Novell eDirectory™

8.8

www.novell.com

GUIDE D'ADMINISTRATION

15 septembre 2005

Novell®

Mentions légales

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

Guide d'administration de Novell eDirectory 8.8
15 septembre 2005

Documentation en ligne : pour consulter la documentation en ligne relative à ce produit et à d'autres produits Novell ou pour obtenir des mises à jour, visitez le site Web de documentation des produits Novell à l'adresse www.novell.com/documentation.

Marques commerciales de Novell

Client32 est une marque de Novell, Inc.
eDirectory est une marque de Novell, Inc.
NetWareest une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
NetWare Core Protocol et NCP sont des marques de Novell, Inc.
NMAS est une marque de Novell, Inc.
Novell est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
Novell Client est une marque de Novell, Inc.
Novell Directory Services et NDS sont des marques déposées de Novell, Inc. aux États-Unis et dans d'autres pays.
Ximiamest une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.
ZENworks est une marque déposée de Novell, Inc. aux États-Unis et dans d'autres pays.

Third-Party Materials

Toutes les marques commerciales de fabricants tiers appartiennent à leur propriétaire respectif.
Ce produit inclut des logiciels développés via OpenSSL Project destinés à être utilisés dans le toolkit OpenSSL (http://www.openssl.org).

Tables de matières

À propos de ce guide

Ce guide, destiné aux administrateurs réseau, contient les instructions relatives à la gestion et à la configuration de Novell® eDirectory™ 8.8. Il comprend les sections suivantes :

Documentation complémentaire

Pour connaître les instructions d'installation de eDirectory, consultez le manuel *Novell eDirectory 8.8 Installation Guide (Guide d'installation de Novell eDirectory 8.8)* (http://www.novell.com/documentation/edir88/index.html).

Pour obtenir la documentation relative à l'utilitaire de gestion eDirectory, consultez le manuel *Novell iManager 2.5 Administration Guide (Guide d'administration de Novell iManager 2.5)* (http://www.novell.com/documentation/imanager25/index.html).

Mises à jour de la documentation

Pour obtenir la dernière version de ce guide, consultez le manuel *Novell eDirectory 8.8 Administration Guide (Guide d'administration de Novell eDirectory 8.8)* (http://www.novell.com/documentation/edir88/index.html).

Conventions relatives à la documentation

Dans cette documentation, le signe « supérieur à » (>) est utilisé pour séparer les opérations d'une procédure et les éléments d'une référence ou d'un renvoi.

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

Lorsqu'un nom de chemin peut contenir une barre oblique inverse pour certaines plates-formes ou une barre oblique pour d'autres, il apparaît avec une barre oblique inverse. Les utilisateurs de plates-formes, comme Linux et UNIX*, qui nécessitent une barre oblique, doivent utiliser ce type de barre, comme l'exige votre logiciel.

1 Présentation de Novell eDirectory

Novell® eDirectory™ est un logiciel de services d'annuaire sécurisé, extrêmement évolutif et performant. Il peut stocker et gérer des millions d'objets, tels que des utilisateurs, des applications, des périphériques réseau et des données. Novell eDirectory est une solution de gestion d'identités multiplate-forme sécurisée et évolutive, qui autorise un déploiement sur Internet.

Offrant une gestion centralisée des identités, cette solution apporte l'infrastructure, la sécurité à l'échelle du réseau et l'évolutivité à tous les types d'applications qui tournent derrière un pare-feu ou au-delà de celui-ci. Novell eDirectory comprend des fonctions de gestion à partir du Web et de périphériques sans fil. Vous pouvez ainsi accéder à l'annuaire, aux utilisateurs, aux droits d'accès et aux ressources réseau, et les gérer à partir d'un navigateur Web et de divers périphériques de poche.

Novell eDirectory gère en mode natif la norme d'annuaire LDAP (Lightweight Directory Access Protocol) 3 et prend en charge les services TLS/SSL basés sur le code source OpenSSL.

Pour plus d'informations sur le moteur eDirectory, consultez le site Web eDirectory Process Requests (Requêtes de traitement eDirectory) (http://developer.novell.com/research/sections/netmanage/dirprimer/2002/august/p020801.htm).

Ce chapitre comprend les informations suivantes :

Novell eDirectory

Pour simplifier, Novell eDirectory est une liste d'objets qui représentent les ressources réseau, telles que les utilisateurs, les serveurs, les imprimantes, les files d'attente d'impression et les applications. La Figure 1 montre une partie des objets, tels qu'ils apparaissent dans l'utilitaire de gestion Novell iManager.

Figure 1 Objets eDirectory dans iManager

Il se peut que certaines classes d'objet ne soient pas disponibles, en fonction du schéma effectif configuré sur le serveureDirectory et du système d'exploitation exécutant eDirectory.

Pour plus d'informations sur les objets, reportez-vous à la section « Classes d'objet et propriétés », page 22.

Si le réseau compte plusieurs serveurseDirectory, l'annuaire peut être répliqué sur plusieurs serveurs.

Gestion simplifiée grâce à Novell iManager

Novell eDirectory autorise une gestion aisée, souple et efficace des ressources réseau. Il sert également de référentiel d'informations utilisateur pour les collecticiels et autres applications. Ces applications peuvent accéder à l'annuaire au moyen du protocole standard LDAP (Lightweight Directory Access Protocol).

Les fonctions eDirectory d'aide à la gestion comprennent une arborescence élaborée, un utilitaire de gestion intégré, ainsi qu'un système de login et d'authentification unique.

Novell iManager permet de gérer l'annuaire et les utilisateurs, ainsi que les droits d'accès et les ressources réseau qui figurent dans l'annuaire, depuis un navigateur Web et tout un éventail de périphériques de poche. Grâce aux plug-ins eDirectory pour iManager, vous accédez aux tâches élémentaires de gestion d'annuaire, ainsi qu'aux utilitaires de gestion eDirectory que vous deviez auparavant exécuter sur le serveur eDirectory, tels que DSRepair, DSMerge et l'utilitaire de sauvegarde et de restauration.

Pour plus d'informations, consultez le manuel *Novell iManager 2.5 Administration Guide (Guide d'administration de Novell iManager 2.5)* (http://www.novell.com/documentation/imanager25/index.html).

Arborescence élaborée

Novell eDirectory organise les objets dans une arborescence au sommet de laquelle se trouve l'objet Arborescence, qui porte le nom de cette arborescence.

Que les serveurs eDirectory exécutent NetWare, Linux, UNIX ou Windows, toutes les ressources peuvent être gérées dans la même arborescence. Vous n'avez pas besoin d'accéder à un serveur ou à un domaine spécifique pour créer des objets, octroyer des droits, modifier des mots de passe ou gérer des applications.

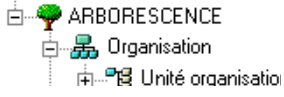
La structure hiérarchique de l'arborescence vous permet de bénéficier d'une grande souplesse et d'une grande efficacité en matière de gestion. Ces avantages résultent principalement des deux fonctionnalités suivantes :

- « Objets Conteneur », page 19
- « Héritage », page 20

Objets Conteneur

Les objets Conteneur permettent de gérer d'autres objets collectivement, plutôt qu'individuellement. Trois classes courantes sont disponibles pour les objets Conteneur, comme le montre la Figure 2 :

Figure 2 Classes courantes d'objets Conteneur



L'objet Arborescence est l'objet Conteneur situé au sommet de l'arborescence. Il contient en règle générale l'objet Organisation qui représente votre entreprise.

L'objet Organisation est en principe la première classe de conteneurs sous l'objet Arborescence. Il porte généralement le nom de votre entreprise. Les petites entreprises simplifient la gestion en plaçant tous les autres objets directement sous cet objet Organisation.

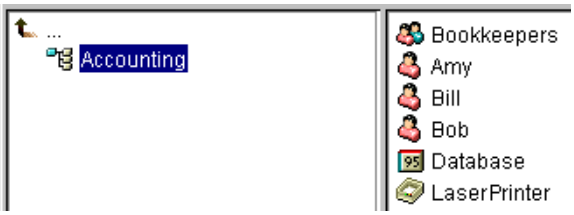
Des objets Unité organisationnelle peuvent toutefois être créés sous l'Organisation afin de représenter des régions géographiques, des complexes réseau ou des services. Vous pouvez également créer des objets Unité organisationnelle sous d'autres objets de ce même type pour subdiviser l'arborescence.

Pays et Lieu sont des classes d'objet Conteneur utilisées en principe uniquement dans les réseaux multinationaux.

L'objet Domaine peut être créé sous l'objet Arborescence ou sous les objets Organisation, Unité organisationnelle, Pays et Lieu.

Vous pouvez effectuer une tâche sur un objet Conteneur et l'appliquer ainsi à tous les objets qu'il contient. Supposons que vous souhaitiez donner à une utilisatrice nommée Annie le contrôle total de la gestion des objets inclus dans le conteneur Facturation (Reportez-vous à la section Figure 3.)

Figure 3 Objet Conteneur

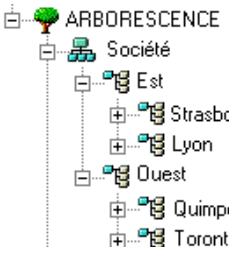


Pour ce faire, cliquez avec le bouton droit sur l'objet Facturation, sélectionnez Ayants droit de cet objet et ajoutez Annie comme ayant droit. Sélectionnez ensuite les droits à accorder à Annie, puis cliquez sur OK. Annie dispose désormais de droits de gestion sur l'application de base de données, le groupe Comptables, l'imprimante laser et les utilisateurs Annie, Bernard et Bruno.

Héritage

Une autre fonctionnalité particulièrement intéressante de eDirectory est l'héritage des droits. Le terme « héritage » signifie que les droits sont transmis à tous les conteneurs de l'arborescence en aval. Ainsi, vous pouvez accorder des droits en procédant à très peu d'assignations. Supposons, ar exemple, que vous souhaitiez accorder des droits de gestion sur les objets illustrés à la Figure 4, page 20.

Figure 4 Exemples d'objets eDirectory



Vous pouvez effectuer l'une des assignations suivantes :

- Si vous accordez à un utilisateur des droits sur Strasbourg, l'utilisateur peut uniquement gérer les objets du conteneur Strasbourg.
- Si vous accordez à un utilisateur des droits sur Est, cet utilisateur peut alors gérer les objets situés dans les conteneurs Est, Strasbourg et Metz.
- Si vous accordez à un utilisateur des droits sur VotreSociété, cet utilisateur peut gérer tous les objets qui figurent dans les conteneurs illustrés.

Pour plus d'informations sur l'assignation de droits, reportez-vous à la section « Droits eDirectory », page 58.

Utilitaire de gestion basé sur le Web

Novell iManager est un outil basé sur un navigateur qui permet d'administrer, de gérer et de configurer les objets eDirectory. Novell iManager vous donne la possibilité d'assigner des tâches ou des responsabilités particulières aux utilisateurs, et de leur présenter uniquement les outils (et les droits associés) qui leur sont nécessaires.

Pour exécuter iManager, vous devez utiliser un poste de travail sur lequel est installé l'un des navigateurs suivants : Internet Explorer 6.0 SP1 (navigateur recommandé), Mozilla 1.7, Mozilla Firefox 0.9.2 ou toute version ultérieure de ces produits.

IMPORTANT : même s'il est possible d'accéder au logiciel par le biais d'un autre navigateur Web que ceux mentionnés ci-dessus, nous ne garantissons pas une compatibilité intégrale avec iManager.

iManager permet d'effectuer les tâches de supervision suivantes :

- configurer les accès LDAP et XML à eDirectory ;
- créer des objets représentant des utilisateurs, des périphériques et des ressources au sein du réseau ;
- définir des modèles pour la création de comptes utilisateur ;
- rechercher, modifier, déplacer ou supprimer des objets réseau ;
- définir des droits et des rôles pour déléguer la responsabilité d'administration ;
- étendre le schéma eDirectory afin d'autoriser les propriétés et les types personnalisés pour les objets ;
- partitionner et répliquer la base de données eDirectory sur plusieurs serveurs ;
- exécuter des utilitaires de gestion eDirectory tels que DSRepair et DSMerge, ou encore l'utilitaire de sauvegarde et de restauration.

iManager permet en outre d'exécuter d'autres fonctions de gestion, selon les plug-ins qui ont été chargés. Les plug-ins eDirectory installés avec iManager 2.5 sont les suivants :

- Sauvegarde et restauration de eDirectory
- Fichiers journaux eDirectory
- Fusion de eDirectory
- Réparation de eDirectory
- Gestionnaire de services eDirectory
- Contenu de eGuide
- Contenu de base iManager
- Assistant Importation/Conversion/Exportation
- Gestion des index
- iPrint
- LDAP
- Application du mot de passe universel
- Synchronisation de priorité

- Attributs codés
- Réplication codée
- NLS
- NMAS
- PKI/Certificat
- Assistant de configuration de réplique filtrée
- SNMP
- Gestionnaire de trafic WAN

Pour plus d'informations sur l'installation, la configuration et l'exécution de iManager, consultez le manuel *Novell iManager 2.5 Administration Guide (Guide d'administration de Novell iManager 2.5)* (http://www.novell.com/documentation/imanager25/index.html).

Login et authentification uniques

Avec eDirectory, les utilisateurs se connectent à un annuaire global. Par conséquent, il est inutile de gérer plusieurs comptes de serveur ou de domaine pour chaque utilisateur. Il est également inutile de gérer les relations approuvées ou l'authentification directe entre domaines.

L'authentification des utilisateurs est une fonction de sécurité de l'annuaire. Pour qu'un utilisateur puisse se loguer, un objet Utilisateur doit être créé dans l'annuaire. L'objet Utilisateur possède certaines propriétés, telles qu'un nom et un mot de passe.

Lorsque l'utilisateur se logue, eDirectory compare son mot de passe à celui qui est enregistré dans l'annuaire pour cet utilisateur et, s'ils sont identiques, autorise l'accès.

Classes d'objet et propriétés

Chaque type d'objet eDirectory est défini par une classe d'objet. Par exemple, Utilisateur et Organisation sont des classes d'objet. Chaque classe d'objet possède certaines propriétés. Un objet Utilisateur, par exemple, possède un prénom, un nom et beaucoup d'autres propriétés.

Le schéma définit les classes et les propriétés des objets, ainsi que les règles d'endiguement (tel conteneur peut contenir tels objets). Un schéma de base est livré avec eDirectory. Vous pouvez l'étendre ; les applications que vous utilisez, également. Pour plus d'informations sur les schémas, reportez-vous à la section « Schéma », page 42.

Les objets Conteneur contiennent d'autres objets et sont utilisés pour diviser l'arborescence en branches, alors que les objets Feuille représentent les ressources réseau.

Liste des objets

Les tableaux suivants présentent les classes d'objet eDirectory. Des services supplémentaires permettent de créer dans eDirectory de nouvelles classes d'objets qui ne sont pas listées ci-dessous.

Classes d'objet Conteneur eDirectory

Icône dans iManager	Objet Conteneur (abréviation)	Description
	Arborescence	Représente le premier élément de votre arborescence. Pour plus d'informations, reportez-vous à la section « Arborescence », page 25.
	Pays (C)	Désigne les pays couverts par votre réseau et organise les autres objets Annuaire au sein de ces pays. Pour plus d'informations, reportez-vous à la section « Pays », page 28.
	Conteneur de licences (LC)	Créé automatiquement quand vous installez un certificat de licence ou quand vous créez un certificat avec compteur à l'aide de la technologie NLS (Novell Licensing Services). Lorsqu'une application utilisant les NLS est installée, elle ajoute un objet Conteneur de licences à l'arborescence et un objet Feuille Certificat de licence à ce conteneur.
	Organisation (O)	Vous permet d'organiser d'autres objets dans l'annuaire. L'objet Organisation est situé un niveau en dessous de l'objet Pays (si vous utilisez ce dernier). Pour plus d'informations, reportez-vous à la section « Organisation », page 26.
	Unité organisationnelle (OU)	Vous permet d'organiser d'autres objets dans l'annuaire. L'objet Unité organisationnelle (« Organizational Unit » en anglais) est situé un niveau en dessous de l'objet Organisation. Pour plus d'informations, reportez-vous à la section « Unité organisationnelle », page 27.
	Domaine (DC)	Vous permet d'organiser d'autres objets dans l'annuaire. L'objet Domaine peut être créé sous l'objet Arborescence ou sous les objets Organisation, Unité organisationnelle, Pays et Localité. Pour plus d'informations, reportez-vous à la section « Domaine », page 28.

Classes d'objet Feuille eDirectory

Icône dans iManager	Objet Feuille	Description
	Serveur AFP	Représente un serveur AppleTalk* Filing Protocol qui fonctionne comme un noeud sur votre réseau eDirectory. En général, il fait également office de routeur NetWarevers plusieurs ordinateurs Macintosh* et de serveur AppleTalk pour ces mêmes ordinateurs.
	Alias	Pointe vers l'emplacement réel d'un objet dans l'annuaire. Tout objet situé à un emplacement donné de l'annuaire peut également apparaître ailleurs dans l'annuaire par le biais d'un alias. Pour plus d'informations, reportez-vous à la section « Alias », page 36.
	Application	Représente une application réseau. Les objets Application simplifient les tâches administratives telles que l'assignation de droits, la personnalisation de scripts de login et le lancement d'applications.
	Ordinateur	Représente un ordinateur au sein du réseau.
	Assignation de répertoire	Fait référence à un répertoire du système de fichiers. Pour plus d'informations, reportez-vous à la section « Assignation de répertoire », page 37.
	Groupe	Permet d'attribuer un nom à une liste d'objets Utilisateur de l'annuaire. Vous pouvez assigner des droits au groupe, plutôt que de le faire pour chacun des utilisateurs qui le composent. Ces droits sont alors répercutés sur chaque utilisateur du groupe. Pour plus d'informations, reportez-vous à la section « Groupe », page 32.
	Certificat de licence	S'emploie avec la technologie NLSpour installer les certificats de licence du produit en tant qu'objets dans la base de données. Des objets Certificat de licence sont ajoutés au conteneur Produit sous licence lorsqu'une application reconnaissant la technologie NLS est installée.
	Rôle organisationnel	Définit un poste ou un rôle au sein d'une organisation.
	File d'attente d'impression	Représente une file d'attente d'impression du réseau.
	Serveur d'impression	Représente un serveur d'impression du réseau.

Icône dans iManager	Objet Feuille	Description
	Imprimante	Représente un périphérique d'impression du réseau.
	Profil	Représente un script de login utilisé par un groupe d'utilisateurs qui doivent partager les commandes d'un script de login commun. Les utilisateurs ne doivent pas nécessairement se trouver dans le même conteneur. Pour plus d'informations, reportez-vous à la section « Profil », page 38.
	Serveur	Représente un serveur exécutant un système d'exploitation. Pour plus d'informations, reportez-vous à la section « Serveur », page 29.
	Modèle	Représente les propriétés standard des objets Utilisateur qui peuvent être appliquées aux nouveaux objets Utilisateur.
	Inconnu	Représente un objet pour lequel iManager ne possède pas d'icône spécifique.
	Utilisateur	Représente les utilisateurs de votre réseau. Pour plus d'informations, reportez-vous à la section « Utilisateur », page 30.
	Volume	Représente un volume physique au sein du réseau. Pour plus d'informations, reportez-vous à la section « Volume », page 29.

Classes d'objet Conteneur

Arborescence

 Le conteneur Arborescence, anciennement appelé [Root] (Racine), est créé lorsque vous installez eDirectory pour la première fois sur un serveur de votre réseau. En tant que conteneur le plus élevé de l'arborescence, il contient en général des objets Organisation, Pays ou Alias.

Définition

L'objet Arborescence représente le sommet de votre arborescence.

Syntaxe

L'objet Arborescence est utilisé pour les assignations universelles de droits. Du fait de l'héritage, les assignations de droits que vous effectuez sur l'objet Arborescence (cible) sont appliquées à tous les objets de l'arborescence. Pour plus de détails, reportez-vous à la section « Droits eDirectory », page 58. Par défaut, l'ayant droit [Public] dispose du droit Parcourir et l'administrateur, du droit Superviseur, sur l'objet Arborescence.

Propriétés importantes

L'objet Arborescence possède une propriété Nom, qui correspond au nom d'arborescence que vous avez indiqué lors de l'installation du premier serveur. Le nom d'arborescence est indiqué dans la hiérarchie de iManager.

Organisation

 Un objet Conteneur Organisation est créé lorsque vous installez pour la première fois eDirectory sur un serveur de votre réseau. En tant que conteneur le plus élevé après l'objet Arborescence, il contient généralement des objets Unité organisationnelle et Feuille.

L'objet Utilisateur Admin est créé par défaut dans votre premier conteneur Organisation.

Définition

En principe, l'objet Organisation représente votre entreprise. Vous pouvez toutefois créer d'autres objets Organisation sous l'objet Arborescence. Cela se fait couramment pour les réseaux qui couvrent des zones géographiques distinctes, ou en cas de fusion d'entreprises avec des arborescences eDirectory distinctes.

Syntaxe

L'utilisation que vous faites des objets Organisation de votre arborescence dépend de la taille et de la structure de votre réseau. Si le réseau est petit, il est conseillé de stocker tous les objets Feuille sous un seul objet Organisation.

Pour les réseaux plus importants, vous pouvez créer des objets Unité organisationnelle sous l'objet Organisation afin de faciliter la recherche et la gestion des ressources. Par exemple, vous pouvez créer des objets Unité organisationnelle pour chacun des services ou chacune des divisions de votre entreprise.

Pour un réseau couvrant plusieurs sites, vous avez intérêt à créer, pour chacun d'eux, un objet Unité organisationnelle sous l'objet Organisation. Ainsi, si vous disposez (ou prévoyez de disposer) de suffisamment de serveurs pour effectuer la partition de l'annuaire, vous pouvez le faire de manière logique, en respectant les limites des sites.

Pour simplifier le partage des ressources de l'entreprise (telles que les imprimantes, les volumes ou les applications), créez les objets correspondants sous l'Organisation.

Propriétés importantes

Les propriétés les plus utiles pour l'objet Organisation sont indiquées ci-dessous. Seule la propriété Nom est obligatoire. Pour obtenir la liste complète des propriétés d'un objet Organisation, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur Aide.

- Nom

  Généralement, la propriété Nom correspond au nom de votre entreprise. Vous pouvez bien sûr raccourcir le nom pour plus de facilité. Par exemple, si votre entreprise s'appelle Chaussures et Compagnie, vous pouvez utiliser Chaussures

  Le nom de l'objet Organisation est intégré au contexte pour tous les objets qui lui sont subordonnés.

- Script de login

  La propriété Script de login contient les commandes exécutées par les objets Utilisateur situés immédiatement sous l'objet Organisation. Ces commandes sont exécutées lorsqu'un utilisateur se logue.

Unité organisationnelle


Vous pouvez créer des objets Unité organisationnelle (OU) pour subdiviser l'arborescence. Les unités organisationnelles sont créées à l'aide de iManager sous une organisation, un pays ou une autre unité organisationnelle.

Elles peuvent contenir d'autres unités organisationnelles, ainsi que des objets Feuille tels que des utilisateurs et des applications.

Définition

En principe, l'objet Unité organisationnelle représente un service qui englobe un groupe d'objets ayant besoin d'accéder les uns aux autres. L'exemple typique est un groupe d'objets Utilisateur, ainsi que les objets Imprimante, Volume et Application dont ces utilisateurs ont besoin.

Au niveau le plus élevé des objets Unité organisationnelle, chacun de ces objets peut représenter un site particulier du réseau (connecté aux autres sites par une liaison WAN).

Syntaxe

L'utilisation que vous faites des objets Unité organisationnelle de votre arborescence dépend de la taille et de la structure de votre réseau. Si celui-ci est petit, vous n'aurez sans doute pas besoin de créer des objets Unité organisationnelle.

Pour les réseaux plus importants, vous pouvez créer des objets Unité organisationnelle sous l'objet Organisation afin de faciliter la recherche et la gestion des ressources. Par exemple, vous pouvez créer des objets Unité organisationnelle pour chacun des services ou chacune des divisions de votre entreprise. N'oubliez pas que la méthode d'administration la plus simple consiste à réunir dans l'objet Unité organisationnelle les objets Utilisateur et les ressources qu'ils emploient le plus souvent.

Pour un réseau couvrant plusieurs sites, vous pouvez créer, pour chacun d'eux, un objet Unité organisationnelle sous l'objet Organisation. Ainsi, si vous disposez (ou prévoyez de disposer) de suffisamment de serveurs pour effectuer la partition de l'annuaire, vous pouvez le faire de manière logique, en respectant les limites des sites.

Propriétés importantes

Les propriétés les plus utiles pour l'objet Unité organisationnelle sont indiquées ci-dessous. Seule la propriété Nom est obligatoire. Pour obtenir la liste complète des propriétés d'un objet Unité organisationnelle, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur Aide.

- Nom

  Généralement, la propriété Nom correspond au nom du service (ou de la division). Vous pouvez bien sûr raccourcir le nom pour plus de facilité. Par exemple, si votre service s'appelle Comptabilité Fournisseurs, vous pouvez le raccourcir en entrant simplement CF.

  Le nom de l'objet Unité organisationnelle est intégré au contexte pour tous les objets qui lui sont subordonnés.

- Script de login

  La propriété Script de login contient les commandes exécutées par les objets Utilisateur situés immédiatement sous l'objet Unité organisationnelle. Ces commandes sont exécutées lorsqu'un utilisateur se logue.

Pays

 Vous pouvez créer des objets Pays directement sous l'objet Arborescence à l'aide de iManager. Les objets Pays sont facultatifs. Ils sont requis uniquement en cas de connexion à certains annuaires globaux X.500.

Définition

L'objet Pays représente l'identité politique de la branche correspondante de l'arborescence.

Syntaxe

Le plus souvent, les administrateurs ne créent pas d'objet Pays, même si le réseau couvre plusieurs pays. En effet, ce type d'objet ne fait qu'ajouter un niveau superflu à l'arborescence. Vous pouvez créer un ou plusieurs objets Pays sous l'objet Arborescence, en fonction de la nature multinationale de votre réseau. Les objets Pays ne peuvent contenir que des objets Organisation.

Si vous ne créez pas d'objet Pays et constatez par la suite que vous en avez besoin, vous pouvez alors en ajouter à l'arborescence.

Propriétés importantes

L'objet Pays possède une propriété Nom composée de deux lettres. Ce nom correspond à un code à deux lettres standard, comme par exemple US, UK ou FR.

Domaine

 Vous pouvez créer des objets Domaine directement sous l'objet Arborescence à l'aide de iManager. Vous pouvez également en créer sous des objets Organisation, Unité organisationnelle, Pays et Lieu.

Définition

L'objet Domaine représente des composants DNS. Les objets Domaine vous permettent d'utiliser l'emplacement DNS (Domain Name System Système de nom de domaine) des enregistrements de ressources de type service (services resource records SRV) afin de localiser des services dans votre arborescence.

À l'aide d'objets Domaine, une arborescence peut être structurée comme suit :

DS=Novell.DC=Provo.DC=USA

Dans cet exemple, tous les sous-conteneurs sont des domaines. Vous pouvez également utiliser des objets Domaine dans une arborescence mixte. Exemple :

DC=Novell.O=Provo.C=USA

Ou

OU=Novell.DC=Provo.C=USA

En règle générale, l'objet Domaine le plus élevé correspond à l'objet Arborescence global et contient tous les sous-domaines. Par exemple, ordinateur1.novell.com pourrait être représenté comme suit dans une arborescence : DC=ordinateur1.DC=novell.DC=com. Les domaines vous offrent un moyen plus générique d'élaborer une arborescence eDirectory. Si tous les conteneurs et sous-conteneurs sont des objets DC, les utilisateurs n'ont pas besoin de mémoriser les objets C, O ou OU lorsqu'ils recherchent des objets.

Syntaxe

Les arborescences NetWare 4 et 5 ne peuvent pas comporter d'objets Domaine à leur sommet. Sous NetWare 4 et 5, l'objet Serveur NCP peut être placé dans un conteneur Organisation, Pays, Unité organisationnelle ou Lieu, mais pas dans un conteneur Domaine. Par contre, NetWare 6 permet de placer des objets Domaine au sommet de l'arborescence et l'objet Serveur NCP, dans un conteneur Domaine.

Pour des installations plus anciennes de NetWare (telles que NetWare 4), lorsque vous préparez l'arborescence pour une installation ou une mise à niveau vers NetWare 5 (ou une version ultérieure), le fichier nds500.sch est lancé automatiquement. Après l'installation du premier serveur dans l'arborescence, ce fichier étend le schéma afin que le conteneur Domaine puisse être créé à n'importe quel endroit et qu'il puisse contenir la plupart des objets d'annuaire.

Classes d'objet Feuille

Serveur

 Un objet Serveur est automatiquement créé dans l'arborescence chaque fois que vous installez eDirectory sur un serveur. La classe d'objet peut correspondre à n'importe quel serveur exécutant eDirectory.

Vous pouvez également créer un objet Serveur pour représenter un serveur de Bindery NetWare 2 ou 3.

Définition

L'objet Serveur représente un serveur qui exécute eDirectory ou un serveur de Bindery (NetWare 2 ou 3).

Syntaxe

L'objet Serveur sert de point de référence pour les opérations de réplication. Un objet Serveur qui représente un serveur de Bindery vous permet de gérer les volumes du serveur à l'aide de iManager.

Propriétés importantes

L'objet Serveur possède, entre autres, une propriété Adresse réseau. Celle-ci indique le protocole et le numéro d'adresse du serveur. Ces informations sont utiles pour rechercher d'éventuels problèmes au niveau des paquets.

Pour obtenir la liste complète des propriétés d'un objet Serveur, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur Aide.

Volume

 Lorsque vous créez un volume physique sur un serveur, un objet Volume est automatiquement créé dans l'arborescence. Par défaut, le nom de l'objet Volume est le nom du serveur suivi d'un caractère de soulignement et du nom du volume physique (par exemple, VOTRESERVEUR_SYS).

Les objets Volume sont pris en charge sous NetWare uniquement. Les partitions d'un système de fichiers Linux ou UNIX ne peuvent pas être gérées à l'aide d'objets Volume.

Définition

Un objet Volume représente un volume physique d'un serveur, qu'il s'agisse d'un disque accessible en écriture, d'un CD ou d'un autre support de stockage. L'objet Volume de eDirectory ne contient pas d'informations sur les fichiers et répertoires du volume. Pour accéder à ces informations, utilisez iManager. Elles sont enregistrées dans le système de fichiers lui-même.

Syntaxe

Dans iManager, cliquez sur l'icône Volume pour gérer les fichiers et les répertoires du volume considéré. iManager fournit les informations relatives au volume, comme l'espace disque disponible, l'espace correspondant aux entrées de répertoire et les statistiques de compression.

Vous pouvez également créer des objets Volume dans l'arborescence pour les volumes NetWare 2 et 3.

Propriétés importantes

Outre les propriétés Nom et Serveur hôte, qui sont obligatoires, les objets Volume ont d'autres propriétés importantes.

- Nom

  Nom de l'objet Volume dans l'arborescence. Ce nom reprend par défaut le nom du volume physique. Vous pouvez toutefois le remplacer.

- Serveur hôte

  Serveur sur lequel réside le volume.

- Version

  Version NetWare ou eDirectory du serveur qui héberge le volume.

Utilisateur

Un objet Utilisateur est requis pour se loguer. Lorsque vous installez le premier serveur dans une arborescence, un objet Utilisateur appelé Admin est créé. Loguez-vous la première fois en tant qu'utilisateur Admin.

Pour créer ou importer des objets Utilisateur, vous pouvez appliquer les méthodes suivantes :

- iManager

  Pour plus d'informations sur iManager, consultez le manuel *Novell iManager 2.5 Administration Guide (Guide d'administration de Novell iManager 2.5)* (http://www.novell.com/documentation/imanager25/index.html).

- Fichiers de traitement par lots de la base de données

  Pour plus d'informations sur l'utilisation des fichiers de traitement par lots, reportez-vous à la section « Conception de l'arborescence eDirectory », page 72.

- Utilitaires de mise à niveau NetWare

  Pour plus d'informations sur les utilitaires de mise à niveau, notamment sur l'importation d'utilisateurs à partir de serveurs de Bindery existants, reportez-vous à la section « Conception de l'arborescence eDirectory », page 72.

Définition

Un objet Utilisateur représente une personne qui utilise le réseau.

Syntaxe

Nous vous conseillons de créer des objets Utilisateur pour toutes les personnes qui ont besoin d'utiliser le réseau. Bien que vous puissiez gérer les objets Utilisateur individuellement, il est plus rapide de procéder comme suit :

- Servez-vous d'objets Modèle afin de définir des propriétés par défaut pour la plupart des objets Utilisateur. L'objet Modèle est automatiquement appliqué aux objets Utilisateur que vous créez (mais non aux objets Utilisateur existants).
- Créez des objets Groupe pour gérer des ensembles d'utilisateurs.
- Assignez des droits en utilisant les objets Conteneur comme ayants droit si vous souhaitez que ces droits soient appliqués à tous les objets Utilisateur du conteneur.
- Sélectionnez plusieurs objets Utilisateur en maintenant la touche Maj ou Ctrl enfoncée tout en cliquant. Vous pouvez ainsi changer les propriétés en même temps pour tous les utilisateurs sélectionnés.

Propriétés importantes

Les objets Utilisateur possèdent plus de quatre-vingtspropriétés. Pour obtenir la liste complète des propriétés d'un objet Utilisateur, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur Aide.

Les propriétés Nom de login et Nom sont obligatoires. Ces propriétés, ainsi que d'autres très utiles, sont présentées ci-dessous.

- Date d'expiration du compte vous permet de limiter la durée de vie d'un compte utilisateur. Après la date d'expiration, le compte est verrouillé et l'utilisateur ne peut plus se loguer.
- Compte désactivé est une valeur générée par le système, qui indique que le compte est verrouillé. L'utilisateur ne peut donc plus se loguer. Le compte peut être verrouillé s'il a expiré ou si l'utilisateur a entré successivement trop de mots de passe incorrects.
- Changement périodique du mot de passe obligatoire vous permet de renforcer la sécurité en demandant à l'utilisateur de changer son mot de passe après un certain laps de temps.
- Adhésion aux groupes permet de lister tous les objets Groupe dont l'utilisateur est membre.
- Répertoire privé indique le chemin d'un système de fichiers et d'un volume NetWare pour les fichiers de l'utilisateur. La plupart des administrateurs créent ce type de répertoire pour que les fichiers de travail d'un utilisateur puissent être stockés sur le réseau.

  Le répertoire auquel cette propriété fait référence peut être créé automatiquement au moment de la création de l'objet Utilisateur.
- Dernier login est une propriété générée par le système, qui indique la date et l'heure auxquelles l'utilisateur s'est logué pour la dernière fois.
- Bien qu'elle soit obligatoire, la propriété Nom n'est pas utilisée directement par eDirectory. Les applications qui se servent de la base de noms eDirectory peuvent utiliser cette propriété, ainsi que d'autres propriétés d'identification, telles que Prénom, Titre, Emplacement et Numéro de télécopie.
- Limiter les connexions simultanées permet de définir le nombre maximal de sessions qu'un utilisateur peut ouvrir de façon simultanée sur le réseau.
- Nom de login est le nom indiqué par l'icône Utilisateur dans iManager. Il s'agit également du nom fourni par l'utilisateur lorsqu'il se logue.

  eDirectory ne requiert pas que les noms de login soient uniques sur tout le réseau ; ils doivent seulement l'être dans chacun des conteneurs. Vous pouvez malgré tout décider d'avoir des noms de login uniques dans toute l'entreprise, afin de simplifier l'administration.

En général, le nom de login est une combinaison du nom et du prénom de l'utilisateur. Par exemple, JEANT ou JTHOMAS pour Jean Thomas.

- Script de login vous permet de créer des commandes de login spécifiques à un objet Utilisateur. Quand un utilisateur se logue, le script de login du conteneur est exécuté en premier. Si l'objet Utilisateur a été ajouté à la liste des membres d'un objet Profil, le script de login du profil est ensuite exécuté. Ensuite, le script de login de l'utilisateur est exécuté (le cas échéant).

  Il est recommandé de placer la plupart des commandes de login dans des scripts de login de conteneur pour gagner du temps. Vous pouvez modifier le script de login de l'utilisateur pour gérer les exceptions aux besoins communs.
- Restrictions des heures de login vous permet de définir les heures et les jours de login autorisés pour l'utilisateur.
- Adresses réseau représente des valeurs générées par le système qui répertorient toutes les adresses IPX™ et/ou IP à partir desquelles l'utilisateur se logue. Ces valeurs sont utiles pour identifier les problèmes réseau au niveau des paquets.
- Exiger un mot de passe vous permet de déterminer si l'utilisateur doit fournir un mot de passe. D'autres propriétés liées à cette dernière permettent de définir des contraintes communes pour les mots de passe, notamment d'en limiter la longueur.
- Droits sur les fichiers et les répertoires indique toutes les assignations de droits effectuées pour cet utilisateur sur le système de fichiers NetWare. Vous pouvez également contrôler, à l'aide de iManager, les droits effectifs que possède un utilisateur sur des fichiers et des répertoires, y compris les droits hérités d'autres objets.

Groupe

 Vous pouvez créer des objets Groupe pour faciliter la gestion d'ensembles d'objets Utilisateur.

Définition

Un objet Groupe représente un ensemble d'objets Utilisateur.

Syntaxe

Les objets Conteneur permettent de gérer tous les objets Utilisateur du conteneur considéré, alors que les objets Groupe servent à gérer des sous-ensembles dans un ou plusieurs conteneurs.

Les objets Groupe sont utilisés principalement dans deux cas:

- Ils permettent d'allouer des droits à plusieurs objets Utilisateur en même temps.
- Ils permettent d'entrer des commandes de script de login à l'aide de la syntaxe `IF MEMBER OF`.

Groupes statiques

Les groupes statiques permettent d'identifier les objets membres de manière explicite. Chaque membre est assigné explicitement à un groupe.

Ces groupes fournissent une liste statique des membres et assurent l'intégrité référentielle entre la liste des membres du groupe et les membres des attributs d'un objet. L'adhésion au groupe est gérée explicitement au moyen de l'attribut member.

Groupes dynamiques

Les groupes dynamiques utilisent une URL LDAP pour définir un ensemble de règles qui, si elles sont satisfaites par des objets Utilisateur eDirectory, déterminent les membres du groupe. Les membres d'un groupe dynamique partagent un ensemble d'attributs communs, définis par le filtre de recherche spécifié dans l'URL. Pour plus d'informations sur le format d'URL LDAP, consultez le site Web RFC 2255 (http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2255.html).

Les groupes dynamiques vous permettent de définir les critères à utiliser lors de l'évaluation des adhésions à un groupe. Les membres du groupe sont évalués de manière dynamique par eDirectory, ce qui vous permet de les définir en termes de regroupement logique. eDirectory peut ainsi ajouter et supprimer automatiquement des membres d'un groupe. Cette solution, plus facilement adaptable, permet de réduire les coûts d'administration et peut compléter les groupes classiques dans LDAP pour offrir une flexibilité accrue.

eDirectory vous permet de créer un groupe dynamique lorsque vous souhaitez regrouper automatiquement des utilisateurs en fonction d'un attribut, ou lorsque vous souhaitez appliquer des listes de contrôle d'accès (Access Control Lists ACL) à des groupes spécifiques qui contiennent des noms distinctifs (Distinguished Name DN) correspondants. Vous pouvez, par exemple, créer un groupe qui inclut automatiquement tout DN possédant l'attribut Department=Marketing. Si vous appliquez un filtre de recherche pour Department=Marketing, la recherche renvoie un groupe comprenant l'ensemble des DN possédant l'attribut Department=Marketing. Vous pouvez ensuite définir un groupe dynamique à partir du résultat de la recherche obtenu au moyen de ce filtre. Tout objet Utilisateur ajouté à l'annuaire, qui satisfait au critère Department=Marketing est alors automatiquement ajouté au groupe. De la même façon, tout objet Utilisateur pour lequel la valeur de « Department » a été modifiée (ou tout objet Utilisateur supprimé de l'annuaire) est automatiquement supprimé du groupe.

Dans eDirectory, les groupes dynamiques sont créés par l'intermédiaire d'objets du type objectclass=dynamicGroup. Il est possible de convertir un groupe statique en groupe dynamique en associant une classe auxiliaire (dynamicGroupAux) à l'objet Groupe. L'attribut memberQueryURL est associé au groupe dynamique.

L'attribut dgIdentity pour l'objet Groupe dynamique peut prendre comme valeur le nom distinctif d'une entrée dont les références et les droits doivent être utilisés pour augmenter le nombre de membres dynamiques du groupe.

La gestion des groupes s'effectue au moyen de l'attribut memberQueryURL. Un attribut memberQueryURL type comporte un DN de base, une étendue, un filtre et une extension facultative. Le DN de base précise la base de recherche. L'étendue définit les niveaux sur lesquels doit porter la recherche sous la base. Le filtre permet de sélectionner des entrées spécifiques de l'étendue lors des recherches.

REMARQUE : afin de prendre en charge les exceptions à la liste créée par l'attribut memberQueryURL, les groupes dynamiques permettent aussi l'inclusion et l'exclusion explicite d'utilisateurs.

Les groupes dynamiques peuvent être créés et gérés via Novell iManager. Pour accéder aux tâches de gestion des groupes dynamiques, cliquez sur le rôle Groupes dynamiques dans la page Rôles et tâches.

Vous pouvez également utiliser des commandes LDAP pour gérer ces groupes. Les propriétés les plus utiles associées aux groupes dynamiques sont dgIdentity et memberQueryURL.

Propriétés importantes

Les propriétés les plus utiles de l'objet Groupe sont Membres et Droits sur les fichiers et les répertoires. Pour obtenir la liste complète des propriétés d'un objet Groupe, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur Aide.

- dgAllowDuplicates

  Indique si les doublons sont autorisés ou non lors de l'impression de membres de groupes dynamiques. La valeur par défaut est TRUE.

- dgIdentity

  Cette propriété indique le DN dont l'identité est utilisée par le groupe dynamique pour les authentifications au cours des recherches. L'identité doit figurer sur la même partition que le groupe dynamique. L'objet spécifié par dgldentity doit avoir les droits requis pour effectuer la recherche définie dans l'attribut memberQueryURL.

  Par exemple, si la valeur de memberQueryURL est

  ```
  "ldap:///o=nov??sub?(title=*)"
  ```

  gldentity doit avoir les droits de lecture/comparaison sur l'intitulé d'attribut figurant sous le conteneur o=nov.

- dgTimeout

  Cette propriété indique le délai maximal alloué à un serveur pour lire ou comparer un attribut member avant expiration. Lorsque ce délai est dépassé, l'erreur -6016 s'affiche.

- memberQueryURL

  Cette propriété définit l'ensemble des règles qui correspondent aux attributs des membres du groupe.

  memberQueryURL est un attribut à valeurs multiples, conformément à sa définition dans le schéma. Cependant, les serveurs eDirectory 8.6.1 n'utilisaient que la première valeur.

  Par exemple :

  Un administrateur crée un groupe dynamique possédant deux valeurs memberQueryURL :

  ```
  "ldap:///o=nov??sub?cn=*"
  ```

  ```
  "ldap:///o=org??sub?cn=*"
  ```

  Les serveurs eDirectory 8.6.

  x utilisent « ldap:///o=nov??sub?cn=* » pour déterminer les membres du groupe. Ils acceptent plusieurs requêtes, mais ne lisent que la première.

  Cette limitation n'existe plus depuis eDirectory 8.7.3. Les serveurs eDirectory 8.7.3 déterminent les membres en fonction de l'ensemble des valeurs memberQueryURL. Ainsi, l'ensemble de membres correspond à la synthèse des membres obtenus à partir de chacune des valeurs de memberQueryURL.

  Dans l'exemple ci-dessus, les membres résultants du groupe dynamique correspondent à l'ensemble des entrées sous o=org et o=nov, qui possèdent des valeurs cn.

- member

  Cette propriété liste tous les objets du groupe. Les droits assignés à l'objet Groupe s'appliquent à tous les membres du groupe correspondant. L'ajout de valeurs à la propriété member d'un groupe dynamique entraîne l'ajout des membres statiques à ce groupe. Cela peut servir à inclure certains membres.

- excludedMember

  Cette propriété indique les DN spécifiquement exclus de la liste d'adhésion à un groupe dynamique. Elle peut servir à constituer des listes d'exclusion pour les groupes dynamiques.

  excludedMember s'emploie pour interdire à des DN de devenir des membres dynamiques d'un groupe dynamique.

  Ainsi, un DN est un membre dynamique d'un groupe dynamique uniquement s'il a été sélectionné en fonction des critères définis par l'attribut memberQueryURL et s'il n'est pas spécifié dans excludedMember ou ajouté de manière explicite à uniqueMember ou member.

- staticMember

  Cette propriété lit les membres statiques d'un groupe dynamique et détermine si un DN est un membre statique d'un groupe dynamique. staticMember permet de rechercher les groupes dynamiques dans lesquels un DN est un membre statique unique, ainsi que ceux ne comprenant que des membres dynamiques (sans aucun membre statique).

  Pour l'ajouter aux groupes dynamiques existants, étendez le schéma à l'aide du fichier dgstatic.sch.

Mise à niveau de groupes dynamiques dans des bases de données antérieures à eDirectory 8.6.1

La mise en oeuvre de la fonctionnalité des groupes dynamiques fait appel à certaines valeurs stockées dans les objets Groupe dynamique, qui sont créées lorsqu'un groupe dynamique est créé localement ou reçu dans le cadre d'une synchronisation.

S'ils sont capables de contenir des groupes dynamiques, les serveurs plus anciens ne peuvent pas générer ces valeurs, puisque les groupes dynamiques ont été introduits avec eDirectory 8.6.1.

eDirectory 8.6.2 prévoit la mise à niveau automatique des objets Groupe dynamique d'une base de données antérieure à la version 8.6.1, afin que celle-ci corresponde à une base de données eDirectory 8.6.1.

Prise en charge d'autres syntaxes de memberQueryURL

L'attribut memberQueryURL peut contenir un filtre de recherche utilisé par le serveur eDirectory pour déterminer les membres d'un groupe dynamique.

Dans eDirectory 8.6.1, les syntaxes des attributs employés dans le filtre étaient limitées aux types de chaîne élémentaire suivants :

- SYN_CE_STRING
- SYN_CI_STRING
- SYN_PR_STRING
- SYN_NU_STRING
- SYN_CLASS_NAME
- SYN_TEL_NUMBER

- SYN_INTEGER
- SYN_COUNTER
- SYN_TIME
- SYN_INTERVAL
- SYN_BOOLEAN
- SYN_DIST_NAME
- SYN_PO_ADDRESS
- SYN_CI_LIST
- SYN_FAX_NUMBER
- SYN_EMAIL_ADDRESS

Depuis eDirectory 8.7.3, les syntaxes d'attributs ci-dessous sont également reconnues pour une valeur memberQueryURL :

- SYN_PATH
- SYN_TIMESTAMP
- SYN_TYPED_NAME

Dans eDirectory 8.6.1 comme dans eDirectory 8.7.x, les syntaxes binaires telles que SYN_OCTET_STRING et SYN_NET_ADDRESS ne sont pas admises dans les filtres de recherche memberQueryURL.

Pour plus d'informations, consultez le site Web How to Manage and Use Dynamic Groups in Novell eDirectory (Gestion et utilisation des groupes dynamiques dans Novell eDirectory) (http://developer.novell.com/research/appnotes/2002/april/05/a020405.htm).

Alias


Vous pouvez créer un objet Alias qui fait référence à un autre objet de l'arborescence. Un objet Alias offre à un utilisateur un nom local pour un objet qui se trouve à l'extérieur de son conteneur.

Lorsque vous renommez un conteneur, vous pouvez créer, à l'emplacement où il se trouvait, un objet Alias qui pointe vers le nouveau nom. Ainsi, les postes de travail et les commandes de script de login qui font référence à des objets du conteneur peuvent toujours accéder à ces objets, même si le nom du conteneur n'a pas été mis à jour.

Définition

Un objet Alias représente un conteneur, un utilisateur ou tout autre objet de l'arborescence. Il n'est pas doté de droits d'ayant droit qui lui sont propres. Tout droit d'ayant droit assigné à un objet Alias s'applique en réalité à l'objet qu'il représente. Cependant, l'objet Alias peut être la cible d'une assignation d'ayant droit.

Syntaxe

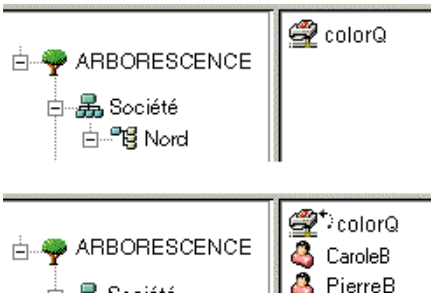
Vous pouvez créer un objet Alias pour faciliter la résolution d'un nom. Étant donné qu'il est plus simple d'attribuer un nom aux objets situés dans le contexte en cours, il est conseillé d'y créer des alias se rapportant aux ressources situées en dehors de ce contexte.

Supposons, par exemple, que des utilisateurs se loguent et établissent un contexte actuel dans le conteneur Sud (comme le montre la Figure 5), mais qu'ils ont besoin d'accéder à l'objet File d'attente d'impression QualCoul dans le conteneur Nord.

Figure 5 Exemples de conteneurs

Vous pouvez créer un objet Alias dans le conteneur Sud, comme l'illustre la Figure 6.

Figure 6 Objet Alias dans un conteneur eDirectory



L'objet Alias pointe vers l'objet QualCoul d'origine ; la configuration de l'impression pour les utilisateurs implique donc un objet local.

Propriétés importantes

Les objets Alias possèdent une propriété dénommée Objet en alias, qui associe l'objet Alias à l'objet d'origine.

Assignation de répertoire

L'objet Assignation de répertoire pointe vers un chemin du système de fichiers du serveur. Il permet de faire plus simplement référence aux répertoires.

Si votre réseau n'inclut aucun volume NetWare, vous ne pouvez pas créer d'objets Assignation de répertoire.

Définition

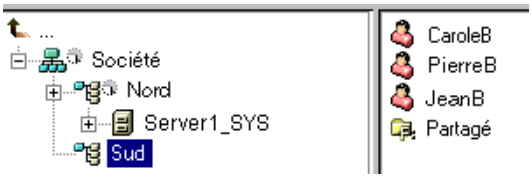
Un objet Assignation de répertoire correspond à un répertoire de volume NetWare (tandis qu'un objet Alias représente un objet).

Syntaxe

Vous pouvez créer un objet Assignation de répertoire pour faciliter l'assignation d'unités, en particulier dans les scripts de login. L'utilisation d'un objet de ce type vous permet de limiter à un simple nom les chemins de système de fichiers complexes.

En outre, quand vous déplacez un fichier, il est inutile de modifier les scripts de login et les fichiers de traitement par lots pour qu'ils indiquent le nouvel emplacement. Il vous suffit de modifier l'objet Assignation de répertoire. Supposons, par exemple, que vous soyez en train de modifier le script de login du conteneur Sud (voir Figure 7).

Figure 7 Exemple de conteneur eDirectory



Une commande qui associe des unités au répertoire Partagé sur le volume sys: se présente comme suit :

MAP N:=sys.North.:Partagé

Si vous avez créé l'objet Assignation de répertoire Partagé, la commande d'assignation est beaucoup plus simple :

MAP N:=Partagé

Propriétés importantes

L'objet Assignation de répertoire possède les propriétés suivantes :

- Nom

  Identifie l'objet dans l'annuaire (par exemple, Partagé). Le nom est également utilisé dans les commandes MAP.

