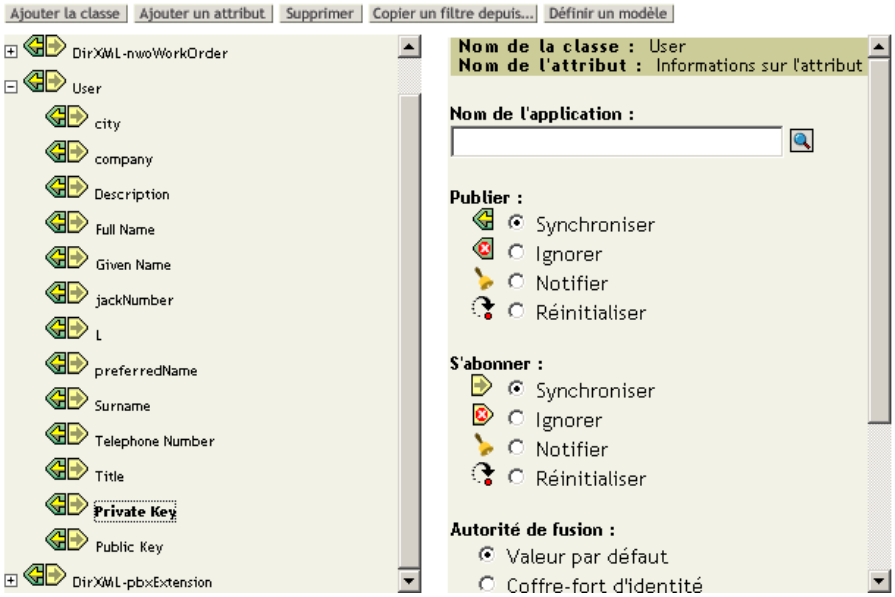
Aucun. Les paramètres de la page Synchronisation de mot de passe pour un pilote n'ont aucun effet sur cette méthode de synchronisation du mot de passe NDS.

Configuration de pilote

Supprimez les stratégies de synchronisation des mots de passe répertoriées à la Section 5.3.4, « Stratégies requises pour la configuration du pilote », page 91. Ces stratégies ont pour objet de prendre en charge le mot de passe universel et le mot de passe de distribution. Le mot de passe NDS est synchronisé à l'aide des attributs Clé publique et Clé privée et non à l'aide de ces stratégies.

Vérifiez que le filtre des deux pilotes du coffre-fort d'identité synchronise les attributs Clé publique et Clé privée pour toutes les classes d'objet nécessitant la synchronisation des mots de passe. La figure suivante en montre un exemple.

Figure 5-7 *Synchronisation des attributs Clé publique et Clé privée*



Dépannage du scénario 1

- Activez l'option DSTrace.
- Vérifiez le filtre du pilote pour vous assurer que les attributs Clé publique et Clé privée sont paramétrés sur Synchroniser et non sur Ignorer.
- Reportez-vous également aux astuces de la Section 5.13, « Dépannage des problèmes de synchronisation des mots de passe », page 160.

5.8.3 Scénario 2 : synchronisation avec le mot de passe universel

Grâce à Identity Manager, vous pouvez synchroniser un mot de passe de système connecté avec le mot de passe universel dans le coffre-fort d'identité.

Lors de la mise à jour du mot de passe universel, il est également possible de mettre à jour le mot de passe NDS, le mot de passe de distribution ou le mot de passe simple, en fonction des paramètres de la stratégie de mot de passe NMAS.

Tout système connecté peut publier des mots de passe vers Identity Manager, bien que tous les systèmes connectés ne puissent pas fournir le mot de passe de l'utilisateur. Active Directory, par exemple, peut publier le mot de passe d'un utilisateur vers Identity Manager. Même si PeopleSoft ne fournit pas de mot de passe provenant directement du système PeopleSoft lui-même, il peut fournir un mot de passe initial créé dans une stratégie lors de la configuration du pilote, par exemple un mot de passe basé sur l'ID de l'employé ou sur son nom. Tous les pilotes ne peuvent pas s'abonner aux

modifications de mots de passe depuis Identity Manager. Reportez-vous à la Section 5.2, « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 84.

Avantages et inconvénients du scénario 2

Tableau 5-12 *Avantages : synchronisation avec le mot de passe universel*

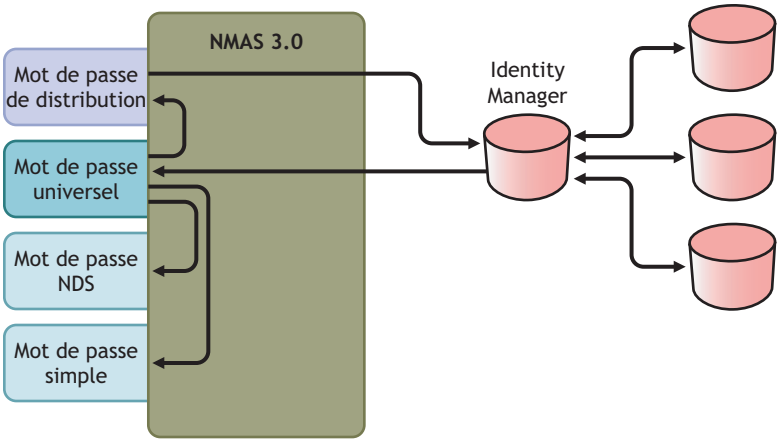
Avantages	Inconvénients
Permet la synchronisation bidirectionnelle des mots de passe entre le coffre-fort d'identité et le système connecté. Permet la validation des mots de passe par rapport à la stratégie de mot de passe NMAS. Permet l'envoi de notifications par message électronique en cas d'échec des opérations de mot de passe, par exemple lorsqu'un mot de passe provenant d'un système connecté ne se conforme pas au mot de passe. Prend en charge la tâche Vérifier l'état des mots de passe dans iManager, si le mot de passe universel est synchronisé avec le mot de passe de distribution et si le système connecté prend en charge la vérification des mots de passe. NMAS applique les règles de mot de passe avancées si vous les avez activées. Lorsqu'un mot de passe provenant d'un système connecté n'est pas conforme, une erreur est générée et une notification par message électronique est envoyée si vous avez spécifié cette option. Si vous ne souhaitez pas appliquer de stratégies de mot de passe, vous pouvez désactiver l'option Activer les règles de mots de passe avancées dans la stratégie NMAS.	Pour des raisons de conception, cette méthode ne permet pas la réinitialisation des mots de passe dans le système connecté ; en effet, le mot de passe de distribution et le mot de passe universel pourraient ne pas être identiques, selon les paramètres définis dans les stratégies de mot de passe.

Ce scénario est illustré dans la figure suivante.

1. Les mots de passe arrivent par le biais de Identity Manager.
2. Identity Manager met directement à jour le mot de passe universel par le biais de NMAS.
3. NMAS synchronise le mot de passe universel avec le mot de passe de distribution et les autres mots de passe, en fonction des paramètres de la stratégie de mot de passe NMAS.
4. Identity Manager récupère le mot de passe de distribution et le communique aux systèmes connectés paramétrés pour accepter les mots de passe.

Même si, dans ce diagramme, il est indiqué que plusieurs systèmes connectés se connectent à Identity Manager, n'oubliez pas que vous créez chaque paramètre individuellement pour chaque pilote du système connecté.

Figure 5-8 *Synchronisation des mots de passe avec le mot de passe universel*



Implémentation du scénario 2

Pour implémenter ce type de synchronisation des mots de passe :

- « Déploiement du mot de passe universel » page 117
- « Configuration de la stratégie de mot de passe » page 117
- « Paramètres de la synchronisation des mots de passe » page 119
- « Configuration de pilote » page 120

Déploiement du mot de passe universel

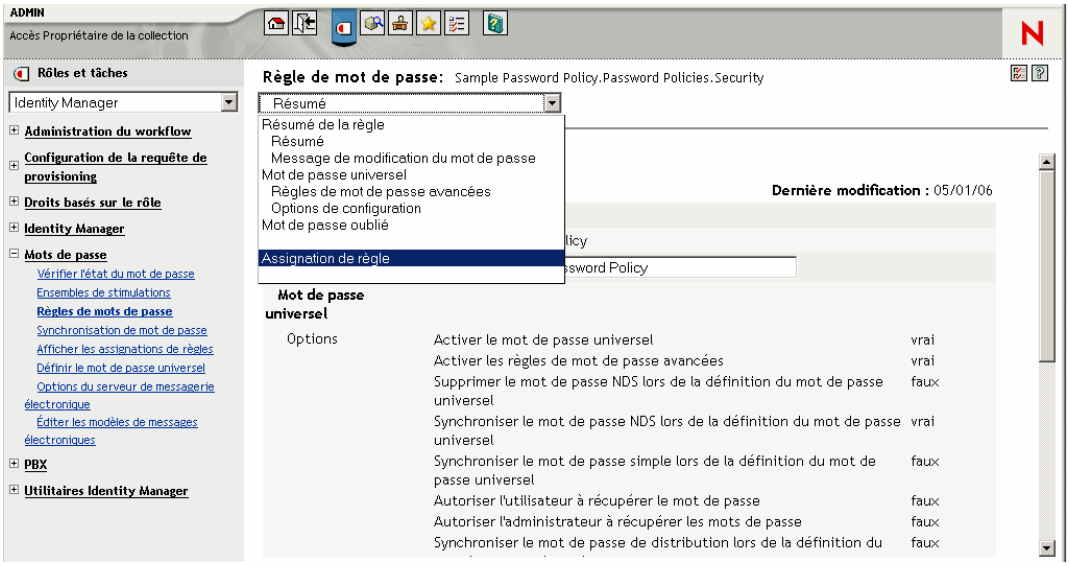
Vérifiez que votre environnement est prêt à utiliser le mot de passe universel. Reportez-vous à la Section 5.4, « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 96.

Configuration de la stratégie de mot de passe

Vérifiez qu'une stratégie de mot de passe NMAS est assignée aux parties du coffre-fort d'identité pour lesquelles vous voulez disposer de la synchronisation des mots de passe.

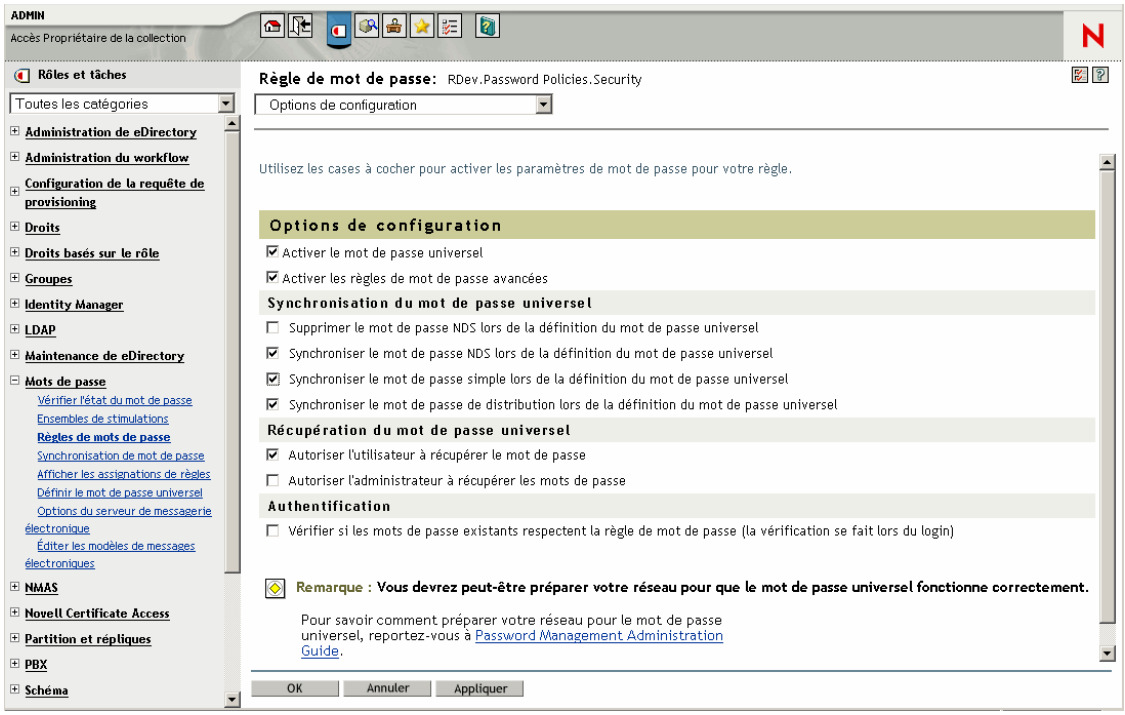
1. Dans iManager, sélectionnez *Mots de passe* > *Stratégies de mots de passe*.
2. Sélectionnez une stratégie, puis cliquez sur *Éditer*.

3 Localisez et sélectionnez l'objet dans lequel vous souhaitez que la synchronisation se fasse.



Vous pouvez affecter la stratégie à la totalité de l'arborescence (en localisant et en sélectionnant l'objet Stratégie de login dans le conteneur Sécurité), à un conteneur racine de partition, à un conteneur, voire à un utilisateur particulier. Pour simplifier la gestion, nous vous recommandons d'assigner des stratégies de mot de passe au niveau le plus élevé possible de l'arborescence.

4 Vérifiez que les éléments suivants sont sélectionnés dans la stratégie de mot de passe :



- *Activer le mot de passe universel*

- *Synchroniser le mot de passe NDS lors de la définition du mot de passe universel*
- *Supprimer le mot de passe NDS lors de la définition du mot de passe universel*

  Comme Identity Manager récupère le mot de passe de distribution pour communiquer les mots de passe aux systèmes connectés, il est important que cette option soit sélectionnée pour autoriser la synchronisation bidirectionnelle des mots de passe.

5 Terminez votre stratégie de mot de passe comme vous le souhaitez.

NMAS applique les règles de mot de passe avancées si vous les avez activées. Si vous ne souhaitez pas appliquer les règles des stratégies de mot de passe, désactivez l'option *Activer les règles de mots de passe avancées*.

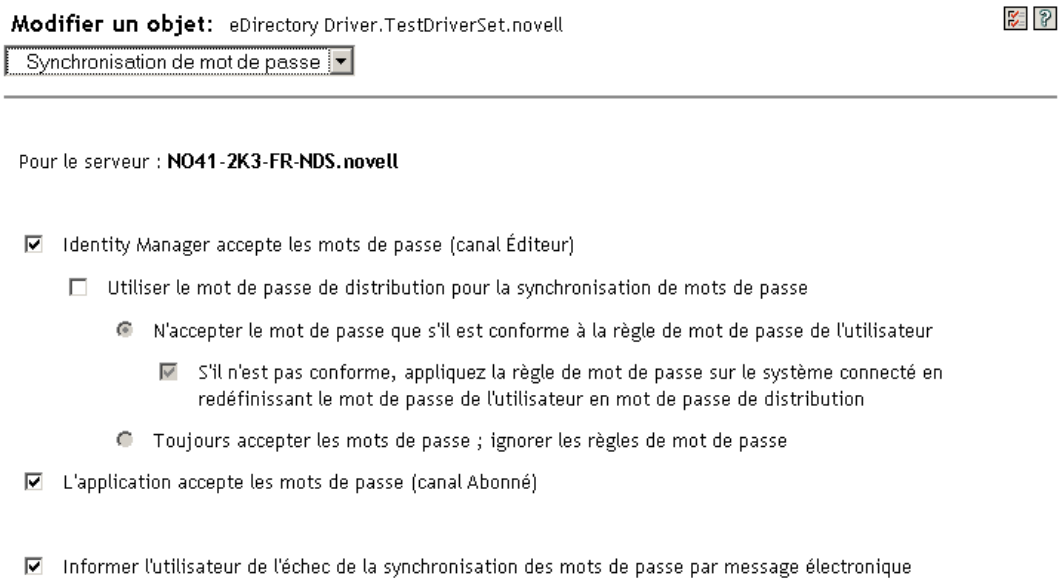
Si vous utilisez les règles de mot de passe avancées, vérifiez qu'elles n'entrent pas en conflit avec les stratégies de mot de passe des systèmes connectés abonnés aux mots de passe.

Paramètres de la synchronisation des mots de passe

1 Dans iManager, sélectionnez *Mots de passe* > *Synchronisation de mot de passe*.

2 Recherchez les pilotes des systèmes connectés, puis sélectionnez-en un.

3 Créer les paramètres du pilote pour le système connecté.



Vérifiez que les éléments suivants sont sélectionnés :

- *Identity Manager accepte les mots de passe (canal Éditeur)*

  Un message s'affiche si le manifeste du pilote ne contient pas la capacité password-publish. Il informe les utilisateurs que les mots de passe ne peuvent pas être récupérés depuis l'application, mais uniquement publiés en créant un mot de passe dans la configuration d'un pilote à l'aide d'une stratégie.

- *L'application accepte les mots de passe (canal Abonné)*

  Si le système connecté ne prend pas en charge l'acceptation des mots de passe, l'option est grisée.

Ces paramètres permettent la synchronisation bidirectionnelle des mots de passe lorsqu'elle est prise en charge par le système connecté.

Vous pouvez adapter les paramètres à vos stratégies d'activité pour la source experte des mots de passe. Si, par exemple, un système connecté doit s'abonner aux mots de passe, mais ne pas les publier, ne sélectionnez que l'option *L'application accepte les mots de passe (canal Abonné)*.

4 Assurez-vous que la case *Utiliser le mot de passe de distribution pour la synchronisation de mots de passe* n'est pas cochée.

Dans ce scénario, Identity Manager met directement à jour le mot de passe universel. Le mot de passe de distribution est toujours utilisé pour distribuer les mots de passe sur les systèmes connectés, mais il est mis à jour à partir du mot de passe universel par NMAS et non par Identity Manager.

5 (En option) Sélectionnez les éléments suivants si vous le souhaitez :

- *Informer l'utilisateur de l'échec de la synchronisation des mots de passe par message électronique*

  N'oubliez pas que, pour les notifications par message électronique, l'attribut Adresse de messagerie Internet doit être indiqué pour l'objet Utilisateur eDirectory.

  Les notifications par message électronique n'ont pas une présence insistante. Elles n'ont aucune incidence sur le traitement du document XML qui a déclenché la notification. En cas d'échec, elles ne font pas l'objet d'une nouvelle tentative, sauf si l'opération elle-même est recommencée. Toutefois, les messages de débogage pour les notifications par message électronique sont écrits dans le fichier de trace.

Configuration de pilote

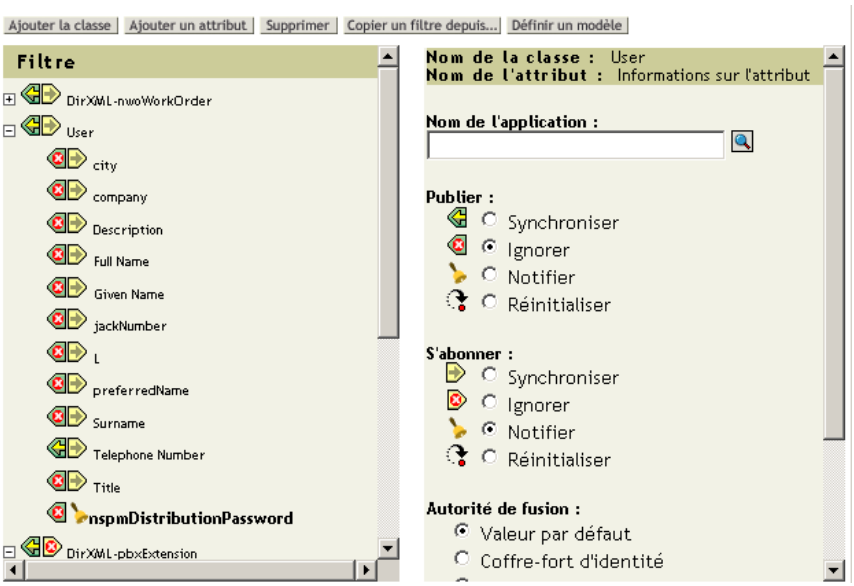
1 Vérifiez que les stratégies obligatoires de synchronisation des mots de passe de script Identity Manager sont incluses dans les configurations de pilote pour chaque pilote qui doit participer à la synchronisation des mots de passe.

Ces stratégies doivent se trouver dans la configuration de votre pilote, à l'endroit correct et dans le bon ordre. Afin d'obtenir la liste des stratégies, reportez-vous à la Section 5.3.4, « Stratégies requises pour la configuration du pilote », page 91.

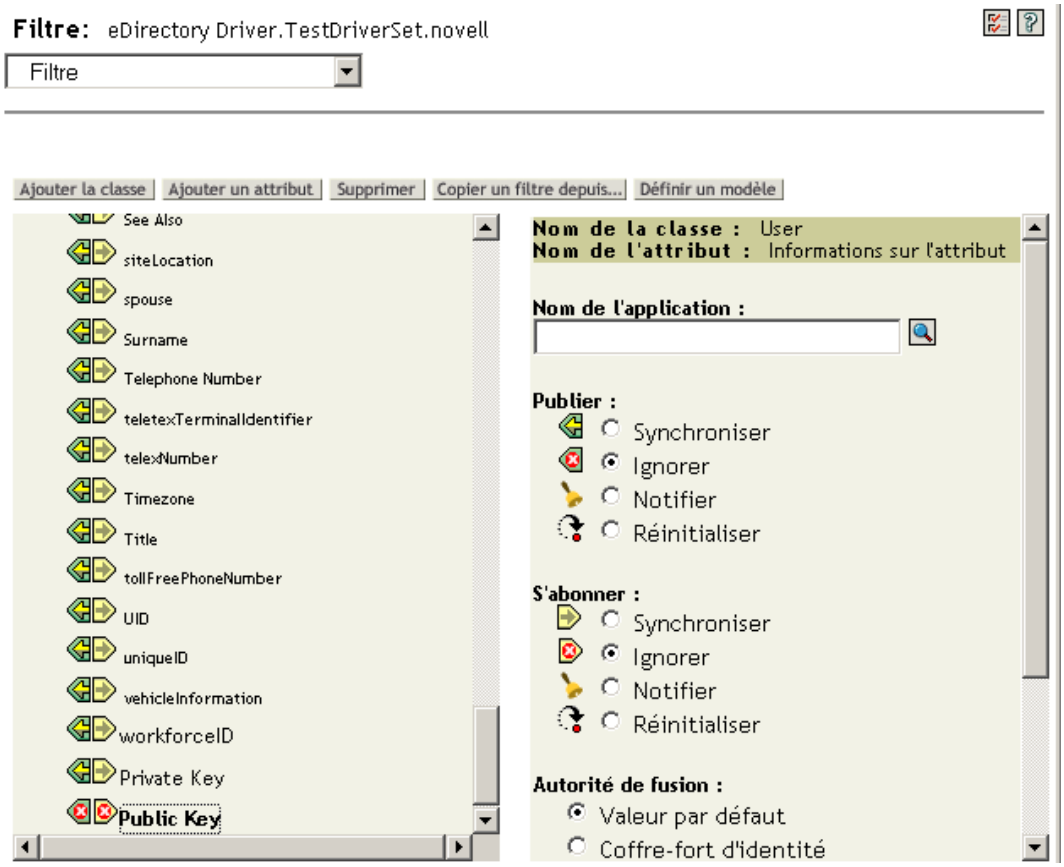
Les exemples de configuration Identity Manager contiennent déjà les stratégies. Si vous effectuez la mise à niveau d'un pilote existant, vous pouvez ajouter les stratégies à l'aide des instructions de la Section 5.7, « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe », page 101.

2 Définissez correctement le filtre pour l'attribut nspmDistributionPassword :

- Pour le canal Éditeur, définissez le filtre du pilote sur *Ignorer* pour l'attribut nspmDistributionPassword, pour toutes les classes d'objet.
- Pour le canal Abonné, définissez le filtre du pilote sur *Notifier* pour l'attribut nspmDistributionPassword, pour toutes les classes d'objet qui doivent s'abonner aux modifications de mot de passe.



3 Pour tous les objets pour lesquels l'attribut nspmDistributionPassword est défini sur *Notifier*, définissez les attributs Clé publique et Clé privée sur *Ignorer*.



4 Pour assurer la sécurité des mots de passe, contrôlez l'identité des personnes disposant de droits sur les objets Identity Manager.

Dépannage du scénario 2

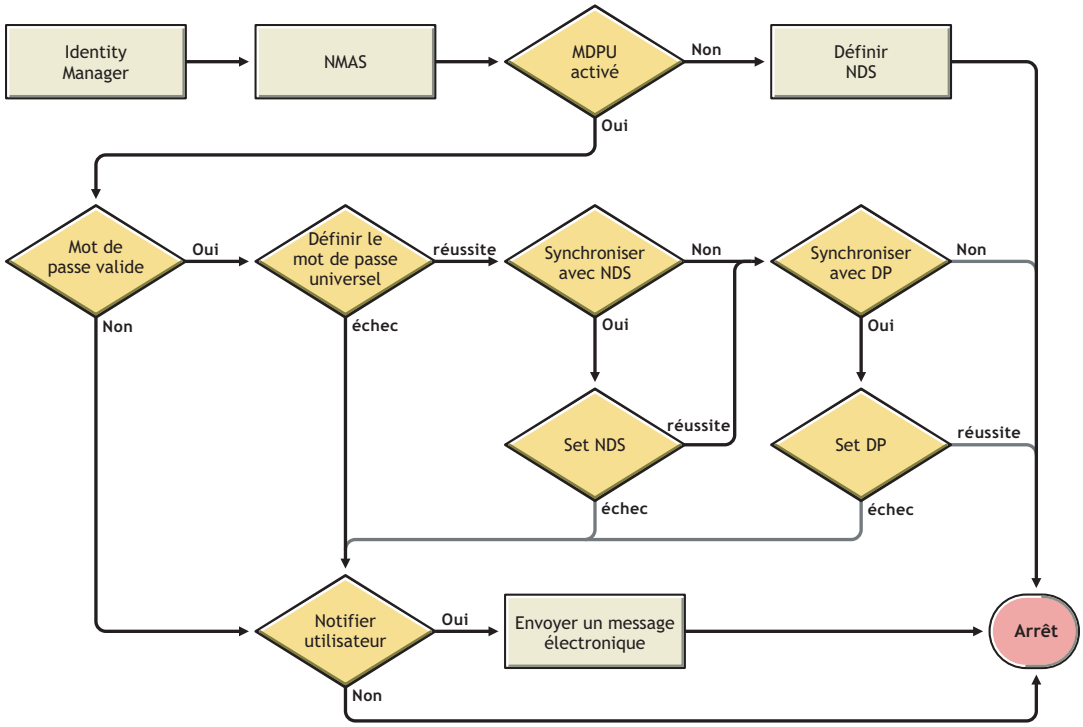
Reportez-vous également aux astuces de la Section 5.13, « Dépannage des problèmes de synchronisation des mots de passe », page 160.

Diagramme du scénario 2

Le diagramme suivant montre comment NMAS gère le mot de passe qu'il reçoit de Identity Manager. Ici, le mot de passe est synchronisé avec le mot de passe universel. NMAS décide comment gérer le mot de passe, en fonction des éléments suivants :

- Le mot de passe universel est-il activé ou non dans la stratégie de mot de passe NMAS.
- Les règles de mot de passe avancées que doivent respecter les mots de passe entrants sont-elles activées ou non.
- Quels sont les autres paramètres de la stratégie de mot de passe pour la synchronisation du mot de passe universel avec les autres mots de passe.

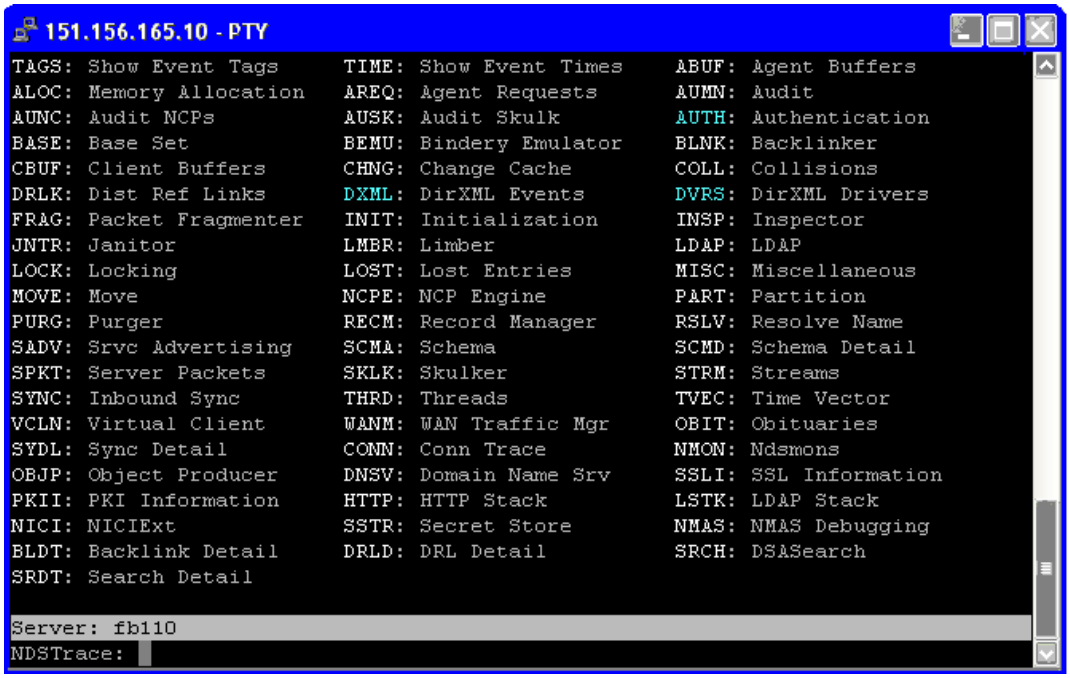
Figure 5-9 *Gestion par NMAS du mot de passe reçu de Identity Manager*



Problème de connexion au coffre-fort d'identité

- Activez les paramètres *+AUTH*, *+DXML* et *+DVRS* dans DSTrace.

Figure 5-10 *Commandes DSTrace*



- Vérifiez que les éléments <password ou <modify-password sont transférés à Identity Manager. Pour ce faire, reportez-vous à l'écran de trace avec ces options activées.
- Vérifiez que le mot de passe est valide, en vous référant aux règles de la stratégie de mot de passe.
- Vérifiez la configuration et l'assignation de la stratégie de mot de passe NMAS. Essayez d'assigner directement la stratégie à l'utilisateur, en vérifiant que vous utilisez la bonne stratégie.
- Sur la page Synchronisation de mot de passe du pilote, vérifiez que l'option *DirXML accepte les mots de passe* est sélectionnée.
- Dans la stratégie de mot de passe, vérifiez que l'option *Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel* est sélectionnée.

Problème pour se loguer à un autre système connecté qui s'abonne aux mots de passe

Cette section permet de corriger le problème suivant : le système connecté publie des mots de passe sur Identity Manager, mais un autre système connecté abonné aux mots de passe ne semble pas recevoir les modifications envoyées par ce système. Cette relation s'appelle aussi un système connecté secondaire, ce qui signifie que le système reçoit des mots de passe du premier système connecté via Identity Manager.

- Activez les paramètres *+DXML* et *+DVRS* dans DSTrace pour voir comment sont traitées les stratégies Identity Manager.
- Définissez le niveau de trace Identity Manager pour le pilote sur *3*.
- Dans la page Synchronisation de mot de passe, vérifiez que l'option *Identity Manager accepte les mots de passe* est sélectionnée.
- Vérifiez que, dans le filtre du pilote, l'attribut nspmDistributionPassword est correctement défini, comme expliqué à l'Étape 2 page 120.
- Vérifiez que le <*mot de passe*>, pour un élément ajout ou <modify-password>, est transféré au système connecté. Pour cela, reportez-vous à l'écran DSTrace ou le fichier contenant les options de trace actives indiquées dans les premiers points.
- Vérifiez que la configuration du pilote inclut les stratégies de mot de passe de script Identity Manager dans le site correct et dans le bon ordre, tel que décrit à la Section 5.3.4, « Stratégies requises pour la configuration du pilote », page 91.
- Comparez la stratégie de mot de passe NMAS dans le coffre-fort d'identité avec toute stratégie de mot de passe appliquée par le système connecté, pour vérifier leur compatibilité.

Le message électronique n'est pas généré en cas d'échec du mot de passe

- Activez les paramètres *+DXML* dans DSTrace pour savoir comment sont traitées les règles Identity Manager.
- Définissez le niveau de trace Identity Manager pour le pilote sur *3*.
- Vérifiez que la règle de génération des messages électroniques est sélectionnée.
- Vérifiez que l'objet Coffre-fort d'identité contient l'adresse de messagerie électronique correcte de l'utilisateur, indiquée dans l'attribut Adresse de messagerie Internet.
- Dans la tâche Configuration de la notification, vérifiez que le serveur SMTP et le modèle de messagerie sont correctement configurés. Reportez-vous à la Section 5.12, « Configuration de la notification par message électronique », page 147.

Erreur lors de l'utilisation de la vérification du mot de passe de l'objet

La tâche iManager Vérifier l'état du mot de passe amène le pilote à vérifier le mot de passe de l'objet. Pour tout problème, revoyez les points suivants :

- Si la vérification du mot de passe de l'objet renvoie -603, cela signifie que l'objet de coffre-fort d'identité ne contient pas d'attribut nspmDistributionPassword. Dans le filtre du pilote, vérifiez les paramètres corrects pour les attributs nspmDistributionPassword. Dans la stratégie de mot de passe, vérifiez également que l'option *Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel* est sélectionnée.
- Si la vérification du mot de passe de l'objet renvoie `Non synchronisé`, vérifiez que la configuration du pilote contient les stratégies de synchronisation des mots de passe appropriées.
- Comparez la stratégie de mot de passe NMAS dans le coffre-fort d'identité avec toute stratégie de mot de passe appliquée par le système connecté, pour vérifier leur compatibilité.
- La vérification du mot de passe de l'objet fonctionne à partir du mot de passe de distribution. Si le mot de passe de distribution n'est pas mis à jour, la vérification du mot de passe de l'objet pourrait ne pas signaler que les mots de passe sont synchronisés.
- Sachez que pour le pilote Identity Manager uniquement, l'option Vérifier l'état du mot de passe vérifie le mot de passe NDS, et non le mot de passe de distribution.

Commandes DSTrace utiles

+DXML : affiche le traitement des règles Identity Manager et les messages d'erreur potentiels.

+DVRS : affiche les messages du pilote Identity Manager.

+AUTH : affiche les modifications des mots de passe NDS.

5.8.4 Scénario 3 : synchronisation d'un coffre-fort d'identité et des systèmes connectés avec mise à jour du mot de passe de distribution dans Identity Manager

Dans ce scénario, Identity Manager met directement à jour le mot de passe de distribution et permet à NMAS de déterminer la manière dont les autres mots de passe du coffre-fort d'identité sont synchronisés.

Tout système connecté peut publier des mots de passe vers Identity Manager, bien que tous les systèmes connectés ne puissent pas fournir le mot de passe de l'utilisateur. Active Directory, par exemple, peut publier le mot de passe d'un utilisateur vers Identity Manager. Même si PeopleSoft ne fournit pas de mot de passe provenant directement du système PeopleSoft lui-même, il peut fournir un mot de passe initial créé dans une stratégie lors de la configuration du pilote, par exemple un mot de passe basé sur l'ID de l'employé ou sur son nom. Tous les pilotes ne peuvent pas s'abonner aux modifications de mots de passe depuis Identity Manager. Reportez-vous à la Section 5.2, « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 84.

- « Avantages et inconvénients du scénario 3 » page 126
- « Implémentation du scénario 3 » page 127
- « Dépannage du scénario 3 » page 131

Avantages et inconvénients du scénario 3

Tableau 5-13 *Avantages : synchronisation d'un coffre-fort d'identité et des systèmes connectés par la mise à jour du mot de passe de distribution*

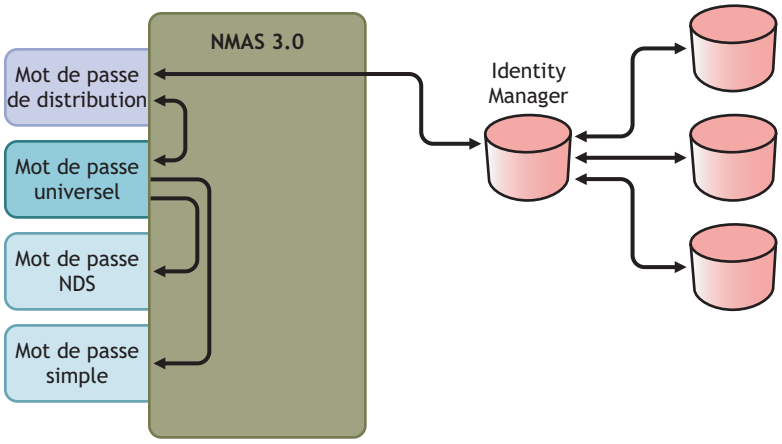
Avantages	Inconvénients
Permet la synchronisation des mots de passe entre le coffre-fort d'identité et les systèmes connectés. Permet de choisir s'il convient ou non d'appliquer les stratégies aux mots de passe provenant des systèmes connectés. Vous pouvez demander à ce qu'une notification soit envoyée en cas d'échec de la synchronisation des mots de passe. Si vous appliquez les stratégies de mot de passe et si un mot de passe n'est pas conforme, vous pouvez choisir de le réinitialiser sur le système connecté au mot de passe de distribution.	

Ce scénario est illustré dans la figure suivante.

1. Les mots de passe arrivent par le biais de Identity Manager.
2. Identity Manager met directement à jour le mot de passe de distribution par le biais de NMAS.
3. Identity Manager utilise également le mot de passe de distribution pour effectuer la répartition vers les systèmes connectés paramétrés pour accepter les mots de passe.
4. NMAS synchronise le mot de passe universel avec le mot de passe de distribution et les autres mots de passe, en fonction des paramètres de la stratégie de mot de passe.

Même si, dans ce diagramme, il est indiqué que plusieurs systèmes connectés se connectent à Identity Manager, n'oubliez pas que vous créez chaque paramètre individuellement pour chaque pilote du système connecté.

Figure 5-11 *synchronisation d'un coffre-fort d'identité et des systèmes connectés par la mise à jour du mot de passe de distribution*



Implémentation du scénario 3

Pour implémenter ce type de synchronisation des mots de passe :

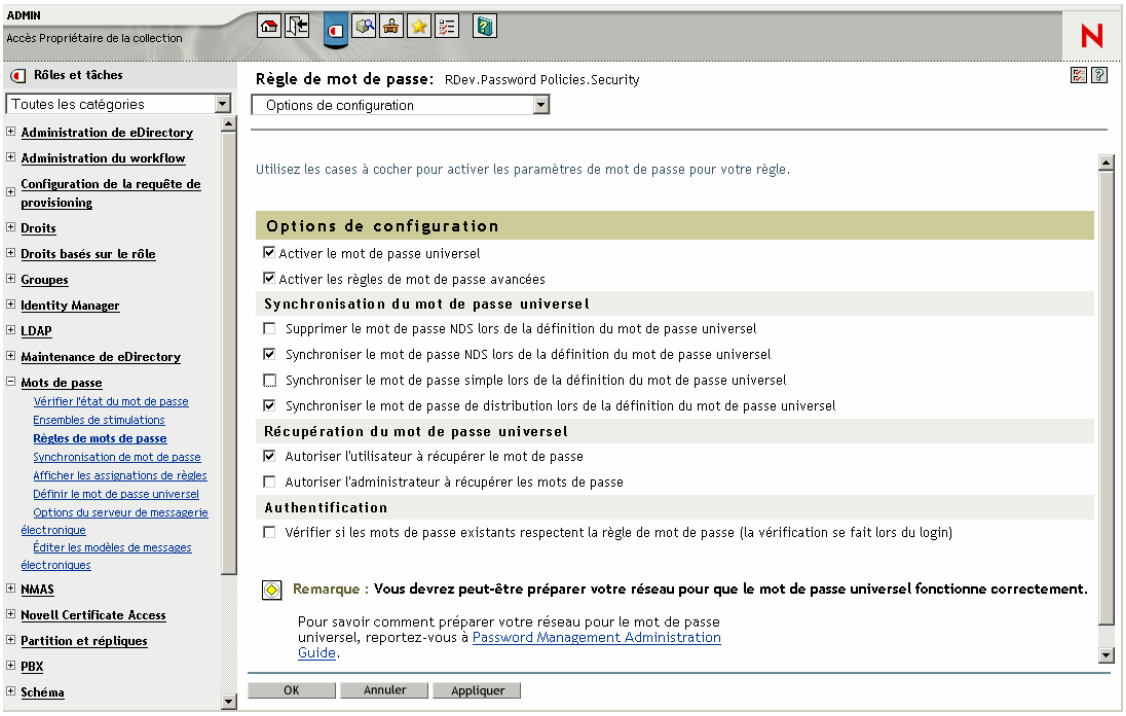
- « Déploiement du mot de passe universel » page 127
- « Configuration de la stratégie de mot de passe » page 127
- « Paramètres de la synchronisation des mots de passe » page 128
- « Configuration de pilote » page 129

Déploiement du mot de passe universel

Vérifiez que votre environnement est prêt à utiliser le mot de passe universel. Reportez-vous à la Section 5.4, « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 96.

Configuration de la stratégie de mot de passe

1. Dans iManager, sélectionnez *Mots de passe* > *Stratégies de mots de passe*.
2. Vérifiez qu'une stratégie de mot de passe est assignée aux parties de l'arborescence du coffre-fort d'identité auxquelles vous souhaitez que la synchronisation des mots de passe soit applicable. Vous pouvez l'assigner à la totalité de l'arborescence, à un conteneur racine de partition, à un conteneur, voire à un utilisateur particulier. Pour simplifier la gestion, nous vous recommandons d'assigner des stratégies de mot de passe au niveau le plus élevé possible de l'arborescence.
3. Vérifiez que les éléments suivants sont sélectionnés dans la stratégie de mot de passe :



- *Activer le mot de passe universel*
- *Synchroniser le mot de passe NDS lors de la définition du mot de passe universel*

- *Supprimer le mot de passe NDS lors de la définition du mot de passe universel*

  Comme Identity Manager récupère le mot de passe de distribution pour communiquer les mots de passe aux systèmes connectés, il est important que cette option soit sélectionnée pour autoriser la synchronisation bidirectionnelle des mots de passe.

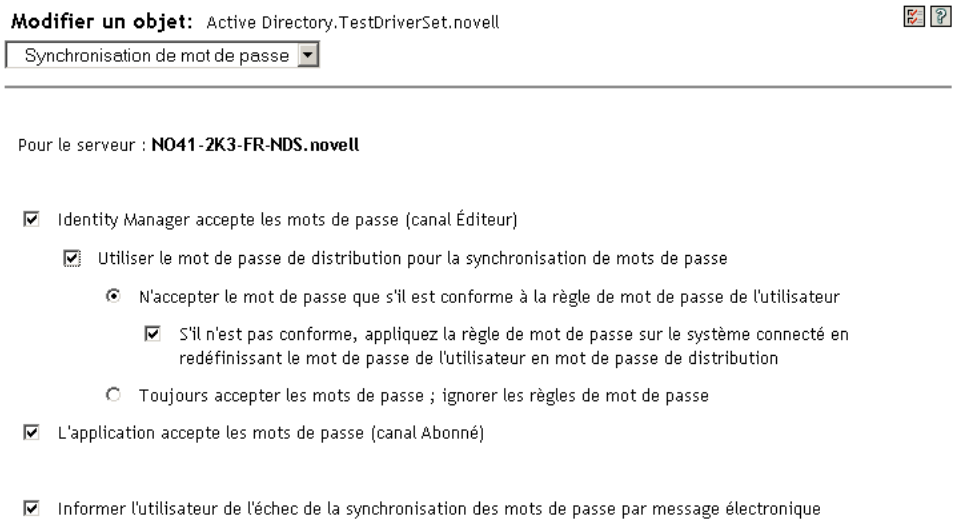
4 Si vous utilisez les règles de mot de passe avancées, vérifiez qu'elles n'entrent pas en conflit avec les stratégies de mot de passe des systèmes connectés qui s'abonnent aux mots de passe.

Paramètres de la synchronisation des mots de passe

1 Dans iManager, sélectionnez *Mots de passe > Synchronisation de mot de passe*.

2 Recherchez les pilotes des systèmes connectés, puis sélectionnez-en un.

3 Créer les paramètres du pilote pour le système connecté.



Vérifiez que les éléments suivants sont sélectionnés :

- *Identity Manager accepte les mots de passe (canal Éditeur)*
- *Utiliser le mot de passe de distribution pour la synchronisation de mot de passe*

  Un message s'affiche si le manifeste du pilote ne contient pas la capacité password-publish. Les utilisateurs sont ainsi informés que les mots de passe ne peuvent pas être récupérés, mais uniquement publiés, par la création d'un mot de passe dans la configuration d'un pilote à l'aide d'une stratégie.
- *L'application accepte les mots de passe (canal Abonné)*

Ces paramètres permettent la synchronisation bidirectionnelle des mots de passe lorsqu'elle est prise en charge par le système connecté.

Vous pouvez adapter les paramètres à vos stratégies d'activité pour la source experte des mots de passe. Si, par exemple, un système connecté doit s'abonner aux mots de passe, mais ne pas les publier, ne sélectionnez que l'option *L'application accepte les mots de passe (canal Abonné)*.

4 Indiquez si vous souhaitez que les stratégies de mot de passe NMAS soient appliquées ou ignorées, en vous servant des options de la section *Utiliser le mot de passe de distribution pour la synchronisation de mots de passe*.

5 (Conditionnel) Si vous avez indiqué que vous souhaitez appliquer les stratégies de mot de passe, indiquez également si vous souhaitez que Identity Manager réinitialise le mot de passe du système connecté en cas de non-conformité.

6 (En option) Sélectionnez les éléments suivants si vous le souhaitez :

- *Informer l'utilisateur de l'échec de la synchronisation des mots de passe par message électronique*

  Gardez en tête que les notifications par message électronique exigent l'attribut Adresse de messagerie Internet sur l'objet utilisateur eDirectory à remplir.

  Les notifications par message électronique n'ont pas une présence insistante. Elles n'ont aucune incidence sur le traitement du document XML qui a déclenché la notification. En cas d'échec, elles ne font pas l'objet d'une nouvelle tentative, sauf si l'opération elle-même est recommencée. Toutefois, les messages de débogage pour les notifications par message électronique sont écrits dans le fichier de trace.

Configuration de pilote

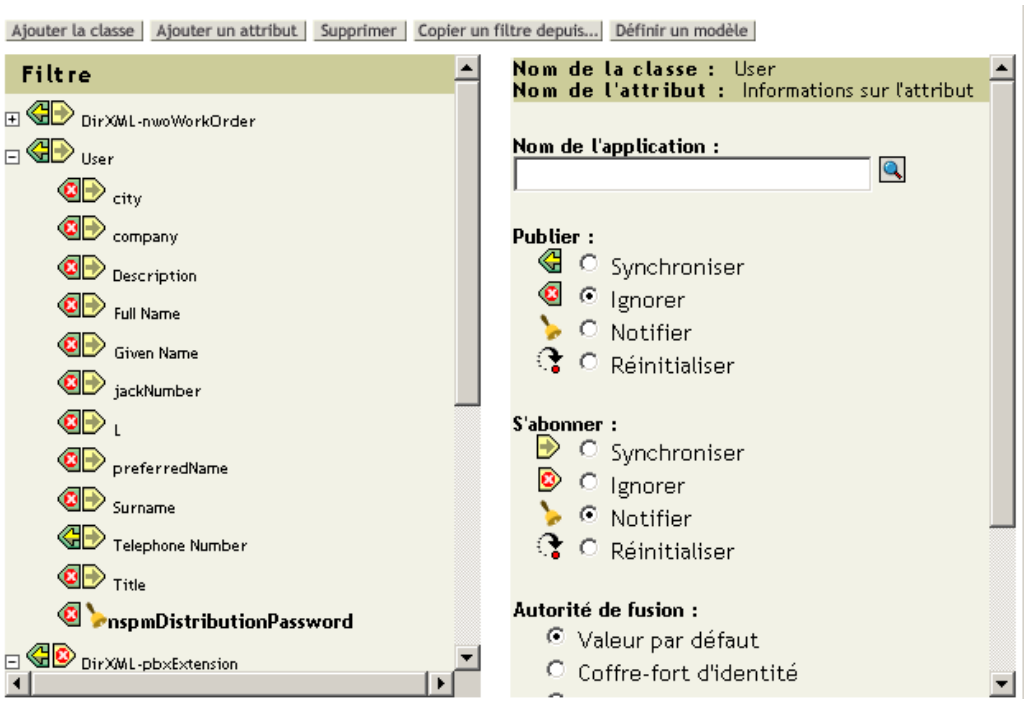
1 Vérifiez que les stratégies obligatoires de synchronisation des mots de passe de script Identity Manager sont incluses dans les configurations de pilote pour chaque pilote qui doit participer à la synchronisation des mots de passe.

  Ces stratégies doivent se trouver dans la configuration de votre pilote, à l'endroit correct et dans le bon ordre. Afin d'obtenir la liste des stratégies, reportez-vous à la Section 5.3.4, « Stratégies requises pour la configuration du pilote », page 91.

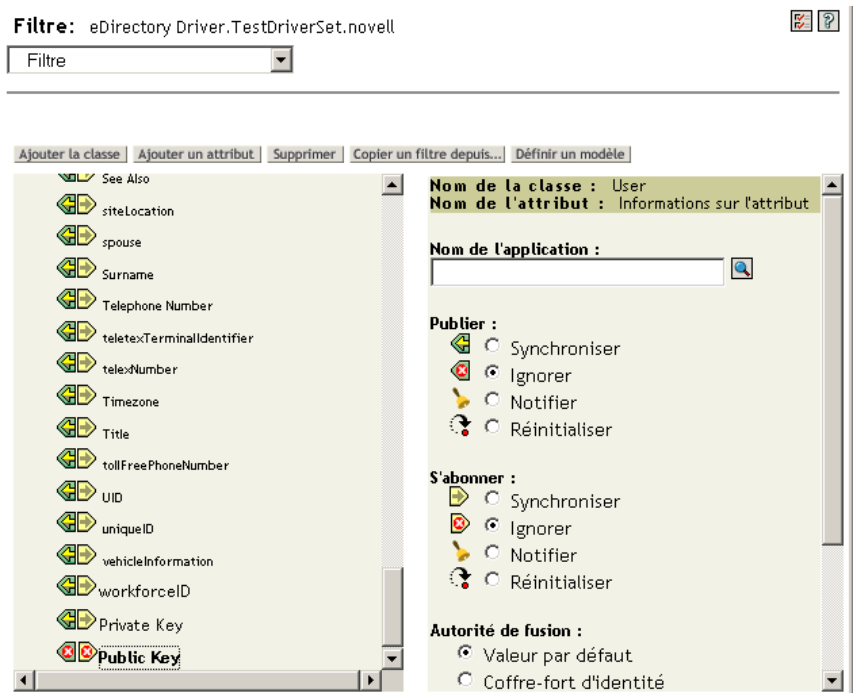
  Les exemples de configuration Identity Manager contiennent déjà les stratégies. Si vous effectuez la mise à niveau d'un pilote existant, vous pouvez ajouter les stratégies à l'aide des instructions de la Section 5.7, « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe », page 101.

2 Définissez correctement le filtre pour l'attribut nspmDistributionPassword :

- Pour le canal Éditeur, définissez le filtre du pilote sur *Ignorer* pour l'attribut nspmDistributionPassword, pour toutes les classes d'objet.
- Pour le canal Abonné, définissez le filtre du pilote sur *Notifier* pour l'attribut nspmDistributionPassword, pour toutes les classes d'objet qui doivent s'abonner aux modifications de mot de passe.



3 Pour tous les objets pour lesquels l'attribut nspmDistributionPassword est défini sur *Notifier*, définissez les attributs Clé publique et Clé privée sur *Ignorer* dans le filtre du pilote.



4 Pour assurer la sécurité des mots de passe, contrôlez l'identité des personnes disposant de droits sur les objets Identity Manager.

Dépannage du scénario 3

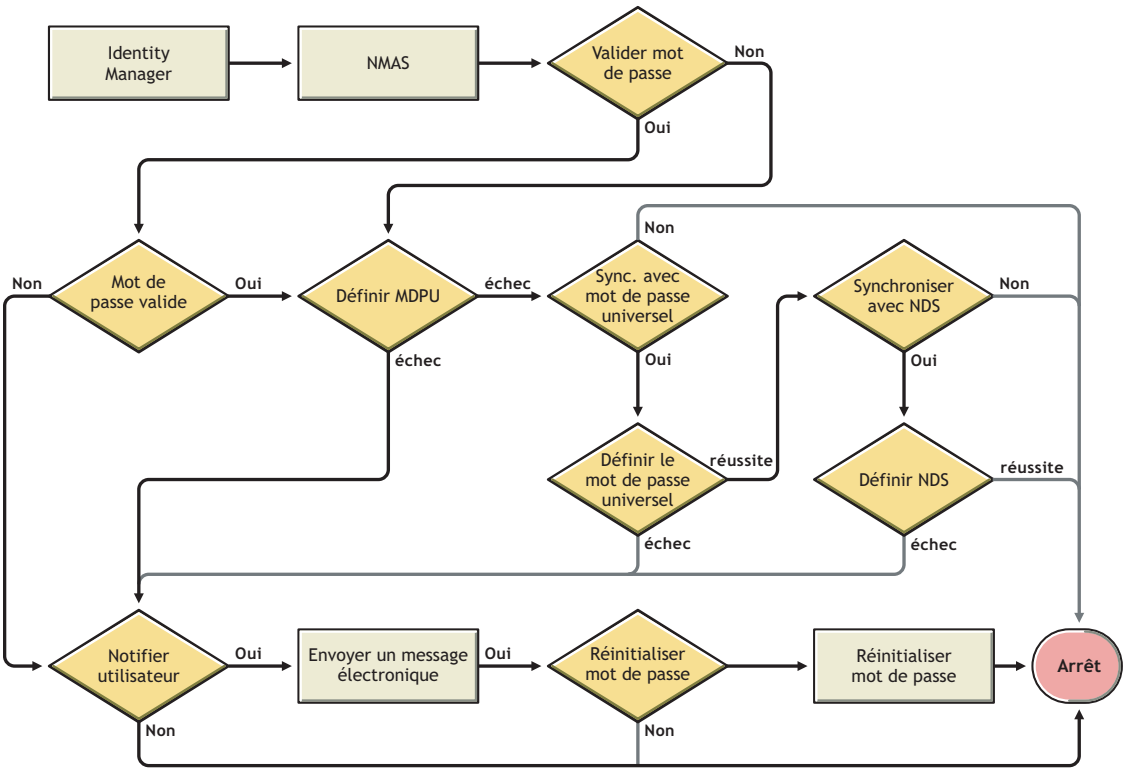
Reportez-vous également aux astuces de la Section 5.13, « Dépannage des problèmes de synchronisation des mots de passe », page 160.

Diagramme du scénario 3

Le diagramme suivant montre comment NMAS gère le mot de passe qu'il reçoit de Identity Manager. Dans ce scénario, le mot de passe est synchronisé sur le mot de passe de distribution et NMAS détermine :

- Comment gérer le mot de passe, selon que vous avez spécifié ou non que les mots de passe entrants doivent être validés par rapport aux stratégies de mots de passe (si le mot de passe universel et les règles de mots de passe avancées sont activés).
- Quels sont les autres paramètres de la stratégie de mot de passe pour la synchronisation du mot de passe universel avec les autres mots de passe.

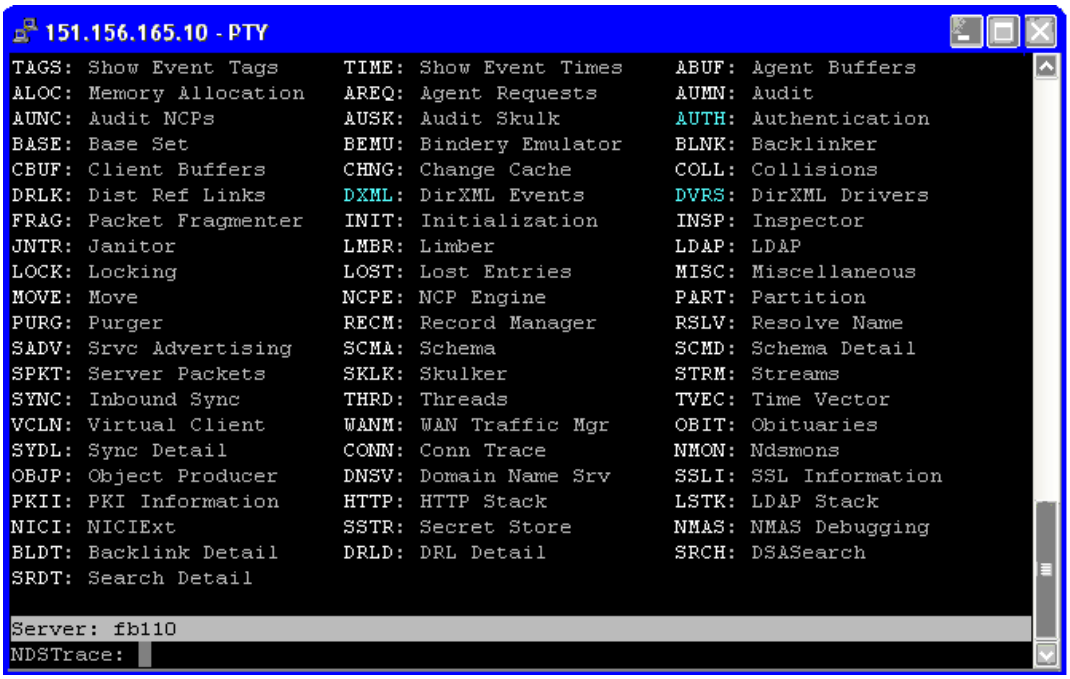
Figure 5-12 *Synchronisation du mot de passe Identity Manager avec le mot de passe de distribution*



Problème de connexion à eDirectory

- Activez les paramètres *+AUTH*, *+DXML* et *+DVRS* dans DSTrace.

Figure 5-13 *Commandes DSTrace*



- Vérifiez que les éléments `<password` ou `<modify-password` sont transférés à Identity Manager. Pour cela, reportez-vous à l'écran DSTtrace ou au fichier contenant les options de trace actives, indiquées dans le premier point.
- Vérifiez que le mot de passe est conforme aux règles de la stratégie de mot de passe NMAS.
- Vérifiez la configuration et l'assignation de la stratégie de mot de passe NMAS. Essayez d'assigner directement la stratégie à l'utilisateur, en vérifiant que vous utilisez la bonne stratégie.
- Sur la page Synchronisation de mot de passe pour le pilote, vérifiez que l'option *Identity Manager accepte les mots de passe (canal Éditeur)* est sélectionnée.
- Dans la stratégie de mot de passe NMAS, vérifiez que l'option *Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel* est sélectionnée.
- Dans la stratégie de mot de passe NMAS, vérifiez que l'option *Synchroniser le mot de passe NDS lors de la définition du mot de passe universel* est sélectionnée, si vous le souhaitez.
- Si les utilisateurs se connectent via le client Novell ou ConsoleOne, vérifiez la version. Les clients Novell et ConsoleOne hérités risquent de ne pas pouvoir se connecter au coffre-fort d'identité si le mot de passe universel n'est pas synchronisé avec le mot de passe NDS.

  Certaines versions du client Novell et de ConsoleOne connaissent le mot de passe universel. Reportez-vous au *NMAS 3.0 Administration Guide (Guide d'administration de NMAS 3.0)* (http://www.novell.com/documentation/nmas30/index.html).
- Certains utilitaires hérités s'authentifient à l'aide du mot de passe NDS mais ne peuvent pas se connecter au coffre-fort d'identité si le mot de passe universel n'est pas synchronisé avec le mot

de passe NDS. Si vous ne souhaitez pas utiliser le mot de passe NDS pour la plupart des utilisateurs, mais si certains administrateurs ou utilisateurs du service d'assistance doivent s'authentifier sur les utilitaires hérités, essayez d'utiliser une autre stratégie de mot de passe pour les utilisateurs du service d'assistance afin de spécifier pour eux des options de synchronisation différentes pour les mots de passe universels.

Problème pour se loguer à un autre système connecté qui s'abonne aux mots de passe

Cette section permet de corriger les situations dans lesquelles ce système connecté publie des mots de passe vers Identity Manager ; par contre, un autre système connecté qui s'abonne aux mots de passe ne semble pas recevoir les modifications de ce système. Cette relation s'appelle aussi un système connecté secondaire, ce qui signifie que le système reçoit des mots de passe du premier système connecté via Identity Manager.

- Activez les paramètres *+DXML* et *+DVRS* dans DSTrace pour voir comment sont traitées les stratégies Identity Manager, ainsi que les erreurs potentielles.
- Définissez le niveau de trace Identity Manager pour le pilote sur *3*.
- Sur la page Synchronisation de mot de passe, vérifiez que l'option *Identity Manager accepte les mots de passe (canal Éditeur)* est sélectionnée.
- Dans la stratégie de mot de passe, vérifiez que l'option *Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel* n'est pas sélectionnée.

  Identity Manager utilise le mot de passe de distribution pour synchroniser les mots de passe sur les systèmes connectés. Le mot de passe universel doit être synchronisé avec le mot de passe de distribution pour cette méthode de synchronisation.
- Vérifiez le filtre du pilote pour l'attribut nspmDistributionPassword.
- Vérifiez que l'élément `<password>` d'un élément Add ou `<modify-password>` a été converti pour les opérations Ajouter et Modifier l'attribut de nspmDistributionPassword. Pour cela, reportez-vous à l'écran DSTrace ou au fichier contenant les options actives, indiquées dans les premiers points.
- Vérifiez que la configuration du pilote inclut les stratégies de mot de passe de script Identity Manager dans le site correct et dans le bon ordre, tel que décrit à la Section 5.3.4, « Stratégies requises pour la configuration du pilote », page 91.
- Comparez la stratégie de mot passe dans le coffre-fort d'identité avec toute stratégie de mot de passe appliquée par le système connecté, pour vérifier leur compatibilité.

Le message électronique n'est pas généré en cas d'échec du mot de passe

- Activez les paramètres *+DXML* dans DSTrace pour savoir comment sont traités les règles Identity Manager.
- Définissez le niveau de trace Identity Manager pour le pilote sur *3*.
- Vérifiez que la règle de génération des messages électroniques est sélectionnée.
- Vérifiez que l'objet Coffre-fort d'identité contient la valeur correcte de l'utilisateur, indiquée dans l'attribut Adresse de messagerie Internet.
- Dans la tâche Configuration de la notification, vérifiez que le serveur SMTP et le modèle de messagerie sont configurés. Reportez-vous à la Section 5.12, « Configuration de la notification par message électronique », page 147.

Les notifications par message électronique n'ont pas une présence insistante. Elles n'ont aucune incidence sur le traitement du document XML qui a déclenché la notification. En cas d'échec, elles

ne font pas l'objet d'une nouvelle tentative, sauf si l'opération elle-même est recommencée. Les messages de débogage pour les notifications par message électronique sont écrits dans le fichier de trace.

Erreur lors de l'utilisation de la vérification de l'état du mot de passe

Avec la tâche iManager Vérifier l'état du mot de passe, le pilote vérifie le mot de passe de l'objet.

- Vérifiez que le système connecté accepte la vérification des mots de passe. Reportez-vous à la Section 5.2, « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 84.

