Novell Nsure™ Identity Manager

2

www.novell.com

GUIDE D'ADMINISTRATION

30 juin 2004

Novell®

Notices légales

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

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

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

Brevets américains n° 5,349,642 ; 5,608,903 ; 5,671,414 ; 5,677,851 ; 5,758,344 ; 5,784,560 ; 5,818,936 ; 5,828,882 ; 5,832,275 ; 5,832,483 ; 5,832,487 ; 5,870,561 ; 5,870,739 ; 5,873,079 ; 5,878,415 ; 5,884,304 ; 5,919,257 ; 5,933,503 ; 5,933,826 ; 5,946,467 ; 5,956,718 ; 6,016,499 ; 6,065,017 ; 6,105,062 ; 6,105,132 ; 6,108,649 ; 6,167,393 ; 6,286,010 ; 6,308,181 ; 6,345,266 ; 6,424,976 ; 6,516,325 ; 6,519,610 ; 6,539,381 ; 6,578,035 ; 6,615,350 ; 6,629,132. Brevets en cours d'homologation.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
États-Unis

www.novell.com

Guide d'administration de Novell Nsure Identity Manager 2
30 juin 2004

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

Marques commerciales de Novell

ConsoleOne est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
DirXML est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
eDirectory est une marque de Novell, Inc.
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.
Nsure est une marque de Novell, Inc.
SUSE est une marque déposée de SUSE LINUX AG, une société Novell.

Autres marques commerciales

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

Table des matières

À propos de ce guide

Novell® Nsure Identity Manager 2, anciennement DirXML®, est un service de partage des données et de synchronisation qui permet à des applications, répertoires et bases de données de partager des informations. Il relie des informations dispersées et permet d'établir des règles 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 Single Sign-on, 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 décrit les fonctions d'installation, d'administration et de configuration.

Documentation supplémentaire

Pour plus d'informations sur l'utilisation des pilotes DirXML, reportez-vous au site Web de documentation d'Identity Manager (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

Mises à jour de la documentation

Vous trouverez la version la plus récente de ce document sur le site Web de documentation d'Identity Manager (http://www.novell.com/documentation/fr-fr/dirxml20/index.html).

Conventions utilisées dans la documentation

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.

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

Commentaires de l'utilisateur

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

1 Présentation

Primé par l'industrie, Novell® Nsure™ Identity Manager 2, anciennement DirXML®, est une solution de partage de données et de synchronisation qui révolutionne la gestion des données. Ce service utilise votre système de protection des identités pour synchroniser, transformer et distribuer des informations entre différentes applications ou bases de données, ou encore entre différents répertoires.

Lorsque les données d'un système sont modifiées, le moteur DirXML détecte et diffuse ces modifications aux autres entités connectées sur la base des règles définies. Cette solution permet d'extraire des éléments de données spécifiques de sources de données expertes (par exemple, une application HR peut gérer l'ID d'un utilisateur alors qu'un système de messagerie peut contenir des informations sur le compte de messagerie d'un utilisateur).

Identity Manager permet à une application (comme SAP*, PeopleSoft*, Lotus Notes*, Microsoft* Exchange, Active Directory*, etc.) de :

- partager des données avec le système de protection des identités (Novell eDirectory™) ;
- synchroniser et transformer des données partagées avec le système de protection des identités lors de leur modification dans la base de données de l'application ;
- synchroniser et transformer des données partagées avec la base de données de l'application lors de leur modification dans le système de protection des identités.

Pour cela, Identity Manager contient un cadre bidirectionnel qui permet aux administrateurs de spécifier les données qui seront transmises du système de protection des identités vers l'application et de l'application vers le système de protection des identités. Ce cadre utilise XML pour offrir des fonctions qui permettent la conversion des données et événements du système de protection des identités au format d'application spécifié. Il convertit également des formats d'application compréhensibles par le système de protection des identités. Toutes les interactions avec l'application se font grâce à son API native.

Identity Manager permet de ne sélectionner que les attributs et classes eDirectory relatifs aux enregistrements et champs correspondants de l'application. Par exemple, une base de données eDirectory peut partager des objets Utilisateur avec une base de données Ressources humaines mais pas les objets Ressource réseau tels que les serveurs, les imprimantes et les volumes. La base de données Ressources humaines peut, quant à elle, partager les prénoms, noms, initiales, numéros de téléphone et emplacements de travail des utilisateurs avec eDirectory, mais pas leurs informations personnelles, ni leurs antécédents professionnels.

Si les données que vous souhaitez partager avec d'autres applications n'ont pas de classe ou d'attribut dans eDirectory, vous pouvez étendre le schéma eDirectory afin de les inclure. Dans ce cas, eDirectory devient un référentiel d'informations dont il n'a pas besoin, mais que d'autres applications peuvent utiliser. La base de données spécifique à l'application gère le référentiel à l'aide des informations requises uniquement par l'application.

Identity Manager :

- utilise des événements pour capturer les modifications apportées au système de protection des identités ;
- centralise ou distribue la gestion des données, en jouant le rôle d'un hub chargé de rassembler toutes les données ;
- fournit des données du répertoire au format XML, ce qui permet de les utiliser et de les partager dans des applications XML ou des applications intégrées via Identity Manager ;
- contrôle le flux de données à l'aide de filtres spécifiques qui régissent les éléments de données définis dans le système ;
- met en œuvre de sources de données expertes via l'utilisation d'autorisations et de filtres ;
- applique des règles aux données d'annuaire au format XML, régissent l'interprétation et la transformation des données lorsque des modifications transitent par Identity Manager ;
- transforme des données XML en pratiquement tous les formats de données, ce qui permet à Identity Manager de partager des données avec n'importe quel type d'application ;
- gère des associations entre des objets du système de protection des identités et des objets des autres systèmes intégrés, afin de garantir que les modifications de données sont reflétées de façon appropriée sur tous les systèmes intégrés.

Avec Identity Manager, votre entreprise peut simplifier les procédures de gestion des ressources humaines, réduire les coûts de gestion des données, établir des relations client via un service personnalisé performant et supprimer les barrières d'interopérabilité qui entravent le succès. Voici quelques exemples d'activités qu'Identity Manager permet de mener à bien :

Activité	Solution Identity Manager
Gestion des comptes utilisateur	En une seule opération : Identity Manager autorise ou supprime presque instantanément l'accès d'un employé aux ressources. Identity Manager contient une fonction de provisioning employé automatique, qui permet aux nouveaux employés d'accéder au réseau, à la messagerie électronique, aux applications, aux ressources, etc. Identity Manager peut également limiter ou désactiver l'accès lorsqu'un employé quitte l'entreprise.
Suivi et intégration des biens	Identity Manager peut ajouter à eDirectory des profils pour tous les biens (ordinateurs, moniteurs, téléphones, ressources de bibliothèques, chaises, bureaux, etc.) et les intégrer aux profils utilisateur (personnes, services ou organisations, par exemple).
Automatisation des annuaires pages blanches/pages jaunes	Identity Manager peut créer des annuaires unifiés comportant différents niveaux d'informations à usage interne et externe. Les annuaires externes ne peuvent contenir que des adresses électroniques ; les annuaires internes peuvent inclure notamment le lieu de travail, le numéro de téléphone, le numéro de télécopie, le numéro de téléphone portable, l'adresse du domicile.

Activité	Solution Identity Manager
Optimisation des profils utilisateur	Identity Manager permet d'optimiser les profils utilisateur, grâce à l'ajout ou à la synchronisation d'informations telles que l'adresse électronique, le numéro de téléphone, l'adresse personnelle, les préférences, les rapports hiérarchiques, les biens matériels, les téléphones, les clés, les articles de stock, entre autres.
Unification de l'accès aux communications	Identity Manager simplifie l'accès au réseau, au téléphone, à l'alphapage, à Internet, aux équipements sans fil, tant pour les personnes que pour les groupes, grâce à la synchronisation des différents annuaires avec une interface commune de gestion.
Renforcement des relations avec les partenaires	Identity Manager renforce les partenariats en créant des profils (employé, client, etc.) au sein de systèmes de partenaires situés hors du dispositif de firewall, pour permettre aux partenaires d'offrir un service immédiat en cas de besoin.
Amélioration de la chaîne d'approvisionnement	Identity Manager permet d'améliorer les services client en reconnaissant et en consolidant des instances de comptes client multiples.
Fidélisation des clients	Identity Manager offre de nouveaux services qui prennent en compte les besoins des clients et qui résultent d'un affichage global de données autrefois isolées.
Personnalisation des services	Identity Manager offre aux utilisateurs (employés, clients, partenaires, etc.) des profils qui incluent des informations synchronisées sur les relations, les états et les services. Ces profils peuvent être utilisés pour fournir différents niveaux d'accès aux services et aux informations et pour offrir des services en temps réel, personnalisés en fonction des clients.

Nouveautées d'Identity Manager 2

Cette section contient les informations suivantes :

Interface du Générateur de règles et script DirXML pour la création de règles

Dans les versions précédentes de DirXML, les règles utilisées dans une configuration de pilote étaient appelées objets Règle et objets Feuille de style. Dans Identity Manager 2, chaque composant de la configuration de pilote est appelé objet Règle, ces règles contenant des principes.

Pour les tâches communes, vous pouvez désormais utiliser la nouvelle interface du Générateur de règles pour créer des règles pour vos pilotes sans devoir écrire le code XSLT. Le Générateur de règles permet de configurer jusqu'à vingt-cinq des règles les plus fréquentes qui utilisent le nouveau script DirXML. Pour plus d'informations, reportez-vous à la section « Création de règles », page 99.

Cette version contient une fonctionnalité étendue du Générateur de règles avec de nouvelles conditions, opérations et valeurs. Le Générateur de règles comporte désormais un Presse-papiers intégré, la capacité d'importer, d'exporter et de référencer des règles XML ainsi que plusieurs autres nouvelles fonctionnalités. Reportez-vous au *Guide de personnalisation des pilotes et du générateur de règles* (http://www.novell.com/documentation/dirxml20/policies/data/front.html#bktitle).

Gestion des mots de passe

Identity Manager 2 inclut des fonctionnalités nouvelles et des fonctionnalités améliorées de gestion des mots de passe.

- Les nouvelles règles de mots de passe permettent de créer des règles pour les mots de passe et de les assigner à des utilisateurs, à des conteneurs ou à toute l'arborescence eDirectory. Vous pouvez activer le mot de passe universel, qui permet de spécifier des critères détaillés pour les mots de passe et autorise des caractères spéciaux.
- La synchronisation des mots de passe d'Identity Manager est désormais multiplates-formes ; elle permet de mettre en œuvre vos règles de mots de passe sur des systèmes connectés. De nouveaux modèles de notification permettent d'envoyer automatiquement des messages aux utilisateurs sur le statut de synchronisation de leur mot de passe.
- Les règles de mot de passe permettent de fournir un libre-service Mot de passe oublié et un libre-service Réinitialiser mot de passe à vos utilisateurs. Ces nouvelles fonctionnalités aident à réduire les appels au service d'assistance. Des modèles de notification sont également inclus pour l'envoi automatique de mots de passe oubliés et de messages d'optimisation du mot de passe aux utilisateurs.

Pour plus d'informations, reportez-vous au Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101 et au Chapitre 9, « Synchronisation de mot de passe sur des systèmes connectés », page 165.

Droits basés sur le rôle

Les droits basés sur le rôle permettent d'accorder des droits sur des systèmes connectés à un groupe d'utilisateurs de Novell eDirectory. Avec les règles de droits, vous pouvez rationaliser la gestion des règles dans votre entreprise et réduire la nécessité de configurer vos pilotes DirXML.

Les droits basés sur le rôle sont une autre façon d'administrer Identity Manager. Vous pouvez choisir de les utiliser si vous préférez un modèle centralisé d'administration d'Identity Manager.

Une règle de droits est un objet Groupe eDirectory dynamique, avec des fonctions supplémentaires pour les systèmes connectés. Lorsque vous créez une règle de droits, vous définissez les membres de la règle et les droits qui doivent leur être accordés.

Les droits basés sur le rôle permettent d'accorder des droits sur des systèmes connectés et des droits dans eDirectory. Les droits sur les systèmes connectés peuvent être les suivants :

- Comptes
- Appartenance aux listes de distribution de courrier électronique
- Appartenance au groupe
- Attributs pour les objets correspondants des systèmes connectés, peuplés avec les valeurs que vous spécifiez
- D'autres droits sur des systèmes connectés que vous personnalisez

La fonctionnalité des droits basés sur le rôle reposant sur Identity Manager, les pilotes DirXML doivent être installés et configurés correctement pour que vous puissiez gérer des systèmes connectés. En outre, pour éviter des conflits possibles entre les assignations de règles de droits et les configurations des pilotes DirXML, vous devez connaître vos règles d'entreprise et la façon dont elles sont gérées via Identity Manager.

Création de rapport et notification avec Novell Nsure Audit

Avec Identity Manager 2, vous pouvez désormais utiliser Novell Nsure Audit pour des services de création de rapport et de notification. Novell Nsure Audit est un service d'audit multiplates-formes centralisé. Il collecte des données d'événements à partir de plusieurs applications et plates-formes et écrit ces données sur une banque de données unique, non reniable. Nsure Audit peut aussi créer des banques de données filtrées. En fonction des critères que vous définissez, Nsure Audit saisit des types spécifiques d'événements et écrit ces événements sur des banques de données secondaires.

Les composants Nsure Audit ont été mis à jour vers la version 1.0.2. Cette version fournit des champs d'événements supplémentaires qui permettent de consulter et de générer des rapports, ainsi qu'un champ de données étendu pouvant contenir de gros documents XML. Pour plus d'informations, reportez-vous au Chapitre 13, « Consignation et création de rapports avec Nsure Audit », page 291.

Le service de création de rapport et de notification (RNS - Reporting and Notification Service) est désapprouvé, mais le moteur continue à traiter les fonctions RNS si vous utilisez effectivement RNS. Envisagez de passer à Nsure Audit ; ce système étend en effet la fonctionnalité fournie par RNS. De plus, RNS pourrait ne plus être pris en charge dans une version future d'Identity Manager. Pour plus d'informations sur la documentation RNS, reportez-vous au *Guide d'administration de DirXML 1.1a* (http://www.novell.com/documentation/fr-fr/dirxml11a/dirxml/data/afae8bz.html).

Valeurs de configuration globales

Les valeurs de configuration globales (GCV) sont de nouveaux paramètres similaires aux paramètres du pilote. Elles peuvent être spécifiées tant pour un ensemble de pilotes que pour un pilote individuel. Si un pilote n'a pas de valeur pour une GCV donnée, le pilote hérite de la valeur, pour cette GCV, de l'ensemble de pilotes.

Les GCV permettent de spécifier des paramètres pour les nouvelles fonctions, telles que la synchronisation des mots de passe, ainsi que des paramètres spécifiques à la fonction d'une configuration de pilote individuelle. Certaines GCV sont fournies avec les pilotes, mais vous pouvez aussi ajouter les vôtres. Vous pouvez faire référence à ces valeurs dans une règle pour vous aider à personnaliser votre configuration de pilote.

Pour plus d'informations, reportez-vous à la section « Utilisation de valeurs de configuration globales », page 84.

Pulsation pilote

Le moteur DirXML accepte désormais des documents de pulsation pilote et les pilotes peuvent être configurés pour les envoyer.

Pour plus d'informations, reportez-vous à la section « Ajout de la pulsation du pilote », page 96.

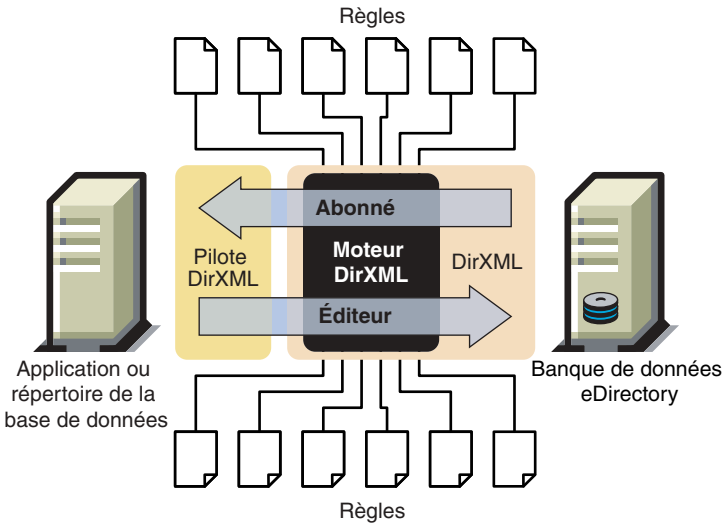
Invite flexible lors de l'importation des configurations de pilote

Plusieurs exemples de configuration de pilote utilisent une nouvelle fonctionnalité - l'invite flexible - pour diminuer la complexité lors de l'importation de la configuration. Par exemple, une seule invite peut être fournie dans l'écran d'importation initial pour utiliser ou non une fonction, comme le chargeur distant ou des droits basés sur le rôle. Si vous choisissez oui, une autre page d'invites d'importation peut s'afficher dans l'assistant qui permet de fournir d'autres informations pour ces fonctionnalités.

Compréhension de l'architecture d'Identity Manager

La technologie d'Identity Manager compte plusieurs composants différents. Son principal objectif est de permettre un échange de données satisfaisant entre le système de protection des identités et une application, un répertoire ou une base de données. Pour cela, Identity Manager dispose d'une interface bien conçue qui convertit les données et les événements d'annuaire au format XML. Cette interface permet d'obtenir un flux bidirectionnel des données de et vers eDirectory.

L’illustration ci-dessous présente les composants de base d’Identity Manager ainsi que les relations qui existent entre eux.



Le moteur DirXML constitue le module clé de l’architecture d’Identity Manager. Il contient l’interface qui permet aux pilotes DirXML de synchroniser les informations avec eDirectory, ce qui permet à des systèmes de données disparates de se connecter et de partager des données.

Le moteur DirXML fournit les données et les événements eDirectory au format XML. Il utilise un processeur de règles et un moteur de transformation de données pour manipuler les données lorsqu’elles évoluent entre deux systèmes.

Lors de son initialisation, eDirectory :

1. lit le filtre pour tous les pilotes DirXML ;
2. enregistre les pilotes pour les événements eDirectory appropriés ;
3. filtre les données conformément aux spécifications de chaque pilote ;
4. configure un cache pour les événements eDirectory acheminés vers chaque pilote.

Une fois qu’un événement a été mis en cache, le pilote qui possède ce cache lit l’événement.

Le pilote reçoit alors des données eDirectory au format eDirectory natif, les convertit au format XDS (le vocabulaire XML utilisé par Identity Manager et pouvant être transformé par une règle), puis envoie l’événement au moteur DirXML. Le moteur lit toutes les règles configurées pour votre pilote d’application (règles d’assignation, de concordance, de placement, de création, de transformation et feuilles de style), puis crée des données au format XML en fonction de ces règles. Il envoie ensuite ces données à votre pilote d’application. Il envoie également les données à l’application et surveille leur mise à jour jusqu’à ce qu’il reçoive un code indiquant le succès et la fin de l’opération.

La partie Éditeur du pilote rassemble et envoie les mises à jour de la base de données d’application externe vers le système de protection des identités. Une fois le pilote d’application informé des modifications apportées aux informations partagées par les deux bases de données, il rassemble ces informations, puis s’assure qu’elles ont été filtrées correctement. Il convertit ensuite les données au format DirXML et les envoie au moteur.

Moteur DirXML

Le moteur DirXML (parfois appelé moteur de jointure) peut être subdivisé en deux composants : l'interface NDS® et le moteur de jointure.

Interface NDS

L'interface NDS (intégrée au moteur DirXML) est utilisée pour la détection d'événements qui se produisent dans eDirectory. Cette interface garantit la transmission d'événements à Identity Manager grâce à l'utilisation du cache d'événements. L'interface NDS prend en charge le chargement de plusieurs pilotes, ce qui signifie qu'une seule instance d'Identity Manager est en cours d'exécution, mais elle peut communiquer avec plusieurs applications. La détection de retour en boucle est intégrée à cette interface afin d'éviter la survenue d'événements de retour en boucle entre eDirectory et l'application. Bien que l'interface contienne un système de protection contre les retours en boucle, les développeurs sont sensibilisés à l'utilisation de la détection des retours en boucle dans les pilotes d'application.

Moteur de jointure

Le moteur de jointure applique les règles au format XML d'Identity Manager (XDS) à chaque événement qui lui est présenté. Les règles Identity Manager peuvent également être au format XSLT (Extensible Stylesheet Language Transformation), ce qui représente un vocabulaire XML plus puissant, défini pour l'utilisation et la transformation de documents XML.

Le moteur de jointure applique chaque type de règle au document source. La capacité à apporter ces modifications constitue l'un des atouts majeurs d'Identity Manager. Les données sont transformées en temps réel lorsqu'elles sont partagées entre eDirectory et les différentes applications.

Module d'interface pilote de DirXML

Le module d'interface pilote de DirXML (souvent appelé le pilote) représente le canal de transmission des informations entre eDirectory et l'application, l'annuaire ou la base de données. Les communications entre le moteur DirXML et le module d'interface pilote sont gérées via des documents XML qui décrivent les événements, les requêtes et les résultats.

Le module d'interface pilote est écrit en Java* ou en C++.

Fichiers de configuration du pilote

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

Ces configurations de pilote contiennent des exemples de règles qu'il convient de modifier avant d'utiliser en environnement de production.

Cache d'événements d'Identity Manager

Tous les événements générés par l'intermédiaire d'eDirectory sont conservés dans un cache d'événements jusqu'à ce qu'ils soient traités avec succès. Aucune donnée ne sera ainsi 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.

Composants d’Identity Manager

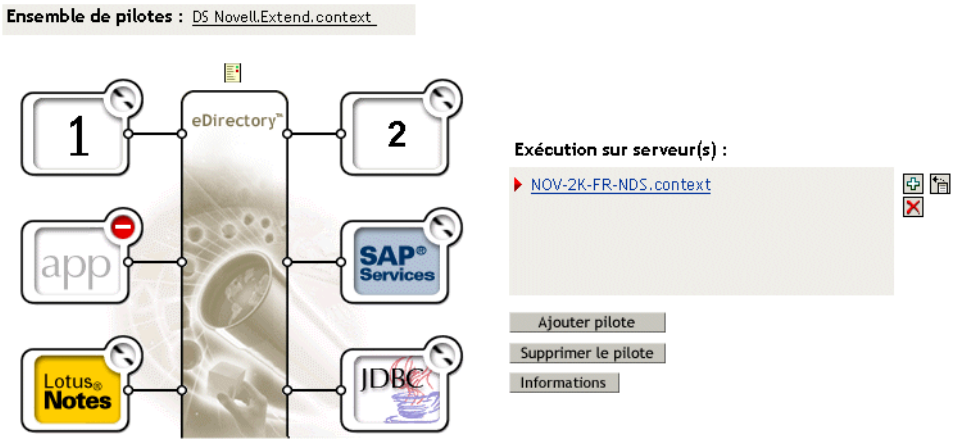
Cette section présente les concepts relatifs à Identity Manager et les différents composants d’Identity Manager.

Ensemble de pilotes

Un ensemble de pilotes est un conteneur qui stocke des pilotes DirXML. Vous ne pouvez activer qu’un seul ensemble de pilotes à la fois sur un serveur. Par conséquent, tous les pilotes actifs doivent être regroupés au sein du même ensemble de pilotes. Il n’est pas nécessaire d’activer tous les pilotes de l’ensemble de pilotes sur chacun des serveurs qui utilisent cet ensemble de pilotes.

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 une partition pour l’ensemble de pilotes. Ainsi, lorsque des répliques d’utilisateurs sont déplacées vers un autre serveur, les objets Pilote ne le sont pas.

La figure suivante illustre un ensemble de pilotes dans iManager.



Dans la page Présentation de iManager (illustrée plus haut), vous pouvez :

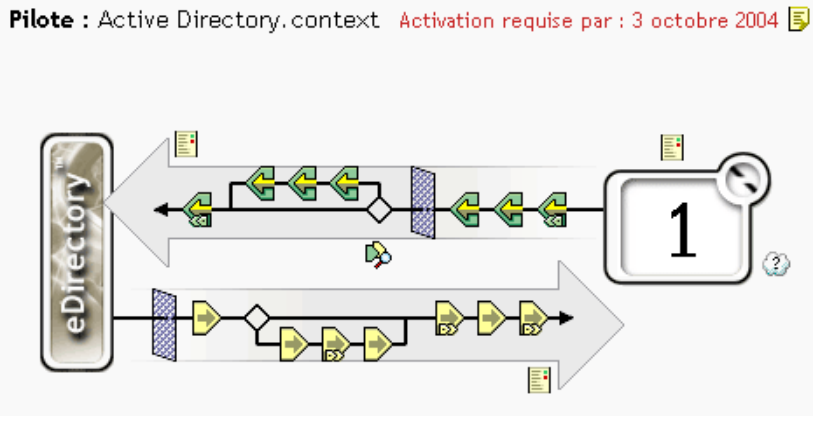
- afficher et modifier l’ensemble de pilotes et de ses propriétés ;
- afficher les pilotes au sein de l’ensemble de pilotes ;
- modifier l’état d’un pilote ;
- associer un ensemble de pilotes à un serveur ;
- ajouter ou supprimer des pilotes ;
- afficher des informations d’activation relatives à l’ensemble de pilotes ;
- afficher le journal d’état de l’ensemble de pilotes.

Objet Pilote

Un objet Pilote représente un pilote qui se connecte à une application s'intégrant à eDirectory. 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 Règles référencés par les objets Pilote, Abonné et Éditeur ;
- un module d'interface pilote exécutable référencé par l'objet Pilote ;
- des paramètres propres au module d'interface pilote configurés par l'administrateur ;
- un mot de passe eDirectory applicable à l'objet Pilote, qui peut être utilisé par le module d'interface pilote pour l'authentification auprès d'une partie distante de ce dernier ;
- des paramètres d'authentification utilisés pour la connexion ou l'authentification auprès de l'application ou de l'annuaire pris en charge ;
- une option de démarrage du pilote qui inclut les éléments suivants :
  - Désactivé : le pilote ne s'exécute pas.
  - Manuel : le démarrage du pilote doit se faire manuellement à l'aide d'iManager.
  - Démarrage auto : le pilote démarre automatiquement en même temps qu'eDirectory.
- une référence à une règle d'assignation de schéma ;
- une représentation XML du schéma de l'application ou de l'annuaire pris en charge. Cela se fait automatiquement via le module d'interface pilote, à partir de l'application ou de l'annuaire.

Dans iManager, vous pouvez afficher Présentation du pilote DirXML et modifier les paramètres, les règles et les feuilles de style de pilote existants. La présentation du pilote DirXML est illustrée ci-dessous.



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 synchronisera, ou des équivalences de sécurité doivent être accordées à l'objet Pilote.

Pour plus d'informations sur les assignations de droits, reportez-vous à la section eDirectory Rights (Droits eDirectory) (http://www.novell.com/documentation/fr-fr/edir87/edir87/data/fbachifb.html) dans le document *Novell eDirectory 8.7.3 Administration Guide (Guide d'administration de Novell eDirectory 8.7.3)*.

Module d'interface pilote

Le module d'interface pilote est utilisé comme canal d'informations entre l'application, le répertoire ou la base de données et eDirectory. Il est écrit en Java, en C ou en C++.

Les communications entre le moteur DirXML et le module d'interface pilote sont gérées via des documents XML qui décrivent les événements, les requêtes et les résultats.

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

- Ajouter (créer)
- Modifier
- Supprimer
- Renommer
- Déplacer

Le module d'interface pilote doit également prendre en charge une fonction d'interrogation définie qui permet à Identity Manager d'interroger l'application, la base de données ou l'annuaire synchronisé.

Lorsqu'un événement se produit dans eDirectory et qu'il nécessite une opération au niveau de l'application ou de l'annuaire synchronisé, Identity Manager crée un document XML qui décrit l'événement eDirectory et le soumet au module d'interface pilote via le canal Abonné.

Lorsqu'un événement se produit dans l'application, la base de données ou l'annuaire synchronisé, le module d'interface pilote génère un document XML qui décrit cet événement. Le module d'interface pilote soumet ensuite le document XML à Identity Manager via le canal Éditeur. Une fois l'événement traité par les règles de l'une des applications, Identity Manager demande à eDirectory d'exécuter les opérations appropriées.

Canaux Éditeur et Abonné

Les pilotes DirXML contiennent deux canaux de traitement des données : le canal Éditeur et le canal Abonné. Chacun de ces canaux contient ses propres règles, qui définissent le traitement et la transformation des données.

Événements et commandes

La distinction entre événements et commandes au sein d'Identity Manager est importante. Si un élément est envoyé à un pilote, il s'agit d'une commande. Si cet élément est envoyé à Identity Manager, il représente une notification d'événement. Lorsque le pilote envoie une notification d'événement à Identity Manager, le pilote signale à Identity Manager qu'une modification a été apportée au sein de l'application. Sur la base des règles configurables, Identity Manager détermine ensuite les éventuelles commandes à envoyer à eDirectory.

Lorsqu'Identity Manager envoie une commande au pilote, Identity Manager a déjà accepté en entrée un événement eDirectory, appliqué les règles appropriées et déterminé que la modification représentée par la commande était nécessaire.

Règles et filtres

Les règles et les filtres permettent de contrôler la façon dont les flux de données transitent entre les systèmes. Pour plus d'informations sur les règles et les filtres, reportez-vous au *Guide de personnalisation des pilotes et du Générateur de règles* (http://www.novell.com/documentation/fr-fr/dirxml20/policies/data/boswupw.html).

Associations

Les produits de gestion des identités requièrent, pour la plupart, que l'application connectée stocke un identificateur afin d'associer les objets d'une application à l'annuaire. Grâce à Identity Manager, aucune modification de l'application n'est requise. Dans eDirectory, chaque objet contient une table d'associations qui assigne à l'objet eDirectory un identificateur unique dans les applications et les annuaires connectés. Cette table est dotée d'un index inversé afin que l'application connectée n'ait pas à fournir d'identificateur eDirectory (tel qu'un nom distinctif) au pilote d'intégration lors de la mise à jour de eDirectory.

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 réseau. Pour qu'une association puisse être créée, les critères minimum définissables de chaque objet doivent correspondre. Par exemple, vous créez une règle indiquant que lorsque deux des quatre attributs sont concordants à plus de 90 % (nom, numéro de téléphone, ID de l'employé et adresse électronique), l'objet est associé.

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

Pour créer des associations, utilisez l'une des deux méthodes suivantes :

- par concordance entre des objets ;
- par la création d'objet à un emplacement spécifique.

Une association créée entre différents objets reste active jusqu'à ce que la suppression des objets ou de l'association par un administrateur eDirectory.

Table d’associations

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 l’installation initiale d’Identity Manager, le schéma eDirectory est étendu sous NetWare® et Windows* NT*/2000. Si vous utilisez Solaris* ou Linux*, ce schéma n’est pas automatiquement 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’associations. Les tables d’associations conservent une trace de tous les objets d’applications externes auxquels un objet eDirectory est lié. Cette table est créée et gérée automatiquement. Par conséquent, la modification manuelle de ces informations est rarement requise, bien qu’il soit souvent utile d’afficher ces informations.

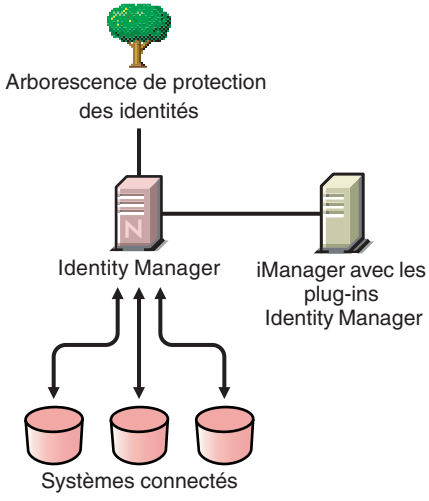
2 Planification

Cette section contient les informations suivantes :

Scénarios d'installation communs

Les scénarios suivants sont des exemples de l'environnement dans lequel Identity Manager peut être utilisé. Pour chaque scénario, des instructions sont fournies pour vous aider avec la mise en œuvre.

Nouvelle installation d'Identity Manager



Nsure™ Identity Manager est une solution de partage des données qui permet à votre système de protection des identités de synchroniser, de transformer et de distribuer automatiquement des informations à des applications, des bases de données et des répertoires.

Votre solution Identity Manager inclut les composants ci-dessous.

Arborescence du système de protection des identités avec Identity Manager

L'arborescence du système de protection des identités contient les données utilisateur ou objet que vous voulez partager ou synchroniser avec d'autres systèmes connectés. Nous vous recommandons d'installer Identity Manager dans sa propre arborescence et de l'utiliser comme votre système de protection des identités.

iManager Server avec les plugs-in Identity Manager

Utilisez Novell® iManager et les plugs-in Identity Manager pour administrer votre solution Identity Manager.

Systèmes connectés

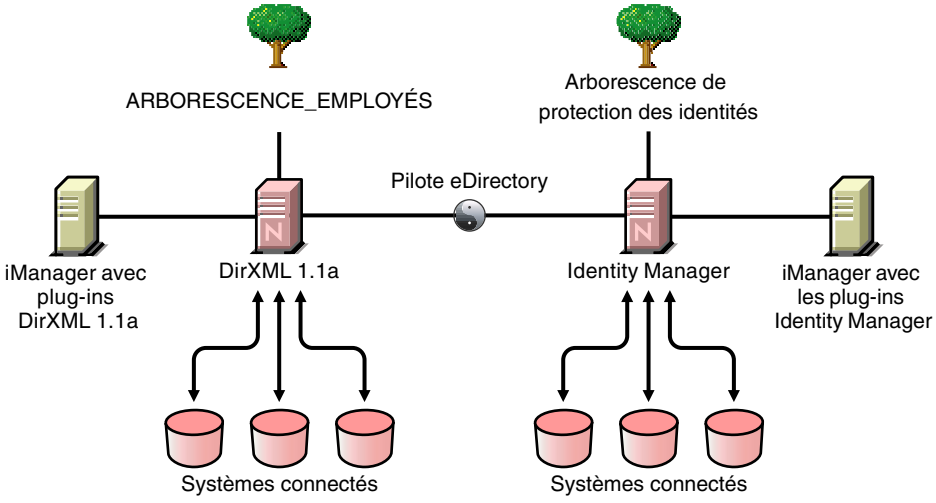
Les systèmes connectés peuvent inclure d'autres applications, répertoires et bases de données, qui devront partager ou synchroniser des données avec votre système de protection des identités. Pour établir une connexion à partir de votre système de protection des identités au système connecté, installez le pilote correspondant à ce système. Pour plus d'informations, reportez-vous aux Guides de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers/index.html).

Tâches communes d'Identity Manager

- **Installation des composants système :** votre solution Identity Manager pouvant être distribuée sur plusieurs ordinateurs, serveurs ou plates-formes, exécutez le programme d'installation pour installer les composants appropriés en fonction du système. Pour plus de détails, reportez-vous à la section « Composants d'Identity Manager et configuration système minimale », page 52.
- **Configuration de systèmes connectés :** pour plus d'informations, reportez-vous à la section « Composants d'Identity Manager et configuration système minimale », page 52 et aux Guides de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers/index.html).
- **Activation de votre solution :** les produits Identity Manager (éditions professionnelles ou serveur et groupes de pilotes) requièrent une activation dans un délai de 90 jours à compter de l'installation. Reportez-vous à l'Annexe A, « Activation des produits Novell Identity Manager », page 305.
- **Définition des règles d'entreprise :** les règles d'entreprise permettent de personnaliser le flux des informations de et vers Novell eDirectory™ pour un environnement donné. Les règles 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. Un guide détaillé de ces règles se trouve dans le *Guide de personnalisation des pilotes et du générateur de règles*.

- **Configuration de la gestion des mots de passe :** avec les règles de mot de passe, vous pouvez accroître la sécurité en définissant des règles pour la création, par les utilisateurs, des mots de passe. Vous pouvez aussi réduire les coûts du service d'assistance en fournissant aux utilisateurs des options de libre-service pour les mots de passe oubliés et pour la réinitialisation des mots de passe. Pour plus d'informations sur la gestion des mots de passe, reportez-vous au Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101.
- **Configuration des droits basés sur le rôle :** les droits basés sur le rôle permettent d'accorder des droits sur des systèmes connectés à un groupe d'utilisateurs de Novell eDirectory. Avec les règles de droits, vous pouvez rationaliser la gestion des règles d'entreprise et réduire la nécessité de configurer vos pilotes DirXML. Pour plus d'informations, reportez-vous au Chapitre 10, « Utilisation des droits basés sur le rôle », page 261.
- **Consignation d'événements avec Nsure Audit :** Nsure Identity Manager est paramétré pour utiliser Novell Nsure Audit à des fins d'audit et de création de rapport. Nsure Audit est un recueil de technologies fournissant des capacités de surveillance, de consignation, de création de rapport et de notification. Grâce à l'intégration avec Nsure Audit, Identity Manager fournit des informations détaillées sur l'état actuel et un historique 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. Reportez-vous au Chapitre 13, « Consignation et création de rapports avec Nsure Audit », page 291.

Utilisation d'Identity Manager et de DirXML 1.1a dans le même environnement



Si vous exécutez Identity Manager et DirXML® 1.1a dans le même environnement, n'oubliez pas les points suivants.

Création d'un système de protection des identités

- Nous vous recommandons d'installer Identity Manager dans sa propre arborescence et de l'utiliser comme système de protection des identités.

Outils de gestion

- ConsoleOne® est pris en charge pour DirXML 1.1a, mais pas pour Identity Manager.
- Deux serveurs iManager sont nécessaires, un pour les plugs-in DirXML 1.1a et un pour les plugs-in Identity Manager. Les plugs-in ont été améliorés et les pilotes Identity Manager utilisent le script DirXML.
- Les plugs-in iManager pour DirXML 1.1a ne peuvent pas lire le script DirXML, qui est utilisé dans les exemples de configuration du pilote pour la plupart des pilotes Identity Manager.

Compatibilité amont

- Vous pouvez exécuter les modules d'interface pilote et les configurations du pilote DirXML 1.1a sur un serveur Identity Manager, mais aussi afficher les pilotes de iManager dans la présentation DirXML de l'ensemble de pilotes. Toutefois, les plugs-in d'Identity Manager ne permettent pas d'afficher ou de modifier les configurations de pilote tant que vous ne les avez pas converties au format Identity Manager.

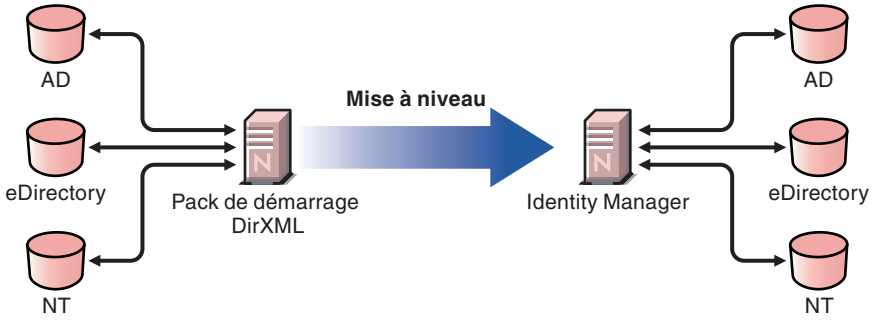
  Dans les plugs-in d'Identity Manager, si vous cliquez sur un pilote au format 1.1a, une invite vous demande de terminer la conversion. Il s'agit un processus simple qui se fait à l'aide d'un assistant et qui ne modifie pas la fonctionnalité de la configuration du pilote. Au cours du processus, une copie de sauvegarde de la version DirXML 1.1a est enregistrée.
- L'activation pour les pilotes DirXML 1.*x* est encore valide lorsque vous les exécutez avec le moteur Identity Manager. Toutefois, si vous mettez à niveau le module d'interface pilote vers une version Identity Manager, vous avez besoin d'une nouvelle activation.
- Dans la plupart des cas, un module d'interface pilote Identity Manager peut exécuter une configuration DirXML 1.1a. Pour plus d'informations sur la mise à niveau, reportez-vous aux Guides de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers/index.html).

  Il existe cependant une exception notable : la version 1.0 de la synchronisation des mots de passe ne s'exécute pas correctement pour AD et NT après la mise à niveau du module d'interface pilote, sauf si vous ajoutez des règles de pilote. Pour plus d'informations, reportez-vous aux sections sur la synchronisation des mots de passe dans les Guides de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers/index.html) des pilotes DirXML pour Active Directory et NT Domain.
- L'exécution des configurations de pilote et des modules d'interface pilote Identity Manager avec le moteur DirXML 1.1a n'est pas prise en charge.
- L'exécution des configurations de pilote Identity Manager avec les modules d'interface pilote du moteur DirXML 1.1a n'est pas prise en charge.
- Si vous exécutez la même configuration du pilote DirXML sur plusieurs serveurs, vérifiez que les serveurs exécutent la même version de DirXML ou d'Identity Manager et d'eDirectory.

Gestion des mots de passe

- Vous pouvez créer des règles de mots de passe qui fournissent des fonctionnalités telles que des règles de mot de passe avancées pour exiger des mots de passe plus résistants, ainsi que le libre-service mot de passe oublié et la réinitialisation du mot de passe pour les utilisateurs. Reportez-vous au Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101 et au Chapitre 8, « Mot de passe en livre service », page 125.
- Si vous avez commencé à utiliser le mot de passe universel avec la version initiale de NetWare 6.5, une mise à niveau est nécessaire avant que vous ne puissiez utiliser les nouvelles fonctionnalités de règles de mot de passe. Reportez-vous à la section « (NetWare 6.5 uniquement) Nouvelle création des assignations du mot de passe universel », page 117. La procédure est inutile si vous avez commencé à utiliser le mot de passe universel avec NetWare 6.5 SP2.
- La synchronisation des mots de passe fournie avec Identity Manager fournit une synchronisation bidirectionnelle des mots de passe et prend en charge plus de plates-formes que la version 1.0 de la synchronisation des mots de passe.
- Si vous utilisez la version 1.0 de la synchronisation des mots de passe avec AD ou NT, n'oubliez pas de suivre les instructions de mise à niveau avant d'installer les nouveaux modules d'interface pilote. Reportez-vous à la section « Mise à niveau de la version 1.0 de la synchronisation des mots de passe vers la synchronisation des mots de passe sous Identity Manager », page 33.
- Des support packs intégrés pour les règles de pilotes sont fournis pour vous aider à ajouter aux pilotes existants la fonctionnalité de synchronisation bidirectionnelle des mots de passe. Reportez-vous à la section « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.

Mise à niveau du pack de démarrage vers Identity Manager



Les solutions de pack de démarrage DirXML incluses avec d'autres produits Novell fournissent une synchronisation sous licence des informations contenues dans NT Domain, Active Directory et eDirectory. En outre, les pilotes d'évaluation pour plusieurs autres systèmes, dont PeopleSoft*, GroupWise® et Lotus Notes*, sont inclus pour permettre d'explorer la synchronisation des données pour vos autres systèmes.

Cette solution permet aussi de synchroniser les mots de passe utilisateur. Avec PasswordSync, un utilisateur ne doit se souvenir que d'un seul mot de passe pour se connecter à un de ces systèmes. Les administrateurs peuvent gérer les mots de passe dans le système de leur choix. Chaque fois qu'un mot de passe est modifié dans un de ces environnements, il sera mis à jour dans tous les autres.

Les packs de démarrage DirXML livrés avec NetWare 6.5 et Nterprise Linux Services 1.0 reposaient sur la technologie DirXML 1.1a. Lorsque vous mettez à niveau d'un pack de démarrage vers la version la plus récente d'Identity Manager, tenez compte des éléments suivants.

Outils de gestion

- ConsoleOne est pris en charge pour DirXML 1.1a, mais pas pour Identity Manager.

Compatibilité amont

- Vous pouvez exécuter les modules d'interface pilote et les configurations du pilote DirXML 1.1a sur un serveur Identity Manager, mais aussi afficher les pilotes de iManager dans la présentation DirXML de l'ensemble de pilotes. Toutefois, les plugs-in d'Identity Manager ne permettent pas d'afficher ou de modifier les configurations de pilote tant que vous ne les avez pas converties au format Identity Manager.

  Dans les plugs-in d'Identity Manager, si vous cliquez sur un pilote au format 1.1a, une invite vous demande de terminer la conversion. Il s'agit un processus simple qui se fait à l'aide d'un assistant et qui ne modifie pas la fonctionnalité de la configuration du pilote. Au cours du processus, une copie de sauvegarde de la version DirXML 1.1a est enregistrée.

- L'activation pour les pilotes DirXML 1.*x* est encore valide lorsque vous les exécutez avec le moteur Identity Manager. Toutefois, si vous mettez à niveau le module d'interface pilote vers une version Identity Manager, vous avez besoin d'une nouvelle activation.

- Dans la plupart des cas, un module d'interface pilote Identity Manager peut exécuter une configuration DirXML 1.1a. Pour plus d'informations sur la mise à niveau, reportez-vous aux Guides de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers/index.html).

  Il existe cependant une exception notable : la version 1.0 de la synchronisation des mots de passe ne s'exécute pas correctement pour AD et NT après la mise à niveau du module d'interface pilote, sauf si vous ajoutez des règles de pilote. Pour plus d'informations, reportez-vous aux sections sur la synchronisation des mots de passe dans les Guides de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers/index.html) des pilotes DirXML pour Active Directory et NT Domain.

- L'exécution des configurations de pilote et des modules d'interface pilote Identity Manager avec le moteur DirXML 1.1a n'est pas prise en charge.

- L'exécution des configurations de pilote Identity Manager avec les modules d'interface pilote du moteur DirXML 1.1a n'est pas prise en charge.

- Si vous exécutez la même configuration du pilote DirXML sur plusieurs serveurs, vérifiez que les serveurs exécutent la même version de DirXML ou d'Identity Manager et d'eDirectory.

Gestion des mots de passe

- La version 1.0 de la synchronisation des mots de passe, livrée avec les packs de démarrage (DirXML 1.1a), ne s'exécute pas correctement pour AD et NT après la mise à niveau du module d'interface pilote, sauf si vous ajoutez des règles de pilotes. Pour plus d'informations, reportez-vous aux sections sur la synchronisation des mots de passe dans les Guides de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers/index.html) des pilotes DirXML pour Active Directory et NT Domain.

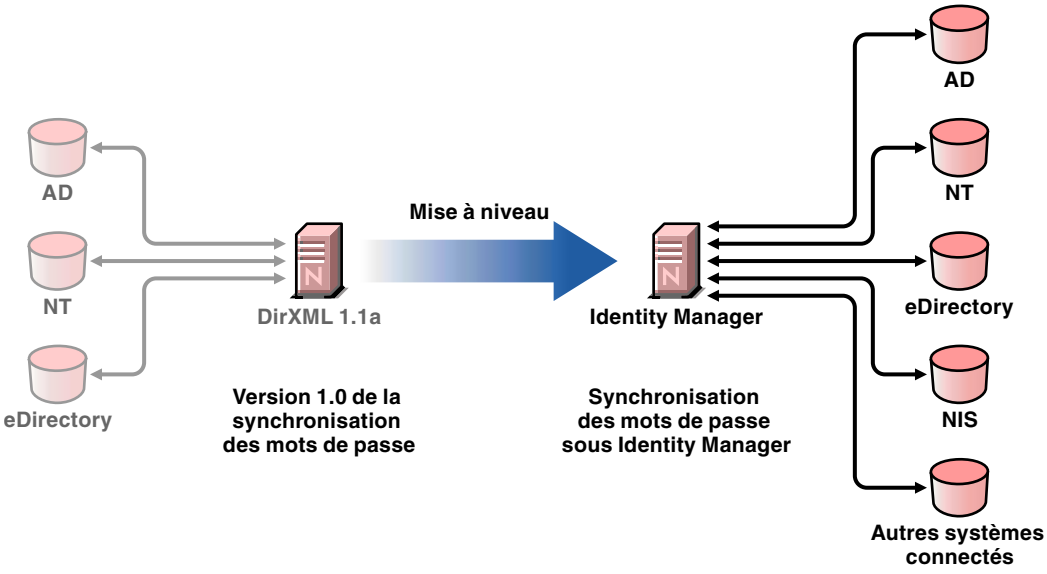
- Pour plus d'informations sur ce processus de mise à niveau, reportez-vous à la section « Mise à niveau de la version 1.0 de la synchronisation des mots de passe vers la synchronisation des mots de passe sous Identity Manager », page 33.

Activation

- Tous les produits Identity Manager et DirXML doivent être activés dans un délai de 90 jours. Lorsque vous avez acheté d'autres logiciels Novell, le pack de démarrage DirXML incluait des activations pour le moteur DirXML 1.1a et les pilotes NT, AD et eDirectory. Lorsque vous mettez à niveau à partir du pack de démarrage DirXML, vous devrez peut-être appliquer vos références d'activation pour ces pilotes.

  Pour plus d'informations sur l'activation, reportez-vous à l'Annexe A, « Activation des produits Novell Identity Manager », page 305.

Mise à niveau de la version 1.0 de la synchronisation des mots de passe vers la synchronisation des mots de passe sous Identity Manager



La synchronisation des mots de passe d'Identity Manager offre de nombreuses fonctionnalités nouvelles, y compris la synchronisation bidirectionnelle des mots de passe, des plates-formes supplémentaires et la notification par courrier électronique lorsque la synchronisation des mots de passe à échoué.

Si vous utilisez la version 1.0 de la synchronisation des mots de passe avec Active Directory ou NT Domain, il est très important de suivre les instructions de mise à niveau avant d'installer les nouveaux modules d'interface pilote.

Pour plus d'informations sur la synchronisation des mots de passe sous Identity Manager, reportez-vous au Chapitre 9, « Synchronisation de mot de passe sur des systèmes connectés », page 165. Cette section contient des informations conceptuelles, y compris une comparaison des anciennes et des nouvelles fonctionnalités, les configurations système requises, une liste des fonctionnalités prises en charge pour chaque système connecté, des instructions sur l'ajout de la prise en charge des pilotes existants et plusieurs scénarios vous montrant comment vous pouvez utiliser les nouvelles fonctionnalités.

Cette section contient les informations suivantes :

- « Mise à niveau de la synchronisation des mots de passe pour AD ou NT », page 34
- « Mise à niveau de la synchronisation des mots de passe pour eDirectory », page 35
- « Mise à niveau des pilotes des autres systèmes connectés », page 35
- « Gestion des informations sensibles », page 35

Mise à niveau de la synchronisation des mots de passe pour AD ou NT

La nouvelle fonctionnalité de synchronisation des mots de passe est effectuée par les règles de pilote, et non par un agent séparé. Ainsi, si vous installez le nouveau module d'interface pilote sans mettre à niveau simultanément la configuration du pilote, la version 1.0 de la synchronisation des mots de passe ne continue à s'exécuter que pour les utilisateurs existants. Les utilisateurs nouveaux, déplacés ou renommés ne participent pas à la synchronisation des mots de passe tant que vous n'avez pas terminé la mise à niveau de la configuration du pilote.

Suivez les étapes générales ci-dessous pour mettre à niveau.

1. Mettez à niveau votre environnement pour qu'il prenne en charge les mots de passe universels, y compris la mise à niveau du client Novell si vous l'utilisez.
2. Installez le module d'interface pilote d'Identity Manager à la place de celui de DirXML 1.*x* pour AD ou NT.
3. Créez immédiatement la compatibilité amont avec la version 1.0 de la synchronisation des mots de passe, en ajoutant une nouvelle règle à la configuration du pilote.

   Cette étape permet à la version 1.0 de la synchronisation des mots de passe de continuer à s'exécuter correctement jusqu'à ce que vous passiez à la synchronisation des mots de passe sous Identity Manager.
4. Ajoutez la prise en charge de la nouvelle version de la synchronisation des mots de passe sous Identity Manager, en utilisant des règles de pilotes.
5. Installez et configurez les nouveaux filtres de synchronisation des mots de passe.
6. Configurez SSL, si nécessaire.
7. Activez le mot de passe universel en utilisant les règles de mot de passe, si nécessaire.
8. Configurez le scénario de synchronisation des mots de passe sous Identity Manager que vous voulez utiliser.

   Reportez-vous à la section Implementing Password Synchronization (Mise en œuvre de la synchronisation des mots de passe) dans le *Novell Nsure Identity Manager 2 Administration Guide (Guide d'administration Novell Nsure Identity Manager 2)*
9. Supprimez la version 1.0 de la synchronisation des mots de passe.

Pour plus d'informations, reportez-vous aux Guides de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers/index.html) des pilotes DirXML pour Active Directory et NT Domain.

Mise à niveau de la synchronisation des mots de passe pour eDirectory

La mise à niveau d'eDirectory est relativement simple. Le nouveau module d'interface pilote doit s'exécuter avec la configuration de votre pilote sans que des modifications soient nécessaires, à condition que vous ayez appliqué les correctifs les plus récents à votre module d'interface pilote et à la configuration. Pour plus d'informations, reportez-vous au Guide de mise en œuvre du pilote DirXML pour eDirectory (http://www.novell.com/documentation/dirxmldrivers/index.html).

Mise à niveau des pilotes des autres systèmes connectés

La synchronisation des mots de passe sous Identity Manager prend en charge plus systèmes connectés que la version 1.0 de la synchronisation des mots de passe.

Pour obtenir la liste des fonctionnalités prises en charge dans d'autres systèmes, reportez-vous à la section « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 175.

Des support packs intégrés pour les règles de pilotes sont fournis pour vous aider à ajouter la fonctionnalité de synchronisation bidirectionnelle des mots de passe aux pilotes existants pour les systèmes connectés non pris en charge au préalable. Reportez-vous à la section « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.

Gestion des informations sensibles

Le mot de passe universel est protégé par quatre couches de codage dans eDirectory ; il est donc très sûr dans cet environnement. Si vous avez choisi d'utiliser la synchronisation bidirectionnelle des mots de passe et si vous synchronisez le mot de passe universel avec le mot de passe de distribution, n'oubliez pas que vous extrayez le mot de passe eDirectory et que vous l'envoyez à d'autres systèmes connectés. Sécurisez le transport du mot de passe, ainsi que les systèmes connectés avec lesquels il est synchronisé. Reportez-vous à la section « Gestion des informations sensibles », page 184.

Planification des aspects de la gestion des projets lors de la mise en œuvre d'Identity Manager

Cette section souligne des aspects importants de la gestion des projets et des règles globales de mise en œuvre d'Identity Manager. Pour plus d'informations sur les aspects techniques, reportez-vous à la section « Planification des aspects technique de la mise en œuvre d'Identity Manager », page 42.

Ce matériel de planification fournit un aperçu des activités généralement effectuées du début d'un projet Identity Manager jusqu'à son déploiement complet en production. Lors de la mise en œuvre d'une stratégie de gestion des identités, trouvez quels sont les besoins et qui sont les participants dans votre environnement, concevoir une solution, obtenir la participation des participants, et tester et déployer la solution. Cette section vise à vous donner les informations nécessaires concernant le processus afin que vous puissiez optimiser les performances d'Identity Manager.

Il est vivement conseillé de faire appel à un expert Identity Manager pour vous assister dans chacune des phases du déploiement. Pour plus d'informations sur les options de partenariat, reportez-vous au site Web de Novell® Nsure™ Solution Partner (http://www.novell.com/solutions/nsure/partners). Novell Education propose également des cours qui concernent la mise en œuvre d'Identity Manager.

Cette section n'est pas exhaustive ; elle ne présente pas toutes les configurations possibles et doit être adaptée aux besoins des clients. Chaque environnement est différent et nécessite une certaine souplesse dans le type d'activités utilisé.

Déploiement de Novell Identity Manager

Plusieurs activités sont conseillées dans le cadre d'un déploiement optimal d'Identity Manager :

- « Découverte », page 36
- « Analyse des besoins et de la conception », page 37
- « Preuve de conception », page 40
- « Validation et préparation des données », page 41
- « Pilote de production », page 41
- « Planification du déploiement vers la production », page 42
- « Déploiement vers la production », page 42

Découverte

Vous pouvez commencer la mise en œuvre d'Identity Manager par un processus de découverte qui :

- identifie les objectifs principaux de la gestion des informations d'identité ;
- définit ou clarifie les objectifs d'entreprise analysés ;
- détermine les initiatives nécessaires pour résoudre les problèmes restants ;
- détermine les ressources nécessaires pour mener une ou plusieurs de ces initiatives ;
- développe une stratégie ou un plan de mise en œuvre de la solution global, ainsi qu'une ligne directive approuvée pour son exécution.

La procédure de découverte offre à tous les participants une vue claire des problèmes et solutions. Elle fournit une excellente base pour la phase d'analyse, qui exige des participants des connaissances de base concernant les annuaires, Novell eDirectory™, Novell NSure Identity Manager et l'intégration XML en général.

- Elle apporte des connaissances de base à tous les participants.
- Elle permet de regrouper les informations clés concernant l'entreprise et les systèmes fournies par chaque participant.
- Elle permet de développer un plan de mise en œuvre de la solution.

La procédure de découverte identifie également les étapes à suivre sans plus attendre, parmi lesquelles :

- l'identification des activités de planification en préparation d'une phase d'évaluation des besoins et de conception ;
- la définition d'une formation complémentaire destinée aux participants.

Éléments clés

- Entrevues structurées avec les professionnels intervenant dans les processus clés de l'entreprise et les techniciens
- Résumé détaillé des problèmes et techniques au sein de l'entreprise
- Recommandations pour les étapes suivantes
- Présentation complète soulignant les résultats de la découverte

Analyse des besoins et de la conception

Cette phase d'analyse capture tous les aspects techniques et commerciaux du projet et crée un modèle de données ainsi qu'une conception détaillée de l'architecture d'Identity Manager. Cette activité essentielle sert de base à la mise en œuvre de la solution.

La conception a pour principal objectif la gestion des informations d'identité ; cependant, de nombreux éléments généralement associés à un annuaire de gestion des ressources, tels que les fichiers et les imprimantes, peuvent également être traités. Voici un exemple des éléments que vous pouvez évaluer :

- Quelles sont les versions de logiciels utilisées ?
- La structure de l'annuaire est-elle adaptée ?
- La qualité des données dans tous les systèmes est-elle suffisante ? Si la qualité des données est insuffisante, la règle d'entreprise risque de ne pas être mise en œuvre comme souhaité.

Après l'analyse des besoins, vous pouvez définir l'étendue et le plan du projet à mettre en œuvre, puis déterminer si des activités préalables doivent être effectuées. Pour éviter des erreurs coûteuses, soyez aussi méticuleux que possible lors de la collecte des informations et de la description des besoins.

Vous pouvez appliquer les tâches suivantes lors de l'évaluation des besoins :

- « Définition des procédures d'entreprise », page 37
- « Analyser vos processus d'entreprise », page 39
- « Conception d'un modèle de données d'entreprise », page 39

Définition des procédures d'entreprise

Collectez les informations relatives aux processus d'entreprise de votre organisation et aux procédures qui les définissent.

Par exemple, une procédure d'entreprise pour supprimer un employé peut définir que les comptes de messagerie et réseau de ce dernier doivent être supprimés ou archivés le jour même de son départ.

Les tâches suivantes peuvent vous aider à définir les procédures d'entreprise :

- Établir les flux de processus, les déclencheurs de processus et les relations d'assignation de données.

  Par exemple, si un événement va survenir dans un processus donné, quelles seront les conséquences de ce processus ? Quels sont les autres processus déclenchés ?

- Assigner des flux de données entre les applications.
- Identifier les transformations de données devant être effectuées d'un format à un autre (par exemple de 2/25/2002 à 25 Fév 2002).
- Décrire les dépendances qui existent entre les données.

  Si une valeur donnée a changé, il est important de savoir s'il existe une dépendance au niveau de cette valeur. Si un processus donné a changé, il est important de savoir s'il existe une dépendance au niveau de ce processus.

  Par exemple, la sélection de la valeur d'état d'employé temporaire dans un système de ressources humaines signifie que le service informatique doit créer, dans eDirectory, un objet Utilisateur doté de droits restreints et d'un accès réseau à certaines heures seulement.

- Lister les priorités.

  Il n'est pas possible de répondre immédiatement à chaque exigence, souhait ou désir de toutes les parties. Les priorités définies pour la conception et le déploiement du système de provisioning vous aideront à planifier la mise en œuvre.

  Il peut s'avérer nécessaire de diviser le déploiement en phases qui permettront de mettre en œuvre une première partie de la solution, puis les autres parties ultérieurement.

- Définir la configuration requise.

  Décrivez la configuration requise pour la mise en œuvre d'une phase donnée du déploiement.

- Identifier les sources de données expertes.

  En identifiant le plus tôt possible les éléments qui relèvent de la responsabilité des administrateurs système et des directeurs, vous pourrez obtenir et maintenir la coopération de chaque partie.

  Par exemple, l'administrateur de comptes peut vouloir la propriété sur l'octroi des droits d'accès à des fichiers et des répertoires spécifiques pour un employé. Pour cela, vous pouvez mettre en œuvre des assignations d'ayants droit locales dans le système de comptes.

Analyser vos processus d'entreprise

L'analyse des processus d'entreprise commence souvent par l'interrogation des personnes clés telles que des directeurs, des administrateurs et des employés qui utilisent effectivement l'application ou le système. Les problèmes à résoudre comprennent les points suivants :

- D'où proviennent les données ?
- Où sont acheminées les données ?
- Qui est responsable des données ?
- Qui est propriétaire de la fonction à laquelle appartiennent les données ?
- Qui faut-il contacter pour modifier les données ?
- Quelles sont les conséquences de la modification des données ?
- Quelles pratiques existent en matière de gestion (collecte et/ou modification) des données ?
- Quels types d'opérations ont lieu ?
- Quelles méthodes sont utilisées pour garantir la qualité et l'intégrité des données ?
- Où résident les systèmes (sur quels serveurs, dans quels services) ?
- Quels processus ne sont pas adaptés à la gestion automatisée ?

Par exemple, les questions ci-après peuvent être posées à l'administrateur d'un système PeopleSoft de gestion des ressources humaines :

- Quelles données sont stockées dans la base PeopleSoft ?
- Quelles informations apparaissent dans les divers volets d'un compte d'employé ?
- Quelles opérations doivent être reflétées sur le système de provisioning (telles qu'ajouts, modifications ou suppressions) ?
- Lesquelles sont obligatoires ? Lesquelles sont facultatives ?
- Quelles opérations doivent être déclenchées en fonction d'opérations effectuées dans PeopleSoft ?
- Quels événements, opérations et actions doivent être ignorés ?

Les entrevues avec les personnes clés peuvent vous conduire vers d'autres parties de l'organisation et permettre d'obtenir une idée plus précise du processus complet.

Conception d'un modèle de données d'entreprise

Une fois vos processus d'entreprise définis, vous pouvez commencer la conception d'un modèle de données qui reflète votre processus d'entreprise actuel.

Le modèle doit indiquer la provenance des données, leur destination ainsi que les déplacements possibles. Il doit également rendre compte de la manière dont les événements critiques affectent le flux de données.

Vous pouvez également développer un diagramme qui reflète le processus d'entreprise proposé et l'avantage de mettre en œuvre une solution de provisioning automatisée dans ce processus.

Pour développer ce modèle, commencez par répondre aux questions suivantes :

- Quels sont les types d'objets (Utilisateurs, Groupes, etc.) déplacés ?
- Quels sont les événements intéressants ?
- Quels attributs doivent être synchronisés ?
- Quelles sont les données stockées dans votre entreprise pour les différents types d'objets gérés ?
- S'agit-il d'une synchronisation unidirectionnelle ou bidirectionnelle ?
- Quel système représente la source experte et pour quels attributs ?

Il est également important de considérer les relations entre différentes valeurs sur les différents systèmes.

Par exemple, un champ d'état d'employé dans PeopleSoft peut avoir trois valeurs définies : employé, contractuel et interne. Cependant, dans le système Active Directory, il ne peut exister que deux valeurs : permanent et temporaire. En l'occurrence, définissez la relation entre l'état contractuel dans PeopleSoft et ces valeurs dans Active Directory.

L'objectif de ce travail est de comprendre chaque système d'annuaire et la manière dont les annuaires sont liés, mais aussi de connaître les objets et les attributs à synchroniser dans ces systèmes.

Éléments clés

- Modèle de données affichant tous les systèmes, les sources de données expertes, les événements, le flux d'informations et les normes de format de données
- Architecture Identity Manager adaptée à la solution
- Conditions détaillées pour la connexion à des systèmes supplémentaires
- Stratégies de validation des données et de concordance des enregistrements
- Conception de l'annuaire pour la prise en charge de l'infrastructure Identity Manager

Dépendances

- Le personnel familier avec les systèmes externes (tels que l'administrateur de la base de données des ressources humaines ou l'administrateur du réseau et du système de messagerie)
- Disponibilité des schémas système et de l'exemple de données
- Modèle de données issu de la phase d'analyse et de conception
- Disponibilité des informations de base telles que l'organigramme de l'organisation, l'infrastructure serveur et WAN

Preuve de conception

L'objectif de cette activité est d'obtenir un exemple de mise en œuvre dans un environnement de test qui reflète la règle d'entreprise et le flux de données de votre société. Elle s'appuie sur la conception du modèle de données développé au cours de l'analyse des besoins et constitue l'étape finale avant d'introduire le pilote dans l'environnement de production.

Remarque : cette étape permet souvent d'améliorer la gestion en prévision de la mise en œuvre finale.

Éléments clés

- Preuve de la conception d'une solution Identity Manager fonctionnant avec toutes les connexions système opérationnelles

Dépendances

- Plate-forme matérielle
- Logiciels requis
- Phase d'analyse et de conception qui identifie les connexions requises
- Disponibilité et accès aux autres systèmes à des fins de test
- Modèle de données issu de la phase d'analyse et de conception

Validation et préparation des données

La qualité et la cohérence des données présentes dans les systèmes de production peuvent varier et entraîner des erreurs lors de la synchronisation des systèmes. Cette phase constitue une séparation nette entre l'équipe de mise en œuvre Nsure Resources et les unités ou groupes au sein de l'entreprise, qui possèdent ou gèrent les données des systèmes à intégrer. Il arrive parfois que les facteurs combinés de risque et de coût n'entrent pas dans le projet de provisioning.

Éléments clés

- Ensembles de données de production adaptés au chargement dans eDirectory (tels qu'identifiés dans les activités d'analyse et de conception). Cela comprend la méthode de chargement (chargement en bloc ou via des connecteurs). Les conditions requises pour les données validées ou formatées sont également identifiées.

Dépendances

- Modèle de données issu de la phase d'analyse et de conception (concordance des enregistrements et stratégie de format des données proposées)
- Accès aux ensembles de données de production

Pilote de production

L'objectif de cette activité est de commencer la migration vers l'environnement de production. Pendant cette phase, des opérations de personnalisation supplémentaires peuvent avoir lieu. Dans cette courte introduction, les résultats des activités précédentes peuvent être confirmés et un accord peut être conclu pour le déploiement vers la production.

Remarque : cette phase peut fournir les critères d'acceptation de la solution et/ou le jalon nécessaire en vue de la pleine production.

Éléments clés

- Solution de pilote qui propose une preuve de conception en direct et une validation du modèle de données et des résultats de processus souhaités

Dépendances

- Toutes les activités précédentes (analyse et conception, plate-forme de technologie Identity Manager).

Planification du déploiement vers la production

Lors de cette phase, le déploiement vers la production est planifié. Le plan doit :

- Confirmer les plates-formes de serveur, les versions logicielles et les service packs
- Confirmer l'environnement général
- Confirmer l'introduction d'eDirectory et la coexistence d'arborescences mixtes
- Confirmer les stratégies de partitionnement et de réplication
- Confirmer la mise en œuvre d'Identity Manager
- Planifier le passage au nouveau processus
- Planifier une stratégie de retour à l'état initial en cas d'incident

Éléments clés

- Plan de déploiement de production
- Plan de passage au nouveau processus
- Plan de secours de retour à l'état initial en cas d'incident

Dépendances

- Toutes les activités précédentes

Déploiement vers la production

Lors de cette phase, la solution de pilote est étendue afin de prendre en compte toutes les données actuelles de l'environnement de production. Elle s'appuie généralement sur le fait que le pilote de production répond à tous les critères techniques et d'entreprise.

Éléments clés

- Solution de production prête pour la transition

Dépendances

- Toutes les activités précédentes

Planification des aspects technique de la mise en œuvre d'Identity Manager

Réplication des objets dont Identity Manager a besoin sur le serveur

Lors de votre planification, vérifiez que certains objets eDirectory sont répliqués sur les serveurs sur lesquels vous voulez exécuter les pilotes DirXML.

Vous pouvez utiliser les répliques filtrées, tant que tous les objets et attributs dont le pilote a besoin pour lire ou synchroniser sont inclus dans les répliques filtrées.

N'oubliez pas que vous devez attribuer à l'objet pilote DirXML des droits eDirectory suffisants sur les objets qu'il doit synchroniser, soit en attribuant explicitement des droits soit en rendant la sécurité de l'objet Pilote équivalente à un objet qui dispose des droits souhaités.

Un serveur eDirectory qui exécute un pilote DirXML (ou auquel le pilote fait référence, si vous utilisez le chargeur distant) doit contenir une réplique principale ou une réplique en lecture/écriture des éléments suivants :

- L'objet Ensemble pilote pour ce serveur.

  Vous devez disposer d'un objet Ensemble de pilotes pour chaque serveur qui exécute Identity Manager. Sauf en cas de besoins spécifiques, n'associez pas plusieurs serveurs au même objet Ensemble de pilotes.

  Remarque : lorsque vous créez un objet Ensemble de pilotes, le paramètre par défaut doit créer une partition séparée, mais cela n'est pas obligatoire.

- L'objet Serveur pour ce serveur.

  L'objet Serveur est nécessaire parce qu'il permet au pilote de générer des paires de clés pour les objets. Il est également important pour l'authentification du chargeur distant.

- Les objets que vous voulez que cette instance du pilote synchronise.

  Le pilote ne peut pas synchroniser d'objet sauf si une réplique de ces objets se trouve sur le même serveur que le pilote. En fait, un pilote DirXML synchronisera les objets dans *tous* les conteneurs répliqués sur le serveur sauf si vous créez des règles indiquant le contraire (règles de filtrage d'étendue).

  Si vous voulez qu'un pilote synchronise, par exemple, tous les objets Utilisateur, la façon la plus simple est d'utiliser une instance du pilote sur un serveur qui contient une réplique principale ou une réplique en lecture/écriture de tous vos utilisateurs.

  Toutefois, dans de nombreux environnements, une réplique de tous les utilisateurs ne se trouve pas sur un seul serveur. L'ensemble complet des utilisateurs est plutôt réparti sur plusieurs serveurs. Dans ce cas, deux choix se présentent :

  - **Des utilisateurs regroupés sur un seul serveur :** vous pouvez créer un seul serveur qui contient tous les utilisateurs en ajoutant des répliques à un serveur existant. Vous pouvez utiliser des répliques filtrées pour réduire si nécessaire la taille de la base de données eDirectory, tant que les objets et les attributs utilisateur nécessaires font partie des répliques filtrées.
  - **Utiliser plusieurs instances du pilote sur plusieurs serveurs, avec le filtrage d'étendue :** si vous ne voulez *pas* regrouper des utilisateurs sur un seul serveur, vous devrez déterminer l'ensemble de serveurs qui contiendra tous les utilisateurs et configurer une instance du pilote DirXML sur chacun de ces serveurs.

    Pour éviter que des instances séparées d'un pilote n'essaient de synchroniser les mêmes utilisateurs, utilisez le filtrage d'étendue pour définir les utilisateurs que chaque instance du pilote synchronisera. Le filtrage d'étendue signifie que vous ajoutez des règles à chaque pilote pour limiter l'étendue de la gestion par le pilote de conteneurs spécifiques. Reportez-vous à la section « Gestion des utilisateurs sur différents serveurs avec le filtrage d'étendue », page 44.

- Les objets Modèle que vous voulez que le pilote utilise lors de la création d'utilisateurs, si vous choisissez d'utiliser des modèles.

  Les pilotes DirXML ne requièrent pas que vous spécifiez des objets Modèle eDirectory pour la création d'utilisateurs. Toutefois, si vous spécifiez qu'un pilote doit utiliser un modèle lors de la création d'utilisateurs dans eDirectory, l'objet Modèle doit être répliqué sur le serveur sur lequel le pilote s'exécute.

- Tout conteneur que vous voulez que le pilote DirXML utilise pour la gestion des utilisateurs.

  Par exemple, si vous avez créé un conteneur nommé Utilisateurs inactifs pour contenir des comptes utilisateur désactivés, vous devez disposer d'une réplique principale ou une réplique en lecture/écriture (de préférence une réplique principale) de ce conteneur sur le serveur sur lequel le pilote s'exécute.

- Tous les autres objets auxquels le pilote a besoin de se référer (par exemple, les objets Ordre de travail pour le pilote Avaya PBX).

  Si les autres objets ne doivent être lus que par le pilote et ne doivent pas être modifiés, la réplique pour ces objets sur le serveur peut être une réplique en lecture seule.

Gestion des utilisateurs sur différents serveurs avec le filtrage d'étendue

Le filtrage d'étendue signifie que vous ajoutez des règles à chaque pilote pour limiter l'étendue des opérations du pilote sur des conteneurs spécifiques. Voici deux situations dans lesquelles vous devrez utiliser le filtrage d'étendue :

- Vous voulez que le pilote ne synchronise que les utilisateurs qui se trouvent dans un conteneur donné.

  Un pilote DirXML par défaut synchronise les objets dans tous les conteneurs répliqués sur le serveur sur lequel il s'exécute. Pour réduire cette étendue, créez des règles de filtrage d'étendue.

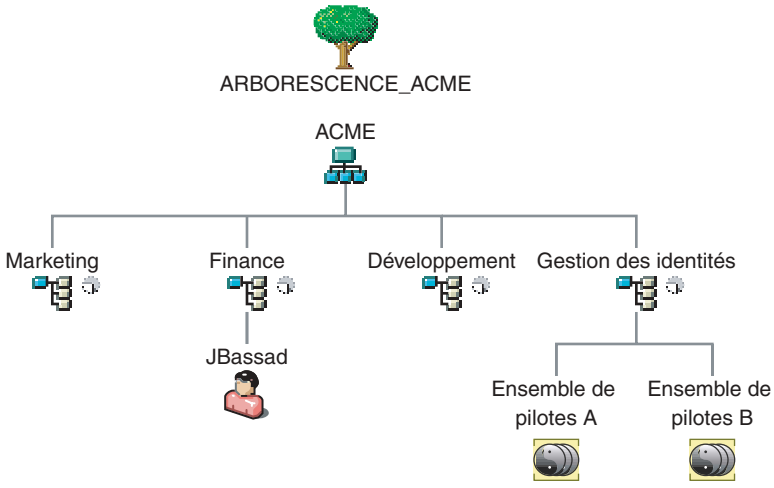
- Vous voulez qu'un pilote DirXML synchronise tous les utilisateurs, mais vous ne voulez pas que tous les utilisateurs soient répliqués sur le même serveur.

  Pour synchroniser tous les utilisateurs sans avoir à les répliquer sur un seul serveur, déterminez l'ensemble de serveurs qui contient tous les utilisateurs, puis créez une instance du pilote DirXML sur chacun de ces serveurs. Pour éviter que deux instances du pilote essaient de synchroniser les mêmes utilisateurs, utilisez le filtrage d'étendue pour définir les utilisateurs que chaque instance du pilote synchronisera.

  Remarque : utilisez le filtrage d'étendue même si les répliques de votre serveur ne se chevauchent pas. Il est possible que des répliques soient ultérieurement ajoutées à vos serveurs et un chevauchement involontairement créé. Si la fonction de filtrage d'étendue est activée, vos pilotes DirXML n'essaieront pas de synchroniser les mêmes utilisateurs, même si des répliques sont plus tard ajoutées à vos serveurs.

Voici un exemple de l'utilisation du filtrage d'étendue.

L'illustration suivante montre une arborescence avec trois conteneurs qui contiennent des utilisateurs : Marketing, Finance et Développement. Elle montre également un conteneur Identity Manager qui contient les ensembles de pilotes. Chacun de ces conteneurs représente une partition distincte.



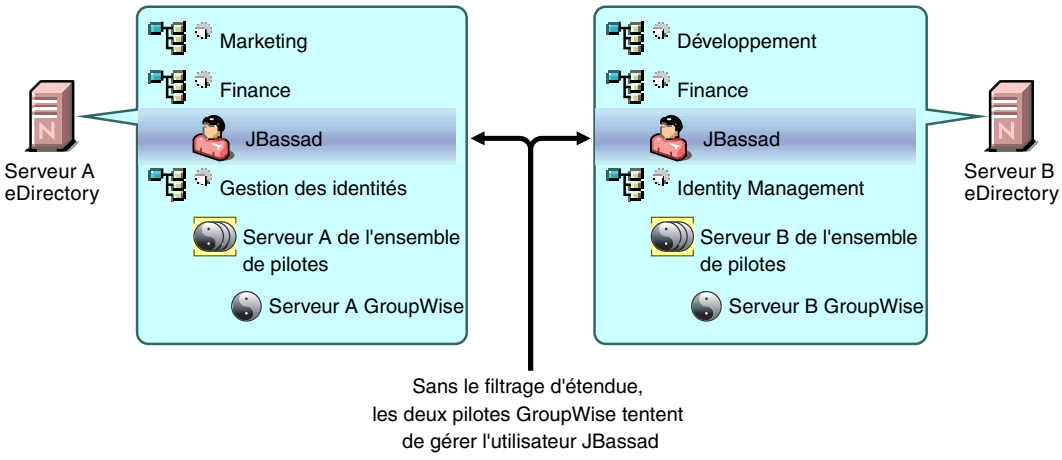
Dans cet exemple, l'administrateur eDirectory dispose de deux serveurs eDirectory, le serveur A et le serveur B, représentés dans l'illustration suivante. Aucun serveur ne contient de copie de tous les utilisateurs. Chaque serveur contient deux des trois partitions ; il y a donc un chevauchement dans l'étendue de ce que les serveurs contiennent.

L'administrateur veut que tous les utilisateurs de l'arborescence soient synchronisés par le pilote GroupWise, mais ne veut pas de répliques regroupés d'utilisateurs sur un seul serveur. Il choisit plutôt d'utiliser deux instances du pilote GroupWise, une sur chaque serveur. Il installe Identity Manager et configure le pilote GroupWise sur chaque serveur eDirectory.

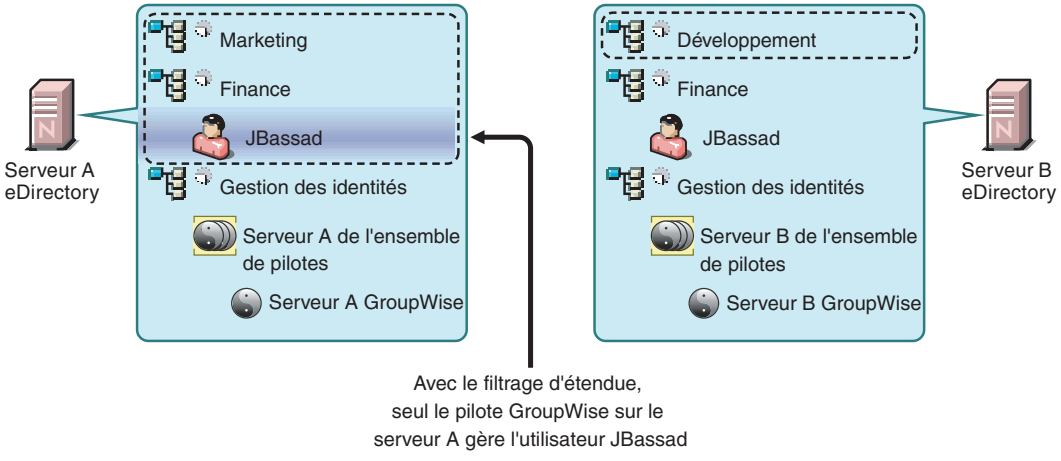
Le serveur A contient des répliques des conteneurs Marketing et Finance. Le serveur comporte également une réplique du conteneur Gestion des identités, qui contient l'ensemble de pilotes du serveur A et l'objet Pilote GroupWise du serveur A.

Le serveur B contient des répliques des conteneurs Développement et Finance ; le conteneur Gestion des identités contient l'ensemble de pilotes du serveur B et l'objet Pilote GroupWise du serveur B.

Le serveur A et le serveur B contiennent tous deux une réplique du conteneur Finance. Les deux serveurs contiennent donc l'utilisateur JBassad, qui se trouve dans le conteneur Finance. Sans filtrage d'étendue, le pilote GroupWise du serveur A et le pilote GroupWise du serveur B synchroniseraient JBassad.



L'illustration suivante montre que le filtrage d'étendue empêche les deux instances du pilote de gérer le même utilisateur ; en effet, il définit quel pilote synchronise chaque conteneur.



Voici un exemple de la manière de créer une règle pour le filtrage d'étendue. Placez la règle dans la feuille de style Transformation d'événement du canal Abonné.

```
<xsl:transform version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
   xmlns:jstring="http://www.novell.com/nxsl/java/java.lang.String"
   exclude-result-prefixes="jstring">

   <!--
   To select different containers for scoping, add/delete/modify the <value>
   elements in the body of the variable "in-scope-containers-rtf"

   Note that if the container is not in the root of the tree, then the DN
   (minus the tree name) of the container must be specified, e.g.,
   Corporate\Executives

   Note: THESE MUST BE ENTERED IN THE TABLE AS ALL UPPERCASE
   -->

   <xsl:variable name="in-scope-containers-rtf">
      <value>CORPORATE\USERS\ACTIVE</value>
      <value>CORPORATE\USERS\INACTIVE</value>
   </xsl:variable>
   <xsl:variable name="in-scope-containers" select="document('')/xsl:transform/
```

```
xsl:variable[@name='in-scope-containers-rtf']/value"/>

   <!--
   "identity" transformation - copies unchanged everything not explicitly
   matched by other templates
   -->

   <xsl:template match="node()|@*">
      <xsl:copy>
         <xsl:apply-templates select="@*|node()"/>
      </xsl:copy>
   </xsl:template>

   <!-- throw away events that are out of scope -->

   <xsl:template match="input/*[@src-dn]">
      <xsl:variable name="in-scope">
         <xsl:call-template name="in-scope"/>
      </xsl:variable>
      <xsl:choose>
         <xsl:when test="$in-scope = '1'">
            <xsl:copy>
               <xsl:apply-templates select="@*|node()"/>
            </xsl:copy>
         </xsl:when>
         <xsl:otherwise>
            <xsl:message>
               <status level="warning">Operation vetoed by Event Transformation
               Rule - out of scope</status>
            </xsl:message>
         </xsl:otherwise>
      </xsl:choose>
   </xsl:template>

   <!--
   check to see if an object is in the scope defined by the variable
   "in-scope-containers"
   -->

   <xsl:template name="in-scope">
      <!-- validate that the container is in scope -->
      <xsl:variable name="src-dn" select="substring-after(substring-after(@src-dn,'\'),'\')"/>
      <xsl:variable name="src-dn-i" select="jstring:lastIndexOf($src-dn,'\')"/>
      <xsl:if test="$src-dn-i != -1">
         <xsl:variable name="src-dn-container" select="jstring:substring($src-dn, 0, $src-dn-
i)"/>

         <!--
         the following test takes advantage of the XPath existential
         quantification semantics:
         basically, if one node in the node-set has a string value that matches
         the string, then the statement is true
         -->

         <xsl:if test="jstring:toUpperCase($src-dn-container) = $in-scope-containers">
            <xsl:value-of select="'1'"/>
         </xsl:if>
      </xsl:if>
   </xsl:template>
</xsl:transform>
```

3 Mise à niveau

Cette section contient les informations suivantes :

Certains scénarios sont décrits à la section « Scénarios d'installation communs », page 27.