- Volume

  Indique le nom de l'objet Volume désigné par l'objet Assignation de répertoire. Par exemple, Sys.Nord.VotreSociété.

- Chemin

  Désigne le répertoire par un chemin d'accès à partir de la racine du volume. Par exemple, public\winnt\nls\francais.

Profil

Les objets Profil vous aident à gérer les scripts de login.

Définition

Un objet Profil représente un script de login qui est exécuté après le script de login du conteneur et avant celui de l'utilisateur.

Syntaxe

Créez un objet Profil si vous souhaitez que les commandes de script de login ne soient exécutées que pour certains utilisateurs. Les objets Utilisateur peuvent se trouver dans le même conteneur ou dans des conteneurs différents. Une fois l'objet Profil créé, vous devez ajouter les commandes à sa propriété Script de login. Définissez ensuite les objets Utilisateur en ayants droit de cet objet Profil et ajoutez ce dernier à leur propriété Profil de membre de groupe.

Propriétés importantes

L'objet Profil possède deux propriétés importantes:

- Script de login

  Contient les commandes que vous souhaitez exécuter pour les utilisateurs du profil.

- Droits sur les fichiers et les répertoires

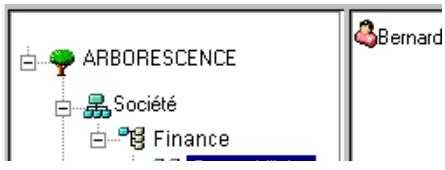
  Si le script de login contient des instructions de type INCLUDE, vous devez accorder à l'objet Profil des droits sur les fichiers inclus avec la propriété Droits sur les fichiers et les répertoires.

Contexte et dénomination

Le contexte d'un objet représente sa position dans l'arborescence. Il est pratiquement équivalent à un domaine DNS.

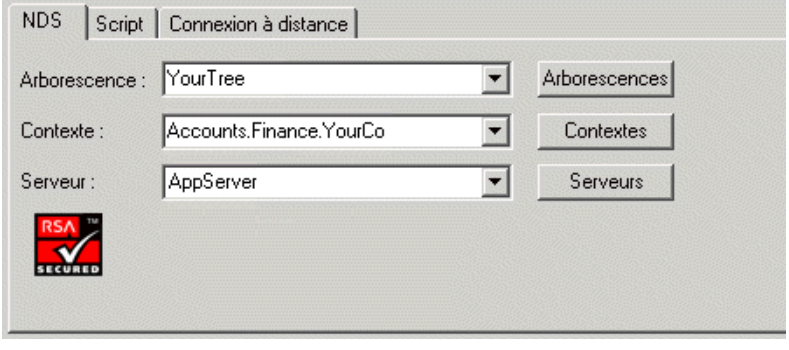
Vous pouvez observer dans la figure suivante que l'utilisateur nommé Bruno se trouve dans l'unité organisationnelle Comptabilité, elle-même dans l'unité organisationnelle Finances, laquelle se trouve dans l'organisation VotreSociété.

Figure 8 Exemple de conteneur eDirectory



Il est parfois nécessaire d'indiquer explicitement le contexte d'un objet dans un utilitaire eDirectory. Par exemple, si vous configurez le poste de travail de Bruno, vous pouvez être amené à indiquer un contexte de nom, comme le montre la Figure 9, page 39.

Figure 9 Page NDS du client Novell



Le contexte se présente sous la forme d'une liste de conteneurs séparés par des points, entre l'objet concerné et le sommet de l'arborescence. Dans l'exemple précédent, l'objet Utilisateur Bruno se trouve dans le conteneur Comptabilité, lui-même inclus dans le conteneur Finances, lequel se trouve à son tour dans le conteneur VotreSociété.

Nom distinctif

Le nom distinctif d'un objet est le nom de cet objet, suivi du contexte. Par exemple, le nom complet de l'objet Utilisateur Bruno est Bruno.Comptabilité.Finances.VotreSociété.

Nom avec type

Des noms avec type apparaissent parfois dans les utilitaires eDirectory. Ces noms comprennent les abréviations de type d'objet indiquées dans le tableau ci-dessous :

Classe d'objet	Type	Abréviation
Toutes les classes d'objet Feuille	Nom commun	CN
Organisation	Organisation	O
Unité organisationnelle	Unité organisationnelle	OU
Pays	Pays	C
Lieu	Lieu, département ou région	L ou S

Pour créer un nom avec type, eDirectory utilise l'abréviation du type, suivie du signe égal et du nom de l'objet. Par exemple, le nom partiel avec type de Bruno est le suivant : CN=Bruno. Le nom complet avec type de Bruno est le suivant : CN=Bruno.OU=Comptabilité.OU=Finances.O=VotreSociété. Vous pouvez utiliser des noms avec ou sans type dans les utilitaires eDirectory.

Résolution des noms

Le processus mis en oeuvre par eDirectory pour trouver l'emplacement d'un objet dans l'arborescence Annuaire est appelé *résolution de nom*. Lorsque vous utilisez des noms d'objet dans les utilitaires eDirectory, eDirectory résout les noms par rapport au contexte actuel ou au sommet de l'arborescence.

Contexte de poste de travail actuel

Un contexte est défini pour les postes de travail lorsque les logiciels de gestion de réseau sont exécutés. Ce contexte identifie de manière relative l'emplacement du poste de travail sur le réseau. Par exemple, le poste de travail de Bruno a le contexte actuel suivant :

Comptabilité.Finances.VotreSociété

Le contexte actuel permet de comprendre l'utilisation des points initiaux, des noms relatifs et des points finaux (voir sections suivantes).

Point initial

Utilisez un point initial pour résoudre le nom depuis le sommet de l'arborescence, indépendamment de l'endroit où le contexte actuel est défini. Dans l'exemple suivant, le point initial permet d'indiquer à l'utilitaire CX (utilitaire de changement de contexte) de résoudre le nom par rapport au sommet de l'arborescence.

CX .Finances.VotreSociété

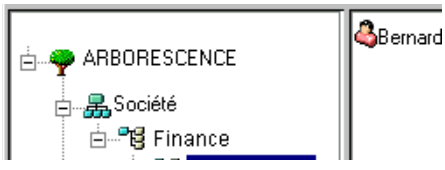
eDirectory interprète la commande de la manière suivante : « changer le contexte en utilisant le conteneur Finances, qui se trouve dans le conteneur VotreSociété, à partir du sommet de l'arborescence ».

Assignation d'un nom relatif

L'assignation d'un nom relatif implique que les noms sont résolus en fonction du contexte actuel du poste de travail, et non à partir du sommet de l'arborescence. Un nom relatif ne comprend jamais de point initial, puisqu'un tel point indique une résolution à partir du sommet de l'arborescence.

Supposons par exemple que le contexte actuel d'un poste de travail soit Finances (Reportez-vous à la section Figure 10.)

Figure 10 Exemple de conteneur eDirectory



Le nom relatif de l'objet Bruno est alors:

```
Bruno.Comptabilité
```

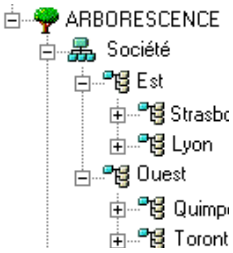
eDirectory interprète le nom de la manière suivante : « Bruno, qui se trouve dans Comptabilité, résolu à partir du contexte actuel qui est Finances ».

Points finaux

Les points finaux s'emploient uniquement pour les noms relatifs. Par conséquent, vous ne pouvez pas utiliser à la fois un point initial et un point final. Un point final change le conteneur à partir duquel eDirectory résout le nom.

Chaque point final déplace le point de résolution d'un conteneur vers le sommet de l'arborescence. Par exemple, supposons que vous vouliez déplacer le contexte actuel de votre poste de travail de Quimper à Strasbourg (voir Figure 11, page 42).

Figure 11 Exemple de conteneur eDirectory



La commande CX correspondante utilise la fonction d'assignation de nom relatif et des points finaux:

```
CX Strasbourg.Est..
```

eDirectory interprète cette commande de la manière suivante : «changer le contexte en utilisant Strasbourg, qui se trouve dans Est et qui est résolu à partir des deux conteneurs au-dessus du contexte actuel dans l'arborescence».

De même, si Bruno se trouve dans le conteneur Strasbourg et que le contexte actuel de votre poste de travail est Quimper, le nom relatif de Bruno est :

```
Bruno.Strasbourg.Est..
```

Contexte et dénomination sous Linux et UNIX

Lorsque des comptes utilisateur Linux et UNIX sont migrés vers eDirectory, le contexte eDirectory n'est pas utilisé pour nommer les utilisateurs.

Schéma

Le *schéma* définit les types d'objets (Utilisateur, Imprimante ou Groupe, par exemple) qui peuvent être créés dans l'arborescence, et indique quelles informations sont obligatoires ou facultatives lors de la création d'un objet. Chaque objet possède une classe de schéma définie pour le type d'objet correspondant.

Le schéma livré avec le produit s'appelle « schéma de base ». Une fois que le schéma de base a été modifié de quelque manière que ce soit (par exemple en lui ajoutant une nouvelle classe ou un nouvel attribut), il est considéré comme un schéma étendu.

Vous n'êtes pas tenu d'étendre le schéma, mais vous avez la possibilité de le faire. Le rôle Schéma de iManager vous permet d'étendre le schéma pour répondre aux besoins de votre organisation. Vous pouvez, par exemple, étendre le schéma si le personnel de votre organisation utilise des chaussures spéciales et si vous devez consigner les pointures des employés. Dans un tel cas, vous pouvez créer un attribut nommé Pointure de chaussure, puis l'ajouter à la classe Utilisateur.

Pour plus d'informations, reportez-vous à la section Chapitre 4, « Gestion du schéma », page 121.

Gestion du schéma

Le rôle Schéma de Novell iManager permet aux utilisateurs disposant de droits Superviseur sur une arborescence de personnaliser le schéma de cette arborescence. Le rôle Schéma et les tâches qui lui sont associées sont accessibles à partir de la page Rôles et tâches de iManager.

Le rôle Schéma permet :

- afficher une liste de l'ensemble des classes et attributs du schéma ;
- afficher les informations concernant un attribut, par exemple sa syntaxe et ses drapeaux ;
- étendre le schéma par l'ajout d'une classe ou d'un attribut ;
- créer une classe en lui attribuant un nom et en définissant des attributs, des drapeaux, des conteneurs auxquels elle peut être ajoutée, ainsi que des classes parentes dont elle peut hériter les attributs ;
- créer un attribut en lui assignant un nom et en spécifiant sa syntaxe et ses drapeaux ;
- ajouter un attribut facultatif à une classe existante ;
- supprimer une classe ou un attribut inutilisé ou obsolète.

Classes, attributs et syntaxes de schéma

Classes

Une classe correspond à un modèle d'objet d'annuaire. Un objet d'annuaire est une classe qui est complétée par des données. En d'autres termes :

CLASSE + DONNÉES = OBJET ANNUAIRE

Chaque classe possède un nom, une classe d'héritage (sauf si elle se trouve au sommet de la hiérarchie des classes), des drapeaux et un groupe d'attributs. Les classes sont nommées de la même façon que les objets d'annuaire (Utilisateur, Imprimante, File d'attente, Serveur, etc.), bien qu'elles ne soient que des structures vides.

Une classe d'héritage est une classe prise comme point de départ pour définir d'autres classes d'objet. Les classes situées en aval de celle-ci dans la hiérarchie héritent de tous les attributs de cette classe.

Une hiérarchie de classes indique la manière dont une classe est associée à ses classes parentes. C'est une façon d'associer des classes similaires et de permettre l'héritage d'attributs. Cela permet en outre de définir les types de conteneurs dans lesquels une classe est correcte.

Lorsque vous créez une classe, vous pouvez utiliser la hiérarchie de classes et les attributs supplémentaires disponibles pour personnaliser chaque classe. Vous pouvez indiquer une classe d'héritage (ce qui permet à la nouvelle classe d'hériter de tous les attributs et drapeaux de la classe supérieure dans la hiérarchie), puis personnaliser la nouvelle classe en sélectionnant un ou plusieurs attributs à ajouter aux attributs hérités. Les attributs supplémentaires peuvent être sélectionnés en tant qu'attributs obligatoires, de dénomination ou facultatifs.

Vous pouvez également modifier des classes existantes en leur ajoutant des attributs facultatifs.

Attributs

Les attributs sont les champs de données de la base de données eDirectory. Par exemple, si vous assimilez une classe à un formulaire, un attribut correspond à un champ de ce formulaire. Lorsqu'un attribut est créé, un nom (comme *nom de famille* ou *numéro d'employé*) et un type de syntaxe (par exemple *chaîne* ou *nombre*) lui sont associés. L'attribut est alors disponible dans les listes d'attributs du Gestionnaire de schéma.

Syntaxes

Vous pouvez choisir entre plusieurs options de syntaxe. Ces options permettent d'indiquer le type des données entrées pour chaque attribut. La syntaxe ne peut être spécifiée que lors de la création d'un attribut. Vous ne pouvez donc pas la modifier ultérieurement. Les syntaxes disponibles sont les suivantes :

- Lien en amont

  Syntaxe utilisée pour assurer le suivi des autres serveurs qui font référence à un objet. Ce lien est utilisé à des fins de gestion interne dans eDirectory.

- Booléen

  Syntaxe utilisée par les attributs dont les valeurs sont Vrai (chiffre1) ou Faux (chiffre0). Le drapeau à valeur unique est employé pour ce type de syntaxe.

- Chaîne avec distinction de la casse

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes Unicode différenciées selon la casse lors des opérations de comparaison. Deux chaînes avec distinction de la casse concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques, y compris pour la casse.

- Liste sans distinction de la casse

  Syntaxe utilisée par les attributs dont les valeurs sont des séquences ordonnées de chaînes Unicode non différenciées selon la casse lors des opérations de comparaison. Deux listes sans distinction de la casse concordent lorsqu'elles comptent toutes deux le même nombre de chaînes et que toutes les chaînes correspondantes concordent (c'est-à-dire qu'elles sont de la même longueur et que leurs caractères respectifs sont identiques).

- Chaîne sans distinction de la casse

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes Unicode non différenciées selon la casse lors des opérations de comparaison. Deux chaînes sans distinction de la casse concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques, exception faite de la casse.

- Nom de classe

  Syntaxe utilisée par les attributs dont les valeurs sont des noms de classe d'objet. Deux noms de classe concordent lorsqu'ils sont de la même longueur et que leurs caractères respectifs sont identiques, exception faite de la casse.

- Counter (Compteur)

  Syntaxe utilisée par les attributs dont les valeurs sont des entiers numériques signés, modifiés par incrémentation. Tout attribut défini à l'aide de Compteur est un attribut à valeur unique. Cette syntaxe se distingue de la syntaxe Nombre entier par le fait que les valeurs ajoutées à un attribut qui l'applique sont ajoutées au total de façon arithmétique, et que les valeurs supprimées sont soustraites de ce total de façon arithmétique également.

- Nom distinctif

  Syntaxe utilisée par les attributs dont les valeurs sont des noms d'objets de l'arborescence eDirectory. Les noms distinctifs (DN) ne sont pas différenciés selon la casse, même si l'un des attributs d'assignation de nom fait la distinction de la casse.

- Adresse électronique

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes d'informations binaires. eDirectory n'impose aucun critère quant à la structure interne de cette syntaxe.

- Numéro de télécopie

  Syntaxe spécifiant une chaîne conforme à la norme E.123 de stockage des numéros de téléphone internationaux, ainsi qu'une chaîne de bits facultative formatée selon la recommandation T.20. Les valeurs Numéro de télécopie concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques, exception faite des espaces et des traits d'union, qui sont ignorés lors des opérations de comparaison.

- En attente

  Syntaxe utilisée par les attributs correspondant à des quantités comptables et dont les valeurs sont des entiers signés. Cette syntaxe est une quantité comptable, à savoir un montant provisoirement mis en attente par rapport à la limite de crédit d'un objet, jusqu'à l'achèvement d'une transaction. Le montant en attente est traité comme dans le cas de la syntaxe Compteur: les nouvelles valeurs sont ajoutées ou soustraites du total de base. Lorsque le montant en attente évalué atteint la valeur zéro (0), l'enregistrement En attente est supprimé.

- Nombre entier

  Syntaxe utilisée par les attributs représentés sous forme de valeurs numériques signées. Deux valeurs Nombre entier concordent si elles sont identiques. La comparaison pour le classement fait appel aux règles applicables aux nombres entiers signés.

- Intervalle

  Syntaxe utilisée par les attributs dont les valeurs sont des entiers numériques signés, qui représentent des intervalles de temps. La syntaxe Intervalle utilise la même représentation que la syntaxe Nombre entier. La valeur Intervalle est le nombre de secondes dans un intervalle de temps.

- Adresse réseau

  Syntaxe qui représente une adresse de couche réseau dans l'environnement serveur. L'adresse est au format binaire. Deux adresses réseau concordent lorsque leur type, leur longueur et leur valeur sont identiques.

- Chaîne numérique

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes numériques, selon la définition de chaîne numérique X.208 du CCITT. Deux chaînes numériques concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques. Les chiffres (0 à 9) et le caractère d'espacement sont les seuls caractères valides dans une chaîne numérique.

- ACL des objets

  Syntaxe utilisée par les attributs dont les valeurs représentent des entrées de liste de contrôle d'accès (ACL). Une valeur ACL des objets peut protéger un objet ou un attribut.

- Liste d'octets

  Syntaxe décrivant une séquence ordonnée de chaînes d'informations binaires ou chaîne d'octets. Une liste d'octets concorde avec une liste stockée si elle est un sous-ensemble de cette dernière. Deux listes d'octets sont équivalentes si elles sont de même longueur et si leurs séquences de bits (octet) sont identiques.

- Chaîne d'octets

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes d'informations binaires qui ne sont pas interprétées par eDirectory. Ces chaînes d'octets sont des chaînes non Unicode. Deux chaînes d'octets concordent lorsqu'elles sont de la même longueur et que leurs séquences de bits (octet) sont identiques.

- Chemin

  Les attributs qui représentent un chemin d'accès à un système de fichiers contiennent toutes les informations nécessaires pour localiser un fichier sur un serveur. Deux chemins d'accès concordent lorsqu'ils sont de la même longueur et que leurs caractères respectifs sont identiques, casse incluse.

- Adresse postale

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes Unicode représentant des adresses postales. L'adresse postale est habituellement constituée d'attributs sélectionnés à partir de la spécification MHS version1, « Unformatted Postal O/R Address », conformément à la recommandationF.401. Elle doit compter au maximum 6lignes de 30caractères chacune, y compris un nom de pays. Deux adresses postales concordent lorsqu'elles comptent toutes deux le même nombre de chaînes et que celles-ci correspondent (c'est-à-dire qu'elles sont de la même longueur et que leurs caractères respectifs sont identiques).

- Chaîne imprimable

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes imprimables, selon la définition X.208 du CCITT. Le jeu de caractères imprimables inclut les éléments suivants :

  - Caractères alphabétiques majuscules et minuscules
  - Chiffres (0 à 9)
  - Caractère d'espacement
  - Apostrophe (')
  - Parenthèses gauche et droite ( )
  - Signe plus (+)
  - Virgule (,)
  - Trait d'union (-)
  - Point (.)
  - Barre oblique (/)
  - Deux-points (:)
  - Signe égal (=)
  - Point d'interrogation (?)

  Deux chaînes imprimables sont équivalentes lorsqu'elles ont la même longueur et que leurs caractères respectifs sont identiques. Les majuscules et les minuscules sont différenciées.

- Pointeur sur réplique

  Syntaxe utilisée par les attributs dont les valeurs représentent des répliques de partition. Une partition d'une arborescence eDirectory peut être répliquée sur différents serveurs. Cette syntaxe est constituée de six éléments :

  - Nom de serveur
  - Type de réplique (maîtresse, secondaire, lecture seule ou référence subordonnée)
  - Numéro de réplique
  - ID de racine de réplique
  - Numéro d'adresse
  - Enregistrement d'adresse

- Flux

  Syntaxe représentant des informations binaires arbitraires. La syntaxe Flux permet de créer un attribut eDirectory à partir d'un fichier situé sur un serveur de fichiers. Elle est utilisée par les scripts de login et d'autres attributs de flux. Les données enregistrées dans un fichier de flux ne respectent aucune syntaxe particulière. Il s'agit de données totalement arbitraires, définies par l'application qui les a créées et les utilise.

- Numéro de téléphone

  Syntaxe utilisée par les attributs dont les valeurs sont des numéros de téléphone. Les chaînes Numéro de téléphone doivent compter entre 1 et 32caractères. Deux numéros de téléphone concordent lorsqu'ils sont de la même longueur et que leurs caractères respectifs sont identiques, exception faite des espaces et des traits d'union qui sont ignorés au cours des opérations de comparaison.

- Heure

  Syntaxe utilisée par les attributs dont les valeurs sont des entiers non signés qui représentent une heure exprimée en secondes.

- Tampon horaire

  Syntaxe utilisée par les attributs dont les valeurs indiquent l'heure à laquelle un événement particulier s'est produit. Lorsqu'un événement important survient, un serveur eDirectory crée une valeur Tampon horaire et l'associe à l'événement. Chaque valeur Tampon horaire est unique au sein d'une partition eDirectory. Cela permet d'obtenir une liste ordonnée de tous les événements qui se sont produits sur tous les serveurs contenant des répliques d'une partition.

- Nom avec type

  Syntaxe utilisée par les attributs dont les valeurs représentent un niveau et un intervalle associés à un objet. Cette syntaxe attribue un nom à un objet eDirectory et associe à ce dernier les deux valeurs numériques suivantes :

  - un niveau d'attribut, qui indique la priorité ;
  - un intervalle représentant le nombre de secondes entre certains événements ou la fréquence de la référence.

- Inconnu

  Syntaxe utilisée par les attributs dont la définition a été supprimée du schéma. Cette syntaxe représente des chaînes dinformations binaires.

Attributs obligatoires et facultatifs

À chaque objet est associée une classe de schéma définie pour le type dobjet correspondant. Une classe est un groupe dattributs organisés de façon logique. Certains de ces attributs sont obligatoires, alors que d'autres sont facultatifs.

Attributs obligatoires

Un attribut obligatoire doit être fourni au moment de la création d'un objet. Par exemple, si vous décidez de créer un utilisateur à l'aide de la classe Utilisateur, où le numéro d'employé est un attribut obligatoire, le nouvel objet Utilisateur ne peut être créé que si vous indiquez un numéro d'employé.

Attributs facultatifs

Un attribut facultatif est un attribut qui peut être renseigné si souhaité. Par exemple, si vous décidez de créer un objet Utilisateur à l'aide de la classe Utilisateur, dont l'un des attributs facultatifs est Autres noms, le nouvel objet peut être créé avec ou sans les données correspondant à cet attribut, selon que le nouvel utilisateur porte ou non d'autres noms.

Une exception est faite à cette règle lorsqu'un attribut facultatif est utilisé pour la dénomination ; dans ce cas, l'attribut devient obligatoire.

Exemple de schéma

La Figure 12, page 48 fournit un exemple de partie de schéma qui peut être similaire à votre schéma de base. Elle affiche des informations sur la classe Organisation. La plupart des informations apparaissant sur cet écran ont été spécifiées lors de la création de la classe. Certains attributs facultatifs ont toutefois été ajoutés ultérieurement.

 Cette icône est assignée à tous les attributs et classes qui sont des extensions du schéma de base.

Figure 12 Page Informations sur la classe de iManager

Conception du schéma

La tâche de conception initiale de votre schéma peut vous épargner du temps et des efforts à long terme. Vous pouvez afficher le schéma de base et déterminer s'il répond à vos besoins ou si des modifications sont requises. Si des modifications sont nécessaires, étendez le schéma à l'aide du Gestionnaire de schéma. Pour plus d'informations, reportez-vous aux sections « Extension du schéma », page 122 et « Affichage du schéma », page 126.

Partitions

Une partition est une division logique de la base de données eDirectory. Une partition d'annuaire forme une unité de données distincte dans l'arborescence qui contient des informations de l'annuaire.

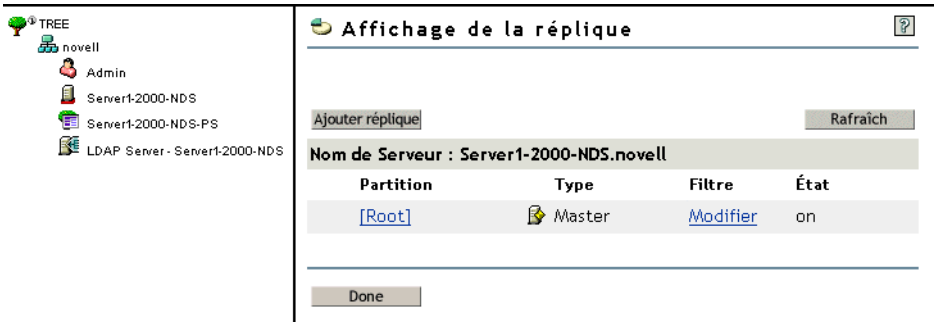
Le partitionnement permet de déplacer une partie de l'annuaire d'un serveur vers un autre.

Si vos liaisons WAN sont lentes ou peu fiables, ou si l'annuaire comprend un nombre élevé d'objets qui entraîne une surcharge du serveur et ralentit l'accès, partitionnez l'annuaire. Pour obtenir des informations complètes sur les partitions, reportez-vous au Chapitre 5, « Gestion des partitions et des répliques », page 133.

Chaque partition de l'annuaire se compose d'un ensemble d'objets Conteneur, de tous les objets qu'ils incluent et des données concernant ces objets. Les partitions eDirectory ne comprennent pas d'informations sur le système de fichiers, ni sur les répertoires et fichiers de ce système.

Le partitionnement est effectué à l'aide de Novell iManager. Les partitions sont identifiées dans iManager par l'icône de partition suivante : ( ).

Figure 13 Affichage des répliques d'un serveur



Dans l'exemple ci-dessus, l'icône de partition se trouve en regard de l'objet Arborescence. Cela signifie que cet objet est le conteneur le plus élevé dans la partition. Aucune icône de partition n'apparaît en regard des autres conteneurs. C'est donc la seule partition.

La partition par défaut pour eDirectory consiste en effet à conserver l'annuaire complet dans une seule partition.

Notez que, dans cet exemple, l'affichage des répliques apparaît. Lorsque l'affichage des répliques apparaît pour un serveur dans iManager, toutes les répliques de ce serveur sont affichées dans la partie droite de l'écran. Dans le cas présent, Serveur1 contient une réplique de la partition unique Pour plus d'informations, reportez-vous au « Répliques », page 52 et à l'« Affichage des répliques sur un serveur eDirectory », page 141.

Partitions

Les partitions reçoivent le nom du conteneur le plus élevé qu'elles comprennent. La Figure 14 présente deux partitions: Arborescence et Finances. La partition Finances est appelée partition enfant de la partition Arborescence, car elle est extraite de cette dernière. La partition Arborescence est appelée partition parente de Finances.

Figure 14 Affichage des répliques d'une partition

Vous pouvez envisager de créer cette partition si l'annuaire compte tellement d'objets que le serveur est surchargé et que l'accès à eDirectory est lent. La création de cette partition permet de scinder la base de données et de placer les objets de cette branche sur un autre serveur.

L'exemple ci-dessus représente l'affichage des répliques de la partition Finances. Lorsque l'affichage des répliques apparaît pour une partition dans iManager, tous les serveurs comportant une réplique de cette partition sont affichés dans la partie droite de l'écran. Dans le cas présent, Serveur1 contient une réplique Lecture/écriture de la partition Finances. Pour plus d'informations, reportez-vous à la section « Affichage des répliques d'une partition », page 143.

Répartition optimale des répliques

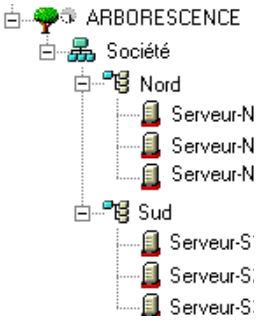
Dans l'exemple précédent, supposez que Serveur1 contienne des répliques des partitions Arborescence et Finances. À ce stade, les performances de eDirectory ne sont pas supérieures puisque Serveur1 contient toujours l'annuaire complet (les répliques des deux partitions).

Pour accroître les performances, vous devez déplacer l'une des répliques vers un autre serveur. Par exemple, si vous déplacez la partition Arborescence vers Serveur2, ce dernier contient tous les objets des conteneurs Arborescence et VotreSociété. Serveur1 ne contient alors plus que les objets des conteneurs Finances et Comptes. La charge de Serveur1 et de Serveur2 est inférieure à la charge globale sans partitionnement.

Partitions et liaisons WAN

Supposez que votre réseau couvre deux sites, Nord et Sud, connectés entre eux par une liaison WAN. Chacun des sites comporte trois serveurs.

Figure 15 Exemple de conteneurs eDirectory



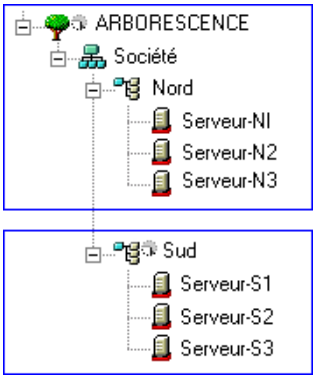
Dans ce cas, le fonctionnement de eDirectory est plus rapide et plus fiable si l'annuaire est divisé en deux partitions.

Avec une seule partition, les répliques sont soit conservées sur un site, soit partagées entre les deux sites. Cette solution s'avère difficile à gérer pour deux raisons :

- Si toutes les répliques sont stockées sur les serveurs du site Nord, par exemple, les utilisateurs du site Sud subissent des contretemps lorsqu'ils veulent se loguer ou accéder aux ressources. Si la liaison est interrompue, ces utilisateurs ne peuvent plus du tout se loguer ni accéder aux ressources.
- Si les répliques sont réparties entre les sites, les utilisateurs peuvent accéder en local à l'annuaire. Toutefois, la synchronisation des répliques entre les serveurs s'effectue via la liaison WAN ; il peut donc se produire des erreurs eDirectory si cette liaison n'est pas fiable. Par ailleurs, la propagation des modifications apportées à l'annuaire via cette liaison est lente.

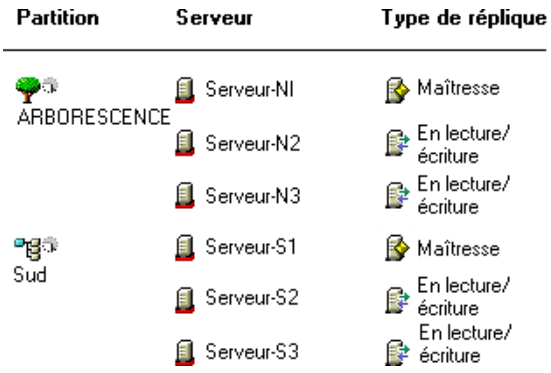
La solution à deux partitions présentée à la Figure 16, page 51 permet de résoudre ces problèmes de performances et de fiabilité sur la liaison WAN.

Figure 16 Exemple de partitions



Les répliques de la partition Arborescence sont conservées sur les serveurs du site Nord. Celles de la partition Sud sont conservées sur les serveurs du site Sud, comme l'illustre la Figure 17.

Figure 17 Exemple de partitions, serveurs et répliques



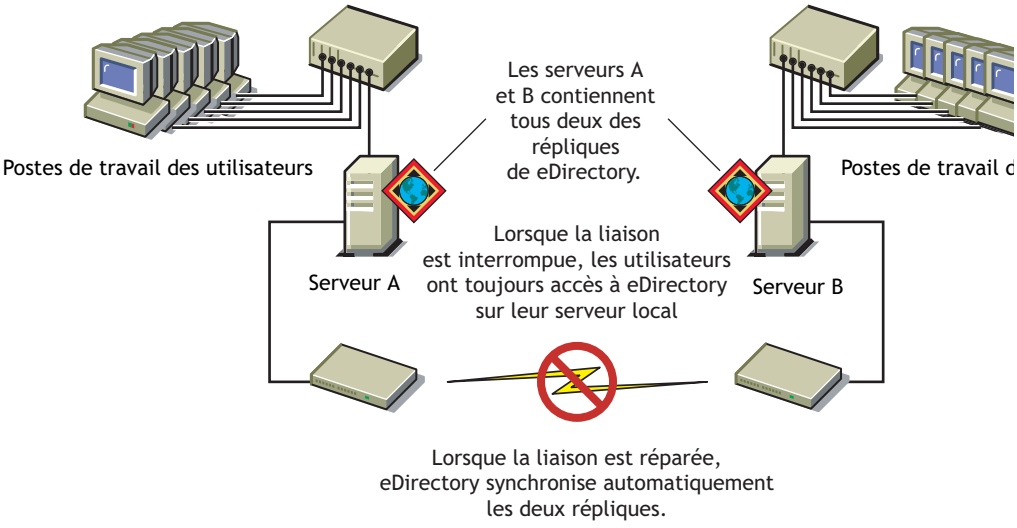
Pour chacun des sites, les objets qui représentent les ressources locales sont conservés localement. Le trafic de synchronisation entre les serveurs s'effectue également au niveau local, par le réseau LAN, plutôt que par la liaison WAN à débit faible et peu fiable.

Cependant, lorsqu'un utilisateur ou un administrateur accède aux objets d'un autre site, le trafic eDirectory est généré sur la liaison WAN.

Répliques

Une réplique est une copie (ou instance) d'une partition définie par l'utilisateur, qui est placée sur un serveur eDirectory. Si votre réseau comporte plusieurs serveurseDirectory, vous pouvez avoir plusieurs répliques (copies) de l'annuaire. Ainsi, en cas de panne d'un serveur ou d'échec d'une connexion réseau à ce serveur, les utilisateurs peuvent toujours se loguer et avoir recours aux ressources réseau restantes (voir Figure 18, page 52).

Figure 18 Répliques eDirectory



Chaque serveur peut héberger plus de soixante-cinq mille répliques eDirectory. Toutefois, un serveur ne peut contenir qu'une seule réplique d'une même partition définie par l'utilisateur. Pour obtenir des informations complètes sur les répliques, reportez-vous au Chapitre 5, « Gestion des partitions et des répliques », page 133.

Il est recommandé de posséder trois répliques pour garantir la tolérance aux pannes dans eDirectory (en supposant que vous disposiez de trois serveurs eDirectory sur lesquels les stocker). Un même serveur peut héberger les répliques de plusieurs partitions.

Un serveur de répliques est un serveur employé uniquement pour stocker des répliqueseDirectory. Ce type de serveur est quelquefois appelé serveur DSMASTER. Cette configuration est appréciée de certaines entreprises qui possèdent de nombreux bureaux distants dotés d'un seul serveur. Le serveur de répliques permet de stocker des répliques supplémentaires pour la partition d'un bureau distant. (Il peut aussi faire partie d'un plan de reprise après sinistre, comme expliqué à la section « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre », page 397.)

La fonction de réplication eDirectory ne garantit pas la tolérance aux pannes au niveau du système de fichiers du serveur, car seules les informations relatives aux objets eDirectory sont répliquées. Vous pouvez toutefois assurer cette tolérance grâce au système de suivi des transactions TTS™ (Transaction Tracking System™), à des disques en mode miroir/duplexé, à des systèmes RAID ou aux services NRS (Novell Replication Services).

Une réplique maîtresse ou une réplique Lecture/écriture est requise sur les serveurs NetWare qui fournissent des services de Bindery.

Si les utilisateurs accèdent régulièrement aux informations eDirectory au moyen d'une liaison WAN, vous pouvez réduire le temps d'accès et le trafic WAN en plaçant une réplique contenant les informations nécessaires sur un serveur auquel ils peuvent accéder localement.

Il en va de même, mais à moindre échelle, pour un réseau local (LAN). La répartition des répliques entre les serveurs du réseau signifie que les informations sont généralement extraites du serveur le plus proche.

Types de répliques

eDirectory prend en charge les types de répliques représentés dans la figure suivante :

Figure 19 Types de répliques

- « Réplique maîtresse », page 54
- « Réplique Lecture/écriture », page 54
- « Réplique Lecture seule », page 54
- « Réplique Lecture/écriture filtrée », page 55
- « Réplique Lecture seule filtrée », page 55
- « Réplique de référence subordonnée », page 55

Réplique maîtresse

Une réplique maîtresse est une réplique inscriptible utilisée pour apporter des modifications à un objet ou à une partition. Ce type de réplique permet d'effectuer les opérations suivantes sur les partitions eDirectory:

- ajouter des répliques sur des serveurs ;
- supprimer des répliques sur des serveurs ;
- créer des partitions dans l'arborescence eDirectory ;
- supprimer des partitions dans l'arborescence eDirectory ;
- déplacer une partition dans l'arborescence eDirectory.

La réplique maîtresse permet également d'effectuer les opérations suivantes sur les objets eDirectory:

- ajouter de nouveaux objets à l'arborescence eDirectory ;
- supprimer, renommer ou déplacer des objets dans l'arborescence eDirectory ;
- authentifier des objets pour l'arborescence eDirectory ;
- ajouter de nouveaux attributs d'objet à l'arborescence eDirectory ;
- modifier ou supprimer des attributs.

Par défaut, le premier serveur eDirectory du réseau est celui qui héberge la réplique maîtresse. Chaque partition ne peut avoir qu'une seule réplique maîtresse à la fois. Si d'autres répliques sont créées, ce sont par défaut des répliques Lecture/écriture.

Si vous envisagez d'arrêter plus d'un jour ou deux le serveur qui héberge une réplique maîtresse, vous pouvez transformer lune des répliques Lecture/écriture en maîtresse. La réplique maîtresse d'origine est alors automatiquement transformée en réplique Lecture/écriture.

Une réplique maîtresse doit être disponible sur le réseau pour que eDirectory puisse effectuer des opérations telles que la création d'une réplique ou d'une partition.

Réplique Lecture/écriture

eDirectory peut consulter les informations sur les objets et les modifier aussi bien dans une réplique Lecture/écriture que dans la réplique maîtresse. Toutes les modifications sont automatiquement répercutées dans toutes les répliques.

Si eDirectory fonctionne lentement en raison de retards dans l'infrastructure réseau (liaisons WAN à faible débit ou routeurs occupés, par exemple), vous pouvez créer une réplique Lecture/écriture plus proche des utilisateurs qui en ont besoin. Vous pouvez disposer d'autant de répliques Lecture/écriture que vous avez de serveurs pour les stocker. Notez cependant qu'une augmentation du nombre de répliques entraîne un accroissement du trafic pour assurer leur synchronisation.

Réplique Lecture seule

Une réplique Lecture seule est une réplique lisible qui s'emploie pour obtenir des informations sur tous les objets qui se trouvent dans les limites d'une partition. Les répliques Lecture seule reçoivent des mises à jour de synchronisation des répliques maîtresse et des répliques Lecture/écriture. Aucune modification n'est reçue directement des clients.

Ce type de réplique ne permet pas d'émuler la Bindery, mais garantit la tolérance aux pannes dans eDirectory. Si la réplique maîtresse et toutes les répliques Lecture/écriture viennent à être détruites ou endommagées, la réplique Lecture seule peut devenir la nouvelle réplique maîtresse.

Ce type de réplique autorise en outre la lecture des objets NDS, la tolérance aux pannes (la réplique contient tous les objets compris dans les limites de la partition) et les connexions à l'arborescence NDS (la réplique contient l'objet Racine de partition).

Une réplique Lecture seule ne doit cependant jamais servir à l'établissement d'une règle de sécurité au sein d'une arborescence pour limiter les opérations de modification des objets, étant donné que le client peut toujours accéder à une réplique Lecture/écriture pour apporter des modifications. L'annuaire comporte d'autres outils pour la sécurité, notamment le filtre de droits hérités. Pour plus d'informations, reportez-vous à la section « Filtre des droits hérités (IRF) », page 64.

Réplique Lecture/écriture filtrée


Les répliques Lecture/écriture filtrées contiennent un ensemble filtré d'objets ou de classes d'objet accompagné d'un ensemble filtré d'attributs et de valeurs pour ces objets. Le contenu est limité aux types d'objets et propriétés eDirectory propres au filtre de réplication du serveur hôte. Les utilisateurs peuvent lire et modifier le contenu de la réplique ; eDirectory peut accéder aux informations d'objet sélectionnées et les modifier. Les modifications sélectionnées sont alors automatiquement répercutées sur toutes les répliques.

Dans le cas des répliques filtrées, vous ne pouvez disposer que d'un filtre par serveur. Cela signifie que tout filtre défini pour un serveur s'applique à toutes les répliques filtrées présentes sur ce serveur. Vous pouvez toutefois disposer d'autant de répliques filtrées que vous possédez de serveurs pour les stocker, mais un nombre élevé de répliques entraîne une augmentation du trafic pour assurer leur synchronisation.

Pour plus d'informations, reportez-vous à la section « Répliques filtrées », page 56.

Réplique Lecture seule filtrée


Les répliques Lecture seule filtrées contiennent un ensemble filtré d'objets ou de classes d'objet, accompagné d'un ensemble filtré d'attributs et de valeurs pour ces objets. Elles reçoivent des mises à jour de synchronisation des répliques maîtresses et des répliques Lecture/écriture, mais aucune modification ne provient directement des clients. Les utilisateurs peuvent lire le contenu de ces répliques, mais ils ne peuvent pas le modifier. Le contenu est limité aux types d'objets et propriétés eDirectory propres au filtre de réplication du serveur hôte.

Pour plus d'informations, reportez-vous à la section « Répliques filtrées », page 56.

Réplique de référence subordonnée

Les répliques de référence subordonnée sont créées par le système. Elles ne contiennent pas toutes les données d'objet d'une réplique maîtresse ou d'une réplique Lecture/écriture. Elles ne contribuent donc pas à la tolérance aux pannes. Il s'agit de pointeurs internes générés pour contenir assez d'informations afin que eDirectory puisse résoudre les noms d'objet entre les partitions.

Vous ne pouvez pas supprimer une réplique de référence subordonnée ; eDirectory la supprime automatiquement lorsqu'elle devient inutile. Les répliques de ce type sont créées uniquement sur les serveurs qui contiennent une réplique d'une partition parente, mais aucune réplique des partitions enfants de cette dernière.

Si une réplique de partition enfant est copiée sur un serveur contenant la réplique de la partition parent, la réplique de référence subordonnée est automatiquement supprimée.

Répliques filtrées

Les répliques filtrées contiennent un ensemble filtré d'objets ou de classes d'objet, accompagné d'un ensemble filtré d'attributs et de valeurs pour ces objets. Par exemple, vous pouvez avoir besoin de créer sur un même serveur un ensemble de répliques filtrées qui contienne uniquement des objets Utilisateur provenant de diverses partitions de l'arborescence eDirectory. En outre, vous pouvez choisir de n'inclure qu'un sous-ensemble des données des objets Utilisateur (par exemple Prénom, Nom et Numéro de téléphone).

Une réplique filtrée peut générer une vue des données eDirectory sur un seul serveur. À cette fin, la fonction de réplique filtrée vous permet de créer une étendue et un filtre. Le serveur eDirectory peut alors héberger un ensemble de données bien défini provenant de nombreuses partitions de l'arborescence.

Les descriptions de l'étendue du serveur et des filtres de données sont enregistrées dans eDirectory et peuvent être gérées dans iManager, via l'objet Serveur.

Un serveur qui héberge une ou plusieurs répliques filtrées possède un seul filtre de réplication. Par conséquent, toutes les répliques filtrées sur le serveur contiennent le même sous-ensemble d'informations provenant de leurs partitions respectives. La réplique de partition maîtresse d'une réplique filtrée doit être hébergée sur un serveur eDirectory exécutant eDirectory 8.5 ou une version ultérieure.

Les répliques filtrées présentent les avantages suivants :

- Réduction du trafic de synchronisation vers le serveur par diminution du volume de données à répliquer à partir d'autres serveurs.
- Réduction du nombre d'événements que Novell Nsure Identity Manager doit filtrer.

  Pour plus d'informations sur Novell Nsure Identity Manager, consultez le manuel *DirXML Administration Guide (Guide d'administration de DirXML)*. (http://www.novell.com/documentation/dirxml20/index.html)
- Réduction de la taille de la base de données d'annuaire.

  Chaque réplique augmente la taille de la base de données. En créant une réplique filtrée (et non une réplique complète), qui contient uniquement des classes spécifiques, vous pouvez réduire la taille de la base de données locale.

  Par exemple, si l'arborescence contient 10 000 objets, mais que seul un pourcentage réduit de ceux-ci correspond à des objets Utilisateur, vous pouvez créer une réplique filtrée contenant uniquement des objets Utilisateur, au lieu d'une réplique complète contenant 10 000 objets.

Tout en permettant de filtrer les données stockées dans une base de données locale, la réplique filtrée est semblable à une réplique eDirectory normale. Vous pouvez à tout instant la convertir en une réplique complète.

REMARQUE : par défaut, les répliques filtrées ont pour filtres obligatoires Organisation et Unité organisationnelle.

Pour plus d'informations sur la création et la gestion de répliques filtrées, reportez-vous à la section « Configuration et gestion des répliques filtrées », page 140.

Émulation de la Bindery NetWare

De nombreuses applications, comme les serveurs d'impression et les logiciels de sauvegarde, ont été créées pour des versions de NetWare antérieures à NetWare 4. Ces applications utilisaient la Bindery NetWare au lieu de eDirectory pour l'accès au réseau et la manipulation des objets.

La Bindery est une base de données à deux dimensions, composée d'objets identifiés pour un serveur particulier (objets Utilisateur, Groupe et Volume, par exemple). Elle est propre au serveur et centrée sur lui.

Les anciens logiciels client de NetWare (par exemple le shell de Bindery NETX) utilisaient une procédure de login de Bindery par laquelle un utilisateur ne pouvait se loguer qu'à un serveur particulier. L'accès à plusieurs serveurs nécessitait plusieurs logins et plusieurs comptes utilisateur.

eDirectory permet aux applications conçues pour une Bindery de fonctionner avec les services de Bindery. Les services de Bindery permettent de définir jusqu'à 12contextes eDirectory en tant que Bindery virtuelle d'un serveur eDirectory. Le contexte que vous définissez est appelé contexte de Bindery du serveur.

Voici quelques points importants en ce qui concerne les services de Bindery:

- Pour pouvoir utiliser les services de Bindery, vous devez définir un contexte de Bindery pour le serveur eDirectory.
- Tous les objets ne peuvent pas être représentés par des objets de Bindery. De nombreux objets, comme les alias, n'ont pas d'objet de Bindery équivalent.
- La plupart des applications de Bindery ont été mises à niveau pour fonctionner avec eDirectory. Contactez votre fournisseur pour vous procurer la dernière version.
- Chaque serveur eDirectory doté d'un contexte de Bindery doit contenir une réplique maîtresse ou une réplique Lecture/écriture de la partition qui comprend ce contexte de Bindery.

Synchronisation des serveurs dans un anneau de répliques

Lorsque plusieurs serveurs contiennent des répliques de la même partition, ils constituent un anneau de répliques. La synchronisation est le transfert d'informations sur l'annuaire d'une réplique vers une autre, pour garantir la cohérence des deux partitions. eDirectory garde automatiquement ces serveurs synchronisés. Pour plus d'informations, reportez-vous à la section « Synchronisation », page 108.

Les types de synchronisation eDirectory sont les suivants :

- la synchronisation normale ou synchronisation des répliques et
- la synchronisation de priorité.

Accès aux ressources

eDirectory offre un niveau de sécurité élémentaire pour l'accès au réseau, au moyen de droits définis par défaut. Vous pouvez renforcer cette sécurité en exécutant les tâches décrites ci-dessous.

- Assignation de droits

  Chaque fois qu'un utilisateur tente d'accéder à une ressource réseau, le système détermine ses droits effectifs sur cette ressource. Pour vous assurer que les utilisateurs disposent de droits effectifs appropriés sur les ressources, vous pouvez effectuer des assignations d'ayant droit explicites, accorder des équivalences de sécurité et filtrer les droits hérités.

  Pour simplifier l'assignation de droits, vous pouvez créer des objets Groupe et Rôle organisationnel, puis assigner des utilisateurs à ces objets.

- Sécurisation du login

  Aucune sécurité n'est fournie par défaut au niveau du login. Vous pouvez mettre en oeuvre plusieurs mesures de sécurité facultatives, à savoir des mots de passe de login, des restrictions de temps et d'emplacement de login, des limites sur les sessions de login simultanées, la détection des intrus et la désactivation du login.

- Configuration d'une administration basée sur le rôle

  Vous pouvez désigner des administrateurs pour certaines propriétés d'objet et leur octroyer des droits sur ces seules propriétés. Vous pouvez ainsi créer des administrateurs ayant des responsabilités spécifiques dont les subordonnés d'un objet Conteneur donné peuvent hériter. Un administrateur défini sur la base d'un rôle peut avoir des responsabilités sur toutes sortes de propriétés, comme celles qui ont trait aux informations concernant les employés ou aux mots de passe.

  Pour obtenir des instructions sur la configuration des services basés sur le rôle, consultez la section Installing RBS (http://www.novell.com/documentation/imanager25/imanager_admin_25/data/am757mw.html#bu1rlq9) (Installation de RBS) dans le manuel *Novell iManager 2.5 Administration Guide* (Guide d'administration de Novell iManager 2.5).

  Vous pouvez également définir des rôles sous forme de tâches spécifiques que les administrateurs peuvent effectuer dans des applications d'administration basée sur les rôles. Pour plus d'informations, reportez-vous à la section « Configuration des services basés sur le rôle », page 104.

Droits eDirectory

Lorsque vous créez une arborescence, les assignations de droits par défaut accordent à votre réseau des conditions généralisées d'accès et de sécurité. Parmi ces assignations par défaut, citons:

- L'utilisateur Admin dispose du droit Superviseur sur le sommet de l'arborescence, ce qui lui procure un contrôle total sur l'intégralité de l'annuaire. Admin possède également le droit Superviseur sur l'objet Serveur NetWare. Il peut ainsi contrôler tous les volumes de ce serveur.
- L'utilisateur [Public] dispose du droit Parcourir sur le sommet de l'arborescence. Tous les utilisateurs sont donc autorisés à afficher les objets situés dans cette arborescence.
- Les objets créés au moyen d'un processus de mise à niveau, tel qu'une migration NetWare, une mise à niveau d'impression ou une migration d'utilisateur de Windows NT, reçoivent des assignations d'ayant droit appropriées pour la plupart des situations.

Assignations d'ayants droit et objets cibles

L'assignation de droits implique un ayant droit et un objet cible. L'ayant droit représente l'utilisateur ou le groupe d'utilisateurs qui reçoit l'autorité. L'objet cible représente les ressources réseau sur lesquelles le ou les utilisateurs possèdent des droits.

- Si vous choisissez un alias comme ayant droit, les droits sont appliqués uniquement à l'objet que l'alias représente. Lobjet Alias peut cependant constituer une cible explicite.
- Un fichier ou un répertoire du système de fichiers NetWare peut également constituer une cible, même si les droits sur ce système de fichiers sont enregistrés dans le système lui-même et non dans eDirectory.

REMARQUE : l'ayant droit [Public] n'est pas un objet. Il s'agit d'un ayant droit spécial qui représente n'importe quel utilisateur réseau, logué ou non, à des fins d'assignation de droits.

Concepts relatifs aux droits eDirectory

Les concepts ci-dessous peuvent contribuer à une meilleure compréhension des droits eDirectory.

- « Droits d'objet (droits d'entrée) », page 59
- « Droits de propriété », page 59
- « Droits effectifs », page 60
- « Détermination des droits effectifs », page 60
- « Équivalence de sécurité », page 63
- « Liste de contrôle d'accès (ACL) », page 63
- « Filtre des droits hérités (IRF) », page 64

Droits d'objet (droits d'entrée)

Lorsque vous procédez à une assignation d'ayant droit, vous pouvez accorder des droits d'objet et des droits de propriété. Les droits d'objet concernent la manipulation de l'ensemble de l'objet, alors que les droits de propriété s'appliquent uniquement à certaines propriétés de l'objet. Un droit d'objet équivaut à un droit d'entrée, car il fournit une entrée dans la base de données eDirectory.