  Cette opération n'est pas disponible via iManager si le manifeste du pilote n'indique pas que le système connecté prend en charge la fonction password-check.
- Si la vérification du mot de passe de l'objet renvoie -603, cela signifie que l'objet de coffre-fort d'identité ne contient pas d'attribut nspmDistributionPassword. Vérifiez le filtre du pilote et l'option *Synchroniser le mot de passe universel et le mot de passe de distribution* dans la stratégie de mot de passe.
- Si la vérification du mot de passe de l'objet renvoie `Non synchronisé`, vérifiez que la configuration du pilote contient les stratégies appropriées de synchronisation des mots de passe pour Identity Manager.
- Comparez la stratégie de mot passe dans le coffre-fort d'identité avec toute stratégie de mot de passe appliquée par le système connecté, pour vérifier leur compatibilité.
- L'option *Vérifier le mot de passe de l'objet* traite le mot de passe de distribution. Si le mot de passe de distribution n'est pas mis à jour, la *vérification du mot de passe de l'objet* risque de ne pas signaler que les mots de passe sont synchronisés.
- Sachez que pour le coffre-fort d'identité, l'option *Vérifier l'état du mot de passe* vérifie le mot de passe NDS et non le mot de passe universel. Cela signifie que si la stratégie de mot de passe de l'utilisateur ne spécifie que le mot de passe NDS doit être synchronisé avec le mot de passe universel, les mots de passe sont toujours signalés comme n'étant pas synchronisés. En fait, le mot de passe de distribution et le mot de passe sur le système connecté pourraient être synchronisés, mais l'option Vérifier l'état des mots de passe ne sera pas exacte, à moins que le mot de passe NDS et le mot de passe de distribution ne soient synchronisés avec le mot de passe universel.

Commandes DSTrace utiles

+DXML : affiche le traitement des règles Identity Manager et les messages d'erreur potentiels.

+DVRS : affiche les messages du pilote Identity Manager.

+AUTH : affiche les modifications des mots de passe NDS.

5.8.5 Scénario 4 : passage en tunnel—synchronisation des systèmes connectés (mais pas du coffre-fort d'identité) avec mise à jour du mot de passe de distribution par Identity Manager

Identity Manager permet de synchroniser les mots de passe entre les systèmes connectés tout en maintenant le mot de passe du coffre-fort d'identité séparé d'eux. On parle de « tunnellisation ».

Dans ce scénario, Identity Manager met directement à jour le mot de passe de distribution. Ce scénario est presque identique au scénario décrit à la Section 5.8.4, « Scénario 3 : synchronisation d'un coffre-fort d'identité et des systèmes connectés avec mise à jour du mot de passe de distribution dans Identity Manager », page 125. Toutefois, ici, vous devez vous assurer que le mot de passe universel et le mot de passe de distribution ne sont pas synchronisés. Pour ce faire, n'utilisez pas les stratégies de mot de passe NMAS, ou utilisez-les mais désactivez l'option *Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel*.

- « Avantages et inconvénients du scénario 4 » page 135
- « Implémentation du scénario 4 » page 136
- « Dépannage du scénario 4 » page 138

Avantages et inconvénients du scénario 4

Tableau 5-14 *Avantages de la tunnellisation*

Avantages	Inconvénients
Permet de synchroniser les mots de passe entre les systèmes connectés, tout en maintenant le mot de passe du coffre-fort d'identité séparé. Les stratégies de mot de passe ne sont pas obligatoires. Si vous utilisez une stratégie de mot de passe, il n'est pas nécessaire que le mot de passe universel y soit activé. Toutefois, l'environnement doit prendre en charge le mot de passe universel. Prend en charge la tâche Vérifier l'état des mots de passe dans iManager, si le système connecté la prend en charge. Vous pouvez demander à ce qu'une notification soit envoyée en cas d'échec de la synchronisation des mots de passe. Vous pouvez réinitialiser un mot de passe du système connecté qui ne se conforme pas à la stratégie de mot de passe. Si le mot de passe universel et les règles de mot de passe avancées sont activés, les stratégies de mot de passe s'appliquent à condition que vous l'ayez spécifié ; les mots de passe des systèmes connectés peuvent être réinitialisés.	Si le mot de passe universel ou les règles de mot de passe avancées ne sont pas activés, les stratégies de mot de passe ne sont pas appliquées et les mots de passe des systèmes connectés ne peuvent pas être réinitialisés.

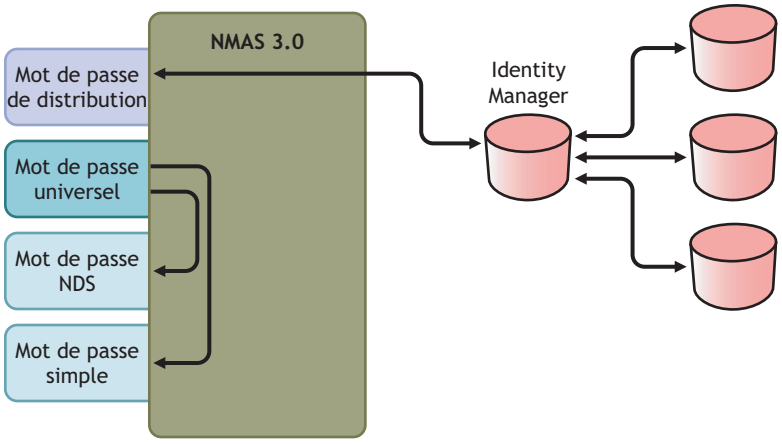
Ce scénario est illustré dans la figure suivante.

1. Les mots de passe arrivent par le biais de Identity Manager.
2. Identity Manager met directement à jour le mot de passe de distribution par le biais de NMAS.
3. Identity Manager utilise également le mot de passe de distribution pour effectuer la répartition vers les systèmes connectés paramétrés pour accepter les mots de passe.

La clé de ce scénario est que, dans la règle de mot de passe NMAS, l'option *Synchroniser le mot de passe universel avec le mot de passe de distribution* est désactivée. Le mot de passe de distribution n'étant pas synchronisé avec le mot de passe universel, Identity Manager synchronise les mots de passe sur les systèmes connectés, sans modifier les mots de passe du coffre-fort d'identité.

Même si, dans ce diagramme, il est indiqué que plusieurs systèmes connectés se connectent à Identity Manager, n'oubliez pas que vous créez chaque paramètre individuellement pour chaque pilote du système connecté.

Figure 5-14 *Tunnellisation, avec mise à jour du mot de passe de distribution par Identity Manager*



Implémentation du scénario 4

Pour implémenter ce type de synchronisation des mots de passe, configurez les éléments suivants :

- « Déploiement du mot de passe universel » page 136
- « Configuration de la stratégie de mot de passe » page 136
- « Paramètres de la synchronisation des mots de passe » page 137
- « Configuration de pilote » page 137

Déploiement du mot de passe universel

Même s'il n'est pas obligatoire que le mot de passe universel soit activé dans les stratégies de mot de passe, votre environnement doit malgré tout utiliser eDirectory 8.7.3, qui prend en charge ce mot de passe. Reportez-vous à la Section 5.4, « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 96.

Configuration de la stratégie de mot de passe

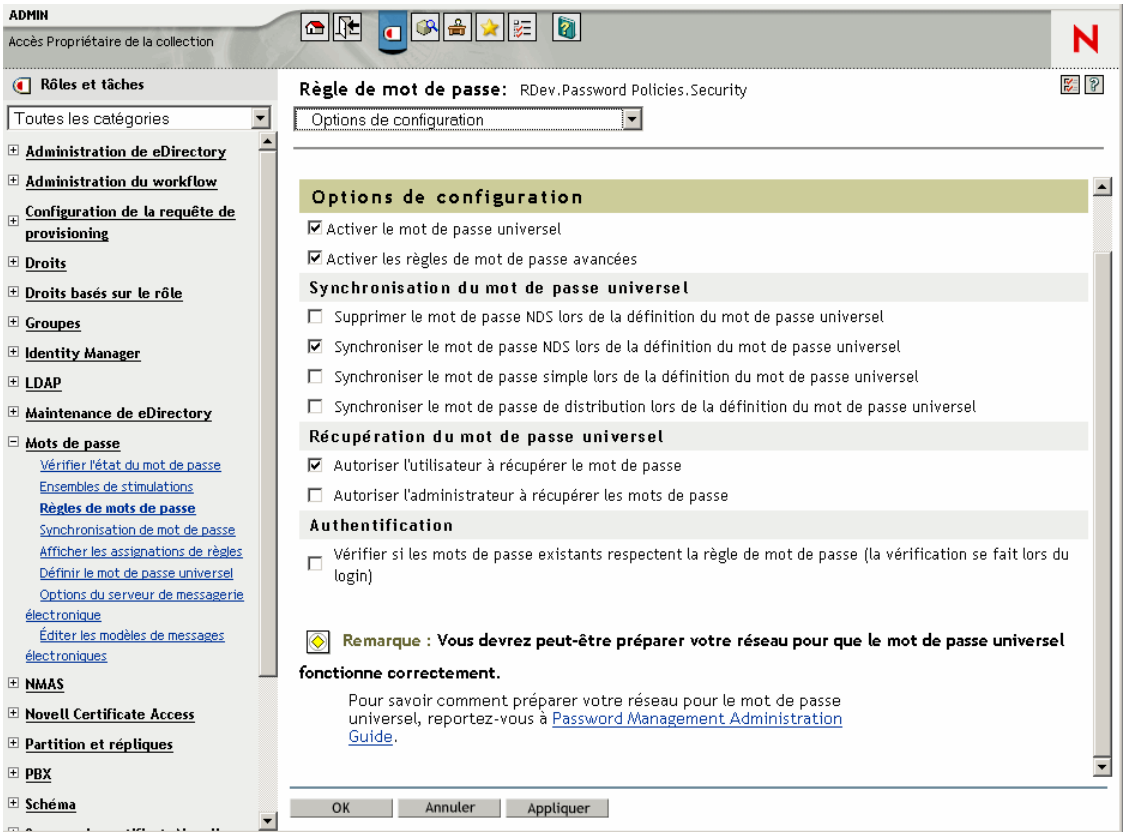
Aucune stratégie de mot de passe n'est obligatoire pour les utilisateurs du coffre-fort d'identité qui font appel à cette méthode.

Toutefois, si vous utilisez une stratégie de mot de passe :

1. Vérifiez que les éléments suivants ne sont pas sélectionnés :
   - *Supprimer le mot de passe NDS lors de la définition du mot de passe universel*

     Cela est essentiel pour tunnelliser les mots de passe sans que le mot de passe du coffre-fort d'identité ne soit affecté. En refusant la synchronisation du mot de passe universel avec le

mot de passe de distribution, vous maintenez le mot de passe de distribution séparé, pour que Identity Manager ne l'utilise que sur les systèmes connectés. Identity Manager agit à la manière d'une conduite : il distribue les mots de passe de et vers les systèmes connectés, sans affecter le mot de passe du coffre-fort d'identité.



2 Définissez les autres paramètres de la stratégie de mot de passe comme vous le souhaitez.

Les autres paramètres de la stratégie de mot de passe sont facultatifs.

Paramètres de la synchronisation des mots de passe

Utilisez les mêmes paramètres que dans Paramètres de la synchronisation des mots de passe à la Section 5.8.4, « Scénario 3 : synchronisation d'un coffre-fort d'identité et des systèmes connectés avec mise à jour du mot de passe de distribution dans Identity Manager », page 125.

Configuration de pilote

Utilisez les mêmes paramètres que dans Configuration de pilote à la Section 5.8.4, « Scénario 3 : synchronisation d'un coffre-fort d'identité et des systèmes connectés avec mise à jour du mot de passe de distribution dans Identity Manager », page 125.

Dépannage du scénario 4

Si la tunnellisation est paramétrée pour la synchronisation des mots de passe, le mot de passe de distribution diffère du mot de passe universel et du mot de passe NDS.

- « Problème pour se loguer à un autre système connecté qui s'abonne aux mots de passe » page 138
- « Les messages électroniques ne sont pas générés en cas d'échec du mot de passe » page 138
- « Erreur lors de l'utilisation de la vérification de l'état du mot de passe » page 139
- « Commandes DSTrace utiles » page 139

Reportez-vous également aux astuces de la Section 5.13, « Dépannage des problèmes de synchronisation des mots de passe », page 160.

Problème pour se loguer à un autre système connecté qui s'abonne aux mots de passe

Cette section permet de corriger les situations dans lesquelles ce système connecté publie des mots de passe vers Identity Manager ; par contre, un autre système connecté qui s'abonne aux mots de passe ne semble pas recevoir les modifications de ce système. Cette relation s'appelle aussi un système connecté secondaire, ce qui signifie que le système reçoit des mots de passe du premier système connecté via Identity Manager.

- Activez les paramètres *+DXML* et *+DVRS* dans DSTrace pour voir comment sont traitées les stratégies Identity Manager, ainsi que les erreurs potentielles.
- Définissez le niveau de trace Identity Manager pour le pilote sur *3*.
- Sur la page Synchronisation de mot de passe, vérifiez que l'option *Identity Manager accepte les mots de passe (canal Éditeur)* est sélectionnée.
- Dans la stratégie de mot de passe, vérifiez que l'option *Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel* n'est pas sélectionnée.

  Identity Manager utilise le mot de passe de distribution pour synchroniser les mots de passe sur les systèmes connectés. Le mot de passe universel doit être synchronisé avec le mot de passe de distribution pour cette méthode de synchronisation.
- Vérifiez que le filtre du pilote possède les paramètres corrects pour l'attribut nspmDistributionPassword.
- Vérifiez que l'élément `<password>` d'un élément Add et `<modify-password>` a été converti pour les opérations Ajouter et Modifier l'attribut de nspmDistributionPassword. Pour cela, reportez-vous à l'écran DSTrace ou au fichier contenant les options de trace actives, indiquées dans les premiers points.
- Vérifiez que la configuration du pilote inclut les stratégies de mot de passe de script Identity Manager dans le site correct et dans le bon ordre, tel que décrit à la Section 5.3.4, « Stratégies requises pour la configuration du pilote », page 91.
- Comparez la stratégie de mot passe dans le coffre-fort d'identité avec toute stratégie de mot de passe appliquée par le système connecté, pour vérifier leur compatibilité.

Les messages électroniques ne sont pas générés en cas d'échec du mot de passe

- Activez les paramètres *+DXML* dans DSTrace pour savoir comment sont traitées les règles Identity Manager.
- Définissez le niveau de trace Identity Manager pour le pilote sur *3*.

- Vérifiez que la règle de génération des messages électroniques est sélectionnée.
- Vérifiez que l'objet Coffre-fort d'identité contient la valeur correcte de l'utilisateur, indiquée dans l'attribut Adresse de messagerie Internet.
- Dans la tâche Configuration de la notification, vérifiez le serveur SMTP et le modèle de message. Reportez-vous à la Section 5.12, « Configuration de la notification par message électronique », page 147.

Les notifications par message électronique n'ont pas une présence insistante. Elles n'ont aucune incidence sur le traitement du document XML qui a déclenché la notification. En cas d'échec, elles ne font pas l'objet d'une nouvelle tentative, sauf si l'opération elle-même est recommencée. Les messages de débogage pour les notifications par message électronique sont écrits dans le fichier de trace.

Erreur lors de l'utilisation de la vérification de l'état du mot de passe

La tâche Vérifier l'état des mots de passe dans iManager amène le pilote à procéder à une vérification du mot de passe de l'objet.

- Vérifiez que le système connecté accepte la vérification des mots de passe. Reportez-vous à la Section 5.2, « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 84.

  Cette opération n'est pas disponible via iManager si le manifeste du pilote n'indique pas que le système connecté prend en charge la capacité password-check.
- Si la vérification du mot de passe de l'objet renvoie -603, cela signifie que l'objet de coffre-fort d'identité ne contient pas d'attribut nspmDistributionPassword. Vérifiez le filtre de l'attribut Identity Manager et l'option *Synchroniser le mot de passe universel et le mot de passe de distribution* dans la stratégie de mot de passe.
- Si la vérification du mot de passe de l'objet renvoie `Non synchronisé`, vérifiez que la configuration du pilote contient les stratégies appropriées de synchronisation des mots de passe pour Identity Manager.
- Comparez la stratégie de mot passe dans le coffre-fort d'identité avec toute stratégie de mot de passe appliquée par le système connecté, pour vérifier leur compatibilité.
- La vérification du mot de passe de l'objet traite le mot de passe de distribution. Si le mot de passe de distribution n'est pas mis à jour, la vérification du mot de passe de l'objet pourrait ne pas signaler que les mots de passe sont synchronisés.

Commandes DSTrace utiles

+DXML : pour afficher le traitement des règles Identity Manager et les messages d'erreur potentiels.

+DVRS : affiche les messages du pilote Identity Manager.

+AUTH : affiche les modifications des mots de passe NDS.

+DCLN : affiche les messages NDS Dclient.

5.8.6 Scénario 5 : synchronisation des mots de passe de l'application avec le mot de passe simple

Ce scénario utilise de façon spécifique les fonctions de synchronisation de mot de passe. Grâce à Identity Manager et NMAS, vous pouvez prendre un mot de passe d'un système connecté et le synchroniser directement avec le mot de passe simple du coffre-fort d'identité. Si le système connecté ne fournit que des mots de passe hachés, vous pouvez les synchroniser sur le mot de passe simple, sans inverser le hachage. D'autres applications peuvent alors s'authentifier sur le coffre-fort d'identité à l'aide du mot de passe en texte clair ou haché via LDAP ou le client Novell, les composants NMAS étant configurés pour utiliser le mot de passe simple comme méthode de connexion.

Si le mot de passe est en texte clair dans le système connecté, il peut être publié tel quel depuis le système connecté dans la zone de mot de passe simple du coffre-fort d'identité.

Si le système connecté ne fournit que des mots de passe hachés (les codages MD5, SHA, SHA1 et UNIX Crypt sont pris en charge), vous devez les publier vers le mot de passe simple avec une indication du type de hachage, par exemple {MD5}.

Pour qu'une autre application s'authentifie avec le même mot de passe, vous devez la personnaliser pour qu'elle prenne le mot de passe de l'utilisateur et l'authentifie sur le mot de passe simple avec LDAP.

NMAS compare la valeur du mot de passe de l'application avec la valeur contenue dans le mot de passe simple. Si le mot de passe stocké dans le mot de passe simple est une valeur de hachage, NMAS utilise d'abord la valeur de mot de passe de l'application pour créer le bon type de valeur de hachage, avant d'effectuer la comparaison. Si le mot de passe de l'application et le mot de passe simple sont identiques, NMAS authentifie l'utilisateur.

Dans ce scénario, il n'est pas possible d'utiliser le mot de passe universel.

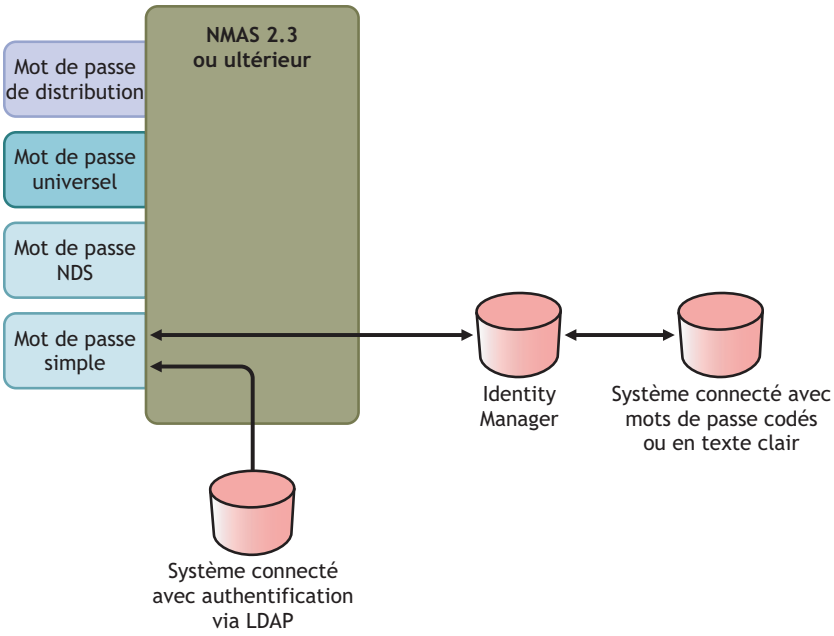
- « Avantages de la synchronisation avec le mot de passe NDS » page 140
- « Implémentation du scénario 5 » page 141

Avantages de la synchronisation avec le mot de passe NDS

Tableau 5-15 *Avantages de la synchronisation avec le mot de passe NDS*

Avantages	Inconvénients
• Permet de mettre directement à jour le mot de passe simple. • Permet de synchroniser un mot de passe haché et de l'utiliser pour s'authentifier sur plusieurs applications, sans inverser le hachage.	• Ce scénario n'autorise pas l'utilisation du mot de passe universel. • Les fonctionnalités en libre-service Mot de passe oublié et Mot de passe peuvent toujours être utilisées. Elles sont en effet prises en charge pour le mot de passe NDS, mais elles ne fonctionnent pas pour le mot de passe simple. • Comme la tâche Définir le mot de passe universel dépend du mot de passe universel, l'administrateur ne peut pas l'utiliser pour définir le mot de passe d'un utilisateur dans le coffre-fort d'identité.

Figure 5-15 *Synchronisation avec le mot de passe NDS*



Implémentation du scénario 5

- « Configuration de la stratégie de mot de passe » page 141
- « Paramètres de la synchronisation des mots de passe » page 141
- « Configuration de pilote » page 142

Configuration de la stratégie de mot de passe

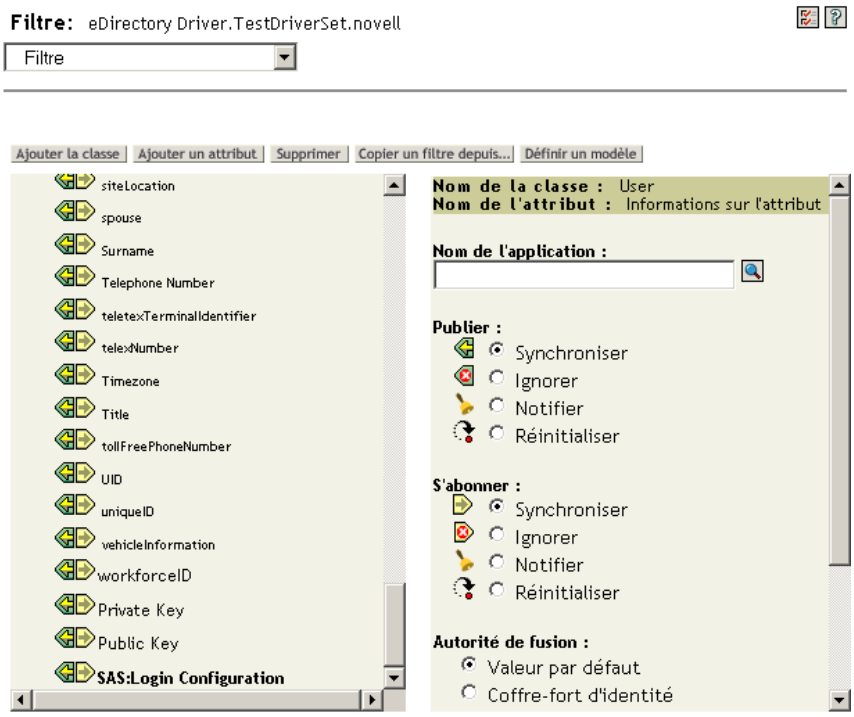
Aucune stratégie de mot de passe n'est obligatoire pour les utilisateurs qui font appel à ce scénario. Il n'est pas possible d'utiliser le mot de passe universel.

Paramètres de la synchronisation des mots de passe

Dans ce scénario, utilisez le script Identity Manager pour modifier directement l'attribut SAS:Login Configuration. Cela signifie que les valeurs de configuration globale de la synchronisation des mots de passe, définies sur la page Synchronisation de mot de passe dans iManager, n'ont aucun effet.

Configuration de pilote

1 Vérifiez que le paramètre *Synchroniser* est défini dans l'attribut SAS:Login Configuration du filtre, pour les canaux Abonné et Éditeur.



2 Configurez les stratégies du pilote, de manière à publier le mot de passe à partir du système connecté.

3 Pour les mots de passe hachés, configurez les stratégies du pilote, de manière à ajouter, en préfixe, le type du hachage, s'il n'est pas déjà fourni par l'application :

- {MD5}*hashed_password*

  Ce mot de passe est codé en Base64.

- {SHA}*hashed_password*

  Ce mot de passe est codé en Base64.

- {CRYPT}*hashed_password*

Les mots de passe en texte clair et les hachages de mots de passe de codage Unix ne sont pas codés en Base64.

4 Pour placer le mot de passe dans le mot de passe simple, configurez les stratégies du pilote pour modifier l'attribut SAS:Login Configuration.

L'exemple suivant montre comment utiliser un élément modify-attr dans une opération de modification pour changer le mot de passe simple en mot de passe haché MD5 :

```
<modify-attr attr-name="SAS:Login Configuration>
    <add-value>
        <value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value>
```

```
    </add-value>
</modify-attr>
```

Pour les mots de passe en texte clair, suivez cet exemple.

```
<modify-attr attr-name="SAS:Login Configuration>
    <add-value>
        <value>clearpwd</value>
    </add-value>
</modify-attr>
```

Pour les opérations d'ajout, l'élément add-attr contiendrait l'un de ceux-ci :

```
<add-attr attr-name="SAS:Login Configuration>
    <value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value>
</add-attr>
```

ou

```
<add-attr attr-name="SAS:Login Configuration>
    <value>clearpwd</value>
</add-attr>
```

5.9 Définition des filtres de mots de passe

Certains systèmes connectés peuvent proposer le mot de passe de l'utilisateur à Identity Manager.

Pour capturer les mots de passe sous Active Directory, NIS et NT Domain, vous devez effectuer une légère configuration pour installer les filtres de mot de passe sur les systèmes connectés.

- Section 5.9.1, « Définition des filtres de synchronisation de mots de passe pour Active Directory et NT Domain », page 143
- Section 5.9.2, « Définition des filtres de synchronisation des mots de passe pour NIS », page 144

5.9.1 Définition des filtres de synchronisation de mots de passe pour Active Directory et NT Domain

Pour plus d'informations, reportez-vous aux sections Password Synchronization (Synchronisation de mot de passe) des guides d'implémentation des pilotes Identity Manager pour Active Directory et NT Domain, disponibles à la page Identity Manager Drivers (Pilotes Identity Manager) (http://www.novell.com/documentation/dirxmldrivers/index.html).

Le pilote Identity Manager pour AD ou NT Domain doit être installé sur un seul ordinateur Windows. Il n'est pas nécessaire que le pilote soit installé pour les autres contrôleurs de domaine, mais chaque contrôleur a besoin d'un fichier `pwfilter.dl` pour capturer les mots de passe et les envoyer à Identity Manager.

Un utilitaire vous est fourni pour simplifier la configuration et l'administration. Il permet de réaliser ces opérations pour tous les contrôleurs de domaine de la machine Windows sur laquelle le pilote est installé.

5.9.2 Définition des filtres de synchronisation des mots de passe pour NIS

Le pilote Identity Manager pour NIS 3.0 peut fonctionner avec trois zones de stockage d'authentification UNIX : fichiers, NIS et NIS+. Le module PAM fourni permet de capturer les mots de passe et de les envoyer au pilote Identity Manager pour NIS.

Le déploiement du module PAM pour le pilote NIS est décrit dans le manuel *Identity Manager Driver for NIS Implementation Guide (Guide d'implémentation du pilote Identity Manager pour NIS)*, disponible à la page Identity Manager Drivers (Pilotes Identity Manager) (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

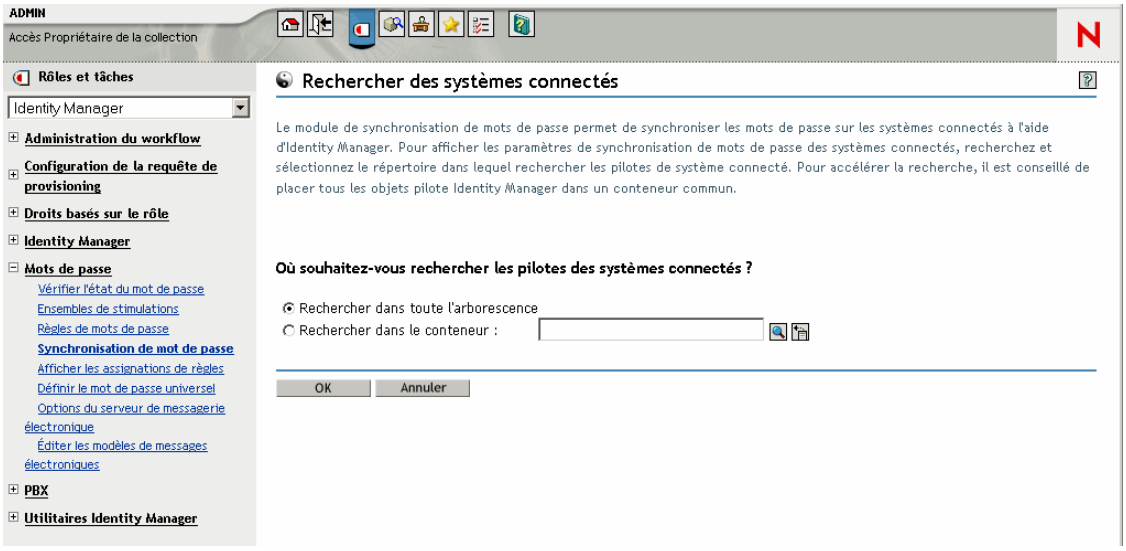
5.10 Gestion de la synchronisation des mots de passe

- « Définition du flux des mots de passe sur les différents systèmes » page 144
- « Application des stratégies de mot de passe sur les systèmes connectés » page 146
- « Séparation du mot de passe eDirectory et du mot de passe synchronisé » page 146

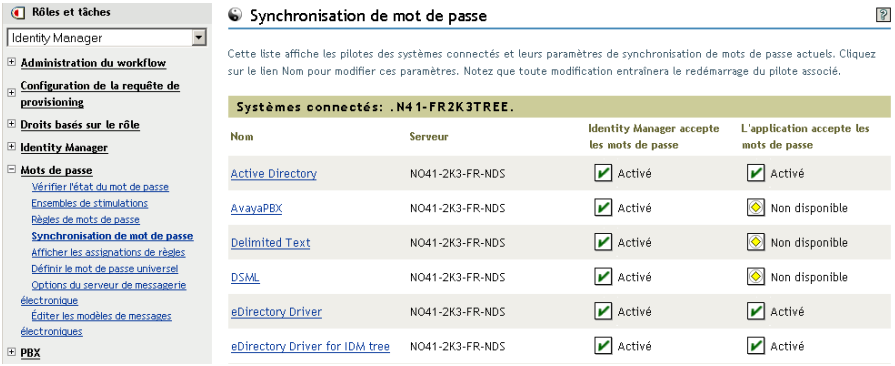
5.10.1 Définition du flux des mots de passe sur les différents systèmes

Pour voir comment vos systèmes sont configurés pour accepter ou publier des mots de passe :

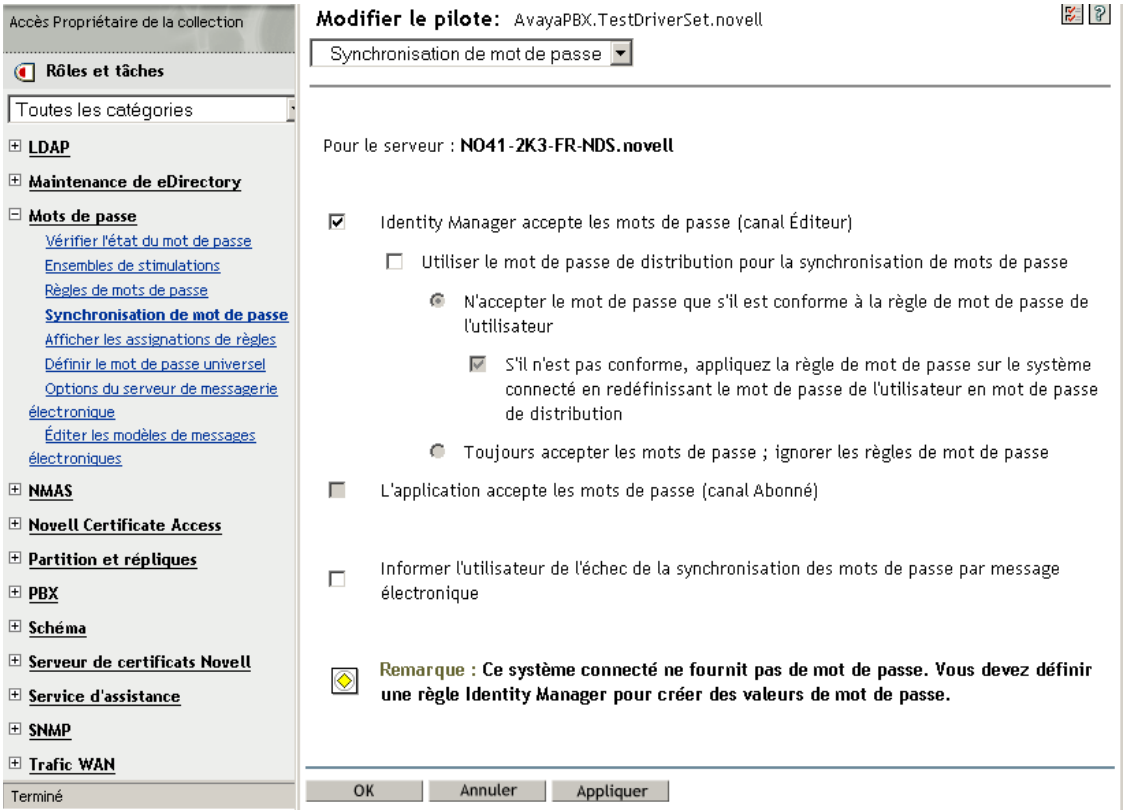
1. Dans iManager, sélectionnez *Mots de passe* > *Synchronisation de mot de passe*.
2. Recherchez les pilotes correspondant aux systèmes connectés.



Les résultats de la recherche montrent les paramètres du flux de mots de passe de et vers Identity Manager et les systèmes connectés.



Pour modifier ces paramètres, cliquez sur le nom du pilote d'un système connecté.



Sur la page Modifier le pilote, vous pouvez décider si la stratégie de mot de passe doit être appliquée aux mots de passe entrant dans Identity Manager et si elle doit être appliquée sur le système connecté en réinitialisant le mot de passe de ce système.

Les paramètres de cette page sont des valeurs de configuration globale (GCV), stockées pour chaque serveur. Reportez-vous à la Section 5.3.3, « Contrôle de la synchronisation des mots de passe à l'aide des valeurs de configuration globale », page 88.

5.10.2 Application des stratégies de mot de passe sur les systèmes connectés

Si vous utilisez les règles de mot de passe avancées et la fonction de synchronisation des mots de passe Identity Manager, il est conseillé d'entreprendre les actions suivantes :

1. Recherchez les stratégies de mot de passe de tous les systèmes connectés.
2. Vérifiez que les règles de mot de passe avancées sont compatibles avec les stratégies de mot de passe des systèmes connectés.

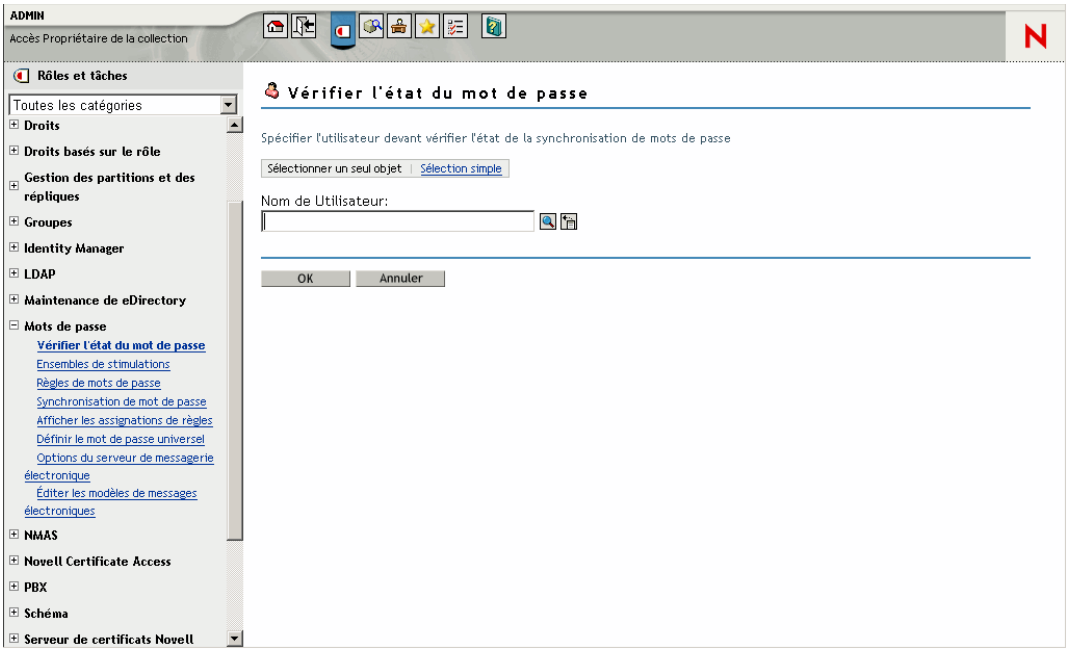
5.10.3 Séparation du mot de passe eDirectory et du mot de passe synchronisé

Ce scénario est décrit à la Section 5.8.5, « Scénario 4 : passage en tunnel—synchronisation des systèmes connectés (mais pas du coffre-fort d'identité) avec mise à jour du mot de passe de distribution par Identity Manager », page 134.

5.11 Vérification de l'état de synchronisation du mot de passe pour un utilisateur

Vous pouvez déterminer si le mot de passe de distribution d'un utilisateur donné est identique à celui du système connecté.

1. Dans iManager, sélectionnez *Mots de passe* > *Vérifier l'état du mot de passe*.



2. Localisez l'utilisateur et sélectionnez-le.

La tâche *Vérifier l'état du mot de passe* amène le pilote à procéder à une vérification du mot de passe de l'objet.

Tous les pilotes ne prennent pas en charge la vérification du mot de passe. Pour ceux qui le font, cette fonctionnalité doit apparaître dans le manifeste. iManager n'autorise pas l'envoi d'opérations de vérification de mot de passe aux pilotes dont le manifeste ne fait pas mention de cette fonctionnalité.

La vérification du mot de passe de l'objet traite le mot de passe de distribution. Si le mot de passe de distribution n'est pas mis à jour, la vérification du mot de passe de l'objet pourrait signaler que les mots de passe ne sont pas synchronisés.

Le mot de passe de distribution n'est pas mis à jour dans les cas suivants :

- Vous utilisez la méthode de synchronisation décrite à la Section 5.8.2, « Scénario 1 : utilisation du mot de passe NDS pour la synchronisation entre deux coffres-forts d'identité », page 112.
- Vous synchronisez le mot de passe universel, comme décrit à la Section 5.8.3, « Scénario 2 : synchronisation avec le mot de passe universel », page 115, mais vous n'avez pas activé l'option de configuration de la stratégie de mot de passe permettant de synchroniser le mot de passe universel avec le mot de passe de distribution.

Remarque : sachez que pour le coffre-fort d'identité, l'option Vérifier l'état du mot de passe vérifie le mot de passe NDS et non le mot de passe universel. Autrement dit, si la stratégie de mot de passe de l'utilisateur ne spécifie pas que le mot de passe NDS doit être synchronisé avec le mot de passe universel, les mots de passe sont toujours signalés comme n'étant pas synchronisés. En fait, le mot de passe de distribution et le mot de passe sur le système connecté pourraient être synchronisés, mais l'option Vérifier l'état des mots de passe ne sera pas exacte, à moins que le mot de passe NDS et le mot de passe de distribution ne soient synchronisés avec le mot de passe universel.

5.12 Configuration de la notification par message électronique

Les tâches iManager permettent de spécifier le serveur de messagerie et de personnaliser les modèles pour les notifications par message électronique.

Des modèles de messages sont prévus pour permettre à la synchronisation des mots de passé et au libre-service des mots de passe d'envoyer automatiquement des messages électroniques aux utilisateurs.

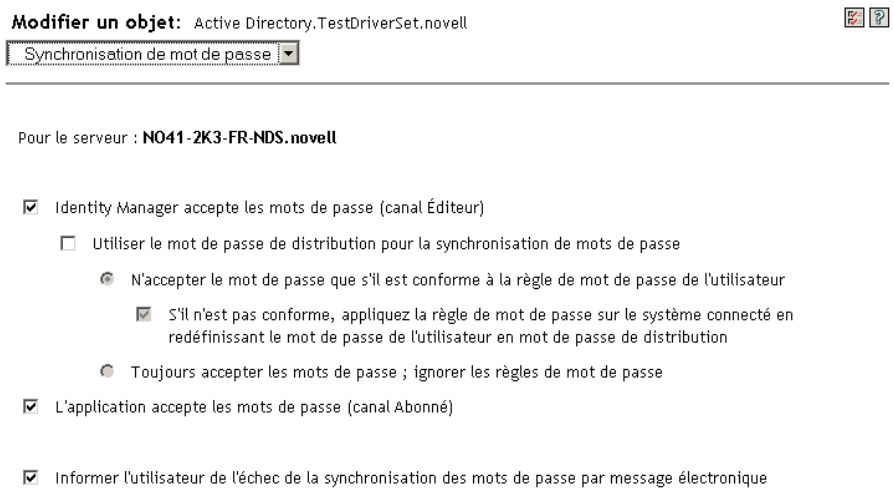
Vous ne créez pas de modèles. Ces modèles sont fournis par l'application qui doit les utiliser. Les modèles de message électronique sont des objets Modèle dans le coffre-fort d'identité. Ils sont placés dans le conteneur Sécurité, qui se trouve généralement à la racine de votre arborescence. Même s'il s'agit d'objets du coffre-fort d'identité, vous ne devez les modifier que dans iManager.

Ce cadre est modulaire. À mesure que vous ajoutez de nouvelles applications qui utilisent les modèles de messages électroniques, les modèles peuvent être installés en même temps que les applications qui les utilisent.

Vous contrôlez l'envoi de messages, en fonction des choix que vous avez faits dans iManager. En ce qui concerne les oublis de mots de passe, les notifications ne sont envoyées que si vous choisissez d'utiliser l'une des opérations Mot de passe oublié amenant à l'envoi d'un message électronique : envoi à l'utilisateur d'un mot de passe ou d'un indice par courrier électronique. Reportez-vous à la section « Providing Users with Forgotten Password Self-Service (Libre-service Mot de passe oublié pour les utilisateurs) » du *Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe)* (http://www.novell.com/documentation/password_management/index.html).

Lorsque vous sélectionnez l'option *Informer l'utilisateur de l'échec de la synchronisation des mots de passe par message électronique*, la synchronisation des mots de passe est configurée de telle sorte qu'un message électronique soit envoyé uniquement en cas d'échec de la synchronisation, et uniquement pour les pilotes spécifiés.

Figure 5-16 *Configuration de la synchronisation des mots de passe*



Vous devez également vérifier que les informations d'authentification SMTP figurent dans les stratégies de pilotes.

- Section 5.12.1, « Conditions préalables », page 148
- Section 5.12.2, « Configuration du serveur SMTP pour envoyer la notification par message électronique », page 149
- « Configuration des modèles de message électronique destinés à la notification » page 150
- Section 5.12.4, « Indication des informations d'authentification SMTP dans les stratégies de pilote », page 151
- Section 5.12.5, « Ajout de vos balises de remplacement aux modèles de notification par message électronique », page 153
- Section 5.12.6, « Envoi de notifications par message électronique à l'administrateur », page 159
- Section 5.12.7, « Localisation des modèles de notification par l'adresse de messagerie électronique », page 160

5.12.1 Conditions préalables

- ❑ Vérifiez que les utilisateurs du coffre-fort d'identité ont rempli l'attribut Adresse de messagerie Internet.
- ❑ Si vous utilisez les notifications par message électronique pour la synchronisation des mots de passe, vérifiez que les stratégies de pilote définies à cet effet contiennent le mot de passe pour le serveur SMTP. Reportez-vous à la Section 5.12.4, « Indication des informations d'authentification SMTP dans les stratégies de pilote », page 151.
- ❑ Si vous craignez que certains utilisateurs n'indiquent pas l'adresse de messagerie électronique ou si vous souhaitez enregistrer toutes les notifications d'échec, vous pouvez choisir un compte

d'administrateur de mot de passe auquel seront envoyées toutes les notifications, en plus d'être envoyées à l'utilisateur.

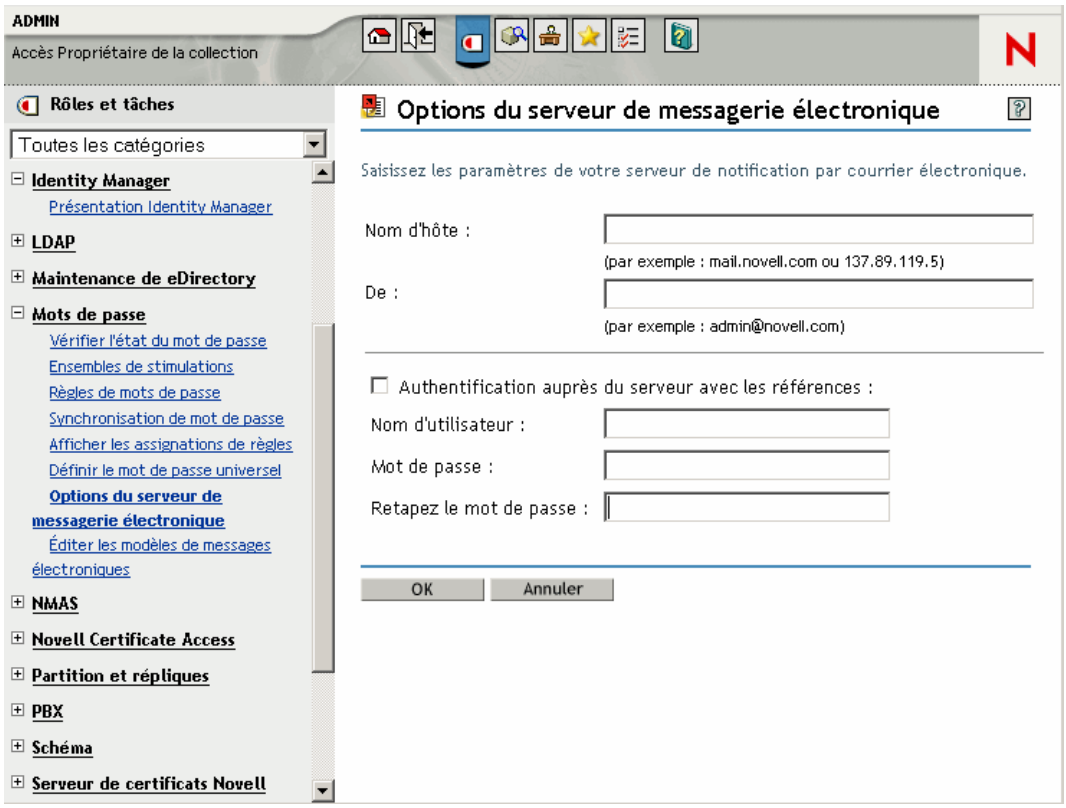
Cette adresse doit se trouver dans le champ *À* de la stratégie de script Identity Manager. Pour plus d'informations, reportez-vous à la Section 5.12.6, « Envoi de notifications par message électronique à l'administrateur », page 159.

- Si eDirectory et Identity Manager se trouvent sur un serveur UNIX, celui-ci doit contenir une réplique des objets de modèle de message électronique.

  Ces objets sont situés dans le conteneur Sécurité, à la racine. Le serveur a donc besoin d'une réplique de la partition racine.

5.12.2 Configuration du serveur SMTP pour envoyer la notification par message électronique

1 Dans iManager, sélectionnez *Mots de passe* > *Options du serveur de messagerie électronique*.



2 Saisissez les informations suivantes :

- le nom de l'hôte,
- le nom (par exemple, Administrateur) qui doit apparaître dans le champ De du message électronique,
- le nom d'utilisateur et le mot de passe permettant de s'authentifier sur le serveur, le cas échéant.

3 Cliquez sur *OK*.

4 Si vous utilisez la synchronisation des mots de passe avec vos pilotes Identity Manager et si vous souhaitez utiliser la fonction de notification par message électronique, vous devez également :

4a Vérifier que les stratégies de pilote contiennent le mot de passe si votre serveur SMTP exige une authentification avant l'envoi du message électronique. Reportez-vous à la Section 5.12.4, « Indication des informations d'authentification SMTP dans les stratégies de pilote », page 151 pour plus d'informations.

Pour les notifications de mot de passe oublié, la spécification des informations d'authentification indiquées à l'Étape 2 dans la page Options du serveur de messagerie électronique suffit, mais pas pour les notifications de synchronisation des mots de passe.

4b Redémarrez les pilotes Identity Manager qui doivent être mis à jour avec les modifications.

Le pilote lit les modèles et les informations du serveur SMTP au démarrage uniquement.

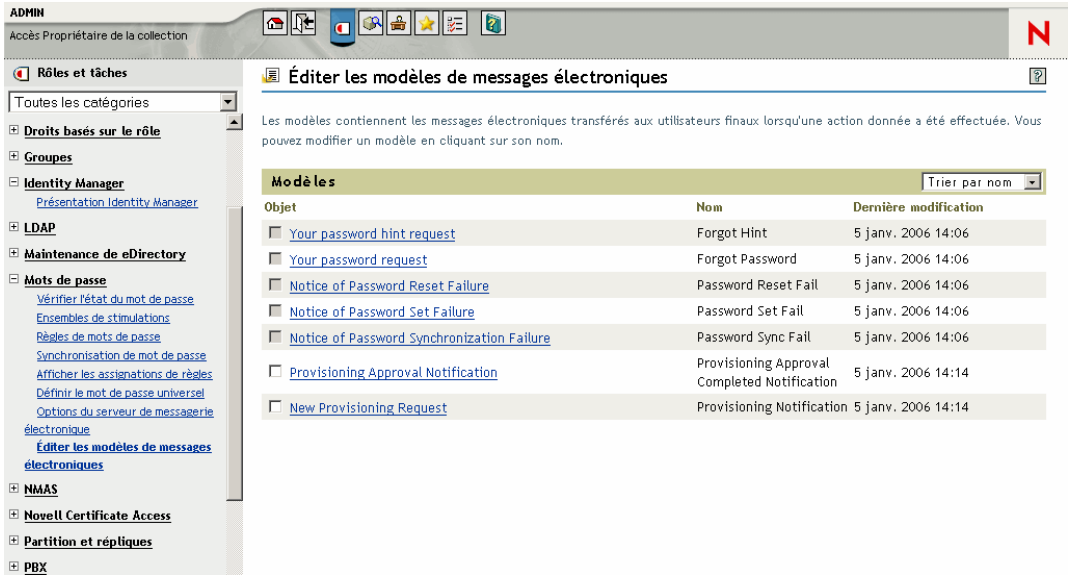
5 Personnalisez les modèles de message électronique comme décrit à « Configuration des modèles de message électronique destinés à la notification » page 150.

Une fois le serveur de messagerie configuré, les messages électroniques peuvent être envoyés par les applications qui les utilisent, si vous faites appel aux fonctionnalités qui entraînent l'envoi des messages.

5.12.3 Configuration des modèles de message électronique destinés à la notification

Vous pouvez personnaliser ces modèles avec le texte de votre choix. Le nom du modèle traduit son utilisation.

1 Dans iManager, sélectionnez *Mots de passe* > *Éditer les modèles de messages électroniques*.



2 Modifiez les modèles comme vous le souhaitez.

N'oubliez pas que, si vous souhaitez ajouter des balises de remplacement, vous aurez peut-être besoin de tâches complémentaires. Suivez les instructions de la Section 5.12.5, « Ajout de vos balises de remplacement aux modèles de notification par message électronique », page 153.

3 Redémarrez les pilotes Identity Manager qui doivent être mis à jour avec les modifications.

Le pilote lit les modèles et les informations du serveur SMTP au démarrage uniquement.

5.12.4 Indication des informations d'authentification SMTP dans les stratégies de pilote

Indiquez le nom d'utilisateur et le mot de passe pour le serveur SMTP à la Section 5.12.2, « Configuration du serveur SMTP pour envoyer la notification par message électronique », page 149. Cela suffit pour les notifications d'oubli de mot de passe.

Par contre, pour les notifications de synchronisation des mots de passe, vous devez également indiquer le mot de passe dans les stratégies de pilote. Le moteur méta-annuaire peut accéder au nom d'utilisateur mais pas au mot de passe, qui doit être fourni par la stratégie de pilote.

Vous devez terminer cette procédure dans les cas suivants :

- Le serveur SMTP est sécurisé et exige une authentification avant d'envoyer le message électronique.
- Vous utilisez la synchronisation des mots de passe Identity Manager avec un pilote Identity Manager.
- Dans les paramètres de synchronisation des mots de passe, vous avez choisi *Informer l'utilisateur de l'échec de la synchronisation des mots de passe par message électronique*.

Pour ajouter le mot de passe du serveur SMTP à la stratégie du pilote :

1 Vérifiez que le pilote possède les stratégies nécessaires à la synchronisation des mots de passe.

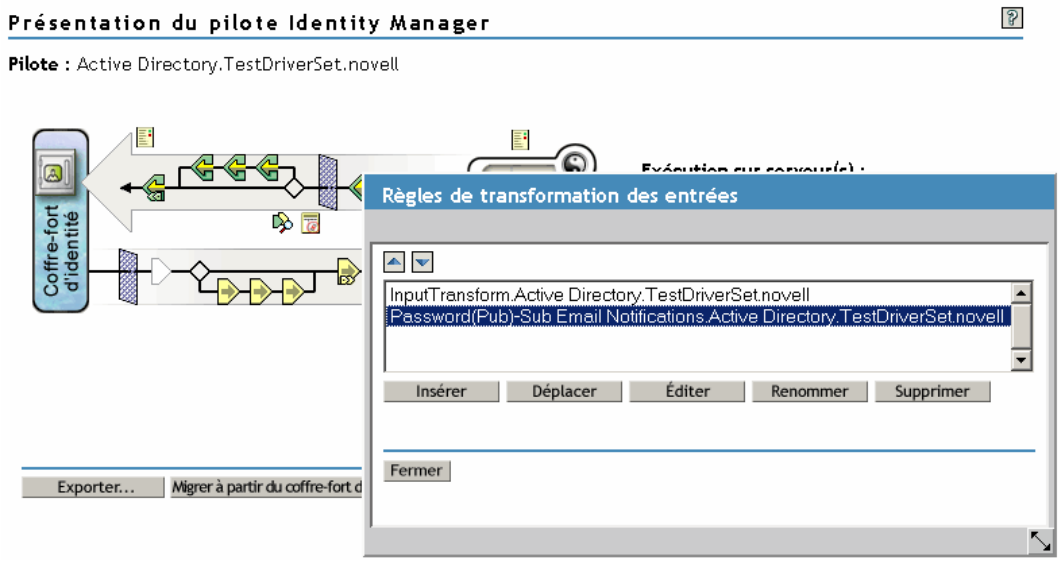
Ces stratégies sont fournies dans les exemples de configuration du pilote ou peuvent être ajoutées, comme indiqué à la Section 5.7, « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe », page 101.

2 Dans iManager, sélectionnez *Identity Manager > Présentation de Identity Manager*.

3 Recherchez les ensembles de pilotes ou recherchez et sélectionnez un conteneur qui contient l'ensemble de pilotes.

4 Dans Présentation du pilote Identity Manager, cliquez sur l'icône du pilote.

5 Sélectionnez l'icône Transformation de l'entrée ou Transformation de la sortie.



6 Sélectionnez une stratégie, puis cliquez sur *Éditer*.

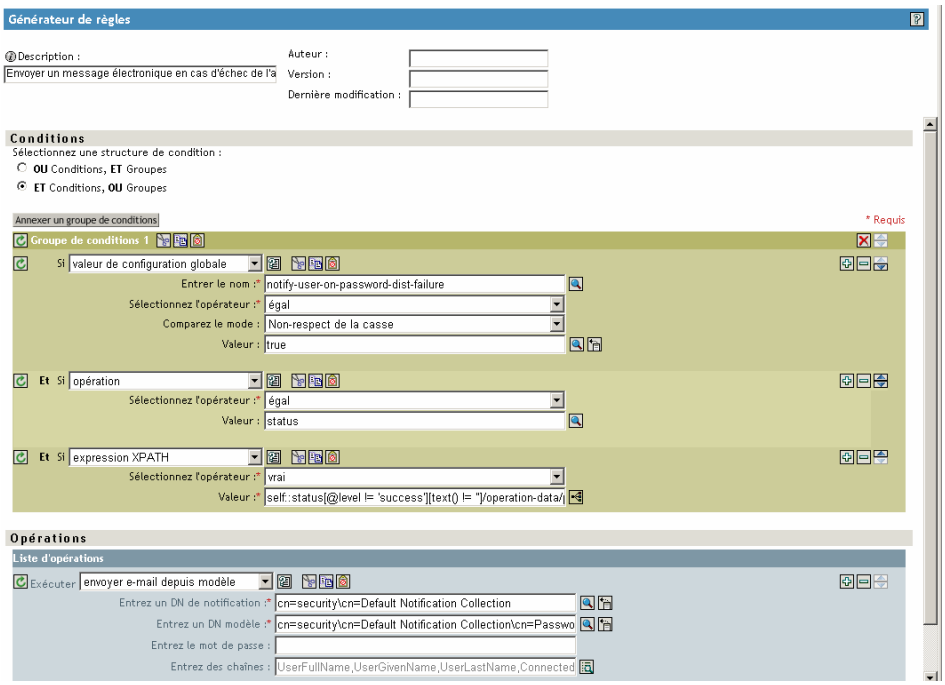
7 Cliquez sur une règle.

8 Indiquez le mot de passe du serveur SMTP dans les règles qui incluent les opérations d'envoi d'un message électronique à partir d'un modèle.

Si vous utilisez par exemple les exemples de configuration de pilote, les stratégies suivantes doivent être modifiées pour la synchronisation des mots de passe.

Ensemble de stratégies	Nom de la stratégie	Nom de la règle
Transformation en entrée	Password(Pub)-Sub Email Notifications	• Envoyer un message électronique en cas d'échec de l'abonnement aux mots de passe • Envoyer un message électronique en cas d'échec de la réinitialisation du mot de passe du système connecté à l'aide du mot de passe de la zone de stockage Identity Manager
Transformation en sortie	Password(Sub)-Pub Email Notifications	• Envoyer un message électronique en cas d'échec de la publication d'un mot de passe

La figure suivante montre un exemple de l'opération d'envoi d'un message électronique à partir d'un modèle qui exige le mot de passe.



Le mot de passe est masqué lorsqu'il est stocké dans le coffre-fort d'identité.

9 Sélectionnez (marquez) la règle, puis cliquez sur OK.

5.12.5 Ajout de vos balises de remplacement aux modèles de notification par message électronique

Les modèles de notifications par message électronique disposent de certaines balises, qui sont définies par défaut, pour vous aider à personnaliser le message pour l'utilisateur. Vous pouvez également ajouter vos propres balises.

La capacité à ajouter des balises dépend de l'application qui utilise le modèle.

- « Ajout de balises de remplacement aux modèles de notification par message électronique pour la synchronisation des mots de passe » page 153
- « Ajout de balises de remplacement aux modèles de notification par message électronique pour les mots de passe oubliés » page 159

Ajout de balises de remplacement aux modèles de notification par message électronique pour la synchronisation des mots de passe

Vous pouvez ajouter des balises de remplacement aux modèles de notification par message électronique pour la synchronisation des mots de passe. Toutefois, elles ne fonctionneront que si vous les définissez également dans chaque règle de la stratégie de synchronisation de mot de passe qui fait référence au modèle de notification par message électronique. Lorsque vous utilisez une opération d'envoi d'un message électronique à partir d'un modèle, toutes les balises de remplacement déclarées dans le modèle doivent être définies sous la forme d'éléments arg-strings enfants de l'opération.

À titre d'exemple, Identity Manager fournit des balises de remplacement par défaut, incluses avec les modèles de notification par message électronique. Il propose également des stratégies par défaut pour la synchronisation des mots de passe dans les configurations de pilote. Chaque balise par défaut fournie avec le modèle de message électronique est également définie dans chaque règle de la stratégie de synchronisation des mots de passe qui utilise le modèle de message.

Par exemple, la balise UserGivenName est l'une des balises par défaut définies dans le modèle de message électronique Password Set Fail (Échec de définition du mot de passe). Une règle de stratégie intitulée *Envoyer un message électronique en cas d'échec de l'abonnement aux mots de passe* fait référence à ce modèle lors d'une opération d'envoi d'un message électronique à partir d'un modèle. Cette règle, utilisée dans une stratégie, permet l'envoi d'une notification à l'utilisateur en cas d'échec de la synchronisation d'un mot de passe. Cette même balise UserGivenName est définie sous forme d'élément arg-string dans cette règle.

Comme dans cet exemple, chaque nouvelle balise ajoutée doit être définie dans le modèle de message électronique et dans les règles de stratégie qui font référence à ce modèle, afin que le moteur méta-annuaire puisse insérer les données appropriées à la place de la balise de remplacement lors de l'envoi du message électronique à l'utilisateur.

Vous pouvez faire référence aux balises qui figurent dans les configurations de pilote Identity Manager livrées à titre d'exemple avec Identity Manager.

Vous devez en outre vous souvenir que :

- Les éléments appelés balises de remplacement dans les modèles de messages électroniques sont appelés jetons dans le Générateur de stratégies.
- Utilisez le Générateur de stratégies pour faciliter la définition des chaînes d'arguments pour les balises de remplacement, tel qu'expliqué dans cette section.
- Les balises que vous ajoutez peuvent être définies sur l'un des points suivants :
  - Tout attribut Source ou Destination pour l'utilisateur

    À la différence de l'ajout de balises pour les modèles de messages électroniques en cas d'oubli du mot de passe, l'ajout d'une balise ayant le même nom qu'un attribut sur l'objet Utilisateur du coffre-fort d'identité ne permet pas de faire fonctionner la balise. Comme avec toutes les balises utilisées dans les modèles de notification par message électronique pour la synchronisation des mots de passe, vous devez également définir la balise dans la stratégie qui fait référence au modèle de message électronique.
  - Une valeur de configuration globale
  - Une expression XPATH

  Cela s'oppose aux balises des modèles de message électronique pour le Mot de passe oublié, limités aux attributs utilisateurs eDirectory.
- À la différence de l'ajout de balises pour les modèles de message électronique de mot de passe oublié, qui exigent que vous utilisiez le nom exact d'un attribut utilisateur eDirectory, vous pouvez nommer les balises de remplacement comme vous le souhaitez. Il suffit que le nom corresponde à celui utilisé pour définir la balise dans les stratégies qui référencent le modèle de message électronique.

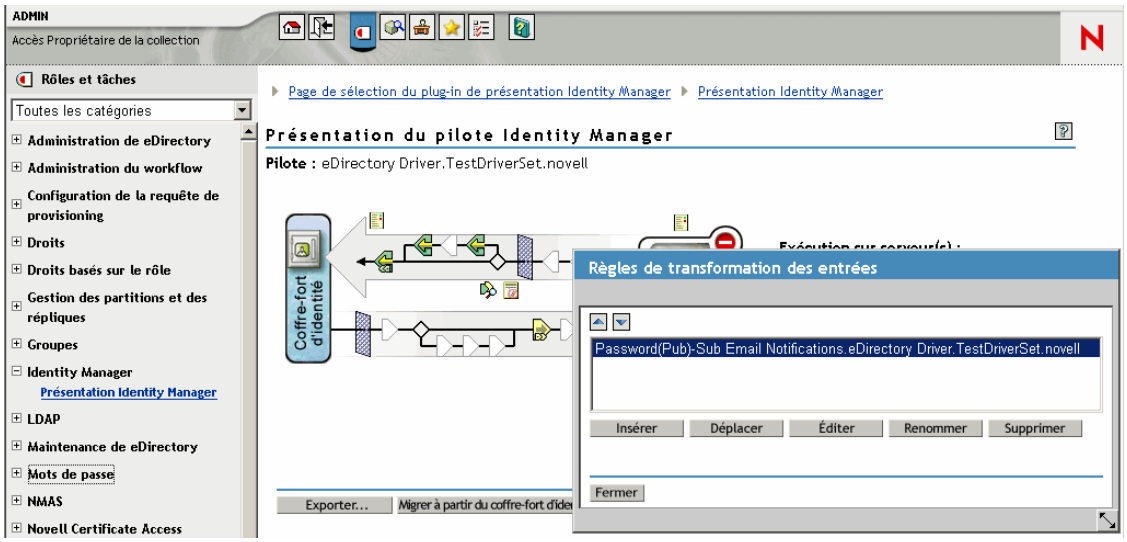
Pour définir les balises d'une stratégie, retrouvez toutes les stratégies qui font référence au modèle de notification par message électronique et utilisez le Générateur de stratégies pour leur ajouter les balises. Dans chaque stratégie, modifiez chaque règle faisant référence au modèle.