Mise à niveau de la synchronisation des mots de passe

Reportez-vous à la section « Mise à niveau de la version 1.0 de la synchronisation des mots de passe vers la synchronisation des mots de passe sous Identity Manager », page 196.

Mise à niveau de RNS vers Nsure Audit

Le service de création de rapport et de notification (RNS - Reporting and Notification Service) est désapprouvé, mais le moteur continue à traiter les fonctions RNS si vous utilisez effectivement RNS. Envisagez de passer à Nsure Audit ; ce système étend en effet la fonctionnalité fournie par RNS. De plus, RNS pourrait ne plus être pris en charge dans une version future d'Identity Manager.

Pour plus d'informations, reportez-vous au Chapitre 13, « Consignation et création de rapports avec Nsure Audit », page 291.

Mise à niveau des configurations de pilote

La mise à niveau des configurations de pilote comporte deux aspects :

- Conversion des règles vers les règles Identity Manager : cette fonction utilise un outil de conversion et n'améliore pas la fonctionnalité du pilote. Les pilotes hérités s'exécutent sans cette conversion, mais elle permet d'afficher la configuration existante du pilote dans les plugs-in DirXML iManager.
- Mise à niveau des règles de pilote pour ajouter une nouvelle fonctionnalité : cette fonction est gérée de façon optimale par un expert Identity Manager.

Reportez-vous aux sections « Mise à niveau de la configuration d'un pilote de DirXML 1.x au format Identity Manager », page 83 et « Gestion des pilotes DirXML 1.x dans un environnement Identity Manager », page 83.

Il est également possible de commencer avec les configurations de pilote Identity Manager et de les personnaliser pour appliquer les mêmes opérations que votre configuration DirXML 1.x.

4 Installation

Cette section contient la configuration requise et des instructions d'installation des pilotes Nsure™ Identity Manager et DirXML®.

Avant l'installation

Avant d'installer Identity Manager, revoyez les informations suivantes :

- « Scénarios d'installation communs », page 27
- Pour plus d'informations sur la planification, reportez-vous aux sections « Planification des aspects de la gestion des projets lors de la mise en œuvre d'Identity Manager », page 35 et « Planification des aspects technique de la mise en œuvre d'Identity Manager », page 42.
- Vérifiez que vous répondez à la configuration système minimale. Reportez-vous à la section « Composants d'Identity Manager et configuration système minimale », page 52.
- Faites une sauvegarde de votre serveur Novell® eDirectory™. Reportez-vous à la documentation Novell pour plus d'informations sur la sauvegarde et la restauration de eDirectory (http://www.novell.com/documentation/fr-fr/edir871/edir871/data/a2n4mb6.html).
- Une installation Identity Manager sur un serveur ne permet de synchroniser que les informations qui se trouvent physiquement dans les répliques de partitions du serveur eDirectory hôte. Cela peut vous obliger à regrouper plusieurs partitions sur un même serveur si vous souhaitez obtenir une vue de l'arborescence entière des données de eDirectory pour une application de synchronisation spécifique. Pour plus d'informations, reportez-vous à la section « Réplication des objets dont Identity Manager a besoin sur le serveur », page 42.
- L'objet Ensemble de pilotes doit exister dans une réplique en lecture/écriture complète sur le serveur sur lequel résident les pilotes.
- Attribuez à l'objet Pilote des droits eDirectory suffisants sur les objets qu'il est chargé de synchroniser ou assignez-lui une équivalence de sécurité avec un objet qui possède les droits souhaités.

Composants d'Identity Manager et configuration système minimale

Nsure Identity Manager contient des composants qui peuvent être installés dans votre environnement sur plusieurs systèmes et plates-formes. En fonction de votre configuration système, vous devrez peut-être exécuter plusieurs fois le programme d'installation d'Identity Manager afin d'installer les composants Identity Manager sur les systèmes appropriés.

Le tableau suivant liste les quatre composants d'installation d'Identity Manager et la configuration requise pour chaque système.

Composant système	Configuration système requise	Notes
Serveur DirXML ◆ Moteur DirXML ◆ Agent Nsure Audit ◆ Pilotes DirXML Service ◆ Pilotes DirXML ◆ Composants NMAS (Novell Modular Authentication Services)	Un des systèmes d'exploitation suivants ◆ NetWare® 6 ou 6.5 avec le dernier Support Pack ◆ Windows NT*, 2000 ou 2003 avec le dernier Service Pack ◆ Linux Red Hat* AS ou ES 2.1 ◆ SUSE® LINUX Enterprise Server 8 ◆ Solaris 8 ou 9 ◆ AIX 5.2L Une des versions suivantes d'eDirectory ◆ eDirectory 8.6.2 avec le dernier Support Pack ◆ eDirectory 8.7.2 avec le dernier Support Pack	◆ Certaines fonctionnalités ne sont pas prises en charge sur eDirectory 8.6.2. Pour plus d'informations sur les fonctionnalités spécifiques et les versions d'eDirectory, reportez-vous à la section « Prise en charge des fonctionnalités pour eDirectory 8.6.2 et eDirectory 8.7.3 », page 313.
Serveur système connecté ◆ Chargeur distant DirXML ◆ Outil de configuration du chargeur distant (Windows uniquement) ◆ Agent Nsure Audit ◆ Module d'interface pilote du système connecté ◆ Outils du système connecté	Pour plus d'informations sur les configurations requises du système d'exploitation et du système connecté spécifiques à chaque système, reportez-vous à la documentation du pilote Identity Manager (http://www.novell.com/documentation/fr-fr/dirxmldrivers).	

Composant système	Configuration système requise	Notes
Serveur d'administration Web ◆ Plugs-in DirXML et de gestion des mots de passe iManager ◆ Configurations de pilote ◆ Fonction de mot de passe en libre-service pour les utilisateurs finals ◆ eGuide	Un des systèmes d'exploitation suivants ◆ NetWare 6 ou 6.5 avec le dernier Support Pack ◆ Windows 2000, XP ou 2003 avec le dernier Service Pack ◆ Linux Red Hat AS ou ES 2.1 Glibc version 2.1.2 ou version ultérieure et Kernel version 2,2 *xx* ou version ultérieure ◆ Solaris 8 ou 9 Le logiciel suivant ◆ Novell iManager 2.0.2 (inclut Apache 2.0.44 ou version ultérieure et Tomcat 4.1.18 ou version ultérieure)	◆ La prise en charge du navigateur est déterminée par iManager 2.0.2. Pour plus d'informations, notamment sur les problèmes connus, reportez-vous au *Novell iManager 2.0.2 Administration Guide (Guide d'administration Novell iManager 2.0.2)* (http://www.novell.com/documentation/fr-fr/imanager20/imanager20/data/bobxl9n.html). ◆ Utilisez l'assistant de configuration iManager pour installer le contenu du portail dans eDirectory. Cette étape est nécessaire pour utiliser les tâches Identity Manager prête à l'emploi, comme les fonctionnalités libre-service de mot de passe et de mot de passe oublié. Cela peut se faire pendant l'installation de iManager, qui est la valeur par défaut. Si vous avez choisi de ne pas le faire pendant l'installation, faites-le plus tard. ◆ Si vous installez eGuide, un serveur Web et un serveur d'application doivent être installés avant de lancer le programme d'installation. ◆ Si vous installez iManager 2.0.2 sur le même serveur qu'eDirectory, la version d'eDirectory doit être la version 8.7.3. ◆ (Netware) Pour installer Novell eGuide 2.1.2, un JVM valide doit être installé sur le serveur. ◆ (Windows) Le Novell Client™ 4.83 est disponible sur le site Novell Software Downloads (téléchargements de logiciels Novell) (http://www.novell.com/download/index.html). ◆ Lorsque vous vous connectez à d'autres arborescences avec iManager pour gérer les serveurs Identity Manager distants, vous pouvez rencontrer des erreurs si vous utilisez le nom du serveur au lieu de l'adresse IP du serveur distant. En outre, l'objet Groupe du serveur LDAP dans NDS doit être configuré pour demander TLS sur des liaisons simples. Le certificat racine approuvé de l'arborescence distante doit également être importé en tant que certificat approuvé sur le serveur Web.

Composant système	Configuration système requise	Notes
Utilitaires DirXML • DirXML License Auditing Tool • Outils d'application (AD, Notes, SAP, PeopleSoft et JDBC) • Outil de configuration de Nsure Audit	Pour plus d'informations sur la configuration requise pour chaque système, reportez-vous à la documentation du pilote Identity Manager (http://www.novell.com/documentation/fr-fr/dirxmldrivers).	

Installation d'Identity Manager sous NetWare

Avant de commencer, vérifiez que votre système répond à la configuration système requise listée à la section « Composants d'Identity Manager et configuration système minimale », page 52.

1. Depuis la console du serveur, saisissez **`nwconfig.nlm`**.
2. Sélectionnez Options de produit > Installer un produit non listé.
3. Appuyez sur F3 (ou sur F4 si vous utilisez RCONSOLE), puis spécifiez le chemin d'accès aux fichiers d'installation d'Identity Manager NetWare.

   L'utilitaire d'installation graphique démarre quelques secondes après.
4. Cliquez sur Suivant.

   Une fois la copie des fichiers terminée, l'écran de bienvenue de DirXML s'affiche. Cliquez sur Suivant pour commencer l'installation.
5. Revoyez les pages Présentation décrivant les types de systèmes, puis cliquez sur Suivant pour continuer.
6. Lisez l'accord de licence, puis cliquez sur J'accepte.
7. Sélectionnez les composants à installer. Les options suivantes sont disponibles :
   - **Serveur DirXML :** permet d'installer le moteur DirXML et les pilotes de service, les pilotes DirXML pour eDirectory, LDAP, JDBC*, GroupWise®, fichier texte délimité et SIF, les composants NMAS™ et l'agent Nsure Audit, et étend le schéma eDirectory.

     Installez Novell eDirectory avant d'installer cette option.
   - **Système connecté :** permet d'installer le chargeur distant et les pilotes LDAP, JDBC, eDirectory, GroupWise, SIF et fichier texte délimité.
   - **Composants Web DirXML :** permet d'installer les plugs-in DirXML, les configurations du pilote DirXML et Novell eGuide.

     Installez iManager avant d'installer cette option.
   - **Utilitaires :** permet d'installer les scripts supplémentaires pour le pilote JDBC.
8. Cliquez sur Suivant.
9. Dans l'écran Extension du schéma, saisissez :
   - **Nom d'utilisateur :** saisissez le nom (au format LDAP) d'un utilisateur qui dispose des droits pour étendre le schéma.
   - **Mot de passe :** saisissez le mot de passe de l'utilisateur.

10 Cliquez sur Suivant.

11 Lisez et vérifiez vos sélections sur la page Résumé, puis cliquez sur Terminer.

12 Une fois l'installation terminée, la boîte de dialogue Installation terminée apparaît. Cliquez sur Fermer.

Installation d'Identity Manager sous Windows

Avant de commencer, vérifiez que votre système répond à la configuration système requise listée à la section « Composants d'Identity Manager et configuration système minimale », page 52.

1 Téléchargez et extrayez le fichier d'installation Identity Manager.

2 Exécutez install.exe à partir du répertoire NT.

3 Lisez les information de bienvenue, puis cliquez sur Suivant.

4 Lisez l'accord de licence, puis cliquez sur J'accepte.

5 Revoyez les pages Présentation sur les différents systèmes et composants, puis cliquez sur Suivant pour lancer l'installation.

6 Sélectionnez les composants à installer.

- **Serveur DirXML :** permet d'installer le moteur et les pilotes de service DirXML, les pilotes DirXML, les composants NMAS, l'agent Nsure Audit et étend le schéma eDirectory.

  Installez Novell eDirectory avant d'installer cette option.

- **Système connecté :** permet d'installer le chargeur distant et les pilotes DirXML que vous sélectionnez.

- **Composants Web DirXML :** permet d'installer les plugs-in DirXML, les configurations du pilote DirXML et Novell eGuide.

  Installez iManager avant d'installer cette option.

- **Utilitaires :** permet d'installer les utilitaires Application que vous sélectionnez.

Le pilote pour Java Message Service (JMS) et WebSphere MQ doivent être installés séparément. Pour plus d'informations, reportez-vous au Guide de mise en œuvre des pilotes (http://www.novell.com/documentation/dirxmldrivers).

7 Dans l'écran Extension du schéma, saisissez :

- **Nom d'utilisateur :** saisissez le nom (au format LDAP) d'un utilisateur qui dispose des droits pour étendre le schéma.

- **Mot de passe :** saisissez le mot de passe de l'utilisateur.

8 Sélectionnez les composants Web que vous souhaitez installer, puis cliquez sur Suivant.

9 Sélectionnez les utilitaires que vous souhaitez installer, puis cliquez sur Suivant. Le programme d'installation affiche le chemin d'installation. Si vous voulez changer l'emplacement par défaut, saisissez ou recherchez l'emplacement désiré, puis cliquez sur Suivant.

10 Sélectionnez les composants système que vous voulez installer (JDBC, PeopleSoft, DirXML License Auditing Utility, Active Directory Discovery Tool, Lotus Notes Discovery Tool), puis cliquez sur Suivant.

11 Revoyez les éléments listés dans la page Résumé. Si vous approuvez, cliquez sur Terminer pour installer les composants.

12 Cliquez sur Fermer pour quitter le programme d'installation.

Installation d'Identity Manager sur les plates-formes UNIX

Avant de commencer, vérifiez que votre système répond à la configuration système requise listée à la section « Composants d'Identity Manager et configuration système minimale », page 52.

1 Téléchargez et extrayez le fichier .tar vers un emplacement de votre choix.

2 Sur l'ordinateur hôte, connectez-vous en tant qu'utilisateur root.

3 Dans le répertoire dans lequel vous avez extrait le fichier .tar, saisissez une des commandes suivantes pour lancer le programme d'installation.

Sous Linux : `/unix/Linux/setup/dirxml_linux.bin`

Sous Solaris : `/unix/Solaris/setup/dirxml_solaris.bin`

Sous AIX : `/unix/AIX/setup/dirxml_aix.bin`

4 Revoyez les informations de bienvenue, puis appuyez sur Entrée pour continuer l'installation.

5 Lisez l'accord de licence et saisissez **`Y`** pour accepter les conditions d'utilisation. Sinon, saisissez **`N`** pour quitter le programme d'installation.

6 Spécifiez le nombre approprié (1-4) pour l'ensemble d'installation que vous voulez installez. Les ensembles d'installation contiennent les composants suivants :

- **Serveur DirXML :** permet d'installer le moteur et les pilotes de service DirXML, les pilotes DirXML, les composants NMAS, l'agent Nsure Audit et étend le schéma eDirectory.

  Installez Novell eDirectory avant d'installer cette option.

  Remarque : pour configurer le stockage partagé pour une haute disponibilité, reportez-vous au Chapitre 12, « Disponibilité élevée », page 285.

- **Serveur système connecté :** permet d'installer le chargeur distant et les pilotes LDAP, JDBC, eDirectory, SAP, fichier texte délimité, GroupWise (Linux SUSE 8 uniquement) et Lotus Notes.

- **Serveur d'administration Web :** permet d'installer les plugs-in DirXML, les configurations du pilote DirXML et Novell eGuide.

  Installez iManager avant d'installer cette option.

- **Personnaliser :** permet d'installer les composants spécifiques que vous sélectionnez dans une liste de tous les composants.

  Remarque : saisissez **`prev`** pour revenir aux menus précédents et modifier vos options d'installation.

7 (Facultatif) En fonction des options que vous avez entrées, une invite peut vous demander de spécifier le nom d'utilisateur et le mot de passe LDAP ou le port Web Server Secure.

Important : (Solaris uniquement) si vous installez votre serveur d'administration Web sur le même serveur que celui sur lequel eDirectory réside, à l'invite pour le port Web Server Secure, faites passer la valeur par défaut à 8443.

8 Vérifiez que les informations contenues dans le résumé sont correctes ; en effet, eDirectory s'arrête temporairement lors de l'installation du moteur DirXML et des fichiers de schéma. Si le résumé d'installation est correct, appuyez sur Entrée pour commencer l'installation des ensembles de pilotes.

9 Une fois l'installation terminée, saisissez **OK** pour fermer le programme d'installation.

Tâches suivant l'installation

Si eDirectory s'exécute, il lance automatiquement le module Identity Manager. Cela évite de charger ou décharger manuellement Identity Manager. Lorsqu'Identity Manager est installé, configurez-le (ainsi que les pilotes que vous avez installés) pour répondre aux règles et aux contraintes définies par vos processus d'entreprise. Les tâches suivant l'installation incluent en général les points suivants :

- Configuration d'un système d'application (pour des instructions spécifiques sur la configuration de pilote, reportez-vous à la documentation du pilote Identity Manager (http://www.novell.com/documentation/fr-fr/dirxmldrivers))
- « Création et configuration d'un pilote », page 81
- « Création de règles », page 99
- « Démarrage, arrêt ou redémarrage d'un pilote », page 84
- « Activation des produits Identity Manager », page 80

Chargeurs distants

Cette section donne des informations sur les points suivants :

- « Présentation », page 58
- « Installation des chargeurs distants », page 59
- « Configuration des chargeurs distants », page 61
- « Configuration du nouveau pilote pour utilisation avec le chargeur distant Java », page 77
- « Exécution des chargeurs distants », page 77

Présentation

Le chargeur distant est un service qui permet au moteur DirXML d'échanger des données avec les pilotes DirXML fonctionnant comme différents processus et dans différents emplacements, y compris les suivants :

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

  Le moteur DirXML est intégré au processus eDirectory. Certains pilotes DirXML peuvent s'exécuter sur le même serveur que le moteur DirXML. En fait, ils peuvent faire partie du même processus que le moteur DirXML.

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

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

  Certains pilotes DirXML ne peuvent pas s'exécuter au même emplacement que le moteur DirXML. Le chargeur distant permet d'exécuter le moteur DirXML dans un environnement tout en exécutant un pilote DirXML sur un serveur dont l'environnement est différent.

  Scénario : serveurs séparés. Le pilote DirXML s'exécute sur un serveur NetWare. Exécutez le pilote DirXML 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 fournit un canal de communication entre le pilote Active Directory et le moteur DirXML.

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

Le chargeur distant permet au moteur DirXML de communiquer avec les pilotes DirXML s'exécutant dans les environnements suivants :

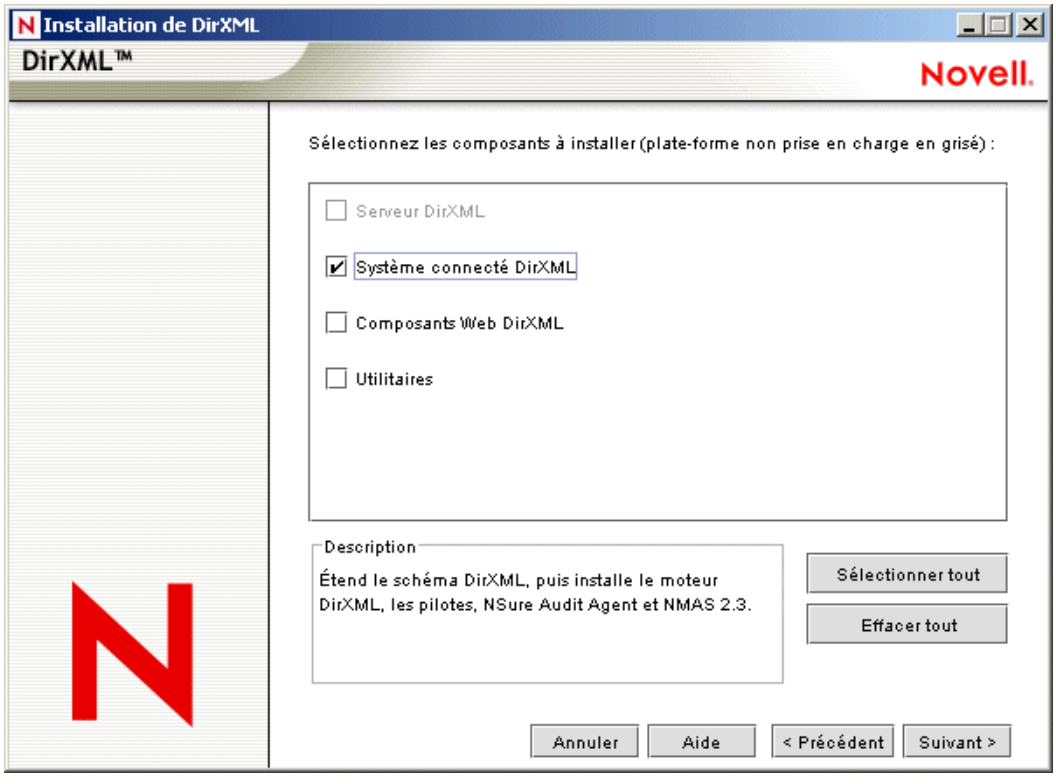
- Windows
- Linux, Solaris ou AIX

Le chargeur distant DirXML Java est une application Java pure. Il permet d'échanger des données entre le pilote DirXML qui s'exécute sur un serveur et les pilotes DirXML qui s'exécutent dans un autre emplacement sur lequel rdxml ne s'exécute pas. Il doit pouvoir fonctionner sur n'importe quel système avec un JRE compatible (1.4.0 minimum, 1.4.2 ou ultérieur recommandé) et des sockets Java, mais n'est pas officiellement pris en charge sur HP-UX, AS/400, OS/390 ou z/OS.

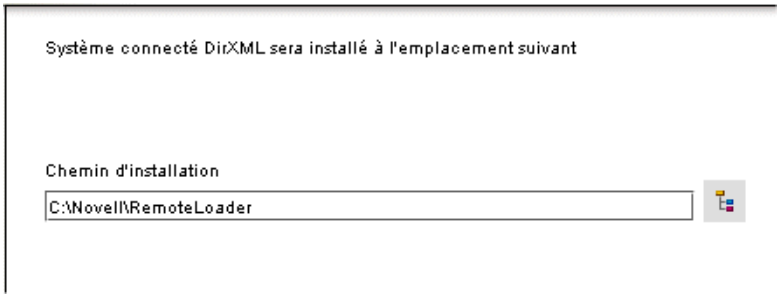
Installation des chargeurs distants

Installation d'un chargeur distant sur un serveur Windows

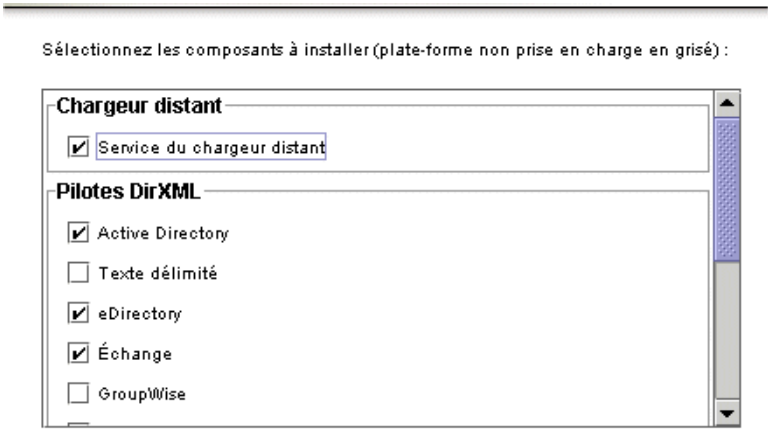
1. Exécutez le programme d'installation d'Identity Manager 2 (par exemple, \nt\install.exe).
2. Affichez la page de bienvenue, acceptez l'accord de licence, puis affichez les deux pages Présentation.
3. Dans la boîte de dialogue Installation de DirXML, désélectionnez tous les composants sauf Système connecté DirXML, 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 le service du chargeur distant DirXML 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

Une fois que vous avez décompressé le fichier Identity Manager 2 que vous avez téléchargé du site Web Novell, procédez aux étapes suivantes :

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

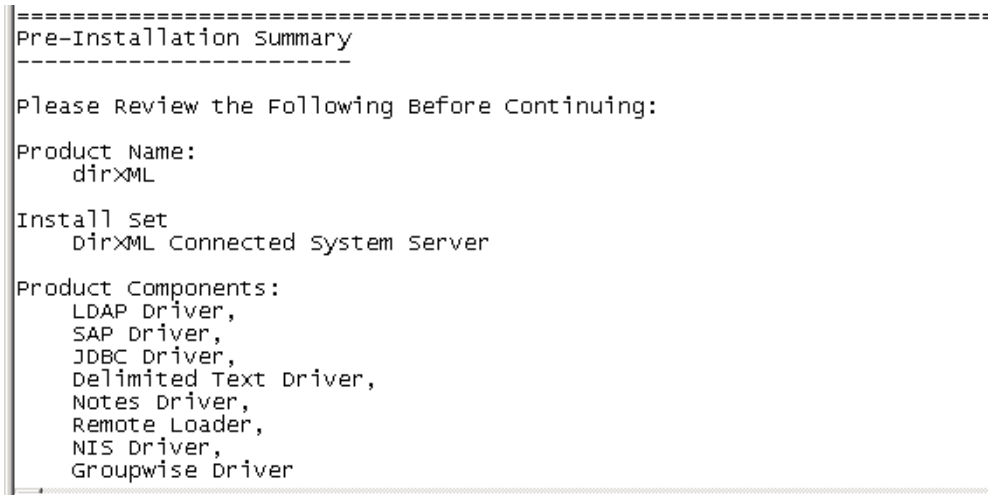
- dirxml_solaris.bin
- dirxml_linux.bin
- dirxml_aix.bin

2 Après avoir accepté l'accord de licence, appuyez sur Entrée pour arriver à la page Choose Install Set (Sélectionnez les paramètres d'installation) :

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

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

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

    4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
   : 2
```

3 Sélectionnez DirXML Connected System Server (Serveur du système connecté DirXML) en tapant 2, puis appuyez sur Entrée.

4 Dans l'écran Pre-Installation Summary (Résumé avant installation), revoyez les composants que vous avez sélectionnés pour installation, puis appuyez sur Entrée.



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

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

2 À partir du CD Identity Manager 2 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 z/OS	dirxml_jremote.tar.gz
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 pilotes, copiez manuellement les pilotes dans le répertoire lib.

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

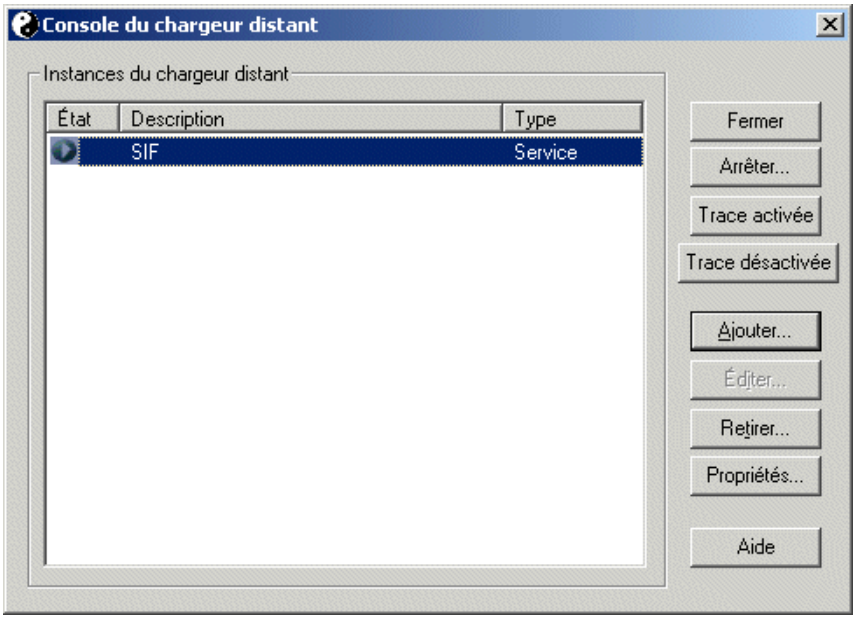
Configuration des chargeurs distants

Le chargeur distant DirXML peut héberger les modules d'interface pilote de l'application DirXML contenus dans les fichiers .dll, .nlm, .so ou .jar. Le chargeur distant Java héberge les modules d'interface pilote Java. Il ne chargera ni n'hébergera un module d'interface pilote (C++) natif.

Configuration du chargeur distant sous Windows

Dirxml_remote.exe exécute le chargeur distant sur la plate-forme Windows. Vous pouvez configurer le chargeur distant DirXML en exécutant dirxml_remote.exe sans aucun paramètre. Ce fichier exécute un assistant de configuration qui vous guide lors de la configuration du chargeur distant.

La console du chargeur distant est une nouvelle fonctionnalité dans Identity Manager 2. Nous vous recommandons d'utiliser la console du chargeur distant au lieu de l'assistant lancé par dirxml_remote.exe. Cliquez sur l'icône de la console du chargeur distant sur votre bureau pour ouvrir la console du chargeur distant :



La console permet de gérer tous les pilotes DirXML (ou les instances de ces pilotes) qui s'exécutent sur le chargeur distant de cet ordinateur :

- Ajoutez et configurez les nouvelles instances du chargeur distant sur l'ordinateur local.
- Modifiez les paramètres de configuration.
- Démarrez et arrêtez les instances du chargeur distant.
- Démarrez et arrêtez la trace pour chaque instance de pilote.

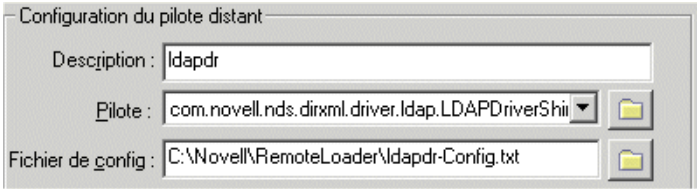
Remarque : si vous mettez à niveau vers Identity Manager 2, la console détecte et importe les instances existantes du chargeur distant. Pour être automatiquement importées, les configurations du pilote doivent être stockées dans le répertoire remoteloader, en général c:\novell\remoteloader. Vous pouvez ensuite utiliser la console pour gérer les pilotes distants.

L'utilisation conjointe de la console et de l'assistant peut provoquer un comportement inattendu. Nous vous recommandons d'utiliser la console en avançant et de mettre à niveau vos configurations existantes dans la console.

Fourniture d'informations pour les instances du chargeur distant

Lorsque vous ajoutez ou que vous modifiez une instance du chargeur distant, une invite vous demande les informations ci-dessous.

Configuration du chargeur distant



- Description

  Spécifiez une description pour identifier l'instance du chargeur distant.

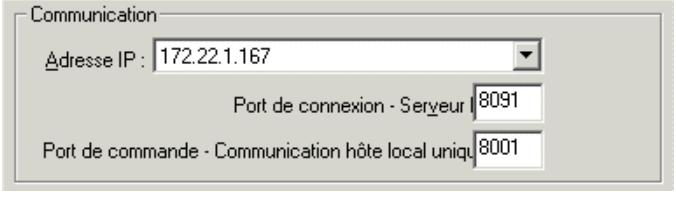
- Pilote

  Recherchez et sélectionnez le module d'interface pilote.

- Fichier config

  Spécifiez 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.

Communication



- Adresse IP

  Spécifiez l'adresse IP sur laquelle le chargeur distant écoute les connexions à partir du serveur DirXML.

- Port de connexion - Serveur DirXML

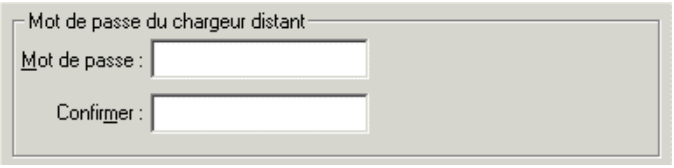
  Spécifiez le port TCP sur lequel le chargeur distant écoute les connexions à partir du serveur DirXML. Le port TCP/IP par défaut pour cette connexion est 8090. Avec chaque nouvelle instance que vous créez, le numéro du port par défaut passe automatiquement au numéro supérieur.

- Port de commande - Communication seule de l'hôte local

  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



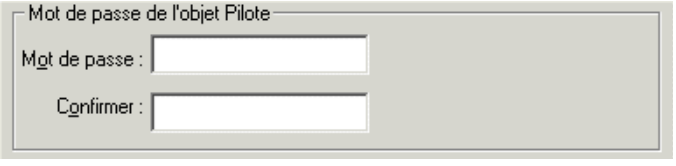
- Mot de passe

  Ce mot de passe permet de contrôler l'accès à une instance du chargeur distant pour un pilote. Il doit être identique à celui que vous spécifiez lorsque vous configurez le pilote pour une connexion à distance (via la page Paramètres du pilote dans Novell iManager.)

- Confirmez

  Ressaisissez le mot de passe.

Mot de passe de l'objet Pilote



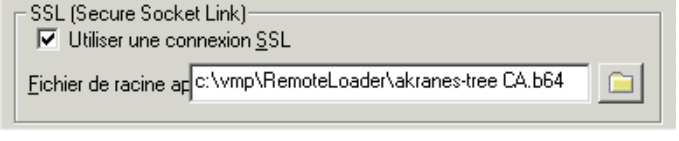
- Mot de passe

  Le chargeur distant utilise ce mot de passe pour s'authentifier auprès du serveur DirXML. Il doit être identique à celui que vous spécifiez lorsque vous configurez le pilote pour une connexion à distance (via la page Paramètres du pilote dans Novell iManager.)

- Confirmez

  Ressaisissez le mot de passe.

SSL (Secure Socket Link)



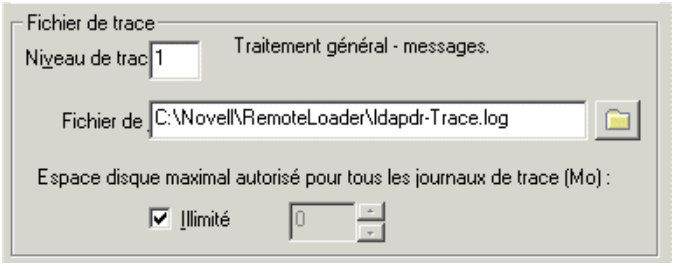
- Utiliser une connexion SSL

  Sélectionnez cette option pour spécifier une connexion SSL.

- Fichier racine approuvé

  Recherchez et sélectionnez le fichier de certificat qui contient la bonne certification racine approuvée. Il s'agit du certificat signé automatiquement issu de l'autorité de certification organisationnelle de l'arborescence eDirectory. Le certificat doit être exporté au format Base64 (par exemple, akranes-tree CA.b64).

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 et par le pilote.

- Fichier 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. Si vous ne sélectionnez pas Illimité, la valeur par défaut est réglée sur 4 096 Mo ou 4 gigaoctets.

Établir un service du 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.

Création de fichiers de configuration pour le chargeur distant

L'exécutable rdxml exécute le chargeur distant sur les plates-formes Solaris, Linux ou AIX. Il peut héberger des pilotes natifs ou Java. Vous pouvez utiliser rdxml pour configurer le chargeur distant. Exécutez rdxml depuis la ligne de commande.

Le fichier rdxml charge le JVM pour prendre en charge les pilotes Java via une interface native. Il charge également les pilotes natifs.

Vous pouvez utiliser les commandes du tableau suivant pour

- spécifier des options et des paramètres de ligne de commande dans un fichier de configuration ;

  Ouvrez ou créez, dans un éditeur de texte, un fichier de configuration, avant d'ajouter les commandes.

- démarrer le fichier de configuration ;
- modifier certains paramètres lorsque le chargeur distant s'exécute.

Option	Autre nom	Paramètre	Description
-class	-cl	Nom de la classe Java	Spécifie le nom de la classe Java du module d'interface pilote de l'application DirXML à héberger. L'option de classe et l'option de module s'excluent mutuellement. Exemple : -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim
-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 pilote de l'application, le port de commande est un 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 de fichier	Spécifie un fichier de configuration. Le fichier de configuration peut contenir toutes les options de ligne de commande à l'exception de *config*. Les options spécifiées sur la ligne de commande remplacent celles spécifiées dans le fichier de configuration. Exemple : -config config.txt

Option	Autre nom	Paramètre	Description
-connection	-conn	Chaîne de configuration de connexion	Spécifie les paramètres de connexion à utiliser pour la connexion au serveur DirXML sur lequel est exécuté le module d'interface pilote distant DirXML. 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 DirXML. Différentiez 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"
-description	-desc	Description succincte	Spécifiez une chaîne de description succincte pour le titre de la fenêtre de trace et pour la consignation de Nsure Audit. Exemple : -description SAP -desc SAP
-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 pilote Java. Cette option n'est utile qu'en association avec l'option de définition des 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. Cette option est particulièrement utile pour les développeurs des modules d'interface pilote de l'application DirXML. Exemple : -javadebugport 8080 -jdp 8080

Option	Autre nom	Paramètre	Description
-module	-m	Nom du module	Spécifie le module qui contient le module d'interface pilote de l'application DirXML à héberger. L'option de module et l'option de classe s'excluent mutuellement. Exemple : -module c:\drivers\exchanges\exdrivr.dll -m c:\drivers\exchanges\exdrivr.dll
-password	-p	Mot de passe	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 est l'objet de la commande. Si une option de commande (déchargement, modification de 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 qui représente la cible de la commande. Exemple : -password novell4 -p novell4
-service	-serv	Aucun, ou installation/ désinstallation	Pour installer une instance en tant que service, utilisez l'argument d'installation avec les autres arguments requis pour l'hébergement du module d'interface pilote de l'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 de désinstallation avec les autres arguments requis pour l'hébergement du module d'interface pilote de l'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.

Option	Autre nom	Paramètre	Description
-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 DirXML 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 DirXML associé au module d'interface pilote distant sur le serveur DirXML. Aucun mot de passe ou les deux doivent être spécifiés. Si aucun mot de passe n'est spécifié, le chargeur distant demande les mots de passe. Il s'agit d'une option de configuration. L'utilisation de cette option 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 DirXML ni de communiquer avec une autre instance du chargeur. Exemple : -setpasswords novell4 staccato3 -sp novell4 staccato3
-trace	-t	Nombre entier	Spécifie le niveau de trace. Cette option n'est utilisée que lorsqu'un module d'interface pilote de l'application est hébergé. Les niveaux de trace correspondent à ceux utilisés sur le serveur DirXML. 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 DirXML. Exemple : -tracechange 1 -tc 1
-tracefile	-tf	Nom de 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

Option	Autre nom	Paramètre	Description
-tracelfilechange	-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
-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 kilooctets, 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 25M -tfm 25M
-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	Activer/Désactiver	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. Notez que l'exécution de dirxml_remote.exe sans paramètre de ligne de commande permet également de lancer l'assistant. 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.

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

Configuration du chargeur distant pour exécution avec SSL

1. (Conditionnel) Si SSL doit être utilisé pour la communication entre le serveur DirXML et le chargeur distant Java, procédez comme suit :

   1a. Exportez le certificat signé automatiquement de l'autorité de certification organisationnelle de l'arborescence dans laquelle le serveur DirXML apparaît.

   Il n'est pas nécessaire (ni souhaitable) d'exporter la clé privée avec le certificat. Enregistrez le certificat en utilisant le format binaire (DER).

   1b. Exécutez le script create_keystore pour créer le fichier java keystore utilisé par le chargeur distant.

   Par exemple, saisissez

   ```
   create_keystore tree-root.der my.keystore
   ```

   Notez les paramètres de configuration affichés par le script create_keystore pour les utiliser dans le fichier de configuration. Le script create_keystore spécifie un mot de passe codé en dur, dirxml, pour le mot de passe keystore. Ce ne pose pas de risque de sécurité ; en effet, seuls un certificat public et une clé publique sont mémorisés dans le keystore.

2 Modifiez l'exemple de fichier de configuration (config8000.txt) et spécifiez les propriétés désirées.

   En particulier, spécifiez le nom de classe du pilote à exécuter, les paramètres de connexion et le port de commande.

3 (Conditionnel) Si SSL doit être utilisé pour une communication entre le serveur DirXML et le chargeur distant Java, ajoutez les valeurs keystore et storepass indiquées par le script create_keystore à la chaîne de connexion.

Configuration d'un pilote DirXML pour utilisation avec le chargeur distant

Utilisez le même processus que pour l'installation de n'importe quel module d'interface pilote. Avec iManager, sélectionnez Gestion DirXML > Présentation, puis ajoutez un module d'interface pilote à un ensemble de pilotes.

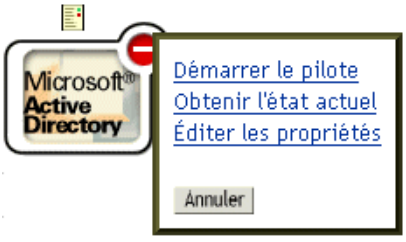
Configuration des propriétés de l'objet Pilote

Une fois que vous avez installé le chargeur distant et un pilote DirXML, spécifiez des paramètres sur l'objet Pilote pour la connexion au chargeur distant.

1 Dans Novell iManager, cliquez sur Gestion DirXML > Présentation.

2 Recherchez et sélectionnez l'objet Pilote que vous voulez configurer.

3 Cliquez sur l'icône d'état du pilote, puis cliquez sur Éditer les propriétés.



4 Saisissez des paramètres pour le chargeur distant.

- Communication
  - Adresse IP

    Si vous ne saisissez pas ce paramètre de communication, il prend par défaut la valeur localhost.
  - Port de connexion

    Il s'agit du port sur lequel le chargeur distant accepte des connexions à partir du module interface distant. Si vous ne saisissez pas ce paramètre de communication, il prend par défaut la valeur 8090.
- 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.

- 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.

- SSL (Secure Socket Link)

  Si vous ne saisissez pas ce paramètre de communication, aucune valeur ne sera mémorisée. Cela signifie que SSL ne sera pas utilisé.

5. Cliquez sur OK.

Utilisation des paramètres et des options de ligne de commande

Vous pouvez utiliser les options de la ligne de commande avec le chargeur distant DirXML pour :

- Spécifier plusieurs paramètres pour une instance de chargeur distant qui héberge le module d'interface pilote de l'application DirXML.

  Ces options incluent la spécification du nom de classe du module d'interface pilote, la spécification des paramètres de connexion utilisés pour communiquer avec le module d'interface pilote distant sur le serveur DirXML ou la définition du niveau de trace.

- Envoyer des commandes à une instance de chargeur distant qui héberge le module d'interface pilote de l'application DirXML.

  Ces options incluent l'ouverture et la fermeture de la fenêtre de trace et le déchargement du chargeur distant.

- Configurer le chargeur distant.

  Ces options incluent la définition des mots de passe et l'installation, et la désinstallation d'une instance du chargeur distant comme service Win32.

Pour obtenir la liste des options, reportez-vous au tableau de la section « Création de fichiers de configuration pour le chargeur distant », page 65.

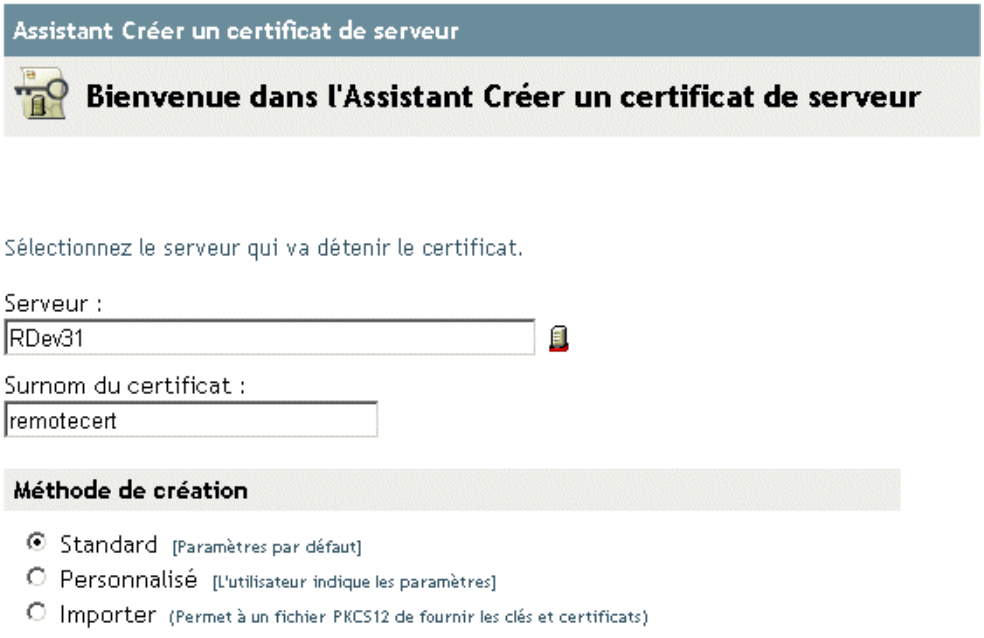
Sécurisation des transferts de données

Si vous envisagez d'utiliser SSL pour sécuriser le transfert des données, remplissez les tâches suivantes :

- Créez un certificat de serveur.
- Exportez un certificat signé automatiquement.
- Configurez votre connexion SSL entre le moteur DirXML et le chargeur distant.

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-lui un surnom (par exemple, remotecert).



Important : notez le surnom du certificat (par exemple, remotecert). Vous utiliserez ce surnom 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.

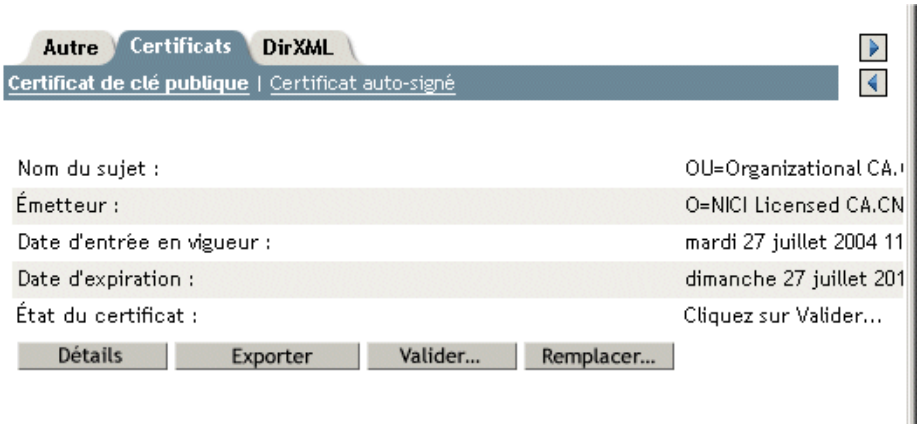
   Vous avez créé un certificat de serveur. Passez à la section « Exportation d'un certificat signé automatiquement », page 74.

Exportation d'un certificat signé automatiquement

1. 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 le certificat signé automatiquement, puis sur Exporter.



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

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

5 Choisissez d'exporter le fichier au format Base64, puis cliquez sur Suivant.

6 Choisissez d'enregistrer le certificat exporté dans un fichier, spécifiez un emplacement, puis cliquez sur Enregistrer.

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

8 Cliquez sur Fermer.

Configuration du pilote pour utiliser une connexion SSL

Avant de configurer votre connexion SSL, vérifiez que vous avez exporté le certificat signé automatiquement et que le chargeur distant a accès au fichier exporté. Reportez-vous à la section « Création d'un certificat de serveur », page 74.

Vous devez maintenant modifier les paramètres du pilote pour utiliser ce certificat.

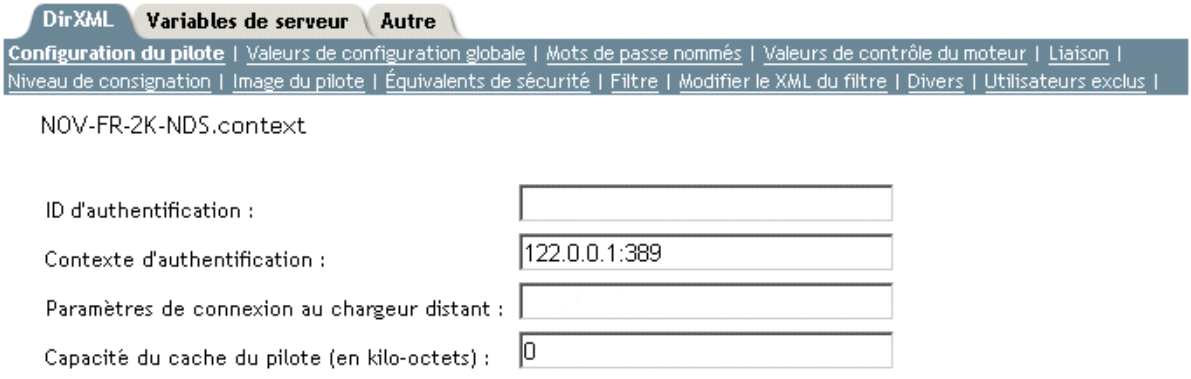
1 Dans Novell iManager, cliquez sur Gestion DirXML > Présentation.

2 Recherchez et sélectionnez l'objet Pilote pour lequel vous voulez configurer une connexion SSL.

3 Spécifiez les paramètres de connexion du chargeur distant.

Par exemple, saisissez

```
192.168.0.1 port=8090 remotecert
```



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

Suggestion : le nom de l'objet KMO est la valeur du surnom que vous avez spécifiée à l'étape 2 de la section « Création d'un certificat de serveur », page 74.

Création d'un script 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 DirXML et si vous utilisez un module d'interface pilote Java, créez un fichier keystore.

Keystore sous Windows

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

Keystore sous Solaris, Linux ou AIX

Dans des environnements Solaris, Linux ou AIX, utilisez le fichier create_keystore. Create_keystore est installé avec rdxml ; il est également inclus dans le fichier dirxml_jremote.tar.gz, qui se trouve dans le répertoire \dirxml\java_remoteloader. Le fichier create_keystore est un script de shell qui appelle l'utilitaire Keytool.

Saisissez ce qui suit dans la ligne de commande :

`create_keystore` *self-signed_certificate_name keystorename*

Keystorename peut être n'importe quel nom (par exemple, rdev_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).

Configuration du nouveau pilote pour utilisation avec le chargeur distant Java

1. Dans Présentation, cliquez sur l'objet Pilote DirXML.
2. Dans la page Configuration du pilote, sélectionnez Se connecter au chargeur distant.
3. Saisissez un mot de passe dans la zone de texte Objet pilote.

   Le chargeur distant utilise ce mot de passe pour s'authentifier auprès du module d'interface pilote distant.
4. Sur la page Authentification, saisissez un mot de passe d'application.

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

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

   Les paramètres sont des paires clé-valeur.

   - hostname

     Nom d'hôte ou adresse IP (par exemple, 190.162.0.1). Spécifie l'adresse ou le nom de l'ordinateur sur lequel le chargeur distant s'exécute.
   - port

     Numéro de port TCP (par exemple, 8090). Spécifie le port sur lequel le chargeur distant accepte les connexions du module d'interface pilote distant.
   - kmo

     Spécifie le nom de clé (par exemple, kmo=remote.cert) de l'objet Matériel clé qui contient les clés et le certificat utilisés pour SSL.

   Exemple de paramètres de communication : hostname=192.168.0.1 port=8090 kmo=remotecert

Exécution des chargeurs distants

Exécution du chargeur distant à partir de la console du chargeur distant sous Windows

Pour exécuter le chargeur distant sous Windows, cliquez sur l'icône de la console du chargeur distant sur le bureau.

Exécution 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, la valeur par défaut est c:\novell\RemoteLoader.

Pour exécuter le chargeur distant :

1. Définissez le mot de passe.

Plate-forme	Commande
Windows	**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*

2. Démarrez le chargeur distant en entrant une commande pour démarrer le fichier de configuration.

Plate-forme	Commande
Windows	**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.

   Utilisez la commande ps ou un fichier de trace pour vérifier si les ports de commande et de connexion écoutent.

   Alors que le chargeur distant Java s'exécute, vous pouvez surveiller sa progression grâce à la commande tail de tracefile :

   ```
   tail -f trace filename
   ```

   Si la dernière ligne du journal affiche ce qui suit, le chargeur s'exécute correctement et attend la connexion du module d'interface pilote distant DirXML :

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

   Le chargeur distant ne charge le module d'interface pilote de l'application DirXML que lorsque le chargeur distant est en communication avec le module d'interface pilote distant du serveur DirXML. Cela signifie par exemple que le module d'interface pilote de l'application s'arrête si le chargeur distant perd la communication avec le serveur DirXML.

Pour arrêter le chargeur distant, saisissez ce qui suit à la ligne de commande :

Plate-forme	Commande
Windows	**`dirxml_remote`** -config *path_to_config_file* -U
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, transmettez l'option -cp *port de commande* pour que le chargeur distant puisse arrêter l'instance appropriée.

Configuration des paramètres de connexion

Spécifiez les paramètres de connexion en utilisant l'option de ligne de commande de connexion.

Le chargeur distant DirXML autorise des méthodes de connexion personnalisée entre le chargeur distant et le module d'interface pilote distant hébergé sur le serveur DirXML. La méthode de connexion par défaut est TCP/IP avec SSL. Pour plus d'informations sur ce qui est attendu et permis dans la chaîne de connexion d'une connexion personnalisée, reportez-vous à la documentation livrée avec le module de connexion personnalisé.

Le chargeur distant ouvre un socket serveur et écoute les connexions du module d'interface pilote distant. Lorsque le module d'interface pilote distant se connecte au chargeur distant, une connexion SSL a lieu pour établir un canal sécurisé. Une fois le canal sécurisé établi, le module d'interface pilote distant s'authentifie auprès du chargeur distant.

Si l'authentification du module d'interface pilote distant réussit, le chargeur distant s'authentifie auprès du module d'interface pilote distant. Le trafic de synchronisation n'intervient que lorsque les deux parties ont vérifié qu'elles communiquent avec une entité autorisée.

Cette section contient les noms d'arguments et les paramètres utilisés pour les connexions TCP/IP.

1. Ouvrez ou créez un fichier de configuration dans un éditeur de texte.
2. Configurez la connexion TCP/IP en vous basant sur le tableau suivant :

Option	Paramètre	Description
address	Adresse IP	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 qu'il doit utiliser une seule adresse. Si aucune adresse n'est spécifiée, le chargeur distant écoute sur toutes les adresses IP locales. Exemple : address=137.65.134.83

Option	Paramètre	Description
keypass	keypass	Utilisée uniquement pour les modules d'interface pilote de l'application DirXML contenus dans les fichiers .jar. Spécifie le mot de passe du fichier keystore Java indiqué par le paramètre keystore. Exemple : keypass=mypassword Cette option ne s'applique qu'au chargeur distant Java.
keystore	keystore	Utilisée uniquement pour les modules d'interface pilote de l'application DirXML contenus dans les fichiers .jar. Spécifie le nom du fichier keystore Java qui contient le certificat racine approuvé de l'émetteur du certificat utilisé par le module d'interface pilote distant. Il s'agit en général de l'autorité de certification de l'arborescence eDirectory qui héberge le module d'interface pilote distant. Exemple : keystore=my.keystore
port	Numéro de port décimal	Spécifie le port TCP/IP sur lequel le chargeur distant écoute des connexions du module d'interface pilote distant. Exemple : port=8090
rootfile	Nom de fichier	Utilisée uniquement pour les modules d'interface pilote de l'application DirXML contenus dans les fichiers .dll. Spécifie le fichier qui contient le certificat racine approuvé de l'émetteur du certificat utilisé par le module d'interface pilote distant. Il s'agit en général de l'autorité de certification de l'arborescence eDirectory qui héberge le module d'interface pilote distant. Le fichier de certificat doit être au format Base64 (PEM). Cette option n'est pas disponible sur le chargeur distant Java.

Activation des produits Identity Manager

L'activation est requise pour vos produits Identity Manager. Pour plus de détails, reportez-vous à l'Annexe A, « Activation des produits Novell Identity Manager », page 305.

Installation d'un pilote personnalisé

Un pilote personnalisé peut comprendre les éléments suivants :

- un ensemble de fichiers .jar ou natifs (.dll, .nlm ou .so) ;
- des fichiers de règles XML pour la configuration du pilote ;
- de la documentation.

Pour plus d'informations sur la création ou l'installation d'un pilote personnalisé, reportez-vous au Novell Developer Kit (Kit du développeur Novell) (http://developer.novell.com/ndk/dirxml-index.htm).

5 Gestion des pilotes DirXML

Cette section contient des informations qui vous aideront à créer et à gérer votre pilote DirXML®. Elle contient les informations suivantes :

Création et configuration d'un pilote

Pour chaque pilote DirXML que vous envisagez d'utiliser, créez un objet Pilote et importez la configuration d'un pilote. L'objet Pilote contient des paramètres et des règles 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 règles par défaut. Il permet de commencer dans de bonnes conditions la mise en œuvre 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 la section « Création d'un objet Pilote », page 82.
- 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 « Création de plusieurs pilotes », page 82.

Création d'un objet Pilote

Le fichier de configuration de pilote (XML) crée et configure les objets nécessaires au bon fonctionnement du pilote. Il inclut également des règles de base que vous pouvez modifier pour votre mise en œuvre.

1. Dans iManager, sélectionnez Utilitaires DirXML > Créer un pilote.
2. Sélectionnez l'ensemble de pilotes dans lequel vous voulez créer le pilote, puis cliquez sur Suivant.

   Si vous placez ce pilote dans un nouvel ensemble de pilotes, spécifiez le nom de l'ensemble, le contexte et le serveur associé.
3. Cochez la case Importer une configuration de pilote du serveur (fichier .xml) et sélectionnez le fichier .xml.

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

Les objets Nsure™ 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.

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 fichier de configuration du pilote (XML) créent et configurent les objets nécessaires au bon fonctionnement des pilotes.

Pour importer simultanément plusieurs pilotes :

1. Dans iManager, sélectionnez Utilitaires DirXML > 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 de pilotes, spécifiez le nom de l'ensemble de pilotes, un contexte et un serveur associé.
3. Sélectionnez les pilotes 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.

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.

Gestion des pilotes DirXML 1.*x* dans un environnement Identity Manager

Les pilotes existants qui ont été créés pour DirXML 1.*x* continuent à s'exécuter avec Identity Manager.

Le moteur DirXML livré avec Nsure Identity Manager 2 est compatible en amont avec les pilotes plus anciens (à condition que les modules d'interface pilote et les configurations des pilotes plus anciens aient été mis à jour avec les mises à jours et correctifs du produit les plus récents), grâce à la conversion des configurations pilote au format Identity Manager, à la volée. Cette conversion ne sert qu'au moteur et ne modifie pas de façon permanente les configurations existantes du pilote DirXML 1.*x*. Le moteur étant compatible en amont, vous pouvez exécuter les pilotes DirXML 1.*x* 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. Les pilotes plus anciens être affichés sur la Présentation d'un ensemble de pilotes, mais la configuration du pilote ne peut pas être affichée ni modifiée. Lorsque vous cliquez sur un pilote DirXML 1.*x* dans la Présentation de l'ensemble de pilotes, les plugs-in DirXML découvrent que le pilote est au format 1.*x* et vous invitent à convertir le pilote au format 2.0 avec l'assistant.

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

Pour modifier un pilote 1.*x* au format 1.*x*, utilisez les plugs-in DirXML 1.*x*. Pour cela, utilisez un serveur Web iManager séparé sur lequel les plugs-in 1.*x* sont installés. Vous ne pouvez pas utiliser les plugs-in DirXML livrés avec Identity Manager pour modifier la configuration d'un pilote sans convertir le pilote au format Identity Manager 2.

Mise à niveau de la configuration d'un pilote de DirXML 1.*x* au format Identity Manager

Le programme d'installation d'Identity Manager installe de nouveaux modules d'interface pilote mais ne modifie pas les objets ou les configurations pilote existants.

Les configurations de pilote existantes qui ont été créées pour DirXML 1.*x* continuent à s'exécuter sous Identity Manager. Toutefois, les plugs-in iManager DirXML pour Identity Manager permettent de n'éditer que les pilotes au format Identity Manager.

Important : l'exécution d'un module d'interface pilote ou la configuration d'un pilote Identity Manager DirXML avec le moteur DirXML 1.*x* n'est pas prise en charge.

Un assistant est fourni pour vous aider à convertir les pilotes DirXML 1.*x* au format Identity Manager.

Pour démarrer l'assistant :

1. Dans iManager, cliquez sur Gestion DirXML > Présentation. Recherchez l'ensemble de pilotes qui contient le pilote à convertir.
2. Cliquez sur l'icône du pilote que vous voulez convertir.

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

Démarrage, arrêt ou redémarrage d'un pilote

1. Dans iManager, cliquez sur Gestion DirXML > Présentation.
2. Recherchez l'ensemble qui contient le pilote.
3. Cliquez sur le pilote dont vous voulez modifier le statut, puis choisissez l'option appropriée (démarrer, arrêter, redémarrer.)

Utilisation de valeurs de configuration globales

Les valeurs de configuration globales (GCV) sont de nouveaux paramètres similaires aux paramètres du pilote. Elles peuvent être spécifiées tant pour un ensemble de pilotes que pour un pilote individuel. Si un pilote n'a pas de valeur pour une GCV donnée, le pilote hérite, pour cette GCV, de la valeur de l'ensemble de pilotes.

Les GCV permettent de spécifier des paramètres pour les nouvelles fonctions d'Identity Manager, telles que la synchronisation des mots de passe ou la pulsation de pilote, ainsi que des paramètres spécifiques à la fonction d'une configuration de pilote individuelle. Certaines GCV sont fournies avec les pilotes, mais vous pouvez aussi ajouter les vôtres. Vous pouvez faire référence à ces valeurs dans une règle pour vous aider à personnaliser votre configuration de pilote.

Important : les paramètres de synchronisation des mots de passe sont des 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 d'Identity Manager :

1. Dans iManager, cliquez sur Gestion DirXML > Présentation.
2. Recherchez l'ensemble de pilotes ou l'objet Pilote, puis cliquez sur l'onglet Valeurs de configuration globales.
3. Ajoutez, supprimez ou modifiez le XML, puis cliquez sur OK pour appliquer vos modifications.

Utilisation de l'utilitaire de ligne de commande DirXML

L'utilitaire de ligne de commande DirXML permet d'accéder à tous les sous-verbes DirXML et de réaliser des tâches de gestion de pilote communes, comme le démarrage et l'arrêt d'un pilote à partir de la ligne de commande. Il est installé avec Identity Manager, mais fonctionne aussi avec les mises en œuvre de DirXML 1.*x*.

Bien que nous recommandions d'utiliser iManager pour administrer Identity Manager, l'utilitaire de ligne de commande DirXML est une autre option disponible pour mener à bien des opérations communes. Vous pouvez utiliser cet utilitaire en mode interactif ou en mode de ligne de commande pur.

L'utilitaire et les scripts sont installés sur toutes les plates-formes pendant l'installation d'Identity Manager. L'utilitaire est installé aux emplacements suivants :

Windows : \Novell\Nds\dxcmd.bat

NetWare : sys:\system\dxcmd.ncf

UNIX : /usr/bin/dxcmd

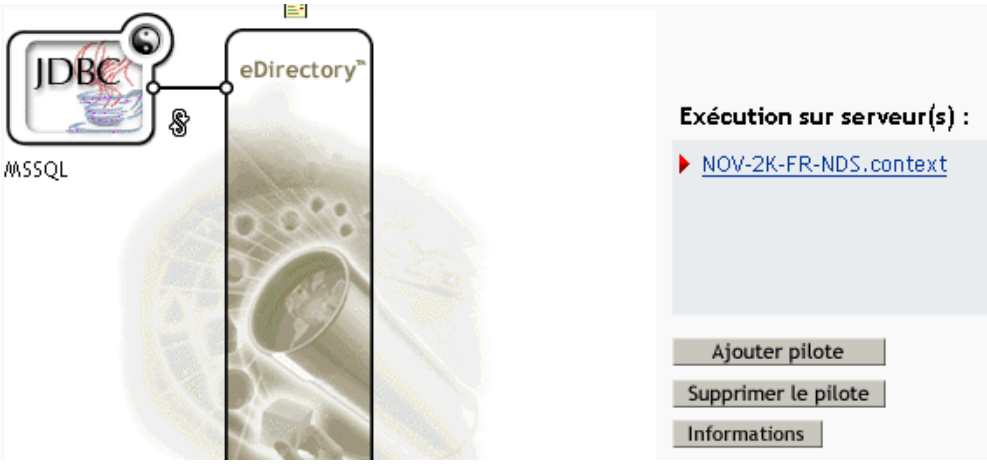
Affichage des informations de versions

L'outil d'identification de version permet :

- d'afficher une vue hiérarchique des informations de version sur votre configuration DirXML ;
- d'afficher dans un fichier de texte des informations identiques à celles disponibles dans l'affichage hiérarchique ;
- d'enregistrer des informations de version dans un fichier d'une unité locale ou réseau.

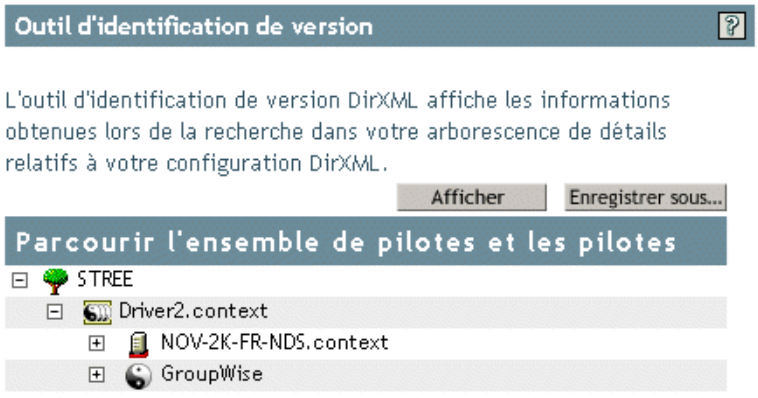
Affichage d'une vue hiérarchique des informations de versions

1 Dans la boîte de dialogue Présentation DirXML d'un ensemble de pilotes, cliquez sur Informations.



Vous pouvez aussi sélectionner Utilitaires DirXML > Outil d'identification de version, recherchez l'ensemble de pilotes, puis cliquez sur Informations.

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

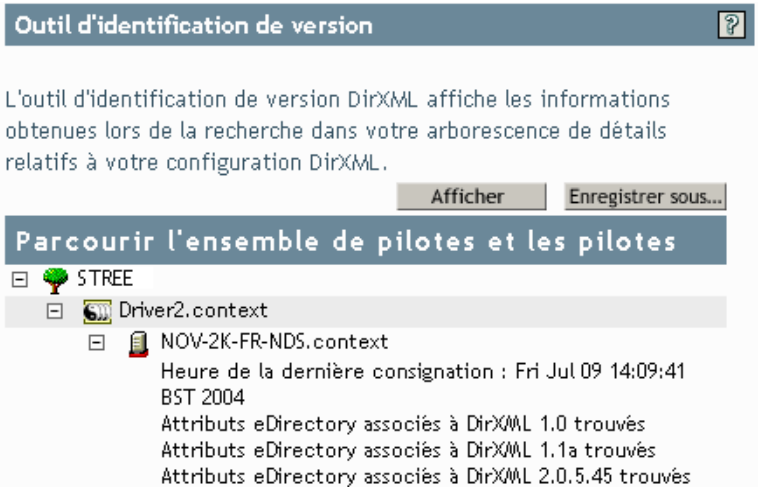


La vue hiérarchique non développée affiche :

- L’arborescence sur 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 DirXML sur chaque serveur.
- Les pilotes.

3 Affichez les informations de version liées aux serveurs en développant l’icône du serveur.



La vue développée d'une icône de serveur globale affiche :

- L'heure de la dernière consignation.
- Les versions DirXML qui s'exécutent ou se sont exécutées sur le serveur.

  Dans l'Outil d'identification de version, Identity Manager 2 est appelé DirXML 2.x.x.x. Dans cet exemple, l'entrée Attributs eDirectory associés à DirXML 2.0.5.39 trouvés indique la version de DirXML exécutée sur le serveur.

  Les versions DirXML antérieures à la version 2.x.x.x ne mémorisaient pas les numéros de versions. Si des versions antérieures de DirXML se sont exécutées sur le serveur, l'Outil d'identification de version affiche des marqueurs dans le répertoire. Dans cet exemple, trois lignes Attributs eDirectory associés à DirXML xxx trouvés identifient les marqueurs de versions antérieures de DirXML : 1.0, 1.1a et 1.1.

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

La vue développée d'une icône de pilote globale affiche les éléments suivants :

- le nom du pilote,
- le module du pilote (par exemple, com.vmp.nds.dirxml.driver.jdbc.JDBCDriverShim).

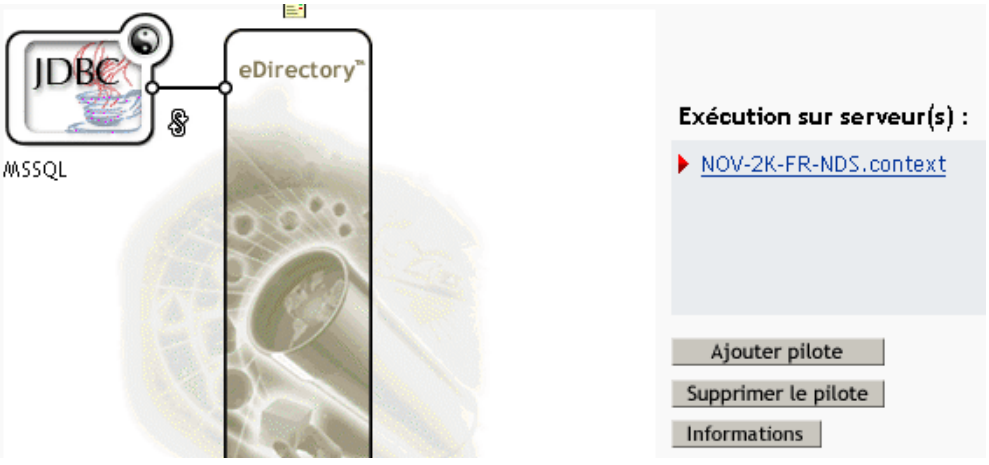
La vue développée d'un serveur sous une icône de pilote affiche les éléments suivants :

- l'ID du pilote,
- la version de l'instance du pilote s'exécutant sur ce serveur.

Affichage d’un fichier texte

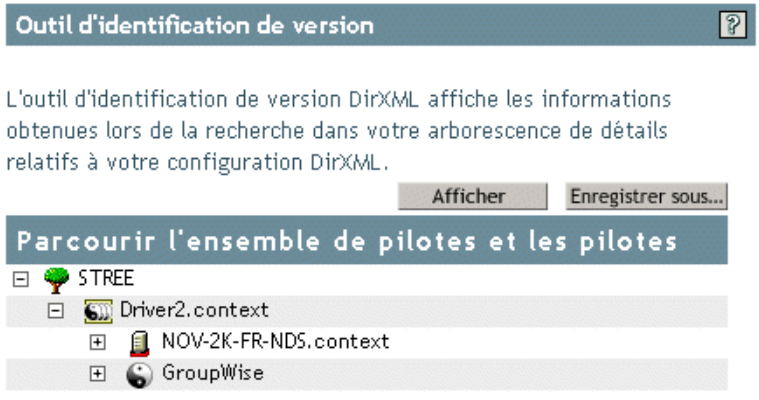
DirXML publie des informations de version dans un fichier. Vous pouvez afficher ces informations au format texte. La représentation textuelle contient les mêmes informations que la vue hiérarchique.

1 Dans la boîte de dialogue Présentation DirXML d’un ensemble de pilotes, cliquez sur Informations.



Vous pouvez aussi sélectionner Utilitaires DirXML > Outil d’identification de version, recherchez l’ensemble de pilotes, puis cliquez sur Informations.

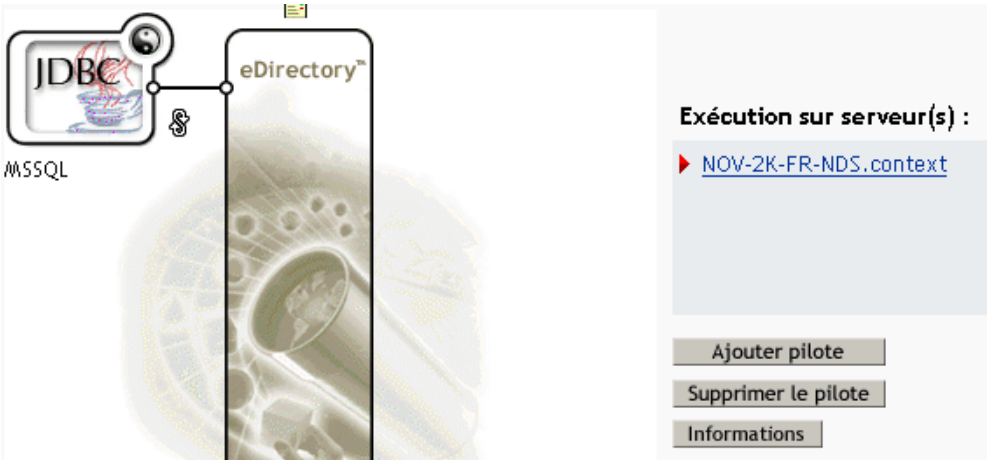
2 Dans la boîte de dialogue Outil d’identification de version, cliquez sur Afficher.



Enregistrement des informations de version

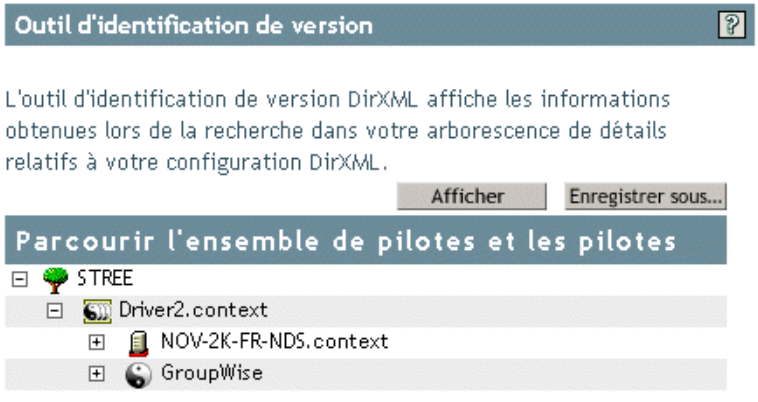
Vous pouvez enregistrer des informations de version dans un fichier texte de votre unité locale ou réseau.

1. Dans la boîte de dialogue Présentation DirXML d'un ensemble de pilotes, cliquez sur Informations.



   Vous pouvez aussi sélectionner Utilitaires DirXML > Outil d'identification de version, recherchez l'ensemble de pilotes, puis cliquez sur Informations.

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



3. Dans la boîte de dialogue Téléchargement de fichier, cliquez sur Enregistrer.
4. Recherchez le répertoire désiré, saisissez un nom de fichier, puis cliquez sur Enregistrer.

   Identity Manager enregistre les données dans un fichier texte.

Utilisation de mots de passe nommés

Avec DirXML 1.*x*, il était possible de stocker un mot de passe en toute sécurité, de sorte qu'un pilote pouvait utiliser ce mot de passe sans que ce dernier apparaisse en texte clair dans les règles du pilote.

Identity Manager permet de stocker plusieurs mots de passe de façon sécurisée pour un pilote donné. Cette nouvelle fonctionnalité s'appelle 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 de façon sûre, par exemple un nom d'utilisateur.

Pour utiliser un mot de passe nommé dans une règle de pilote, désignez-le par le nom du mot de passe plutôt que d'utiliser le mot de passe réel ; le moteur DirXML 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 DirXML 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 sur les Mots de passe nommés dans le *Guide de mise en œuvre du pilote DirXML 2.1 pour Lotus Notes* (http://www.novell.com/documentation/fr-fr/dirxmldrivers).

Cette section contient les informations suivantes :

Configuration des mots de passe nommés avec iManager

1. Dans iManager, cliquez sur Gestion DirXML > Présentation. Recherchez les ensembles de pilotes ou recherchez et sélectionnez un conteneur qui contient l'ensemble de pilotes.

   Une représentation graphique de l'ensemble de pilotes apparaît.

2. Dans Présentation DirXML, cliquez sur l'icône pour le pilote.

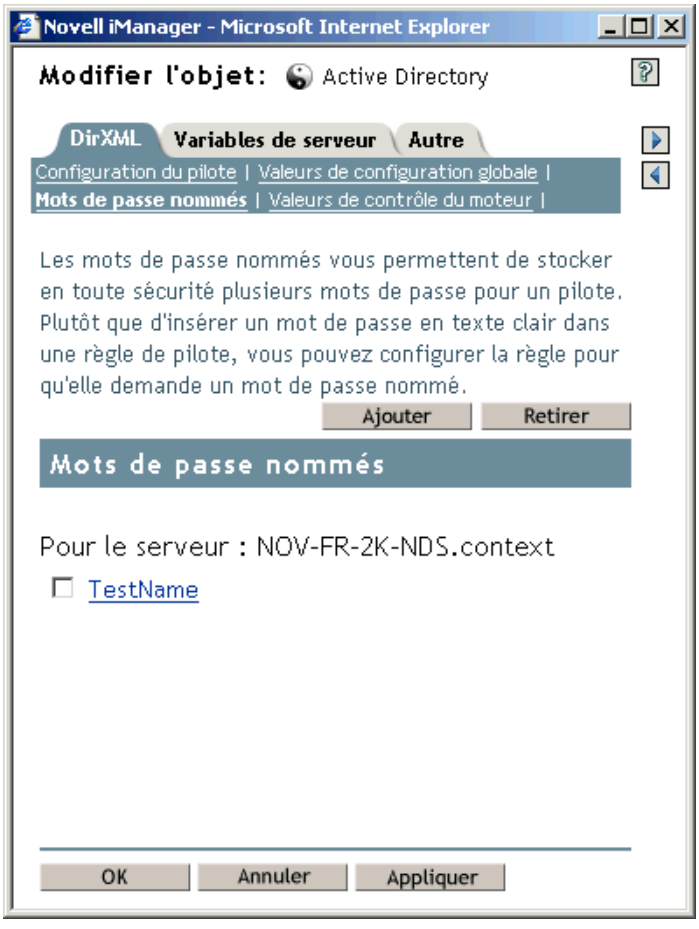
   Une représentation graphique de la configuration du pilote apparaît.

3. Dans Présentation pilote DirXML, cliquez sur l'icône du pilote.

   La page de modification de l'objet apparaît.

4 Dans la page de modification de l'objet de l'onglet DirXML, cliquez sur Mots de passe nommés.

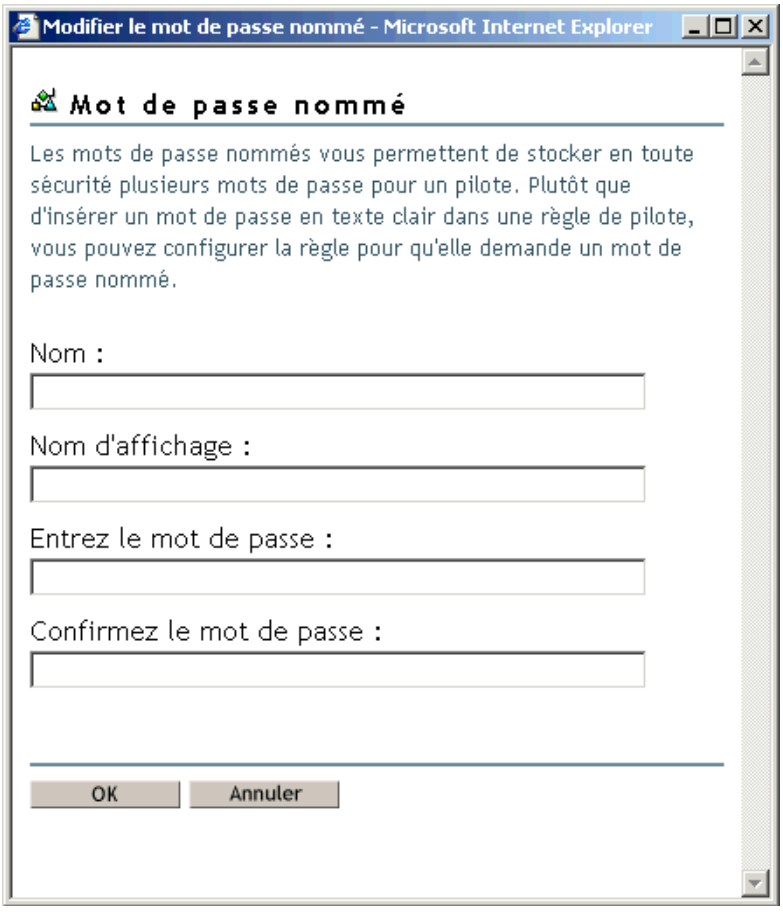
La page Mots de passe nommés apparaît, listant les Mots de passe nommés actuels pour ce pilote. Si vous n'avez pas configuré de mots de passe nommés, la liste est vide.



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

Une page apparaît permettant de spécifier le nom, le nom d'affichage et le mot de passe.

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



6 Pour supprimer un mot de passe nommé, cliquez sur Supprimer.

Le mot de passe est supprimé sans invite vous demandant de confirmer l'opération.

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 93
- « Suppression d'un mot de passe nommé dans l'utilitaire de ligne de commande DirXML », page 94

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 la section « Utilisation de l'utilitaire de ligne de commande DirXML », page 84.

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 password
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 DXCommand.

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 la section « Utilisation de l'utilitaire de ligne de commande DirXML », page 84.

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 password
99: Exit

Enter choice:
```

6 (Facultatif) Saisissez 5 pour voir 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 password
99: Exit

Enter choice:
```

10 (Facultatif) Saisissez 5 pour voir 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 DXCommand.

Utilisation des mots de passe nommés dans les règles de pilotes

L'exemple suivant montre comment un mot de passe nommé peut être référencé dans une règle 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/>
```

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 DirXML (Identity Manager 2), vous obtenez l'erreur UniqueSPIException error -783.
- Aucun serveur n'est listé près du pilote dans la Présentation DirXML.
- Un serveur est listé près du pilote dans la Présentation DirXML, mais le nom est du texte corrompu.

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

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

Ajout de la pulsation du pilote

La pulsation du pilote est une nouvelle fonctionnalité des pilotes DirXML, livrée avec Identity Manager 2 ; son utilisation est facultative. La pulsation du pilote est configurée en utilisant un paramètre de pilote et en spécifiant un intervalle de temps. Si un paramètre de pulsation de pilote existe et la valeur de son intervalle est différente de 0, le pilote envoie un document de pulsation de pilote au moteur DirXML s'il n'y a pas de communication sur le canal Éditeur pour 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 DirXML accepte le document de pulsation mais ne prend 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 Gestion DirXML > Présentation. Recherchez votre pilote et cliquez sur l'icône du pilote.
2. Dans la vue graphique de la configuration du pilote, cliquez sur l'icône du pilote.
3. Sur la page DirXML, 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 la mettre en œuvre différemment, par exemple en utilisant des secondes.
4. Si aucun paramètre de pilote n'existe pour la pulsation, cliquez sur Édition XML.
5. 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.
6. 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 globales, vous pouvez régler la pulsation du pilote au niveau de l'ensemble de pilotes plutôt que sur 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 la valeur de l'ensemble de pilotes.