Chaque droit d'objet est décrit ci-dessous :

- **Superviseur** inclut tous les droits sur l'objet et toutes ses propriétés.
- **Parcourir** permet à l'ayant droit d'afficher l'objet dans l'arborescence. Il ne donne pas le droit de consulter les propriétés de l'objet.
- **Créer** ne s'applique que lorsque l'objet cible est un conteneur. Le droit Créer permet à l'ayant droit de créer des objets subordonnés au conteneur ; il comprend également le droit Parcourir.
- **Supprimer** permet à l'ayant droit de supprimer la cible de l'annuaire.
- **Renommer** permet à l'ayant droit de changer le nom de la cible.

Droits de propriété

Lorsque vous procédez à une assignation d'ayant droit, vous pouvez accorder des droits d'objet et des droits de propriété. Les droits d'objet concernent la manipulation de l'ensemble de l'objet, alors que les droits de propriété s'appliquent uniquement à certaines propriétés de l'objet.

iManager propose deux options de gestion des droits de propriété :

- Vous pouvez gérer toutes les propriétés à la fois lorsque l'élément [Tous les droits d'attribut] est sélectionné.
- Vous pouvez gérer une ou plusieurs propriétés individuellement lorsque les propriétés correspondantes sont sélectionnées.

Chaque droit de propriété est décrit ci-dessous :

- **Superviseur** permet à l'ayant droit de contrôler entièrement la propriété.
- **Comparer** permet à l'ayant droit de comparer la valeur d'une propriété à une valeur donnée. Ce droit permet d'effectuer une recherche et ne renvoie qu'un résultat, à savoir vrai ou faux. Il ne permet pas à layant droit de visualiser à proprement parler la valeur de la propriété.
- **Lire** permet à l'ayant droit d'afficher les valeurs d'une propriété. Ce droit comprend le droit Comparer.
- **Écrire** permet à l'ayant droit de créer, de modifier et de supprimer les valeurs d'une propriété.
- **S'ajouter** permet à l'ayant droit d'ajouter ou de retirer son nom en tant que valeur de propriété. Ce droit ne s'applique qu'aux propriétés dont les valeurs sont des noms d'objet, telles que les listes d'adhésion ou les listes de contrôle d'accès (ACL).

Droits effectifs

Les utilisateurs peuvent recevoir des droits de plusieurs manières, notamment par le biais d'une assignation d'ayant droit explicite, d'un héritage ou d'une équivalence de sécurité. Vous pouvez également limiter les droits par l'intermédiaire des filtres des droits hérités, et les modifier ou les révoquer à l'aide d'assignations d'ayant droit inférieures. Le résultat de toutes ces opérations, c'est-à-dire les droits que possède un utilisateur, correspond aux *droits effectifs*.

Les droits effectifs d'un utilisateur sur un objet sont déterminés chaque fois que cet utilisateur tente d'effectuer une opération.

Détermination des droits effectifs

Chaque fois qu'un utilisateur tente d'accéder à une ressource réseau, eDirectory détermine les droits effectifs dont il dispose sur la ressource cible en procédant de la manière suivante :

1. eDirectory liste les ayants droit dont les droits doivent être pris en compte dans le processus, à savoir:
   - l'utilisateur qui tente d'accéder à la ressource cible ;
   - les objets sur lesquels l'utilisateur dispose d'une équivalence de sécurité.
2. eDirectory détermine les droits effectifs de chaque ayant droit de la liste de la manière suivante :
   a. eDirectory commence par les droits héritables que l'ayant droit possède au sommet de l'arborescence.

      eDirectory recherche, dans la propriété Ayants droit de l'objet (ACL) de l'objet Arborescence, les entrées où figure l'ayant droit. Si des droits héritables existent dans ces entrées, eDirectory les utilise comme groupe de droits effectifs initial pour l'ayant droit.

   b. eDirectory descend d'un niveau dans la branche de l'arborescence qui contient la ressource cible.

c. eDirectory supprime tous les droits filtrés à ce niveau.

   eDirectory recherche, dans la liste ACL de ce niveau, les IRF (Inherited Rights Filters filtres des droits hérités) qui correspondent aux types (objet, toutes propriétés ou propriété spécifique) des droits effectifs de l'ayant droit. Si de tels filtres existent, eDirectory retire des droits effectifs de l'ayant droit les droits bloqués par ces IRF.

   Par exemple, si les droits effectifs de l'ayant droit contiennent une assignation de droit d'écriture sur toutes les propriétés, mais qu'un IRF bloque cette assignation à ce niveau, le système supprime ce droit d'écriture des droits effectifs de l'ayant droit.

d. eDirectory ajoute les droits héritables assignés à ce niveau, en remplaçant, le cas échéant, les assignations existantes.

   eDirectory recherche, dans la liste ACL de ce niveau, les entrées où figure l'ayant droit. S'il en existe et que leurs droits sont héritables, eDirectory copie ceux-ci dans les droits effectifs de l'ayant droit, en remplaçant les assignations existantes, le cas échéant.

   Par exemple si, jusqu'ici, les droits effectifs de l'ayant droit comprennent les droits d'objet Créer et Supprimer, mais aucun droit de propriété, et qu'aucun droit d'objet n'est spécifié dans la liste ACL à ce niveau, mais que cette dernière contient plutôt une assignation de droit d'écriture sur toutes les propriétés pour cet ayant droit, le système remplace alors les droits d'objets existants de l'ayant droit (Créer et Supprimer) par une assignation à blanc et lui ajoute les nouveaux droits d'écriture sur toutes les propriétés.

e. eDirectory répète les opérations de filtrage et d'ajout (étapesc et d ci-dessus) à chaque niveau de l'arborescence, y compris au niveau de la ressource cible.

f. eDirectory ajoute les droits non héritables assignés au niveau de la ressource cible, en remplaçant les assignations existantes, le cas échéant.

   eDirectory utilise le même processus que celui de l'étape2d. L'ensemble de droits obtenu au terme de cette procédure représente les droits effectifs de l'ayant droit.

3. eDirectory associe les droits effectifs de tous les ayants droit de la liste comme suit :

   a. eDirectory inclut tous les droits détenus par les ayants droit de la liste et exclut uniquement les droits qui ne sont assignés à aucun d'eux. Il ne mélange pas les différents types de droit. Par exemple, eDirectory n'ajoute pas les droits sur une propriété donnée à ceux qui existent sur toutes les propriétés, ou vice versa.

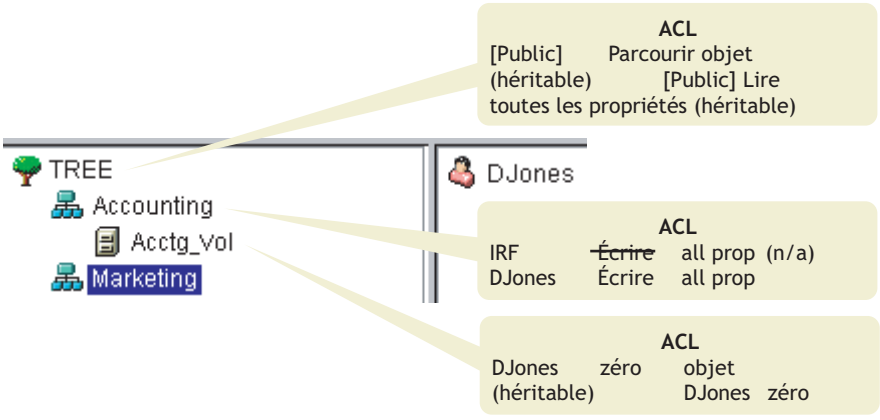
   b. eDirectory ajoute les droits qui dépendent des droits effectifs actuels.

      Lensemble de droits résultant constitue les droits effectifs de lutilisateur sur la ressource cible.

Exemple

L'utilisateur DJean tente d'accéder au volume Vol_Compta (voir Figure 20).

Figure 20 Exemple de droits d'ayant droit



Le processus suivant montre la façon dont eDirectory détermine les droits effectifs de DJean sur le volume Vol_Compta :

1. Les ayants droit dont les droits doivent être pris en compte dans le processus sont DJean, Marketing, Arborescence et [Public].

   Il est admis que DJean n'appartient à aucun groupe ou rôle et qu'aucune équivalence de sécurité ne lui a été explicitement assignée.

2. Pour chaque ayant droit, les droits effectifs sont les suivants :

   - DJean : aucun droit sur les objets, aucun droit sur toutes les propriétés

     L'assignation d'aucun droit sur toutes les propriétés au niveau de Vol_Compta est prioritaire par rapport à l'assignation d'un droit d'écriture sur toutes les propriétés au niveau de Comptabilité.

   - Marketing : aucun droit sur toutes les propriétés

     L'assignation du droit d'écriture sur toutes les propriétés au sommet de l'arborescence est rejetée par les IRF au niveau de Comptabilité.

   - Arborescence : aucun droit

     Aucun droit n'est assigné pour Arborescence dans la branche correspondante de l'arborescence.

   - [Public] : droits Parcourir objet et Lire toutes les propriétés

     Ces droits sont assignés à la racine. Ils ne sont filtrés ou remplacés à aucun emplacement de la branche pertinente de l'arborescence.

3. En combinant les droits de tous ces ayants droit, nous obtenons :

   DJean : droits Parcourir objet et Lire toutes les propriétés

4. Après ajout du droit de comparaison de toutes les propriétés, qui découle du droit Lire toutes les propriétés, nous obtenons pour DJean l'ensemble de droits effectifs suivant sur Vol_Compta :

   DJean : Parcourir objet, Lire et Comparer toutes les propriétés

Blocage des droits effectifs

Étant donné le mode de détermination des droits effectifs, vous pouvez éprouver des difficultés à éviter que des droits particuliers deviennent effectifs pour un utilisateur sans avoir recours à un IRF (en effet, un IRF bloque les droits de tous les utilisateurs).

Pour empêcher que des droits particuliers deviennent effectifs pour un utilisateur sans recourir à un IRF, procédez de l'une des manières suivantes :

- Assurez-vous que ni l'utilisateur ni aucun des objets pour lesquels l'utilisateur dispose d'une équivalence de sécurité n'obtient ces droits, que ce soit au niveau de la ressource cible ou à un niveau supérieur dans l'arborescence.
- Si l'utilisateur ou tout objet pour lequel il bénéficie d'une équivalence de sécurité se voit malgré tout attribuer ces droits, veillez à ce qu'il existe une assignation qui les exclut à un niveau inférieur dans l'arborescence. Procédez ainsi pour tous les ayants droit (associés à lutilisateur) disposant des droits non souhaités.

Équivalence de sécurité

L'équivalence de sécurité signifie qu'un objet dispose des mêmes droits qu'un autre objet. Lorsque vous attribuez à un objet une sécurité équivalente à celle d'un autre objet, les droits de ce dernier sont ajoutés à ceux du premier lorsque le système détermine les droits effectifs du premier objet.

Supposons, par exemple, que vous attribuiez à l'objet Utilisateur Julien une équivalence de sécurité par rapport à l'objet Admin. Une fois l'équivalence de sécurité créée, Julien dispose des mêmes droits qu'Admin sur l'arborescence et sur le système de fichiers.

Trois types d'équivalence de sécurité sont disponibles :

- Explicite : par assignation
- Automatique : par adhésion à un groupe ou à un rôle
- Implicite : par équivalence avec tous les conteneurs parents et l'ayant droit [Public]

L'équivalence de sécurité est valable une fois seulement. Par exemple, si vous accordez à un troisième utilisateur une sécurité équivalente à celle de Julien dans lexemple précédent, cet utilisateur ne reçoit pas les droits dAdmin.

Léquivalence de sécurité est enregistrée dans eDirectory sous la forme de valeurs de la propriété Sécurité égale à pour lobjet Utilisateur.

Lorsque vous ajoutez un objet Utilisateur en tant qu'occupant d'un objet Rôle organisationnel, cet utilisateur obtient automatiquement une équivalence de sécurité avec l'objet Rôle organisationnel. Il en va de même lorsqu'un utilisateur devient membre d'un objet Rôle de groupe.

Liste de contrôle d'accès (ACL)

La liste de contrôle d'accès (Access Control List ACL) est également connue sous le nom de propriété Ayants droit de l'objet. Lorsque vous créez une assignation d'ayant droit, l'ayant droit est ajouté en tant que valeur à la propriété Ayants droit de l'objet (ACL) de la cible.

Cette propriété a de fortes implications dans le domaine de la sécurité réseau pour les raisons suivantes :

- Toute personne disposant du droit Superviseur ou Écrire sur la propriété Ayants droit de l'objet (ACL) d'un objet peut déterminer qui est un ayant droit de cet objet.
- Tout utilisateur possédant le droit S'ajouter sur la propriété Ayants droit de lobjet (ACL) d'un objet donné peut modifier ses propres droits vis-à-vis de cet objet. Par exemple, il peut s'accorder à lui-même le droit Superviseur.

C'est pourquoi vous devez être vigilant lorsque vous attribuez le droit S'ajouter sur toutes les propriétés d'un objet Conteneur. Du fait de cette assignation, l'ayant droit peut devenir le superviseur de ce conteneur, de tous les objets qui y sont contenus et de tous les objets des conteneurs qui lui sont subordonnés.

Filtre des droits hérités (IRF)

Le filtre des droits hérités (Inherited Rights Filter IRF) permet de bloquer la transmission des droits vers le bas de l'arborescence eDirectory. Pour plus d'informations sur la configuration de ce filtre, reportez-vous à la section « Blocage des droits hérités sur un objet ou une propriété eDirectory », page 69.

Droits par défaut pour un nouveau serveur

Lorsque vous installez un nouvel objet Serveur dans une arborescence, les assignations d'ayant droit suivantes sont effectuées :

Ayants droit par défaut	Droits par défaut
Admin (pour le premier serveur eDirectory dans l'arborescence)	Droit d'objet Superviseur sur l'objet Arborescence. L'administrateur dispose du droit d'objet Superviseur sur l'objet Serveur NetWare, ce qui signifie qu'il possède également ce droit sur le répertoire racine du système de fichiers des volumes installés sur le serveur.
[Public] (pour le premier serveur eDirectory dans l'arborescence)	Droit d'objet Parcourir sur l'objet Arborescence.
Arborescence	Droit de propriété Lecture de l'arborescence sur les propriétés Nom du serveur hôte et Ressource hôte de tous les objets Volume. Ainsi, tous les objets ont accès au nom du volume et du serveur physiques.
Objets Conteneur	Droits de lecture et d'analyse de fichiers sur sys:\public. Les objets Utilisateur subordonnés à l'objet Conteneur peuvent ainsi accéder aux utilitaires NetWare du répertoire \public.
Objets Utilisateur	Si des répertoires privés sont automatiquement créés pour les utilisateurs, ces derniers disposent du droit Superviseur sur ces répertoires.

Administration déléguée

eDirectory vous permet de déléguer l'administration d'une branche de l'arborescence, en révoquant vos propres droits de gestion sur cette branche. Cette délégation peut s'imposer du fait de besoins spécifiques en matière de sécurité, qui nécessitent lintervention dun autre administrateur possédant un contrôle complet sur cette branche.

Pour déléguer l'administration:

1. Accordez le droit d'objet Superviseur sur un conteneur.
   - **1a** Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
   - **1b** Cliquez sur Droits > Modifier les ayants droit.
   - **1c** Entrez le nom et le contexte de l'objet Conteneur dont vous voulez contrôler l'accès, puis cliquez sur OK.
   - **1d** Cliquez sur Droits assignés.
   - **1e** Cochez la case Superviseur pour les propriétés souhaitées.
   - **1f** Cliquez sur Terminé, puis sur OK.
2. Créez un IRF dans le conteneur qui filtre le droit Superviseur et les autres droits que vous voulez bloquer.
   - **2a** Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
   - **2b** Cliquez sur Droits > Modifier le filtre des droits hérités.
   - **2c** Spécifiez le nom et le contexte de l'objet dont vous voulez modifier le filtre des droits hérités, puis cliquez sur OK.
   - **2d** Modifiez la liste des filtres de droits hérités, le cas échéant.

     Pour modifier la liste des filtres, vous devez avoir le droit Superviseur ou Contrôle d'accès sur la propriété ACL de l'objet. Vous pouvez définir des filtres qui bloquent les droits hérités sur la totalité de l'objet, sur toutes les propriétés de celui-ci ou sur des propriétés individuelles.

     REMARQUE : ces filtres ne peuvent pas bloquer des droits explicitement accordés à un ayant droit sur cet objet, étant donné que de tels droits ne sont pas hérités.
   - **2e** Cliquez sur OK.

IMPORTANT : si vous déléguez l'administration à un objet Utilisateur et que vous supprimez cet objet par la suite, plus aucun objet ne dispose de droits pour gérer cette branche.

Pour déléguer l'administration de propriétés eDirectory spécifiques, telles que la gestion des mots de passe, reportez-vous à la section « Octroi d'équivalence », page 67.

Pour déléguer l'utilisation de fonctions spécifiques dans les applications d'administration basée sur le rôle, reportez-vous à la section « Configuration des services basés sur le rôle », page 104.

Gestion des droits

- « Assignation explicite de droits », page 66
- « Octroi d'équivalence », page 67
- « Blocage des droits hérités sur un objet ou une propriété eDirectory », page 69
- « Affichage des droits effectifs sur un objet ou une propriété eDirectory », page 69

Assignation explicite de droits

Lorsque les assignations de droits par défaut de votre arborescence eDirectory offrent aux utilisateurs un accès trop important ou insuffisant aux ressources, vous pouvez créer ou modifier des assignations de droits explicites. Lorsque vous créez ou modifiez une assignation de droits, vous commencez par sélectionner la ressource dont vous voulez contrôler l'accès ou l'ayant droit (c'est-à-dire l'objet eDirectory qui possède, ou qui possédera, les droits).

SUGGESTION : pour gérer des droits d'utilisateurs collectivement plutôt qu'individuellement, faites d'un objet Groupe, Rôle ou Conteneur, l'ayant droit. Pour restreindre globalement (c'est-à-dire pour tous les utilisateurs) l'accès à une ressource, reportez-vous à la section « Blocage des droits hérités sur un objet ou une propriété eDirectory », page 69.

- « Contrôle de l'accès à Novell eDirectory par ressource », page 66
- « Contrôle de l'accès à Novell eDirectory par ayant droit », page 66

Contrôle de l'accès à Novell eDirectory par ressource

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Droits > Modifier les ayants droit.
3. Spécifiez le nom et le contexte de la ressource eDirectory (objet) dont vous voulez contrôler l'accès, puis cliquez sur OK.

   Sélectionnez un conteneur si vous souhaitez contrôler l'accès à tous les objets en aval de cette ressource.
4. Le cas échéant, modifiez la liste des ayants droit ainsi que les assignations de droits correspondantes.

   4a Pour modifier l'assignation de droits d'un ayant droit, sélectionnez l'ayant droit, cliquez sur Droits assignés, modifiez l'assignation, puis cliquez sur Terminé.

   4b Pour ajouter un objet comme ayant droit, cliquez sur Ajouter un ayant droit, sélectionnez l'objet, cliquez sur OK, puis sur Droits assignés pour attribuer les droits d'ayant droit et, pour finir, cliquez sur Terminé.

   Lorsque vous créez ou modifiez une assignation de droits, vous pouvez accorder ou refuser l'accès à la totalité de l'objet, à toutes les propriétés de l'objet ou à des propriétés individuelles.

   4c Pour supprimer un objet en tant qu'ayant droit, sélectionnez l'ayant droit, puis cliquez sur Supprimer l'ayant droit.

   L'ayant droit supprimé n'a plus de droits explicites sur l'objet ou les propriétés de celui-ci, mais peut toujours disposer de droits effectifs via l'héritage ou l'équivalence de sécurité.
5. Cliquez sur OK.

Contrôle de l'accès à Novell eDirectory par ayant droit

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Droits > Droits sur d'autres objets.
3. Entrez le nom et le contexte de l'ayant droit (c'est-à-dire l'objet qui possède, ou possèdera, les droits) dont vous voulez modifier les droits.
4. Dans la zone Contexte à partir duquel effectuer la recherche, indiquez la partie de l'arborescence eDirectory où doivent être recherchés les objets eDirectory sur lesquels l'ayant droit a actuellement des assignations de droits.

5 Cliquez sur OK.

Un écran apparaît, affichant la progression de la recherche. Une fois la recherche terminée, la page Droits sur d'autres objets apparaît, avec les résultats de la recherche.

6 Le cas échéant, modifiez les assignations de droits eDirectory.

6a Pour ajouter une assignation de droits, cliquez sur Ajouter un objet, sélectionnez l'objet dont l'accès doit être contrôlé, cliquez sur OK, puis sur Droits assignés, attribuez les droits d'ayant droit et cliquez sur Terminé.

6b Pour modifier une assignation de droits, sélectionnez l'objet dont vous voulez contrôler l'accès, cliquez sur Droits assignés, modifiez l'assignation de droits de l'ayant droit, puis cliquez sur Terminé.

Lorsque vous créez ou modifiez une assignation de droits, vous pouvez accorder ou refuser l'accès à la totalité de l'objet, à toutes les propriétés de l'objet ou à des propriétés individuelles.

6c Pour supprimer une assignation de droits, sélectionnez l'objet dont vous voulez contrôler l'accès, puis cliquez sur Supprimer un objet.

L'ayant droit n'a plus de droits explicites sur l'objet ou les propriétés de celui-ci, mais peut toujours disposer de droits effectifs via l'héritage ou l'équivalence de sécurité.

7 Cliquez sur OK.

Octroi d'équivalence

Un utilisateur qui bénéficie d'une sécurité équivalente à celle d'un autre objet eDirectory possède de fait tous les droits de cet objet. Un utilisateur dispose automatiquement du même niveau de sécurité que les groupes et rôles auxquels il appartient. Tous les utilisateurs bénéficient implicitement d'une équivalence de sécurité avec l'ayant droit [Public] ainsi qu'avec chaque conteneur au-dessus de leurs objets Utilisateur dans l'arborescence eDirectory, y compris l'objet Arborescence. Vous pouvez également accorder à un utilisateur une sécurité équivalente à celle d'un quelconque objet eDirectory.

REMARQUE : les tâches de cette section vous permettent de déléguer la responsabilité d'administration à l'aide de droits eDirectory. Si vous avez des applications d'administration qui utilisent les rôles RBS (Role-Based Services Services basés sur le rôle), vous pouvez également déléguer la responsabilité d'administration en assignant à des utilisateurs une adhésion à ces rôles.

- « Octroi d'une équivalence de sécurité par adhésion », page 67
- « Octroi explicite d'une équivalence de sécurité », page 68
- « Configuration d'un administrateur pour les propriétés eDirectory spécifiques d'un objet », page 68

Octroi d'une équivalence de sécurité par adhésion

1 Si vous ne l'avez pas déjà fait, créez l'objet Groupe ou Rôle à partir duquel vous voulez accorder une équivalence de sécurité aux utilisateurs.

Pour plus d'informations, reportez-vous à la section « Création d'un objet », page 96.

2 Attribuez au groupe ou au rôle les droits eDirectory que vous voulez accorder aux utilisateurs.

Pour plus d'informations, reportez-vous à la section « Assignation explicite de droits », page 66.

3 Éditez la liste d'adhésion au groupe ou au rôle pour y inclure les utilisateurs auxquels vous souhaitez accorder les droits du groupe ou du rôle.

- Pour un objet Groupe, utilisez la page de propriétés Membres.

  Dans Novell iManager, cliquez sur Administration de eDirectory > Modifier un objet, spécifiez le nom et le contexte d'un objet Groupe, cliquez sur OK, puis sur l'onglet Membres.

- Pour un objet Rôle organisationnel, utilisez le champ Occupant de la fonction dans la page de propriétés de même nom.

  Dans Novell iManager, cliquez sur Administration de eDirectory > Modifier un objet, spécifiez le nom et le contexte d'un objet RôleRBS, cliquez sur OK, puis sur Occupant de la fonction dans l'onglet Général.

- Pour un objet RôleRBS, utilisez la page Modifier les membres de iManager.

  Dans Novell iManager, cliquez sur le bouton Configurer  , sélectionnez Configuration des rôles > Modifier les rôles iManager, cliquez sur le bouton Modifier les membres  situé à gauche du rôle à modifier, puis utilisez les options de la page Modifier les membres de iManager pour ajouter ou supprimer des membres dans un rôle.

4. Cliquez sur OK.

Octroi explicite d'une équivalence de sécurité

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Modifier un objet.
3. Entrez le nom et le contexte de l'utilisateur ou de l'objet à partir duquel vous voulez accorder l'équivalence de sécurité à l'utilisateur, puis cliquez sur OK.
4. Cliquez sur l'onglet Sécurité, puis accordez l'équivalence de sécurité comme suit :

   - Si vous avez choisi un utilisateur, cliquez sur Sécurité égale à, saisissez le nom et le contexte de l'objet à partir duquel vous voulez accorder une équivalence de sécurité à l'utilisateur, appuyez sur Entrée, puis cliquez sur OK.
   - Si vous avez choisi un objet à partir duquel vous voulez accorder une équivalence de sécurité à l'utilisateur, cliquez sur Sécurité égale à moi, saisissez le nom et le contexte de l'utilisateur à partir duquel vous voulez accorder une équivalence de sécurité à l'objet, appuyez sur Entrée, puis cliquez sur OK.

   Le contenu de ces deux pages de propriétés est synchronisé par le système.
5. Cliquez sur OK.

Configuration d'un administrateur pour les propriétés eDirectory spécifiques d'un objet

1. Si vous ne l'avez pas déjà fait, créez l'objet Utilisateur, Groupe, Rôle ou Conteneur que vous voulez définir comme ayant droit des propriétés spécifiques d' un objet donné.

   Si vous créez un conteneur en tant qu'ayant droit, tous les objets à l'intérieur et en aval de ce conteneur disposeront des droits que vous accordez. Toutefois, la propriété doit être héritable pour que le conteneur et ses membres puissent bénéficier des droits en aval de celui-ci.

   Pour plus d'informations, reportez-vous à la section « Création d'un objet », page 96.
2. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
3. Cliquez sur Droits > Modifier les ayants droit.
4. Spécifiez le nom et le contexte du conteneur de niveau supérieur qui doit être géré par l'administrateur, puis cliquez sur OK.

5. Accédez à la page Modifier les ayants droit, cliquez sur Ajouter un ayant droit, sélectionnez l'objet qui représente l'administrateur, puis cliquez sur OK.
6. Cliquez sur Droits assignés pour l'ayant droit que vous venez d'ajouter, puis cliquez sur Ajouter une propriété.
7. Sélectionnez les propriétés que vous voulez ajouter à la liste des propriétés, puis cliquez sur OK.
8. Assignez les droits requis pour chaque propriété que l'administrateur doit gérer.

   Vérifiez que la case Héritable est cochée pour chaque assignation de droits.
9. Cliquez sur Terminé, puis sur OK.

Blocage des droits hérités sur un objet ou une propriété eDirectory

Dans eDirectory, les assignations de droits relatives aux conteneurs peuvent être héritables ou non. Dans le système de fichiers NetWare, les assignations de droits relatives aux dossiers sont toutes héritables. Dans eDirectory comme dans NetWare, vous pouvez toutefois bloquer le processus d'héritage au niveau de certains éléments subordonnés, afin que les droits ne soient pas effectifs pour ces éléments, et ce quel que soit l'ayant droit. Une exception est le droit Superviseur, qui ne peut pas être bloqué dans le système de fichiers Netware.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Droits > Modifier le filtre des droits hérités.
3. Spécifiez le nom et le contexte de l'objet dont vous voulez modifier le filtre des droits hérités, puis cliquez sur OK.

   La liste des filtres des droits hérités déjà définis pour cet objet s'affiche.
4. Dans la page des propriétés, apportez les modifications voulues à la liste des filtres de droits hérités.

   Pour modifier la liste des filtres, vous devez avoir le droit Superviseur ou Contrôle d'accès sur la propriété ACL de l'objet. Vous pouvez définir des filtres qui bloquent les droits hérités sur la totalité de l'objet, sur toutes les propriétés de celui-ci ou sur des propriétés individuelles.

   REMARQUE : ces filtres ne peuvent pas bloquer des droits qui ont été explicitement accordés à un ayant droit sur cet objet, car de tels droits ne sont pas hérités.
5. Cliquez sur OK.

Affichage des droits effectifs sur un objet ou une propriété eDirectory

Les droits effectifs sont les droits que les utilisateurs peuvent concrètement exercer sur des ressources spécifiques du réseau. Ils sont déterminés par eDirectory en fonction des assignations de droits explicites, de l'héritage et des équivalences de sécurité. Vous pouvez interroger le système pour connaître les droits effectifs d'un utilisateur sur une ressource donnée.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Droits > Afficher les droits effectifs.
3. Entrez le nom et le contexte de l'ayant droit dont vous voulez afficher les droits effectifs et cliquez sur OK.

4 Choisissez parmi les options suivantes :

Option	Description
Nom de propriété	Liste les propriétés sur lesquelles l'ayant droit dispose de droits effectifs. Les propriétés sont lues à partir de eDirectory et sont dès lors toujours affichées en anglais. Chaque élément de la liste appartient à l'un des types suivants : [Tous les droits d'attribut] Représente toutes les propriétés de l'objet. [Droits d'entrée] Représente l'objet comme un tout. Les droits sur cet élément ne présupposent aucun droit de propriété, sauf dans le cas du Superviseur. Propriétés spécifiques Il s'agit de propriétés spécifiques sur lesquelles l'ayant droit possède individuellement des droits. Par défaut, seules les propriétés de cette classe d'objet sont listées (voir ci-après).
Droits effectifs	Affiche les droits effectifs de l'ayant droit sur la propriété sélectionnée, tels qu'ils ont été déterminés par eDirectory.
Afficher toutes les propriétés dans le schéma	Laissez cette case désélectionnée pour n'afficher que les propriétés de cette classe d'objet. Cochez cette case pour afficher les propriétés de toutes les classes définies dans le schéma eDirectory. Les propriétés supplémentaires n'ont d'intérêt que si l'objet est un conteneur, ou s'il a été étendu pour inclure les propriétés d'une classe auxiliaire. Les propriétés supplémentaires ne sont pas précédées d'une puce.

5 Cliquez sur Terminé.

2 Conception de votre réseau Novell eDirectory

La conception de Novell® eDirectory™ a une incidence sur presque tous les utilisateurs et toutes les ressources réseau. Un réseau eDirectory bien conçu permet d'améliorer les performances et la valeur de l'ensemble du réseau en optimisant l'efficacité, la tolérance aux pannes, la sécurité, l'évolutivité et le fonctionnement. Ce chapitre propose des idées de conception de réseau eDirectory.

Notions de base relatives à la conception d'un réseau eDirectory

Un réseau eDirectory efficace repose sur la topologie réseau et sur la structure organisationnelle de la société ; elle implique également une préparation appropriée.

Si vous concevez un réseau eDirectory pour l'e-Business, reportez-vous à la section « Conception de eDirectory pour l'e-Business », page 84.

Topologie réseau

La topologie réseau correspond à la configuration physique de votre réseau. Pour développer une conception de réseau eDirectory efficace, vous devez tenir compte des éléments suivants :

- Liaisons WAN
- Utilisateurs nécessitant un accès à distance
- Ressources réseau (par exemple, nombre de serveurs)
- Conditions du réseau (par exemple, pannes de courant fréquentes)
- Modifications envisagées de la topologie réseau

Structure organisationnelle

La structure organisationnelle de la société influe sur la conception du réseau eDirectory. Pour développer une conception eDirectory efficace, vous avez besoin :

- de l'organigramme de l'entreprise et d'une bonne compréhension du fonctionnement de la société ;
- d'un personnel suffisamment qualifié pour effectuer la conception et la mise en oeuvre de l'arborescence eDirectory.

  Vous devez identifier le personnel capable d'effectuer les opérations suivantes :

  - cibler et planifier la conception du réseau eDirectory ;
  - comprendre la conception du réseau eDirectory, ses normes et sa sécurité ;
  - comprendre la structure physique du réseau et en assurer la maintenance ;
  - gérer l'épine dorsale inter-réseau, les télécommunications, la conception des liaisons WAN et le placement du routeur.

Préparation de la conception du réseau eDirectory

Avant d'implémenter la conception du réseau eDirectory, vous devez effectuer les opérations suivantes :

- définir des attentes réalistes en matière d'étendue et de planification ;
- avertir tous les utilisateurs concernés par la conception de la mise en oeuvre du réseau eDirectory ;
- passer en revue les informations contenues dans les sections « Topologie réseau », page 71 et « Structure organisationnelle », page 72.

Conception de l'arborescence eDirectory

La conception de l'arborescence eDirectory est la procédure la plus importante lorsqu'il s'agit de créer et de mettre en place un réseau. Cette conception est composée des tâches suivantes :

- « Création d'un document relatif aux normes de dénomination », page 72
- « Conception des couches supérieures de l'arborescence », page 75
- « Conception des couches inférieures de l'arborescence », page 77

Création d'un document relatif aux normes de dénomination

L'utilisation de noms standard, notamment pour les objets, rend l'utilisation du réseau plus intuitive, aussi bien pour les utilisateurs que pour les administrateurs. Des normes écrites peuvent également indiquer la façon dont les administrateurs doivent définir les autres valeurs de propriété, telles que les adresses et les numéros de téléphone.

Les recherches et la navigation dans l'annuaire reposent principalement sur la cohérence des valeurs de dénomination et de propriété.

L'utilisation de noms standard permet également à Novell Nsure Identity Manager de transférer plus facilement les données entre eDirectory et les autres applications. Pour plus d'informations sur Novell Nsure Identity Manager, consultez le manuel *DirXML Administration Guide (Guide d'administration de DirXML).* (http://www.novell.com/documentation/dirxml20/index.html)

Objets

- Le nom doit être unique dans le conteneur. Par exemple, SylvieJouanel et SimonJouanel ne peuvent pas être tous les deux appelés SJOUANEL sils se trouvent dans le même conteneur.
- Les caractères spéciaux sont autorisés. Cependant, les signes plus (+) et égal (=) et le point (.) doivent toujours être précédés d'une barre oblique inverse (\). D'autres conventions de dénomination sont appliquées aux objets Serveur et Pays, ainsi qu'aux services de Bindery et aux environnements multilingues.
- Les lettres majuscules et minuscules, de même que les caractères de soulignement et les espaces, sont affichés tels que vous les avez saisis, mais sans distinction. Par exemple, Manager_Profile et MANAGER PROFILE sont considérés comme identiques.
- Si vous utilisez des espaces, vous devez mettre le nom entre guillemets lorsque vous l'entrez dans la ligne de commande ou dans les scripts de login.

Objets Serveur

- Les objets Serveur sont automatiquement créés lorsque vous installez de nouveaux serveurs.
- Vous pouvez créer d'autres objets Serveur pour les serveurs NetWare® et NT existants, ainsi que pour les serveurs eDirectory se trouvant dans d'autres arborescences. Toutefois, ils sont tous traités comme des objets de Bindery.
- Lors de la création d'un objet Serveur, le nom doit correspondre au nom du serveur physique, qui:
  - est unique sur l'ensemble du réseau ;
  - comporte de 2 à 47 caractères ;
  - ne contient que des lettres (A-Z), des chiffres (0-9), des traits d'union (-), des points (.) et des traits de soulignement (_) ;
  - ne peut avoir un point pour premier caractère.
- Une fois l'objet Serveur nommé, il ne peut pas être renommé dans Novell iManager. Si vous le renommez à partir du serveur, son nouveau nom apparaît automatiquement dans iManager.

Objets Pays

Les objets Pays doivent respecter le code ISO pour les pays (deux lettres).

Pour plus d'informations, reportez-vous à la liste des codes ISO3166 (http://www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html).

Objets de Bindery

Si vous accédez à l'objet sur un poste de travail NetWare 2 ou NetWare 3 via les services de Bindery, les restrictions suivantes s'appliquent :

- Les espaces du nom sont remplacés par des caractères de soulignement.
- Les noms sont tronqués à 47 caractères.
- Les caractères suivants ne sont pas autorisés: barre oblique (/), barre oblique inverse (\), deux-points (:), virgule (,), astérisque (*) et point d'interrogation (?).

IMPORTANT : l'émulation de la Bindery n'est pas prise en charge sur les plates-formes Linux, Solaris, AIX ou HP-UX.

Questions relatives aux langues

Si vous utilisez des postes de travail configurés dans diverses langues, vous voudrez sans doute limiter les noms dobjet à des caractères qui soient affichables sur tous les postes. Il peut arriver, par exemple, qu'un nom entré en japonais contienne des caractères qui ne puissent pas être affichés dans les langues occidentales.

HP-UX ne prend en charge que l'anglais.

IMPORTANT : le nom de l'arborescence doit toujours être indiqué en anglais.

Exemple de document relatif aux normes

Le tableau suivant est un exemple de document contenant des normes pour la dénomination de certaines des propriétés les plus fréquemment utilisées. Vous avez uniquement besoin des normes correspondant aux propriétés que vous utilisez. Distribuez ce document à tous les administrateurs chargés de la création et de la modification des objets.

Classe d'objet | Propriété	Norme	Exemples	Explication
Utilisateur | Nom de login	Initiale du prénom, du deuxième prénom (le cas échéant) et nom (tout en minuscules). Huit caractères au maximum. Tous les noms communs doivent être uniques dans l'entreprise.	mdupont, bjohnson	eDirectory n'exige pas l'utilisation de noms uniques au niveau de l'entreprise, mais cette méthode permet d'éviter des conflits au sein d'un même contexte (ou d'un contexte de Bindery).
Utilisateur | Nom	Nom de famille (utilisation normale des majuscules et des minuscules).	Dupont	Utilisé pour générer des étiquettes d'expédition.
Numéros de téléphone et de télécopie	Numéros séparés par des tirets.	États-Unis: 123-456-7890 Autres: 44-344-123456	Utilisé par le logiciel de numérotation automatique.
Classes multiples | Emplacement	Code d'emplacement à deux lettres (majuscules), tiret, boîte postale.	BA-C23	Utilisé par les coursiers interservices.
Organisation | Nom	Nom de votre entreprise pour toutes les arborescences.	Chaussures	En cas d'arborescences distinctes, choisissez un nom standard pour l'objet Organisation, afin de pouvoir fusionner ultérieurement les arborescences.
Unité organisationnelle | Nom (basé sur l'emplacement)	Code d'emplacement à deux ou trois lettres, toutes en majuscules.	ATL, CHI, CUP, LA, BAT, BOS, DAL	Utilisez des noms courts et standard pour une recherche plus efficace.
Unité organisationnelle | Nom (basé sur le service)	Nom ou abréviation du service.	Ventes, Méca	Utilisez des noms courts, standard pour faciliter l'identification du service pris en charge par le conteneur.
Groupe | Nom	Nom descriptif.	Chefs de projet	Évitez les noms trop longs: certains utilitaires ne peuvent pas les afficher.

Classe d'objet | Propriété	Norme	Exemples	Explication
Assignation de répertoire | Nom	Contenu du répertoire indiqué par l'assignation.	DOSAPPS	Utilisez des noms courts, standard pour faciliter l'identification du service pris en charge par le conteneur.
Profil | Nom	Objet du profil.	Utilisateur mobile	Utilisez des noms courts, standard pour faciliter l'identification du service pris en charge par le conteneur.
Serveur | Nom	SERV, tiret, service, tiret, numéro unique.	SERV-Méca-1	eDirectory nécessite que les noms de serveur soient uniques dans l'arborescence.

Conception des couches supérieures de l'arborescence

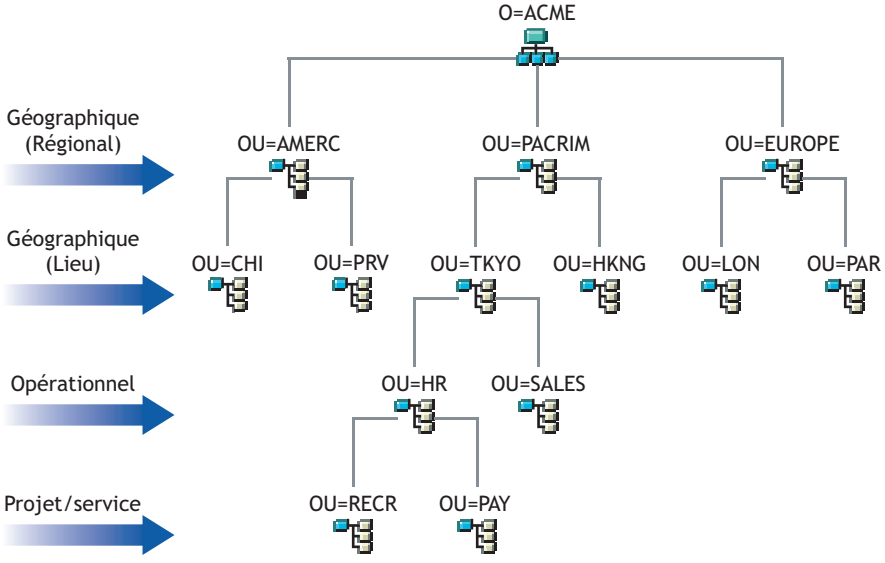
Vous devez concevoir très soigneusement les couches supérieures de l'arborescence ; en effet, si jamais vous devez par la suite apporter des modifications à ces couches, la totalité de l'arborescence en est affectée, notamment si votre entreprise est dotée de liaisons WAN. Vous devez concevoir le sommet de l'arborescence de manière à minimiser les modifications à apporter ultérieurement.

Utilisez les règles de conception suivantes pour créer l'arborescence eDirectory:

- Utilisez une conception pyramidale.
- Utilisez une seule arborescence eDirectory portant un nom unique.
- Créez un seul objet Organisation.
- Créez des unités organisationnelles de premier niveau qui représentent l'infrastructure physique du réseau.

La Figure 21 illustre les règles de conception de eDirectory.

Figure 21 Règles de conception de eDirectory



Pour créer les couches supérieures de l'arborescence, reportez-vous aux sections « Création d'un objet », page 96 et « Modification des propriétés d'un objet », page 96.

Utilisation d'une conception pyramidale

Les réseaux eDirectory conçus en pyramide facilitent la gestion, la modification de grands groupes et la création de partitions logiques.

L'alternative à une conception pyramidale est une arborescence simple dans laquelle tous les objets sont placés dans les couches supérieures de l'arborescence. eDirectory prend en charge une conception d'arborescence simple. Toutefois, ce type de conception peut rendre plus difficile la gestion et le partitionnement.

Utilisation d'une seule arborescence eDirectory portant un nom unique

Une seule arborescence est la conception optimale pour la plupart des organisations. Ainsi, par défaut, une seule arborescence est créée. Une arborescence unique implique une seule identité d'utilisateur sur le réseau, une administration de la sécurité plus simple et un seul point de gestion.

Ces recommandations concernant une arborescence unique pour une utilisation commerciale n'excluent pas la mise en place d'arborescences supplémentaires pour les tests et le développement.

Certaines organisations, cependant, peuvent avoir besoin de plusieurs arborescences pour des motifs juridiques, politiques ou professionnels. Par exemple, une organisation constituée de plusieurs entités autonomes peut avoir besoin de créer plusieurs arborescences. Si votre organisation requiert la création de plusieurs arborescences, envisagez l'utilisation de Novell Nsure Identity Manager pour en faciliter la gestion. Pour plus d'informations sur Novell Nsure Identity Manager, consultez le manuel *DirXML Administration Guide (Guide d'administration de DirXML)*. (http://www.novell.com/documentation/dirxml20/index.html)

REMARQUE : HP-UX ne prend pas en charge Novell Nsure Identity Manager.

Lorsque vous attribuez un nom à l'arborescence, utilisez un nom unique qui n'entrera pas en conflit avec celui d'autres arborescences. Utilisez un nom court et descriptif, comme ARBO-EDL.

Si deux arborescences portent le même nom et qu'elles sont situées sur le même réseau, vous risquez de rencontrer les problèmes suivants :

- Mises à jour appliquées à l'arborescence inappropriée
- Disparition de ressources
- Disparition de droits
- Altération

Vous pouvez modifier le nom de l'arborescence à l'aide de l'utilitaire DSMERGE, mais procédez avec précaution. La modification du nom d'une arborescence a une incidence sur le réseau, car vous devez reconfigurer les clients pour qu'ils prennent en compte le nouveau nom de l'arborescence.

Création d'un seul objet Organisation

En règle générale, une arborescence eDirectory doit comporter un objet Organisation. Par défaut, un objet Organisation unique est créé et nommé en fonction de la société. Vous pouvez ainsi configurer les modifications qui s'appliquent à la totalité de la société à partir d'un emplacement unique dans l'arborescence.

Par exemple, vous pouvez utiliser ZENworks® pour créer un objet Règle d'importation de postes de travail dans l'objet Organisation. Dans cette règle, qui influe sur la totalité de l'organisation, vous définissez la manière dont les objets Poste de travail sont nommés lorsqu'ils sont créés dans eDirectory.

Dans le conteneur Organisation, les objets créés sont les suivants :

- Admin
- Serveur
- Volume

  Les réseaux qui ne comportent qu'un seul serveur Windows, Linux, Solaris, AIX ou HP-UX exécutant eDirectory ne contiennent aucun objet Volume.

Vous pouvez créer plusieurs objets Organisation si votre société présente les caractéristiques suivantes :

- Elle comporte plusieurs sociétés qui ne partagent pas le même réseau.
- Elle a besoin de représenter séparément les différentes unités ou organisations.
- Elle dispose d'une règle ou de directives internes qui oblige les organisations à rester séparées.

Création d'unités organisationnelles représentant le réseau physique

La conception d'unités organisationnelles de premier niveau est importante, car elle a une incidence sur le partitionnement et l'efficacité de eDirectory.

Dans le cas de réseaux couvrant plusieurs bâtiments ou emplacements à l'aide de liaisons LAN ou WAN, la conception de l'objet Unité organisationnelle de premier niveau doit être basée sur l'emplacement. Vous pouvez ainsi créer des partitions eDirectory de manière à conserver tous les objets d'une partition à un même emplacement. Vous obtenez en outre un emplacement naturel où effectuer les assignations de sécurité et d'administrateur pour chaque emplacement.

Conception des couches inférieures de l'arborescence

Vous devez concevoir les couches inférieures d'une arborescence en fonction de l'organisation des ressources réseau. La conception des couches inférieures d'une arborescence eDirectory n'ayant d'impact que sur les objets situés au même emplacement, elle vous laisse plus de liberté que celle des couches supérieures.

Pour créer les couches inférieures de l'arborescence, reportez-vous aux sections « Création d'un objet », page 96 et « Modification des propriétés d'un objet », page 96.

Détermination de la taille du conteneur, de l'arborescence et de la base de données

Le nombre d'objets Conteneur de niveau inférieur que vous créez dépend du nombre total d'objets de l'arborescence, de l'espace disque disponible et des limitations de vitesse d'E/S au niveau du disque. eDirectory a été testé avec plus d'un milliard d'objets regroupés au sein d'une arborescence eDirectory unique. Ses performances sont donc uniquement limitées par l'espace disque, la vitesse d'E/S du disque et la mémoire vive. N'oubliez pas qu'une réplication peut avoir un impact important sur une arborescence de grande taille.

La taille habituelle d'un objet dans eDirectory est comprise entre 3 et 5 ko. À l'aide de cette taille d'objet, vous pouvez rapidement calculer l'espace requis sur le disque dur pour le nombre d'objets que vous possédez ou dont vous avez besoin. N'oubliez pas que la taille des objets augmente en fonction du nombre d'attributs pour lesquels des données ont été définies et en fonction de la nature de ces données. Lorsque des objets contiennent des données BLOB (Binary Large Object Objet binaire de grande taille), telles que des images, du son ou des informations biométriques, leur taille est forcément accrue.

Plus les partitions sont volumineuses, plus le temps de réplication est long. Si vous utilisez des produits qui requièrent l'utilisation de eDirectory, tels que ZENworks et les services DNS/DHCP, les objets eDirectory créés par de tels produits ont une incidence sur la taille des conteneurs dans lesquels ils sont situés. Il est recommandé de placer dans leur propre partition les objets créés à des fins uniquement administratives, tels que les objets DNS/DHCP, afin que l'accès utilisateur ne soit pas affecté par une réplication plus lente. La gestion des partitions et des répliques en est également facilitée.

Si cela vous intéresse, vous pouvez facilement déterminer la taille de votre base de données eDirectory ou de l'ensemble DIB (Directory Information Base).

- Pour NetWare, téléchargez le fichier toolbox.nlm à partir du site Web du support de Novell (http://support.novell.com) pour voir le répertoire sys:_netware de votre serveur.
- Pour Windows, recherchez l'ensemble DIB dans le répertoire \novell\nds\dibfiles.
- Pour Linux, Solaris, AIX ou HP-UX, recherchez l'ensemble DIB dans le répertoire indiqué lors de l'installation.

Choix des conteneurs à créer

Généralement, vous devez créer des conteneurs pour des objets qui partagent les besoins d'accès avec d'autres objets eDirectory. Cela permet de gérer de nombreux utilisateurs avec une assignation d'ayant droit ou un script de login. Vous pouvez créer des conteneurs dans le but précis de rendre les scripts de login des conteneurs plus efficaces ou vous pouvez placer deux services dans un même conteneur pour faciliter la gestion des scripts de login.

Conservez les utilisateurs dans des emplacements proches des ressources dont ils ont besoin afin de limiter le trafic réseau. Par exemple, les personnes au sein d'un même service travaillent généralement en étroite collaboration. Elles ont généralement besoin d'accéder au même système de fichiers et elles utilisent les mêmes imprimantes.

Il est simple de gérer les exceptions aux limites générales des groupes de travail. Par exemple, si deux groupes de travail utilisent une imprimante commune, vous pouvez créer un objet Alias pour l'imprimante dans l'un des groupes. Vous pouvez créer des objets Groupe pour gérer certains objets Utilisateur au sein d'un groupe de travail ou des objets Utilisateur répartis sur plusieurs groupes de travail. Vous pouvez créer des objets Profil pour les sous-groupes d'utilisateurs requérant des conditions uniques de script de login.

Instructions concernant la partition de votre arborescence

Lorsque vous partitionnez eDirectory, vous permettez à des parties de la base de données d'exister sur plusieurs serveurs. Grâce à cette fonctionnalité, vous pouvez optimiser l'utilisation du réseau en répartissant sur plusieurs serveurs la charge que représentent le stockage et le traitement des données eDirectory. Par défaut, une seule partition est créée. Pour plus d'informations sur les partitions, reportez-vous à la section « Partitions », page 49. Pour plus d'informations sur la création de partitions, reportez-vous au Chapitre 5, « Gestion des partitions et des répliques », page 133.

Vous trouvez ci-après des instructions convenant à la plupart des réseaux. Cependant, en fonction de la configuration, du matériel et du débit du trafic propres au réseau, vous devrez peut-être en adapter certaines.

Détermination des partitions pour les couches supérieures de l'arborescence

Tout comme vous concevez votre arborescence de façon pyramidale, vous créez également des partitions avec une structure pyramidale. La structure des partitions est la suivante : les partitions sont peu nombreuses au sommet de l'arborescence, mais leur nombre augmente au fur et à mesure que vous vous déplacez vers le bas de cette arborescence. Une telle conception génère moins de références subordonnées qu'une structure d'arborescence eDirectory qui contient plus de partitions en haut qu'en bas.

Vous pouvez obtenir cette conception pyramidale si vous créez toujours les partitions relativement près des objets Feuille, notamment des utilisateurs. (La partition créée à la racine de l'arborescence au cours de l'installation est une exception.)