Pour vous assurer de retrouver toutes ces stratégies, vous pouvez exporter vos configurations de pilote et rechercher dans XML une opération do-send-e-mail associée à un modèle correspondant au nom du modèle de notification.

1. Dans iManager, sélectionnez *Identity Manager > Présentation de Identity Manager*.
2. Sélectionnez l'ensemble de pilotes qui contient le pilote disposant de la stratégie à modifier.
3. Cliquez sur l'icône du pilote contenant la stratégie à modifier.
4. Sur le canal Éditeur ou Abonné, cliquez sur l'ensemble de stratégies contenant la stratégie à modifier.

   Par exemple, la configuration du pilote eDirectory livré avec Identity Manager contient une stratégie dans l'ensemble de stratégies Transformation de l'entrée qui fait référence aux deux modèles de notification par message électronique pour la synchronisation des mots de passe.
5. Cliquez sur la stratégie, puis sur *Éditer*.

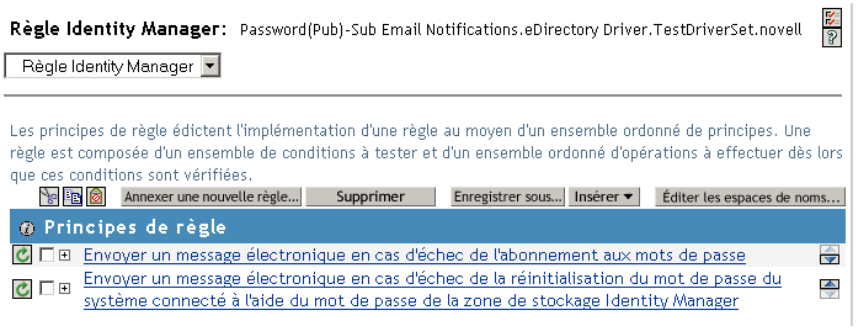
   L'illustration suivante montre comment éditer la stratégie Password(Pub)-Sub Email Notifications pour le pilote eDirectory :



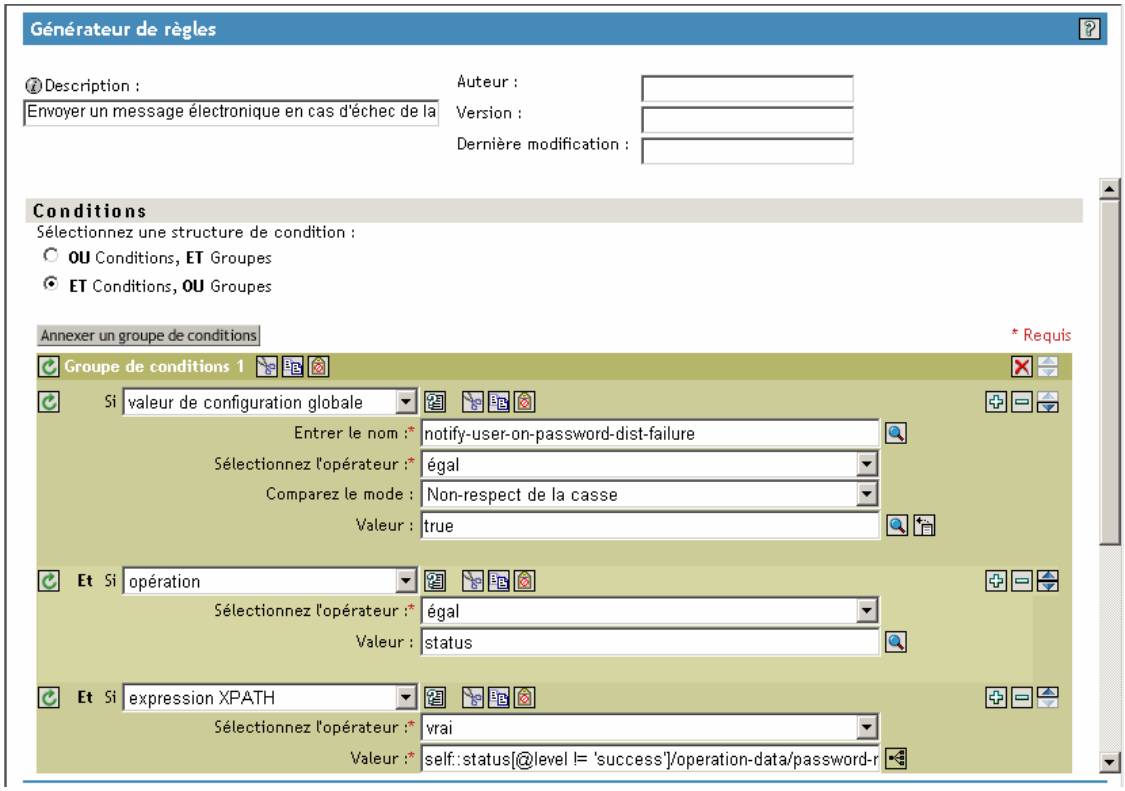
6. Dans la liste des règles qui s'ouvre, cliquez sur celle qui fait référence au modèle de notification par message électronique.

   Cette liste de règles apparaît par exemple dans la stratégie Password(Pub)-Sub Email Notifications. Ces deux règles font référence à l'un des modèles de message électronique pour

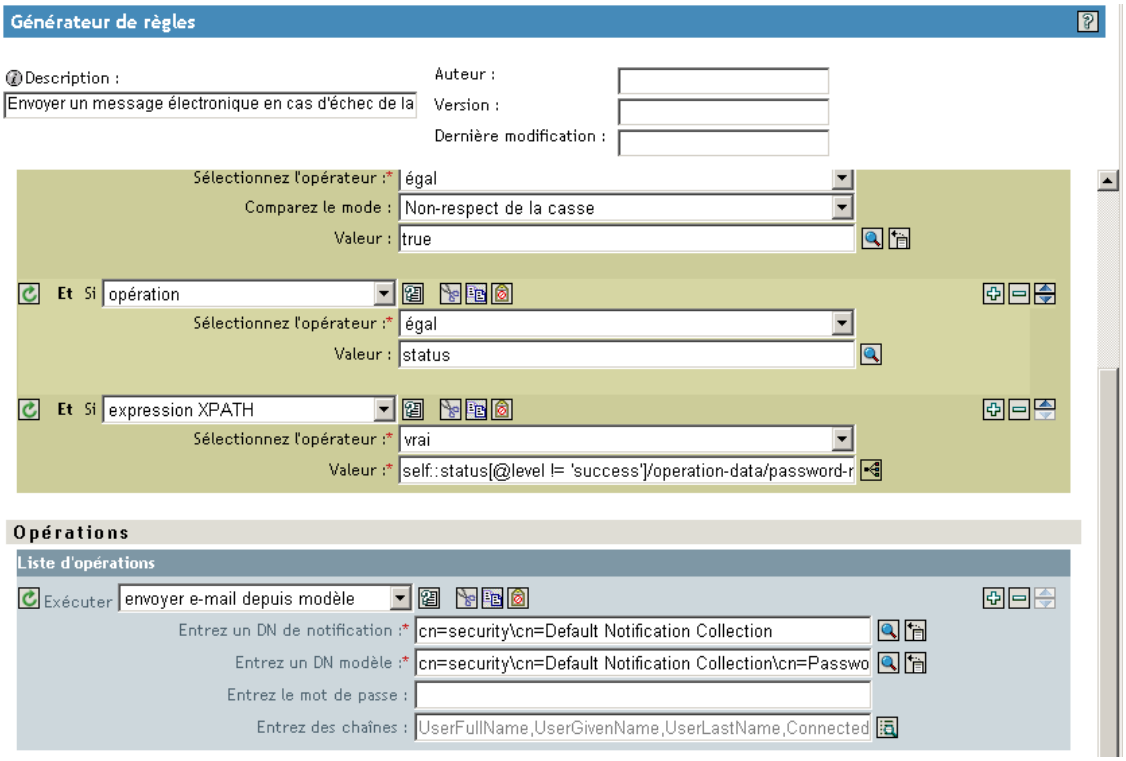
la synchronisation des mots de passe. Vous devez modifier les deux règles si vous ajoutez des balises aux deux modèles.



Si vous cliquez sur la première règle, la page suivante s'affiche :



7 Défilez jusqu'à la section *Opérations*.



8 Pour la règle *Envoyer un message électronique à partir d'un modèle*, cliquez sur le bouton Parcourir pour le champ *Saisissez des chaînes*.

Le Générateur de chaînes s'ouvre. La figure suivante montre la liste des chaînes qui s'afficherait pour cet exemple. Les balises par défaut utilisées dans les modèles de notification par message électronique sont déjà définies dans les stratégies de synchronisation des mots de passe faisant partie des configurations de pilote Identity Manager, comme celle-ci. Vous pouvez utiliser les balises par défaut à titre d'exemple.

9 Pour définir une balise utilisable dans un modèle de notification par message électronique, cliquez sur *Nouvelle chaîne*, puis saisissez le nom de la balise.

Assurez-vous que le nom est exactement identique au nom utilisé dans le modèle de notification par message électronique.

10 Dans le champ *Valeur de chaîne*, cliquez sur le bouton Parcourir pour vous aider à définir la balise.

11 Sur la page Générateur d'arguments, spécifiez la valeur à intégrer lorsque cette balise est utilisée dans un modèle de notification par message électronique.

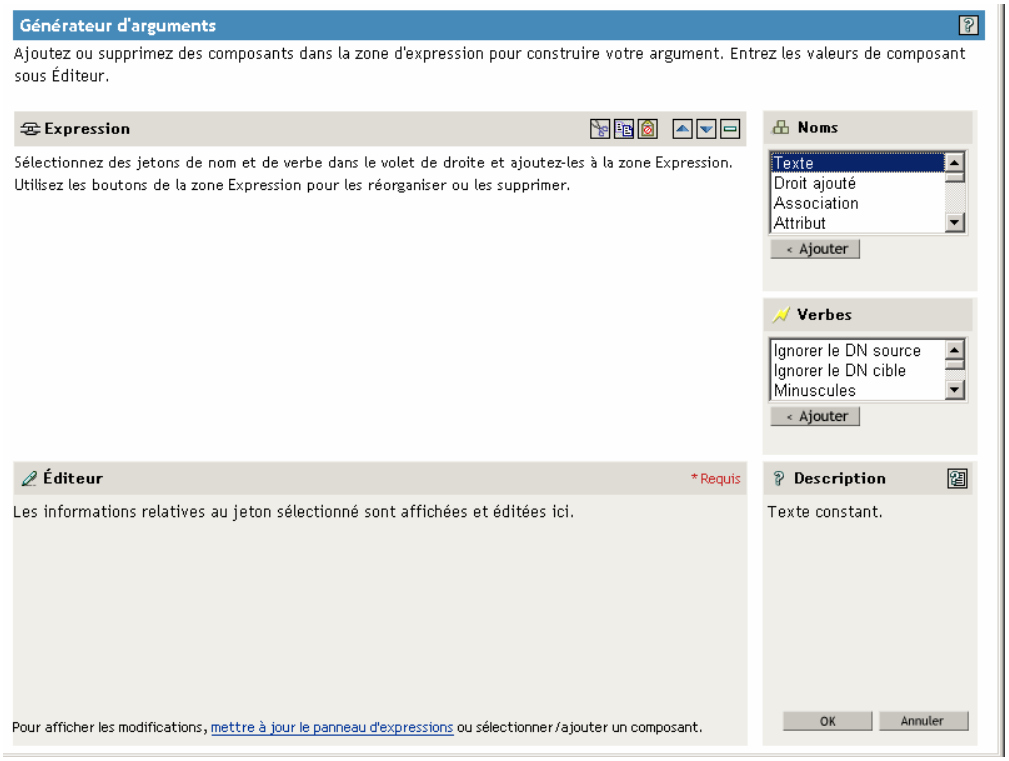
Vous pouvez définir la balise sur l'un des points suivants :

- Tout attribut Source ou Destination pour l'utilisateur

  À la différence de l'ajout de balises pour les modèles de messages électroniques en cas d'oubli du mot de passe, l'ajout d'une balise ayant le même nom qu'un attribut sur l'objet Utilisateur du coffre-fort d'identité ne permet pas de faire fonctionner la balise. Comme avec toutes les balises utilisées dans les modèles de notification par message électronique pour la synchronisation des mots de passe, vous devez également définir la balise dans la stratégie qui fait référence au modèle de message électronique.

- Une valeur de configuration globale
- Une expression XPATH

L'illustration suivante montre comment définir la balise :



Lorsque vous avez défini la balise et cliqué sur *OK*, la balise apparaît comme l'une des chaînes de la page du Générateur de chaînes.

12 N'oubliez pas de cliquer sur *OK* pour valider toutes les pages, afin d'enregistrer les modifications apportées à la stratégie.

13 Répétez les étapes de modification des règles dans toutes les stratégies qui font référence au modèle de notification par message électronique.

14 Ajoutez la balise définie dans la stratégie pour le modèle de notification par message électronique, à l'aide du nom exact utilisé dans les stratégies.

   À ce point de la procédure, vous pouvez utiliser le nom de balise présent dans le corps du modèle de notification par message électronique.

15 Enregistrez vos modifications et redémarrez le pilote.

Ajout de balises de remplacement aux modèles de notification par message électronique pour les mots de passe oubliés

Pour ajouter les balises aux modèles de notification par message électronique pour les mots de passe oubliés, aidez-vous des instructions suivantes :

- Vous ne pouvez ajouter que des balises correspondant aux attributs LDAP sur l'objet Utilisateur auquel le message est envoyé.
- Le nom de la balise que vous ajoutez doit être exactement le même que le nom de l'attribut LDAP sur l'objet utilisateur.

  Pour voir en quoi les attributs LDAP correspondent aux noms des attributs eDirectory, reportez-vous à la stratégie d'assignation de schéma fournie dans le pilote Identity Manager pour LDAP.
- Aucune autre configuration n'est nécessaire.

5.12.6 Envoi de notifications par message électronique à l'administrateur

La configuration par défaut indique que la notification par message électronique n'est adressée qu'à l'utilisateur. Les stratégies livrées avec Identity Manager utilisent l'adresse électronique de l'objet du coffre-fort d'identité pour l'utilisateur concerné.

Vous pouvez toutefois configurer les stratégies de synchronisation des mots de passe de sorte que les notifications soient également adressées à l'administrateur. Pour cela, vous devez modifier le script Identity Manager pour l'une de ces stratégies.

Adressez une copie cachée à l'administrateur en définissant le jeton avec son adresse électronique.

Pour mettre un administrateur en copie, modifiez la stratégie de génération du message électronique (par exemple PublishPasswordEmails.xml, qui recherche l'adresse électronique où envoyer les notifications), et ajoutez un élément `<arg-string>` à l'adresse électronique de l'administrateur.

L'exemple suivant montre l'élément arg-string ajouté :

```
<arg-string name="to">

<token-text>Admin@company.com</token-text>

</arg-string>
```

N'oubliez pas de redémarrer le pilote après avoir apporté les modifications.

5.12.7 Localisation des modèles de notification par l'adresse de messagerie électronique

Vous devez en outre vous souvenir que :

- Les modèles par défaut sont rédigés en anglais, mais vous pouvez les personnaliser dans votre langue.
- Les noms et les définitions des balises de remplacement doivent rester en anglais, de sorte que les définitions de jetons arg-string des stratégies concordent avec les noms des balises de remplacement.
- Pour les notifications de mot de passe oublié envoyées uniquement par message électronique, vous devez ajouter un paramètre dans le fichier `portalservlet.properties` afin d'indiquer le codage à utiliser dans le courrier. Par exemple :

  ```
  ForgottenPassword.MailEncoding=EUC-JP
  ```

  Si ce paramètre n'existe pas, la transformation du courrier ne fera appel à aucun codage.
- Pour les messages électroniques de synchronisation des mots de passe, vous pouvez spécifier un attribut XML nommé charset sur les éléments suivants : `<mail>`, `<message>` et `<‘>`.

  Pour plus d'informations sur l'utilisation de ces éléments, reportez-vous au *DirXML Driver for Manual Task Service Implementation Guide (Guide d'implémentation du pilote DirXML pour le service de tâches manuelles)* (http://www.novell.com/documentation/dirxmldrivers/index.html). Vous y trouverez davantage de détails sur les modèles de messages électroniques.

5.13 Dépannage des problèmes de synchronisation des mots de passe

- Pour plus d'informations sur les astuces, reportez-vous à la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111.
- Vérifiez que la méthode de login par mot de passe simple NMAS est installée.
- Vérifiez que vous disposez d'une copie de la racine de l'arborescence sur les serveurs sur lesquels NMAS doit appliquer les stratégies de mot de passe sur les méthodes de login de eDirectory ou sur les mots de passe des systèmes connectés synchronisés par Identity Manager.
- Vérifiez que tous les utilisateurs nécessitant une synchronisation des mots de passe sont répliqués sur le même serveur que le pilote chargé de la synchronisation des mots de passe. Comme pour ses autres fonctions, le pilote ne peut gérer que les utilisateurs se trouvant sur une réplique principale ou en lecture/écriture du même serveur.
- Vérifiez que SSL est correctement configuré entre le serveur Web et le coffre-fort d'identité.
- Si un message d'erreur indique qu'un mot de passe correctement configuré dans le coffre-fort d'identité n'est pas conforme lorsqu'un utilisateur est créé, le mot de passe par défaut de la stratégie du pilote n'est peut-être pas conforme à la stratégie de mots de passe qui s'applique à cet utilisateur.

  Le scénario suivant utilise le pilote Active Directory. Ce problème peut toutefois se produire avec un autre pilote.

  Spécification d'un mot de passe initial : vous souhaitez que le pilote Active Directory fournisse le mot de passe initial d'un utilisateur lorsqu'il crée dans le coffre-fort d'identité un nouvel objet Utilisateur correspondant à un utilisateur Active Directory. L'exemple de

configuration du pilote Active Directory envoie le mot de passe initial et ajoute un utilisateur de manière séparée ; l'exemple de configuration comprend également une stratégie fournissant un mot de passe par défaut à l'utilisateur, si Active Directory ne fournit aucun mot de passe.

Comme l'ajout de l'utilisateur et la définition du mot de passe se font séparément, tout nouvel utilisateur se voit systématiquement attribuer le mot de passe par défaut, ne serait-ce que provisoirement. Très vite, ce mot de passe par défaut est mis à jour puisque le pilote Active Directory l'envoie immédiatement après avoir ajouté l'utilisateur. Si le mot de passe par défaut ne répond pas aux exigences de la stratégie de mots de passe du coffre-fort d'identité pour l'utilisateur, un message d'erreur apparaît.

Par exemple, si le mot de passe par défaut créé à partir du nom de l'utilisateur est trop court, un message d'erreur –216 apparaît, indiquant que le mot de passe est trop court. Cependant, ce problème se résout de lui-même dès que le pilote Active Directory envoie un mot de passe initial respectant la stratégie.

Si vous souhaitez avoir un système connecté qui crée des objets Utilisateur pour fournir le mot de passe initial, quel que soit le pilote que vous utilisez, choisissez l'une des options suivantes. Ces mesures sont particulièrement importantes si le mot de passe initial n'accompagne pas l'événement d'ajout mais qu'il vient plus tard.

- Sur le canal Éditeur, modifiez la stratégie qui crée le mot de passe par défaut afin que ce dernier soit conforme aux stratégies définies pour votre société dans le coffre-fort d'identité. Sélectionnez pour cela *Mots de passe*, puis *Stratégies de mots de passe*.

  Lorsque le mot de passe provient de l'application experte, il remplace le mot de passe par défaut.

  Il vaut mieux choisir cette option : en effet, Novell recommande la création d'une stratégie de mots de passe par défaut, afin que le niveau de sécurité du système soit aussi élevé que possible.
- Sur le canal Éditeur, supprimez la stratégie qui crée le mot de passe par défaut. Dans l'exemple de configuration, cette stratégie est fournie par l'ensemble de stratégies de transformation de la commande. Dans le coffre-fort d'identité, l'ajout d'un utilisateur sans mot de passe est autorisé. En effet, dans ce cas, l'objet Utilisateur nouvellement créé passe par le canal Éditeur ; l'absence de mot de passe n'est que temporaire.

- Les stratégies de mot de passe sont assignées dans une perspective centrée sur l'arborescence. La synchronisation des mots de passe, en revanche, est définie pilote par pilote. Les pilotes sont installés pour chaque serveur et ne peuvent gérer que les utilisateurs se trouvant sur une réplique principale ou en lecture/écriture.

  Pour que la synchronisation des mots de passe donne les résultats escomptés, vérifiez que les conteneurs d'une réplique principale ou en lecture/écriture sur le serveur, exécutant les pilotes et auxquels s'applique la synchronisation, correspondent aux conteneurs pour lesquels vous avez assigné des stratégies de mot de passe en activant le mot de passe universel. L'assignation d'une stratégie de mot de passe au conteneur racine d'une partition garantit que cette stratégie s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.
- Commandes DSTrace utiles :

  +DXML : pour afficher le traitement des règles Identity Manager et les messages d'erreur potentiels.

  +DVRS : affiche les messages du pilote Identity Manager.

  +AUTH : affiche les modifications des mots de passe NDS.

  +DCLN : affiche les messages NDS Dclient.

Création et utilisation des droits

6

Identity Manager permet de synchroniser les données entre des systèmes connectés. Les droits permettent de définir des critères pour une personne ou un groupe. Lorsque ces critères sont remplis, un événement accordant ou révoquant l'accès aux ressources de l'entreprise, au sein du système connecté, est lancé. Vous bénéficiez ainsi d'un niveau de contrôle et d'automatisation supplémentaire pour accorder ou refuser l'accès aux ressources.

Le fonctionnement des droits comporte deux étapes : une étape de création et une étape de gestion. Les droits sont créés dans iManager ou dans Designer. Pour créer un droit dans iManager, sélectionnez l'option *Créer un droit* sous l'en-tête Utilitaires Identity Manager de iManager. Pour plus d'informations, reportez-vous à la Section 6.4, « Rédaction de droits en langage XML dans iManager », page 168.

Vous pouvez également utiliser Designer pour créer des droits et les déployer dans les pilotes Identity Manager existants. Designer permet de créer des droits depuis l'interface graphique de l'assistant de création de droits, qui vous guide tout au long du processus. Dans iManager, vous créez les droits dans une interface simple, mais vous pouvez ajouter des propriétés supplémentaires dans un éditeur XML. Nous vous recommandons de créer et de modifier les droits dans le Concepteur, puisqu'il comporte une interface graphique.

Après avoir créé des droits (ou utilisé des droits préconfigurés dans certains pilotes Identity Manager), vous devez les gérer. Les droits sont gérés par deux progiciels ou agents : iManager, via les stratégies de droits basés sur le rôle, ou le provisioning basé sur le workflow dans l'application utilisateur.

Les stratégies de droits basés sur le rôle permettent d'octroyer des ressources d'entreprise, si les critères définis sont remplis. Supposons, par exemple, qu'un utilisateur remplissant les critères 1, 2 et 3 devienne membre du groupe H conformément à une stratégie de droits basés sur le rôle. En revanche, s'il remplit les critères 4 et 5, il devient membre du groupe I. Pour que ce droit fonctionne dans le provisioning basé sur le workflow, une approbation préalable est nécessaire.

6.1 Terminologie

Voici quelques termes que vous rencontrerez dans ce chapitre.

Tableau 6-1 *Terminologie*

Termes	Explication
Droit	Objet du coffre-fort d'identité représentant une ressource de l'entreprise dans un système connecté.
Agent de droit	Accorde ou révoque des droits. Pour les droits basés sur le rôle, l'agent est le pilote du service de droits.
Accorder ou révoquer	L'interprétation de l'accord ou de la révocation d'un droit est contrôlée par les variables de configuration globale (GCV) sur un pilote Identity Manager.
Consommateur de droits	Tout élément utilisant les informations relatives aux droits. Les consommateurs de droits peuvent être iManager, l'application utilisateur et les règles Identity Manager.

6.2 Création de droits : présentation

Vous devez savoir au départ ce que vous souhaitez faire avec les droits. Le fonctionnement des droits dépend des fonctionnalités intégrées aux pilotes Identity Manager par le biais des stratégies. Ces stratégies implémentent les règles et traitent les événements entre le coffre-fort d'identité et le système connecté. Si les stratégies du pilote Identity Manager n'indiquent pas ce que vous voulez faire, les droits ne peuvent pas fonctionner. Si, par exemple, vous n'indiquez rien dans la section Opération de la règle Vérifier la modification de l'utilisateur pour une appartenance au groupe dans la stratégie Command, les tentatives d'octroi ou de révocation d'un droit d'appartenance au groupe ne seront pas prises en compte.

Vous devez savoir précisément ce que vous souhaitez faire avec Identity Manager pour pouvoir ensuite définir correctement les fonctions d'octroi ou de révocation pour les ressources des systèmes connectés. Les quatre étapes de la procédure suivante vous aideront à planifier la création et l'utilisation des droits :

1. Sachez ce que vous souhaitez accomplir dans votre activité. Identity Manager permet de concevoir et d'implémenter pratiquement tout ce que vous souhaitez, à condition que vous sachiez ce que vous voulez faire. Faites la liste de ce que vous voulez faire, avec des numéros.
2. Définissez un droit représentant l'un des points de votre liste. Vous pouvez créer des droits avec ou sans valeur. Les droits associés à une valeur peuvent tirer celle-ci d'une requête externe, ils peuvent être définis par l'administrateur ou avoir une structure libre. Vous trouverez des exemples à la Section 6.4.6, « Modèles de droits », page 178.
3. Ajoutez des stratégies au pilote Identity Manager pour implémenter le droit préalablement défini. Pour créer une stratégie pour un pilote Identity Manager, vous devez bien connaître les scripts XSLT ou DirXML, savoir comment le système connecté gère et reçoit les informations, et savoir comment Novell® eDirectory™ stocke les informations. Sauf si vous êtes un programmeur chevronné en langage DirXML*, cette tâche est réservée aux consultants.
4. Définissez un agent de gestion chargé d'accorder ou de révoquer le droit. Si vous souhaitez un processus automatisé, utilisez les droits basés sur le rôle. Si vous préférez un processus manuel, utilisez le provisioning basé sur le workflow.

6.2.1 Pilotes Identity Manager dotés de préconfigurations prenant en charge les droits

Identity Manager est fourni avec un certain nombre de pilotes dotés de préconfigurations contenant déjà des droits et des stratégies permettant de les implémenter. Le pilote est activé pour écouter les activités liées aux droits. Vous devez activer les droits à la première installation du pilote pour que celui-ci intègre les éléments préconfigurés. Les pilotes suivants s'accompagnent de préconfigurations prenant en charge les droits :

- Active Directory*
- Exchange
- GroupWise®
- LDAP
- NIS
- Lotus* Notes*
- NT Domain
- RACF

Ces pilotes préconfigurés respectent les trois premières étapes indiquées plus haut. Les exemples de droits qu'ils contiennent sont utilisables dans les scénarios les plus courants : octroi et révocation de comptes utilisateurs, de groupes et de listes de distribution de courrier électronique. Ils comprennent les éléments suivants :

- Active Directory : octroi et révocation de comptes, d'appartenance à un groupe, de boîtes aux lettres Exchange
- Exchange 5.5 : octroi et révocation de boîtes aux lettres et d'appartenance à un groupe
- GroupWise : octroi et révocation de comptes et de membres de listes de distribution
- LDAP : octroi et révocation de comptes utilisateur
- Linux* et UNIX* : octroi et révocation de comptes
- Lotus Notes : octroi et révocation de comptes utilisateur et d'appartenance à un groupe
- NT Domain : octroi et révocation de comptes utilisateur et d'appartenance à un groupe
- RACF : octroi et révocation de comptes de groupe et d'appartenance à un groupe

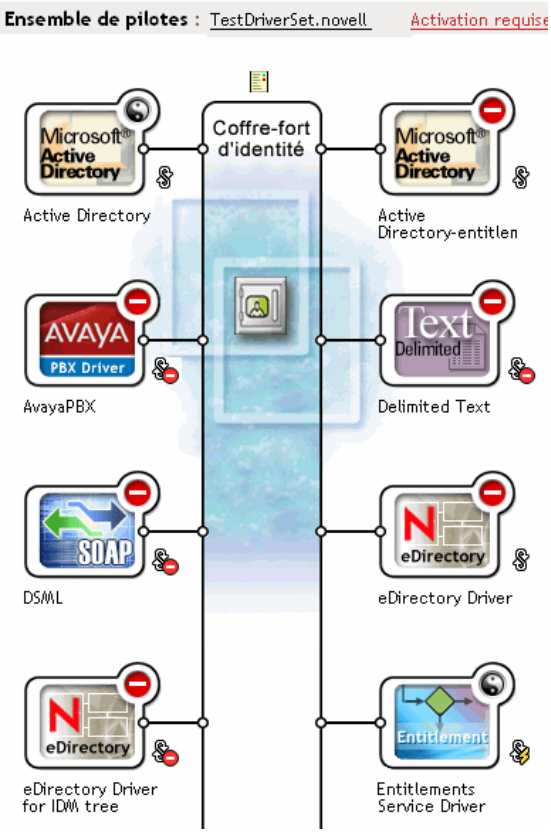
Il s'agit là d'exemples de droits et de stratégies que vous pouvez utiliser tels quels (s'ils vous conviennent) ; vous pouvez également les adapter à vos besoins, ou les utiliser comme exemples pour créer vos propres droits et stratégies dans iManager ou Designer. Encore une fois, si vous souhaitez utiliser les droits d'un pilote préconfiguré, vous devez activer les droits lorsque vous créez ce pilote dans Designer ou dans iManager. Les droits préconfigurés ne peuvent pas être ajoutés par la suite, à moins de recréer le pilote.

Si vous avez utilisé des droits avec Identity Manager 2.x et si vous souhaitez les utiliser dans Identity Manager 3, lancez la fonction *Mettre à niveau des droits* sous *Utilitaires Identity Manager*.

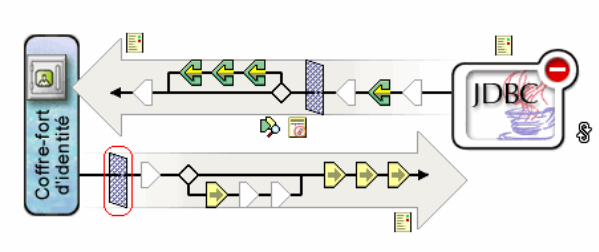
6.2.2 Activation des droits sur les autres pilotes Identity Manager

Vous pouvez aussi utiliser les droits sur les pilotes Identity Manager ne comportant pas de droits préconfigurés. Pour activer votre pilote afin qu'il prenne en charge les droits, ajoutez l'attribut DirXML-EntitlementRef au filtre du pilote. Pour ce faire :

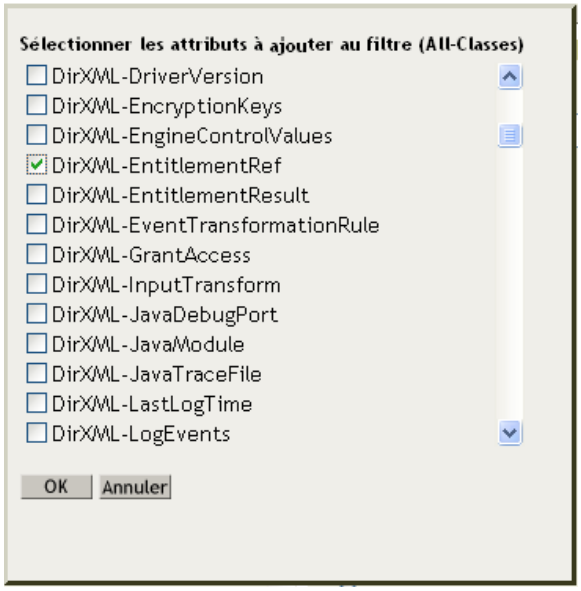
1. Sélectionnez *Identity Manager* > *Présentation de Identity Manager*.
2. Recherchez l'ensemble de pilotes contenant le pilote concerné, puis cliquez sur *Rechercher*.
3. Dans l'écran Présentation de Identity Manager, sélectionnez l'objet Pilote dans l'ensemble proposé.



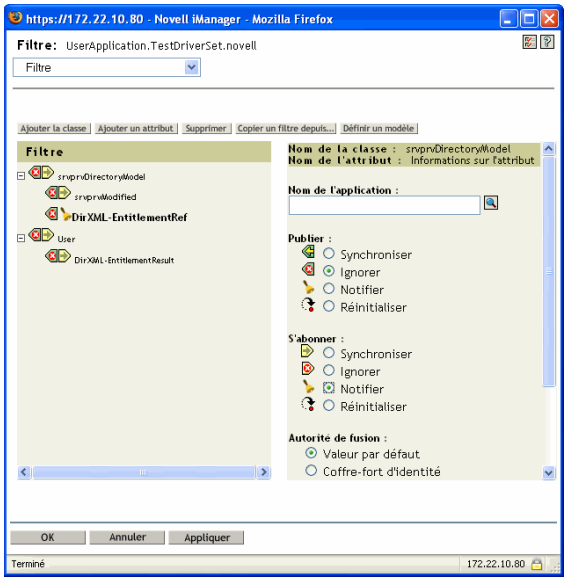
4. Dans l'ensemble de pilotes, double-cliquez sur le pilote pour afficher l'écran correspondant. Cliquez sur l'icône *Filtre du pilote* à droite du coffre-fort d'identité (entourée d'un cercle rouge).



5. Sur la page Filtre, sélectionnez *Ajouter un attribut*, puis descendez en bas de la liste et sélectionnez *Afficher tous les attributs*. Sélectionnez l'attribut *DirXML-EntitlementRef* et cliquez sur *OK*.



6. Sur la page Filtre, sélectionnez *DirXML-EntitlementRef*. Sous l'en-tête S'abonner, sélectionnez *Notifier*. Cliquez sur *OK*.



7. Cette opération se fait automatiquement lorsque vous créez des droits sur un pilote dans Designer.

6.3 Conditions préalables à la création de droits

- ❑ eDirectory, version 8.7.3 ou ultérieure.
- ❑ Identity Manager 2 ou 3

- ❑ Un pilote de service de droits

  Vous devez disposer d'un tel pilote pour chaque ensemble de pilotes dans lequel vous souhaitez utiliser des droits. Pour cela, vous devez procéder à une configuration simple et ponctuelle pour chaque ensemble de pilotes.

- ❑ Une configuration de pilote prenant en charge les droits

  Avant de pouvoir utiliser les droits avec un système connecté, effectuez l'une des opérations suivantes :

  - Importez la configuration du pilote Identity Manager et précisez que les droits sont activés pour ce pilote.
  - Activez votre pilote pour qu'il prenne en charge les droits. Pour ce faire :
    a. Créez des droits à l'aide de iManager ou du Designer (de préférence Designer).
    b. Ajoutez l'attribut DirXML-EntitlementRef au filtre du pilote, comme indiqué à la Section 6.2.2, « Activation des droits sur les autres pilotes Identity Manager », page 166.
    c. Rédigez des stratégies permettant d'implémenter les droits créés à l'étape 1.

6.4 Rédaction de droits en langage XML dans iManager

Pour mieux comprendre ce que vous devez inclure dans un droit, vous pouvez consulter les droits et les stratégies qui figurent dans l'un des pilotes préconfigurés avec les droits activés (Active Directory, AD). Pour ce faire, examinez le fichier DTD (Document Type Definition) de Novell, puis reportez-vous aux exemples de droits rédigés en XML qui s'appuient sur ce DTD.

Dans cette section :

6.4.1 Ajouts effectués par le pilote Active Directory lorsque les droits sont activés

Lorsque les droits sont activés, la structure du pilote AD présente les modifications suivantes :

- Ajout de l'attribut DirXML-EntitlementRef au filtre du pilote. L'attribut DirXML-EntitlementRef permet au filtre du pilote d'écouter les activités liées aux droits.
- Création d'un droit sur le compte utilisateur. Ce droit permet d'accorder un compte à l'utilisateur dans Active Directory ou de le révoquer. Lorsque le compte est accordé, l'utilisateur obtient un

compte de connexion actif. Lorsqu'il est révoqué, le compte de connexion est soit désactivé, soit supprimé, selon la configuration du pilote.

- Création d'un droit d'appartenance au groupe. Ce droit accorde ou révoque l'appartenance à un groupe dans Active Directory. Le groupe doit être associé à un groupe du coffre-fort d'identité. Si l'appartenance au groupe est révoquée, l'utilisateur est retiré de ce groupe. Le droit d'appartenance au groupe n'est pas appliqué sur le canal Éditeur. Si un utilisateur est ajouté par un outil externe à un groupe contrôlé dans Active Directory, il n'est pas supprimé par le pilote. De plus, si le droit est retiré de l'objet Utilisateur et non simplement révoqué, le pilote AD ne fait rien.
- Création d'un droit à une boîte aux lettres Exchange. Ce droit accorde à l'utilisateur une boîte aux lettres dans Microsoft Exchange ou la révoque.
- Ajout d'informations sur les droits dans de nombreuses stratégies.

Les stratégies suivantes contiennent des règles supplémentaires permettant aux droits de fonctionner correctement :

- InputTransform (niveau pilote). La règle Vérifier la cible de l'ajout d'une association pour les droits d'appartenance au groupe de cette stratégie vérifient si la cible de « add-association » comprend des droits d'appartenance à un groupe. Les droits d'appartenance à un groupe ne peuvent être traités que lorsque l'utilisateur concerné a été correctement créé dans Active Directory. Add-association indique qu'un objet a été créé par le pilote dans Active Directory. Si l'objet est également marqué pour le traitement des droits d'appartenance au groupe, le traitement a lieu.
- Event Transform (canal Éditeur). La règle Interdire la suppression des comptes utilisateur de cette stratégie interdit la suppression d'un compte utilisateur dans le coffre-fort d'identité. Si vous utilisez le droit au compte utilisateur, les comptes utilisateur gérés sont contrôlés par ce droit dans le coffre-fort d'identité. Une suppression effectuée dans Active Directory n'entraîne pas la suppression de l'objet de contrôle dans le coffre-fort d'identité. Une modification ultérieure de l'objet dans le coffre-fort d'identité ou une opération de fusion peuvent permettre de recréer le compte dans Active Directory.
- Command (canal Abonné). La stratégie Command contient les règles suivantes relatives aux droits :
  - Règle Modification du droit au compte utilisateur (option Supprimer). Ce droit permet d'accorder à l'utilisateur un compte activé dans Active Directory. Si le droit est révoqué, le compte Active Directory est désactivé ou supprimé, selon la valeur sélectionnée pour la variable globale *Lorsque le droit d'un compte est annulé*. Cette règle s'exécute lorsque le droit change et que vous avez sélectionné l'option Supprimer.
  - Règle Modification du droit au compte utilisateur (option Désactiver). Ce droit permet d'accorder à l'utilisateur un compte activé dans Active Directory. Si le droit est révoqué, le compte Active Directory est désactivé ou supprimé, selon la valeur sélectionnée pour la variable globale *Lorsque le droit d'un compte est annulé*. Cette règle s'exécute lorsque le droit change et que vous avez sélectionné l'option Désactiver.
  - Règle Vérifier la modification de l'utilisateur pour une appartenance au groupe en cours d'accord ou d'annulation.
  - Règle Vérifier la modification de l'utilisateur pour une boîte aux lettres Exchange en cours d'accord ou de révocation.
- Matching (canal Abonné). Il s'agit de la règle Droit au compte : ne pas faire correspondre les comptes existants de cette stratégie. Lorsque vous utilisez le droit Compte utilisateur avec l'application utilisateur Identity Manager ou les droits basés sur le rôle, les comptes sont créés

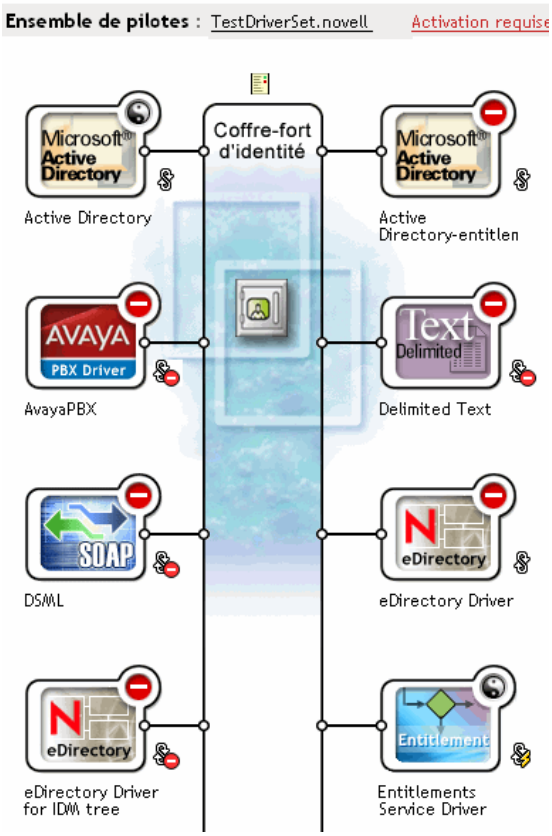
et supprimés ou désactivés par l'octroi ou la révocation du droit. La stratégie par défaut n'associe pas de compte existant dans Active Directory si l'utilisateur n'a pas droit à un tel compte. Modifiez ou supprimez cette règle si vous souhaitez que la stratégie de droit s'applique aux comptes correspondants dans Active Directory. Notez que cela peut entraîner la suppression ou la désactivation du compte Active Directory.

- Creation (canal Abonné). La stratégie Creation contient les règles suivantes relatives aux droits :
  - Droits du compte : bloquer la création du compte si le droit n'est pas accordé. Lorsque vous utilisez le droit Compte utilisateur avec l'application utilisateur Identity Manager ou les droits basés sur le rôle, les comptes sont créés uniquement pour les utilisateurs auxquels le droit au compte a été spécifiquement accordé. Cette règle oppose son veto à la création d'un compte utilisateur si le droit n'est pas accordé.
  - Comptes du coffre-fort d'identité activés si Login désactivé n'existe pas.
  - Préparer la vérification des droits du groupe après ajout. Les droits de groupe sont traités après l'ajout, parce que les objets ajoutés doivent exister pour pouvoir être ajoutés à un groupe. L'ajout est signalé par une propriété fonctionnelle vérifiée dans la transformation de l'entrée à la fin du processus d'ajout.
  - Signaler la nécessité de vérifier les droits Exchange après ajout.
  - Associer le nom d'utilisateur au nom de login Windows. Lorsque userPrincipalName est paramétré pour suivre le nom d'utilisateur eDirectory, définissez userPrincipalName sur le nom de l'objet eDirectory et le nom du domaine Active Directory.

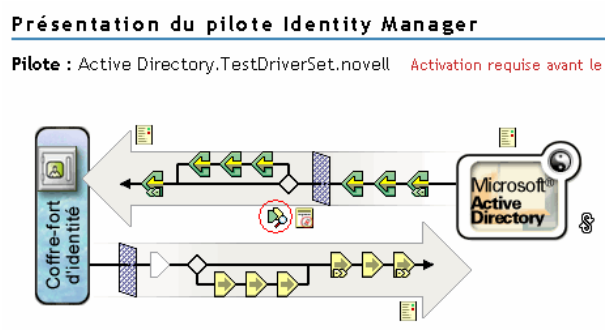
Pour voir le code XML de chaque stratégie, procédez comme suit dans iManager :

1. Sélectionnez *Identity Manager > Présentation de Identity Manager*.
2. Recherchez l'ensemble de pilotes contenant le pilote concerné, puis cliquez sur *Rechercher*.

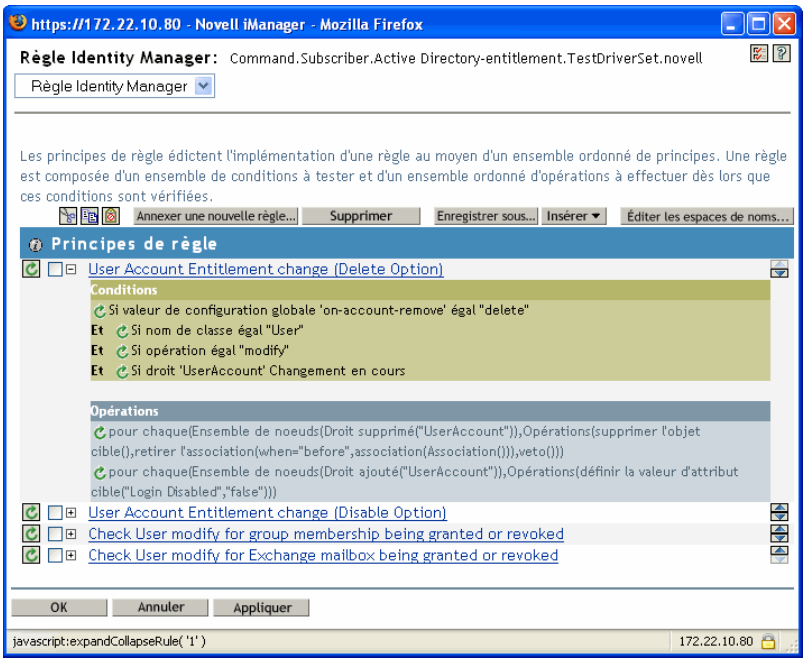
3. Dans l'écran Présentation de Identity Manager, sélectionnez l'objet Pilote dans l'ensemble proposé.



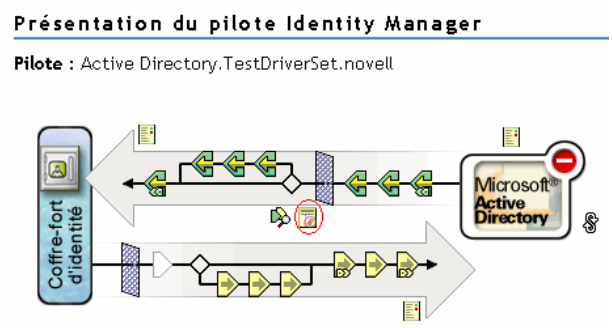
4. Dans l'ensemble de pilotes, double-cliquez sur le pilote pour afficher l'écran correspondant. Cliquez sur l'icône *Afficher toutes les stratégies* au centre du pilote (dans un cercle rouge).



5. Lorsque vous avez sélectionné une stratégie dans l'écran Afficher toutes les stratégies, vous pouvez afficher les conditions et les opérations qui la constituent.



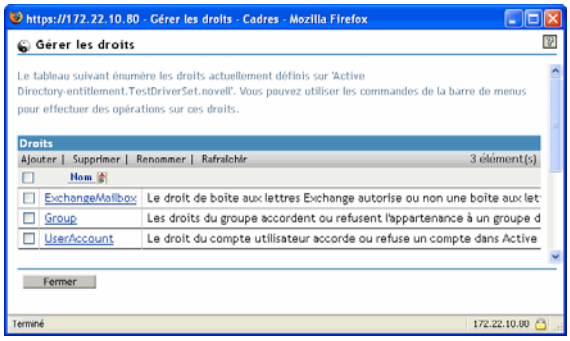
6. Pour afficher le code XML qui sous-tend les stratégies, sélectionnez *Édition XML* dans le menu déroulant (par défaut, il s'agit du menu Stratégie Identity Manager). Pour plus d'informations sur la création et la modification des stratégies, reportez-vous au *Policy Builder and Driver Customization Guide (Guide de création des stratégies et de personnalisation des pilotes)* et au guide du pilote Identity Manager (http://www.novell.com/documentation/dirxmldrivers/index.html) sélectionné pour créer des stratégies spécifiques au pilote en question.
7. Pour afficher les droits qui accompagnent les pilotes préconfigurés (dans notre exemple, Active Directory) avec les droits activés, suivez les étapes 1 à 4. Toutefois, sélectionnez l'icône *Afficher tous les droits* au centre du pilote (dans un cercle rouge).



8. Sur la page Gérer les droits, cliquez sur le nom du droit pour l'afficher dans la visionneuse XML. Pour en modifier le code, cliquez sur *Activer l'édition XML*.

Si les droits sont activés, le pilote Active Directory s'accompagne de trois droits : Compte utilisateur, Groupe et Boîte aux lettres Exchange.

Figure 6-1 *Droits fournis avec le pilote AD*



Vous pouvez consulter le code XML de ces droits dans les exemples de rédaction de la Section 6.4.6, « Modèles de droits », page 178.

6.4.2 Utilisation du fichier DTD (Document Type Definition) des droits Novell

Certains droits sont prédéfinis sur les pilotes, si les droits sont activés sur les pilotes en question. Vous pouvez utiliser ces droits ou en créer de nouveaux dans iManager ou Designer. Pour vous aider à créer vos propres droits, utilisez le fichier DTD Novell suivant comme modèle.

Cette description du fichier DTD est suivie de quatre exemples de rédaction des droits au format XML dans iManager. Si vous ne voulez pas utiliser le format XML, servez-vous de l'assistant de création de droits du Designer, qui vous facilitera la tâche.

Fichier DTD de droits de Novell

```
<!-************************************************************->
<!-- DirXML Entitlements DTD  <!-- Novell Inc. <!-- 1800 South Novell
Place <!-- Provo, UT 84606-6194 <!-- Version=1.0.0 <!-- Copyright 2005
Novell, Inc. All rights reserved --> <!--
********************************************************** --> <!--
Entitlement definition stored in the XmlData attribute of a
DirXML-Entitlement object. --> <!ELEMENT entitlement (values?)>
<!ATTLIST entitlement conflict-resolution (priority | union)
"priority" display-name CDATA #REQUIRED description CDATA #REQUIRED >
<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-valued
(true | false) "true" > <!ELEMENT value (#PCDATA)> <!ELEMENT query-app
(query-xml, result-set)> <!ELEMENT query-xml ANY> <!ELEMENT result-set
(display-name, description, ent-value)> <!ELEMENT display-name(token-
attr | token-src-dn | token-association)> <!ELEMENT ent-value (token-
association | token-src-dn | token-attr)> <!ELEMENT description
(token-association | token-src-dn | token-attr)> <!ELEMENT token-
association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr
attr-name CDATA #REQUIRED > <!ELEMENT token-src-dn EMPTY> <!--
Entitlement reference stored in the DirXML-EntitlementRef attribute of
a DirXML-EntitlementRecipient or a DirXML-SharedProfile object. -->
<!ELEMENT ref (src?, id?, param?)> <!ELEMENT param (#PCDATA)>
```

```
<!ELEMENT id (#PCDATA)> <!ELEMENT src (#PCDATA)> <!--     Entitlement
result stored in the DirXML-EntitlementResult attribute of a DirXML-
EntitlementRecipient object. --> <!ELEMENT result(dn, src, id?,
param?, state, status, msg?,timestamp)> <!ELEMENT dn (#PCDATA)>
<!ELEMENT state (#PCDATA)> <!ELEMENT status (#PCDATA)> <!ELEMENT msg
ANY> <!ELEMENT timestamp (#PCDATA)> <!--    Cached query results stored
in the DirXML-SPCachedQuery attribute of a DirXML-Entitlement object.
--> <!ELEMENT items (item*)> <!ELEMENT item (item-display-name?, item-
description?, item-value)> <!ELEMENT item-display-name (#PCDATA)>
<!ELEMENT item-description (#PCDATA)> <!ELEMENT item-value (#PCDATA)>
<!--    Representation of a DirXML-EntitlementRef within the DirXML
Script and within the operation-data of an operation in an XDS
document. --> <!ELEMENT entitlement-impl (#PCDATA)> <!ATTLIST
entitlement-impl name CDATA #REQUIRED src CDATA #REQUIRED id CDATA
#IMPLIED state (0 | 1) #REQUIRED src-dn CDATA #REQUIRED src-entry-id
CDATA #IMPLIED >
```

6.4.3 Description du DTD de droits

Le DTD de droits se divise en cinq parties : définition, référence, résultat, requête en cache et informations de référence interne. L'en-tête représente juste un commentaire. Il est facultatif. Dans le DTD, l'en-tête de la définition du droit est le suivant :

```
<!-- Entitlement definition stored in the XmlData attribute of a
DirXML-Entitlement object. -->
```

Les en-têtes sont suivis par des éléments (ELEMENT) et des listes d'attributs (ATTLIST). Voici la description détaillée des éléments et attributs sous l'en-tête de définition du droit, autrement dit du principal en-tête auquel vous devez vous attacher lorsque vous créez des droits.

```
<!ELEMENT entitlement (values?)>
```

L'élément du niveau racine est `<entitlement>`, qui peut contenir un élément `<values>` enfant facultatif et unique. Il est suivi de la liste d'attributs, qui comprend notamment les attributs conflict-resolution (résolution des conflits), display-name (nom d'affichage) et description. L'attribut de résolution des conflits utilise les valeurs d'attribut Priority (Priorité) ou Union.

```
conflict-resolution (priority | union) "priority"
```

Les droits basés sur le rôle utilisent l'attribut de résolution des conflits pour déterminer ce qui doit se passer lorsqu'un droit avec valeur est appliqué plusieurs fois au même objet. Supposons par exemple que l'utilisateur U soit membre de la stratégie de droit A et de la stratégie de droit B, qui contiennent toutes deux le même droit E accompagné d'ensembles de valeurs différents. Le droit E de la stratégie de droit A est associé aux valeurs (a, b, c). Le droit E de la stratégie de droit B, lui, est associé aux valeurs (c, d, e).

L'attribut de résolution des conflits détermine quel ensemble de valeurs doit s'appliquer à l'utilisateur U. S'il est défini sur Union, l'utilisateur U se voit attribuer les deux séries de valeurs (a, b, c, d, e). S'il est défini sur Priority, il ne reçoit que la série de valeurs de la stratégie de droits dotée de la priorité la plus élevée.

Si un droit doit être associé à une seule valeur, les conflits doivent être résolus par priorité, puisque l'attribut Union entraînerait l'application de plusieurs valeurs. Les droits basés sur le rôle utilisent

actuellement cet attribut. Dans le futur, cela pourrait également être le cas des droits basés sur le workflow.

```
display-name CDATA #REQUIRED description CDATA #REQUIRED
```

Le nom littéral du droit ne correspond pas nécessairement au nom affiché par le droit. Les attributs Display-name et Description déterminent ce qui s'affiche pour l'utilisateur final. Dans Designer, une option permet de choisir le nom d'affichage du droit à la place du nom réel.

```
<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-
valued (true | false) "true"
```

L'élément `<values>` est facultatif. Il indique qu'un droit est associé à une valeur. Si vous n'utilisez pas cet élément, le droit est « sans valeur ». Un droit accordant une liste de distribution est un droit avec valeur. Un droit accordant un compte dans une application (par exemple le droit Compte utilisateur fourni avec le pilote Active Directory) est un droit sans valeur.

Les valeurs des droits qui en sont dotés proviennent de trois sources. La première est l'application externe (désignée par l'élément `<query-app>`). La deuxième est une liste prédéfinie de valeurs (un ou plusieurs éléments `<value>`). La troisième est le client de droit (élément `<values>` sans enfant `<value>`. Les exemples fournis vous aideront à comprendre le fonctionnement des valeurs.

Les droits avec valeur peuvent comporter une ou plusieurs valeurs. Par défaut, ils en comptent plusieurs. Le client de droits est chargé d'appliquer cette restriction.

```
<!ELEMENT value (#PCDATA)>
```

Les valeurs des droits sont des chaînes qui ne sont pas saisies.

```
<!ELEMENT query-app (query-xml, result-set)>
```

Si les valeurs proviennent d'une application externe (par exemple, une liste de distribution de messagerie électronique), vous devez spécifier une requête d'application par le biais de l'élément `<query-xml>`. Les résultats de la requête sont extraits par le biais de l'élément `<result-set>`. Vous en trouverez deux exemples à « Exemple 2 : droit de requête d'application : requête externe » page 178.

```
<!ELEMENT query-xml ANY>
```

Les requêtes XML sont au format XDS. La commande `<query-xml>` permet de rechercher et de lire des objets de l'application connectée. Les fonctions des règles DirXML, de migration d'objet, etc., dépendent de l'implémentation de la commande de requête par le pilote. Pour plus d'informations sur les requêtes XML, reportez-vous à la documentation Novell sur les requêtes (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html).

```
<!ELEMENT result-set (display-name, description, ent-value)>
<!ELEMENT display-name(token-attr | token-src-dn | token-
association)> <!ELEMENT ent-value (token-association | token-src-dn
| token-attr)> <!ELEMENT description (token-association | token-
src-dn | token-attr)> <!ELEMENT token-association EMPTY> <!ELEMENT
token-attr EMPTY> <!ATTLIST token-attr attr-name CDATA #REQUIRED
```

Aidez-vous de l'élément result-set (ensemble de résultats) pour interpréter le résultat d'une requête sur l'application externe. Trois éléments de données nous intéressent : le nom d'affichage de la

valeur (élément display-name enfant), la description de la valeur (élément description enfant) et la valeur littérale du droit (élément ent-value enfant), qui ne s'affiche pas.

Les éléments jetons `<token-src-dn>`, `<token-association>` et `<token-attr>` sont en fait des marques de réserve pour les expressions XPATH chargées d'extraire respectivement la valeur de l'attribut src-dn, la valeur de l'association ou toute valeur d'attribut provenant d'un document XML au format XDS. Le DTD part de l'hypothèse que le résultat de la requête est au format XDS.

Autres en-têtes dans le DTD

Les autres en-têtes de droits du DTD de droits ont différentes fonctions, mais vous n'avez pas besoin de vous y attarder lorsque vous créez un droit.

```
<!-- Entitlement reference stored in the DirXML-EntitlementRef
attribute of a DirXML-EntitlementRecipient or a DirXML-
SharedProfile object. -->
```

Les informations enregistrées dans la section Entitlement Reference (Référence de droit) du DTD renvoient à un objet Droit. Ces informations sont placées là par l'agent de gestion (par exemple, le pilote de droits basés sur le rôle, `Entitlement.xml`, ou le pilote du flux d'approbation, `UserApplication.xml`). L'événement déclenche une opération dans un système connecté. Vous n'avez rien de spécial à faire sous cet en-tête du DTD, mais vous pouvez utiliser les informations correspondantes pour vous assurer que l'objet Droit est bien référencé.

```
<!-- Entitlement result stored in the DirXML-EntitlementResult
attribute of a DirXML-EntitlementRecipient object. -->
```

La section Entitlement Result (Résultat du droit) indique le résultat (accord ou révocation d'un droit). Elle précise l'état de l'événement et, à l'aide d'un tampon horaire, le moment où l'événement est accordé ou révoqué. Vous n'avez rien de spécial à faire sur les éléments et attributs qui figurent sous cet en-tête.

```
<!-- Cached query results stored in the DirXML-SPCachedQuery
attribute of a DirXML-Entitlement object. -->
```

La section Entitlement Query (Requête de droit) contient les valeurs du droit recueillies à partir d'une application externe. Ces informations peuvent ensuite être réutilisées si le client de droits a besoin de les afficher. Ces valeurs sont enregistrées dans l'attribut `DirXML-SPCachedQuery` de l'objet Droit. Vous n'avez rien de spécial à faire sur les éléments et attributs qui figurent sous cet en-tête.

```
<!-- Representation of a DirXML-EntitlementRef within the DirXML
Script and within the operation-data of an operation in an XDS
document. -->
```

Comme le DTD définit des valeurs pour plusieurs documents, la section EntitlementRef ne fait pas vraiment partie de la définition du droit. Vous n'avez rien de spécial à faire sur les éléments et attributs qui figurent sous cet en-tête.

6.4.4 Création de droits dans Designer

Les exemples de la Section 6.4.5, « Création et modification de droits dans iManager », page 177 présentent le code XML utilisé pour rédiger des droits, mais il est beaucoup plus facile de se servir

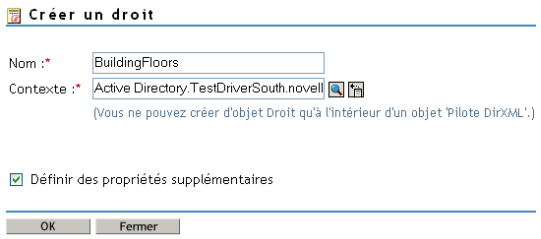
de l'utilitaire Designer fourni avec Identity Manager. Une fois que vous avez ajouté un pilote Identity Manager à un coffre-fort d'identité dans l'espace Modeler du Designer, vous pouvez cliquer sur ce pilote avec le bouton droit de la souris dans la vue Outline (Aperçu) et sélectionner Ajouter un droit. L'assistant de création de droits vous invite à indiquer le type de droit souhaité, puis il vous guide tout au long du processus de création.

Pour plus d'informations sur l'utilisation de l'assistant de création de droits, reportez-vous au manuel Designer for Identity Manager 3: Administration Guide (Guide d'administration de Designer pour Identity Manager 3).

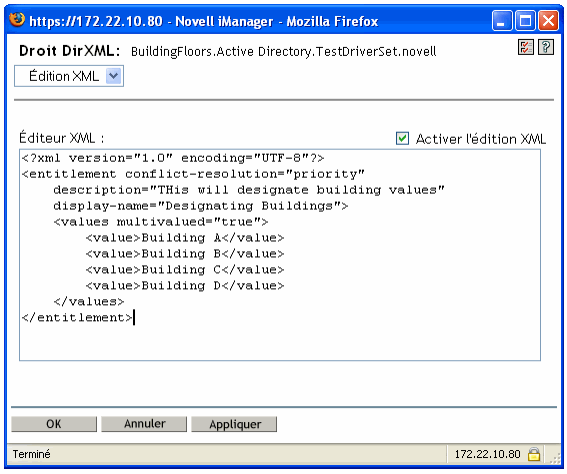
6.4.5 Création et modification de droits dans iManager

Il est conseillé d'utiliser l'assistant de création de droits de Designer pour créer des droits, mais vous pouvez également le faire dans iManager.

1. Sélectionnez l'option Créer un droit sous l'en-tête Utilitaires Identity Manager.
2. Sur la page Créer un droit, saisissez le nom que vous souhaitez donner au droit, puis utilisez le Navigateur d'objet pour trouver l'objet Pilote Identity Manager auquel appartient le droit.



3. Si l'option Définir des propriétés supplémentaires est sélectionnée, la page Éditeur XML s'affiche. Vous pouvez y définir les éléments souhaités.



4. Cochez la case Activer l'édition XML pour ajouter vos éléments au droit.

Remarque : il est fortement déconseillé de changer le nom d'un droit. Si vous le faites, vous devez également changer toutes les références à ce droit dans les stratégies qui l'implémentent. Le nom du droit est enregistré dans les attributs Ref et Result de la stratégie.

6.4.6 Modèles de droits

Vous pouvez créer deux types de droits : avec ou sans valeur. Les droits avec valeurs peuvent tirer celles-ci d'une requête externe, d'une liste définie par l'administrateur ou de valeurs de forme libre. Vous trouverez ci-après des exemples des quatre types de droits que vous pouvez créer.

Remarque : si une ligne ne commence pas par le signe Inférieur à (<), un retour à la ligne a été effectué alors que l'information est généralement affichée sur une ligne et non deux, voire trois. Vous devez également vous rappeler qu'à l'exception des droits du compte, il ne s'agit là que d'exemples des différents types de droits avec valeurs que vous pouvez créer.