Voici un exemple de document de statut 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>
```

6 Création de règles

Les règles permettent de personnaliser le flux d'informations entrant et sortant de Novell® eDirectory™ 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 règle doit être créée pour indiquer au moteur DirXML qu'un utilisateur différent est appelé par chacun des systèmes. Chaque fois que des opérations affectant les utilisateurs sont transmises via les systèmes connectés, Nsure™ Identity Manager applique la règle permettant cette modification.

Les règles 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.

Un guide détaillé de ces règles se trouve dans le *Guide de personnalisation des pilotes et du générateur de règles*. Ce guide contient :

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

Pour plus d'informations sur les règles, reportez-vous au *Guide de création des règles et de personnalisation des pilotes*.

7 Gestion des mots de passe à l'aide des règles de mot de passe

Avec les règles de mot de passe, vous pouvez accroître la sécurité en définissant des règles pour la création par les utilisateurs de mots de passe. Vous pouvez aussi réduire les coûts du service d'assistance en fournissant aux utilisateurs des options en libre-service pour les mots de passe oubliés et pour la réinitialisation des mots de passe.

Cette section contient les informations suivantes :

Pour plus d'informations sur les options en libre-service Mot de passe oublié et Réinitialiser le mot de passe, reportez-vous au Chapitre 8, « Mot de passe en livre service », page 125.

Présentation des options de règles de mot de passe

Une règle de mot de passe est un ensemble de principes définis par l'administrateur et régissant les critères de création et de remplacement des mots de passe par les utilisateurs finals. Nsure™ Identity Manager tire parti du service NMAS™ pour appliquer les règles de mot de passe que vous assignez aux utilisateurs dans Novell® eDirectory™. Grâce à la synchronisation des mots de passe, vous pouvez également appliquer les règles de mot de passe à tous les systèmes connectés, comme expliqué au Chapitre 9, « Synchronisation de mot de passe sur des systèmes connectés », page 165.

Les règles de mot de passe incluent également les options en libre-service Mot de passe oublié, qui permettent de réduire les appels d'assistance liés à l'oubli des mots de passe. Une autre option proposée en libre-service, Réinitialiser le mot de passe, permet aux utilisateurs de modifier leur mot de passe tout en affichant les principes définis par l'administrateur dans la règle. Les utilisateurs peuvent accéder à ces options par l'intermédiaire de la console iManager en libre-service.

La plupart des fonctions de gestion des mots de passe nécessitent que l'option Mot de passe universel soit activée. Idéalement, la console iManager en libre-service doit être intégrée au portail de votre société, si elle en possède un, afin que les utilisateurs accède facilement aux options en libre-service Mot de passe oublié et Réinitialiser le mot de passe.

Les mots de passe sont créés par l'intermédiaire d'un assistant dans iManager, Gestion des mots de passe > Gérer les règles de mot de passe > Nouveau.

Les nouvelles fonctions de gestion des mots de passe permettent d'effectuer les opérations suivantes :

- « Activation du mot de passe universel », page 102
- « Définition des règles de mots de passe avancées », page 104
- « Ajout de votre propre message de modification du mot de passe aux règles de mot de passe », page 105
- « Comment fournir aux utilisateurs le libre-service Mot de passe oublié », page 126
- « Comment fournir aux utilisateurs le libre-service Réinitialiser le mot de passe », page 127
- « Assignation de règles aux utilisateurs eDirectory », page 106
- « Application des règles dans eDirectory », page 107
- « Application des règles sur les systèmes connectés », page 109
- « Affichage de la règle de mot de passe en vigueur pour un utilisateur », page 109
- « Définition du mot de passe universel pour un utilisateur », page 110

Activation du mot de passe universel

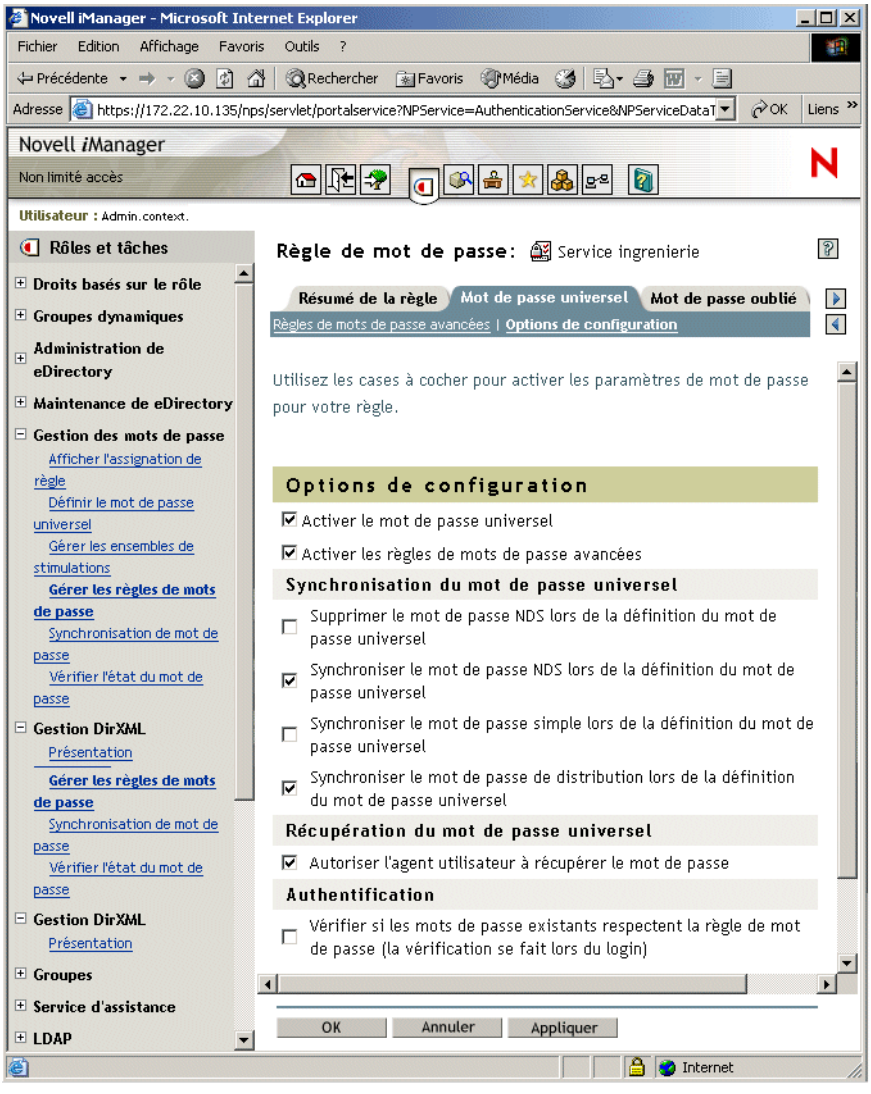
Le mot de passe universel est la nouvelle fonctionnalité d'eDirectory 8.7.1. Vous devez activer cette fonction si vous souhaitez que vos utilisateurs se servent des options Règles de mots de passe avancées, Synchronisation de mot de passe et Mot de passe oublié.

Une règle de mot de passe permet de spécifier si le mot de passe universel est activé. Vous pouvez alors assigner cette règle aux utilisateurs (à l'arborescence, à un conteneur ou à une partition, ou à un utilisateur particulier). Le mot de passe universel n'a pas besoin d'être activé pour toute l'arborescence. En utilisant plusieurs règles de mot de passe, vous pouvez personnaliser votre utilisation du mot de passe universel en fonction de vos besoins. Nous vous recommandons d'assigner des règles de mot de passe au niveau le plus élevé possible de l'arborescence afin de simplifier l'administration.

Il est nécessaire de réaliser une planification supplémentaire afin de préparer votre environnement à l'utilisation des mots de passe universels, en mettant à niveau Novell Client™ (le cas échéant) ou eDirectory.

Vous pouvez également modifier les autres paramètres de mot de passe universel et NMAS dans une règle de mot de passe, pour indiquer par exemple si NDS ou un mot de passe simple sont synchronisés avec le mot de passe universel.

L’illustration suivante propose un exemple de la page de propriétés dans laquelle vous spécifiez les options de configuration du mot de passe universel pour une règle de mot de passe.



Définition des règles de mots de passe avancées

Les règles de mots de passe avancées permettent de définir les critères d'acceptation des mots de passe, par exemple :

- la syntaxe des mots de passe ;
- les propriétés des mots de passe ;
- la durée de vie des mots de passe ;
- l'utilisation des caractères spéciaux ;
- les mots de passe exclus.

  Important : n'oubliez pas qu'il peut être utile d'exclure les mots de passe que vous considérez comme susceptibles de mettre en péril la sécurité de votre système. Cette liste d'exclusion n'est toutefois pas destinée à contenir un très grand nombre de mots, contrairement à un dictionnaire. Les longues listes de mots à exclure peuvent affecter les performances du serveur. Plutôt que d'utiliser une longue liste de mots à exclure pour vous protéger contre les attaques de dictionnaire, nous vous conseillons d'utiliser les règles de mots de passe avancées pour obliger les utilisateurs à inclure au moins un chiffre dans leur mot de passe.

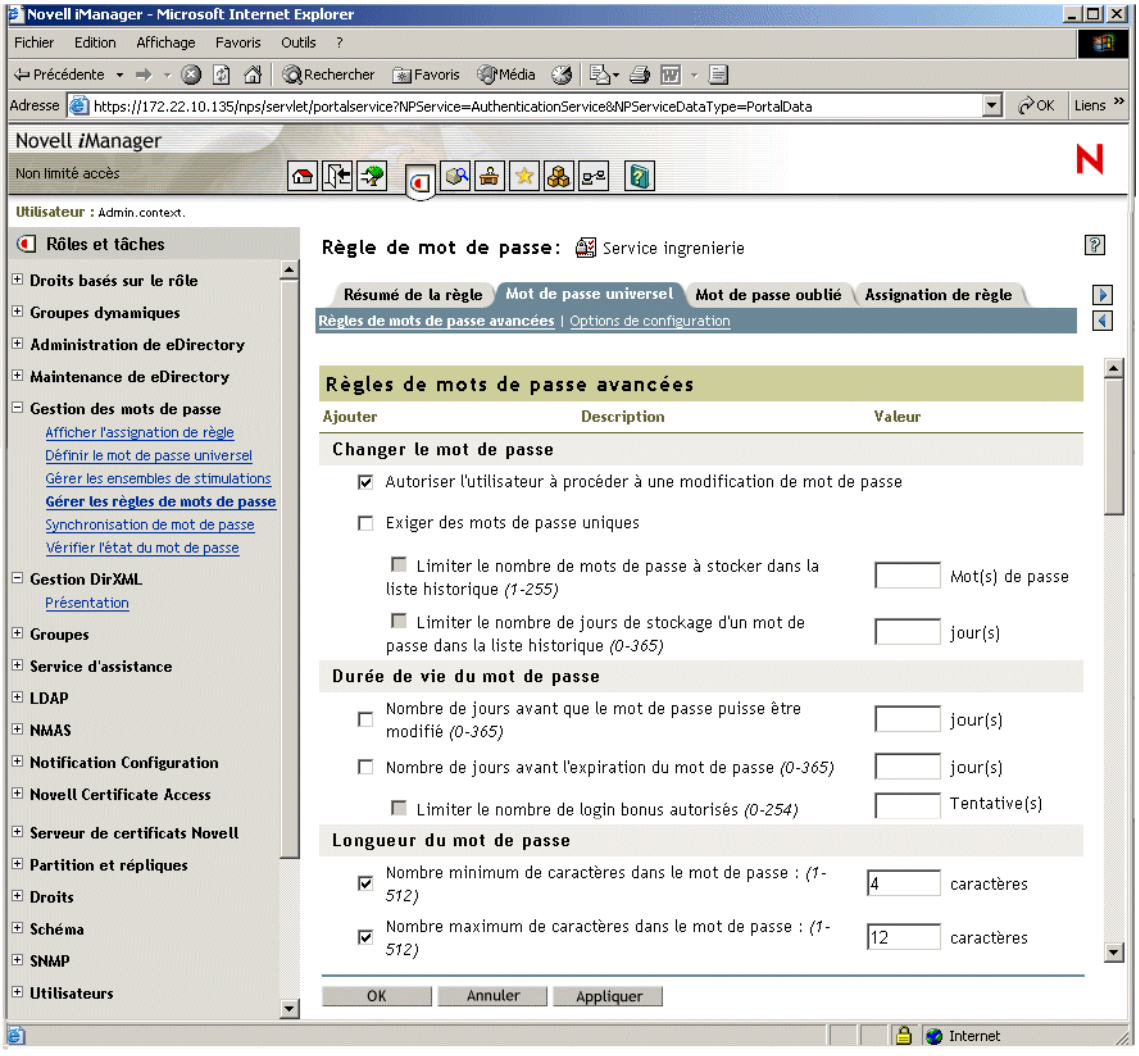
Pour utiliser les règles de mots de passe avancées dans une règle de mot de passe, vous devez activer le mot de passe universel. Si ce n'est pas le cas, les restrictions de mots de passe définies pour le mot de passe NDS® s'appliquent.

Remarque : lorsque vous créez une règle de mot de passe et que vous activez le mot de passe universel, les règles de mots de passe avancées s'appliquent à la place des paramètres de mots de passe définis pour les mots de passe NDS. Les paramètres de mot de passe hérités sont ignorés. Aucune fusion ni copie des paramètres précédents ne s'effectue automatiquement lorsque vous créez des règles de mot de passe.

Par exemple, si vous avez défini un nombre de login bonus pour le mot de passe NDS, lorsque vous activez le mot de passe universel, vous devez recréer le paramètre de login bonus dans les règles de mots de passe avancées de la règle de mot de passe.

Si, par la suite, vous désactivez l'option Mot de passe universel dans la règle de mot de passe, les paramètres de mot de passe existants ne seront plus ignorés. Ils s'appliquent alors pour le mot de passe NDS.

L'illustration suivante propose un exemple de la page de propriétés dans laquelle vous spécifiez les règles de mots de passe avancées d'une règle de mot de passe.



Ajout de votre propre message de modification du mot de passe aux règles de mot de passe

Reportez-vous à la section « Ajout de votre propre message de modification du mot de passe aux règles de mot de passe », page 152.

Comment fournir aux utilisateurs le libre-service Mot de passe oublié

Reportez-vous à la section « Comment fournir aux utilisateurs le libre-service Mot de passe oublié », page 126.

Comment fournir aux utilisateurs le libre-service Réinitialiser le mot de passe

Reportez-vous à la section « Comment fournir aux utilisateurs le libre-service Réinitialiser le mot de passe », page 127.

Assignation de règles aux utilisateurs eDirectory

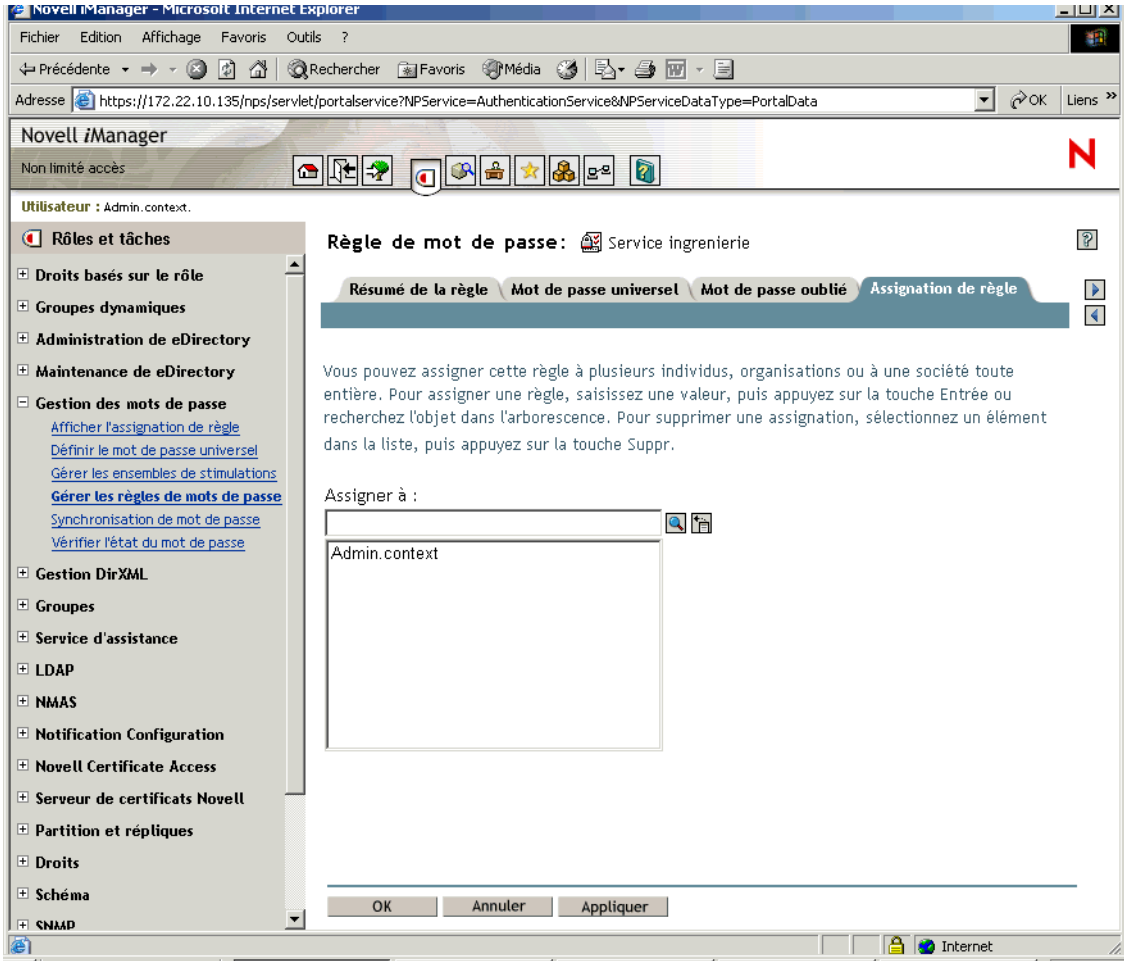
Dans eDirectory, vous pouvez assigner une règle de mot de passe aux utilisateurs à l'arborescence (en utilisant l'objet Règle de login), à un conteneur ou à une partition, ou à des utilisateurs particuliers.

Nous vous conseillons d'assigner une règle par défaut à toute l'arborescence, et d'assigner les éventuelles autres règles de mot de passe au niveau le plus élevé possible de l'arborescence afin de simplifier l'administration.

NMAS détermine quelle règle de mot de passe est en vigueur pour chaque utilisateur. Pour plus d'informations sur l'assignation des règles de mot de passe aux utilisateurs, reportez-vous à la section « Assignation de règles de mot de passe aux utilisateurs », page 120.

Si vous utilisez la synchronisation des mots de passe, n'oubliez pas de vérifier que tous les utilisateurs à qui vous avez assigné des règles de mot de passe correspondent aux utilisateurs que vous souhaitez voir participer à la synchronisation des mots de passe entre les systèmes connectés. Les règles de mot de passe sont assignées dans une perspective centrée sur l'arborescence. Par opposition, la synchronisation des mots de passe est définie par pilote et par serveur. Pour que la synchronisation des mots de passe donne les résultats escomptés, vérifiez que les utilisateurs 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 règles de mot de passe en activant le mot de passe universel. L'assignation d'une règle de mot de passe au conteneur racine d'une partition garantit que cette règle s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

L’illustration suivante propose un exemple de la page de propriétés dans laquelle vous spécifiez à quel objet assigner la règle de mot de passe.



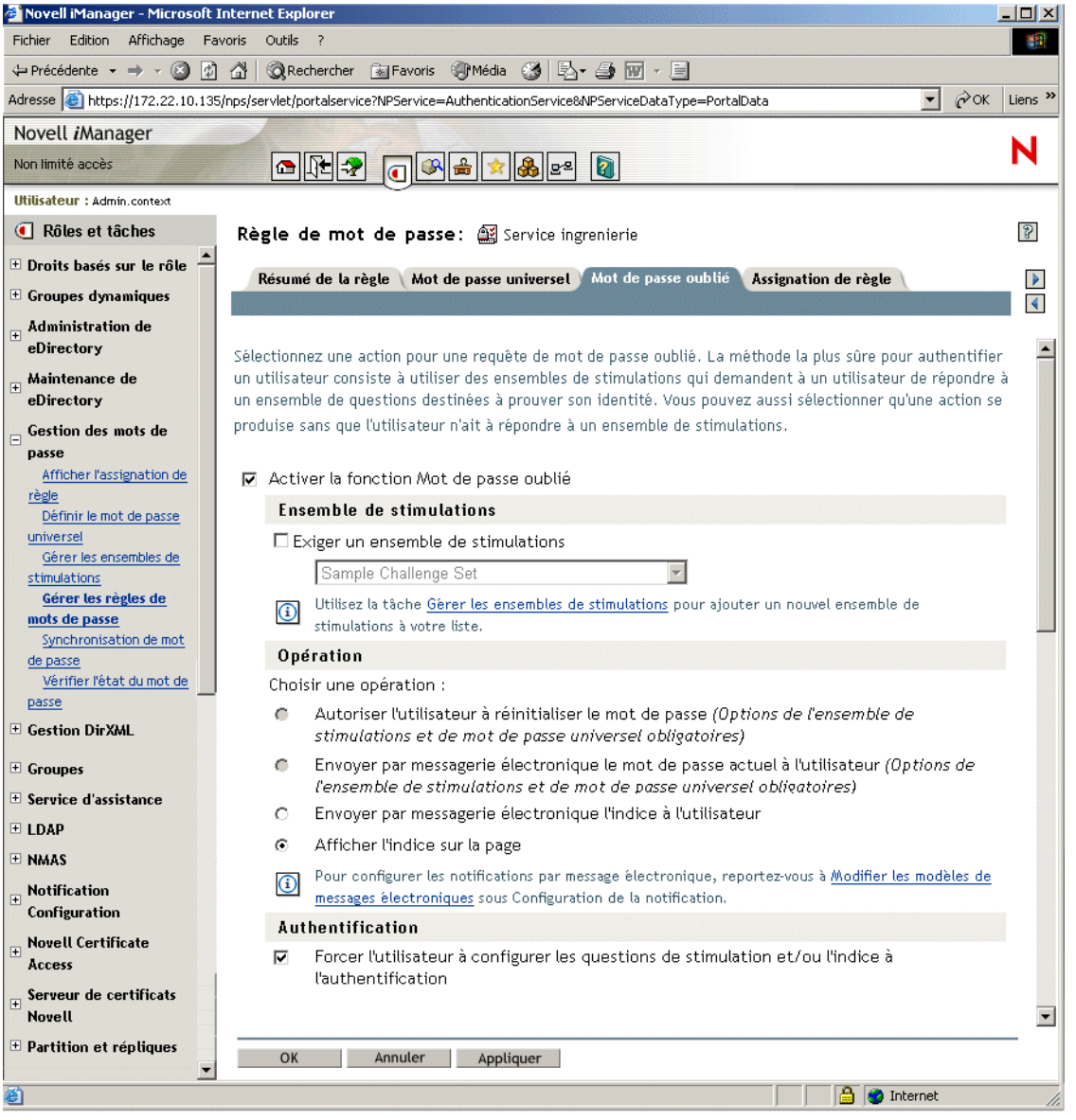
Application des règles dans eDirectory

Lorsque vous assignez une règle de mot de passe à des utilisateurs de l’arborescence, toute modification ultérieure d’un mot de passe doit être conforme aux règles de mots de passe avancées de cette règle. Dans le navigateur, les règles de mot de passe s’affichent sur la page dans laquelle l’utilisateur modifie le mot de passe. Dans Novell Client 4.9 SP2 ou une version ultérieure, les règles s’affichent également. Dans les deux méthodes, tout mot de passe non conforme est refusé. NMAS est l’application permettant de mettre en œuvre ces règles.

Vous pouvez demander de contrôler la conformité de tous les mots de passe existants. En cas de non-conformité, les utilisateurs sont alors invités à modifier leur mot de passe.

Vous pouvez également demander que, au moment de leur authentification via iManager ou la console iManager en libre-service, les utilisateurs soient invités à configurer les fonctions Mot de passe oublié que vous avez activées. Ces services sont appelés les services de post-authentification. Par exemple, si vous souhaitez que les utilisateurs créent un indice de votre mot de passe qui peut leur être envoyé par courrier électronique en cas d’oubli de leur mot de passe, vous pouvez utiliser les services de post-authentification pour les inviter à créer un indice de mot de passe au moment de leur login.

Les paramètres de post-authentification constituent la dernière option de la page de propriétés Mot de passe oublié, comme le montre l'illustration suivante.



Application des règles sur les systèmes connectés

Si vous utilisez la synchronisation des mots de passe, des paramètres sont proposés pour chaque pilote afin d'appliquer les règles de mots de passe avancées d'une règle de mot de passe.

Procédez comme suit :

- Décidez si, en règle générale, Identity Manager doit accepter les mots de passe édités par un système connecté.
- Appliquez les règles aux mots de passe entrants en provenance d'un système connecté. Si le mot de passe n'est pas conforme, Identity Manager le refuse.
- Appliquez les règles au système connecté en réinitialisant les mots de passe non conformes. Si le mot de passe entrant dans Identity Manager n'est pas conforme, Identity Manager peut rejeter la modification du mot de passe en fonction du système de protection des identités. Il peut également utiliser le mot de passe de distribution Identity Manager pour réinitialiser le mot de passe sur le système connecté.
- Informez les utilisateurs lors de l'échec de la synchronisation des mots de passe. Par exemple, si l'utilisateur a créé un mot de passe non conforme sur un système connecté et si Identity Manager ne l'a pas accepté, l'utilisateur en est informé par message électronique afin qu'il sache que le mot de passe modifié n'a pas été synchronisé.

Si vous utilisez les règles de mots de passe avancées et la synchronisation des mots de passe via Identity Manager, nous vous conseillons de rechercher les règles de mot de passe de tous les systèmes connectés afin de vérifier que les règles de mots de passe avancées définies dans la règle de mot de passe eDirectory sont compatibles ; les mots de passe peuvent ainsi être synchronisés sans problème.

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

Les règles de mot de passe sont assignées dans une perspective centrée sur l'arborescence. Par opposition, la synchronisation des mots de passe est définie par pilote ; ceux-ci sont installés sur les serveurs et ne peuvent gérer que les utilisateurs existants d'une réplique principale ou d'une réplique en lecture/écriture. Pour que la synchronisation des mots de passe donne les résultats escomptés, vérifiez que les utilisateurs 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 règles de mot de passe en activant le mot de passe universel. L'assignation d'une règle de mot de passe au conteneur racine d'une partition garantit que cette règle s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

Pour plus d'informations sur la manière de définir les flux de mots de passe, reportez-vous à la section « Paramètres de synchronisation des mots de passe à créer à l'aide des valeurs de configuration globales », page 178.

Affichage de la règle de mot de passe en vigueur pour un utilisateur

Dans iManager, vous pouvez vérifier quelle la règle s'applique à un utilisateur donné. Reportez-vous à la section « Détermination de la règle s'appliquant à un utilisateur », page 121.

Définition du mot de passe universel pour un utilisateur

Pour permettre aux administrateurs ou au service d'assistance d'attribuer un mot de passe universel à un utilisateur, iManager est fourni avec un nouveau plug-in. Ce plug-in affiche les règles de mots de passe avancées depuis la règle de mot de passe des utilisateurs afin d'aider les administrateurs ou le service d'assistance à créer un mot de passe universel conforme à ces règles. La tâche Définir le mot de passe universel est située dans le rôle Gestion des mots de passe.

Planification des règles de mot de passe

Cette section contient les informations suivantes :

- « Planification de la manière d'assigner des règles de mot de passe dans l'arborescence », page 110
- « Planification de vos règles de mot de passe », page 110
- « Planification des méthodes de login et de modification des mots de passe de vos utilisateurs », page 111

Planification de la manière d'assigner des règles de mot de passe dans l'arborescence

Nous vous conseillons d'assigner une règle par défaut à toute l'arborescence, et d'assigner les éventuelles autres règles de mot de passe au niveau le plus élevé possible de l'arborescence afin de simplifier l'administration.

NMAS détermine quelle règle de mot de passe est en vigueur pour chaque utilisateur. Pour plus d'informations sur l'assignation des règles de mot de passe aux utilisateurs, reportez-vous à la section « Assignation de règles de mot de passe aux utilisateurs », page 120.

Planification de vos règles de mot de passe

Dans une règle de mot de passe, vous pouvez utiliser les règles de mots de passe avancées pour appliquer les règles de votre société en matière de mots de passe.

N'oubliez pas que seuls Novell Client (4.9 SP2) et la console iManager en libre-service affichent les règles de mot de passe. Si vos utilisateurs peuvent modifier leur mot de passe via le serveur LDAP ou un système connecté, vous devez rendre les règles de mot de passe accessibles aux utilisateurs afin qu'ils les respectent.

Si vous utilisez la synchronisation des mots de passe, n'oubliez pas de vérifier que tous les utilisateurs à qui vous avez assigné des règles de mot de passe correspondent aux utilisateurs que vous souhaitez voir participer à la synchronisation des mots de passe entre les systèmes connectés. Les règles de mot de passe sont assignées dans une perspective centrée sur l'arborescence. Par opposition, la synchronisation des mots de passe est définie par pilote et par serveur. Pour que la synchronisation des mots de passe donne les résultats escomptés, vérifiez que les utilisateurs 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 règles de mot de passe en activant le mot de passe universel. L'assignation d'une règle de mot de passe au conteneur racine d'une partition garantit que cette règle s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

Planification des méthodes de login et de modification des mots de passe de vos utilisateurs

Un utilisateur peut se loguer ou modifier un mot de passe de plusieurs façons différentes.

Dans tous les cas, vous devez mettre à niveau votre environnement vers eDirectory 8.7.1 ou une version ultérieure, avec le serveur LDAP associé, NMAS 2.3 ou une version ultérieure et iManager 2.0.2 ou une version ultérieure. Pour plus d'informations sur la mise à niveau nécessaire pour la prise en charge du mot de passe universel, reportez-vous à la section Deploying Universal Password (Déploiement du mot de passe universel) du *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html).

Cette section explique les exigences supplémentaires nécessaires à la prise en charge du mot de passe universel dans chaque cas.

- « Novell Client », page 111
- « iManager et la console iManager en libre-service », page 113
- « Autres protocoles tels que LDAP », page 113
- « Systèmes connectés », page 113

Novell Client

Si vous utilisez Novell Client, mettez-le à niveau vers la version 4.9 SP2 ou ultérieure.

N'oubliez pas qu'il n'est pas nécessaire d'utiliser Novell Client ; en effet, en fonction de votre environnement, les utilisateurs peuvent se loguer via la console iManager en libre-service ou par l'intermédiaire d'autres portails de sociétés. En outre, Novell Client n'est plus nécessaire pour synchroniser les mots de passe sur AD ou NT.

Le tableau suivant décrit les différences entre les versions de Novell Client en ce qui concerne le mot de passe universel, et donne des suggestions relatives à la gestion des clients Novell hérités.

Version de Novell Client	Login	Modification du mot de passe
antérieure à 4.9	Ne passe pas par NMAS, et ne prend donc pas en charge le mot de passe universel. Se logue directement en utilisant le mot de passe NDS.	Modifie directement le mot de passe NDS, sans passer par NMAS. Si vous utilisez le mot de passe universel, cela peut générer un problème appelé dérive du mot de passe, qui fait que le mot de passe NDS et le mot de passe universel ne sont pas synchronisés. Pour éviter ce problème, vous avez trois possibilités : ◆ Mettez à niveau tous les clients vers la version 4.9 ou ultérieure. ◆ Empêchez les clients hérités de modifier leur mot de passe, en utilisant une valeur d'attribut sur un conteneur. Avec cette solution, les clients hérités peuvent toujours se connecter, mais ils ne peuvent pas modifier leur mot de passe. La modification des mots de passe doit être réalisée en utilisant une version ultérieure de Novell Client ou d'iManager. Reportez-vous à la section « Pour empêcher les clients hérités de modifier leur mot de passe », page 114. ◆ Utilisez les paramètres de la règle de mot de passe. Supprimez le mot de passe NDS lorsque vous définissez le mot de passe universel. Cette solution est la plus drastique car elle empêche à la fois le login et la modification des mots de passe via le mot de passe NDS.
4.9	Prend en charge le mot de passe universel.	Applique les règles de mot de passe au mot de passe universel. Si un utilisateur tente de créer un mot de passe non conforme, cette modification est rejetée. Toutefois, la liste des règles n'apparaît pas à l'utilisateur.
4.9 SP2	Prend en charge le mot de passe universel.	Applique les règles de mot de passe au mot de passe universel. De plus, dans cette version, les règles s'affichent afin d'aider l'utilisateur à créer un mot de passe conforme.

iManager et la console iManager en libre-service

La console iManager en libre-service propose des options de mot de passe en libre-service permettant aux utilisateurs de réinitialiser leur mot de passe et de configurer l'option en libre-service Mot de passe oublié si la règle de mot de passe l'autorise. La console iManager en libre-service est accessible aux utilisateurs de votre serveur iManager via une URL telle que https://www.*nom_du_serveur*.com/nps. Par exemple, https://www.myiManager.com/nps.

- Vérifiez que les utilisateurs disposent d'un navigateur prenant en charge iManager 2.0.2 ou une version ultérieure.
- Dans vos règles de mot de passe, nous vous conseillons de sélectionner l'option Synchroniser le mot de passe NDS lors de la définition du mot de passe universel. Il s'agit de la configuration par défaut.
- Vérifiez que la méthode de login par mot de passe simple NMAS est installée. Vous pouvez l'installer en même temps qu'eDirectory, ou manuellement ultérieurement.

Autres protocoles tels que LDAP

Comme indiqué plus haut, vérifiez que eDirectory, le serveur LDAP, NMAS et iManager sont mis à niveau pour prendre en charge le mot de passe universel.

Pour plus d'informations sur l'utilisation d'AFP, de CIFS et des autres protocoles avec le mot de passe universel, reportez-vous à la section Deploying Universal Password (Déploiement du mot de passe universel) dans le *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html).

Systèmes connectés

Si vous utilisez la synchronisation des mots de passe sous Identity Manager, vérifiez que les exigences suivantes sont satisfaites afin que les utilisateurs puissent modifier leur mot de passe sans problème.

- Le pilote DirXML du système a été mis à niveau au format Identity Manager.
- La configuration du pilote DirXML inclut les nouvelles règles de synchronisation des mots de passe, décrites aux sections « Nouvelle configuration de pilote et synchronisation des mots de passe sous Identity Manager », page 194 et « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.
- Les paramètres de synchronisation des mots de passe spécifient que le mot de passe universel doit être utilisé, ainsi qu'un mot de passe de distribution si la synchronisation bidirectionnelle des mots de passe est souhaitée.
- Des filtres de mots de passe ont été déployés sur le système connecté pour capturer les mots de passe, si nécessaire.

Pour plus d'informations, reportez-vous au Chapitre 9, « Synchronisation de mot de passe sur des systèmes connectés », page 165.

Pour empêcher les clients hérités de modifier leur mot de passe

Dans les versions de Novell Client antérieures à 4.9, le login et les modifications de mots de passe sont directement transmis au mot de passe NDS et non pas à NMAS. Le mot de passe universel n'est donc pas pris en charge.

Si vous utilisez le mot de passe universel, la modification des mots de passe des clients hérités peut générer un problème appelé dérive du mot de passe, qui fait que le mot de passe NDS et le mot de passe universel ne sont pas synchronisés.

Pour éviter cela, vous devez empêcher les clients des versions antérieures à 4.9 de changer leur mot de passe. Vous devez alors utiliser un attribut eDirectory sur le conteneur racine d'une partition, sur une classe ou sur un objet. Ces attributs font partie du schéma d'eDirectory 8.7.1 ou d'une version ultérieure, et ne sont pas pris en charge par eDirectory 8.7.0 ou une version antérieure.

La méthode utilisée par les clients hérités pour modifier le mot de passe NDS est appelée gestion des mots de passe NDAP. La liste suivante explique comment utiliser un attribut pour désactiver la gestion des mots de passe NDAP au niveau de la partition. Si nécessaire, vous pouvez toujours l'activer par classe ou par objet, en utilisant d'autres attributs.

- **ndapPartitionPasswordMgmt :** pour les conteneurs au niveau de la partition. Si cet attribut est absent ou si sa valeur n'est pas définie au niveau de la partition, la gestion des mots de passe NDAP est activée.

  Pour désactiver la gestion des mots de passe NDAP, ajoutez cet attribut à la partition et définissez-le sur 0. Pour la réactiver, définissez l'attribut sur 1.

  Vous pouvez utiliser les autres attributs listés ci-dessous pour laisser les classes ou les objets utiliser la gestion des mots de passe NDAP même si elle est désactivée au niveau de la partition. Toutefois, si la gestion des mots de passe NDAP est activée au niveau de la partition, elle l'est également pour tous les objets de cette partition, quelles que soient leur classe et les règles de niveau d'entrée.

- **ndapClassPasswordMgmt :** pour une classe. Si vous ajoutez cet attribut à la définition d'une classe, cette classe peut utiliser la gestion des mots de passe NDAP même si la règle au niveau de la partition spécifie que cette gestion est désactivée. La présence de cet attribut active la gestion des mots de passe NDAP. Sa valeur n'a aucune importance.

- **ndapPasswordMgmt :** pour un objet spécifique. Si vous ajoutez cet attribut à un objet spécifique et si vous définissez sa valeur sur 1, l'objet peut utiliser la gestion des mots de passe NDAP même si la partition ou la classe spécifie que cette gestion est désactivée.

  Si vous définissez la valeur sur 0, la gestion des mots de passe NDAP est désactivée, mais uniquement si elle l'est également au niveau de la partition.

Important : rappelez-vous que eDirectory 8.7.0 ou une version antérieure ne prend pas en charge cette fonction. Si un serveur eDirectory 8.7.1 ou une version ultérieure et un serveur eDirectory 8.7.0 ou une version antérieure co-existent dans une arborescence, et si les deux serveurs partagent la même partition, la désactivation de la gestion des mots de passe NDAP risque d'engendrer des problèmes de fiabilité. Le serveur 8.7.1 applique les paramètres définis et empêche les clients hérités de modifier le mot de passe NDS. Toutefois, le serveur 8.7.0 n'applique pas les paramètres définis. Si un utilisateur tente de modifier le mot de passe NDS depuis le serveur 8.7.0, la modification reste donc possible.

Conditions requises pour utiliser les règles de mot de passe

Pour profiter pleinement de toutes les fonctions des règles de mot de passe, vous devez préparer votre environnement en effectuant les étapes suivantes.

1. Mettez à niveau votre environnement afin qu'il prenne en charge le mot de passe universel.

   Pour plus d'informations, reportez-vous à la section Deploying Universal Password (Déploiement du mot de passe universel) du *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html).

   Si vous n'êtes pas encore prêt à déployer le mot de passe universel, ou si vous utilisiez eDirectory 8.6.2, recherchez les règles de mot de passe que vous pouvez appliquer sans mot de passe universel à la section « Prise en charge des fonctionnalités pour eDirectory 8.6.2 et eDirectory 8.7.3 », page 313.

2. Mettez à niveau votre environnement client afin qu'il prenne en charge le mot de passe universel.

   Reportez-vous aux sections « Planification des méthodes de login et de modification des mots de passe de vos utilisateurs », page 111 et Deploying Universal Password (Déploiement du mot de passe universel) du *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html).

3. Si vous n'avez pas exécuté l'assistant de configuration iManager lorsque vous avez configuré iManager (que ce soit pendant ou après son installation), vous devez le faire.

   Important : après avoir exécuté l'assistant de configuration iManager, iManager s'exécute en mode RBS. Cela signifie que les administrateurs ne peuvent pas voir les tâches, sauf s'ils se sont assigné des rôles spécifiques. Vérifiez que vous avez assigné aux administrateurs des rôles leur permettant d'accéder à toutes les taches iManager.

4. Installez Identity Manager, comme expliqué au Chapitre 4, « Installation », page 51.

   Les plugs-in de gestion des mots de passe font partie de cette installation sur le serveur Web iManager.

   Pour les règles de mot de passe, aucune modification de la configuration des pilotes n'est nécessaire, sauf si vous utilisez la fonction de synchronisation des mots de passe pour appliquer les règles de mot de passe lors de la synchronisation des mots de passe entre Identity Manager et les systèmes connectés.

5. Vérifiez que SSL est configuré entre le serveur Web iManager et eDirectory, même si ceux-ci s'exécutent sur le même ordinateur.

   Cette étape est indispensable pour NMAS 2.3 ou une version ultérieure et pour l'Étape 6.

6 Vérifiez que l'objet Groupe de serveur LDAP d'eDirectory est configuré pour exiger TLS en cas de liaison simple.

Il s'agit de la configuration par défaut lorsque vous configurez iManager. Le fait d'exiger TLS en cas de liaison simple est fortement recommandé pour la fonctionnalité de mot de passe en libre-service et est nécessaire pour utiliser la tâche iManager, Gestion des mots de passe > Définir le mot de passe universel.

Si vous exigez TLS en cas de liaison simple, aucune configuration supplémentaire du port SSL LDAP n'est nécessaire.

Important : si vous choisissez de ne pas exiger TLS en cas de liaison simple, tous les utilisateurs sont autorisés à se loguer à la console iManager en libre-service en utilisant un mot de passe en texte clair.

Vous pouvez utiliser cette option, mais une autre étape est nécessaire.

Par défaut, la fonctionnalité de mot de passe en libre-service suppose que le port SSL LDAP est le port spécifié dans le paramètre System.DirectoryAddress du fichier PortalServlet.properties. Si vous utilisez un autre port SSL LDAP, vous devez indiquer le port approprié en ajoutant la paire de clés suivante au fichier PortalServlet.properties :

LDAPSSLPort=numéro_de_votre_port

Par exemple, si vous exécutez Tomcat, vous devez ajouter cette paire de clés au fichier PortalServlet.properties dans le répertoire tomcat\webapps\nps\WEB_INF.

7 Pour activer la notification par message électronique des fonctions Mot de passe oublié, suivez les étapes indiquées à la section « Configuration de la notification par message électronique », page 243.

Vous devez configurer le serveur SMTP et personnaliser les modèles de messages électroniques.

8 (NetWare 6.5 uniquement) Si vous avez déjà configuré le mot de passe universel pour l'utiliser avec NetWare 6.5, suivez les étapes indiquées à la section « (NetWare 6.5 uniquement) Nouvelle création des assignations du mot de passe universel », page 117.

Vous êtes maintenant prêt à utiliser toutes les fonctionnalités proposées par les règles de mot de passe. Créez les règles comme indiqué à la section « Création de règles de mot de passe », page 119.

Déploiement des règles de mot de passe sans mot de passe universel

Nous vous recommandons de préparer votre environnement et d'activer le mot de passe universel afin de pouvoir utiliser toutes les fonctionnalités proposées par les règles de mot de passe et la synchronisation des mots de passe. Toutefois, si vous ne souhaitez pas déployer le mot de passe universel, un certain nombre de ces fonctionnalités peuvent être utilisées quand même.

Pour en connaître la liste, reportez-vous à la section « Prise en charge des fonctionnalités pour eDirectory 8.6.2 et eDirectory 8.7.3 », page 313. Elle indique les fonctions que vous pouvez utiliser avec eDirectory 8.6.2 ou eDirectory 8.7.3 lorsque le mot de passe universel n'est pas activé.

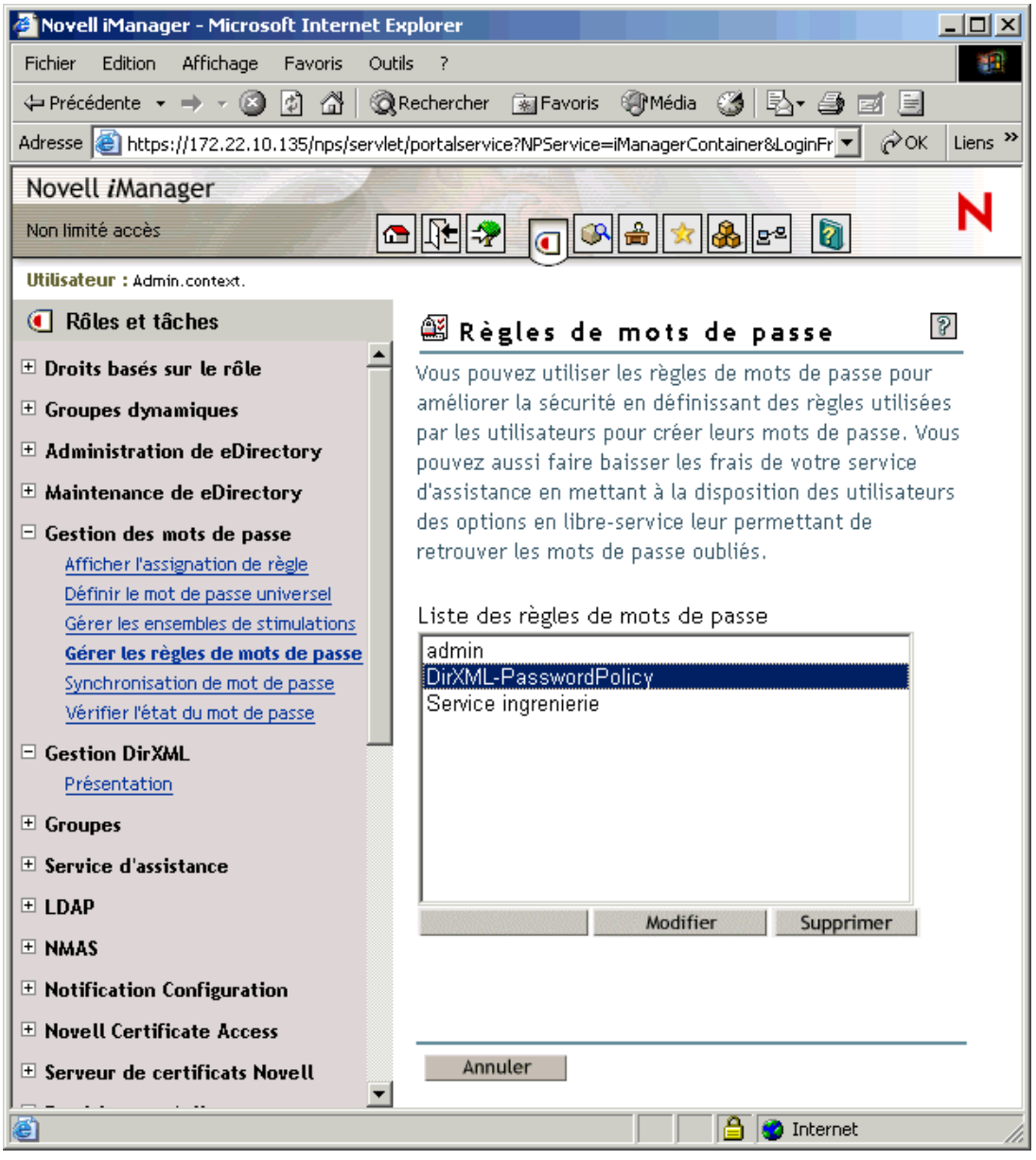
(NetWare 6.5 uniquement) Nouvelle création des assignations du mot de passe universel

Si vous avez déjà configuré le mot de passe universel pour l'utiliser avec NetWare 6.5, vous devez supprimer les anciennes règles de mot de passe et utiliser les nouveaux plugs-in et les nouvelles règles de mot de passe.

- Après avoir installé Identity Manager, les plugs-in NMAS qui étaient précédemment utilisés par NetWare 6.5 pour le mot de passe universel ne sont plus disponibles. Utilisez maintenant l'option Gestion des mots de passe > Gérer les règles de mots de passe, qui vous offre plus de possibilités.
- La première fois que vous utilisez la gestion des règles de mots de passe avec les nouveaux plugs-in, trois objets Règle s'affichent dans une liste qui ne peut pas être modifiée :
  - Mot de passe universel activé
  - Mot de passe universel désactivé
  - Mot de passe universel activé - S

  Ces objets étaient utilisés pour la mise en œuvre par NetWare 6.5 du mot de passe universel. Vous devez les supprimer pour profiter des avantages des fonctionnalités supplémentaires proposées par les règles de mot de passe d'Identity Manager.

L’illustration suivante en présente un exemple :



Pour supprimer les anciens objets Règle et recréez vos propres règles à l’aide des règles de mot de passe :

1. Décidez à quel endroit vous souhaitez activer le mot de passe universel dans votre arborescence.
   - Si vous souhaitez l’activer pour les mêmes conteneurs que ceux pour lesquels vous avez configuré pour la première fois le mot de passe universel avec les plugs-in NetWare 6.5, passez à l’Étape 2.
   - Si vous souhaitez l’activer partout dans l’arborescence, il suffit de créer une nouvelle règle de mot de passe avec le mot de passe universel activé et de l’assigner à l’objet Règle de login. Passez ensuite à l’Étape 4 pour supprimer les anciennes règles.

2 Recherchez dans l'arborescence les emplacements sur lesquels vous aviez précédemment activé le mot de passe universel lorsque vous l'aviez configuré en utilisant les plugs-in fournis avec NetWare 6.5.

   Cette étape est nécessaire car les plugs-in n'affichent pas les emplacements sur lesquels ont été placées les assignations réalisées par l'intermédiaire des anciens plugs-in. Vous devez donc effectuer cette recherche dans l'arborescence.

   2a Recherchez dans l'arborescence les objets possédant l'attribut nspmPasswordPolicyDN contenant l'une des valeurs suivantes :

   - Mot de passe universel activé
   - Mot de passe universel activé - S

   2b Notez tous les conteneurs obtenus suite à cette recherche. Ce sont les conteneurs pour lesquels le mot de passe universel est activé.

3 Si vous souhaitez que le mot de passe universel soit assigné aux mêmes conteneurs que précédemment, créez une ou plusieurs règles de mot de passe avec le mot de passe universel activé et assignez-les aux mêmes conteneurs.

   Reportez-vous à la liste de conteneurs indiquée à l'Étape 2 pour vérifier que vos assignations correspondent.

4 Allez dans Gestion des mots de passe > Gérer les règles de mot de passe et supprimez les objets Règle restant de la première mise en œuvre de NetWare 6.5.

   - Mot de passe universel désactivé
   - Mot de passe universel activé
   - Mot de passe universel activé - S

Après avoir supprimé les anciens objets Règle, utilisez les nouvelles règles de mot de passe pour répondre à vos besoins en matière de mots de passe.

Création de règles de mot de passe

1 Vérifiez que vous avez suivi les étapes indiquées à la section « Conditions requises pour utiliser les règles de mot de passe », page 115. Elles vous préparent à utiliser toutes les fonctionnalités proposées par les règles de mot de passe.

2 Dans iManager, cliquez sur Gestion des mots de passe > Gérer les règles de mot de passe.

3 Cliquez ensuite sur Nouveau pour créer une nouvelle règle de mot de passe.

4 Suivez les instructions de l'assistant pour créer les options Règles de mots de passe avancées et Configuration du mot de passe universel, et pour sélectionner les règles de l'option Mot de passe oublié.

   Consultez l'aide en ligne pour plus d'informations sur chacune des étapes à suivre, ainsi que le Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101 et le Chapitre 8, « Mot de passe en livre service », page 125.

Assignation de règles de mot de passe aux utilisateurs

Nous vous encourageons à assigner des règles de mot de passe au niveau le plus élevé possible de l'arborescence afin de simplifier l'administration.

Une règle n'entre pas en vigueur tant que vous ne lui avez pas assigné un ou plusieurs objets. Vous pouvez assigner une règle de mot de passe aux objets suivants :

- Objet Règle de login

  Nous vous recommandons de créer une règle de mot de passe par défaut pour tous les utilisateurs de l'arborescence. Pour ce faire, créez une règle et assignez-la à l'objet Règle de login. L'objet Règle de login est situé dans le conteneur Sécurité, juste en dessous de la racine de l'arborescence.

- Conteneur racine d'une partition

  Si vous assignez une règle au conteneur racine d'une partition, tous les utilisateurs de cette partition, y compris ceux des sous-conteneurs, héritent de l'assignation de cette règle. Pour déterminer si un conteneur est la racine d'une partition, recherchez-le dans l'arborescence et regardez si une icône de partition s'affiche à côté de lui, comme dans l'exemple suivant.

- Conteneur n'étant pas la racine d'une partition

  Si vous assignez une règle à un conteneur n'étant pas la racine d'une partition, seuls les utilisateurs contenus dans ce conteneur spécifique héritent de l'assignation de cette règle. Les utilisateurs des sous-conteneurs n'héritent pas de cette assignation. Si vous souhaitez que la règle s'applique à tous les utilisateurs situés en aval d'un conteneur n'étant pas la racine d'une partition, assignez-la règle à chaque sous-conteneur.

- Utilisateur spécifique

Remarque : des règles de mot de passe spéciales sont automatiquement créées pour les objets Ensemble de pilotes.

Une seule règle peut s'appliquer à la fois à un utilisateur donné. NMAS (Novell Modular Authentication Services) détermine la règle en vigueur pour un utilisateur, en recherchant les règles dans cet ordre suivant et en appliquant la première règle trouvée.

1. Assignation à un utilisateur spécifique : si une règle de mot de passe a été assignée spécifiquement à un utilisateur, cette règle est appliquée.
2. Conteneur : si l'utilisateur ne bénéficie d'aucune assignation spécifique, NMAS applique la règle assignée au conteneur renfermant cet utilisateur.
3. Conteneur racine de partition : si aucune règle n'est assignée à l'utilisateur ou si le conteneur est situé directement en amont de l'utilisateur, la règle assignée au conteneur racine de partition est appliquée.
4. Objet Règle de login : si aucune règle n'est assignée à l'utilisateur ou aux autres conteneurs, la règle assignée à l'objet Règle de login est appliquée. Il s'agit de la règle par défaut de tous les utilisateurs de l'arborescence.

Détermination de la règle s'appliquant à un utilisateur

Une seule règle peut s'appliquer à la fois à un utilisateur donné. Pour déterminer quelle règle est en vigueur pour un utilisateur ou un conteneur particulier, allez dans iManager > Gestion des mots de passe > Afficher l'assignation de règle.

Si l'arborescence comporte plusieurs règles, NMAS détermine quelle règle s'applique à un utilisateur donné, comme décrit à la section « Assignation de règles de mot de passe aux utilisateurs », page 120.

Définition du mot de passe d'un utilisateur

Les administrateurs ou le service d'assistance peuvent définir le mot de passe universel d'un utilisateur grâce à une nouvelle tâche iManager. Cette tâche affiche les règles de mot de passe en vigueur pour l'utilisateur.

1. Dans iManager, cliquez sur Gestion des mots de passe > Définir le mot de passe universel.

   Si une règle de mot de passe est assignée à un utilisateur et si le mot de passe universel est activé, vous êtes autorisé à modifier le mot de passe en utilisant cette tâche.

   Si les règles de mots de passe avancées sont activées dans la règle, la liste des règles à respecter s'affiche.

   Remarque : si le mot de passe universel n'est pas activé pour un utilisateur donné, la tâche de définition du mot de passe avancé affiche un message d'erreur et le mot de passe n'est pas modifié. Vous devez assigner une règle à l'utilisateur puis revenir à cette tâche ou modifier le mot de passe DNS de l'utilisateur via la tâche Administration eDirectory> Modifier l'objet.

2. Créez un mot de passe pour cet utilisateur, en vérifiant qu'il est conforme aux règles de mot de passe affichées.

   Le mot de passe universel de cet utilisateur est alors modifié.

   Si la synchronisation des mots de passe est configurée dans votre environnement, le nouveau mot de passe de l'utilisateur est distribué aux systèmes connectés configurés pour l'accepter.

Remarque : une fonction d'amélioration de la sécurité a été ajoutée à NMAS 2.3.4 en ce qui concerne 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, pour des raisons de sécurité, le mot de passe précédent expire automatiquement si vous avez activé le paramètre d'expiration des mots de passe dans la règle des 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.

Création ou modification des ensembles de stimulations

Reportez-vous à la section « Création ou modification des ensembles de stimulations », page 153.

Configuration des notifications relatives aux fonctions de mots de passe

Suivez les instructions de la section « Configuration de la notification par message électronique », page 243.

Dépannage des problèmes de règles de mot de passe

- Login iManager en libre-service nécessitant un DN complet : vous pouvez être invité à saisir un DN complet au moment du login si l'objet Utilisateur ne réside pas dans le conteneur spécifié durant la configuration d'iManager/du portail. Vous devez exécuter l'assistant de configuration de la servlet de portail (http://*votre_serveur_iManager*/nps/servlet/), et spécifier les conteneurs de login supplémentaires des logins sans contexte. La fonction Mot de passe oublié utilise également ce paramètre pour résoudre les DN des utilisateurs.
- Erreurs liées à la non-assignation d'une règle de mot de passe à un utilisateur : si un message d'erreur s'affiche indiquant qu'aucune règle de mot de passe n'est assignée à un utilisateur donné dans la tâche Définir le mot de passe universel et si vous savez pertinemment qu'une règle de mot de passe est assignée à cet utilisateur, SSL est probablement la cause du problème.
  - Pour vous aider à confirmer qu la configuration SSL est la source du problème, utilisez la tâche Afficher l'assignation de règle pour savoir quelle est la règle applicable à cet utilisateur. Si la tâche Afficher l'assignation de règle affiche une erreur de transport NMAS, cela peut également indiquer que SSL n'est pas configuré correctement.
  - Vérifiez que SSL est configuré correctement entre le serveur Web exécutant iManager et l'arborescence iManager primaire. Vérifiez qu'un certificat est configuré entre le serveur Web et eDirectory.

    Cela peut poser un problème si vous exécutez iManager sur un ordinateur Windows 2000 avec IIS en tant que serveur Web, car l'installation de iManager ne configure pas automatiquement le certificat pour vous dans ce scénario.
  - Si vous n'exigez pas TLS en cas de liaison simple, vérifiez que vous avez indiqué le bon port SSL LDAP, comme expliqué dans la remarque de l'Étape 6 à la section « Conditions requises pour utiliser les règles de mot de passe », page 115.
- Utilisation des questions de stimulation-réponse : vérifiez que vous utilisez un navigateur pris en charge par iManager 2.0.2.
- Accès pour les utilisateurs appartenant à de nouveaux conteneurs : lorsque vous configurez iManager ou l'un des portails de Novell tel que exteNd™ Director™ Standard Edition, vous devez spécifier le conteneur des utilisateurs du portail. La spécification du conteneur se fait généralement à un niveau élevé de l'arborescence, de façon à ce que tous les utilisateurs de l'arborescence puissent accéder aux fonctions du portail. Si tous vos utilisateurs sont situés en aval de ce conteneur, tous auront accès aux options en libre-service Mot de passe oublié et Réinitialiser le mot de passe.

  Si vous créez ensuite un conteneur dont certains utilisateurs sont situés en dehors du conteneur des utilisateurs du portail, et si ces utilisateurs ne peuvent pas accéder aux options Mot de passe oublié et Réinitialiser le mot de passe, vous devez assigner spécifiquement des droits aux gadgets suivants pour le nouveau conteneur créé : Définition de la stimulation-réponse, Changer le mot de passe universel et Configuration de l'indice.

  Pour plus d'informations sur l'ajout de nouveaux utilisateurs au conteneur des utilisateurs du portail, reportez-vous à la section Portal User (Utilisateurs du portail) du *Novell exteNd Director Platform Edition Installation and Configuration Guide (Guide d'installation et de configuration de Novell exteNd Director Platform Edition)* (http://www.novell.com/documentation/fr-fr/nedpe41/configure/data/ajhotzv.html#ajhotzv).

- Erreur de transport LDAP NMAS : si vous installez iManager dans un environnement multiserveur, et si vous utilisez certains des plugs-in de gestion des mots de passe de iManager, un message d'erreur commençant par Erreur de transport LDAP NMAS peut s'afficher.

  La cause la plus fréquente de cette erreur est que le fichier PortalServlet.properties pointe sur un serveur LDAP ne possédant pas les extensions NMAS™ nécessaires à Identity Manager. Ouvrez le fichier PortalServlet.properties et vérifiez que l'adresse du serveur LDAP est celle du serveur sur lequel vous avez installé Identity Manager.

  Autres causes possibles :

  - Le serveur LDAP n'est pas en cours d'exécution.
  - SSL n'est pas configuré pour LDAP entre le serveur iManager exécutant les plugs-in et le serveur LDAP.
  - Lorsque vous vous connectez à d'autres arborescences avec iManager pour gérer les serveurs DirXML d'Identity Manager distants, vous pouvez rencontrer des erreurs si vous utilisez le nom du serveur au lieu de l'adresse IP du serveur distant.
  - Le certificat racine approuvé de l'arborescence que vous avez authentifiée doit être importé en tant que certificat approuvé dans le serveur Web. Vous pouvez utiliser keytool.exe pour exporter ce certificat vers le serveur Web. Si vous installez eGuide, le certificat est exporté vers le serveur Web lors du processus de configuration.
  - L'objet Groupe du serveur LDAP d'eDirectory doit être configuré pour exiger TLS en cas de liaison simple. Cette option peut être sélectionnée en modifiant les propriétés de l'objet Serveur LDAP dans iManager.

- Si vous utilisez la synchronisation des mots de passe sous Identity Manager, reportez-vous également à :
  - « Dépannage des problèmes de synchronisation des mots de passe », page 258.
  - Les sections relatives au dépannage des différents scénarios à la section « Mise en œuvre de la synchronisation des mots de passe », page 202.
  - La documentation relative aux pilotes spécifiques utilisés sur le site Web de documentation sur les pilotes. (http://www.novell.com/documentation/fr-fr/dirxmldrivers)

8 Mot de passe en livre service

Grâce aux règles de mot de passe, vous pouvez aussi réduire les coûts du service d'assistance en fournissant aux utilisateurs des options en libre-service pour les mots de passe oubliés et pour la réinitialisation des mots de passe.

Avant d'utiliser les options de mot de passe en libre-service, revoyez les informations relatives aux règles de mot de passe dans le Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101.

Cette section contient les informations suivantes :

Présentation des options en libre-service

Les règles de mot de passe incluent les options en libre-service Mot de passe oublié, qui permet de réduire les appels d'assistance liés à l'oubli des mots de passe, et Réinitialiser le mot de passe, qui permet aux utilisateurs de modifier leur mot de passe tout en affichant les règles définies par l'administrateur dans la règle de mot de passe. Les utilisateurs peuvent accéder à ces options par l'intermédiaire de la console iManager en libre-service.

La plupart des fonctions de gestion des mots de passe nécessitent que l'option Mot de passe universel soit activée. Idéalement, la console iManager en libre-service doit être intégrée au portail de votre société, afin que les utilisateurs accède facilement aux options en libre-service Mot de passe oublié et Réinitialiser le mot de passe.

Ces nouvelles options de mot de passe en libre-service permettent d'effectuer les opérations suivantes :

- « Comment fournir aux utilisateurs le libre-service Mot de passe oublié », page 105
- « Comment fournir aux utilisateurs le libre-service Réinitialiser le mot de passe », page 105

Comment fournir aux utilisateurs le libre-service Mot de passe oublié

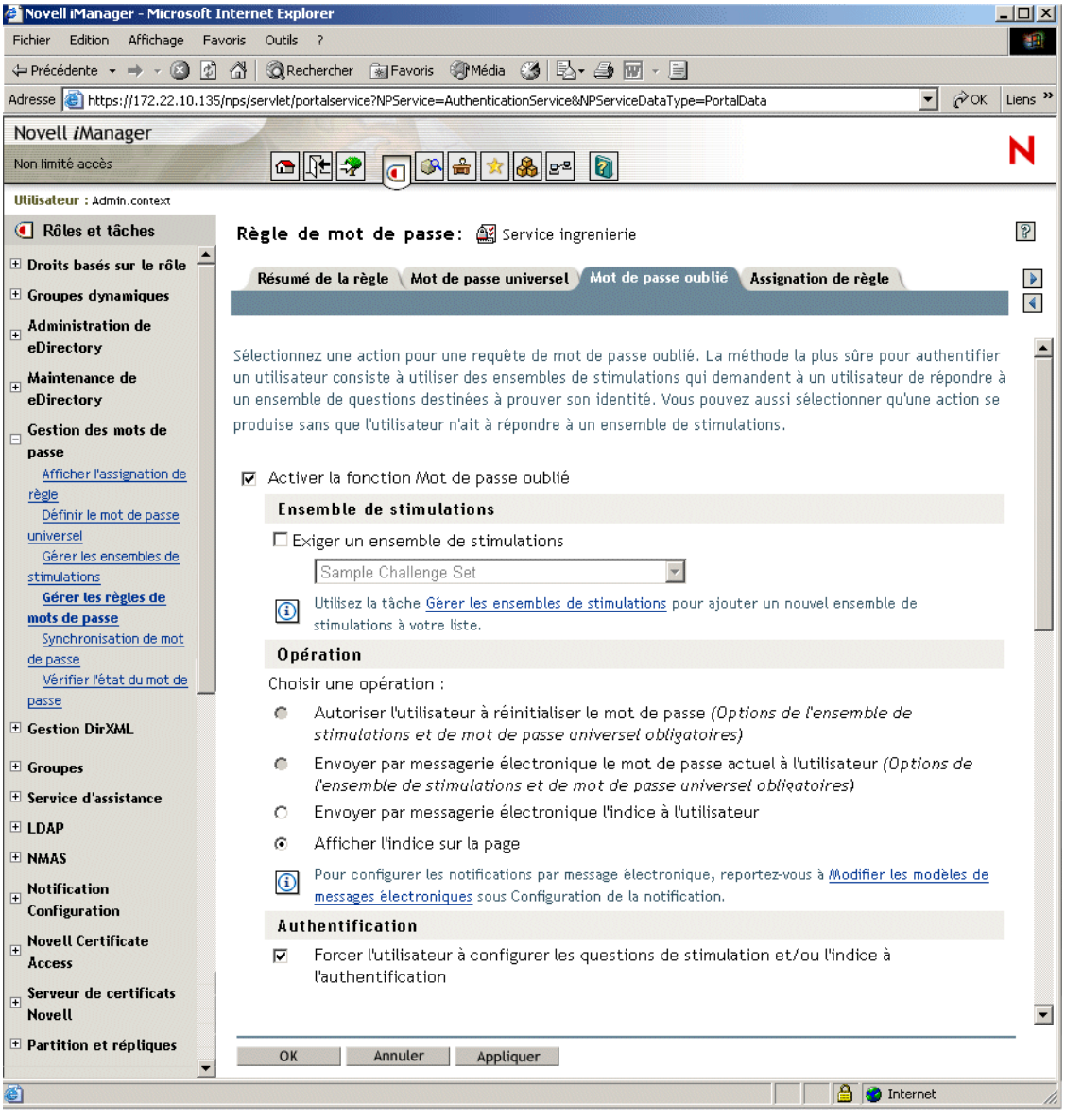
Grâce à l'utilisation d'une règle de mot de passe, vous pouvez fournir aux utilisateurs la possibilité de retrouver un mot de passe oublié sans avoir à appeler le service d'assistance. Le lien Vous avez oublié votre mot de passe ? est disponible lorsque les utilisateurs se loguent à la console iManager en libre-service.

Les fonctionnalités de l'option en libre-service Mot de passe oublié incluent les éléments suivants :

- Des ensembles de stimulations qui permettent à l'utilisateur de répondre à des questions afin de prouver son identité.
- La possibilité d'envoyer à l'utilisateur, par message électronique, un indice de mot de passe ou le mot de passe oublié.
- La possibilité pour un utilisateur de réinitialiser un mot de passe dans le navigateur lors d'une requête de mot de passe oublié.

Pour obtenir des exemples de ce que voit l'utilisateur quand il utilise le lien Vous avez oublié votre mot de passe ?, reportez-vous à la section « Comment fournir aux utilisateurs finals le libre-service Mot de passe oublié », page 129.

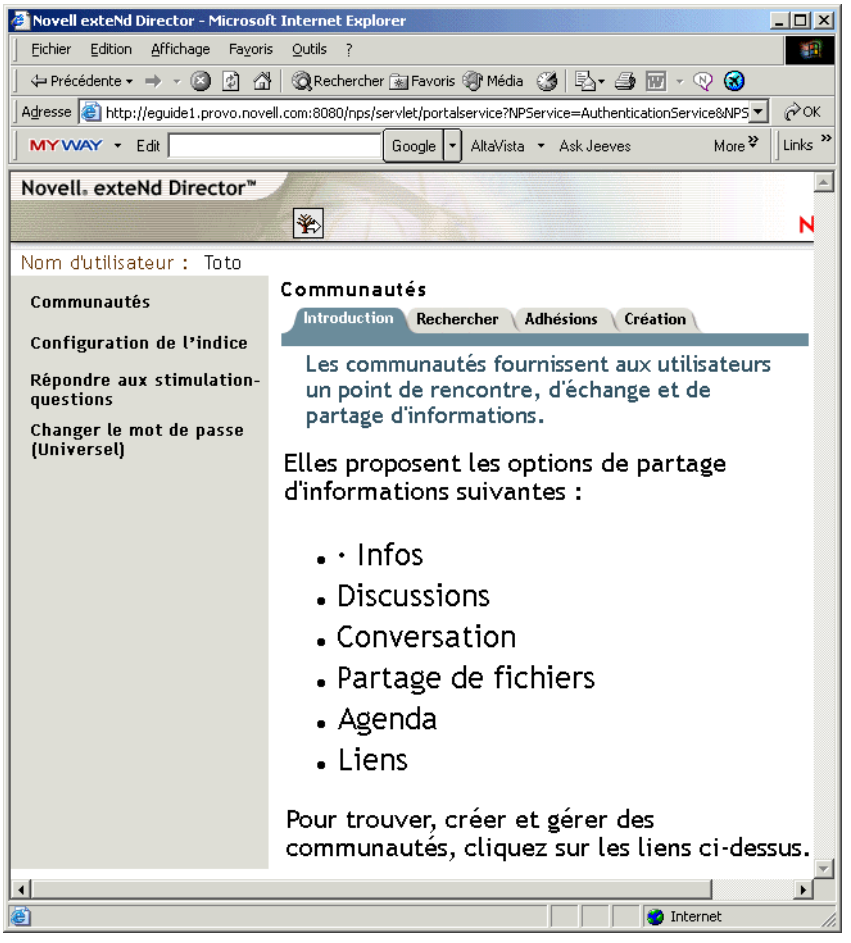
L’illustration suivante propose un exemple de la page de propriétés dans laquelle vous devez spécifier les paramètres de l’option Mot de passe oublié d’une règle de mot de passe.



Comment fournir aux utilisateurs le libre-service Réinitialiser le mot de passe

Via la console iManager en libre-service, les utilisateurs peuvent réinitialiser leur mot de passe tout en visualisant les règles de mots de passe avancées. Pour cela, ils doivent utiliser le gadget Changer le mot de passe (Universel).

Voici un exemple de l'écran qui s'affiche lorsque les utilisateurs se loguent à la console iManager en libre-service sur votre serveur Web iManager via une URL telle que https://www.*nom_du_serveur*.com/nps.



Pour obtenir des exemples de ce que voit l'utilisateur quand il utilise le lien Changer le mot de passe (Universel), reportez-vous à la section « Comment fournir aux utilisateurs finals le libre-service Mot de passe oublié », page 129.

Conditions requises pour utiliser les options de mot de passe en libre-service

Reportez-vous aux informations données dans le Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101 et respectez les conditions requises énoncées à la section « Conditions requises pour utiliser les règles de mot de passe », page 115.

Nous vous recommandons de préparer votre environnement et d'activer le mot de passe universel afin de pouvoir utiliser toutes les fonctionnalités proposées par les règles de mot de passe. Toutefois, si vous ne souhaitez pas déployer le mot de passe universel, un certain nombre de ces fonctionnalités peuvent être utilisées quand même.

Pour en connaître la liste, reportez-vous à la section « Prise en charge des fonctionnalités pour eDirectory 8.6.2 et eDirectory 8.7.3 », page 313. Elle indique les fonctions que vous pouvez utiliser avec Novell® eDirectory™ 8.6.2 ou eDirectory 8.7.3 lorsque le mot de passe universel n'est pas activé.

Planification des méthodes de login des options de mots de passe

La console iManager en libre-service est accessible aux utilisateurs de votre serveur iManager via une URL telle que https://www.*mon_serveur_iManager*.com/nps.

Mettez à niveau votre environnement client afin qu'il prenne en charge le mot de passe universel, comme décrit à la section « Planification des méthodes de login et de modification des mots de passe de vos utilisateurs », page 111.

Pour plus d'informations, reportez-vous à la section Deploying Universal Password (Déploiement du mot de passe universel) du *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html).

Comment fournir aux utilisateurs finals le libre-service Mot de passe oublié

Lorsque vous utilisez l'assistant de création d'une règle de mot de passe, une invite vous demande quelles sont les fonctions de mot de passe oublié que vous souhaitez fournir à vos utilisateurs finals.

Cette section donne des informations détaillées sur les différentes options possibles et présente des exemples de ce que voit l'utilisateur final lorsqu'il utilise le lien Vous avez oublié votre mot de passe ?.

Cette section contient les informations suivantes :

Ensembles de stimulations

Un ensemble de stimulation est un ensemble de questions auxquelles doit répondre un utilisateur pour prouver son identité au lieu d'utiliser son mot de passe. Un tel ensemble est assigné à une règle de mot de passe et sert de méthode d'authentification de règle de mot de passe. Vous pouvez proposer à vos utilisateurs les ensembles de stimulations comme option en libre-service de mot de passe oublié. Exiger qu'un utilisateur réponde aux questions d'un ensemble de stimulation avant de pouvoir recevoir son mot de passe oublié permet d'obtenir un niveau de sécurité supplémentaire. Pour utiliser un ensemble de stimulation, utilisez la tâche Gérer les règles de mot de passe pour créer une règle de mot de passe et configurer l'option Mot de passe oublié.

Lorsque vous créez une règle de mot de passe, vous pouvez activer l'option en libre-service Mot de passe oublié de façon à ce que les utilisateurs puissent obtenir de l'aide sans avoir à contacter le service d'assistance. Pour rendre les options en libre-service encore plus sûres, vous pouvez créer un ensemble de stimulation et demander à ce que les utilisateurs répondent aux questions de cet ensemble avant de pouvoir obtenir de l'aide. Vous pouvez également spécifier l'opération qui va aider les utilisateurs après qu'ils aient répondu correctement aux questions, par exemple afficher un indice de mot de passe. Ces fonctions en libre-service sont accessibles aux utilisateurs par l'intermédiaire de la console Novell iManager en libre-service. Les différents choix possibles sont décrits à la section « Opérations liées à l'option Mot de passe oublié », page 132.

La structure des questions de l'ensemble de stimulation peut être définie selon les méthodes suivantes :

Questions définies par l'administrateur : l'administrateur peut créer des questions qui seront soumises à tous les utilisateurs. Leurs réponses, quant à elles, seront uniques.

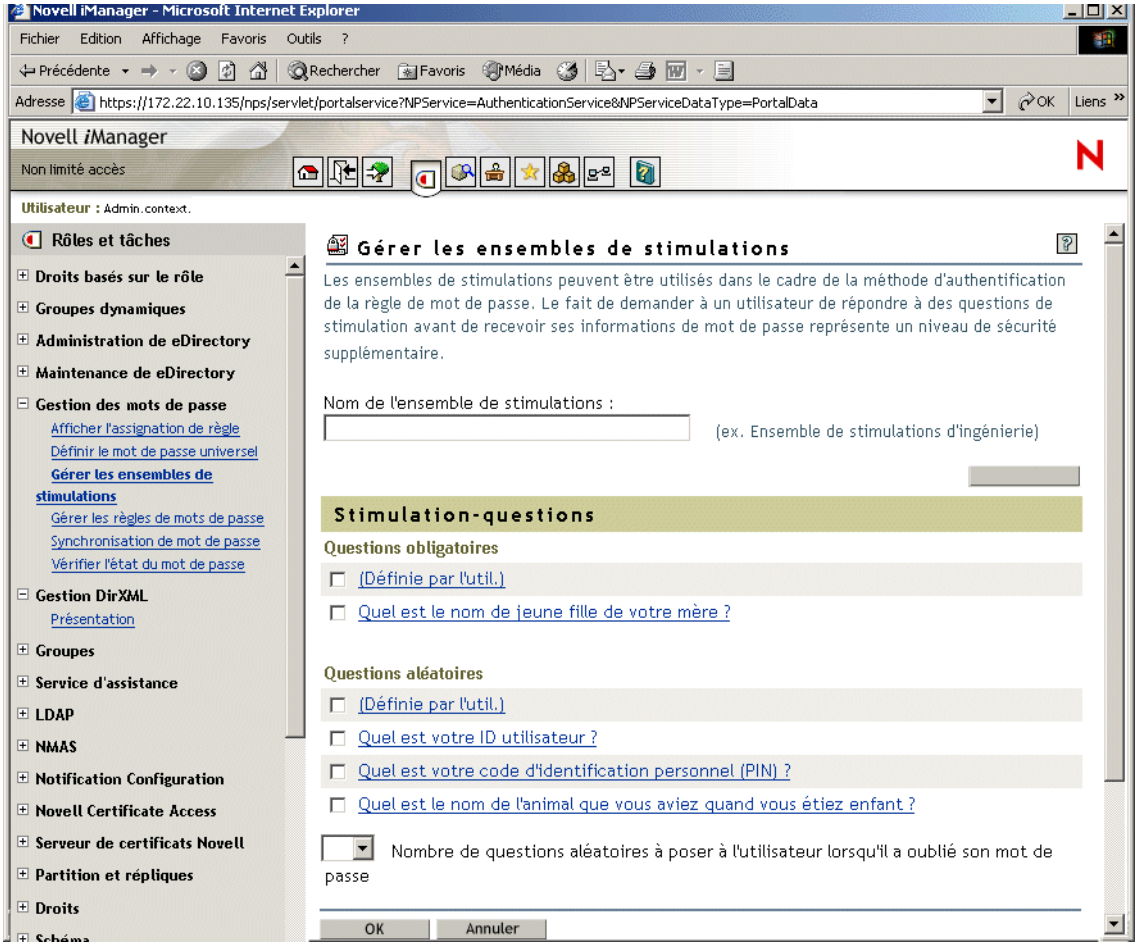
Questions définies par l'utilisateur : l'administrateur peut spécifier qu'une ou plusieurs questions soient créées par l'utilisateur. Dans ce cas, les questions et les réponses sont uniques pour chaque utilisateur.

Questions obligatoires : les questions de cette liste sont systématiquement soumises aux utilisateurs lorsqu'ils utilisent l'option en libre-service Mot de passe oublié.

Questions aléatoires : les questions de cette liste ne sont soumises qu'une seule fois aux utilisateurs dans leur intégralité, lorsqu'ils configurent l'option Mot de passe oublié en répondant pour la première fois aux questions de l'ensemble de stimulation. Lorsque l'utilisateur doit accéder au mot de passe oublié, seules quelques questions lui sont posées. Le nombre de questions aléatoires posées est déterminé par l'administrateur.

Les réponses des utilisateurs et les questions définies par l'utilisateur sont stockées dans Novell eDirectory par NMAS (Novell Modular Authentication Services).

Voici un exemple de l’écran qui s’affiche lorsque vous créez un nouvel ensemble de stimulation. Vous pouvez choisir vos questions parmi celles proposées par défaut, ou en ajouter d’autres.



Opérations liées à l'option Mot de passe oublié

Les opérations liées à l'option Mot de passe oublié qui suivent sont fournies dans une règle de mot de passe, à condition que l'option Mot de passe oublié soit activée.

- **Autoriser l'utilisateur à réinitialiser le mot de passe :** après avoir répondu aux questions de l'ensemble de stimulation pour prouver son identité, l'utilisateur est autorisé à définir un nouveau mot de passe. L'utilisateur s'étant authentifié en répondant aux stimulation-questions, il est autorisé à définir un nouveau mot de passe sans avoir à fournir l'ancien. Pour utiliser cette option, l'administrateur doit exiger un ensemble de stimulation, et l'utilisateur doit avoir au préalable configuré l'option Mot de passe oublié dans la console iManager en libre-service en répondant aux questions de stimulation.
- **Envoyer par messagerie électronique le mot de passe actuel à l'utilisateur :** après avoir répondu aux questions de l'ensemble de stimulation pour prouver son identité, l'utilisateur reçoit le mot de passe actuel par messagerie électronique. Pour utiliser cette option, l'administrateur doit activer le mot de passe universel pour la règle, activer l'option Autoriser l'agent utilisateur à récupérer le mot de passe (ces deux options se trouvent dans Mot de passe universel > Options de configuration), puis configurer la notification par courrier électronique comme décrit à la section « Configuration de la notification par message électronique », page 243. En outre, l'utilisateur doit d'abord avoir configuré l'option Mot de passe oublié dans la console iManager en libre-service en répondant aux questions de stimulation.
- **Envoyer par messagerie électronique l'indice à l'utilisateur :** l'utilisateur reçoit l'indice de son mot de passe par courrier électronique. Pour utiliser cette option, l'administrateur doit configurer la notification par courrier électronique comme décrit à la section « Configuration de la notification par message électronique », page 243, et l'utilisateur doit avoir au préalable configuré l'option Mot de passe oublié dans la console iManager en libre-service en fournissant un indice de mot de passe.
- **Afficher l'indice sur la page :** l'indice du mot de passe s'affiche sur la console iManager en libre-service. Pour utiliser cette option, l'utilisateur doit avoir au préalable configuré l'option Mot de passe oublié dans la console iManager en libre-service en fournissant un indice de mot de passe.

Indices de mots de passe

Si vous spécifiez une opération liée à l'option Mot de passe oublié et nécessitant un indice de mot de passe, l'utilisateur peut saisir un indice qui lui permettra de se souvenir de son mot de passe. Cet indice est ensuite contrôlé pour vérifier qu'il ne contient pas le mot de passe de l'utilisateur.

L'attribut Indice de mot de passe (nsimHint) est 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 largement contribuer à réduire les appels de demande d'assistance.

Pour des raisons de sécurité, les indices de mot de passe sont contrôlés pour 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.

Pour 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 de créer des indices de mots de passe qu'eux seuls peuvent comprendre. L'option Message de modification du mot de passe, dans la règle de mot de passe, est l'une des manières de le faire. Reportez-vous à la section « Ajout de votre propre message de modification du mot de passe aux règles de mot de passe », page 152.

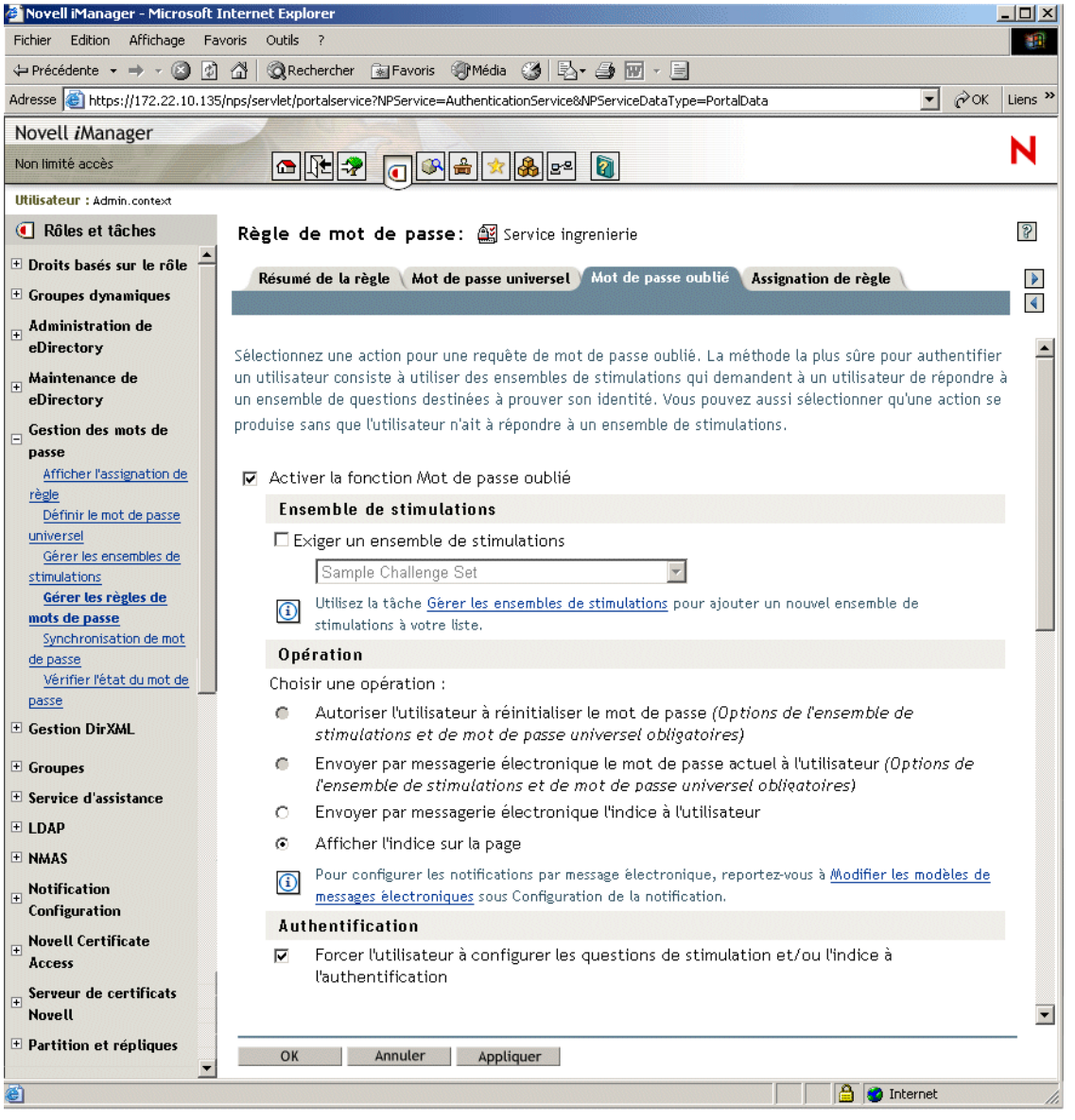
Si vous choisissez ne pas utiliser d'indice de mot de passe, vérifiez que vous ne l'utilisez dans aucune règle de mot de passe que ce soit. Pour empêcher de définir des indices de mots de passe, vous pouvez être plus radical et supprimer totalement le gadget Configuration de l'indice, comme décrit à la section « Désactivation du mot de passe par suppression du gadget Indice », page 149.

Comment inviter les utilisateurs finals à configurer l'option Mot de passe oublié

Pour certaines des opérations liées à l'option Mot de passe oublié, l'utilisateur final doit configurer un certain nombre de paramètres avant de pouvoir utiliser les options en libre-service Mot de passe oublié. Par exemple, si la règle de mot de passe spécifie qu'un ensemble de stimulation est utilisé pour permettre à un utilisateur de prouver son identité, et si l'opération préconisée est de lui envoyer un indice de mot de passe par courrier électronique, l'utilisateur devra tout d'abord répondre aux questions de l'ensemble de stimulation puis créer un indice de mot de passe avant de pouvoir utiliser les options en libre-service Mot de passe oublié.

Les utilisateurs peuvent configurer ces fonctionnalités dans la console iManager en libre-service, ou vous pouvez exiger que les utilisateurs les configurent par l'intermédiaire des services de post-authentification (dans les pages qui s'affichent lorsque les utilisateurs se loguent à la console iManager en libre-service).

Pour inviter les utilisateurs à configurer ces fonctionnalités au moment du login, sélectionnez l'option Forcer l'utilisateur à configurer les questions de stimulation et/ou l'indice à l'authentification, située dans l'interface des règles de mot de passe au bas de la page Mot de Passe oublié. Cette option est sélectionnée par défaut lors de la création d'une règle.



Pour permettre aux utilisateurs de configurer l'option Mot de passe oublié quand ils le souhaitent, vous devez leur fournir l'URL de la console iManager en libre-service, par exemple https://www.*mon_serveur_iManager*.com/nps.

Configuration des utilisateurs finals dans l'option en libre-service Mot de passe oublié

Le fait pour un utilisateur de cliquer sur le lien Vous avez oublié votre mot de passe ? au moment de son login à la console iManager en libre-service (par exemple https://www.*nom_du_serveur*.com/nps) ne mène à rien si les conditions suivantes ne sont pas satisfaites :

- L'administrateur a configuré une règle de mot de passe dans laquelle l'option Mot de passe est activée.
- L'utilisateur a configuré des stimulation-questions ou un indice de mot de passe qu'il a spécifié(es) dans les paramètres de l'option Mot de passe oublié.

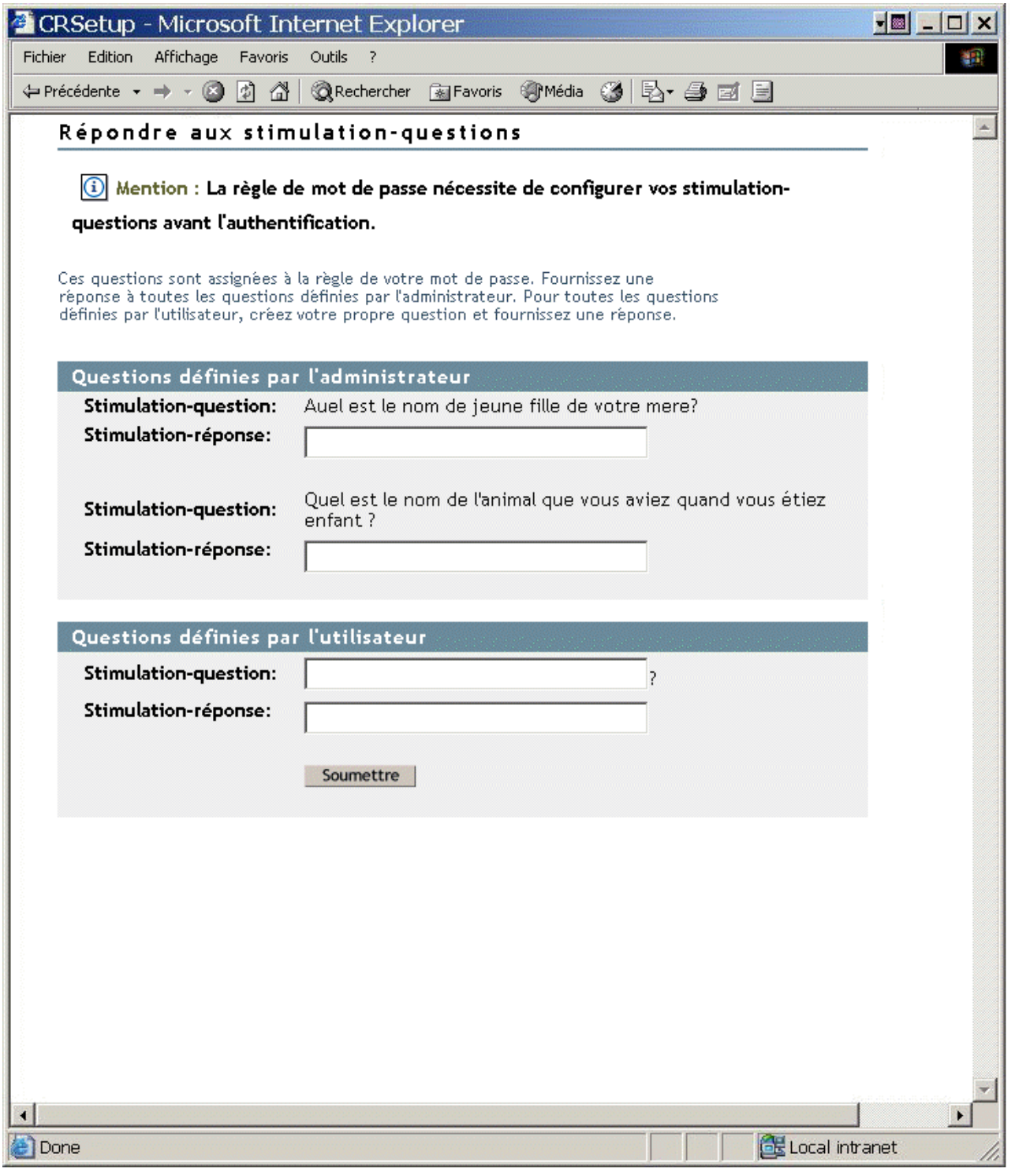
La partie de la configuration revenant à l'utilisateur peut être effectuée de deux manières :

- « Configuration par l'utilisateur de l'option Mot de passe oublié, post-authentification », page 135
- « Configuration par l'utilisateur de l'option Mot de passe oublié dans la console iManager en libre-service », page 137

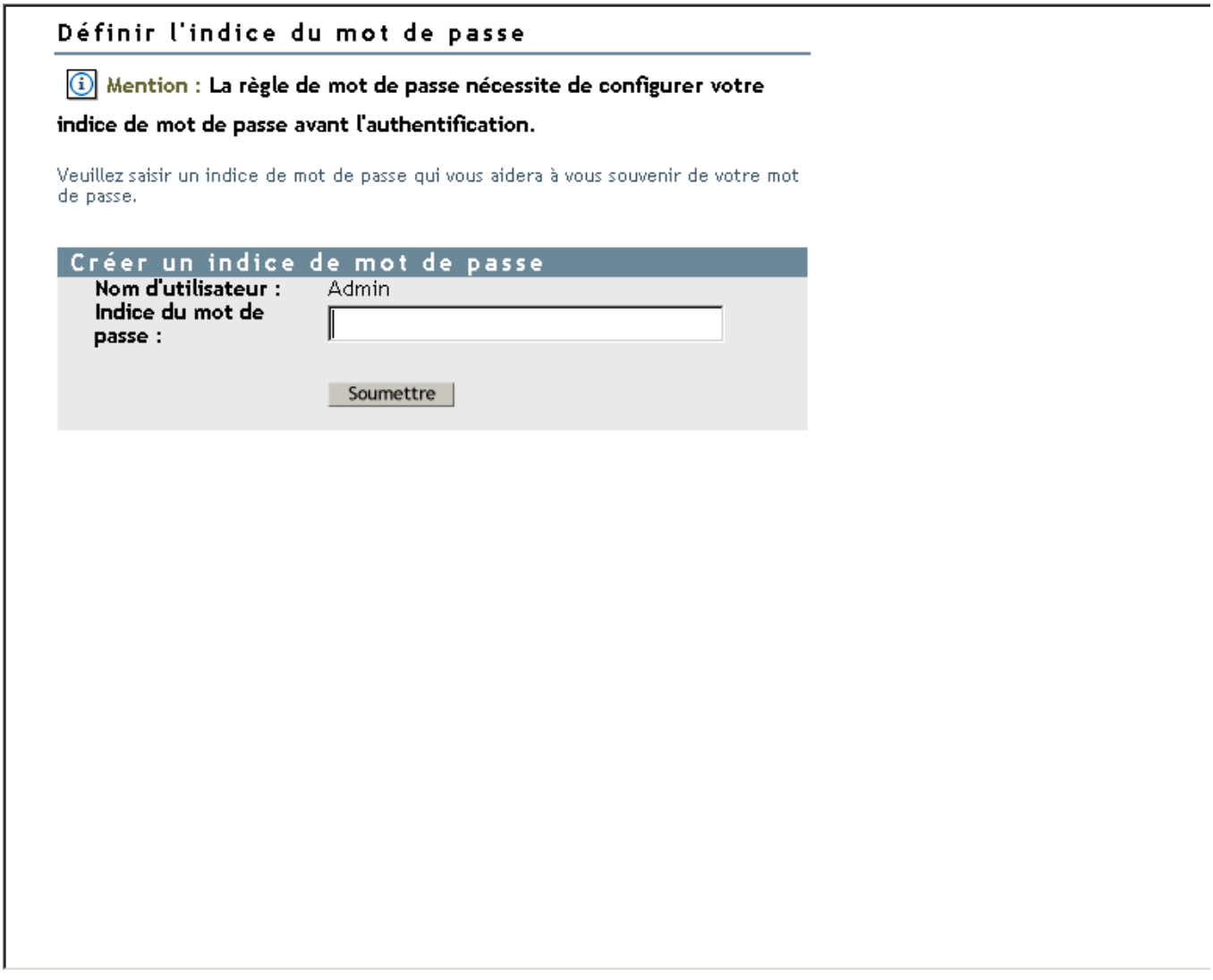
Configuration par l'utilisateur de l'option Mot de passe oublié, post-authentification

L'utilisateur peut exiger que l'utilisateur configure les fonctions de l'option Mot de passe oublié après un login réussi. Il doit pour cela sélectionner cette option afin de forcer l'utilisateur à configurer les stimulation-questions et/ou l'indice à l'authentification. Si cette option est sélectionnée et si l'utilisateur n'a pas configuré de questions ou d'indice, les gadgets de configuration Mot de passe oublié s'afficheront la prochaine fois qu'il se loguera via la console iManager en libre-service (par exemple https://www.*nom_du_serveur*.com/nps). Cette option est appelée la configuration post-authentification.

L’écran suivant présente l’interface de configuration de l’ensemble de stimulation, post-authentification.



L’écran suivant présente l’interface de configuration de l’indice de mot de passe, post-authentification.



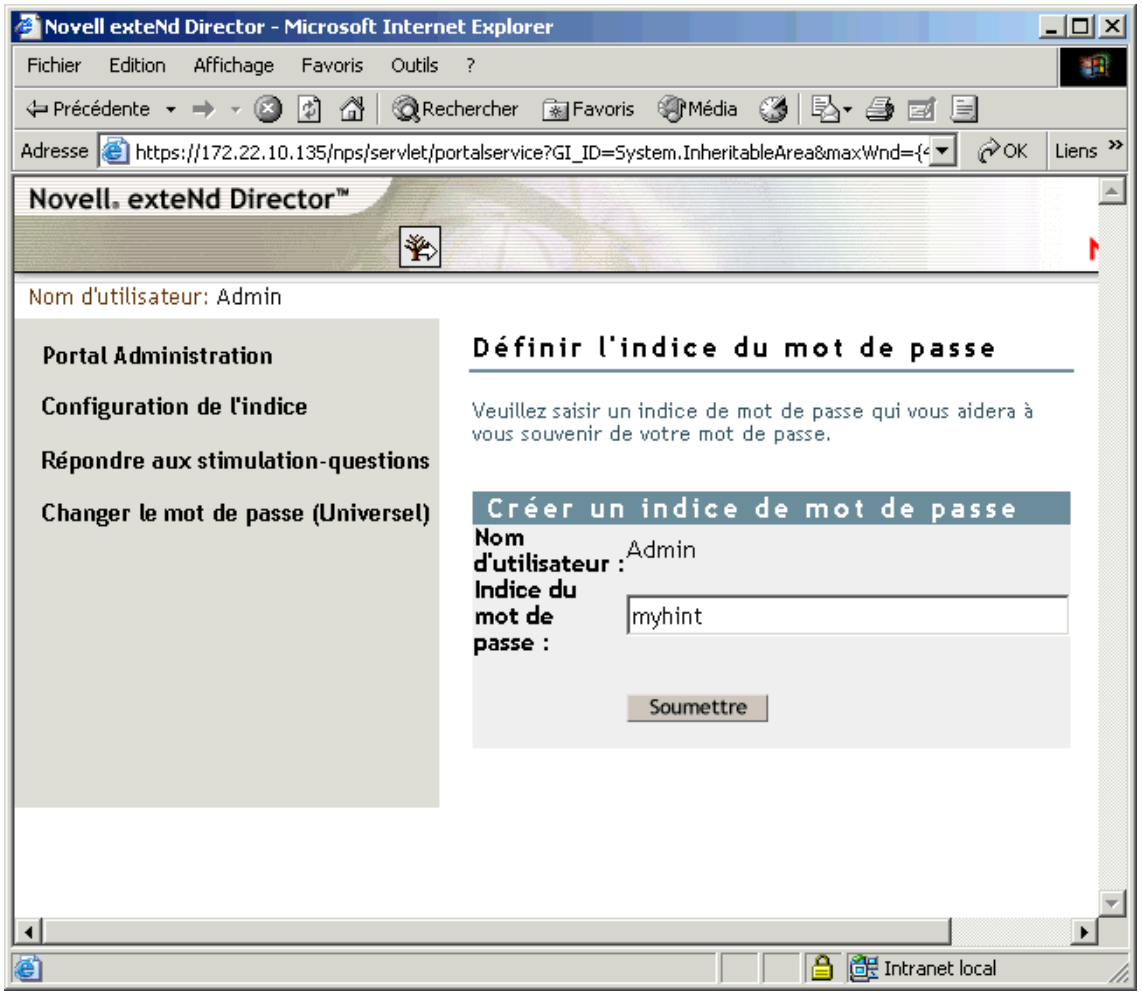
Configuration par l’utilisateur de l’option Mot de passe oublié dans la console iManager en libre-service

Lorsque les utilisateurs se loguent par l’intermédiaire du portail, ils entrent dans la console iManager en libre-service, qui leur permet d’accéder aux gadgets de configuration ou de modification des ensembles de stimulations et des indices de mots de passe associés à l’option en libre-service Mot de passe oublié. C’est également ici que les utilisateurs peuvent effectuer modifier leur mot de passe. Les noms des gadgets auxquels les utilisateurs peuvent accéder sont les suivants :

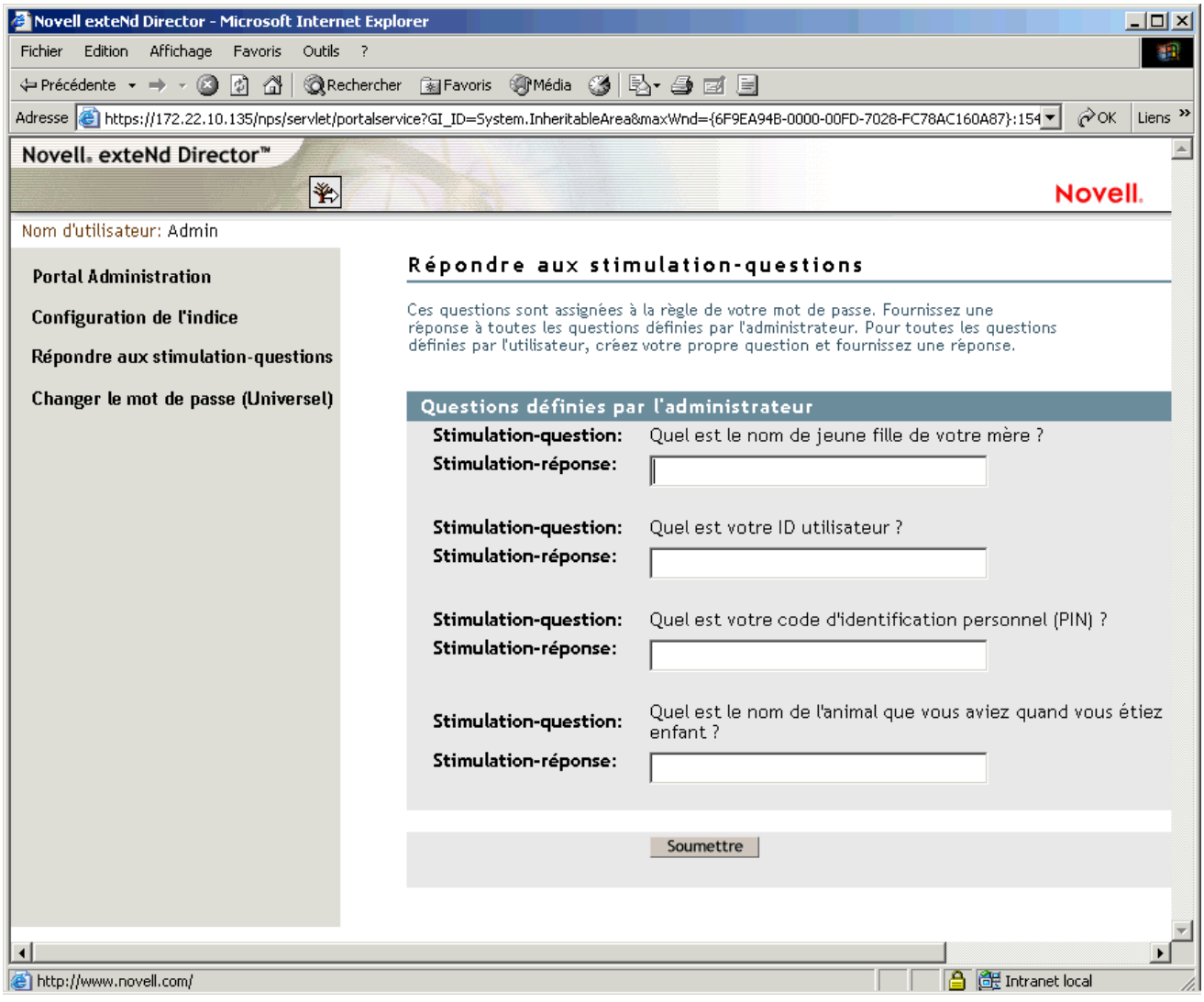
- Configuration de l’indice
- Répondre aux stimulation-questions
- Changer le mot de passe (Universel)

L’utilisateur peut décider de modifier ces gadgets à tout moment. Si aucun indice ni ensemble de stimulation n’est requis dans la règle de mot de passe de l’utilisateur, ce dernier ne pourra pas les modifier. Un message s’affichera pour indiquer que ces options ne sont pas accessibles.

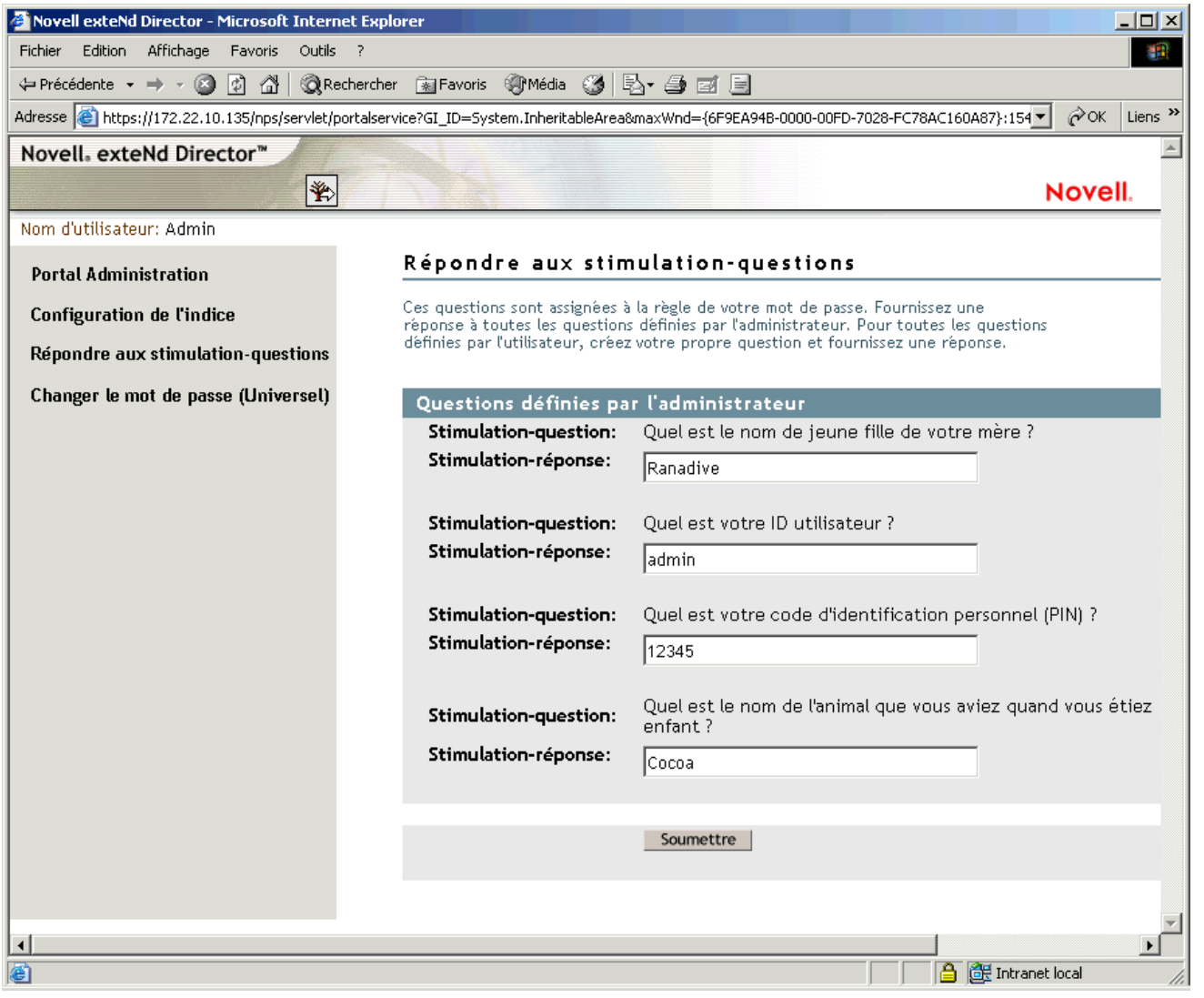
L’illustration suivante présente la page de configuration de l’indice.



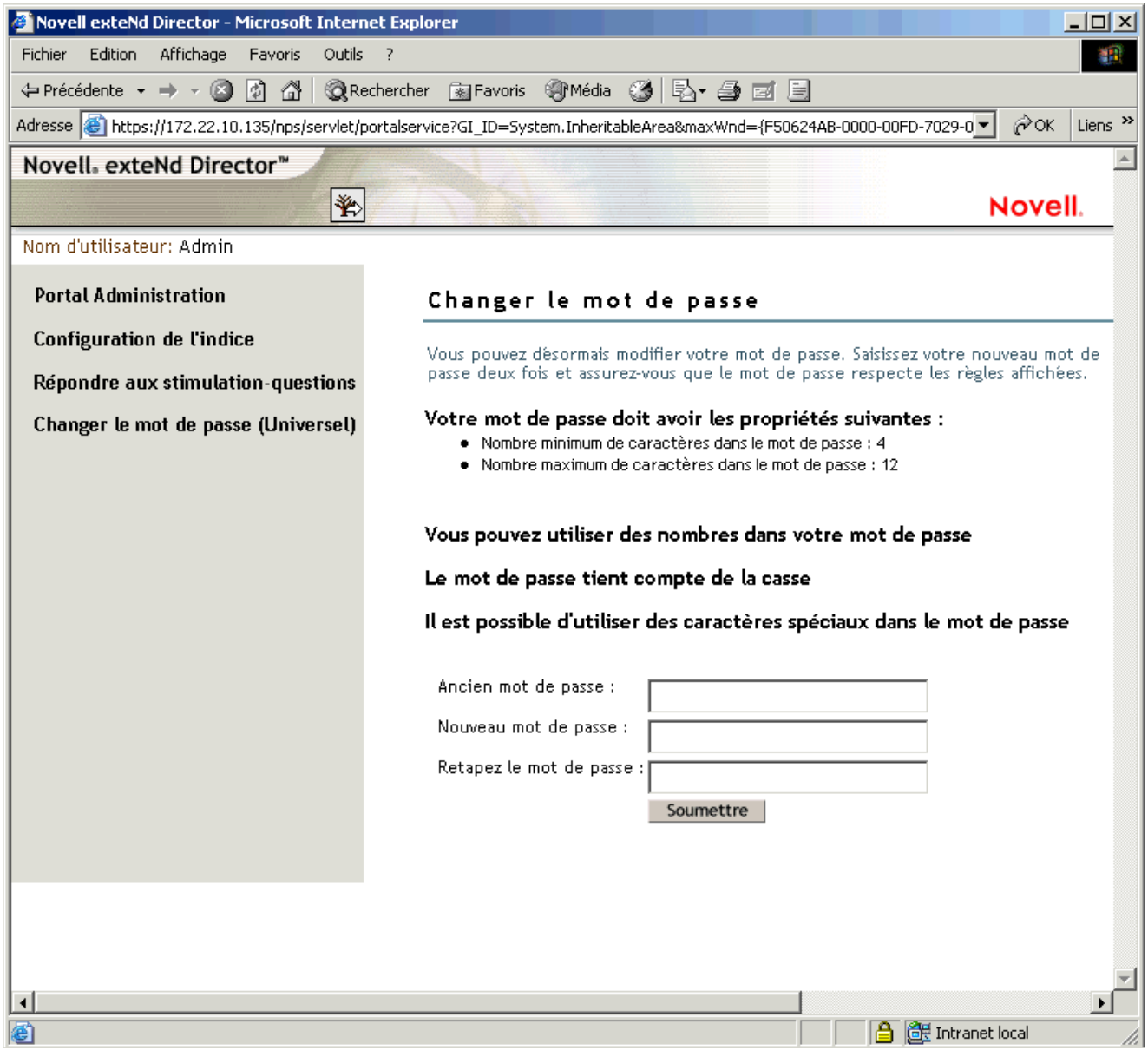
L’illustration suivante présente la page Répondre aux stimulation-questions.



Les premières questions listées dans cet exemple sont définies par l'administrateur. Les suivantes le sont par l'utilisateur. L'utilisateur répond aux questions de l'administrateur, puis crée les questions et leurs réponses, comme dans l'exemple suivant :



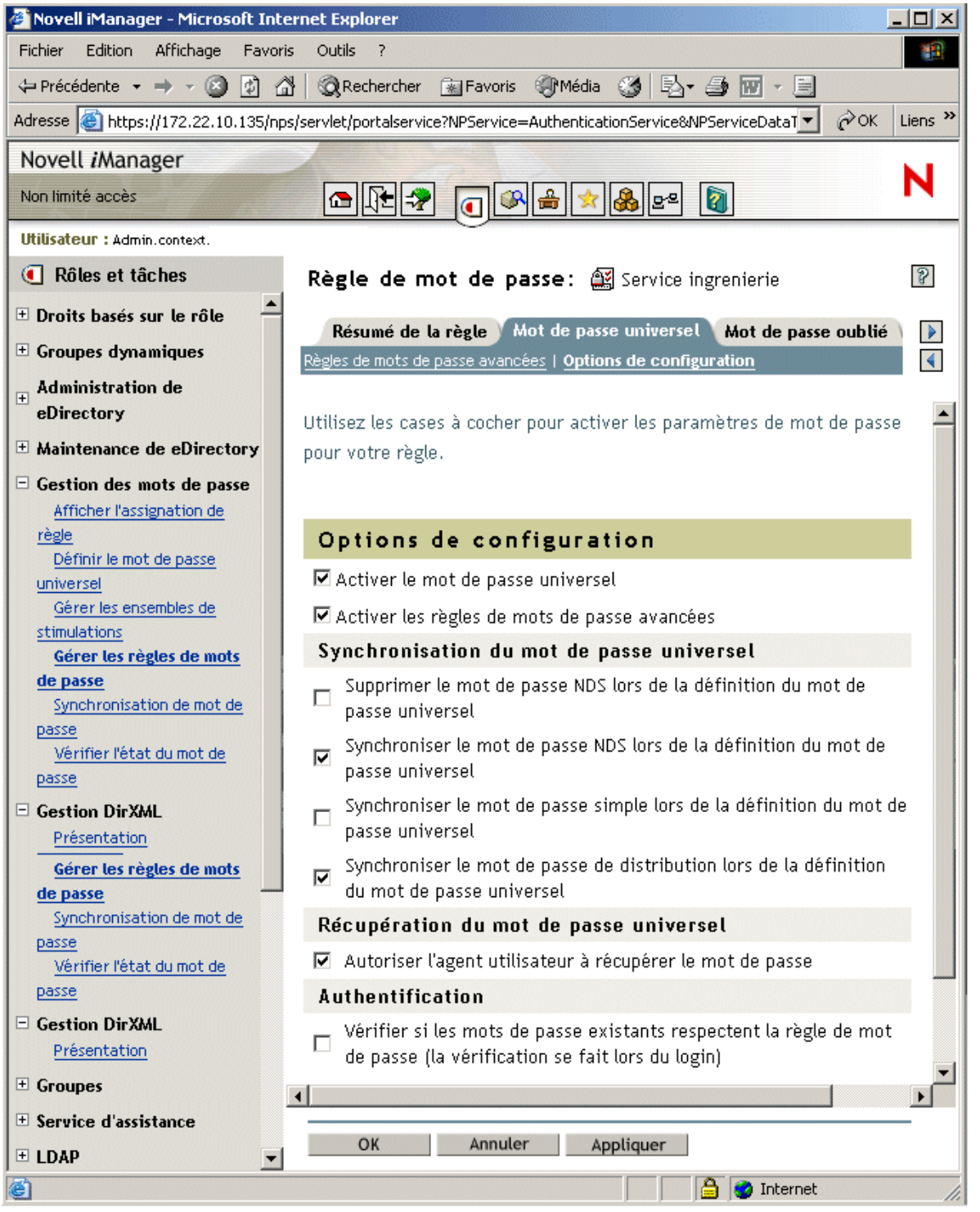
L’illustration suivante présente la page Changer le mot de passe (Universel).



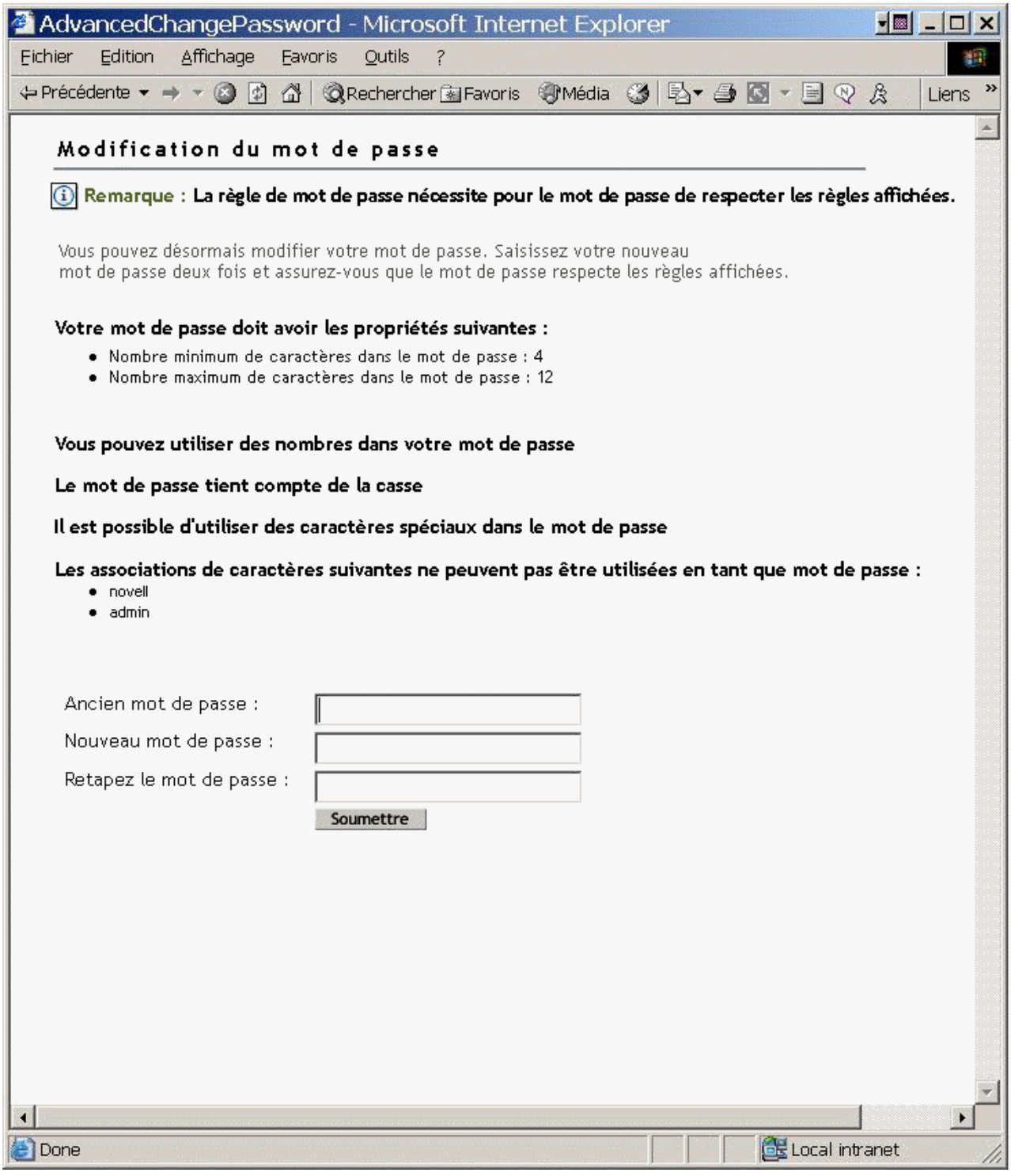
Comment exiger la conformité des mots de passe existants

Si un administrateur crée ou modifie une règle de mot de passe, il peut exiger des utilisateurs qu’ils modifient leurs mots de passe, s’ils ne sont plus conformes, lors de leur prochain login via le portail.

Pour cela, ils doivent utiliser une option de la règle de mot de passe située dans l'onglet Mot de passe universel, sous Options de configuration. Cette option s'appelle Vérifier si les mots de passe existants respectent la règle de mot de passe (la vérification se fait lors du login). Par défaut, cette option est désactivée lorsque vous créez une nouvelle règle de mot de passe. L'illustration suivante présente la page sur laquelle se configure cette option.



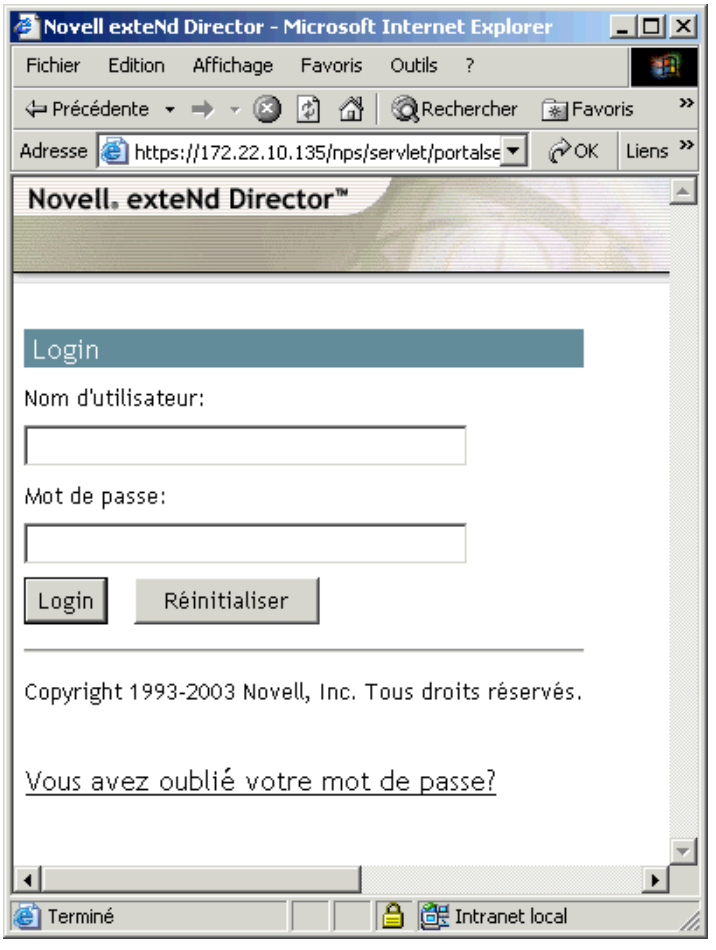
Si cette option est activée, au prochain login des utilisateurs via le portail, la conformité de leur mot de passe avec la règle sera contrôlée. Si un mot de passe n'est pas conforme, une page comme celle-ci s'affiche, et l'utilisateur n'est pas autorisé à se loguer tant qu'il n'a pas modifié son mot de passe.



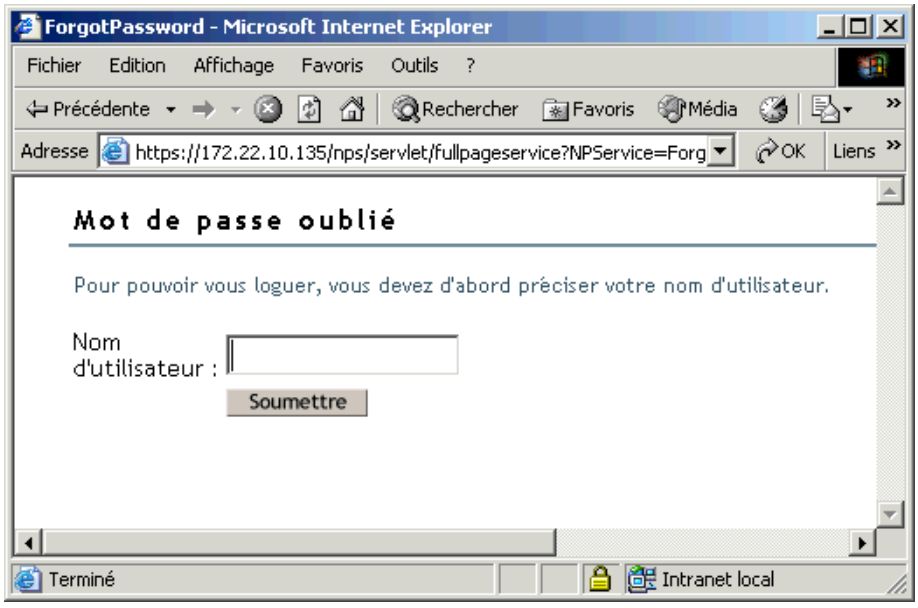
Que voient les utilisateurs finals lorsqu'ils ont oublié leur mot de passe ?

Cette section décrit ce que voient les utilisateurs lorsqu'ils utilisent l'option en libre-service Mot de passe oublié.

Après avoir installé les plugs-in iManager fournis avec Identity Manager, le lien Mot de passe oublié s'affiche dans la console iManager en libre-service (par exemple https://www.*nom_du_serveur*.com/nps), comme illustré ci-dessous.

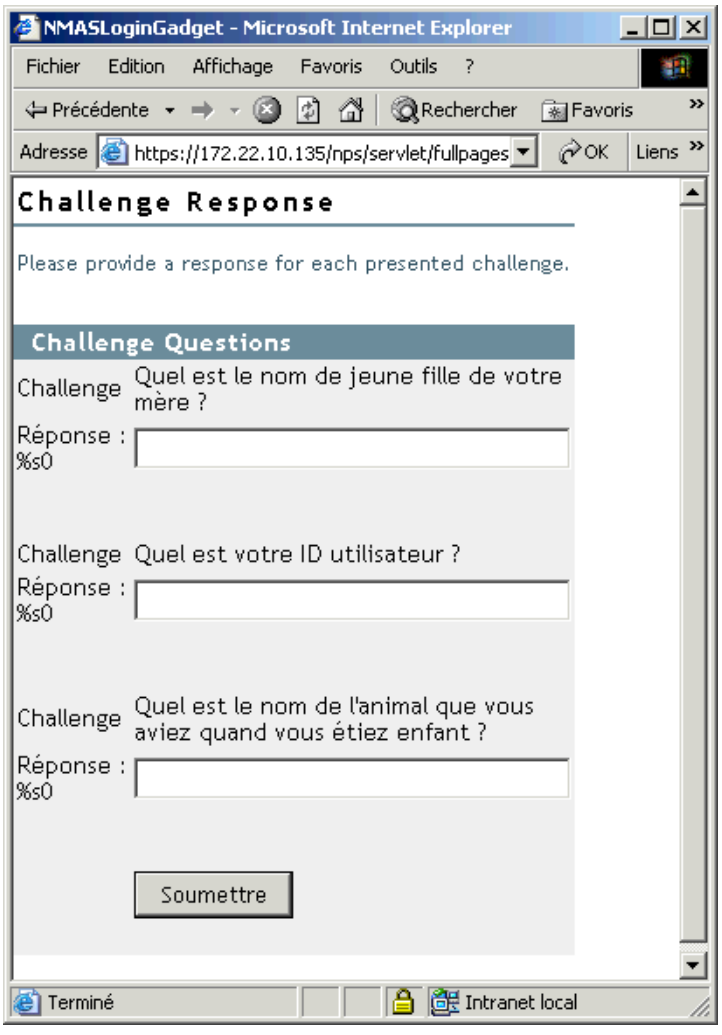


Lorsqu'un utilisateur clique sur ce lien, la page suivante s'affiche, dans laquelle il est invité à saisir son nom.

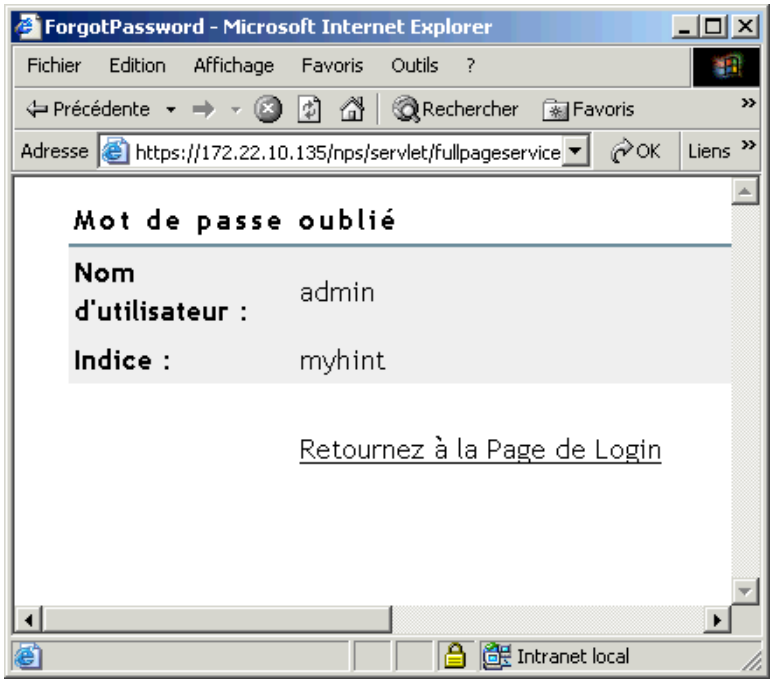


Une fois ce nom saisi, ce sont les paramètres définis pour l'option Mot de passe oublié qui déterminent ce que voit l'utilisateur.

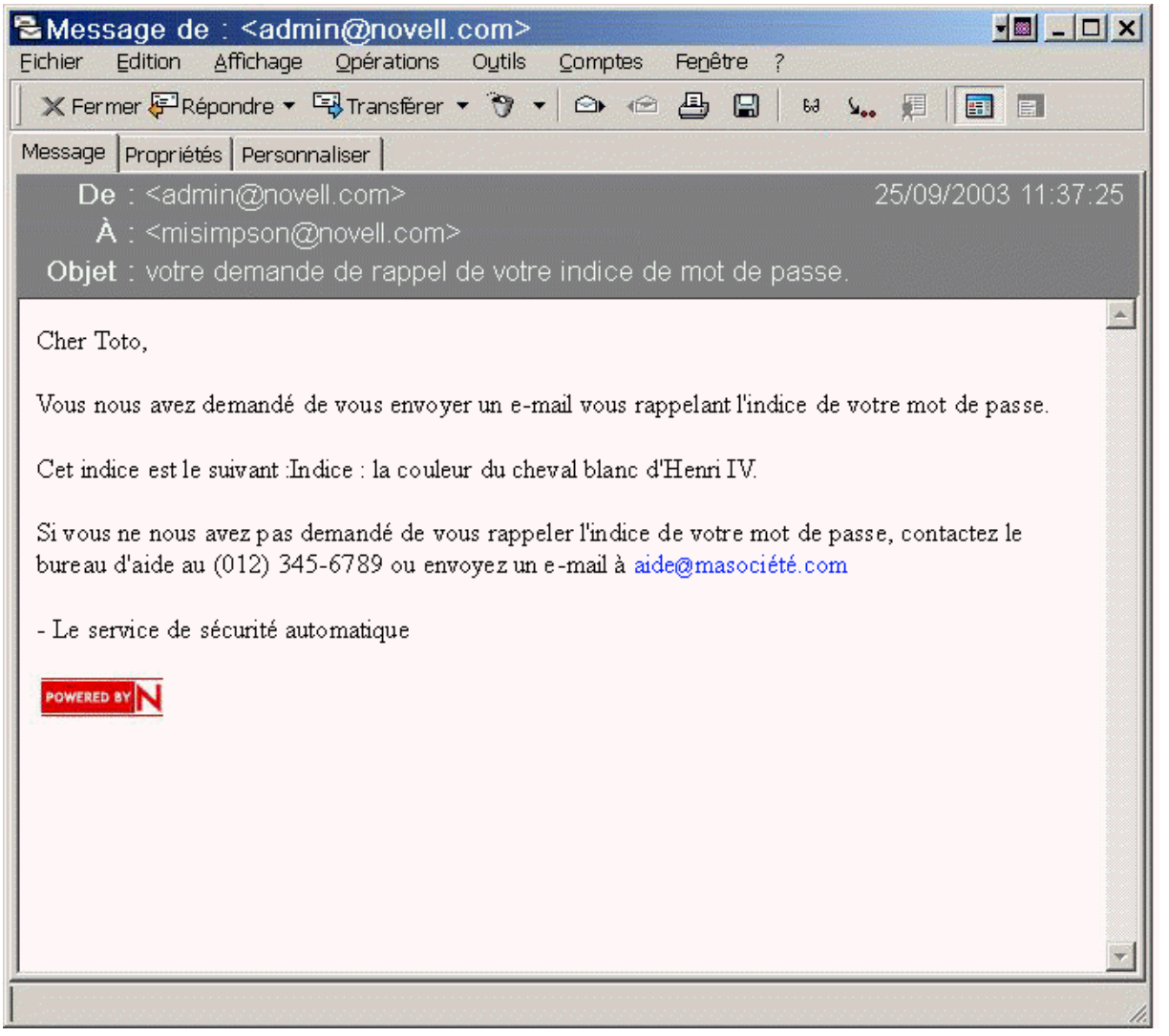
Par exemple, si l'administrateur a spécifié dans la règle de mot de passe qu'un ensemble de stimulation devait être utilisé, une page comme celle qui suit s'affiche, et l'utilisateur doit répondre aux questions posées pour prouver son identité.



Si l'administrateur a spécifié que l'opération liée à l'option Mot de passe oublié à effectuer était Afficher l'indice sur la page, une page comme celle qui suit s'affiche :



Si l'administrateur a spécifié que l'opération liée à l'option Mot de passe oublié à effectuer était Envoyer par messagerie électronique le mot de passe actuel à l'utilisateur ou Envoyer par messagerie électronique l'indice à l'utilisateur, un message s'affiche sur cette page pour indiquer que le mot de passe ou l'indice a été envoyé. L'utilisateur reçoit un message électronique semblable à celui-ci :



Désactivation du lien Mot de asse oublié

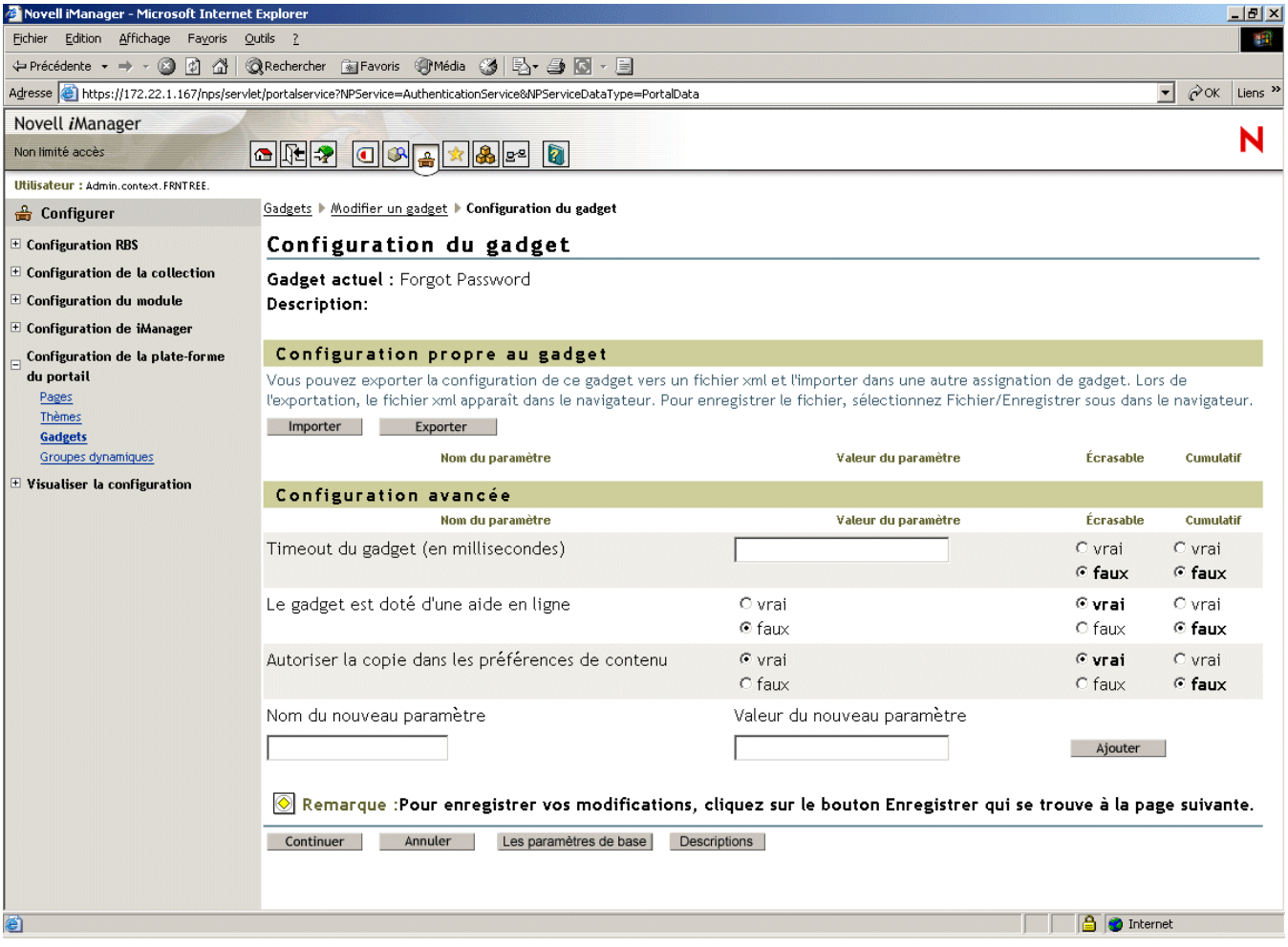
Si vous ne souhaitez pas que le lien Vous avez oublié votre mot de passe ? s'affiche sur le portail, vous pouvez le désactiver en procédant comme suit :

1. Dans iManager, cliquez sur l'icône Configurer pour entrer dans le gadget Administration.
2. Cliquez sur Configuration de la plate-forme du portail > Gadgets.
3. Dans la liste des gadgets, sélectionnez le gadget Mot de passe oublié.
4. Cliquez sur le bouton Modifier, puis sur Configuration. Cliquez sur le bouton Tous les paramètres.

5 Ajoutez une paire de clés aux paramètres du gadget, comme indiqué dans l'illustration.