Lorsque vous concevez les partitions pour les couches supérieures, tenez compte des points suivants :

- Partitionnez le sommet de l'arborescence sur la base de l'infrastructure WAN. Placez un nombre moins élevé de partitions en haut de l'arborescence et un nombre plus élevé en bas.

  Vous pouvez créer des conteneurs pour chaque site séparé par des liaisons WAN (en plaçant chaque objet Serveur dans son conteneur local), puis créer une partition pour chaque site.

- Dans un réseau comportant des liaisons WAN, les partitions ne doivent pas couvrir plusieurs emplacements.

  Cette conception garantit que le trafic de réplication entre différents sites ne consomme pas inutilement la largeur de bande WAN.

- Effectuez un partitionnement local autour des serveurs. Gardez les serveurs physiquement distants dans des partitions différentes.

Pour plus d'informations sur la gestion du trafic WAN, reportez-vous au Chapitre 11, « Gestionnaire de trafic WAN », page 289.

Détermination des partitions pour les couches inférieures de l'arborescence

Lorsque vous concevez les partitions pour les couches inférieures de l'arborescence eDirectory, tenez compte des points suivants :

- Définissez les partitions de couche inférieure par divisions organisationnelles, par services et par groupes de travail ; définissez également les ressources qui leur sont associées.

- Créez des partitions de telle sorte que tous les objets d'une même partition se trouvent à un emplacement unique. Vous avez ainsi l'assurance que les mises à jour vers eDirectory peuvent se faire sur un serveur local.

Détermination de la taille des partitions

Avec eDirectory, nous vous recommandons les limites de conception suivantes pour les tailles des partitions :

Élément	Limite
Taille de la partition	Objets illimités Base de données des informations de l'Annuaire (DIB) de répliques limitée à ITB
Nombre total de partitions dans l'arborescence	Illimité
Nombre de partitions enfants par parent	150
Nombre de répliques par partition	50 Limité par la DIB de répliques
Nombre de répliques par serveur de répliques	250

Cette modification des instructions de conception par rapport aux versions 6 et 7 des services NDS® vient des modifications apportées à l'architecture de la version 8 des NDS. Ces recommandations s'appliquent aux environnements distribués, tels que les sociétés. Ces recommandations risquent de ne pas être valables pour l'e-Business ou certaines applications.

Bien que les utilisateurs de l'e-Business requièrent généralement que toutes les données soient stockées sur un serveur unique, eDirectory fournit des répliques filtrées qui contiennent un sous-ensemble d'objets et d'attributs issus de différentes zones de l'arborescence. Cela permet de répondre aux mêmes besoins en e-Business sans avoir à stocker toutes les données sur le serveur. Pour plus d'informations, reportez-vous à la section « Répliques filtrées », page 56.

Prise en compte des variables réseau

Lorsque vous planifiez des partitions, tenez compte des variables réseau suivantes et de leurs limitations.

- Nombre et vitesse des serveurs
- Vitesse de l'infrastructure réseau (adaptateurs réseau, hubs et routeurs)
- Niveau de trafic du réseau

Instructions concernant la réplication de votre arborescence

La création de plusieurs partitions eDirectory n'augmente pas la tolérance aux pannes et n'améliore pas les performances de l'annuaire, contrairement à une utilisation stratégique de plusieurs répliques. L'emplacement des répliques est extrêmement important pour des questions d'accessibilité et de tolérance aux pannes. Les données eDirectory doivent en effet être disponibles aussi rapidement que possible et être copiées à plusieurs endroits pour garantir cette tolérance. Pour plus d'informations sur la création de répliques, reportez-vous au Chapitre 5, « Gestion des partitions et des répliques », page 133.

Les instructions suivantes permettent de déterminer la stratégie de placement des répliques.

Besoins des groupes de travail

Placez des répliques de chaque partition sur des serveurs physiquement proches du groupe de travail qui utilise les informations situées dans les partitions concernées. Si les utilisateurs à une extrémité d'une liaison WAN accèdent souvent à une réplique stockée sur un serveur situé à l'autre extrémité, placez une réplique sur des serveurs aux deux extrémités de la liaison.

Placez les répliques aux emplacements les plus fréquemment utilisés par les utilisateurs, les groupes et les services. Si des groupes d'utilisateurs appartenant à deux conteneurs distincts ont besoin d'accéder au même objet au sein des limites d'une autre partition, placez la réplique sur un serveur appartenant au conteneur situé au-dessus des deux conteneurs contenant le groupe.

Tolérance aux pannes

En cas de panne d'un disque ou d'arrêt d'un serveur, les répliques résidant sur des serveurs qui se trouvent à d'autres emplacements peuvent toujours authentifier les utilisateurs auprès du réseau et fournir des informations sur les objets des partitions stockées sur le serveur désactivé.

Étant donné que les mêmes informations sont distribuées sur plusieurs serveurs, vous ne dépendez pas d'un seul serveur pour vous authentifier auprès du réseau ou pour fournir des services (par exemple, le login).

Pour rendre possible la tolérance aux pannes, prévoyez trois répliques pour chaque partition si l'arborescence Annuaire contient assez de serveurs pour prendre en charge ce nombre. Il doit exister au moins deux répliques locales de la partition locale. Trois répliques sont suffisantes, sauf si vous avez besoin de fournir un accès aux données à d'autres emplacements, si vous ne prenez part à l'e-Business ou si vous utilisez d'autres applications qui requièrent plusieurs instances des données pour assurer l'équilibrage de la charge et garantir la tolérance aux pannes.

Vous ne pouvez avoir qu'une seule réplique maîtresse. Les autres répliques doivent être de type Lecture/écriture, Lecture seule ou filtrées. La plupart des répliques doivent être de type Lecture/écriture. Elles prennent en charge l'affichage et la gestion d'objets ainsi que les logins d'utilisateur, à l'instar de la réplique maîtresse. Ces répliques envoient les informations à synchroniser lorsqu'une modification est effectuée.

Les répliques Lecture seule ne sont pas accessibles en écriture. Elles permettent de rechercher et d'afficher les objets, et sont automatiquement mises à jour lors de la synchronisation des répliques de la partition.

Pour rendre possible la tolérance aux pannes, vous ne devez dépendre ni d'une référence subordonnée, ni de répliques filtrées. Une référence subordonnée est un pointeur et ne contient pas d'objets autres que l'objet racine de la partition. Les répliques filtrées ne contiennent pas la totalité des objets situés dans la partition.

eDirectory autorise un nombre illimité de répliques par partition, mais la quantité de trafic réseau augmente alors proportionnellement à ce nombre. Trouvez donc un équilibre entre les besoins de garantie d'une tolérance aux pannes et les besoins de performances réseau.

Vous ne pouvez stocker sur un serveur qu'une seule réplique par partition. Un même serveur peut stocker les répliques de plusieurs partitions.

En fonction du plan de reprise après sinistre de votre organisation, la majeure partie du travail de reconstruction du réseau après la perte d'un serveur ou d'un emplacement peut être assurée grâce aux répliques de partition. Si l'emplacement ne comporte qu'un seul serveur, sauvegardez régulièrement eDirectory. (Certains logiciels de sauvegarde ne sont pas compatibles avec eDirectory.) Envisagez d'acquérir un autre serveur pour la réplication dans le cadre de la tolérance aux pannes.

Détermination du nombre de répliques

Les facteurs limitatifs en matière de création de répliques sont le temps de traitement et la quantité de trafic requis pour la synchronisation de celles-ci. Lorsqu'un objet est modifié, ce changement est transmis à toutes les répliques de l'anneau de répliques. Plus un anneau de répliques comporte de répliques, plus la communication requise pour synchroniser les changements est importante. Si vous devez synchroniser des répliques via une liaisonWAN, l'opération demande plus de temps.

Si vous planifiez des partitions pour de nombreux sites géographiques, certains serveurs recevront de nombreuses répliques de références subordonnées. eDirectory peut distribuer ces références subordonnées sur un plus grand nombre de serveurs si vous créez des partitions régionales.

Réplication de la partition Arborescence

La partition Arborescence est la partition la plus importante de l'arborescence eDirectory. Si l'unique réplique de cette partition est altérée, le fonctionnement du réseau l'est aussi jusqu'à ce que la partition soit réparée ou que l'arborescence eDirectory soit complètement reconstruite. Par ailleurs, vous ne pourrez pas effectuer de modifications de conception au niveau de l'objet Arborescence.

Lorsque vous créez des répliques de la partition Arborescence, trouvez un équilibre entre le coût de la synchronisation des références subordonnées et le nombre de répliques de la partition Arborescence.

Réplication pour l'administration

Étant donné que les partitions ne peuvent être initialement modifiées qu'au niveau des répliques maîtresses, placez ces dernières sur des serveurs proches de l'administrateur réseau, dans un emplacement central. Il pourrait sembler plus logique de conserver les répliques maîtresses sur des sites distants ; elles doivent pourtant se trouver là où les opérations de partition ont lieu.

Il est préférable que les principales opérations eDirectory, comme le partitionnement, soient gérées par une seule personne ou un seul groupe dans un emplacement central. Cette façon de procéder permet de limiter les erreurs qui pourraient avoir des effets néfastes sur les opérations eDirectory ; elle permet également une sauvegarde centralisée des répliques maîtresses.

L'administrateur réseau doit effectuer des activités exigeant des ressources considérables, telles que la création d'une réplique, à des moments où le trafic réseau est peu important.

Satisfaction des besoins des services de Bindery pour NetWare

Si vous utilisez eDirectory sous NetWare et que les utilisateurs requièrent un accès à un serveur via des services de Bindery, ce serveur doit contenir une réplique maîtresse ou une réplique Lecture/écriture comportant le contexte de Bindery. L'instruction SET BINDERY CONTEXT dans le fichier autoexec.ncf définit le contexte de Bindery.

Les utilisateurs ne peuvent accéder aux objets fournissant des services de Bindery que si le serveur contient des objets réels. Lorsque vous ajoutez une réplique de partition au serveur, des objets réels lui sont également ajoutés et les utilisateurs disposant d'objets Utilisateur dans cette partition peuvent se loguer au serveur via une connexion de Bindery.

Pour plus d'informations sur les services de Bindery, reportez-vous à la section « Émulation de la Bindery NetWare », page 57.

Gestion du trafic WAN

Si les utilisateurs consultent certaines informations de l'annuaire via une liaison WAN, vous pouvez réduire le temps d'accès et le trafic WAN en plaçant une réplique contenant les informations voulues sur un serveur auquel les utilisateurs peuvent accéder localement.

Si vous répliquez les répliques maîtresses vers un site distant, ou si vous êtes obligé de placer des répliques sur le WAN pour des raisons d'accessibilité ou de tolérance aux pannes, n'oubliez pas la largeur de bande qui sera utilisée pour la réplication.

Vous devez placer les répliques sur des sites non locaux afin de garantir la tolérance aux pannes si vous ne parvenez pas à disposer des trois répliques recommandées, afin d'augmenter l'accessibilité et de fournir une gestion et un stockage centralisés des répliques maîtresses.

Pour contrôler la réplication du trafic eDirectory sur des liaisons WAN, utilisez le Gestionnaire WAN. Pour plus d'informations, reportez-vous à la section Chapitre 11, « Gestionnaire de trafic WAN », page 289.

Planification de l'environnement utilisateur

Une fois que vous avez conçu la structure de base de l'arborescence eDirectory et que vous avez configuré les opérations de partitionnement et de réplication, vous devez planifier l'environnement utilisateur pour simplifier la gestion et optimiser l'accès aux ressources réseau. Pour créer un plan d'environnement utilisateur, analysez les besoins des utilisateurs et créez des instructions d'accessibilité pour chaque zone.

Analyse des besoins des utilisateurs

Lorsque vous analysez les besoins des utilisateurs, tenez compte des éléments suivants :

- Besoins physiques du réseau, tels que les imprimantes ou l'espace de stockage des fichiers

  Déterminez si les ressources sont partagées par des groupes d'utilisateurs au sein d'une même arborescence ou par des groupes d'utilisateurs issus de plusieurs conteneurs. Tenez compte également des besoins en ressources physiques des utilisateurs distants.

- Besoins en services de Bindery des utilisateurs NetWare

  Déterminez les applications basées sur des services de Bindery et leurs utilisateurs.

- Besoins des applications

  Déterminez les applications et les fichiers de données dont ont besoin les utilisateurs, les systèmes d'exploitation présents et les groupes ou utilisateurs ayant besoin d'accéder à ces

applications. Prenez en compte le lancement manuel ou automatique des applications partagées par des applications telles que ZENworks.

Création des instructions d'accessibilité

Une fois que vous avez rassemblé les informations concernant les besoins des utilisateurs, vous devez définir les objets eDirectory que vous allez utiliser pour créer les environnements des utilisateurs. Par exemple, si vous créez des ensembles de règles ou des objets Application, vous devez déterminer leur nombre et l'endroit où ils devront être placés dans l'arborescence.

Vous devez également déterminer comment mettre en oeuvre les mesures de sécurité permettant de restreindre l'accès des utilisateurs. Vous devez identifier toutes les mesures de sécurité à prendre dans certains cas. Par exemple, vous pouvez avertir les administrateurs réseau de ne pas octroyer de droit Superviseur eDirectory sur des objets Serveur, car ce droit est hérité par le système de fichiers.

Conception de eDirectory pour l'e-Business

Si vous utilisez eDirectory pour l'e-Business, que vous fournissiez un portail pour des services ou que vous partagiez des données avec d'autres entreprises, les recommandations mentionnées dans ce chapitre ne sont pas forcément applicables à votre cas.

Vous pouvez suivre les instructions de conception de eDirectory pour l'e-Business suggérées ci-après.

Créez une arborescence avec un nombre limité de conteneurs.

Cette instruction dépend des applications que vous utilisez et de votre implémentation de eDirectory. Par exemple, le déploiement global d'un serveur de messagerie requiert des instructions de conception de eDirectory plus traditionnelles, telles que celles présentées plus haut dans ce chapitre. En outre, si vous vous apprêtez à distribuer l'administration des utilisateurs, vous pouvez créer une unité organisationnelle (OU) différente pour chaque zone de responsabilité administrative.

- Conservez au moins deux partitions.

  Conservez la partition par défaut au niveau Arborescence et créez une partition pour le reste de l'arborescence. Si vous avez créé des unités organisationnelles à des fins administratives, créez une partition pour chacune d'elles.

  Si vous répartissez la charge sur plusieurs serveurs, essayez de limiter le nombre de partitions ; conservez-en toutefois au moins deux pour la sauvegarde et la récupération en cas de sinistre.

- Créez au moins trois répliques de votre arborescence pour garantir la tolérance aux pannes et assurer l'équilibrage des charges.

  N'oubliez pas que LDAP n'équilibre pas lui-même la charge. Pour équilibrer la charge sur LDAP, pensez à utiliser des commutateurs de niveau 4.

- Créez une autre arborescence pour l'e-Business. Limitez les ressources réseau, telles que les serveurs et les imprimantes, incluses dans cette arborescence. Envisagez la création d'une arborescence qui ne contiendrait que des objets Utilisateur.

  Vous pouvez utiliser Novell Nsure Identity Manager pour lier cette arborescence utilisateur à d'autres arborescences contenant des informations sur le réseau. Pour plus d'informations, consultez le manuel *DirXML Administration Guide (Guide d'administration de DirXML)* (http://www.novell.com/documentation/dirxml20/index.html).

- Utilisez des classes auxiliaires pour personnaliser le schéma.

  Si un client ou une application requiert un objet Utilisateur différent du standard inetOrgPerson, utilisez les classes auxiliaires pour personnaliser le schéma. L'utilisation de classes auxiliaires permet aux concepteurs d'applications de modifier les attributs utilisés dans la classe sans avoir à recréer l'arborescence.

- Augmentez les performances d'importation LDIF.

  Lors de l'exécution de l'utilitaire d'importation, de conversion et d'exportation Novell, eDirectory indexe chaque objet pendant le processus. Cette opération risque de ralentir le processus d'importation au format LDIF. Pour améliorer les performances d'importation LDIF, interrompez l'indexation des attributs des objets créés, exécutez l'utilitaire d'importation, de conversion et d'exportation Novell, puis reprenez l'indexation des attributs.

- Implémentez des noms communs (CN) globalement uniques.

  eDirectory autorise la présence d'un même nom commun dans plusieurs conteneurs. Toutefois, si vous utilisez des noms communs globalement uniques, vous pouvez effectuer des recherches sur ces noms, sans mettre en place de logique de gestion de réponses multiples.

Présentation du serveur de certificats Novell

Le serveur de certificats Novell (Novell Certificate Server™) permet d'inventer, de publier et de gérer des certificats numériques en créant un objet Conteneur Sécurité et un objet Autorité de certification organisationnelle (CA). L'objet Autorité de certification organisationnelle permet de sécuriser la transmission des données. Il est requis pour les produits en relation avec Internet, tels que NetWare Web Manager et NetWare Enterprise Web Server. Le premier serveur eDirectory crée automatiquement et stocke physiquement les objets Conteneur Sécurité et Autorité de certification organisationnelle pour l'ensemble de l'arborescence eDirectory. Ces deux objets sont créés au sommet de l'arborescence eDirectory et doivent y rester.

Il ne peut y avoir qu'un seul objet Autorité de certification organisationnelle dans une arborescence eDirectory. Une fois que l'objet Autorité de certification organisationnelle a été créé sur un serveur, il n'est pas possible de le déplacer vers un autre serveur. La suppression ou le remplacement d'un objet Autorité de certification organisationnelle annule tout certificat associé auparavant à cet objet.

IMPORTANT : vérifiez que le premier serveur eDirectory est bien celui qui doit être l'hôte permanent de l'objet Autorité de certification organisationnelle. Vérifiez également qu'il est fiable, accessible et qu'il fait partie intégrante du réseau.

Si ce serveur n'est pas le premier serveur eDirectory sur le réseau, le programme d'installation recherche le serveur eDirectory qui contient l'objet Autorité de certification organisationnelle et fait référence à ce serveur. Il accède au conteneur Sécurité et crée un objet Certificat de serveur.

Si aucun objet Autorité de certification organisationnelle n'est disponible sur le réseau, les produits Web ne peuvent pas fonctionner.

Droits requis pour réaliser des tâches sur le serveur de certificats Novell

Pour effectuer les tâches associées à la configuration du serveur de certificats Novell, l'administrateur doit disposer des droits décrits dans le tableau suivant.

Tâche du serveur de certificats Novell	Droits requis
Configuration de la sécurité de base pour l'installation du premier serveur dans une nouvelle arborescence ou la mise à niveau du premier serveur dans une arborescence où aucun système de sécurité de base n'a été installé	Droit Superviseur au niveau de la racine Droit Superviseur sur le conteneur Sécurité
Configuration de la sécurité de base pour l'installation des autres serveurs	Droit Superviseur sur le conteneur du serveur Droit Superviseur sur l'objet W0 (situé à l'intérieur du conteneur Sécurité)
Création de l'autorité de certification organisationnelle	Droit Superviseur sur le conteneur Sécurité
Création d'objets Certificat de serveur	Droit Superviseur sur le conteneur du serveur Droit Lire sur l'attribut NDSPKI:Private Key de l'objet Autorité de certification organisationnelle

De plus, l'administrateur à la racine peut déléguer la responsabilité d'utiliser l'autorité de certification organisationnelle en assignant les droits suivants aux administrateurs de sous-conteneurs. Les administrateurs de sous-conteneurs doivent posséder les droits suivants pour pouvoir installer Novell eDirectory avec la sécurité SSL :

- Droit Lire sur l'attribut NDSPKI:Private Key de l'objet Autorité de certification organisationnelle situé dans le conteneur Sécurité.
- Droit Superviseur sur l'objet W0 situé dans le conteneur Sécurité, à l'intérieur de l'objet KAP.

Ces droits sont assignés à un groupe ou à un rôle dans le cadre duquel tous les utilisateurs administratifs sont définis. Pour obtenir la liste complète des droits requis pour effectuer des tâches spécifiques associées au serveur de certificats Novell, consultez la documentation en ligne de Novell Certificate Server (serveur de certificats Novell) (http://www.novell.com/documentation/beta/crt30/index.html).

Opérations eDirectory sécurisées sur les systèmes Linux, Solaris, AIX et HP-UX

eDirectory inclut des PKCS (Public Key Cryptography Services Services de cryptographie par clé publique) contenant le serveur de certificats Novell qui fournit des services d'infrastructure de clé publique (PKI), d'infrastructure cryptographique internationale Novell (NICI) et le serveurSAS*-SSL.

Les sections suivantes fournissent des informations sur l'exécution d'opérations sécurisées eDirectory :

- « Vérification de l'installation et de l'initialisation de NICI sur le serveur », page 87
- « Initialisation du moduleNICI sur le serveur », page 87
- « Démarrage du serveur de certificats (services PKI) », page 88
- « Arrêt du serveur de certificats (services PKI) », page 88

- « Création dun objet Autorité de certification organisationnelle », page 88
- « Création d'un objet Certificat de serveur », page 89
- « Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle », page 89

Pour obtenir des informations sur l'utilisation de l'autorité de certification externe, consultez le manuel *Novell Certificate Server Administration Guide (Guide d'administration du serveur de certificats Novell)* (http://www.novell.com/documentation/beta/crt30/index.html).

Vérification de l'installation et de l'initialisation de NICI sur le serveur

Vérifiez les conditions suivantes, qui indiquent si le moduleNICI a été installé et initialisé correctement :

- Le fichier /etc/nici.cfg existe.
- Le répertoire /var/novell/nici existe.
- Le fichier /var/novell/nici/primenici existe.

Si ces conditions ne sont pas remplies, suivez la procédure décrite à la section suivante, « Initialisation du moduleNICI sur le serveur ».

Initialisation du moduleNICI sur le serveur

1. Arrêtez le serveur eDirectory.
   - Sur les systèmes Linux, entrez

     `/etc/init.d/ndsd stop`
   - Sur les systèmes Solaris, entrez

     `/etc/init.d/ndsd stop`
   - Sur les systèmes AIX, entrez

     `/etc/ndsd stop`
   - Sur les systèmes HP-UX, entrez

     `/sbin/init.d/ndsd stop`

   IMPORTANT : Nous vous recommandons d'utiliser ndsmanage pour démarrer ou arrêter ndsd.
2. Vérifiez si le progiciel NICI est installé.
   - Sur les systèmes Linux, entrez

     `rpm -qa | grep nici`
   - Sur les systèmes Solaris, entrez

     `pkginfo | grep NOVLniu0`
   - Sur les systèmes AIX, entrez

     `lslpp -l | grep NOVLniu0`
   - Sur les systèmes HP-UX, entrez

     `swlist | grep NOVLniu0`

3 (Conditionnel) Si le progiciel NICI n'est pas installé, installez-le maintenant.

Vous ne pourrez pas continuer si le progiciel NICI n'est pas installé.

4 Copiez le fichier .nfk fourni avec le paquetage dans le répertoire /var/novell/nici.

Exécutez le programme /var/novell/nici/primenici.

5 Lancez le serveur eDirectory.

- Sur les systèmes Linux, entrez

  `/etc/init.d/ndsd start`

- Sur les systèmes Solaris, entrez

  `/etc/init.d/ndsd start`

- Sur les systèmes AIX, entrez

  `/etc/ndsd start`

- Sur les systèmes HP-UX, entrez

  `/sbin/init.d/ndsd start`

IMPORTANT : Nous vous recommandons d'utiliser ndsmanage pour démarrer ou arrêter ndsd.

Démarrage du serveur de certificats (services PKI)

Pour démarrer les services PKI, entrez la commande

`npki -1`.

Arrêt du serveur de certificats (services PKI)

Pour arrêter les services PKI, entrez la commande

`npki -u`.

Création dun objet Autorité de certification organisationnelle

1 Lancez Novell iManager.

2 Loguez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la section Creating an Organizational CA (Création d'une autorité de certification organisationnelle) (http://www.novell.com/documentation/beta/crt30/crtadmin/data/fbgccghh.html) dans le manuel *Novell Certificate Server Administration Guide (Guide d'administration du serveur de certificats Novell)*.

3 Cliquez sur le bouton Rôles et tâches  , sur PKI Certificate Management (Gestion des certificats PKI), puis sur Créer une autorité de certification.

L'assistant de création d'une autorité de certification organisationnelle apparaît. Suivez les instructions à l'écran pour créer l'objet. Pour plus d'informations sur une page spécifique de l'assistant, cliquez sur Aide.

REMARQUE : vous ne pouvez avoir qu'un seul objet Autorité de certification organisationnelle dans votre arborescence eDirectory.

Création d'un objet Certificat de serveur

Les objets Certificat de serveur sont créés dans le conteneur qui contient l'objet Serveur eDirectory. Selon vos besoins, vous pouvez créer un objet Certificat de serveur distinct pour chaque application prenant en charge la cryptographie sur le serveur, ou vous pouvez créer un objet Certificat de serveur pour toutes les applications utilisées sur ce serveur.

REMARQUE : les termes « objet Certificat de serveur » et « objet Matériel clé » (KMO Key Material Object) sont synonymes. Le nom de schéma de l'objet eDirectory est NDSPKI:Key Material.

1. Lancez Novell iManager.
2. Loguez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la section Creating Server Certificate Objects (Création d'objets Certificat de serveur) (http://www.novell.com/documentation/beta/crt30/crtadmin/data/fbgcdhec.html) dans le manuel *Novell Certificate Server Administration Guide (Guide d'administration du serveur de certificats Novell)*.
3. Cliquez sur le bouton Rôles et tâches  , sur PKI Certificate Management (Gestion des certificats PKI), puis sur Créer un certificat de serveur.

   L'assistant Créer un certificat de serveur apparaît. Suivez les instructions à l'écran pour créer l'objet. Pour plus d'informations sur une page spécifique de l'assistant, cliquez sur Aide.

Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle

Un certificat auto-signé peut être utilisé pour vérifier l'identité de l'autorité de certification organisationnelle ainsi que la validité d'un certificat signé par cette autorité.

À partir de la page de propriétés de l'autorité de certification organisationnelle, vous pouvez afficher les certificats et les propriétés associés à cet objet. À partir de la page de propriétés du certificat auto-signé, vous pouvez exporter le certificat auto-signé dans un fichier qui pourra être utilisé dans des applications prenant en charge la cryptographie.

Le certificat auto-signé qui réside dans l'autorité de certification organisationnelle est identique au certificat de racine approuvée d'un objet Certificat de serveur qui, lui, est signé par l'autorité de certification organisationnelle. Tout service qui reconnaît le certificat auto-signé de l'autorité de certification organisationnelle en tant que racine approuvée accepte un certificat utilisateur ou un certificat de serveur valide signé par cette autorité.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Modifier un objet.
3. Spécifiez le nom et le contexte d'un objet Autorité de certification organisationnelle, puis cliquez sur OK.

   Les objets Autorité de certification organisationnelle se trouvent dans le conteneur Sécurité.
4. Cliquez sur l'onglet Certificats, puis sur Certificat auto-signé.
5. Cliquez sur Exporter.

   L'assistant d'exportation du certificat apparaît. Suivez les instructions à l'écran pour exporter le certificat. Pour plus d'informations sur une page spécifique de l'assistant, cliquez sur Aide.

6 Dans la page Exporter le certificat - Résumé, cliquez sur Enregistrer le certificat exporté dans un fichier.

   Une fois enregistré dans un fichier, le certificat peut être importé en tant que racine approuvée dans une application prenant en charge la cryptographie.

7 Cliquez sur Fermer.

Insérez ce fichier dans toutes les opérations de ligne de commande qui établissent des connexions sécurisées avec eDirectory.

Synchronisation des heures réseau

La synchronisation horaire est un service qui assure la cohérence des heures sur les serveurs du réseau. Elle est assurée par le système d'exploitation du serveur et non par eDirectory. eDirectory gère sa propre heure interne pour garantir l'ordre approprié des paquets eDirectory, mais il obtient cette heure à partir du système d'exploitation du serveur.

Cette section est consacrée à l'intégration de la synchronisation horaire de NetWare dans celle de Windows, Linux, Solaris, AIX et HP-UX.

Synchronisation de l'heure sur les serveurs NetWare

Sur les réseaux IP et les réseaux à protocoles mixtes, les serveurs NetWare 5 communiquent l'heure aux autres serveurs utilisant le protocole IP. Les serveurs NetWare 5 utilisent timesync.nlm et le protocole NTP (Network Time Protocol) pour accomplir cette opération.

Sous NetWare 5 et 6, la synchronisation horaire utilise toujours timesync.nlm, que les serveurs emploient uniquement le protocole IP ou IPX™ ou les deux à la fois. Timesync.nlm est chargé lorsqu'un serveur est installé. Le protocole NTP peut être configuré via timesync.nlm.

Si votre réseau utilise également Windows, Linux, Solaris, AIX ou HP-UX, vous devez employer le protocole NTP pour synchroniser les serveurs, car il s'agit d'un standard en matière de synchronisation horaire.

Pour NetWare 3 et NetWare 4, des services horaires NTP de fabricants tiers sont disponibles.

Pour plus d'informations sur le logiciel de synchronisation horaire, consultez le site Web The Network Time Protocol (protocole NTP) (http://www.ntp.org).

NTP

NTP fait partie de la suite de protocole UDP, qui fait elle-même partie de la suite de protocole TCP/IP. Par conséquent, la suite protocole TCP/IP doit être chargée sur les ordinateurs qui utilisent NTP. Les ordinateurs de votre réseau qui ont accès à Internet peuvent obtenir l'heure des serveurs NTP via Internet.

NTP synchronise les horloges avec le temps universel (Universal Time Coordinated UTC), qui est la norme horaire internationale.

NTP introduit le concept de strate. Un serveur de strate 1 est relié à un appareil de mesure précise de l'heure, par exemple une horloge atomique. Un serveur de strate1 donne l'heure à un serveur de strate 2, et ainsi de suite.

Pour les serveurs NetWare 5 et 6, vous pouvez charger ntp.nlm pour implémenter la synchronisation horaireNTP via timesync.nlm. Lorsque le protocole NTP est configuré avec timesync.nlm sur un serveur IP, NTP devient la source horaire pour les serveurs IP et IPX. Dans ce cas, les serveurs IPX doivent être définis en tant que serveurs secondaires.

Pour plus d'informations sur la synchronisation horaire, consultez les manuels *Network Time Management Administration Guide (Guide d'administration de la gestion de l'heure réseau)* (http://www.novell.com/documentation/lg/nw65/time_enu/data/hl5k6r0y.html) et *Network Time Protocol Administration Guide (Guide d'administration du protocole NTP)* (http://www.novell.com/documentation/lg/nw65/ntp/data/aizwub2.html).

TIMESYNC.NLM

Timesync.nlm synchronise l'heure entre les serveurs NetWare. Vous pouvez utiliser timesync.nlm avec une source horaire externe, par exemple un serveurNTP Internet. Vous pouvez également configurer les postes de travail Novell Client™ pour mettre à jour leur horloge avec des serveurs en exécutant timesync.nlm.

Pour plus d'informations sur la synchronisation horaire, consultez le manuel *Network Time Management Administration Guide (Guide d'administration de la gestion de l'heure réseau)* (http://www.novell.com/documentation/lg/nw65/time_enu/data/hl5k6r0y.html).

Synchronisation de l'heure sur les serveurs Windows

Pour plus d'informations sur la synchronisation horaire pour des serveurs Windows NT et Windows 2000, consultez la documentation du système d'exploitation.

Synchronisation horaire sur les systèmes Linux, Solaris, AIX ou HP-UX

Vous pouvez utiliser le daemon xntpd NTP pour synchroniser l'heure sur les serveurs Linux, Solaris, AIX et HP-UX. xntpd est un daemon du système d'exploitation qui définit et gère la synchronisation entre l'heure du système et des serveurs d'heure standard sur Internet.

Pour plus d'informations sur l'exécution de xntpd sur un système AIX, reportez-vous à la section xntpd Daemon (Daemon xntpd) (http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/cmds/aixcmds6/xntpd.htm) dans le manuel *AIX Commands Reference (Référence des commandes AIX), Volume 6*.

Pour plus d'informations sur l'exécution de xntpd sur un système Solaris, consultez la page Web http://docs.sun.com/?p=/doc/806-0625/6j9vfim2v&a=view#xntpd-1m-indx-2 (http://docs.sun.com/?p=/doc/806-0625/6j9vfim2v&a=view#xntpd-1m-indx-2).

Pour plus d'informations sur l'exécution de xntpd sur un système HP-UX, consultez la page Web Configuring NTP (Configuration de NTP) (http://docs.hp.com/cgi-bin/fsearch/framedisplay?top=/hpux/onlinedocs/B2355-90147/B2355-90147_top.html&con=/hpux/onlinedocs/B2355-90147/00/00/58-con.html&toc=/hpux/onlinedocs/B2355-90147/00/00/58-toc.html&searchterms=ntp%7cconfiguring&queryid=20030922-153023).

Pour plus d'informations sur l'exécution de ntpd sur un système Linux, consultez le site Web ntpd - Network Time Protocol (NTP) Daemon (ntpd DaemonNTP) (http://www.eecis.udel.edu/~mills/ntp/html/ntpd.html).

Vérification de la synchronisation horaire

Pour vérifier que l'heure est synchronisée dans l'arborescence, exécutez DSRepair à partir d'un serveur de l'arborescence qui dispose au moins de droits en lecture/écriture sur l'objet Arborescence.

NetWare

1. Sur la console du serveur, chargez dsrepair.nlm.
2. Sélectionnez Synchronisation horaire.

   Pour obtenir de l'aide sur l'interprétation du journal, appuyez sur F1.

REMARQUE : la commande suivante vous aide à résoudre les problèmes de synchronisation horaire :

```
set timesync debug=7
```

Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration > Services Novell eDirectory.
2. Cliquez sur dsrepair.dlm > Démarrer.
3. Cliquez sur Réparer > Synchronisation horaire.

Linux, Solaris, AIX et HP-UX

1. Exécutez la commande suivante :

   ndsrepair -T

Conseils relatifs à la sécurité

Les liaisons LDAP doivent s'effectuer via une connexion sécurisée. Il est conseillé de toujours utiliser une connexion SSL/TLS. Dans le cas contraire, veillez aux points suivants :

- La clé transmise sur le réseau peut être détectée. Par conséquent, sécurisez physiquement le réseau de l'entreprise contre l'écoute électronique ou le « reniflage de paquets ».
- Gardez les serveurs à un emplacement sécurisé physiquement, uniquement accessible par le personnel autorisé.
- Si le produit est employé par des utilisateurs en dehors du pare-feu de l'entreprise, utilisez un réseau privé virtuel (VPN Virtual Private Network).
- Si un serveur est accessible à l'extérieur du réseau de l'entreprise, utilisez un pare-feu pour empêcher tout accès direct par un éventuel intrus.
- Vérifiez régulièrement les journaux d'audit.
- Attribuez les différentes responsabilités administratives à des personnes distinctes.
- Il est recommandé de désigner un serveur LDAP particulier pour la gestion Kerberos. Le nom de ce serveur peut être spécifié dans iManager.

IMPORTANT : l'utilisateur doit pouvoir accéder au serveur LDAP à l'aide du nom DNS au lieu de l'adresse IP du serveur, car la conversion de cette dernière en nom DNS n'est pas sécurisée.

3 Gestion des objets

Novell® eDirectory™ 8.8 comprend Novell iManager 2.5, une application de gestion réseau de type Web qui vous permet de gérer les objets de votre arborescence eDirectory. Pour comprendre les fonctions et avantages de Novell iManager, reportez-vous au manuel *Novell iManager 2.5 Administration Guide* (Guide d'administration de Novell iManager 2.5) (http://www.novell.com/documentation/imanager25/index.html).

La gestion des objets eDirectory implique la création, la modification et la manipulation de ces objets. Par exemple, vous pouvez avoir besoin de créer des comptes utilisateur et de gérer les droits Utilisateur. Avec Novell iManager, vous pouvez effectuer les opérations suivantes :

- Exécuter des opérations d'administration de base, telles que la navigation, la création, l'édition et l'organisation d'objets ;
- Créer des comptes utilisateur (notamment spécification d'un nom de login utilisateur et indication d'autres informations utilisées par eDirectory) ;
- Gérer des droits (assigner des droits, accorder des équivalences, bloquer des héritages et afficher des droits effectifs). Pour plus d'informations, reportez-vous à la section « Gestion des droits », page 65.
- Configurer une administration basée sur les rôles (définir les rôles de l'administrateur pour des applications d'administration spécifiques via l'objet RBS services basés sur le rôle).

Ce chapitre contient des informations sur les rubriques suivantes :

Tâches d'objet générales

Cette section décrit les procédures des tâches de base impliquées dans la gestion de l'arborescence eDirectory :

Recherche dans l'arborescence eDirectory

Le bouton Afficher les objets () dans Novell iManager vous permet de rechercher ou d'atteindre des objets dans votre arborescence eDirectory. Vous pouvez afficher la structure de votre arborescence et cliquer avec le bouton droit sur des objets pour effectuer des tâches. Les tâches disponibles dépendent du type d'objet que vous sélectionnez.

La page Sélecteur d'objet eDirectory dans Novell iManager vous permet également de rechercher ou d'atteindre des objets. Dans la plupart des champs d'entrée de Novell iManager, vous pouvez spécifier le nom de l'objet et son contexte ou cliquer sur le bouton Sélecteur d'objet  pour rechercher ou atteindre l'objet voulu. La sélection d'un objet dans la page Sélecteur d'objet eDirectory entraîne l'insertion de cet objet et de son contexte dans le champ d'entrée.

Cette section comprend les informations suivantes :

- « Utilisation du bouton Afficher les objets », page 94
- « Utilisation du bouton Sélecteur d'objet », page 95

Utilisation du bouton Afficher les objets

Procédez de la manière suivante pour rechercher les objets spécifiques à gérer.

- « Utilisation de Parcourir », page 94
- « Utilisation de Rechercher », page 95

Utilisation de Parcourir

1. Dans Novell iManager, cliquez sur le bouton Afficher les objets  .
2. Cliquez sur Parcourir.
3. Utilisez les options suivantes pour atteindre un objet :

Option	Description
	Permet de descendre d'un niveau dans l'arborescence.
	Permet de remonter d'un niveau dans l'arborescence.
Contexte	Permet de spécifier le nom du conteneur dont vous souhaitez afficher le contenu. Pour utiliser cette option, précisez le nom du conteneur souhaité, puis cliquez sur Appliquer.
Nom	Permet de spécifier le nom d'un objet. Vous pouvez utiliser l'astérisque (*) comme caractère générique dans ce champ. Par exemple, g* recherche tous les objets qui commencent par un g, tels que Grande-Bretagne ou Grégoire, et *té recherche toutes les entrées qui se terminent par té, telles que Société. Pour utiliser cette option, saisissez le nom souhaité, puis cliquez sur Appliquer.
Type	Permet de spécifier le type d'objet à rechercher. La valeur par défaut est Tous les types disponibles. Pour utiliser cette option, sélectionnez un type d'objet dans la liste déroulante, puis cliquez sur Appliquer.

4 Après avoir trouvé l'objet recherché, cliquez avec le bouton droit sur cet objet et sélectionnez une tâche dans la liste des tâches disponibles.

Utilisation de Rechercher

1 Dans Novell iManager, cliquez sur le bouton Afficher les objets  .

2 Cliquez sur Rechercher.

3 Dans le champ Contexte, indiquez le nom du conteneur dans lequel vous souhaitez effectuer la recherche.

Cliquez sur Rechercher dans les sous-conteneurs pour élargir la recherche aux sous-conteneurs appartenant au conteneur en cours.

4 Dans le champ Nom, indiquez le nom de l'objet à rechercher.

Vous pouvez utiliser l'astérisque (*) comme caractère générique dans ce champ. Par exemple, g* recherche tous les objets qui commencent par un g, tels que Grande-Bretagne ou Grégoire, et *té recherche toutes les entrées qui se terminent par té, telles que Société.

5 Sélectionnez le type d'objet à rechercher dans la liste déroulante Type.

6 Cliquez sur Rechercher.

7 Après avoir trouvé l'objet recherché, cliquez avec le bouton droit sur cet objet et sélectionnez une tâche dans la liste des tâches disponibles.

Utilisation du bouton Sélecteur d'objet

Procédez de la manière suivante pour rechercher les objets spécifiques à gérer.

- « Utilisation de Parcourir », page 95
- « Utilisation de Rechercher », page 96

Utilisation de Parcourir

1 Cliquez sur le bouton Sélecteur d'objet  dans une page de propriétés de iManager.

2 Cliquez sur Parcourir.

3 Utilisez les options suivantes pour atteindre un objet :

Option	Description
	Permet de descendre d'un niveau dans l'arborescence.
	Permet de remonter d'un niveau dans l'arborescence.
Rechercher dans	Indiquez le nom du conteneur dont vous souhaitez afficher le contenu, puis cliquez sur Appliquer.
Rechercher les objets nommés	Permet de spécifier le nom d'un objet. Vous pouvez utiliser l'astérisque (*) comme caractère générique dans ce champ. Par exemple, g* recherche tous les objets qui commencent par un g, tels que Grande-Bretagne ou Grégoire, et *té recherche toutes les entrées qui se terminent par té, telles que Société. Pour utiliser cette option, saisissez le nom souhaité, puis cliquez sur Appliquer.

Utilisation de Rechercher

1. Cliquez sur le bouton Sélecteur d'objet  dans une page de propriétés de iManager.
2. Cliquez sur Rechercher.
3. Dans le champ Démarrer la recherche dans, indiquez le nom du conteneur dans lequel vous souhaitez effectuer la recherche.

   Cliquez sur Rechercher dans les sous-conteneurs pour élargir la recherche aux sous-conteneurs appartenant au conteneur en cours.
4. Dans le champ Rechercher les objets nommés, indiquez le nom de l'objet à rechercher.

   Vous pouvez utiliser l'astérisque (*) comme caractère générique dans ce champ. Par exemple, g* recherche tous les objets qui commencent par un g, tels que Grande-Bretagne ou Grégoire, et *té recherche toutes les entrées qui se terminent par té, telles que Société.
5. Cliquez sur Rechercher.

Création d'un objet

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Créer un objet.
3. Sélectionnez un objet dans la liste des classes d'objet disponibles, puis cliquez sur OK.
4. Précisez les informations recherchées, puis cliquez sur OK.

   Les informations recherchées dépendent du type d'objet que vous créez. Pour plus dinformations, cliquez sur  .
5. Cliquez sur OK.

Modification des propriétés d'un objet

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Modifier un objet.
3. Spécifiez le nom et le contexte du ou des objets à modifier, puis cliquez sur OK.
4. Éditez les pages de propriétés souhaitées.

   Pour plus d'informations sur des pages de propriétés spécifiques, cliquez sur  .
5. Cliquez sur OK.

Copie d'objets

Cette option permet de créer un objet avec les mêmes valeurs d'attribut qu'un objet existant ou de copier les valeurs d'un objet sur un autre.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Copier un objet.
3. Dans le champ Copier à partir de cet objet, spécifiez le nom et le contexte de l'objet à copier.
4. Sélectionnez une des options suivantes :
   - Créer un objet et copier des valeurs d'attribut
   - Copier des valeurs d'attributs vers un objet existant

5 Si vous voulez copier des droits Liste de contrôle d'accès (ACL) sur l'objet que vous créez/modifiez, sélectionnez Copier les droits ACL.

   Le processus de copie des droits ACL peut être plus ou moins long en fonction de votre environnement système et réseau.

6 Cliquez sur OK.

Déplacement d'objets

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Administration de eDirectory > Déplacer un objet.

3 Dans le champ Nom de l'objet, spécifiez le nom et le contexte du ou des objets à déplacer.

4 Dans le champ Déplacer vers, indiquez le conteneur vers lequel transférer le ou les objets.

5 Pour créer un alias à l'ancien emplacement de chaque objet déplacé, sélectionnez Créer un alias à la place de l'objet déplacé.

   Si vous créez un alias, les opérations qui sont tributaires de l'ancien emplacement se poursuivent sans interruption jusqu'à ce que vous puissiez les mettre à jour pour qu'elles reflètent le nouvel emplacement.

6 Cliquez sur OK.

Suppression d'objets

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Administration de eDirectory > Supprimer un objet.

3 Spécifiez le nom et le contexte du ou des objets à supprimer.

4 Cliquez sur OK.

Attribution de nouveaux noms à des objets

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Administration de eDirectory > Renommer un objet.

3 Dans le champ Nom de l'objet, spécifiez le nom et le contexte de l'objet à renommer.

4 Dans le champ Nouveau nom de l'objet, spécifiez le nouveau nom de l'objet.

   N'entrez pas le contexte de l'objet dans ce champ.

5 Pour créer un alias pour l'objet renommé, sélectionnez Créer un alias à la place de l'objet renommé.

   Si vous créez un alias, les opérations qui dépendent de l'ancien nom de l'objet se poursuivent sans interruption jusqu'à ce que vous puissiez les mettre à jour pour qu'elles reflètent le nouveau nom.

6 Pour enregistrer l'ancien nom de l'objet, sélectionnez Enregistrer l'ancien nom.

   Ainsi, l'ancien nom est enregistré comme valeur supplémentaire (non officielle) de la propriété Nom. L'enregistrement de l'ancien nom permet aux utilisateurs de rechercher un objet à partir de son ancien nom. Une fois l'objet renommé, vous pouvez afficher l'ancien nom dans le champ Autre nom, dans l'onglet Identification générale pour cet objet.

7 Cliquez sur OK.

Gestion des comptes utilisateur

La configuration d'un compte utilisateur eDirectory implique la création d'un objet Utilisateur et la définition de propriétés permettant de contrôler le login et l'environnement informatique réseau de l'utilisateur. Vous pouvez utiliser un objet Modèle pour simplifier ces tâches.

Vous pouvez créer des scripts de login pour entraîner la connexion automatique des utilisateurs aux fichiers, imprimantes et autres ressources réseau nécessaires lors du login. Si plusieurs utilisateurs utilisent les mêmes ressources, vous pouvez placer les commandes de script de login dans les scripts de login du conteneur et du profil.

Cette section comprend les informations suivantes :

Création et modification des comptes utilisateur

Un compte utilisateur est un objet Utilisateur dans l'arborescence eDirectory. Un objet Utilisateur indique le nom de login d'un utilisateur et fournit d'autres informations utilisées par eDirectory pour contrôler l'accès utilisateur aux ressources réseau.

Cette section comprend les informations suivantes :

Création d'un objet Utilisateur

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilisateurs > Créer un utilisateur.
3. Spécifiez un nom d'utilisateur et un nom de famille pour l'utilisateur.
4. Indiquez un conteneur dans lequel l'utilisateur sera créé.
5. Indiquez éventuellement d'autres informations, puis cliquez sur OK.

   Pour plus d'informations sur les options disponibles, cliquez sur  .
6. Cliquez sur OK.

Modification d'un compte utilisateur

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilisateurs > Modifier un utilisateur.
3. Spécifiez le nom et le contexte du ou des utilisateurs à modifier, puis cliquez sur OK.

4 Éditez les pages de propriétés souhaitées.

   Pour plus d'informations sur des propriétés spécifiques, cliquez sur .

5 Cliquez sur OK.

Activation d'un compte utilisateur

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches .

2 Cliquez sur Utilisateurs > Activer un compte.

3 Spécifiez le nom et le contexte de l'utilisateur, puis cliquez sur OK.

Désactivation d'un compte utilisateur

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches .

2 Cliquez sur Utilisateurs > Désactiver un compte.

3 Spécifiez le nom et le contexte de l'utilisateur, puis cliquez sur OK.

Configuration des fonctions facultatives du compte

Après avoir créé un objet Utilisateur, vous pouvez configurer l'environnement informatique réseau de l'utilisateur et implémenter les fonctions de sécurité supplémentaire du login.

Configuration de l'environnement informatique réseau d'un utilisateur

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches .

2 Cliquez sur Utilisateurs > Modifier un utilisateur.

3 Spécifiez le nom et le contexte du ou des utilisateurs à modifier, puis cliquez sur OK.

4 Dans l'onglet Général, sélectionnez la page Environnement.

5 Complétez la page de propriétés.

   Pour plus d'informations sur des propriétés spécifiques, cliquez sur .

6 Cliquez sur OK.

Configuration de la sécurité supplémentaire du login pour un utilisateur

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches .

2 Cliquez sur Utilisateurs > Modifier un utilisateur.

3 Spécifiez le nom et le contexte du ou des utilisateurs à modifier, puis cliquez sur OK.

4 Dans l'onglet Restrictions, complétez les pages de propriétés désirées.

Pour plus d'informations sur une page, cliquez sur  .

Page	Description
Restrictions de mot de passe	Définit un mot de passe de login.
Restrictions de login	◆ Active ou désactive le compte. ◆ Limite le nombre de sessions de login simultanées. ◆ Définit une date de verrouillage et d'expiration du login.
Restrictions horaires	Limite les heures pendant lesquelles l'utilisateur peut être logué. Si vous définissez une restriction et si l'objet est logué lorsque l'heure limite arrive, le système affiche un avertissement indiquant cinq minutes, puis (après ces cinq minutes) délogue l'objet. Si l'utilisateur se logue à distance, reportez-vous à la section « Restrictions d'heures de login pour les utilisateurs distants », page 103.
Restrictions d'adresse	Limite les emplacements réseau (postes de travail) à partir desquels l'utilisateur peut se loguer. Si vous ne définissez pas de restrictions dans cette page, l'utilisateur peut se loguer à partir de n'importe quel emplacement réseau.
Solde de compte	Montant facturé pour l'usage du serveur par cet utilisateur.
Verrouillage en cas d'intrusion	Vous permet d'utiliser ce compte s'il a été verrouillé en raison de la détection d'un intrus. Pour gérer la configuration de la détection d'intrus, utilisez la page de propriétés Détection d'intrus du conteneur parent.

5 Cliquez sur OK.

Configuration de la détection d'intrus pour tous les utilisateurs dans un conteneur

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Administration de eDirectory > Modifier un objet.

3 Spécifiez le nom et le contexte d'un objet Conteneur, puis cliquez sur OK.

4 Dans l'onglet Général, sélectionnez la page Détection d'intrus.

5 Choisissez parmi les options suivantes :

Option	Description
Détecter les intrus	Active le système de détection d'intrus pour les comptes utilisateur situés dans le conteneur.
Tentatives de logins incorrects	Indique le nombre autorisé de tentatives consécutives de logins incorrects avant l'activation de la détection d'intrus. Si une personne utilise l'un des comptes utilisateur de ce conteneur pour se loguer et échoue consécutivement un nombre de fois supérieur à celui indiqué, le système active la détection d'intrus. Ce nombre est stocké dans la propriété Login Intruder Limit (Limite de tentatives de login d'intrus) du conteneur.
Fenêtre temporelle des tentatives d'intrusion	Précise la période pendant laquelle les logins incorrects consécutifs doivent avoir lieu pour que le système active la détection d'intrus. Entrez le nombre de jours, d'heures et de minutes.
Verrouillage du compte après détection	Indique si le système doit désactiver le login si la détection d'intrus est activée sur un compte utilisateur de ce conteneur. Si vous ne cochez pas cette case, le système n'effectue aucune opération lorsque la détection d'intrus est activée. Si vous cochez cette case et si le système verrouille un compte utilisateur en raison de la détection d'un intrus, vous pouvez déverrouiller le compte en désélectionnant la case Compte verrouillé dans la page de propriétés Verrouillage en cas d'intrusion de l'objet Utilisateur.
Jours, Heures, Minutes	Ces trois champs indiquent la durée pendant laquelle le login est désactivé lorsque la détection d'intrus est activée sur un compte utilisateur de ce conteneur. Entrez le nombre de jours, d'heures et de minutes de votre choix ou acceptez la valeur par défaut de 15minutes. Une fois la durée spécifiée écoulée, le système réactive le login pour le compte utilisateur. Le contenu de ces champs est stocké dans la propriété Durée du verrouillage en cas d'intrusion du conteneur.