Exemple 1 : droits du compte : sans valeur

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="priority"
    description="This is an Account Entitlement"
    display-name="Account Entitlement"/>
```

Dans cet exemple, le nom du droit sans valeur est Account. Il est suivi de la ligne conflict-resolution, avec l'attribut par défaut (Priority), qui signifie généralement que si le droit est utilisé par les droits basés sur le rôle, celui qui a la priorité la plus élevée détermine la valeur retenue. Toutefois, comme il s'agit d'un exemple de droit sans valeur, les paramètres de valeur ne s'appliquent pas. Le droit a pour description « This is an Account Entitlement », et pour nom d'affichage Account Entitlement. Ces informations sont suffisantes pour créer un droit de compte utilisable pour accorder un compte dans une application.

Le pilote Active Directory, comporte un droit UserAccount qui lui sert à accorder ou révoquer les comptes utilisateur.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
      description="The User Account entitlement grants or denies an
      account in ActiveDirectory for the user. When granted, the user
      is given an enabled logon account.When revoked, the logon
      account is either disabled or deleted depending on how the drive
      is configured."display-name="User Account Entitlement"
name="UserAccount">
</entitlement>
```

Dans cet exemple, le paramètre de résolution des conflits est Union. Il permet au droit de fusionner les valeurs assignées. Encore une fois, les paramètres avec valeur ne s'appliquent pas aux droits sans valeur. Le champ Description explique le rôle du droit et la raison de sa création. Ces informations seront utiles en cas de modification ultérieure du droit. Le nom effectif du droit est UserAccount, mais le `<display-name>` affiche User Account Entitlement dans l'agent de gestion.

Exemple 2 : droit de requête d'application : requête externe

Les droits Groupe et Boîte aux lettres Exchange fournis avec les pilotes Active Directory avec droits activés proposent des exemples de requêtes d'application. Utilisez ces droits lorsque vous avez besoin d'informations externes en provenance d'un système connecté pour réaliser un événement.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
   description="The Group Entitlement grants or denies membership in
   a group in Active Directory. The group must be associated with a
   group in the Identity Vault. When revoked, the user is removed from
   the group. The group membership entitlement is not enforced on the
   publisher channel: If a user is added to a controlled group in
   Active Directory by some external tool, the user is not removed by
   the driver. Further, if the entitlement is removed from the user
  object instead of being simply revoked, the driver takes no action."
display-name="Group Membership Entitlement" name="Group">
   <values>
      <query-app>
         <query-xml>
            <nds dtd-version="2.0">
               <input>
                  <query class-name="Group"
                     scope="subtree">
                     <search-class class-name="Group"/>
                     <read-attr attr-name="Description"/>
                  </query>
               </input>
            </nds>
         </query-xml>
         <result-set>
            <display-name>
                <token-src-dn/>
            </display-name>
            <description>
               <token-attr attr-name="Description"/>
            </description>
            <ent-value>
               <token-association/>
            </ent-value>
         </result-set>
      </query-app>
   </values>
</entitlement>
```

Dans cet exemple, le droit Groupe utilise le paramètre Union pour résoudre les conflits si le droit est appliqué plusieurs fois au même objet. Cet attribut fusionne les droits de toutes les stratégies de droits basés sur le rôle concernées. Si une stratégie révoque un droit alors qu'une autre l'accorde, le droit est finalement accordé.

La description, très détaillée, précise les éléments configurés par le biais des règles des stratégies du pilote. Cette description est un bon exemple du niveau de détail à fournir lors de la première définition d'un droit.

Le `<display-name>` est Group Membership Entitlement. Il apparaît dans les agents de gestion, par exemple iManager, pour les droits basés sur le rôle. Le nom est le Nom distinctif relatif (RDN) du droit. Si vous ne définissez pas de nom d'affichage, le RDN est utilisé.

Les valeurs de requête initiales cherchent le nom de classe du Groupe en haut de l'arborescence et continuent dans les arborescences secondaires. Ces valeurs sont issues du serveur Active Directory connecté. La requête de l'application démarre à la balise <nds>. Sous la balise <query-xml>, cette requête reçoit des informations de ce type :

```
<instance class-name="Group" src-dn="o=Blanston,cn=group1">
   <association>o=Blanston,cn=group1</association>
   <attr attr-name="Description"> the description for group1</attr>
</instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group2">
   <association>o=Blanston,cn=group2</association>
   <attr attr-name="Description"> the description for group2</attr>
</instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group3">
   <association>o=Blanston, cn=group3</association>
   <attr attr-name="Description"> the description for group3</attr>
</instance>
<!-- ... ->
```

Ensuite, sous la balise <result-set>, les informations obtenues par la requête renseignent les différents champs. Dans notre exemple, le champ <display-name> indiquerait o=Blanston,cn=group1. Le champ <description> indiquerait the description for group1 (description du groupe 1), et le champ <ent-value> indiquerait o=Blanston,cn=group1. Comme il existe plusieurs groupes répondant aux critères de la requête, ces informations sont également recueillies et affichées pour d'autres instances.

Remarque : la valeur du format d'association est unique pour chaque système externe. Aussi le format et la syntaxe sont-ils différents pour chaque système externe interrogé.

Le droit Boîte aux lettres Exchange est un autre exemple de droit.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
  description="The Exchange Mailbox Entitlement grants or denies an
  Exchange mailbox for the user in Microsoft Exchange."
  display-name="Exchange Mailbox Entitlement" name="ExchangeMailbox">
  <values>
      <query-app>
         <query-xml>
            <nds dtd-version="2.0">
               <input>
                  <query class-name="msExchPrivateMDB"
                     dest-dn="CN=Configuration," scope="subtree">
                     <search-class class-name="msExchPrivateMDB"/>
                     <read-attr attr-name="Description"/>
                     <read-attr attr-name="CN"/>
                  </query>
               </input>
            </nds>
          </query-xml>
          <result-set>
            <display-name>
```

```
            <token-attr attr-name="CN"/>
          </display-name>
          <description>
            <token-attr attr-name="Description"/>
          </description>
          <ent-value>
            <token-src-dn/>
          </ent-value>
        </result-set>
      </query-app>
   </values>
</entitlement>
```

Dans cet exemple, le droit Boîte aux lettres Exchange utilise le paramètre Union pour résoudre les conflits si le droit est appliqué plusieurs fois au même objet. Cet attribut fusionne les droits de toutes les stratégies de droits basés sur le rôle concernées. Si une stratégie révoque un droit alors qu'une autre l'accorde, le droit est finalement accordé.

La description indique que le droit accorde à l'utilisateur une boîte aux lettres dans Microsoft Exchange ou la révoque. Cette description est suffisamment détaillée pour le rôle du droit. Le display-name est Exchange Mailbox Entitlement. Il apparaît dans les agents de gestion, par exemple iManager, pour les droits basés sur le rôle. Le nom est le Nom distinctif relatif (RDN) du droit. Si vous ne définissez pas de nom d'affichage, le RDN est utilisé.

Les valeurs de requête initiales cherchent le nom de classe de msExchPrivateMDB, un appel fonction qui commence la recherche dans le conteneur Configuration et la poursuit dans les arborescences secondaires. Ces valeurs sont issues de la base de données Active Directory connectée. La requête de l'application démarre à la balise `<nds>`. La classe msExchPrivateMDB n'a pas d'équivalent dans eDirectory. Vous devez donc bien connaître les appels de fonction Microsoft Exchange pour effectuer ce type de requête. Mais la requête est achevée grâce aux règles et stratégies du pilote Active Directory.

Les consommateurs de droits utilisent les informations récupérées par la requête. Par exemple, la valeur du droit (ent-value) est transmise aux stratégies Identity Manager par le biais de l'attribut DirXML-EntitlementRef. Le nom d'affichage et la description sont affichés par iManager ou par l'application utilisateur. Ils sont enregistrés dans l'attribut DirXML-SPCachedQuery.

Exemple 3 : droit défini par l'administrateur : avec listes

Ce troisième exemple concerne un droit défini par l'administrateur qui accorde ou révoque un événement après sélection d'un élément dans une liste.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="union"
    description="This will show Administrator-defined Values">
         <display-name="Admin-defined Entitlement"/>
         <values multi-valued="true">
            <value>Building A</value>
            <value>Building B</value>
            <value>Building C</value>
            <value>Building D</value>
            <value>Building E</value>
            <value>Building F</value>
```

```
      </values>
</entitlement>
```

Dans cet exemple, le nom du droit est Admin-defined, avec le nom d'affichage défini Admin-defined Entitlement. Vous pouvez indiquer uniquement le nom d'affichage si vous souhaitez qu'il soit différent du RDN du droit. La ligne de résolution des conflits contient le paramètre Union, qui permet au droit de fusionner les valeurs assignées.

La description du droit est la suivante : *This will show Administrator-defined Values* (Cela affichera les valeurs définies par l'administrateur). L'attribut multi-value (valeurs multiples) est défini sur true (vrai), ce qui permet au droit d'assigner plusieurs fois une valeur. Dans cet exemple, les valeurs correspondent aux lettres des bâtiments de la société, du bâtiment A au bâtiment F. Puis, à travers un client de droits, par exemple une tâche RBE de iManager ou de l'application utilisateur, les utilisateurs ou les responsables des tâches définies peuvent spécifier les informations sur le bâtiment, qui sont ensuite intégrées à l'application externe, par exemple Novell eDirectory.

Exemple 4 : droits définis par l'administrateur : sans liste

Le quatrième exemple représente un droit défini par l'administrateur qui oblige ce dernier à saisir une valeur pour que le droit puisse accorder ou révoquer un événement. Vous pouvez utiliser ce type de droit si vous ne disposez pas de toutes les informations nécessaires au moment de la configuration initiale et si vous ne pouvez donc pas créer de liste de tâches.

```
<?xml version="1.0" encoding="UTF-8"?>
<entitlement conflict-resolution="priority"
    description="There will be no pre-defined list">
    <values multi-valued="false"/>
</entitlement>
```

Dans cet exemple, le droit a pour nom Admin-defined (no list). Le nom du droit est utilisé comme nom d'affichage, ce dernier n'étant pas spécifié. Cette fois encore, le paramètre de résolution des conflits par défaut (Priority) est défini : si le droit est utilisé par les droits basés sur le rôle, celui qui a la priorité la plus élevée détermine la valeur. Vous spécifiez les informations sur le bâtiment par le biais d'un client de droits, par exemple une tâche RBE de iManager ou l'application utilisateur. Ces informations sont ensuite intégrées à l'application externe, par exemple eDirectory.

6.4.7 Dernières étapes de la procédure de création de droits

Les exemples de création de droits fournis plus haut illustrent les deux premières étapes de la procédure de création et d'utilisation de droits décrites à la Section 6.2, « Création de droits : présentation », page 164. Il y a d'abord l'étape 1, qui consiste à établir la liste des exigences auxquelles doit répondre le droit, et l'étape 2, qui consiste à rédiger le droit de telle sorte qu'il réponde aux exigences définies dans cette liste. L'étape 3, la création de stratégies pour le pilote Identity Manager, n'est pas décrite dans ce chapitre. Pour plus d'informations sur la création et la modification de stratégies, reportez-vous au *Policy Builder and Driver Customization Guide (Guide de création des stratégies et de personnalisation des pilotes)* et au guide du pilote Identity Manager (http://www.novell.com/documentation/idmdrivers/index.html) concerné.

Une fois que vous avez créé des droits (ou utilisé les droits préconfigurés fournis avec certains pilotes Identity Manager), vous devez les gérer, à l'étape 4. Les droits sont gérés par deux ensembles ou agents : via les stratégies de droits basés sur les rôles de iManager, ou via l'application utilisateur, dans le provisioning basé sur le workflow. Pour les droits utilisés dans le provisioning basé sur le

workflow, reportez-vous à la Section V : Conception et gestion des demandes de provisioning du Guide d'administration de l'application utilisateur de Identity Manager. Le reste de ce chapitre traite essentiellement des droits basés sur le rôle.

6.5 Présentation de la gestion des droits basés sur le rôle

Les droits sur les systèmes connectés sont habituellement administrés pilote par pilote ; il suffit de créer et de modifier les stratégies de configuration des pilotes, telles que celles créées avec le Générateur de stratégies. Selon ce modèle distribué traditionnel, un administrateur différent contrôle souvent chaque pilote Identity Manager et chaque système connecté ; les stratégies d'entreprise qui déterminent si un utilisateur a le droit ou non d'accéder aux ressources de ce système sont « codées en dur » séparément dans les stratégies de configuration des pilotes de chaque système connecté.

Le modèle de droits basés sur le rôle est particulièrement adapté à un environnement dans lequel un seul administrateur, ou un petit nombre d'entre eux, est chargé du contrôle des stratégies de droit. Un tel administrateur doit connaître Identity Manager dans sa globalité, mais n'est pas obligé de maîtriser parfaitement les scripts DirXML, Identity Manager ou XSLT pour utiliser l'interface des droits basés sur le rôle.

Les stratégies de droits en fonction des rôles permettent d'accorder ou de révoquer automatiquement des ressources d'entreprise, si les critères définis sont remplis. Les droits peuvent être comparés à une feuille d'autorisation donnant accès à une ressource. Avec cette feuille d'autorisation, vous pouvez accéder à la ressource spécifiée. Sans elle, vous ne le pouvez pas. Par exemple, spécifiez que si l'utilisateur remplit les critères 1, 2 et 3, il devient, aux termes d'une stratégie de droits basés sur le rôle, membre du groupe H. En revanche, s'il remplit les critères 4 et 5, il devient membre du groupe I.

Le paramétrage pour la gestion des droits basés sur le rôle se fait en trois étapes :

1. Si ce n'est pas déjà fait, activez l'attribut DirXML-EntitlementRef de l'objet Pilote Identity Manager, comme indiqué à la Section 6.2.2, « Activation des droits sur les autres pilotes Identity Manager », page 166.
2. Installez le pilote de service de droits (`Entitlement.xml`), comme indiqué à la Section 6.6, « Création d'un objet Pilote de service de droits », page 184.
3. Créez des stratégies de droits basés sur le rôle dans iManager, comme indiqué à la Section 6.7, « Création de stratégies de droits », page 186.

6.5.1 Fonctionnement du pilote de service de droits

Les droits basés sur le rôle s'appuient sur le pilote de service de droits (`Entitlement.xml`). Il s'agit d'un service de moteur qui contrôle si les utilisateurs sont membres d'une stratégie de droit. Si un utilisateur satisfait aux critères d'appartenance à un groupe dynamique de stratégies de droits ou est inclus de manière statique, le pilote de service de droits met à jour les informations dans l'attribut DirXML-EntitlementRef sur l'objet Utilisateur.

Pour les systèmes répertoriés à la Section 6.2.1, « Pilotes Identity Manager dotés de préconfigurations prenant en charge les droits », page 165, vous pouvez activer les droits au moment de l'importation de la configuration du pilote Identity Manager. Identity Manager est fourni avec un certain nombre de pilotes dotés de préconfigurations contenant déjà des droits et des stratégies

permettant de les implémenter. Le pilote est activé pour écouter les activités liées aux droits. Vous pouvez ensuite revoir les stratégies fournies. Pour appliquer les droits, ces stratégies vérifient l'attribut DirXML-EntitlementRef et accordent ou révoquent des droits.

Le pilote de service de droits met à jour l'attribut DirXML-EntitlementRef uniquement dans les cas suivants :

- Vous utilisez la tâche Réévaluer les membres.
- Vous spécifiez dans quelle partie de l'arborescence les utilisateurs doivent être réévalués.
- Un utilisateur est déplacé.
- Un utilisateur est renommé.
- Un attribut utilisé pour l'appartenance à une stratégie de droit est modifié.

Les stratégies de droit permettent d'accorder des droits sur les systèmes connectés et dans le coffre-fort d'identité. Les droits disponibles sur les systèmes connectés sont les suivants :

- Comptes
- Appartenance aux listes de distribution de courrier électronique
- Appartenance à un groupe
- Attributs pour les objets correspondants des systèmes connectés, peuplés avec les valeurs que vous spécifiez
- Placement
- Autres droits que vous personnalisez

Certaines des options qui peuvent être créées avec les droits figurent dans les configurations des pilotes dans lesquels les droits sont activés.

Un seul pilote de service de droits étant utilisé pour chaque ensemble de pilotes, une stratégie de droit ne peut gérer que les utilisateurs qui sont dans une réplique principale ou en lecture/écriture sur le serveur associé à cet ensemble de pilotes.

La fonctionnalité des stratégies de droits basés sur le rôle s'appuie sur Identity Manager. Pour administrer les systèmes connectés, vous devez donc d'abord installer les pilotes et les plugs-in Identity Manager avant de configurer correctement les pilotes.

Par ailleurs, pour éviter d'éventuels conflits entre les stratégies de droit attribuées et les configurations de pilotes Identity Manager, vous devez connaître vos stratégies d'entreprise et savoir comment elles sont administrées dans Identity Manager. Lorsqu'elles gèrent un attribut, les stratégies de droit Identity Manager et celles qui figurent dans une configuration de pilote ne doivent pas se chevaucher ni entrer en conflit.

6.6 Création d'un objet Pilote de service de droits

Pour créer des stratégies de droits, vous avez besoin d'un objet Pilote de service de droits. Vous devez en créer un pour chaque ensemble de pilotes.

Si vous n'en avez pas encore, vous êtes invité à créer cet objet lorsque vous cliquez sur la tâche et le rôle des droits basés sur le rôle.

1. Vérifiez si vous disposez déjà d'un pilote de service de droits.

Dans iManager, cliquez sur *Droits basés sur le rôle* > *Droits basés sur le rôle*, puis sélectionnez l'ensemble de pilotes.

- Si la page Aucun pilote de service de droits s'affiche, passez à l'Étape 2 pour créer un objet Pilote de service de droits.
- Si une page Droits basés sur le rôle s'affiche avec une liste des stratégies de droits, vous disposez déjà d'un objet Pilote de service de droits. Vous n'avez alors pas besoin de terminer cette procédure. Passez à la Section 6.7, « Création de stratégies de droits », page 186.

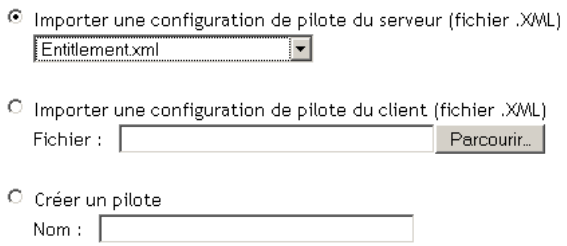
2 Sur la page Aucun pilote de service de droits, cliquez sur *Oui*.

L'assistant de création d'un pilote s'ouvre.

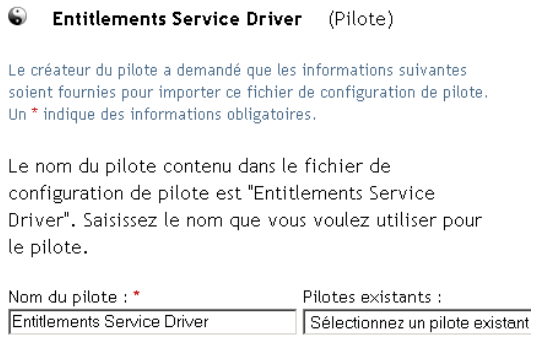
Vous pouvez également cliquer sur *Utilitaires DirXML* > *Importer des pilotes*.

3 Sur la page Assistant de création d'un pilote, sélectionnez *Dans un ensemble de pilotes existant*, puis cliquez sur *Suivant*.

4 Dans la liste déroulante *Importer une configuration de pilote du serveur (fichier .XML)* sélectionnez *Entitlement.xml*.



5 Nommez l'objet Pilote de service de droits (ou acceptez le nom par défaut), puis cliquez sur *Suivant*.



Le bon fichier de configuration de pilote est automatiquement choisi. Il suffit de spécifier un nom pour l'objet Pilote ou d'utiliser le nom par défaut.

6 Nous vous recommandons de définir des équivalences de sécurité et d'exclure les rôles administratifs. Ajoutez l'utilisateur Admin à ces deux sélections, puis cliquez sur *Suivant*.

7 Lisez le résumé puis cliquez sur *Terminer*.

Le module d'interface pilote pour le pilote de droits est installé par défaut lors de l'installation de Identity Manager. Le fichier de configuration du pilote de droits est installé par défaut au moment de l'installation des plug-ins Identity Manager sur le serveur iManager.

Une fois les étapes de l'assistant terminées, vous pouvez accéder aux plugs-in pour les droits et commencer à créer des stratégies de droits basés sur le rôle pour l'ensemble de pilotes.

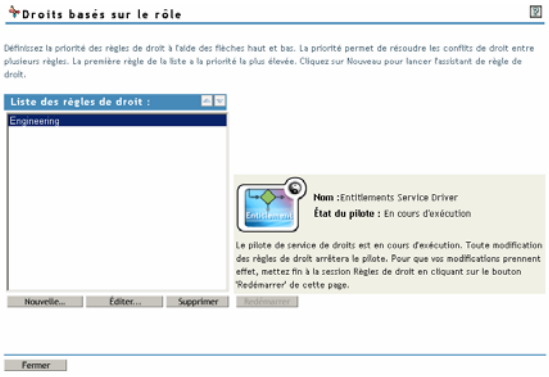
6.7 Création de stratégies de droits

Utilisez l'assistant fourni pour créer une stratégie de droit.

1. Vérifiez que vous avez configuré le pilote de service de droits et que vous avez créé les configurations de pilote nécessaires.
2. Dans iManager, cliquez sur *Droits basés sur le rôle* > *Droits basés sur le rôle*.
3. Sélectionnez un ensemble de pilotes

   Chaque ensemble de pilotes possède ses propres stratégies de droits.

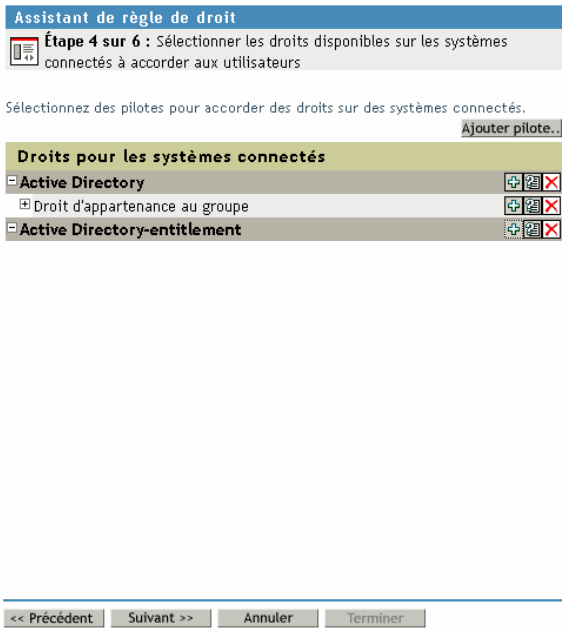
   La liste des stratégies de droits existantes s'ouvre, comme sur la page illustrée ci-après. Si vous utilisez les droits basés sur le rôle pour la première fois, aucune règle ne figure dans la liste.



4. Cliquez sur *Nouveau*.

   L'*Assistant de stratégie de droit* s'ouvre.
5. Suivez les étapes 1 à 6 de l'assistant pour créer une nouvelle stratégie. Reportez-vous à l'aide en ligne pour plu d'informations sur chaque étape de l'assistant.
   - **5a** À l'étape 1, spécifiez le nom et la description de la stratégie.
   - **5b** À l'étape 2, définissez le filtre d'appartenance et les paramètres de recherche.
   - **5c** À l'étape 3, définissez les membres statiques. Vous devez pour cela inclure des membres dans les critères de recherche et en exclure.
   - **5d** À l'étape 4, sélectionnez un pilote Identity Manager et indiquez les droits à inclure. Pour créer des droits, reportez-vous à la Section 6.4, « Rédaction de droits en langage XML

dans iManager », page 168. Cliquez sur *Ajouter un pilote*, puis sélectionnez le droit à ajouter.



5e À l'étape 5, localisez les objets dont vous souhaitez que la stratégie de droits soit un ayant droit.

5f À l'étape 6, lisez le résumé pour vous assurer que la stratégie de droits a bien le rôle souhaité. Si tel le cas, cliquez sur *Terminer*. Sinon, cliquez sur *Précédent*.

6 Le processus de création de la stratégie de droit éteint le pilote de service de droits. Cliquez sur *Redémarrer* pour terminer la session.

6.7.1 Définition de l'appartenance à un groupe pour une stratégie de droit

Comme les pilotes Identity Manager, une stratégie de droit ne peut gérer que les objets présents dans une réplique maîtresse ou en lecture/écriture sur le serveur correspondant. Chaque stratégie de droit est associée à un seul objet Ensemble de pilotes, lui-même affecté à un serveur donné.

Seuls les objets Utilisateur (et d'autres types d'objets dérivés de la classe Utilisateur) peuvent être membres d'une stratégie de droit. Pour ouvrir la page Membres d'une stratégie de droits, sélectionnez *Droits basés sur le rôle* > *Droits basés sur le rôle*, puis mettez en surbrillance la stratégie de droits à modifier dans la liste des stratégies de droit et sélectionnez l'option *Éditer*. Dans Internet Explorer, sélectionnez l'onglet *Membres* ; dans le navigateur Firefox, sélectionnez Éditer les membres dynamiques dans le menu déroulant.

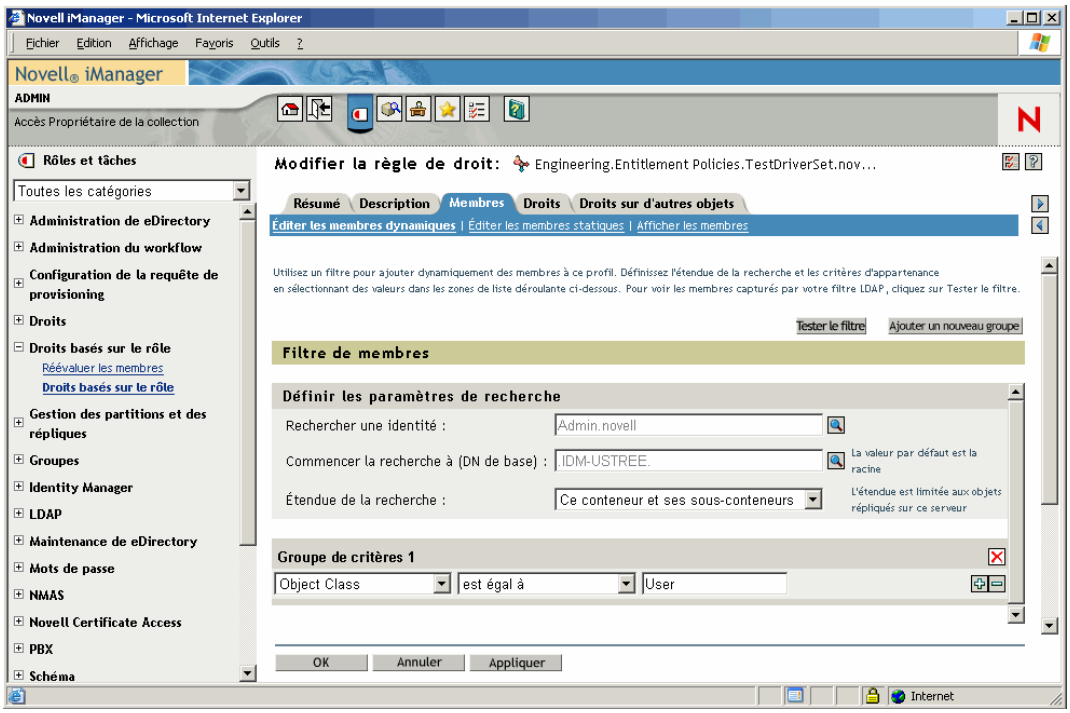
Une stratégie de droit est un objet de groupe dynamique. Les membres d'une stratégie de droit peuvent être définis selon deux méthodes, dynamique ou statique. Les deux méthodes peuvent être utilisées dans une même stratégie de droit.

- **Dynamique :** vous pouvez définir des critères d'appartenance à un groupe fondés sur les valeurs des attributs de l'objet, par exemple si l'appellation d'emploi doit ou non contenir le terme Responsable. Les critères que vous spécifiez sont convertis en un filtre LDAP.

Les utilisateurs qui répondent aux critères choisis appartiennent automatiquement à la stratégie de droit. Vous n'avez pas à les ajouter un par un. La sélection dynamique de membres revient à définir un objet Groupe dynamique.

Si un objet est modifié et ne satisfait alors plus aux critères d'appartenance à un groupe dynamique, ses droits sont automatiquement supprimés.

Figure 6-2 *Édition des membres dynamiques et statiques*



- **Statique :** outre la création de critères pour l'appartenance à un groupe dynamique (un filtre LDAP), vous pouvez inclure ou exclure des utilisateurs.

  Vous pouvez ajouter statiquement des membres qui ne satisfont pas aux critères du filtre. Vous pouvez exclure des membres qui satisfont aux critères du filtre mais qui ne doivent pas être inclus dans la stratégie de droit.

6.7.2 Choix des droits pour une stratégie de droit

- « Comptes sur les systèmes connectés » page 189
- « Appartenance à des listes de distribution de courrier électronique et des listes NOS » page 190
- « Valeurs d'attribut sur les systèmes connectés » page 191

Les droits permettent d'accorder ou de révoquer l'accès aux services des systèmes connectés et des droits dans le coffre-fort d'identité.

Les pilotes installés avec les droits activés sont fournis avec une liste de droits qui peuvent être attribués à l'aide d'une stratégie de droit. Vous pouvez également créer vos propres droits utilisables

dans une stratégie de droit. Les droits que le pilote peut fournir sont des objets enfants du pilote, créé par le développeur pour représenter les fonctions du pilote et du système connecté.

Des droits d'ayant droit sur les objets du coffre-fort d'identité sont immédiatement accordés aux membres de la stratégie de droit. Par défaut, les droits dans les systèmes connectés sont accordés à chaque membre de la stratégie de droit lors de la modification pour cet utilisateur d'un attribut utilisé pour l'appartenance à la stratégie de droit, ou lorsqu'un utilisateur est déplacé dans un autre conteneur ou renommé.

Les droits disponibles sur les systèmes connectés sont les suivants :

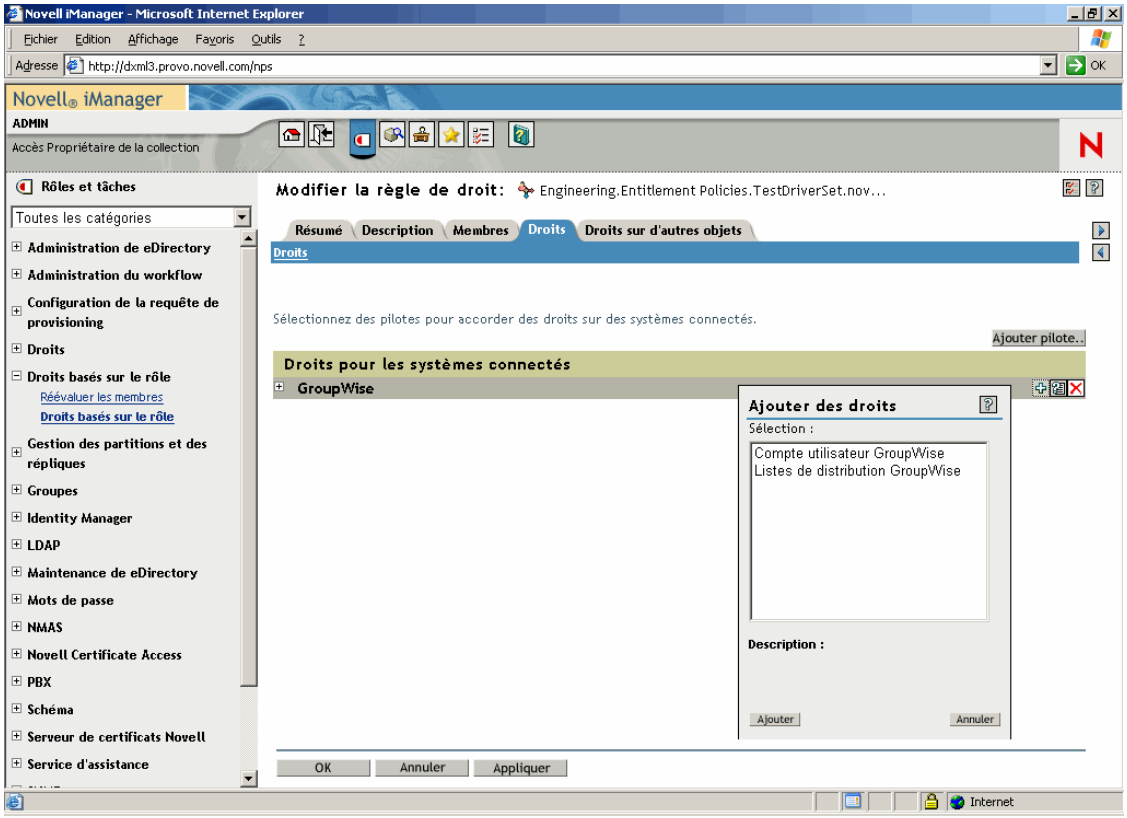
- Comptes
- Appartenance aux listes de distribution de courrier électronique
- Appartenance à des listes NOS
- Attributs pour les objets correspondants des systèmes connectés, peuplés avec les valeurs que vous spécifiez
- Autres droits que vous personnalisez

Comptes sur les systèmes connectés

Pour ajouter des droits à une stratégie de droit, allez sur la page Droits, puis sélectionnez un pilote. Une fenêtre contextuelle indiquant les droits proposés par ce pilote s'affiche.

Ainsi, sur la capture suivante, deux sortes de droits sont proposés par un pilote GroupWise, le premier dans la liste étant un compte utilisateur GroupWise.

Figure 6-3 *Interface de définition des droits*

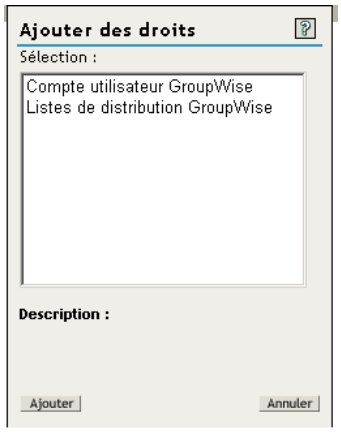


Appartenance à des listes de distribution de courrier électronique et des listes NOS

Pour assigner une appartenance à des groupes sur des systèmes connectés, choisissez le droit d'appartenance dans la liste des droits proposés par un pilote.

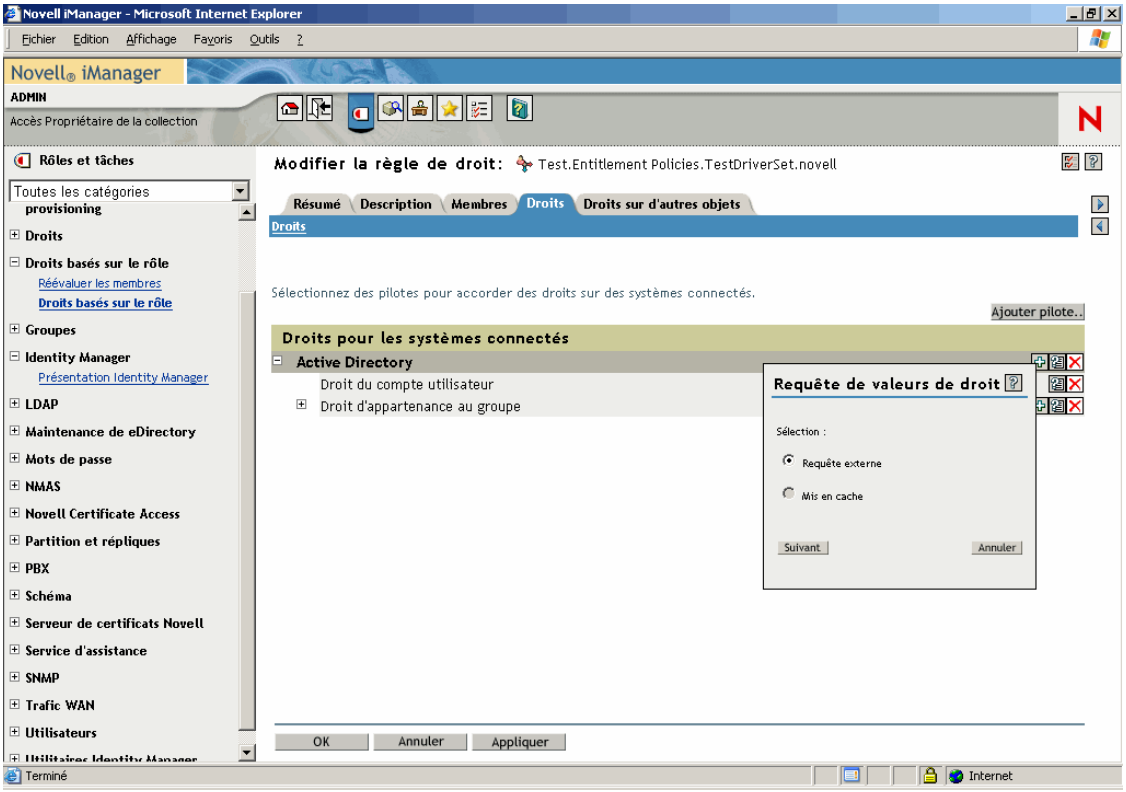
La capture suivante présente un exemple, les listes de distribution GroupWise figurant en deuxième position dans la liste.

Figure 6-4 *Sélection de listes de distribution GroupWise*



Si, dans cet exemple, vous choisissez *Listes de distribution GroupWise*, une fenêtre contextuelle de requête s'affiche, comme illustré à la capture suivante.

Figure 6-5 *Requêtes de valeurs de droits*



L'interface de stratégie de droit permet de lancer une requête afin d'obtenir une liste de distribution de courrier électronique ou des listes NOS. Une fois la requête effectuée, vous pouvez choisir de consulter la liste mise en cache.

Les pilotes sont configurés pour renvoyer la liste complète afin que vous puissiez faire votre choix dans la liste qui se trouve sur le système connecté.

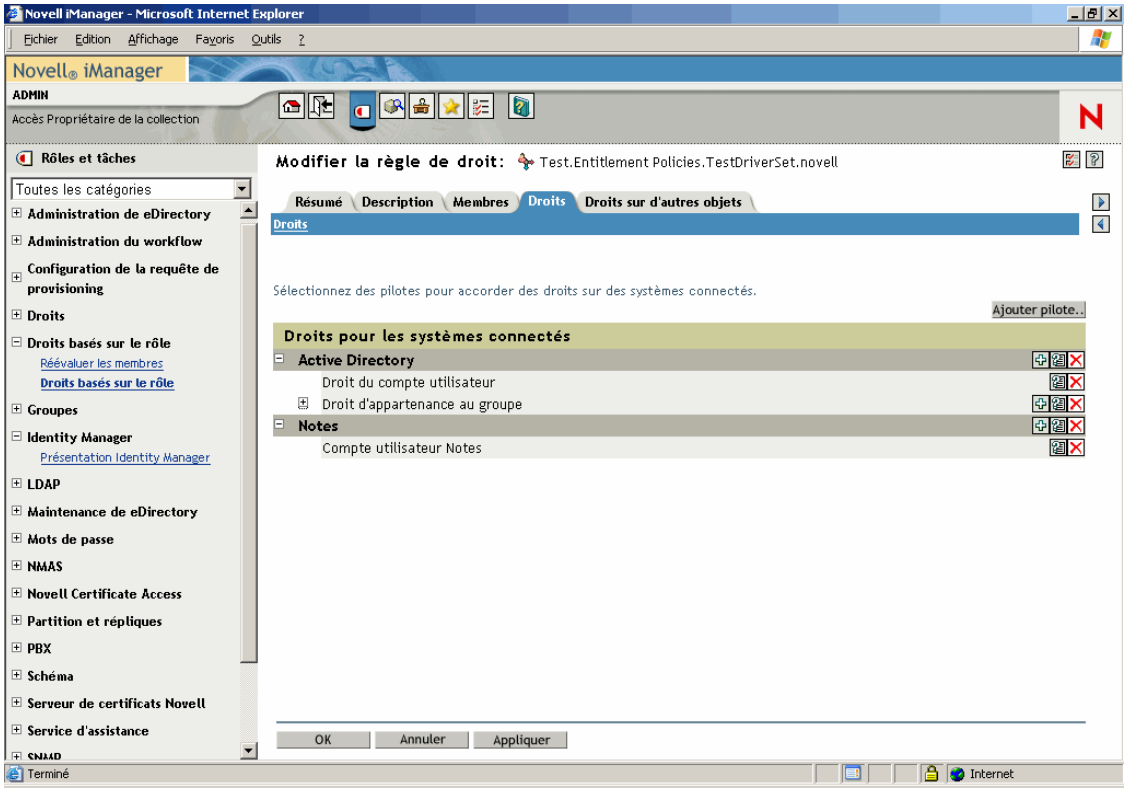
Remarque : vous pouvez personnaliser un pilote pour limiter la liste aux noms de groupes spécifiés plutôt que d'utiliser une requête qui renvoie la liste complète.

Valeurs d'attribut sur les systèmes connectés

Vous pouvez assigner des valeurs d'attribut aux comptes utilisateur sur les systèmes connectés. L'interface permet de saisir la valeur que vous souhaitez attribuer aux comptes utilisateur.

La capture suivante présente un exemple d'ajout d'une valeur d'attribut pour un attribut Notes, Service.

Figure 6-6 *Ajout d'une valeur d'attribut*



6.8 Résolution des conflits entre les stratégies de droits basés sur le rôle

6.8.1 Présentation des conflits

Lorsque vous créez des stratégies de droits, il se peut que les stratégies qui concernent un utilisateur donné soient en conflit avec l'assignation de droits à ce même utilisateur.

Procédez de la manière suivante pour résoudre ces conflits. Pour certains droits, vous pouvez modifier la résolution de conflit.

- **Les droits qui ne sont pas associés à des valeurs s'ajoutent.** Dans la plupart des cas, les droits sur les comptes ne comportent pas de valeur. Si une stratégie de droit accorde à un utilisateur un compte sur un système connecté, cet utilisateur obtient ce compte. Peu importe s'il y a un conflit avec une autre stratégie de droit ; le résultat s'ajoute.

Cela est toujours le cas ; il n'est pas possible de modifier la méthode de résolution de conflit pour l'attribution de comptes.

Les droits n'ayant pas de valeur peuvent être comparés à un interrupteur ; ils sont soit activés soit désactivés, c'est-à-dire accordés ou non.

Ainsi, si la stratégie de droit Responsable attribue à Jean Chandler un compte Exchange mais si cet utilisateur est exclu de la stratégie de droit des employés du service courrier qui attribue également des comptes Exchange, Jean reçoit quand même un compte Exchange.

- **Les droits qui ont des valeurs s'ajoutent par défaut, mais vous pouvez choisir de les résoudre par priorité.** Les droits tels que l'appartenance à un groupe sont associés à une liste de noms de groupes pour les valeurs, ou à un attribut doté d'une valeur. Par défaut, ce type de droits s'ajoute également.

  Si vous le souhaitez, vous pouvez modifier la méthode de résolution des conflits pour ce type de droits.

  Le paramètre qui commande la résolution des conflits pour chaque droit est défini dans le droit en question. Chaque type de droit offert par un pilote figure séparément dans le manifeste. Les droits qui ont des valeurs possèdent un attribut de résolution de conflit défini indépendamment pour chaque droit. Le paramètre par défaut de résolution des conflits est Priorité (`conflict-resolution="priority"`). L'autre valeur possible est `conflict-resolution="union"`.

  - **conflict-resolution="union" —** La valeur union signifie que les droits s'ajoutent. Tous les droits accordés du fait de l'appartenance à un stratégie d'un utilisateur lui sont assignés. Les valeurs de droits différentes sont simplement ajoutées et l'utilisateur les obtient toutes.

    Ainsi, si Jameel est membre de la stratégie Organisateurs de salons qui attribue l'appartenance à une liste de distribution de courrier électronique GroupWise nommée Liste de distribution de courrier électronique des salons, mais s'il est exclu de l'appartenance à la stratégie Responsables de salons qui attribue également cette même Liste de distribution de courrier électronique des salons, il obtiendra quand même son appartenance à la liste de distribution de courrier électronique.

    Autre exemple : si Consuela se voit accorder l'appartenance au groupe AD nommé Personnel du service courrier par la stratégie Service courrier, ainsi que l'appartenance au groupe AD nommé Réaction en cas d'urgence par la stratégie Volontaires d'urgence, l'appartenance aux deux groupes lui est accordée dans AD.

    Avec ce paramètre, la position d'une stratégie de droit dans la liste des stratégies est sans importance pour le droit en question.

  - **conflict-resolution="priority" —** La valeur « priority » signifie que, si des valeurs dans deux stratégies sont en conflit ou si une stratégie inclut l'utilisateur et si une autre l'exclut, les seuls droits attribués à l'utilisateur sont ceux compris dans la stratégie de droit qui figure en premier dans la liste des stratégies de droit.

    On aurait alors, avec ce paramètre, un résultat différent pour les exemples précédents.

    Dans l'exemple précédent, pour Jameel, si le droit de la liste de distribution de courrier électronique GroupWise avait une valeur de priorité, et la stratégie des responsables de salons était plus haut dans la liste que la stratégie des organisateurs de salons, l'appartenance à la liste de distribution de courrier électronique des salons ne lui serait pas accordée.

    Dans l'exemple ci-dessus, pour Consuela, si le droit d'appartenance au groupe NOS AD avait la valeur « priority », et si la stratégie Service courrier était plus haut dans la liste que

la stratégie Volontaires d'urgence, elle ne se verrait accorder que l'appartenance au groupe Personnel du service courrier. On ne lui accorderait pas l'appartenance au groupe de réaction en cas d'urgence car la résolution de conflit ne s'ajoute, prioritairement, pas.

Cette fonctionnalité peut se révéler utile si, par exemple, vous configurez votre environnement de manière à utiliser les droits basés sur le rôle pour placer les utilisateurs dans une structure hiérarchique sur un autre système. Vous voulez que chaque utilisateur soit placé à un endroit et pas à deux endroits à la fois.

N'oubliez pas que ce paramètre peut être différent pour chaque droit offert par chaque pilote.

En général, si vous utilisez le paramètre priorité, il est conseillé de placer les stratégies d'administrateur ou de responsable plus haut dans la liste que les stratégies concernant les utilisateurs finals ou les collaborateurs individuels. Placez les groupes les plus étroits avant les groupes les plus larges.

6.8.2 Modification de la méthode de résolution de conflit pour un droit individuel

1 Dans iManager, sélectionnez *Identity Manager* > *Présentation de Identity Manager*, puis sélectionnez un ensemble de pilotes.

Une page avec une représentation graphique de tous les pilotes de l'ensemble de pilotes s'affiche.

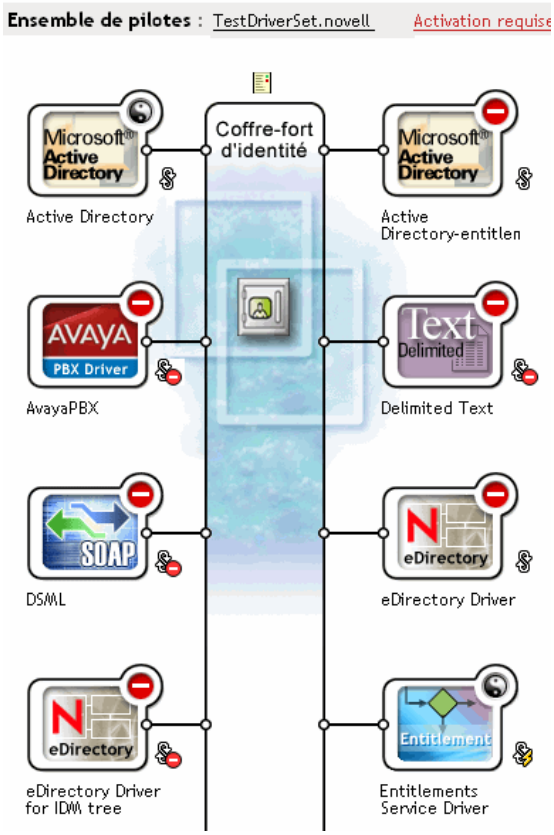
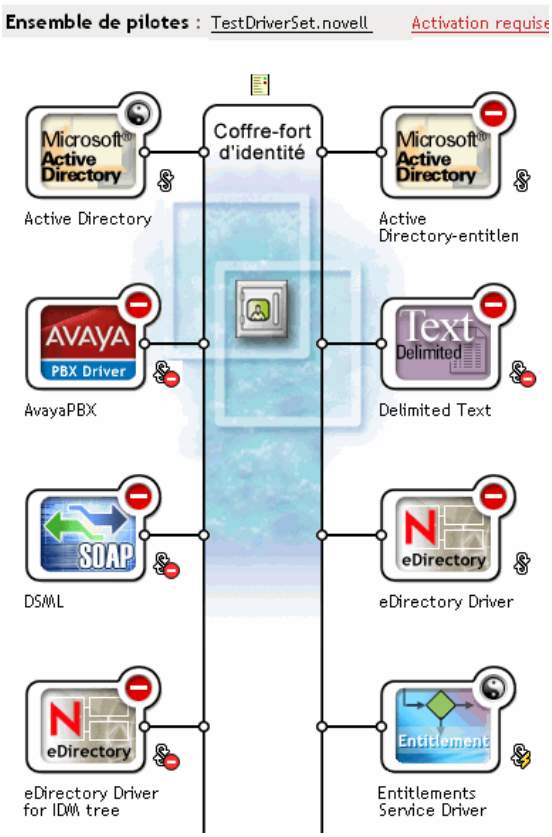


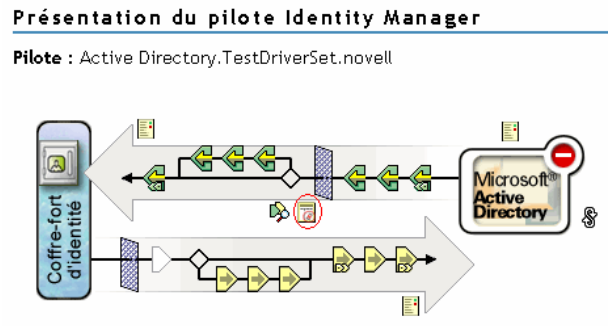
Figure 6-7 *Ensemble de pilotes*



2 Cliquez sur le bouton d'état du pilote et sélectionnez *Arrêter le pilote*.

3 Cliquez sur l'icône du pilote qui propose le droit que vous souhaitez modifier.

Une page proposant des icônes pour le pilote et ses stratégies s'affiche. Sélectionnez l'icône *Afficher tous les droits* au centre de l'écran (dans un cercle rouge).



4 Sur la page Gérer les droits, cliquez sur le nom du droit pour l'afficher dans la visionneuse XML.

5 Cochez la case *Activer l'édition XML*.

6 Dans le XML, repérez la définition du droit que vous souhaitez modifier.

Voici un exemple de la ligne qu'il vous faut repérer :

```
<entitlement conflict-resolution="union" description="Grants
membership to GroupWise Distribution lists" display-name="GroupWise
Distribution Lists" name="gwDistLists">
```

7 Modifiez la valeur conflict-resolution. Les deux valeurs possibles sont les suivantes :