```
ShowForgotLink=false
```

Si cette paire de clés n'existe pas dans les paramètres du gadget, la valeur par défaut est true.



6 Cliquez sur Continuer puis sur Enregistrer à la page suivante pour enregistrer vos modifications.

7 Redémarrez le serveur Web pour que ces modifications soient prises en compte.

Désactivation du mot de passe par suppression du gadget Indice

L'indice de mot de passe est une méthode destinée à aider les utilisateurs à se souvenir de leur mot de passe, dans le cadre des fonctionnalités de l'option en libre-service Mot de passe oublié. Dans la règle de mot de passe, les opérations liées à l'option Mot de passe oublié et utilisant un indice de mot de passe sont : Envoyer par messagerie électronique l'indice à l'utilisateur ou Afficher l'indice sur la page.

Pour qu'un indice de mot de passe soit utile à quelqu'un ayant oublié son mot de passe, les utilisateurs non authentifiés doivent pouvoir accéder librement à cet attribut (nsimHint). Bien que l'indice du mot de passe soit contrôlé lors de sa création pour vérifier que l'utilisateur n'y a pas fait mention de son mot de passe, vous devez considérer cet accès libre comme un problème de sécurité potentiel.

Si vous ne souhaitez pas utiliser d'indice de mots de passe, choisissez une autre option dans la règle de mot de passe.

De plus, vous pouvez complètement supprimer le gadget Configuration de l'indice si vous le souhaitez.

Après avoir installé les plugs-in Identité Manager pour iManager, utilisez la vue Configurer pour supprimer le gadget Configuration de l'indice.

1. Dans iManager, cliquez sur l'icône Configurer  .
2. Cliquez sur Configuration de la plate-forme du portail > Gadgets.
3. Dans la liste des gadgets, sélectionnez Configuration de l'indice.
4. Cliquez sur Supprimer.

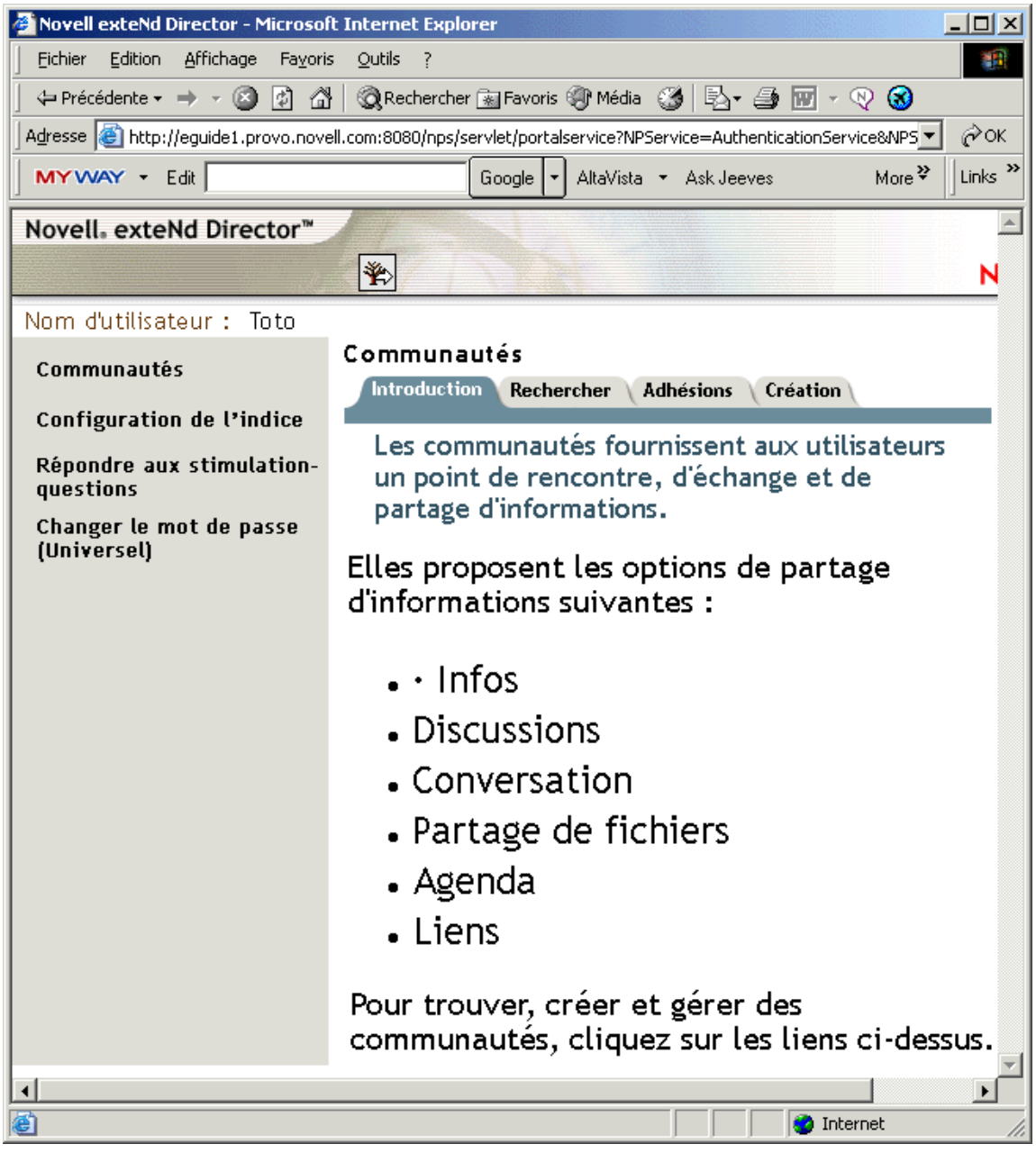
Après avoir supprimé le gadget, l'option Configurer l'indice n'est plus accessible à l'utilisateur. Les services de post-authentification effectuent une requête pour les gadgets existants avant de les ajouter à la liste de suppression. Quel que soit l'état des règles pour les services de post-authentification, si le gadget n'existe pas, le service n'est pas proposé à l'utilisateur par les services de post-authentification ni dans la console iManager en libre-service.

Après avoir supprimé le gadget Indice, vérifiez que vous n'avez sélectionné ni l'envoi de l'indice par message électronique ni son affichage.

Comment fournir aux utilisateurs finals l'option en libre-service Réinitialisation du mot de passe

Pour réinitialiser leur mot de passe, les utilisateurs peuvent se servir de la console iManager en libre-service, accessible via une adresse URL du type : https://www.*nom_du_serveur*.com/nps. Par exemple, https://www.myiManager.com/nps.

Voici un exemple de la console iManager en libre-service après le login.



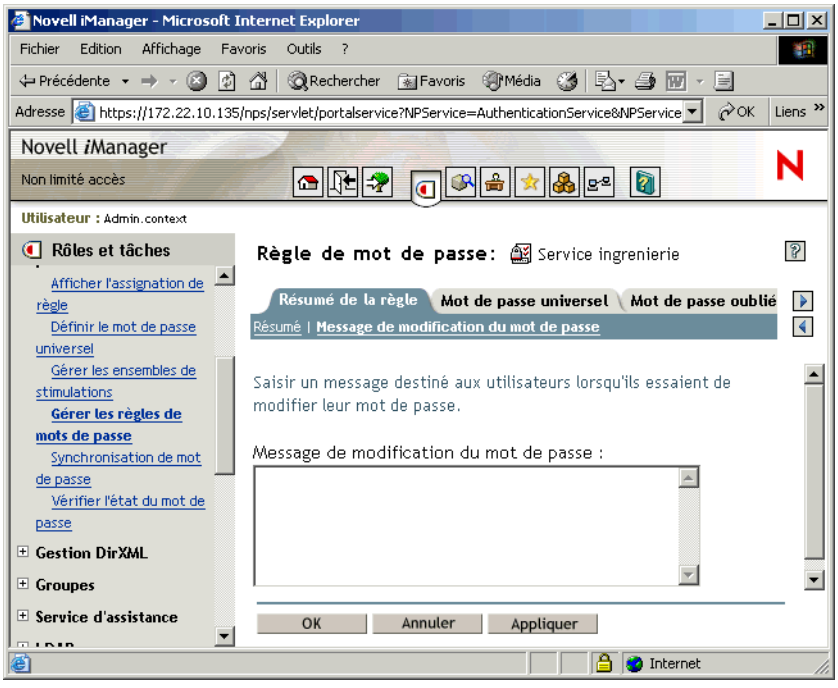
Ajout de votre propre message de modification du mot de passe aux règles de mot de passe

Dans une règle de mot de passe, vous pouvez créer un message de modification du mot de passe. Ce message est soumis aux utilisateurs avec les règles de mot de passe que vous spécifiez. Les utilisateurs voient ce message ainsi que les règles de mot de passe correspondantes chaque fois qu'ils lancent ou qu'ils sont invités à modifier leur mot de passe.

Pour créer ce message, modifiez la règle de mot de passe :

1. Dans iManager, cliquez sur Gestion des mots de passe > Gérer les règles de mot de passe.
2. Cliquez sur la règle de mot de passe à laquelle vous voulez ajouter un message, puis cliquez sur Modifier.
3. Dans l'onglet Résumé de la règle, cliquez sur Message de modification du mot de passe.

   La page suivante s'affiche.



4. Saisissez le message à soumettre aux utilisateurs ainsi que les règles de mot de passe, puis cliquez sur OK.

Création ou modification des ensembles de stimulations

Les ensembles de stimulations sont une fonctionnalité des règles de mot de passe permettant de configurer l'option en libre-service Mot de passe oublié pour vos utilisateurs. Un ensemble de stimulation est un ensemble de questions auxquelles doit répondre un utilisateur pour prouver son identité au lieu d'utiliser son mot de passe.

Lorsque vous créez une règle de mot de passe, vous pouvez activer l'option en libre-service Mot de passe oublié de façon à ce que les utilisateurs puissent obtenir de l'aide sans avoir à contacter le service d'assistance. Pour rendre les options en libre-service encore plus sûres, vous pouvez créer un ensemble de stimulation et demander à ce que les utilisateurs répondent aux questions de cet ensemble avant de pouvoir obtenir de l'aide.

Vous pouvez créer un ensemble de stimulation lorsque vous créez une règle de mot de passe. Dans iManager, accédez à Gestion des mots de passe > Gérer les règles de mot de passe > Nouveau.

Vous pouvez également les gérer en tant que tâche distincte. Dans iManager, accédez à Gestion des mots de passe > Gérer les ensembles de stimulations.

Pour qu'un utilisateur puisse utiliser des ensembles de stimulations, il doit d'abord configurer les questions et leurs réponses. Vous pouvez obliger l'utilisateur à les configurer la prochaine fois qu'il se loguera à iManager ou à la console iManager en libre-service à l'aide d'une option de la zone Règle de mot de passe dans l'onglet Mot de passe oublié. Il s'agit de l'option Forcer l'utilisateur à configurer les questions de stimulation et/ou l'indice à l'authentification. Un utilisateur peut lancer ou modifier cette configuration dans la console iManager en libre-service.

Vous définissez la structure des questions de l'ensemble de stimulation. Les réponses des utilisateurs et les questions définies par l'utilisateur sont stockées dans Novell eDirectory par NMAS (Novell Modular Authentication Services).

Configuration de la notification de l'option de mot de passe en libre-service

Suivez les instructions de la section « Configuration de la notification par message électronique », page 243.

Test des options de mot de passe en libre-service

Pour vérifier que les fonctions sont correctement configurées et tester les options de mot de passe en libre-service, vous pouvez exécuter les tâches suivantes.

1. Créez une règle ayant les caractéristiques suivantes :
   - Activez la fonction Mot de passe oublié.
   - Exigez un ensemble de stimulation.
   - Sélectionnez l'option permettant de vérifier que les stimulation-réponses et les indices sont configurés au login.
   - Assignez la règle de mot de passe à un conteneur renfermant au moins un utilisateur que vous pouvez utiliser pour le test, et dont l'adresse électronique est indiquée dans l'objet Utilisateur de l'attribut Adresse de messagerie Internet.
2. Vérifiez que vous disposez d'un autre utilisateur à qui aucune règle de mot de passe n'a été assignée.

3 Loguez-vous Virtual Office en tant qu'utilisateur à qui une règle de mot de passe a été assignée et vérifiez que vous exécutez toute la procédure de post-authentification (réponse aux stimulation-questions et définition d'un indice).

4 Retournez sur la page de login de la console iManager en libre-service, puis cliquez sur le lien Vous avez oublié votre mot de passe ?. En conservant l'ID du même utilisateur, vérifiez que les stimulation-questions sont correctement présentées et que le fait de donner les réponses appropriées exécute l'opération correcte (affichage de l'indice, autorisation donnée à l'utilisateur de réinitialiser son mot de passe, etc.).

5 Retournez sur la page de login de la console iManager en libre-service, puis cliquez sur le lien Vous avez oublié votre mot de passe ?. Entrez l'ID de l'utilisateur auquel aucune règle de mot de passe n'a été assignée. Vérifiez que les messages d'erreur appropriés s'affichent et que l'utilisateur est informé du fait qu'il n'a pas accès à la fonctionnalité Mot de passe oublié.

Ajout des options de mot de passe en libre-service au portail de votre société

Pour la plupart des procédures présentées à la section Mot de passe en livre service, il est supposé que vous utilisez les options de mot de passe en libre-service sur un serveur iManager 2.0.2.

Consultez le tableau ci-dessous pour obtenir des instructions sur l'utilisation des options de mot de passe en libre-service avec des produits du portail, notamment avec d'autres produits que iManager.

Produit	Prise en charge des options de mot de passe en libre-service	Suivez les instructions…
iManager 2.0.2	Vous pouvez intégrer ces fonctions. Si vous installez les plugs-in de gestion des mots de passe, ce produit prend en charge les options de mot de passe en libre-service. Ces plugs-in sont fournis avec les plugs-in DirXML 2 ; ils sont également disponibles individuellement sur le site download.novell.com.	Suivez les étapes indiquées aux sections ◆ « Conditions requises pour utiliser les règles de mot de passe », page 115. Ces instructions sont présentées au Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101 ◆ Mot de passe en livre service. Les informations présentées à la section « Ajout des options de mot de passe en libre-service au portail de votre société », page 154 ne sont pas nécessaires pour iManager 2.02.
exteNd™ Director™ Standard Edition 4.1 avec Support Pack 1	Vous pouvez intégrer ces fonctions. Si vous installez les fichiers .npm requis (NPM - Novell Portal Module), cette version d'exteNd Director prend en charge les options de mot de passe en libre-service. Pour cela, vous devez disposer du Support Pack version 1 ou ultérieure.	« Intégration à exteNd Director 4.1 des options de mots de passe en libre-service », page 156

Produit	Prise en charge des options de mot de passe en libre-service	Suivez les instructions…
Virtual Office, fourni avec NetWare 6.5 Support Pack 2, exécuté sur un serveur iManager	Vous pouvez intégrer ces fonctions. Si vous installez les plugs-in nécessaires et si vous exécutez quelques étapes supplémentaires, vous pouvez utiliser les options de mot de passe en libre-service sur le serveur NetWare utilisé par Virtual Office et iManager.	« Intégration des options de mot de passe en libre-service avec Virtual Office », page 158
exteNd Director 5	Vous devez établir un lien vers ces fonctions. Étant donné que exteNd Director 5 est basé sur des portlets et que l'option en libre-service Mot de passe est basée sur des modules NPM (Novell Portal Module), vous ne pouvez pas utiliser les options de mot de passe en libre-service directement dans un autre produit. Pour utiliser ce produit avec les options de mot de passe en libre-service, vous devez créer des liens entre le portail de votre société et les fonctions de mot de passe pour l'utilisateur final sur un serveur iManager.	« Lien vers les options de mot de passe en libre-service à partir du portail d'une société », page 158
Versions de Novell Portal Services (NPS) antérieures à la version 4.1	Vous devez établir un lien vers ces fonctions. Bien que ces produits NPS hérités exécutent des modules NPM (Novell Portal Module), ils ne bénéficient pas de toutes les améliorations requises pour les options de mot de passe en libre-service du module ForgottenPassword.npm. Pour utiliser ce produit avec les options de mot de passe en libre-service, vous devez créer des liens entre le portail de votre société et les fonctions de mot de passe pour l'utilisateur final sur un serveur iManager.	« Lien vers les options de mot de passe en libre-service à partir du portail d'une société », page 158
Produits tiers	Vous devez établir un lien vers ces fonctions. Étant donné que les produits tiers n'exécutent pas de module NPM (Novell Portal Module), vous ne pouvez pas utiliser les options de mot de passe en libre-service directement dans un autre produit. Pour utiliser ces produits tiers avec les options de mot de passe en libre-service, vous devez créer des liens entre le portail de votre société et les fonctions de mot de passe pour l'utilisateur final sur un serveur iManager.	« Lien vers les options de mot de passe en libre-service à partir du portail d'une société », page 158

Intégration à exteNd Director 4.1 des options de mots de passe en libre-service

Si vous utilisez exteNd Director Standard Edition 4.1 avec Support Pack 1 pour un portail de société, vous pouvez ajouter le module Mot de passe oublié à votre portail comme tout autre module NPM. Ce module fournit les mêmes fonctionnalités que lorsqu'il est utilisé sous iManager 2.0.2 :

- Nouvelles tâches pour l'utilisateur du portail relatives aux options de mots de passe en libre-service :
  - Configuration de l'indice
  - Répondre aux stimulation-questions
  - Changer le mot de passe (Universel)
- Option en libre-service Mot de passe oublié, accessible via le lien Vous avez oublié votre mot de passe ? sur la page de login au portail
- Fonctions de post-authentification pour inviter les utilisateurs à modifier les mots de passe non conformes ou à mettre à jour les éléments de l'option Mot de passe oublié tels que les indices et les stimulation-questions

Pour ajouter ces fonctions :

1. Vérifiez que le Support Pack 1 est installé.

   Il comporte des améliorations requises par le module ForgottenPassword.npm.

2. Vérifiez que SSL est configuré entre le serveur Web exteNd Director et eDirectory, même si ceux-ci s'exécutent sur le même ordinateur.

   Il s'agit d'une exigence de NMAS version 2.3 ou ultérieure.

3. Pour garantir la sécurité des gadgets Mot de passe oublié, vérifiez votre numéro de port SSL LDAP.

   Si vous n'utilisez pas le port SSL LDAP 636, vous devez effectuer la procédure de configuration suivante :

   Ajoutez la paire de clés suivantes au fichier PortalServlet.properties :

   LDAPSSLPort=*votre_numéro_de_port*

   Par exemple, si votre serveur Web exécute Active Directory, vous devez effectuer cette modification, car Active Directory utilise le port 636. Si vous exécutez Tomcat, modifiez le paramètre dans le fichier PortalServlet.properties qui se trouve dans le répertoire tomcat\webapps\nps\WEB_INF.

   Ce paramètre est prioritaire par rapport à la valeur 636 par défaut (si cette valeur est présente dans le fichier).

4. Après avoir modifié ce paramètre, redémarrez le serveur Web.

5. Vérifiez que tous les utilisateurs eDirectory présents dans le conteneur des utilisateurs du portail ont des droits en libre-service pour l'attribut Indice intitulé nsimHint.

   Lorsque vous installez les plugs-in DirXML sur un serveur Web iManager, cette étape est automatiquement exécutée pour l'arborescence pour laquelle iManager est configuré.

   Toutefois, si vous pointez vers une autre arborescence, vous devez exécuter cette étape manuellement.

Un utilitaire est fourni pour vous aider dans cette procédure. Vous pouvez le télécharger et l'exécuter en procédant comme suit :

5a Accédez au site http:\\download.novell.com.

5b Entrez les informations requises dans les champs suivants :

- **Search by: (Rechercher par :)**Produit
- **Choose a Product: (Sélectionner un produit :)** Nsure Identity Manager

5c Téléchargez l'élément intitulé 2.0 Password Management Plug-in for iManager 2.0*x* (Plug-in de gestion des mots de passe 2.0 pour iManager 2.0.*x*).

5d Suivez les instructions fournies dans le fichier nsimhintreadme.txt.

Si les utilisateurs ne disposent pas de droits en libre-service pour l'attribut nsimHint, ils obtiennent une erreur du type suivant lorsqu'ils tentent de créer un indice :