6 Cliquez sur OK.

Configuration de scripts de login

Un script de login est une liste de commandes qui s'exécutent lorsqu'un utilisateur se logue. Il permet de connecter l'utilisateur à des ressources réseau telles que des fichiers et des imprimantes. Les scripts de login s'exécutent sur le poste de travail de l'utilisateur dans l'ordre suivant :

1. Script de login du conteneur
2. Script de login du profil
3. Script de login de l'utilisateur

Lors du login, si le système ne trouve pas l'un de ces scripts, il passe au suivant dans la liste. S'il n'en trouve aucun, il exécute un script par défaut qui assigne une unité de recherche à un dossier sur le serveur par défaut de l'utilisateur. Le serveur par défaut est défini dans la page de propriétés Environnement de l'objet Utilisateur.

Création d'un script de login

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Modifier un objet.
3. Spécifiez le nom et le contexte de l'objet sur lequel créer le script de login.

Pour que le script de login s'applique à	Créez-le sur
Un seul utilisateur	L'objet Utilisateur
Un ou plusieurs utilisateurs qui n'ont pas encore été créés	Un objet Modèle
Tous les utilisateurs d'un conteneur	L'objet Conteneur
Un groupe d'utilisateurs dans un ou plusieurs conteneurs	Un objet Profil

4. Cliquez sur OK.
5. Dans l'onglet Général, sélectionnez la page Script de login.
6. Entrez les commandes du script de login de votre choix.

   Pour plus d'informations, reportez-vous au manuel *Login Script Commands Guide (Commandes du script de login)* (http://www.novell.com/documentation/lg/noclienu/index.html).
7. Cliquez sur OK.

Assignation d'un profil à un utilisateur

Si vous associez un profil à un objet Utilisateur, le script de login du profil s'exécute pendant le login de l'utilisateur. Assurez-vous que l'utilisateur possède le droit Parcourir sur l'objet Profil et le droit Lire sur la propriété Script de login de l'objet Profil.

Pour plus d'informations, reportez-vous à la section « Affichage des droits effectifs sur un objet ou une propriété eDirectory », page 69.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilisateur > Modifier un utilisateur.
3. Spécifiez le nom et le contexte de l'objet Utilisateur sur lequel créer le script de login.
4. Cliquez sur OK.
5. Dans l'onglet Général, sélectionnez la page Script de login.
6. Pour associer un objet Profil à cet objet, entrez le nom et le contexte de l'objet Profil dans le champ Profil.
7. Cliquez sur OK.

Restrictions d'heures de login pour les utilisateurs distants

Dans la page de propriétés Restrictions horaires d'un objet Utilisateur, vous pouvez limiter les heures pendant lesquelles l'utilisateur peut être logué à eDirectory. (Par défaut, aucune restriction d'heure de login n'est définie.) Si vous définissez une restriction d'heure de login et si l'utilisateur est logué lorsque l'heure limite arrive, le système affiche un avertissement invitant l'utilisateur à se déloguer dans les cinq minutes. Si l'utilisateur est encore logué après ces cinq minutes, le système le délogue automatiquement et toutes les données non enregistrées sont perdues.

Si un utilisateur se logue à distance à partir d'un fuseau horaire différent de celui du serveur qui traite la requête de login, les restrictions d'heures de login éventuellement définies pour l'utilisateur sont modifiées en fonction du décalage horaire. Par exemple, si vous interdisez à un utilisateur de se loguer le lundi de 1à 6heures du matin et s'il se logue à distance à partir d'un fuseau horaire comptant une heure d'avance par rapport au serveur, la restriction s'applique alors entre 2 et 7 heures du matin pour cet utilisateur.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilisateurs > Modifier un utilisateur.
3. Spécifiez le nom et le contexte du ou des utilisateurs à modifier, puis cliquez sur OK.
4. Dans l'onglet Restrictions, cliquez sur Restrictions horaires.
5. Choisissez parmi les options suivantes :

Option	Description
Grille horaire	Chaque cellule de la grille horaire représente une demi-heure dans un jour de la semaine. Les cellules rouges représentent les heures de restriction (heures pendant lesquelles l'objet ne peut pas être logué). Les cellules grises représentent les heures sans restriction (heures pendant lesquelles l'objet peut être logué). Pour créer une restriction horaire, cliquez sur les heures de votre choix pour les rendre gris foncé. Vous pouvez aussi sélectionner plusieurs heures en maintenant la touche Maj enfoncée, en cliquant sur une cellule, puis en faisant glisser le curseur sur les cellules correspondantes. Les restrictions d'heures de login que vous définissez sont stockées dans la propriété Login Allowed Time Map (Tableau des horaires de login autorisés) de cet objet.
Ajouter une restriction horaire	Pour ajouter une restriction horaire, sélectionnez une cellule grise, puis cochez cette option.
Supprimer une restriction horaire	Pour supprimer une restriction horaire, sélectionnez une cellule rouge, puis cochez cette option.
Mettre à jour	Cliquez sur ce bouton pour activer la sélection.
Réinitialiser	Cliquez sur ce bouton pour que la grille horaire retrouve son état antérieur à l'ouverture de cette page de propriétés.

6. Cliquez sur OK.

Suppression de comptes utilisateur

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilisateurs > Supprimer un utilisateur.
3. Spécifiez le nom et le contexte du ou des utilisateurs à supprimer.
4. Cliquez sur OK.

Configuration des services basés sur le rôle

Novell iManager permet aux administrateurs d'assigner des responsabilités particulières aux utilisateurs et de leur présenter uniquement les outils (et les droits associés) nécessaires à l'exécution de celles-ci. Cette fonctionnalité s'appelle *Services basés sur le rôle (RBS)*.

Les services basés sur le rôle permettent aux administrateurs de limiter l'utilisateur à un groupe spécifique de fonctions, appelées *tâches*, et à des d'objets déterminés par le regroupement de tâches, appelés *rôles*. Les tâches que voit un utilisateur à l'écran lorsqu'il accède à iManager dépendent de ses assignations de rôles dans eDirectory. Seules les tâches qui lui sont assignées sont affichées. L'utilisateur n'a pas besoin de parcourir l'arborescence pour trouver un objet à gérer, le plug-in de iManager pour cette tâche présente les outils et l'interface nécessaires à sa réalisation.

Vous pouvez assigner plusieurs rôles à un seul utilisateur et un même rôle à plusieurs utilisateurs.

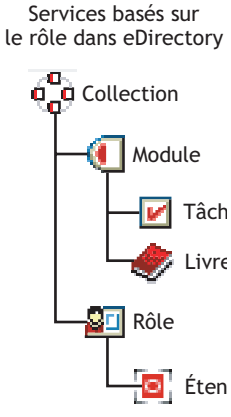
Les services basés sur le rôle sont représentés par des objets définis dans eDirectory. Le schéma eDirectory de base est étendu lors de l'installation de iManager. Les types d'objet RBS sont listés dans le tableau ci-dessous :

Objet	Description
 rbsCollection	Objet Conteneur qui contient tous les objets Rôle et Module RBS. Les objets rbsCollection sont les conteneurs du niveau le plus élevé pour tous les objets RBS. Une arborescence peut contenir autant d'objets rbsCollection que nécessaire. Ces objets ont des « propriétaires », autrement dit des utilisateurs qui disposent de droits de gestion sur la collection. Les objets rbsCollection peuvent être créés dans l'un des conteneurs suivants : ◆ Pays ◆ Domaine ◆ Lieu ◆ Organisation ◆ Unité organisationnelle
 rbsRole	Objet Conteneur qui précise les tâches que les utilisateurs (membres) sont autorisés à effectuer. La définition d'un rôle comprend la création d'un objet rbsRole et la spécification des tâches que le rôle peut effectuer. Les membres d'un rôle peuvent être des utilisateurs, groupes, organisations ou unités organisationnelles et sont associés à un rôle dans une étendue spécifique de l'arborescence. Les objets rbsTask et rbsBook sont assignés à des objets rbsRole. Les objets rbsRole ne peuvent être créés que dans des conteneurs rbsCollection.

Objet	Description
rbsModule	Objet Conteneur qui contient les objets rbsTask et rbsBook. Les objets rbsModule ont un attribut de nom de module qui représente le nom du produit définissant les tâches ou les livres (par exemple, Utilitaires de maintenance eDirectory, Gestion NMAS ou Accès au serveur de certificats Novell). Les objets rbsModule ne peuvent être créés que dans des conteneurs rbsCollection.
rbsTask	Objet Feuille qui représente une fonction spécifique, telle que la réinitialisation des mots de passe de login. Les objets rbsTask se situent exclusivement dans des conteneurs rbsModule.
rbsBook	Objet Feuille contenant une liste de pages assignées au livre. Un objet rbsBook peut être assigné à un ou plusieurs rôles et à un ou plusieurs types de classe d'objet. Les objets rbsBook se situent exclusivement dans des conteneurs rbsModule.
rbsScope	Objet Feuille utilisé pour les assignations ACL (à la place des assignations pour chaque objet Utilisateur). Les objets rbsScope représentent le contexte dans l'arborescence dans lequel un rôle sera exécuté et sont associés aux objets rbsRole. Ils héritent de la classe Groupe. Les objets Utilisateur sont assignés à un objet rbsScope. Ces objets ont une référence à l'étendue de l'arborescence à laquelle ils sont associés. Ces objets sont créés de manière dynamique lorsqu'ils sont nécessaires, puis supprimés automatiquement quand ils sont devenus superflus. Ils sont situés exclusivement dans des conteneurs rbsRole. **Avertissement :** ne modifiez jamais la configuration d'un objet Étendue. En effet, ceci peut avoir de graves conséquences et risque d'endommager le système.

Les objets RBS sont situés dans l'arborescence eDirectory, comme l'indique le schéma suivant :

Figure 22 Objets RBS dans l'arborescence eDirectory



Définition des rôles RBS

Les rôles RBS spécifient les tâches que les utilisateurs sont autorisés à effectuer. La définition d'un rôle RBS comprend la création d'un objet rbsRole et la spécification des tâches que le rôle peut effectuer et des objets Utilisateur, Groupe ou Conteneur qui peuvent effectuer ces tâches. Dans certains cas, les plug-ins de Novell iManager (livrés avec le produit) fournissent des rôles RBS prédéfinis que vous pouvez modifier.

Les tâches que les rôles RBS peuvent effectuer sont présentées sous la forme d'objets rbsTask dans votre arborescence eDirectory. Le système ajoute automatiquement ces objets lors de l'installation des produits. Ils sont organisés en un ou plusieurs objets rbsModules ; il s'agit de conteneurs qui correspondent aux différents modules fonctionnels du produit.

Pour plus d'informations sur l'assignation de membres à un rôle, reportez-vous à la section « Assignation de membres à un rôle RBS et définition d'une étendue », page 106.

Création d'un objet Rôle

Utilisez l'Assistant Créer un rôle iManager pour créer un objet rbsRole. Il est recommandé de créer cet objet rbsRole dans le même conteneur rbsCollection que les autres objets rbsRole (par exemple, le conteneur Collection de services basés sur le rôle).

1. Dans Novell iManager, cliquez sur le bouton Configurer  .
2. Cliquez sur Configuration des rôles > Créer un rôle iManager.
3. Suivez les instructions de l'Assistant Créer un rôle iManager.

Pour plus d'informations sur l'ajout de membres aux rôles, reportez-vous à la section « Définition de tâches RBS personnalisées », page 107.

Modification des tâches associées à un rôle

Un groupe de tâches disponibles est associé à chaque rôle RBS. Vous pouvez déterminer quelles tâches sont assignées à un rôle particulier en ajoutant ou en supprimant des tâches si nécessaire.

1. Dans Novell iManager, cliquez sur le bouton Configurer  .
2. Cliquez sur Configuration des rôles > Modifier les rôles iManager.
3. Pour ajouter ou supprimer des tâches pour un rôle, cliquez sur le bouton Modifier les tâches  situé à gauche du rôle à modifier.
4. Ajoutez ou supprimez des tâches dans la liste des tâches assignées.
5. Cliquez sur OK.

Assignation de membres à un rôle RBS et définition d'une étendue

Après avoir défini les rôles RBS nécessaires dans votre organisation, vous pouvez assigner des membres à chaque rôle. Ainsi, vous spécifiez l'étendue de l'exercice des fonctions du rôle pour chaque membre. L'étendue correspond à l'emplacement ou au contexte dans l'arborescence eDirectory dans lequel ce rôle peut être effectué.

Vous pouvez assigner un utilisateur à un rôle de différentes manières:

- Directement
- Via des assignations de groupes et de groupes dynamiques. Si un utilisateur est membre d'un groupe ou d'un groupe dynamique assigné à un rôle, il a accès à ce rôle.
- Via des assignations de rôles organisationnels. Si un utilisateur est titulaire d'un rôle organisationnel assigné à un rôle, il a accès à ce rôle.
- Via des assignations de conteneurs. Un objet Utilisateur a accès à tous les rôles auxquels son conteneur parent est assigné. Cela concerne également d'autres conteneurs jusqu'à la racine de l'arborescence.

Un utilisateur peut être associé à un rôle plusieurs fois, chaque fois avec une étendue différente. Vous pouvez également assigner la même tâche à plusieurs membres.

Pour assigner des membres à un rôle et définir une étendue, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Configurer  .
2. Cliquez sur Configuration des rôles > Modifier les rôles iManager.
3. Pour ajouter ou supprimer des membres pour un rôle, cliquez sur le bouton Modifier les membres  situé à gauche du rôle à modifier.
4. Dans le champ Nom, spécifiez un nom d'objet (objet Utilisateur, Groupe ou Conteneur) et un contexte.
5. Dans le champ Étendue, spécifiez un nom d'objet Organisation ou Unité organisationnelle et un contexte pour cet objet.
6. Cliquez sur Ajouter, puis sur OK.

Suppression d'un objet Services basés sur le rôle

1. Dans Novell iManager, cliquez sur le bouton Configurer  .
2. Cliquez sur Configuration des rôles > Supprimer un rôle.
3. Spécifiez le nom et le contexte du rôle RBS à supprimer.
4. Cliquez sur OK.

Définition de tâches RBS personnalisées

- « Création d'une tâche iManager », page 107
- « Création d'une tâche d'administration du serveur », page 108
- « Modification de l'assignation des rôles », page 108
- « Suppression d'une tâche », page 108

Création d'une tâche iManager

1. Dans Novell iManager, cliquez sur le bouton Configurer  .
2. Cliquez sur Configuration des tâches > Créer une tâche iManager.
3. Suivez les instructions du Générateur de tâches pour créer une tâche personnalisée.

Création d'une tâche d'administration du serveur

Utilisez l'assistant de création d'une tâche d'administration du serveur pour créer des tâches personnalisées afin d'accéder aux services d'un serveur. L'administrateur système doit vérifier que le service est disponible sur le serveur.

1. Dans Novell iManager, cliquez sur le bouton Configurer .
2. Cliquez sur Configuration des tâches > Créer une tâche d'administration du serveur.
3. Suivez les instructions de l'Assistant de création d'une tâche d'administration du serveur.

Modification de l'assignation des rôles

1. Dans Novell iManager, cliquez sur le bouton Configurer .
2. Cliquez sur Configuration des tâches > Modifier l'assignation des rôles.
3. Spécifiez le nom et le contexte de la tâche à modifier, puis cliquez sur Suivant.
4. Déplacez les rôles de votre choix de la colonne Rôles disponibles vers la colonne Rôles assignés.
5. Cliquez sur OK.

Suppression d'une tâche

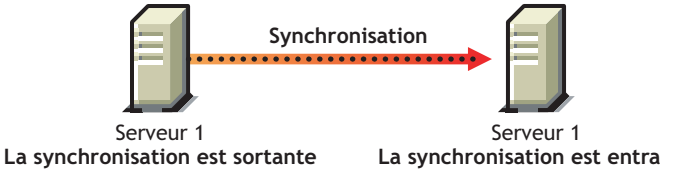
1. Dans Novell iManager, cliquez sur le bouton Configurer .
2. Cliquez sur Configuration des tâches > Supprimer la tâche.
3. Spécifiez le nom et le contexte de la tâche à supprimer, puis cliquez sur OK.

Synchronisation

La synchronisation désigne le transfert d'informations sur l'annuaire d'une réplique vers une autre, pour garantir la cohérence des deux partitions. eDirectory garde automatiquement les serveurs de l'anneau de répliques synchronisés.

La synchronisation peut être entrante ou sortante. Par exemple, si les modifications de données doivent être synchronisées à partir des serveurs1 et 2, le terme *sortant* désigne le processus de synchronisation envoyé du serveur1 au serveur 2, tandis que le terme *entrant* désigne le processus de synchronisation reçu du serveur1 par le serveur 2.

Figure 23 Synchronisations entrante et sortante



Il existe deux types de synchronisation:

- la synchronisation normale ou synchronisation des répliques et
- la synchronisation de priorité (dans eDirectory version 8.8 ou ultérieure).

Le tableau ci-dessous compare les synchronisations normale et de priorité:

Tableau 1 Comparaison entre la synchronisation normale (ou des répliques) et la synchronisation de priorité

Synchronisation normale ou synchronisation des répliques	Synchronisation de priorité
Se déclenche en cas de modifications de données sur n'importe quel serveur de l'anneau de répliques. Pour plus d'informations, reportez-vous à la section « Synchronisation normale ou des répliques », page 111.	Se déclenche uniquement en cas de modifications des données identifiées comme essentielles. Pour plus d'informations, reportez-vous à la section « Synchronisation de priorité », page 113.
Une fois les données modifiées, les changements sont enregistrés dans la mémoire tampon. La synchronisation normale débute environ 30secondes après l'enregistrement des modifications.	Les changements apportés aux données essentielles ne sont pas enregistrés dans la mémoire tampon. La synchronisation de priorité débute immédiatement après la modification des données.
Principale synchronisation dans eDirectory. Elle s'opère, que la synchronisation de priorité soit activée ou non.	Processus complémentaire à la synchronisation normale. Bien que les attributs essentiels soient synchronisés par la synchronisation de priorité, ils le sont à nouveau par la synchronisation normale.
Peut s'opérer entre serveurs eDirectory 8.8 ou avec des serveurs qui hébergent des versions antérieures de eDirectory.	S'opère uniquement entre des serveurs eDirectory 8.8 contenant la même partition.
N'échoue jamais à cause de ses caractéristiques. Pour plus d'informations, reportez-vous à la section « Caractéristiques de la synchronisation », page 109.	Si la synchronisation de priorité échoue, les modifications des données essentielles sont synchronisées par la synchronisation normale. Pour plus d'informations, reportez-vous à la section « Situations d'échec de la synchronisation de priorité », page 119.

Caractéristiques de la synchronisation

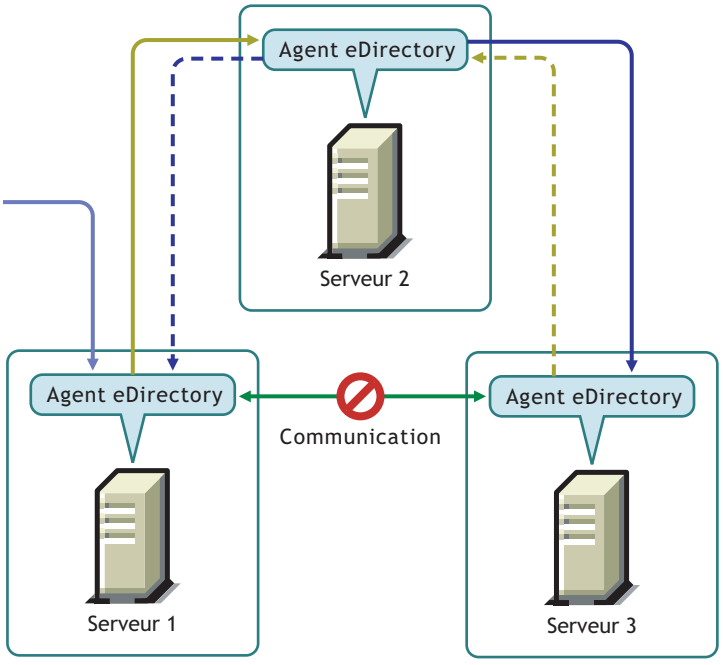
La synchronisation dans eDirectory :

- est transitive ;
- gère le modèle de transactions d'objets ;
- comporte des tampons horaires tels que le vecteur de transition (Transitive Vector), l'heure à laquelle les dernières modifications sont parvenues à la réplique locale (local received up to) et l'heure à laquelle elles sont parvenues à la réplique distante(remote received up to).

Synchronisation transitive

La synchronisation dans eDirectory est transitive. Cela signifie que eDirectory synchronise les modifications apportées aux données sans que l'agent eDirectory doive contacter directement tous les autres agents de l'anneau de répliques pour synchroniser les changements avec chacun d'entre eux.

Figure 24 Synchronisation transitive



Par exemple, si vous modifiez des données sur le serveur1, les changements sont synchronisés du serveur1 vers le serveur2, puis du serveur2 vers le serveur3. Si le serveur1 n'a pas pu entrer directement en contact avec le serveur3 en raison d'un problème de communication, ce dernier reçoit malgré tout les modifications par le biais du serveur2. Il le signale au serveur2 qui, à son tour, indique au serveur1 que le serveur3 et lui-même sont synchronisés.

Modèle de transactions d'objets

La synchronisation dans eDirectory gère le modèle de transactions d'objets, une norme pour les annuaires compatibles X.500 et LDAP. Le modèle de transactions d'objets signifie que toutes les transactions précédentes doivent être synchronisées avant d'en synchroniser de nouvelles.

Imaginons, par exemple, que vous avez apporté les modifications D1, D2 et D3 aux données d'un serveur. En raison d'une défaillance réseau, ces modifications ne sont pas synchronisées sur les autres serveurs. Si vous apportez ensuite une modification D4 sur le serveur, celle-ci ne sera synchronisée qu'après la synchronisation de D1, D2 et D3 sur tous les serveurs de l'anneau de répliques.

Transitive Vector

Un vecteur de transition est un tampon horaire pour une réplique. Ce tampon est constitué d'une représentation du nombre de secondes écoulées depuis un point de référence historique commun (1erjanvier1970), du numéro de réplique et du numéro d'événement en cours. Par exemple :

s3D35F377 r02 e002

Pour plus d'informations, reportez-vous à la section « Vecteurs de transition et processus de vérification de la restauration », page 399.

Local Received Up To

Local Received Up To (LRUT) désigne l'heure à laquelle les dernières modifications sont parvenues à la réplique locale.

Pour plus d'informations, reportez-vous à la section « Accès aux objets de votre arborescence », page 209.

Remote Received Up To

Remote Received Up To (RRUT) désigne l'heure à laquelle les dernières modifications sont parvenues à la réplique distante.

Pour plus d'informations, reportez-vous à la section « Accès aux objets de votre arborescence », page 209.

Synchronisation normale ou des répliques

La synchronisation normale, également appelée synchronisation des répliques, désigne l'un des deux processus de synchronisation dans eDirectory. Elle synchronise toutes les modifications apportées aux données d'un serveur avec les autres serveurs de l'anneau de répliques.

La synchronisation normale s'opère sur tous les serveurs hébergeant une quelconque version de eDirectory, qui possèdent la même partition.

Pour plus d'informations, reportez-vous à la section « Gestion des répliques », page 137.

Vous pouvez activer ou désactiver la synchronisation normale en activant ou désactivant les synchronisations entrante et sortante dans Novell iMonitor. Par défaut, ces deux formes de synchronisation sont activées. Pour que les modifications apportées aux données soient synchronisées sur les différents serveurs par le biais de la synchronisation normale, vous devez configurer les paramètres de synchronisation dans iMonitor. Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agentDS », page 205.

Avec la synchronisation normale, lorsque vous modifiez des données, les changements sont enregistrés dans la mémoire tampon avant d'être synchronisés sur les autres serveurs. Vous pouvez consulter l'état de synchronisation des serveurs de votre configuration dans iMonitor. Pour plus d'informations, reportez-vous à la section « Accès aux objets de votre arborescence », page 209.

La synchronisation normale est transitive et gère le modèle de transactions d'objets. Pour plus d'informations, reportez-vous aux sections « Synchronisation transitive » et « Modèle de transactions d'objets » à la page 101.

Configuration de la synchronisation normale

Vous pouvez configurer la synchronisation normale à l'aide de Configuration de l'agent sous Synchronisation de l'agent dans iMonitor.

Cette section fournit les informations suivantes :

- « Activation/désactivation de la synchronisation normale », page 112
- « Activation/désactivation du cache en ligne », page 112
- « Threads de synchronisation », page 112
- « Méthode de synchronisation », page 112

Activation/désactivation de la synchronisation normale

Vous pouvez activer ou désactiver la synchronisation normale en activant ou désactivant les synchronisations entrante et sortante dans iMonitor. Pour plus d'informations, reportez-vous à la section to « Contrôle et configuration de l'agentDS », page 205.

La synchronisation sortante est activée par défaut. Si l'option est désactivée pour un serveur, les modifications apportées aux données sur ce serveur ne seront pas synchronisées avec les autres serveurs. Vous pouvez indiquer, en heures, le délai pendant lequel la synchronisation sortante doit être désactivée. La valeur par défaut de ce paramètre est 24heures, ce qui correspond également au délai maximal autorisé. Une fois le délai spécifié écoulé, les modifications apportées aux données sur ce serveur sont synchronisées avec les autres serveurs.

La synchronisation entrante est activée par défaut. Si l'option est désactivée pour un serveur, les modifications apportées aux données sur d'autres serveurs ne seront pas synchronisées avec ce serveur.

Activation/désactivation du cache en ligne

Le cache de changement en ligne peut être activé ou désactivé pour un serveur. Cette option ne peut toutefois être désactivée que si la synchronisation sortante est elle-même désactivée. Si la synchronisation sortante est activée, le cache de changement en ligne l'est également.

La désactivation du cache de changement en ligne rend ce cache non valide pour la réplique concernée ; il apparaît avec un drapeau non valide dans Configuration de l'agent > Partitions. Si le cache de changement en ligne est réactivé, le drapeau non valide est supprimé lors de la reconstruction du cache.

Threads de synchronisation

Pour la synchronisation sortante, vous devez configurer les threads de synchronisation. iMonitor vous permet de spécifier le nombre de threads de synchronisation à l'aide de Configuration de l'agent sous Synchronisation de l'agent. Les valeurs prises en charges sont comprises entre 1 et 16.

Pour plus d'informations, reportez-vous à la section to « Contrôle et configuration de l'agentDS », page 205.

Méthode de synchronisation

En principe, eDirectory choisit automatiquement la méthode en fonction du nombre de répliques et de partenaires de réplication. Les différentes méthodes de synchronisation sont les suivantes :

- **Par partition :** les modifications apportées aux données sont synchronisées simultanément avec les autres répliques, à l'aide de plusieurs threads. Ainsi, si vous apportez les modifications D1, D2 et D3 aux données de la réplique R1 et que celles-ci doivent être synchronisées avec les répliques R2 et R3, elles le sont simultanément.
- **Par serveur :** les modifications apportées aux données sont synchronisées séquentiellement par le biais d'un seul thread. Si vous apportez les modifications D1, D2 et D3 aux données de la répliqueR1 et que celles-ci doivent être synchronisées avec les répliques R2 et R3, D1 est d'abord synchronisée avec R2 et R3, puis D2, et ainsi de suite.
- **Par ajustement dynamique :** eDirectory choisit automatiquement la méthode de synchronisation en fonction des ressources système allouées.

iMonitor vous permet de spécifier la méthode de synchronisation à l'aide de Configuration de l'agent sous Synchronisation de l'agent. Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agentDS », page 205.

Synchronisation de priorité

La synchronisation de priorité désigne l'un des deux processus de synchronisation dans eDirectory. Dans eDirectory 8.8 ou version ultérieure, elle permet de synchroniser les données essentielles immédiatement, sans devoir attendre la synchronisation normale.

La synchronisation de priorité vient compléter le processus de synchronisation normale dans eDirectory. Contrairement à cette dernière, pour la synchronisation de priorité, les changements ne sont pas enregistrés dans la mémoire tampon avant d'être synchronisés sur les autres serveurs, ce qui accélère le processus.

La synchronisation de priorité est activée par défaut. Pour plus d'informations, reportez-vous à la section « Activation/désactivation de la synchronisation de priorité entrante/sortante », page 114.

Pour synchroniser les modifications apportées aux données essentielles par le biais de la synchronisation de priorité :

1. Spécifiez le nombre de threads pour la synchronisation de priorité.

   Pour plus d'informations, reportez-vous à la section « Synchronisation de priorité – Threads », page 114.

2. Spécifiez la taille de la file d'attente pour la synchronisation de priorité.

   Pour plus d'informations, reportez-vous à la section « Synchronisation de priorité – Taille de la file d'attente », page 114.

3. Créez et définissez une règle de synchronisation de priorité en identifiant les attributs essentiels à synchroniser en priorité.

   Pour plus d'informations, reportez-vous à la section « Création et définition d'une règle de synchronisation de priorité », page 116.

4. Appliquez la règle de synchronisation de priorité à une ou plusieurs partitions.

   Pour plus d'informations, reportez-vous à la section « Application d'une règle de synchronisation de priorité », page 117.

Le processus de synchronisation de priorité vise uniquement la synchronisation des modifications apportées aux attributs essentiels. Si vous créez un objet qui comporte des attributs essentiels, il n'est pas synchronisé avec les autres serveurs.

La synchronisation de priorité gère le modèle de transactions d'objets. Dès lors, si des données non essentielles ont été modifiées et ne sont pas encore synchronisées et que des données essentielles sont changées pour la même entrée, les premières et les secondes sont synchronisées simultanément.

Imaginons, par exemple, qu'un utilisateur possède les attributs Salaire, N°employé, Adresse et N°unité, et que vous identifiez Salaire et Adresse comme essentiels. N°employé et N°unité ont été modifiés, mais ne sont pas encore synchronisés. Lorsque les modifications de Salaire et Adresse sont synchronisées par le biais de la synchronisation de priorité, N°employé et N°unité le sont également, bien qu'ils ne soient pas identifiés comme essentiels.

Cette section fournit les informations suivantes :

Activation/désactivation de la synchronisation de priorité entrante/sortante

Dans eDirectory 8.8 ou version ultérieure, vous pouvez activer ou désactiver la synchronisation de priorité entrante et/ou sortante à l'aide de iMonitor. Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agentDS », page 205.

La synchronisation de priorité entrante est activée par défaut. Si l'option est désactivée pour un serveur, les modifications apportées aux données essentielles sur les autres serveurs ne sont pas synchronisées avec ce serveur par le biais de la synchronisation de priorité. Elles le sont toutefois par le processus de synchronisation normale.

La synchronisation de priorité sortante est activée par défaut. Si l'option est désactivée pour un serveur, les modifications apportées aux données essentielles sur ce serveur ne sont pas synchronisées avec les autres serveurs par le biais de la synchronisation de priorité. Elles le sont toutefois par le processus de synchronisation normale.

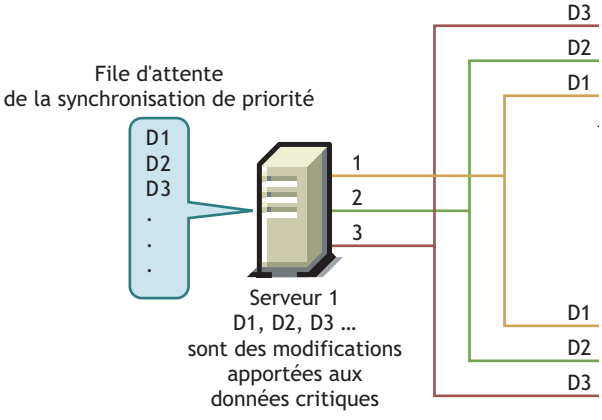
Synchronisation de priorité – Threads

Vous devez configurer le nombre de threads à utiliser pour la synchronisation de priorité sortante. Dans iMonitor, vous pouvez spécifier le nombre de threads de la synchronisation de priorité à l'aide de Configuration de l'agent sous Synchronisation de l'agent. Pour plus d'informations, reportez-vous à la section to « Contrôle et configuration de l'agentDS », page 205. Les valeurs prises en charges sont comprises entre 1 et 32. La valeur par défaut est 4.

Synchronisation de priorité – Taille de la file d'attente

Ce paramètre indique le nombre maximal d'entrées essentielles modifiées que la file d'attente peut contenir avant de les synchroniser. Dès que vous modifiez les entrées essentielles, elles s'ajoutent dans la file d'attente de la synchronisation de priorité et sont synchronisées l'une après l'autre. Imaginons, par exemple, que D1, D2 et D3 sont les entrées essentielles modifiées sur le serveur 1 et qu'elles doivent être synchronisées sur les serveurs 2 et 3 par la synchronisation de priorité. D1 est synchronisée avec les serveurs 2 et 3, puis D2 est synchronisée et enfin, D3. Si une entrée antérieure de la file d'attente n'est pas correctement synchronisée avec l'un des serveurs, cela n'affecte pas la synchronisation des autres entrées.

Figure 25 File d'attente de la synchronisation de priorité



Vous pouvez spécifier la taille de la file d'attente pour la synchronisation de priorité dans iMonitor à l'aide de Configuration de l'agent sous Synchronisation de l'agent. Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agentDS », page 205.

Lors d'un processus de synchronisation de priorité, si plusieurs modifications sont apportées en peu de temps, la file d'attente risque d'atteindre sa taille maximale. Dans ce cas, elle expire et une nouvelle file d'attente est formée. Les modifications dans l'ancienne file d'attente qui n'ont pas encore été synchronisées le seront par la synchronisation normale.

La taille de la file d'attente pour la synchronisation de priorité peut être comprise entre 0 et 232 - 1. Par défaut, elle est de 232 - 1. Si la taille de la file d'attente de la synchronisation de priorité est définie sur 0, les modifications ne sont pas synchronisées par cette synchronisation. Elles le sont toutefois par la synchronisation normale.

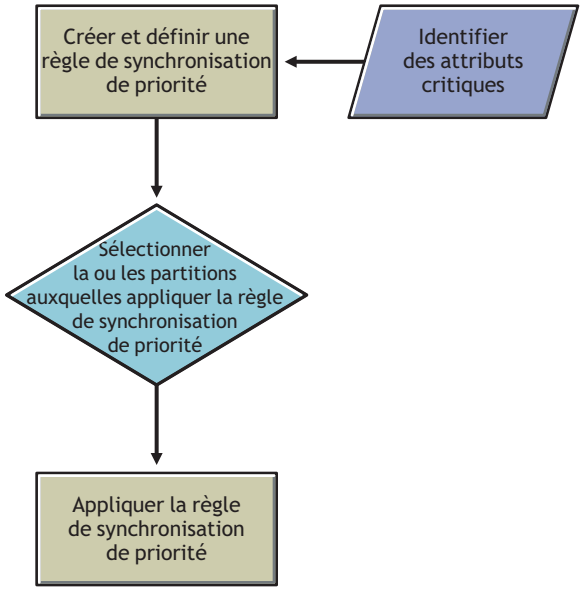
La valeur -1 implique une taille de file d'attente illimitée. -1 correspond à 232 - 1. Si une valeur négative est spécifiée, -3 par exemple, cela signifie -3 = -1-2, ce qui correspond à 232 - 1-2.

Gestion des règles de synchronisation de priorité

Pour gérer la synchronisation de priorité, vous pouvez créer et définir des règles et les appliquer à des partitions via iManager ou LDAP. Vous définissez une règle de synchronisation de priorité en identifiant les attributs qui sont essentiels.

REMARQUE : les plug-ins sont uniquement disponibles dans Novell iManager 2.5 et version ultérieure.

Figure 26 Processus de synchronisation de priorité



Par exemple, si les attributs Mot de passe et Numéro de compte sont essentiels, vous pouvez créer une règle de synchronisation de priorité PS1 qui contient ces attributs. Vous pouvez ensuite appliquer cette règle à une partition P1. Si vous modifiez le mot de passe ou le numéro de compte d'une entrée sur un serveur, les changements sont immédiatement synchronisés avec les autres serveurs qui ont la partition P1.

Pour que la synchronisation de priorité s'effectue, vous devez vérifier que les synchronisations de priorité entrante et sortante sont activées dans iMonitor. Elles le sont par défaut. Si vous désactivez les synchronisations de priorité entrante et sortante, les modifications apportées aux données sont synchronisées par la synchronisation normale.

Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agentDS », page 205.

Cette section fournit les informations suivantes :

- « Création et définition d'une règle de synchronisation de priorité », page 116
- « Édition d'une règle de synchronisation de priorité », page 117
- « Application d'une règle de synchronisation de priorité », page 117
- « Suppression d'une règle de synchronisation de priorité », page 118

Lorsque vous créez une partition enfant, la règle de synchronisation de priorité appliquée au parent est héritée par la partition enfant. Lorsque vous fusionnez des partitions, la règle de synchronisation de priorité du parent est conservée.

Création et définition d'une règle de synchronisation de priorité

Pour définir une règle de synchronisation de priorité, vous pouvez sélectionner les attributs directement ou par le biais d'une classe d'objet. Dans ce dernier cas, tous les attributs de la classe d'objet sont sélectionnés pour la synchronisation de priorité. Vous pouvez sélectionner les attributs obligatoires ou facultatifs pour cette synchronisation.

La règle de synchronisation de priorité peut être créée n'importe où dans l'arborescence eDirectory à l'aide de iManager ou de LDAP.

À l'aide de iManager :

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Règles de synchronisation de priorité.
3. Dans l'Assistant de gestion des règles de synchronisation de priorité, sélectionnez Créer une règle de synchronisation de priorité.
4. Suivez les instructions de l'Assistant de création d'une règle de synchronisation de priorité pour créer la règle.

   Vous pouvez obtenir de l'aide via l'Assistant.

À l'aide de LDAP :

Pour créer une règle de synchronisation de priorité vide:

```
dn:cn=policy1,o=policies

changetype:add

objectclass:prsyncpolicy
```

Pour définir la règle de synchronisation de priorité en marquant les attributs pour la synchronisation de priorité:

```
dn:cn=policy2,o=policies

changetype:add

objectclass:prsyncpolicy

prsyncattributes:description
```

Dans l'exemple ci-dessus, Description désigne l'attribut marqué pour la synchronisation de priorité.

Édition d'une règle de synchronisation de priorité

Vous pouvez éditer un objet Règle de synchronisation de priorité à l'aide de iManager ou de LDAP.

À l'aide de iManager :

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Règles de synchronisation de priorité.
3. Dans l'Assistant de gestion des règles de synchronisation de priorité, sélectionnez Éditer la règle de synchronisation de propriété.
4. Suivez les instructions de l'Assistant d'édition de la règle de synchronisation de priorité pour éditer la règle.

   Vous pouvez obtenir de l'aide via l'Assistant.

À l'aide de LDAP :

Dans l'exemple suivant, la règle de synchronisation de priorité est modifiée en marquant Surname (Nom de famille) pour la synchronisation de priorité au lieu de Description.

```
dn:cn=policy2,o=policies

changetype:modify

add:prsyncattribute

sprsyncattributes:surname
```

Pour supprimer de la règle de synchronisation de priorité un attribut marqué pour la synchronisation de priorité :

```
dn:cn=policy2,o=policies

changetype:modify

add:prsyncattribute

sprsyncattributes:description
```

Dans l'exemple ci-dessus, l'attribut Description est supprimé de la règle de synchronisation de priorité.

Application d'une règle de synchronisation de priorité

Vous pouvez appliquer une règle de synchronisation de priorité à plusieurs partitions, mais une seule règle par partition.

Vous pouvez appliquer une règle de synchronisation de priorité à une partition à l'aide de iManager ou de LDAP.

À l'aide de iManager :

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Règles de synchronisation de priorité.
3. Dans l'Assistant de gestion des règles de synchronisation de priorité, sélectionnez Apply Priority Sync Policy (Appliquer la règle de synchronisation de priorité).
4. Suivez les instructions de l'Assistant d'application de la règle de synchronisation de priorité pour appliquer la règle.

   Vous pouvez obtenir de l'aide via l'Assistant.

À l'aide de LDAP :

Pour appliquer une règle de synchronisation de priorité à une partition racine :

```
dn:

changdn:cn=policy2,o=policies

add:prsyncpolicydn

prsyncpolicydn:cn=policy2,o=policies
```

Dans l'exemple ci-dessus, la règle policy2 est appliquée à la partition racine.

Pour appliquer une règle de synchronisation de priorité à une partition non racine :

```
dn:o=org

changetype:modify

add:prsyncpolicydn

prsyncpolicydn:cn=policy2,o=policies
```

Dans l'exemple ci-dessus, la règle policy2 est appliquée à la partition non racine.

Pour remplacer une règle de synchronisation de priorité pour une partition non racine :

```
dn:o=org

changetype:modify

replace:prsyncpolicydn

prsyncpolicydn:cn=policy1,o=policies
```

Dans l'exemple ci-dessus, la règle policy2 est remplacée par la règle policy1.

Pour dissocier une règle de synchronisation de priorité d'une partition non racine :

```
dn:o=org

changetype:modify

delete:prsyncpolicydn
```

Dans l'exemple ci-dessus, la règle de synchronisation de priorité est dissociée de la partition non racine O=Org.

Suppression d'une règle de synchronisation de priorité

Vous pouvez supprimer une règle de synchronisation de priorité à l'aide de iManager ou de LDAP.

À l'aide de iManager :

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Règles de synchronisation de priorité.
3. Dans l'Assistant de gestion des règles de synchronisation de priorité, sélectionnez Delete Priority Sync Policy (Supprimer la règle de synchronisation de priorité).
4. Suivez les instructions de l'Assistant de suppression de la règle de synchronisation de priorité pour supprimer la règle.

   Vous pouvez obtenir de l'aide via l'Assistant.

À l'aide de LDAP :

```
dn:cn=policy1,o=policies

changetype:delete
```

Situations d'échec de la synchronisation de priorité

La synchronisation de priorité peut échouer dans l'une des situations suivantes :

- Défaillance réseau: la synchronisation de priorité n'enregistre pas les modifications si elle ne parvient pas à les envoyer au serveur distant en raison d'une défaillance réseau ;
- Taille maximale de la file d'attente de la synchronisation de priorité atteinte : la synchronisation de priorité ignore les changements dans la file d'attente de la synchronisation de priorité si le nombre d'entrées dépasse la taille de cette file d'attente ;
- Échec de la synchronisation des schémas : si le schéma n'est pas synchronisé, le processus de synchronisation de priorité échoue ;
- Objet inexistant sur les autres serveurs : si la création de l'objet n'est pas synchronisée, la synchronisation de priorité échoue ;
- Serveurs mixtes dans l'anneau de répliques : si vous disposez de serveurs eDirectory 8.8 et d'autres dotés d'une version antérieure, la synchronisation de priorité échoue.

Lorsque la synchronisation de priorité échoue pour l'une des raisons susmentionnées, les changements apportés aux données essentielles sont synchronisés par le processus normal.

4 Gestion du schéma

Le schéma de l'arborescence Novell® eDirectory™ définit les classes d'objets (Utilisateurs, Groupes et Imprimantes, par exemple) que peut contenir cette arborescence. Il désigne les attributs (propriétés) qui composent chaque type d'objet, notamment ceux qui sont requis lors de la création de l'objet et ceux qui sont facultatifs.

Chaque objet eDirectory appartient à une classe d'objet qui spécifie les attributs qui peuvent être associés à l'objet. Tous les attributs sont basés sur un ensemble de types d'attribut, eux-mêmes basés sur un ensemble standard de syntaxes d'attribut.

Le schéma eDirectory contrôle non seulement la structure des différents objets, mais aussi les relations entre les objets dans l'arborescence eDirectory. Les règles de schéma autorisent des objets définis à contenir d'autres objets subordonnés. Le schéma définit ainsi la structure de l'arborescence eDirectory.

Votre schéma devra peut-être être adapté en fonction de l'évolution des besoins en information de votre entreprise. Par exemple, si vous avez besoin aujourd'hui d'un numéro de télécopie pour un objet Utilisateur, alors que vous n'en avez jamais demandé auparavant, vous pouvez créer une classe Utilisateur pour laquelle le numéro de télécopie est un attribut obligatoire, puis l'utiliser pour créer des objets Utilisateur.

Le rôle Gestion du schéma de Novell iManager vous permet, si vous disposez du droit Superviseur sur une arborescence, de personnaliser le schéma de cette arborescence et d'exécuter les tâches suivantes :

- afficher une liste de l'ensemble des classes et attributs du schéma ;
- étendre le schéma par l'ajout d'une classe ou d'un attribut ;
- créer une classe en lui assignant un nom et en définissant les attributs, drapeaux et conteneurs auxquels cette dernière peut être ajoutée et en spécifiant les classes parentes dont elle peut hériter les attributs ;
- créer un attribut en lui assignant un nom et en spécifiant sa syntaxe et ses drapeaux ;
- ajouter un attribut à une classe existante ;
- supprimer une classe ou un attribut inutilisé ou obsolète ;
- identifier et résoudre les problèmes éventuels.

Ce chapitre contient des informations sur les rubriques suivantes :

- « Drapeaux de schéma ajoutés à eDirectory 8.7 », page 129
- « Utilisation du client eMBox pour effectuer des opérations sur le schéma », page 131

Pour plus d'informations sur les schémas, reportez-vous à la page *NDS Schema Reference (Référence de schema NDS)* (http://developer.novell.com/ndk/doc/ndslib/index.html?schm_enu/data/h4q1mn1i.html).

Extension du schéma

Pour étendre le schéma d'une arborescence, créez une nouvelle classe ou un nouvel attribut. Pour étendre le schéma de votre arborescence eDirectory, vous devez disposez du droit Superviseur pour l'ensemble de l'arborescence.

Les opérations suivantes permettent d'étendre le schéma :

- Création d'une classe
- Suppression d'une classe
- Création d'un attribut
- Ajout d'un attribut facultatif à une classe
- Suppression d'un attribut

Les opérations suivantes permettent d'étendre le schéma pour les attributs auxiliaires :

- Création d'une classe auxiliaire
- Extension d'un objet avec les propriétés d'une classe auxiliaire
- Modification des propriétés auxiliaires d'un objet
- Suppression des propriétés auxiliaires d'un objet

Création d'une classe

Vous pouvez ajouter des classes à votre schéma au fur et à mesure que vos besoins organisationnels évoluent.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Schéma > Créer une classe.
3. Suivez les instructions de l'Assistant de création de classes pour définir la classe d'objet.

   Vous pouvez obtenir de l'aide via l'Assistant.

   Si vous souhaitez définir des propriétés personnalisées à ajouter à la classe d'objet, quittez d'abord l'Assistant. Pour plus d'informations, reportez-vous à la section « Création d'un attribut », page 123.

Suppression d'une classe

Vous pouvez supprimer les classes inutilisées qui ne font pas partie du schéma de base de l'arborescence eDirectory. iManager vous empêche uniquement de supprimer les classes en cours d'utilisation dans les partitions localement répliquées.

Vous pouvez également supprimer une classe du schéma dans les cas suivants :

- lorsque la fusion de deuxarborescences est effectuée et que les différences de classes sont résolues ;
- chaque fois qu'une classe devient obsolète.

Pour supprimer une classe:

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Schéma > Supprimer une classe.
3. Sélectionnez la classe à supprimer.

   Seules les classes dont la suppression est autorisée sont affichées.
4. Cliquez sur Supprimer.

Création d'un attribut

Vous pouvez définir des types d'attribut personnalisés et les ajouter en tant qu'attributs facultatifs aux classes d'objet existantes. Vous ne pouvez toutefois pas ajouter d'attributs obligatoires aux classes existantes.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Schéma > Créer un attribut.
3. Suivez les instructions de l'Assistant de création d'attributs pour définir le nouvel attribut.

   Vous pouvez obtenir de l'aide via l'Assistant.

Ajout d'un attribut facultatif à une classe

Vous pouvez ajouter des attributs facultatifs aux classes existantes. Cette opération peut s'avérer nécessaire si :

- les besoins en information de votre entreprise changent ;
- vous vous préparez à fusionner des arborescences.

REMARQUE : les attributs obligatoires ne peuvent être définis qu'au moment de la création d'une classe.

Pour ajouter un attribut facultatif à une classe :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Schéma > Ajouter un attribut.
3. Sélectionnez la classe à laquelle vous souhaitez ajouter un attribut, puis cliquez sur OK.
4. Dans la liste Attributs facultatifs disponibles, sélectionnez les attributs à ajouter, puis cliquez sur ➡ pour les ajouter à la liste Ajouter le ou les attributs facultatifs suivants.

   Si vous ajoutez un attribut par erreur ou si vous changez d'avis, sélectionnez l'attribut dans la liste Ajouter le ou les attributs facultatifs suivants, puis cliquez sur ⬅ pour le supprimer de la liste des attributs à ajouter.

5 Cliquez sur OK.

Les objets de cette classe que vous créez à partir de maintenant possèdent les propriétés que vous venez d'ajouter. Pour définir des valeurs pour les propriétés ajoutées, utilisez la page de propriétés générique Autre de l'objet.

SUGGESTION : vous pouvez modifier une classe existante en lui ajoutant des attributs dans cette page. Seuls les attributs que vous avez ajoutés avant de cliquer sur OK peuvent être supprimés. Vous ne pouvez pas supprimer un attribut ajouté qui a déjà été sauvegardé.

Suppression d'un attribut

Vous pouvez supprimer les attributs inutilisés qui ne font pas partie du schéma de base de votre arborescence eDirectory.

Vous pouvez également supprimer un attribut du schéma dans les cas suivants :

- lorsque la fusion de deuxarborescences est effectuée et que les différences d'attributs sont résolues ;
- chaque fois qu'un attribut devient obsolète.

Pour supprimer un attribut :

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Schéma > Supprimer un attribut.

3 Sélectionnez l'attribut à supprimer.

Seuls les attributs dont la suppression est autorisée sont affichés.

4 Cliquez sur Supprimer.

Création d'une classe auxiliaire

Une classe auxiliaire est un ensemble de propriétés (attributs) ajouté à des instances d'objet eDirectory définies, et non à l'intégralité d'une classe d'objets. Par exemple, une application de messagerie électronique peut étendre le schéma de l'arborescence eDirectory afin d'inclure une classe auxiliaire Propriétés des courriers électroniques, puis étendre différents objets avec ces propriétés selon les besoins.

Grâce au Gestionnaire de schéma, vous pouvez définir vos propres classes auxiliaires. Vous pouvez ensuite étendre différents objets avec les propriétés définies dans ces classes auxiliaires.

Pour créer une classe auxiliaire :

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Schéma > Créer une classe.

3 Spécifiez un nom de classe et un ID ASN1 (facultatif), puis cliquez sur Suivant.

4 Sélectionnez Classe auxiliaire lorsque vous définissez les drapeaux de classe, puis cliquez sur Suivant.

5 Suivez les instructions de l'Assistant de création de classes pour définir la nouvelle classe auxiliaire.

Vous pouvez obtenir de l'aide via l'Assistant.

Extension d'un objet avec les propriétés d'une classe auxiliaire

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Schéma > Extensions d'objet.
3. Spécifiez le nom et le contexte de l'objet à étendre, puis cliquez sur OK.
4. Selon que la classe auxiliaire à utiliser figure ou non dans la liste Extensions de classe auxiliaire actuelles, effectuez l'opération correspondante :

La classe auxiliaire figure-t-elle déjà dans la liste ?	Opération
Oui	Quittez cette procédure. Reportez-vous plutôt à la section « Modification des propriétés auxiliaires d'un objet », page 125.
Non	Cliquez sur Ajouter, sélectionnez la classe auxiliaire, puis cliquez sur OK.