```
conflict-resolution="union"
```

```
conflict-resolution="priority"
```

Pour plus d'informations sur ces valeurs, reportez-vous à « Résolution des conflits entre les stratégies de droits basés sur le rôle » page 192.

8 Cliquez sur *Redémarrer* pour redémarrer le pilote de service de droits.

6.8.3 Classement des stratégies de droits par ordre de priorité

Par défaut, l'ordre de la liste des stratégies de droits n'a pas d'importance, dans la mesure où les configurations de pilote livrées avec Identity Manager ont comme méthode de résolution des conflits `conflict-resolution="union"` pour chaque droit.

Si vous modifiez un droit pour lui attribuer la valeur `conflict-resolution="priority"`, l'ordre des stratégies de droits dans la liste a une importance, mais uniquement pour les droits que vous avez modifiés. Pour plus d'informations sur ces valeurs, reportez-vous à « Résolution des conflits entre les stratégies de droits basés sur le rôle » page 192.

Pour modifier l'ordre des stratégies de droits, utilisez les flèches en regard de la liste des stratégies de droits. La première stratégie dans la liste a la plus haute priorité.

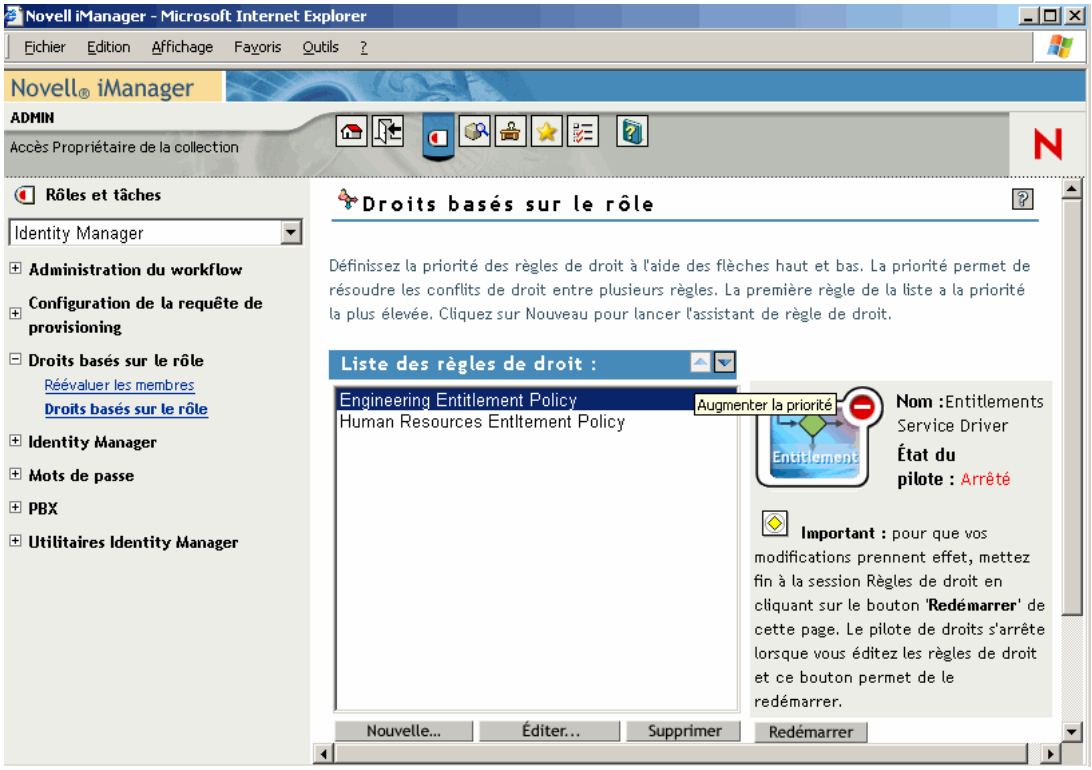
1 Dans iManager, cliquez sur *Droits basés sur le rôle* > *Droits basés sur le rôle*.

2 Recherchez un ensemble de pilotes, puis sélectionnez-le.

Une page avec une liste des stratégies de droits s'affiche.

3 Modifiez la priorité des stratégies de droits à l'aide des flèches pour déplacer les stratégies vers le haut ou vers le bas de la liste.

Pour attribuer une priorité plus élevée à une stratégie de droit, déplacez-la vers le haut.



4 Cliquez sur *Fermer* pour redémarrer le pilote.

Vous devez redémarrer le pilote pour que les modifications de priorités soient appliquées.

6.9 Dépannage des droits basés sur le rôle

Lorsque vous procédez au dépannage, n'oubliez pas les éléments suivants :

- Lorsque vous modifiez des stratégies en cliquant sur *Nouveau*, *Modifier* ou *Supprimer* sur la page où sont répertoriées les stratégies, le *Pilote de service de droits* est arrêté. Il n'est redémarré que lorsque vous cliquez sur le bouton *Redémarrer*, sur cette même page.

  Cette fonctionnalité empêche le pilote d'attribuer ou de supprimer des droits dans votre environnement de production tant que vos modifications de stratégies ne sont pas terminées.
- De même, le pilote de service de droits ne démarre pas s'il apparaît que plusieurs personnes modifient les stratégies de droits en même temps.
- Un seul pilote de service de droits étant utilisé pour chaque ensemble de pilotes, une stratégie de droit ne peut gérer que les utilisateurs qui sont dans une réplique principale ou en lecture/écriture sur le serveur associé à cet ensemble de pilotes.

6.10 Éléments qui s'appliquent aux droits basés sur le rôle et aux droits de provisioning basé sur le workflow

Les informations suivantes s'appliquent à tous les droits et non à une implémentation spécifique.

6.10.1 Contrôle de la signification de l'octroi ou de la révocation de droits

Vous pouvez contrôler les conséquences de l'attribution ou de la suppression d'un droit. Chaque pilote fournit une liste des choix pris en charge qui contrôlent la signification des verbes « accorder » et « révoquer ».

Ainsi, lors de l'ajout d'un compte GroupWise, vous pouvez spécifier que « accorder » signifie en fait attribuer à l'utilisateur un compte désactivé, ce qui oblige l'administrateur à intervenir pour que l'utilisateur puisse accéder au compte en question. Vous pouvez sinon choisir d'activer le compte, ce qui est l'option par défaut.

Par défaut, les configurations de pilote utilisent l'option susceptible de protéger au mieux les données. Ainsi, la signification par défaut de supprimer pour un compte GroupWise est fixée à désactiver, pour empêcher la perte involontaire de comptes en cas d'erreur lorsque l'administrateur modifie des stratégies. Autre exemple : les configurations des pilotes Identity Manager ne révoquent pas les droits qui tirent leurs valeurs d'un compte utilisateur dans un autre système. Si un utilisateur se voit accorder l'appartenance à une liste de distribution de courrier électronique et si, par la suite, l'utilisateur ne satisfait plus aux critères de la stratégie de droit, il est tout simplement exclu de l'appartenance à la stratégie. Les comptes sont désactivés mais l'appartenance à un groupe et les valeurs d'attribut ne sont pas supprimées. Un expert Identity Manager peut personnaliser les configurations de pilote si vous souhaitez un autre résultat.

L'interprétation de la révocation d'un droit est particulièrement importante dans la mesure où la fonctionnalité des droits basés sur le rôle permet de modifier radicalement les droits d'une entreprise dans un environnement de production sans tester les résultats en laboratoire.

Vous pouvez modifier le paramètre d'interprétation des termes « accorder » et « révoquer » en modifiant les variables de configuration globale sur un pilote préconfiguré. Si vous créez votre propre configuration personnalisée, vous pouvez ajouter des GCV permettant d'interpréter l'octroi et la révocation des droits.

6.10.2 Comment éviter des pertes de données

Les droits basés sur le rôle sont conçus pour permettre de modifier radicalement les droits, par exemple les droits sur les comptes, en fonction de l'appartenance à la stratégie. Cela signifie cependant que des erreurs faites lors de la modification de stratégies risquent d'engendrer des problèmes. Les configurations de pilote fournies avec Identity Manager utilisent les paramètres les

plus bénins. Vous devez savoir comment utiliser les GCV pour éviter de perdre accidentellement des données.

Nous vous recommandons, par exemple, de ne jamais définir sur Supprimer la GCV chargée de l'interprétation de la révocation d'un droit sur un compte.

Une autre mesure pour protéger vos données lorsque vous modifiez ou créez une nouvelle stratégie de droit consiste à désactiver le pilote pour que les modifications ne soient pas effectuées tant que vous n'avez pas terminé de modifier vos stratégies. Vous pouvez alors ensuite redémarrer manuellement le pilote à l'aide du bouton *Redémarrer* dans l'interface des stratégies de droit. De même, s'il semble qu'un autre utilisateur est en train de modifier des stratégies de droit et si vous essayez de redémarrer le pilote de service de droits à l'aide du bouton *Redémarrer*, vous êtes invité à ne pas le faire tant que l'autre utilisateur n'a pas fini d'effectuer ses modifications.

6.10.3 Synchronisation des mots de passe et droits

La synchronisation des mots de passe se gère de la même manière pour les pilotes qui utilisent les droits basés sur le rôle et pour les autres pilotes, comme indiqué dans « Synchronisation de mot de passe sur des systèmes connectés » page 73.

Sécurité : meilleures pratiques 7

7.1 Utilisation de SSL

Lorsque c'est possible, activez SSL pour tous les transports. SSL doit être activé pour la communication entre le moteur méta-annuaire et le chargeur distant (reportez-vous à la section Section 3.2, « Sécurisation du transfert des données », page 45), et entre le moteur méta-annuaire ou le chargeur distant et les systèmes connectés.

Si vous n'activez pas SSL, des informations comme les mots de passe sont envoyées sans codage.

7.2 Sécurisation de l'accès

Veillez à sécuriser l'accès aux coffres-forts d'identité et aux objets Identity Manager.

Sécurité physique Protégez l'accès à l'emplacement physique des serveurs sur lesquels est installé un coffre-fort d'identité.

Droits d'accès Des droits administratifs sont nécessaires afin de créer les objets Identity Manager et configurer les pilotes. Surveillez et contrôlez l'identité de la personne qui peut créer ou modifier les éléments suivants :

- Les ensembles de pilotes Identity Manager
- Les pilotes Identity Manager
- Les objets de configuration du pilote (filtres, feuilles de style, stratégies), en particulier les stratégies utilisées pour la récupération ou la synchronisation des mots de passe
- Les objets de la stratégie de mot de passe (et la tâche iManager permettant de les modifier), car ils contrôlent les mots de passe qui seront synchronisés avec d'autres et les options du libre-service de mot de passe qui seront utilisées

7.3 Gestion des mots de passe

Lorsque vous choisissez d'échanger des informations entre les systèmes connectés, prenez garde à bien sécuriser l'échange. Cela vaut particulièrement pour les mots de passe.

- L'attribut Indice de mot de passe (nsimHint) est également lisible par tous, ce qui permet aux utilisateurs non authentifiés qui ont oublié leur mot de passe d'accéder à leur indice. Les indices de mots de passe peuvent contribuer à réduire le nombre d'appels au service d'assistance.

Pour des raisons de sécurité, ces indices sont contrôlés afin de vérifier qu'ils ne contiennent pas le mot de passe de l'utilisateur. Toutefois, un utilisateur peut toujours créer un indice de mot de passe fournissant trop d'informations sur le mot de passe.

Afin d'améliorer la sécurité lors de l'utilisation des indices de mots de passe :

- Autorisez l'utilisateur à n'accéder qu'à l'attribut nsimHint sur le serveur LDAP utilisé pour les options de mot de passe en libre-service.
- Exigez que les utilisateurs répondent aux stimulation-questions avant de pouvoir recevoir leur mot de passe.
- Rappelez aux utilisateurs qu'ils doivent créer des indices de mots de passe qu'eux seuls peuvent comprendre. L'option Message de modification du mot de passe, dans la stratégie de mot de passe, est l'une des manières de le faire. Reportez-vous à la section « Adding a Password Change Message (Ajout d'un message de modification du mot de passe) » du Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe) (http://www.novell.com/documentation/password_management/index.html).

Si vous choisissez de ne pas utiliser d'indice de mot de passe, vérifiez que vous n'utilisez cette fonction dans aucune des stratégies de mot de passe. Afin d'éviter que des indices de mot de passe ne soient définis, vous pouvez aller encore plus loin et supprimer complètement la fonction Configuration de l'indice en suivant la procédure décrite à la section « Disabling Password Hint by Removing the Hint Gadget (Désactivation de l'indice de mot de passe par la suppression de la fonction Indice) » du Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe) (http://www.novell.com/documentation/password_management/index.html).

- Les Questions de stimulation peuvent être lues par le public, pour que les utilisateurs non authentifiés ayant oublié leur mot de passe puissent s'authentifier d'une autre manière. Le fait d'exiger les stimulation-questions augmente la sécurité du libre-service Mot de passe oublié ; en effet, l'utilisateur doit prouver son identité en apportant les réponses correctes avant de recevoir son mot de passe oublié ou un indice de mot de passe ou encore de réinitialiser son mot de passe.

  Un paramètre de verrouillage contre les intrus est appliqué pour les stimulation-questions, de manière à limiter le nombre de tentatives incorrectes que pourrait réaliser un intrus.

  Un utilisateur pourrait créer des stimulation-questions qui contiennent des indices sur le mot de passe. Rappelez aux utilisateurs qu'ils doivent créer des stimulation-questions et des réponses qu'eux seuls peuvent comprendre. L'option Message de modification du mot de passe, dans la stratégie de mot de passe, est l'une des manières de le faire. Reportez-vous à la section « Adding a Password Change Message (Ajout d'un message de modification du mot de passe) » du Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe) (http://www.novell.com/documentation/password_management/index.html).
- Pour des raisons de sécurité, les opérations consécutives à l'oubli du mot de passe (*Envoyer par messagerie électronique le mot de passe actuel à l'utilisateur* et *Autoriser l'utilisateur à réinitialiser le mot de passe*) ne sont disponibles que si vous exigez de l'utilisateur qu'il réponde aux stimulation-questions.
- Une nouvelle fonction a été ajoutée à NMAS™ 2.3.4 afin d'améliorer la sécurité de la modification des mots de passe universels par un administrateur. Elle fonctionne de façon très similaire à la fonction précédemment proposée pour le mot de passe NDS®.

  Lorsqu'un administrateur modifie le mot de passe d'un utilisateur, par exemple lors de la création d'un nouvel utilisateur ou en réponse à un appel de dépannage, le mot de passe

précédent expire automatiquement si vous avez activé le paramètre d'expiration des mots de passe dans la stratégie de mots de passe. Ce paramètre se trouve dans les règles de mots de passe avancées ; il est appelé *Nombre de jours avant l'expiration du mot de passe (0-365)*. Dans cette fonction, ce n'est pas le nombre de jours défini qui est important, c'est son activation.

7.4 Création de stratégies de mot de passe performantes

Les objets de la stratégie de mot de passe sont lisibles par tous, afin de permettre aux applications de vérifier si les mots de passe sont conformes. Cela signifie qu'un utilisateur non authentifié peut interroger le coffre-fort d'identité et trouver les stratégies de mot de passe appliquées. Si vos stratégies de mot de passe exigent des utilisateurs qu'ils créent des mots de passe performants, cela ne représente pas un risque (reportez-vous à la section « Create Strong Password Policies (Création de stratégies de mot de passe performantes) » du Password Management Administration Guide (Guide d'administration pour la gestion des mots de passe) (http://www.novell.com/documentation/password_management/index.html)).

La synchronisation des mots de passe dans Identity Manager permet de simplifier les mots de passe utilisateur et de réduire les coûts inhérents au service d'assistance. La synchronisation bidirectionnelle des mots de passe permet de partager de différentes façons des mots de passe entre eDirectory et les systèmes connectés (reportez-vous aux scénarios de la Section 5.8, « Implémentation de la synchronisation des mots de passe », page 111).

Les stratégies de mot de passe et le mot de passe universel permettent d'appliquer auprès des utilisateurs des exigences fortes pour les mots de passe. Utilisez les règles de mot de passe avancées afin de vous conformer aux meilleures pratiques du marché en matière de mots de passe.

Vous pouvez par exemple exiger que les mots de passe utilisateur se conforment à des règles comme celles qui suivent :

- Exigez des mots de passe uniques.

  Vous pouvez empêcher les utilisateurs de réutiliser des mots de passe et contrôler le nombre de mots de passe que le système doit stocker dans la liste d'historique à des fins de comparaison.
- Exigez un nombre minimum de caractères.

  Le fait d'avoir des mots de passe plus longs est l'une des meilleures manières de renforcer la sécurité des mots de passe.
- Exigez un nombre minimum de chiffres.

  Le fait d'exiger au moins un caractère numérique dans un mot de passe aide à le protéger des attaques de dictionnaire, dans lesquelles les intrus essaient de se connecter en utilisant des mots du dictionnaire.
- Excluez les mots de passe de votre choix.

  Vous pouvez exclure les mots qui, selon vous, présentent un risque, par exemple le nom ou un site de votre société, ou encore les mots test ou admin. Même si la liste d'exclusion n'a pas pour objet de remplacer tout un dictionnaire, elle peut être assez longue. Souvenez-vous simplement qu'une longue liste d'exclusions ralentit la connexion des utilisateurs. Afin de mieux se protéger des attaques de dictionnaire, il est préférable d'exiger l'utilisation de chiffres ou de caractères spéciaux.

N'oubliez pas que vous pouvez créer plusieurs stratégies de mot de passe si vous avez des exigences différentes dans les diverses parties de l'arborescence. Vous pouvez assigner une stratégie de mot de

passe à la totalité de l'arborescence, au conteneur racine d'une partition, à un conteneur, voire à un utilisateur. Afin de simplifier l'administration, nous vous recommandons d'assigner des stratégies de mot de passe au niveau le plus élevé possible de l'arborescence.

Vous pouvez également utiliser le verrouillage contre les intrus. Comme toujours, cette fonctionnalité eDirectory permet de spécifier le nombre d'échecs autorisés dans les tentatives de connexion avant le verrouillage du compte. Il s'agit d'un paramètre du conteneur parent et non d'un paramètre de la stratégie de mot de passe. Reportez-vous à la section « Managing User Accounts (Gestion des comptes utilisateur) » du *Novell eDirectory 8.7.3 Administration Guide (Guide d'administration de Novell eDirectory 8.7.3)* (http://www.novell.com/documentation/edir873/edir873/data/afxkmdi.html#amm7bjv).

7.5 Sécurisation des systèmes connectés

Sachez que les systèmes connectés avec lesquels vous synchronisez des données pourraient présenter un risque au niveau du stockage ou du transport.

Sécurisez les systèmes avec lesquels vous échangez des mots de passe. LDAP, NIS ou encore Windows présentent des failles de sécurité qu'il est utile d'étudier avant d'activer la synchronisation des mots de passe.

De nombreux fournisseurs de logiciels proposent des instructions spécifiques de sécurité qu'il convient de suivre.

7.6 Designer pour Identity Manager

Lorsque vous utilisez Designer pour Identity Manager, vous devez tenir compte des points suivants :

- Surveillez et contrôlez l'identité des personnes qui peuvent créer ou modifier un pilote Identity Manager.

  Des droits administratifs sont nécessaires afin de créer les objets Identity Manager et configurer les pilotes.
- Avant de donner à un consultant un mot de passe administrateur pour un coffre-fort d'identité, limitez les droits affectés à cet administrateur aux zones de l'arborescence auxquelles le consultant en question doit pouvoir accéder.
- Supprimez les fichiers de projet (`.proj`) ou enregistrez-les dans un répertoire réservé à la société.

  Les fichiers `.proj` de Designer doivent rester sur le site de projets de la société. Le consultant n'emporte pas les fichiers à la fin du projet.
- Lorsque vous n'avez plus besoin des fichiers de projet, des fichiers journaux et des fichiers de trace, effacez-les.
- Avant de mettre un ordinateur portable au rebut ou en réserve, vérifiez que tous les fichiers de projet ont été effacés.
- Vérifiez que la connexion entre Designer et le coffre-fort d'identité est physiquement sécurisée.

  Sinon, il serait possible de surveiller le câble et d'en tirer des informations sensibles.
- Lorsque vous créez des documents avec le Générateur de documents, prêtez-y attention.

  Ils peuvent contenir des mots de passe et des données sensibles en texte clair.

- Si Designer doit lire ou écrire des données dans un attribut eDirectory, ne signalez pas ce dernier comme attribut codé.

  Designer est incapable de lire ou d'écrire des données dans des attributs codés.

- N'enregistrez pas les mots de passe sensibles.

  Actuellement, les projets Designer ne sont pas codés. Les mots de passe sont simplement codés. Vous ne devez donc pas partager des projets Designer associés dont les mots de passe sont enregistrés.

  Afin d'enregistrer un mot de passe pour une session sans l'enregistrer dans le projet :

  a. Dans la vue Aperçu développée, cliquez avec le bouton droit de la souris sur un coffre-fort d'identité.

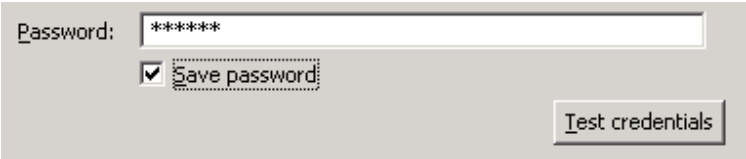
  b. Sélectionnez Propriétés.

  c. Dans la page Configuration, saisissez un mot de passe puis cliquez sur *OK*.

     Vous pouvez saisir un mot de passe par session. À la fermeture du projet, le mot de passe est perdu.

  Afin d'enregistrer un mot de passe sur le disque dur, effectuez les étapes 1 à 3, sélectionnez *Enregistrer le Mot de passe*, puis cliquez sur *OK*.

Figure 7-1 *Enregistrer le Mot de passe*



7.7 Meilleures pratiques du marché en matière de sécurité

Respectez les meilleures pratiques de sécurité du marché, concernant notamment le blocage des ports non utilisés sur le serveur.

7.8 Suivi des modifications apportées aux informations sensibles

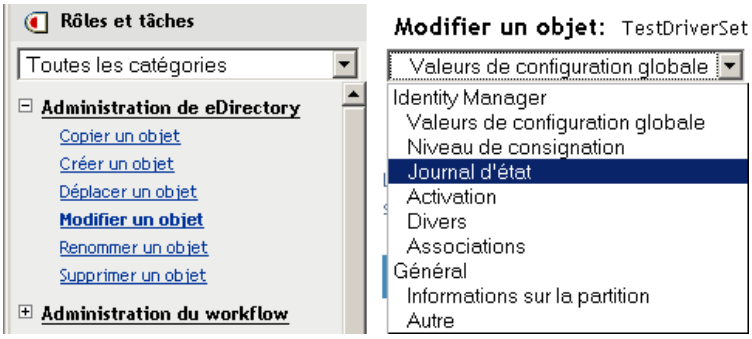
- Section 7.8.1, « Consignation des événements avec iManager », page 205
- Section 7.8.2, « Consignation des événements avec Designer », page 207

7.8.1 Consignation des événements avec iManager

Vous pouvez utiliser Novell Audit afin de consigner les événements que vous considérez importants pour la sécurité. Pour plus d'informations sur Novell Audit, reportez-vous au Chapitre 10, « Consignation et création de rapports avec Novell Audit », page 235.

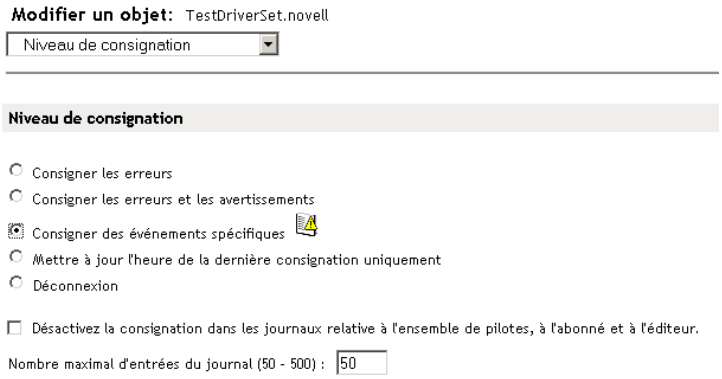
Vous pouvez par exemple consigner les modifications apportées aux mots de passe pour un pilote Identity Manager particulier, voire pour un ensemble de pilotes, en procédant comme suit :

1. Sélectionnez *Administration eDirectory* > *Modifier l'objet* > *Niveau de consignation*.



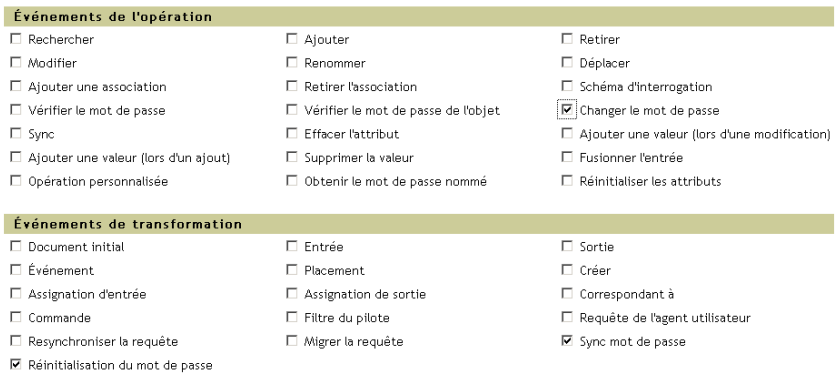
   Sélectionnez un onglet ou une option dans la liste déroulante, selon la version d'iManager que vous utilisez.

2. Sélectionnez *Consigner des événements spécifiques*.



3. Afin de sélectionner des événements spécifiques, cliquez sur l'icône de consignation des événements  .

4. Dans la page Événements, sélectionnez les éléments suivants :



   - Dans Événements de l'opération, sélectionnez *Changer le mot de passe*.

Cet élément surveille les modifications directes du mot de passe NDS.

- Dans Événements de transformation, sélectionnez *Mot de passe défini* et *Sync mot de passe*. Ces deux éléments surveillent les événements qui concernent le mot de passe universel et le mot de passe de distribution.

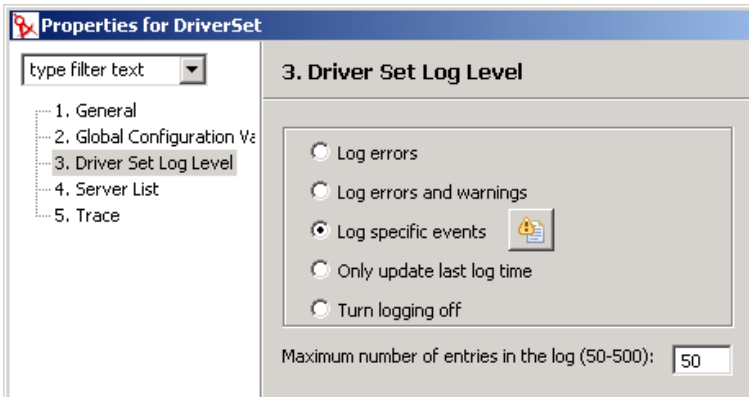
5 Cliquez sur *OK* deux fois.

7.8.2 Consignation des événements avec Designer

Vous pouvez consigner les événements concernant un pilote ou un ensemble de pilotes.

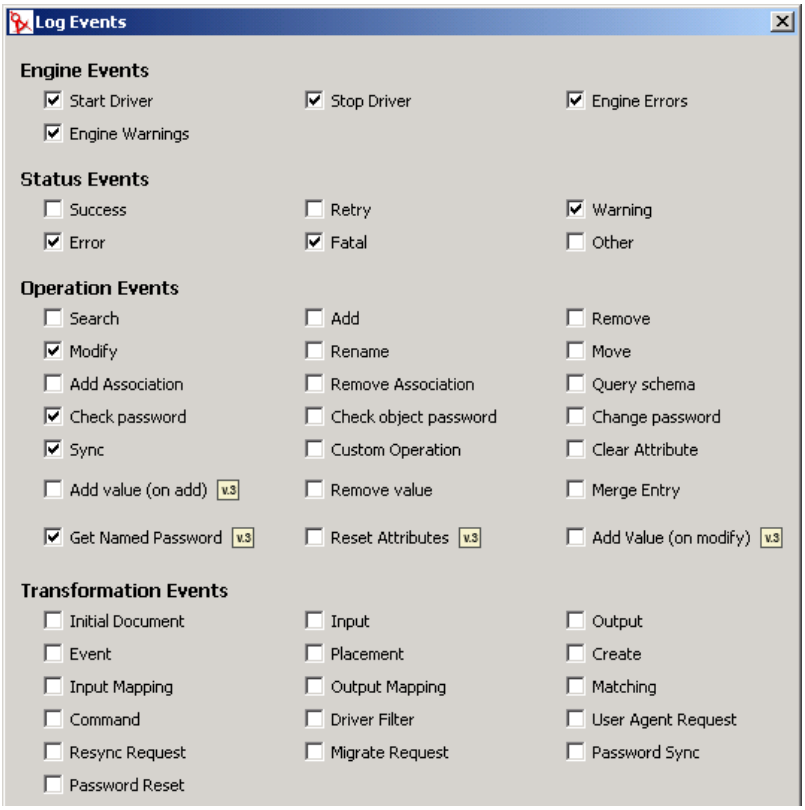
Consignation des événements pour un ensemble de pilotes

1 Dans Designer, cliquez avec le bouton droit de la souris sur un ensemble de pilotes, puis sélectionnez *Propriétés*.



2 Sélectionnez le *niveau de consignation de l'ensemble de pilotes*, puis *Consigner des événements spécifiques*.

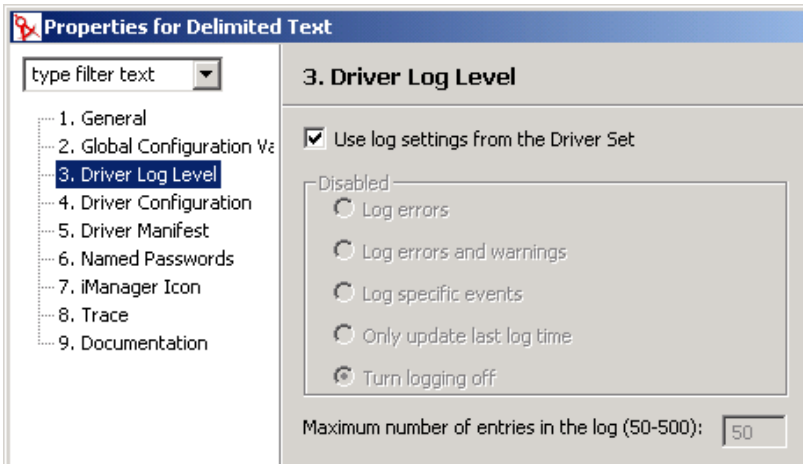
3 Cliquez sur l'icône *Sélectionner les événements à consigner*  .



4 Sélectionnez les événements à consigner, puis cliquez sur *OK*.

Consignation des événements pour un pilote

1 Dans Designer, cliquez sur un pilote avec le bouton droit de la souris, puis sélectionnez *Propriétés*.



2 Sélectionnez le *niveau de consignation du pilote*, puis *Consigner des événements spécifiques*.

   Si vous préférez, vous pouvez valider les paramètres définis pour l'ensemble de pilotes, puis cliquer sur *OK*. Sinon, désactivez la case *Utiliser les paramètres de consignation de l'ensemble de pilotes*, sélectionnez *Consigner des événements spécifiques*, puis cliquez sur *OK*.

3 Cliquez sur *Sélectionner les événements à consigner*.

4 Sélectionnez les événements à consigner, puis cliquez sur *OK*.

Gestion des services de moteur

8

Les pilotes suivants ne sont utilisés que pour les services de moteur méta-annuaire et non pour les systèmes connectés externes. Ils sont installés automatiquement en même temps que Identity Manager.

8.1 Pilote de service de droits

Reportez-vous au Chapitre 6, « Création et utilisation des droits », page 163.

8.2 Pilote de service de tâches manuelles

Le pilote de services de tâches manuelles a été conçu pour notifier à un ou plusieurs utilisateurs la survenue d'un événement au niveau des données et, le cas échéant, la nécessité d'une opération de leur part. Par exemple, dans un scénario de provisioning d'employé, il peut s'agir de la création d'un nouvel objet Utilisateur et l'opération de l'utilisateur peut consister à assigner un numéro de bureau en saisissant des données dans eDirectory ou dans une application. D'autres scénarios incluent l'envoi d'une notification à l'administrateur pour lui signaler la création d'un objet Utilisateur, la modification des données d'un objet par un utilisateur, etc.

Pour configurer le pilote de service de tâches manuelles, vous devez en général configurer deux sous-systèmes séparés mais liés : les modèles de courrier électronique et les stratégies de canal Abonné, ainsi que les modèles du serveur Web du canal Éditeur et ses stratégies.

En outre, les paramètres de pilote comme le nom du serveur SMTP, le numéro de port du serveur Web, etc., doivent être définis.

Dans cette section :

8.2.1 Installation

- **Installation :** le pilote de services de tâches manuelles est automatiquement installé lorsque vous installez l'option *Serveur méta-annuaire* depuis le programme d'installation de Identity Manager.
- **Plates-formes :** le pilote s'exécute sur les plates-formes prises en charge par Identity Manager et le chargeur distant.
- **Activation :** le pilote n'a pas besoin d'être activé séparément. Il est activé en même temps que le moteur méta-annuaire.

8.2.2 Présentation

Vous trouverez dans cette section des informations sur le fonctionnement des différentes fonctionnalités du pilote.

Modes de fonctionnement

Deux principaux modes de fonctionnement sont pris en charge :

- **Demande directe de données :** un message électronique est envoyé pour demander à l'utilisateur de saisir des données dans eDirectory (ces données pourront être éventuellement utilisées par une autre application). Le destinataire répond en cliquant sur l'URL fournie dans le message. L'URL désigne le serveur Web fonctionnant sur le canal Éditeur du pilote de service de tâches manuelles. L'utilisateur interagit avec les pages Web dynamiques générées par le serveur Web pour s'authentifier auprès de eDirectory™ et pour entrer les données demandées.
- **Notification d'événement :** un message électronique est envoyé à l'utilisateur sans utiliser le canal Éditeur. Il peut simplement s'agir de la notification d'une opération effectuée dans eDirectory ou d'une requête de données par un moyen autre que le serveur Web du canal Éditeur, par exemple Novell iManager, une autre application ou une interface personnalisée.

Exemple : message électronique du canal Abonné, réponse du serveur Web du canal Éditeur

Voici un scénario d'exemple de provisioning d'employé dans lequel le responsable d'un nouvel employé affecte à celui-ci un numéro de bureau :

1. Un objet Utilisateur est créé dans eDirectory (par exemple, par le pilote DirXML du système des ressources humaines de la société).
2. Le canal Abonné du pilote de service de tâches manuelles envoie un message SMTP au responsable de l'utilisateur et à l'assistant du responsable. Ce message contient une URL qui désigne le serveur Web du canal Éditeur. L'URL contient par ailleurs des éléments de données qui identifient l'utilisateur et les personnes autorisées à soumettre les données requises.
3. Le responsable ou son assistant clique sur l'URL dans le message électronique pour afficher une page HTML dans un navigateur Web. Le responsable ou son assistant procède ensuite comme suit :
   - Il sélectionne le DN de son objet Utilisateur eDirectory afin de s'identifier en tant qu'auteur de la réponse au message.
   - Il saisit son mot de passe eDirectory.

- Il saisit le numéro de bureau du nouvel employé.
- Il clique sur le bouton Submit (Soumettre).

4. Le numéro de bureau du nouvel employé est soumis à eDirectory via le canal Éditeur du pilote de service de tâches manuelles.

Exemple : message électronique du canal Abonné, aucune réponse du canal Éditeur

Voici un exemple de scénario dans lequel le responsable d'un nouvel employé assigne à celui-ci un ordinateur dans un système de gestion des ressources :

1. Un objet Utilisateur est créé dans eDirectory (par exemple, par le pilote DirXML du système des ressources humaines de la société).
2. Le canal Abonné du pilote de service de tâches manuelles envoie un message SMTP au responsable de l'utilisateur et à l'assistant du responsable. Ce message contient des instructions qui permettront d'entrer les données dans le système de gestion des ressources.
3. Le responsable ou son assistant saisit les données dans le système de gestion des ressources.
4. (Facultatif) Les données d'identification de l'ordinateur sont transmises à eDirectory via le pilote DirXML du système de gestion des ressources.

Comment les messages électroniques et les pages Web sont créés par le pilote de service de tâches manuelles

Les messages électroniques, les pages Web au format HTML et les documents XDS peuvent tous être considérés comme des documents. Le pilote de service de tâches manuelles crée des documents de manière dynamique, en fonction des informations fournies au pilote.

Les modèles sont des documents XML qui contiennent les textes standard ou parties fixes d'un document, ainsi que des jetons de remplacement qui indiquent l'emplacement des parties dynamiques (de remplacement) du document final construit.

Le canal Abonné et le canal Éditeur du pilote de service de tâches manuelles utilisent des modèles pour créer des documents. Le canal Abonné crée des messages électroniques et le canal Éditeur, des pages Web et des documents XDS.

La partie dynamique d'un document est fournie via des données de remplacement. Les données de remplacement sur le canal Abonné sont fournies par les stratégies de canal Abonné (par exemple la stratégie de transformation de la commande). Celles du canal Éditeur proviennent des données HTTP (données d'URL et données HTTP POST) envoyées au serveur Web. Le pilote de service de tâches manuelles peut automatiquement fournir certaines données qu'il connaît (par exemple, l'adresse du serveur Web).

Les modèles sont traités par des feuilles de style XSLT. Ces feuilles de style de traitement des modèles sont séparées des feuilles de style utilisées comme stratégies DirXML dans le canal Abonné ou le canal Éditeur.

Les données de remplacement sont fournies à la feuille de style XSLT sous forme de paramètre. Le résultat du traitement de la feuille de style est un document XML, HTML ou texte. Il sera utilisé comme corps d'un message électronique, comme page Web ou sera envoyé à DirXML sur le canal Éditeur.

Les données de remplacement sont acheminées du canal Abonné vers le canal Éditeur via l'URL qui figure dans le message électronique. L'URL comprend une section requête qui contient les éléments de données de remplacement.

Le pilote de service de tâches manuelles est fourni avec suffisamment de feuilles de style prédéfinies pour traiter les modèles et créer des documents électroniques, des documents HTML et des documents XDS. D'autres feuilles de style personnalisées peuvent être créées afin de fournir, au besoin, d'autres options de traitement.

Une méthode avancée de création de documents est également disponible, qui utilise uniquement une feuille de style XSLT et des données de remplacement. Aucun modèle n'intervient dans la procédure. Toutefois, ce guide suppose l'utilisation de la méthode modèle parce que la méthode modèle est plus facile à configurer et à maintenir sans connaissance de la programmation XSLT.

Modèles

Cette section décrit les modèles de création de documents utilisés dans le pilote de service de tâches manuelles.

Les modèles sont des documents XML qui sont traités par une feuille de style afin de générer un document final. Le document final peut être un document XML, HTML ou du texte ordinaire (ou tout autre document qui peut être généré en utilisant XSLT).

Les modèles permettent de générer le texte de messages électroniques sur le canal Abonné, ainsi que des pages Web dynamiques et des documents XDS sur le canal Éditeur.

Les modèles contiennent du texte, des éléments et des jetons de remplacement. Les jetons de remplacement sont remplacés dans le document final par les données fournies à la feuille de style qui traite le modèle.

Plusieurs exemples de modèles (qui ont des fonctions diverses) sont présentés ci-dessous. Dans ces exemples, les jetons de remplacement correspondent aux chaînes de caractères comprises entre les deux signes $ et apparaissant en gras.

Les modèles peuvent aussi contenir des éléments d'opération. Ce sont des éléments de commande interprétés par la feuille de style de traitement des modèles. Les éléments d'opération sont décrits dans l'Annexe F, « Pilote de services de tâches manuelles : référence de modèles d'éléments d'opération », page 311. Dans les exemples suivants, les éléments d'opération apparaissent également en gras.

Le modèle de l'exemple suivant permet de produire le corps d'un message électronique au format HTML :

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head></head>
<body>
Dear $manager$,<p/>
<p>
This message is to inform you that your new employee <b>$given-name$
$surname$</b> has been hired.
<p>
You need to assign a room number for this individual. Click <a
href="$url$">Here</a> to do this.
</p>
```

```
<p>
Thank you,<br/>
HR Department
</p>
</body>
</html>
```

Le modèle de l'exemple suivant permet de produire le corps d'un message électronique au format texte ordinaire :

```
<form:text xmlns:form="http://www.novell.com/dirxml/manualtask/form">
Dear $manager$,
This message is to inform you that your new employee $given-name$
$surname$ has been hired.
You need to assign a room number for this individual. Use the following
link to do this:$url$
Thank you,
The HR Department</form:text>
```

L'élément <form:text> est requis parce que les modèles doivent être des documents XML. L'élément <form:text> est supprimé lors du traitement du modèle.

Le modèle suivant permet de produire un formulaire HTML utilisé comme page Web pour l'entrée de données :

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head>
<title>Enter room number for $subject-name$</title>
</head>
<body>
    <link href="novdocmain.css" rel="style sheet" type="text/css"/>
    <br/><br/><br/><br/>
    <form class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl">
        <table cellpadding="5" cellspacing="10" border="1"
align="center">
          <tr><td>
          <input TYPE="hidden" name="template" value="post_form.xml"/>
          <input TYPE="hidden" name="subject-name" value="$subject-
name$"/>
          <input TYPE="hidden" name="association"
value="$association$"/>
          <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="response-template"
value="post_response.xml"/>
          <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="auth-template"
value="auth_response.xml"/>
        <input TYPE="hidden" name="protected-data" value="$protected-
data$"/>
          You are:<br/>          <form:if-single-item name="responder-
```

```
dn">
            <input TYPE="hidden" name="responder-dn" value="$responder-
dn$"/>
             $responder-dn$          </form:if-single-item>
<form:if-multiple-items name="responder-dn">            <form:menu
name="responder-dn"/>          </form:if-multiple-items>
        </td></tr>
        <tr><td>
          Enter your password: <br/>
<input name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/>
        </td></tr>
        <tr><td>
          Enter room number for $subject-name$:<br/>
          <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="$query:roomNumber$"/>
        </td></tr>
        <tr><td>
          <input TYPE="submit" value="Submit"/> <input TYPE="reset"
value="Clear"/>
        </td></tr>
      </table>
    </form>
  </body>
</html>
```

Le modèle suivant permet de produire un document XDS :

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable">
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

Jetons de remplacement

Les éléments délimités par des signes $ dans les exemples de modèles ci-dessus sont des jetons de remplacement. Par exemple, $manager$ est remplacé par le nom réel du responsable.

Les jetons de remplacement peuvent apparaître dans les valeurs d'attribut texte ou XML (notez la valeur href sur l'élément <a> dans le premier exemple ci-dessus).

Données de remplacement

Les données de remplacement sont des chaînes qui vont prendre la place des jetons de remplacement dans le document final généré à partir d'un modèle. Ces chaînes proviennent soit de données du

canal Abonné, soit de données HTTP du canal Éditeur ou sont automatiquement fournies par le pilote. Un type supplémentaire de données de remplacement sont les données récupérées de eDirectory via Identity Manager (données de requête). Les données de remplacement sont décrites plus en détail dans l'Annexe D, « Pilote de services de tâches manuelles : données de remplacement », page 303.

Données du canal Abonné : les données de remplacement qui proviennent du canal Abonné sont de deux types. Le premier fournit les valeurs des jetons de remplacement contenus dans les modèles utilisés pour créer des messages électroniques. Le second est placé dans la partie requête d'une URL pour que les données puissent être utilisées sur le canal Éditeur lorsque l'URL est soumise au serveur Web du canal Éditeur.

Données HTTP : les données de remplacement sont fournies au serveur Web du canal Éditeur sous la forme de données de chaîne de requête d'URL, données HTTP POST ou les deux.

Données automatiques : le pilote de service de tâches manuelles fournit des données automatiques. Les données automatiques sont décrites dans l'Annexe E, « Pilote de services de tâches manuelles : éléments de données de remplacement automatiques », page 309.

Données de requête : les jetons de remplacement qui commencent par query: sont considérés comme des demandes de données actuelles auprès de eDirectory. La partie du jeton qui suit query: est le nom d'un attribut d'objet eDirectory. L'objet à interroger est spécifié par l'une des données de remplacement `association`, `src-dn` ou `src-entry-id`. Les éléments sont considérés dans l'ordre présenté dans la phrase précédente.

Éléments d'opération contenus dans les modèles

Les éléments d'opération sont des éléments qualifiés par un espace de nom. Ils figurent dans le modèle et sont utilisé pour une commande simple ou pour créer des éléments HTML pour des formulaires HTML. L'espace de nom utilisé pour qualifier les éléments est http://www.novell.com/dirxml/manualtask/form. Dans ce document et dans les exemples de modèles fournis avec le pilote de service de tâches manuelles, le préfixe utilisé est form.

Les éléments qui apparaissent en gras dans les exemples ci-dessus sont des éléments d'opération.

Les éléments d'opération sont décrits en détail dans l'Annexe F, « Pilote de services de tâches manuelles : référence de modèles d'éléments d'opération », page 311.

Message électronique du canal Abonné

Le canal Abonné du pilote de service de tâches manuelles est conçu pour envoyer des messages électroniques. Pour ce faire, le pilote prend en charge un élément XML personnalisé nommé <mail>. Les stratégies sur le canal Abonné construisent un élément <mail> en réponse à un événement eDirectory (par exemple, la création d'un utilisateur). Un exemple d'élément <mail> est fourni ci-dessous :

```
<mail src-dn="\PERIN-TAO\novell\Provo\Joe">
  <to>JStanley@novell.com</to>
  <cc>carol@novell.com</cc>
  <reply-to>HR@novell.com</reply-to>
  <subject>Room Assignment Needed for: Joe the Intern</subject>
  <message mime-type="text/html">
    <stylesheet>process_template.xsl</stylesheet>
```

```
    <template>html_msg_template.xml</template>
    <replacement-data>
      <item name="manager">JStanley</item>
      <item name="given-name">Joe</item>
      <item name="surname">The Intern</item>
      <url-data>
        <item name="file">process_template.xsl</item>
        <url-query>
          <item name="template">form_template.xml</item>
          <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\phb</item>
          <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\carol</item>
          <item name="subject-name">Joe The Intern</item>
        </url-query>
      </url-data>
    </replacement-data>
    <resource cid="css-1">novdocmain.css</resource>
  </message>
  <message mime-type="text/plain">
    <stylesheet>process_text_template.xsl</stylesheet>
    <template>txt_msg_template.xml</template>
    <replacement-data>
      <item name="manager">JStanley</item>
      <item name="given-name">Joe</item>
      <item name="surname">The Intern</item>
      <url-data>
          <item name="file">process_template.xsl</item>
          <url-query>
            <item name="template">form_template.xml</item>
            <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\phb</item>
            <item name="responder-dn" protect="yes">\PERIN-TAO\big-
org\carol</item>
            <item name="subject-name">Joe The Intern</item>
          </url-query>
        </url-data>
      </replacement-data>
    </message>
  <attachment>HR.gif</attachment>
</mail>
```

Le canal Abonné du pilote de services de tâches manuelles utilise les informations contenues dans l'élément <mail> pour construire un message électronique SMTP. Une URL peut être construite et insérée dans le message électronique via laquelle le destinataire du message peut répondre au message. L'URL peut pointer vers le serveur Web du canal Éditeur ou pointer vers un autre serveur Web.

L'élément <mail> et son contenu sont décrits en détail dans l'Annexe G, « Pilote de services de tâches manuelles : référence à l'élément <mail> », page 315.

Serveur Web du canal Éditeur

Le canal Éditeur du pilote de service de tâches manuelles exécute un serveur Web configuré de telle sorte que les utilisateurs puissent entrer des données dans eDirectory via un navigateur Web. Le serveur Web est conçu pour fonctionner en association avec les messages électroniques envoyés du canal Abonné du pilote de service de tâches manuelles.

Le serveur Web du canal Éditeur peut fournir des fichiers statiques et des contenus dynamiques. Les fichiers statiques comprennent par exemple les feuilles de style .css, les images, etc. Les contenus dynamiques sont par exemple les pages Web qui changent selon les données de remplacement contenues dans les données d'URL ou HTTP POST.

Le serveur Web du canal Éditeur est normalement configuré pour permettre à un utilisateur d'entrer des données dans eDirectory en réponse à un message électronique envoyé par le canal Abonné. Une interaction typique de l'utilisateur avec le serveur Web se ferait comme suit :

1. L'utilisateur soumet l'URL du message au serveur Web à partir d'un navigateur Web. L'URL précise la feuille de style, le modèle et les données de remplacement utilisés pour créer une page Web dynamique (qui contient généralement un formulaire HTML).
2. Le serveur Web crée une page HTML en traitant le modèle à l'aide de la feuille de style et des données de remplacement. La page HTML est renvoyée au navigateur Web de l'utilisateur comme ressource désignée par l'URL.
3. Le navigateur affiche la page HTML et l'utilisateur entre les informations requises.
4. Le navigateur envoie une requête HTTP POST qui contient les informations entrées, ainsi que d'autres informations issues de l'URL du message électronique. Le DN de l'utilisateur correspondant au message et le mot de passe de l'utilisateur doivent se trouver dans les données POST.
5. Le serveur Web authentifie l'utilisateur en utilisant son DN et son mot de passe. Si l'authentification échoue, une page Web contenant un message d'échec est renvoyée comme résultat de la requête POST. Le message d'échec peut être construit en utilisant une feuille de style et un modèle spécifié dans les données POST. Si l'authentification réussit, le traitement continue.
6. Le serveur Web construit un document XDS à l'aide de la feuille de style et du modèle spécifiés dans les données POST. Le document XDS est soumis à Identity Manager sur le canal Éditeur.
7. Le résultat de la soumission du document XDS, conjugué à la feuille de style et au modèle spécifiés dans les données POST, permet de construire une page Web qui indique à l'utilisateur le résultat de la soumission des données. Cette page Web est envoyée au navigateur comme résultat de la requête POST.

8.2.3 Configuration

Cette section décrit la configuration des paramètres et des modèles du pilote de services de tâches manuelles.

Configuration du pilote

Cette section décrit les paramètres qui apparaissent dans la section “Configuration du pilote” de l'interface utilisateur de l'objet pilote.

Plusieurs de ces paramètres concernent en fait le serveur Web du canal Éditeur. Ils apparaissent dans la zone Configuration du pilote parce que l'Abonné du pilote de service de tâches manuelles a également besoin d'y accéder.

DN de la base de documents

Ce paramètre est le DN eDirectory d'un objet Conteneur. Le pilote de service de tâches manuelles peut charger des documents XML (y compris des feuilles de style XSLT) à partir de eDirectory et à partir du disque. Si vous devez charger des documents XML à partir de eDirectory, ce paramètre identifie le conteneur racine à partir duquel les documents seront chargés.

Les documents chargés à partir de eDirectory résident dans la valeur d'attribut d'un objet eDirectory. Si aucun attribut n'est pas précisé, XmlData est utilisé par défaut. Vous pouvez spécifier l'attribut en ajoutant le symbole # suivi du nom d'attribut au nom de l'objet contenant le document.

Par exemple, supposons que le DN de base de documents est spécifié comme « novell\Manual Task Documents » et qu'il y a dans « Documents Manual Task » un conteneur nommé « templates ».

Si un objet Feuille de style DirXML nommé « e-mail _template » réside sous le répertoire « templates », les identificateurs de ressources suivants peuvent être utilisés pour faire référence au document XML : “templates/e-mail _template” ou “templates/e-mail _template#XmlData”.

Les identificateurs de ressource peuvent être fournis sous la forme de données de remplacement, données d'URL ou données HTTP POST. Par exemple, l'élément suivant peut apparaître sous un élément <message> dans le canal Abonné :

```
<template>templates/e-mail _template#XmlData</template>
```

Répertoire des documents

Ce paramètre identifie un répertoire de système de fichiers qui sert de répertoire de base pour la localisation des ressources telles que les modèles, les feuilles de style XSLT et d'autres ressources fichier fournies par le serveur Web du canal Éditeur. Exemples de valeurs :

Fenêtres	c:\Novell\Nds\mt_files
NetWare	SYS:\SYSTEM\mt_files
UNIX	/usr/lib/dirxml/rules/manualtask/mt_files

Use HTTP Server (true|false) (Utiliser serveur HTTP (vrai/faux)

Ce paramètre indique si le canal Éditeur doit exécuter ou non un serveur Web. Réglez le paramètre sur vrai si le serveur Web doit être exécuté ou faux si le serveur Web ne doit pas être exécuté.

Si le pilote de service de tâches manuelles n'est utilisé que pour envoyer un message électronique sans URL de réponse ou avec une URL qui pointe vers une autre application, le serveur HTTP ne doit pas être exécuté, pour enregistrer les ressources système.

Adresse IP HTTP ou nom d'hôte

Ce paramètre permet de spécifier à quelle adresse, parmi les multiples adresses IP locales, le serveur Web du canal Éditeur écoutera les requêtes HTTP.

Si vous laissez la valeur du paramètre nom d'hôte ou adresse HTTP IP vide, le serveur Web du canal Éditeur écoutera sur l'adresse IP par défaut. Pour les serveurs avec une seule adresse IP, cela est suffisant. Si vous placez une adresse IP à points comme valeur de paramètre, le serveur Web du canal Éditeur écoutera les requêtes HTTP sur l'adresse spécifiée.

Notez que la valeur spécifiée pour l'adresse IP HTTP ou le nom d'hôte est utilisée par le gestionnaire de messagerie du canal Abonné pour construire les URL si aucun nom d'hôte ni adresse n'est précisé dans l'élément de commande de courrier. Si le paramètre Use HTTP server (true|false) est réglé sur faux, l'adresse HTTP IP ou le nom d'hôte peut servir à spécifier l'adresse ou le nom d'un serveur Web à utiliser dans la construction des URL pour les messages de courrier électronique.

Port HTTP

Ce paramètre est un nombre entier qui indique le port TCP sur lequel le serveur Web du canal Éditeur doit écouter les requêtes entrantes. Si cette valeur n'est pas spécifiée, le numéro de port prend par défaut la valeur 80 ou 443, selon que le SSL est utilisé ou non pour les connexions du serveur Web.

Si le pilote de services de tâches manuelles fonctionne sur le serveur Identity Manager (c'est-à-dire, s'il n'est pas exécuté sous le chargeur distant sur une machine distante), le port HTTP doit être défini sur une valeur différente de 80 ou 443. En effet, les ports 80 et 443 sont généralement utilisés par iMonitor ou d'autres processus.

Nom du KMO

Ce paramètre, lorsqu'il est renseigné, indique le nom de l'objet Matériel clé (KMO) eDirectory qui contient le certificat et la clé de serveur utilisés pour SSL par le serveur Web du canal Éditeur.

La définition de ce paramètre oblige le serveur Web du canal Éditeur à utiliser SSL pour traiter les requêtes HTTP.

Il a la priorité sur tous les paramètres Keystore Java* (reportez-vous ci-dessous).

L'utilisation de SSL est recommandée pour des raisons de sécurité parce que les mots de passe eDirectory sont transmis dans les données HTTP POST lors de l'utilisation du serveur Web du canal Éditeur

Nom du fichier Keystore

Ce paramètre, ainsi que le mot de passe Keystore, le nom du certificat (alias de la clé) et le mot de passe du certificat (mot de passe clé) sert à spécifier un fichier keystore Java qui contient un certificat et une clé utilisés pour SSL par le serveur Web du canal Éditeur.

La définition de ce paramètre oblige le serveur Web du canal Éditeur à utiliser SSL pour traiter les requêtes HTTP.

Si le nom du paramètre KMO est défini, ce paramètre et ses paramètres associés sont ignorés.

L'utilisation de SSL est recommandée pour des raisons de sécurité à condition que les mots de passe eDirectory soient transmis sous la forme de données HTTP POST lors de l'utilisation du serveur Web du canal Éditeur.

Mot de passe Keystore

Ce paramètre spécifie le mot de passe pour le fichier keystore Java spécifié avec le paramètre Nom du fichier keystore.

Nom du certificat (alias de la clé)

Ce paramètre spécifie le nom du certificat à utiliser dans le fichier keystore Java spécifié avec le paramètre Nom du fichier keystore.

Mot de passe du certificat (mot de passe de la clé)

Ce paramètre spécifie le mot de passe pour le certificat spécifié en utilisant le paramètre Nom du certificat (alias de la clé).

Configuration de l'abonné

Cette section décrit les paramètres du canal Abonné.

Serveur SMTP

Ce paramètre précise le nom du serveur SMTP utilisé par le canal Abonné pour l'envoi des messages électroniques.

Nom de compte SMTP

Si le serveur SMTP spécifié en utilisant le paramètre du serveur SMTP nécessite une authentification, ce paramètre spécifie le nom de compte à utiliser pour l'authentification. Le mot de passe utilisé est le mot de passe Application associé aux paramètres Authentification du pilote.

Default “From” Address (Adresse De par défaut)

Lorsqu'elle est précisée, cette adresse électronique est celle utilisée dans le champ SMTP « De » pour les messages électroniques envoyés par le canal Abonné. Lorsque cette adresse n'est pas indiquée, les éléments <mail> envoyés au canal Abonné doivent contenir un élément <from>.

Tout élément <from> contenu dans des éléments <mail> envoyés au canal Abonné a priorité sur ce paramètre.

Gestionnaires supplémentaires

Lorsqu'il est précisé, ce paramètre correspond à une liste de noms de classes Java séparés par des blancs. Chaque nom de classe est une classe personnalisée qui implémente l'interface com.novell.nds.dirxml.driver.manualtask.CommandHandler et gère un élément XDS personnalisé. Le gestionnaire qui traite l'élément <mail> est un gestionnaire intégré.

Des informations supplémentaires sur les gestionnaires personnalisés sont disponibles dans l'Annexe I, « Pilote de service de tâches manuelles : gestionnaires des éléments personnalisés pour le canal Abonné », page 331.

Configuration du canal Éditeur

Cette section décrit les paramètres du canal Éditeur.

Servlets supplémentaires

Lorsque ce paramètre est précisé, il correspond à une liste de noms de classes Java séparés par des blancs. Chaque nom de classe est une classe personnalisée qui étend javax.servlet.http.HttpServer. Les servlets personnalisées peuvent servir à étendre la fonctionnalité du serveur Web du canal Éditeur.

Des informations supplémentaires sur les servlets personnalisées sont disponibles dans l'Annexe J, « Pilote de service de tâches manuelles : servlets personnalisés pour le canal Éditeur », page 335.

Stratégies de canal Abonné

La configuration des stratégies de canal Abonné dépend de ce qu'une installation particulière accomplira avec le pilote de service de tâches manuelles. Toutefois, certaines instructions peuvent vous aider.

En général, le meilleur endroit pour construire un élément <mail> à envoyer à l'Abonné est la stratégie de transformation de la commande. En effet, la plus grande partie du traitement du moteur DirXML a été effectuée lorsque les commandes atteignent la stratégie de transformation de la commande. Cela signifie que les stratégies de création ont été traitées pour les événements d'ajout (ce qui permet par exemple d'opposer un veto sur les événements d'ajout d'objets qui ne possèdent pas tous les attributs nécessaires à la construction du message électronique). Cela signifie également que les événements de modification d'objets sans association ont déjà été convertis en événements d'ajout.

La feuille de style XSLT qui construit le message électronique peut ou non avoir besoin d'interroger eDirectory pour des informations supplémentaires.

Par exemple, si le message électronique est simplement un message de bienvenue destiné à un employé nouvellement embauché, la commande d'ajout peut contenir toutes les informations nécessaires : prénom, nom et adresse de messagerie Internet. Il faut spécifier dans la stratégie de création que le prénom, le nom et l'adresse de messagerie Internet sont des attributs requis. Ainsi, seules les commandes d'ajout qui contiennent les informations nécessaires peuvent parvenir à la transformation de la commande.

Toutefois, si le message électronique est un message au responsable d'un employé, la feuille de style doit interroger eDirectory. Le DN du responsable s'obtient auprès de l'événement d'ajout de l'objet Utilisateur de l'employé, mais une requête doit être envoyée afin d'obtenir son adresse électronique car ces informations sont un attribut de l'objet Utilisateur du responsable.

En outre, si des notifications par courrier électronique sont générées suite au résultat des commandes de modification d'objets associés au pilote, des requêtes doivent être envoyées afin d'obtenir les informations non contenues dans la commande de modification.

Blocage des commandes pour les empêcher d'atteindre le canal Abonné

Si des messages électroniques doivent être générés à partir d'événements différents des événements d'ajout, les événements d'ajout doivent être autorisés à atteindre le canal Abonné associé aux objets à surveiller. L'autorisation d'envoi des événements d'ajout à l'Abonné donne une valeur d'association générée qui est renvoyée par l'Abonné à Identity Manager.

Il est important que les objets eDirectory qui doivent être surveillés par les stratégies du pilote de service de tâches manuelles aient une association pour le pilote de service de tâches manuelles. Seuls les objets dotés d'une association verront les événements de suppression, de réassignation de nom et de déplacement signalés au pilote. En outre, les événements de modification sur des objets sans association sont convertis en événements d'ajout après la transformation de l'événement sur le canal Abonné.

Toutes les autres commandes (modifier, déplacer, renommer et supprimer) doivent être bloquées par la stratégie de transformation de la commande et ne pourront pas atteindre l'Abonné. L'Abonné gère

uniquement les commandes <add> et les commandes <mail>. Les autres commandes donnent une erreur renvoyée par l'Abonné.

Génération de messages électroniques

Des messages électroniques sont envoyés par le canal Abonné en réponse à la réception d'un élément <mail> qui décrit le message électronique à envoyer. Reportez-vous à l'Annexe G, « Pilote de services de tâches manuelles : référence à l'élément <mail> », page 315 pour voir la description de l'élément <mail> et de son contenu.

Des messages électroniques peuvent être générés en réponse à tout événement Identity Manager (ajout, modification, réassignation de nom, déplacement, suppression).

Les données de remplacement qui sont fournies avec les éléments <message> enfants d'un élément <mail> dépendent de deux facteurs principaux :

- Le modèle utilisé pour générer le corps du message. Les éléments de remplacement devant être utilisés par le modèle de message électronique apparaissent comme enfants de l'élément <replacement-data>.
- Les informations nécessaires aux modèles de page Web sur le canal Éditeur si le message électronique doit donner lieu à une réponse sur ce canal. Les éléments de remplacement devant être utilisés par les modèles de page Web apparaissent comme enfants de l'élément <url-query> qui est un enfant de <url-data>, lui-même enfant de <replacement-data>.

Si le message électronique doit contenir une URL qui pointe sur le serveur Web du canal Éditeur et est utilisée pour solliciter des informations auprès d'un utilisateur, les données de remplacement doivent contenir au moins un élément responder-dn. Les valeurs des éléments « responder-dn » doivent correspondre aux DN des objets Utilisateur des utilisateurs auxquels le message est envoyé.

Si un jeton de remplacement de requête (reportez-vous à la Section , « Données de remplacement », page 216) est utilisé dans le modèle, les données de remplacement pour l'élément <message> doivent contenir un élément nommé src-dn, src-entry-id ou une association à la valeur appropriée. Un élément d'association ne peut être utilisé que si l'objet eDirectory sur lequel porte la requête est déjà doté d'une association pour le pilote de service de tâches manuelles. L'association générée par l'Abonné pour les objets non associés ne peut pas être utilisée parce qu'elle n'a pas été écrite sur l'objet eDirectory lorsque la requête a eu lieu.

L'élément <message> peut spécifier le type MIME du corps du message. Si le type MIME est spécifié mais qu'aucune feuille de style ne l'est (autrement dit, il n'y a pas d'élément <stylesheet> enfant de <message>), une des deux feuilles de style par défaut est utilisée. Si le type MIME a pour valeur text/plain, le nom de la feuille de style par défaut est process_text_template.xsl. Si le type MIME a une valeur autre que text/plain, le nom de la feuille de style par défaut est process_template.xsl.

Modèles de messages électroniques du canal Abonné

Les modèles de messages électroniques sont des documents XML qui contiennent du texte standard et des jetons de remplacement. Ils permettent de générer le texte du corps d'un message. Reportez-vous à la Section , « Modèles », page 214 afin d'obtenir des informations générales sur les modèles.

Les jetons de remplacement utilisés dans un modèle de message électronique déterminent les éléments <item> qui doivent être fournis comme enfants de l'élément <replacement-data> construit par la stratégie du canal Abonné qui construit l'élément <mail>. Par exemple, si le modèle de message électronique comporte le jeton de remplacement $employee-name$, il doit y avoir un

élément <item name=“employee-name”> dans les données de remplacement pour l'élément <message>. Si l'élément du nom employé est absent, le corps du message électronique résultant ne comporte pas de texte dans l'emplacement occupé par le jeton de remplacement dans le modèle.

Les modèles de messages électroniques peuvent être utilisés pour générer des corps de messages au format texte ordinaire, HTML ou XML.

Si un modèle de message électronique génère un message au format texte ordinaire, il doit être traité par une feuille de style qui précise « texte ordinaire » comme type de sortie. Si la feuille de style ne précise pas qu'il s'agit de texte ordinaire, des caractères d'échappement XML indésirables seront générés. La feuille de style par défaut du pilote de services de tâches manuelles, process_text_template.xsl, est normalement utilisée pour traiter les modèles qui produisent des documents au format texte ordinaire.

Stratégies de canal Éditeur

Dans la plupart des implémentations du pilote de service de tâches manuelles, aucune stratégie de canal Éditeur n'est nécessaire. En effet, il est possible de construire la page Web et les modèles XDS pour qu'ils donnent exactement le XDS requis et le XDS n'aura plus besoin ensuite d'être traité par les stratégies.

Si des stratégies sont requises, elles seront très spécifiques à une installation.

Modèles de pages Web du canal Éditeur

Les modèles de pages Web sont des documents XML qui contiennent du texte standard et des jetons de remplacement. Ils permettent de générer des documents de pages Web (généralement des documents HTML). Reportez-vous à la Section , « Modèles », page 214 afin d'obtenir des informations générales sur les modèles.

Les jetons de remplacement dans les modèles de page Web déterminent quelles données de remplacement sont fournies sous la forme de données de requête d'URL sur le canal Abonné. Sur le canal Éditeur, les données de remplacement sont obtenues à partir de la chaîne de requête d'URL correspondant aux requêtes HTTP GET, et à partir de la chaîne de requête d'URL et des données POST correspondant aux requêtes HTTP POST.

Considérez par exemple le flux de données de remplacement du canal Abonné vers le message électronique puis vers le serveur Web du canal Éditeur :

Le pilote de services de tâches manuelles est configuré de telle sorte que le responsable d'un nouvel employé doit assigner à ce dernier un numéro de bureau. L'envoi du message électronique au responsable est déclenché par la commande d'ajout <add> d'un nouvel objet Utilisateur traité par la stratégie de transformation de commande du canal Abonné.

Lorsque le responsable clique sur l'URL qui figure dans le message, une page Web s'affiche dans son navigateur Web. Cette page doit indiquer pour qui le responsable doit entrer un numéro de bureau.

Pour ce faire, l'élément <url-query> du canal Abonné contient un élément de données de remplacement qui identifie le nouvel utilisateur par son nom :

```
<item name=”subject-name”>Joe the Intern</item>
```

La chaîne de requête d'URL contient donc (entre autres) “subject-name=Joe%20the%20Intern” (le “%20” représente un espace codé URL).

Le navigateur Web du responsable soumet l'URL au serveur Web du canal Éditeur dès que le responsable clique sur l'URL dans le message. Le serveur Web construit l'élément de données de remplacement « subject-name » associé à la valeur « Joe le stagiaire ».

Le modèle de page Web également spécifié par l'URL contient le jeton de remplacement $subject-name$. Lorsque le modèle de page Web est traité par la feuille de style pour construire la page Web, le jeton de remplacement est remplacé par « Joe le stagiaire », qui personnalise la page Web correspondant à l'employé dont la création de l'objet Utilisateur a causé l'envoi du message électronique.

Pour obtenir des informations supplémentaires sur une transaction complète canal Abonné à canal Éditeur, reportez-vous à l'Annexe H, « Pilote de services de tâches manuelles : scénario de flux de données pour le nouvel employé », page 319.

Modèles XDS du canal Éditeur

Les modèles XDS sont des documents XML qui contiennent du texte standard et des jetons de remplacement. Les modèles XDS servent à générer des documents XDS qui sont soumis à Identity Manager sur le canal Éditeur du pilote de services de tâches manuelles. Afin d'obtenir des informations générales sur les modèles, reportez-vous à la section Modèles de la section Présentation.

Les jetons de remplacement utilisés dans les modèles XDS déterminent certaines données de remplacement qui sont fournies au serveur Web sous la forme de données de requête HTTP POST.

Considérez par exemple le modèle XDS suivant :

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable">
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

Les jetons de remplacement utilisés dans le modèle indiquent que les données HTTP POST doivent fournir une valeur d'association et une valeur de numéro de bureau.

Normalement, la valeur d'association provient du canal Abonné. Le message électronique du canal Abonné place « association=une certaine valeur » dans la chaîne de requête de l'URL insérée dans le message. Le modèle de page Web utilisé pour générer la page Web lors de la soumission de l'URL au serveur Web place généralement la valeur d'association dans un élément INPUT masqué :

```
<INPUT TYPE="hidden" NAME="association" VALUE="$association$"/>
```

Si on place la valeur d'association comme élément INPUT masqué, la paire « association“une certaine valeur » doit être soumise avec les données HTTP POST.

La valeur de numéro de bureau est entrée dans la page Web à l'aide d'un élément INPUT similaire au suivant :