```
"Could not write user hint" (Task could not be completed).
```

6 (Conditionnel) Si vous n'avez pas installé Identity Manager sur le serveur exécutant eDirectory et NMAS, installez la méthode de login par stimulation-réponses pour NMAS.

Cette méthode de login est installée automatiquement avec Identity Manager. Elle fait partie du produit eDirectory 8.7.3.

Pour installer une méthode de login sous Windows, vous pouvez, entre autres, utiliser la fonction d'installation de méthodes (Method Installer) :

6a Recherchez le fichier MethodInstaller.exe dans le répertoire \nmas\NmasMethods\ du CD eDirectory.

6b Exécutez ce programme sur un poste de travail et sélectionnez la méthode de login par stimulation-réponses.

6c Acceptez le contrat et les paramètres par défaut présentés pour la séquence de login.

La méthode est ajoutée au conteneur de login autorisé Methods.Security.*nom_arborescence*.

Pour plus d'informations sur l'installation d'une méthode de login, y compris sous UNIX, reportez-vous à la section Installing a Login Method (Installation d'une méthode de login) (http://www.novell.com/documentation/fr-fr/nmas23/admin/data/a49tuwk.html#a49tuwk) du manuel *NMAS 2.3 Administration Guide (Guide d'administration de NMAS 2.3)* (http://www.novell.com/documentation/fr-fr/nmas23).

7 Ajoutez les modules suivants à exteNd Director :

- ForgottenPassword.npm
- nmasclient.npm

Ils sont inclus dans le produit DirXML.

Pour plus d'informations sur l'ajout d'un module, reportez-vous au manuel *Novell exteNd Director Standard Edition Installation and Configuration Guide (Guide d'installation et de configuration de Novell exteNd Director Standard Edition)* (http://www.novell.com/documentation/fr-fr/nedse41/configure/data/ajhotzv.html).

Intégration des options de mot de passe en libre-service avec Virtual Office

Dans NetWare 6.5 avec Support Pack 2, Virtual Office prend en charge toutes les fonctions des options de mot de passe en libre-service. Avant d'utiliser ces fonctions, vous devez suivre quelques étapes. Toutefois, certaines d'entre elles sont exécutées automatiquement lors de l'installation d'Identity Manager dans votre arborescence eDirectory et lors de l'installation des plugs-in Identity Manager sur votre serveur iManager.

Pour plus d'informations, reportez-vous au *Novell Virtual Office for NetWare 6.5 Configuration Guide (Guide de configuration de Novell Virtual Office pour NetWare 6.5)* (http://www.novell.com/documentation/nw65/virtualoffice/data/ac6spye.html). Les éléments déjà activés si vous avez installé Identity Manager sont les suivants :

- extension du schéma pour la gestion des mots de passe ;
- installation des plugs-in de gestion des mots de passe ;
- installation de la méthode de login par stimulation-réponse ;
- octroi aux utilisateurs de droits d'accès à un indice de mot de passe.

  Remarque : lorsque vous installez les plugs-in DirXML sur un serveur iManager, les droits d'accès accordés aux utilisateurs pour l'indice de mot de passe sont automatiquement inscrits dans l'arborescence pour laquelle iManager est configuré. Si vous pointez vers une autre arborescence, vous devez exécuter cette étape manuellement.

Lien vers les options de mot de passe en libre-service à partir du portail d'une société

Pour les produits ne fournissant pas l'option en libre-service Mot de passe en exécutant ForgottenPassword.npm (tel que décrit dans le tableau de la section « Ajout des options de mot de passe en libre-service au portail de votre société », page 154), vous pouvez utiliser l'option en libre-service Mot de passe en créant un autre serveur iManager avec les plugs-in de gestion des mots de passe installés, puis en établissant une liaison entre le portail de votre page d'accueil et la console iManager en libre-service de l'autre serveur, comme https://*adresse_IP_serveur_iManager*/nps.

Les plugs-in de gestion des mots de passe sont inclus dans les plugs-in DirXML 2 et sont disponibles séparément en téléchargeant le plug-in de gestion des mots de passe 2.0 pour iManager 2.0.*x* à partir de l'adresse http:\\download.novell.com.

La seule fonction difficile à intégrer est le service de post-authentification, qui invite les utilisateurs à mettre à jour leur mot de passe afin de respecter les règles de mot de passe puis à installer l'option en libre-service Mot de passe oublié en fonction de la règle de mot de passe, comme la création d'un indice de mot de passe. Pour que les utilisateurs possèdent des mots de passe conformes et soient configurés pour utiliser l'option en libre-service Mot de passe oublié, vous devez vérifier que les utilisateurs se loguent à la console iManager en libre-service au moins une fois afin de créer des mots de passe conformes et d'achever la configuration de la gestion des mots de passe, puis à chaque fois que vous apportez des modifications aux règles de mot de passe.

Suivez les instructions de ces sections :

- « Conditions préalables », page 159
- « Lien vers l'option en libre-service Mot de passe oublié », page 159
- « Lien vers les tâches de gestion des mots de passe de l'utilisateur final », page 160
- « Renvoi des utilisateurs des options en libre-service vers le portail de la société », page 161
- « Comment vérifier que les utilisateurs ont configuré les fonctionnalités des options de mot de passe », page 162

Conditions préalables

Le serveur iManager et l'arborescence utilisés doivent être préparés pour :

- répondre aux exigences définies au Chapitre 4, « Installation », page 51 ;
- répondre aux conditions préalables définies à la section « Conditions requises pour utiliser les règles de mot de passe », page 115 ;
- vérifier l'installation des règles de mot de passe pour vos utilisateurs eDirectory.

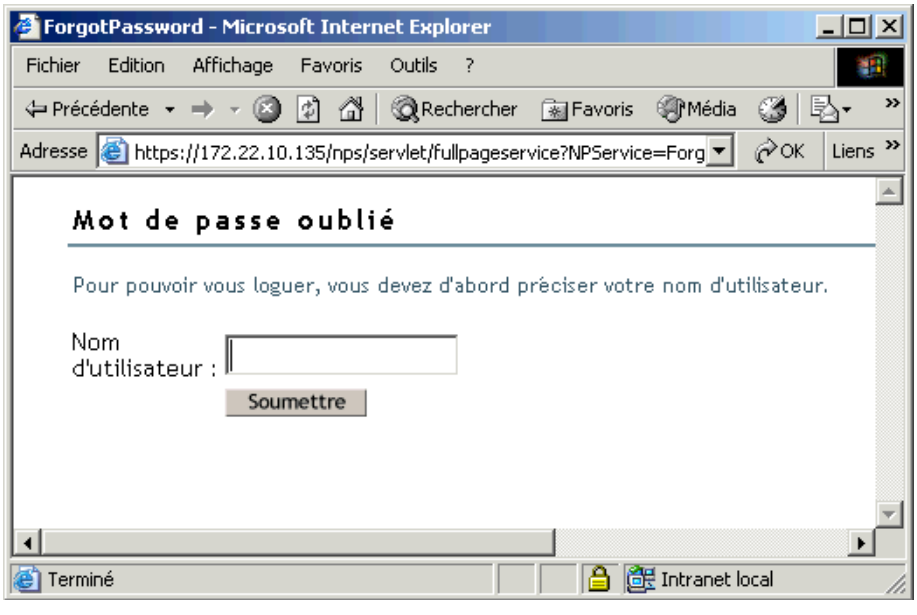
Lien vers l'option en libre-service Mot de passe oublié

Pour que les utilisateurs accèdent à l'option en libre-service Mot de passe oublié à partir du portail de votre société, vous pouvez créer un lien vers ce service depuis un serveur Web iManager séparé.

1 Créez un lien tel que Vous avez oublié votre mot de passe ? sur la page de login du portail de votre société et faites-le pointer vers l'adresse suivante sur votre serveur Web iManager :

http://*adresse_IP_serveur_iManager*/nps/servlet/fullpageservice?NPService=ForgotPassword&nextState=getUserID

Cette URL emmène l'utilisateur sur la page suivante, depuis laquelle vous lancez le processus Mot de passe oublié. Pour voir des exemples des autres pages du processus, reportez-vous à la section « Comment fournir aux utilisateurs finals le libre-service Mot de passe oublié », page 129.



2 Suivez les étapes indiquées à la section « Renvoi des utilisateurs des options en libre-service vers le portail de la société », page 161.

Lien vers les tâches de gestion des mots de passe de l'utilisateur final

1 Vérifiez que tous les utilisateurs eDirectory présents dans le conteneur des utilisateurs du portail ont des droits en libre-service pour l'attribut Indice intitulé nsimHint.

Lorsque vous installez les plugs-in DirXML sur un serveur Web iManager, cette étape est automatiquement exécutée pour l'arborescence pour laquelle iManager est configuré.

Si vous pointez vers une autre arborescence, vous devez exécuter cette étape manuellement.

Un utilitaire est fourni pour vous aider dans cette procédure. Vous pouvez le télécharger et l'exécuter en procédant comme suit :

1a Accédez au site http:\\download.novell.com.

1b Entrez les informations requises dans les champs suivants :

- **Search by: (Rechercher par :)** Produit
- **Choose a Product: (Sélectionner un produit :)** Nsure Identity Manager

1c Téléchargez l'élément intitulé 2.0 Password Management Plug-in for iManager 2.0*x* (Plug-in de gestion des mots de passe 2.0 pour iManager 2.0.*x*).

1d Suivez les instructions fournies dans le fichier nsimhintreadme.txt.

Si les utilisateurs ne disposent pas de droits en libre-service pour l'attribut nsimHint, ils obtiennent une erreur du type suivant lorsqu'ils tentent de créer un indice :

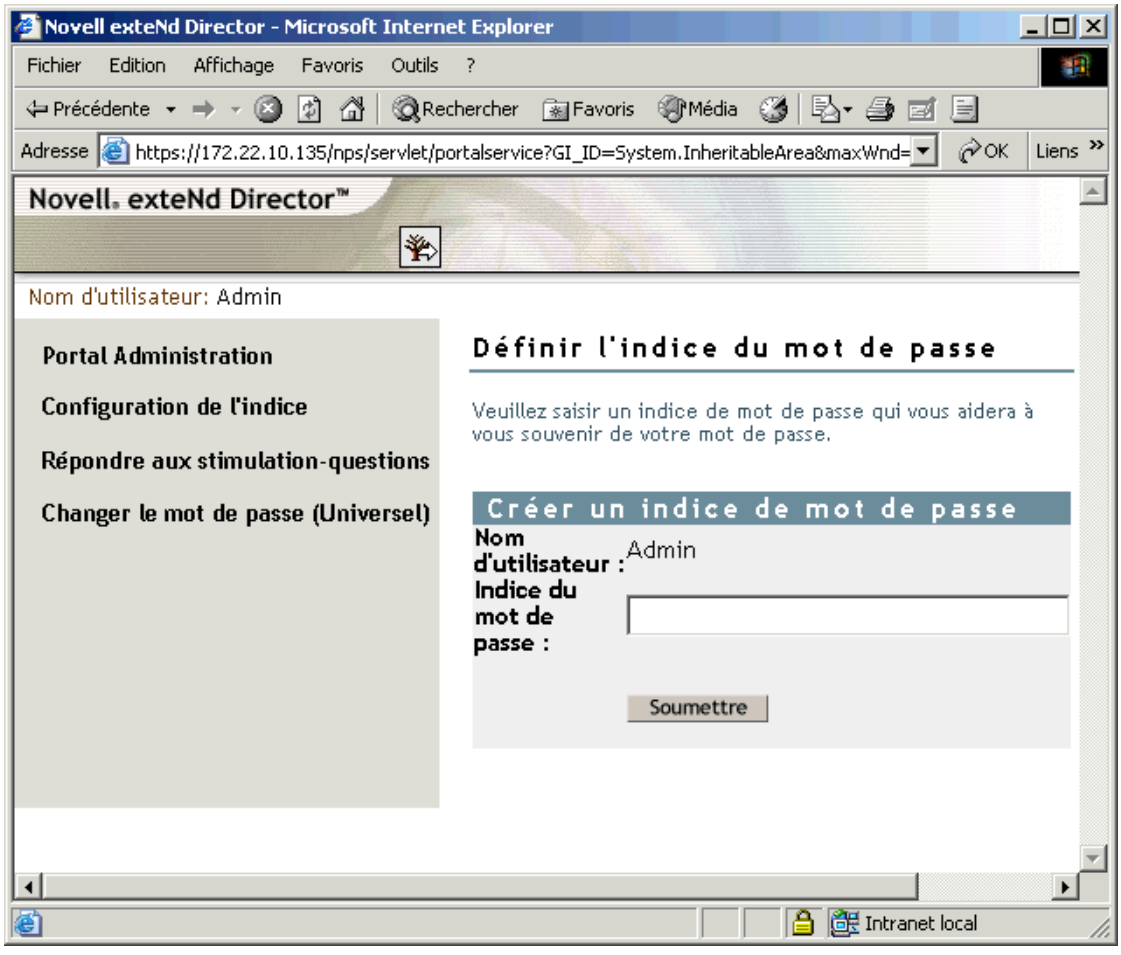
```
"Could not write user hint" (Task could not be completed).
```

2 Fournissez aux utilisateurs un lien à partir du portail de votre société vers les tâches de gestion des mots de passe.

Vous pouvez créer un lien Gérer les mots de passe à partir du portail de votre société et le lier à https://*autre_serveur_iManager*/nps. Ce lien permettra d'accéder aux tâches de gestion des mots de passe des utilisateurs finals :

- Configuration de l'indice
- Répondre aux stimulation-questions
- Changer le mot de passe (Universel)

Un utilisateur cliquant sur le lien devra d'abord se loguer. Il verra ensuite une page similaire à l'exemple suivant.



3 Suivez les étapes indiquées à la section « Renvoi des utilisateurs des options en libre-service vers le portail de la société », page 161.

Renvoi des utilisateurs des options en libre-service vers le portail de la société

Les options en libre-service Mot de passe intègrent des scénarios dans lesquels les utilisateurs disposent d'un lien permettant de revenir à la page de login. Par exemple, lorsqu'un utilisateur modifie son mot de passe à l'aide de l'option en libre-service Mot de passe oublié, la page suivante s'affiche : Your password has been successfully changed. Click here to return to login page. (Votre mot de passe a été changé. Cliquez ici pour revenir à la page de login).

Si, à partir du portail de votre société, vous pointez sur les options de mot de passe en libre-service d'un serveur iManager séparé, il peut être nécessaire de personnaliser la page de retour par défaut afin que les utilisateurs soient renvoyés automatiquement sur la page de login du portail une fois les tâches liées aux mots de passe achevées. Par défaut, le fait de cliquer sur le bouton renvoie l'utilisateur vers une page du serveur Web iManager.

Un lien de renvoi vers la page de login figure à ces trois emplacements :

- la page sur laquelle un utilisateur peut définir un nouveau mot de passe ;
- la page affichée après la modification réussie de son mot de passe par un utilisateur ;
- la page sur laquelle un utilisateur peut consulter un indice.

Pour personnaliser la page de retour et la diriger vers la page de login du portail de votre société :

1. Sur le serveur Web iManager actuellement utilisé pour l'option en libre-service de mot de passe oublié, recherchez le répertoire suivant :

   \tomcat\webapps\nps\portal\modules\ForgottenPassword\skins\default\devices\default

2. Recherchez le fichier suivant au sein de ce répertoire :

   forgottenpassword.xsl

3. Modifiez le fichier forgottenpassword.xsl afin de personnaliser la page de retour par défaut.

   Remplacez le code suivant

   ```
   href="{LoginURL}"
   ```

   par une adresse URL codée en dur, par exemple

   ```
   href="(http:\\www.page_accueil_portail_société.com)"
   ```

   Vous devez apporter cette modifications à trois emplacements dans le fichier.

4. Arrêtez et redémarrez Tomcat sur le serveur iManager.

   Le lien Retournez à la Page de Login renvoie désormais les utilisateurs vers la page de login du portail de votre société

Comment vérifier que les utilisateurs ont configuré les fonctionnalités des options de mot de passe

Lorsque les utilisateurs se loguent à la console iManager en libre-service à l'adresse https://*adresse_IP_serveur_iManager*/nps, ils sont invités à suivre les consignes figurant dans plusieurs pages de post-authentification si les conditions suivantes s'appliquent :

- Le mot de passe de l'utilisateur ne respecte pas les règles de mots de passe avancées.
- La règle de mot de passe exige des stimulation-questions lors de l'utilisation de l'option en libre-service Mot de passe oublié, mais l'utilisateur ne les a pas configurées.
- La règle de mot de passe utilise l'option Mot de passe oublié avec, comme opération, l'affichage de l'indice du mot de passe, mais l'utilisateur n'a pas créé d'indice.

Par exemple, ces invites sont nécessaires pour vérifier que l'utilisateur peut utiliser l'option en libre-service Mot de passe oublié. Si la règle de mot de passe demande à l'utilisateur de répondre aux stimulation-questions et si l'utilisateur ne les a jamais configurées, il ne peut pas accéder à l'option en libre-service Mot de passe oublié. Si l'utilisateur n'a pas créé d'indice de mot de passe, il ne peut pas le récupérer pour l'aider à se souvenir de son mot de passe.

Les produits issus des autres portails ne fournissant pas automatiquement les fonctionnalités de post-authentification, vous devrez vérifier que les utilisateurs se loguent à la console iManager en libre-service au moins une fois afin de créer des mots de passe conformes et d'achever l'installation de la gestion des mots de passe, puis de façon régulière chaque fois que vous apporterez des modifications aux règles de mot de passe.

Vérifiez pour cela que les utilisateurs utilisent le lien de gestion des mots de passe que vous avez fourni, qui est décrit à la section « Lien vers les tâches de gestion des mots de passe de l'utilisateur final », page 160, et qui exige que les utilisateurs se loguent à la console iManager en libre-service.

Résolution des problèmes des options de mot de passe en libre-service

- Pour utiliser les questions de stimulation-réponse, vérifiez que vous utilisez un navigateur pris en charge par iManager 2.02.
- Si SSL n'est pas correctement configuré, vous ne pourrez pas vous loguer à iManager ou à la console en libre-service. Mais si vous pouvez vous loguer avec succès à iManager et si vous exigez TLS en cas de liaison simple, SSL est correctement configuré et vous pouvez traiter les problèmes liés à SSL lors de la résolution des problèmes de mot de passe en libre-service.
- Reportez-vous également aux sections suivantes :
  - « Dépannage des problèmes de règles de mot de passe », page 122
  - « Dépannage des problèmes de synchronisation des mots de passe », page 258 si vous utilisez la synchronisation des mots de passe sous Identity Manager, « Mise en œuvre de la synchronisation des mots de passe », page 202 pour la résolution des problèmes liés à chaque scénario, et à la documentation relative aux pilotes spécifiques concernés du site Web de documentation sur les pilotes. (http://www.novell.com/documentation/fr-fr/dirxmldrivers)

9 Synchronisation de mot de passe sur des systèmes connectés

La synchronisation des mots de passe dans Nsure™ Identity Manager offre plusieurs avantages innovants :

- la synchronisation bidirectionnelle des mots de passe ;
- l'application des règles de mots de passe sur les systèmes connectés ;
- la notification par courrier électronique en cas d'échec de la synchronisation ;
- la possibilité de vérifier l'état de la synchronisation des mots de passe pour un utilisateur.

Pour mieux comprendre les options, reportez-vous aux scénarios de la section « Mise en œuvre de la synchronisation des mots de passe », page 202.

Cette section contient les informations suivantes :

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 édition.

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

Présentation des mots de passe

eDirectory dispose de plusieurs mots de passe, dont les utilisations varient. Dans les versions précédentes de eDirectory et de DirXML, les systèmes connectés ne pouvaient actualiser que le mot de passe NDS, et il s'agissait d'une synchronisation unilatérale.

Les mots de passe universels, qui ont fait leur apparition dans eDirectory 8.7.1, sont des mots de passe réversibles, pouvant être synchronisés avec les mots de passe eDirectory si nécessaire. Ils sont protégés par quatre niveaux de codage.

NMAS contrôle la relation entre les mots de passe universels et les autres mots de passe eDirectory, notamment si la synchronisation est maintenue entre le mot de passe universel d'une part et le mot de passe NDS, le mot de passe simple ou le mot de passe de distribution d'autre part. NMAS intercepte les requêtes entrantes concernant la modification des mots de passe et les gère en fonction de vos paramètres dans les règles de mots de passe, à l'exception de certaines méthodes existantes. Pour plus d'informations, reportez-vous à la section « Planification des méthodes de login et de modification des mots de passe de vos utilisateurs », page 111. Pour obtenir un exemple de l'interface de règle de mot de passe dans laquelle vous pouvez contrôler la relation entre les mots de passe eDirectory, consultez la figure de la section « Activation du mot de passe universel », page 102.

Identity Manager contrôle la relation entre les mots de passe eDirectory 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 eDirectory que vous pouvez fournir aux systèmes connectés. À l'instar du mot de passe universel, le mot de passe de distribution est protégé par quatre niveaux de codage et il est réversible.

Dans la règle de mot de passe, vous pouvez préciser si le mot de passe de distribution doit être identique au mot de passe universel, grâce au 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 d'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. Pour plus d'informations, reportez-vous à la section « Gestion des informations sensibles », page 184. 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 règle de mot de passe, vous pouvez transférer les mots de passe dans des tunnels entre les systèmes connectés à l'aide du mot de passe de distribution, sans utiliser ni affecter le mot de passe universel ou le mot de passe NDS.

Pour plus d'informations sur les divers mots de passe eDirectory, reportez-vous au manuel *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html). Pour obtenir différents exemples d'utilisation de la synchronisation des mots de passe avec Identity Manager, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202.

Comparaison entre la version 1.0 de la synchronisation des mots de passe et la 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
Version du produit	Produit distinct de DirXML.	Fonctionnalité incluse dans Identity Manager et qui n'est pas vendue séparément.

	Version 1.0 de la synchronisation des mots de passe	Version de la synchronisation des mots de passe fournie avec Identity Manager 2
Plate-formes	◆ Active Directory ◆ NT Domain ◆ eDirectory	Ces plate-formes prennent entièrement en charge la synchronisation bidirectionnelle des mots de passe : ◆ Active Directory ◆ eDirectory ◆ NIS ◆ NT Domain Ces systèmes connectés prennent en charge l'acheminement des mots de passe vers Identity Manager. Le mot de passe universel et le mot de passe de distribution sont réversibles ; Identity Manager peut donc distribuer les mots de passe aux systèmes connectés. Tout système connecté prenant en charge l'élément de mot de passe Abonné peut souscrire à des mots de passe d'Identity Manager. Reportez-vous à la section Connected System Support for Password Synchronization (Prise en charge des systèmes connectés pour la synchronisation des mots de passe) dans le manuel *Novell Nsure Identity Manager 2 Administration Guide (Guide d'administration Novell Nsure Identity Manager 2)*
Mot de passe utilisé dans eDirectory	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 Implementing Password Synchronization (Mise en œuvre de la synchronisation des mots de passe) dans le manuel *Novell Nsure Identity Manager 2 Administration Guide (Guide d'administration Novell Nsure Identity Manager 2)*

	Version 1.0 de la synchronisation des mots de passe	Version de la synchronisation des mots de passe fournie avec Identity Manager 2
Fonctionnalité principale pour les systèmes Windows connectés	Pour envoyer des mots de passe à DirXML de sorte que les mots de passe eDirectory et Windows soient synchronisés. 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 prises en charge.	Prises en charge.
Novell Client™	Obligatoire.	Non obligatoire.
Attribut nadLoginName	Utilisé pour garantir la mise à jour des mots de passe.	Non utilisé.
Composant contenant la fonctionnalité de synchronisation des mots de passe	Le pilote DirXML contenait la fonctionnalité destinée à la mise à jour de nadLoginName.	Les règles de la configuration du pilote possèdent 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 DirXML, et qui sont issues de la logique des règles. Le manifeste du pilote, les valeurs de configuration globales (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 « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.
Agents	Partie distincte du logiciel.	Aucun agent n'est installé : la fonctionnalité fait maintenant partie intégrante du pilote.

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 d'Identity Manager et peuvent aussi fournir le mot de passe de l'utilisateur à Identity Manager. Ces systèmes connectés prennent en charge la synchronisation bidirectionnelle des mots de passe avec Identity Manager. Il s'agit de :

- Active Directory
- Novell® eDirectory™
- NIS
- NT Domain

Pour ces systèmes connectés, l'utilisateur peut modifier un mot de passe dans l'un des systèmes et de procéder à la synchronisation de ce mot de passe avec les autres systèmes via Identity Manager. Toutefois, si vous utilisez les règles de mots de passe avancées, il vaut mieux que les utilisateurs modifient leurs mots de passe dans la console en libre-service d'iManager, qui reste le meilleur endroit pour modifier les mots de passe car tous les principes 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 à les envoyer à Identity Manager, en définissant des règles au sein même de la configuration du pilote.

Plusieurs autres systèmes peuvent accepter des mots de passe d'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 « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 175.

Fonctionnalités de la synchronisation des mots de passe d'Identity Manager

Pour expliquer les fonctionnalités proposées par la synchronisation des mots de passe d'Identity Manager, nous pouvons orienter la synchronisation bidirectionnelle dans deux directions : les mots de passe envoyés par des systèmes connectés et acceptés par Identity Manager, et les mots de passe distribués par Identity Manager et acceptés par les systèmes connectés.

Les sections suivantes décrivent les fonctionnalités de synchronisation des mots de passe d'Identity Manager :

Identity Manager accepte les mots de passe des systèmes connectés

Comme dans les versions précédentes de DirXML®, tout système connecté peut éditer un mot de passe sur le système de protection des identités.

Vous pouvez préciser les applications des systèmes connectés dont Identity Manager acceptera les mots de passe. Vous pouvez même choisir si Identity Manager doit mettre à jour le mot de passe des utilisateurs dans l'arborescence eDirectory dans laquelle s'exécute Identity Manager ou s'il doit simplement agir à la manière d'une conduite ou d'un tunnel, en ne synchronisant les mots de passe qu'entre les systèmes connectés. Cela implique qu'il est possible de distinguer le mot de passe eDirectory de celui distribué par Identity Manager aux systèmes connectés.

Certains systèmes connectés (AD, autres arborescences eDirectory, 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 le mot de passe à Identity Manager dans une feuille de style, par exemple un mot de passe initial basé sur le nom ou l'ID du salarié.

Identity Manager distribue les mots de passe aux systèmes connectés

La synchronisation des mots de passe d'Identity Manager permet désormais de distribuer un mot de passe commun aux système connectés.

Dans les versions précédentes de DirXML, un pilote pouvait envoyer des mots de passe à DirXML 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® dans eDirectory n'étant pas réversible, il était impossible de transférer un mot de passe du système central de protection des identités d'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 nouveau mot de passe universel fourni par eDirectory 8.7.3 est réversible, et peut donc être distribué.

Identity Manager accepte les mots de passe des systèmes connectés ; du fait de sa réversibilité, le mot de passe Identity Manager peut être distribué depuis le système de protection des identités vers les systèmes connectés qui prennent en charge la définition des mots de passe initiaux pour les 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 règles de mot de passe.

Pour plus d'informations sur le mot de passe universel et le mot de passe de distribution dans la synchronisation des mots de passe, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202.

Comme avec les autres attributs d'un utilisateur, vous pouvez choisir quels systèmes deviendront des sources expertes pour les mots de passe ; Identity Manager distribuera les mots de passe depuis la source experte vers les autres systèmes connectés.

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

Identity Manager applique les règles de mot de passe dans la banque de données et sur les systèmes connectés

En appelant NMAS™, Identity Manager permet d'appliquer les règles de mot de passe sur les mots de passe entrants. Si le mot de passe édité depuis un système connecté vers Identity Manager ne respecte pas les règles, vous pouvez paramétrer Identity Manager de sorte qu'il n'accepte pas le mot de passe dans le système de protection des identités. Cela signifie aussi que les mots de passe qui ne respectent pas vos règles ne seront pas distribués aux autres systèmes connectés.

En outre, Identity Manager permet d'appliquer les règles de mot de passe sur les systèmes connectés. Si le mot de passe édité vers Identity Manager ne respecte pas les règles, vous pouvez paramétrer Identity Manager de sorte qu'il n'accepte pas le mot de passe pour la distribution, voire qu'il réinitialise le mot de passe incompatible sur le système connecté à l'aide du mot de passe de distribution actuel dans le système de protection des identités.

Par exemple, si vous voulez que les mots de passe incluent au moins un caractère numérique, mais si le système connecté ne peut pas appliquer une telle règle, vous pouvez demander à Identity Manager que les mots de passe du système connecté non-conforme soient réinitialisés.

Si vous utilisez les règles de mots de passe avancées et la synchronisation des mots de passe via Identity Manager, nous vous conseillons de rechercher les règles de mot de passe de tous les systèmes connectés afin de vérifier que les règles de mots de passe avancées définies dans la règle de mot de passe eDirectory sont compatibles ; les mots de passe peuvent ainsi être synchronisés sans problème.

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

Les règles de mot de passe sont assignées dans une perspective centrée sur l'arborescence. Par opposition, la synchronisation des mots de passe est définie par pilote ; ceux-ci sont installés sur les serveurs et ne peuvent gérer que les utilisateurs existants d'une réplique principale ou d'une réplique 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 règles de mot de passe en activant le mot de passe universel. L'assignation d'une règle de mot de passe au conteneur racine d'une partition garantit que cette règle s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

Pour plus d'informations sur l'assignation des règles de mot de passe aux utilisateurs, reportez-vous à la section « Assignation de règles de mot de passe aux utilisateurs », page 120.

Identity Manager propose plusieurs scénarios pour synchroniser les mots de passe

Comme avec d'autres attributs d'objet, Identity Manager permet de choisir les systèmes qui deviendront des sources expertes pour les mots de passe. Identity Manager permet de choisir comment faire circuler les mots de passe.

La plupart des nouvelles fonctionnalités de la synchronisation des mots de passe dans Identity Manager repose sur le mot de passe universel, la nouvelle fonction de mot de passe réversible d'eDirectory.

Toutefois, certains scénarios fonctionnent sans déploiement du mot de passe universel.

La synchronisation des mots de passe dans Identity Manager repose aussi sur le mot de passe de distribution, c'est-à-dire sur le référentiel à partir duquel Identity Manager distribue les mots de passe vers les systèmes connectés. Comme pour le mot de passe universel, une règle peut être appliquée au mot de passe de distribution.

Pour obtenir une liste des principales manières de mettre en œuvre la synchronisation des mots de passe, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202. Ces scénarios peuvent être associés pour répondre aux besoins de votre environnement.

Identity Manager peut synchroniser les mots de passe sous Windows en l'absence du client Novell

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

Identity Manager peut avertir les utilisateurs des échecs de synchronisation des mots de passe

La section précédente, « Identity Manager applique les règles de mot de passe dans la banque de données et sur les systèmes connectés », page 172, explique comment Identity Manager peut appliquer les règles de mot de passe en refusant les mots de passe non-concordants des systèmes connectés.

Grâce à la nouvelle fonctionnalité de notification par message électronique, vous pouvez demander à Identity Manager d'avertir l'utilisateur lorsqu'une modification de mot de passe a échoué.

Supposons que vous avez paramétré Identity Manager pour ne pas accepter un mot de passe entrant dans NT Domain s'il ne respecte pas votre règle de mot passe, et que vous avez activé la notification par message électronique. L'un des principes de votre règle de mot de passe indique que le nom de la société ne peut pas servir de mot de passe ; l'utilisateur change son mot de passe sur le système connecté à NT Domain et utilise le nom de la société. Dans ce cas, 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 le texte des messages envoyés par Identity Manager ou encore en adresser une copie à l'administrateur. Pour plus d'informations, reportez-vous à la section « Configuration de la notification par message électronique », page 243.

Identity Manager peut vérifier l'état de synchronisation du mot de passe pour un utilisateur

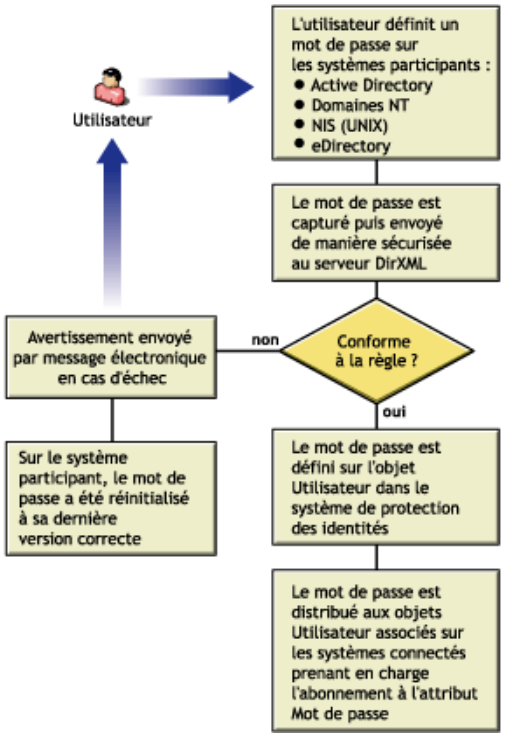
Identity Manager permet d'interroger les systèmes connectés pour vérifier la situation de la synchronisation du mot de passe pour un utilisateur. Si le système connecté prend en charge la vérification du mot de passe, vous verrez si la synchronisation des mots de passe a réussi.

Pour plus d'informations sur la vérification des mots de passe, reportez-vous à la section « Vérification de l'état de synchronisation du mot de passe pour un utilisateur », page 242.

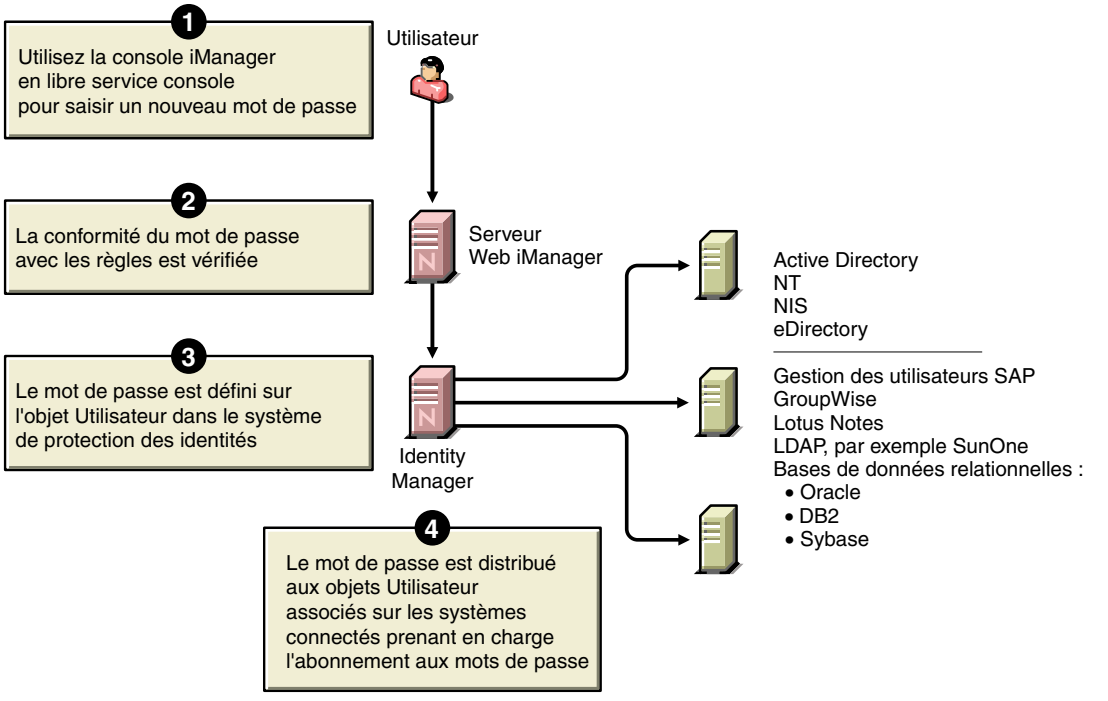
Pour obtenir une liste des systèmes qui prennent en charge la vérification des mots de passe, reportez-vous à la section « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 175.

Diagrammes des flux de synchronisation des mots de passe

Voici une présentation des systèmes connectés qui éditent des mots de passe vers Identity Manager :



Voici une présentation d'Identity Manager distribuant des mots de passe vers les systèmes connectés :



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

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 un mot de passe de la part d'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.

D'autres systèmes peuvent fournir des données qui permettront de créer des mots de passe, grâce à la définition d'une règle au sein même de la configuration du canal Éditeur. Les exemples de configuration pour la plupart des pilotes décrivent ceci ; une règle est incluse qui propose un mot de passe par défaut basé sur le Nom.

Les systèmes connectés peuvent, de diverses manières, accepter un mot de passe de la part d'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.

Cette section contient une liste des systèmes connectés et des éléments pris en charge par les exemples de configuration de pilotes.

Les fonctionnalités des exemples de configuration de pilotes sont notées dans le manifeste du pilote. Ce tableau fournit des informations complémentaires qui ne se trouvent pas dans le manifeste du pilote :

- En ce qui concerne la capacité de l'application à accepter un mot de passe, le tableau indique si une application accepte un ensemble initial de mots de passe pour le nouveau compte ou si, au contraire, elle accepte la modification d'un mot de passe existant.

  Le manifeste indique si le système connecté accepte un mot de passe, mais ne fait pas cette distinction.

- Le groupement des pilotes permet de voir quels exemples de configuration des pilotes ont les mêmes capacités.

Pilote de système connecté	Canal Abonné L'application accepte la définition du mot de passe initial	Canal Abonné L'application accepte la modification du mot de passe	Canal Abonné L'application prend en charge la vérification du mot de passe	Canal Éditeur L'application peut fournir (synchroniser) un mot 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 sur le système connecté et acceptent les mots de passe provenant d'Identity Manager.**				
Active Directory	Oui	Oui	Oui	Oui
eDirectory[1]	Oui	Oui	Oui	Oui
NT Domain	Oui	Oui	Non	Oui
NIS	Oui	Oui	Oui	Oui
SIF	Oui	Oui	Non	Oui

Pilote de système connecté	Canal Abonné L'application accepte la définition du mot de passe initial	Canal Abonné L'application accepte la modification du mot de passe	Canal Abonné L'application prend en charge la vérification du mot de passe	Canal Éditeur L'application peut fournir (synchroniser) un mot de passe
Les systèmes connectés suivants acceptent, à un certain degré, des mots de passe provenant d'Identity Manager. Ils ne peuvent pas fournir à Identity Manager le mot de passe de l'utilisateur sur le système connecté. **Néanmoins, ils peuvent être configurés de manière à créer un mot de passe qui utilisera une règle sur le canal Éditeur, en fonction d'autres données utilisateur présentes dans le système connecté (les exemples de configuration de pilotes montrent le mot de passe par défaut basé sur le nom de famille).**				
GroupWise®	Oui	Oui	Non	Non[2]
JDBC	Oui[3]	Non[4]	Non	Non[5]
LDAP	Oui[6]	Oui[6]	Oui	Non
Notes	Oui	Oui[7]	Oui[7]	Non
Gestion des utilisateurs SAP	Oui	Oui	Non	Non
Les systèmes connectés suivants n'acceptent pas les mots de passe et ne fournissent pas le mot de passe de l'utilisateur sur le système connecté à l'aide de l'exemple de configuration du pilote. **Néanmoins, ils peuvent être configurés de manière à créer un mot de passe qui utilisera une règle sur le canal Éditeur, en fonction d'autres données utilisateur présentes dans le système connecté (les exemples de configuration de pilotes montrent le mot de passe par défaut basé sur le nom de famille).**				
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
Les systèmes connectés suivants n'ont pas pour objet d'être utilisés avec la synchronisation des mots 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 Manual Task Service	Non	Non	Non	Non

[1]La synchronisation bidirectionnelle des mots de passe est disponible pour les utilisateurs entre les arborescences eDirectory, même si le mot de passe universel n'est pas activé pour ces utilisateurs. Reportez-vous à la section « Scénario 1 : synchronisation des mots de passe dans eDirectory à l'aide du mot de passe NDS », page 203.

[2]GroupWise prend en charge deux méthodes d'authentification. 1) GroupWise fournit sa propre authentification et conserve les mots de passe utilisateur. 2) GroupWise utilise LDAP pour procéder à l'authentification par rapport à eDirectory et ne conserve pas les mots de passe. Avec l'option 2, les mots de passe synchronisés par le pilote sont ignorés par GroupWise.

[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 DirXML pour JDBC peut servir à modifier un mot de passe sur le système connecté, mais la 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.

[8]Le pilote DirXML 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.

Conditions préalables à la synchronisation des mots de passe

La synchronisation des mots de passe dépend de la mise en œuvre des éléments suivants :

- « Prise en charge du mot de passe universel », page 177
- « Capacités de synchronisation des mots de passe déclarées dans le manifeste du pilote », page 178
- « Paramètres de synchronisation des mots de passe à créer à l'aide des valeurs de configuration globales », page 178
- « Règles requises pour la configuration du pilote », page 182
- « Filtres que vous installez sur le système connecté pour capturer les mots de passe », page 183
- « Règles de mot de passe que vous créez pour vos utilisateurs », page 184
- « Méthodes de login NMAS », page 184

Prise en charge du mot de passe universel

Reportez-vous à la section « Préparation à l'utilisation du mot de passe universel », page 192.

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 :

- Édition du mot de passe de l'utilisateur vers Identity Manager
- Acceptation d'un mot de passe provenant d'Identity Manager (le manifeste ne fait pas la distinction entre l'acceptation de la création d'un mot de passe initial et l'acceptation des modifications apportées au mot de passe)
- 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 pour un utilisateur

Remarque : le manifeste du pilote est rédigé par le développeur du pilote ou par l'expert Identity Manager qui crée sa configuration. Il n'a pas pour objet d'être modifié par un administrateur réseau. Il représente les véritables fonctionnalités du module d'interface pilote et sa configuration ; la modification du manifeste seul ne modifie donc pas les fonctionnalités. Pour ajouter des fonctionnalités, il faudrait améliorer le module d'interface pilote, le système connecté ou la configuration du pilote.

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 « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.

Paramètres de synchronisation des mots de passe à créer à l'aide des valeurs de configuration globales

Identity Manager a introduit les valeurs de configuration globales, qui permettent de définir une valeur constante que vous pouvez référencer dans une règle. On les appelle parfois variables de serveurs, car elles sont contenues dans un attribut dépendant de chaque réplique.

Pour la synchronisation bidirectionnelle 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 règles de synchronisation des mots de passe étant écrites de manière à se comporter différemment selon vos paramètres de valeur de configuration globale, il est désormais plus facile de changer le flux des mots de passe sans avoir à modifier les règles.

Grâce aux valeurs de configuration globales, vous contrôlez les paramètres suivants séparément pour chaque système connecté. Sachez qu'Identity Manager est appelé DirXML au niveau de l'interface.

- Si Identity Manager accepte les mots de passe 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 règles lors de 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 Identity Manager.

- La méthode de synchronisation utilisée par Identity Manager, en mettant directement à jour le mot de passe universel ou 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 de ce que vous avez défini dans la règle de mot de passe, sous Mot de passe universel > Options de configuration.

  Pour consulter des exemples de scénarios avec ces méthodes, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202.

- Si les règles de mot de passe sont appliquées sur les mots de passe entrants dans Identity Manager depuis un système connecté.

  Si elles sont appliquées, cela signifie que les mots de passe entrants ne sont pas écrits dans la banque de données Identity Manager s'ils ne sont pas conformes.

- Si Identity Manager applique les règles de mot de passe sur un système connecté en réinitialisant les mots de passe non-conformes, à l'aide du mot de passe Identity Manager.

  Cette option est grisée dans l'interface si le système connecté ne la prend pas en charge (tel que déclaré dans le manifeste du pilote).

- Si le système connecté accepte les mots de passe.

  Ce paramètre s'applique à un mot de passe distribué par Identity Manager, ainsi qu'à un mot de passe qui pourrait être créé par les règles 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.

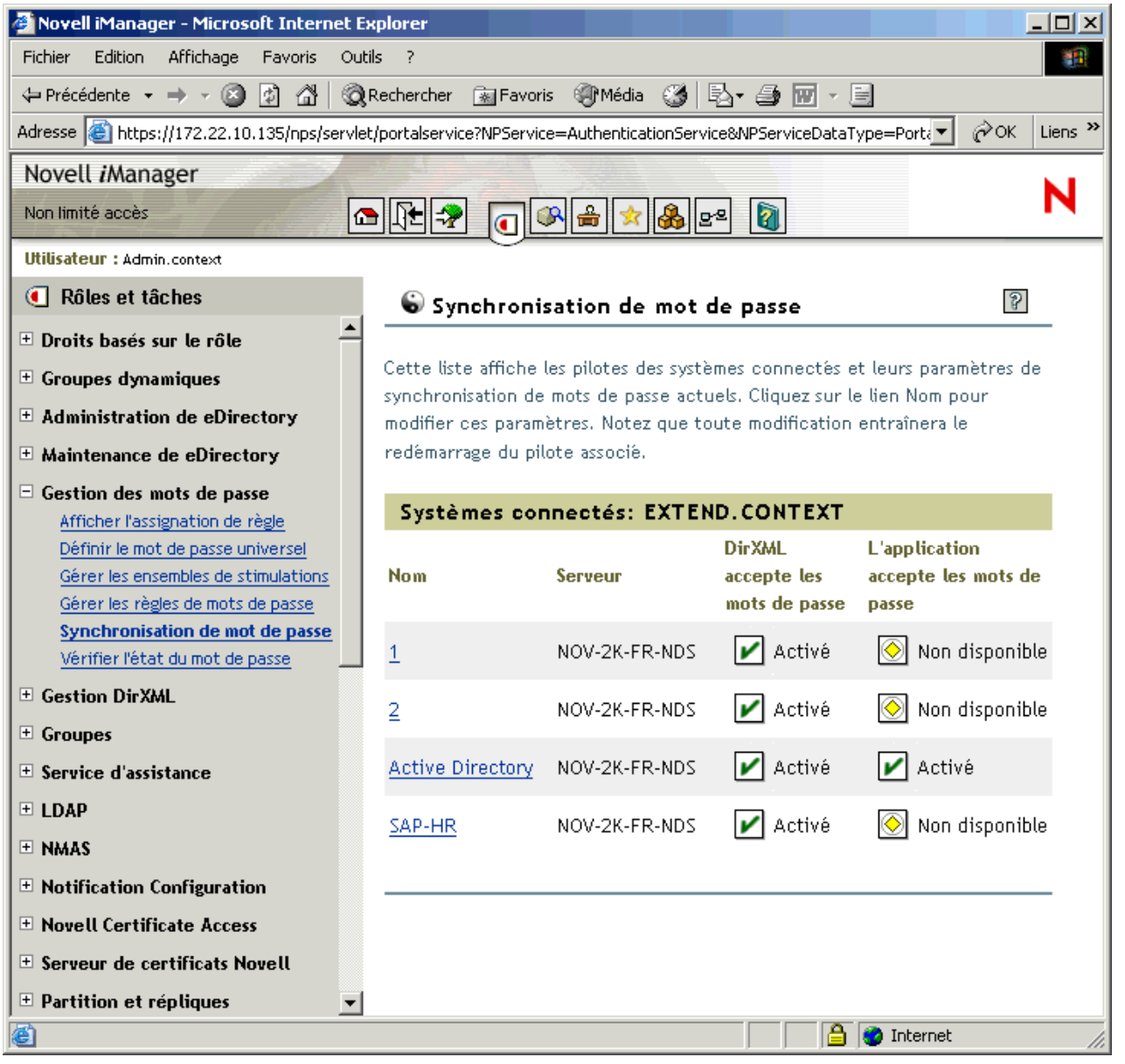
  Cette option est grisée dans l'interface si le système connecté ne la prend pas en charge (tel que déclaré dans le manifeste du pilote).

- Si les utilisateurs sont avertis par message électronique lorsqu'un mot de passe n'est pas synchronisé.

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 « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.

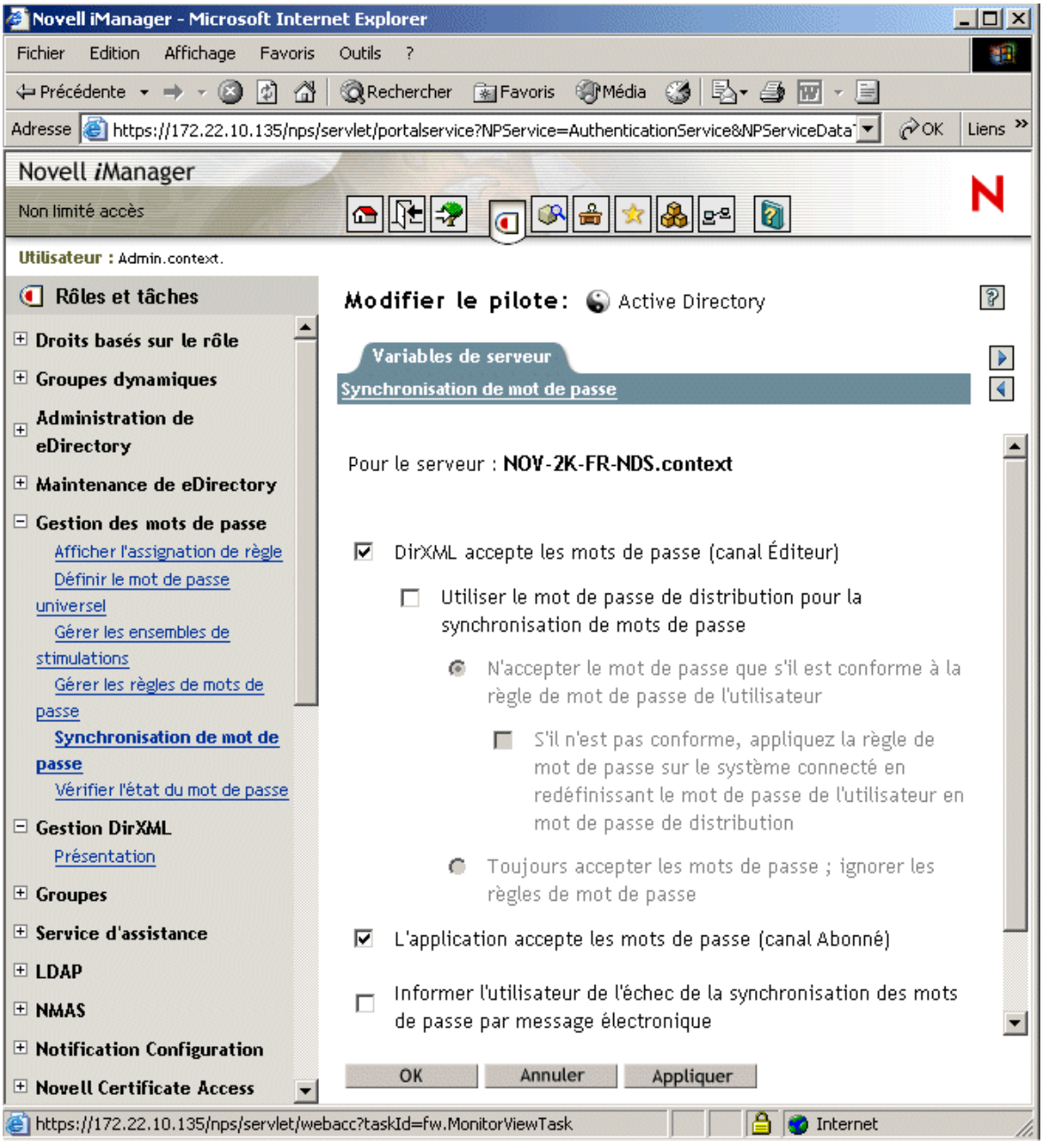
La tâche de synchronisation des mots de passe dans in iManager (Gestion des mots de passe > Synchronisation de mot de passe) permet de modifier ces GCV. Cette interface graphique permet de spécifier la manière dont les mots de passe doivent être répartis entre les systèmes connectés et Identity Manager.

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



Sur cette page, cliquez sur le nom d'un pilote pour voir tous les paramètres que vous contrôlez.

La figure ci-après montre la page qui s'affiche. Il s'agit de l'interface graphique permettant de définir les valeurs de configuration globales pour la synchronisation des mots de passe.



Lorsqu'une option de cette page est grisée, cela signifie que le système connecté ne la prend pas en charge, tel qu'indiqué dans le manifeste du pilote.

Remarque : cette interface permet de définir les valeurs de configuration globales séparément sur chaque pilote. Les valeurs de configuration globales d'un pilote écrasent celles de l'ensemble de pilotes ; leur définition sur un pilote spécifique permet un contrôle plus granulaire. Cette page peut n'afficher que les valeurs de configuration globales présentes sur chaque pilote.

Les valeurs de configuration globales peuvent être définies sur l'objet Ensemble de pilotes ; un pilote de cet ensemble peut en hériter s'il ne dispose pas de valeurs propres. Si un pilote ne possède pas de paramètres propres et s'il hérite donc des valeurs de configuration globales de l'ensemble de pilotes, cette interface ne les affiche pas. Elles seront malgré tout honorées par les règles de synchronisation des mots de passe.

Règles requises pour la configuration du pilote

Les règles des canaux Éditeur et Abonné pour chaque pilote régissent le flux des mots de passe, en fonction des paramètres que vous avez définis dans les valeurs de configuration globales décrites ci-dessus.

Ces règles sont incluses dans les configurations de pilote d'Identity Manager.

Si, au lieu de la remplacer, vous mettez à niveau la configuration de pilote existante, vous devrez ajouter ces règles à la configuration. Pour plus d'informations, reportez-vous à la section « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.

Pour que la synchronisation des mots de passe fonctionne, ces règles doivent se trouver dans la configuration de votre pilote, au bon emplacement.

Emplacement dans la configuration de pilote	Nom de la règle de synchronisation des mots de passe	Action de la règle
Transformation de commande du canal Éditeur Ces règles doivent être insérées dans cet ordre, puisqu'elles doivent apparaître en dernier dans l'ensemble de règles 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 règle et la règle Password(Sub)-Default Password Policy sont les seules que vous pouvez modifier ou supprimer. Les autres ne doivent pas être modifiées pour que la synchronisation des mots de passe fonctionne.
	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. Le GCV indique enable-password-publish ; le message DirXML accepte les mots de passe de l'application s'affiche.
	Password(Pub)-Publish Distribution Password	Transforme l'élément <password> pour mettre à jour le mot de passe universel. Cette règle référence les GCV suivantes : publish-password-to-dp et 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 règle 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 règle de synchronisation des mots de passe	Action de la règle
Transformation de l'entrée du canal Éditeur Nous vous recommandons de répertorier cette règle en dernier s'il existe plusieurs règles dans la transformation de l'entrée.	Password(Pub)-Sub Email Notifications	Si les informations de charge traversent 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 règle référence la GCV nommée notify-user-on-password-dist-failure pour déterminer s'il faut envoyer les messages électroniques de notification.
Transformation de commande du canal Abonné Ces règles doivent être insérées dans cet ordre, puisqu'elles doivent apparaître en dernier dans l'ensemble de règles de 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 règle et la règle Password(Pub)-Default Password Policy sont les seules que vous pouvez modifier ou supprimer. Les autres ne doivent pas être modifiées pour que la synchronisation des mots de passe fonctionne.
	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. Le GCV indique enable-password-subscribe ; le message L'application accepte les mots de passe de la zone de stockage DirXML s'affiche.
	Password(Sub)-Add Password Payload	Intègre des données de charge transférées dans le moteur, à des fins de notification par message électronique.
Transformation de la sortie du canal Abonné Nous vous recommandons de répertorier cette règle en dernier s'il existe plusieurs règles dans la transformation de la sortie.	Password(Sub)-Pub Email Notifications	Si les informations de charge traversent et si l'état indique un problème, il envoie un message électronique à l'utilisateur. Cette règle référence la GCV nommée notify-user-on-password-dist-failure pour déterminer s'il faut envoyer les messages électroniques de notification.

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

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

Reportez-vous à la section « Définition des filtres de mots de passe », page 237.

Règles de mot de passe que vous créez pour vos utilisateurs

Les règles de mot de passe doivent permettre d'activer le mot de passe universel pour vos utilisateurs, même si vous pouvez utiliser certaines fonctionnalités de la synchronisation des mots de passe en l'absence de mot de passe universel. La règle 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 de l'utilisateur avec les règles a été vérifiée.

Vous devez comprendre les règles de mot de passe pour utiliser la synchronisation des mots de passe d'Identity Manager.

Les règles de mot de passe sont décrites au Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101.

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 en savoir plus sur les méthodes de login, reportez-vous au manuel *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html).

Gestion des informations sensibles

La synchronisation des mots de passe dans Identity Manager permet de simplifier les mots de passe utilisateur et de réduire les frais du service d'assistance. Parmi les nouvelles fonctionnalités, on compte la synchronisation bidirectionnelle des mots de passe, qui permet de partager les mots de passe entre eDirectory et les systèmes connectés de plusieurs manières, tel que décrit dans les scénarios de la section « Mise en œuvre de la synchronisation des mots de passe », page 202.

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.

Dans le cadre de la planification de l'utilisation d'Identity Manager et de la synchronisation des mots de passe, consultez les conseils de sécurité suivants.

- « Utilisation de SSL », page 185
- « Accès sécurisé à eDirectory et aux objets Identity Manager », page 185
- « Révision des points de sécurité pour la gestion des mots de passe », page 185
- « Création de règles de mot de passe performantes », page 187
- « Sécurisation des systèmes connectés qui participent à la synchronisation des mots de passe », page 187
- « Meilleures pratiques du marché à suivre en matière de sécurité », page 188
- « Utilisation de Nsure Audit pour suivre les modifications apportés aux informations sensibles », page 188

Utilisation de SSL

Lorsque c'est possible, il est conseillé d'activer SSL pour tous les transports. SSL doit être activé pour la communication entre le moteur DirXML et le Chargeur distant (reportez-vous à la section « Sécurisation des transferts de données », page 73), et entre le moteur DirXML 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.

Accès sécurisé à eDirectory et aux objets Identity Manager

Sécurité physique : protégez l'accès à l'emplacement physique des serveurs sur lesquels est installé Novell eDirectory.

Droits d'accès : des droits administratifs sont nécessaires pour 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 :

- L'ensemble de pilotes DirXML
- Le pilote DirXML
- Les objets de configuration des pilotes (filtres, feuilles de style, règles), en particulier les règles utilisées pour la récupération ou la synchronisation des mots de passe
- Les objets de la règle 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

Révision des points de sécurité pour la gestion des mots de passe

- Les objets de la règle de mot de passe sont lisibles par le public, pour permettre aux applications de vérifier si les mots de passe sont compatibles. Cela signifie qu'un utilisateur non-authentifié pourrait demander à eDirectory de trouver les règles de mot de passe appliquées. Si ces règles exigent des utilisateurs qu'ils créent des mots de passe forts, cela ne présentera aucun risque, comme indiqué à la section « Création de règles de mot de passe performantes », page 187.
- 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 largement contribuer à réduire les appels de demande d'assistance.

  Pour des raisons de sécurité, les indices de mot de passe sont contrôlés pour 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.

Pour 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 règle de mot de passe, est l'une des manières de le faire. Reportez-vous à la section « Ajout de votre propre message de modification du mot de passe aux règles de mot de passe », page 152.

Si vous choisissez ne pas utiliser d'indice de mot de passe, vérifiez que vous ne l'utilisez dans aucune règle de mot de passe que ce soit. Pour empêcher de définir des indices de mots de passe, vous pouvez être plus radical et supprimer totalement le gadget Configuration de l'indice, comme décrit à la section « Désactivation du mot de passe par suppression du gadget Indice », page 149.

- 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 règle de mot de passe, est l'une des manières de le faire. Reportez-vous à la section « Ajout de votre propre message de modification du mot de passe aux règles de mot de passe », page 152.
- Pour des raisons de sécurité, les opérations relatives à l'oubli de 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 fonction d'amélioration de la sécurité a été ajoutée à NMAS 2.3.4 en ce qui concerne 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, pour des raisons de sécurité, le mot de passe précédent expire automatiquement si vous avez activé le paramètre d'expiration des mots de passe dans la règle des 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.

Création de règles de mot de passe performantes

Les règles 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 pour 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. Pour mieux se protéger des attaques de dictionnaire, il vaut probablement mieux exiger l'utilisation de chiffres ou de caractères spéciaux.

N'oubliez pas que vous pouvez créer plusieurs règles de mot de passe si vous avez des exigences différentes dans les diverses parties de l'arborescence. Vous pouvez assigner une règle de mot de passe à la totalité de l'arborescence, au conteneur racine d'une partition, à un conteneur, voire à un utilisateur. Pour simplifier l'administration, nous vous recommandons d'assigner des règles 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 règle de mot de passe. Reportez-vous à la section Managing User Accounts (Gestion des comptes utilisateur) du manuel *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).

Sécurisation des systèmes connectés qui participent à la synchronisation des mots de passe

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.

Meilleures pratiques du marché à suivre en matière de sécurité

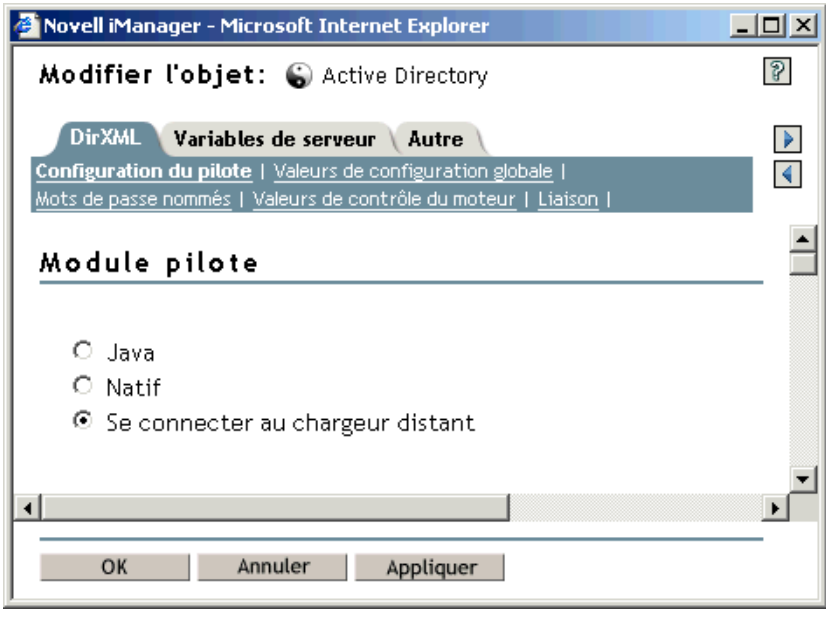
Respectez bien les meilleures pratiques de sécurité du marché, concernant notamment le blocage des ports non utilisés sur le serveur.

Utilisation de Nsure Audit pour suivre les modifications apportés aux informations sensibles

Vous pouvez utiliser Nsure Audit pour consigner les événements que vous considérez importants pour la sécurité. Pour plus d'informations sur Nsure Audit, reportez-vous au Chapitre 13, « Consignation et création de rapports avec Nsure Audit », page 291.

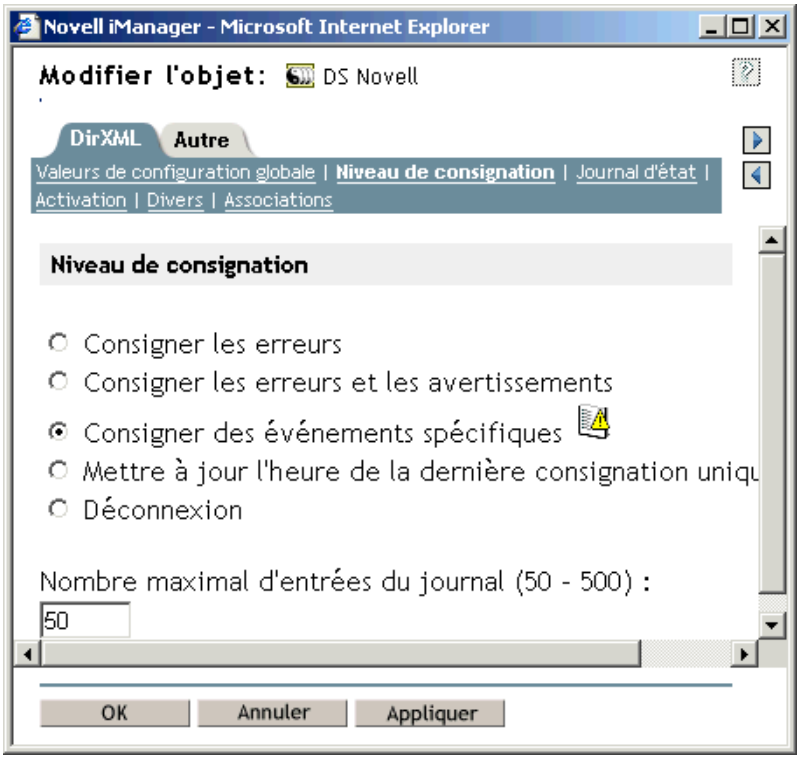
Vous pouvez par exemple consigner les modifications apportées aux mots de passe pour un pilote DirXML particulier, voire pour un ensemble de pilotes, en procédant comme suit :

1. Dans l'onglet DirXML des propriétés d'un pilote (ou d'un ensemble de pilotes), cliquez sur Niveau de consignation.



2 Sur la page Niveau de consignation, cliquez sur Consigner des événements spécifiques.

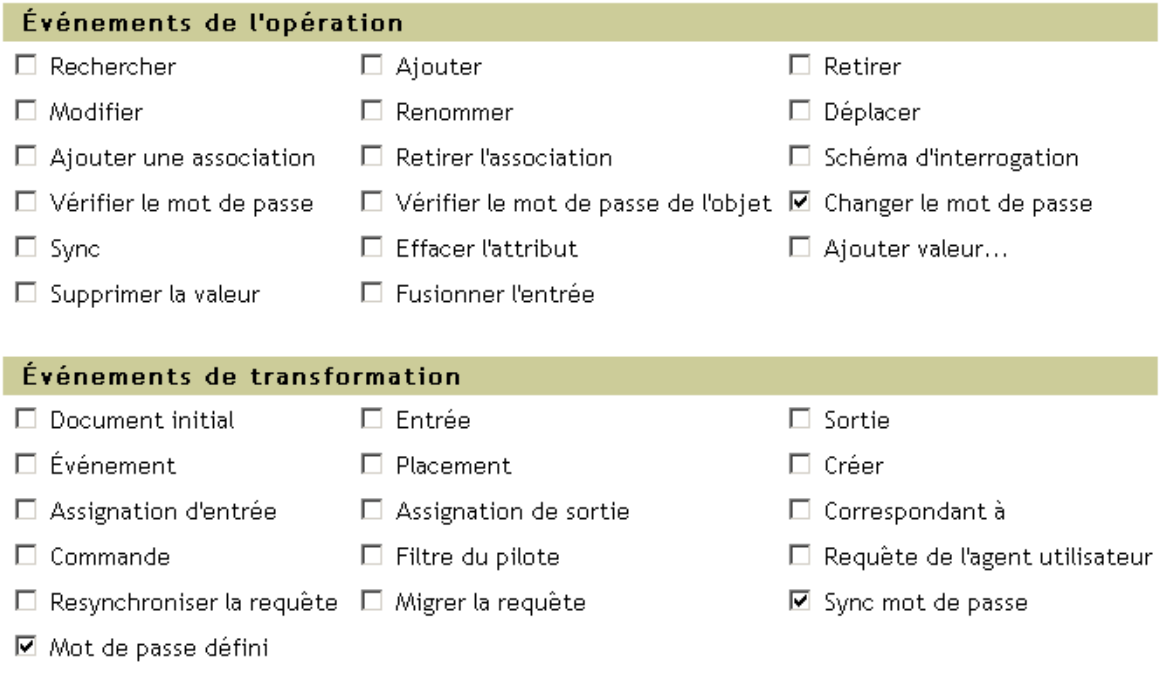
Dans cette page, indiquez si le pilote possède ses propres paramètres ou s'il utilise ceux de l'ensemble de pilotes.



3 Pour sélectionner des événements spécifiques, cliquez sur l'icône de consignation des événements .

4 Sur la page Activités, cochez les cases suivantes :

- Dans Événements de l'opération, Changer le mot de passe. Cet élément surveille les modifications directes du mot de passe NDS.
- Dans Événements de transformation, 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 sur la page Activités et à nouveau sur la page Niveau de consignation.

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

Cette section contient les informations suivantes :

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 règle de mot de passe, l'utilisateur doit renseigner le mot de passe.

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 (il n'est pas obligatoire pour la synchronisation des mots de passe dans Identity Manager), déployez le nouveau client Novell qui prend en charge le mot de passe universel. À la prochaine connexion des utilisateurs à l'aide du nouveau 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. Pour plus d'informations, reportez-vous à la section « Planification des méthodes de login et de modification des mots de passe de vos utilisateurs », page 111.
- Si vous n'utilisez pas le client Novell, demandez aux utilisateurs de se connecter à la console en libre-service d'iManager. Cette méthode de connexion renseigne le mot de passe universel. Pour accéder à la console en libre-service d'iManager, accédez à /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.

Modification des mots de passe à l'aide de la console en libre-service d'iManager ou du client Novell

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

Selon la configuration du flux de mots de passe, un utilisateur pourrait modifier un mot de passe sur un système connecté ; il serait alors synchronisé avec Identity Manager et 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 incompatibles, il est recommandé de demander aux utilisateurs de ne modifier le mot de passe que dans la console en libre-service d'iManager ou le client Novell, ou au moins de s'assurer que les règles de mot de passe avancées sont bien communiquées aux utilisateurs.

Dans un système connecté, l'utilisateur est autorisé à modifier le mot de passe sans consulter les principes de la règle de mot de passe ; il est alors possible qu'il en oublie certains. Seules les règles du système connecté lui-même seront 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 règle 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 eDirectory. 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 incompatibles sur les systèmes connectés, l'utilisateur ne pourra pas se connecter avec le nouveau mot de passe choisi sur le système connecté.

  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 compatible que l'utilisateur a créé.

Préparation à l'utilisation du mot de passe universel