5. Cliquez sur Fermer.

Modification des propriétés auxiliaires d'un objet

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Modifier un objet.
3. Spécifiez le nom et le contexte de l'objet à modifier, puis cliquez sur OK.
4. Dans l'onglet Général, cliquez sur la page Autre.
5. Dans l'écran qui apparaît, définissez les valeurs d'attributs de votre choix.
   - Double-cliquez sur un attribut non défini pour l'ajouter à la liste des attributs définis.
   - Sélectionnez un attribut défini, puis cliquez sur Éditer pour le modifier ou sur Supprimer pour le supprimer.
   - Vous devez connaître la syntaxe d'une propriété pour la définir correctement. Pour plus d'informations, reportez-vous à la section de la documentation en ligne Understanding Schema Manager (Gestionnaire de schémaPrésentation) (http://www.novell.com/documentation/lg/ndsv8/docui/index.html#../usnds/schm_enu/data/hnpkthb2.html).
6. Cliquez sur Appliquer, puis sur OK.

Suppression des propriétés auxiliaires d'un objet

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Schéma > Extensions d'objet.
3. Spécifiez le nom et le contexte de l'objet à étendre, puis cliquez sur OK.
4. Dans la liste des extensions de classe auxiliaire actuelles, sélectionnez la classe auxiliaire dont vous souhaitez supprimer les propriétés.
5. Cliquez sur Retirer, puis sur OK.

   Cette opération supprime la totalité des propriétés qui ont été ajoutées par la classe auxiliaire, à l'exception de celles inhérentes à l'objet.
6. Cliquez sur Fermer.

Affichage du schéma

Vous pouvez afficher le schéma pour voir dans quelle mesure il répond aux besoins en information de votre entreprise. Plus votre entreprise est grande et sa structure complexe, plus la personnalisation du schéma s'avère nécessaire. Cependant, même les petites entreprises peuvent avoir des besoins de suivi particuliers. Visualisez le schéma pour vous aider à déterminer les éventuelles extensions nécessaires au niveau du schéma de base.

Affichage des informations sur la classe

La page Informations sur la classe de iManager fournit des informations sur la classe sélectionnée et vous permet d'ajouter des attributs. La plupart des informations figurant dans cette page ont été spécifiées lors de la création de la classe. Certains attributs facultatifs peuvent avoir été ajoutés ultérieurement.

Si, lors de sa création, la classe a été définie de façon à hériter d'attributs d'une autre classe, ceux-ci sont classés de la même manière que dans la classe parente. Par exemple, si la classe d'objet est un attribut obligatoire pour la classe parente, elle apparaît sur cet écran comme attribut obligatoire pour la classe sélectionnée.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Schéma > Informations sur la classe.
3. Sélectionnez la classe pour laquelle vous souhaitez des informations, puis cliquez sur Afficher.

   Pour plus dinformations, cliquez sur  .

Affichage des informations sur l'attribut

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Schéma > Informations sur l'attribut.
3. Sélectionnez l'attribut pour lequel vous souhaitez des informations, puis cliquez sur Afficher.

   Pour plus dinformations, cliquez sur  .

Extension manuelle du schéma

Vous pouvez étendre manuellement le schéma eDirectory à l'aide des fichiers avec une extension .sch.

Cette section comprend les informations suivantes :

- « Extension du schéma sur NetWare », page 127
- « Extension du schéma sur Windows », page 127
- « Extension du schéma sur les systèmes Linux, Solaris, AIX ou HP-UX », page 127

Extension du schéma sur NetWare

Utilisez NWConfig.nlm pour étendre le schéma sur les serveurs NetWare. Les fichiers de schéma (*.sch) fournis avec eDirectory sont installés dans le répertoire sys:\system\schema.

1. À l'invite de la console du serveur, entrez la commande **nwconfig**.
2. Sélectionnez Annuaire > Étendre le schéma.
3. Loguez-vous en tant qu'utilisateur doté de droits d'administrateur.
4. Appuyez sur F3 pour changer de chemin, puis tapez la commande **sys:\system\schema** (ou le chemin d'accès à votre fichier *.sch) et le nom de votre fichier de schéma.
5. Appuyez sur Entrée.

Extension du schéma sur Windows

Utilisez NDSCons.exe pour étendre le schéma sur des serveurs Windows. Par défaut, les fichiers de schéma (*.sch) fournis avec eDirectory sont installés dans le répertoire C:\Novell\NDS.

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration > Services Novell eDirectory.
2. Cliquez sur install.dlm, puis sur Démarrer.
3. Cliquez sur Installer d'autres fichiers de schéma, puis sur Suivant.
4. Loguez-vous en tant qu'utilisateur doté de droits d'administrateur, puis cliquez sur OK.
5. Indiquez le nom du fichier de schéma et le chemin d'accès correspondant.
6. Cliquez sur Terminer.

Extension du schéma sur les systèmes Linux, Solaris, AIX ou HP-UX

Les sections suivantes fournissent des informations relatives à l'extension du schéma sur les systèmes Linux, Solaris, AIX et HP-UX :

- « Utilisation de l'utilitaire ndssch pour étendre le schéma sur Linux, Solaris, AIX ou HP-UX », page 127
- « Extension du schéma RFC 2307 », page 128

Utilisation de l'utilitaire ndssch pour étendre le schéma sur Linux, Solaris, AIX ou HP-UX

Outre Novell iManager, vous pouvez faire appel à ndssch, l'utilitaire d'extension de schéma de eDirectory, pour étendre le schéma sur les systèmes Linux, Solaris, AIX ou HP-UX. Les attributs et les classes que vous indiquez dans le fichier de schéma (.sch) sont utilisés pour modifier le schéma de l'arborescence. Les associations entre les attributs et les classes sont créées selon les indications du fichier .sch.

1. Utilisez la syntaxe suivante :

```
ndssch [-h nom_hôte[:port]] [-t nom_arborescence] FDN_admin
fichier_schéma ...

ndssch [-h nom_hôte[:port]][-t nom_arborescence] [-d] FDN_admin
fichier_schéma [description_schéma] ...
```

Paramètre ndssch	Description
-h *nom_hôte*	Nom ou adresse IP du serveur sur lequel le schéma doit être étendu. Le schéma de l'arborescence à laquelle appartient le serveur spécifié est étendu. Ce paramètre est facultatif si l'arborescence se situe sur l'hôte dont le schéma doit être étendu. Dans le cas contraire, il est obligatoire.
port	Port du serveur.
-t *nom_arborescence*	Nom de l'arborescence sur laquelle le schéma doit être étendu. Ce paramètre est facultatif. Le nom d'arborescence par défaut est indiqué dans le fichier /etc/opt/novell/eDirectory/conf/nds.conf. Pour plus d'informations, reportez-vous à la section Configuration Parameters (Paramètres de configuration) du manuel *Novell eDirectory 8.8 Installation Guide (Guide d'installation de Novell eDirectory 8.8)*.
FDN_admin	Nom et contexte complet de l'utilisateur disposant de droits d'administrateur eDirectory sur l'arborescence.
fichier_schéma	Nom du fichier qui contient les informations sur le schéma à étendre.
-d, *description_schéma*	Si cette option est activée, chaque fichier de schéma doit être suivi de sa description.

Extension du schéma RFC 2307

Les attributs et les classes d'objets définis dans RFC 2307 (http://www.ietf.org/rfc/rfc2307.txt) sont liés à l'utilisateur ou au groupe, ainsi qu'aux NIS (Network Information Services-services d'information réseau). Les définitions associées à l'utilisateur ou au groupe sont compilées dans le fichier /opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-usergroup.sch. Les définitions liées aux NIS sont compilées dans le fichier /opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-nis.sch. Les fichiers correspondants au format LDIF sont également fournis (/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-usergroup.ldif et /opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-nis.ldif).

Vous pouvez étendre le schéma RFC 2307 à l'aide de l'utilitaire ndssch ou de l'outil ldapmodify.

- « Utilisation de l'utilitaire ndssch », page 128
- « Utilisation de l'utilitaire ldapmodify », page 129

Utilisation de l'utilitaire ndssch

Entrez l'une des commandes suivantes :

```
ndssch -t /opt/novell/eDirectory/lib/nds-schema/rfc2307-
usergroup.sch
```

ou

```
ndssch -t /opt/novell/eDirectory/lib/nds-schema/rfc2307-nis.sch
```

Paramètre	Description
-t	Nom de l'arborescence sur laquelle le schéma doit être étendu. Ce paramètre est facultatif. Si ce paramètre n'est pas spécifié, le nom de l'arborescence utilisé est tiré du fichier /etc/opt/novell/eDirectory/conf/nds.conf.

Utilisation de l'utilitaire ldapmodify

Entrez l'une des commandes suivantes :

```
ldapmodify -h -D -w -f /opt/novell/eDirectory/lib/nds-schema/
rfc2307-usergroup.ldif
```

ou

```
ldapmodify -h -D -w -f /opt/novell/eDirectory/lib/nds-schema/
rfc2307-nis.ldif
```

Paramètre	Description
-h *hôte_LDAP*	Définit un autre hôte sur lequel le serveur LDAP est exécuté.
-D *DN_liaison*	Utilise *DN_liaison* pour établir une liaison vers l'annuaire X.500. Il doit s'agir d'un nom distinctif sous forme de chaîne, conformément à la définition dans RFC 1779.
-w *mot_de_passe*	Utilise *mot_de_passe* comme mot de passe pour l'authentification simple.
-f *fichier*	Lit les informations de modification de l'entrée à partir du fichier et non de l'entrée standard.

Drapeaux de schéma ajoutés à eDirectory 8.7

Les drapeaux de schéma READ_FILTERED et BOTH_MANAGED ont été ajoutés à eDirectory 8.7.

Le drapeau READ_FILTERED sert à préciser qu'un attribut est opérationnel pour LDAP. LDAP utilise ce drapeau lors des requêtes de lecture du schéma pour indiquer qu'un attribut est « opérationnel ». READ_FILTERED est activé pour certains attributs de schéma définis en interne. La définition de l'état « opérationnel » pour LDAP comprend trois drapeaux de schéma. Outre le nouveau drapeau READ_FILTERED, les autres qui servent à spécifier l'état « opérationnel » sont READ_ONLY et HIDDEN. Si l'un d'eux est activé dans une définition de schéma, LDAP considère l'attribut comme « opérationnel » et ne le renvoie pas, sauf demande contraire.

Le drapeau BOTH_MANAGED offre un nouveau mécanisme de renforcement de la sécurité des droits. Il n'est significatif que sur un attribut de syntaxe de nom distinctif. S'il est activé pour un tel attribut, la connexion qui fait une demande doit disposer des droits à la fois sur l'objet et l'attribut cible, ainsi que sur l'objet référencé par l'attribut cible. Il s'agit d'une extension de la fonctionnalité actuelle du drapeau WRITE_MANAGED. Il n'est actuellement activé sur aucun attribut de schéma de base. Cette nouvelle stratégie de sécurité ne s'applique qu'à un serveur eDirectory 8.7*.x*. Pour bénéficier d'une stratégie homogène, vous devez donc mettre à niveau la totalité de l'arborescence vers Directory, version 8.7 ou ultérieure.

Étant donné que ces drapeaux ne sont reconnus que par un serveur eDirectory 8.7.*x*, ils peuvent uniquement être activés dans une définition de schéma par un serveur eDirectory 8.7.*x* qui détient une copie de la partition racine. (En effet, seuls les serveurs détenteurs de la racine peuvent modifier le schéma.) L'installation normale d'un nouveau serveur ou la mise à niveau d'un serveur existant qui ne détient pas la partition racine ne permet pas d'ajouter ces nouveaux drapeaux au schéma de votre arborescence.

Si vous voulez activer une de ces nouvelles fonctions dans votre arborescence, assurez-vous que le schéma a été étendu afin de pouvoir ajouter ces drapeaux. Vous pouvez effectuer cette tâche de deux manières. La première consiste à choisir un serveur qui possède une copie accessible en écriture de la partition racine à mettre à niveau vers eDirectory version 8.7 ou ultérieure. Le nouveau schéma est alors automatiquement étendu avec les nouveaux drapeaux.

La seconde méthode est plus complexe et comprend deux étapes :

1. Installez un nouveau serveur 8.7.*x* ou mettez à niveau un serveur de l'arborescence. Il n'est pas nécessaire que ce serveur possède une copie de [Root].
2. Ajoutez manuellement une copie de la partition racine au nouveau serveur.
3. Exécutez de nouveau les fichiers d'extension de schéma appropriés sur ce serveur pour étendre le schéma :

Plate-forme	Instructions
Windows	Chargez install.dlm, puis cliquez sur Installer d'autres fichiers de schéma.
NetWare	Chargez nwconfig, puis sélectionnez Annuaire/Étendre le schéma.
Linux, Solaris, AIX et HP-UX	Utilisez l'utilitaire ndssch. Pour plus d'informations, reportez-vous à la section « Utilisation de l'utilitaire ndssch pour étendre le schéma sur Linux, Solaris, AIX ou HP-UX », page 127.

4. Installez les nouveaux fichiers de schéma de votre choix dont les nouveaux drapeaux sont activés.
5. (Facultatif) Une fois le schéma synchronisé, vous pouvez supprimer la réplique racine de ce serveur.

REMARQUE : ces nouveaux drapeaux de schéma proposent des fonctions facultatives. Si vous n'en avez pas besoin, l'absence des nouveaux drapeaux sur les définitions de schéma ne perturbe pas le fonctionnement normal de eDirectory dans votre arborescence. Le drapeau READ_FILTERED ne sera pas présent sur certaines définitions d'attributs. Dès lors, une requête de lecture LDAP de tous les attributs d'un objet peut renvoyer des données supplémentaires qu'elle n'aurait pas reçues dans le cas contraire. Certains attributs seront toujours traités comme étant opérationnels du fait de la présence des drapeaux READ_ONLY et/ou HIDDEN. Le drapeau BOTH_MANAGED doit uniquement être activé sur des arborescences entièrement mises à niveau, car il ne peut fonctionner de manière homogène que dans cet environnement.

Utilisation du client eMBox pour effectuer des opérations sur le schéma

Le client eDirectory Management Toolbox (eMBox) est un client Java à ligne de commande qui permet d'accéder à distance aux opérations DSSchema. Vous pouvez utiliser l'outil eMTool DSSchema pour synchroniser le schéma, importer un schéma distant, déclarer une nouvelle période, réinitialiser le schéma local et réaliser une mise à jour du schéma (opérations normalement réalisées à l'aide de DSRepair. Pour plus d'informations, reportez-vous à la section « Maintenance du schéma », page 273.

Le fichier emboxclient.jar est installé sur votre serveur comme élément de eDirectory. Vous pouvez l'exécuter sur toute machine dotée d'une JVM. Pour plus d'informations sur le client eMBox, reportez-vous à la section « Utilisation du client à ligne de commande eMBox », page 553.

Utilisation de l'outil eMTool DSSchema

1. Exécutez le client eMBox en mode interactif en entrant les éléments suivants dans la ligne de commande :

   java -cp *chemin_fichier*/emboxclient.jar embox -i

   (Si le fichier emboxclient.jar figure déjà dans votre chemin d'accès à la classe, il vous suffit d'entrer la commande **java embox -i**.)

   L'invite du client eMBox apparaît :

   ```
   Client eMBox>
   ```

2. Loguez-vous au serveur à réparer en entrant la commande suivante :

   login -s*nom_ou_adresse_IP_serveur* -p*numéro_port*
   -u*nom_utilisateur.contexte* -w*mot_de_passe* -n

   Le numéro de port est généralement 80 ou 028, à moins qu'il ne soit déjà utilisé par un serveur Web. L'option -n ouvre une connexion non sécurisée.

   Le client eMBox indique si le login a réussi.

3. Entrez une commande de réparation à l'aide de la syntaxe suivante :

   dsschema.*options_ tâche*

   Par exemple :

   dsschema.rst invite la réplique maîtresse de la racine de l'arborescence à synchroniser son schéma avec ce serveur.

   dsschema.irs -n*MonArborescence* importe le schéma distant de l'arborescence nommée MonArborescence.

   Les paramètres doivent être séparés les uns des autres par un espace. L'ordre des paramètres n'a pas d'importance.

   Le client eMBox indique la réussite ou l'échec de la réparation.

   Pour plus d'informations sur les options de l'outil eMTool DSSchema, reportez-vous à la section « Options de l'outil EMTool DSSchema », page 132.

4. Déloguez-vous du client eMBox en entrant la commande suivante :

   logout

5. Quittez le client eMBox en entrant la commande suivante :

   exit

Options de l'outil EMTool DSSchema

Les tableaux suivants répertorient les options de l'outil EMTool DSSchema. Vous pouvez également utiliser la commande list -tdsschema du client eMBox pour visualiser en détail les options DSSchema. Pour plus d'informations, reportez-vous à la section « Liste des outils eMTools et de leurs services », page 557.

Option	Description
rst	Synchronise le schéma de la réplique maîtresse de la racine de l'arborescence avec le serveur.
irs -n*nom_arborescence*	Importe un schéma distant à partir d'une autre arborescence.
dse	Établit une nouvelle période de schéma sur le serveur qui contient la réplique maîtresse de la racine.
rls	Réinitialise le schéma local à l'aide d'une copie du serveur qui contient la réplique maîtresse de la partition de la racine.
gsu	Met à jour l'ensemble du schéma vers une version de NetWare postérieure à NetWare 5.
scc	Ajoute des règles d'endiguement circulaire du schéma à la classe Domaine.

5 Gestion des partitions et des répliques

Les partitions sont des divisions logiques de la base de données Novell® eDirectory™ qui forment une unité de données distincte dans l'arborescence eDirectory. Les administrateurs s'en servent pour stocker et répliquer des informations sur eDirectory. Chaque partition se compose d'un objet Conteneur, de tous les objets qu'il inclut et des informations sur ces objets. Les partitions ne comprennent pas d'informations sur le système de fichiers, ni sur les répertoires et fichiers qu'il contient.

Plutôt que de stocker une copie de toute la base de données eDirectory sur chaque serveur, vous pouvez faire une copie de la partition eDirectory et la stocker sur plusieurs serveurs du réseau. Chaque copie de la partition constitue une réplique. Vous pouvez créer autant de répliques que vous le souhaitez pour chaque partition eDirectory et les stocker sur n'importe quel serveur. Les répliques peuvent être de type Maîtresse, Lecture/écriture, Lecture seule, Références subordonnées, Lecture/écriture filtrée et Lecture seule filtrée.

Le tableau suivant décrit les types de répliques.

Réplique	Description
Maîtresse, Lecture/écriture et Lecture seule	Contiennent tous les objets et attributs d'une partition donnée.
Références subordonnées	Utilisées pour la connectivité de l'arborescence.
Répliques filtrées	Contiennent un sous-ensemble d'informations extraites de la partition entière, comprenant uniquement les classes et attributs voulus définis par le filtre de réplication du serveur. Ce filtre permet d'identifier les classes et attributs autorisés à passer en cas de synchronisation entrante et de changements locaux. Les répliques filtrées permettent aux administrateurs de créer des répliques éparses et fractionnaires. ◆ Les répliques éparses contiennent uniquement les classes d'objets que vous indiquez. ◆ Les répliques fractionnaires contiennent uniquement les attributs que vous indiquez. La fonctionnalité des répliques filtrées permet d'obtenir des réponses rapides lorsque les données stockées dans eDirectory sont fournies par les applications. Les répliques filtrées permettent également de stocker davantage de répliques sur un seul serveur.
Répliques filtrées Lecture/écriture	Permettent d'apporter des modifications locales aux classes et aux attributs qui constituent un sous-ensemble du filtre de réplication du serveur. Cependant, ces répliques ne peuvent créer des objets que si tous les attributs obligatoires de la classe se trouvent dans le filtre de réplication.
Répliques filtrées Lecture seule	Ne permettent pas les modifications locales.

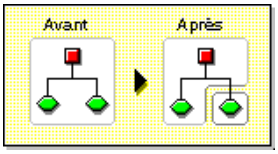
Ce chapitre indique comment gérer les partitions et les répliques.

Création d'une partition

Lorsque vous créez des partitions, vous effectuez des divisions logiques de votre arborescence. Ces divisions peuvent être répliquées et distribuées entre les différents serveurs eDirectory de votre réseau.

Pour créer une partition, vous divisez la partition parente de manière à obtenir deux partitions. La nouvelle partition devient une partition enfant, comme l'indique la figure ci-dessous.

Figure 27 Avant et après la division d'une partition



Par exemple, pour créer un objet Unité organisationnelle en tant que nouvelle partition, vous devez séparer cet objet et tous ceux qui lui sont subordonnés de la partition parente.

L'objet Unité organisationnelle choisi devient alors la racine de la nouvelle partition. Les répliques de la nouvelle partition se trouvent sur les mêmes serveurs que celles de la partition parente, et les objets de cette nouvelle partition sont placés dans son objet Racine.

La création d'une partition peut prendre un certain temps, car toutes les répliques doivent être synchronisées avec les informations de cette nouvelle partition. Si vous tentez d'effectuer une autre opération de partition pendant la création d'une partition, un message vous indique que la partition est occupée.

Comme vous pouvez le vérifier en consultant la liste des répliques de la nouvelle partition, l'opération est terminée quand toutes les répliques de la liste sont à l'état Actif. Vous devez régulièrement actualiser cette vue manuellement, car l'affichage des états n'est pas rafraîchi automatiquement.

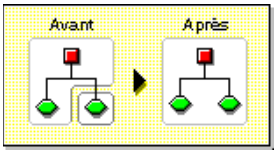
Pour créer une partition, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Créer une partition.
3. Entrez le nom et le contexte du conteneur à partir duquel vous voulez créer une partition, puis cliquez sur OK.

Fusion d'une partition

Lorsque vous fusionnez une partition avec sa partition parente, la partition choisie et ses répliques sont combinées avec la partition parente. Aucune partition n'est supprimée ; il s'agit en fait de fusionner et de créer des partitions pour définir la méthode de division logique de l'arborescence Annuaire, comme l'indique la figure ci-dessous.

Figure 28 Avant et après la fusion d'une partition



Vous pouvez fusionner une partition avec sa partition parente pour plusieurs raisons:

- Les informations sur l'annuaire dans les deux partitions sont étroitement liées.
- Vous souhaitez supprimer une partition subordonnée sans supprimer les objets qu'elle contient.
- Vous êtes sur le point de supprimer les objets de la partition.
- Vous voulez supprimer toutes les répliques de la partition. (La fusion d'une partition avec sa partition parente est la seule façon de supprimer la réplique maîtresse de la partition.)
- Vous avez déplacé un conteneur (il doit s'agir de la racine d'une partition sans partition subordonnée) et vous ne souhaitez plus que ce dernier soit une partition.
- L'organisation de votre entreprise subit des changements ; vous souhaitez donc revoir votre arborescence Annuaire et modifier la structure des partitions.

Séparez les partitions si elles sont volumineuses (c'est-à-dire si elles contiennent des centaines d'objets), car les partitions de grande taille augmentent le temps de réponse du réseau.

La partition racine de l'arborescence ne peut pas être fusionnée puisqu'il s'agit de la partition la plus élevée et qu'elle ne peut donc pas fusionner avec une partition parente.

La partition est fusionnée lorsque le processus est terminé sur les serveurs. La durée de cette opération peut être plus ou moins longue selon la taille des partitions, le trafic réseau, la configuration du serveur, etc.

IMPORTANT : avant de fusionner une partition, vérifiez la synchronisation des deux partitions et corrigez les erreurs éventuelles. La correction des erreurs permet d'isoler les problèmes rencontrés dans l'annuaire. Vous évitez ainsi l'apparition et la propagation d'erreurs.

Avant de tenter une fusion, assurez-vous que tous les serveurs qui contiennent des répliques (y compris des références subordonnées) de la partition à fusionner sont en service. Si un serveur est hors service, eDirectory ne peut pas lire ses répliques et l'opération ne peut donc pas être effectuée.

Si des erreurs apparaissent au cours du processus de fusion d'une partition, corrigez-les au fur et à mesure. N'essayez pas de les corriger en continuant à effectuer des opérations ; cela génère des erreurs supplémentaires.

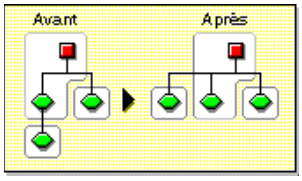
Pour fusionner une partition enfant avec sa partition parente, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Fusionner la partition.
3. Spécifiez le nom et le contexte de la partition à fusionner avec sa partition parente, puis cliquez sur OK.

Déplacement de partitions

Si vous déplacez une partition, la sous-arborescence correspondante est déplacée dans l'arborescence Annuaire. Vous ne pouvez déplacer un objet Racine de partition (qui est un objet Conteneur) que si celui-ci ne comporte pas de partitions subordonnées.

Figure 29 Avant et après le déplacement d'une partition



Lorsque vous déplacez une partition, vous devez respecter les règles d'endiguement de eDirectory. Par exemple, vous ne pouvez pas déplacer un objet Unité organisationnelle qui se trouve directement sous la racine de l'arborescence en cours, car les règles d'endiguement de la racine autorisent uniquement le déplacement des objets Lieu, Pays et Organisation.

Lorsque vous déplacez une partition, eDirectory modifie toutes les références à son objet Racine. Contrairement au nom commun de l'objet qui demeure inchangé, le nom complet du conteneur (et de tous ses subordonnés) est modifié.

Lorsque vous déplacez une partition, vous avez tout intérêt à créer un objet Alias pour remplacer le conteneur que vous déplacez. Ainsi, les utilisateurs peuvent continuer à se loguer au réseau et à rechercher des objets dans l'annuaire à leur emplacement d'origine.

L'objet Alias créé porte le même nom commun que le conteneur déplacé et fait référence à son nouveau nom complet.

IMPORTANT : si vous déplacez une partition sans la remplacer par un objet Alias, les utilisateurs qui ne connaissent pas le nouvel emplacement de la partition retrouvent difficilement les objets qu'elle contient dans l'arborescence Annuaire, puisqu'ils les recherchent à leur emplacement d'origine.

De plus, les postes de travail client risquent de ne pas permettre le login si la valeur du paramètre NAME CONTEXT correspond à l'emplacement d'origine du conteneur dans l'arborescence Annuaire.

Lorsque vous déplacez un objet, son contexte change. Les utilisateurs dont le contexte de nom fait référence à l'objet déplacé doivent donc mettre à jour le paramètre NAME CONTEXT de manière à ce que celui-ci mentionne le nouveau nom de l'objet.

Vous pouvez mettre à jour automatiquement le paramètre NAME CONTEXT des utilisateurs après avoir déplacé un objet Conteneur à l'aide de l'utilitaire NCUPDATE.

Si, une fois la partition déplacée, vous ne voulez plus qu'il s'agisse d'une partition, fusionnez-la avec sa partition parente.

Vérifiez que la synchronisation de l'arborescence Annuaire s'effectue correctement avant de déplacer une partition. En cas d'erreur de synchronisation soit dans la partition à déplacer, soit dans la partition cible, n'effectuez pas ce déplacement. Corrigez d'abord les erreurs de synchronisation.

Pour déplacer une partition, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Déplacer une partition.
3. Dans le champ Nom de l'objet, spécifiez le nom et le contexte de l'objet Partition à déplacer.

4 Dans le champ Déplacer vers, indiquez le nom et le contexte du conteneur vers lequel vous souhaitez transférer la partition.

5 Pour créer un alias à l'ancien emplacement de la partition déplacée, sélectionnez Créer un alias à la place de l'objet déplacé.

Si vous créez un alias, les opérations qui sont tributaires de l'ancien emplacement se poursuivent sans interruption jusqu'à ce que vous puissiez les mettre à jour pour qu'elles reflètent le nouvel emplacement.

6 Cliquez sur OK.

Annulation des opérations de création ou de fusion de partitions

Vous pouvez annuler la création ou la fusion d'une partition tant que la modification à part entière n'a pas été exécutée. Utilisez cette fonction pour annuler une opération, si votre réseau eDirectory renvoie des erreurs eDirectory ou s'il ne parvient pas à effectuer la synchronisation à la suite d'une opération de partition.

Si des erreurs de synchronisation se produisent pour les répliques de votre arborescence Annuaire, l'opération d'annulation ne permet pas forcément de résoudre le problème. Vous pouvez cependant utiliser cette fonction comme première option de dépannage.

Si une opération de partition ne peut pas être effectuée parce qu'un serveur est hors service (ou non disponible pour une autre raison), rendez le serveur visible par le réseau pour que l'opération puisse être effectuée ou abandonnez cette dernière. Si eDirectory ne peut pas effectuer la synchronisation car la base de données est altérée, vous devez annuler les opérations de partition en cours.

La synchronisation complète des partitions sur le réseau peut demander un temps considérable, selon le nombre de répliques concernées, la visibilité des serveurs impliqués et le trafic réseau existant.

Si un message d'erreur signale que la partition est occupée, vous ne devez pas pour autant abandonner l'opération. Vous pouvez généralement vous attendre à ce que les opérations de partition s'effectuent dans les 24heures, en fonction de la taille de la partition, des problèmes de connexion, etc. Si une fois ce délai écoulé, l'opération n'est pas terminée, vous devez essayer d'annuler l'opération en cours.

Gestion des répliques

Avant d'ajouter ou de supprimer une réplique ou de modifier un type de réplique, planifiez soigneusement les emplacements des répliques cibles. Pour plus de détails, reportez-vous à la section « Instructions concernant la réplication de votre arborescence », page 80.

Ajout d'une réplique

Ajoutez une réplique à un serveur pour que votre annuaire bénéficie des avantages suivants :

- Tolérance aux pannes
- Accès plus rapide aux données
- Accès plus rapide via une liaison WAN
- Accès aux objets dans un contexte défini (à l'aide des services de Bindery)

Pour ajouter une réplique, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Spécifiez le nom et le contexte de la partition ou du serveur à répliquer, puis cliquez sur OK.
4. Cliquez sur Ajouter une réplique.
5. Spécifiez le nom et le contexte de la partition ou du serveur.
6. Choisissez l'un des types de réplique suivants :

Type de réplique	Description
 Lecture/écriture	Les utilisateurs peuvent lire et modifier le contenu de la nouvelle réplique. Sélectionnez cette option si aucune réplique modifiable ne se trouve suffisamment près des utilisateurs qui gèrent les objets eDirectory de cette partition.
 Lecture seule	Les utilisateurs peuvent lire le contenu de la nouvelle réplique, mais ne peuvent pas le modifier. Sélectionnez cette option si aucune réplique ne se trouve suffisamment près des utilisateurs qui lisent les objets eDirectory de cette partition mais ne peuvent pas les modifier.
 Lecture/écriture filtrée	Les utilisateurs peuvent lire et modifier le contenu de la nouvelle réplique, qui est limité aux types d'objets et de propriétés eDirectory spécifiés dans un filtre.
 Lecture seule filtrée	Les utilisateurs peuvent lire le contenu de la nouvelle réplique mais ne peuvent pas le modifier. Ce contenu est limité aux types d'objets et de propriétés eDirectory spécifiés dans un filtre.

7. Cliquez sur OK.

Pour plus d'informations, reportez-vous à la section « Types de répliques », page 53.

Suppression d'une réplique

Une fois supprimée, la réplique de la partition est retirée du serveur.

Pour retirer un serveur de l'arborescence Annuaire, vous pouvez supprimer ses répliques avant de retirer le serveur lui-même. Si vous supprimez les répliques, vous réduisez les risques de problèmes au moment du retrait du serveur.

La suppression des répliques permet aussi de réduire le trafic réseau lié à la synchronisation. Souvenez-vous qu'il est conseillé de ne pas créer plus de six répliques par partition.

Vous ne pouvez pas supprimer une réplique maîtresse ou une référence subordonnée.

Si la réplique à supprimer est une réplique maîtresse, vous avez deux possibilités :

- Vous connecter à un serveur possédant une autre réplique de la partition et la transformer en nouvelle réplique maîtresse

  La réplique maîtresse initiale est alors automatiquement convertie en réplique Lecture/écriture et peut alors être supprimée.

- Fusionner la partition avec sa partition parente

  Ceci a pour effet de fusionner les répliques de la partition avec celles de sa partition parente et de les supprimer du serveur sur lequel elles se trouvent. Le processus de fusion supprime les limites des partitions, mais pas les objets. Les objets continuent d'exister sur chacun des serveurs contenant une réplique de la partition «jointe».

Lorsque vous supprimez des répliques, gardez en tête les indications suivantes :

- Pour faciliter la tolérance aux pannes, il est souhaitable de conserver au moins trois répliques de chaque partition sur différents serveurs.
- Si vous supprimez une réplique, une copie d'une partie de la base de données d'annuaire est supprimée sur le serveur cible.

  Vous pouvez toujours accéder à la base de données à partir d'autres serveurs du réseau, et le serveur sur lequel était stockée la réplique fonctionne toujours dans eDirectory.

  Vous ne pouvez pas supprimer ni gérer les répliques de type Référence subordonnée. Elles sont automatiquement créées par eDirectory sur les serveurs contenant une réplique d'une partition mais pas de réplique de sa partition enfant.

Pour supprimer une réplique, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Spécifiez le nom et le contexte de la partition ou du serveur qui contient la réplique à supprimer, puis cliquez sur OK.
4. Cliquez sur  , à gauche de la réplique à supprimer.
5. Cliquez sur OK.

Changement du type d'une réplique

Modifier le type d'une réplique permet de contrôler l'accès aux informations de cette réplique. Par exemple, vous pouvez convertir une réplique Lecture/écriture en réplique Lecture seule pour empêcher les utilisateurs d'écrire dans cette réplique et de modifier des données de l'annuaire.

Vous pouvez modifier le type d'une réplique Lecture/écriture ou d'une réplique Lecture seule. Vous ne pouvez pas modifier le type d'une réplique maîtresse. En revanche, vous pouvez transformer une réplique Lecture/écriture ou Lecture seule en réplique maîtresse (la réplique maîtresse initiale devenant alors automatiquement une réplique Lecture/écriture).

La plupart des répliques doivent être de type Lecture/écriture. Les opérations client y accèdent en écriture. Ces répliques envoient les informations à synchroniser lorsqu'une modification est effectuée. Les opérations client ne peuvent par contre pas accéder en écriture aux répliques Lecture seule, qui sont mises à jour lors de la synchronisation des répliques.

Vous ne pouvez pas modifier le type de réplique d'une référence subordonnée. Pour placer une réplique d'une partition sur un serveur possédant une référence subordonnée, vous devez effectuer une opération d'ajout de réplique. Une réplique de référence subordonnée n'est pas une copie complète d'une partition. Les répliques de référence subordonnée sont placées et gérées par eDirectory. Elles sont automatiquement créées par eDirectory sur les serveurs contenant une réplique d'une partition mais pas de réplique de sa partition enfant.

Pour modifier le type d'une réplique, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Spécifiez le nom et le contexte de la partition ou du serveur qui contient la réplique à modifier, puis cliquez sur OK.
4. Cliquez sur le type (dans la colonne Type) de la réplique à modifier.
5. Sélectionnez un nouveau type de réplique et cliquez sur OK.

Type de réplique	Description
 Maîtresse	Les utilisateurs peuvent lire et modifier le contenu de cette réplique qui constitue le point de départ de toute activité ultérieure de partitionnement s'appliquant à cette partition, comme la création ou la fusion d'une sous-partition. Une seule réplique maîtresse par partition est autorisée.
 Lecture/écriture	Les utilisateurs peuvent lire et modifier le contenu de la nouvelle réplique. Sélectionnez cette option si aucune réplique modifiable ne se trouve suffisamment près des utilisateurs qui gèrent les objets eDirectory de cette partition.
 Lecture seule	Les utilisateurs peuvent lire le contenu de la nouvelle réplique, mais ne peuvent pas le modifier. Sélectionnez cette option si aucune réplique ne se trouve suffisamment près des utilisateurs qui lisent les objets eDirectory de cette partition mais ne peuvent pas les modifier.
 Lecture/écriture filtrée	Les utilisateurs peuvent lire et modifier le contenu de la nouvelle réplique, qui est limité aux types d'objets et de propriétés eDirectory spécifiés dans un filtre.
 Lecture seule filtrée	Les utilisateurs peuvent lire le contenu de la nouvelle réplique, mais ils ne peuvent pas le modifier. Ce contenu est limité aux types d'objets et de propriétés eDirectory spécifiés dans un filtre.

6. Cliquez sur OK.

Pour plus d'informations, reportez-vous à la section « Types de répliques », page 53.

Configuration et gestion des répliques filtrées

Les répliques filtrées gèrent un sous-ensemble filtré d'informations d'une partition eDirectory (objets ou classes d'objets et ensemble filtré d'attributs et de valeurs de ces objets).

Les administrateurs utilisent généralement la fonction de réplique filtrée pour créer un serveur eDirectory qui contient un ensemble de répliques filtrées constitué uniquement d'objets et d'attributs spécifiques qui seront synchronisés.

Pour ce faire, iManager fournit des outils qui permettent de créer une étendue de partition de réplique filtrée et un filtre. Une étendue est tout simplement l'ensemble de partitions dont vous voulez placer les répliques sur un serveur. En revanche, un filtre de réplication contient l'ensemble des classes et des attributs eDirectory à héberger sur l'ensemble de répliques filtrées du serveur.

Le serveur eDirectory peut alors héberger un ensemble de données bien défini provenant de nombreuses partitions de l'arborescence.

La description de l'étendue des partitions et des filtres de réplication du serveur est stockée dans eDirectory. Elle peut être gérée via l'objet Serveur ou le rôle Partition et répliques dans iManager.

- « Utilisation de l'Assistant de répliques filtrées », page 141
- « Définition d'une étendue de partition », page 141
- « Configuration d'un filtre de serveur », page 142

Utilisation de l'Assistant de répliques filtrées

L'Assistant de répliques filtrées vous guide tout au long de la procédure de configuration d'un filtre de réplication et d'une étendue de partition de serveur.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Assistant de répliques filtrées.
3. Indiquez le serveur sur lequel une réplique filtrée doit être configurée, puis cliquez sur Suivant.
4. Pour définir les classes et les attributs d'un ensemble de filtres sur ce serveur, cliquez sur Définir l'ensemble de filtres.

   Le filtre de réplication contient l'ensemble des classes et des attributs eDirectory à héberger dans l'ensemble des répliques filtrées du serveur. Pour plus d'informations sur la définition d'un ensemble de filtres, reportez-vous à la section « Configuration d'un filtre de serveur », page 142.
5. Cliquez sur Suivant.
6. Pour définir l'étendue de la partition de ce serveur, cliquez sur Définir l'étendue de la partition.

   Pour plus d'informations sur les étendues de partition, reportez-vous à la section « Définition d'une étendue de partition », page 141.
7. Cliquez sur Suivant puis sur Terminer.

Définition d'une étendue de partition

Une étendue de partition est un ensemble de partitions dont vous voulez placer les répliques sur un serveur. La page Affichage des répliques de iManager offre une vue de la hiérarchie des partitions de l'arborescence eDirectory. Vous pouvez sélectionner les partitions une à une, un ensemble de partitions d'une branche donnée ou toutes les partitions de l'arborescence. Vous pouvez ensuite sélectionner le type des répliques de ces partitions à ajouter au serveur. Vous pouvez aussi modifier les types de répliques existantes.

Un serveur peut contenir à la fois des répliques complètes et des répliques filtrées. Pour plus d'informations, reportez-vous à la section « Répliques filtrées », page 56.

Affichage des répliques sur un serveur eDirectory

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Spécifiez le nom et le contexte du serveur à afficher, puis cliquez sur OK pour afficher la liste des répliques sur ce serveur.

Ajout d'une réplique filtrée à un serveur eDirectory

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Spécifiez le nom et le contexte du serveur auquel vous voulez ajouter une réplique filtrée, puis cliquez sur OK.
4. Cliquez sur Ajouter une réplique.
5. Spécifiez le nom et le contexte de la partition.
6. Cliquez sur Lecture/écriture filtrée ou sur Lecture seule filtrée puis cliquez sur OK.

Transformation d'une réplique complète en réplique filtrée

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Spécifiez le nom et le contexte de la partition ou du serveur qui contient la réplique à modifier, puis cliquez sur OK.
4. Cliquez sur le type (dans la colonne Type) de la réplique à modifier.
5. Cliquez sur Lecture/écriture filtrée ou sur Lecture seule filtrée puis cliquez sur OK.

Configuration d'un filtre de serveur

Un filtre de réplication de serveur contient l'ensemble des classes et des attributs eDirectory à héberger dans toutes les répliques filtrées du serveur. Vous pouvez configurer un filtre depuis n'importe quel objet Serveur. Pour les répliques filtrées, vous disposez uniquement d'un filtre par serveur. En d'autres termes, tout filtre défini pour un serveur eDirectory s'applique à l'ensemble des répliques filtrées de ce serveur. Ce filtre ne s'applique cependant pas aux répliques complètes.

Un filtre de serveur peut être modifié si nécessaire, mais cette opération génère une resynchronisation de la réplique et risque donc de prendre du temps. Il est recommandé de planifier attentivement la fonction du serveur.

Vous pouvez configurer ou modifier un filtre de serveur de l'une des façons suivantes :

- « Utilisation de l'affichage des répliques », page 142
- « Utilisation de l'objet Serveur », page 143

Utilisation de l'affichage des répliques

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Spécifiez le nom et le contexte de la partition ou du serveur qui contient la réplique à modifier, puis cliquez sur OK.
4. Cliquez sur Éditer dans la colonne Filtre du serveur ou de la partition à modifier.
5. Ajoutez les classes et les attributs désirés, puis cliquez sur OK.
6. Cliquez sur Terminé.

Utilisation de l'objet Serveur

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Modifier un objet.
3. Spécifiez le nom et le contexte du serveur qui contient la réplique à modifier, puis cliquez sur OK.
4. Cliquez sur l'onglet Réplique.
5. Si aucun filtre n'a été défini pour ce serveur, cliquez sur Le filtre est vide afin d'ouvrir la fenêtre Boîte de dialogue Éditer le filtre, puis ajoutez les classes et les attributs désirés.

   ou

   Cliquez sur Copier un filtre depuis pour rechercher un objet (un autre serveur, par exemple) dont vous voulez copier le filtre.
6. Pour éditer un filtre existant, cliquez sur un élément doté d'un hyperlien dans le filtre pour ouvrir la fenêtre Boîte de dialogue Éditer le filtre, puis ajoutez ou supprimez les classes et les attributs désirés.

Affichage des partitions et des répliques

Cette section comprend les informations suivantes :

Affichage des partitions d'un serveur

Vous pouvez afficher les partitions allouées à un serveur à l'aide de Novell iManager. Vous pouvez avoir besoin d'afficher les partitions stockées sur un serveur pour retirer un objet Serveur de l'arborescence Annuaire. Si tel est le cas, vous pouvez afficher les répliques à supprimer avant de retirer l'objet.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Entrez le nom et le contexte d'un objet Serveur, puis cliquez sur OK.

Affichage des répliques d'une partition

Cette opération vous permet d'identifier les éléments suivants :

- les serveurs sur lesquels se trouvent les répliques de la partition ;
- le serveur qui héberge la réplique maîtresse de la partition ;
- les serveurs qui hébergent les répliques Lecture/écriture, Lecture seule et de référence subordonnée de la partition ;
- l'état de chacune des répliques de la partition.

Pour afficher les répliques d'une partition, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Entrez le nom et le contexte d'une partition, puis cliquez sur OK.

Affichage des informations sur une partition

L'affichage des informations sur une partition permet principalement de contrôler sa synchronisation (dernière synchronisation réussie et dernière tentative de synchronisation).

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Afficher les informations sur la partition.
3. Entrez le nom et le contexte d'une partition, puis cliquez sur OK.

Affichage de la hiérarchie des partitions

Vous pouvez facilement afficher la hiérarchie des partitions dans iManager. Il est possible de développer des objets Conteneur pour afficher les partitions parentes et les partitions enfants.

Chaque conteneur qui représente la racine d'une partition est marqué par l'icône suivante :  .

Affichage des informations sur une réplique

L'affichage des informations sur une réplique permet principalement de contrôler son état. Une réplique eDirectory peut avoir différents états selon les opérations de partition ou de réplication exécutées. Le tableau suivant décrit les différents états de réplique que vous pouvez rencontrer dans iManager.

État	Description
Actif	Aucune opération de partition ni de réplication en cours
Nouveau	Réplique en cours d'ajout sur le serveur sous la forme d'une nouvelle réplique
Mourant	Réplique en cours de suppression du serveur
Mort	Réplique supprimée du serveur
Maîtresse - démarrage	Réplique en cours de transformation en une réplique maîtresse
Maîtresse - fin	Réplique transformée en une réplique maîtresse
Changement de type	Réplique en cours de changement de type
Verrouillé	Réplique verrouillée en préparation d'un déplacement de partition ou d'une réparation
Transition déplacement	Début de déplacement de partition
Déplacement	Déplacement de partition en cours
Transition - division	Début de division de partition (création d'une partition enfant)

État	Description
Division	Division de partition en cours (création d'une partition enfant)
Jonction	Réplique en cours de fusion avec la partition parente
Transition - actif	Réplique sur le point de retourner à l'état Actif
Inconnu	Réplique dans un état non connu de iManager

Pour afficher des informations sur une réplique, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Partition et répliques > Affichage des répliques.
3. Entrez le nom et le contexte d'une partition ou d'un serveur, puis cliquez sur OK.

6 Utilitaires de gestion de Novell eDirectory

Ce chapitre contient des informations sur les utilitaires Novell® eDirectory™ suivants :

Utilitaire d'importation, de conversion et d'exportation Novell

L'utilitaire d'importation, de conversion et d'exportation Novell vous permet d'effectuer les opérations suivantes :

- importer des données à partir de fichiers LDIF vers un annuaire LDAP ;
- exporter des données de l'annuaire LDAP vers un fichier LDIF ;
- migrer des données entre des serveursLDAP ;
- effectuer une comparaison et une mise à niveau de schéma ;
- charger des informations dans eDirectory à l'aide d'un modèle ;
- importer un schéma à partir de fichiers SCH dans un annuaire LDAP.

L'utilitaire d'importation, de conversion et d'exportation Novell contrôle un ensemble de gestionnaires qui lisent ou écrivent des données dans divers formats. Les gestionnaires source lisent les données et les gestionnaires cible les écrivent. Un module exécutable unique peut être à la fois un gestionnaire source et un gestionnaire cible. Le moteur reçoit des données d'un gestionnaire source, les traite, puis les transmet à un gestionnaire cible.

Par exemple, si vous souhaitez importer des données LDIF dans un annuaire LDAP, le moteur d'importation, de conversion et d'exportation Novell utilise un gestionnaire source LDIF pour lire le fichier LDIF et un gestionnaire cible LDAP pour transmettre ces données au serveur d'annuaire LDAP. Reportez-vous à la section « Dépannage des fichiers LDIF » pour plus d'informations sur la syntaxe, la structure et le débogage des fichiers LDIF.

Vous pouvez exécuter l'utilitaire d'importation, de conversion et d'exportation Novell à partir de la ligne de commande, d'un snap-in de ConsoleOne® ou de l'Assistant d'importation, de conversion et d'exportation de Novell iManager. Le gestionnaire de données séparées par une virgule n'est cependant disponible que dans l'utilitaire de ligne de commande et dans Novell iManager.

Vous pouvez exécuter l'utilitaire d'importation, de conversion et d'exportation Novell de l'une des manières suivantes :

- « Utilisation de l'Assistant Importation/Conversion/Exportation de Novell iManager », page 148
- « Utilisation de l'interface de ligne de commande », page 155

L'Assistant et l'interface de ligne de commande permettent d'accéder au moteur d'importation, de conversion et d'exportation Novell. L'interface de ligne de commande offre cependant des options supplémentaires pour combiner des gestionnaires source et cible.

L'utilitaire d'importation, de conversion et d'exportation Novell remplace à la fois les utilitaires BULKLOAD et ZONEIMPORT inclus dans les versions précédentes de NDS et eDirectory.

Utilisation de l'Assistant Importation/Conversion/Exportation de Novell iManager

L'Assistant Importation/Conversion/Exportation de Novell permet d'effectuer les opérations suivantes :

- importer des données à partir d'un fichier LDIF, d'un fichier texte délimité, d'un fichier de schéma ou d'un fichier LOAD ;
- exporter des données vers un fichier LDIF ;
- migrer des données entre des serveurs ;
- ajouter des données d'un fichier de schéma ou LDIF sur un serveur ;
- ajouter des données d'un serveur sur un autre ;
- comparer des données entre un fichier de schéma ou LDIF et un autre fichier LDIF ;
- comparer les données entre un serveur et un fichier LDIF ;
- générer un fichier d'ordre.

Pour plus d'informations sur l'accès à Novell iManager et sur son utilisation, consultez le manuel *Novell iManager 2.5 Administration Guide (Guide d'administration de Novell iManager 2.5)* (http://www.novell.com/documentation/imanager25/index.html).

Importation de données à partir d'un fichier

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.
3. Cliquez sur Importer les données depuis un fichier du disque, puis sur Suivant.
4. Sélectionnez le type de fichier à importer.
5. Entrez le nom du fichier qui contient les données à importer, spécifiez les options appropriées, puis cliquez sur Suivant.

   Les options de cette page dépendent du type de fichier que vous avez sélectionné. Pour plus d'informations sur les options disponibles, cliquez sur Aide.
6. Spécifiez le serveur LDAP dans lequel importer les données.
7. Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom DNS/Adresse IP du serveur	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de login	Login authentifié ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

8 Cliquez sur Suivant puis sur Terminer.

Exportation de données vers un fichier

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.

3 Cliquez sur Exporter les données vers un fichier du disque, puis sur Suivant.

4 Spécifiez le serveur LDAP comportant les entrées à exporter.

Les paramètres avancés vous permettent de configurer des options supplémentaires pour le gestionnaire source LDAP. Pour plus d'informations sur les options disponibles, cliquez sur Aide.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom DNS/Adresse IP du serveur	Nom DNS ou adresse IP du serveur LDAP source
Port	Numéro de port (nombre entier) du serveur LDAP source
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de login	Login authentifié ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

6 Cliquez sur Suivant.

7 Spécifiez les critères de recherche (décrits ci-dessous) relatifs aux entrées à exporter.

Option	Description
DN de base	Nom distinctif de base pour la requête de recherche Si vous ne renseignez pas ce champ, la valeur par défaut utilisée est «» (chaîne vide).
Étendue	Étendue de la requête de recherche
Filtre	Filtre de recherche conforme à la norme RFC1558 La valeur par défaut est objectclass=*.
Attributs	Attributs qui doivent vous être renvoyés pour chaque entrée de la recherche

8. Cliquez sur Suivant.
9. Sélectionnez le type de fichier d'exportation.

   Le fichier exporté est enregistré à un emplacement temporaire. Vous pouvez le télécharger à la fin de l'exécution de l'Assistant.
10. Cliquez sur Suivant puis sur Terminer.

Migration de données entre des serveursLDAP

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.
3. Cliquez sur Migrer les données entre les serveurs, puis sur Suivant.
4. Sélectionnez le serveur LDAP comportant les entrées à migrer.

   Les paramètres avancés vous permettent de configurer des options supplémentaires pour le gestionnaire source LDAP. Pour plus d'informations sur les options disponibles, cliquez sur Aide.
5. Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom DNS/Adresse IP du serveur	Nom DNS ou adresse IP du serveur LDAP source
Port	Numéro de port (nombre entier) du serveur LDAP source
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de login	Login authentifié ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

6. Cliquez sur Suivant.

7 Spécifiez les critères de recherche (décrits ci-dessous) relatifs aux entrées à migrer :

Option	Description
DN de base	Nom distinctif de base pour la requête de recherche Si vous ne renseignez pas ce champ, la valeur par défaut utilisée est «» (chaîne vide).
Étendue	Étendue de la requête de recherche
Filtre	Filtre de recherche conforme à la norme RFC2254 La valeur par défaut est objectclass=*.
Attributs	Attributs qui doivent vous être renvoyés pour chaque entrée de la recherche

8 Cliquez sur Suivant.

9 Spécifiez le serveur LDAP vers lequel les données doivent migrer.

10 Cliquez sur Suivant puis sur Terminer.

REMARQUE : vérifiez que le schéma est cohérent dans tous les services LDAP.