```
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"/>
```

Si le responsable saisit 1234 et clique sur Soumettre, le navigateur Web envoie « room-number=1234 » parmi les données HTTP POST.

Le serveur Web génère ensuite un élément de données de remplacement <item name="“association”> et un élément de données de remplacement <item name="“room-number”> qui sont utilisés lors du traitement du modèle XDS.

Le document XDS est généré en traitant le modèle XDS à l'aide de la feuille de style spécifiée dans les données POST. Ensuite, le document XDS est soumis à Identity Manager sur le canal Éditeur du pilote de services de tâches manuelles.

Configuration du niveau de trace

Le pilote de service de tâches manuelles émet des messages avec différents niveaux de suivi :

Niveau	Description du message de trace
0	Pas de message de trace
1	Messages à une seule ligne suivant une opération de base
2	Aucun message supplémentaire (le moteur DirXML effectue le suivi des documents XML à ce niveau et aux niveaux supérieurs)
3	Aucun message supplémentaire
4	Messages liés à la construction du document à partir de modèles et de feuilles de style
5	Suivi des documents de données de remplacement

8.2.4 Informations complémentaires

Pour plus d'informations sur les paramètres du pilotes de services de tâches manuelles, reportez-vous aux annexes suivantes :

- Annexe D, « Pilote de services de tâches manuelles : données de remplacement », page 303
- Annexe E, « Pilote de services de tâches manuelles : éléments de données de remplacement automatiques », page 309
- Annexe F, « Pilote de services de tâches manuelles : référence de modèles d'éléments d'opération », page 311
- Annexe G, « Pilote de services de tâches manuelles : référence à l'élément <mail> », page 315
- Annexe H, « Pilote de services de tâches manuelles : scénario de flux de données pour le nouvel employé », page 319
- Annexe I, « Pilote de service de tâches manuelles : gestionnaires des éléments personnalisés pour le canal Abonné », page 331
- Annexe J, « Pilote de service de tâches manuelles : servlets personnalisés pour le canal Éditeur », page 335

Disponibilité élevée

9

Vous pouvez utiliser Identity Manager avec un stockage partagé pour disposer d'une disponibilité élevée. Certaines étapes sont nécessaires pour utiliser Novell® eDirectory™ et Identity Manager dans un environnement en grappes.

Dans cette section :

9.1 Configuration de eDirectory et de Identity Manager pour une utilisation avec un stockage partagé sous Linux et UNIX

Cette section présente les étapes nécessaires pour configurer eDirectory et Identity Manager pour la reprise après échec dans une grappe de disponibilité élevée avec stockage partagé. Les informations de cette section sont générales, elles s'appliquent aux grappes de disponibilité élevée avec stockage partagé sur n'importe quelle plate-forme Linux ou UNIX ; elles ne sont pas spécifiques d'un gestionnaire de grappes particulier.

À la base, les données d'état de eDirectory et de Identity Manager doivent se trouver sur le stockage partagé pour être disponibles pour le noeud de grappe qui exécute actuellement les services. Dans la pratique, le magasin de données eDirectory, qui se trouve généralement dans /var/nds/dib, doit être placé dans la zone de stockage partagé de la grappe. Les données d'état de Identity Manager se trouvent également dans /var/nds/dib. Chaque instance eDirectory sur les noeuds de grappe doit être configurée pour utiliser le magasin de données sur le stockage partagé. D'autres données de configuration eDirectory doivent également résider sur le stockage partagé.

Outre le magasin de données eDirectory, il faut partager les données NICI (Novell International Cryptographic Infrastructure) pour que les clés spécifiques du serveur soient répliquées sur les noeuds de grappe. Plutôt que de déplacer les données NICI dans le stockage partagé, il est généralement préférable de copier les données NICI dans un stockage local sur chaque noeud de grappe. La fonctionnalité NICI cliente est ainsi disponible sur un noeud de grappe même lorsque le noeud de grappe est dans un état secondaire et n'héberge pas le stockage partagé.

Le partage des données eDirectory et NICI est présenté dans les sections suivantes. Il est fondé sur les éléments suivants :

- Vous utilisez les emplacements d'installation par défaut pour les données et la configuration NICI, eDirectory et Identity Manager.

  Les données Identity Manager ne sont pas traitées séparément des données eDirectory parce que les plus intéressantes d'entre elles se trouvent avec les données eDirectory.
- Vous connaissez les procédures d'installation de eDirectory et de Identity Manager.
- Vous utilisez une grappe à deux noeuds.

Une grappe à deux noeuds est de loin la configuration la plus couramment utilisée pour une disponibilité élevée. Cependant, les concepts présentés dans cette section peuvent facilement être étendus à une grappe de *n* noeuds.

Dans cette section :

9.1.1 Installation de eDirectory

Remarque : NICI est installé dans le cadre de l'installation de eDirectory.

1. Installez eDirectory sur le noeud de grappe principal.
2. Configurez eDirectory sur le noeud de grappe principal. Créez une nouvelle arborescence sur le noeud de grappe principal ou installez le serveur dans une arborescence existante. Utilisez pour le nom du serveur eDirectory un nom différent de celui du serveur UNIX. Utilisez un nom qui concerne la grappe plutôt qu'un des noeuds de grappe.
3. Installez la même version de eDirectory sur le noeud de grappe secondaire. Ne configurez pas eDirectory sur le noeud de grappe secondaire.

   Le noeud secondaire ne possède pas d'arborescence séparée.

9.1.2 Installation de Identity Manager

1. Installez Identity Manager sur le noeud de grappe principal via l'option *Serveur méta-annuaire*.

   Le processus d'installation installe les fichiers Identity Manager et configure l'arborescence eDirectory pour une utilisation avec Identity Manager.
2. Installez la même version de Identity Manager sur le noeud de grappe secondaire à l'aide du paramètre de grappe secondaire, en saisissant :

   ```
   dirxml_platform.bin -DCLUSTER_INSTALL="true"
   ```

   Pendant l'installation, choisissez l'option *Serveur méta-annuaire*.

   L'utilisation du paramètre de grappe secondaire permet d'installer les fichiers Identity Manager sans procéder à la moindre configuration eDirectory supplémentaire. Aucune configuration n'est nécessaire dans la mesure où le noeud secondaire ne possède pas d'arborescence séparée.

9.1.3 Partage des données NICI

NICI fournit les services cryptographiques utilisés par eDirectory, Identity Manager et les applications clientes Novell. Utilisé avec eDirectory, NICI fournit des clés spécifiques du serveur. Ces clés spécifiques doivent être identiques sur tous les noeuds de grappe sur lesquels eDirectory est exécuté en tant que service de grappe.

Il existe deux méthodes possibles pour partager les données NICI :

- Placer les données NICI sur le stockage partagé de la grappe.

  L'inconvénient de cette méthode réside dans le fait que les applications qui dépendent de NICI échouent sur un noeud de grappe quand le noeud de grappe n'héberge pas le stockage partagé.
- Copier les données NICI du serveur principal sur le stockage local du serveur secondaire.

Pour copier les données NICI :

1. Renommez /var/novell/nici sur le noeud de grappe secondaire (par exemple, nommez-le /var/novell/nici.sav).
2. Copiez le répertoire /var/novell/nici du noeud de grappe principal vers le noeud de grappe secondaire.

   Pour ce faire, utilisez scp ou créez un fichier tar du répertoire /var/novell/nici sur le noeud principal, transférez-le sur le noeud secondaire et décompressez-le sur le noeud secondaire.

9.1.4 Partage des données eDirectory et Identity Manager

Par défaut, eDirectory stocke son magasin de données dans /var/nds/dib. D'autres éléments de configuration et d'état sont également enregistrés dans /var/nds et dans ses sous-répertoires. Le répertoire de configuration par défaut de eDirectory est /etc. Vous devez accomplir les étapes suivantes pour configurer eDirectory et Identity Manager pour une utilisation avec le stockage partagé dans une grappe à disponibilité élevée. Ces étapes partent de l'hypothèse que le stockage partagé est monté au niveau de /shared.

- « Sur le noeud principal » page 231
- « Sur le noeud secondaire » page 232

Sur le noeud principal

1. Copiez les sous-répertoires de /var/nds vers /shared/var/nds.
2. Renommez le répertoire /var/nds (par exemple, en /var/nds.sav).

   Ce n'est pas obligatoire, mais la création d'une sauvegarde à ce niveau vous offre la possibilité de redémarrer, si besoin, sans avoir à réinstaller eDirectory.
3. Créez un lien symbolique de /var/nds vers /shared/var/nds (par exemple, `ln -s /shared/var/nds /var/nds`).
4. Créez les liens symboliques suivants :

Lien de	Lien vers
/shared/var/nds/class16.conf	/etc/class16.conf
/shared/var/nds/class32.conf	/etc/class32.conf
/shared/var/nds/help.conf	/etc/help.conf
/shared/var/nds/ndsimonhealth.conf	/etc/ndsimonhealth.conf
/shared/var/nds/miscicon.conf	/etc/miscicon.conf
/shared/var/nds/ndsimon.conf	/etc/ndsimon.conf

Lien de	Lien vers
/shared/var/nds/macaddr	/etc/macaddr

5. Faites une copie de sauvegarde de /etc/nds.conf.
6. Déplacez /etc/nds.conf vers /shared/var/nds.
7. Modifiez /shared/var/nds/nds.conf et placez les entrées suivantes dans le fichier (en écrasant toute entrée portant le même nom) :
   - n4u.nds.dibdir=/shared/var/nds/dib
   - n4u.server.configdir=/shared/var/nds
   - n4u.server.vardir=/shared/var/nds
   - n4u.nds.preferred-server=localhost

   Pour les entrées suivantes, remplacez eth0:0 par le nom de l'interface Ethernet partagée de la grappe. Remplacez également lo par le nom de l'interface Ethernet de localhost.
   - n4u.nds.server.interfaces=eth0:0@524,lo@524
   - http.server.interfaces=eth0:0@8008,lo@8008
   - https.server.interfaces=eth0:0@8009,lo@8009
8. Créez un lien symbolique entre /etc/nds.conf et /shared/var/nds/nds.conf.
9. Démarrez ndsd et vérifiez que ndsd fonctionne avec le stockage partagé.
10. Arrêtez ndsd.
11. Placez ndsd dans la liste de ressources à héberger du gestionnaire de grappe.
12. Supprimez ndsd de la liste de daemons à démarrer par le processus init lors de l'amorçage.

Sur le noeud secondaire

1. Renommez le répertoire /var/nds (par exemple, en /var/nds.sav). Ce n'est pas strictement nécessaire, mais les sauvegardes représentent une manière de redémarrer à un point ultérieur à l'installation de eDirectory.
2. Créez un lien symbolique entre /var/nds et /shared/var/nds.
3. Faites une copie de sauvegarde de /etc/nds.conf.
4. Supprimez /etc/nds.conf.
5. Créez un lien symbolique entre /etc/nds.conf et /shared/var/nds/nds.conf.
6. Placez ndsd dans la liste de ressources à héberger du gestionnaire de grappe.
7. Supprimez ndsd de la liste de daemons à démarrer par le processus init lors de l'amorçage.

Une fois les étapes pour les noeuds principal et secondaire terminées, démarrez les services de grappe. eDirectory et Identity Manager démarrent alors sur le noeud principal.

9.1.5 Remarques sur les pilotes Identity Manager

La plupart des pilotes Identity Manager peuvent être exécutés dans une configuration en grappe. Les éléments suivants doivent toutefois être pris en considération :

- Les exécutables du pilote (fichiers .jar et/ou objets partagés) doivent être installés sur chaque noeud de la grappe.
- Si le pilote doit être exécuté sur le même serveur que l'application prise en charge par le pilote, l'application doit également être configurée pour être exécutée dans le cadre des services de grappe.
- S'il est possible de configurer un emplacement pour les données d'état spécifiques du pilote, cet emplacement doit se trouver sur le stockage partagé de la grappe.

  Exemple : le pilote LDAP utilisé sans journal des modifications ou le pilote JDBC utilisé en mode sans déclencheur.
- Si les données de configuration du pilote sont stockées en dehors de eDirectory, elles doivent se trouver sur le stockage partagé ou être dupliquées sur chaque noeud de grappe. Exemple : les répertoires du modèle du pilote de tâches manuelles.

9.2 Étude de cas pour SuSE Linux

Pour une description de l'exécution de Identity Manager sur un stockage partagé avec SUSE LINUX Enterprise Server 8, reportez-vous au document TID10093317 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm).

Consignation et création de rapports avec Novell Audit

10

Identity Manager est paramétré pour utiliser Novell® Audit à des fins d'audit et de création de rapport.

10.1 Présentation

Novell Audit est un recueil de technologies fournissant des capacités de surveillance, de consignation, de création de rapports et de notification. Grâce à l'intégration avec Novell Audit, Identity Manager fournit des informations détaillées sur l'état actuel et passé de l'activité du pilote et du moteur. Ces informations sont fournies par un ensemble de rapports préconfigurés, de services de notification standard et d'une consignation définie par l'utilisateur.

Vous pouvez surveiller les événements Identity Manager en temps réel, envoyer des notifications par courrier électronique pour tous les événements Identity Manager et générer des rapports sur l'activité de Identity Manager à l'aide de Novell Audit.

Les types de messages envoyés à Novell Audit sont contrôlés à l'aide de plugs-in semblables à ceux du service de création de rapport et de notification (RNS - Reporting and Notification Service). Des niveaux supplémentaires sont ajoutés à ces plugs-in pour sélectionner le type d'opérations ou d'informations de débogage que vous souhaitez suivre, telles que l'état, l'ajout d'entrées, la recherche, etc.

Services de création de rapport et de notification (RNS - Reporting and Notification Services)

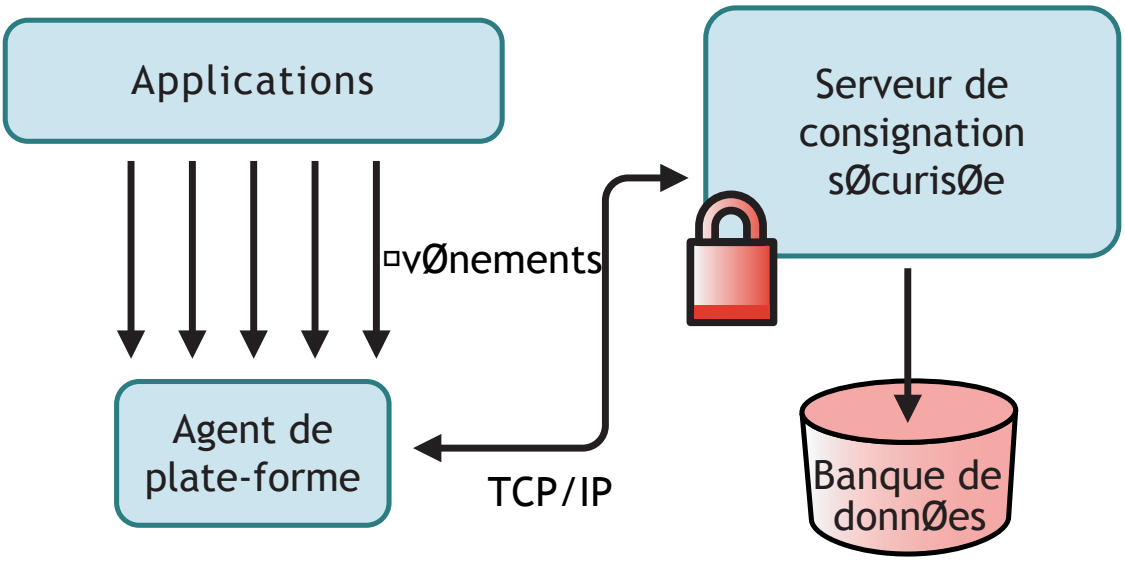
Bien que le service de création de rapport et de notification RNS soit décrié, le moteur méta-annuaire continue à traiter les fonctions RNS si vous utilisez actuellement ce service. Envisagez de passer à Novell Audit, car il étend les fonctionnalités apportées par le service RNS. De plus, ce dernier pourrait ne plus être pris en charge dans les versions futures de Identity Manager. Pour plus d'informations sur le service RNS, reportez-vous au manuel *DirXML 1.1a Administration Guide (Guide d'administration de DirXML 1.1a)* (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html).

10.2 Novell Audit

Novell Audit est un service de consignation multiplates-formes centralisé qui peut consigner les données de plusieurs applications dans une banque de données centralisée. Une fois les données d'événement consignées, vous pouvez exécuter des rapports détaillés, personnaliser des requêtes et déclencher l'envoi de notifications en fonction des événements consignés.

La figure suivante illustre l'architecture de Novell Audit :

Figure 10-1 *Présentation de l'architecture*



Sur cette illustration, Identity Manager est l'une des applications qui utilisent l'agent de plate-forme pour envoyer des rapports sur les événements au serveur de consignation sécurisée Novell Audit.

10.3 Installation de Novell Audit

Comme nous l'avons déjà vu dans la présentation, Novell Audit contient deux composants fondamentaux :

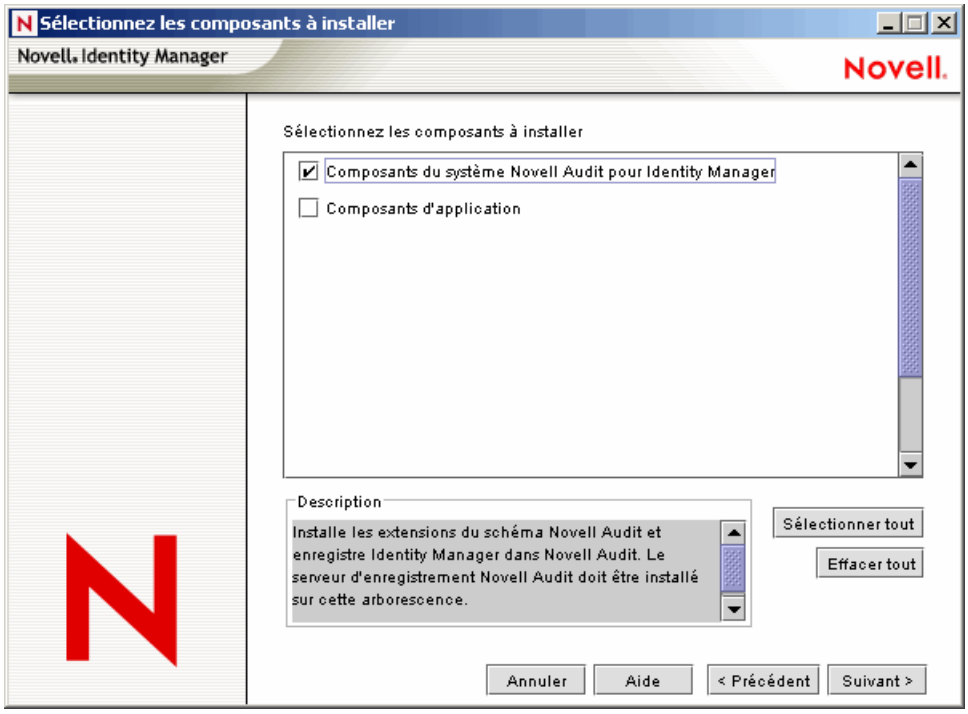
- Agent de plate-forme
- Serveur de consignation sécurisée

L'agent de plate-forme est le composant exécuté avec Identity Manager pour communiquer des événements au serveur de consignation sécurisée. Il s'installe avec Identity Manager. Le serveur de consignation sécurisée est le composant qui reçoit des données d'événement de Identity Manager et d'autres applications ; il est installé séparément de Identity Manager, avec Novell Audit 1.0.3.

10.3.1 Configuration de l'agent de plate-forme

Pour installer l'agent de plate-forme, sélectionnez l'option Composants du système Novell Audit pour Identity Manager pendant l'installation.

Figure 10-2 *Installation de Identity Manager*



Vous pouvez installer l'agent de plate-forme en même temps que Identity Manager ou plus tard.

Remarque : si vous installez l'agent de plate-forme après le démarrage du moteur méta-annuaire, Identity Manager doit être redémarré pour être lié à l'agent de plate-forme. Identity Manager n'essaie de se connecter à l'agent de plate-forme que lors du démarrage.

Une fois l'agent de plate-forme installé, procédez comme suit pour le configurer :

1. Ouvrez le fichier de configuration de Novell Audit, `logevent.cfg`, dans un éditeur de texte. L'emplacement par défaut de ce fichier est :

Système d'exploitation	Chemin d'accès
NetWare®	`sys:\etc\logevent.cfg`
Fenêtres	*`windows_directory`*`\logevent.cfg`
Linux\Solaris	`/etc/logevent.conf`

2. Remplacez la valeur du paramètre LogHost par l'adresse IP ou le nom DNS de votre serveur de consignation sécurisée.
3. Redémarrez Identity Manager.

10.3.2 Configuration du serveur de consignation sécurisée

Remarque : le serveur de consignation sécurisée Novell Audit n'est pas fourni avec Identity Manager. Il fait partie de Novell Audit 1.0.3. Pour plus d'informations sur le téléchargement de Novell Audit 1.0.3, reportez-vous à la page du produit Novell Audit (http://www.novell.com/products/nsureaudit).

Le serveur de consignation sécurisée fonctionne sous NetWare 5.1 ou version ultérieure, Windows* NT 4.0, Windows 2000 Server, Windows 2003 Server, Solaris* 8 ou 9 et différentes versions de Linux*, y compris SUSE* Enterprise Linux Server 8 et SUSE 9.0.

Le serveur de consignation sécurisée peut consigner des événements vers les applications MySQL*, Oracle*, Microsoft* SQL Server, Java* et plusieurs autres emplacements, y compris les fichiers plats. Novell Audit contient une application personnalisée, Novell Audit Report, conçue pour interroger les bases de données et y rechercher des données d'événements. Vous devez utiliser une banque de données équipée d'un connecteur ODBC pour utiliser cet outil de création de rapports avancé.

Un guide de démarrage rapide contenant les instructions de configuration du serveur de consignation sécurisée est disponible pour chaque plate-forme ; il est compris dans l'installation de Novell Audit 1.0.3. Les guides de démarrage rapide peuvent aussi être consultés sur le Web, avec le manuel *Novell Audit 1.0.3 Administration Guide (Guide d'administration de Novell Audit 1.0.3)* sur le site Web de la documentation Novell Audit (http://www.novell.com/documentation/nsureaudit).

10.4 Configuration de la consignation

Identity Manager permet de configurer les événements consignés selon différents niveaux prédéfinis ou en sélectionnant individuellement chaque événement à consigner. Les modifications des paramètres de configuration sont également consignées.

Les événements définis par l'utilisateur, présentés à la Section 10.4.2, « Événements définis par l'utilisateur », page 244, sont consignés à chaque fois que la consignation est activée ; ils ne sont jamais filtrés par le moteur méta-annuaire.

La consignation se configure sur un ensemble de pilotes ou sur un pilote individuel. Les pilotes peuvent hériter de la configuration de consignation de leur ensemble de pilotes. Pour plus d'informations sur les attributs eDirectory™ contenant des informations de consignation, reportez-vous à la Section 10.4.3, « Objets eDirectory », page 246.

Par défaut, seuls les événements critiques et définis par l'utilisateur sont consignés.

10.4.1 Sélection des événements à consigner

Vous pouvez sélectionner des événements pour un ensemble de pilotes ou pour un pilote spécifique.

Consignation des événements pour un ensemble de pilotes :

1. Dans iManager, sélectionnez *Identity Manager* > *Présentation de Identity Manager*, puis cliquez sur *Suivant*.
2. Recherchez et sélectionnez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.

3 Cliquez sur le nom de l'ensemble de pilotes. La page de modification de l'objet apparaît.

4 Dans l'onglet *Identity Manager*, sélectionnez *Niveau de consignation*.

5 Sélectionnez l'option de consignation requise pour votre environnement.

Option	Description
Consigner les erreurs	Il s'agit du niveau de consignation par défaut. Cette option permet de consigner tous les événements en erreur, ainsi que les événements définis par l'utilisateur. Lorsque cette option est sélectionnée, vous ne recevez que les événements dont l'ID décimal est 196646, avec un message d'erreur dans le premier champ textuel.
Consigner les erreurs et les avertissements	Cette option permet de consigner tous les événements en erreur ou en avertissement, ainsi que les événements définis par l'utilisateur. Lorsque cette option est sélectionnée, vous ne recevez que les événements dont l'ID décimal est 196646 et 196647, avec un message d'erreur ou d'avertissement dans le premier champ textuel.

Option	Description
Consigner des événements spécifiques	Cette option permet de sélectionner dans une liste les événements spécifiques à consigner. Cliquez sur l'icône pour sélectionner les événements. Les événements définis par l'utilisateur sont toujours consignés. Pour consigner tout événement autre qu'une erreur ou un avertissement, vous devez le sélectionner dans cette liste. Si vous sélectionnez cette option, vous devez également sélectionner les erreurs et les avertissements si vous souhaitez continuer à les consigner. Pour une liste de tous les événements disponibles, reportez-vous à « Événements Identity Manager » page 242.
Mettre à jour l'heure de la dernière consignation uniquement	Seuls les événements définis par l'utilisateur sont consignés. Lors d'un événement, la dernière heure de consignation est mise à jour pour que vous puissiez voir l'heure et la date de la dernière erreur dans le journal d'état.
Se déloguer	Seuls les événements définis par l'utilisateur sont consignés.
Désactiver la consignation dans les journaux DriverSet, Subscriber et Publisher	Désactive la consignation dans le journal de l'objet Driver Set, et dans les journaux Subscriber et Publisher.
Nombre maximal d'entrées du journal	Ce paramètre permet de spécifier le nombre maximal d'entrées à consigner dans les journaux d'état. Pour plus de détails, reportez-vous à la Section 10.7.2, « Affichage des journaux d'état », page 250.

6 Une fois les événements que vous souhaitez consigner sélectionnés, cliquez sur *OK*.

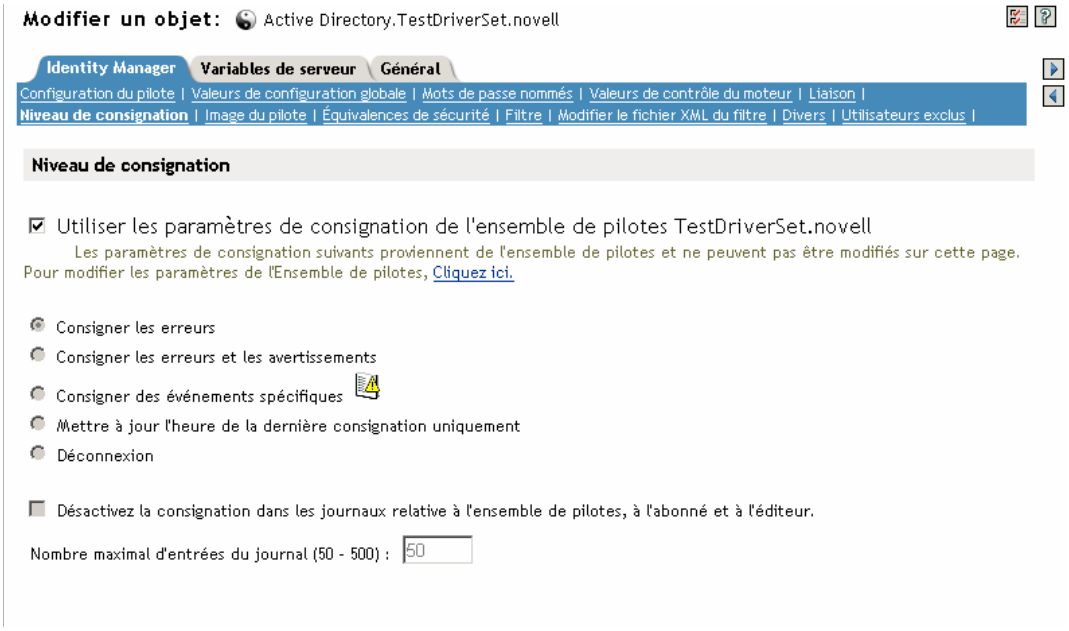
Consignation des événements pour un pilote :

1 Dans iManager, sélectionnez *Identity Manager* > *Présentation de Identity Manager*, puis cliquez sur *Suivant*.

2 Recherchez et sélectionnez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.

3 Cliquez dans l'angle supérieur droit de l'icône du pilote, puis sélectionnez *Éditer les propriétés*.

4 Dans l'onglet *Identity Manager*, sélectionnez *Niveau de consignation*.



5 (Facultatif) Par défaut, l'objet Pilote est configuré pour hériter ses paramètres de consignation de l'objet Ensemble de pilotes. Pour sélectionner les événements consignés pour le pilote en question uniquement, désactivez l'option Utiliser les paramètres de consignation de l'ensemble de pilotes.

6 Sélectionnez l'option de consignation requise pour votre environnement.

Option	Description
Consigner les erreurs	Il s'agit du niveau de consignation par défaut. Cette option permet de consigner tous les événements en erreur, ainsi que les événements définis par l'utilisateur. Lorsque cette option est sélectionnée, vous ne recevez que les événements dont l'ID décimal est 196646, avec un message d'erreur dans le premier champ textuel.
Consigner les erreurs et les avertissements	Cette option permet de consigner tous les événements en erreur ou en avertissement, ainsi que les événements définis par l'utilisateur. Lorsque cette option est sélectionnée, vous ne recevez que les événements dont l'ID décimal est 196646 et 196647, avec un message d'erreur ou d'avertissement dans le premier champ textuel.

Option	Description
Consigner des événements spécifiques	Cette option permet de sélectionner dans une liste les événements spécifiques à consigner. Cliquez sur l'icône pour sélectionner les événements. Les événements définis par l'utilisateur sont toujours consignés. Pour consigner tout événement autre qu'une erreur ou un avertissement, vous devez le sélectionner dans cette liste. Si vous sélectionnez cette option, vous devez également sélectionner les erreurs et les avertissements si vous souhaitez continuer à les consigner. Pour une liste de tous les événements disponibles, reportez-vous à « Événements Identity Manager » page 242.
Mettre à jour l'heure de la dernière consignation uniquement	Seuls les événements définis par l'utilisateur sont consignés. Lors d'un événement, la dernière heure de consignation est mise à jour pour que vous puissiez voir l'heure et la date de la dernière erreur dans le journal d'état.
Consignation désactivée	Seuls les événements définis par l'utilisateur sont consignés.
Désactiver la consignation dans les journaux DriverSet, Subscriber et Publisher	Désactive la consignation dans le journal de l'objet Driver Set, et dans les journaux Subscriber et Publisher.
Nombre maximal d'entrées du journal	Ce paramètre permet de spécifier le nombre maximal d'entrées à consigner dans les journaux d'état. Pour plus de détails, reportez-vous à la Section 10.7.2, « Affichage des journaux d'état », page 250.

7 Une fois les événements que vous souhaitez consigner sélectionnés, cliquez sur *OK*.

Événements Identity Manager

La liste de tous les événements consignés par Identity Manager figure dans l'Annexe C, « Événements et rapports Identity Manager », page 271.

Événements de démarrage et d'arrêt du pilote

Identity Manager peut générer un événement à chaque démarrage ou arrêt d'un pilote. Le tableau suivant recense les détails de ces événements :

Tableau 10-1 *Événements de démarrage et d'arrêt du pilote*

Événement	Niveau de consignation	Informations
EV_LOG_DRIVER_START	LOG_INFO	Pour consigner les démarrages du pilote, vous devez utiliser l'option *Consigner des événements spécifiques*, puis sélectionner cet événement.

Événement	Niveau de consignation	Informations
EV_LOG_DRIVER_STOP	LOG_WARNING	Pour consigner les arrêts du pilote, sélectionnez *Consigner les erreurs et les avertissements* ou utilisez l'option *Consigner des événements spécifiques* et sélectionnez cet événement.

Pour plus d'informations sur la création de notifications Novell Audit fondées sur ces événements, reportez-vous à la Section 10.6, « Envoi de notifications fondées sur les événements », page 248.

Événements d'erreur et d'avertissement

Identity Manager génère un événement à chaque fois qu'il rencontre une erreur ou un avertissement. Le tableau suivant recense les détails de ces événements :

Tableau 10-2 *Événements d'erreur et d'avertissement*

Événement	Niveau de consignation	Informations
DirXML_Error	LOG_ERROR	Toutes les erreurs Identity Manager consignent cet événement. Le code d'erreur rencontré est enregistré dans l'événement. Pour consigner les erreurs, sélectionnez *Consigner les erreurs*, *Consigner les erreurs et les avertissements* ou utilisez l'option *Consigner des événements spécifiques* et sélectionnez cet événement.
DirXML_Warning	LOG_WARNING	Tous les avertissements Identity Manager consignent cet événement. Le code d'avertissement rencontré est enregistré dans l'événement. Pour consigner les avertissements, sélectionnez *Consigner les erreurs et les avertissements* ou utilisez l'option *Consigner des événements spécifiques* et sélectionnez cet événement.

Pour plus d'informations sur la création de notifications Novell Audit fondées sur ces événements, reportez-vous à la Section 10.6, « Envoi de notifications fondées sur les événements », page 248.

Événements du chargeur distant

Les événements suivants sont consignés à partir du chargeur distant :

Tableau 10-3 *Événements du chargeur distant*

Événement	Niveau de consignation	Informations
Démarrage du chargeur distant	LOG_INFO	Pour consigner les démarrages du chargeur distant, vous devez utiliser l'option *Consigner des événements spécifiques*, puis sélectionner cet événement.
Arrêt du chargeur distant	LOG_INFO	Pour consigner les arrêts du chargeur distant, vous devez utiliser l'option *Consigner des événements spécifiques*, puis sélectionner cet événement.
Connexion au chargeur distant établie	LOG_INFO	Pour consigner l'établissement des connexions au chargeur distant, vous devez utiliser l'option *Consigner des événements spécifiques*, puis sélectionner cet événement.
Connexion au chargeur distant perdue	LOG_INFO	Pour consigner les interruptions de la connexion au chargeur distant, vous devez utiliser l'option *Consigner des événements spécifiques*, puis sélectionner cet événement.

Pour plus d'informations sur la création de notifications Novell Audit fondées sur ces événements, reportez-vous à la Section 10.6, « Envoi de notifications fondées sur les événements », page 248.

10.4.2 Événements définis par l'utilisateur

Identity Manager permet de configurer vos propres événements à consigner dans Novell Audit. Vous pouvez consigner les événements à l'aide d'une opération dans le Générateur de stratégies ou dans une feuille de style. Toutes les informations auxquelles vous avez accès lorsque vous définissez des stratégies peuvent être consignées.

ID d'événement

Les ID d'événement compris entre1 000 et 1 999 sont réservés aux événements définis par l'utilisateur. Vous devez spécifier une valeur dans cette plage pour l'ID d'événement lorsque vous définissez vos propres événements. Dans Novell Audit, cet ID est combiné avec l'ID de l'application Identity Manager, 003.

Niveaux de consignation

Les niveaux de consignation permettent de grouper des événements en fonction du type d'événement consigné. Les niveaux de consignation prédéfinis suivants sont disponibles :

Tableau 10-4 *Niveaux de consignation*

Niveau de consignation	Description
log-emergency	Événements qui entraînent la fermeture du moteur méta-annuaire ou du pilote.

Niveau de consignation	Description
log-alert	Événements qui nécessitent une attention immédiate.
log-critical	Événements susceptibles de provoquer un dysfonctionnement de certaines parties du moteur méta-annuaire ou du pilote.
log-error	Événements qui décrivent des erreurs pouvant être traitées par le moteur méta-annuaire ou le pilote.
log-warning	Événements négatifs ne représentant pas un problème.
log-notice	Événements (positifs ou négatifs) qu'un administrateur peut utiliser pour comprendre ou améliorer l'utilisation et les opérations.
log-info	Événements positifs de quelque importance que ce soit.
log-debug	Événements significatifs pour l'assistance technique ou les ingénieurs chargés de déboguer le moteur méta-annuaire ou le pilote.

Génération d'événements avec le Générateur de stratégies

Dans le Générateur de stratégies, pour consigner des événements, sélectionnez l'opération *Générer un événement*.

1. Sélectionnez la condition nécessaire à la génération de l'événement, puis sélectionnez l'opération *Générer un événement*.
2. Spécifiez un ID d'événement.
3. Sélectionnez un niveau de consignation.
4. Cliquez sur l'icône près du champ *Saisissez des chaînes* pour lancer le Générateur de chaînes nommées.
5. Utilisez le Générateur de chaînes nommées pour élaborer des chaînes nommées correspondant aux champs de données personnalisés :

6. Cliquez sur *OK* pour retourner au Générateur de stratégies et élaborer le reste de votre stratégie.

Reportez-vous à la section « Generate Event (Génération d'événements) » du *Policy Builder and Driver Customization Guide (Guide de création des stratégies et de personnalisation des pilotes)* pour plus d'informations sur la configuration des stratégies pour la consignation des événements.

Génération d'événements avec des documents d'état

Les documents d'état générés à l'aide de feuilles de style avec l'élément <xsl:message> sont envoyés à Novell Audit avec un ID d'événement qui correspond à l'attribut de niveau du document d'état spécifié dans le tableau suivant :

Tableau 10-5 *Documents d'état*

Niveau d'état	ID d'événement d'état
Succès	EV_LOG_STATUS_SUCCESS (1)
Réessayer	EV_LOG_STATUS_RETRY (2)
Avertissement	EV_LOG_STATUS_WARNING (3)
Erreur	EV_LOG_STATUS_ERROR (4)
Fatal	EV_LOG_STATUS_FATAL (5)
Défini par l'utilisateur	EV_LOG_STATUS_OTHER (6)

L'exemple suivant génère l'événement Novell Audit 0x004 et la valeur value1=7777, avec le niveau EV_LOG_STATUS_ERROR:

```
<xsl:message>
   <status level="error" text1="This would be text1" value="7777">This
data would be in the blob and in text 2, since no value is specified
for text2 in the attributes.</status>
</xsl:message>
```

L'exemple suivant génère l'événement Novell Audit 0x004 et la valeur value1=7778, avec le niveau EV_LOG_STATUS_ERROR:

```
<xsl:message>
   <status level="error" text1="This would be text1" text2="This would
be text2" value1="7778">This data would be in the blob only for this
case, since a value for text2 is specified in the attributes.</status>
</xsl:message>
```

10.4.3 Objets eDirectory

Cette section présente les détails des attributs Novell eDirectory où sont stockées les données de consignation. Vous n'avez pas besoin de modifier ces attributs directement, car ces objets sont automatiquement configurés en fonction des sélections que vous avez effectuées dans iManager.

Les événements Identity Manager que vous souhaitez consigner sont stockés dans l'attribut DirXML-LogEvent sur l'objet Ensemble de pilotes ou l'objet Pilote. L'attribut est un entier à plusieurs valeurs, chaque valeur identifiant un ID d'événement à consigner.

Avant de consigner un événement, le moteur compare le type d'événement actuel au contenu de cet attribut pour déterminer si cet événement doit être consigné.

Les versions précédentes de Identity Manager utilisaient l'attribut DirXML-DriverTraceLevel pour configurer les niveaux de consignation. Le niveau de consignation était spécifié sur chaque objet Pilote et ne prenait pas en charge l'héritage. À partir de la version 2 de Identity Manager, les objets Pilote peuvent hériter ces informations de l'objet Ensemble de pilotes. L'attribut DirXML-DriverTraceLevel d'un objet Pilote a la plus haute priorité lors de la détermination des paramètres de consignation. Si un objet Pilote ne contient pas d'attribut DirXML-DriverTraceLevel, le moteur utilise les paramètres de consignation de l'objet Ensemble de pilotes parent.

10.5 Lancement de requêtes et création de rapports

Novell Audit propose deux outils permettant de lancer des requêtes sur des événements dans la base de données Novell Audit : le plug-in Novell Audit iManager et Novell Audit Report (LReport).

Le plug-in Novell Audit iManager est une application de requête de base de données JDBC basée sur le Web qui permet de créer rapidement et de stocker des requêtes à l'aide de listes déroulantes et de macros.

Novell Audit Report est une application compatible ODBC, basée sur Windows qui peut utiliser les instructions de requête SQL ou les rapports Crystal Decision pour interroger les magasins de données Oracle et MySQL (ou toute autre base de données qui prend en charge les pilotes ODBC).

Suivez les instructions du manuel *Novell Audit Administration Guide (Guide d'administration de Novell Audit)* pour accéder au plug-in Novell Audit iManager ou pour configurer Novell Audit Report. Ce manuel est disponible sur le site Web de documentation Novell Audit (http://www.novell.com/documentation/nsureaudit).

10.5.1 Rapports Identity Manager

Identity Manager propose un certain nombre de rapports Crystal Decision (*.rpt) qui simplifient la collecte d'informations sur les opérations courantes effectuées dans Identity Manager. Ces rapports se trouvent sur le CD d'installation de Identity Manager.

Une fois Novell Audit Report configuré, ces rapports, ainsi que les requêtes et rapports personnalisés que vous avez définis, peuvent être exécutés. Reportez-vous à la section Working with Reports in Novell Audit Report (Utilisation des rapports dans Novell Audit Report) (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/alsn2fj.html) du *Novell Audit 1.0.3 Administration Guide (Guide d'administration de Novell Audit 1.0.3* pour plus d'informations sur l'utilisation de ces rapports dans Novell Audit Report. Vous trouverez des exemples de rapports dans la Section C.11, « Rapports », page 294 de l'Annexe C, « Événements et rapports Identity Manager », page 271.

10.5.2 Affichage des événements Identity Manager

1. Dans l'espace de travail Novell Audit Report, cliquez dans l'onglet *Événements*, puis développez le dossier *DirXML*.

   Cette liste contient tous les événements Identity Manager prédéfinis. Double-cliquez sur n'importe quel événement dans la liste pour afficher ses propriétés.

2. Pour lancer une requête de recherche d'un événement Identity Manager, cliquez avec le bouton droit de la souris dans l'espace de travail, puis sélectionnez *Define Query (Définir une requête)*.

3. Quand le Query Expert (Expert en requêtes) s'affiche, spécifiez une plage horaire et vérifiez l'événement.

4. Pour exécuter cette requête, sélectionnez l'onglet *Query (Requête)* dans l'espace de travail, cliquez avec le bouton droit de la souris sur le nom de la requête, puis sélectionnez *Run (Exécuter)*.

Vous pouvez aussi créer des requêtes à l'aide d'instructions SQL. Tous les événements Identity Manager sont associés à un ID d'événement décimal compris entre 109608 et 262144.

10.6 Envoi de notifications fondées sur les événements

Novell Audit permet d'envoyer une notification si un événement spécifique a ou n'a pas lieu. Les notifications peuvent être envoyées en fonction d'un ou de plusieurs événements et de toute valeur contenue dans ces événements. Elles peuvent être envoyées à n'importe quel canal de consignation, ce qui permet de consigner des notifications dans une base de données, une application Java ou un système de gestion SNMP, ou plusieurs autres emplacements.

Pour plus d'informations sur la création de notifications, reportez-vous à la section« Configuring Filters and Event Notifications (Configuration des filtres et des notifications d'événements) » du *Novell Audit 1.0.3 Administration Guide (Guide d'administration de Novell Audit 1.0.3)* (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/al0lg08.html#al0lg08).

10.7 Utilisation des journaux d'état

Outre les fonctionnalités de Novell Audit, Identity Manager consigne un certain nombre d'événements sur l'objet Ensemble de pilotes et l'objet Pilote. Ces journaux d'état proposent une vue de l'activité récente de Identity Manager. Lorsque le journal atteint la taille définie, la moitié la plus ancienne du journal est supprimée de manière définitive pour faire de la place pour les événements les plus récents. Ainsi, tout événement que vous souhaitez suivre dans le temps doit être consigné dans Novell Audit ou dans le service de création de rapports et de notification RNS.

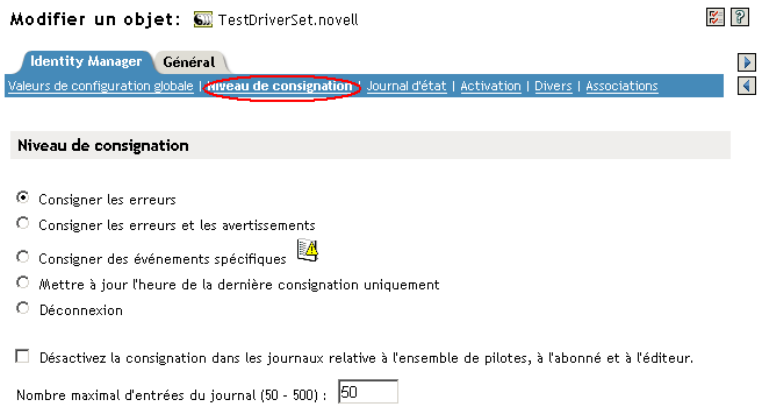
10.7.1 Définition de la taille maximale du journal

Les journaux d'état peuvent être configurés pour contenir de 50 à 500 événements. Ce paramètre peut être configuré sur l'objet Ensemble de pilotes et être hérité par tous les pilotes de l'ensemble ou bien encore être configuré pour chaque pilote de l'ensemble. La taille maximale du journal est indépendante des événements que vous voulez consigner ; vous pouvez donc configurer les événements que vous souhaitez consigner sur l'ensemble de pilotes, puis spécifier une taille de journal différente pour chaque pilote dans l'ensemble.

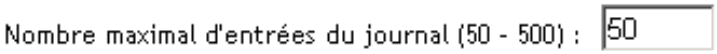
Définition de la taille du journal sur l'ensemble de pilotes

1. Dans iManager, sélectionnez *Identity Manager* > *Présentation de Identity Manager*, puis cliquez sur *Suivant*.
2. Recherchez et sélectionnez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.
3. Cliquez sur le nom de l'ensemble de pilotes. La fenêtre Modifier l'objet s'affiche.

4 Dans l'onglet *Identity Manager*, sélectionnez *Niveau de consignation*.



5 Spécifiez la taille maximale du journal dans le champ *Nombre maximal d'entrées du journal* :



6 Une fois le nombre maximal spécifié, cliquez sur *OK*.

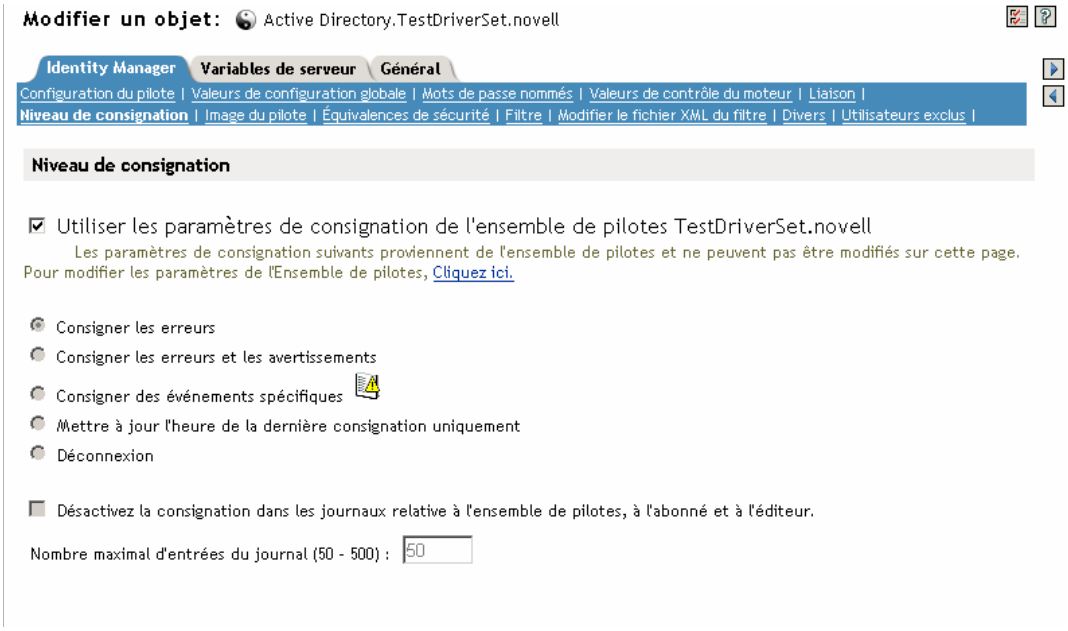
Définition de la taille du journal sur le pilote

1 Dans iManager, sélectionnez *Identity Manager* > *Présentation de Identity Manager*, puis cliquez sur *Suivant*.

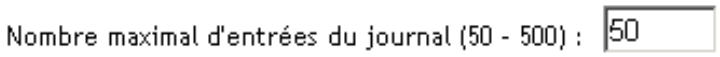
2 Recherchez et sélectionnez l'objet Ensemble de pilotes, puis cliquez sur *Rechercher*.

3 Cliquez dans l'angle supérieur droit de l'icône du pilote, puis sélectionnez *Éditer les propriétés*.

4 Dans l'onglet *Identity Manager*, sélectionnez *Niveau de consignation*.



5 Spécifiez la taille maximale du journal dans le champ *Nombre maximal d'entrées du journal* :



6 Une fois le nombre maximal spécifié, cliquez sur *OK*.

10.7.2 Affichage des journaux d'état

Les entrées des journaux d'état sont représentées dans iManager par une icône de journal d'état . Où que vous voyiez cette icône dans iManager, cela signifie que vous pouvez consulter un journal à court terme. Les journaux d'état suivants sont disponibles :

- Sur l'ensemble de pilotes.
- Sur le canal Éditeur pour chaque pilote de l'ensemble.
- Sur le canal Abonné pour chaque pilote de l'ensemble.

Les journaux d'état des canaux Éditeur et Abonné contiennent des messages spécifiques à chaque canal générés par le pilote, par exemple les messages indiquant qu'une opération s'est heurtée à un veto pour un objet non associé.

Le journal d'état d'un ensemble de pilotes ne contient que les messages générés par le moteur, notamment les messages signalant les changements d'état des pilotes de l'ensemble. Tous les messages du moteur sont consignés.

Utilitaire de ligne de commande DirXML

A

L'utilitaire et les scripts sont installés sur toutes les plates-formes pendant l'installation de Identity Manager. L'utilitaire est installé aux emplacements suivants :

- Windows : `\Novell\Nds\dxcmd.bat`
- NetWare : `sys:\system\dxcmd.ncf`
- UNIX : `/usr/bin/dxcmd`

L'utilitaire de ligne de commande DirXML est utilisable selon deux méthodes différentes.

A.1 Mode interactif

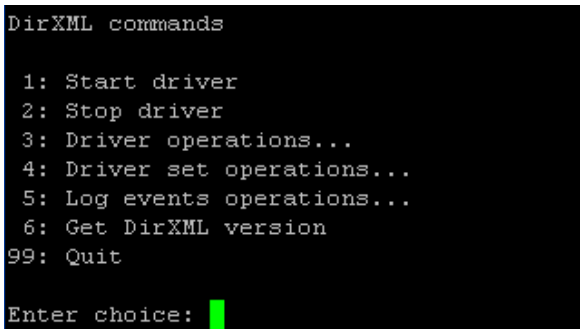
Le mode interactif propose une interface textuelle qui permet de commander et d'utiliser l'utilitaire de ligne de commande DirXML.

1. À l'invite de la console, saisissez `dxcmd`.
2. Saisissez le nom d'un utilisateur disposant des droits suffisants sur les objets Identity Manager.

   Exemple : admin.novell
3. Saisissez le mot de passe de l'utilisateur spécifié plus haut.

   Exemple : novell

   Figure A-1 *Commandes DXCMD*

4. Saisissez le numéro de la commande à exécuter.

   Le Tableau A-1 page 252 contient la liste des options et des fonctions disponibles.
5. Pour quitter l'utilitaire, saisissez 99.

Remarque : si vous exécutez eDirectory™ 8.8 sous Unix/Linux, vous devez spécifier les paramètres -host et -port. Exemple : `dxcmd -host 10.0.0.1 -port 524`. Si ces paramètres ne sont pas spécifiés, l'erreur jclient est renvoyée.