La plupart des informations dont vous avez besoin se trouvent à la section Deploying Universal Password (Déploiement du Mot de passe universel) du manuel *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html).

Vous devez en outre vous souvenir que :

- eDirectory version 8.7.1 ou supérieure est nécessaire à l'utilisation du mot de passe universel. NetWare 6.5 n'est pas obligatoire et la documentation NetWare a été mise à jour pour traduire cet état de fait.
- La synchronisation des mots de passe dans Identity Manager repose sur le mot de passe universel et sur un nouveau type de mot de passe, le mot de passe de distribution, c'est-à-dire sur le référentiel à partir duquel Identity Manager distribue les mots de passe vers les systèmes connectés. Comme pour le mot de passe universel, les règles peuvent être appliquées au mot de passe de distribution.
- Les plugs-in DirXML iManager, livrés avec Identity Manager, incluent les nouveaux plugs-in de gestion des mots de passe, qui permettent de créer des Règles de mot de passe. Ces plugs-in permettent 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 ceux du mot de passe universel qui étaient livrés avec NetWare 6.5. Ils sont décrits au Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101.
- eDirectory 8.6. 2 ne peut pas être utilisé pour l'arborescence qu'Identity Manager utilise. Toutefois, eDirectory 8.6. 2 est pris en charge pour un sous-ensemble de fonctions de synchronisation des mots de passe, de sorte qu'il puisse être utilisé avec d'autres arborescences si vous n'êtes pas prêt à mettre votre environnement à niveau.
- 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 système de protection des identités. De nombreux environnements utilisent déjà un système de protection des identités pour DirXML et les pilotes.

- Le mot de passe universel vous apporte de nouvelles fonctionnalités qui n'étaient pas prises en charge par les précédents outils de gestion des mots de passe, comme l'application des règles 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 « Planification des méthodes de login et de modification des mots de passe de vos utilisateurs », page 111.
- La version la plus récente du client Novell prend en charge le mot de passe universel, peut le compléter pour un utilisateur lorsque vous activez le mot de passe universel pour la première fois pour cet utilisateur, et peut afficher et appliquer les règles de mot de passe lorsque les utilisateurs modifient leurs mots de passe.
- Un système connecté n'affiche pas les règles de mot de passe avancées que vous créez dans une règle de mot de passe. Pour l'heure, c'est également le cas du client Novell, même s'il les applique.

  Il vaut mieux demander aux utilisateurs de ne modifier le mot de passe que dans la console en libre-service d'iManager.

  Si vous autorisez les utilisateurs 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 compatible et à garantir que les principes de la règle de mot de passe ont été communiqués aux utilisateurs.
- Avertissez les administrateurs et les utilisateurs du service d'assistance 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 la dérive des mots de passe, c'est-à-dire la désynchronisation entre le mot de passe NDS et le mot de passe universel.

  Le manuel *Novell Modular Authentication Services (NMAS) 2.3 Administration Guide (Guide d'administration de NMAS (Novell Modular Authentication Services) 2.3)* (http://www.novell.com/documentation/nmas23/index.html) référence un TID qui répertorie les utilitaires et la façon dont ils prennent en charge le mot de passe universel.

Planification des répliques et des règles de mot de passe

Les règles de mot de passe sont assignées dans une perspective centrée sur l'arborescence. Par opposition, la synchronisation des mots de passe est définie par pilote ; ceux-ci sont installés sur les serveurs et ne peuvent gérer que les utilisateurs existants d'une réplique principale ou d'une réplique 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 règles de mot de passe en activant le mot de passe universel. L'assignation d'une règle de mot de passe au conteneur racine d'une partition garantit que cette règle s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

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 eDirectory ont rempli l'attribut Adresse de messagerie Internet.

Suivez les instructions de la section « Configuration de la notification par message électronique », page 243.

Nouvelle configuration de pilote et synchronisation des mots de passe sous Identity Manager

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 nouveau pilote ou remplacez une configuration Identity Manager existante par une nouvelle configuration, respectez les instructions suivantes pour configurer la nouvelle 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 « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 190.
2. Créez un nouveau pilote ou remplacez la configuration du pilote existant par la configuration d'Identity Manager 2.

   Les configurations d'Identity Manager contiennent les règles et autres éléments nécessaires à la synchronisation des mots de passe dans Identity Manager. Pour plus d'informations sur l'importation de nouveaux exemples de configuration de pilotes, reportez-vous aux Guide des pilotes DirXML (http://www.novell.com/documentation/beta/dirxmldrivers).
3. Activez le mot de passe universel pour les utilisateurs en créant les règles de mot de passe, l'option Mot de passe universel étant activée.

   Reportez-vous à la section « Création de règles de mot de passe », page 119. Si vous avez déjà utilisé le mot de passe universel avec NetWare 6.5, des étapes complémentaires sont décrites à la section « (NetWare 6.5 uniquement) Nouvelle création des assignations du mot de passe universel », page 117.

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

   Dans une règle de mot de passe, Mot de passe universel > Options de configuration, des options permettent de définir les méthodes de synchronisation des différents mots de passe par NMAS.

   Pour obtenir des exemples de scénarios utilisant la synchronisation des mots de passe et savoir comment intégrer les règles de mot de passe, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202. Consultez également l'aide en ligne.

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

Pour plus d'informations, consultez le guide de mise en œuvre du pilote de chacun de ces pilotes, disponible sur le site de documentation sur les pilotes DirXML (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

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

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 Consultez les paramètres actuels pour le flux de mots de passe. Il s'agit d'une interface graphique permettant de définir les valeurs de configuration globales (GCV). Modifiez-les en cliquant sur le nom d'un pilote.

Vous pouvez modifier les paramètres pour 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 de ce que vous avez défini dans la règle de mot de passe, sous Mot de passe universel > Options de configuration
- si la règle de mot de passe pour l'utilisateur est appliquée aux modifications de mots de passe entrants dans Identity Manager
- si la règle 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

Pour plus d'informations et pour consulter des captures d'écran de ces options, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202. Consultez également l'aide en ligne.

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 éditent les mots de passe vers Identity Manager.

Pour obtenir des astuces de dépannage, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202.

Mise à niveau de la version 1.0 de la synchronisation des mots de passe vers la synchronisation des mots de passe sous Identity Manager

Cette tâche ne s'applique qu'aux pilotes DirXML 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, consultez les guides de mise en œuvre de chaque pilote DirXML pour Active Directory, disponible sur le site de documentation sur les pilotes DirXML (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

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

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 vos configurations de pilote existantes par des exemples de configuration sous Identity Manager.

Important : si vous mettez à niveau un pilote DirXML pour AD ou NT Domain, et s'il 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 de mise en œuvre des pilotes DirXML pour Active Directory et NT Domain, disponible sur le site de documentation sur les pilotes DirXML (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

Remarque : les règles 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 eDirectory pour ne synchroniser que le mot de passe NDS, il est recommandé de ne pas utiliser ces règles dans la configuration de pilote eDirectory. Le mot de passe NDS est synchronisé à l'aide des attributs Clé publique et Clé privée et non à l'aide de ces règles, comme cela est décrit à la section « Scénario 1 : synchronisation des mots de passe dans eDirectory à l'aide du mot de passe NDS », page 203.

Voici les tâches que vous devrez accomplir en suivant les procédures de cette section :

- Convertissez le pilote au format Identity Manager 2.
- Ajoutez le manifeste de pilote, les valeurs de configuration globales et les règles de synchronisation des mots de passe à la configuration du pilote. Pour obtenir une liste des règles que vous ajoutez, reportez-vous à la section « Règles requises pour la configuration du pilote », page 182.
- Modifiez les paramètres de filtre pour l'attribut nspmDistributionPassword.
- Configurez le flux de synchronisation des mots de passe.

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 ne fonctionnent pas sans le nouveau module d'interface pilote Identity Manager, comme la fonction Vérifier l'état des mots de passe par exemple.

  Important : si vous mettez à niveau un pilote DirXML pour AD ou NT Domain, et s'il est utilisé avec la version 1.0 de la synchronisation des mots de passe, n'installez pas le module d'interface pilote tant que vous n'avez pas consulté les instructions de mise à niveau. Suivez les instructions de mise à niveau des guides de mise en œuvre de chaque pilote DirXML pour Active Directory, disponible sur le site de documentation sur les pilotes DirXML (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

Procédure

1. Vérifiez que votre environnement est prêt à utiliser le mot de passe universel. Reportez-vous à la section « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 190.
2. Convertissez le pilote au format Identity Manager à l'aide d'un assistant. Reportez-vous à la section « Mise à niveau de la configuration d'un pilote de DirXML 1.x au format Identity Manager », page 83.
3. Dans iManager, cliquez sur Utilitaires DirXML > Importer des pilotes.

   Vous pouvez ajouter la prise en charge de la synchronisation des mots de passe sous Identity Manager à chaque pilote devant participer à la synchronisation des mots de passe, en important un fichier de configuration de type support pack intégré, de manière à ajouter en une seule fois les règles, le manifeste du pilote et les GCV.

   Après cela, ajoutez également l'attribut nspmDistributionPassword au filtre.

   Ces tâches sont décrites dans les étapes suivantes.
4. Sélectionnez l'ensemble de pilotes dans lequel se trouve le pilote existant.
5. Dans la liste des configurations de pilote, ne sélectionnez que l'élément intitulé Règles de synchronisation de mot de passe 2.0. Ce choix est répertorié sous Autres règles. Cliquez sur Suivant.

   Une liste des invites d'importation s'affiche.
6. Sélectionnez le pilote existant que vous souhaitez mettre à jour.
7. Sélectionnez le type de pilote dans la liste déroulante.

   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 d'Identity Manager ?
   - Le système connecté peut-il vérifier si le mot de passe correspond à celui d'Identity Manager ?

Les entrées du manifeste du pilote doivent être correctes pour que les règles 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 DirXML et des règles de configuration des pilotes ; il ne doit généralement pas être modifié par l'administrateur réseau.

8 Cliquez sur Suivant. Choisissez de mettre à jour tout ce qui concerne le pilote.

Cette option fournit le manifeste du pilote, les valeurs de configuration globales et les règles nécessaires à la synchronisation des mots de passe.

Le manifeste du pilote et les valeurs de configuration globales remplacent toute valeur existante. Il ne devrait toutefois pas y avoir de valeur à remplacer pour DirXML 1.*x* ; en effet, ces types de paramètres constituent une nouvelle fonctionnalité d'Identity Manager 2.

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

Remarque : si, malgré tout, vous devez enregistrer un manifeste de pilote ou des valeurs de configuration globales, choisissez l'option Ne mettre à jour que les règles sélectionnées dans ce pilote, puis cochez les cases correspondant à toutes ces règles. Cette option importe les règles de mot de passe mais ne modifie ni le manifeste de pilote ni les valeurs de configuration globales. Vous devez coller manuellement toute valeur supplémentaire.

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

À ce moment de la procédure, les nouvelles règles ont été créées en tant qu'objets Règle 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.

10 Insérez chacune des nouvelles règles à l'endroit qui convient dans la configuration du pilote existante. Si l'ensemble de règles comprend plusieurs règles, vérifiez que ces règles de synchronisation de mot de passe apparaissent au bas de la liste.

La liste des règles et l'endroit auquel les insérer se trouvent à la section « Règles requises pour la configuration du pilote », page 182.

Répétez ces étapes pour chaque règle.

10a Cliquez sur Gestion DirXML > Présentation. Sélectionnez l'ensemble de pilotes pour le pilote que vous êtes en train de mettre à jour.

10b Cliquez sur le pilote que vous venez de mettre à jour. Une page montrant une représentation graphique de la configuration de pilote s'affiche.

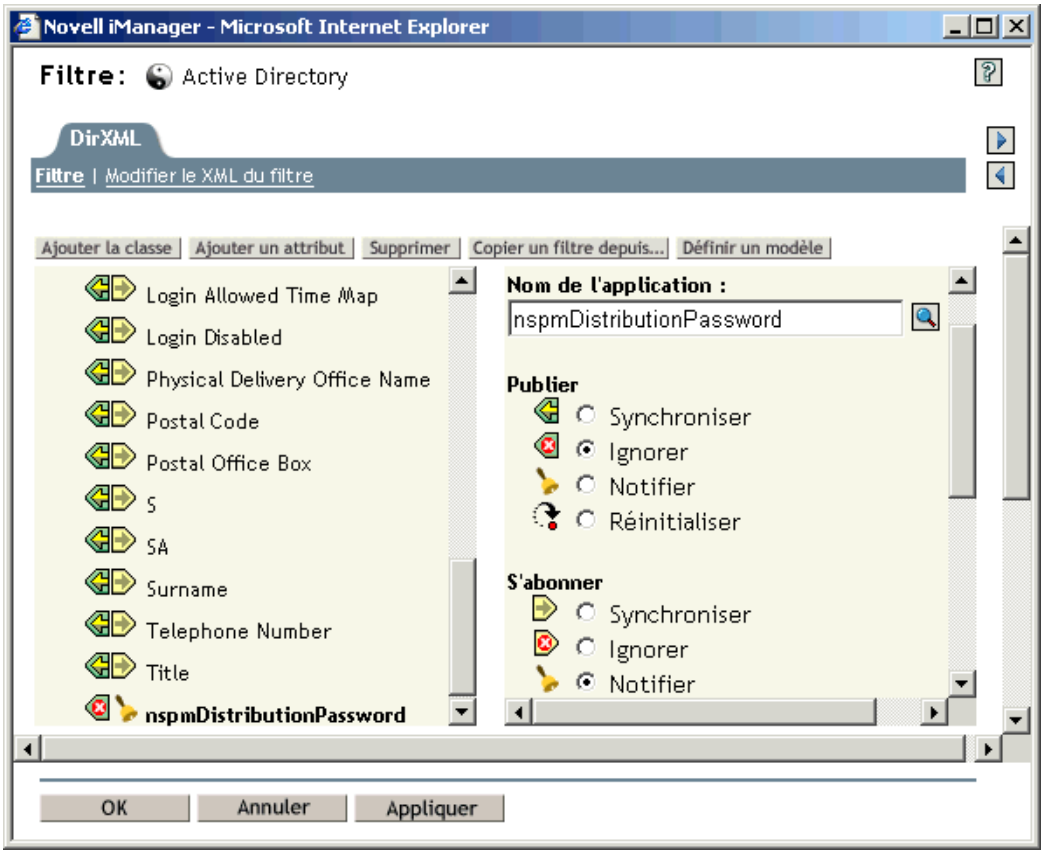
10c Cliquez sur l'icône pour savoir à quel endroit ajouter l'une des nouvelles règles.

10d Cliquez sur Insérer pour ajouter la nouvelle règle. Dans la page qui s'affiche, cliquez sur Utiliser une règle existante et recherchez le nouvel objet Règle. Cliquez sur OK.

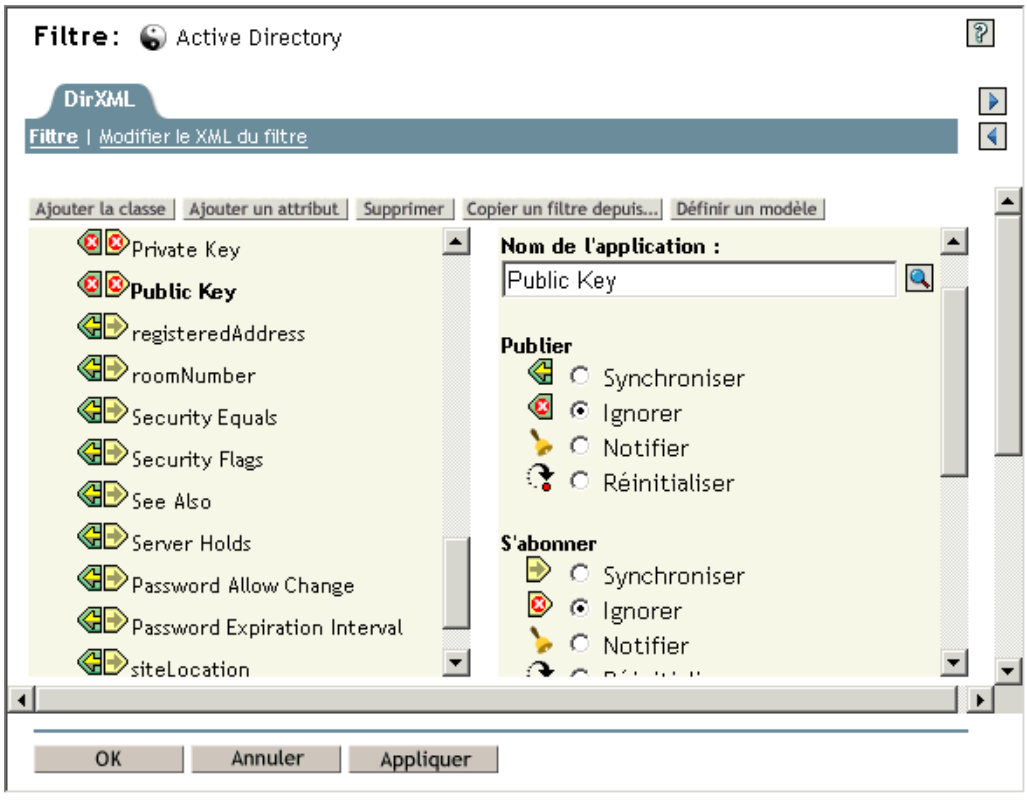
10e Si la liste contient plusieurs règles pour chacune des trois nouvelles règles, utilisez les flèches  pour déplacer les nouvelles règles vers le bon emplacement dans la liste. Vérifiez que les règles soient bien dans l'ordre indiqué à la section « Règles requises pour la configuration du pilote », page 182.

11 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 nspmDistributionPassword.



12 Ignorez les attributs Clé publique et Clé privée dans le filtre du pilote pour tous les objets dont l'attribut nspmDistributionPassword est défini sur Notifier.



13 Répétez cette procédure de l'Étape 2 à l'Étape 12 pour tous les pilotes que vous souhaitez mettre à niveau pour les voir participer à la synchronisation des mots de passe.

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 règles de synchronisation de mot de passe et les paramètres de filtre.

14 Reportez-vous aux guides de mise en œuvre de chaque pilote pour voir si des étapes ou des informations complémentaires sont nécessaires pour la configuration de la synchronisation des mots de passe dans Identity Manager, disponible sur le site de documentation sur les pilotes DirXML (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

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

Reportez-vous à la section « Création de règles de mot de passe », page 119. Si vous avez déjà utilisé le mot de passe universel avec NetWare 6.5, des étapes complémentaires sont décrites à la section « (NetWare 6.5 uniquement) Nouvelle création des assignations du mot de passe universel », page 117.

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

Dans une règle de mot de passe, Mot de passe universel > Options de configuration, des options permettent de définir les méthodes de synchronisation des différents mots de passe par NMAS. Les paramètres par défaut doivent convenir à la plupart des mises en œuvre. Pour plus d'informations, consultez l'aide en ligne de cette page.

Pour obtenir des exemples de scénarios utilisant la synchronisation des mots de passe et savoir comment intégrer les règles de mot de passe, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202.

Les règles de mot de passe sont assignées dans une perspective centrée sur l'arborescence. Par opposition, la synchronisation des mots de passe est définie par pilote ; ceux-ci sont installés sur les serveurs et ne peuvent gérer que les utilisateurs existants d'une réplique principale ou d'une réplique 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 règles de mot de passe en activant le mot de passe universel. L'assignation d'une règle de mot de passe au conteneur racine d'une partition garantit que cette règle s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

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

16a Dans iManager, cliquez sur Gestion des mots de passe > Synchronisation de mot de passe, puis recherchez les pilotes pour les systèmes connectés à gérer.

16b Consultez les paramètres actuels pour le flux de mots de passe. Il s'agit d'une interface graphique permettant de définir les valeurs de configuration globales (GCV). Modifiez-les en cliquant sur le nom d'un pilote.

Vous pouvez modifier les paramètres pour 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 de ce que vous avez défini dans la règle de mot de passe, sous Mot de passe universel > Options de configuration.
- si la règle de mot de passe pour l'utilisateur est appliquée aux modifications de mots de passe entrants dans Identity Manager
- si la règle 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

Pour plus d'informations et pour consulter des captures d'écran de ces options, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202. Consultez également l'aide en ligne.

17 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 éditent les mots de passe vers Identity Manager.

Pour obtenir des astuces de dépannage, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202.

Mise en œuvre de la synchronisation des mots de passe

La fonctionnalité de synchronisation des mots de passe fournie dans Identity Manager permet de mettre en œuvre 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 et les règles de mot de passe affectent la synchronisation des mots de passe. Ces scénarios peuvent être associés pour répondre aux besoins de votre environnement.

Cette section contient les informations suivantes :

Présentation de la relation entre Identity Manager et NMAS

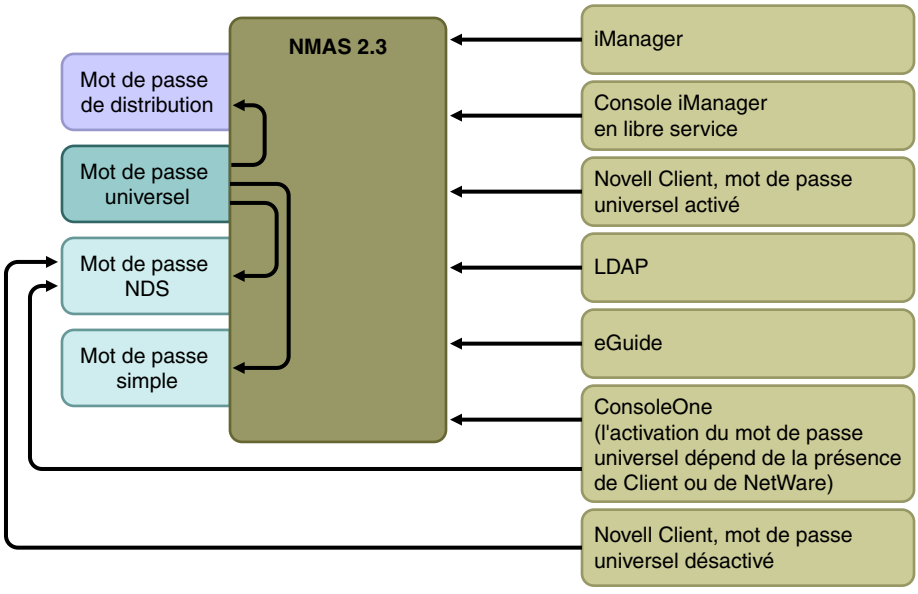
Cette section contient les informations suivantes :

Utilitaires et NMAS

Les derniers utilitaires en date, comme iManager et le client Novell, communiquent avec NMAS plutôt que de mettre à jour directement un mot de passe spécifique. NMAS est également l'entité qui détermine les mots de passe à mettre à jour.

NMAS synchronise les mots de passe dans eDirectory, en fonction des paramètres que vous avez configurés dans les règles de mot de passe.

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 de quelle manière les utilisateurs et les administrateurs du service d'assistance utilisent les utilitaires de votre environnement. Ils peuvent générer une désynchronisation entre le mot de passe universel et le mot de passe NDS (dérive du mot de passe) si vous utilisez le mot de passe universel et NMAS 2.3, car les utilitaires existants mettent directement à jour le mot de passe NDS au lieu de passer par NMAS. Vous devrez par exemple 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 pour assurer la prise en charge du mot de passe universel.



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 eDirectory.

Dans le scénario 1, le pilote DirXML 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, décrits plus loin dans cette section, Identity Manager permet de mettre à jour le mot de passe universel ou le mot de passe de distribution ; Identity Manager passe par NMAS pour effectuer ces modifications. Cela permet à NMAS de mettre à jour d'autres mots de passe eDirectory, comme déterminé par les paramètres des règles de mot de passe, et d'appliquer les règles de mot de passe avancées pour ceux qui sont 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 réside dans les différentes combinaisons de paramètres des règles de mot de passe NMAS et les paramètres de synchronisation de mot de passe Identity Manager pour chaque pilote de système connecté.

Scénario 1 : synchronisation des mots de passe dans eDirectory à l'aide du mot de passe NDS

Comme dans la version 1.0 de la synchronisation des mots de passe, vous pouvez synchroniser le mot de passe NDS entre deux arborescences eDirectory à l'aide du pilote eDirectory. Ce scénario n'exige pas la mise en œuvre du mot de passe universel et peut être utilisé avec eDirectory 8.6.2 ou 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 synchroniser des mots de passe au sein d'eDirectory. Elle ne fait pas appel à NMAS et ne peut donc pas être utilisée pour synchroniser les mots de passe avec les applications connectées.

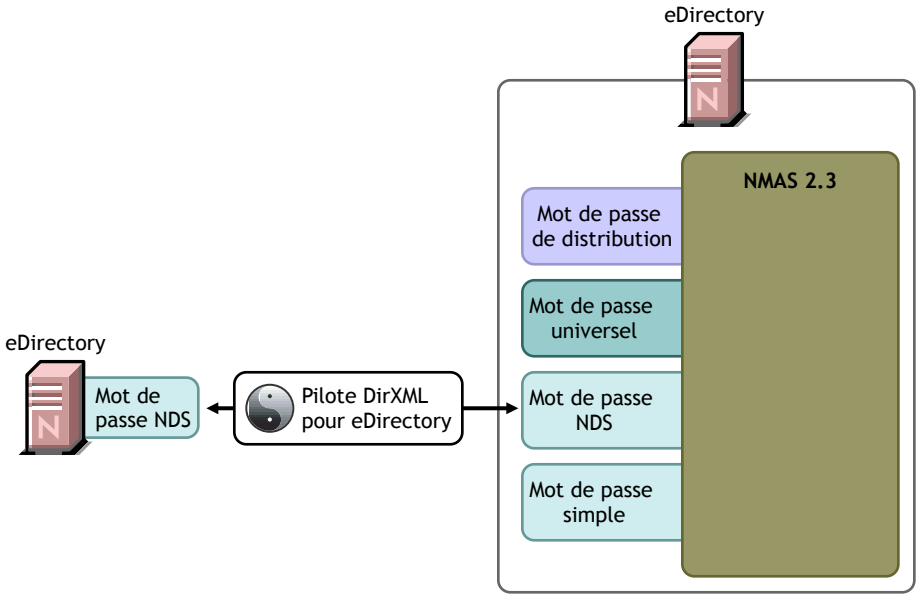
Cette section contient les informations suivantes :

Avantages et inconvénients du scénario 1

Avantages	Inconvénients
Simplicité de la configuration. N'inclut que les attributs adéquats dans le filtre de pilote. Si vous déployez Identity Manager 2et 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 règles de synchronisation des mots de passe aux configurations de pilote. ◆ N'exige pas que le mot de passe universel soit mis en œuvre dans l'arborescence Identity Manager 2. ◆ Peut être utilisé avec les arborescences connectées exécutant eDirectory version 8.6. 2ou 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 synchronise les mots de passe entre les arborescences eDirectory. 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'une autre arborescence 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 l'arborescence eDirectory connectée s'ils ne se conforment pas à la règle de mot de passe. Aucune notification par message électronique n'est fournie en cas d'échec de synchronisation des mots de passe. Les opérations Vérifier l'état des mots de passe, dans la tâche iManager, ne sont pas prises en charge (le mot de passe de distribution est obligatoire pour cette fonction).

Diagramme du scénario 1

Le diagramme montre que, comme dans DirXML 1.*x*, le pilote DirXML pour eDirectory peut être utilisé pour synchroniser le mot de passe NDS entre deux arborescences eDirectory. Ce scénario ne passe pas par NMAS.



Mise en œuvre du scénario 1

Pour mettre en œuvre ce type de synchronisation des mots de passe :

Déploiement du mot de passe universel

Inutile.

Configuration de la règle de mot de passe

Aucune.

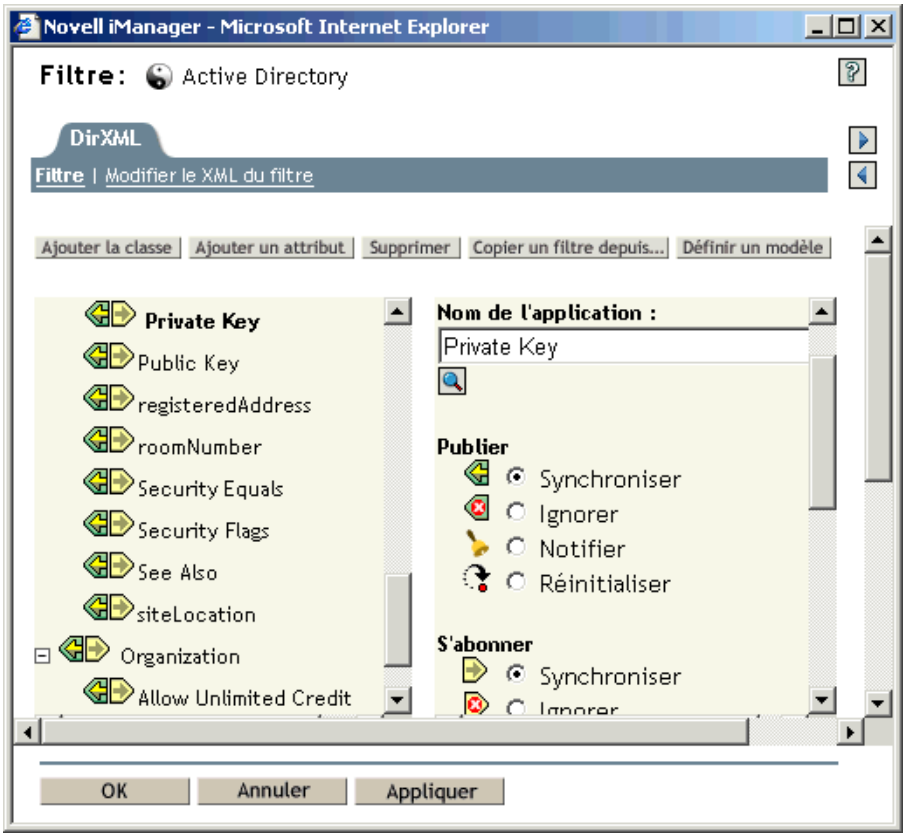
Paramètres de la synchronisation des mots de passe

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 règles de synchronisation des mots de passe répertoriées à la section « Règles requises pour la configuration du pilote », page 182. Ces règles 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 règles.

Vérifiez que le filtre des deux pilotes eDirectory synchronise les attributs Clé publique et Clé privée pour toutes les classes d'objet pour lesquelles les mots de passe doivent être synchronisés. La figure suivante en montre un exemple.



Dépannage du scénario 1

- Activez l'option DXML 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.
- Consultez également les astuces de la section « Dépannage des problèmes de synchronisation des mots de passe », page 258.

Scénario 2 : synchronisation du 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 eDirectory.

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 règle de mot de passe.

Tout système connecté peut éditer des mots de passe sur Identity Manager, bien que tous les systèmes connectés ne puissent pas fournir le mot de passe de l'utilisateur. Active Directory, par exemple, peut éditer 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 règle 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 « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 175.

Cette section contient les informations suivantes :

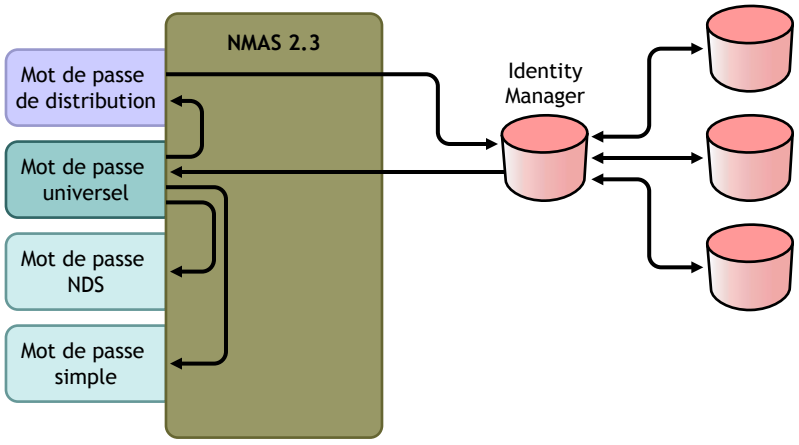
Avantages et inconvénients du scénario 2

Avantages	Inconvénients
Permet la synchronisation des mots de passe de et vers eDirectory et le système connecté. Permet la validation des mots de passe par rapport à la règle 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 à la règle de 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 règles de mot de passe, vous pouvez désactiver l'option Activer les règles de mots de passe avancées.	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 établis dans les règles de mot de passe.

Diagramme du scénario 2

Le diagramme montre que, dans ce scénario, les mots de passe entrent par Identity Manager, qui passe par NMAS pour mettre directement à jour le mot de passe universel. NMAS synchronise ensuite le mot de passe universel avec le mot de passe de distribution et les autres mots de passe, en fonction des paramètres de la règle de mot de passe. Enfin, 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.



Mise en œuvre du scénario 2

Pour mettre en œuvre ce type de synchronisation des mots de passe :

- « Déploiement du mot de passe universel », page 208
- « Configuration de la règle de mot de passe », page 208
- « Paramètres de la synchronisation des mots de passe », page 210
- « Configuration de pilote », page 212

Déploiement du mot de passe universel

Vérifiez que votre environnement est prêt à utiliser le mot de passe universel. Reportez-vous à la section « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 190.

Configuration de la règle de mot de passe

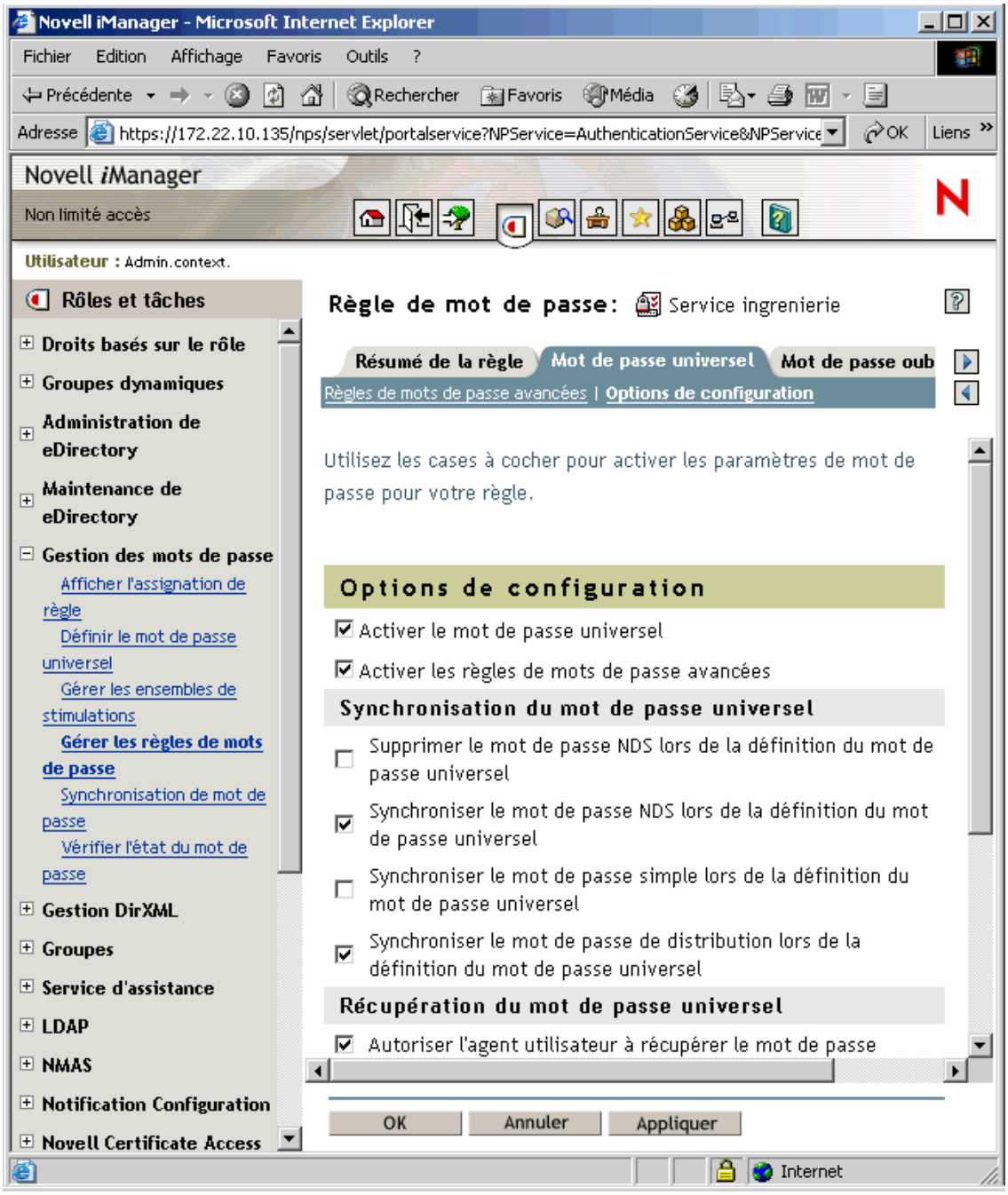
Dans Gestion des mots de passe > Gérer les règles de mots de passe, procédez comme suit :

1. Vérifiez qu'une règle de mot de passe est assignée aux parties de l'arborescence eDirectory pour lesquelles vous voulez disposer de la synchronisation des mots de passe. Vous pouvez l'assigner à la totalité de l'arborescence (grâce à un objet Règle de login), à un conteneur racine de partition, à un conteneur, voire à un utilisateur particulier. Nous vous recommandons d'assigner des règles de mot de passe au niveau le plus élevé possible de l'arborescence afin de simplifier l'administration.

2 Vérifiez que les éléments suivants sont sélectionnés dans la règle 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
- Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel

  Identity Manager récupérant 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.



3 Terminez votre règle 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 principes des règles de mot de passe, désactivez l'option Activer les règles de mots de passe avancées.

4 Si vous utilisez les règles de mot de passe avancées, vérifiez qu'elles n'entrent pas en conflit avec les règles de mot de passe de tout système connecté qui s'abonne aux mots de passe.

Paramètres de la synchronisation des mots de passe

Dans Gestion des mots de passe > Synchronisation de mot de passe, créez ces paramètres pour le pilote du système connecté :

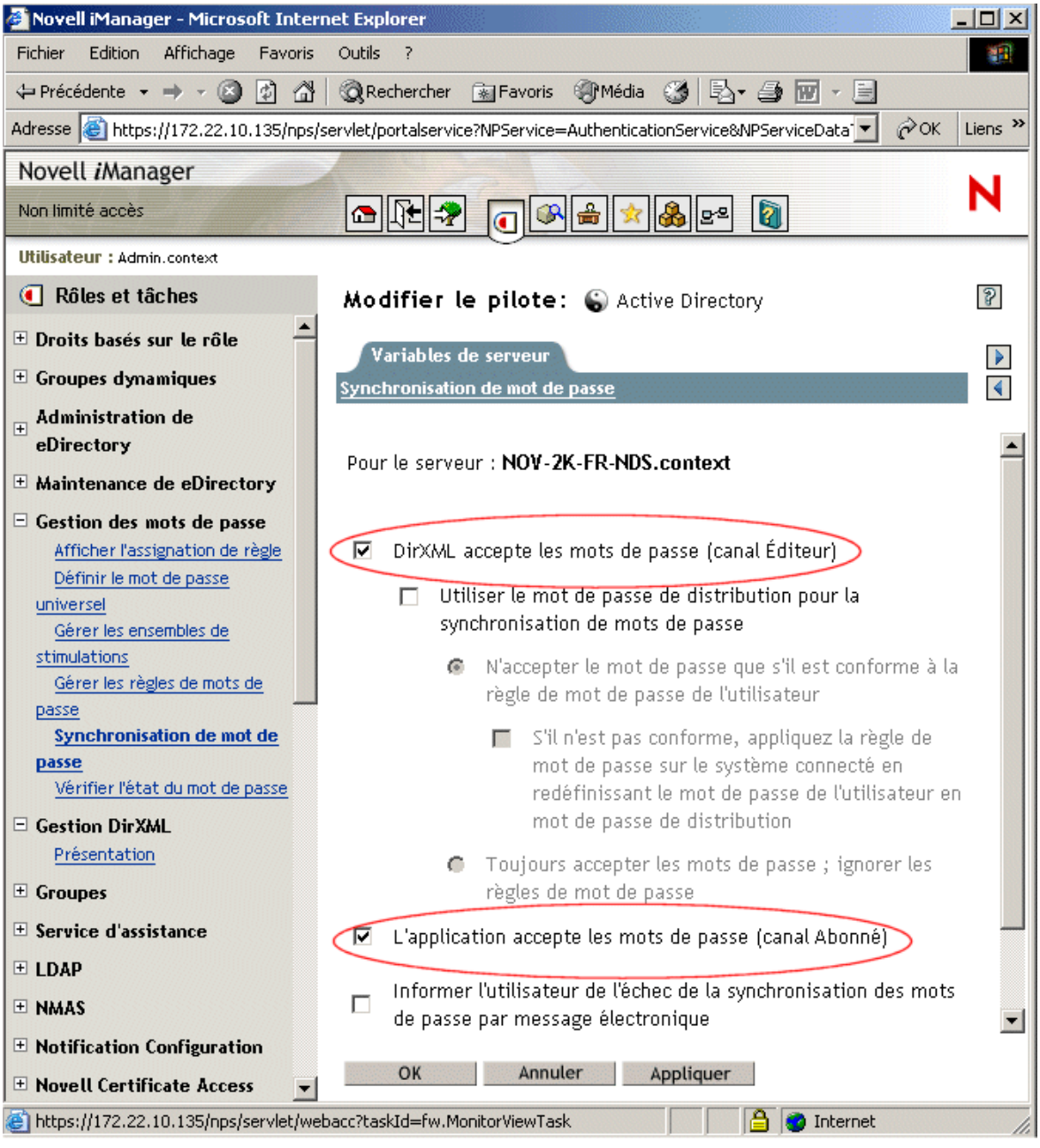
1 Vérifiez que les éléments suivants sont sélectionnés :

- DirXML accepte les mots de passe (canal Éditeur)

  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 édités, par la création d'un mot de passe dans la configuration d'un pilote à l'aide d'une règle.

- 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 règles 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 éditer, ne sélectionnez que l'option L'application accepte les mots de passe (canal Abonné).

2 Vérifiez que les éléments suivants sont sélectionnés :

- Utiliser le mot de passe de distribution pour la synchronisation de mots de passe

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.

3 (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'affectent pas le traitement du document XML qui a déclenché le message électronique ; si elles échouent, elles ne sont pas tentées à nouveau, à moins que l'opération elle-même ne le soit.

  Toutefois, les messages de débogage pour les notifications par message électronique sont écrits dans le fichier de trace.

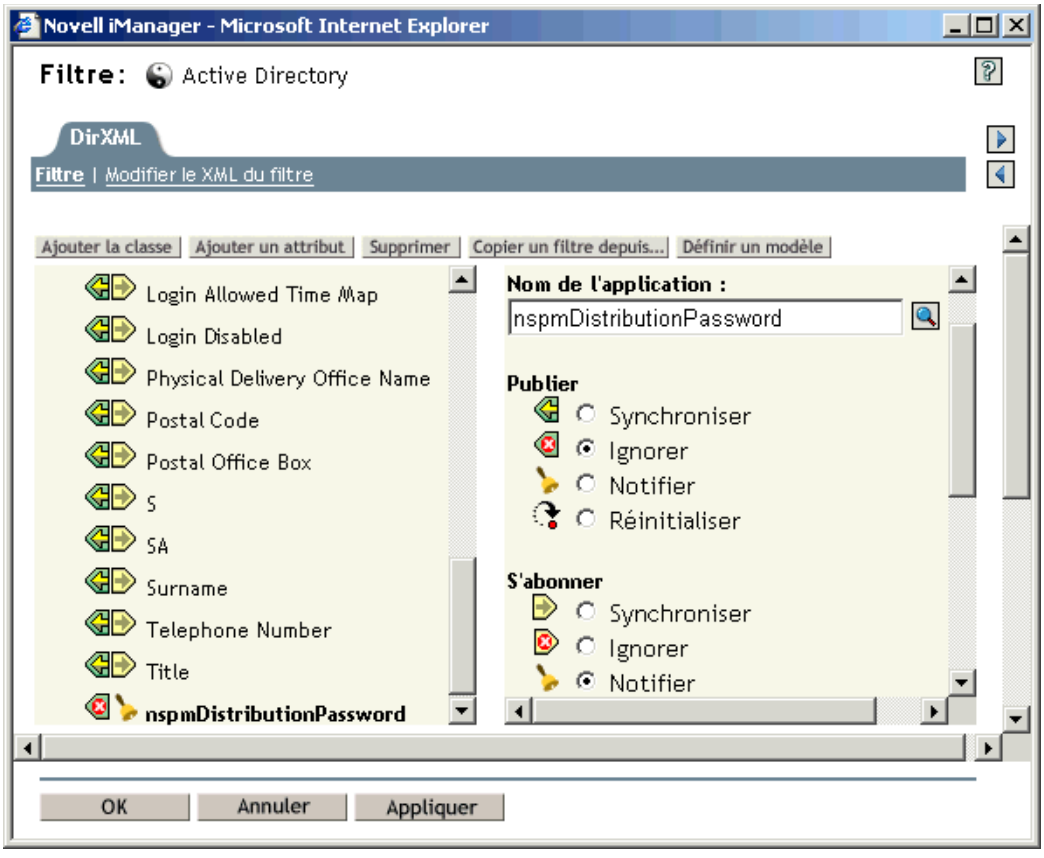
Configuration de pilote

1 Vérifiez que les règles 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 règles doivent se trouver dans la configuration de votre pilote, à l'endroit correct et dans le bon ordre. Pour obtenir la liste des règles, reportez-vous à la section « Règles requises pour la configuration du pilote », page 182.

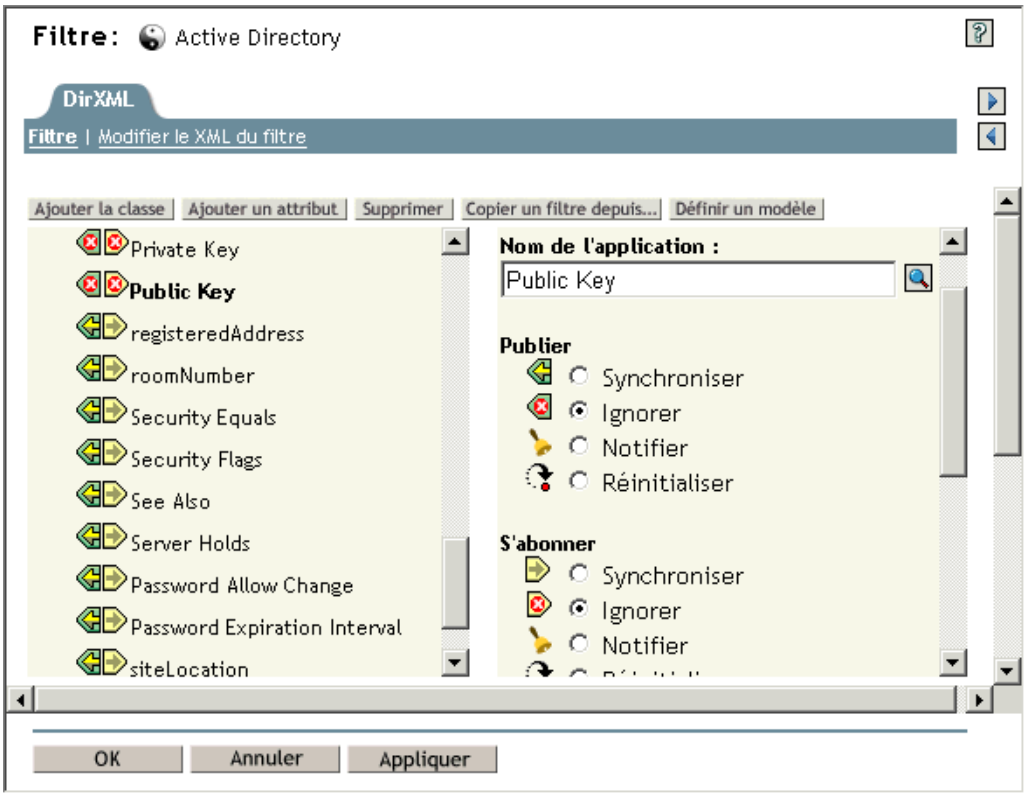
Les exemples de configuration Identity Manager contiennent déjà les règles. Si vous effectuez la mise à niveau d'un pilote existant, vous pouvez ajouter les règles à l'aide des instructions de la section « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.

2 Définissez correctement le filtre pour l'attribut nspmDistributionPassword :

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



3 Ignorez les attributs Clé publique et Clé privée dans le filtre du pilote pour tous les objets dont l'attribut nspmDistributionPassword est défini sur Notifier.



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

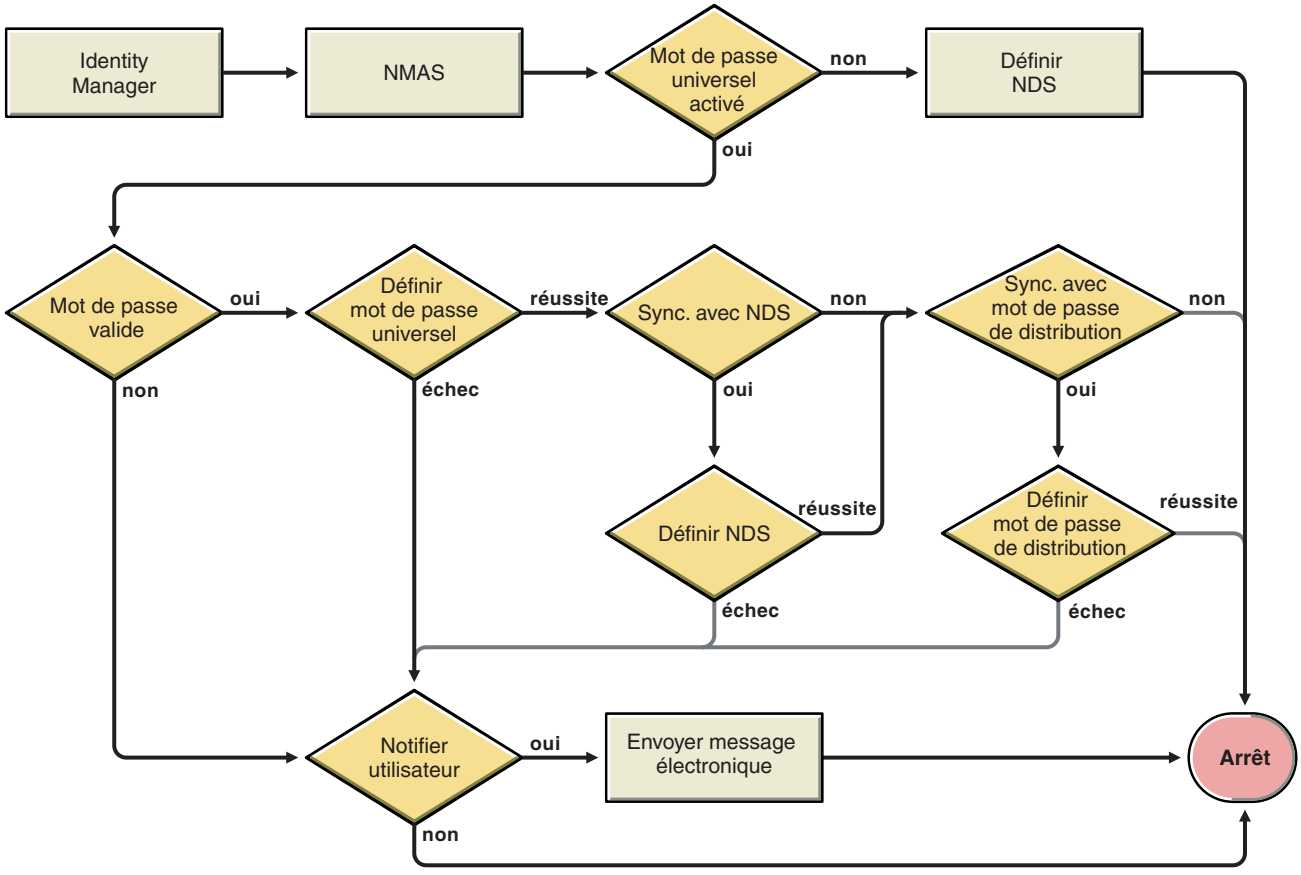
Cette section contient les informations suivantes :

- « Diagramme du scénario 2 », page 215
- « Problème de connexion à eDirectory », page 215
- « Problème pour se loguer à un autre système connecté qui s'abonne aux mots de passe », page 216
- « Le message électronique n'est pas généré en cas d'échec du mot de passe », page 216
- « Erreur lors de l'utilisation de la vérification du mot de passe de l'objet », page 217
- « Commandes DSTrace utiles », page 217

Consultez également les astuces de la section « Dépannage des problèmes de synchronisation des mots de passe », page 258.

Diagramme du scénario 2

Le diagramme suivant montre comment NMAS gère le mot de passe qu'il reçoit d'Identity Manager. Dans ce scénario, le mot de passe est synchronisé sur le mot de passe universel ; NMAS décide de la manière de gérer le mot de passe en fonction de son activation dans la règle de mot de passe, de l'activation des règles de mot de passe avancées pour les mots de passe entrants qui doivent s'y conformer, et des autres paramètres de la règle de mot de passe pour la synchronisation du mot de passe universel avec les autres mots de passe.



Problème de connexion à eDirectory

- Activez les paramètres +AUTH, +DCLN, +DXML et +DVRS dans DSTrace.
- Vérifiez que les éléments <password> ou <modify-password> sont transférés à Identity Manager. Pour ce faire, consultez l'écran de trace avec ces options activées.
- Vérifiez que le mot de passe est valide, en fonction des principes de la règle de mot de passe.
- Vérifiez la configuration et l'assignation de la règle de mot de passe NMAS. Essayez d'assigner directement la règle à l'utilisateur, en vérifiant que vous utilisez la bonne règle.
- Sur la page Synchronisation de mot de passe pour le pilote, vérifiez que l'option DirXML accepte les mots de passe est sélectionnée.
- Dans la règle 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 les situations dans lesquelles ce système connecté édite des mots de passe sur Identity Manager ; 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 traités les règles Identity Manager.
- Définissez le niveau de trace DirXML pour le pilote sur 3.
- Dans la page Synchronisation de mot de passe, vérifiez que l'option DirXML 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 213.
- Vérifiez que les éléments <password> pour un ajout ou <modify-password> sont transférés au système connecté. Pour cela, consultez l'écran DSTRACE ou le fichier contenant les options de trace actives, comme indiqué dans les premiers points.
- Vérifiez que la configuration du pilote inclut les règles de mot de passe de script DirXML dans le site correct et dans le bon ordre, tel que décrit à la section « Règles requises pour la configuration du pilote », page 182.
- Comparez la règle de mot de passe dans eDirectory avec toute règle 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 le paramètre +DXML dans DSTrace pour voir le traitement des principes DirXML.
- Définissez le niveau de trace DirXML pour le pilote sur 3.
- Vérifiez que le principe de génération des messages électroniques est sélectionné.
- Vérifiez que l'objet eDirectory 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 « Configuration de la notification par message électronique », page 243.

Erreur lors de l'utilisation de la vérification du mot de passe de l'objet

La tâche Vérifier l'état des mots de passe amène le pilote à recevoir une opération de vérification du 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 eDirectory ne contient pas d'attribut nspmDistributionPassword. Vérifiez que les paramètres de l'attribut nspmDistributionPassword sont corrects dans le filtre du pilote et que Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel est sélectionné dans la règle 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 règles appropriées de synchronisation de mot de passe.
- Comparez la règle de mot de passe dans eDirectory avec toute règle 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 eDirectory uniquement, l'option Vérifier l'état des mots 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 DirXML et le message d'erreur potentiel.

+DVRS : affiche les messages du pilote DirXML.

+AUTH : affiche les modifications des mots de passe NDS.

+DCLN : affiche les messages NDS Dclient.

Scénario 3 : synchronisation d'eDirectory et des systèmes connectés lors de la mise à jour du mot de passe de distribution dans Identity Manager

Dans cette méthode, 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 eDirectory sont synchronisés.

Tout système connecté peut éditer des mots de passe sur Identity Manager, bien que tous les systèmes connectés ne puissent pas fournir le mot de passe de l'utilisateur. Active Directory, par exemple, peut éditer 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 règle 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 « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 175.

Cette section contient les informations suivantes :

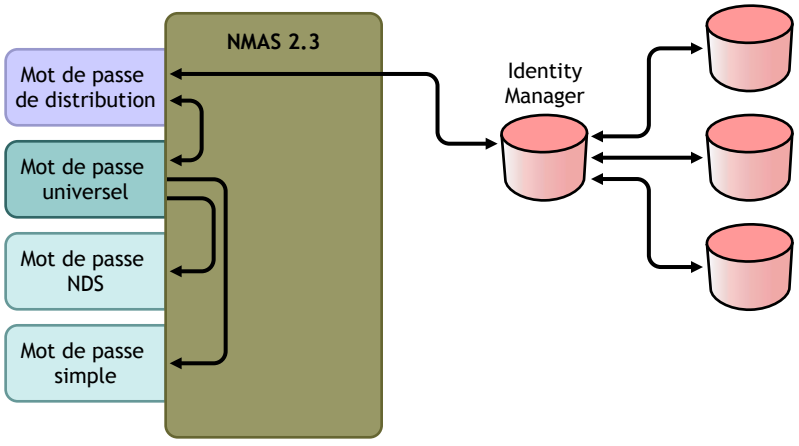
Avantages et inconvénients du scénario 3

Avantages	Inconvénients
Permet la synchronisation des mots de passe entre eDirectory et les systèmes connectés. Permet de choisir s'il convient ou non d'appliquer les règles de mot 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 règles de mot de passe, vous pouvez choisir de réinitialiser un mot de passe sur le système connecté au mot de passe de distribution si le mot de passe n'est pas conforme.	

Diagramme du scénario 3

Le diagramme montre que, dans ce scénario, les mots de passe entrent par Identity Manager, qui passe par NMAS pour mettre directement à jour le mot de passe de distribution. 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. 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 règle 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.



Mise en œuvre du scénario 3

Pour mettre en œuvre ce type de synchronisation des mots de passe :

- « Déploiement du mot de passe universel », page 219
- « Configuration de la règle de mot de passe », page 219
- « Paramètres de la synchronisation des mots de passe », page 221
- « Configuration de pilote », page 222

Déploiement du mot de passe universel

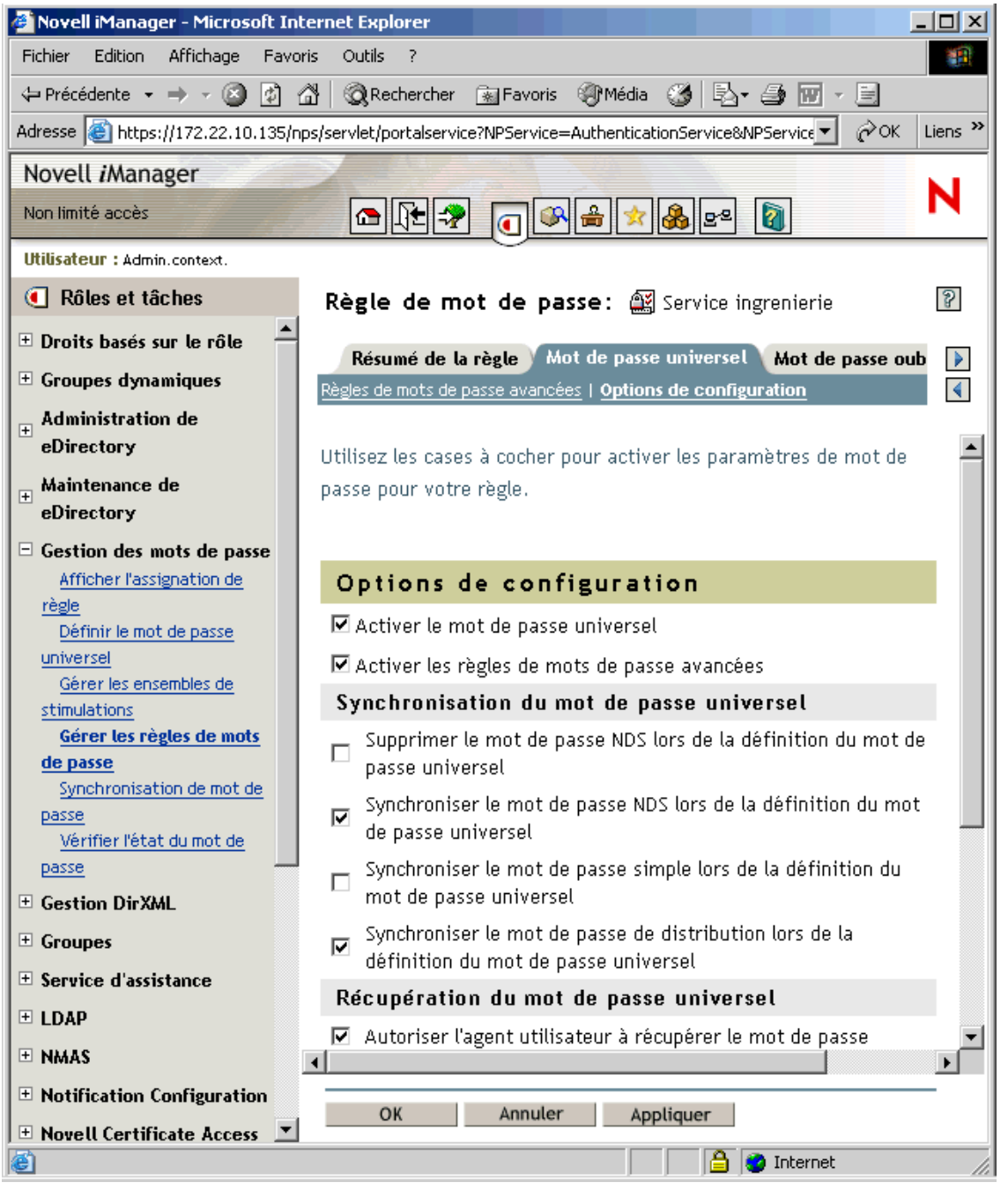
Vérifiez que votre environnement est prêt à utiliser le mot de passe universel. Reportez-vous à la section « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 190.

Configuration de la règle de mot de passe

Dans Gestion des mots de passe > Gérer les règles de mots de passe, procédez comme suit :

1. Vérifiez qu'une règle de mot de passe est assignée aux parties de l'arborescence eDirectory pour lesquelles vous voulez disposer de la synchronisation des mots de passe. Vous pouvez l'assigner à la totalité de l'arborescence, à un conteneur racine de partition, à un conteneur, voire à un utilisateur particulier. Nous vous recommandons d'assigner des règles de mot de passe au niveau le plus élevé possible de l'arborescence afin de simplifier l'administration.
2. Vérifiez que les éléments suivants sont sélectionnés dans la règle 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
   - Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel

Identity Manager récupérant 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.



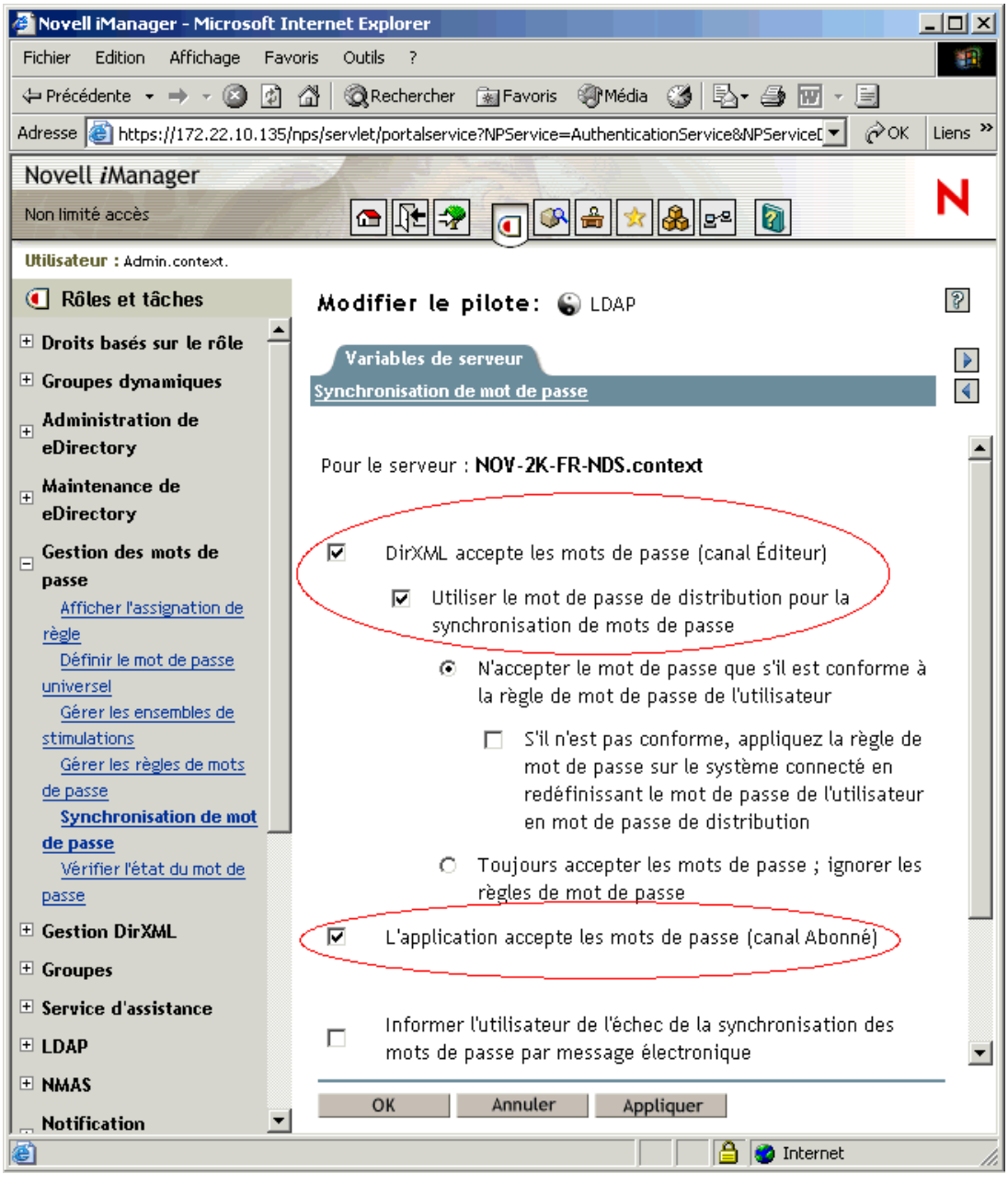
3 Si vous utilisez les règles de mot de passe avancées, vérifiez qu'elles n'entrent pas en conflit avec les règles de mot de passe de tout système connecté qui s'abonne aux mots de passe.

Paramètres de la synchronisation des mots de passe

Dans Gestion des mots de passe > Synchronisation de mot de passe, utilisez les éléments suivants :

1. Vérifiez que les éléments suivants sont sélectionnés :
   - DirXML accepte les mots de passe (canal Éditeur)
     - Utiliser le mot de passe de distribution pour la synchronisation de mots 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 édités, par la création d'un mot de passe dans la configuration d'un pilote à l'aide d'une règle.
   - 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 règles 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 éditer, ne sélectionnez que l'option L'application accepte les mots de passe (canal Abonné).

2. Indiquez si vous souhaitez que les règles de mot de passe 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.
3. (Conditionnel) Si vous avez indiqué que vous souhaitez appliquer les règles de mot de passe, indiquez également si vous souhaitez qu'Identity Manager réinitialise le mot de passe du système connecté en cas de non-conformité.
4. (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'affectent pas le traitement du document XML qui a déclenché le message électronique ; si elles échouent, elles ne sont pas tentées à nouveau, à moins que l'opération elle-même ne le soit.

     Toutefois, les messages de débogage pour les notifications par message électronique sont écrits dans le fichier de trace.

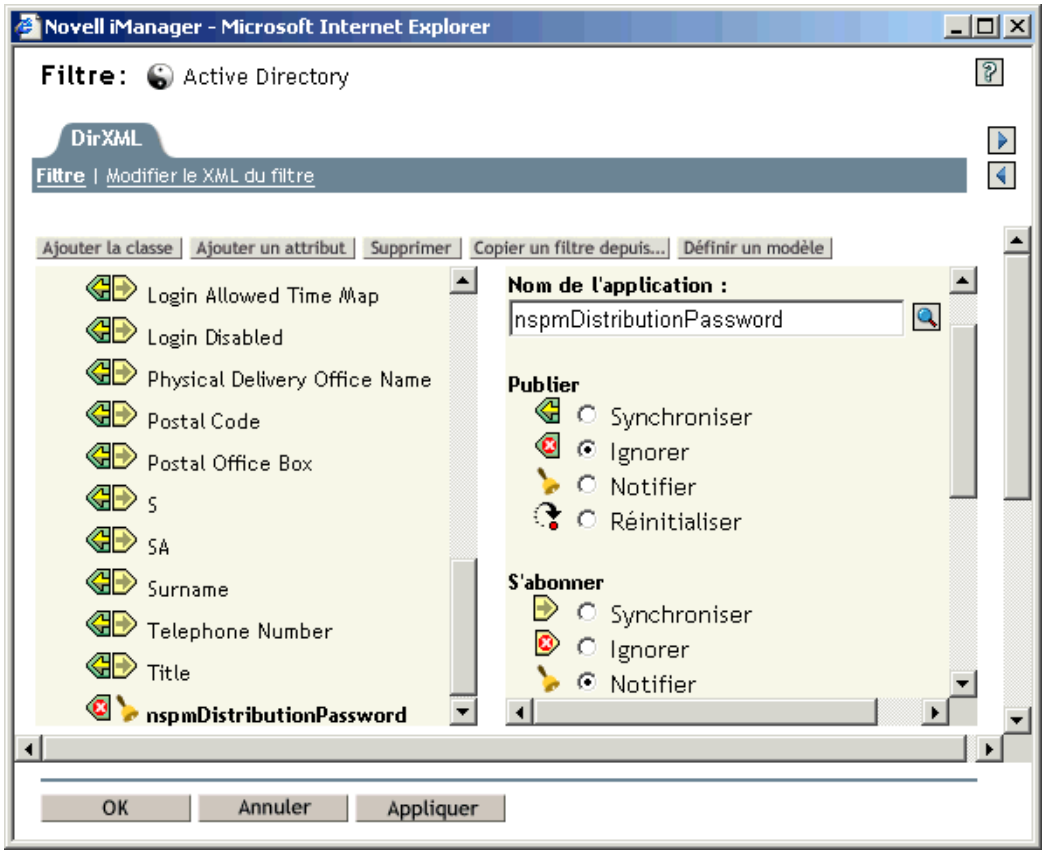
Configuration de pilote

1. Vérifiez que les règles obligatoires de synchronisation des mots de passe de script DirXML sont incluses dans les configurations de pilote pour chaque pilote qui doit participer à la synchronisation des mots de passe. Ces règles doivent se trouver dans la configuration de votre pilote, à l'endroit correct et dans le bon ordre. Pour obtenir la liste des règles, reportez-vous à la section « Règles requises pour la configuration du pilote », page 182.

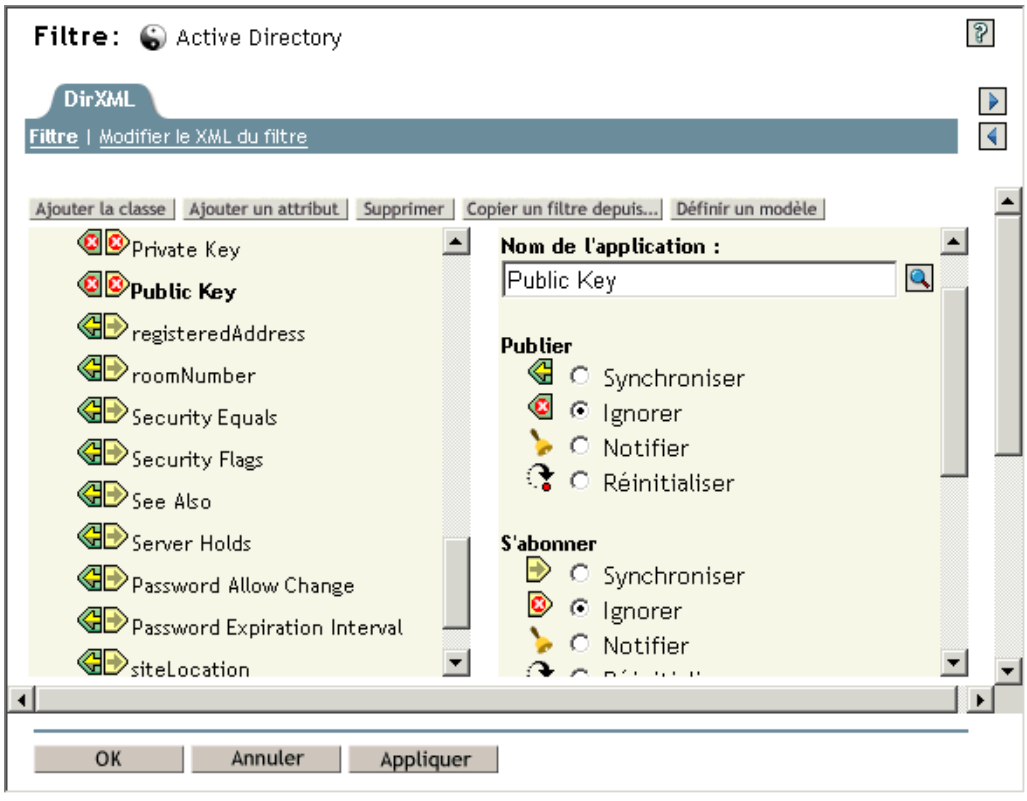
   Les exemples de configuration Identity Manager contiennent déjà les règles. Si vous effectuez la mise à niveau d'un pilote existant, vous pouvez ajouter les règles à l'aide des instructions de la section « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.

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 Ignorez les attributs Clé publique et Clé privée dans le filtre du pilote pour tous les objets dont l'attribut nspmDistributionPassword est défini sur Notifier.



4 Pour assurer la sécurité des mots de passe, contrôlez l'identité des personnes disposant de droits sur les objets DirXML.

Dépannage du scénario 3

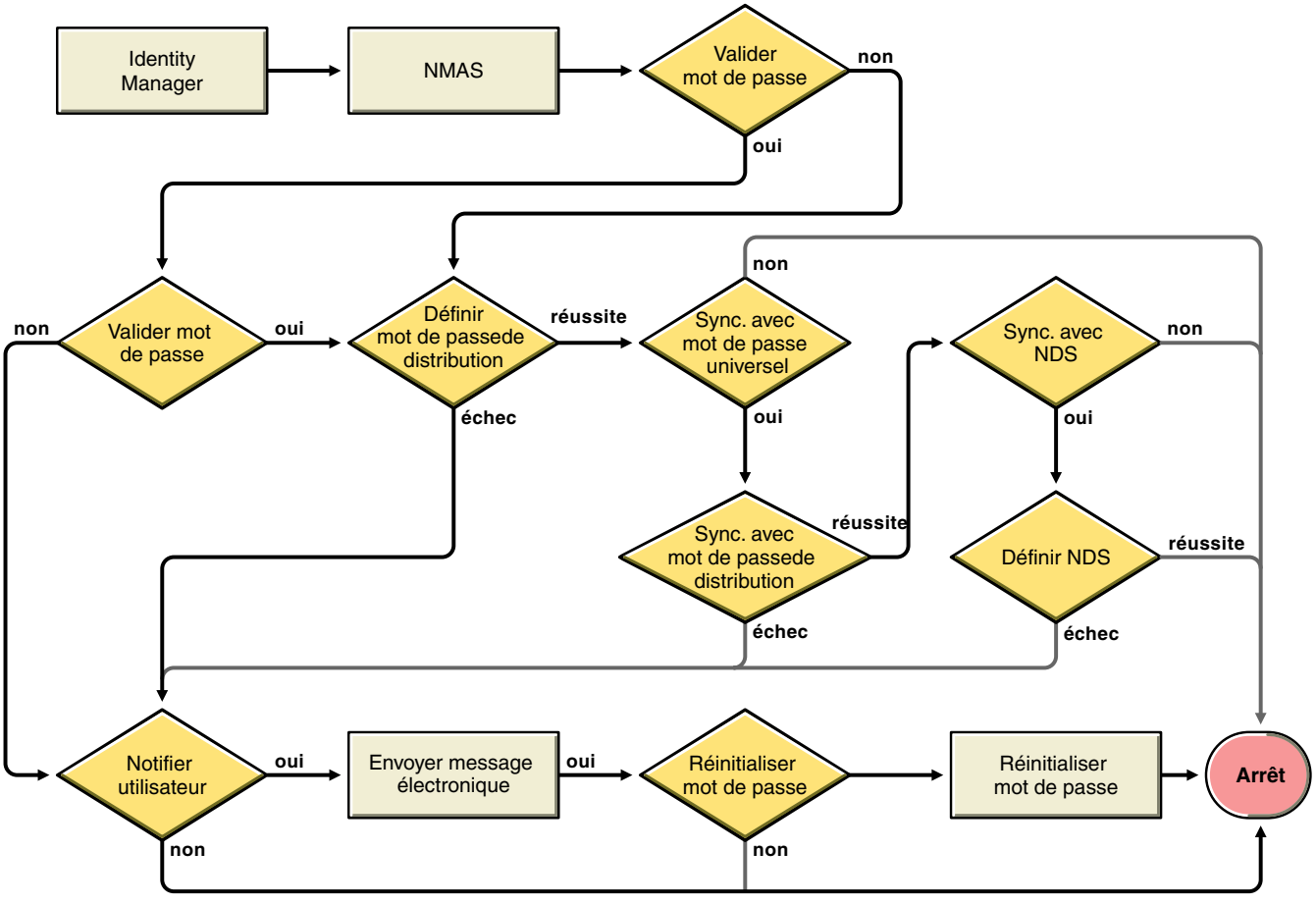
Cette section contient les informations suivantes :

- « Diagramme du scénario 3 », page 225
- « Problème de connexion à eDirectory », page 225
- « Problème pour se loguer à un autre système connecté qui s'abonne aux mots de passe », page 226
- « Le message électronique n'est pas généré en cas d'échec du mot de passe », page 227
- « Erreur lors de l'utilisation de la vérification de l'état du mot de passe », page 227
- « Commandes DSTrace utiles », page 228

Consultez également les astuces de la section « Dépannage des problèmes de synchronisation des mots de passe », page 258.

Diagramme du scénario 3

Le diagramme suivant montre comment NMAS gère le mot de passe qu'il reçoit d'Identity Manager. Dans ce scénario, le mot de passe est synchronisé sur le mot de passe de distribution. NMAS décide de la manière de gérer de mot de passe, selon que si vous avez spécifié que les mots de passe entrants doivent être validés par rapport aux règles de mot de passe (si les règles de mot de passe avancées et le mot de passe universel sont activés) et des autres paramètres de la règle de mot de passe pour la synchronisation du mot de passe universel avec les autres mots de passe.



Problème de connexion à eDirectory

- Activez les paramètres +AUTH, +DCLN, +DXML et +DVRS dans DSTrace.
- Vérifiez que les éléments <password> ou <modify-password> sont transférés à Identity Manager. Pour cela, consultez l'écran DSTRACE ou le fichier contenant les options de trace actives, comme indiqué dans les premiers points.
- Vérifiez que le mot de passe est valide, en fonction des principes de la règle de mot de passe.
- Vérifiez la configuration et l'assignation de la règle de mot de passe. Essayez d'assigner directement la règle à l'utilisateur, en vérifiant que vous utilisez la bonne règle.
- Sur la page Synchronisation de mot de passe pour le pilote, vérifiez que l'option DirXML accepte les mots de passe (canal Éditeur) est sélectionnée.
- Dans la règle 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.

- Dans la règle de mot de passe, vérifiez que l'option Synchroniser le mot de passe NDS lors de la définition du mot de passe universel est sélectionnée, si nécessaire.
- Si les utilisateurs se connectent via le client Novell ou ConsoleOne, vérifiez la version. Les clients Novell et ConsoleOne hérités pourraient ne pas pouvoir se connecter à eDirectory 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 manuel *NMAS 2.3 Administration Guide (Guide d'administration de NMAS 2.3)* (http://www.novell.com/documentation/fr-fr/nmas23).
- Certains utilitaires hérités s'authentifient à l'aide du mot de passe NDS et ne peuvent toutefois pas se connecter à eDirectory 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 règle 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 édite des mots de passe sur Identity Manager ; 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 pour voir le traitement des règles DirXML et les erreurs potentielles.
- Définissez le niveau de trace DirXML pour le pilote sur 3.
- Sur la page Synchronisation de mot de passe, vérifiez que l'option DirXML accepte les mots de passe (canal Éditeur) est sélectionnée.
- Dans la règle 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.

  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> pour un ajout ou un élément <modify-password> a été converti pour ajouter et modifier des opérations d'attribut pour nspmDistributionPassword. Pour cela, consultez l'écran DSTRACE ou le fichier contenant les options actives, comme indiqué dans les premiers points.
- Vérifiez que la configuration du pilote inclut les règles de mot de passe de script Identity Manager dans le site correct et dans le bon ordre, tel que décrit à la section « Règles requises pour la configuration du pilote », page 182.
- Comparez la règle de mot de passe dans eDirectory avec toute règle 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 le paramètre +DXML dans DSTrace pour voir le traitement des principes DirXML.
- Définissez le niveau de trace DirXML pour le pilote sur 3.
- Vérifiez que le principe de génération des messages électroniques est sélectionné.
- Vérifiez que l'objet eDirectory 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 « Configuration de la notification par message électronique », page 243.

Les notifications par message électronique n'ont pas une présence insistante. Elles n'affectent pas le traitement du document XML qui a déclenché le message électronique ; si elles échouent, elles ne sont pas tentées à nouveau, à moins que l'opération elle-même ne le soit.

Toutefois, 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 amène le pilote à recevoir une opération de 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 « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 175.

  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 eDirectory 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 règle 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 règles appropriées de synchronisation de mot de passe pour Identity Manager.
- Comparez la règle de mot de passe dans eDirectory avec toute règle 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.
- Sachez que pour eDirectory, l'option Vérifier l'état des mots de passe vérifie le mot de passe NDS et non le mot de passe universel. Cela signifie que si la règle de mot de passe de l'utilisateur ne spécifie pas une synchronisation du mot de passe NDS 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 DirXML et le message d'erreur potentiel.

+DVRS : affiche les messages du pilote DirXML.

+AUTH : affiche les modifications des mots de passe NDS.

+DCLN : affiche les messages NDS Dclient.

Scénario 4 : passage en tunnel — synchronisation des systèmes connectés mais pas d'eDirectory avec Identity Manager Mise à jour du mot de passe de distribution

Identity Manager permet de synchroniser les mots de passe entre les systèmes connectés tout en maintenant le mot de passe eDirectory séparé d'eux. Dans cette documentation, l'opération est dénommée tunnellisation.

Dans ce scénario, Identity Manager met directement à jour le mot de passe de distribution. Cette méthode est presque identique à la précédente, décrite à la section « Scénario 3 : synchronisation d'eDirectory et des systèmes connectés lors de la mise à jour du mot de passe de distribution dans Identity Manager », page 217. Toutefois, ici, vous devez vous assurer que le mot de passe universel et le mot de passe de distribution ne sont pas synchronisés. Vous y parvenez en n'utilisant pas les Règles de mot de passe ou en les utilisant mais en désactivant l'option Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel.

Cette section contient les informations suivantes :

Avantages et inconvénients du scénario 4

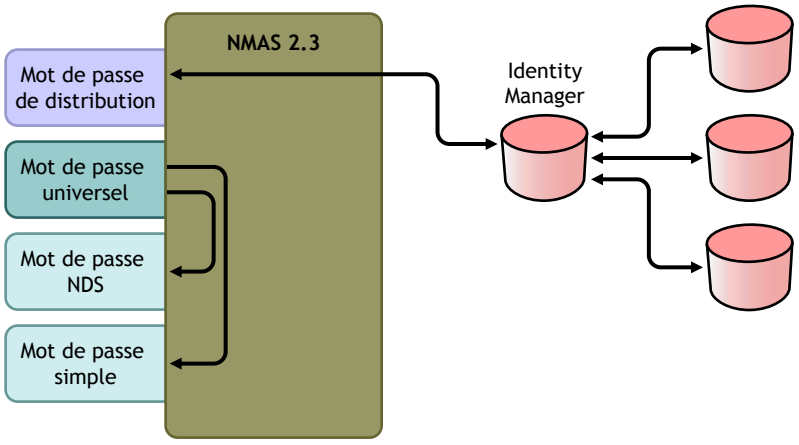
Avantages	Inconvénients
Permet de synchroniser les mots de passe entre les systèmes connectés, tout en maintenant le mot de passe eDirectory séparé. Les règles de mot de passe ne sont pas obligatoires. Si vous utilisez une règle de mot de passe, il n'est pas nécessaire que le mot de passe universel y 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 règle de mot de passe. Si le mot de passe universel et les règles de mot de passe avancées sont activés, les règles 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 règles de mot de passe ne sont pas appliquées ; les mots de passe des systèmes connectés ne peuvent pas être réinitialisés.

Diagramme du scénario 4

Le diagramme montre que, dans ce scénario, les mots de passe entrent par Identity Manager, qui passe par NMAS pour mettre directement à jour le mot de passe de distribution. 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, le paramètre est désactivé pour la synchronisation du mot de passe universel avec le mot de passe de distribution. 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 affecter de mot de passe dans eDirectory.

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.



Mise en œuvre du scénario 4

Pour mettre en œuvre ce type de synchronisation des mots de passe :

- « Déploiement du mot de passe universel », page 230
- « Configuration de la règle de mot de passe », page 230
- « Paramètres de la synchronisation des mots de passe », page 231
- « Configuration de pilote », page 232

Déploiement du mot de passe universel

Même s'il n'est pas forcément nécessaire que les règles de mot de passe soient activées avec le mot de passe universel, votre environnement doit malgré tout utiliser eDirectory 8.7.3, qui prend en charge le mot de passe universel. Reportez-vous à la section « Préparation à l'utilisation de la synchronisation des mots de passe et du mot de passe universel dans Identity Manager », page 190.

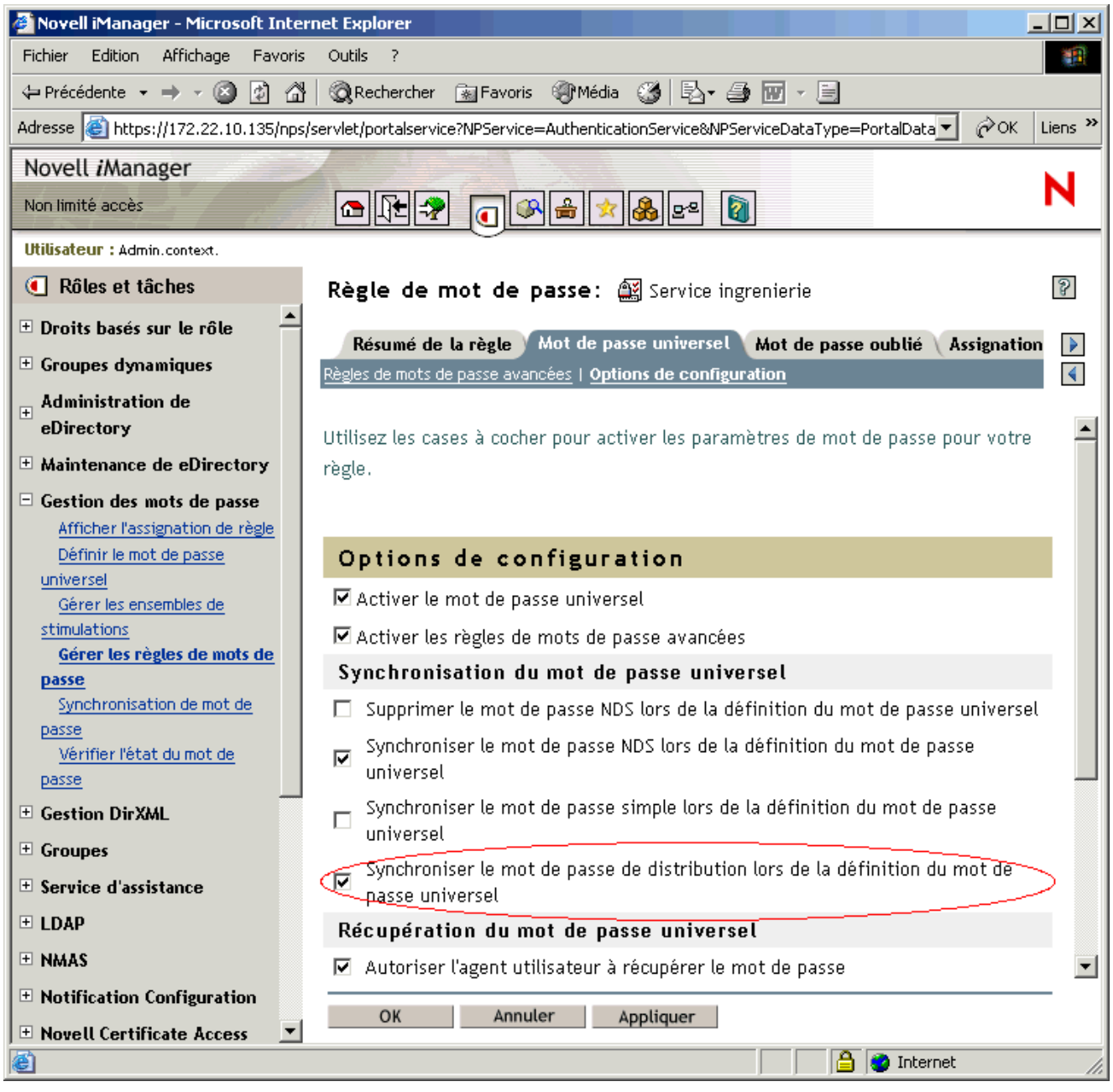
Configuration de la règle de mot de passe

Aucune règle de mot de passe n'est obligatoire pour les utilisateurs eDirectory qui font appel à cette méthode.

Toutefois, si vous utilisez une règle de mot de passe :

1. Vérifiez que les éléments suivants sont sélectionnés :
   - Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel

     Cela est essentiel pour tunnelliser les mots de passe sans que le mot de passe eDirectory 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 qu'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 eDirectory.



2 Complétez les autres paramètres de la règle de mot de passe comme vous le souhaitez.

La décision vous revient quant aux autres paramètres de mot de passe dans la règle de mot de passe.

Paramètres de la synchronisation des mots de passe

Utilisez les mêmes paramètres que dans la section Paramètres de la synchronisation des mots de passe de la section « Scénario 3 : synchronisation d'eDirectory et des systèmes connectés lors de la mise à jour du mot de passe de distribution dans Identity Manager », page 217.

Configuration de pilote

Utilisez les mêmes paramètres que dans la section Configuration de pilote de la section « Scénario 3 : synchronisation d'eDirectory et des systèmes connectés lors de la mise à jour du mot de passe de distribution dans Identity Manager », page 217.

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.

Cette section contient les informations suivantes :

- « Problème pour se loguer à un autre système connecté qui s'abonne aux mots de passe », page 232
- « Les messages électroniques ne sont pas générés en cas d'échec du mot de passe », page 233
- « Erreur lors de l'utilisation de la vérification de l'état du mot de passe », page 233
- « Commandes DSTrace utiles », page 234

Consultez également les astuces de la section « Dépannage des problèmes de synchronisation des mots de passe », page 258.

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 édite des mots de passe sur Identity Manager ; 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 le traitement des règles DirXML et les erreurs potentielles.
- Définissez le niveau de trace DirXML pour le pilote sur 3.
- Sur la page Synchronisation de mot de passe, vérifiez que l'option DirXML accepte les mots de passe (canal Éditeur) est sélectionnée.
- Dans la règle 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.

  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> pour un ajout ou un élément <modify-password> a été converti pour ajouter et modifier des opérations d'attribut pour nspmDistributionPassword. Pour cela, consultez l'écran DSTRACE ou le fichier contenant les options de trace actives, comme indiqué dans les premiers points.

- Vérifiez que la configuration du pilote inclut les règles de mot de passe de script DirXML dans le site correct et dans le bon ordre, tel que décrit à la section « Règles requises pour la configuration du pilote », page 182.
- Comparez la règle de mot de passe dans eDirectory avec toute règle 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 le paramètre +DXML dans DSTrace pour voir le traitement des principes DirXML.
- Définissez le niveau de trace DirXML pour le pilote sur 3.
- Vérifiez que le principe de génération des messages électroniques est sélectionné.
- Vérifiez que l'objet eDirectory 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 « Configuration de la notification par message électronique », page 243.

Les notifications par message électronique n'ont pas une présence insistante. Elles n'affectent pas le traitement du document XML qui a déclenché le message électronique ; si elles échouent, elles ne sont pas tentées à nouveau, à moins que l'opération elle-même ne le soit.

Toutefois, 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 amène le pilote à recevoir une opération de 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 « Prise en charge par les systèmes connectés de la synchronisation des mots de passe », page 175.

  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 eDirectory ne contient pas d'attribut nspmDistributionPassword. Vérifiez le filtre de l'attribut DixXML et l'option Synchroniser le mot de passe universel et le mot de passe de distribution dans la règle 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 règles appropriées de synchronisation de mot de passe DirXML.
- Comparez la règle de mot de passe dans eDirectory avec toute règle 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 : affiche le traitement des règles DirXML et les messages d'erreur potentiels.

+DVRS : affiche les messages du pilote DirXML.

+AUTH : affiche les modifications des mots de passe NDS.

+DCLN : affiche les messages NDS Dclient.

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 eDirectory. 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 eDirectory à l'aide du mot de passe en texte clair ou haché via LDAP ou le client Novell, avec des composants NMAS 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 édité tel quel depuis le système connecté dans la zone de mot de passe simple d'eDirectory.

Si le système connecté ne fournit que des mots de passe hachés (les codages MD5, SHA ou UNIX sont pris en charge), vous devez les éditer sur le mot de passe simple avec une indication du type de hachage, comme {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.

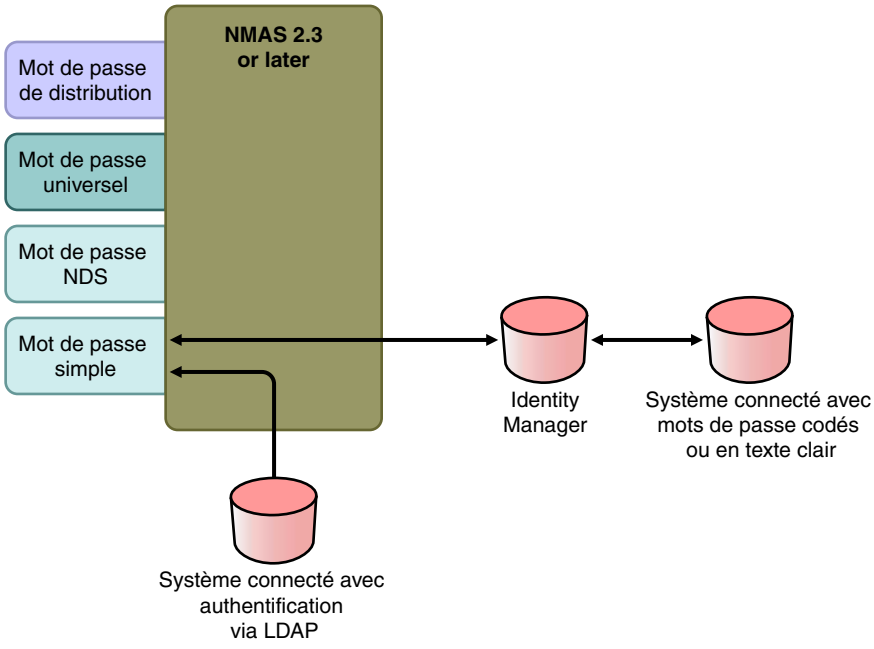
Cette section contient les informations suivantes :

- « Avantages et inconvénients », page 235
- « Diagramme du scénario 5 », page 235
- « Mise en œuvre du scénario 5 », page 235

Avantages et inconvénients

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, dans la mesure où elles sont prises en charge pour le mot de passe NDS, mais elles ne fonctionnent pas pour le mot de passe simple. ◆ Étant donné que la tâche Gestion des mots de passe > Définir le mot de passe universel dépend du mot de passe universel, l'administrateur ne peut pas définir un mot de passe utilisateur dans eDirectory à l'aide de cette tâche.

Diagramme du scénario 5



Mise en œuvre du scénario 5

- « Configuration de la règle de mot de passe », page 235
- « Paramètres de la synchronisation des mots de passe », page 236
- « Configuration de pilote », page 236

Configuration de la règle de mot de passe

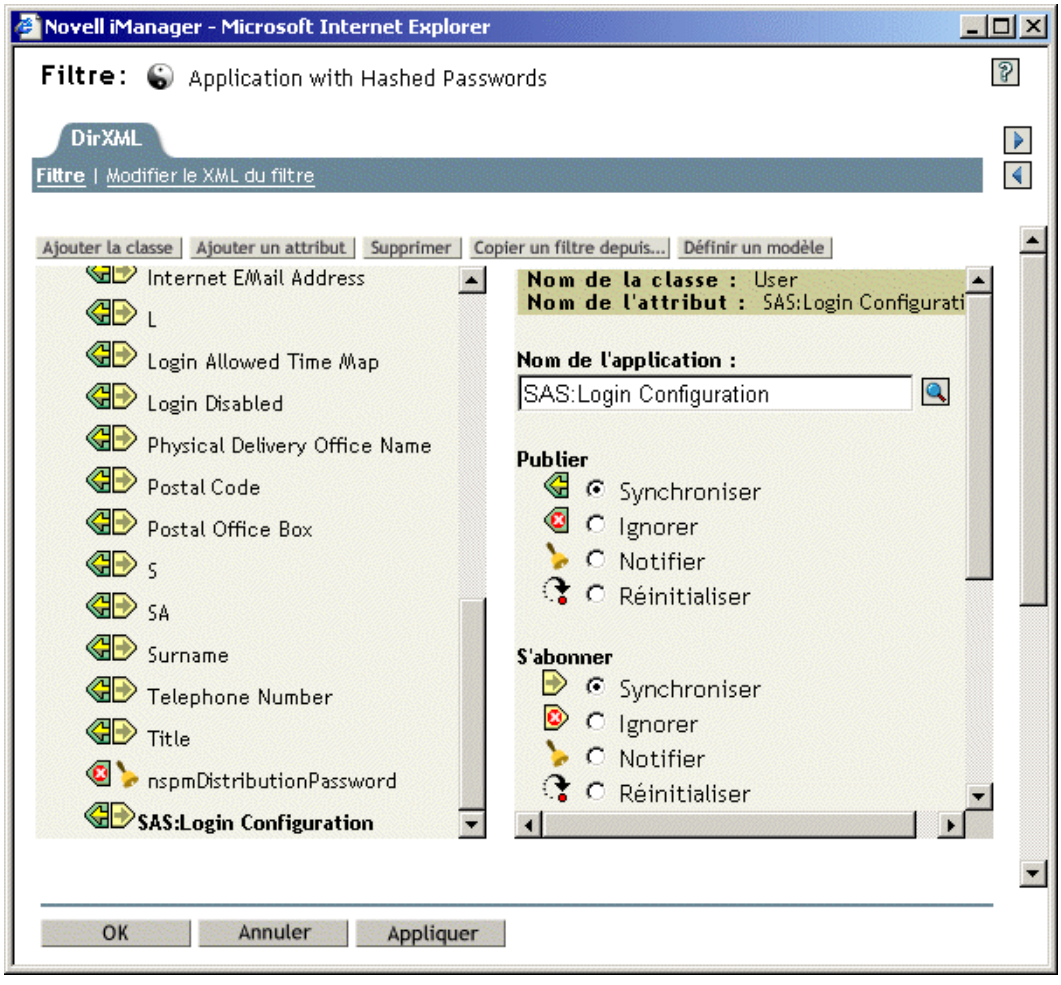
Aucune règle de mot de passe n'est obligatoire pour les utilisateurs qui font appel à ce scénario. Il n'est pas possible d'utiliser le mot de passe universel.

Paramètres de la synchronisation des mots de passe

Dans ce scénario, utilisez le script DirXML pour modifier directement l'attribut SAS:Login Configuration. Cela signifie que les valeurs de configuration globales de la synchronisation des mots de passe, définies par la tâche Gestion des mots de passe > Synchronisation de mot de passe dans iManager, n'ont aucun effet.

Configuration de pilote

1 Vérifiez que le filtre dispose du paramètre de synchronisation pour les canaux Abonné et Éditeur pour l'attribut SAS:Login Configuration.



2 Configurez les règles du pilote, de manière à éditer le mot de passe à partir du système connecté.

3 Pour les mots de passe hachés, configurez les règles du pilote, de manière à ajouter, en préfixe, le type du hachage, s'il n'est pas déjà fourni par l'application :

- {MD5}*mot_de_passe_haché*

  Ce mot de passe est codé en Base64.

- {SHA}*mot_de_passe_haché*

  Ce mot de passe est codé en Base64.

- {CRYPT}*mot_de_passe_haché*

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 règles du pilote pour modifier l'attribut SAS:Login Configuration.

C'est par exemple la manière d'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>
```