Mise à jour d'un schéma à partir d'un fichier

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.

3 Cliquez sur Ajouter un schéma depuis un fichier > Suivant.

4 Sélectionnez le type de fichier à ajouter.

Vous avez le choix entre les types Fichier LDIF et Fichier de schéma.

5 Entrez le nom du fichier qui contient le schéma à ajouter, spécifiez les options appropriées, puis cliquez sur Suivant.

Sélectionnez Ne pas ajouter mais comparer le schéma si vous souhaitez simplement comparer le schéma sans ajouter de schéma supplémentaire au serveur cible. Dans ce cas, le schéma supplémentaire n'est pas ajouté au serveur cible, mais les différences de schéma peuvent être affichées en cliquant sur le lien disponible à la fin de l'opération.

Les options de cette page dépendent du type de fichier que vous avez sélectionné. Pour plus d'informations sur les options disponibles, cliquez sur Aide.

6 Spécifiez le serveur LDAP dans lequel importer le schéma.

7 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom DNS/Adresse IP du serveur	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL

Option	Description
Méthode de login	Login authentifié ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

8 Cliquez sur Suivant > Terminer.

Ajout d'un schéma à partir d'un serveur

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.

3 Cliquez sur Ajouter un schéma depuis un serveur > Suivant.

4 Spécifiez le serveur LDAP à partir duquel ajouter le schéma.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom DNS/Adresse IP du serveur	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de login	Login authentifié ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

Sélectionnez Ne pas ajouter mais comparer le schéma si vous souhaitez simplement comparer le schéma sans ajouter de schéma supplémentaire au serveur cible. Dans ce cas, le schéma supplémentaire n'est pas ajouté au serveur cible, mais les différences de schéma peuvent être affichées en cliquant sur le lien disponible à la fin de l'opération.

6 Spécifiez le serveur LDAP dans lequel ajouter le schéma.

7 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom DNS/Adresse IP du serveur	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible

Option	Description
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de login	Login authentifié ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

8 Cliquez sur Suivant > Terminer.

Comparaison de fichiers de schéma

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.

3 Cliquez sur Comparer les fichiers de schéma > Suivant.

4 Sélectionnez le type de fichier à comparer.

Vous avez le choix entre les types Fichier LDIF et Fichier de schéma.

5 Entrez le nom du fichier qui contient le schéma à comparer, spécifiez les options appropriées, puis cliquez sur Suivant.

Les options de cette page dépendent du type de fichier que vous avez sélectionné. Pour plus d'informations sur les options disponibles, cliquez sur Aide.

6 Spécifiez le fichier de schéma avec lequel le comparer.

Vous pouvez uniquement sélectionner un fichier LDIF.

7 Cliquez sur Suivant > Terminer.

Pour afficher les différences entre les deux fichiers de schéma, cliquez sur le lien disponible à la fin de l'opération.

Comparaison de schéma à partir d'un serveur et d'un fichier

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.

3 Cliquez sur Comparer un schéma entre serveur et fichier > Suivant.

4 Spécifiez le serveur LDAP à partir duquel comparer le schéma.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom DNS/Adresse IP du serveur	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de login	Login authentifié ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

6 Sélectionnez le type de fichier avec lequel effectuer la comparaison.

7 Entrez le nom du fichier qui contient les données à comparer, spécifiez les options appropriées, puis cliquez sur Suivant.

Les options de cette page dépendent du type de fichier que vous avez sélectionné. Pour plus d'informations sur les options disponibles, cliquez sur Aide.

8 Cliquez sur Suivant > Terminer.

Pour afficher les différences entre le schéma du serveur et le fichier de schéma, cliquez sur le lien disponible à la fin de l'opération.

Génération d'un fichier d'ordre

Cette option crée un fichier d'ordre à utiliser avec le gestionnaire DELIM pour l'importation de données à partir d'un fichier de données séparées par une virgule. L'Assistant vous aide à créer ce fichier d'ordre qui contient une liste des attributs pour une classe d'objet spécifique.

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.

3 Cliquez sur Générer un fichier d'ordre, puis cliquez sur Suivant.

4 Sélectionnez la classe pour laquelle générer le fichier d'ordre, puis cliquez sur Afficher.

Sélectionnez les attributs à ajouter à la liste Attributs en séquence.

Sélectionnez la classe auxiliaire et ajoutez-la à la liste Classes auxiliaires sélectionnées.

Pour plus d'informations sur les listes Attributs en séquence et Classes auxiliaires, consultez l'aide en ligne de iMonitor.

Cliquez sur Suivant.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Contexte	Contexte auquel les objets créés sont associés
Sélectionner le fichier de données	Emplacement du fichier de données
Sélectionner le séparateur dans le fichier de données	Séparateur à utiliser dans le fichier de données. Le séparateur par défaut est une virgule (,)
Sélectionner l'attribut d'assignation de nom	Attributs d'assignation de nom de la liste des attributs disponibles pour la classe sélectionnée

Les paramètres avancés vous permettent de configurer des options supplémentaires pour le gestionnaire source LDAP. Pour plus d'informations sur les options disponibles, cliquez sur Aide.

Utilisez Enregistrements à traiter pour sélectionner les enregistrements à traiter dans le fichier de données. Pour plus d'informations sur les options disponibles, cliquez sur Aide.

6 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom DNS/Adresse IP du serveur	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de login	Login authentifié ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

Les paramètres avancés vous permettent de configurer des options supplémentaires pour le gestionnaire source LDAP. Pour plus d'informations sur les options disponibles, cliquez sur Aide.

7 Cliquez sur Suivant puis sur Terminer.

Utilisation de l'interface de ligne de commande

Vous pouvez faire appel à la version ligne de commande de l'utilitaire d'importation, de conversion et d'exportation Novell pour effectuer les opérations suivantes :

- importer des fichiers LDIF ;
- exporter des fichiers LDIF ;
- importer des données séparées par une virgule ;

- exporter des données séparées par une virgule ;
- migrer des données entre des serveurs LDAP ;
- comparer et mettre à jour des schémas ;
- charger des informations dans eDirectory à l'aide d'un modèle ;
- importer des schémas.

L'Assistant Importation/Conversion/Exportation Novell est installé avec Novell iManager. Une versionWin32* (ice.exe) et une version NetWare® (ice.nlm) sont incluses dans l'installation. Sur les systèmes Linux, Solaris, AIX et HP-UX, l'utilitaire d'importation et d'exportation est inclus dans le paquetage NOVLice.

Syntaxe d'importation, de conversion et d'exportation Novell

Pour lancer l'utilitaire d'importation, de conversion et d'exportation Novell, utilisez la syntaxe suivante :

```
ice options_générales
-S[LDIF | LDAP | DELIM | LOAD | SCH] options_source
-D[LDIF | LDAP | DELIM] options_cible
```

ou, si vous utilisez le cache de schéma :

```
ice -C options_schéma
-S[LDIF | LDAP] options_source
-D[LDIF | LDAP] options_cible
```

Un fichier LDIF ne représente pas une destination valide en cas de mise à jour au moyen du cache de schéma.

Les options générales sont facultatives ; elles doivent toutefois être définies avant toute option source ou cible. L'ordre des sections du gestionnaire -S (source) et -D (cible) est indifférent.

Ci-dessous la liste des gestionnaires source et cible disponibles :

- « Options du gestionnaire source LDIF », page 159
- « Options du gestionnaire cible LDIF », page 160
- « Options du gestionnaire source LDAP », page 160
- « Options du gestionnaire cible LDAP », page 162
- « Options du gestionnaire source DELIM », page 164
- « Options du gestionnaire cible DELIM », page 165
- « Options du gestionnaire source SCH », page 166
- « Options du gestionnaire source LOAD », page 166

Options générales

Les options générales ont une incidence sur l'ensemble du traitement effectué par le moteur d'importation, de conversion et d'exportation Novell.

Option	Description
-C	Indique que vous utilisez le cache de schéma pour procéder à la comparaison et à la mise à jour de schémas.
-l *fichier_journal*	Indique le nom du fichier dans lequel les messages de sortie (notamment les messages d'erreur) sont consignés. Si vous n'utilisez pas cette option, les messages d'erreur sont enregistrés dans le fichier ice.log. Si vous ne sélectionnez pas cette option sur les systèmes Linux, Solaris, AIX ou HP-UX, aucun message d'erreur ne sera consigné.
-o	Écrase le fichier journal existant. Si ce drapeau n'est pas défini, les messages sont annexés au fichier journal.
-e *fichier_journal_ erreurs_ LDIF*	Indique le nom du fichier dans lequel les entrées qui échouent sont consignées au format LDIF. Vous pouvez consulter ce fichier, le modifier afin de corriger les erreurs et l'appliquer de nouveau à l'annuaire.
-p *URL*	Indique l'emplacement de la règle de placement XML que le moteur doit utiliser. Les règles de placement permettent de modifier le placement d'une entrée. Pour plus d'informations, reportez-vous à la section « Règles de conversion », page 173.
-c *URL*	Indique l'emplacement de la règle de création XML que le moteur doit utiliser. Les règles de création vous permettent de fournir les informations manquantes dont peut dépendre la réussite de la création d'une entrée lors d'une importation. Pour plus d'informations, reportez-vous à la section « Règles de conversion », page 173.
-s *URL*	Indique l'emplacement de la règle d'assignation de schéma XML que le moteur doit utiliser. Les règles d'assignation de schéma vous permettent d'assigner un élément de schéma d'un serveur source à un élément de schéma différent mais équivalent sur un serveur cible. Pour plus d'informations, reportez-vous à la section « Règles de conversion », page 173.
-b (NetWare uniquement)	Permet de ne pas suspendre l'entrée au niveau de l'écran de la console ICE à la fin de l'exécution.
-h ou -?	Affiche l'aide relative à la ligne de commande.

Options de schéma

Les options de schéma vous permettent d'utiliser le cache de schéma pour effectuer des comparaisons et des mises à jour de schémas.

Option	Description
-C -a	Met à jour le schéma cible (ajoute le schéma manquant).
-C -c *nom_fichier*	Génère le schéma cible dans le fichier spécifié.
-C -n	Désactive la pré-vérification du schéma.

Options du gestionnaire source

L'option du gestionnaire source (-S) permet de déterminer la source des données à importer. Vous ne pouvez spécifier qu'une seule des options suivantes dans la ligne de commande.

Option	Description
-SLDIF	Indique que la source est un fichier LDIF. Pour obtenir la liste des options LDIF prises en charge, reportez-vous à la section « Options du gestionnaire source LDIF », page 159.
-SLDAP	Indique que la source est un serveur LDAP. Pour obtenir la liste des options LDAP prises en charge, reportez-vous à la section « Options du gestionnaire source LDAP », page 160.
-SDELIM	Indique que la source est un fichier de données séparées par une virgule. Pour obtenir la liste des options DELIM prises en charge, reportez-vous à la section « Options du gestionnaire source DELIM », page 164.
-SSCH	Indique que la source est un fichier de schéma. Pour obtenir la liste des options SCH prises en charge, reportez-vous à la section « Options du gestionnaire source SCH », page 166.
-SLOAD	Indique que la source est un modèle DirLoad. Pour obtenir la liste des options LOAD prises en charge, reportez-vous à la section « Options du gestionnaire source LOAD », page 166.

Options du gestionnaire cible

L'option du gestionnaire cible (-D) permet de déterminer la destination des données à exporter. Vous ne pouvez spécifier qu'une seule des options suivantes dans la ligne de commande.

Option	Description
-DLDIF	Indique que la destination est un fichier LDIF. Pour obtenir la liste des options prises en charge, reportez-vous à la section « Options du gestionnaire cible LDIF », page 160.
-DLDAP	Indique que la destination est un serveur LDAP. Pour obtenir la liste des options prises en charge, reportez-vous à la section « Options du gestionnaire cible LDAP », page 162.
-DDELIM	Indique que la destination est un fichier de données séparées par une virgule. Pour obtenir la liste des options prises en charge, reportez-vous à la section « Options du gestionnaire cible DELIM », page 165.

Options du gestionnaire source LDIF

Le gestionnaire source LDIF lit les données à partir d'un fichier LDIF, puis les transmet au moteur d'importation, de conversion et d'exportation Novell.

Option	Description
-f *fichier_LDIF*	Indique le nom du fichier qui contient les enregistrements LDIF que le gestionnaire source LDIF lit et transmet au moteur. Si vous ne spécifiez pas cette option sur les systèmes Linux, Solaris, AIX ou HP-UX, les données sont récupérées à partir de stdin.
-a	Si les enregistrements du fichier LDIF sont des enregistrements de contenu (c'est-à-dire qu'ils ne contiennent aucun type de modification), ils sont traités comme des enregistrements dont le type de modification est Ajouter (Add).
-c	Empêche le gestionnaire source LDIF de s'arrêter sur les erreurs. Cela comprend aussi bien les erreurs survenues au cours de l'analyse LDIF que celles renvoyées par le gestionnaire cible. Lorsque cette option est définie et qu'une erreur se produit, le gestionnaire source LDIF la signale, recherche l'enregistrement suivant dans le fichier LDIF et continue.
-e	Prévoit le schéma (DES / 3DES) qui sera utilisé pour le codage ou le décodage des attributs codés en provenance ou à destination du serveur LDAP, selon qu'il s'agisse d'une exportation ou d'une importation de données.
-E	Mot de passe pour le décodage des attributs codés présents dans le fichier LDIF.
-n	N'exécute pas les opérations de mise à jour, mais affiche les résultats qui seraient obtenus. Lorsque cette option est définie, le gestionnaire source LDIF analyse le fichier LDIF, mais n'envoie aucun enregistrement au moteur d'importation, de conversion et d'exportation Novell (ou au gestionnaire cible).
-m	Si les enregistrements du fichier LDIF sont des enregistrements de contenu (c'est-à-dire qu'ils ne contiennent aucun type de modification), ils sont traités comme des enregistrements dont le type de modification est Modifier (Modify).
-x	Si les enregistrements du fichier LDIF sont des enregistrements de contenu (c'est-à-dire qu'ils ne contiennent aucun type de modification), ils sont traités comme des enregistrements dont le type de modification est Supprimer (Delete).
-R *valeur*	Indique la plage d'enregistrements à traiter.
-v	Active le mode verbeux du gestionnaire.

Options du gestionnaire cible LDIF

Le gestionnaire cible LDIF reçoit les données transmises par le moteur d'importation, de conversion et d'exportation Novell et les écrit dans un fichier LDIF.

Option	Description
-f *fichier_LDIF*	Indique le nom du fichier pouvant consigner les enregistrements LDIF. Si vous ne spécifiez pas cette option sur les systèmes Linux, Solaris, AIX ou HP-UX, les données de sortie sont envoyées dans stdout.
-B	Indique de ne pas supprimer l'impression des valeurs binaires.
-b	Indique de ne pas coder au format base64 les données LDIF.
-e	Prévoit le schéma (DES / 3DES) qui sera utilisé pour le codage ou le décodage des attributs codés en provenance ou à destination du serveur LDAP, selon qu'il s'agisse d'une exportation ou d'une importation de données.
-E	Mot de passe pour le codage des attributs codés provenant du serveur LDAP.

Options du gestionnaire source LDAP

Le gestionnaire source LDAP lit les données d'un serveur LDAP en lui envoyant une requête de recherche. Il envoie ensuite au moteur d'importation, de conversion et d'exportation Novell les entrées résultant de cette opération de recherche.

Option	Description
-s *nom_serveur*	Indique le nom DNS ou l'adresse IP du serveur LDAP auquel le gestionnaire envoie une requête de recherche. L'hôte local est défini par défaut.
-p *port*	Désigne le numéro de port (nombre entier) du serveur LDAP indiqué par *nom_serveur*. Le numéro de port par défaut est 389. Pour les opérations sécurisées, le numéro de port par défaut est 636. Lorsque ICE communique avec un serveur LDAP sur le port SSL (636 par défaut) sans certificat, il choisit d'accepter n'importe quel certificat de serveur et suppose que celui-ci est approuvé. Cette option doit être utilisée uniquement dans des environnements contrôlés où une communication codée entre serveurs et clients est souhaitée mais la vérification serveur superflue.
-d *DN*	Indique le nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur.
-w *mot_de_passe*	Indique l'attribut de mot de passe de l'entrée spécifiée par *DN*.
-W	Invite à entrer le mot de passe de l'entrée spécifiée par *DN*. Cette option n'est applicable qu'aux systèmes Linux, Solaris, AIX et HP-UX.
-F *filtre*	Indique un filtre de recherche conforme à la norme RFC 1558. Si vous ne spécifiez pas cette option, la valeur par défaut utilisée est objectclass=*.
-n	N'exécute pas réellement la recherche, mais affiche un aperçu des résultats qui seraient obtenus.

Option	Description
-a *liste_attributs*	Indique la liste des attributs, séparés par une virgule, à récupérer au cours de la recherche. En plus des noms d'attribut, trois autres valeurs sont disponibles : ◆ Aucun attribut (1.1) ◆ Tous les attributs utilisateur (*) ◆ Une liste vide permet d'obtenir tous les attributs non opérationnels Si vous ne spécifiez pas cette option, la liste des attributs est par défaut une liste vide.
-o *liste_attributs*	Indique la liste des attributs, séparés par une virgule, à ne pas inclure dans les résultats de la recherche transmis par le serveur LDAP avant l'envoi au moteur. Cette option est pratique dans les cas où vous souhaitez utiliser un caractère générique avec l'option a afin d'obtenir tous les attributs d'une classe donnée, puis retirer certains d'entre eux des résultats de la recherche avant de transmettre les données au moteur. Par exemple, -a* -o Numéro_téléphone recherche tous les attributs de niveau utilisateur et filtre les numéros de téléphone dans les résultats.
-R	Indique de ne pas suivre automatiquement les renvois. Le paramétrage par défaut consiste à suivre les renvois avec le nom et le mot de passe spécifiés dans les options -d et -w.
-e *valeur*	Précise les drapeaux de débogage à activer dans le kit de développement (SDK) client LDAP. Pour plus d'informations, reportez-vous à la section « Utilisation des drapeaux de débogage SDK LDAP ».
-b *DN_base*	Indique le nom distinctif de base de la requête de recherche. Si cette option n'est pas définie, la valeur par défaut du nom distinctif de base est « » (chaîne vide).
-c *étendue_recherche*	Définit l'étendue de la requête de recherche. Les valeurs valides sont les suivantes : ◆ One : recherche uniquement les enfants immédiats de l'objet de base. ◆ Base : recherche uniquement l'entrée de l'objet de base. ◆ Sub : effectue la recherche dans la sous-arborescence racine LDAP, objet de base compris. Si vous ne définissez pas cette option, la valeur par défaut utilisée est Sub.

Option	Description
-r *suppr_réf_alias*	Indique le mode de suppression des références aux alias au cours de l'opération de recherche. Les valeurs sont les suivantes : ◆ Never : empêche le serveur de supprimer les références aux alias. ◆ Always : entraîne la suppression des références aux alias lors de la localisation de l'objet de base de la recherche et lors de l'évaluation d'entrées correspondant au filtre de recherche. ◆ Search : entraîne la suppression des références aux alias lors de l'application du filtre aux entrées dans l'étendue de la recherche après la localisation de l'objet de base, mais pas lors de cette localisation. ◆ Find : entraîne la suppression des références aux alias lors de la localisation de l'objet de base de la recherche, mais pas lors de l'évaluation des entrées correspondant au filtre de recherche. Si vous ne spécifiez pas cette option, la suppression des références aux alias prend par défaut la valeur Never.
-l *limite_temps*	Indique la limite temporelle (en secondes) de la recherche.
-z *limite_taille*	Indique le nombre maximal d'entrées que la recherche peut renvoyer.
-V *version*	Indique la version du protocole LDAP à utiliser pour la connexion. Cette valeur doit être 2 ou 3. Si cette option n'est pas définie, la valeur par défaut est 3.
-v	Active le mode verbeux du gestionnaire.
-L *nom_fichier*	Indique le fichier au format DER qui contient la clé de serveur utilisée pour l'authentification SSL.
-A	Récupère uniquement le nom des attributs. L'opération de recherche ne renvoie pas les valeurs des attributs.
-t	Empêche le gestionnaire LDAP de s'arrêter sur les erreurs.
-m	Les opérations LDAP seront des modifications.
-x	Les opérations LDAP seront des suppressions.
-k	Utilise SSL pour la connexion.
-M	Active la commande Gérer DSA IT.
-MM	Active la commande Gérer DSA IT et la rend prioritaire.

Options du gestionnaire cible LDAP

Le gestionnaire cible LDAP reçoit des données du moteur d'importation, de conversion et d'exportation Novell et les renvoie à un serveur LDAP sous forme d'opérations de mise à jour que le serveur doit exécuter.

Pour des informations sur les mots de passe codés dans les fichiers LDIF, reportez-vous à la section « Représentation des mots de passe codés dans les fichiers LDIF ».

Option	Description
-s *nom_serveur*	Indique le nom DNS ou l'adresse IP du serveur LDAP auquel le gestionnaire envoie une requête de recherche. L'hôte local est défini par défaut.
-p *port*	Désigne le numéro de port (nombre entier) du serveur LDAP indiqué par *nom_serveur*. Le numéro de port par défaut est 389. Pour les opérations sécurisées, le numéro de port par défaut est 636.
-d *DN*	Indique le nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur.
-w *mot_de_passe*	Indique l'attribut de mot de passe de l'entrée spécifiée par *DN*.
-W	Invite à entrer le mot de passe de l'entrée spécifiée par *DN*. Cette option n'est applicable qu'aux systèmes Linux, Solaris, AIX et HP-UX.
-B	Sélectionnez cette option si vous ne voulez pas utiliser des requêtes LBURP (LDAP Bulk Update/Replication Protocol) asynchrones pour transférer les mises à jour vers le serveur. À la place, utilisez des requêtes d'opération de mise à jour LDAP synchrones standard. Pour plus d'informations, reportez-vous à la section « Protocole LBURP », page 182.
-F	Autorise la création de références en aval. Lorsqu'une entrée doit être créée avant son parent, une marque de réservation appelée *référence en aval* est ajoutée pour le parent de cette entrée afin d'en assurer la création correcte. Si une opération ultérieure crée le parent, la référence en aval se transforme en entrée normale.
-I	Stocke les valeurs de mot de passe à l'aide de la méthode du mot de passe simple du service NMAS™ (Novell Modular Authentication Service). Les mots de passe sont conservés dans un emplacement sécurisé de l'annuaire ; les paires de clés ne sont pas générées tant qu'elles ne sont pas réellement requises pour l'authentification entre les serveurs. Cela améliore la vitesse de chargement d'un objet doté d'informations de mot de passe.
-e *valeur*	Précise les drapeaux de débogage à activer dans le kit de développement (SDK) client LDAP. Pour plus d'informations, reportez-vous à la section « Utilisation des drapeaux de débogage SDK LDAP ».
-V *version*	Indique la version du protocole LDAP à utiliser pour la connexion. Cette valeur doit être 2 ou 3. Si cette option n'est pas définie, la valeur par défaut est 3.
-L *nom_fichier*	Indique le fichier au format DER qui contient la clé de serveur utilisée pour l'authentification SSL.
-k	Utilise SSL pour la connexion.
-M	Active la commande Gérer DSA IT.
-MM	Active la commande Gérer DSA IT et la rend prioritaire.
-P	Active le traitement LBURP concurrent. Cette option n'est activée que si toutes les opérations dans LDIF sont des ajouts. Lorsque l'option -F est sélectionnée, -P est activé par défaut.
-Z	Indique le nombre de requêtes asynchrones. Cette option indique le nombre d'entrées que le client ICE peut envoyer au serveur LDAP en mode asynchrone avant d'attendre l'envoi des résultats par le serveur.

Options du gestionnaire source DELIM

Le gestionnaire source DELIM lit des données provenant d'un fichier de données séparées par une virgule, avant de les envoyer au gestionnaire cible.

Option	Description
-f *nom_fichier*	Indique le nom d'un fichier qui contient des enregistrements séparés par une virgule que le gestionnaire source DELIM lit et transmet au gestionnaire cible.
-F *valeur*	Indique le nom d'un fichier qui contient l'ordre des données d'attribut pour le fichier spécifié par f. Si cette option n'est pas définie, vous devez entrer directement cette information en utilisant t. Pour plus d'informations, reportez-vous à la section « Importation de données séparées par une virgule », page 169.
-t *valeur*	Liste des attributs, séparés par une virgule, indiquant l'ordre des données d'attribut pour le fichier spécifié par -f. Vous devez utiliser cette option ou l'option -F. Pour plus d'informations, reportez-vous à la section « Importation de données séparées par une virgule », page 169.
-c	Empêche le gestionnaire source DELIM de s'arrêter sur les erreurs. Cela comprend aussi bien les erreurs survenues au cours de l'analyse de fichiers de données séparées par une virgule que celles renvoyées par le gestionnaire cible. Lorsque cette option est définie et qu'une erreur se produit, le gestionnaire source DELIM la signale, recherche l'enregistrement suivant dans le fichier de données séparées par une virgule et continue.
-n *valeur*	Indique l'attribut d'assignation de nom LDAP du nouvel objet. Cet attribut doit être compris dans les données définies à l'aide des options -F ou -t.
-l *valeur*	Indique le chemin d'accès auquel le RDN doit être annexé (par exemple, o=maSociété). En cas de transmission du DN, cette valeur est facultative.
-o *valeur*	Liste des classes d'objet (si aucune ne figure dans votre fichier d'entrée) ou des classes d'objet supplémentaires, telles que les classes auxiliaires, séparées par une virgule. La valeur par défaut est inetorgperson.
-i *valeur*	Liste des colonnes à ignorer, séparées par des virgules. Cette valeur est un nombre entier correspondant au numéro de la colonne à ignorer. Par exemple, pour ignorer les troisième et cinquième colonnes, entrez i3,5.
-d *valeur*	Indique le séparateur. Le séparateur par défaut est une virgule (,). Les valeurs ci-dessous sont des séparateurs spéciaux : [q] = guillemet (guillemet " utilisé comme séparateur) [t] = tabulation Par exemple, pour indiquer qu'une tabulation est un séparateur, vous devez spécifier -d[t].

Option	Description
-q *valeur*	Indique le séparateur secondaire. Les guillemets simples (’ ’) sont utilisés comme séparateurs secondaires par défaut. Les valeurs ci-dessous sont des séparateurs spéciaux : [q] = guillemet (guillemet " utilisé comme séparateur) [t] = tabulation Par exemple, pour indiquer qu'une tabulation est un séparateur, vous devez spécifier -d[t].
-v	Exécution en mode verbeux.

Options du gestionnaire cible DELIM

Le gestionnaire cible DELIM reçoit les données provenant d'un gestionnaire source et les écrit dans un fichier de données séparées par une virgule.

Option	Description
-f *nom_fichier*	Indique le nom du fichier dans lequel des enregistrements séparés par une virgule peuvent être écrits.
-F *valeur*	Indique le nom d'un fichier qui contient l'ordre des données d'attribut pour les données source. Si cette option n'est pas définie, vous devez saisir directement cette information en utilisant -t.
-t *valeur*	Liste des attributs, séparés par une virgule, indiquant l'ordre des données d'attribut pour les données source. Cette option ou l'option -F doit être définie.
-l *valeur*	Peut être soit RDN ou DN. Indique si le pilote doit placer le DN entier, ou seulement le RDN, dans les données. Par défaut, seul le RDN est placé dans les données.
-d *valeur*	Indique le séparateur. Le séparateur par défaut est une virgule (,). Les valeurs ci-dessous sont des séparateurs spéciaux : [q] = guillemet (guillemet " utilisé comme séparateur) [t] = tabulation Par exemple, pour indiquer qu'une tabulation est un séparateur, vous devez spécifier -d[t].
-q *valeur*	Indique le séparateur secondaire. Les guillemets simples (’ ’) sont utilisés comme séparateurs secondaires par défaut. Les valeurs ci-dessous sont des séparateurs spéciaux : [q] = guillemet (guillemet " utilisé comme séparateur) [t] = tabulation Par exemple, pour indiquer qu'une tabulation est un séparateur, vous devez spécifier -d[t].
-n *valeur*	Indique un attribut d'assignation de nom à ajouter au cours de l'importation, par exemple, cn.

Options du gestionnaire source SCH

Le gestionnaire SCH lit les données à partir d'un fichier de schéma NDS ou eDirectory hérité (fichiers avec l'extension *.sch), puis les envoie au moteur d'importation, de conversion et d'exportation Novell. Vous pouvez utiliser ce gestionnaire pour mettre en oeuvre des opérations liées au schéma sur un serveur LDAP, par exemple des extensions avec un fichier *.sch en entrée.

Le gestionnaire SCH est uniquement un gestionnaire source. Vous pouvez l'utiliser pour importer des fichiers *.sch dans un serveur LDAP, mais pas pour en exporter.

Les options prises en charge par le gestionnaire SCH sont indiquées dans le tableau suivant.

Option	Description
-f *nom_fichier*	Indique le chemin d'accès complet au fichier *.sch.
-c	(Facultatif) Empêche le gestionnaire SCH de s'arrêter sur les erreurs.
-v	(Facultatif) Exécution en mode verbeux.

Options du gestionnaire source LOAD

Le gestionnaire DirLoad génère les informations eDirectory à partir des commandes d'un modèle. Ce fichier de modèle est spécifié avec l'argument -f et contient les informations de spécification d'attribut et les informations de contrôle de programme.

Option	Description
-f *nom_fichier*	Indique le fichier modèle qui contient toutes les spécifications d'attribut et toutes les informations de contrôle pour exécuter le programme.
-c	Continue l'exécution sur l'enregistrement suivant si une erreur est signalée.
-v	Exécution en mode verbeux.
-r	Transforme la requête en requête de suppression : les données sont supprimées au lieu d'être ajoutées. Cette option permet de supprimer des enregistrements ajoutés à l'aide d'un modèle DirLoad.
-m	Indique que le fichier modèle contient des demandes de modification.

Les spécifications d'attributs déterminent le contexte des nouveaux objets.

Reportez-vous à l'exemple de fichier de spécification d'attributs suivant :

```
givenname: $R(first)
initial: $R(initial)
sn: $R(last)
dn:cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn),ou=dev,ou=ds,o=novell
objectclass: inetorgperson
telephonenumber: 1-800-$N(1-999,%03d)-$C(%04d)
title: $R(titles)
locality: Our location
```

Le format du fichier de spécification d'attributs est semblable à celui d'un fichier LDIF. Cependant, il permet d'exploiter des structures performantes pour fournir des informations supplémentaires et définir des relations entre les attributs.

La valeur numérique unique insère dans une valeur d'attribut une valeur numérique unique pour un objet donné.

```
Syntaxe: $C[(<format)]
```

La variable facultative <*format* indique le format d'impression à appliquer à la valeur. Notez que si aucun format n'est spécifié, il est également impossible d'utiliser les parenthèses :

```
$C
$C(%d)
$C(%04d)
```

La séquence simple $C insère la valeur numérique courante dans une valeur d'attribut. Elle équivaut à $C(%d) car « %d » est le format par défaut utilisé par le programme si aucun autre format n'est spécifié. La valeur numérique est incrémentée après chaque objet : si vous utilisez $C à plusieurs reprises dans la spécification d'attribut, la valeur est identique pour un même objet. La valeur initiale peut être spécifiée dans le fichier de paramètres à l'aide de la syntaxe !COUNTER=*valeur*.

La valeur numérique aléatoire insère une valeur numérique aléatoire dans une valeur d'attribut, conformément à la syntaxe suivante :

```
$N(<bas-<haut[,<format])]
```

Les variables <*bas* et <*haut* fixent respectivement les limites inférieure et supérieure employées pour générer un nombre aléatoire. La variable facultative <*format* indique le format d'impression à appliquer à une valeur de la liste.

```
$N(1-999)
$N(1-999,%d)
$N(1-999,%03d)
```

La valeur de chaîne aléatoire provenant d'une liste insère dans une valeur d'attribut une chaîne sélectionnée de façon aléatoire dans une liste spécifiée, conformément à la syntaxe suivante :

```
$R(<nom_fichier[,<format])]
```

La variable <*nom_fichier* désigne un fichier qui contient une liste de valeurs. Il peut s'agir du chemin absolu ou relatif d'un fichier. Divers fichiers contenant les listes sont inclus avec ce paquetage. Les valeurs doivent être séparées par un caractère de retour à la ligne.

La variable facultative <*format* indique le format d'impression à appliquer à une valeur de la liste.

```
$A(givenname)
$A(givenname,%s)
$A(givenname,%.1s)
```

Notez que les références en aval ne sont pas autorisées. Tout attribut dont vous prévoyez d'utiliser la valeur doit précéder l'attribut actuel dans le fichier de spécification d'attributs. Dans l'exemple ci-dessous, le cn, en tant qu'élément du dn, est constitué à partir de givenname, initial et sn. Par conséquent, ces attributs doivent précéder le dn dans le fichier de paramètres.

```
givenname: $R(first)
initial: $R(initial)
sn: $R(last)
dn:o=novell,ou=dev,ou=ds,cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn)
```

Le dn fait l'objet d'un traitement particulier dans le fichier LDIF : quel que soit son emplacement dans les paramètres, il sera écrit en premier (conformément à la syntaxe LDIF) dans le fichier LDIF. Tous les autres attributs sont écrits dans l'ordre dans lequel ils apparaissent.

Les paramètres de contrôle fournissent des contrôles supplémentaires pour la création d'objets. Pour tous les contrôles, un point d'exclamation (!) figure en début de ligne et permet de les distinguer des paramètres d'attribut. Les contrôles peuvent apparaître n'importe où dans le fichier.

```
!COUNTER=300
!OBJECTCOUNT=2
!CYCLE=title
!UNICYCLE=first,last
!CYCLE=ou,BLOCK=10
```

- Counter (Compteur)

  Fournit la valeur initiale pour la valeur de compteur unique. La valeur du compteur est insérée dans tout attribut avec la syntaxe $C.

- Object Count (Nombre d'objets)

  Le paramètre OBJECTCOUNT détermine le nombre d'objets créés à partir du modèle.

- Cycle

  Le paramètre CYCLE peut servir à modifier le mode d'extraction des valeurs aléatoires à partir des fichiers (syntaxe $R). Il peut présenter trois valeurs.

  ```
  !CYCLE=title
  ```

  Dès que la liste nommée « title » (titre) est utilisée, le système extrait la valeur suivante de la liste au lieu de sélectionner une valeur de façon aléatoire. Une fois toutes les valeurs utilisées dans l'ordre, la liste reprend au début.

  ```
  !CYCLE=ou,BLOCK=10
  ```

  Chaque valeur de la liste « ou » doit être utilisée 10fois avant de passer à la valeur suivante.

  La variante la plus intéressante du paramètre de contrôle CYCLE est UNICYCLE. Elle indique une liste de sources qui sont parcourues de façon cyclique de gauche à droite, permettant ainsi de créer, si nécessaire, des valeurs dont l'unicité est garantie. En cas d'emploi de ce contrôle, le contrôle OBJECTCOUNT sert uniquement à limiter le nombre d'objets au nombre maximum d'objets uniques pouvant être créés à partir des listes. En d'autres termes, si les listes désignées dans UNICYCLE peuvent produire 15 000 objets, OBJECTCOUNT peut servir à réduire ce nombre, mais pas à l'augmenter.

  Par exemple, supposons que le fichier « givenname » contienne deux valeurs (Doug et Karl) et que le fichier « sn » en contienne trois (Hoffman, Schultz et Grieger). Avec le paramètre de contrôle !UNICYCLE=givenname,sn et la définition d'attribut cn : $R(givenname) $R(sn), les cn suivants sont créés :

  cn: Doug Hoffmancn
  cn: Karl Hoffmancn
  cn: Doug Schultzcn
  cn: Karl Schultzcn
  cn: Doug Griegercn
  cn: Karl Grieger

Exemples

Vous trouverez ci-dessous plusieurs exemples de commandes auxquelles vous pouvez faire appel via l'utilitaire de ligne de commande d'importation, de conversion et d'exportation Novell pour exécuter les fonctions suivantes :

- « Exécution d'une importation LDIF », page 169
- « Exécution d'une exportationLDIF », page 169

Exécution d'une importation LDIF

Pour exécuter une importation LDIF, associez le gestionnaire source LDIF et le gestionnaire cible LDAP. Par exemple :

```
ice -S LDIF -f entries.ldif -D LDAP -s server1.acme.com -p 389 -d
cn=admin,c=us -w secret
```

Cette ligne de commande permet de lire les données LDIF à partir du fichier entries.ldif et de les envoyer au serveur LDAP server1.acme.com sur le port 389 à l'aide de l'identité cn=admin,c=us et du mot de passe « secret ».

Exécution d'une exportationLDIF

Pour effectuer une exportation LDIF, associez le gestionnaire source LDAP et le gestionnaire cible LDIF. Par exemple :

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D LDIF -f server1.ldif
```

Cette ligne de commande permet de rechercher dans une sous-arborescence tous les objets situés sur le serveur server1.acme.com au niveau du port 389, à l'aide de l'identité cn=admin,c=us et du mot de passe « password », ainsi que de générer les données au format LDIF dans le fichier server1.ldif.

Importation de données séparées par une virgule

Pour exécuter une importation délimitée par des virgules, utilisez une commande similaire à la suivante :

```
ice -S DELIM -f/tmp/in.csv -F /tmp/order.csv -ncn -lo=acme -D LDAP -s
server1.acme.com -p389 -d cn=admin,c=us -w secret
```

Cette commande lit les données séparées par une virgule du fichier /tmp/in.csv ainsi que l'ordre des attributs, défini dans le fichier /tmp/order.csv. Le type des attributs du fichier in.csv est défini dans le fichier order.csv. Par exemple, si le fichier in.csv contient

```
pat,pat,engineer,john
```

le fichier order.csv contient

```
dn,cn,title,sn
```

Les informations du fichier order.csv peuvent être saisies directement à l'aide de l'option -t.

Les données sont ensuite envoyées au serveur LDAP server1.acme.com sur le port 389 à l'aide de l'identité cn=admin,c=us et du mot de passe « secret ».

Dans cet exemple, nous avons utilisé l'option -n pour indiquer que cn devait devenir le nouveau DN pour cet objet, et l'option -l pour ajouter cet objet au conteneur Organisation acme.

Exportation de données séparées par une virgule

Pour exécuter une exportation délimitée par des virgules, utilisez une commande similaire à la suivante :

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -l
objectClass=* -c sub -D DELIM -f /tmp/server1.csv -F order.csv
```

Cette ligne de commande permet de rechercher dans une sous-arborescence tous les objets situés sur le serveur server1.acme.com au niveau du port 389, à l'aide de l'identité cn=admin,c=us et du mot de passe « password », ainsi que de générer les données, séparées par une virgule, dans le fichier /tmp/server1.csv.

Exécution d'une migration de données entre des serveurs LDAP

Pour exécuter une migration de données entre des serveurs LDAP, associez les gestionnaires source et cible LDAP. Par exemple :

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D LDAP -s server2.acme.com -p 389 -d cn=admin,c=us -w
secret
```

Cette ligne de commande permet de rechercher dans une sous-arborescence tous les objets situés sur le serveur server1.acme.com au niveau du port 389, à l'aide de l'identité cn=admin,c=us et du mot de passe « password », ainsi que d'envoyer les données au serveur LDAP server2.acme.com sur le port 389 à l'aide de l'identité cn=admin,c=us et du mot de passe « secret ».

Exécution d'une importation de schéma

Pour exécuter une importation de schéma, utilisez une commande similaire à la suivante :

```
ice -S SCH -f $HOME/myfile.sch -D LDAP -s myserver -d cn=admin,o=novell -w
passwd
```

Cette ligne de commande permet de lire les données de schéma à partir du fichier myfile.sch et de les envoyer au serveur LDAP myserver à l'aide de l'identité cn=admin,o=novell et du mot de passe « passwd ».

Exécution d'une importation de fichier LOAD

Pour exécuter une importation de fichier LOAD, utilisez une commande similaire à la suivante :

```
ice -S LOAD -f attrs -D LDIF -f new.ldf
```

Dans cet exemple, le contenu du fichier d'attributs attrs est le suivant :

```
#=====================================================================

#  DirLoad 1.00
#=====================================================================

!COUNTER=300

!OBJECTCOUNT=2
#---------------------------------------------------------------------

#  ATTRIBUTE TEMPLATE
# ---------------------------------------------------------------------

objectclass: inetorgperson

givenname: $R(first)
```

```
initials: $R(initial)

sn: $R(last)

dn: cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn),ou=$R(ou),ou=dev,o=novell,

telephonenumber: 1-800-$N(1-999,%03d)-$C(%04d)

title: $R(titles)
```

L'exécution de la commande précédente à partir de l'invite de commande génère le fichier LDIF suivant :

```
version : 1

dn: cn=JohnBBill,ou=ds,ou=dev,o=novell

changetype: add

objectclass: inetorgperson

givenname: John

initials: B

sn: Bill

telephonenumber: 1-800-290-0300

title: Amigo


dn: cn=BobJAmy,ou=ds,ou=dev,o=novell

changetype: add

objectclass: inetorgperson

givenname: Bob

initials: J

sn: Amy

telephonenumber: 1-800-486-0301

title: Pomo
```

L'exécution de la commande suivante à partir de l'invite de commande entraîne l'envoi des données à un serveur LDAP via le gestionnaire LDAP :

```
ice -S LOAD -f attrs -D LDAP -s www.novell.com -d cn=admin,o=novell -w admin
```

Si le fichier modèle précédent est utilisé avec la ligne de commande suivante, tous les enregistrements ajoutés via la commande ci-dessus sont supprimés.

```
ice -S LOAD -f attrs -r -D LDAP -s www.novell.com -d cn=admin,o=novell -w
admin
```

L'exemple ci-dessous illustre comment modifier des enregistrements à l'aide du paramètre m :

```
# ======================================================================
#  DirLoad 1.00
# ======================================================================
!COUNTER=300
!OBJECTCOUNT=2
#----------------------------------------------------------------------
#  ATTRIBUTE TEMPLATE
# ----------------------------------------------------------------------
dn: cn=$R(first),%.1s)($R(initial),%.1s)$R(last),ou=$R(ou),ou=dev,o=novell
delete: givenname
add: givenname
givenname: test1
replace: givenname
givenname: test2
givenname: test3
```

Si le fichier attrs contient les données ci-dessus et que vous utilisez la commande suivante :

```
ice -S LOAD -f attrs -m -D LDIF -f new.ldf
```

les données LDIF suivantes sont générées :

```
version : 1
dn: cn=BillTSmith,ou=ds,ou=dev,o=novell
changetype: modify
delete: givenname
-
add: givenname
givenname: test1
-
replace: givenname
givenname: test2
givenname: test3
-
dn: cn=JohnAWilliams,ou=ldap,ou=dev,o=novell
changetype: modify
```

```
delete: givenname

-

add: givenname

givenname: test1

-

replace: givenname

givenname: test2

givenname: test3

-
```

Règles de conversion

Le moteur d'importation, de conversion et d'exportation Novell permet de définir un ensemble de règles qui décrivent les opérations de traitement à réaliser sur chaque enregistrement reçu du gestionnaire source, avant sa transmission au gestionnaire cible. Ces règles sont définies au format XML (sous la forme soit d'un fichier XML, soit de données XML stockées dans l'annuaire) et résolvent les problèmes suivants lors de l'importation d'entrées depuis un annuaire LDAP vers un autre :

- informations manquantes ;
- différences hiérarchiques ;
- différences de schéma.

Trois types de règle de conversion sont disponibles :

Règle	Description
Placement	Modifie le placement d'une entrée. Par exemple, si vous importez un groupe d'utilisateurs dans le conteneur l=San Francisco, c=US et que vous souhaitez ensuite placer ces utilisateurs dans le conteneur l=Los Angeles, c=US une fois l'importation terminée, vous pouvez le faire en utilisant une règle de placement. Pour plus d'informations sur le format de ces règles, reportez-vous à la section « Règles de placement », page 178.
Création	Fournit les informations manquantes qui peuvent s'avérer nécessaires à la création d'une entrée lors de l'importation. Par exemple, supposons que vous ayez exporté des données LDIF à partir d'un serveur dont le schéma requiert uniquement l'attribut cn (commonName) pour les entrées utilisateur, mais que le serveur dans lequel vous importez ces données LDIF nécessite à la fois les attributs cn et sn (surname). Vous pouvez alors utiliser la règle de création pour fournir une valeur sn par défaut (telle que « ») pour chacune des entrées lors de leur traitement par le moteur. Lorsque ces entrées sont envoyées au serveur cible, elles contiennent l'attribut sn requis et leur ajout peut s'effectuer correctement. Pour plus d'informations sur le format de ces règles, reportez-vous à la section « Règles de création », page 176.

Règle	Description
Assignation de schéma	Si, lors du transfert de données entre des serveurs (directement ou via LDIF), il existe des différences entre les schémas des serveurs, vous pouvez utiliser la règle Assignation de schéma pour effectuer les opérations suivantes : ◆ étendre le schéma sur le serveur cible afin d'intégrer les classes d'objet et les types d'attribut dans des entrées provenant du serveur source ; ◆ assigner un élément de schéma du serveur source à un élément de schéma différent mais équivalent sur le serveur cible. Pour plus d'informations sur le format de ces règles, reportez-vous à la section « Règles d'assignation de schéma », page 175.

Vous pouvez activer les règles de conversion dans l'Assistant d'importation et d'exportation Novell eDirectory, ainsi que dans l'interface de ligne de commande. Pour plus d'informations sur les règles XML, reportez-vous à la section « Utilisation des règles XML », page 175.

Utilisation de l'Assistant d'importation, de conversion et d'exportation Novell eDirectory

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.
3. Sélectionnez la tâche à exécuter.
4. Dans Paramètres avancés, sélectionnez l'une des options suivantes :

Option	Description
Règles de schéma	Indique l'emplacement de la règle d'assignation de schéma XML que le moteur doit utiliser.
Règles de placement	Indique l'emplacement de la règle de placement XML que le moteur doit utiliser.
Règles de création	Indique l'emplacement de la règle de création XML que le moteur doit utiliser.

5. Cliquez sur Suivant.
6. Suivez les instructions en ligne pour terminer la tâche sélectionnée.

Utilisation de l'interface de ligne de commande

Vous pouvez activer les règles de conversion à l'aide des options générales -p, -c et -s dans l'exécutable de l'utilitaire d'importation, de conversion et d'exportation Novell. Pour plus d'informations, reportez-vous à la section « Options générales », page 157.

Option	Description
-p *URL*	Emplacement de la règle de placement XML que le moteur doit utiliser.
-c *URL*	Emplacement de la règle de création XML que le moteur doit utiliser.
-s *URL*	Emplacement de la règle d'assignation de schéma XML que le moteur doit utiliser.

Pour ces trois options, la variable *URL* doit se présenter comme suit :

- URL au format suivant :

  `file://[chemin/]nom_fichier`

  Le fichier doit se trouver sur le système de fichiers local.

- URL LDAP conforme à la norme RFC2255 qui spécifie une recherche de niveau de base et une liste d'attributs comportant la description d'un seul attribut pour un type d'attribut à valeur unique.

Utilisation des règles XML

Les règles de conversion de l'utilitaire d'importation, de conversion et d'exportation Novell utilisent le même format XML que Novell Nsure Identity Manager. Pour plus d'informations sur Novell Nsure Identity Manager, consultez le manuel *DirXML Administration Guide (Guide d'administration de DirXML)*. (http://www.novell.com/documentation/dirxml20/index.html)

Règles d'assignation de schéma

L'élément <attr-name-map> est l'élément le plus élevé pour les règles d'assignation de schéma. Les règles d'assignation déterminent le mode d'interaction du schéma d'importation avec le schéma d'exportation. Elles associent les définitions et les attributs de classe d'importation indiqués aux définitions correspondantes dans le schéma d'exportation.

Vous pouvez définir des règles d'assignation pour des noms d'attribut ou des noms de classe.

- Pour une assignation d'attribut, la règle doit spécifier qu'il s'agit d'une assignation d'attribut, mais elle doit également indiquer un espace de noms (nds-name est la balise pour le nom source), le nom dans l'espace de noms eDirectory, puis l'autre espace de noms (app-name est la balise pour le nom cible) et le nom dans ce dernier. Elle peut indiquer que l'assignation s'applique à une classe particulière ou à toutes les classes comportant l'attribut.
- Pour une assignation de classe, la règle doit spécifier qu'il s'agit d'une assignation de classe, mais elle doit également indiquer un espace de noms (eDirectory ou l'application) et le nom dans cet espace, ainsi que l'autre espace de noms et le nom dans ce dernier.

Voici la DTD formelle des règles d'assignation de schéma :

```
<!ELEMENT attr-name-map (attr-name | class-name)*>

<!ELEMENT attr-name (nds-name, app-name)>
<!ATTLIST attr-name
          class-name    CDATA    #IMPLIED>

<!ELEMENT class-name (nds-name, app-name)>

<!ELEMENT nds-name (#PCDATA)>

<!ELEMENT app-name (#PCDATA)>
```

Le fichier peut comporter plusieurs éléments d'assignation. Chaque élément est traité dans l'ordre où il apparaît dans le fichier. Si vous assignez la même classe ou le même attribut plusieurs fois, c'est la première assignation qui est prioritaire.

Les exemples suivants illustrent la création d'une règle d'assignation de schéma.

Règle d'assignation de schéma 1 : la règle suivante assigne l'attribut « surname » source à l'attribut « sn » cible pour la classe inetOrgPerson.

```
<attr-name-map>
   <attr-name class-name="inetOrgPperson">
      <nds-name>surname</nds-name>
      <app-name>sn</app-name>
   </attr-name>
</attr-name-map>
```

Règle d'assignation de schéma 2 : la règle suivante assigne la définition de classe inetOrgPerson source à la définition de classe User cible.

```
<attr-name-map>
   <class-name>
      <nds-name>inetOrgPerson</nds-name>
      <app-name>User</app-name>
   </class-name>
</attr-name-map>
```

Règle d'assignation de schéma 3 : l'exemple suivant contient deux règles. La première règle assigne l'attribut « surname » source à l'attribut « sn » cible pour toutes les classes qui utilisent ces attributs. La deuxième règle assigne la définition de classe inetOrgPerson source à la définition de classe User cible.

```
<attr-name-map>
   <attr-name>
      <nds-name>surname</nds-name>
      <app-name>sn</app-name>
   </attr-name>
   <class-name>
      <nds-name>inetOrgPerson</nds-name>
      <app-name>User</app-name>
   </class-name>
</attr-name-map>
```

Exemple de commande : si les règles de schéma sont enregistrées dans un fichier sr1.xml, la commande suivante demande à l'utilitaire de les exploiter lors du traitement du fichier 1entry.ldf et d'envoyer les résultats dans un fichier cible, outt1.ldf.

```
ice -o -sfile://sr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

Règles de création

Les règles de création spécifient les conditions de création d'une entrée dans l'annuaire cible. Elles prennent en charge les éléments suivants :

- **Attributs requis (required-attr) :** indique qu'un enregistrement d'ajout doit avoir des valeurs pour tous les attributs requis, faute de quoi l'ajout échoue. La règle peut fournir une valeur par défaut pour un attribut requis. Si un enregistrement n'a pas de valeur pour cet attribut, l'entrée se voit attribuer la valeur par défaut. Si l'enregistrement possède une valeur, celle-ci est utilisée.
- **Attributs correspondants (match-attr) :** indique qu'un enregistrement d'ajout doit avoir les attributs spécifiés et que leurs valeurs doivent correspondre à celles indiquées, faute de quoi l'ajout échoue.
- **Modèles (template) :** indique le nom distinctif d'un objet Modèle dans eDirectory. Actuellement, l'utilitaire d'importation, de conversion et d'exportation Novell ne prend pas en charge la spécification de modèles dans les règles de création.