```
novell.jclient.JCException: connect (to address) 111 UNKNOWN ERROR
```

Par défaut, eDirectory 8.8 n'écoute pas localhost. L'utilitaire de ligne de commande DirXML doit résoudre l'adresse IP du serveur ou le nom d'hôte et le port pour pouvoir s'authentifier.

Tableau A-1 *Options du mode interactif*

Option	Description
1 : Démarrer le pilote	Démarre le pilote. S'il y a plusieurs pilotes, chacun d'eux est accompagné d'un numéro. Saisissez le numéro du pilote que vous souhaitez démarrer.
2 : Arrêter le pilote	Arrête le pilote. S'il y a plusieurs pilotes, chacun d'eux est accompagné d'un numéro. Saisissez le numéro du pilote que vous souhaitez arrêter.
3 : Actions du pilote...	Affiche la liste des opérations disponibles pour le pilote. S'il y a plusieurs pilotes, chacun d'eux est accompagné d'un numéro. Saisissez le numéro du pilote pour lequel vous souhaitez afficher les opérations disponibles. Reportez-vous au Tableau A-2 page 253 pour connaître les opérations disponibles.
4 : Actions du jeu de pilotes...	Affiche la liste des opérations disponibles pour l'ensemble de pilotes. • 1 : Associer l'ensemble de pilotes au serveur • 2 : Dissocier l'ensemble de pilotes du serveur • 99 : Quitter
5 : Actions de consignation des événements...	Affiche la liste des opérations disponibles pour la consignation des événements avec Novell Audit. Reportez-vous au Tableau A-5 page 257 pour voir la description de ces options.
6 : Obtenir la version de DirXML	Indique la version de Identity Manager installée.
99 : Quitter	Quitte l'utilitaire de ligne de commande DirXML.

Figure A-2 *Options de pilote*

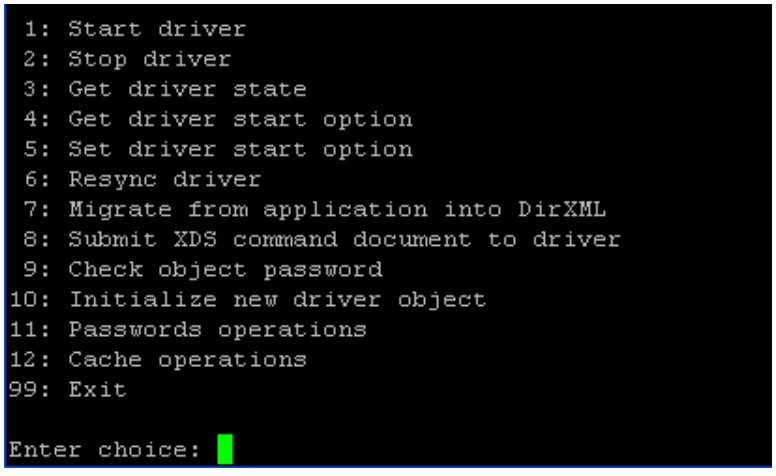


Tableau A-2 *Options de pilote*

Opération	Description
1 : Démarrer le pilote	Démarre le pilote.
2 : Arrêter le pilote	Arrête le pilote.
3 : Obtenir l'état du pilote	Indique l'état du pilote. • 0 - Le pilote est arrêté • 1 - Démarrage du pilote • 2 - Le pilote est en cours d'exécution • 3 - Le pilote est en cours d'arrêt
4 : Obtenir l'option de démarrage du pilote	Indique l'option actuelle de démarrage du pilote. • 1 - Désactivé • 2 - Manuel • 3 - Auto
5 : Définir l'option de démarrage du pilote	Modifie l'option de démarrage du pilote. • 1 - Désactivé • 2 - Manuel • 3 - Auto • 99 - Quitter
6 : Resynchroniser le pilote	Effectue une resynchronisation forcée du pilote. Invite à définir un délai. *Voulez-vous indiquer une durée minimale de resynchronisation ? (oui/non) :* Si vous répondez oui, saisissez la date et l'heure de la resynchronisation. *Saisissez une date/heure (format 9/27/05 3:27 PM)* Si vous répondez non, la resynchronisation se fait immédiatement.

Opération	Description
7 : Migrer de l'application vers DirXML	Traite un document XML contenant une commande de requête. *Saisissez le nom de fichier du document de requêtes XDS :* Créez le document XML contenant une commande de requête via Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html). Exemples : NetWare : `sys:\files\query.xml` Windows : `c:\files\query.xml` Linux : `/files/query.xml`
8 : Envoyer un document de commandes XDS au pilote	Traite un document de commande XDS. *Saisissez le nom de fichier du document de commandes XDS :* Exemples : NetWare : `sys:\files\user.xml` Windows : `c:\files\user.xml` Linux : `/files/user.xml` *Saisissez le nom du fichier de réponses :* Exemples : NetWare : `sys:\files\user.log` Windows : `c:\files\user.log` Linux : `/files/user.log`
9 : Vérifier le mot de passe de l'objet	Confirme que le mot de passe d'un objet dans le système connecté associé à un pilote correspond au mot de passe de l'objet dans eDirectory (mot de passe de distribution, utilisé avec le mot de passe universel). Saisissez le nom de l'utilisateur :
10 : Initialiser le nouvel objet Pilote	Effectue une initialisation interne des données sur un nouvel objet Pilote. Cette fonction sert uniquement pour effectuer des test.
11 : Actions sur les mots de passe	Il existe neuf options de mots de passe. Reportez-vous au Tableau A-3 page 255 pour voir la description de ces options.
12 : Actions sur le cache	Il existe cinq actions associées au cache. Reportez-vous au Tableau A-4 page 256 pour voir la description de ces options.

Opération	Description
99 : Quitter	Quitte les options du pilote.

Figure A-3 *Actions sur les mots de passe*

Tableau A-3 *Actions sur les mots de passe*

Opération	Description
1 : Définir le mot de passe du module d'interface	Définit le mot de passe de l'application. Il s'agit du mot de passe du compte utilisateur que vous utilisez pour vous authentifier sur le système connecté.
2 : Effacer le mot de passe du module d'interface	Efface le mot de passe de l'application.
3 : Définir le mot de passe du chargeur distant	Le mot de passe du chargeur distant permet de contrôler l'accès à l'instance du chargeur distant. Pour plus d'informations, reportez-vous au Chapitre 3, « Configuration d'un système connecté », page 43. Saisissez le mot de passe du chargeur distant, puis ressaisissez-le pour le confirmer.
4 : Effacer le mot de passe du chargeur distant	Efface le mot de passe du chargeur distant, qui n'est alors plus défini sur l'objet Pilote.
5 : Définir le mot de passe nommé	Permet d'enregistrer un mot de passe ou d'autres informations de sécurité sur le pilote. Pour plus d'informations, reportez-vous à la Section 2.9, « Utilisation de mots de passe nommés », page 27. Vous devez répondre à quatre invites : • Saisir le nom du mot de passe • Saisir la description du mot de passe : • Saisir le mot de passe : • Confirmer le mot de passe :

Opération	Description
6 : Effacer le ou les mots de passe nommés	Efface un mot de passe nommé précis ou tous les mots de passe nommés enregistrés sur l'objet Pilote. Do you want to clear all named passwords? (yes/no) : Si vous répondez oui, tous les mots de passe nommés sont effacés. Si vous répondez non, vous êtes invité à saisir le nom du mot de passe à effacer.
7 : Lister les mots de passe nommés	Affiche la liste de tous les mots de passe nommés enregistrés sur l'objet Pilote. Cette liste contient le nom et la description de chaque mot de passe.
8 : Obtenir l'état des mots de passe	Indique si un mot de passe est défini pour : • Mot de passe de l'objet Pilote : • Mot de passe de l'application : • Mot de passe du chargeur distant : L'utilitaire dxcmd permet de définir le mot de passe de l'application et celui du chargeur distant, mais pas le mot de passe de l'objet Pilote. En revanche, il indique si ce mot de passe est défini ou non.
99 : Quitter	Quitte le menu en cours et vous ramène aux options du pilote.

Figure A-4 *Opérations de cache*

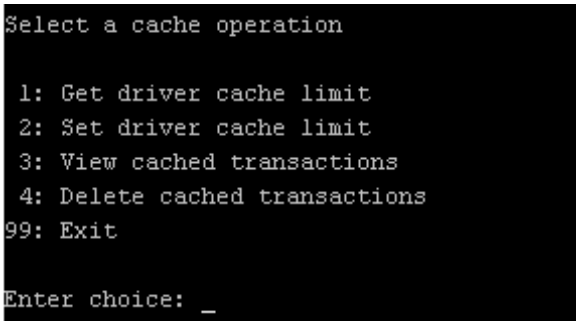


Tableau A-4 *Opérations de cache*

Opération	Description
1 : Obtenir la limite du cache du pilote	Affiche la capacité maximale du cache actuellement définie pour le pilote.
2 : Définir la limite du cache du pilote	Définit la capacité maximale du cache du pilote, en kilo-octets. Si elle est définie sur 0, la capacité du cache est illimitée.

Opération	Description
3 : Afficher les transactions mises en cache	Crée un fichier texte contenant les événements enregistrés dans le cache. Il est possible de sélectionner le nombre de transactions à afficher. • Saisissez le jeton d'option (par défaut=0) : • Saisissez le nombre maximum d'enregistrements de transactions à renvoyer (par défaut=1) : • Saisissez le nom du fichier de réponses :
4 : Supprimer les transactions mises en cache	Supprime les transactions enregistrées dans le cache. • Saisissez le jeton d'emplacement (par défaut=0) : • Saisissez la valeur d'ID d'événement du premier enregistrement de transaction à supprimer (facultatif) : • Saisissez le nombre d'enregistrements de transaction à supprimer (par défaut=1) :
99 : Quitter	Quitte le menu en cours et vous ramène aux options du pilote.

Figure A-5 *Actions de consignation des événements*

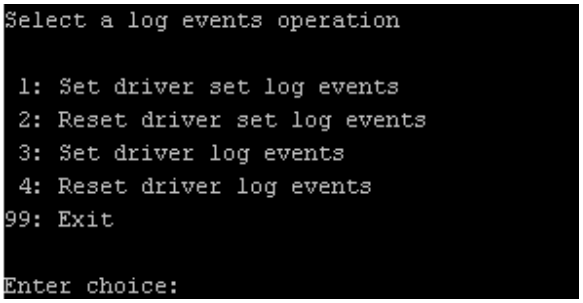


Tableau A-5 *Actions de consignation des événements*

Opération	Description
1 : Définir la consignation des événements de l'ensemble de pilotes	Permet de consigner les événements de l'ensemble de pilotes dans Novell Audit. Vous pouvez sélectionner 49 éléments à consigner. Reportez-vous au Tableau A-6 page 258 pour en voir la liste. Saisissez le numéro de l'élément à consigner. Une fois les éléments sélectionnés, saisissez 99 pour les valider.
2 : Réinitialiser la consignation des événements de l'ensemble de pilotes	Réinitialise toutes les options de consignation des événements.

Opération	Description
3 : Définir la consignation des événements du pilote	Permet de consigner les événements du pilote dans Novell Audit. Vous pouvez sélectionner 49 éléments à consigner. Reportez-vous au Tableau A-6 page 258 pour en voir la liste. Saisissez le numéro de l'élément à consigner. Une fois les éléments sélectionnés, saisissez 99 pour les valider.
4 : Réinitialiser la consignation des événements du pilote	Réinitialise toutes les options de consignation des événements.
99 : Quitter	Quitte le menu d'actions sur la consignation des événements.

Tableau A-6 *Événements du pilote et de l'ensemble de pilotes à consigner*

Options
1 : État Succès
2 : État Réessayer
3 : État Avertissement
4 : État Erreur
5 : État Fatal
6 : État Autre
7 : Éléments Interroger
8 : Éléments Ajouter
9 : Éléments Supprimer
10 : Éléments Modifier
11 : Éléments Renommer
12 : Éléments Déplacer
13 : Éléments Ajouter une association
14 : Éléments Supprimer une association
15 : Éléments Interroger un schéma
16 : Éléments Vérifier le mot de passe
17 : Éléments Vérifier le mot de passe de l'objet
18 : Éléments Modifier le mot de passe
19 : Éléments Synchroniser
20 : Document XDS pré-transformé dans le module d'interface
21 : Publier le document XDS de transformation d'entrée

Options
22 : Publier le document XDS de transformation de sortie
23 : Publier le document XDS de transformation d'événement
24 : Publier le document XDS de transformation de placement
25 : Publier le document XDS de transformation de création
26 : Publier le document XDS <entrant> de transformation d'assignation
27 : Publier le document XDS <sortant> de transformation d'assignation
28 : Publier le document XDS de transformation de concordance
29 : Publier le document XDS de transformation de commande
30 : Document XDS post-filtré <Publisher>
31 : Document de commandes XDS de l'agent utilisateur
32 : Demande de resynchronisation des pilotes
33 : Migration des pilotes de l'application
34 : Démarrage des pilotes
35 : Arrêt des pilotes
36 : Sync mot de passe
37 : Demande de mot de passe
38 : Erreur du moteur
39 : Avertissement du moteur
40 : Ajouter un attribut
41 : Effacer l'attribut
42 : Ajouter valeur
43 : Supprimer la valeur
44 : Fusionner les entrées
45 : Obtenir le mot de passe nommé
46 : Inconnu
47 : Inconnu
48 : ID définis par l'utilisateur
99 : Accepter les éléments cochés

A.2 Mode Ligne de commande

Le mode Ligne de commande permet d'utiliser des scripts ou des fichiers séquentiels. Le Tableau A-7 page 260 présente les différentes options disponibles.

Pour utiliser les options de ligne de commande, déterminez les éléments à utiliser et concaténez-les.

Exemple : `dxcmd -user admin.headquarters -host 10.0.0.1 -password n0vell -start test.driverset.headquarters`

Cette commande permet de démarrer le pilote.

Tableau A-7 *Options de ligne de commande*

Option	Description
Configuration	
-user <user name>	Saisissez le nom d'un utilisateur doté de droits administratifs sur les pilotes à tester.
-host <name or IP address>	Indiquez l'adresse IP du serveur sur lequel le pilote est installé.
-password <user password>	Saisissez le mot de passe de l'utilisateur spécifié précédemment.
-port <port number>	Si le port par défaut n'est pas utilisé, saisissez un numéro de port.
-q <quiet mode>	Affiche des informations succinctes lors de l'exécution de la commande.
-v <verbose mode>	Affiche des informations détaillées lors de l'exécution de la commande.
-? <show this message>	Affiche le menu d'aide.
-help <show this message>	Affiche le menu d'aide.
Actions	
-start <driver dn>	Démarre le pilote.
-stop <driver dn>	Arrête le pilote.
-getstate <driver dn>	Affiche l'état du pilote (en cours d'exécution ou arrêté).
-getstartoption <driver dn>	Affiche l'option de démarrage du pilote.
-setstartoption <driver dn> <disabled|manual|auto> <resync|noresync>	Détermine le mode de démarrage du pilote en cas de redémarrage du serveur. Détermine si, dans un tel cas, les objets doivent être resynchronisés.
-getcachelimit <driver dn>	Indique la taille maximale du cache définie pour le pilote.
-setcachelimit <driver dn> <0 or positive integer>	Définit la taille maximale du cache pour le pilote.
-migrateapp <driver dn> <filename>	Traite un document XML contenant une commande de requête. Créez le document XML contenant une commande de requête via Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html).

Option	Description
-setshimpassword <driver dn> <password>	Définit le mot de passe de l'application. Il s'agit du mot de passe du compte utilisateur que vous utilisez pour vous authentifier sur le système connecté.
-clearshimpassword <driver dn> <password>	Efface le mot de passe de l'application.
-setremoteloaderpassword <driver dn> <password>	Définit le mot de passe du chargeur distant. Le mot de passe du chargeur distant permet de contrôler l'accès à l'instance du chargeur distant. Pour plus d'informations, reportez-vous au Chapitre 3, « Configuration d'un système connecté », page 43.
<clearremoteloaderpassword <driver dn>	Efface le mot de passe du chargeur distant.
-sendcommand <driver dn> <input filename> <output filename>	Traite un document de commande XDS. Spécifie le document de commandes XDS comme fichier d'entrée. Exemples : NetWare : `sys:\files\user.xml` Windows : `c:\files\user.xml` Linux : `/files/user.log` Spécifiez le nom du fichier de sortie pour afficher les résultats. Exemples : NetWare : `sys:\files\user.log` Windows : `c:\files\user.log` Linux : `/files/user.log`
-setlogevents <dn> <integer ...>	Définit les événements de consignation Novell Audit sur le pilote. L'entier correspond au numéro de l'élément à consigner. Reportez-vous au Tableau A-6 page 258 pour connaître la liste des numéros à saisir.
-clearlogevents <dn>	Efface tous les événements de consignation Novell Audit définis sur le pilote.
-setdriverset <driver set dn>	Associe un ensemble de pilotes au serveur.
-cleardriverset	Supprime l'association entre un ensemble de pilotes et le serveur.
-getversion	Affiche la version de Identity Manager installée.
-initdriver object <dn>	Effectue une initialisation interne des données sur un nouvel objet Pilote. Cette fonction sert uniquement pour effectuer des test.

Option	Description
-setnamedpassword <driver dn> <name> <password> [description]	Définit les mots de passe nommés sur l'objet Pilote. Vous devez préciser le nom, le mot de passe et la description du mot de passe nommé.
-clearnamedpassword <driver dn> <name>	Efface le mot de passe nommé spécifié.
-clearallnamedpaswords <driver dn>	Efface tous les mots de passe nommés définis sur un pilote donné.

Options de configuration d'un chargeur distant

B

Les options du tableau suivant permettent de configurer un chargeur distant.

Tableau B-1 *Options du chargeur distant*

Option	Autre nom	Paramètre	Description
adresse		adresse IP	Un paramètre facultatif. Spécifie que le chargeur distant écoute à partir d'une adresse IP locale spécifique. Cette information est utile si le serveur qui héberge le chargeur distant possède plusieurs adresses IP et si ce dernier doit utiliser une seule adresse. Vous disposez de trois options : address=*address number* address='localhost' N'utilisez pas ce paramètre. Si vous n'utilisez pas l'option -address, le chargeur distant écoute sur toutes les adresses IP locales. Exemple : address=137.65.134.83
-class	-cl	Nom de la classe Java	Spécifie le nom de la classe Java du module d'interface d'application Identity Manager à héberger. Par exemple, pour un pilote Java, saisissez un des éléments suivants : -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java utilise un keystore pour lire les certificats. L'option -class et l'option -module s'excluent mutuellement. La liste des noms de classe Java est présentée dans le Tableau B-2 page 270.

Option	Autre nom	Paramètre	Description
-commandport	-cp	Numéro de port	Spécifie le port TCP/IP utilisé par l'instance du chargeur distant à des fins de contrôle. Si l'instance du chargeur distant héberge un module d'interface pilote de l'application, le port de commande est un port utilisé par une autre instance du chargeur distant pour communiquer avec l'instance qui héberge le module d'interface pilote. Si l'instance du chargeur distant envoie une commande à une instance qui héberge un module d'interface d'application, le port de commande est le port utilisé par cette dernière instance. Si le port de commande n'est pas spécifié, le port 8000 est utilisé par défaut. Plusieurs instances du chargeur distant peuvent être exécutées sur le même serveur qui héberge différentes instances de pilote ; il suffit de spécifier des ports de connexion et des ports de commande différents. Exemple : -commandport 8001 -cp 8001
-config	Aucun	nom_fichier	Spécifie un fichier de configuration. Le fichier de configuration peut contenir toutes les options de ligne de commande à l'exception de l'option `config`. Les options spécifiées sur la ligne de commande remplacent celles spécifiées dans le fichier de configuration. Exemple : -config config.txt
-connection	-conn	Chaîne de configuration de connexion	Spécifie les paramètres de connexion à utiliser pour la connexion au serveur méta-annuaire sur lequel est exécuté le module d'interface pilote distant Identity Manager. Par défaut, la méthode de connexion utilisée pour le chargeur distant est TCP/IP avec SSL. Le port TCP/IP par défaut pour cette connexion est 8090. Plusieurs instances du chargeur distant peuvent s'exécuter sur le même serveur. Chaque instance du chargeur distant héberge une instance du module d'interface pilote de l'application Identity Manager. Différenciez les multiples instances du chargeur distant en spécifiant des ports de connexion et des ports de commande différents pour chaque instance du chargeur distant. Exemple : -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"

Option	Autre nom	Paramètre	Description
-description	-desc	brève description	Spécifiez une chaîne de description abrégée (par exemple, SAP) pour le titre de la fenêtre de trace et pour la consignation dans Novell® Audit. Exemple : -description SAP -desc SAP La console du chargeur distant place les formes longues des options dans les fichiers de configuration. Vous pouvez utiliser soit la forme longue (par exemple, -description), soit la forme abrégée (par exemple, -desc).
-help	-?	Aucun	Affiche l'aide. Exemple : -help -?
-java	-j	Aucun	Spécifie que les mots de passe doivent être définis pour une instance de module d'interface Java. Cette option n'est utile qu'en association avec l'option de définition de mots de passe (setpasswords). Si -class est spécifié avec -setpasswords, cette option n'est pas nécessaire.
-javadebugport	-jdp	Numéro de port	Spécifie que l'instance du chargeur distant doit activer le débogage Java sur le port spécifié. Cela est particulièrement utile pour les développeurs de modules d'interface d'application Identity Manager. Exemple : -javadebugport 8080 -jdp 8080

keystore			Paramètres conditionnels. Cette option est utilisée uniquement pour les modules d'interface d'application DirXML contenus dans les fichiers .JAR.
			
			Spécifie le nom du fichier keystore Java qui contient le certificat de racine approuvée de l'émetteur du certificat utilisé par le module d'interface distant. Il s'agit en général de l'autorité de certification de l'arborescence eDirectory™ qui héberge le module d'interface pilote distant.
			
			Si vous exécutez SSL et si vous souhaitez que le chargeur distant communique avec un pilote Java, saisissez une paire clé-valeur :
			
			`keystore='`*`keystorename`*`'`
			`storepass='`*`password`*`'`

Option	Autre nom	Paramètre	Description
-module	-m	Nom de module	Spécifie le module qui contient le module d'interface d'application Identity Manager à héberger. Par exemple, pour un pilote natif, saisissez un des éléments suivants : -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" ou -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" L'option -module utilise un certificat rootfile. L'option -module et l'option -class s'excluent mutuellement.
-password	-p	password	Spécifie le mot de passe d'authentification des commandes. Ce mot de passe doit être identique au premier mot de passe spécifié dans `setpasswords` pour l'instance de chargeur qui fait l'objet de la commande. Si une option de commande (déchargement, modification du niveau de trace, etc.) est spécifiée et si l'option `password` ne l'est pas, l'utilisateur est invité à entrer le mot de passe du chargeur représentant la cible de la commande. Exemple : -password novell4 -p novell4
port		Numéro de port décimal	Un paramètre requis. Il spécifie le port TCP/IP sur lequel le chargeur distant écoute des connexions du module d'interface pilote distant. Exemple : port=8090
rootfile			Un paramètre conditionnel. Si vous exécutez SSL et si vous souhaitez que le chargeur distant communique avec un pilote natif, saisissez `rootfile='`*`trusted certname`*`'`

Option	Autre nom	Paramètre	Description
-service	-serv	Aucun, ou install/uninstall	Pour installer une instance en tant que service, utilisez l'argument install avec les autres arguments requis pour l'hébergement du module d'interface d'application. Par exemple, les arguments utilisés doivent inclure -module, mais tous les arguments peuvent inclure -connection, -commandport, etc. Cette option installe le service Win32 mais ne le démarre pas. Pour désinstaller une instance en tant que service, utilisez l'argument uninstall en avec les autres arguments requis pour l'hébergement du module d'interface d'application. La version sans argument de cette option n'est utilisée au niveau de la ligne de commande que pour une instance exécutée en tant que service Win32. Cette fonctionnalité est automatiquement configurée au moment de l'installation d'une instance en tant que service. Exemple : -service install -serv uninstall Cette option n'est pas disponible sur le chargeur distant Java ou rdxml.
-setpasswords	-sp	Mot de passe Mot de passe	Spécifie le mot de passe de l'instance du chargeur distant et celui de l'objet Pilote Identity Manager du module d'interface pilote distant avec lequel le chargeur distant va communiquer. Le premier mot de passe de l'argument est celui du chargeur distant. Le deuxième, dans les arguments facultatifs, est celui de l'objet Pilote Identity Manager associé au module d'interface pilote distant sur le serveur méta-annuaire. Aucun mot de passe ne doit être spécifié ou les deux doivent l'être. Si aucun mot de passe n'est spécifié, le chargeur distant demande les mots de passe. Il s'agit d'une option de configuration. Elle permet de configurer l'instance du chargeur distant à l'aide des mots de passe spécifiés, mais ne permet pas de charger le module d'interface pilote de l'application Identity Manager ni de communiquer avec une autre instance du chargeur. Exemple : -setpasswords novell4 staccato3 -sp novell4 staccato3

Option	Autre nom	Paramètre	Description
-storepass		storepass	Cette option est utilisée uniquement pour les modules d'interface d'application DirXML contenus dans les fichiers .JAR. Spécifie le mot de passe du fichier keystore Java indiqué par le paramètre keystore. Exemple : storepass=mypassword Cette option ne s'applique qu'au chargeur distant Java.
-trace	-t	Nombre entier	Spécifie le niveau de trace. Cette option est utilisée uniquement lorsqu'un module d'interface d'application est hébergé. Les niveaux de trace correspondent à ceux utilisés sur le serveur de méta-annuaire. Exemple : -trace 3 -t 3
-tracechange	-tc	Nombre entier	Commande à une instance du chargeur distant qui héberge un module d'interface pilote de l'application de modifier son niveau de trace. Les niveaux de trace correspondent à ceux utilisés sur le serveur de méta-annuaire. Exemple : -tracechange 1 -tc 1
-tracefile	tf	nom_fichier	Spécifie le fichier dans lequel consigner les messages de trace. Les messages de trace sont consignés si le niveau de trace est supérieur à zéro, que la fenêtre de trace soit ouverte ou non. Exemple : -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt
-tracefilechange	tfc	Aucun, ou Nom de fichier	Commande à une instance du chargeur distant qui héberge un module d'interface pilote de l'application de commencer à utiliser un fichier de trace ou de fermer celui qui est en cours d'utilisation pour en utiliser un autre. L'utilisation de la version sans argument de cette option entraîne la fermeture, par l'instance qui héberge le module, de tout fichier de trace utilisé. Exemple : -tracefilechange c:\temp\newtrace.txt tfc c:\temp\newtrace.txt

Option	Autre nom	Paramètre	Description
-tracefilemax	-tfm	taille	Spécifie la taille maximum que les données du fichier de trace peuvent occuper sur le disque. Si vous spécifiez cette option, il y a un fichier de trace avec le nom spécifié via l'option tracefile et jusqu'à 9 fichiers de purge supplémentaires. Ces fichiers sont nommés en utilisant la base du nom de fichier de trace principal plus "_*n*", avec n allant de 1 à 9. Le paramètre de taille est le nombre d'octets. Spécifiez la taille en utilisant les suffixes K, M ou G pour kilo-octets, mégaoctets ou gigaoctets. Si la taille des données du fichier de trace est supérieure au maximum spécifié lorsque le chargeur distant est démarré, les données du fichier de trace restent supérieures au maximum spécifié jusqu'à ce que la purge soit terminée sur les 10 fichiers Exemple : -tracefilemax 1000M -tfm 1000M Dans cet exemple, le fichier de trace ne peut pas dépasser 1 Go.
-unload	-u	Aucun	Décharge l'instance du chargeur distant. Si le chargeur distant s'exécute comme un service Win32, cette commande arrête le service. Exemple : -unload -u
-window	-w	On/Off	Active ou désactive la fenêtre de trace d'une instance du chargeur distant. Exemple : -window on -w off Cette option n'est disponible que sur les plates-formes Windows. Elle n'est pas disponible sur le chargeur distant Java.

Option	Autre nom	Paramètre	Description
-wizard	-wiz	Aucun	Permet de lancer l'Assistant de configuration. Il est également possible de lancer l'assistant en exécutant dirxml_remote.exe sans paramètre de ligne de commande. Cette option est utile lorsqu'un fichier de configuration est également spécifié. Dans ce cas, l'assistant utilise les valeurs qui figurent dans le fichier de configuration, et cet assistant peut être utilisé pour modifier la configuration sans modifier directement le fichier de configuration. Exemple : -wizard -wiz Cette option n'est disponible que sur les plates-formes Windows. Elle n'est pas disponible sur le chargeur distant Java.

Tableau B-2 *Noms de classes Java*

Nom de la classe Java	Pilote
com.novell.nds.dirxml.driver.avaya.PBXDriverShim	Pilote Avaya PBX
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Pilote pour fichier texte délimité
com.novell.nds.dirxml.driver.nds.DriverShimImpl	Pilote eDirectory
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Pilote de services de droits
com.novell.gw.dirxml.driver.gw.GWdriverShim	Pilote GroupWise
com.novell.nds.dirxml.jdbc.JDBCDriverShim	Pilote JDBC
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	Pilote LDAP
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Pilote de service de boucle
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Pilote de tâches manuelles
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	Pilote NIS
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Pilote Notes
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	Pilote PeopleSoft
com.novell.nds.dirxml.driver.SAPShim.SAPDriverShim	Pilote SAP HR
com.novell.nds.dirxml.driver.sapusershim.SAPDriverShim	Pilote de gestion des utilisateurs SAP
com.novell.nds.dirxml.driver.sifagent.SIFShim	Pilote SIF
com.novell.nds.dirxml.driver.soap.SOAPDriver	Pilote Soap
com.novell.idm.driver.ComposerDriverShim	Application utilisateur
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	Pilote pour Remedy ARS

Événements et rapports Identity Manager

C

Cette section contient la liste de tous les événements Novell® Audit consignés par Identity Manager. Elle contient également, dans la Section C.11, « Rapports », page 294, des exemples de rapports exécutables avec Novell Audit.

Les informations suivantes sont enregistrées avec chaque événement : EventID (ID d'événement), Description, Originator Title (Titre d'origine), Target Title (Titre de la cible), Subtarget Title (Titre de la cible secondaire), Text1 Title (Titre Texte1), Text2 Title (Titre Texte2), Text3 Title (Titre Texte3), Value1 Title (Titre Valeur1), Value1 Type (Type Valeur1), Value2 Title (Titre Valeur2), Value2 Type (Type Valeur2), Value3 Title (Titre Valeur3), Value3 Type (Type Valeur3), Group Title (Titre du groupe), Group Type (Type de groupe), Data Title (Titre des données), Data Type (Type de données), Display Schema (Schéma d'affichage).

Les événements correspondant aux différents composants figurent dans les tableaux suivants.

C.1 Événements du moteur

Les tableaux suivants contiennent la liste des événements du moteur pouvant faire l'objet d'un audit dans Novell Audit.

Tableau C-1 *Champs des événements du moteur : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Subtarget Title (Titre de la cible secondaire)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
30001	État Succès	Canal	src-dn (dest-dn)	Niveau
30002	État Réessayer	Canal	src-dn (dest-dn)	Niveau
30003	État Avertissement	Canal	src-dn (dest-dn)	Niveau

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
30004	État Erreur	Canal	src-dn (dest-dn)	Niveau
30005	État Fatal	Canal	src-dn (dest-dn)	Niveau
30006	État Autre	Canal	src-dn (dest-dn)	Niveau
30007	Rechercher	Canal	dest-dn ou association	Étendue
30008	Ajouter l'entrée	Canal	dest-dn ou association	Nom d'attribut
30009	Supprimer l'entrée	Canal	dest-dn ou association	Nom d'attribut
3000A	Modifier l'entrée	Canal	dest-dn ou association	Nom d'attribut
3000B	Renommer l'entrée	Canal	dest-dn ou association	Type d'objet
3000C	Déplacer l'entrée	Canal	dest-dn ou association	Déplacer la destination
3000D	Ajouter une association	Canal	dest-dn	Nom d'attribut
3000E	Retirer l'association	Canal		Nom d'attribut
3000F	Schéma d'interrogation	Canal		
30010	Vérifier le mot de passe	Canal	Pilote	
30011	Vérifier le mot de passe de l'objet	Canal	dest-dn ou association	
30012	Changer le mot de passe	Canal	dest-dn ou association	
30013	Sync	Canal	dest-dn ou association	Nom d'attribut
30014	Document XML d'entrée	Canal		Nom d'attribut
30015	Document de transformation de l'entrée	Canal		
30016	Document de transformation de la sortie	Canal		
30017	Document de transformation de l'événement	Canal		
30018	Document de transformation de règle de placement	Canal		

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
30019	Document de transformation de règle de création	Canal		
3001A	Document de transformation de la règle de correspondance des entrées	Canal		
3001B	Document de transformation de la règle de mise en correspondance des sorties	Canal		
3001C	Créer un document de transformation de correspondance	Canal		
3001D	Document de transformation de la commande	Canal		
3001E	Document de transformation du filtre Éditeur	Canal		
3001F	Requête de l'agent utilisateur	Canal		
30020	Resynchroniser le pilote	Canal	Pilote	
30021	Migrate	Canal	Association	Nom d'attribut
30022	Démarrage du pilote	Ensemble de pilotes	Pilote	
30023	Arrêt du pilote	Arrêt du pilote	Pilote	
30024	Sync mot de passe	Canal	Objet	Nom d'attribut
30025	Réinitialisation du mot de passe	Canal	dest-dn ou association	Nom d'attribut
30026	Erreur DirXML	Canal	Objet	
30027	Avertissement DirXML	Canal	Objet	
30028	Opération personnalisée	Canal		
30029	Effacer l'attribut	Canal	dest-dn ou association	Nom d'attribut
3002A	Ajouter la valeur - Modifier l'entrée	Canal	dest-dn ou association	Nom d'attribut
3002B	Supprimer la valeur	Canal	dest-dn ou association	Nom d'attribut
3002C	Fusionner les entrées	Canal	Objet	Nom d'attribut

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
3002D	Obtenir le mot de passe nommé	Pilote ou canal	Objet	
3002E	Réinitialiser les attributs	Canal	Objet	Canal
3002F	Ajouter la valeur – Ajouter l'entrée	Canal	dest-dn ou association	Nom d'attribut

Tableau C-2 *Champs des événements du moteur : Text1 Title (Titre Texte1), Text2 Title (Titre Texte2) et Text3 Title (Titre Texte3)*

ID événement	Description	Titre Texte1	Titre Texte2	Titre Texte3
30001	État Succès	Type	Document d'état	ID de l'événement
30002	État Réessayer	Type	Document d'état	ID de l'événement
30003	État Avertissement	Type	Document d'état	ID de l'événement
30004	État Erreur	Type	Document d'état	ID de l'événement
30005	État Fatal	Type	Document d'état	ID de l'événement
30006	État Autre	Type	Document d'état	ID de l'événement
30007	Rechercher	Type d'objet		ID de l'événement
30008	Ajouter l'entrée	Type d'objet	src-dn	ID de l'événement
30009	Supprimer l'entrée	Type d'objet	src-dn	ID de l'événement
3000A	Modifier l'entrée	Type d'objet	src-dn	ID de l'événement
3000B	Renommer l'entrée	Nouveau nom	src-dn	ID de l'événement
3000C	Déplacer l'entrée	Déplacer l'association	src-dn	ID de l'événement
3000D	Ajouter une association	Association		ID de l'événement
3000E	Retirer l'association	Association		ID de l'événement
3000F	Schéma d'interrogation			ID de l'événement
30010	Vérifier le mot de passe			
30011	Vérifier le mot de passe de l'objet			ID de l'événement
30012	Changer le mot de passe	Type d'objet	src-dn	ID de l'événement
30013	Sync	Type d'objet	association	Type
30014	Document XML d'entrée			Message d'avertissement
30015	Document de transformation de l'entrée			Message d'avertissement

ID événement	Description	Titre Texte1	Titre Texte2	Titre Texte3
30016	Document de transformation de la sortie			Message d'avertissement
30017	Document de transformation de l'événement			Message d'avertissement
30018	Document de transformation de règle de placement			Message d'avertissement
30019	Document de transformation de règle de création			Message d'avertissement
3001A	Document de transformation de la règle de correspondance des entrées			Message d'avertissement
3001B	Document de transformation de la règle de mise en correspondance des sorties			Message d'avertissement
3001C	Créer un document de transformation de correspondance			Message d'avertissement
3001D	Document de transformation de la commande			Message d'avertissement
3001E	Document de transformation du filtre Éditeur			Message d'avertissement
3001F	Requête de l'agent utilisateur			
30020	Resynchroniser le pilote			Message d'erreur
30021	Migrate	Type d'objet		Message d'avertissement
30022	Démarrage du pilote			Message du pilote
30023	Arrêt du pilote			Message du pilote
30024	Sync mot de passe			
30025	Réinitialisation du mot de passe		src-dn	
30026	Erreur DirXML	Message d'erreur		

ID événement	Description	Titre Texte1	Titre Texte2	Titre Texte3
30027	Avertissement DirXML	Message d'avertissement		
30028	Opération personnalisée			
30029	Effacer l'attribut		src-dn	ID de l'événement
3002A	Ajouter la valeur - Modifier l'entrée	Valeur	src-dn	ID de l'événement
3002B	Supprimer la valeur	Valeur	src-dn	ID de l'événement
3002C	Fusionner les entrées	Type d'objet	Canal	Association
3002D	Obtenir le mot de passe nommé	Nom de mot de passe		ID de l'événement
3002E	Réinitialiser les attributs			
3002F	Ajouter la valeur – Ajouter l'entrée	Valeur	src-dn	ID de l'événement

Tableau C-3 *Champs des événements du moteur : Value1 Title (Titre Valeur1), Value2 Title (Titre Valeur2) et Value3 Title (Titre Valeur3)*

ID événement	Description	Titre Valeur1	Titre Valeur2	Titre Valeur3
30001	État Succès			
30002	État Réessayer			
30003	État Avertissement			
30004	État Erreur			
30005	État Fatal			
30006	État Autre			
30007	Rechercher			Résultat
30008	Ajouter l'entrée			Résultat
30009	Supprimer l'entrée			Résultat
3000A	Modifier l'entrée			Résultat
3000B	Renommer l'entrée			Résultat
3000C	Déplacer l'entrée			Résultat
3000D	Ajouter une association			Résultat
3000E	Retirer l'association			Résultat
3000F	Schéma d'interrogation			Résultat
30010	Vérifier le mot de passe			

ID événement	Description	Titre Valeur1	Titre Valeur2	Titre Valeur3
30011	Vérifier le mot de passe de l'objet			
30012	Changer le mot de passe			Résultat
30013	Sync			Résultat
30014	Document XML d'entrée			
30015	Document de transformation de l'entrée			
30016	Document de transformation de la sortie			
30017	Document de transformation de l'événement			
30018	Document de transformation de règle de placement			
30019	Document de transformation de règle de création			
3001A	Document de transformation de la règle de correspondance des entrées			
3001B	Document de transformation de la règle de mise en correspondance des sorties			
3001C	Créer un document de transformation de correspondance			
3001D	Document de transformation de la commande			
3001E	Document de transformation du filtre Éditeur			
3001F	Requête de l'agent utilisateur			Résultat
30020	Resynchroniser le pilote			Résultat
30021	Migrate			

ID événement	Description	Titre Valeur1	Titre Valeur2	Titre Valeur3
30022	Démarrage du pilote	État		
30023	Arrêt du pilote	État		
30024	Sync mot de passe			Résultat
30025	Réinitialisation du mot de passe			
30026	Erreur DirXML	Code		
30027	Avertissement DirXML	Code		
30028	Opération personnalisée			
30029	Effacer l'attribut			Résultat
3002A	Ajouter la valeur - Modifier l'entrée			Résultat
3002B	Supprimer la valeur			Résultat
3002C	Fusionner les entrées			
3002D	Obtenir le mot de passe nommé			Résultat
3002E	Réinitialiser les attributs			
3002F	Ajouter la valeur – Ajouter l'entrée			Résultat

Tableau C-4 *Champs des événements du moteur : Déclencheurs et type des données*

ID événement	Description	Type de données	Déclencheurs
30001	État Succès	Document XML	De nombreux événements différents peuvent donner lieu à l'événement État Succès. En général, il signifie que l'opération a été effectuée avec succès.
30002	État Réessayer	Document XML	De nombreux événements différents peuvent donner lieu à l'événement État Réessayer. Il signifie que l'opération n'est pas achevée et qu'elle doit être retentée ultérieurement.
30003	État Avertissement	Document XML	De nombreux événements différents peuvent donner lieu à l'événement État Avertissement. En général, il signifie que l'opération a été effectuée malgré des problèmes mineurs.

ID événement	Description	Type de données	Déclencheurs
30004	État Erreur	Document XML	De nombreux événements différents peuvent donner lieu à l'événement État Erreur. En général, il signifie que l'opération a échoué.
30005	État Fatal	Document XML	De nombreux événements différents peuvent donner lieu à l'événement État Fatal. En général, il signifie que l'opération a échoué et que le moteur ou le pilote n'a pas pu poursuivre.
30006	État Autre	Document XML	Tout document d'état traité avec un autre niveau que l'un des cinq niveaux définis précédemment donne lieu à un événement État Autre. Ces événements ne peuvent être générés que dans une feuille de style ou dans une règle.
30007	Rechercher	Document XML	Survient lorsqu'un document de requête est envoyé au pilote ou au moteur IDM.
30008	Ajouter l'entrée	Document XML	Survient lorsqu'un objet est ajouté.
30009	Supprimer l'entrée	Document XML	Survient lorsqu'un objet est supprimé.
3000A	Modifier l'entrée	Document XML	Survient lorsqu'un objet est modifié.
3000B	Renommer l'entrée	Document XML	Survient lorsqu'un objet est renommé.
3000C	Déplacer l'entrée	Document XML	Survient lorsqu'un objet est déplacé.
3000D	Ajouter une association	Document XML	Survient lorsqu'une association est ajoutée. Peut avoir lieu en cas d'ajout ou de mise en correspondance.
3000E	Retirer l'association	Document XML	Lorsqu'un objet est supprimé, il n'y a pas d'événement Retirer l'association. Celui-ci survient lorsqu'un objet Utilisateur est supprimé dans l'autre application, et que la suppression est convertie en modification entraînant l'annulation de l'association.

ID événement	Description	Type de données	Déclencheurs
3000F	Schéma d'interrogation	Document XML	Survient lorsqu'une opération de schéma d'interrogation est envoyée au pilote ou au moteur IDM.
30010	Vérifier le mot de passe		Fonction manuelle lancée depuis iManager.
30011	Vérifier le mot de passe de l'objet	Document XML	Survient lorsqu'une requête est émise pour vérifier le mot de passe d'un objet autre que le pilote.
30012	Changer le mot de passe	Document XML	Survient lorsqu'une requête est émise pour vérifier le mot de passe du pilote.
30013	Sync	Document XML	Survient lorsqu'un événement de synchronisation est demandé.
30014	Document XML d'entrée	Document XML	Est généré chaque fois qu'un document d'entrée est créé par le moteur ou le pilote.
30015	Document de transformation de l'entrée	Document XML	Est généré après traitement des stratégies de transformation des entrées, ce qui permet à l'utilisateur d'afficher le document transformé.
30016	Document de transformation de la sortie	Document XML	Est généré après traitement des stratégies de transformation des sorties, ce qui permet à l'utilisateur d'afficher le document transformé.
30017	Document de transformation de l'événement	Document XML	Est généré après traitement des stratégies de transformation des événements, ce qui permet à l'utilisateur d'afficher le document transformé.
30018	Document de transformation de règle de placement	Document XML	Est généré après traitement des stratégies de placement, ce qui permet à l'utilisateur d'afficher le document transformé.
30019	Document de transformation de règle de création	Document XML	Est généré après traitement des stratégies de règle de création, ce qui permet à l'utilisateur d'afficher le document transformé.
3001A	Document de transformation de la règle de correspondance des entrées	Document XML	Est généré après traitement des règles de correspondance des schémas, qui convertissent le document en schéma eDirectory.

ID événement	Description	Type de données	Déclencheurs
3001B	Document de transformation de la règle de correspondance des sorties	Document XML	Est généré après traitement des règles de correspondance des schémas, qui convertissent le document en schéma d'application.
3001C	Créer un document de transformation de correspondance	Document XML	Est généré après traitement des stratégies de correspondance, ce qui permet à l'utilisateur d'afficher le document transformé.
3001D	Document de transformation de la commande	Document XML	Est généré après traitement des stratégies de transformation des commandes, ce qui permet à l'utilisateur d'afficher le document transformé.
3001E	Document de transformation du filtre Éditeur	Document XML	Est généré après traitement du filtre de notification sur le canal Éditeur, ce qui permet à l'utilisateur d'afficher le document transformé.
3001F	Requête de l'agent utilisateur	Document XML	Survient lorsqu'un document de commande XDS de l'agent utilisateur est envoyé au pilote sur le canal Abonné.
30020	Resynchroniser le pilote		Survient lorsqu'une demande de resynchronisation est émise.
30021	Migrate		Survient lorsqu'une demande de migration est émise.
30022	Démarrage du pilote	Document XML	Survient lorsque le pilote est démarré.
30023	Arrêt du pilote	Document XML	Survient lorsque le pilote est arrêté.
30024	Sync mot de passe		Est généré lors de la définition d'un mot de passe simple ou d'un mot de passe de distribution sur un objet.
30025	Réinitialisation du mot de passe		Est généré lors de la réinitialisation du mot de passe de l'application connectée après échec d'une opération de synchronisation des mots de passe.
30026	Erreur DirXML		Est généré chaque fois que le moteur renvoie une erreur interne.

ID événement	Description	Type de données	Déclencheurs
30027	Avertissement DirXML		Est généré chaque fois que le moteur renvoie un avertissement interne.
30028	Opération personnalisée	Document XML	Survient lorsqu'une opération inconnue apparaît dans un document d'entrée. Les opérations connues sont notamment l'ajout, la suppression ou la modification.
30029	Effacer l'attribut		Survient lorsqu'une opération de modification contient un élément remove-all-value.
3002A	Ajouter la valeur – Modifier l'entrée	Valeur	Survient lorsqu'une valeur est ajoutée pendant la modification d'un objet.
3002B	Supprimer la valeur	Valeur	Survient lorsqu'une opération de modification contient un élément remove-value.
3002C	Fusionner les entrées	Document XML	Survient lorsque deux objets sont fusionnés.
3002D	Obtenir le mot de passe nommé	Document XML	Est généré lors d'une opération Obtenir un mot de passe nommé.
3002E	Réinitialiser les attributs	Document XML	Survient lorsqu'un document de réinitialisation est émis sur le canal Éditeur ou Abonné.
3002F	Ajouter la valeur – Ajouter l'entrée	Valeur	Survient lorsqu'une valeur est ajoutée pendant la création d'un objet.

C.2 Événements du serveur

Les tableaux suivants contiennent la liste des événements du serveur pouvant faire l'objet d'un audit dans Novell Audit.

Tableau C-5 *Champs des événements du serveur : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Subtarget Title (Titre de la cible secondaire)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
307D0	Config:Journal des événements	Serveur	Pilote	Nom d'attribut
307D1	Config:Limite du cache de pilote	Serveur	Pilote	Nom d'attribut

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
307D2	Config:Ensemble de pilotes	Serveur	Serveur	Nom d'attribut
307D3	Config:Option de démarrage du pilote	Serveur	Pilote	Nom d'attribut
307D4	Resynchronisation du pilote	Serveur	Pilote	
307D5	Migrer le serveur d'application	Serveur	Pilote	
307D6	Définir le mot de passe du module d'interface	Serveur	Pilote	Nom d'attribut
307D7	Définir le mot de passe avec clé	Serveur	Pilote	
307D8	Définir le mot de passe du chargeur distant	Serveur	Pilote	Nom d'attribut

Tableau C-6 *Champs des événements du serveur : Text1 Title (Titre Texte1), Text2 Title (Titre Texte2) et Text3 Title (Titre Texte3)*

ID événement	Description	Titre Texte1	Titre Texte2	Titre Texte3
307D0	Config:Journal des événements			Opération
307D1	Config:Limite du cache de pilote			
307D2	Config:Ensemble de pilotes	Ensemble de pilotes	Type	
307D3	Config:Option de démarrage du pilote			Message
307D4	Resynchronisation du pilote			
307D5	Migrer le serveur d'application			
307D6	Définir le mot de passe du module d'interface			
307D7	Définir le mot de passe avec clé		Type	

ID événement	Description	Titre Texte1	Titre Texte2	Titre Texte3
307D8	Définir le mot de passe du chargeur distant			

Tableau C-7 *Champs des événements du serveur : Value1 Title (Titre Valeur1), Value2 Title (Titre Valeur2) et Value3 Title (Titre Valeur3)*

ID événement	Description	Titre Valeur1	Titre Valeur2	Titre Valeur3
307D0	Config:Journal des événements			Résultat
307D1	Config:Limite du cache de pilote	Limit		Résultat
307D2	Config:Ensemble de pilotes			Résultat
307D3	Config:Option de démarrage du pilote	Option de démarrage		Résultat
307D4	Resynchronisation du pilote			Résultat
307D5	Migrer le serveur d'application			Résultat
307D6	Définir le mot de passe du module d'interface		Version	Résultat
307D7	Définir le mot de passe avec clé			Résultat
307D8	Définir le mot de passe du chargeur distant		Version	Résultat

Tableau C-8 *Champs des événements du serveur : Déclencheurs et type des données*

ID événement	Description	Type de données	Déclencheurs
307D0	Config:Journal des événements	Tampon d'entrée	Survient lorsque l'attribut d'événement de consignation est modifié sur l'objet Pilote ou Ensemble de pilotes.
307D1	Config:Limite du cache de pilote		Survient lorsque l'attribut de limite du cache du pilote est modifié sur un objet Pilote.
307D2	Config:Ensemble de pilotes	Tampon d'entrée	Survient lorsque l'association Ensemble de pilotes/Serveur est modifiée.

ID événement	Description	Type de données	Déclencheurs
307D3	Config:Option de démarrage du pilote	Tampon d'entrée	Survient lorsque l'option de démarrage du pilote est modifiée pour un objet Pilote.
307D4	Resynchronisation du pilote		Survient lorsqu'une resynchronisation du pilote est demandée.
307D5	Migrer le serveur d'application	Document XML	Survient lorsque la migration du serveur d'application a lieu.
307D6	Définir le mot de passe du module d'interface		Survient lorsque le mot de passe de l'application est défini.
307D7	Définir le mot de passe avec clé		
307D8	Définir le mot de passe du chargeur distant		Survient lorsque le mot de passe du chargeur distant est défini.

C.3 Événements du chargeur distant

Les tableaux suivants contiennent la liste des événements du chargeur distant pouvant faire l'objet d'un audit dans Novell Audit.

Tableau C-9 *Champs des événements du chargeur distant : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Subtarget Title (Titre de la cible secondaire)*

ID événement	Description	Titre d'origine	Déclencheurs
30BB8	Démarrage du chargeur distant	Instance	Survient au démarrage du chargeur distant.
30BB9	Arrêt du chargeur distant	Instance	Survient lorsque le chargeur distant s'arrête.
30BBA	Connexion au chargeur distant établie	Instance	Survient lorsque la connexion au chargeur distant est établie.
30BBB	Connexion au chargeur distant perdue	Instance	Survient lorsque la connexion au chargeur distant est coupée.

C.4 Détail des portlets

Tableau C-10 *Champs détaillés des portlets : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Subtarget Title (Titre de la cible secondaire)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
31400	Delete_Entity	Nom d'utilisateur	DN de l'entité	Définition de l'entité
31401	Update_Entity	Nom d'utilisateur	DN de l'entité	Définition de l'entité

Tableau C-11 *Champs détaillés des portlets : Group Title (Titre du groupe), Group Type (Type de groupe) et Triggers (Déclencheurs)*

ID événement	Description	Titre du groupe	Type de groupe	Déclencheurs
31400	Delete_Entity	Numéro de groupe	Numéro	Survient lorsqu'un objet est supprimé.
31401	Update_Entity	Numéro de groupe	Numéro	Survient lorsqu'un objet est modifié.

C.5 Portlet de modification du mot de passe

Tableau C-12 *Changer les champs du portlet de mot de passe : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Text3 Title (Titre Texte3)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre Texte3
31420	Change_Password_Failure	ID initiateur	DN cible	Message d'erreur
31421	Change_Password_Success	ID initiateur	DN cible	

Tableau C-13 *Changer les champs du portlet de mot de passe : Value3 Title (Titre Valeur3), Value3 Type (Type Valeur3) et Triggers (Déclencheurs)*

ID événement	Description	Titre Valeur3	Type Valeur3	Déclencheurs
31420	Change_Password_Failure	Numéro d'erreur	Opérateur booléen	Survient lorsque la modification d'un mot de passe échoue.
31421	Change_Password_Success			Survient lorsque la modification d'un mot de passe réussit.

C.6 Portlet de changement de mot de passe en cas d'oubli

Tableau C-14 *Champs du portlet de changement de mot de passe en cas d'oubli : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Text3 Title (Titre Texte3)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre Texte3
31420	Forgot_Password_Change_Failure	ID initiateur	DN cible	Message d'erreur
31421	Forgot_Password_Change_Success	ID initiateur	DN cible	

Tableau C-15 *Champs du portlet de changement de mot de passe en cas d'oubli : Value3 Title (Titre Valeur3), Value3 Type (Type Valeur3) et Group Title (Titre du groupe)*

ID événement	Description	Titre Valeur3	Type Valeur3	Titre du groupe
31420	Forgot_Password_Change_Failure	Numéro d'erreur	Opérateur booléen	Numéro de groupe
31421	Forgot_Password_Change_Success			Numéro de groupe

Tableau C-16 *Champs du portlet de changement de mot de passe en cas d'oubli : Group Type (Type de groupe) et Triggers (Déclencheurs)*

ID événement	Description	Type de groupe	Déclencheurs
31420	Forgot_Password_Change_Failure	Numéro	Survient lorsque la modification d'un mot de passe oublié échoue.
31421	Forgot_Password_Change_Success	Numéro	Survient lorsque la modification d'un mot de passe oublié réussit.

C.7 Portlet de liste de recherche

Tableau C-17 *Champs du portlet de liste de recherche : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Group Title (Titre du groupe)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre du groupe
31430	Search_Request	ID utilisateur	Clé de recherche	ID utilisateur
31431	Search_Saved	ID utilisateur	Clé de recherche	ID utilisateur

Tableau C-18 *Champs du portlet de liste de recherche : Group Type (Type de groupe), Data Title (Titre des données) et Data Type (Type de données)*

ID événement	Description	Type de groupe	Titre des données	Type de données
31430	Search_Request	Numéro	Rechercher XML	Chaîne
31431	Search_Saved	Numéro	Rechercher XML	Chaîne

Tableau C-19 *Champs du portlet de liste de recherche : Déclencheurs*

ID événement	Description	Déclencheurs
31430	Search_Request	Survient lorsqu'un utilisateur effectue une demande de recherche.
31431	Search_Saved	Survient lorsque l'utilisateur sélectionne Mes recherches enregistrées.

C.8 Portlet de création

Tableau C-20 *Créer les champs du portlet : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Subtarget Title (Titre de la cible secondaire)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
31440	Create_Entity	Nom d'utilisateur	DN de l'entité	Définition de l'entité

Tableau C-21 *Créer les champs du portlet : Déclencheurs*

ID de l'événement	Description	Déclencheurs
31440	Create_Entity	Survient lorsqu'un objet est créé.

C.9 Contexte de sécurité

Les tableaux suivants contiennent la liste des événements de sécurité pouvant faire l'objet d'un audit dans Novell Audit.

Tableau C-22 *Champs du contexte de sécurité : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Text1 Title (Titre Texte1)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre Texte1
31540	Create_Proxy_Definition_Success	ID initiateur	Définition	Détails
31541	Create_Proxy_Definition_Failure	ID initiateur	Définition	Détails

ID événement	Description	Titre d'origine	Titre de la cible	Titre Texte1
31542	Update_Proxy_Definition_Success	ID initiateur	Définition	Détails
31543	Update_Proxy_Definition_Failure	ID initiateur	Définition	Détails
31544	Delete_Proxy_Definition_Success	ID initiateur	Définition	Détails
31545	Delete_Proxy_Definition_Failure	ID initiateur	Définition	Détails
31546	Create_Delegatee_Definition_Success	ID initiateur	Définition	Détails
31547	Create_Delegatee_Definition_Failure	ID initiateur	Définition	Détails
31548	Update_Delegatee_Definition_Success	ID initiateur	Définition	Détails
31549	Update_Delegatee_Definition_Failure	ID initiateur	Définition	Détails
3154A	Delete_Delegatee_Definition_Success	ID initiateur	Définition	Détails
3154B	Delete_Delegatee_Definition_Failure	ID initiateur	Définition	Détails
3154C	Create_Availability_Success	ID initiateur	Cible	
3154D	Create_Availability_Failure	ID initiateur	Cible	Détails
3154E	Delete_Availability_Success	ID initiateur	Cible	Détails
3154F	Delete_Availability_Failure	ID initiateur	Cible	Détails

Tableau C-23 *Champs du contexte de sécurité : Text3 Title (Titre Texte3), Data Title (Titre des données) et Data Type (Type de données)*

ID événement	Description	Titre Texte3	Titre des données	Type de données
31540	Create_Proxy_Definition_Success			
31541	Create_Proxy_Definition_Failure	Message d'erreur	Trace de pile	Chaîne
31542	Update_Proxy_Definition_Success			
31543	Update_Proxy_Definition_Failure	Message d'erreur	Trace de pile	Chaîne
31544	Delete_Proxy_Definition_Success			
31545	Delete_Proxy_Definition_Failure	Message d'erreur	Trace de pile	Chaîne
31546	Create_Delegatee_Definition_Success			
31547	Create_Delegatee_Definition_Failure	Message d'erreur	Trace de pile	Chaîne
31548	Update_Delegatee_Definition_Success			
31549	Update_Delegatee_Definition_Failure	Message d'erreur	Trace de pile	Chaîne
3154A	Delete_Delegatee_Definition_Success			
3154B	Delete_Delegatee_Definition_Failure	Message d'erreur	Trace de pile	Chaîne
3154C	Create_Availability_Success			

ID événement	Description	Titre Texte3	Titre des données	Type de données
3154D	Create_Availability_Failure	Message d'erreur	Trace de pile	Chaîne
3154E	Delete_Availability_Success			
3154F	Delete_Availability_Failure	Message d'erreur	Trace de pile	Chaîne

Tableau C-24 *Champs du contexte de sécurité : Déclencheurs*

ID événement	Description	Déclencheurs
31540	Create_Proxy_Definition_Success	Survient lorsque la création de la définition d'un proxy réussit.
31541	Create_Proxy_Definition_Failure	Survient lorsque la création de la définition d'un proxy échoue.
31542	Update_Proxy_Definition_Success	Survient lorsque la mise à jour de la définition d'un proxy réussit.
31543	Update_Proxy_Definition_Failure	Survient lorsque la mise à jour de la définition d'un proxy échoue.
31544	Delete_Proxy_Definition_Success	Survient lorsque la suppression de la définition d'un proxy réussit.
31545	Delete_Proxy_Definition_Failure	Survient lorsque la suppression de la définition d'un proxy échoue.
31546	Create_Delegatee_Definition_Success	Survient lorsque la création de la définition d'un délégué réussit.
31547	Create_Delegatee_Definition_Failure	Survient lorsque la création de la définition d'un délégué échoue.
31548	Update_Delegatee_Definition_Success	Survient lorsque la mise à jour de la définition d'un délégué réussit.
31549	Update_Delegatee_Definition_Failure	Survient lorsque la mise à jour de la définition d'un délégué échoue.
3154A	Delete_Delegatee_Definition_Success	Survient lorsque la suppression de la définition d'un délégué réussit.
3154B	Delete_Delegatee_Definition_Failure	Survient lorsque la suppression de la définition d'un délégué échoue.
3154C	Create_Availability_Success	Survient lorsque la création d'un état de disponibilité réussit.
3154D	Create_Availability_Failure	Survient lorsque la création d'un état de disponibilité échoue.
3154E	Delete_Availability_Success	Survient lorsque la suppression d'un état de disponibilité réussit.

ID événement	Description	Déclencheurs
3154F	Delete_Availability_Failure	Survient lorsque la suppression d'un état de disponibilité échoue.

C.10 Flux

Les tableaux suivants contiennent la liste des événements de l'application utilisateur pouvant faire l'objet d'un audit dans Novell Audit.

Tableau C-25 *Champs du workflow : Originator Title (Titre d'origine), Target Title (Titre de la cible) et Subtarget Title (Titre de la cible secondaire)*

ID événement	Description	Titre d'origine	Titre de la cible	Titre de la cible secondaire
31520	Workflow_Error	ID initiateur		
31521	Workflow_Started	ID initiateur		
31522	Workflow_Forwarded	ID initiateur	Destinataire	Nom du processus
31523	Workflow_Reassigned	ID initiateur	Destinataire	Nom du processus
31524	Workflow_Approved	ID initiateur	Destinataire	Nom du processus
31525	Workflow_Refused	ID initiateur	Destinataire	Nom du processus
31526	Workflow_Ended	ID initiateur	Destinataire	Nom du processus
31527	Workflow_Claimed	ID initiateur	Destinataire	Nom du processus
31528	Workflow_Unclaimed	ID initiateur	Destinataire	Nom du processus
31529	Workflow_Denied	ID initiateur	Destinataire	Nom du processus
3152A	Workflow_Completed	ID initiateur	Destinataire	Nom du processus
3152B	Workflow_Timedout	ID initiateur	Destinataire	Nom du processus
3152C	User_Message	ID initiateur	Author	
3152D	Provision_Error	ID initiateur	Destinataire	Nom du processus
3152E	Provision_Submitted	ID initiateur	Destinataire	Nom du processus
3152F	Provision_Success	ID initiateur	Destinataire	Nom du processus
31530	Provision_Failure	ID initiateur	Destinataire	Nom du processus
31531	Provision_Granted	ID initiateur	Destinataire	Nom du processus
31532	Provision_Revoked	ID initiateur	Destinataire	Nom du processus
31533	Workflow_Retracted	ID initiateur	Destinataire	Nom du processus

Tableau C-26 *Champs du workflow : Text1 Title (Titre Texte1), Text2 Title (Titre Texte2) et Text3 Title (Titre Texte3)*

ID événement	Description	Titre Texte1	Titre Texte2	Titre Texte3
31520	Workflow_Error	Activité	ID de processus	Message d'erreur
31521	Workflow_Started	Activité	ID de processus	
31522	Workflow_Forwarded	Activité	ID de processus	
31523	Workflow_Reassigned	Activité	ID de processus	
31524	Workflow_Approved	Activité	ID de processus	Utilisateur secondaire
31525	Workflow_Refused	Activité	ID de processus	Utilisateur secondaire
31526	Workflow_Ended	Activité	ID de processus	
31527	Workflow_Claimed	Activité	ID de processus	Utilisateur secondaire
31528	Workflow_Unclaimed	Activité	ID de processus	Utilisateur secondaire
31529	Workflow_Denied	Activité	ID de processus	Utilisateur secondaire
3152A	Workflow_Completed	Activité	ID de processus	
3152B	Workflow_Timedout	Activité	ID de processus	
3152C	User_Message		Message	
3152D	Provision_Error	Activité	ID de processus	Message d'erreur
3152E	Provision_Submitted	Activité	ID de processus	
3152F	Provision_Success	Activité	ID de processus	
31530	Provision_Failure	Activité	ID de processus	
31531	Provision_Granted	Activité	ID de processus	
31532	Provision_Revoked	Activité	ID de processus	
31533	Workflow_Retracted	Activité	ID de processus	Utilisateur secondaire

Tableau C-27 *Champs du workflow : Value3 Title (Titre Valeur3), Value3 Type (Type Valeur3) et Data Title (Titre des données)*

ID événement	Description	Titre Valeur3	Type Valeur3	Titre des données
31520	Workflow_Error	Numéro d'erreur	Opérateur booléen	Trace de pile
31521	Workflow_Started			
31522	Workflow_Forwarded			
31523	Workflow_Reassigned			

ID événement	Description	Titre Valeur3	Type Valeur3	Titre des données
31524	Workflow_Approved			Type d'utilisateur secondaire
31525	Workflow_Refused			Type d'utilisateur secondaire
31526	Workflow_Ended			
31527	Workflow_Claimed			Type d'utilisateur secondaire
31528	Workflow_Unclaimed			Type d'utilisateur secondaire
31529	Workflow_Denied			Type d'utilisateur secondaire
3152A	Workflow_Completed			
3152B	Workflow_Timedout			
3152C	User_Message			
3152D	Provision_Error	Numéro d'erreur	Opérateur booléen	Trace de pile
3152E	Provision_Submitted			
3152F	Provision_Success			
31530	Provision_Failure			
31531	Provision_Granted			
31532	Provision_Revoked			
31533	Workflow_Retracted			Type d'utilisateur secondaire

Tableau C-28 *Champs du workflow : Déclencheurs et type des données*

ID événement	Description	Type de données	Déclencheurs
31520	Workflow_Error	Chaîne	De nombreux éléments peuvent donner lieu à cet événement.
31521	Workflow_Started		Survient lorsque le workflow démarre.
31522	Workflow_Forwarded		Survient lorsque le workflow est envoyé.
31523	Workflow_Reassigned		Survient lorsque le workflow est réassigné.
31524	Workflow_Approved	Chaîne	Survient lorsque le workflow est approuvé.
31525	Workflow_Refused	Chaîne	Survient lorsque le workflow est refusé.
31526	Workflow_Ended		Survient lorsque le workflow est fini.

ID événement	Description	Type de données	Déclencheurs
31527	Workflow_Claimed	Chaîne	Survient lorsque le workflow est réclamé.
31528	Workflow_Unclaimed	Chaîne	
31529	Workflow_Denied	Chaîne	Survient lorsque le workflow est refusé.
3152A	Workflow_Completed		Survient lorsque le workflow est terminé.
3152B	Workflow_Timedout		Survient lorsque le workflow a expiré.
3152C	User_Message		
3152D	Provision_Error	Chaîne	De nombreux éléments peuvent donner lieu à cet événement.
3152E	Provision_Submitted		
3152F	Provision_Success		
31530	Provision_Failure		
31531	Provision_Granted		
31532	Provision_Revoked		
31533	Workflow_Retracted	Chaîne	Survient lorsque le workflow est retiré.

C.11 Rapports

Vous trouverez ci-après des exemples de rapports Novell Audit. Les rapports suivants peuvent être exécutés :

- Rapport d'actions d'administration
- Rapport historique de flux d'approbation
- Rapport de provisioning de ressources
- Suivi d'audit utilisateur spécifique
- Provisioning d'un utilisateur spécifique
- Provisioning d'utilisateur

Figure C-1 *Rapport d'actions d'administration*

Novell® Audit Report for Identity Manager

Administrative Action Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 5

Total # Events: 121

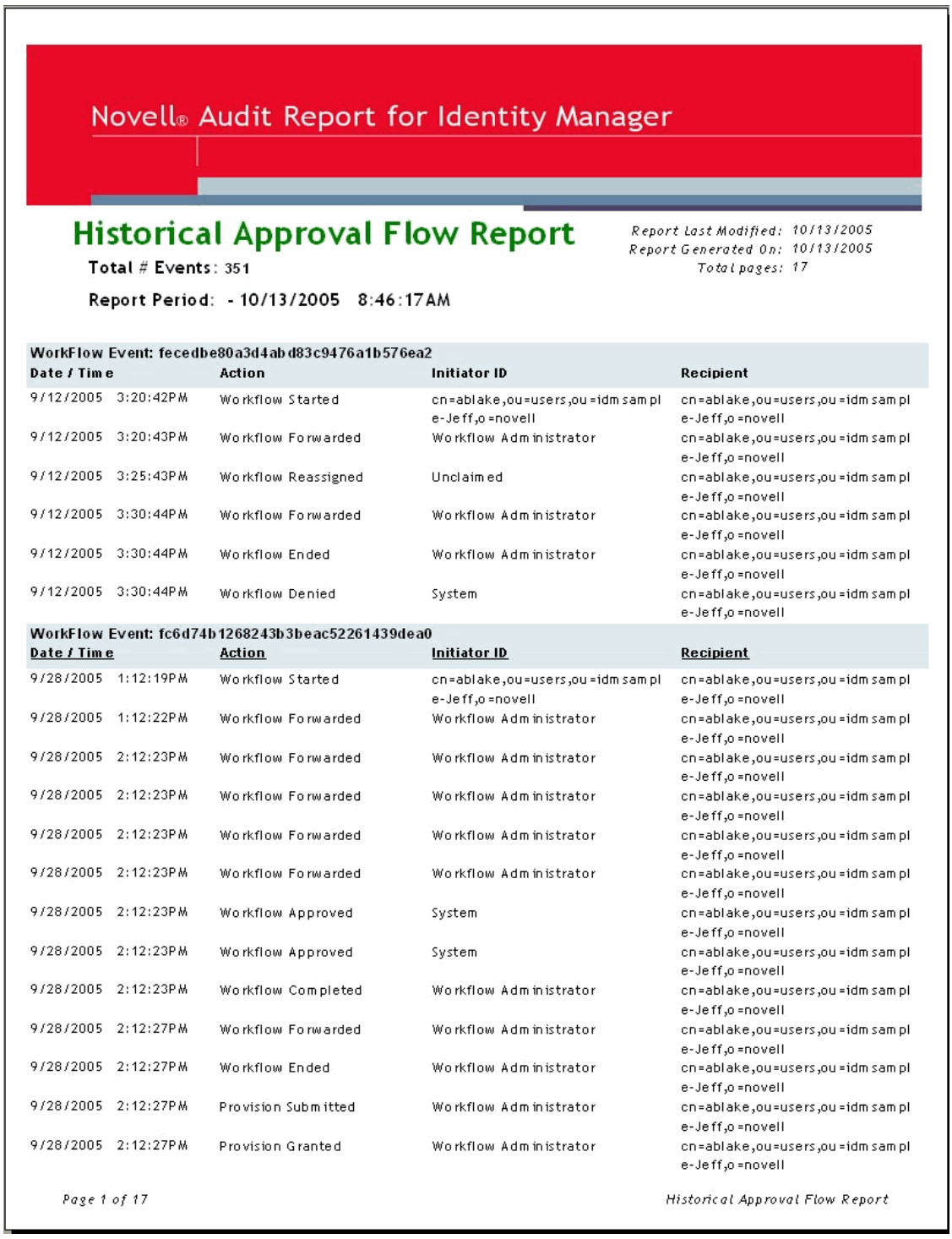
Report Period: - 10/13/2005 8:43:50AM

Date / Time	Administrator	Subject	Action
8/18/2005 5:45:17PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:07:40PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:09:05PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:12:50PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:13:39PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/23/2005 4:56:39PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Deleted
8/31/2005 12:01:55PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:02:18PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:07PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:31PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:27:58PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:28:22PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 2:59:39PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 3:24:30PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 8:11:59PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=testCreateUser,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:23PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:55PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
8/31/2005 8:13:03PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
9/1/2005 10:29:53AM	cn=admin,ou=idmsample-Jeff,o=novell	cn=aa,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
9/1/2005 11:31:45AM	cn=admin,ou=idmsample,o=novell	cn=asoprano,ou=users,ou=idmsample,o=novell	Entity Created

Page 1 of 5

Administrative Action Report

Figure C-2 *Rapport historique de flux d'approbation*



Novell® Audit Report for Identity Manager

Historical Approval Flow Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 17

Total # Events: 351

Report Period: - 10/13/2005 8:46:17AM

WorkFlow Event: fecedbe80a3d4abd83c9476a1b576ea2

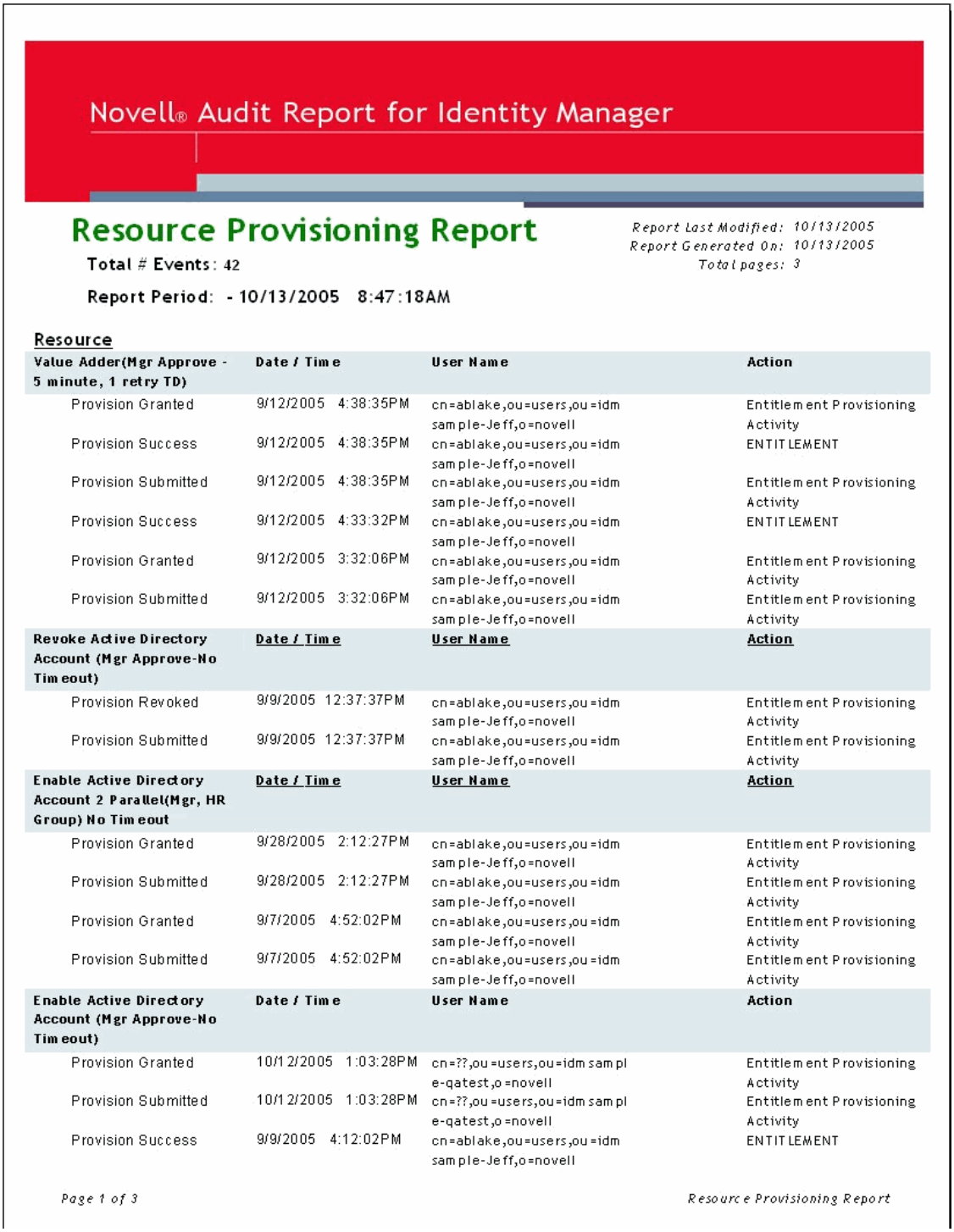
Date / Time	Action	Initiator ID	Recipient
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Denied	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

WorkFlow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID	Recipient
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Page 1 of 17 Historical Approval Flow Report

Figure C-3 *Rapport de provisioning de ressources*



Novell® Audit Report for Identity Manager

Resource Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

Total # Events: 42

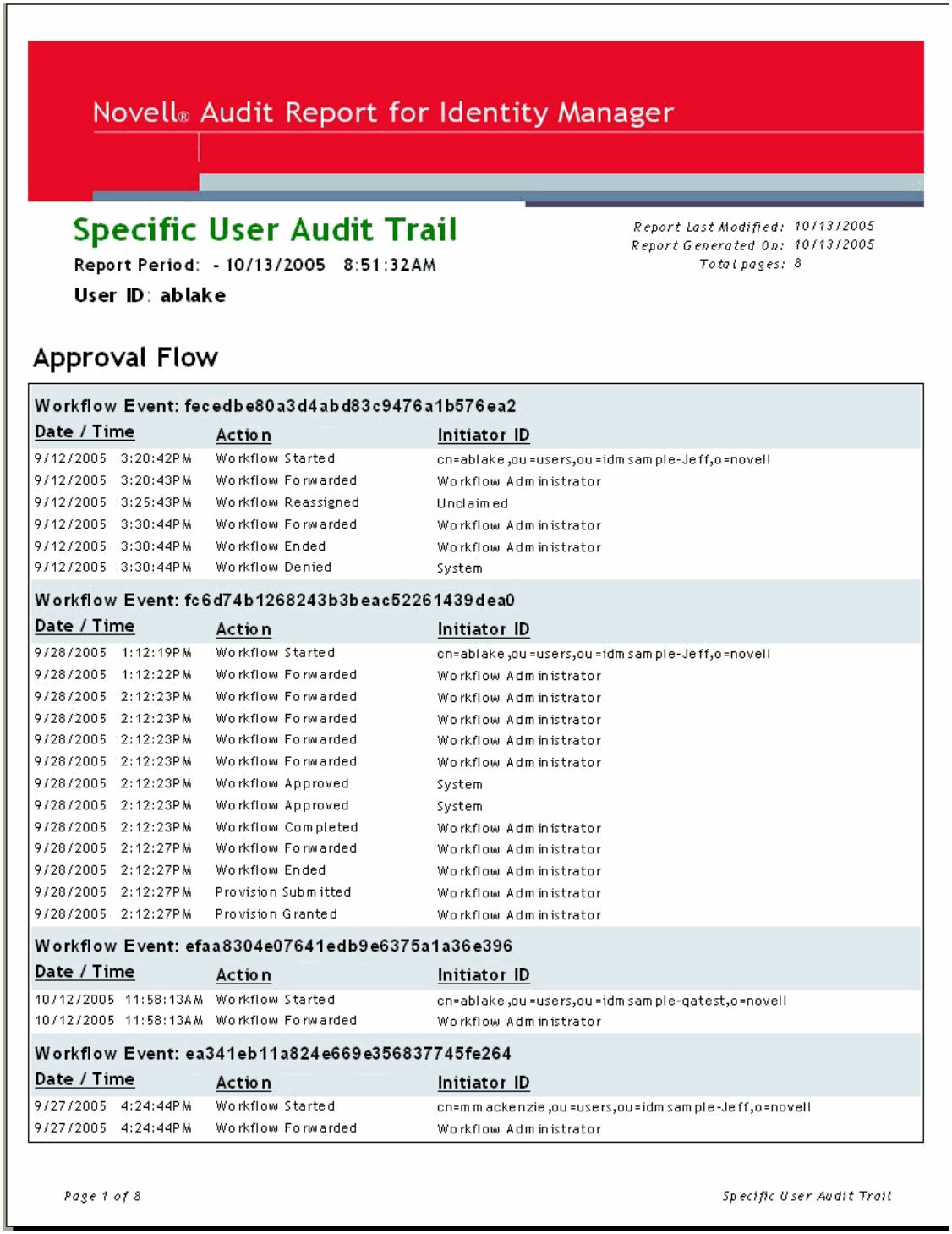
Report Period: - 10/13/2005 8:47:18AM

Resource

Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Date / Time	User Name	Action
Provision Granted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Revoke Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Revoked	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	**Date / Time**	**User Name**	**Action**
Provision Granted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Granted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Granted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Submitted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT

Page 1 of 3 Resource Provisioning Report

Figure C-4 *Suivi d'audit utilisateur spécifique 1*



Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

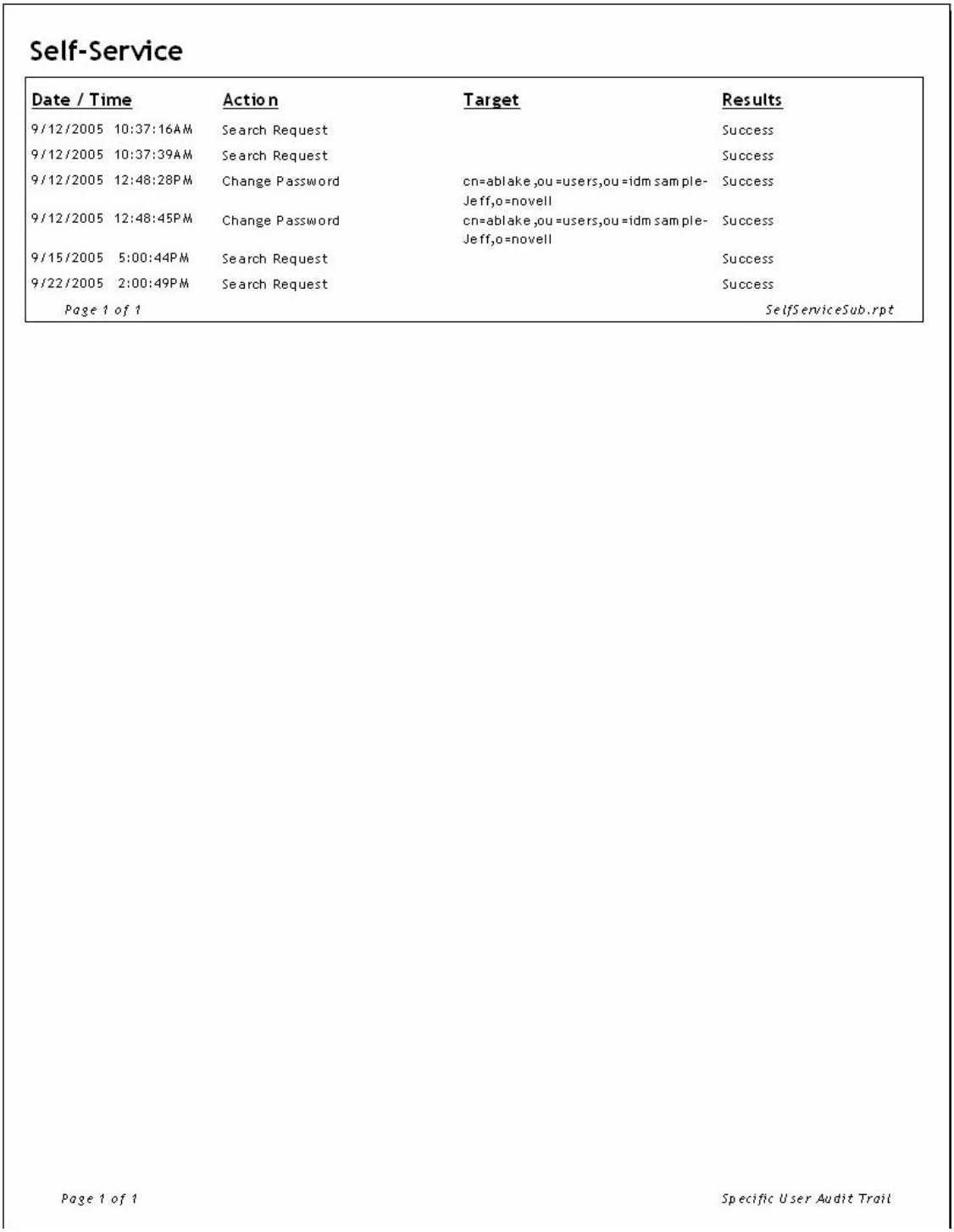
Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8 *Specific User Audit Trail*

Figure C-5 *Suivi d'audit utilisateur spécifique 2*



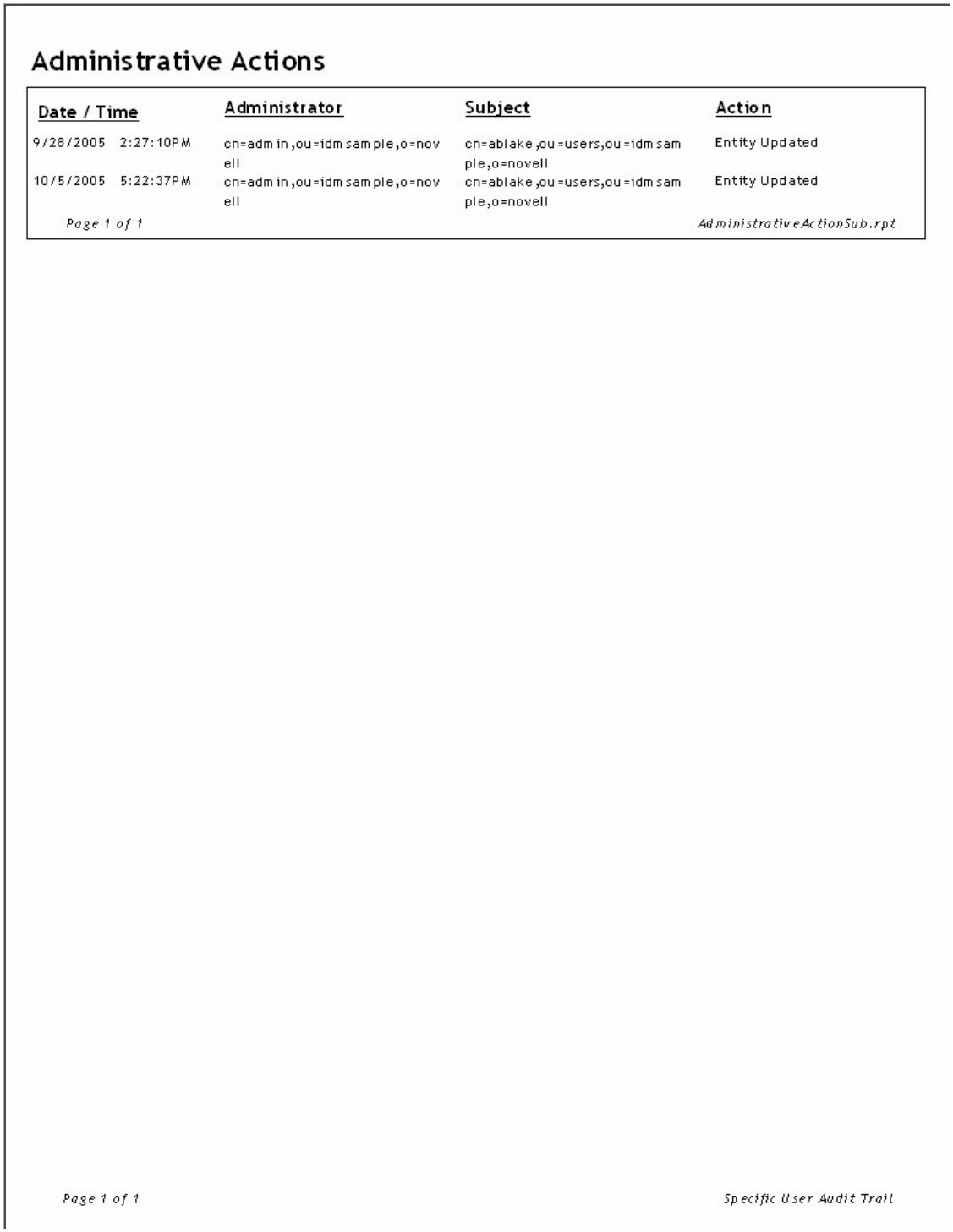
Self-Service

Date / Time	Action	Target	Results
9/12/2005 10:37:16AM	Search Request		Success
9/12/2005 10:37:39AM	Search Request		Success
9/12/2005 12:48:28PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/12/2005 12:48:45PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/15/2005 5:00:44PM	Search Request		Success
9/22/2005 2:00:49PM	Search Request		Success

Page 1 of 1 *SelfServiceSub.rpt*

Page 1 of 1 *Specific User Audit Trail*

Figure C-6 *Suivi d'audit utilisateur spécifique 3*



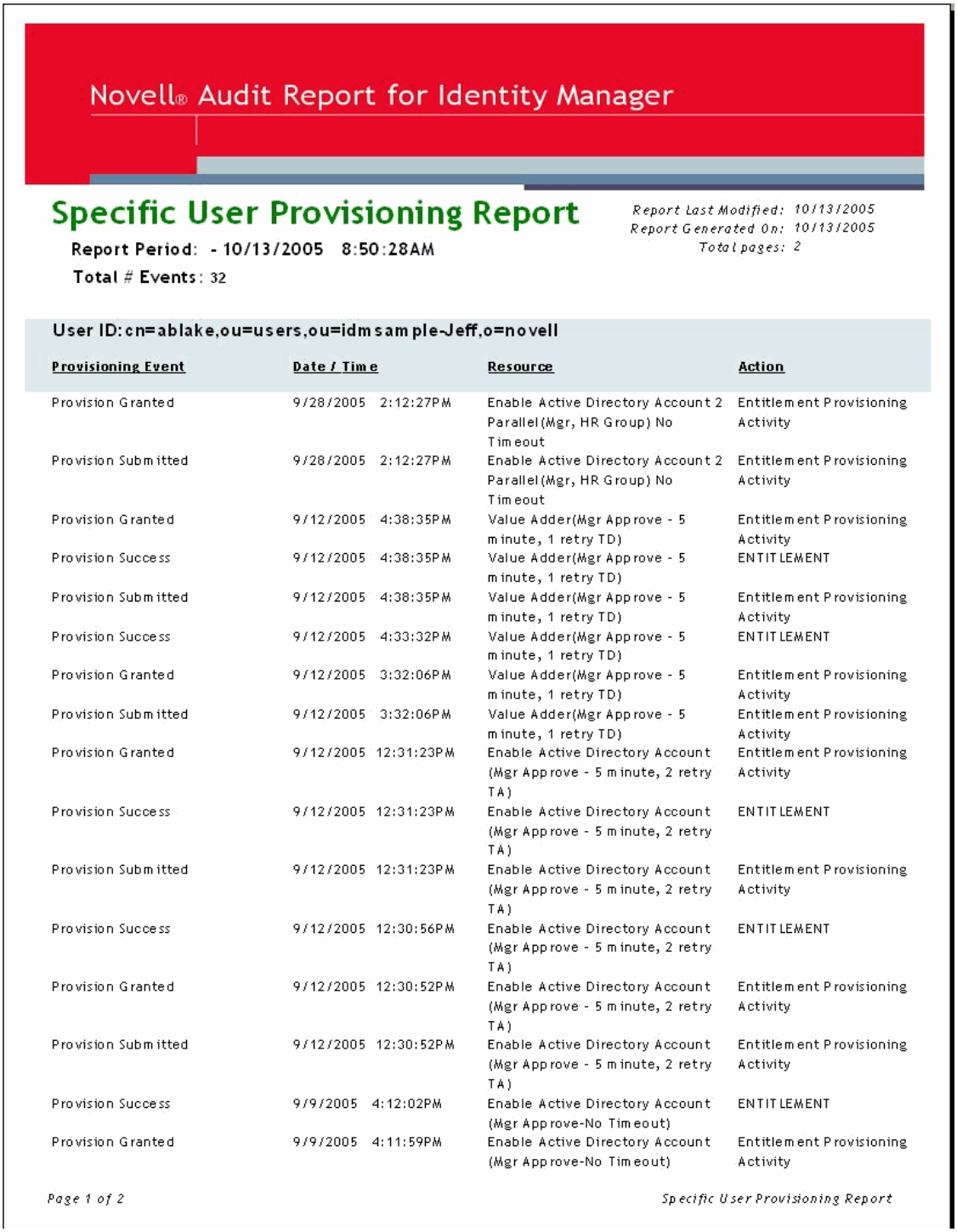
Administrative Actions

Date / Time	Administrator	Subject	Action
9/28/2005 2:27:10PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated
10/5/2005 5:22:37PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated

Page 1 of 1 AdministrativeActionSub.rpt

Page 1 of 1 Specific User Audit Trail

Figure C-7 *Rapport de provisioning d'un utilisateur spécifique*



Novell® Audit Report for Identity Manager

Specific User Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 2

Report Period: - 10/13/2005 8:50:28AM

Total # Events: 32

User ID: cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Provisioning Event	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 2

Specific User Provisioning Report

Figure C-8 *Rapport de provisioning d'utilisateur*

Novell® Audit Report for Identity Manager

User Provisioning Report

Total # Events: 42

Report Period: - 10/13/2005 8:54:20AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

User

cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 3 *User Provisioning Report*

Pilote de services de tâches manuelles : données de remplacement

D

Les données de remplacement sont utilisées avec les documents XML qui servent de modèles pour la construction des messages électroniques, des pages Web et des documents XDS. Le remplacement s'effectue en fait lors du traitement du document modèle à l'aide d'une feuille de style XSLT qui exécute elle-même le remplacement dans le cadre de la construction du document final.

Les données de remplacement sont fournies au pilote de service de tâches manuelles via différents mécanismes sur le canal Abonné et le canal Éditeur.

Canal Abonné

- Les données de remplacement sont fournies dans l'élément <mail>.
- Une partie des données de remplacement fournies peut être des données URL. Si des données URL sont fournies, elles sont traitées, complétées et remplacées par des éléments de données automatiques (reportez-vous à l'Annexe E, « Pilote de services de tâches manuelles : éléments de données de remplacement automatiques », page 309).
- Si l'élément <mail> spécifie qu'une valeur d'association doit être construite (c'est-à-dire que l'élément <mail> a un attribut src-dn), un élément de données automatiques nommé « association » est ajouté aux données de remplacement.

Canal Éditeur

- Les données de remplacement sont fournies avec les données HTTP URL et HTTP POST.
- Les éléments de données de remplacement d'URL automatiques sont ajoutés aux données de remplacement avant leur utilisation dans le traitement du modèle.

Pendant le traitement du modèle, les données de remplacement se présentent sous la forme d'un document XML. Le document contenant les données de remplacement est transmis à la feuille de style qui traite le modèle sous la forme d'un paramètre nommé « replacement-data ». Si aucun modèle n'est utilisé, le document XML est traité directement par la feuille de style.

D.1 Sécurité des données

Les éléments de données sont acheminés du canal Abonné vers le canal Éditeur via une URL qui figure dans le message électronique envoyé par le canal Abonné. La modification de certains éléments de données de l'URL représente un risque pour la sécurité des données. Par exemple, si les valeurs « responder-dn » de l'URL fournie par le canal Abonné sont remplacées par le DN d'un autre utilisateur dans l'URL soumise au serveur Web du canal Éditeur, un utilisateur non autorisé pourra modifier des données dans eDirectory.

Pour garantir la correspondance exacte entre les données contenues dans l'URL soumise et celles fournies à l'origine par le canal Abonné, les données fournies sont protégées. Les données protégées sont des données qui ne peuvent pas être modifiées pour des raisons de sécurité. La configuration de

ces données varie mais elle inclut toujours les éléments de données responder-dn et les éléments de données correspondant à tout objet eDirectory dont les valeurs doivent être modifiées.

Pour protéger les éléments de données; il suffit de coder les valeurs d'origine et de placer les valeurs codées dans une chaîne de requête d'URL. Lorsque le serveur Web du canal Éditeur reçoit les valeurs codées, le canal Éditeur les décode et les compare aux éléments de données non codées fournis par une requête HTTP GET ou POST.

Si l'instance d'un élément de données figure parmi les données codées, une valeur d'élément de données non codées doit correspondre à l'une des valeurs d'élément de données codées. Si la valeur de l'élément de données non codées ne correspond à aucune valeur d'élément de données codées, la requête HTTP est rejetée par le serveur Web du canal Éditeur.

En outre, toute requête HTTP POST qui ne contient pas de données protégées est rejetée.

Exemple

Dans une requête HTTP POST, le serveur Web du canal Éditeur utilise les données POST non codées nommées « responder-dn » pour vérifier le mot de passe fourni par les données POST. Cela permet d'authentifier l'utilisateur qui répond auprès de l'objet eDirectory de l'utilisateur.

Supposons que le contenu de l'élément <url-query> du canal Abonné spécifie deux éléments de données comme suit :