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.

- « Définition des filtres de synchronisation de mots de passe pour Active Directory et NT Domain », page 238
- « Définition des filtres de synchronisation des mots de passe pour NIS », page 238

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) dans les guides de mise en œuvre des pilotes DirXML pour Active Directory et NT Domain, disponible sur le site de documentation sur les pilotes DirXML (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

Le pilote DirXML pour AD ou NT Domain doit être installé sur une seule machine 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.dll 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.

Définition des filtres de synchronisation des mots de passe pour NIS

Le pilote DirXML pour NIS 2.0 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 DirXML pour NIS.

Le déploiement du module PAM pour le pilote NIS est décrit dans le manuel *DirXML Driver for NIS Implementation Guide (Guide de mise en œuvre de DirXML pour NIS)*, disponible sur le site de documentation sur les pilotes DirXML (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

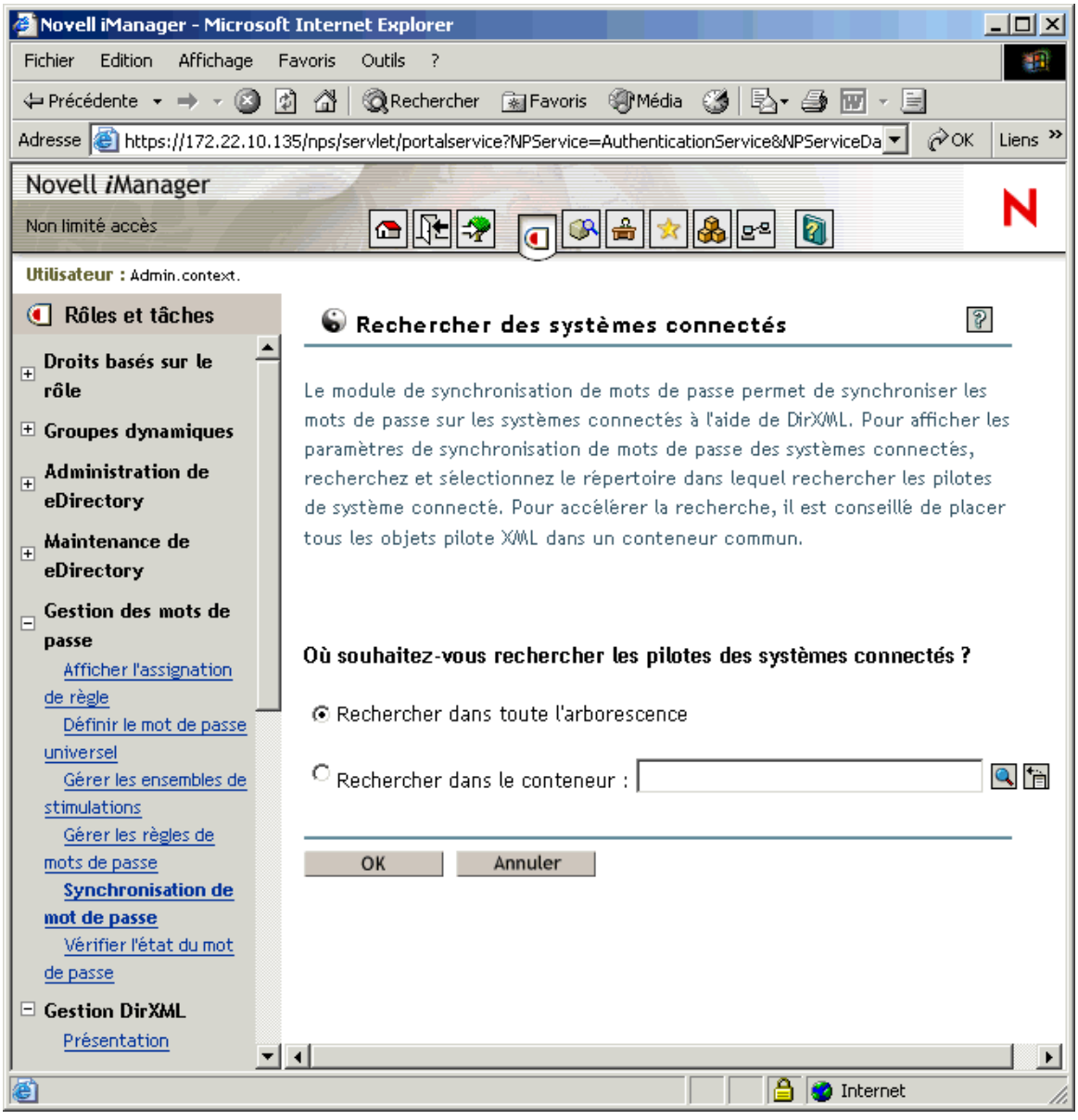
Gestion de la synchronisation des mots de passe

Cette section contient les informations suivantes :

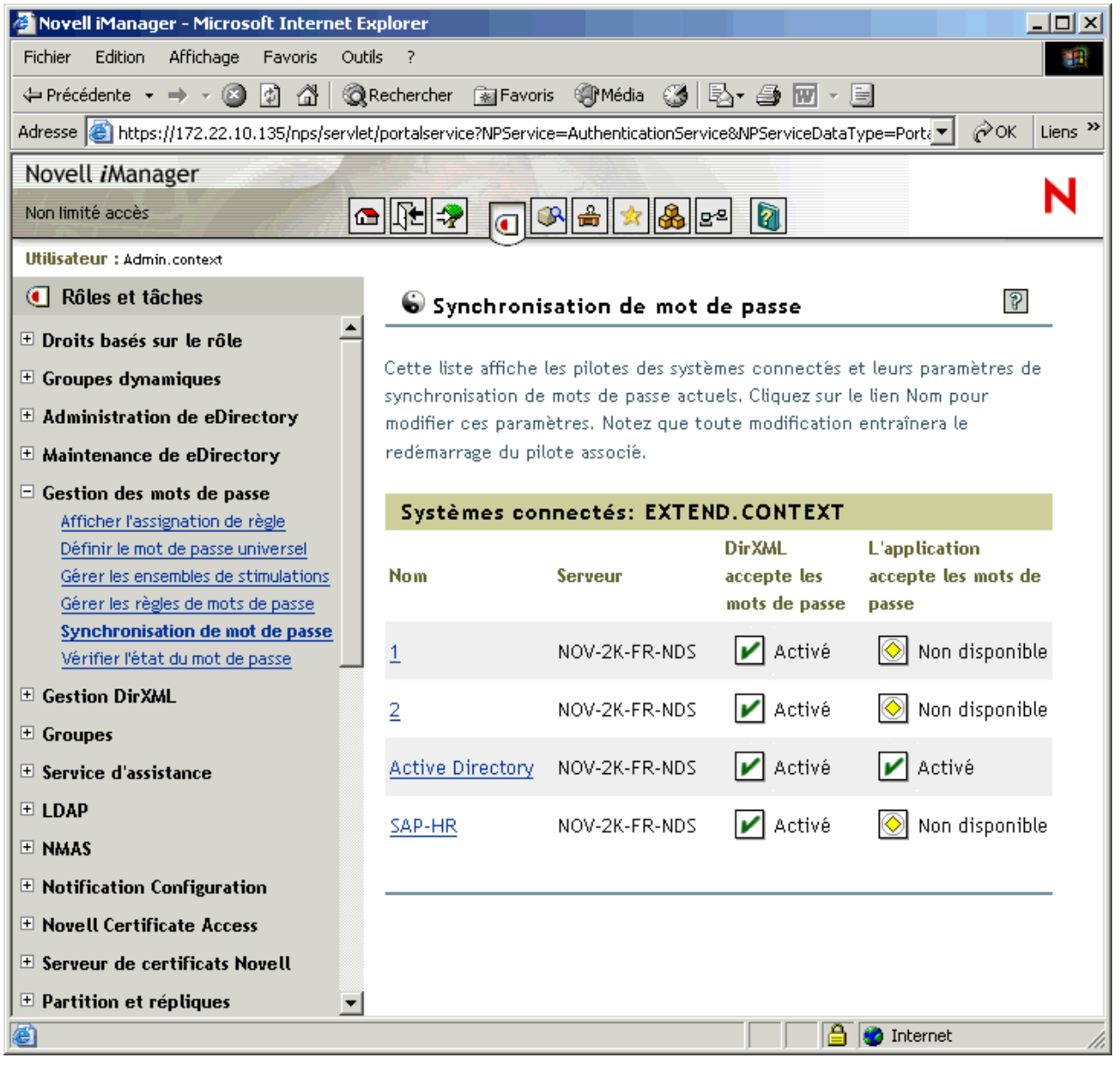
Définition du flux des mots de passe sur les différents systèmes

L'interface qui suit permet de découvrir comment configurer vos systèmes pour qu'ils acceptent ou éditent les mots de passe. Elle se trouve dans la tâche Synchronisation de mot de passe, sous le rôle Gestion de mot de passe.

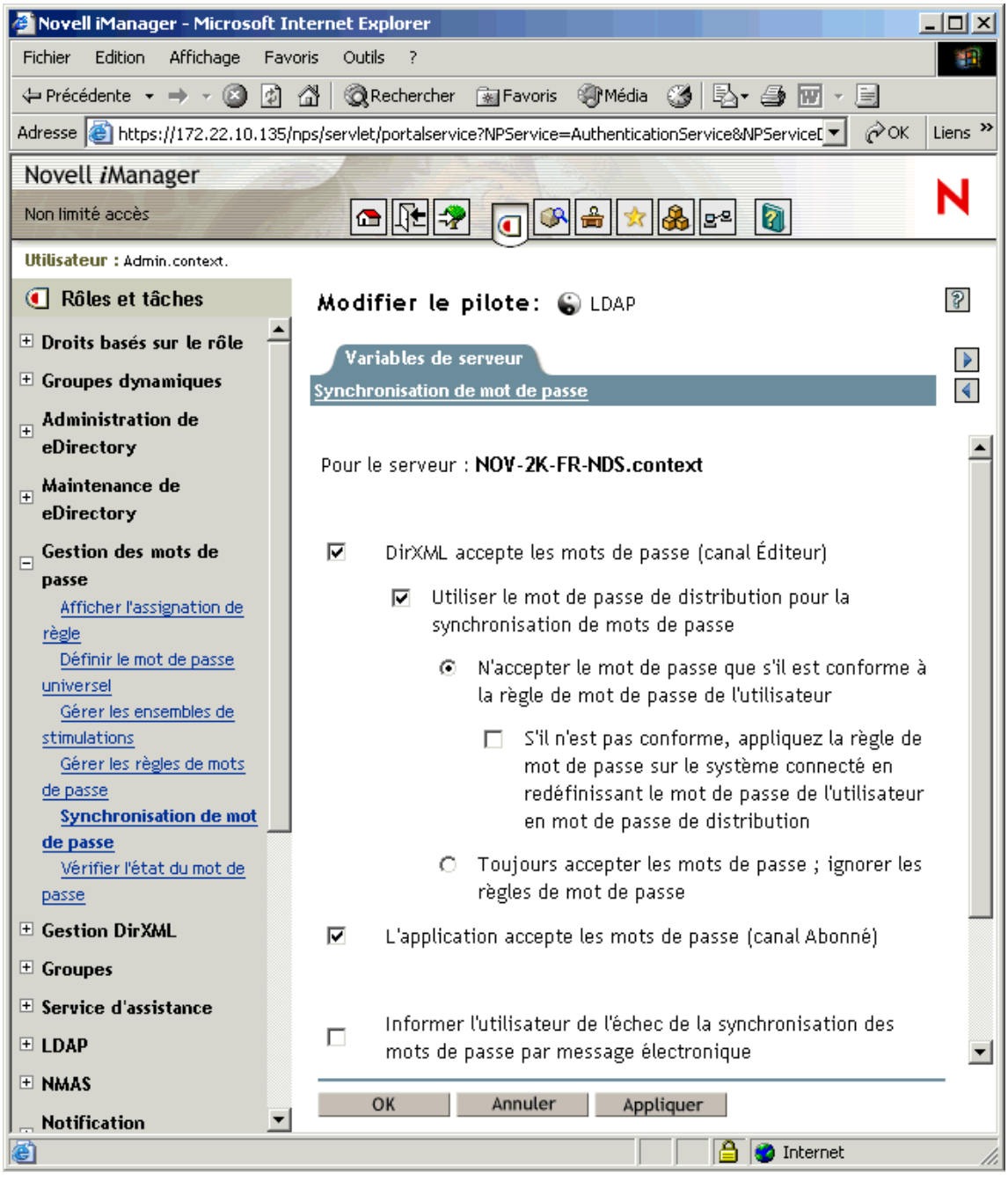
La première page permet de rechercher les pilotes des systèmes connectés.



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. La page suivante s'affiche, dans laquelle vous voyez des informations complémentaires et modifiez les paramètres :



Dans cette page, vous pouvez décider si la règle de mot de passe doit être appliquée pour les mots de passe entrant dans Identity Manager et si elle doit être appliquée sur le système connecté en réinitialisant le mot de passe du système.

Les paramètres de cette page sont des valeurs de configuration globales (GCV), stockées pour chaque serveur. Reportez-vous à la section « Paramètres de synchronisation des mots de passe à créer à l'aide des valeurs de configuration globales », page 178.

Application des règles de mot de passe sur les systèmes connectés

Si vous utilisez les règles de mot de passe avancées et la synchronisation des mots de passe dans Identity Manager, nous vous recommandons de rechercher les règles de mot de passe pour tous les systèmes connectés, puis de vous assurer de leur compatibilité.

Séparation du mot de passe eDirectory et du mot de passe synchronisé

Ce scénario est décrit à la section « Scénario 4 : passage en tunnel — synchronisation des systèmes connectés mais pas d'eDirectory avec Identity Manager Mise à jour du mot de passe de distribution », page 228.

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

Une tâche iManager permet de déterminer si le mot de passe de distribution d'un utilisateur spécifique est le même que celui du système connecté.

Dans iManager, cliquez sur Gestion des mots de passe > Vérifier l'état du mot de passe.

La tâche Vérifier l'état des mots de passe amène le pilote à recevoir une opération de vérification du mot de passe de l'objet.

Tous les pilotes ne prennent pas en charge la vérification du mot de passe. Ceux qui le font doivent contenir une fonctionnalité de vérification des mots de passe dans leur manifeste. iManager n'autorise pas l'envoi des opérations de vérification de mot de passe aux pilotes dont le manifeste ne fait pas mention de cette capacité.

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 si

- Vous utilisez la méthode de synchronisation décrite à la section « Scénario 1 : synchronisation des mots de passe dans eDirectory à l'aide du mot de passe NDS », page 203.
- Vous synchronisez le mot de passe universel, comme décrit à la section « Scénario 2 : synchronisation du mot de passe universel », page 206, mais vous n'avez pas activé l'option de configuration de la règle de mot de passe pour synchroniser le mot de passe universel avec le mot de passe de distribution.

Remarque : sachez que pour eDirectory, l'option Vérifier l'état des mots de passe vérifie le mot de passe NDS et non le mot de passe universel. Cela signifie que si la règle de mot de passe de l'utilisateur ne spécifie pas une synchronisation du mot de passe NDS 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.

Configuration de la notification par message électronique

Le rôle iManager intitulé Configuration de la notification permet de spécifier le serveur de messagerie et de personnaliser les modèles de notification pas 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 les modèles, qui sont fournis par l'application qui les utilise. Les modèles de message électronique sont des objets Modèle dans eDirectory. Ils sont placés dans le conteneur Sécurité, qui se trouve généralement à la racine de votre arborescence. Même s'il s'agit d'objets eDirectory, vous ne pouvez les modifier que dans l'interface 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.

Identity Manager propose des modèles pour la synchronisation des mots de passe et les notifications en cas d'oubli des mots de passe. Vous contrôlez l'envoi éventuel de messages, en fonction des choix que vous avez faits dans l'interface 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 : envoyer le mot de passe à l'utilisateur par messagerie électronique ou lui en envoyer un indice. La page utilisée pour définir cette option est présentée à la section « Comment fournir aux utilisateurs le libre-service Mot de passe oublié », page 105.

La synchronisation des mots de passe est configurée de manière à n'envoyer un message électronique que pour l'échec des opérations de synchronisation et pour les mots de passe spécifiés. La page utilisée pour définir cette option est présentée dans la dernière figure de la section « Paramètres de synchronisation des mots de passe à créer à l'aide des valeurs de configuration globales », page 178. Vous devez également vérifier que les informations d'authentification SMTP figurent dans les règles de pilotes.

Cette section contient les informations suivantes :

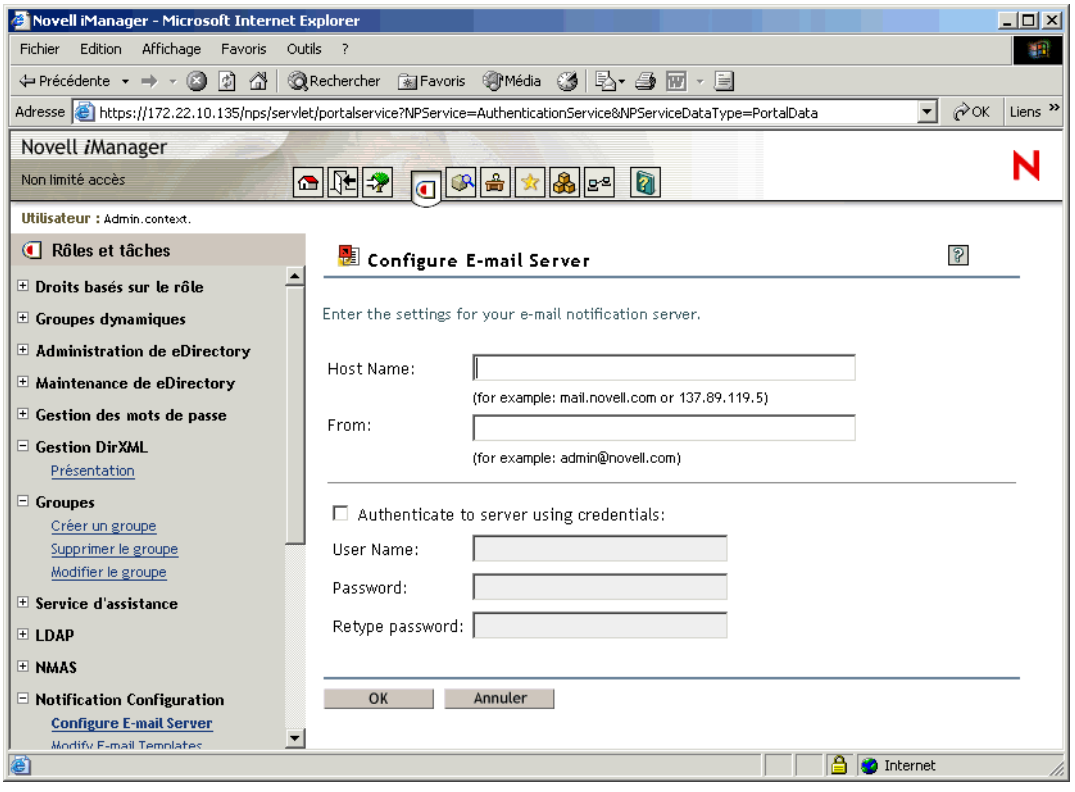
Conditions préalables

- ❑ Vérifiez que les utilisateurs eDirectory 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 règles de pilote définies à cet effet contiennent le mot de passe pour le serveur SMTP. Reportez-vous à la section « Indication des informations d'authentification SMTP dans les règles de pilote », page 246.
- ❑ 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 règle de script DirXML. Pour plus d'informations, reportez-vous à la section « Envoi de notifications par message électronique à l'administrateur », page 257.
- ❑ 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 aura besoin d'une réplique de la partition racine.

Configuration du serveur SMTP pour envoyer la notification par message électronique

1 Dans iManager, cliquez sur Configuration de la notification > Configurer le serveur de messagerie.

La page suivante s'affiche.



2 Entrez les informations suivantes :

- le nom de l'hôte,
- le nom qui doit apparaître dans le champ De du message électronique, par exemple Administrateur,
- le nom d'utilisateur et le mot de passe permettant de s'authentifier sur le serveur, le cas échéant.

3 Cliquez sur Fermer.

4 Si vous utilisez la synchronisation des mots de passe avec vos pilotes DirXML et si vous souhaitez utiliser la notification par message électronique, vous devez également :

4a Vérifier que les règles de pilote contiennent le mot de passe si votre serveur SMTP exige une authentification avant d'envoyer le message électronique. Pour plus d'informations, reportez-vous à la section « Indication des informations d'authentification SMTP dans les règles de pilote », page 246.

Spécifier les informations d'authentification dans la page Configurer le serveur de messagerie à l'Étape 2, ce qui suffit pour les notifications de mot de passe oublié, mais pas pour celles de synchronisation des mots de passe.

4b Redémarrez les pilotes DirXML 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 la section « Configuration des modèles de message électronique destinés à la notification », page 246.

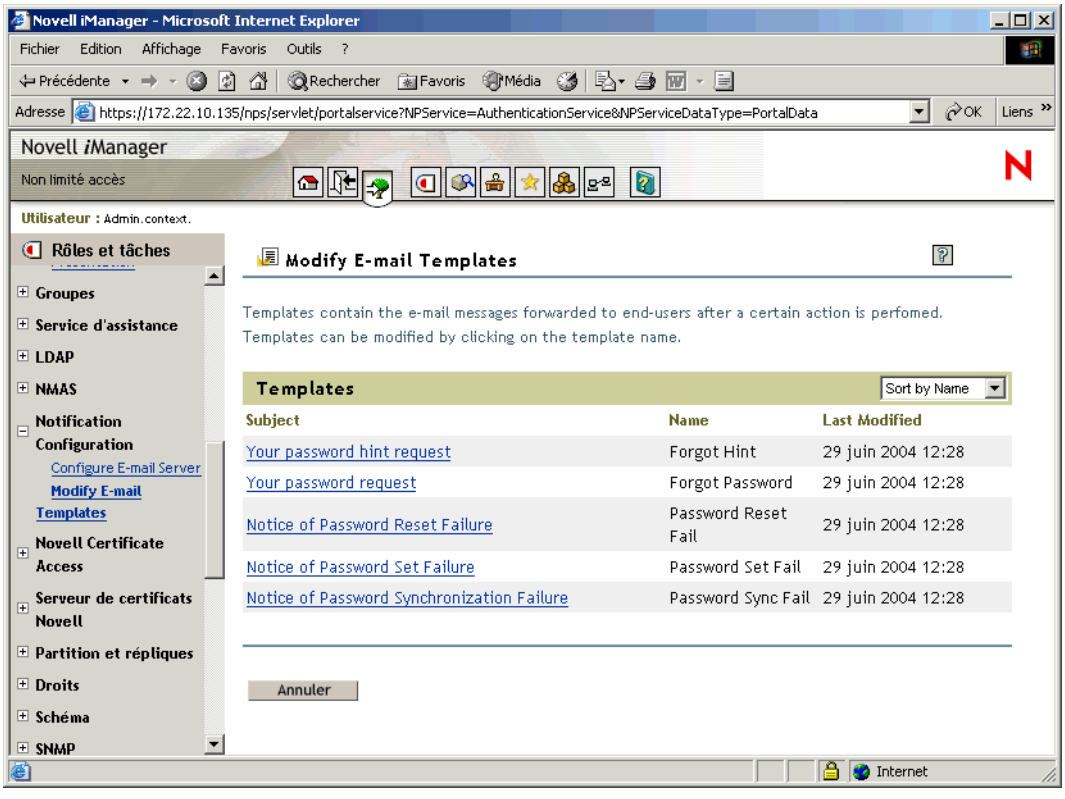
Une fois le serveur de messagerie configuré, les messages électroniques peuvent être envoyés par les applications qui les utilisent, si vous faites appel aux fonctionnalités qui entraînent l'envoi des messages.

Configuration des modèles de message électronique destinés à la notification

Vous pouvez personnaliser ces modèles en y intégrant votre texte. Le nom du modèle traduit son utilisation.

1. Dans iManager, cliquez sur Configuration de la notification > Modifier les modèles de messages électroniques.

   Une liste des modèles apparaît, comme dans l'exemple suivant.



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 « Ajout de vos balises de remplacement aux modèles de notification par message électronique », page 248.

3. Redémarrez les pilotes DirXML qui doivent être mis à jour avec les modifications.

   Le pilote lit les modèles et les informations du serveur SMTP au démarrage uniquement.

Indication des informations d'authentification SMTP dans les règles de pilote

Indiquez le nom d'utilisateur et le mot de passe pour le serveur SMTP à la section « Configuration du serveur SMTP pour envoyer la notification par message électronique », page 244. 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 règles de pilote. Le moteur DirXML peut accéder au nom d'utilisateur, mais pas au mot de passe ; la règle de pilote doit donc le fournir.

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 DirXML.
- 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 règle du pilote :

1. Vérifiez que le pilote possède les règles nécessaires à la synchronisation des mots de passe.

   Ces règles sont fournies dans les exemples de configuration du pilote ou peuvent être ajoutées, comme indiqué à la section « Mise à niveau des configurations de pilote existantes pour la prise en charge de la synchronisation des mots de passe sous Identity Manager », page 196.

2. Dans iManager, cliquez sur Gestion DirXML > Présentation. Recherchez les ensembles de pilotes ou recherchez et sélectionnez un conteneur qui contient l'ensemble de pilotes.

   Une représentation graphique de l'ensemble de pilotes apparaît.

3. Dans Présentation DirXML, cliquez sur l'icône pour le pilote.

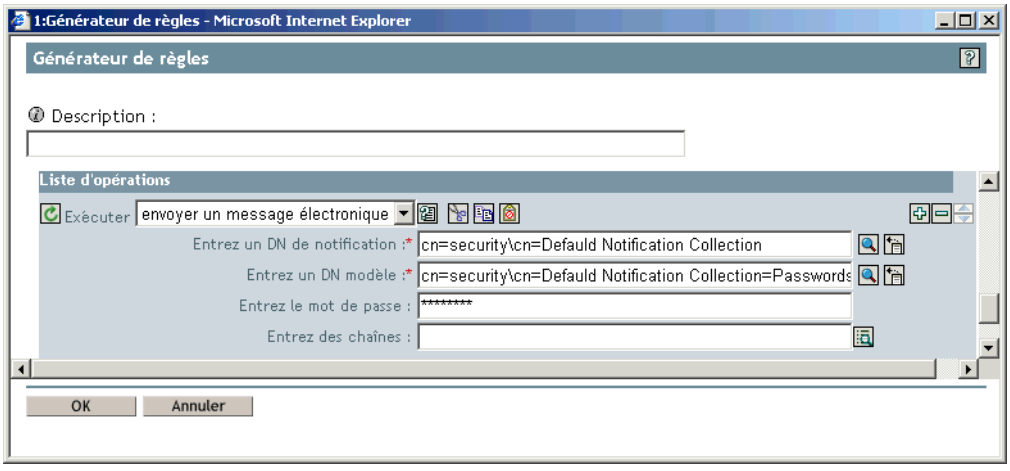
   Une représentation graphique de la configuration du pilote apparaît.

4. Indiquez le mot de passe du serveur SMTP dans les principes 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 règles suivantes doivent être modifiées pour la synchronisation des mots de passe.

Ensemble de règles	Nom de la règle	Nom du principe
Transformation de l'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 DirXML
Transformation de la 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 eDirectory.

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.

Cette section contient les informations suivantes :

- « Ajout de balises de remplacement aux modèles de notification par message électronique pour la synchronisation des mots de passe », page 248
- « Ajout de balises de remplacement aux modèles de notification par message électronique pour les mots de passe oubliés », page 257

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 notifications par message électronique pour la synchronisation des mots de passe. Toutefois, elles ne fonctionneront que si vous les définissez également dans chaque principe de la règle 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 règles 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 principe de la règle 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). Un principe de règle intitulé Envoyer un message électronique en cas d'échec de l'abonnement aux mots de passe fait référence à ce modèle de message électronique dans une opération d'envoi d'un message électronique à partir d'un modèle. Ce principe est utilisé dans une règle qui permet d'envoyer une notification à un utilisateur en cas d'échec de la synchronisation des mots de passe. Cette même balise UserGivenName est définie sous forme d'élément arg-string dans ce principe.

Comme dans cet exemple, chaque nouvelle balise ajoutée doit être définie dans le modèle de message électronique et dans les principes de la règle qui font référence au modèle de message électronique. Le moteur DirXML sait alors comment insérer les bonnes données dans la balise de remplacement lors de l'envoi d'un message électronique à l'utilisateur.

Vous pouvez faire référence aux balises dans les configurations de pilote DirXML livrées avec Identity Manager en guise d'exemples.

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 règles.
- Utilisez le Générateur de règles 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 de mot de passe oublié, l'ajout d'une balise ayant le même nom qu'un attribut sur l'objet Utilisateur dans eDirectory 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 règle 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 règles qui référencent le modèle de message électronique.

Pour définir les balises d'une règle, retrouvez toutes les règles qui font référence au modèle de notification par message électronique et utilisez le Générateur de règles pour leur ajouter les balises :

1. Recherchez toutes les règles qui référencent les modèles de notification par message électronique.

   Pour vous assurer de retrouver toutes ces règles, vous pouvez exporter vos configurations de pilote et rechercher dans XML une opération do-send-e-mail disposant d'un modèle correspondant au nom du modèle de notification.

2. Dans chaque règle, modifiez chaque principe faisant référence au modèle. Dans iManager, cliquez sur Gestion DirXML > Présentation. Sélectionnez l'ensemble de pilotes qui contient le pilote disposant de la règle à modifier.

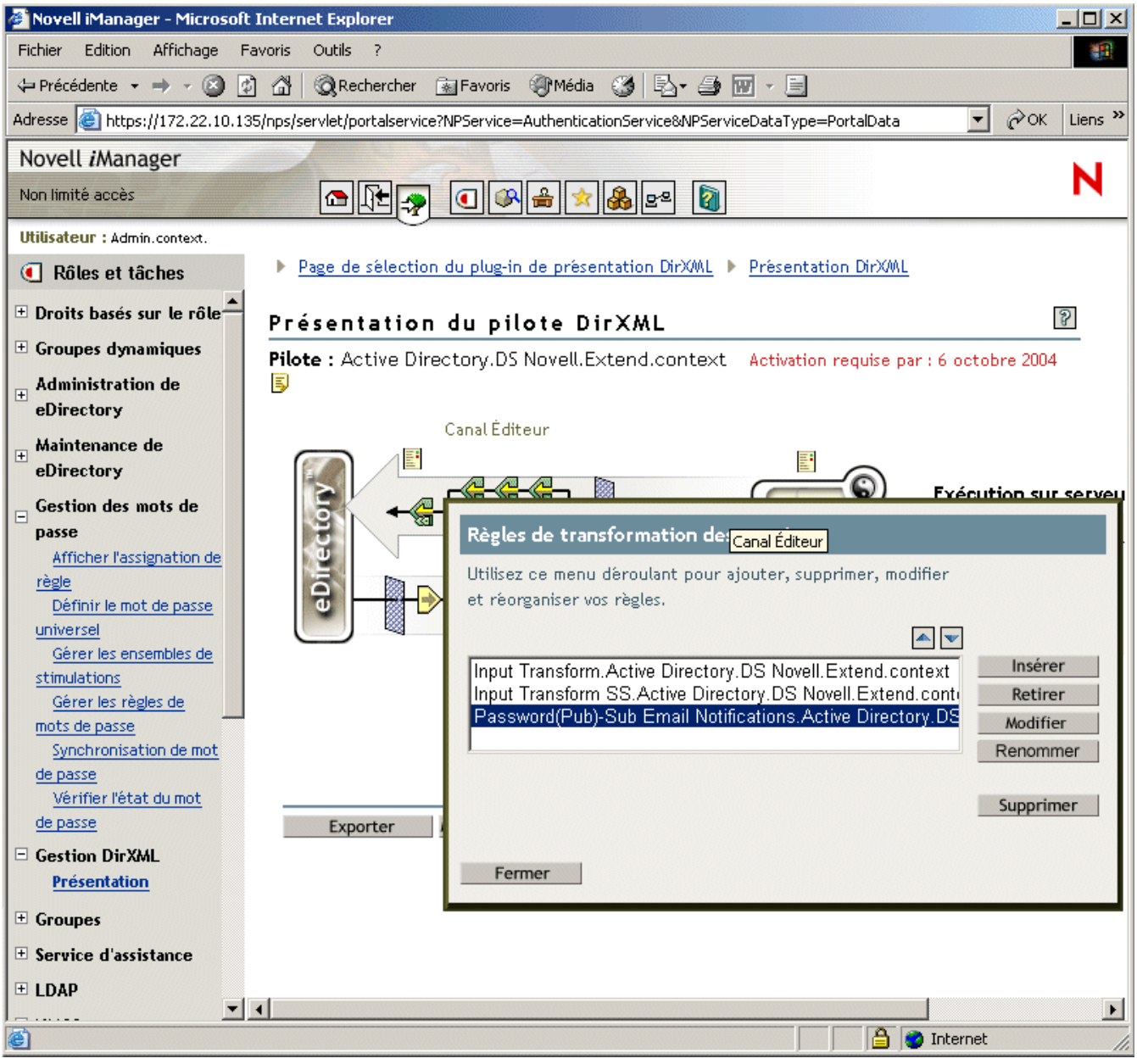
3. Cliquez sur l'icône du pilote contenant la règle à modifier.

4. Cliquez sur l'ensemble de règles qui contient la règle à modifier.

   Par exemple, la configuration du pilote eDirectory livré avec Identity Manager contient une règle dans l'ensemble de règles Transformation de l'entrée qui fait référence aux deux modèles de notification par message électronique pour la synchronisation des mots de passe.

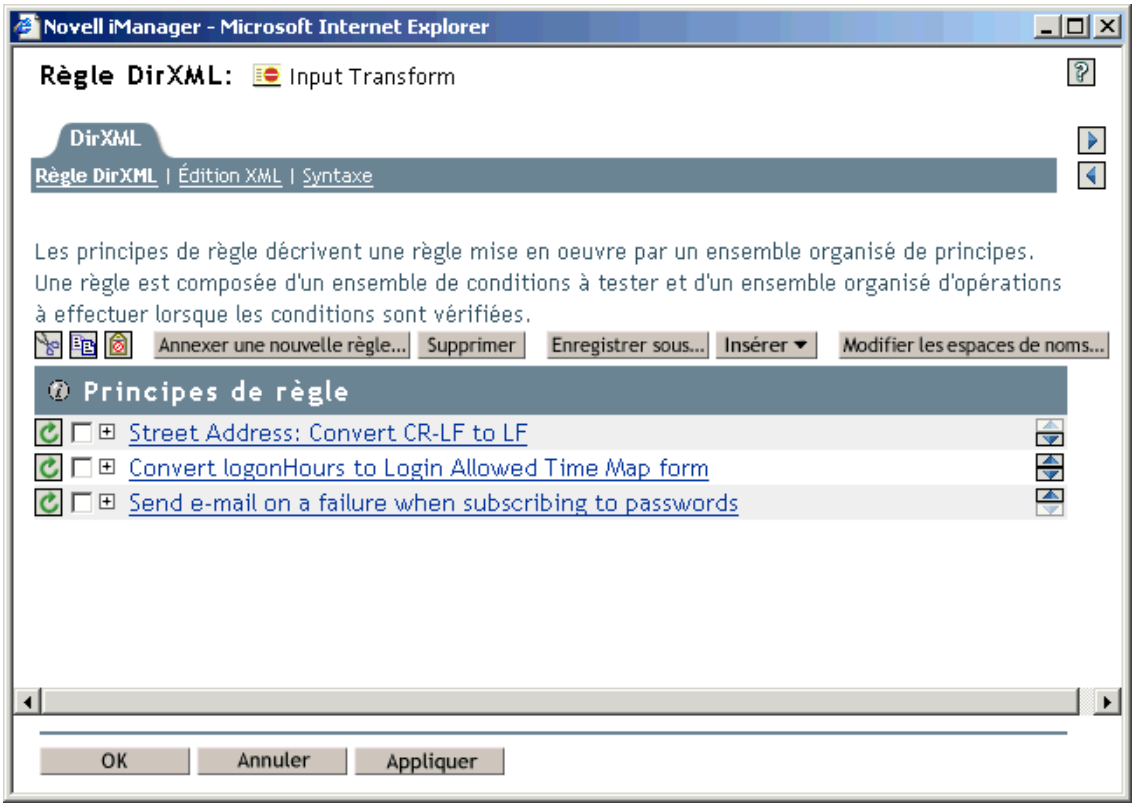
5. Cliquez sur la règle, puis sur Modifier.

   Par exemple, si vous modifiez la règle Password(Pub)-Sub Email Notifications pour le pilote eDirectory, cliquez sur Modifier dans cette page :

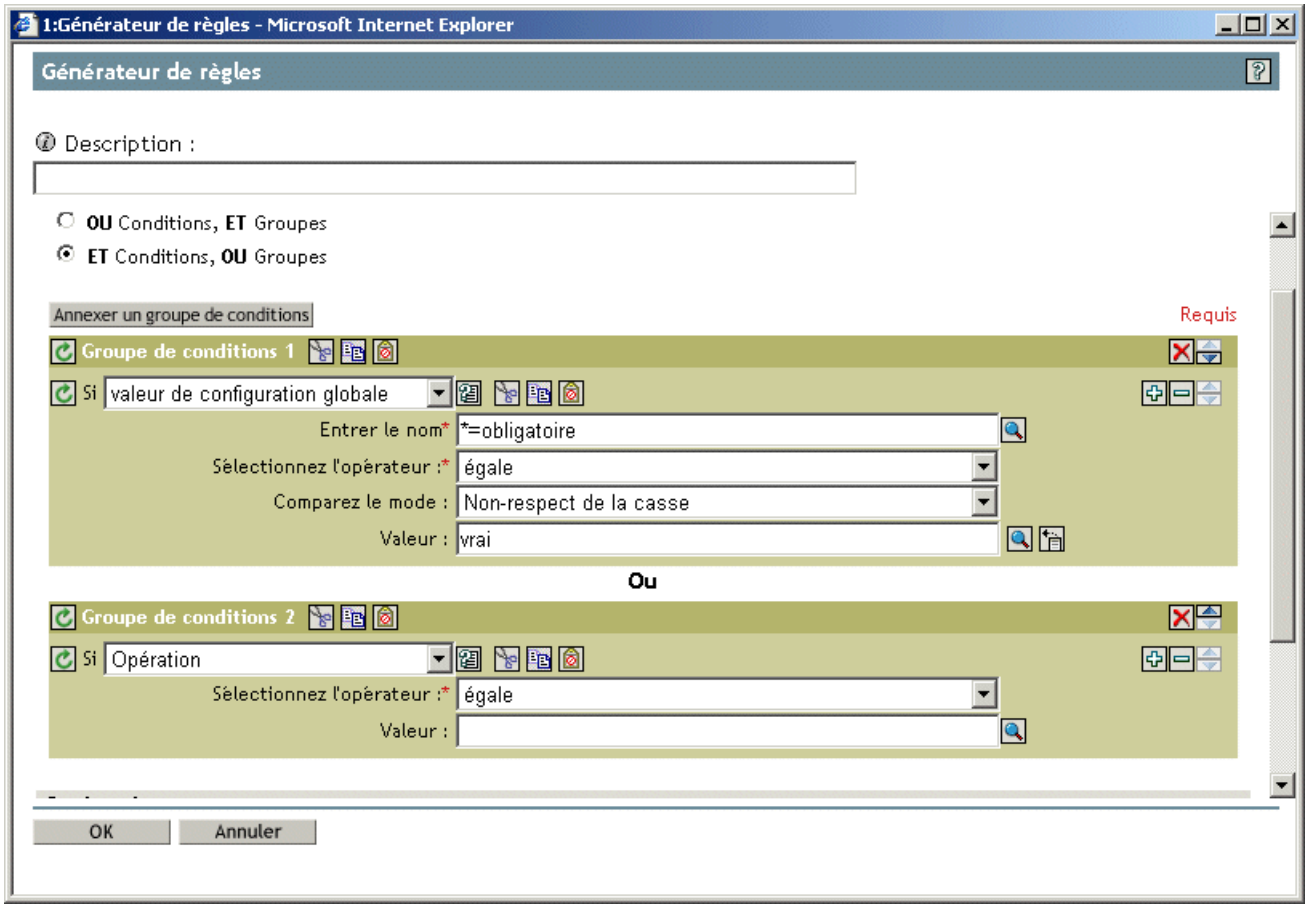

Novell iManager - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente Rechercher Favoris Média
Adresse https://172.22.10.135/nps/servlet/portalservice?NPService=AuthenticationService&NPServiceDataType=PortalData
OK Liens
Novell iManager
Non limité accès
Utilisateur : Admin.context.
Rôles et tâches
Droits basés sur le rôle
Groupes dynamiques
Administration de eDirectory
Maintenance de eDirectory
Gestion des mots de passe
Afficher l'assignation de règle
Définir le mot de passe universel
Gérer les ensembles de stimulations
Gérer les règles de mots de passe
Synchronisation de mot de passe
Vérifier l'état du mot de passe
Gestion DirXML
Présentation
Groupes
Service d'assistance
LDAP
Page de sélection du plug-in de présentation DirXML
Présentation DirXML
Présentation du pilote DirXML
Pilote : Active Directory.DS Novell.Extend.context
Activation requise par : 6 octobre 2004
Canal Éditeur
eDirectory
Exécution sur serveu
Règles de transformation de
Canal Éditeur
Utilisez ce menu déroulant pour ajouter, supprimer, modifier et réorganiser vos règles.
Input Transform.Active Directory.DS Novell.Extend.context
Input Transform SS.Active Directory.DS Novell.Extend.cont
Password(Pub)-Sub Email Notifications.Active Directory.DS
Insérer
Retirer
Modifier
Renommer
Supprimer
Exporter
Fermer
Internet

6 Dans la liste des principes qui s'ouvre, cliquez sur celui qui fait référence au modèle de notification par message électronique.

Cette liste de principes apparaît par exemple dans la règle Password(Pub)-Sub Email Notifications. Ces deux principes 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.

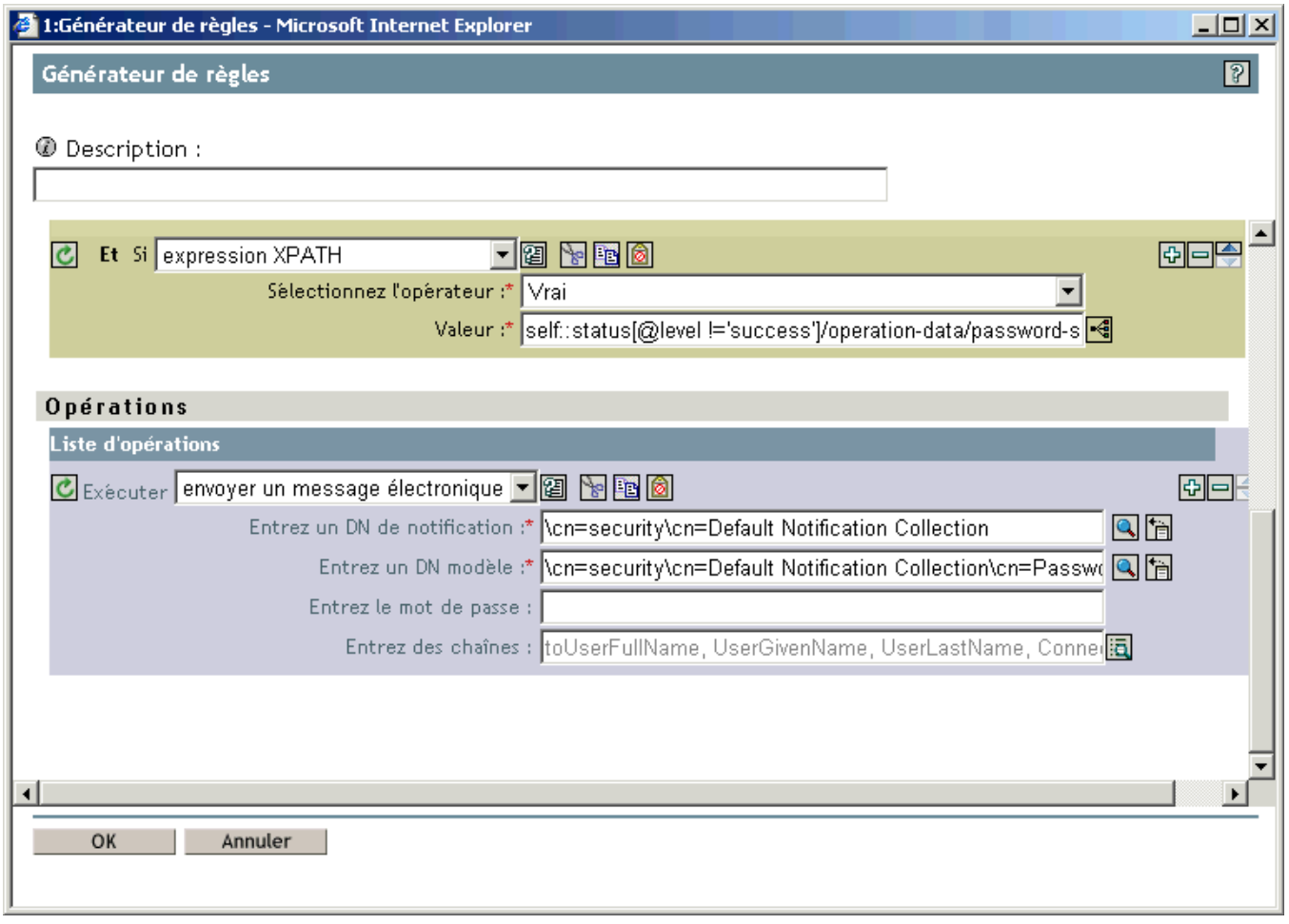


Si vous cliquez sur le premier principe, la page suivante s'affiche :



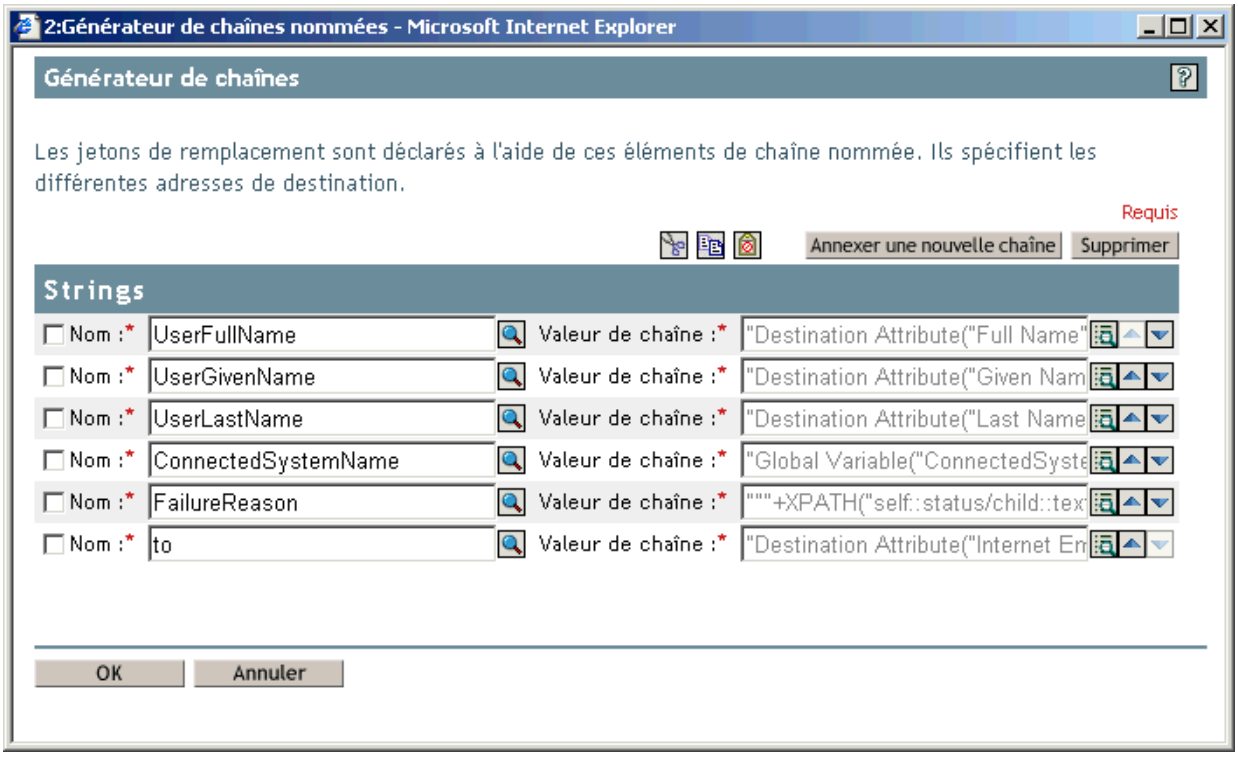
7 Faites défiler l'écran jusqu'à la section des principes qui affiche les opérations.

Dans l'exemple de principe, allez jusqu'à cette section :



8 Pour le principe d'envoi d'un message électronique à partir d'un modèle, cliquez sur le bouton de navigation pour le champ Entrez 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 règles de synchronisation des mots de passe faisant partie des configurations de pilote DirXML, comme celui-ci. Vous pouvez utiliser les balises par défaut à titre d'exemple.



9 Cliquez sur Annexer une nouvelle chaîne pour définir une balise que vous pourrez utiliser dans un modèle de notification par message électronique. Nommez la balise en utilisant le même nom que pour le modèle de notification par message électronique.

10 Dans le champ Jetons de chaîne, cliquez sur le bouton de navigation pour vous aider à définir la balise.

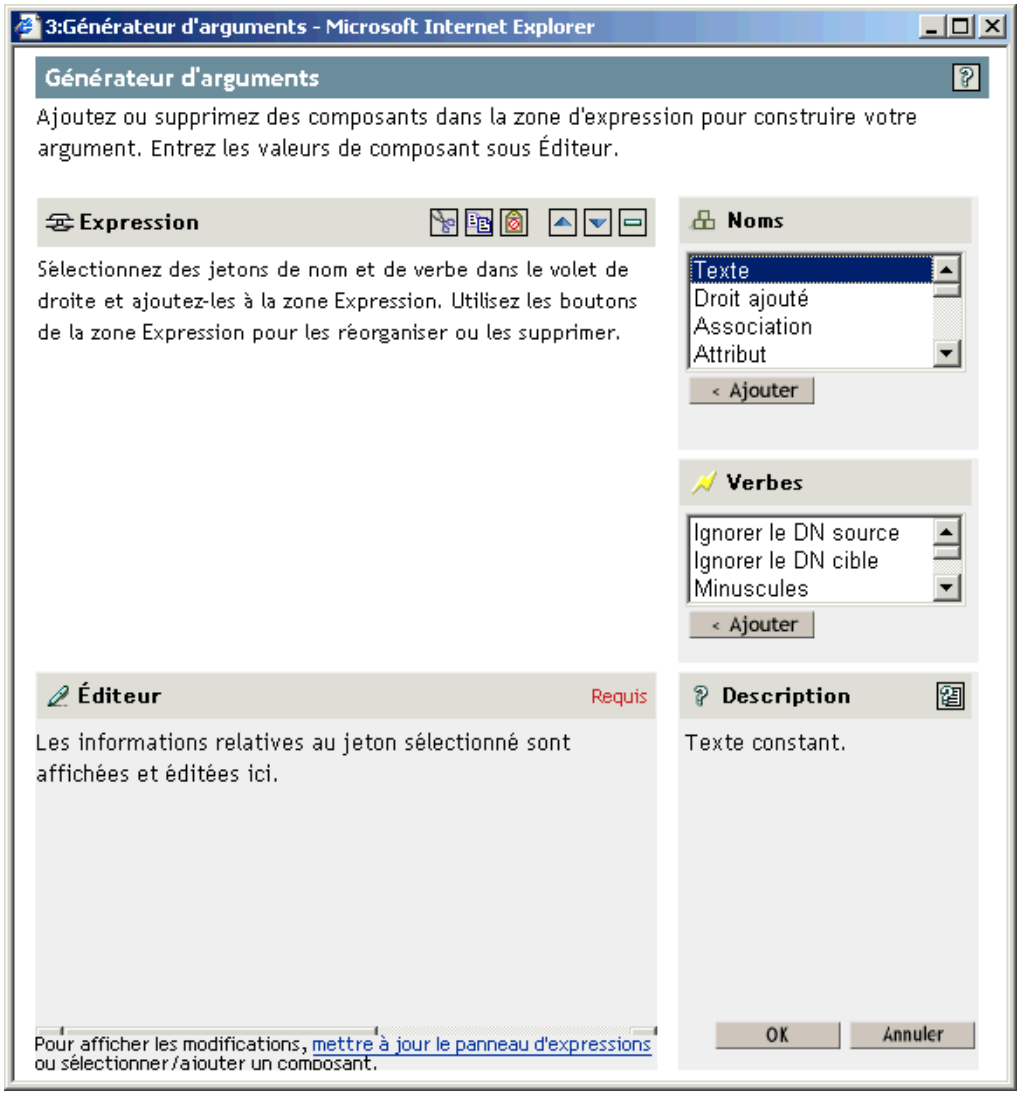
La page du Générateur d'arguments s'affiche. Vous y spécifiez la valeur à intégrer lorsque cette balise est utilisée dans un modèle de notification de message électronique. Vous pouvez définir la balise sur l'un des points suivants :

- Tout attribut Source ou Destination pour l'utilisateur

  À la différence de l'ajout de balises pour les modèles de messages électroniques de mot de passe oublié, l'ajout d'une balise ayant le même nom qu'un attribut sur l'objet Utilisateur dans eDirectory 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 règle qui fait référence au modèle de message électronique.

- Une valeur de configuration globale
- Une expression XPATH

La figure suivante montre un exemple de la page qui vous aide à définir la balise.



Après avoir défini la balise et cliqué sur OK, elle fait partie des chaînes de la page du Générateur de chaînes.

11 N'oubliez pas de cliquer sur OK pour valider toutes les pages, afin d'enregistrer les modifications de la règle.

12 Répétez les étapes de modification des principes dans toutes les règles qui font référence au modèle de notification par message électronique.

13 Ajoutez la balise définie dans la règle pour le modèle de notification par message électronique, à l'aide du nom exact utilisé dans les règles.

À ce point de la procédure, vous pouvez utiliser le nom de balise présent dans le corps du modèle de notification par message électronique.

14 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 d'attributs eDirectory, reportez-vous à la règle d'assignation de schéma fournie dans le pilote DirXML pour LDAP.
- Aucune autre configuration n'est nécessaire.

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 règles livrées avec Identity Manager utilisent l'adresse électronique de l'objet eDirectory pour l'utilisateur concerné.

Vous pouvez toutefois configurer les règles de synchronisation des mots de passe de sorte que les notifications soient également adressées à l'administrateur. Pour cela, vous devez modifier le script DirXML pour l'une de ces règles.

Adressez une copie cachée à l'administrateur en définissant le jeton avec l'adresse électronique de l'administrateur.

Pour mettre un administrateur en copie, modifiez la règle de génération du message électronique, par exemple PublishPasswordEmails.xml, dans laquelle la règle étudie l'adresse électronique pour envoyer les notifications, et ajoutez un élément <arg-string> avec l'adresse électronique de l'administrateur. L'exemple ci-après montre un élément arg-string supplémentaire.

```
<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.

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 règles 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, qui indiquera le codage à utiliser dans le courrier. 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 <attachment>.

  Pour plus d'informations sur l'utilisation de ces éléments, reportez-vous au *Guide d'implémentation du Pilote DirXML pour Manual Task Service* (http://www.novell.com/documentation/dirxmldrivers/index.html), qui vous donnera de plus amples informations sur les modèles de messages électroniques.

Dépannage des problèmes de synchronisation des mots de passe

- Pour plus d'informations sur les astuces, reportez-vous à la section « Mise en œuvre de la synchronisation des mots de passe », page 202.
- 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 règles de mot de passe sur les méthodes de login d'eDirectory ou sur les mots de passe des systèmes connectés synchronisés par Identity Manager.
- Vérifiez que tous les utilisateurs pour lesquels vous souhaitez procéder à la synchronisation des mots de passe sont répliqués sur le même serveur, avec le pilote qui effectue 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 eDirectory.

- Si un message d'erreur indique qu'un mot de passe correctement configuré dans eDirectory ne correspond pas lorsqu'un utilisateur est créé, alors le problème est peut-être lié au mot de passe par défaut de la règle Pilote : ce mot de passe n'est peut-être pas conforme à la règle de mots de passe qui s'applique à cet utilisateur.

  Voici un exemple de l'utilisation du pilote Active Directory, même si ce problème pourrait survenir pour un autre pilote.

  Exemple : vous souhaitez que le pilote Active Directory fournisse le mot de passe utilisateur initial lorsqu'un nouvel objet Utilisateur est créé dans eDirectory pour correspondre à un utilisateur dans 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 règle fournissant un mot de passe par défaut à l'utilisateur, si Active Directory ne fournit aucun mot de passe. Ces deux opérations étant effectuées séparément, tout nouvel utilisateur reçoit toujours un mot de passe par défaut ; celui-ci n'est effectif que le temps qu'Active Directory renvoie le mot de passe, juste après avoir l'ajout de l'utilisateur. Si le mot de passe par défaut ne répond pas aux exigences de la règle de mots de passe d'eDirectory, un message d'erreur apparaît. Par exemple, si le mot de passe par défaut créé en fonction 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 règle.

  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 règle qui crée le mot de passe par défaut, afin que celui-ci soit conforme aux règles de mots de passe définies pour votre organisation dans eDirectory (le mot de passe est créé à l'aide de Gestion des mots de passe > Gérer les règles 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 règle de mots de passe par défaut, afin que le niveau de sécurité du système soit aussi élevé que possible.

    ou

  - Sur le canal Éditeur, supprimez la règle qui crée le mot de passe par défaut. Dans l'exemple de configuration, cette règle est fournie par l'ensemble de règles de transformation de la commande. Dans eDirectory, l'ajout d'un utilisateur sans mot de passe est autorisé. Pour cette option, l'objet utilisateur nouvellement créé est passé par le canal Éditeur ; ainsi, cet objet n'a pas de mot de passe que temporairement.

- Les règles de mot de passe sont assignées dans une perspective centrée sur l'arborescence. Par opposition, la synchronisation des mots de passe est définie par pilote ; ceux-ci sont installés sur les serveurs et ne peuvent gérer que les utilisateurs existants d'une réplique principale ou d'une réplique 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 règles de mot de passe en activant le mot de passe universel. L'assignation d'une règle de mot de passe au conteneur racine d'une partition garantit que cette règle s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

- Commandes DSTrace utiles :

  +DXML : affiche le traitement des règles DirXML et les messages d'erreur potentiels.
  +DVRS : affiche les messages du pilote DirXML.
  +AUTH : affiche les modifications des mots de passe NDS.
  +DCLN : affiche les messages NDS Dclient.

10 Utilisation des droits basés sur le rôle

Les droits basés sur le rôle permettent d'accorder des droits sur des systèmes connectés à un groupe d'utilisateurs de Novell® eDirectory™. Avec les règles de droits, vous pouvez rationaliser la gestion des règles dans votre entreprise et réduire la nécessité de configurer vos pilotes DirXML®.

Cette section contient les informations suivantes :

Présentation

Les droits basés sur le rôle permettent de définir des règles d'entreprise relatives aux personnes auxquelles doivent être accordés des droits dans votre environnement. Utilisez une règle de droit (un groupe dynamique eDirectory amélioré) pour définir les utilisateurs auxquels doivent être accordés des droits en fonction de critères de recherche dynamique, par exemple une appellation d'emploi Testeur. Vous pouvez gérer les exceptions à l'aide d'une liste statique d'inclusions et d'exclusions pour la règle.

Une fois les utilisateurs auxquels s'applique la règle définis, vous spécifiez les droits que vous souhaitez leur accorder sur les systèmes connectés. Vous pouvez aussi accorder des droits dans eDirectory comme pour n'importe quel groupe dynamique.

Les droits sur les systèmes connectés sont accordés par les pilotes DirXML configurés pour prendre en charge les droits basés sur le rôle.

Ce modèle d'administration des règles d'entreprise diffère de la méthode traditionnelle de provisioning avec Identity Manager ; en effet, vous spécifiez les règles d'entreprise en amont de la configuration du pilote DirXML.

Les droits sur les systèmes connectés sont habituellement administrés pilote par pilote ; il suffit de créer et de modifier les règles de configuration des pilotes, telles que celles créées avec le Générateur de règles. Selon ce modèle distribué traditionnel, un administrateur souvent différent contrôle chaque pilote DirXML et système connecté ; les règles d'entreprise qui déterminent si un utilisateur a le droit ou non d'accéder aux ressources de ce système sont codées en dur dans les règles de configuration des pilotes, indépendamment pour le pilote 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 règles d'entreprise. Un tel administrateur doit connaître Identity Manager dans sa globalité, mais n'est pas obligé de maîtriser parfaitement Identity Manager ou XSLT pour utiliser l'interface des droits basés sur le rôle.

Une autre différence entre les droits basés sur le rôle et l'administration traditionnelle d'Identity Manager réside dans le fait que les règles de droit apportent des modifications directement dans un environnement de production. Les modifications apportées aux configurations de pilote sont en général préalablement testées en laboratoire. Les règles de droit permettent de simplifier la modification des règles d'entreprise, mais vous devez être prudent lorsque vous effectuez ces modifications dans votre environnement de production. Pour des suggestions, reportez-vous à la section « Sécurisation des comptes », page 273.

Voici un scénario destiné à vous faire comprendre les différences entre les deux méthodes :

Exemple de règle d'entreprise

Supposons que vous souhaitez accorder automatiquement à chaque nouvel employé l'appellation d'emploi Testeur, en lui attribuant deux éléments :

- Un compte de messagerie GroupWise®
- Un compte dans une base de données Oracle utilisée pour le suivi des défauts

Configuration de la règle d'entreprise

Traditionnelle : dans le modèle traditionnel, un développeur Identity Manager utilise le Générateur de règles ou une feuille de style pour coder en dur la règle d'entreprise dans la configuration des pilotes DirXML pour JDBC et GroupWise.

Droits basés sur le rôle : utilisez les droits basés sur le rôle dans cet exemple, pour créer une règle de droit et définir une appartenance de groupe dynamique pour l'appellation d'emploi Testeur. Un développeur Identity Manager peut également configurer les pilotes DirXML pour GroupWise et JDBC de manière à ce qu'ils prennent en charge les droits basés sur le rôle. Les pilotes accordent alors des comptes aux utilisateurs qui satisfont aux critères d'appartenance de groupe dynamiques.

À ce stade, le résultat est identique dans l'exemple. Quelle que soit la méthode utilisée, un compte est automatiquement accordé aux utilisateurs dont l'appellation d'emploi est Testeur.

Cependant, si vous utilisez le modèle des droits basés sur le rôle, vous n'êtes pas obligé de disposer d'autant de connaissances sur Identity Manager pour modifier cette règle d'entreprise.

Modification de la règle d'entreprise

Supposons qu'après avoir configuré la règle d'entreprise, vous découvrez que vous devez également attribuer les mêmes types de comptes aux utilisateurs dont l'appellation d'emploi est Responsable des tests.

Traditionnelle : selon le modèle traditionnel, un développeur Identity Manager utilise le Générateur de règles pour coder en dur les modifications à apporter à la règle d'entreprise en deux points :

- La configuration du pilote pour GroupWise
- La configuration du pilote pour JDBC

Droits basés sur le rôle : selon le modèle des droits basés sur le rôle, un administrateur réseau maîtrisant les filtres LDAP peut facilement ajouter les critères utilisateur supplémentaires à l'appartenance de groupe dynamique dans la règle de droit sans modifier le script DirXML. Les pilotes JDBC et GroupWise accordent alors les comptes aux utilisateurs appropriés sans modifier la configuration des pilotes.

Fonctionnement des droits basés sur le rôle

La fonctionnalité des droits basés sur le rôle repose sur le pilote de service de droits, un service de moteur qui surveille si des utilisateurs appartiennent ou non à une règle de droit. Si un utilisateur satisfait aux critères d'appartenance d'un groupe dynamique de règles de droits ou est inclus de manière statique, le pilote de service de droits ajoute les informations à l'attribut DirXML-SPEntitlements sur l'utilisateur. Le droit qu'un utilisateur doit recevoir est inscrit dans l'attribut.

Pour les systèmes répertoriés à la section « Configuration des pilotes pour l'utilisation des règles de droits », page 265, vous pouvez choisir l'option des droits basés sur le rôle lorsque vous importez l'exemple de configuration de pilote Identity Manager. Vous pouvez ensuite étudier les règles fournies, qui prennent en charge les droits basés sur le rôle en surveillant l'attribut DirXML-SPEntitlements et en accordant ou en supprimant des droits.

L'attribut DirXML-SPEntitlements est mis à jour par le pilote de service de droits uniquement en cas de survenue de l'un des événements suivants :

- Vous utilisez la tâche Réévaluer les membres.

  Vous pouvez spécifier dans quelle partie de l'arborescence les utilisateurs doivent être réévalués.
- L'utilisateur est déplacé.
- L'utilisateur est renommé.
- Un attribut utilisé pour l'appartenance à une règle de droit est modifié.

Les règles de droit permettent d'accorder des droits sur les systèmes connectés et les droits dans eDirectory. Les droits sur les systèmes connectés peuvent être les suivants :

- Comptes
- Appartenance aux listes de distribution de courrier électronique
- Appartenance au groupe
- Attributs pour les objets correspondants des systèmes connectés, peuplés avec les valeurs que vous spécifiez
- Placement
- Autres droits que vous personnalisez

Certaines options sont décrites dans les exemples de configuration du pilote.

Un seul pilote de service de droits étant utilisé pour chaque ensemble de pilotes, une règle 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 droits basés sur le rôle reposant sur Identity Manager, les pilotes DirXML doivent être installés et configurés correctement pour que vous puissiez gérer des systèmes connectés.

En outre, pour éviter des conflits possibles entre les assignations de règles de droits et les configurations des pilotes DirXML, vous devez connaître vos règles d'entreprise et la façon dont elles sont gérées via Identity Manager. Dans la gestion d'un attribut, il ne doit pas y avoir de chevauchement ou de conflit entre les règles de droit DirXML et les règles dans la configuration d'un pilote.

Conditions préalables

- ❑ eDirectory 8.7.3 (cette fonctionnalité ne prend pas en charge eDirectory 8.7.1).
- ❑ Identity Manager.
- ❑ 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 basés sur le rôle. Pour cela, vous devez procéder à une configuration simple et ponctuelle pour chaque ensemble de pilotes. Reportez-vous à la section « Création d'un objet Pilote pour le pilote de droits », page 264.
- ❑ Une configuration de pilote qui prend en charge les droits basés sur le rôle. Pour utiliser les droits basés sur le rôle avec un système connecté, vous devez importer l'exemple de configuration de pilote Identity Manager pour le pilote et spécifier que ce pilote doit être utilisé avec les droits basés sur le rôle, ou créer votre propre configuration de pilote qui prend en charge les droits basés sur le rôle. Reportez-vous à la section « Configuration des pilotes pour l'utilisation des règles de droits », page 265.

Création d'un pilote de service de droits et configuration des pilotes de systèmes connectés

Cette section contient les informations suivantes :

Création d'un objet Pilote pour le pilote de droits

Pour créer des règles 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 en créer un lorsque vous cliquez sur la tâche et le rôle des droits basés sur le rôle.

1. Pour déterminer si vous possédez déjà un pilote de service de droits, dans iManager, cliquez sur Droits basés sur le rôle > Droits basés sur le rôle. 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 règles de droits, vous disposez déjà d'un objet Pilote de service de droits. Vous n'avez alors pas besoin de terminer cette procédure.
2. Sur la page Aucun pilote de service de droits, cliquez sur OK. L'assistant d'importation des pilotes (également accessible en cliquant sur Utilitaires DirXML > Importer des pilotes) s'ouvre.
3. Suivez les différentes étapes de création d'un objet Pilote en choisissant Pilote de service de droits dans la liste des pilotes.

   Le bon fichier de configuration de pilote est automatiquement choisi. Il suffit de choisir un nom pour l'objet Pilote ; aucune configuration ou information supplémentaire n'est nécessaire.

   Le module d'interface pilote pour le pilote de droits est installé par défaut lors de l'installation de DirXML. Le fichier de configuration du pilote de droits est installé par défaut lors de l'installation des plugs-in DirXML sur votre serveur iManager.
4. Une fois les étapes de l'assistant terminées, vous pouvez accéder aux plugs-in pour les droits basés sur le rôle et commencer à créer des règles de droits pour l'ensemble de pilotes.

Configuration des pilotes pour l'utilisation des règles de droits

Pour utiliser les droits basés sur le rôle avec un système connecté, vous devez installer un module d'interface pilote Identity Manager.

Le pilote doit être configuré pour prendre en charge les droits basés sur le rôle ; les entrées du manifeste de pilote doivent donc être correctes.

Vous pouvez importer un exemple de configuration de pilote Identity Manager pour le pilote et choisir d'utiliser les droits basés sur le rôle, ou personnaliser une configuration de pilote en suivant l'exemple de configuration de pilote.

Les exemples de configuration de pilote suivants prennent en charge, en option, les droits basés sur le rôle :

- Active Directory
- Exchange
- GroupWise
- LDAP
- NIS
- Notes
- NT Domain

Ces configurations représentent des exemples de ce que vous pouvez faire avec les droits basés sur le rôle. Vous pouvez configurer d'autres pilotes de systèmes connectés et d'autres types de droits et variables interprétatives.

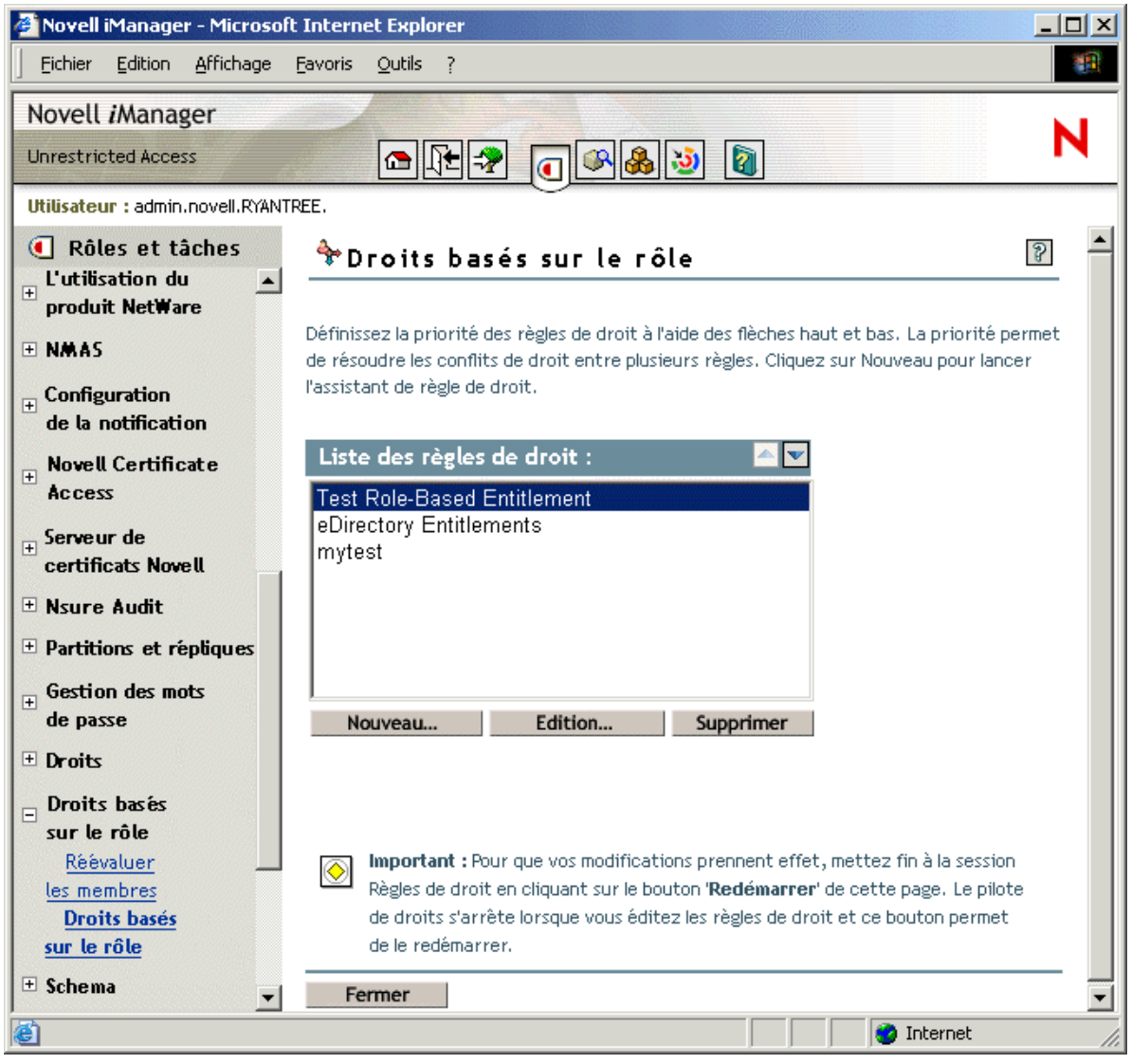
Création de règles de droits

Utilisez l'assistant fourni pour créer une règle 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 règles de droits.

   La liste des règles de droits existantes s'ouvre, comme sur la page de la capture suivante. 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 création d'une nouvelle règle de droit s'ouvre.

5 Suivez les étapes de l'assistant pour créer une nouvelle règle.

Consultez l'aide en ligne pour plu d'informations sur chaque étape de l'assistant.

Définition de l'appartenance à un groupe pour une règle de droit

À l'instar d'un pilote DirXML, chaque règle de droit ne peut gérer que les objets qui se trouvent dans une réplique principale ou en lecture/écriture sur le serveur auquel elle est assignée. Chaque règle de droit est associée à un seul objet ensemble de pilotes qui est assigné à un serveur particulier.

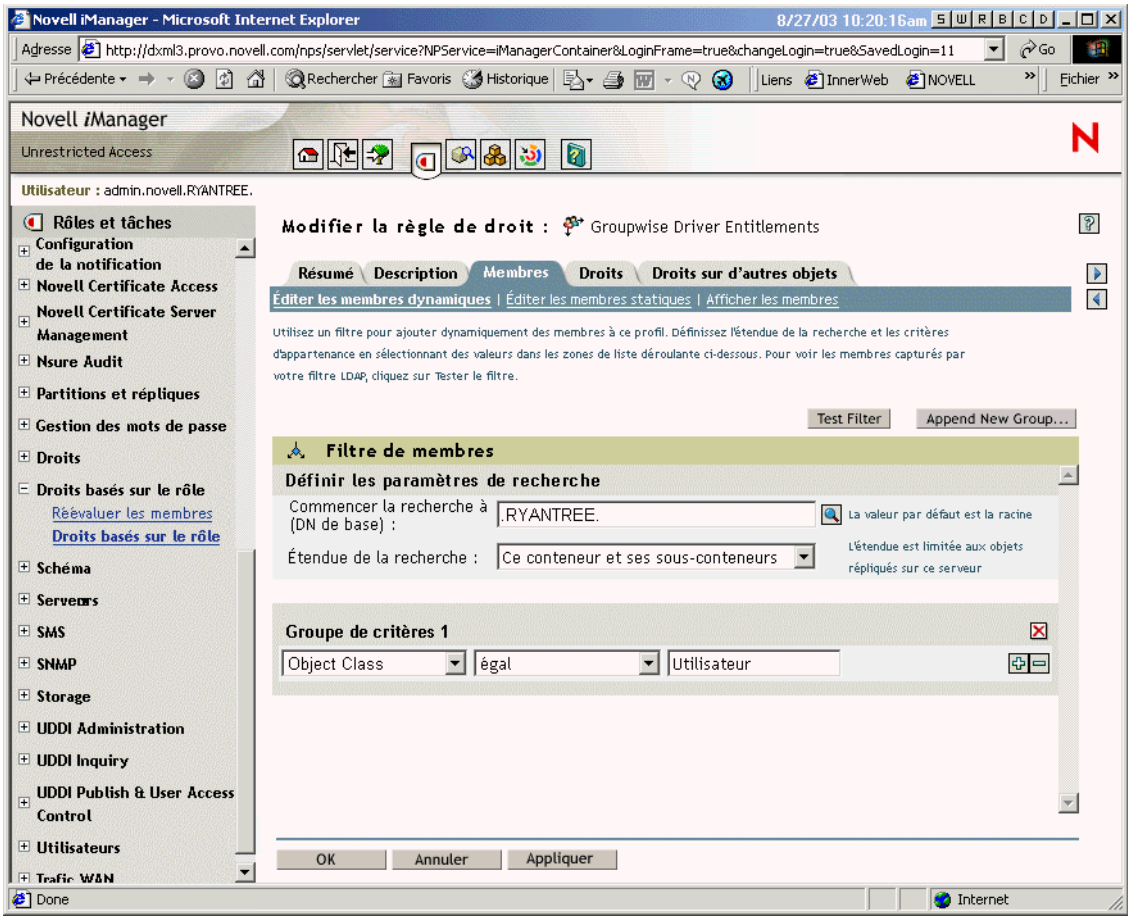
Seuls les objets utilisateur (et d'autres types d'objets dérivés de la classe utilisateur) peuvent être membres d'une règle de droit.

Une règle de droit est un objet de groupe dynamique. Vous pouvez définir l'appartenance à un groupe pour une règle de droit à l'aide de deux méthodes : dynamique et statique. Vous pouvez utiliser ces deux méthodes dans la même règle 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 satisfont ces critères sont automatiquement inclus dans la règle de droit sans que vous ayez à ajouter spécifiquement chaque utilisateur à la règle. L'appartenance à un groupe dynamique est identique à 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.



- **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 règle de droit.

Choix des droits pour une règle de droit

Les droits basés sur le rôle permettent d'accorder des droits sur les systèmes connectés et des droits dans eDirectory.

Les pilotes qui prennent en charge les droits basés sur le rôle proposent une liste de droits qui peuvent être assignés à l'aide d'une règle de droit. Les droits que le pilote peut fournir figurent dans une liste du manifeste de pilote, créée par le développeur du pilote pour représenter les fonctions du pilote et du système connecté. Le manifeste de pilote ne doit pas être modifié par un administrateur Identity Manager.

Des droits d'ayant droit sur les objets dans eDirectory sont immédiatement accordés aux membres de la règle de droit. Par défaut, les droits dans les systèmes connectés sont accordés à chaque membre de la règle de droit lors de la modification pour cet utilisateur d'un attribut utilisé pour l'appartenance à la règle de droit, ou lorsqu'un utilisateur est déplacé dans un autre conteneur ou renommé.

Les droits sur les systèmes connectés peuvent être 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

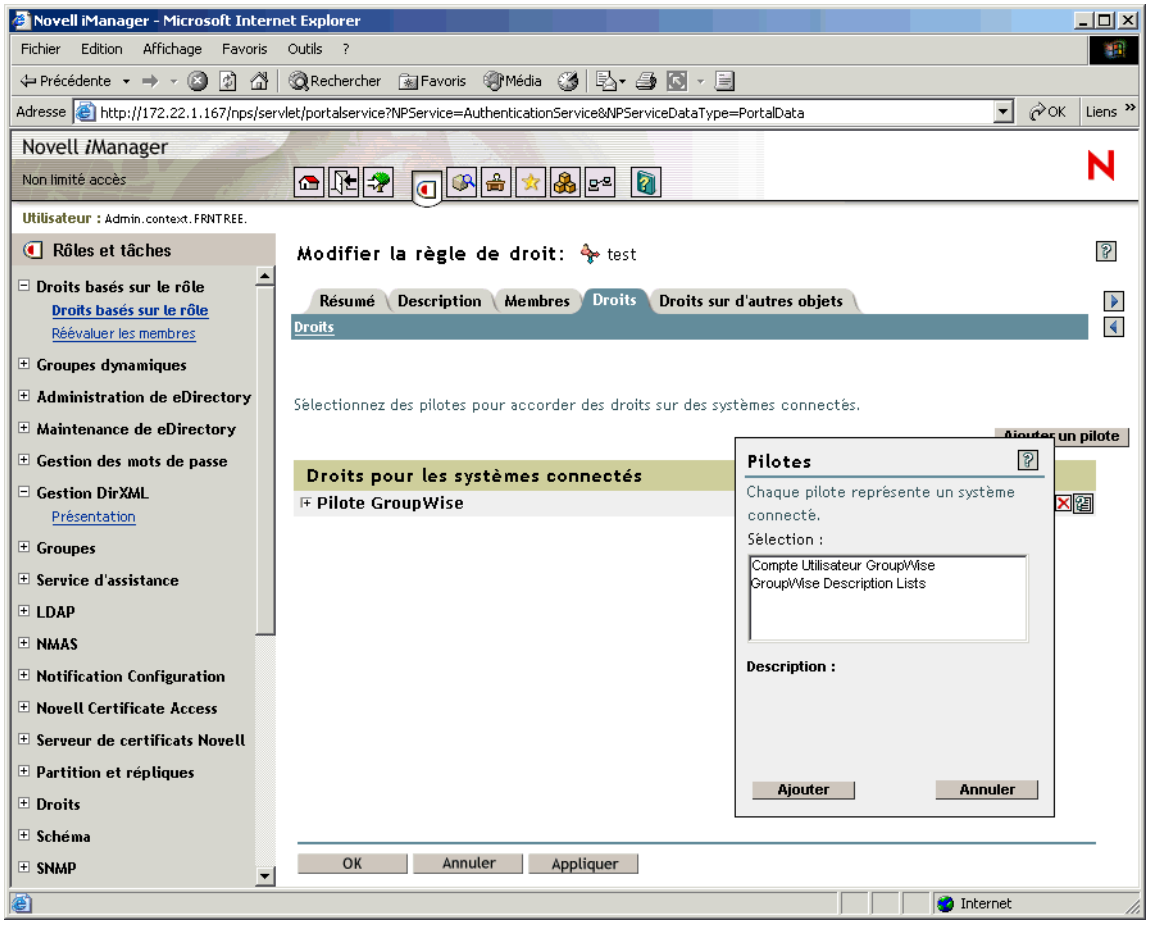
Cette section contient les informations suivantes :

- « Comptes sur les systèmes connectés », page 269
- « Appartenance à des listes de distribution de courrier électronique et des listes NOS », page 270
- « Valeurs d'attribut sur les systèmes connectés », page 271

Comptes sur les systèmes connectés

Pour ajouter des droits à une règle de droit, allez sur la page Droits, puis sélectionnez un pilote. Une fenêtre contextuelle indiquant les droits proposés par ce pilote s'affiche.

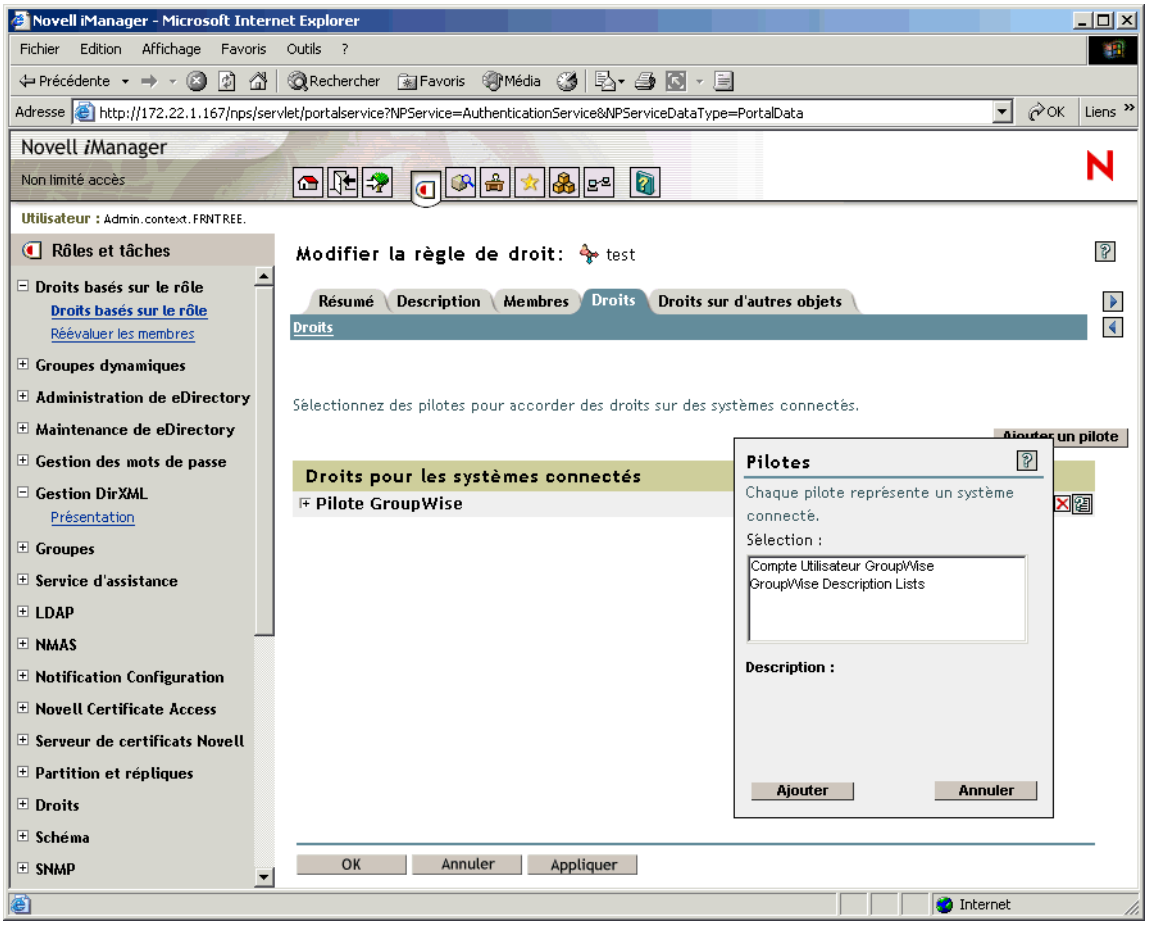
Ainsi, sur la capture suivante, vous pouvez voir deux sortes de droits proposés par un pilote GroupWise, le premier dans la liste étant un compte utilisateur GroupWise.



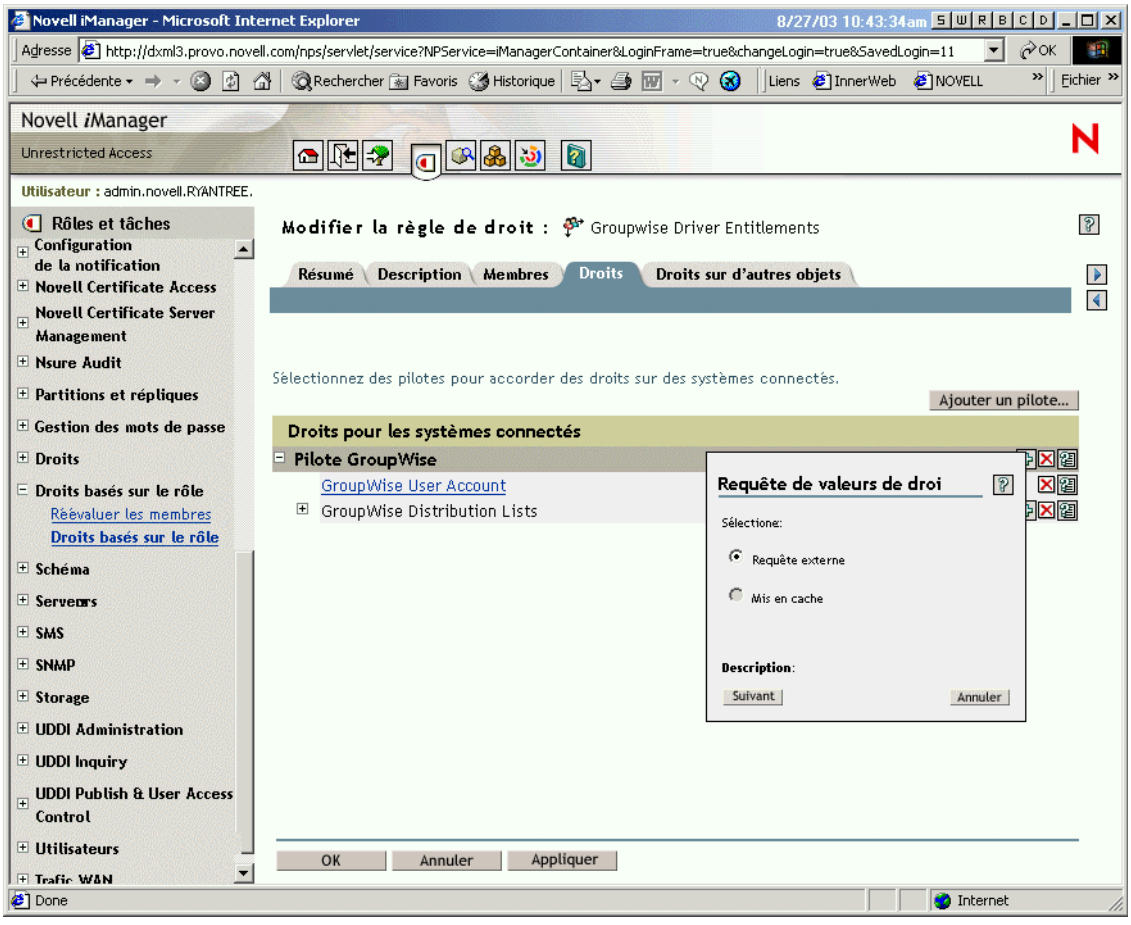
Appartenance à des listes de distribution de courrier électronique et des listes NOS

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.



Si vous choisissez les listes de distribution GroupWise dans cet exemple, une fenêtre contextuelle de requête s'affiche, comme dans l'exemple sur la capture suivante.



L'interface de règle de droit permet de lancer une requête pour 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.

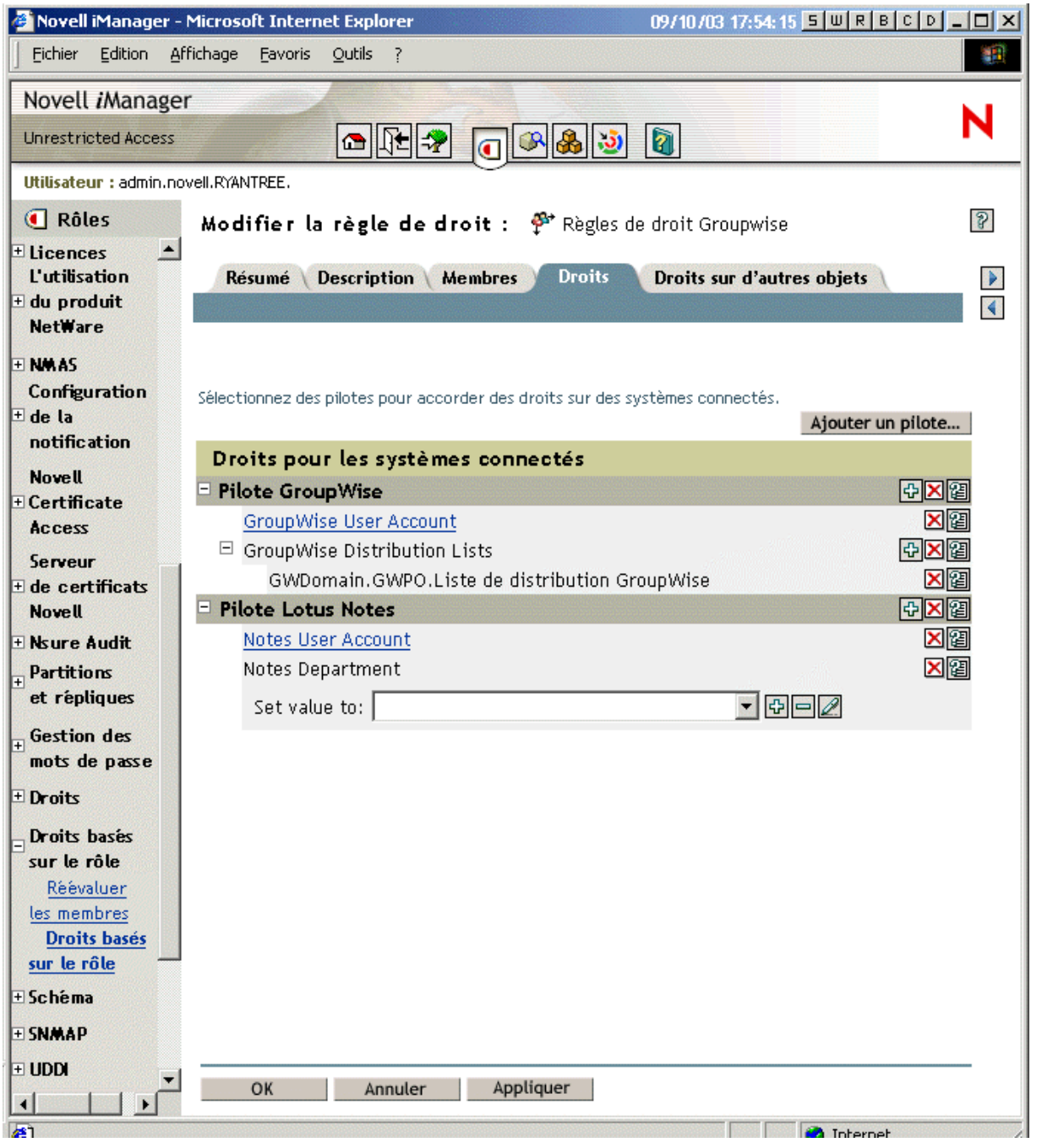
Les pilotes sont configurés pour renvoyer la liste complète afin que vous puissiez faire votre choix dans la liste qui se trouve sur le système connecté.

Remarque : vous pouvez personnaliser un pilote pour limiter la liste aux noms de groupes que vous saisissez 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 fournie permet de saisir la valeur que vous souhaitez que les comptes utilisateur aient.

La capture suivante présente un exemple d’ajout d’une valeur d’attribut pour un attribut Notes, Service.



Sécurisation des comptes

Les droits basés sur le rôle sont conçus pour mettre de l'ordre dans vos droits tels que les comptes et de les modifier en fonction de l'appartenance à la règle. Cela signifie cependant que des erreurs faites lors de la modification de règles risquent d'engendrer des problèmes. Les configurations de pilote fournies avec Identity Manager utilisent les paramètres les plus bénins. Vous devez connaître les paramètres qui permettent d'empêcher la perte de données.

Les deux types de paramètres les plus importants sont les variables interprétatives et la résolution de conflit. Reportez-vous aux sections « Contrôle de la signification de l'ajout ou de la suppression de droits », page 273 et « Résolution de conflit entre les règles de droits », page 274.

Nous vous recommandons, par exemple, de ne jamais utiliser la valeur de suppression pour supprimer un compte dans la variable interprétative. Les droits basés sur le rôle permettent de procéder à des modifications conséquentes dans votre environnement de production sans avoir à exécuter un cycle de test ; il se peut que vous commettiez une erreur en supprimant le droit de compte de quelqu'un sans le faire exprès.

Pour protéger des données, l'administrateur peut s'assurer que la variable interprétative pour supprimer des comptes a la valeur désactiver plutôt que supprimer.

Une autre mesure pour protéger vos données lorsque vous modifiez ou créez une nouvelle règle 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 règles. Vous pouvez alors ensuite redémarrer manuellement le pilote à l'aide du bouton Redémarrer dans l'interface des règles de droit. De même, s'il semble qu'un autre utilisateur est en train de modifier des règles de droit et si vous essayez de redémarrer le pilote 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.

Contrôle de la signification de l'ajout ou de la suppression 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 options d'ajout ou de suppression.

Ainsi, lors de l'ajout d'un compte GroupWise, vous pouvez spécifier qu'ajouter signifie en fait attribuer à un utilisateur un compte dans un état désactivé, si bien que l'administrateur doit intervenir pour que l'utilisateur puisse accéder au compte. 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 règles. Autre exemple : les configurations de pilote DirXML ne suppriment pas de droits qui tirent leurs valeurs d'un compte utilisateur dans un autre système. Si on accorde à un utilisateur l'appartenance à une liste de distribution de courrier électronique et si, par la suite, l'utilisateur ne satisfait plus aux critères de la règle de droit, il est tout simplement exclu de l'appartenance à la règle. 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 suppression d'un droit est particulièrement importante dans la mesure où la fonctionnalité des droits basés sur le rôle permet de mettre de l'ordre dans les droits d'une entreprise et de les modifier dans un environnement de production sans tester les résultats en laboratoire.

Vous pouvez modifier les paramètres pour l'interprétation de l'ajout ou de la suppression en cliquant sur le droit de compte de la page Droits dans la règle de droit. La page qui s'affiche permet de modifier les valeurs de configuration globales qui font partie des paramètres du pilote. N'oubliez pas que, bien que vous puissiez modifier les paramètres d'interprétation sur la page Droits d'une règle de droit individuelle, cette modification affecte toutes les règles de droits qui accordent ce droit particulier depuis ce pilote DirXML et ce système connecté, et pas uniquement la règle de droit que vous étiez en train de modifier. Les paramètres sont propres au droit et au pilote et pas à la règle de droit.

Reportez-vous également à la section « Résolution de conflit entre les règles de droits », page 274.

Dans les configurations de pilote Identity Manager 2, les variables interprétatives ne sont utilisées que sur les droits de compte. Vous pouvez toutefois configurer le pilote pour qu'il ait des variables interprétatives pour d'autres types de droits.

Remarque : les opérations prises en charge par un pilote sont déclarées dans le manifeste de pilote. Ce manifeste est créé par le développeur du pilote pour représenter les fonctions de la configuration de pilote. Ces options ne doivent pas être modifiées par un administrateur réseau. La modification du manifeste de pilote ne permet pas à elle seule au pilote de prendre en charge une nouvelle interprétation ; le pilote ou le système connecté doivent également être améliorés.

Résolution de conflit entre les règles de droits

Cette section contient les informations suivantes :

Présentation

Lorsque vous créez des règles de droits, il se peut que les règles 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 n'ont pas de valeurs s'ajoutent.** La plupart du temps, un compte est un droit qui ne possède pas de valeurs. Si un compte est accordé à un utilisateur sur un système connecté par n'importe quelle règle de droit, l'utilisateur reçoit un compte sur ce système. Peu importe s'il y a un conflit avec une autre règle 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.

  On pourrait utiliser comme métaphore pour les droits n'ayant pas de valeurs, un interrupteur ; il est soit activé soit désactivé, c'est-à-dire attribué ou non.

  Ainsi, si la règle de droit Responsable attribue à Jean Chandler un compte Exchange mais si cet utilisateur est exclu de la règle 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.** Il s'agit de droits tels que l'appartenance à un groupe avec une liste de noms de groupes pour les valeurs ou un attribut avec une valeur. Par défaut, ce type de droits s'ajoute également.

  Vous pouvez modifier la résolution de conflit pour ce type de droits si vous le souhaitez.

  Le paramètre qui réglemente la résolution de conflit pour chaque type de droit se trouve dans le manifeste de pilote d'un pilote en question. Chaque type de droit proposé par un pilote est indiqué 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 est `conflict-resolution="union"`. L'autre valeur possible est `conflict-resolution="priority"`.

  - **conflict-resolution="union" —** La valeur union signifie que les droits s'ajoutent. Tous les droits accordés du fait de l'appartenance à un règle 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 règle des 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, et s'il est exclu de l'appartenance à la règle des responsables de salons qui attribue également la liste de distribution de courrier électronique nommée 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 l'on attribue à Consuela l'appartenance au groupe AD nommé personnel du service courrier par la règle du service courrier ainsi que l'appartenance au groupe AD nommé réaction en cas d'urgence par la règle des volontaires d'urgence, on lui attribue l'appartenance aux deux groupes dans AD.

    Avec ce paramètre, la position d'une règle de droit dans la liste des règles n'est pas importante pour le droit en question.

  - **conflict-resolution="priority" —** Par opposition, une valeur de priorité signifie que, si des valeurs dans deux règles sont en conflit ou si une règle inclut l'utilisateur et qu'une autre l'exclut, les seuls droits attribués à l'utilisateur sont ceux compris dans la règle de droit la plus haut dans la liste des règles 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 règle des responsables de salons était plus haut dans la liste que la règle 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 une valeur de priorité, et si la règle de la salle de courrier était plus haut dans la liste à la règle des volontaires d'urgence, on ne pourrait lui accorder que l'appartenance au groupe du personnel de la salle de 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 souhaiteriez alors placer l'utilisateur à un endroit ou un autre, mais pas aux deux en même temps.

N’oubliez pas que le paramètre est indépendant pour chaque droit proposé par chaque pilote.

En règle générale, si vous utilisez le paramètre priorité, il est conseillé de placer les règles d’administrateur ou de responsable plus haut dans la liste que les règles concernant les utilisateurs finals ou les collaborateurs individuels. De même, il est préférable de placer les groupes avec le moins de membres plus haut que les groupes plus fournis.

Modification de la méthode de résolution de conflit pour un droit individuel

1. Dans iManager, cliquez sur Gestion DirXML > Présentation, puis sélectionnez un ensemble de pilotes.

   Une page avec une représentation graphique de tous les pilotes de l’ensemble de pilotes s’affiche.

2. Arrêtez le pilote.
3. Cliquez sur l’icône du pilote qui propose le droit que vous souhaitez modifier.

   Une page proposant des icônes pour les règles du pilote et le pilote s’affiche.

4. Cliquez sur l’icône du pilote pour ouvrir la page des paramètres du pilote.
5. Cliquez sur Manifeste du pilote.

   Le manifeste du pilote est affiché en XML mais est grisé car il n’est pas en mode d’édition.

6. Cochez la case Activer la modification du XML.
7. 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">
   ```