```
<item name="responder-dn" protect="yes">\PERIN-TAO\novell\phb</item>

<item name="responder-dn" protect="yes">\PERIN-TAO\novell\carol</item>
```

Les données protégées contenues dans l'URL générée par le canal Abonné contiendront deux valeurs « responder-dn ».

Supposons qu'un utilisateur malveillant obtienne l'URL générée et envoyée dans un message électronique. Il utilise ensuite cette URL afin d'obtenir le formulaire HTML qui permet aux utilisateurs de modifier les données d'un objet eDirectory.

Dans la requête HTTP POST soumise au serveur Web, l'utilisateur malveillant utilise son DN eDirectory (responder-dn=\PERIN-TAO\novell\wally) comme valeur « responder-dn » non codée. Il inclut également son propre mot de passe dans les données POST pour que l'authentification effectuée par le serveur Web réussisse.

Toutefois, lorsque le serveur Web du canal Éditeur reçoit les données HTTP POST, il ne peut pas trouver “\PERIN-TAO\novell\wally” dans les données protégées codées et rejette la requête POST.

D.2 Éléments XML

Les éléments qui composent un document de données de remplacement sont décrits ci-dessous. L'absence de description pour un élément indique qu'aucun attribut XML n'est autorisé pour cet élément.

D.2.1 <replacement-data>

L'élément <replacement-data> peut apparaître dans les emplacements suivants :

1. En tant qu'enfant de l'élément <message> sous un élément <mail> du canal Abonné.

   Le pilote de services de tâches manuelles traite l'élément <replacement-data> fourni dans un élément <replacement-data> autonome utilisable lors du traitement du modèle. Le traitement suivant est effectué :

   a. Si une valeur d'association est créée pour l'élément <mail>, un élément <item name="association"> est ajouté aux données de remplacement. La valeur de l'élément créé est la valeur d'association renvoyée à Identity Manager.

   b. Si l'élément <replacement-data> possède un élément <url-data> enfant, celui-ci est remplacé par plusieurs éléments <item> contenant des données d'URL construites. Reportez-vous à <url-data> et <url-query>.

2. Comme élément supérieur autonome d'un document de données de remplacement utilisé pour construire un document avec une feuille de style sur le canal Abonné ou sur le canal Éditeur.

D.2.2 <item>

L'élément <item> peut être un enfant de l'élément <replacement-data>, <url-data> ou <url-query>. Le contenu de l'élément <item> est le texte utilisé lors de la substitution des jetons de remplacement dans les modèles. Les éléments <item> sont toujours désignés par l'attribut de nom.

attributs <item>

name : la valeur de l'attribut name précise le nom sous lequel cet élément de données est désigné par les jetons de remplacement. Par exemple, si la valeur de l'attribut est « manager », le jeton de remplacement $manager$ est remplacé par la valeur contenue dans l'élément <item name="manager">. L'attribut name est obligatoire.

protect : pour les éléments <item> qui sont des enfants des éléments <url-query>, l'attribut protect indique si l'élément est ajouté à la section de données protégées de la chaîne de requête URL (reportez-vous à <url-query>). Si l'attribut protect est présent, sa valeur doit être yes.

Noms <item> prédéfinis

Certains éléments <item> ont des significations prédéfinies pour le canal Abonné, le canal Éditeur ou les deux canaux.

template : le canal Éditeur traite la valeur de l'élément « template » comme le nom du document modèle à utiliser pour produire la réponse à une requête HTTP GET.

Lorsque <item name="template" apparaît comme enfant d'un élément <url-query> sur le canal Abonné, la valeur correspondante est placée dans les données de requête URL afin d'indiquer au serveur Web du canal Éditeur le nom du document modèle à utiliser lors de la réponse à la requête HTTP GET.

responder-dn : le canal Éditeur utilise la valeur de l'élément « responder-dn » qui figure dans les données HTTP POST comme DN de l'objet eDirectory auprès duquel le mot de passe fourni dans les données HTTP POST est validé.

Le serveur Web rejette toute requête HTTP POST qui ne contient pas une valeur responder-dn et une valeur de mot de passe. En outre, si les données HTTP POST ne contiennent pas d'élément de données protégées, la requête est rejetée.

Le canal Abonné fournit un ou plusieurs éléments <item name="responder-dn" protect="yes"> sous l'élément <url-query>. Comme les éléments « responder-dn » sont utilisés pour authentifier l'utilisateur, ils doivent être protégés.

password: fourni par le serveur Web du canal Éditeur via les données HTTP POST. Le contenu de l'élément est le mot de passe, qui est validé par rapport à l'objet eDirectory spécifié par l'élément responder-dn dans les données POST. L'élément « password » est normalement entré dans le formulaire HTML utilisé pour générer la requête HTTP POST.

Exemple :

```
<INPUT TYPE= "password" NAME="password" SIZE="20" MAXLENGTH="40"/>
```

response-template : fourni par le serveur Web via les données HTTP POST. Permet de générer la page Web utilisée en réponse à la requête POST. Cet élément est normalement spécifié par un élément INPUT masqué dans le formulaire HTML utilisé pour générer la requête HTTP POST.

Exemple :

```
<INPUT TYPE="hidden" NAME="response-template" VALUE="post_form.xml"/>
```

response-stylesheet : fourni par le serveur Web via les données HTTP POST. Permet de générer la page Web utilisée en réponse à la requête POST. Cet élément est normalement spécifié par un élément INPUT masqué dans le formulaire HTML utilisé pour générer la requête HTTP POST.

Exemple :

```
<INPUT TYPE="hidden" NAME="response-stylesheet"
VALUE="process_template.xsl"/>
```

auth-template : fourni par le serveur Web via les données HTTP POST. Permet de générer la page Web utilisée en réponse à la requête POST si l'authentification de l'utilisateur échoue. Cet élément est normalement spécifié par un élément INPUT masqué dans le formulaire HTML utilisé pour générer la requête HTTP POST.

Exemple :

```
<INPUT TYPE="hidden" NAME="auth-template" VALUE="auth_response.xml"/>
```

auth-stylesheet : fourni par le serveur Web via les données HTTP POST. Permet de générer la page Web utilisée en réponse à la requête POST si l'authentification de l'utilisateur échoue. Cet élément est normalement spécifié par un élément INPUT masqué dans le formulaire HTML utilisé pour générer la requête HTTP POST.

Exemple :

```
<INPUT TYPE="hidden" NAME="auth-stylesheet"
VALUE="process_template.xsl"/>
```

protected-data : cet élément de données contient les données codées construites par le canal Abonné. Sur le canal Abonné, les données protégées sont un élément fourni automatiquement.

Sur le canal Éditeur, l'élément de données « protected-data » est obtenu à partir de la chaîne de requête d'URL correspondant à une requête HTTP GET, et à partir des données POST correspondant à une requête HTTP POST.

L'élément « protected-data » est généralement transmis de la requête HTTP GET à la page Web utilisée pour générer la requête HTTP POST via un jeton de remplacement contenu dans le modèle utilisé pour construire la réponse à la requête HTTP GET.

Exemple :

```
<INPUT TYPE="hidden" NAME="protected-data" VALUE="$protected-data$"/>
```

D.2.3 <url-data>

L'élément <url-data> est un enfant de l'élément <replacement-data> qui figure sous l'élément <message> sur le canal Abonné. Il contient les éléments <item> qui permettent de construire l'URL et les éléments de données associés fournis au modèle utilisé pour la construction du message électronique. Il contient également l'élément <url-query>.

Dans le cadre du pilote de service de tâches manuelles, les URL comportent cinq parties :

1. Un schéma tel que http, https ou ftp.
2. Un hôte tel que www.novell.com ou 192.168.0.1
3. Un numéro de port. Deux-points, suivis d'un entier décimal. Par exemple, :80 ou :8180.
4. Un fichier ou un identificateur de ressource. En général, un nom de fichier qui peut inclure des informations de chemin. Par exemple, stylesheets/process_template.xsl.
5. Une chaîne de requête. Ensemble de paires « name-value », séparées par des caractères &. Par exemple, template=form_template.xml&protected-data=AabABJKEL=

Predefined <item> Names Under <url-data>

Les éléments <item> qui figurent sous <url-data> sont ignorés, à l'exception de ceux répertoriés ci-après. Tous sont facultatifs.

file : précise la partie fichier de l'URL. S'il est utilisé avec le serveur Web du canal Éditeur, l'élément « file » spécifie la feuille de style à utiliser pour construire la page HTML initiale renvoyée en réponse à l'URL. S'il est utilisé avec un serveur autre que le serveur Web du canal Éditeur, l'élément « file » spécifie le nom de la ressource à laquelle l'URL fera référence.

Si l'élément file n'apparaît pas, la partie fichier de l'URL est, par défaut, process_template.xsl.

scheme : élément optionnel trouvé sous l'élément <url-data>. S'il est présent, spécifie la partie protocole de l'URL (http ou ftp par exemple). L'élément « scheme » est en général utilisé uniquement si l'URL pointe vers un serveur autre que le serveur Web de l'Éditeur.

Si cet élément n'apparaît pas, la partie protocole de l'URL est par défaut http ou https, selon la configuration du serveur Web du canal Éditeur.

host : élément optionnel trouvé sous l'élément <url-data>. S'il est présent, il précise la partie hôte de l'URL. L'élément « host » est en général utilisé uniquement si l'URL pointe vers un serveur autre que le serveur Web de l'Éditeur.

Si l'élément « host » n'apparaît pas, l'hôte URL est par défaut l'adresse IP du serveur sur lequel le pilote de service de tâches manuelles fonctionne (c'est-à-dire, l'adresse IP du serveur Web du canal Éditeur).

port : élément optionnel trouvé sous l'élément <url-data>. S'il est présent, il précise la partie port de l'URL. L'élément « port » est en général utilisé uniquement si l'URL pointe vers un serveur autre que le serveur Web de l'Éditeur.

S'il n'apparaît pas, la partie port de l'URL est par défaut le port sur lequel s'exécute le serveur Web du canal Éditeur.

D.2.4 <url-query>

L'élément <url-query> est un enfant de l'élément <url-data>. Il contient des éléments <item> qui permettent de construire la partie requête de l'URL insérée dans le message électronique.

Chaque élément qui apparaît comme enfant de l'élément <url-query> est placé dans la chaîne de requête sous la forme name=“value” où « name » représente la valeur de l'attribut name de l'élément <item> et « value » est le contenu de type chaîne de l'élément <item>.

Les éléments qui apparaissent sous <url-query> peuvent avoir un attribut de protection avec la valeur « yes ». Si tel le cas, les noms et les valeurs de l'élément sont codés et placés dans une paire nom-valeur générée dans la chaîne de requête d'URL. Le nom de la valeur générée est protected-data. La valeur est la paire ou les paires nom-valeur codées et cryptées Base64 pour les attributs à plusieurs valeurs.

La protection des données garantit qu'elles ne pourront pas être modifiées lors de la soumission de l'URL au serveur Web du canal Éditeur. Par exemple, les éléments de données « responder-dn » doivent être protégés pour garantir que seuls les utilisateurs autorisés à répondre au message électronique pourront modifier les données eDirectory.

Si l'URL générée doit être utilisée avec le serveur Web du canal Éditeur, l'élément <url-query> doit contenir au moins un élément <item name=“responder-dn” protect=“yes”>, sans quoi le serveur Web rejette la requête finale HTTP POST.

Pilote de services de tâches manuelles : éléments de données de remplacement automatiques

E

Le pilote de service de tâches manuelles fournit automatiquement certains éléments de données de remplacement. Ils sont décrits dans cette section.

E.1 Données de remplacement automatiques du canal Abonné

Les éléments de données suivants sont automatiquement ajoutés aux documents de données de remplacement lors du traitement par le canal Abonné :

association : un élément <item name=”association”> est ajouté au document de données de remplacement si l'élément <mail> a un élément <association> enfant ou si l'Abonné renvoie un élément <add-association>. Le contenu de l'élément <item> est la valeur d'association pour l'objet eDirectory associé au message électronique en cours de traitement. Il est possible que la valeur d'association ne soit pas encore écrite dans l'objet eDirectory ; par conséquent, la valeur d'association ne peut pas être utilisée dans les requêtes.

url : le contenu de l'élément <item> est l'URL complète à utiliser dans le message électronique. Sur le canal Abonné, l'élément url est créé à partir des éléments suivants, sous l'élément <url-data> : scheme, host, port, file, ainsi que les éléments figurant sous l'élément <url-query>. En l'absence de valeurs pour ces éléments, les valeurs par défaut sont utilisées. Ces valeurs sont déterminées à partir de la configuration du serveur Web du canal Éditeur.

url-base : le contenu de l'élément <item> est la partie de l'URL générée qui ne contient ni l'identificateur de ressource (file), ni la chaîne de requête (query).

url-query : le contenu de l'élément <item> est une chaîne de requête d'URL générée à partir des éléments <item> qui figurent sous l'élément <url-query>.

url-file : le contenu de l'élément <item> est l'identificateur de ressource pour l'URL.

protected-data : le contenu de l'élément <item> est une forme codée des paires « name-value » obtenues à partir des éléments <item> qui figurent sous l'élément <url-query>. Seuls les éléments <item> dont l'attribut de protection a la valeur « yes » sont ajoutés à la valeur des données protégées. Reportez-vous à la section Sécurité des données de l'Annexe D, « Pilote de services de tâches manuelles : données de remplacement », page 303 afin d'obtenir plus d'informations sur les données protégées.

E.2 Données de remplacement automatiques du canal Éditeur

Les éléments de données suivants sont automatiquement ajoutés aux documents de données de remplacement pendant le traitement par le serveur Web du canal Éditeur :

post-status : un élément <item name="post-status"> est créé et ajouté au document de données de remplacement par le serveur Web du canal Éditeur pendant le traitement d'une requête HTTP POST. Une requête HTTP POST au serveur Web est une requête pour soumettre un document XDS à Identity Manager. Identity Manager renvoie un document d'état comme résultat de la soumission XDS. Le contenu de l'élément <item name="post-status"> est la valeur de l'attribut de niveau de l'élément <status> renvoyé par Identity Manager comme résultat de la soumission à Identity Manager.

L'élément « post-status » est généralement utilisé dans la construction de la page Web renvoyée en réponse à la requête HTTP POST.

post-status message : un élément <item name="post-status-message"> est créé et ajouté au document de données de remplacement par le serveur Web du canal Éditeur pendant le traitement d'une requête HTTP POST. Une requête HTTP POST au serveur Web est une requête pour soumettre un document XDS à Identity Manager. Identity Manager renvoie un document d'état comme résultat de la soumission XDS. Le contenu de l'élément <item name="post-status-message"> est la valeur de l'élément <status> renvoyé par Identity Manager comme résultat de la soumission à Identity Manager. L'élément « post-status-message » est créé uniquement si l'élément <status> renvoyé par Identity Manager a un contenu.

L'élément « post-status-message » est généralement utilisé dans la construction de la page Web renvoyée en réponse à la requête HTTP POST.

url : un élément <item name="url"> est créé et ajouté au document de données de remplacement par le serveur Web du canal Éditeur pendant le traitement des requêtes HTTP GET et HTTP POST. L'élément <item> est ajouté avant utilisation du document de données de remplacement pour construire n'importe quel document. Le protocole, l'hôte et le port (« scheme », « host », « port ») de l'URL sont déterminés par la configuration du serveur Web.

url-base : un élément <item name="url-base"> est créé et ajouté au document de données de remplacement par le serveur Web du canal Éditeur pendant le traitement des requêtes HTTP GET et HTTP POST. L'élément <item> est ajouté avant utilisation du document de données de remplacement pour construire n'importe quel document. Le contenu de l'élément url-base <item> sur le canal Éditeur est identique à celui de l'élément url <item>.

Pilote de services de tâches manuelles : référence de modèles d'éléments d'opération

F

Les éléments d'opération sont des éléments qualifiés par un espace de nom. Ils figurent dans le modèle et sont utilisés pour une commande simple ou pour créer des éléments HTML pour des formulaires HTML. L'espace de nom utilisé pour qualifier les éléments est http://www.novell.com/dirxml/manualtask/form. Dans ce document et dans les exemples de modèles fournis avec le pilote de service de tâches manuelles, le préfixe utilisé est form.

Tout élément d'opération non spécifiquement couvert dans cette section est éliminé du document final par la feuille de style de traitement du modèle (sauf si la feuille de style est personnalisée). Ce comportement permet par exemple d'inclure dans un élément « form:text » les données destinées à la construction d'un message électronique au format texte ordinaire et de créer ainsi un modèle XML valide.

F.1 <form:input>

L'élément <form:input> permet de générer un ou plusieurs éléments HTML INPUT selon qu'un ou plusieurs éléments de données de remplacement sont présents. Le nombre d'éléments INPUT créés correspond au nombre d'éléments de données de remplacement dont le nom est spécifié par l'attribut name de l'élément <form:input>.

Attributs

Name : précise le nom des éléments de données de remplacement utilisés pour créer les éléments INPUT. La valeur d'attribut sert de valeur à l'attribut name des éléments INPUT créés.

type ou TYPE : précise la valeur de l'attribut type des éléments INPUT créés.

value : si la valeur de l'attribut value est égale à « yes », un attribut value est ajouté aux éléments INPUT créés dont la valeur est la valeur de chaîne de l'élément de données de remplacement. Si la valeur de l'attribut value est différente de « yes », le contenu des éléments INPUT créés est réglé sur la valeur de chaîne de l'élément de données de remplacement.

Exemple

```
<form:input name="responder-dn" TYPE="hidden" value="yes"/>
```

crée un ou plusieurs éléments INPUT similaires à

```
<INPUT name="responder-dn" TYPE="hidden" value="\PERIN-
TAO\novell\phb"/>
```

F.2 <form:if-item-exists>

L'élément <form:if-item-exists> permet d'insérer conditionnellement des données dans le document final. Son contenu est traité uniquement si l'élément spécifié apparaît parmi les données de remplacement.

Attributs

Name : précise le nom de l'élément de données de remplacement. Si des exemples de l'élément de données de remplacement existent, le contenu de l'élément <form:if-item-exists> est traité.

Exemple

```
<form:if-item-exists name="post-status-message">
      <tr>
        <td>
          Status message was: $post-status-message$
        </td>
      </tr>
</form:if-item-exists>
```

Cet exemple insère une ligne dans un tableau HTML uniquement s'il y a un élément de données de remplacement désigné par message post-status.

F.3 <form:if-multiple-items>

L'élément « form:if-multiple-items » permet d'insérer conditionnellement des données dans le document final. Son contenu est traité uniquement si l'élément spécifié apparaît plusieurs fois parmi les données de remplacement.

Attributs

name : précise le nom de l'élément de données de remplacement. Si plusieurs exemples de l'élément de données de remplacement existent, le contenu de l'élément « form:if-multiple-items » est traité.

Exemple

```
<form:if-multiple-items name="responder-dn">
    <form:menu name="responder-dn"/>
</form:if-multiple-items>
```

Cet exemple crée un élément HTML SELECT (reportez-vous à <form:menu>) s'il y a plusieurs données de remplacement avec le nom responder-dn.

F.4 <form:if-single-item>

L'élément « form:if-single-item » permet d'insérer conditionnellement des données dans le document final. Son contenu est traité uniquement si l'élément spécifié n'apparaît qu'une seule fois parmi les données de remplacement.

Attributs

name : précise le nom de l'élément de données de remplacement. Si l'élément nommé ne figure qu'une seule fois parmi les données de remplacement, le contenu de l'élément « form:if-single-item » est traité.

Exemple

```
<form:if-single-item name="responder-dn">
  <input TYPE="hidden" name="responder-dn" value="$responder-dn$"/>
  $responder-dn$
</form:if-single-item>
```

Cet exemple insère un élément HTML INPUT et du texte de remplacement dans le document final s'il y a exactement un élément de données de remplacement nommé “responder-dn” dans les données de remplacement.

F.5 <form:menu>

L'élément « form:menu » permet de générer un élément HTML SELECT associé à un ou plusieurs éléments OPTION enfant. Le premier enfant de l'élément OPTION est marqué comme sélectionné.

Attributs

name : précise le nom de l'élément de données de remplacement. Si l'élément nommé figure parmi les données de remplacement, un élément HTML SELECT est créé dans le document final. Un élément HTML OPTION est créé en tant qu'enfant de l'élément SELECT pour chaque instance de l'élément de données qui figure parmi les données de remplacement.

Exemple

```
<form:menu name="responder-dn"/>
```

Cet exemple donne des éléments HTML similaires à ce qui suit :

```
<SELECT name="responder-dn">
    <OPTION selected>\PERIN-TAO\big-org\php</OPTION>
    <OPTION>\PERIN-TAO\big-org\carol</OPTION>
</SELECT>
```

Pilote de services de tâches manuelles : référence à l'élément <mail>

G

L'élément <mail> et son contenu sont décrits en détail dans cette section. Si aucun attribut n'est listé pour un élément, cela signifie qu'aucun attribut n'a été défini pour cet élément.

G.1 <mail>

L'élément <mail> et son contenu décrivent les données nécessaires pour construire un message SMTP.

Attributs <mail>

src-dn : contient la valeur DN de l'objet eDirectory qui déclenche le message électronique. Obligatoire si les données de l'objet doivent être modifiées via le serveur Web du canal Éditeur en réponse au message électronique.

G.2 <to>

L'élément <to> est un enfant de l'élément <mail>. Un ou plusieurs éléments <to> contiennent les adresses électroniques des destinataires principaux du message SMTP. Au moins un élément <to> est obligatoire. Chaque élément <to> doit contenir une seule adresse électronique.

G.3 <cc>

L'élément <cc> est un enfant de l'élément <mail>. Plusieurs éléments <cc> contiennent les adresses électroniques des destinataires en copie du message SMTP. Aucun élément <cc> n'est obligatoire. Chaque élément <cc> doit contenir une seule adresse électronique.

G.4 <bcc>

L'élément <bcc> est un enfant de l'élément <mail>. Plusieurs éléments <bcc> contiennent les adresses électroniques des destinataires en copie cachée du message SMTP. Aucun élément <bcc> n'est obligatoire. Chaque élément <bcc> doit contenir une seule adresse électronique.

G.5 <from>

L'élément <from> est un enfant de l'élément <mail>. L'élément <from> contient l'adresse électronique de l'expéditeur du message. L'élément <from> n'est pas obligatoire. Si l'élément <from> est absent, l'adresse fournie dans les paramètres du pilote de services de tâches manuelles est utilisée par défaut.

G.6 <reply-to>

L'élément <reply-to> est un enfant de l'élément <mail>. L'élément <reply-to> contient l'adresse électronique de l'entité à laquelle les réponses au message SMTP seront adressées. L'élément <reply-to> n'est pas obligatoire.

G.7 <subject>

L'élément <subject> est un enfant de l'élément <mail>. Son contenu de chaîne est utilisé pour définir le champ objet SMTP. L'élément <subject> n'est pas requis mais recommandé, pour des raisons évidentes.

G.8 <message>

L'élément <message> est un enfant de l'élément <mail>. Son contenu permet de construire le corps du message SMTP. Au moins un élément <message> est obligatoire. Des éléments <message> multiples peuvent être fournis lors de la construction d'un message SMTP avec des représentations alternatives du corps du message (par exemple, du texte ordinaire et HTML, ou de l'anglais et une autre langue).

Attributs <message>

mime-type : précise le type MIME du corps du message construit par l'élément <message> (par exemple text/plain ou text/html) (facultatif). Si l'attribut de type mime est absent, le pilote essaie de découvrir automatiquement le type MIME.

Les clients de messagerie peuvent utiliser le type MIME lorsqu'un message SMTP possède plusieurs représentations, ce qui permet de choisir la meilleure à afficher.

language : spécifie la langue du corps du message construit par l'élément <message> (facultatif). La valeur doit suivre la spécification SMTP. En l'absence de l'attribut de langue, aucune langue par défaut n'est fournie.

Les clients de messagerie peuvent utiliser la langue spécifiée lorsqu'un message SMTP possède plusieurs représentations, ce qui permet de choisir la meilleure à afficher.

G.9 <stylesheet>

L'élément <stylesheet> est un enfant de l'élément <message>. Le contenu de l'élément <stylesheet> est le nom de la feuille de style XSLT utilisée pour construire le corps du message. Si l'élément <stylesheet> est absent, le fichier process_template.xsl est utilisé comme feuille de style.

G.10 <template>

L'élément <template> est un enfant de l'élément <message>. Le contenu de l'élément <template> est le nom du document XML utilisé pour construire le corps du message. Si l'élément <template> est absent, le document de données de remplacement est traité par la feuille de style de message pour construire le corps du message.

G.11 <filename>

L'élément <filename> est un enfant de l'élément <attachment>. Le contenu de l'élément <filename> est un nom de fichier. La valeur de nom de fichier permet d'assigner un nom de fichier à une pièce jointe construite.

G.12 <replacement-data>

L'élément <replacement-data> est un enfant de l'élément <message>. Son contenu est utilisé comme paramètre de la feuille de style qui traite le modèle de message ou, en l'absence de modèle, est traité directement par la feuille de style du message. Le contenu de l'élément <replacement-data> est décrit dans l'Annexe D, « Pilote de services de tâches manuelles : données de remplacement », page 303 et l'Annexe E, « Pilote de services de tâches manuelles : éléments de données de remplacement automatiques », page 309.

G.13 <resource>

L'élément <resource> est un enfant de l'élément <message>. Son contenu est utilisé comme nom du fichier à incorporer dans le message SMTP en tant que ressource pour le corps du message. Par exemple, une feuille de style .css correspondant au corps d'un message HTML peut être fournie comme ressource.

Attributs <resource>

cid : précise l'ID de contenu utilisé pour désigner la ressource dans les URL qui figurent dans le corps du message. Par exemple, si une feuille de style .css est la ressource, la valeur cid peut être css-1. Dans le corps du message HTML, l'élément suivant peut servir à désigner la feuille de style .css :

```
<link href="cid:css-1" rel="style sheet" type="text/css">
```

G.14 <attachment>

L'élément <attachment> est un enfant de l'élément <mail>. Il peut avoir le même contenu que <message> ou avoir pour contenu un nom de fichier. Plusieurs éléments <attachment> peuvent apparaître en tant qu'enfants de l'élément <mail>.

Attributs <attachment>

mime-type : précise facultativement le type MIME de la pièce jointe. En l'absence de l'attribut « mime-type », le pilote essaie de découvrir automatiquement le type MIME.

language : précise facultativement la langue de la pièce jointe. En l'absence de l'attribut de langue, aucune langue par défaut n'est fournie.

Pilote de services de tâches manuelles : scénario de flux de données pour le nouvel employé

H

Cette section décrit dans le détail le flux de données généré par exemple dans la situation suivante : suite à l'embauche d'un nouvel employé, un message électronique est envoyé à son responsable. Ce message demande au responsable d'utiliser l'URL qu'il contient pour entrer un numéro de bureau pour l'employé.

La configuration du pilote de service de tâches manuelles est la suivante pour le scénario de l'exemple.

H.1 Configuration du canal Abonné

Filtre

Classe : utilisateur

Attributs : prénom, responsable, nom

Stratégies

Stratégie de création : attributs « Given Name », « manager » et « Surname » obligatoires.

Stratégie de transformation de commande : convertit l'élément <add> en élément <mail>.

H.2 Configuration du canal Éditeur

Filtre

Classe : utilisateur

Attributs : roomNumber

Stratégies

Aucun.

H.3 Description du flux de données

Dans la liste suivante, les éléments de données les plus importants qui circulent dans le processus sont « responder-dn » et « association ». L'élément « responder-dn » permet d'authentifier l'utilisateur qui entre les données via le serveur Web. L'élément « association » identifie l'objet eDirectory dont les données doivent être modifiées.

1. La société embauche un nouvel employé. Les données correspondantes sont entrées dans le système de gestions des ressources humaines (HR) de la société.

2. Le pilote Identity Manager associé au système de gestion des ressources humaines crée un nouvel objet Utilisateur dans eDirectory. Les attributs de l'objet Utilisateur incluent Given Name, Surname et manager.
3. L'événement <add> suivant pour le nouvel objet Utilisateur est soumis au canal Abonné du pilote de services de tâches manuelles :

```
<nds dtdversion="1.1" ndsversion="8.6">
  <input>
    <add class-name="User" src-dn="\PERIN-TAO\novell\Provo\Joe"
src-entry-id="281002" timestamp="1023314433#2">
      <add-attr attr-name="Surname">
        <value type="string">the Intern</value>
      <add-attr>
      <add-attr attr-name="Given Name">
        <value type="string">Joe</value>
      <add-attr>
      <add-attr attr-name="manager">
        <value type="dn">\PERIN-TAO\novell\Provo\phb</value>
      <add-attr>
    </add>
  </input>
</nds>
```

   a. La stratégie de transformation de la commande du canal Abonné utilise le DN du responsable pour envoyer à eDirectory la demande de l'adresse électronique du responsable et le DN de son assistant.
   b. Si le responsable a un assistant, la stratégie de transformation de la commande du canal Abonné envoie à eDirectory la demande d'adresse électronique de l'assistant.
   c. La stratégie de transformation de la commande du canal Abonné construit un élément <mail> et remplace l'élément de commande <add> par l'élément <mail>. Dans l'exemple ci-dessous, les éléments de données de remplacement sont en gras.

```
<nds dtdversion="1.1" ndsversion="8.6">
  <input>
    <mail src-dn="\PERIN-TAO\novell\Provo\Joe">
      <to>phb@company.com</to>
      <cc>carol@company.com</cc>
      <bcc>HR@company.com</bcc>
      <reply-to>HR@company.com</reply-to>
      <subject>Room Assignment Needed for: Joe the Intern</
subject>
      <message mime-type="text/html">
        <stylesheet>process_template.xsl</stylesheet>
        <template>html_msg_template.xml</template>
        <replacement-data>
          <item name="manager">JStanley</item>          <item
name="given-name">Joe</item>          <item name="surname">the
Intern</item>
          <url-data>
            <item name="file">process_template.xsl</item>
            <url-query>
         <item name="template">form_template.xml</item>
```

```
<item name="responder-dn" protect="yes">\PERIN-
TAO\novell\Provo\phb</item>              <item name="responder-
dn" protect="yes">\PERIN-TAO\novell\Provo\carol</item>
<item name="subject-name">Joe the Intern</item>
            </url-query>
          </url-data>
        </replacement-data>
        <resource cid="css-1">novdocmain.css</resource>
      </message>
    </mail>
  </input>
</nds>
```

d. Le canal Abonné du pilote de services de tâches manuelles reçoit l'élément <mail> de Nsure™ Identity Manager.

e. L'Abonné génère une valeur d'association parce que l'élément <mail> a un attribut src-dn.

f. Le canal Abonné construit un document de données de remplacement à partir des données de l'élément <mail>. Ce document sera utilisé pour construire le message électronique. L'URL comporte divers éléments de données dans la partie requête (la partie de l'URL qui suit le caractère « ? » et est en gras). Le serveur Web du canal Éditeur utilise ces éléments de données lorsque l'URL est soumise au serveur Web comme une requête HTTP GET.

```
<replacement-data>
  <item name="manager">JStanley</item>
  <item name="given-name">Joe</item>
  <item name="surname">the Intern</item>
  <item name="template">form_template.xml</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\carol</
item>
  <item name="subject-name">Joe the Intern</item>
  <item name="association">1671b2:ee4246a561:-
7fff:192.168.0.1</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url-file">process_template.xsl</item>
  <item name="protected-data">
rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAARbAA
1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFMAAlw
YXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ4cH
VyAAJbQqzzF/gGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAfgAEAAAA
uMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn+3+fE6SphHr3Hgjli4Jp3rUk
H7y6dXvcu7iq21Vs+9o6iZVzljTIJX/jjRrVZlR5JOuRNhk8JHFZ8FhgsmiIAH
/Fs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z/DBR13pIAobMpWY
kMaz4+G9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7zOU9Uvd9qXtaE2rR0
AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="url-
query">template=form_template.xml&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Cphb&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
```

```
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="url">
https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREV
</item>
</replacement-data>
```

g. Le canal Abonné traite html_msg_template.xml à l'aide du fichier process_template.xsl. Le document de données de remplacement est transmis à la feuille de style en tant que paramètre. Le document html_msg_template.xml suit. Notez les jetons de remplacement en gras. Les jetons de remplacement sont remplacés par la valeur des éléments <item> correspondants dans le document de données de remplacement.

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/
form">
  <head>
  </head>
  <body>
    <link href="cid:css-1" rel="style sheet" type="text/css"/>
    <p>
    Dear $manager$,
    </p>
    <p>
    This message is to inform you that your new employee
<b>$given-name$ $surname$</b> has been hired.
    </p>
    <p>
    Please assign a room number for this individual. Click <a
href="$url$">Here</a> to do this.
    </p>
    <p>
    Thank you,<br/>
    HR<br/>
    HR Department
    </p>
```

```
  </body>
</html>
```

Le message électronique généré suit. Les jetons de remplacement ont été remplacés par la valeur des éléments <item> correspondants dans le document de données de remplacement.

```
<html>
  <head>
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
  </head>
  <body>
    <link href="cid:css-1" rel="style sheet" type="text/css">
    <p>
    Dear J Stanley,
    </p>
    <p>
    This message is to inform you that your new employee <b>Joe
the Intern</b> has been hired.
    </p>
    <p>
    Please assign a room number for this individual. Click <a
href="https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&responder-dn=%5CPERIN-
TAO%5Cnovell%5CProvo%5Ccarol&subject-
name=Joe+the+Intern&association=45f0e3%3Aee45e07709%3A-
7fff%3A192.168.0.1&protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG%2BO3BAgEKdXE
AfgAEAAAAuMU%2FSoFRkebvh2d5SqalF91ttjRY5lyyW5%2B%2FFIfOuDdYikYi
DbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY%2Bi4VoVjUSXS3a8fiXB8moM
dPtLJ%2FGyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL
%2FeFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlP
S0iWzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">Here</a> to
do this.
    </p>
    <p>
    Thank you,<br>
    HR<br>
    HR Department
    </p>
  </body>
</html>
```

h. Le message électronique SMTP est envoyé au responsable et à son assistant.

i. Le canal Abonné renvoie un document XML contenant un élément <status> et un élément <add-association> à Identity Manager.

4. Le responsable ouvre le message électronique et clique sur le lien “Cliquez ici”.

5. Le navigateur Web du responsable soumet l'URL au serveur Web du canal Éditeur en tant que requête HTTP GET.
   a. Le serveur Web construit le document de données de remplacement suivant. La plupart des éléments de données proviennent de la partie requête de l'URL, à l'exception des éléments « url » et « url-base » générés automatiquement.

```
<replacement-data>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="template">form_template.xml</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\carol</
item>
  <item name="subject-name">Joe the Intern</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
</replacement-data>
```

   Le serveur Web traite le document form_templates.xml à l'aide de la feuille de style process_template.xsl. Les jetons de remplacement et les éléments d'opération sont en gras. Notez que divers éléments de données sont placés dans des éléments INPUT masqués pour permettre leur transfert au serveur Web avec les données HTML POST.

   En outre, il existe un jeton de remplacement $query:roomNumber$ qui récupère, le cas échéant, la valeur actuelle de l'attribut roomNumber de l'employé.

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/
form">
  <head>
    <title>Enter room number for $subject-name$</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css"/>
    <br/><br/><br/><br/>
    <form class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl">
        <table cellpadding="5" cellspacing="10" border="1"
align="center">
          <tr><td>
          <input TYPE="hidden" name="template"
```

```
value="post_form.xml"/>
          <input TYPE="hidden" name="subject-name"
value="$subject-name$"/>
          <input TYPE="hidden" name="association"
value="$association$"/>
          <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="response-template"
value="post_response.xml"/>
          <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/>
          <input TYPE="hidden" name="auth-template"
value="auth_response.xml"/>
          <input TYPE="hidden" name="protected-data"
value="$protected-data$"/>
          <form:if-single-item name="responder-dn">
            You are:<br/>
            <input TYPE="hidden" name="responder-dn"
value="$responder-dn$"/>
            $responder-dn$
         </form:if-single-item>        <form:if-multiple-items
name="responder-dn">
            Indicate your identity:<br/>
           <form:menu name="responder-dn"/>         </form:if-
multiple-items>
        </td></tr>
        <tr><td>
          Enter your password: <br/><input name="password"
TYPE="password" SIZE="20" MAXLENGTH="40"/>
        </td></tr>
        <tr><td>
          Enter room number for $subject-name$:<br/>
          <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="$query:roomNumber$"/>
        </td></tr>
        <tr><td>
          <input TYPE="submit" value="Submit"/> <input
TYPE="reset" value="Clear"/>
        </td></tr>
      </table>
    </form>
  </body>
</html>
```

La page HTML suivante en résulte :

```
<html>
  <head>
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
    <title>Enter room number for Joe the Intern</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
```

```
css">
    <br><br><br><br>
<form class="myform" METHOD="POST" ACTION="https://
192.168.0.1:8180/process_template.xsl">
<table cellpadding="5" cellspacing="10" border="1"
align="center">
<tr>
<td>
    <input TYPE="hidden" name="template" value="post_form.xml">
    <input TYPE="hidden" name="subject-name" value="Joe the
Intern">
    <input TYPE="hidden" name="association"
value="45f0e3:ee45e07709:-7fff:192.168.0.1">
    <input TYPE="hidden" name="response-style sheet"
value="process_template.xsl">
    <input TYPE="hidden" name="response-template"
value="post_response.xml">
    <input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl">
    <input TYPE="hidden" name="auth-template"
value="auth_response.xml">
    <input TYPE="hidden" name="protected-data"
value="rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHAC
AARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AA
J4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FIfOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">
    Indicate your identity:<br>
    <SELECT name="responder-dn">
        <OPTION selected>\PERIN-TAO\novell\Provo\phb</OPTION>
        <OPTION>\PERIN-TAO\novell\Provo\carol</OPTION>
    </SELECT>
</td>
</tr>
<tr>
<td>
    Enter your password: <br>
    <input name="password" TYPE="password" SIZE="20"
MAXLENGTH="40">
</td>
</tr>
<tr>
<td>
    Enter room number for Joe the Intern:<br>
    <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value="">
</td>
</tr>
```

```
<tr>
<td>
    <input TYPE="submit" value="Submit"> <input TYPE="reset"
value="Clear">
</td>
</tr>
</table>
</form>
</body>
</html>
```

b. Le responsable sélectionne son DN eDirectory à partir du menu de la page Web, saisit le mot de passe, saisit le numéro de bureau pour le nouvel employé et clique sur Soumettre.

c. Le navigateur Web soumet une requête HTTP POST au serveur Web.

d. Le serveur Web construit le document de données de remplacement suivant à partir des données POST. Notez les données qui étaient dans les différents éléments <INPUT> masqués. Les données entrées dans le formulaire par le responsable sont en gras.

```
<replacement-data>  <item name="room-number">cubicle 1234</
item>
  <item name="template">post_form.xml</item>
  <item name="response-template">post_response.xml</item>
  <item name="auth-template">auth_response.xml</item>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="password" is-sensitive="true"><!-content
suppressed ?</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="auth-style sheet">process_template.xsl</item>
  <item name="response-style sheet">process_template.xsl</item>
  <item name="subject-name">Joe the Intern</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
</replacement-data>
```

e. Le serveur Web vérifie si la valeur de l'élément « responder-dn » correspond à une valeur « responder-dn » contenue dans les données protégées. Si elle ne correspond pas, le serveur Web annule la demande. Si elle correspond, le traitement se poursuit.

f. Le serveur Web soumet une requête XDS <check-object-password> à Identity Manager sur le canal Éditeur pour authentifier l'utilisateur qui soumet la requête HTTP POST.

```
<nds dtdversion="1.0" ndsversion="8.6">
  <source>
    <product build="20020606_0824" instance="Manual Task
Service Driver" version="1.1a">DirXML Manual Task Service
Driver</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <check-object-password dest-dn="\PERIN-
TAO\novell\Provo\phb" event-id="chkpwd">
      <password><!-- content suppressed --></password>
    </check-object-password>
  </input>
</nds>
```

g. Identity Manager renvoie <status level=”success”>. Si Identity Manager renvoie un autre état que Succès, les modèles spécifiés par l'élément de données auth_template et la feuille de style spécifiée par l'élément de données auth_stylesheet servent à construire une page Web qui est renvoyée comme résultat de l'opération POST.

h. Le serveur Web traite le modèle post_form.xml à l'aide de la feuille de style process_template.xsl pour générer un document XDS. Les jetons de remplacement sont en gras.

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable" event-
id=”wfmod”>
      <association>$association$</association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>$room-number$</value>
        </add-value>
      </modify-attr>
    </modify>
  </input>
</nds>
```

i. L'Éditeur soumet le document XDS créé à Identity Manager.

```
<nds>
  <input>
    <modify class-name="User" src-dn="not-applicable" event-
id=”wfmod”>
      <association>45f0e3:ee45e07709:-7fff:192.168.0.1</
association>
      <modify-attr attr-name="roomNumber">
        <remove-all-values/>
        <add-value>
          <value>cubicle 1234</value>
        </add-value>
      </modify-attr>
```

```
    </modify>
  </input>
</nds>
```

j. Identity Manager renvoie un document de résultat

```
<nds dtdversion="1.1" ndsversion="8.6">
  <source>
    <product version="2.0">Identity Manager</product>
    <contact>Novell, Inc.</contact>
  </source>
  <output>
    <status event-id="wfmod" level="success"></status>
  </output>
</nds>
```

k. Le serveur Web ajoute l'élément de données de remplacement « post-status » (et éventuellement l'élément de données de remplacement « post-status-message ») au document de données de remplacement. L'élément de données ajouté apparaît en gras :

```
<replacement-data>
  <item name="room-number">cubicle 1234</item>
  <item name="template">post_form.xml</item>
  <item name="response-template">post_response.xml</item>
  <item name="auth-template">auth_response.xml</item>
  <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item>
  <item name="password" is-sensitive=”true”><!-content
suppressed ?</item>
  <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>
  <item name="responder-dn">\PERIN-TAO\novell\Provo\phb</item>
  <item name="auth-style sheet">process_template.xsl</item>
  <item name="response-style sheet">process_template.xsl</item>
  <item name="subject-name">Joe the Intern</item>
  <item name="url-base">https://192.168.0.1:8180</item>
  <item name="url">https://192.168.0.1:8180</item>
  <status event-id="" level="success"></status>  <item
name="post-status">success</item>
</replacement-data>
```

l. Le serveur Web traite le modèle post_response.xml à l'aide de la feuille de style process_template.xsl. Les jetons de remplacement et les éléments d'opération sont en gras.

```
<htm xmlns:form="http://www.novell.com/dirxml/manualtask/form">
  <head>
    <title>Result of post for $subject-name$</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css"/>
    <br/><br/><br/><br/>
    <table class="formtable" cellpadding="5" cellspacing="20"
border="1" align="center">
      <tr>
        <td>
          DirXML reported status = $post-status$
        </td>
      </tr><form:if-item-exists name="post-status-message">
      <tr>
        <td>
          Status message was: $post-status-message$
        </td>
      </tr></form:if-item-exists>
    </table>
  </body>
</html>
```

m. La page Web générée est renvoyée en réponse à la requête HTTP POST. La deuxième ligne du tableau n'apparaît pas parce que l'élément post-status-message désigné par l'élément <form:if-item-exists> est absent dans le document de données de remplacement.

```
<html>
  <head>
<META http-equiv="Content-Type" content="text/html;
charset=UTF-8">
    <title>Result of post for Joe the Intern</title>
  </head>
  <body>
    <link href="novdocmain.css" rel="style sheet" type="text/
css">
    <br><br><br><br>
    <table class="formtable" cellpadding="5" cellspacing="20"
border="1" align="center">
      <tr>
        <td>
          DirXML reported status = success
        </td>
      </tr>
    </table>
  </body>
</html>
```

Pilote de service de tâches manuelles : gestionnaires des éléments personnalisés pour le canal Abonné

Le pilote fournit un mécanisme d'extension pour l'envoi de notifications utilisateur en utilisant des méthodes autres que Simplified Mail Transport Protocol (SMTP). Par exemple, un client pourrait avoir besoin d'envoyer des notifications via l'interface MAPI (Messaging Application Programming Interface) au lieu de SMTP.

Pour utiliser un mécanisme autre que SMTP pour l'envoi de notifications, vous devez écrire une classe Java chargée de gérer l'élément XML personnalisé soumis sur le canal Abonné du pilote.

Le gestionnaire de l'élément personnalisé Java doit implémenter l'interface Java com.novell.nds.dirxml.driver.manualtask.CommandHandler. Le nom de la classe d'éléments personnalisés est précisé sous Gestionnaires supplémentaires dans la page des paramètres de configuration du canal Abonné.

Lorsque le canal Abonné trouve un élément de commande, il recherche dans son tableau de gestionnaires. Lorsqu'il trouve un gestionnaire qui signale qu'il gère l'élément de commande, l'élément de commande est transmis au gestionnaire. Le gestionnaire exécute ensuite le traitement demandé.

Il existe deux gestionnaires d'éléments de commande intégrés dans le pilote : un gestionnaire pour les éléments <mail> et un autre pour les éléments <add>.

La définition de l'élément de commande personnalisé incombe à l'auteur du gestionnaire personnalisé. La conception de l'élément <mail> est un bon début pour la conception de l'élément de commande personnalisé.

Les éléments personnalisés sont créés par des stratégies sur le canal Abonné de la même façon que l'élément <mail>.

La documentation pour com.novell.nds.dirxml.driver.manualtask.CommandHandler et la documentation pour de nombreuses classes de supports et d'utilitaires se trouvent dans les javadocs livrés avec le pilote. Les javadocs se trouvent dans le fichier nommé manual_task_docs.zip dans l'image de distribution.

I.1 Construction d'URL utilisables avec le serveur Web du canal Éditeur

Pour utiliser de façon sûre le serveur Web du canal Éditeur, il est nécessaire d'employer les classes d'utilitaires pour construire l'URL à inclure dans le message de notification. Le com.novell.nds.dirxml.driver.manualtask.URLData est conçu pour cette tâche.

L'exemple de code contenu dans SampleCommandHandler.java illustre ce processus.

I.2 Construction de documents de messages à l'aide de feuilles de style et de documents de modèles

Il est commode d'utiliser la même méthode pour construire des documents que celle du gestionnaire SMTP, qui est une combinaison de feuilles de style, de documents modèles et de données de remplacement. Pour ce faire, vous devez obtenir les documents feuilles de style et modèles et appeler par programmation le processeur de la feuille de style.

L'exemple de code contenu dans SampleCommandHandler.java illustre ce processus.

I.3 SampleCommandHandler.java

Le code source pour un gestionnaire d'exemple de commande personnalisé est inclus dans la distribution du pilote. Le code source se trouve dans le fichier manual_task_docs.zip, dans l'image de distribution.

Le gestionnaire est implémenté dans la classe com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler.

L'exemple de gestionnaire génère un document utilisant des feuilles de style et des modèles et écrit le document résultant sur un fichier.

I.3.1 Compilation de la classe SampleCommandHandler

Vous pouvez utiliser n'importe quel compilateur Java 2 pour compiler la classe SampleCommandHandler. Vous devez placer nxsl.jar, dirxml.jar, collections.jar et ManualTaskServiceBase.jar dans le chemin de classe du compilateur Java.

I.3.2 Test de la classe SampleCommandHandler

Commencez par importer l'exemple de configuration de numéro de bureau pour le pilote.

Compilez la classe SampleCommandHandler et placez le fichier de classe résultant dans un fichier .jar. Placez le fichier .jar dans le répertoire de fichiers DirXML .jar approprié à la plate-forme sur laquelle vous exécutez le pilote.

Ajoutez l'élément XML suivant sous l'élément <subscriber-options> qui figure dans la section Paramètres du pilote XML des propriétés du pilote :

```
<output-path display-name="Sample Output Path"></output-path>
```

Éditez les paramètres du pilote. Dans l'élément étiqueté Sample Output Path, placez un chemin vers un répertoire dans lequel le SampleCommandHandler écrira les documents qu'il aura créés. Dans l'élément étiqueté Gestionnaires supplémentaires, ajoutez la chaîne com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler.

Remplacez la stratégie de transformation de commande du canal Abonné par CommandXform.xsl qui se trouve dans le même répertoire que le fichier SampleCommandHandler.java.

Créez un objet Utilisateur et ajoutez une référence au responsable à l'objet Utilisateur. Si le responsable a une valeur d'adresse électronique, un élément de commande <sample> est envoyé à l'Abonné et le SampleCommandHandler écrit un fichier dans l'emplacement que vous avez spécifié précédemment.

Pilote de service de tâches manuelles : servlets personnalisés pour le canal Éditeur

J

Le pilote fournit un mécanisme d'extension par lequel une fonctionnalité supplémentaire peut être ajoutée au serveur Web du canal Éditeur. Les servlets personnalisés peuvent être chargés par l'Éditeur en spécifiant le nom des classes servlet dans l'élément de configuration Pilote étiqueté Servlets supplémentaires.

J.1 Utilisation du canal Éditeur

Si une servlet personnalisée doit soumettre des données à Identity Manager, elle doit utiliser le canal Éditeur du pilote. Les classes com.novell.nds.dirxml.driver.manualtask.ServletRegistrar et com.novell.nds.dirxml.driver.manualtask.PublisherData sont fournies pour faciliter cette opération. L'exemple de code contenu dans SampleServlet.java illustre ce processus.

J.2 Authentification

Une servlet personnalisée doit authentifier les utilisateurs qui soumettent des informations. L'exemple de code contenu dans SampleServlet.java illustre ce processus. Toutefois, le type d'authentification effectué en utilisant l'élément <check-object-password> ne contrôle par les droits eDirectory™. Les changements soumis sur le canal Éditeur sont autorisés si l'objet Pilote a les droits pour effectuer les changements, que l'utilisateur ait le droit ou non d'apporter des modifications.

Si vous utilisez une URL générée par un gestionnaire de commande sur le canal Abonné, vous devez utiliser la classe com.novell.nds.dirxml.driver.manualtask.URLData pour valider l'URL afin de garantir que l'élément de données responder-dn n'a pas été modifié. Pour des informations à ce sujet, reportez-vous à la documentation Java (javadocs).

J.3 SampleServlet.java

Le code source pour un exemple de servlet est fourni avec le pilote. Le code source se trouve dans le fichier manualtask_driver_docs.zip, dans l'image de distribution.

La servlet est implémentée dans la classe com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet.

Cette servlet accepte les requêtes HTTP GET pour toute ressource finissant par .sample. La chaîne de requête de l'URL HTTP doit contenir une donnée dest-dn, une donnée attr-name et une donnée value.

La servlet authentifie l'utilisateur puis soumet une requête de modification à Identity Manager via le canal Éditeur du pilote.

J.3.1 Compilation de la classe SampleServlet

Vous pouvez utiliser n'importe quel compilateur Java 2 pour compiler la classe SampleServlet. Vous devez placer nxsl.jar, dirxml.jar, collections.jar et ManualTaskServiceBase.jar dans le chemin de classe du compilateur Java.

J.3.2 Test de la classe SampleServlet

Commencez par importer l'exemple de configuration de numéro de bureau pour le pilote.

Compilez la classe SampleServlet et placez le fichier de classe résultant dans un fichier .jar. Placez le fichier .jar dans le répertoire de fichiers DirXML .jar approprié à la plate-forme sur laquelle vous exécutez le pilote.

Éditez les paramètres du pilote. Dans l'élément étiqueté Servlets supplémentaires, ajoutez la chaîne com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet.

Ajoutez le Numéro de téléphone au filtre du canal Éditeur.

Soumettez l'URL suivante dans un navigateur (en supposant que le navigateur fonctionne sur la même machine que le pilote) :

https:localhost:8180/1.sample?dest-dn=username.container&attr-name=Telephone%20Number&value=555-1212

Remplacez *username.container* par le DN d'un utilisateur de votre arborescence.