8. 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 la section « Résolution de conflit entre les règles de droits », page 274.

9. Redémarrez le pilote de service de droit.

Classement des règles de droits par ordre de priorité

Par défaut, l’ordre de la liste des règles de droits n’a pas d’importance, dans la mesure où les configurations de pilote livrées avec Identity Manager 2 ont comme méthode de résolution de conflit `conflict-resolution="union"` pour chaque droit.

Si vous modifiez un droit pour lui attribuer la valeur `conflict-resolution="priority,"`, alors l’ordre de la liste des règles de droits a une importance, mais uniquement pour les droits que vous avez modifiés. Pour plus d’informations sur ces valeurs, reportez-vous à la section « Résolution de conflit entre les règles de droits », page 274.

Pour modifier l'ordre des règles de droits, utilisez les flèches en regard de la liste des règles de droits. La première règle dans la liste a la plus haute priorité.

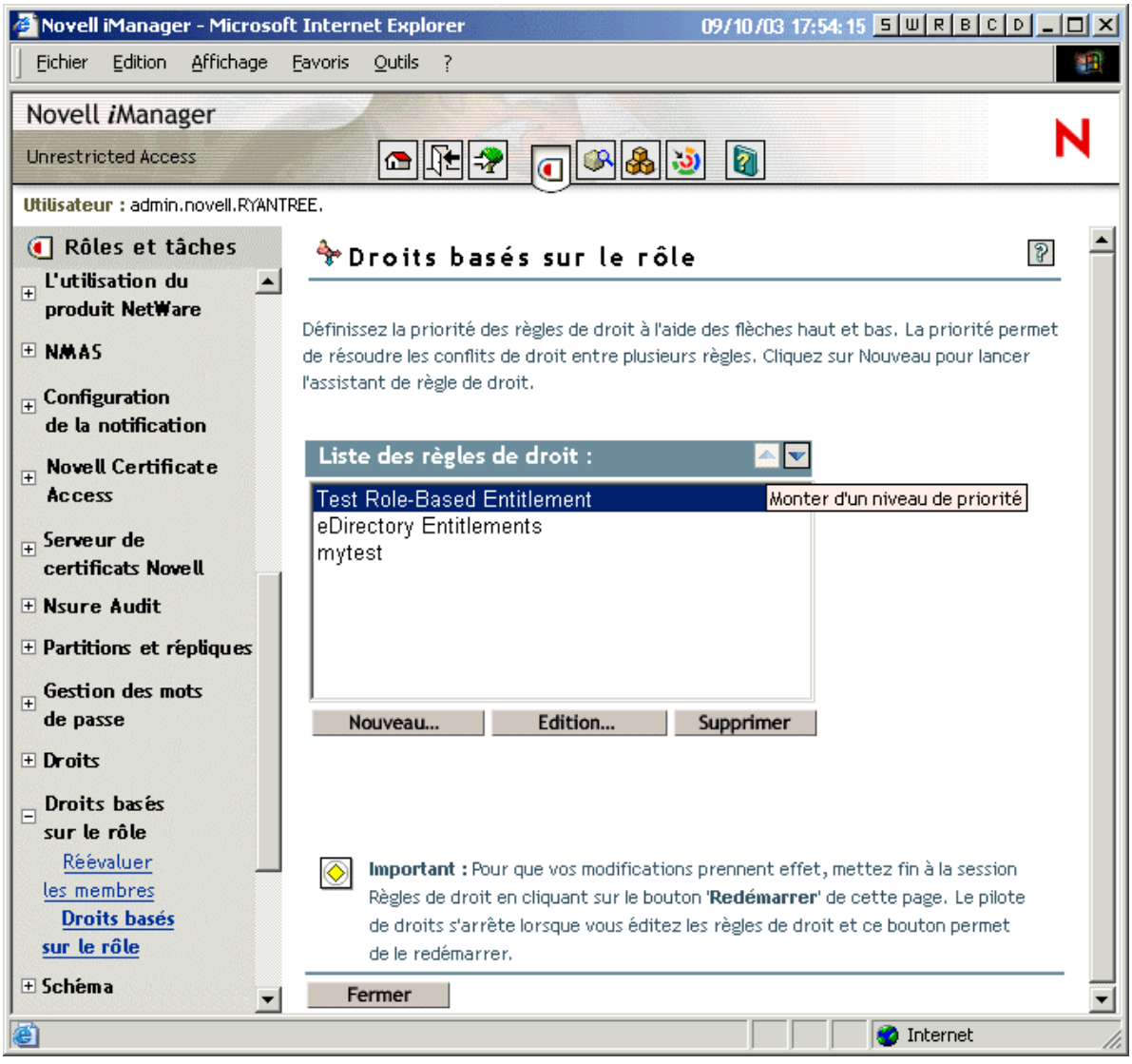
1. Dans iManager, cliquez sur Droits basés sur le rôle > Droits basés sur le rôle.
2. Recherchez un ensemble de pilotes, puis sélectionnez-le.

   Une page avec une liste des règles de droits s'affiche.
3. Modifiez la priorité des règles de droits à l'aide des flèches pour déplacer les règles vers le haut ou le bas de la liste.

   Déplacez une règle de droit plus haut dans la liste pour lui donner une plus haute priorité.
4. Cliquez sur le bouton Fermer pour redémarrer le pilote.

   Vous devez redémarrer le pilote pour que les modifications de priorités soient appliquées.

Observez la capture ci-dessous pour un exemple de page de liste de règles faisant apparaître les flèches.



Synchronisation des mots de passe et droits basés sur le rôle

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, tel que décrit au Chapitre 9, « Synchronisation de mot de passe sur des systèmes connectés », page 165.

Dépannage des droits basés sur le rôle

Lorsque vous procédez au dépannage, n'oubliez pas les éléments suivants :

- Lorsque vous modifiez des règles en cliquant sur Nouveau, Modifier ou Supprimer sur la page sur laquelle figure la liste des règles, le pilote de service de droits est arrêté. Il n'est pas redémarré à moins que vous ne cliquiez sur le bouton Fermer de cette page.

  Cette fonctionnalité empêche le pilote d'attribuer ou de supprimer des droits dans votre environnement de production tant que vos modifications de règles ne sont pas terminées.
- De même, le pilote de service de droits ne démarre pas s'il apparaît que plusieurs personnes modifient les règles de droits en même temps.
- Le pilote de service de droits ne démarre pas si l'objet Pilote est associé à plusieurs serveurs. Cette configuration n'est pas prise en charge.
- La règle de droit attribue des droits sur les systèmes connectés via un pilote DirXML. Le pilote est identifié par le GUID de l'objet Pilote dans eDirectory et pas par le nom de l'objet. Cela signifie que, si vous remplacez un objet Pilote par un autre objet Pilote du même nom, la règle de droit ne va pas fonctionner pour les droits sur ce pilote parce que l'objet a un nouveau GUID.
- Un seul pilote de service de droits étant utilisé pour chaque ensemble de pilotes, une règle 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.

11 Gestion des services de moteur

Certains pilotes ne sont utilisés que pour les services de moteur DirXML® et pas pour les systèmes connectés externes.

Cette section contient les informations suivantes :

Pilote de service de droits

Reportez-vous au Chapitre 10, « Utilisation des droits basés sur le rôle », page 261.

Pilote de service de boucle : faciliter le déplacement d'objets à l'aide du service déplacement de proxy.

Les pilotes DirXML peuvent synchroniser des objets qui sont répliqués sur le même serveur, dans une réplique principale ou en lecture/écriture. Un pilote peut déplacer des objets d'un conteneur dans un autre. Vous pouvez par exemple configurer un pilote pour placer les utilisateurs dans Novell® eDirectory™ en fonction de l'entreprise à laquelle ils sont assignés dans une application de gestion des ressources humaines. Lorsque l'entreprise d'un utilisateur est modifiée dans l'application de ressources humaines, le pilote peut déplacer l'objet utilisateur eDirectory dans le conteneur correspondant.

Si vous souhaitez qu'un pilote puisse déplacer des objets d'un conteneur dans un autre, vous devez effectuer l'une des opérations suivantes :

- Placez le pilote sur un serveur sur lequel se trouvent des répliques principales de tous les conteneurs source ou cible.
- Placez le pilote sur un serveur sur lequel se trouvent des répliques en écriture/lecture et configurer le service de déplacement de proxy sur les serveurs sur lesquels se trouvent les répliques principales pour faciliter le déplacement d'objets, puis configurez le pilote pour déléguer les déplacements au service de déplacement de proxy.

Le service de déplacement de proxy est une configuration particulière que vous pouvez exécuter avec le module d'interface de pilote de services en boucle. Cette section présente le service déplacement de proxy et explique comment le configurer ainsi que d'autres pilotes de systèmes connectés pour tirer parti de ce service.

Cette section contient les informations suivantes :

Présentation du service de déplacement de proxy

Avec Nsure™ Identity Manager et eDirectory, il est préférable de déplacer un objet sur la réplique principale, notamment si d'autres modifications sont apportées à l'objet en même temps.

Si vous souhaitez qu'un pilote puisse déplacer des objets d'un conteneur dans un autre, vous devez effectuer l'une des opérations suivantes :

- Placez le pilote sur un serveur sur lequel se trouvent des répliques principales de tous les conteneurs source ou cible.
- Placez le pilote sur un serveur sur lequel se trouvent des répliques en écriture/lecture et configurer le service de déplacement de proxy sur les serveurs sur lesquels se trouvent les répliques principales pour faciliter le déplacement d'objets, puis configurez le pilote pour déléguer les déplacements au service de déplacement de proxy.

Le service de déplacement de proxy est un objet Pilote avec une configuration spéciale que vous exécutez sur le serveur avec la réplique principale. Le service de déplacement de proxy sert à déplacer des objets pour le compte des pilotes DirXML exécutés sur des serveurs sur lesquels se trouvent des répliques en écriture/lecture. La délégation du déplacement permet de répliquer les modifications d'objets effectuées par le pilote qui délègue sur le serveur principal avant que le déplacement ne soit effectué.

Les étapes suivantes se produisent lorsqu'un déplacement est délégué d'un pilote au service de déplacement de proxy :

1. Un pilote délègue le déplacement en définissant une valeur pour l'attribut moveProxyTrigger de l'objet qui doit être déplacé. Le pilote définit l'attribut moveProxyTrigger pour qu'il ait la valeur du DN du conteneur cible dans lequel l'objet doit être déplacé.
2. Le service de déplacement de proxy surveille les événements d'ajout de valeurs pour repérer l'attribut moveProxyTrigger et convertit les événements en commandes personnalisées qui spécifient le DN source de l'objet à déplacer et le DN du conteneur cible.

   La commande personnalisée est créée par la règle de transformation de l'événement du canal Abonné du pilote du service de déplacement de proxy.
3. Le pilote du service de déplacement de proxy lance le déplacement en lui-même de l'objet sur son canal Éditeur. Le pilote du service de déplacement de proxy supprime ensuite la valeur du DN cible de l'attribut moveProxyTrigger de l'objet.

   Si le déplacement échoue avec un état réessayer (généralement parce le déplacement précédent du même objet n'est pas encore terminé), l'état est renvoyé à Identity Manager via le canal Abonné. Identity Manager soumet à nouveau l'événement d'origine toutes les 30 secondes ou jusqu'à la réussite ou l'échec du déplacement pour d'autres raisons.

Configuration du service de déplacement de proxy

Configurez le service de déplacement de proxy sur le serveur sur lequel se trouve la réplique principale. Pour savoir quand vous pouvez être amené à utiliser ce service, reportez-vous à la section « Présentation du service de déplacement de proxy », page 280.

Une fois cette procédure terminée, configurez les pilotes exécutés sur d'autres serveurs pour déléguer leurs déplacements au pilote de déplacement de proxy pour que les déplacements puissent être effectués sur la réplique principale.

1. Installez Identity Manager sur le serveur sur lequel se trouvent les répliques principales si ce n'est déjà fait.
2. Vérifiez que les fichiers suivants pour le service de déplacement de proxy ont été installés avec Identity Manager. Dans le cas contraire, récupérez-les dans votre distribution de produit ou sur le site Novell Support (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964749.htm).

   - loopback.jar

     Il s'agit du fichier du module d'interface pilote en boucle nécessaire pour exécuter le service de déplacement de proxy. Ce fichier de module d'interface pilote doit être placé dans le répertoire /lib du système d'exploitation correspondant.

   - moveproxy.xml

     Il s'agit du fichier de configuration du pilote. S'il ne se trouve pas à l'emplacement par défaut des autres fichiers de configuration, vous devez le rechercher lorsque vous créez l'objet Pilote à l'Étape 4.

   - moveproxy.xlf

     Ce fichier crée les invites que vous voyez lorsque vous importez le fichier de configuration du pilote moveproxy.xml.

   - mvproxy_client_publisher_command_transformation.xsl

     Ce fichier contient la feuille de style de transformation de commande que vous ajoutez à chaque pilote qui délègue des déplacements au service de déplacement de proxy, tel qu'expliqué à la section « Configuration d'autres pilotes pour déléguer des déplacements au service de déplacement de proxy », page 282.

3. Vérifiez que votre schéma eDirectory contient l'attribut nommé DirXML-moveProxyTrigger. Dans le cas contraire, développez le schéma eDirectory à l'aide du fichier mvproxy.sch et de l'utilitaire approprié en fonction de votre plate-forme (nwconfig sur NetWare, install.dlm sur Win32 et ndssch sur UNIX).

   Procurez-vous le fichier mvproxy.sch auprès du site Novell Support (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964749.htm).

   Remarque : si le schéma contient déjà l'attribut DirXML-moveProxyTrigger, la distribution de votre produit doit également contenir les fichiers énumérés à l'Étape 2. Si votre schéma ne contient pas l'attribut et si vous obtenez le fichier d'extension de schéma mvproxy.sch et les autres fichiers énumérés à l'Étape 2 auprès de Novell Support, n'oubliez pas que les fichiers de Novell Support utilisent un attribut nommé moveProxyTrigger et pas DirXML-moveProxyTrigger. La configuration est identique, mais le nom de l'attribut est légèrement différent.

4. Créez un nouvel objet Pilote DirXML pour le serveur qui contient la réplique principale, en important le fichier moveproxy.xml pour créer la configuration de pilote.

   Le moteur DirXML exécute cet objet Pilote à l'aide du module d'interface de pilote en boucle.

5 Modifiez les filtres Abonné et Éditeur de l'objet Pilote que vous venez de créer pour inclure les classes d'objets dont vous souhaitez déléguer les déplacements. Ajoutez ensuite l'attribut DirXML-moveProxyTrigger ou moveProxyTrigger au filtre pour chacune de ces classes.

   N'ajoutez aucun autre attribut aux classes dans les filtres.

6 Définissez l'option de démarrage du pilote souhaitée pour l'objet Pilote, puis démarrez le pilote.

   Une fois que le pilote est configuré et qu'il fonctionne correctement, l'option de démarrage du pilote préférable est Automatique.

7 Vérifiez que les pilotes d'autres serveurs sont configurés pour tirer parti du service de déplacement de proxy en les configurant en tant que clients du service de déplacement de proxy, tel qu'expliqué à la section « Configuration d'autres pilotes pour déléguer des déplacements au service de déplacement de proxy », page 282.

Configuration d'autres pilotes pour déléguer des déplacements au service de déplacement de proxy

Pour savoir quand vous pouvez être amené à utiliser ce service, reportez-vous à la section « Présentation du service de déplacement de proxy », page 280.

1 Vérifiez que vous avez terminé la section « Configuration du service de déplacement de proxy », page 281.

2 Créez un objet DirXML-Stylesheet dans l'objet DirXML-Publisher du pilote.

3 Vérifiez que le fichier nommé mvproxy_client_publisher_command_transformation.xsl a été installé avec Identity Manager.

   Cette feuille de style est l'un des fichiers de déplacement de proxy que vous avez vérifié à l'Étape 2, page 281. Si elle n'a pas été installée, récupérez-la dans votre distribution de produit ou auprès de Novell Support (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964749.htm).

4 Dans l'objet feuille de style que vous venez de créer, rendez-vous sur la page de propriétés Édition XML et collez le contenu du fichier nommé mvproxy_client_publisher_command_transformation.xsl.

5 Incluez la feuille de style dans la règle de transformation de commande en procédant à l'une des opérations suivantes :

   - Si l'objet DirXML-Publisher ne possède pas de règle de transformation de commande, faites de la nouvelle feuille de style la règle de transformation de commande.
   - Si l'objet DirXML-Publisher possède déjà une règle de transformation de commande, utilisez le chaînage de règles et définissez la transformation suivante de la règle de transformation de commande pour qu'elle devienne la nouvelle feuille de style.

6 Si une feuille de style utilisée dans le canal Abonné ou Éditeur génère et envoie des déplacements à eDirectory via srcCommandProcessor ou destCommandProcessor, modifiez ces feuilles de style pour envoyer un événement de modification semblable à celui généré par la règle de transformation de commande créée à l'Étape 5.

Pilote Manual Task Service (pilote Workflow Service Request)

Pour mieux représenter l'utilisation du pilote, le nom est modifié dans Identity Manager pour passer du pilote Workflow Request Service au pilote Manual Task Service.

Le pilote de Manual Task Service a été conçu pour notifier à un ou plusieurs utilisateurs la survenue d'un événement au niveau des données et la nécessité d'une opération de leur part, le cas échéant. Par exemple, 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 les données dans Novell eDirectory ou dans une application. Dans d'autres scénarios, il peut s'agir de signaler à un administrateur la création d'un objet Utilisateur ou la modification des données d'un objet par un utilisateur.

Pour configurer le pilote Manual Task Service, vous devez en général configurer deux sous-systèmes séparés mais liés : les modèles de courrier électronique et les règles du canal Abonné et les modèles serveur Web du canal Éditeur et ses règles.

En outre, vous devez configurer les paramètres du pilote, par exemple le nom du serveur SMTP et le numéro de port du serveur Web.

Pour plus d'informations, reportez-vous au *Manual Task Service Driver Implementation Guide (Guide d'implémentation du pilote Manual Task Service)* (http://www.novell.com/documentation/fr-fr/dirxmldrivers/index.html).

12 Disponibilité élevée

Vous pouvez utiliser Identity Manager avec un stockage partagé pour disposer d'une disponibilité élevée. Certaines étapes sont nécessaires pour utiliser eDirectory et Identity Manager dans un environnement en grappes.

Cette section contient les informations suivantes :

Configuration d'eDirectory et d'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 généralisées pour les 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 d'eDirectory et d'Identity Manager doivent se trouver sur le stockage partagé pour être disponibles pour le nœud 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 le stockage partagé de la grappe. Les données d'état d'Identity Manager se trouvent également dans /var/nds/dib. Chaque instance eDirectory sur les nœuds de grappe doit être configurée pour utiliser le magasin de données sur le stockage partagé. D'autres données de configuration eDirectory doivent également se trouver 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 nœuds 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 nœud de grappe. La fonctionnalité NICI cliente est ainsi disponible sur un nœud de grappe même lorsque le nœud 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 principes 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 données Identity Manager d'intérêt se trouvent avec les données eDirectory.

- Vous connaissez les procédures d'installation d'eDirectory et d'Identity Manager.

- Vous utilisez une grappe à deux nœuds.

  Une grappe à deux nœuds 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 nœuds.

Cette section contient les informations suivantes :

Installation d'eDirectory

Remarque : NICI est installé dans le cadre de l'installation d'eDirectory.

1. Installez eDirectory sur le nœud de grappe principal.
2. Configurez eDirectory sur le nœud de grappe principal. Créez une nouvelle arborescence sur le nœud 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 nœuds de grappe.
3. Installez la même version d'eDirectory sur le nœud de grappe secondaire. Ne configurez pas eDirectory sur le nœud de grappe secondaire.

   Le nœud secondaire ne possède pas d'arborescence séparée.

Installation d'Identity Manager

1. Installez Identity Manager 2.0.1 (DR1) ou une version ultérieure sur le nœud de grappe principal à l'aide de l'option Serveur DirXML.

   Le processus d'installation installe les fichiers DirXML et configure l'arborescence eDirectory pour une utilisation avec Identity Manager.

2 Installez la même version d'Identity Manager sur le nœud 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 DirXML.

L'utilisation du paramètre de grappe secondaire permet d'installer les fichiers DirXML mais ne tente pas de procéder à la moindre configuration eDirectory supplémentaire. Aucune configuration n'est nécessaire dans la mesure où le nœud secondaire ne possède pas d'arborescence séparée.

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 nœuds 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 nœud de grappe quand le nœud 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 nœud de grappe secondaire (par exemple, /var/novell/nici.sav).

2 Copiez le répertoire /var/novell/nici du nœud de grappe principal vers le nœud de grappe secondaire. Vous pouvez le faire en utilisant scp ou en créant un fichier tar du répertoire /var/novell/nici sur le nœud principal, en le transférant sur le nœud secondaire ou en supprimant l'extension .tar du répertoire sur le nœud secondaire.

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 stockés dans /var/nds et ses sous-répertoires. Le répertoire de configuration par défaut d'eDirectory est /etc. Vous devez appliquer 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 du principe que le stockage partagé est monté au niveau de /shared.

- « Sur le nœud principal », page 287
- « Sur le nœud secondaire », page 288

Sur le nœud principal

1 Copiez la sous-arborescence du répertoire /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
/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 actuelle 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 de /etc/nds.conf vers /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 démons à démarrer par le processus init lors de l'amorçage.

Sur le nœud secondaire

1 Renommez le répertoire /var/nds (par exemple, /var/nds.sav). Ce n'est pas strictement nécessaire, mais les sauvegardes représentent une manière de redémarrer à un point ultérieur à l'installation d'eDirectory.

2 Créez un lien symbolique de /var/nds vers /shared/var/nds

3 Faites une copie de sauvegarde de /etc/nds.conf.

4. Supprimez /etc/nds.conf.
5. Créez un lien symbolique de /etc/nds.conf vers /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 démons à démarrer par le processus init lors de l'amorçage.

Une fois les étapes pour les nœuds principal et secondaire terminées, démarrez les services de grappe. eDirectory et Identity Manager démarrent alors sur le nœud principal.

Considérations relatives au pilote DirXML

La plupart des pilotes DirXML 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 nœud de 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 d'eDirectory, elles doivent se trouver sur le stockage partagé ou être dupliquées sur chaque nœud de grappe. Exemple : les répertoires du modèle du pilote Manual Task.

Étude de cas pour SuSE Linux

Pour une description de l'exécution d'Identity Manager sur un stockage partagé avec SuSE LINUX Enterprise Server 8, reportez-vous au numéro TID NOVL97459 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/NOVL97459.htm).

13 Consignation et création de rapports avec Nsure Audit

Nsure™ Identity Manager a été conçu pour utiliser Novell® Nsure Audit pour la génération d'audits et de rapports.

Nsure Audit est un recueil de technologies fournissant des capacités de surveillance, de consignation, de création de rapport et de notification. Grâce à l'intégration avec Nsure Audit, Identity Manager fournit des informations détaillées sur l'état actuel et un historique 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 de l'activité d'Identity Manager à l'aide de Nsure Audit.

Les types de messages envoyés à Nsure 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.

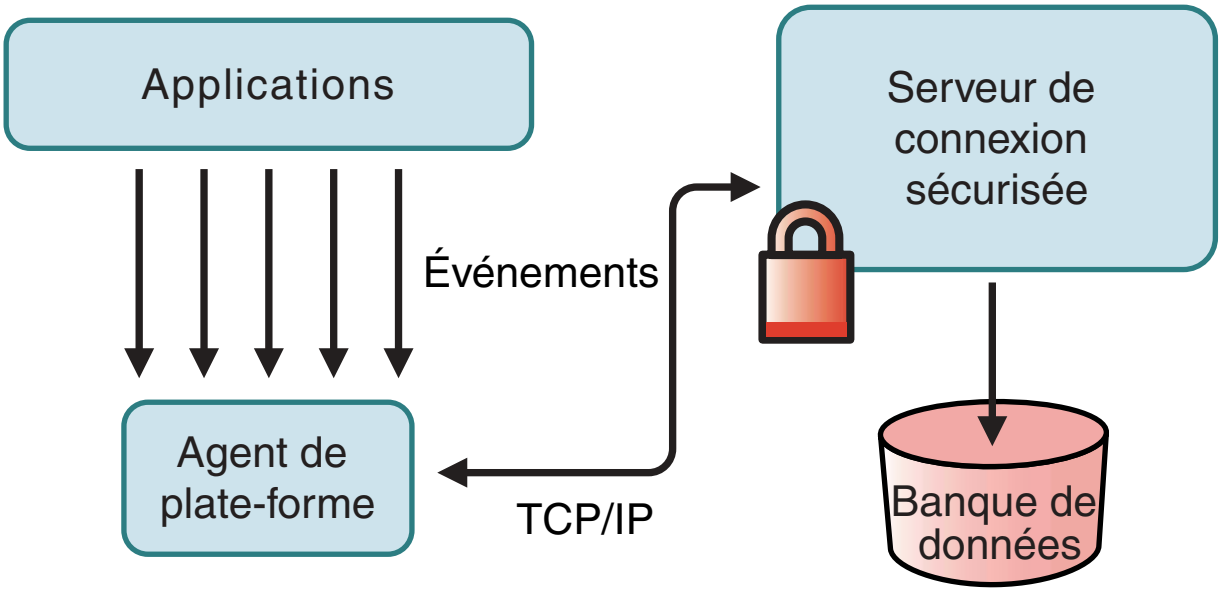
Service de création de rapport et de notification (RNS - Reporting and Notification Service)

Le service de création de rapport et de notification RNS est désapprouvé, mais le moteur continue à traiter les fonctions RNS si vous utilisez effectivement RNS. Envisagez de passer à Nsure Audit ; ce système étend en effet la fonctionnalité fournie par RNS. De plus, RNS pourrait ne plus être pris en charge dans une version future d'Identity Manager. Pour plus d'informations sur la documentation RNS, reportez-vous au *Guide d'administration de DirXML 1.1a* (http://www.novell.com/documentation/fr-fr/dirxml11a/dirxml/data/afae8bz.html).

Présentation

Nsure 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 Nsure Audit :



Sur cette illustration, Identity Manager est l'une des applications qui utilise l'agent de plate-forme pour envoyer des rapports sur les événements au serveur de consignation sécurisée Nsure Audit.

Configuration de Nsure Audit

Comme nous l'avons déjà vu dans la présentation, Nsure 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 d'Identity Manager et d'autres applications ; il est installé séparément d'Identity Manager en tant que constituant de Nsure Audit 1.0.2.

Configuration de l'agent de plate-forme

Pour installer l'agent de plate-forme, sélectionnez l'option Composants du système Novell NSure Audit pour DirXML pendant l'installation. Vous pouvez installer l'agent de plate-forme avec Identity Manager ou plus tard.

Remarque : si vous installez l'agent de plate-forme une fois le moteur DirXML® démarré, Identity Manager doit être redémarré avant que l'agent de plate-forme et Identity Manager ne soient liés. 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, effectuez les étapes suivantes pour configurer l'agent de plate-forme :

1. Ouvrez le fichier de configuration de Nsure Audit, logevent.cfg, dans un éditeur de texte. L'emplacement par défaut de ce fichier est :

Système d'exploitation	Chemin
NetWare®	sys:\etc\logevent.cfg
Windows	*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.

Configuration du serveur de consignation sécurisée

Remarque : le serveur de consignation sécurisée Nsure Audit n'est pas livré avec DirXML. Il fait en fait partie de Nsure Audit 1.0.2. Pour plus d'informations sur le téléchargement de Nsure Audit 1.0.2, reportez-vous à la page du produit Nsure 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.

Le serveur de consignation sécurisée peut consigner des événements vers les applications MySQL*, Oracle*, Microsoft* SQL Server, Java* et plusieurs autres emplacements, y compris un fichier plat. Nsure Audit contient une application personnalisée conçue pour interroger les bases de données et y rechercher des données d'événements, appelée Nsure Audit Report. 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 Nsure Audit 1.0.2. Vous pouvez également consulter les guides de démarrage rapide sur le Web, tout comme le manuel *Nsure Audit 1.0.2 Administration Guide (Guide d'administration de Nsure Audit 1.0.2)* sur le site Web de documentation de Novell Nsure Audit (http://www.novell.com/documentation/fr-fr/nsureaudit).

Configuration de la consignation

Identity Manager permet de configurer les événements consignés selon différents niveaux prédéfinis ou en sélectionnant individuellement chaque événement que vous souhaitez consigner. Les modifications des paramètres de configuration sont également consignées.

Les événements définis par l'utilisateur, présentés à la section « Événements définis par l'utilisateur », page 298, sont consignés à chaque fois que la consignation est activée ; ils ne sont jamais filtrés par le moteur DirXML.

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 « Objets eDirectory », page 300.

Par défaut, seuls les événements critiques et définis par l'utilisateur sont consignés.

Sélection des événements à consigner

Sur l'ensemble de pilotes :

1. Dans iManager, ouvrez le rôle Gestion du pilote DirXML, puis sélectionnez la tâche Présentation.
2. Cliquez sur le lien du nom de l'ensemble de pilotes. La fenêtre Modifier l'objet s'affiche.
3. Cliquez sur le lien du niveau de consignation sur l'onglet DirXML. Les options de consignation suivantes sont disponibles :

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.
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 sélectionner les erreurs et les avertissements si vous souhaitez continuer à les consigner. Pour une liste de tous les événements disponibles, reportez-vous à la section « Événements DirXML », page 296.
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.

Option	Description
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 d'informations, reportez-vous à la section « Affichage des journaux d'état », page 303.

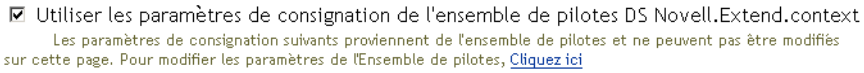
4 Une fois les événements que vous souhaitez consigner sélectionnés, cliquez sur OK.

Sur le pilote :

1 Dans iManager, ouvrez le rôle Gestion du pilote DirXML, puis sélectionnez la tâche Présentation.

2 Cliquez sur l'icône d'état du pilote, puis cliquez sur Éditer les propriétés.

3 Cliquez sur le lien du niveau de consignation sur l'onglet DirXML. Par défaut, le pilote est configuré pour hériter ses paramètres de consignation de son ensemble de pilotes. Pour sélectionner les événements consignés uniquement pour ce pilote, désélectionnez les éléments suivants :



4 Les options de consignation suivantes sont disponibles :

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.
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 sélectionner les erreurs et les avertissements si vous souhaitez continuer à les consigner. Pour une liste de tous les événements disponibles, reportez-vous à la section « Événements DirXML », page 296.

Option	Description
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.
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 d'informations, reportez-vous à la section « Affichage des journaux d'état », page 303.

5 Une fois les événements que vous souhaitez consigner sélectionnés, cliquez sur OK.

Événements DirXML

Vous trouverez une liste de tous les événements consignés par DirXML dans un fichier HTML séparé, DirXML Events (Événements DirXML) (dirxml_events.html).

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 :

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.
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 Nsure Audit fondées sur ces événements, reportez-vous à la section « Envoi de notifications fondées sur les événements », page 301.

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 :

Événement	Niveau de consignation	Informations
DirXML_Error	LOG_ERROR	Toutes les erreurs DirXML consignent cet événement. Le code d'erreur rencontré est enregistré dans l'événement. Pour consigner des 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 DirXML consignent cet événement. Le code d'avertissement rencontré est enregistré dans l'événement. 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 Nsure Audit fondées sur ces événements, reportez-vous à la section « Envoi de notifications fondées sur les événements », page 301.

Événements du chargeur distant

Les événements suivants sont consignés à partir du chargeur distant :

Événement	Niveau de consignation	Informations
Démarrage du chargeur distant	LOG_INFO	Toutes les erreurs DirXML consignent cet événement. Le code d'erreur rencontré est enregistré dans l'événement. Pour consigner des erreurs, sélectionnez Consigner les erreurs, Consigner les erreurs et les avertissements ou utilisez l'option Consigner des événements spécifiques et sélectionnez cet événement.
Arrêt du chargeur distant	LOG_INFO	Tous les avertissements DirXML consignent cet événement. Le code d'avertissement rencontré est enregistré dans l'événement. 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.

Événement	Niveau de consignation	Informations
Connexion au chargeur distant établie	LOG_INFO	Tous les avertissements DirXML consignent cet événement. Le code d'avertissement rencontré est enregistré dans l'événement. 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.
Connexion au chargeur distant perdue	LOG_INFO	Tous les avertissements DirXML consignent cet événement. Le code d'avertissement rencontré est enregistré dans l'événement. 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 Nsure Audit fondées sur ces événements, reportez-vous à la section « Envoi de notifications fondées sur les événements », page 301.

Événements définis par l'utilisateur

Identity Manager permet de configurer vos propres événements pour les consigner dans Nsure Audit. Vous pouvez consigner les événements à l'aide d'une opération dans le Générateur de règles 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 Nsure Audit, cet ID est combiné avec l'ID d'application DirXML 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 :

Niveau de consignation	Description
Urgence	Événements qui amènent le moteur ou le pilote DirXML à s'arrêter.
Alerte	Événements qui exigent une attention immédiate.
Critique	Événements qui peuvent entraîner un mauvais fonctionnement de parties du moteur ou du pilote DirXML.
Erreur	Événements décrivant des erreurs qui peuvent être gérées par le moteur ou le pilote DirXML.
Avertissement	Événements négatifs qui ne présentent pas de problème.

Niveau de consignation	Description
Remarque	Événements (positifs ou négatifs) qu'un administrateur peut utiliser pour comprendre ou améliorer l'utilisation et les opérations.
Informatif	Événements positifs, quelle que soit leur importance.
Débogage	Événements d'importance destinés au personnel d'assistance ou aux ingénieurs leur permettant de corriger le fonctionnement du pilote ou du moteur DirXML.

Génération d'événements avec le Générateur de règles

Dans le Générateur de règles, pour consigner des événements, sélectionnez l'opération Générer un événement.

1. Sélectionnez la condition à satisfaire avant la génération de l'événement, puis sélectionnez l'opération Générer un événement.
2. Spécifiez un IDd'événement.
3. Sélectionnez un niveaude consignation.
4. Cliquez sur l'icône en regard du champ Entrez 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 règles pour élaborer le reste de votre règle.

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 Nsure Audit avec un ID d'événement qui correspond à l'attribut de niveau du document d'état tel que spécifié dans le tableau suivant :

Niveau d'état	ID d'événement d'état
Réussi	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 un événement Nsure Audit 0x004 et value1=7777 avec un niveau de 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 un événement Nsure Audit 0x004 et value1=7778 avec un niveau de EV_LOG_STATUS_ERROR :

```
<xsl:message>
   <status level="error" text1="This would be text1" text2="This would be
text2" value="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>
```

Objets eDirectory

Cette section présente les détails des attributs Novell eDirectory™ qui stockent 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 d'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. Pour Identity Manager 2, 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.

Lancement de requêtes et création de rapports

Nsure Audit propose deux outils pour lancer des requêtes sur des événements dans la base de données Nsure Audit : le plug-in Nsure Audit iManager et Nsure Audit Report (LReport).

Le plug-in Nsure Audit iManager est une application de requête de base de données JDBC, basée sur le Web et qui permet de créer rapidement et de stocker des requêtes à l'aide de listes déroulantes et de macros.

Nsure Audit Report est une application compatible ODBC, basée sur Windows et qui peut utiliser les instructions de requête SQL ou les rapports Crystal Decision pour interroger des magasins de données Oracle et MySQL (ou toute autre base de données qui prend en charge les pilotes ODBC).

Suivez les instructions du manuel *Nsure Audit 1.0.2 Administration Guide (Guide d'administration de Nsure Audit 1.0.2)* pour accéder au plug-in Nsure Audit iManager ou pour configurer Nsure Audit Report. Il est disponible sur le site Web de documentation de Novell Nsure Audit (http://www.novell.com/documentation/fr-fr/nsureaudit).

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 d'Identity Manager.

Une fois Nsure Audit Report configuré, ces rapports ainsi que les requêtes et rapports personnalisés que vous avez définis peuvent être exécutés. Pour plus d'informations sur l'utilisation de ces rapports dans Nsure Audit Report, reportez-vous à la section Working with Reports in Nsure Audit Report (Utilisation des rapports dans Nsure Audit Report) (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/alsn2fj.html) dans le manuel *Nsure Audit 1.0.2 Administration Guide (Guide d'administration de Nsure Audit 1.0.2)*.

Affichage des événements Identity Manager

1. Dans l'espace de travail Nsure Audit Report, cliquez sur l'onglet Événements, puis développez le dossier DirXML. Cette liste contient tous les événements DirXML prédéfinis. Double-cliquez sur n'importe quel événement dans la liste pour afficher ses propriétés.
2. Pour lancer une requête pour rechercher un événement DirXML, 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 DirXML ont un ID d'événement compris entre 109608 et 262144.

Envoi de notifications fondées sur les événements

Nsure Audit permet d'envoyer une notification en cas de survenue ou non d'un événement spécifique. 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 de filtres et de notifications d'événements) du manuel *Nsure Audit 1.0.2 Administration Guide (Guide d'administration de Nsure Audit 1.0.2)* (http://www.novell.com/documentation/fr-fr/nsureaudit/nsureaudit/data/al0fr-fr08.html#al0lfr-fr8)

Utilisation des journaux d'état

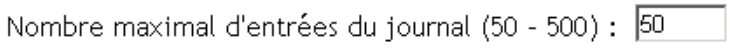
Outre les fonctionnalités de Nsure Audit, Identity Manager consigne un certain nombre d'événements sur l'objet ensemble de pilotes et l'objet Pilote. Ces journaux d'état proposent une vue de l'activité récente d'Identity Manager. Lorsque le journal atteint la taille définie, la moitié la plus ancienne 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 Nsure Audit ou le service de création de rapport et de notification RNS.

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 :

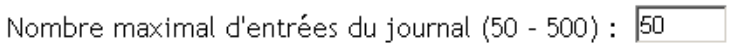
1. Dans iManager, ouvrez le rôle Gestion du pilote DirXML, puis sélectionnez la tâche Présentation.
2. Cliquez sur le lien du nom de l'ensemble de pilotes. La fenêtre Modifier l'objet s'affiche.
3. Cliquez sur le lien du niveau de consignation sur l'onglet DirXML. Spécifiez la taille maximale du journal dans le champ Nombre maximal d'entrées du journal :



4. Une fois le nombre maximal spécifié, cliquez sur OK.

Définition de la taille du journal sur le pilote :

1. Dans iManager, ouvrez le rôle Gestion du pilote DirXML, puis sélectionnez la tâche Présentation.
2. Cliquez sur l'icône d'état du pilote, puis cliquez sur Éditer les propriétés.
3. Cliquez sur le lien du niveau de consignation sur l'onglet DirXML. Spécifiez la taille maximale du journal dans le champ Nombre maximal d'entrées du journal :



4. Une fois le nombre maximal spécifié, cliquez sur OK.

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 pour les canaux Éditeur et Abonné contiennent les messages spécifiques de ces canaux générés par le pilote, tels qu’un veto sur une opération pour un objet non associé.

Le journal d’état pour l’ensemble de pilotes ne contient que les messages générés par le moteur, tels que les modifications d’état d’un pilote dans l’ensemble de pilotes. Tous les messages du moteur sont consignés.

A Activation des produits Novell Identity Manager

Les informations suivantes expliquent comment fonctionne l'activation pour les produits basés sur Novell® Nsure™ Identity Manager. L'édition Identity Manager Professional ou Server et les groupes de pilotes doivent être activés dans les 90 jours suivant l'installation, sinon ils s'arrêteront. Pendant cette période de 90 jours (ou ultérieurement), vous pouvez activer les produits Identity Manager.

Remarque : l'activation d'un pilote ne modifie pas votre configuration actuelle et n'installe pas une nouvelle version du module d'interface pilote. Le pilote passe simplement à un état activé.

Vous pouvez activer Identity Manager et les groupes de pilotes selon l'une des deux méthodes suivantes. La première méthode comprend les tâches suivantes :

- Achat d'une licence de produit Identity Manager
- Activation des produits Identity Manager à l'aide d'une référence générique
- Installation d'une référence d'activation de produit

La deuxième méthode comprend les tâches suivantes :

- Achat d'une licence de produit Identity Manager
- Création d'une requête d'activation de produit
- Soumission d'une requête d'activation de produit
- Installation d'une référence d'activation de produit

Cette section comprend également :

- « Affichage des activations de produit pour Identity Manager et les pilotes DirXML », page 312

Achat d'une licence de produit Identity Manager

Pour acheter une licence de produit Identity Manager, reportez-vous à la page Web Novell Nsure Identity Manager How to Buy (Instructions d'achat de Novell Nsure Identity Manager) (http://www.novell.com/products/nsureidentitymanager/howtobuy.html)

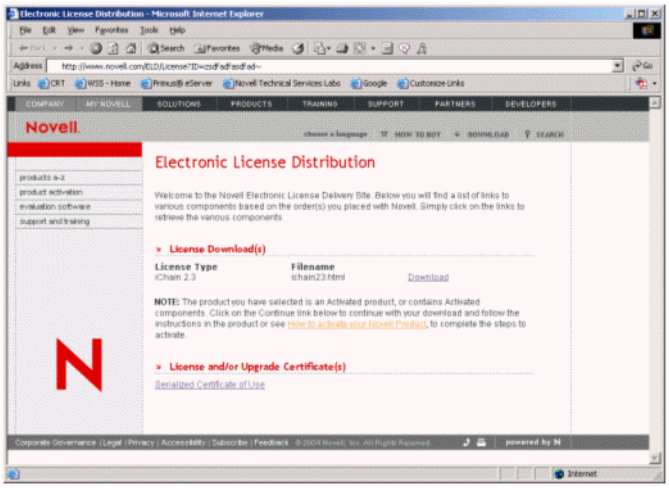
Une fois que vous avez acheté une licence, Novell vous envoie votre ID client par courrier électronique. Ce message contient également une URL vers le site Novell sur lequel vous pourrez obtenir une référence générique. Si vous oubliez votre ID client ou si vous ne le recevez pas, appelez le centre d'activation Novell (Novell Activation Center) au 1-800-418-8373 si vous résidez aux États-Unis. Pour tout autre pays, composez le 1-801-861-8373. (Les appels effectués avec l'indicatif 801 vous seront facturés.)

Activation des produits Identity Manager à l’aide d’une référence générique

1 Après avoir acheté une licence, vous recevrez un courrier électronique de Novell avec votre ID client. Ce message contient également, dans la section sur les détails de la commande, un lien vers le site sur lequel vous pouvez obtenir votre référence générique. Cliquez sur ce lien pour aller sur ce site.

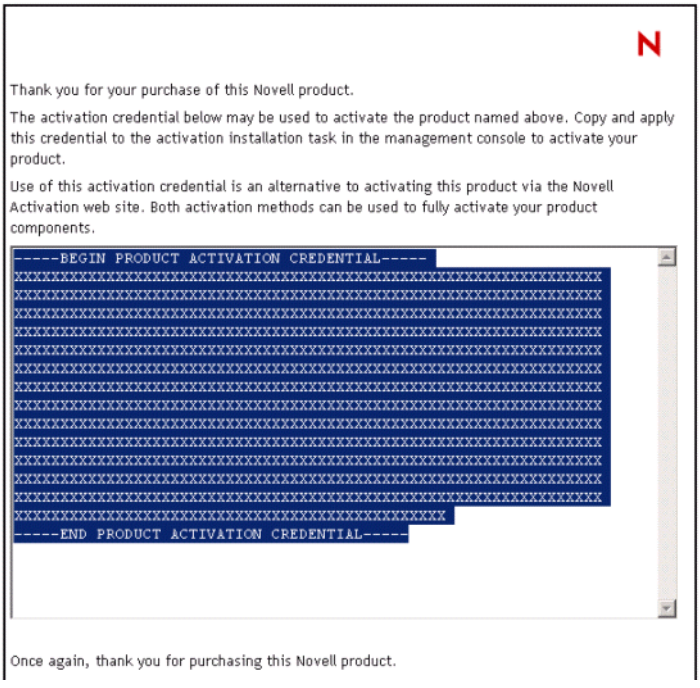
Important : vous ne pouvez utiliser que trois adresses électroniques différentes pour accéder au lien permettant d’obtenir cette référence générique. Si vous essayez d’accéder à ce lien avec plus de trois adresses électroniques, cela est considéré comme un risque en terme de sécurité et l’accès vous est refusé. En outre, seule l’adresse électronique désignée comme propriétaire/contrat pour l’ID client reçoit le message contenant la section Order Detail (Détail de la commande) avec les informations indiquant comment obtenir la licence générique. Si votre message de réponse ne contient pas de section sur les détails de la commande, vous devez contacter la personne responsable des ID client dans votre entreprise pour obtenir la référence générique.

Après avoir cliqué sur le lien, une page similaire à la capture ci-dessous doit s’afficher :



2 Cliquez sur le lien de téléchargement de la licence et enregistrez (téléchargez) ou ouvrez le fichier .html.

Une fois le fichier ouvert, son contenu doit être semblable au contenu figurant sur la capture suivante :



3 Pour plus d'informations sur la manière d'activer Identity Manager et les pilotes, reportez-vous à la section « Installation d'une référence d'activation de produit », page 310.

Création d'une requête d'activation de produit

Votre ID client permet de générer une requête d'activation de produit. Lorsque vous achetez votre produit Identity Manager, Novell envoie au contact principal de votre société (la personne qui a acheté la licence) un courrier électronique qui contient un ID client.

Si vous oubliez votre ID client ou si vous ne le recevez pas, appelez le centre d'activation Novell (Novell Activation Center) au 1-800-418-8373 si vous résidez aux États-Unis. Pour tout autre pays, composez le 1-801-861-8373. (Les appels effectués avec l'indicatif 801 vous seront facturés en tant qu'appels longue distance, le cas échéant).

Remarque : l'acheteur de la licence reçoit un message électronique contenant l'ID client. Si votre entreprise a géré cette transaction par l'intermédiaire de son acheteur, vous devrez peut-être le contacter pour obtenir votre ID client.

Avant de générer une requête d'activation de produit, créez un objet Ensemble de pilotes afin d'activer Identity Manager.

1 Lancez iManager en vous rendant à l'adresse suivante : http://*adresse_IP_du_serveur*/nps/iManager.html.

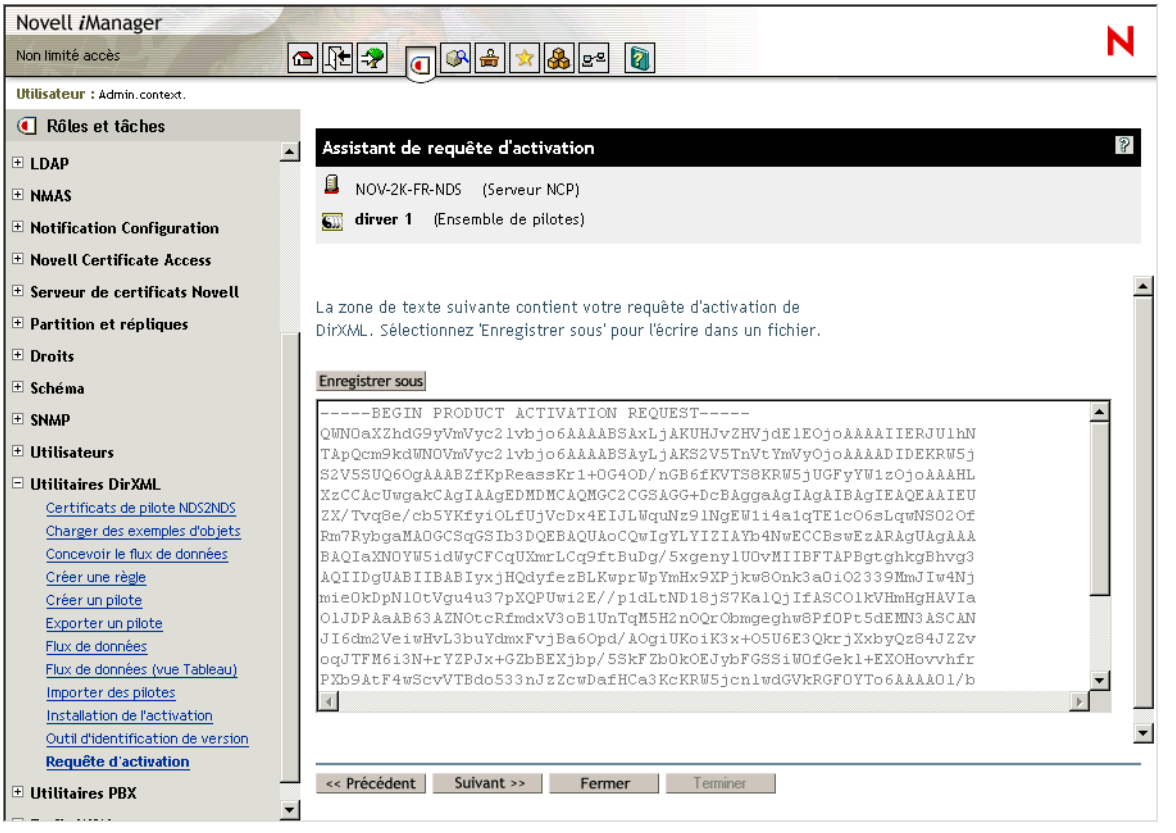
2 Cliquez sur Gestion DirXML > Requête d'activation.

3 Recherchez l'ensemble de pilotes que vous souhaitez activer, puis cliquez sur Suivant.

Remarque : si l'ensemble de pilotes n'est associé à aucun serveur ou s'il est associé à plusieurs serveurs, vous êtes invité à sélectionner le serveur auquel vous souhaitez l'associer.

4 Entrez votre ID client Novell, puis cliquez sur Suivant pour créer votre fichier de requête d'activation.

Votre ID client et des informations permettant d'identifier l'arborescence du serveur sont stockés dans la requête d'activation du produit.



5 Copiez la requête d'activation du produit, qui se trouve dans la zone de texte, dans le Presse-papiers ou enregistrez-la directement dans un fichier, puis cliquez sur Suivant.

Vous aurez besoin de ces informations plus tard sur le site Web d'activation des produits Novell.

Important : ne modifiez pas le contenu de la requête d'activation de produit.

6 Cliquez sur le lien pour accéder au site Web d'activation des produits Novell (http://www.novell.com/products/activation).

ou

Cliquez sur Terminer pour revenir au menu principal d'iManager.

Remarque : pour poursuivre le processus d'activation, vous devez soumettre cette demande d'activation de produit à Novell sur le site Web Product Activation (Clé d'activation des produits Novell) (http://www.novell.com/products/activation). Pour plus d'informations, reportez-vous à la section « Soumission d'une requête d'activation de produit », page 309.

Soumission d’une requête d’activation de produit

Une fois que vous avez créé une requête d’activation de produit, vous devez la soumettre à Novell sur le site Web Product Activation (Clé d’activation des produits Novell) (http://www.novell.com/products/activation). Novell vous envoie alors un message électronique qui contient la référence d’activation du produit. Utilisez cette référence pour activer la suite ou les groupes de pilotes.

1. Connectez-vous au site Web Product Activation (Clé d’activation des produits Novell) (http://www.novell.com/products/activation), puis cliquez sur le(s) produit(s) Identity Manager.
2. Parcourez les écrans d’introduction, puis, lorsque vous y êtes invité, connectez-vous à votre compte MyNovell.

   Vous devez disposer d’un compte MyNovell pour accéder au site Web Product Activation (Clé d’activation de produit). Si vous n’avez pas de compte, vous pouvez créer ce compte gratuit lors de votre visite sur le site Web Product Activation.
3. Cliquez sur Parcourir pour indiquer le chemin d’accès au fichier de requête d’activation de produit ou collez le texte de cette requête dans la zone de texte.

   Si vous avez copié la requête d’activation de produit sur une disquette, vérifiez que cette requête est également disponible sur l’ordinateur sur lequel vous travaillez.

   Important : ne modifiez pas le contenu de la requête d’activation de produit.
4. Cliquez sur Soumettre.

   Vos achats de produits prêts à être activés sont affichés.

5 Cochez le produit que vous activez.

Vous ne pouvez en activer qu'un à la fois. Cochez le produit que vous êtes en train d'activer. Si vous avez besoin d'activer l'un des autres produits de la liste et s'ils seront utilisés dans la même arborescence, soumettez à nouveau la requête d'activation de produit. S'ils sont utilisés dans une autre arborescence, vous devez créer une nouvelle requête d'activation de produit, puis soumettre cette requête pour obtenir une référence.

6 Cliquez sur Submit (Soumettre).

Novell génère une référence d'activation de produit en fonction de la requête d'activation que vous avez soumise puis vous transmet cette référence par courrier électronique. Une copie de la référence est également envoyée au contact principal.

Remarque : certaines sociétés limitent la liste des employés autorisés à recevoir des références. Il se peut que vous n'ayez pas les droits requis pour utiliser l'ID client. Dans ce cas, une fois que vous avez cliqué sur Submit (Soumettre), une notification est envoyée au contact principal. Le contact principal doit approuver le fait que vous utilisiez l'ID client avant que vous ne receviez la référence par courrier électronique.

Installation d'une référence d'activation de produit

Vous devez installer la référence d'activation de produit via iManager. Les procédures ci-après expliquent comment installer la référence d'activation de produit.

1 Ouvrez le message électronique de Novell qui contient la référence d'activation de produit.

2 Exécutez l'une des étapes suivantes :

- Enregistrez le fichier de référence d'activation de produit.

  ou

- Ouvrez le fichier de référence d'activation de produit, puis copiez son contenu dans le Presse-papiers.

  Important : ne modifiez pas le contenu de la référence d'activation de produit.

3 Ouvrez iManager.

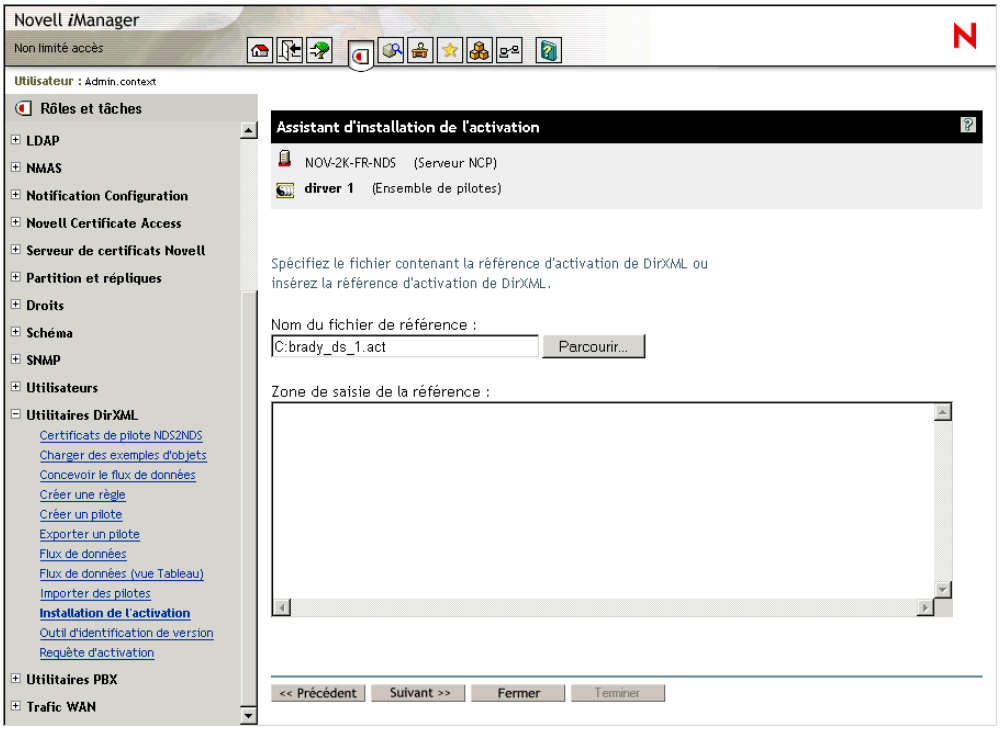
4 Sélectionnez Utilitaires DirXML > Installation de l'activation.

5 Sélectionnez l'ensemble de pilotes ou recherchez-en un dans l'arborescence, puis cliquez sur Suivant.

Important : vérifiez que vous avez choisi un ensemble de pilotes qui se trouve dans la même arborescence que celle dans laquelle la requête d'activation de produit a été créée au départ.

6 Si l'ensemble de pilotes n'est associé à aucun serveur ou s'il est associé à plusieurs serveurs, sélectionnez le serveur auquel vous souhaitez l'associer, puis cliquez sur Suivant.

La boîte de dialogue d'installation s'affiche :



7 Exécutez l'une des étapes suivantes :

- Précisez l'emplacement dans lequel vous avez enregistré la référence d'activation DirXML, puis cliquez sur Suivant.

  ou

- Collez le contenu de la référence d'activation DirXML dans la zone de texte, puis cliquez sur Suivant.

8 Cliquez sur Terminer.

Remarque : vous devrez activer chaque ensemble de pilotes qui contient un pilote. Vous pouvez utiliser la même référence d'activation de produit pour activer d'autres ensembles de pilotes dans la mesure où ces ensembles de pilotes sont dans la même arborescence. Vous ne pouvez utiliser une référence d'activation de produit que dans l'arborescence dans laquelle la requête d'activation de produit a été créée.

Affichage des activations de produit pour Identity Manager et les pilotes DirXML

Pour chacun de vos ensembles de pilotes, vous pouvez afficher les références d'activation de produit que vous avez installées pour le moteur et les pilotes DirXML. Pour afficher les références d'activation de produit, procédez comme suit :

1. Ouvrez iManager.
2. Cliquez sur Administration eDirectory > Modifier l'objet.
3. Dans le champ de nom d'objet, entrez l'ensemble de pilotes ou le pilote pour lequel vous souhaitez afficher les informations d'activation.

   ou

   Recherchez l'ensemble de pilotes ou le pilote pour lequel vous souhaitez afficher les informations d'activation.
4. Dans l'onglet DirXML, sélectionnez Activation.

   Les références d'activation de DirXML et du pilote DirXML apparaissent sur cette page.

   Vous pouvez afficher le texte de la référence d'activation ou, en cas d'erreur, supprimer une référence d'activation.

   Remarque : après l'installation d'une référence d'activation valide pour un ensemble de pilotes, il est possible que la mention Activation requise apparaisse encore en regard du nom du pilote. Dans ce cas, redémarrez le pilote et le message devrait disparaître.

B Prise en charge des fonctionnalités pour eDirectory 8.6.2 et eDirectory 8.7.3

Le tableau suivant répertorie les fonctionnalités non prises en charge par eDirectory 8.6.2 et signale également un certain nombre d'éléments particuliers relatifs à eDirectory 8.7.3.

Remarque : les NDS® hérités font référence aux versions antérieures à eDirectory 8.6.2. Le moteur DirXML livré avec Identity Manager ne peut être exécuté sur les NDS hérités.

Identity Manager n'a pas été testé avec eDirectory 8.7 ; il n'est donc pas pris en charge. Cependant, eDirectory 8.7.3 est pris en charge, et il s'agit d'une mise à niveau gratuite d'eDirectory 8.7.

Fonctionnalité	eDirectory 8.6.2	eDirectory 8.7.3
Générateur de règles	Pris en charge.	Pris en charge.
Script DirXML	Pris en charge.	Pris en charge.
Règles de mot de passe : règles de mot de passe avancées	Non prises en charge par Identity Manager sur eDirectory 8.6.2. En effet, les règles de mot de passe requièrent la fonctionnalité de mot de passe universel. Cependant, dans un environnement mixte, les règles de mot de passe avancées peuvent être appliquées pour une arborescence 8.6.2 si vous réalisez une synchronisation entre deux arborescences et si l'une d'elle est eDirectory 8.7.3. Par exemple, si vous avez un système de protection des identités exécutant 8.7.3 et si vous n'autorisez les utilisateurs qu'à modifier les mots de passe dans cette arborescence, vous pouvez activer le mot de passe universel dans le système de protection des identités, puis réaliser une synchronisation unidirectionnelle avec l'arborescence eDirectory 8.6.2. Vous pouvez synchroniser le mot de passe universel avec le mot de passe NDS et appliquer les règles de mot de passe. Si eDirectory 8.6.2 est utilisé, les restrictions de mot de passe que vous pouvez utiliser sont celles disponibles pour le mot de passe NDS.	Prises en charge si le mot de passe universel est activé dans une règle de mot de passe. Vous pouvez aussi appliquer des règles de mot de passe sur des systèmes connectés.

Fonctionnalité	eDirectory 8.6.2	eDirectory 8.7.3
Règles de mot de passe : libre-service pour les mots de passe oubliés	Toutes les fonctionnalités sont prises en charge à l'exception des suivantes : ◆ Autoriser l'utilisateur à réinitialiser le mot de passe ◆ Envoyer par messagerie électronique le mot de passe actuel à l'utilisateur Cette fonctionnalité requiert un mot de passe réversible. Comme eDirectory 8.6.2 ne prend pas en charge le mot de passe universel, cette fonctionnalité n'est pas disponible.	Toutes les fonctionnalités sont prises en charge si le mot de passe universel est activé pour la règle de mot de passe. Si le mot de passe universel est désactivé pour une règle de mot de passe, l'administrateur ne peut pas proposer les options suivantes aux utilisateurs de cette règle : ◆ Autoriser l'utilisateur à réinitialiser le mot de passe ◆ Envoyer par messagerie électronique le mot de passe actuel à l'utilisateur Ces fonctionnalités requièrent un mot de passe réversible. Elles ne peuvent donc pas être utilisées si le mot de passe universel n'est pas activé.
Règles de mot de passe : ensembles de stimulations	Prises en charge.	Prises en charge.
Règles de mot de passe : libre-service pour la réinitialisation des mots de passe	Prises en charge. Le gadget de réinitialisation des mots de passe modifie le mot de passe NDS si le mot de passe universel n'est pas disponible pour être utilisé sur eDirectory 8.6.2.	Prises en charge. Le gadget de réinitialisation des mots de passe modifie le mot de passe NDS si le mot de passe n'est pas disponible pour être utilisé même si le mot de passe universel n'est pas activé dans la règle de mot de passe d'un utilisateur.
Règles de mot de passe : tâche Définir le mot de passe universel	Non prises en charge pour la modification du mot de passe NDS. Utilisez la tâche Modifier l'objet ou d'autres tâches du service d'assistance pour modifier le mot de passe NDS de l'utilisateur.	Prises en charge si le mot de passe universel est activé. À l'inverse du gadget de réinitialisation des mots de passe, la tâche Définir le mot de passe universel ne fonctionne que si le mot de passe universel est activé dans la règle de mot de passe de l'utilisateur.
Synchronisation des mots de passe	Seule la publication des mots de passe vers Identity Manager est prise en charge. Avec 8.6.2, vous pouvez configurer vos pilotes pour qu'ils reproduisent la même fonctionnalité que celle fournie avec la version 1.0 de la synchronisation des mots de passe, avec en plus une prise en charge des nouvelles plates-formes. Identity Manager peut accepter des mots de passe de systèmes connectés pour mettre à jour le mot de passe NDS. Mais, sans mot de passe universel, Identity Manager ne peut pas distribuer de mots de passe aux systèmes connectés, à moins que le système en question ne soit une autre arborescence eDirectory.	Prise en charge. Cependant, si le mot de passe universel n'est pas activé dans une règle de mot de passe, les mots de passe ne peuvent pas être distribués aux systèmes connectés et les règles de mot de passe peuvent être appliquées sur les mots de passe entrants mais ne peuvent pas l'être sur les systèmes connectés.

Fonctionnalité	eDirectory 8.6.2	eDirectory 8.7.3
Droits basés sur le rôle	Non pris en charge. Les règles de droits sont des groupes dynamiques et certaines fonctionnalités des groupes dynamiques n'étaient pas prises en charge dans eDirectory 8.6.2.	Pris en charge.
Création de rapport et de notification	Prend en charge Novell Nsure Audit. Pour les clients réalisant une mise à niveau uniquement. Prend également en charge RNS, le service de création de rapport et de notification hérité. Les plugs-in RNS sont inclus dans Identity Manager ; les composants RNS du moteur DirXML ne le sont pas.	Prend en charge Novell Nsure Audit. Pour les clients réalisant une mise à niveau uniquement. Prend également en charge RNS, le service de création de rapport et de notification hérité. Les plugs-in RNS sont inclus dans Identity Manager ; les composants RNS du moteur DirXML ne le sont pas.
eGuide	Pris en charge.	Pris en charge.

C Mises à jour

Mars 2004

- Les sections suivantes ont été ajoutées :
  - « Utilisation de l'utilitaire de ligne de commande DirXML », page 84.
  - « Utilisation de mots de passe nommés », page 90.
  - « Valeurs de configuration globales », page 18 et « Pulsation pilote », page 18 dans la section sur les nouvelles fonctionnalités.
- Les références à la version 2.0 de la synchronisation des mots de passe ont été remplacées par la synchronisation des mots de passe sous Identity Manager, pour indiquer que la nouvelle fonctionnalité de synchronisation des mots de passe ne constitue pas un produit distinct mais fait bien partie d'Identity Manager.
- Les références à DirXML® 2.0 ont été remplacées par celles à Nsure™ Identity Manager 2. Le moteur et les pilotes sont encore désignés par moteur DirXML et pilotes DirXML.

1er avril 2004

- Les informations sur le libre-service de mots de passe ont été placées dans un chapitre séparé pour qu'elles soient plus facilement localisables. À présent, les informations sur les règles de mot de passe NMAS™ se trouvent dans deux chapitres :
  - Chapitre 7, « Gestion des mots de passe à l'aide des règles de mot de passe », page 101
  - Chapitre 8, « Mot de passe en livre service », page 125

13 avril 2004

Quelques modifications mineures ont été apportées au texte.

30 juin 2004

Des modifications destinées à mettre à jour le guide d'Identity Manager 2.0.1 ont été effectuées.

- Les sections suivantes ont été ajoutées :
  - « Chargeurs distants », page 57
  - « Présentation des mots de passe », page 166
  - « Gestion des informations sensibles », page 184
  - Chapitre 12, « Disponibilité élevée », page 285
  - « Ajout de votre propre message de modification du mot de passe aux règles de mot de passe », page 152
  - « Désactivation du mot de passe par suppression du gadget Indice », page 149
  - « Configuration des mots de passe nommés avec iManager », page 90
  - « Scénario 5 : synchronisation des mots de passe de l'application avec le mot de passe simple », page 234
  - « Indication des informations d'authentification SMTP dans les règles de pilote », page 246
- Dans la section sur la gestion des mots de passe, la section traitant de la vérification des règles de mot de passe pour Identity Manager a été supprimée. Il n'est plus nécessaire de créer manuellement une règle de mot de passe spécifique pour les ensembles de pilotes ; en effet, cette règle est désormais créée automatiquement.
- Les informations de la section « Intégration des options de mot de passe en libre-service avec Virtual Office », page 158 ont été déplacées dans le *Novell Virtual Office for NetWare 6.5 Configuration Guide (Guide de configuration de Novell Virtual Office pour NetWare 6.5)* (http://www.novell.com/documentation/nw65/virtualoffice/data/ac6spye.html).
- Des informations ont été ajoutées à la section « Planification des méthodes de login et de modification des mots de passe de vos utilisateurs », page 111, notamment sur la manière d'empêcher d'anciens clients de modifier le mot de passe NDS directement, à la section « Pour empêcher les clients hérités de modifier leur mot de passe », page 114.
- Des informations ont été ajoutées à la section « Localisation des modèles de notification par l'adresse de messagerie électronique », page 258.