Voici la DTD formelle des règles de création :

```
<!ELEMENT create-rules (create-rule)*>

<!ELEMENT create-rule (match-attr*,
                       required-attr*,
                       template?) >
<!ATTLIST create-rule
          class-name    CDATA   #IMPLIED
          description   CDATA   #IMPLIED>

<!ELEMENT match-attr    (value)+ >
<!ATTLIST match-attr
          attr-name      CDATA    #REQUIRED>

<!ELEMENT required-attr (value)*>
<!ATTLIST required-attr
          attr-name     CDATA   #REQUIRED>

<!ELEMENT template EMPTY>
<!ATTLIST template
          template-dn   CDATA   #REQUIRED>
```

Le fichier peut comporter plusieurs éléments de règle de création. Chaque règle est traitée dans l'ordre où elle apparaît dans le fichier. Si un enregistrement ne correspond à aucune des règles, il est ignoré sans pour autant générer une erreur.

Les exemples suivants illustrent comment formater des règles de création.

Règle de création 1 : la règle suivante pose trois conditions sur les enregistrements d'ajout qui appartiennent à la classe inetOrgPerson. Ces enregistrements doivent posséder les attributs givenName et Surname. Ils doivent posséder un attribut L, mais si ce n'est pas le cas, la règle de création leur fournit une valeur par défaut de Provo.

```
<create-rules>
   <create-rule class-name="inetOrgPerson">
      <required-attr attr-name="givenName"/>
      <required-attr attr-name="surname"/>
      <required-attr attr-name="L">
         <value>Provo</value>
      </required-attr>
   </create-rule>
</create-rules>
```

Règle de création 2 : la règle de création suivante pose trois conditions sur tous les enregistrements d'ajout, quelle que soit leur classe de base.

- L'enregistrement doit contenir un attribut givenName. Si ce n'est pas le cas, l'ajout échoue.
- L'enregistrement doit contenir un attribut Surname. Si ce n'est pas le cas, l'ajout échoue.
- L'enregistrement doit contenir un attribut L. Si ce n'est pas le cas, l'attribut se voit assigner une valeur de Provo.

```
<create-rules>
   <create-rule>
      <required-attr attr-name="givenName"/>
      <required-attr attr-name="Surname"/>
      <required-attr attr-name="L">
         <value>Provo</value>
```

```
      </required-attr>
   </create-rule>
</create-rules>
```

Règle de création 3 : la règle de création suivante pose deux conditions sur tous les enregistrements, quelle que soit leur classe de base.

- La règle vérifie si l'enregistrement contient un attribut uid avec une valeur de ratuid. Si ce n'est pas le cas, l'ajout échoue.
- La règle vérifie si l'enregistrement possède un attribut L. Si ce n'est pas le cas, l'attribut L se voit attribuer une valeur de Provo.

```
<create-rules>
   <create-rule>
      <match-attr attr-name="uid">
         <value>cn=ratuid</value>
      </match-attr>
      <required-attr attr-name="L">
         <value>Provo</value>
      </required-attr>
   </create-rule>
</create-rules>
```

Exemple de commande : si les règles de création sont enregistrées dans un fichier crl.xml, la commande suivante demande à l'utilitaire de les exploiter lors du traitement du fichier 1entry.ldf et d'envoyer les résultats dans un fichier cible, outt1.ldf.

```
ice -o -cfile://cr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

Règles de placement

Les règles de placement déterminent la position des entrées créées dans l'annuaire cible. Elles prennent en charge les conditions suivantes afin de déterminer si la règle doit être utilisée pour placer une entrée :

- **Classe de concordance (match-class) :** si la règle contient des éléments de classe de concordance (match-class), un attribut objectClass spécifié dans l'enregistrement doit correspondre à l'attribut class-name de la règle. Si la correspondance échoue, la règle de placement n'est pas utilisée pour cet enregistrement.
- **Attribut de concordance (match-attr) :** si la règle contient des éléments d'attribut de concordance (match-attr), l'enregistrement doit contenir une valeur d'attribut pour chacun des attributs spécifiés dans l'élément d'attribut de concordance. Si la correspondance échoue, la règle de placement n'est pas utilisée pour cet enregistrement.
- **Chemin de concordance (match-path) :** si la règle contient des éléments de chemin de concordance (match-path), une partie du dn de l'enregistrement doit correspondre au préfixe indiqué dans l'élément de chemin de concordance. Si la correspondance échoue, la règle de placement n'est pas utilisée pour cet enregistrement.

Le dernier élément de la règle indique où placer l'entrée. La règle de placement peut utiliser un ou plusieurs des éléments suivants, ou aucun :

- **PCDATA :** utilise des données de caractère analysées pour préciser le DN d'un conteneur pour les entrées.
- **Copier le nom (copy-name) :** indique que l'attribut d'assignation de nom de l'ancien DN est utilisé dans le nouveau DN de l'entrée.

- **Copier l'attribut (copy-attr) :** indique l'attribut d'assignation de nom à utiliser dans le nouveau DN de l'entrée. L'attribut d'assignation de nom spécifié doit être un attribut valide pour la classe de base de l'entrée.
- **Copier le chemin (copy-path) :** indique que le DN source doit être utilisé comme DN cible.
- **Copier le suffixe du chemin (copy-path-suffix) :** indique que le DN source, ou une partie de son chemin, doit être utilisé comme DN cible. Si un élément match-path est spécifié, seule la partie de l'ancien DN qui ne correspond pas à l'attribut de préfixe (prefix) de cet élément est utilisée comme composant du DN de l'entrée.

Voici la DTD formelle de la règle de placement :

```
<!ELEMENT placement-rules (placement-rule*)>
<!ATTLIST placement-rules
          src-dn-format    (%dn-format;)   "slash"
          dest-dn-format   (%dn-format;)   "slash"
          src-dn-delims    CDATA           #IMPLIED
          dest-dn-delims   CDATA           #IMPLIED>

<!ELEMENT placement-rule (match-class*,
                          match-path*,
                          match-attr*,
                          placement)>
<!ATTLIST placement-rule
          description      CDATA            #IMPLIED>

<!ELEMENT match-class      EMPTY>
<!ATTLIST match-class
          class-name       CDATA            #REQUIRED>

<!ELEMENT match-path       EMPTY>
<!ATTLIST match-path
          prefix           CDATA            #REQUIRED>

<!ELEMENT match-attr       (value)+ >
<!ATTLIST match-attr
          attr-name        CDATA            #REQUIRED>

<!ELEMENT placement        (#PCDATA |
                           copy-name |
                           copy-attr |
                           copy-path |
                           copy-path-suffix)* >
```

Le fichier peut comporter plusieurs éléments de règle de placement. Chaque règle est traitée dans l'ordre où elle apparaît dans le fichier. Si un enregistrement ne correspond à aucune des règles, il est ignoré sans pour autant générer une erreur.

Les exemples ci-dessous illustrent comment formater des règles de placement. Les attributs scr-dn-format="ldap" et dest-dn-format="ldap" définissent la règle de façon à ce que l'espace de noms relatif au dn de la source et de la cible soit au format LDAP.

L'utilitaire d'importation, de conversion et d'exportation Novell ne prend en charge que les noms de source et de cible au format LDAP.

Exemple de placement 1 : la règle de placement suivante exige que l'enregistrement comporte une classe de base inetOrgPerson. Si l'enregistrement remplit cette condition, l'entrée est immédiatement subordonnée au conteneur test et le composant le plus à gauche de son dn source est utilisé comme composant de son dn.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-class class-name="inetOrgPerson"></match-class>
       <placement>cn=<copy-name/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

Sur la base de cette règle, un enregistrement de la classe de base inetOrgPerson et dont le dn est:

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
```

aura le dn suivant dans l'annuaire cible :

```
dn: cn=Kim Jones, o=test
```

Exemple de placement 2 : la règle de placement suivante exige que l'enregistrement comporte un attribut sn. Si l'enregistrement remplit cette condition, l'entrée est immédiatement subordonnée au conteneur test et le composant le plus à gauche de son dn source est utilisé comme composant de son dn.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement>cn=<copy-name/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

Sur la base de cette règle, un enregistrement comportant le dn et l'attribut sn suivants :

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

aura le dn suivant dans l'annuaire cible :

```
dn: cn=Kim Jones, o=test
```

Exemple de placement 3 : la règle de placement suivante exige que l'enregistrement comporte un attribut sn. Si l'enregistrement remplit cette condition, l'entrée est immédiatement subordonnée au conteneur test et son attribut sn est utilisé comme composant de son dn. L'attribut indiqué dans l'élément copy-attr doit être un attribut d'assignation de nom de la classe de base de l'entrée.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
  <placement-rule>
    <match-attr attr-name="sn"></match-attr>
    <placement>cn=<copy-attr attr-name="sn"/>,o=test</placement>
  </placement-rule>
</placement-rules>
```

Sur la base de cette règle, un enregistrement comportant le dn et l'attribut sn suivants :

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

aura le dn suivant dans l'annuaire cible:

```
dn: cn=Jones, o=test
```

Exemple de placement 4 : la règle de placement suivante exige que l'enregistrement comporte un attribut sn. Si l'enregistrement remplit cette condition, le dn source est utilisé comme dn cible.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement><copy-path/></placement>
    </placement-rule>
 </placement-rules>
```

Exemple de placement 5 : la règle de placement suivante exige que l'enregistrement comporte un attribut sn. Si l'enregistrement remplit cette condition, le DN complet de l'entrée est copié dans le conteneur test.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement><copy-path-suffix/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

Sur la base de cette règle, un enregistrement comportant le dn et l'attribut sn suivants :

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

aura le dn suivant dans l'annuaire cible:

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ, o=test
```

Exemple de placement 6 : la règle de placement suivante exige que l'enregistrement comporte un attribut sn. Si l'enregistrement remplit cette condition, le DN complet de l'entrée est copié dans le conteneur neworg.

```
<placement-rules>
 <placement-rule>
  <match-path prefix="o=engineering"/>
  <placement><copy-path-suffix/>o=neworg</placement>
 </placement-rule>
</placement-rules>
```

Par exemple :

```
dn: cn=bob,o=engineering
```

devient

```
dn: cn=bob,o=neworg
```

Exemple de commande : si les règles de placement sont enregistrées dans un fichier pr1.xml, la commande suivante demande à l'utilitaire de les exploiter lors du traitement du fichier 1entry.ldf et d'envoyer les résultats dans un fichier cible, foutt1.ldf.

```
ice -o -pfile://pr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

Protocole LBURP

L'utilitaire d'importation, de conversion et d'exportation Novell utilise le protocole LBURP (LDAP Bulk Update/Replication Protocol) pour envoyer des requêtes asynchrones à un serveur LDAP. Cela garantit le traitement des requêtes dans l'ordre indiqué par le protocole, et non dans un ordre arbitraire influencé par les interactions multiprocesseurs ou par le planificateur du système d'exploitation.

Le protocole LBURP permet également à l'utilitaire d'importation, de conversion et d'exportation Novell d'envoyer plusieurs mises à jour dans une seule requête et de recevoir une réponse unique pour toutes ces mises à jour. Il permet ainsi d'optimiser l'efficacité du réseau.

Le protocole LBURP fonctionne de la manière suivante :

1. L'utilitaire d'importation, de conversion et d'exportation Novell établit une liaison avec un serveur LDAP.
2. Le serveur envoie une réponse de liaison au client.
3. Le client envoie une requête étendue LBURP de début au serveur.
4. Le serveur envoie une réponse étendue LBURP de début au client.
5. Le client envoie ou non des requêtes étendues d'opération LBURP au serveur.

   Celles-ci peuvent être envoyées en mode asynchrone. Chacune d'entre elles contient un numéro séquentiel identifiant sa place par rapport aux autres requêtes envoyées par le client via la même connexion. Chaque requête contient également au moins une opération de mise à jour LDAP.
6. Le serveur traite chacune des requêtes étendues d'opération LBURP dans l'ordre défini par le numéro séquentiel et envoie une réponse étendue d'opération LBURP pour chaque requête.
7. Une fois que toutes les mises à jour ont été envoyées au serveur, le client envoie une requête étendue LBURP de fin au serveur.
8. Le serveur envoie une réponse étendue LBURP de fin au client.

Le protocole LBURP permet à l'utilitaire d'importation, de conversion et d'exportation Novell de présenter des données au serveur aussi rapidement que la connexion réseau le permet. Si cette dernière est suffisamment rapide, le serveur peut traiter les opérations de mise à jour à 100% de son temps, car il n'a jamais besoin d'attendre que l'utilitaire lui transmette d'autres tâches à réaliser.

Le processeur LBURP de eDirectory exécute également des opérations de mise à jour de la base de données en groupes afin d'optimiser leur traitement. Il peut nettement améliorer l'efficacité des importations LDIF par rapport à une approche synchrone traditionnelle.

Le protocole LBURP est activé par défaut, mais vous pouvez le désactiver au cours d'une importation LDIF.

Pour activer ou désactiver le protocole LBURP au cours d'une importation LDIF :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.
3. Cliquez sur Importer les données depuis un fichier du disque, puis sur Suivant.
4. Sélectionnez LDIF dans la liste déroulante Type de fichier, puis indiquez le nom du fichier LDIF contenant les données à importer.
5. Cliquez sur Suivant.

6 Spécifiez le serveur LDAP sur lequel importer les données, ainsi que le type de login (anonyme ou authentifié).

7 Dans Paramètres avancés, sélectionnez Utiliser LBURP.

8 Cliquez sur Suivant. Suivez les instructions en ligne pour exécuter les autres opérations de l'Assistant d'importation LDIF.

IMPORTANT : le protocole LBURP étant relativement récent, les serveurs eDirectory antérieurs à la version 8.5 (ainsi que la plupart des serveurs non-eDirectory) ne le prennent pas en charge. Si vous utilisez l'Assistant d'importation et d'exportation Novell eDirectory pour importer un fichier LDIF vers l'un de ces serveurs, vous devez désactiver l'option LBURP pour que l'importation LDIF fonctionne.

Vous pouvez utiliser l'option de ligne de commande pour activer ou désactiver LBURP pendant une importation LDIF. Pour plus d'informations, reportez-vous à la section « -B », page 163.

Migration du schéma entre des annuaires LDAP

Pour plus d'informations sur la migration du schéma entre des annuaires LDAP, consultez le site Web *NetWare Application Notes* (http://www.developer.novell.com/research) (Notes sur Netware) sur le portail de développement de Novell.

Amélioration de la vitesse des importations LDIF

Si le fichier LDIF que vous importez contient à lui seul des milliers, voire des millions d'enregistrements, pensez aux points suivants :

- « Importation directe vers un serveur avec une réplique Lecture/écriture », page 183
- « Utilisation du protocole LBURP », page 183
- « Configuration du cache de base de données », page 184
- « Utilisation de mots de passe simples », page 184
- « Utilisation appropriée des index », page 185

Importation directe vers un serveur avec une réplique Lecture/écriture

Si cela est possible, sélectionnez pour l'importation LDIF un serveur cible qui comporte des répliques Lecture/écriture contenant toutes les entrées répertoriées dans le fichierLDIF. Cette opération permet d'optimiser l'efficacité du réseau.

Pour les mises à jour, évitez que le serveur cible soit chaîné à d'autres serveurs eDirectory. Cela risque de réduire nettement les performances. Toutefois, si certaines des entrées à mettre à jour se trouvent uniquement sur des serveurs eDirectory qui n'exécutent pas LDAP, vous serez peut-être obligé d'autoriser le chaînage pour importer le fichier LDIF.

Pour plus d'informations sur la gestion des répliques et des partitions, reportez-vous au Chapitre 5, « Gestion des partitions et des répliques », page 133.

Utilisation du protocole LBURP

L'utilitaire d'importation, de conversion et d'exportation Novell optimise le fonctionnement du réseau et du serveur eDirectory en utilisant le protocole LBURP pour transférer des données entre l'Assistant et le serveur. L'utilisation du protocole LBURP au cours d'une importation LDIF améliore considérablement la vitesse d'exécution de cette opération.

Pour plus d'informations sur le protocole LBURP, reportez-vous à la section « Protocole LBURP », page 182.

Configuration du cache de base de données

La taille du cache de base de données que eDirectory peut utiliser a un impact direct sur la vitesse d'exécution des importations LDIF, notamment lorsque le nombre total d'entrées sur le serveur augmente. Lorsque vous effectuez une importation LDIF, vous pouvez allouer, pendant cette opération, le maximum de mémoire possible à eDirectory. Une fois que l'importation est terminée et que le serveur gère une charge moyenne, vous pouvez alors rétablir les paramètres de mémoire antérieurs. Cela est particulièrement important si l'importation est la seule activité réalisée sur le serveur eDirectory.

Pour plus d'informations sur la configuration du cache de base de données eDirectory, reportez-vous au « Gestion de Novell eDirectory », page 511.

Utilisation de mots de passe simples

Novell eDirectory utilise des paires de clés publiques et privées pour l'authentification. La génération de ces clés est un processus qui monopolise les ressources du processeur. eDirectory 8.7.3 (ou version ultérieure) permet de stocker les mots de passe à l'aide de la fonction de mot de passe simple du service NMAS™ (Novell Modular Authentication Service). Lorsque vous choisissez cette option, les mots de passe sont conservés dans un emplacement sécurisé de l'annuaire et les paires de clés ne sont générées que lorsqu'elles sont réellement requises pour l'authentification entre les serveurs. Cela permet d'augmenter considérablement la vitesse de chargement d'un objet qui contient des informations de mot de passe.

Pour activer des mots de passe simples au cours d'une importation LDIF :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.
3. Cliquez sur Importer les données depuis un fichier du disque, puis sur Suivant.
4. Sélectionnez LDIF dans la liste déroulante Type de fichier, puis indiquez le nom du fichier LDIF contenant les données à importer.
5. Cliquez sur Suivant.
6. Spécifiez le serveur LDAP sur lequel importer les données, ainsi que le type de login (anonyme ou authentifié).
7. Dans Paramètres avancés, sélectionnez Stocker les mots de passe simples NMAS/codés.
8. Cliquez sur Suivant, puis respectez les instructions en ligne pour exécuter les autres opérations de l'Assistant d'importation LDIF.

Si vous choisissez de stocker les mots de passe à l'aide de la fonction de mot de passe simple, vous devez utiliser un logiciel Novell Client™ compatible NMAS afin de vous loguer à l'arborescence eDirectory et d'accéder aux services de fichiers et d'impression traditionnels. Le service NMAS doit également être installé sur le serveur. Les applications LDAP qui créent des liaisons avec un nom et un mot de passe s'exécutent de manière transparente avec la fonction de mot de passe simple.

Pour plus d'informations sur NMAS, consultez le manuel *Novell Modular Authentication Service Administration Guide (Guide d'administration de Novell Modular Authentication Service)* (http://www.novell.com/documentation/beta/nmas30/index.html).

Utilisation appropriée des index

La présence d'index inutiles risque de ralentir l'importation LDIF ; en effet, chaque index défini nécessite un traitement supplémentaire pour chaque entrée dont il stocke les valeurs d'attribut. Avant d'effectuer une importation LDIF, vérifiez que vous n'avez pas d'index superflus ; vous pouvez ensuite envisager de créer certains de vos index une fois que vous avez terminé le chargement des données et passé en revue les statistiques de prédicat afin de déterminer où ces index sont réellement nécessaires.

Pour plus d'informations sur l'optimisation des index, reportez-vous à la section « Gestionnaire d'index », page 185.

Gestionnaire d'index

Le gestionnaire d'index est un attribut de l'objet Serveur qui vous permet de gérer les index de base de données. Ces index sont utilisés par eDirectory pour optimiser les performances des requêtes.

Novell eDirectory est livré avec un ensemble d'index offrant des fonctionnalités d'interrogation élémentaires. Ces index par défaut s'appliquent aux attributs suivants :

CN	Aliased Object Name
dc	Obituary
Given Name	Member
Surname	Reference
uniqueID	Equivalent to Me
GUID	NLS: Common Certificate
cn_SS	Revision
uniqueID_SS	extensionInfo
ldapAttributeList	ldapClassList

Vous pouvez également créer des index personnalisés afin d'améliorer les performances de eDirectory dans votre environnement. Par exemple, si votre entreprise a mis en oeuvre une nouvelle application LDAP qui recherche un attribut qui n'est pas indexé par défaut, il peut s'avérer nécessaire de créer un index pour cet attribut.

REMARQUE : bien que les index améliorent les performances en matière de recherche, l'ajout d'index supplémentaires risque d'augmenter le temps nécessaire à la mise à jour de l'annuaire. En règle générale, créez des index uniquement si vous pensez que les problèmes de performance résultent d'une recherche spécifique dans l'annuaire.

Novell iManager permet de créer ou de supprimer des index. Vous pouvez également afficher et gérer les propriétés de chaque index, comme son nom, son état, son type, sa règle et l'attribut indexé.

Utilisez les données de statistiques de prédicat, uniquement disponibles dans ConsoleOne, pour connaître les index supplémentaires susceptibles de présenter un intérêt dans votre environnement. Pour plus de détails, reportez-vous à la section « Données de prédicat », page 189.

Création d'un index

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Gestion des index.
3. Sélectionnez un serveur dans la liste des serveurs disponibles.
4. Dans la page Modifier les index, cliquez sur Créer.
5. Entrez le nom de l'index.

   Si vous ne saisissez aucun nom pour cet index, l'attribut lui est automatiquement assigné comme nom.

   IMPORTANT : le caractère $ sert de séparateur pour les valeurs d'attribut. Si vous souhaitez utiliser ce caractère dans le nom de l'index, vous devez le faire précéder d'une barre oblique inverse (\) afin de désactiver son effet lors de la manipulation des index via LDAP.
6. Sélectionnez un attribut.
7. Sélectionnez la règle d'index.
   - **Valeur** (value) recherche la valeur complète ou la première partie de la valeur d'un attribut. Par exemple, la concordance de valeur peut être utilisée pour rechercher les entrées dont l'attribut « LastName » (nom de famille) est « Jensen » et celles dont l'attribut « LastName » commence par « Jen ».
   - **Présence** (presence) exige uniquement la présence d'un attribut et non des valeurs d'attribut spécifiques. Une requête visant à rechercher toutes les entrées comportant un attribut Script de login utiliserait un index de présence.
   - **Sous-chaîne** (substring) recherche une sous-chaîne de la chaîne de valeurs d'un attribut. Par exemple, une requête visant à rechercher les entrées dont l'attribut « LastName » (nom de famille) comporte « der » renverrait aussi bien « Derington », que « Anderson » et « Lauder ».

     Un index de sous-chaînes est le type d'index dont la création et la gestion exigent le plus de ressources système.
8. Cliquez sur OK pour mettre à jour la table des index.
9. Cliquez sur Appliquer pour redémarrer le processus de contrôle de la connectivité (Limber) en arrière-plan et appliquer la modification.

Suppression d'un index

Certains index peuvent devenir inutiles. Dans ce cas, qu'ils soient définis par l'utilisateur ou créés automatiquement, vous pouvez les supprimer. Pour identifier les index les moins souvent utilisés, servez-vous des statistiques de prédicat. Pour plus d'informations, reportez-vous à la section « Données de prédicat », page 189.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Gestion des index.
3. Sélectionnez un serveur dans la liste des serveurs disponibles.
4. Dans la page Modifier les index, sélectionnez l'index défini par l'utilisateur ou ajouté automatiquement que vous souhaitez supprimer.
5. Cliquez sur Supprimer pour mettre à jour la table des index.
6. Cliquez sur Appliquer pour redémarrer le processus de contrôle de la connectivité (Limber) en arrière-plan et appliquer la modification.

Mise hors ligne d'un index

Pendant les périodes d'activité intensive, vous pouvez optimiser les performances en mettant temporairement hors ligne certains index. Par exemple, pour accélérer les opérations de chargement par lot, il est possible que vous souhaitiez suspendre tous les index définis par l'utilisateur. Dans la mesure où l'ajout et la modification d'objets impliquent la mise à jour des index définis, l'activation simultanée de tous les index peut ralentir considérablement les opérations de chargement par lot des données. Une fois les opérations de chargement par lot terminées, vous pouvez remettre en ligne les index.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Gestion des index.
3. Sélectionnez un serveur dans la liste des serveurs disponibles.
4. Dans la page Modifier les index, sélectionnez les index à mettre hors ligne, puis cliquez sur Changer l'état.

   L'état de l'index passe de En ligne à Hors ligne dans le tableau d'affichage. Un index peut présenter l'un des états suivants :

   - **En ligne** : en cours d'exécution.
   - **Hors ligne** : index suspendu, que vous pouvez relancer en cliquant sur Mettre en ligne.
   - **Nouveau** : index en attente de passage à l'état En ligne.
   - **Supprimé** : index en attente de suppression de la table des index.
5. Cliquez sur Appliquer.

Gestion des index sur d'autres serveurs

Si vous pensez qu'un index utilisé sur un serveur peut être utile sur un autre serveur, vous pouvez copier sa définition d'un serveur à l'autre. Lors de la révision des données de prédicat, il est également possible que vous vous trouviez dans le cas de figure inverse: un index que vous utilisiez sur plusieurs serveurs n'est désormais plus utile sur l'un de ces serveurs. Dans ce cas, vous pouvez supprimer l'index de ce serveur.

Le gestionnaire d'index permet de cibler une instance spécifique d'un index sans incidence sur les autres instances.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Gestion des index.
3. Sélectionnez un serveur dans la liste des serveurs disponibles.
4. Pour copier une définition d'index vers un autre serveur de la même arborescence, cliquez sur Modifier l'emplacement de l'index.
5. Sélectionnez la définition d'index à copier.

   Lorsque vous choisissez un index, les serveurs de l'arborescence contenant cet index sont listés.
6. Utilisez les colonnes disponibles pour déplacer une copie de l'index vers le serveur de votre choix.
7. Cliquez sur Appliquer.

Exécution de l'utilitaire d'importation, de conversion et d'exportation Novell pour gérer les index

Vous pouvez vous servir de l'utilitaire d'importation, de conversion et d'exportation Novell pour créer ou supprimer des index.

Ces opérations nécessitent l'utilisation d'un fichier LDIF. Une fois le fichier LDIF importé, vous pouvez activer le contrôleur de connectivité (limber) pour lancer l'indexation. Si vous ne l'activez pas, l'indexation s'effectuera lors du déclenchement automatique du contrôleur de connectivité.

Pour spécifier un index dans un fichier LDIF, vous devez indiquer des valeurs car les chaînes séparées par le signe dollar($) sont ignorées dans les cas suivants.

Ordre	Chaîne	Description
1	Index Version (version de l'index)	Réservé pour une utilisation ultérieure. Dans eDirectory, cette valeur doit toujours être égale à zéro (0).
2	Index Name (nom de l'index)	Indique le nom défini par l'utilisateur pour l'index, Par exemple : .Nom_famille. ou .Code_postal. Cette chaîne ne doit pas contenir de signe dollar($).
3	Index State (état de l'index)	État de l'index. Lors de la définition d'un index, ce champ doit présenter la valeur 2 (en ligne). eDirectory prend en charge les valeurs suivantes : ◆ 0 – Mis en attente, indique que l'index n'est pas utilisé dans les requêtes ni mis à jour. ◆ 1 – Mis en ligne, indique que l'index est en cours de création. ◆ 2 – En ligne, indique que l'index est créé et en fonction. ◆ 3 – Création en attente, indique que l'index a été défini et attend l'exécution du processus d'arrière-plan. Le processus d'arrière-plan change l'état dès que la création de l'index commence.
4	Index Rule (règle d'index)	Indique le type de concordance. ◆ 0 – Concordance de valeur. Optimise les requêtes qui impliquent la valeur complète ou la première partie de la valeur. Par exemple, une requête qui concerne toutes les entrées dont le nom équivaut à « Jensen » ou commence par « Jen ». ◆ 1 – Concordance de présence. Optimise les requêtes qui impliquent uniquement la présence d'un attribut. Il s'agit, par exemple, d'une requête qui concerne toutes les entrées comportant l'attribut « surname » (nom de famille). ◆ 2 – Concordance de sous-chaîne. Optimise les requêtes qui impliquent une correspondance de quelques caractères. Par exemple, une requête qui concerne toutes les entrées dont le nom comporte les caractères .der. Cette requête renvoie les entrées qui comportent les noms « Derington », « Anderson » et « Lauder ».

Ordre	Chaîne	Description
5	Index Type (type d'index)	Indique l'auteur de l'index. Lors de la définition d'un index, cette valeur doit être égale à 0. eDirectory prend en charge les valeurs suivantes : ◆ 0 – Défini par l'utilisateur ◆ 1 – Ajouté lors de la création de l'attribut ◆ 2 – Obligatoire pour le fonctionnement ◆ 3 – Index système
6	Index Value State (état de la valeur d'index)	Source de l'index. Lors de la définition d'un index, attribuez à cette chaîne la valeur 1. eDirectory prend en charge les valeurs suivantes : ◆ 0 – Non initialisé ◆ 1 – Ajouté à partir du serveur ◆ 2 – Ajouté à partir de la DIB locale ◆ 3 – Supprimé de la DIB locale ◆ 4 – Modifié à partir de la DIB locale
7	Attribute Name (nom de l'attribut)	Indique le nom NDS de l'attribut. Dans eDirectory, de nombreux attributs ont à la fois un nom LDAP et un nom NDS. Cette chaîne requiert le nom NDS.

Exemple de fichier LDIF permettant de créer des index

```
dn: cn=testServer-NDS,o=Novell

changetype: modify

add: indexDefinition

indexDefinition: 0$indexName$2$2$0$1$attributeName
```

Exemple de fichier LDIF permettant de supprimer des index

```
dn: cn=osg-nw5-7,o=Novell

changetype: modify

delete: indexDefinition

indexDefinition: 0$indexName$2$2$0$1$attributeName
```

Données de prédicat

Les données de prédicat constituent l'historique côté serveur des objets recherchés par les utilisateurs. Les données ainsi que leur collecte sont gérées par l'intermédiaire de l'objet ndsPredicateStats, créé lors de l'installation de eDirectory. Le nom de l'objet ndsPredicateStats est composé du nom du serveur, auquel est ajouté -PS.

Vous pouvez utiliser les données de prédicat pour identifier les objets les plus fréquemment recherchés et créer des index permettant d'accélérer l'accès aux informations.

Gestion des données de prédicat

La fonctionnalité de statistiques de prédicat n'est pas conçue pour une exécution permanente. En effet, cette collecte peut nuire aux performances des recherches. De plus, une accumulation prolongée de statistiques peut être à l'origine de bases de données très volumineuses. Utilisez les statistiques de prédicat si vous pensez que les problèmes de performances que vous rencontrez résultent d'opérations de recherche spécifiques dans un annuaire.

La page de propriétés Données de prédicat de ConsoleOne permet de gérer la collecte des données.

1. Dans ConsoleOne, cliquez avec le bouton droit sur l'objet Serveur.
2. Cliquez sur Propriétés > Données de prédicat > Propriétés.
3. Définissez la configuration appropriée pour l'objet ndsPredicateStats.

   Intervalle de mise à jour : définit le délai d'attente (en secondes) avant le rafraîchissement de l'affichage des données et leur écriture sur le disque.

   Avancé > Activer : indique si le processus de collecte doit être exécuté à l'arrière-plan ou s'il doit être désactivé. Si vous désactivez la collecte de données, les données collectées le plus récemment seront effacées de la mémoire ou, si l'option Écrire sur le disque est activée, déplacées vers le disque.

   Avancé > Écrire sur le disque : détermine l'emplacement de stockage des données de prédicat. Celles-ci peuvent être conservées en mémoire ou déplacées de la mémoire vers le disque, conformément à la valeur de l'option Intervalle de mise à jour.

   Avancé > Afficher le texte de la valeur : détermine si les données doivent être affichées sous forme abrégée ou complète. L'affichage sous forme abrégée fournit suffisamment d'informations pour déterminer quels sont les prédicats intéressants pour les index.
4. Cliquez sur OK pour mettre à jour la configuration de l'objet.

Gestionnaire de services eDirectory

Le gestionnaire de services eDirectory fournit des informations sur les services eDirectory disponibles et leur état. Il permet également de démarrer et d'arrêter ces services.

Le gestionnaire de services gère uniquement les services eDirectory. Il utilise pour cela le fichier de configuration dsservcfg.xml, qui liste les services à gérer sur différentes plates-formes. Il permet également d'ajouter ou de supprimer des services dans la liste.

Pour accéder au Gestionnaire de services eDirectory, utilisez l'une des méthodes suivantes :

- « Utilisation de l'outil Service Manager eMTool du client eMBox », page 190
- « Utilisation du plug-in du gestionnaire de services pour Novell iManager », page 191

Utilisation de l'outil Service Manager eMTool du client eMBox

Le client eDirectory Management Toolbox (eMBox) est un client Java à ligne de commande qui permet d'accéder à distance à l'outil eDirectory Service Manager eMTool. Le fichier emboxclient.jar est installé sur votre serveur comme élément de eDirectory. Vous pouvez l'exécuter sur toute machine dotée d'une JVM. Pour plus d'informations sur le client eMBox, reportez-vous à la section « Utilisation du client à ligne de commande eMBox », page 553.

Pour utiliser l'outil Service Manager eMTool du client eMBox, procédez comme suit :

1. Exécutez le client eMBox en mode interactif en entrant les éléments suivants dans la ligne de commande :

   java -cp *chemin_fichier*/emboxclient.jar embox -i

   (Si le fichier emboxclient.jar figure déjà dans votre chemin d'accès à la classe, il vous suffit d'entrer la commande **java embox -i**.)

   L'invite du client eMBox apparaît :

   ```
   Client eMBox>
   ```

2. Pour vous loguer au serveur qui doit exécuter le gestionnaire de services, entrez ce qui suit :

   login -s*nom_ou_adresse_IP_serveur* -p*numéro_port*
   -u*nom_utilisateur.contexte* -w*mot_de_passe* -n

   Le numéro de port est généralement 80 ou 8028, à moins qu'il ne soit déjà utilisé par un serveur Web. L'option -n ouvre une connexion non sécurisée.

   Le client eMBox indique si le login a réussi.

3. Entrez l'une des commandes suivantes du Gestionnaire de services :

Commande	Description
service.serviceList	Liste les services eDirectory disponibles.
service.serviceStart -n*nom_module*	Démarre le service eDirectory indiqué.
service.serviceStop -n*nom_module*	Arrête le service eDirectory indiqué.
service.serviceInfo -n*nom_module*	Affiche les informations relatives au service indiqué.

   Vous pouvez également utiliser la commande **list -tservice** du client eMBox pour lister les options du gestionnaire de services de manière détaillée. Pour plus d'informations, reportez-vous à la section « Liste des outils eMTools et de leurs services », page 557.

4. Déloguez-vous du client eMBox en entrant la commande suivante :

   logout

5. Quittez le client eMBox en entrant la commande suivante :

   exit

Utilisation du plug-in du gestionnaire de services pour Novell iManager

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Gestionnaire de services.
3. Indiquez le serveur à gérer, puis cliquez sur OK.
4. Authentifiez-vous auprès du serveur sélectionné, puis cliquez sur OK.

5 Utilisez les icônes suivantes pour vérifier l'état d'un service eDirectory quelconque ou pour démarrer ou arrêter un service :

Icône	Description
	Un service est en cours d'exécution.
	Un service est arrêté.
	Démarre un service.
	Arrête un service.
	Un service est en cours d'exécution, mais vous ne pouvez pas l'arrêter.

7 Utilisation de Novell iMonitor 2.1

Novell® iMonitor fournit des fonctionnalités de surveillance et de diagnostic multi plates-formes pour tous les serveurs de l'arborescence eDirectory™. Cet utilitaire permet de surveiller les serveurs à partir de tout emplacement du réseau où un navigateur Web est disponible.

Grâce à iMonitor, vous pouvez procéder à un examen complet de l'environnement eDirectory, en fonction des partitions, des répliques ou des serveurs. Vous pouvez également savoir quelles tâches sont en cours de réalisation, le moment de leur exécution, les résultats qu'elles génèrent et leur durée.

iMonitor propose une alternative Web à de nombreux outils Novell eDirectory utilisant traditionnellement un serveur, tels que DSBrowse, DSTrace, DSDiag ainsi qu'aux fonctionnalités de diagnostic disponibles dans DSRepair. Ainsi, les fonctionnalités de iMonitor sont principalement « orientées serveur », c'est-à-dire qu'elles se concentrent sur l'état de santé de différents agents eDirectory (exécutant des instances du service d'annuaire), et non à l'arborescence eDirectory dans son intégralité.

iMonitor 2.1 offre les fonctions suivantes :

- Résumé de l'état de santé de eDirectory
  - Informations de synchronisation
  - Serveurs connus
  - Configuration de l'agent
- Vérifications de l'état de santé de eDirectory
- DS Trace avec lien hypertexte
- Configuration de l'agent
- Activité de l'agent et statistiques du verbe
- Rapports
- Informations sur les agents
- Informations sur les erreurs
- Navigateur d'objet/de schéma
- Surveillance de Novell Nsure Identity Manager
- Recherche
- Liste de partitions
- État du processus de l'agent
- Planification des processus à l'arrière-plan
- DSRepair
- Surveillance des connexions

Les informations que vous pouvez afficher dans iMonitor dépendent des facteurs suivants :

- Votre identité

  Les droits eDirectory associés à votre identité s'appliquent à l'ensemble des requêtes que vous lancez dans iMonitor. Par exemple, vous devez vous loguer en tant qu'administrateur du serveur ou qu'opérateur de la console du serveur à partir duquel vous essayez d'accéder à la page DSRepair.

- Version de l'agent eDirectory faisant l'objet de la surveillance

  Les versions plus récentes de NDS® et de eDirectory comprennent des fonctions et des options qui n'étaient pas disponibles dans les versions antérieures.

Les informations que vous affichez dans iMonitor reflètent instantanément les opérations effectuées sur le serveur.

Ce chapitre procure des informations sur les sujets suivants :

- « Configuration système requise », page 194
- « Accès à iMonitor », page 195
- « Architecture iMonitor », page 195
- « Fonctions de iMonitor », page 201
- « Opérations iMonitor sécurisées », page 220

Configuration système requise

Pour utiliser iMonitor 2.1, vous avez besoin des logiciels suivants :

- soit Internet Explorer 5.5 ou version ultérieure, soit Netscape 7.02 ou version ultérieure ;
- Novell eDirectory version 8.7.1 ou ultérieure.

Plates-formes

L'utilitaire iMonitor 2.1 fonctionne sur les plates-formes suivantes :

- NetWare® 5.1 Support Pack 4 ou version ultérieure ;

  Novell iMonitor se trouve dans le fichier autoexec.ncf.

- Serveurs Windows 2000 et 2003 (non-SSL)
- Linux
- Solaris
- AIX
- HP-UX

Dans les environnements NetWare et Windows, iMonitor se charge automatiquement au moment de l'exécution de eDirectory. Sous Linux, Solaris, AIX et HP-UX, vous pouvez charger iMonitor à l'aide de la commande ndsimonitor -l. Il peut aussi être chargé automatiquement si vous ajoutez [ndsimonitor] dans le fichier /etc/opt/novell/eDirectory/conf/ndsimon.conf avant le lancement du serveur eDirectory.

Versions de eDirectory compatibles

iMonitor permet de surveiller les versions suivantes des services NDS et de eDirectory :

- Toutes les versions des services NDS et eDirectory pour NetWare 4.11 ou version ultérieure
- Toutes les versions des services NDS et eDirectory pour Windows
- Toutes les versions des services NDS et eDirectory pour Linux, Solaris, AIX et HP-UX

Accès à iMonitor

1. Vérifiez que le fichier exécutable de iMonitor est exécuté sur le serveur eDirectory.
2. Ouvrez votre navigateur Web.
3. Dans le champ de l'adresse URL, entrez :

   http://*adresse_TCPIP_serveur*:*port_pile_http*/nds

   Par exemple :

   `http://137.65.135.150:8028/nds`

   Les noms DNS peuvent être utilisés partout où l'adresse IP ou IPX™ ou le nom distinctif d'un serveur pourraient l'être dans iMonitor. Par exemple, une fois le DNS configuré,

   `http://prv-gromit.provo.novell.com/nds?server=prv-igloo.provo.novell.com`

   est équivalent à :

   `http://prv-gromit.provo.novell.com/nds?server=`*`adresse_IP_ou_IPX`*

   ou

   `http://prv-gromit.provo.novell.com/nds?server=/cn=prv-igloo,ou=ds,ou=dev,o=novell,t=novell_inc`

   Si une pile HTTPS eDirectory est disponible, vous pouvez utiliser iMonitor via HTTPS.
4. Indiquez un nom d'utilisateur, un contexte et un mot de passe.

   Pour avoir accès à toutes les fonctions, loguez-vous avec des droits d'administrateur avec un nom distinctif complet ou avec des droits équivalents.
5. Cliquez sur Login.

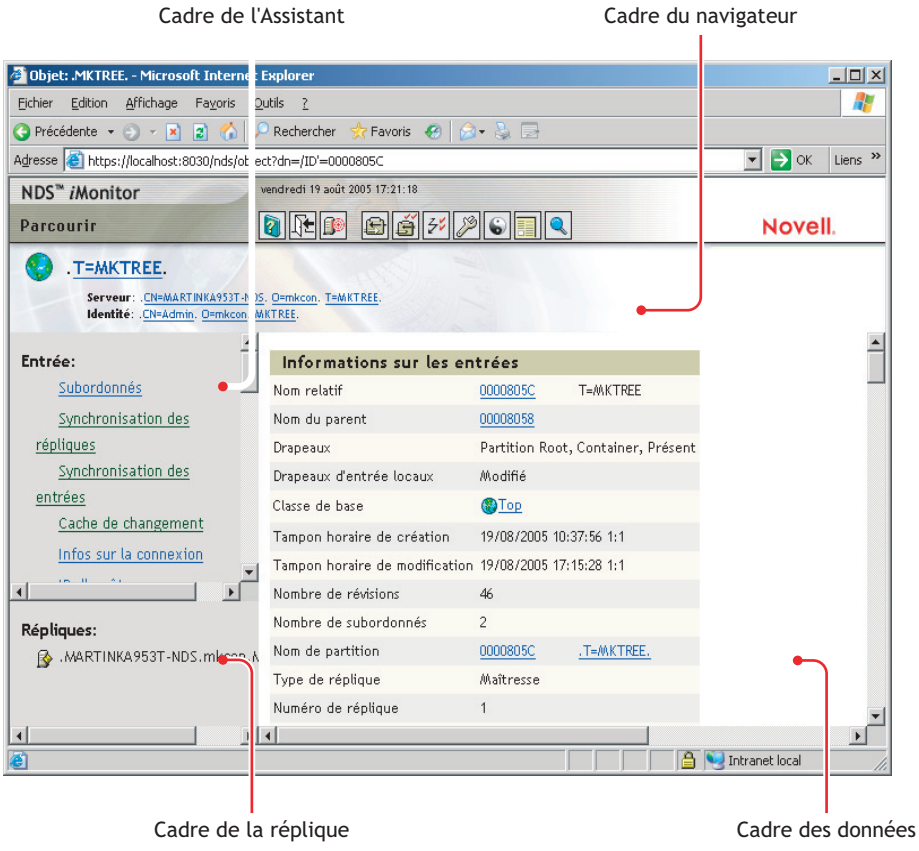
Architecture iMonitor

- « Anatomie d'une page de iMonitor », page 196
- « Modes de fonctionnement », page 197
- « Fonctions de iMonitor disponibles sur chaque page », page 198
- « Intégration dans NetWare Remote Manager », page 198
- « Fichiers de configuration », page 199

Anatomie d'une page de iMonitor

Dans iMonitor, chaque page est divisée en quatre cadres ou sections : le cadre du navigateur, le cadre de l'Assistant, le cadre des données et le cadre de la réplique.

Figure 30 Cadres de iMonitor



Cadre du navigateur : situé dans la partie supérieure de la page. Ce cadre affiche le nom du serveur à partir duquel les données sont lues, votre identité, ainsi que les icônes sur lesquelles vous pouvez cliquer pour accéder à d'autres écrans, notamment à l'aide en ligne, à l'écran de login, au portail du serveur et à d'autres pages iMonitor.

Cadre de l'Assistant : situé dans la partie gauche de la page. Ce cadre contient des aides à la navigation supplémentaires, telles que des liens vers d'autres pages, des éléments qui vous permettent de naviguer dans le cadre de données, ou d'autres éléments qui vous aident à obtenir ou à interpréter les données d'une page donnée.

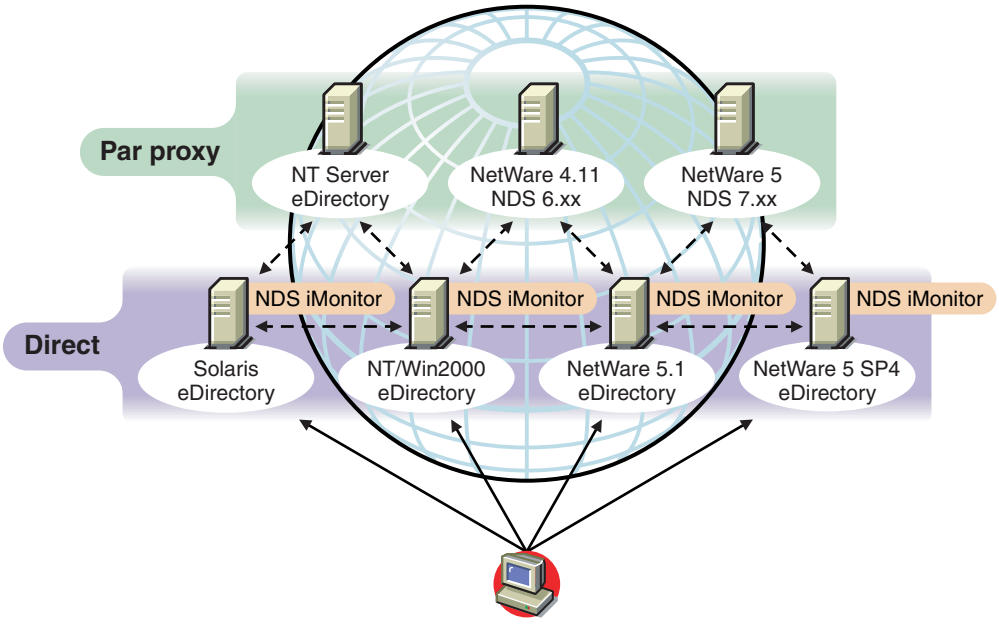
Cadre des données : affiche les informations détaillées sur les serveurs, que vous obtenez en cliquant sur l'un des liens ci-dessus. Si votre navigateur Web ne prend pas en charge les cadres, cette page est la seule qui s'affichera.

Cadre de la réplique : permet de déterminer la réplique actuellement affichée et propose des liens servant à afficher les mêmes informations du point de vue d'une autre réplique ou d'un autre serveur. Ce cadre n'apparaît que lorsque vous affichez des pages sur lesquelles figure une autre réplique des données concernées ou une autre réplique qui présente une vue différente des informations affichées dans le cadre des données.

Modes de fonctionnement

Novell iMonitor peut être utilisé de deux façons: en mode direct et en mode proxy. Le passage d'un mode à l'autre de nécessite aucune modification de configuration. Novell iMonitor passe automatiquement d'un mode à l'autre. Vous devez toutefois les comprendre afin de parcourir aisément l'arborescence eDirectory.

Figure 31 Modes de fonctionnement



Mode direct : utilisez ce mode lorsque le navigateur Web pointe directement sur l'adresse ou le nom DNS d'une machine qui utilise le fichier exécutable de iMonitor et lit uniquement les informations situées dans la DIB eDirectory locale de cette machine.

Certaines fonctions de iMonitor sont centrées sur le serveur: elles ne sont accessibles que par le biais de l'utilitaire iMonitor exécuté sur cette machine. Ces fonctions utilisent des ensembles API locaux qui ne sont pas accessibles à distance. Parmi les fonctions de iMonitor centrées sur le serveur figurent les pages DSTrace, DSRepair et Planification des processus à l'arrière-plan. Lorsque vous utilisez le mode direct, toutes les fonctions de iMonitor sont disponibles sur cette machine.

Principales fonctions du mode direct :

- ensemble complet de fonctions centrées sur le serveur ;
- réduction de la largeur de bande du réseau (accès plus rapide) ;
- accès par proxy toujours possible pour toutes les versions de eDirectory.

Mode proxy : utilisez ce mode lorsque le navigateur Web pointe sur un utilitaire iMonitor exécuté sur une machine, mais recueille des informations d'une autre machine. Étant donné que iMonitor utilise des protocoles traditionnels non centrés sur le serveureDirectory pour des fonctions non centrées sur le serveur, toutes les versions de eDirectory antérieures à la version NDS 6.*x* peuvent être surveillées et diagnostiquées. Toutefois, les fonctions centrées sur le serveur utilisent des API auxquelles il est impossible d'accéder à distance.

Il est possible de passer du mode proxy au mode direct pour un autre serveur à condition que la version de eDirectory installée sur ce dernier soit une version avec laquelle iMonitor est livré. Si le serveur sur lequel vous rassemblez des informations par proxy exécute iMonitor, une icône supplémentaire apparaît dans le cadre du navigateur. Lorsque vous placez le pointeur de la souris sur cette icône, un lien vers l'utilitaire iMonitor du serveur distant apparaît. Si le serveur sur lequel vous collectez des informations par proxy exécute une ancienne version de eDirectory, aucune icône supplémentaire n'apparaît ; vous devrez toujours recueillir des informations sur ce serveur par proxy jusqu'à ce qu'il soit mis à niveau vers une version de eDirectory comprenant iMonitor.

Principales fonctions du mode proxy :

- Les serveurs de l'arborescence ne doivent pas tous obligatoirement exécuter iMonitor pour pouvoir utiliser la plupart de ses fonctions.
- Un seul serveur doit être mis à niveau.
- Un point d'accès unique est offert pour les connexions à distance.
- Vous pouvez accéder à iMonitor via une liaison à débit moins élevé alors que iMonitor accède aux informations eDirectory via des liaisons à plus haut débit.
- Les informations des versions précédentes des NDS sont accessibles.
- Les fonctions centrées sur le serveur ne sont disponibles qu'aux emplacements où iMonitor est installé.

Fonctions de iMonitor disponibles sur chaque page

Vous pouvez accéder aux pages Résumé de l'agent, Informations sur les agents, Configuration de l'agent, Configuration de Trace, DSRepair, Rapports et Recherche à partir de n'importe quelle page iMonitor, à l'aide des icônes du cadre du navigateur. Vous pouvez également vous loguer au site Web du support Novell ou établir un lien vers ce site à partir de n'importe quelle page de iMonitor.

Login/Logout : le bouton Login est disponible si vous n'êtes pas encore logué. Un bouton Logout, qui ferme la fenêtre du navigateur, apparaît si vous êtes logué. À moins que toutes les fenêtres du navigateur ne soient fermées, la session iMonitor reste ouverte et vous n'avez pas besoin de vous loguer de nouveau. Vous pouvez afficher l'état du login sur une page quelconque en consultant la zone Identité du cadre du navigateur.

Lien pour une connexion à la page Support : le logo Novell dans le coin supérieur droit est un lien vers la page Web pour une connexion au Support de Novell. Il constitue un lien direct vers le site Web de Novell sur lequel vous pouvez obtenir des mises à jour et des correctifs de serveur, ainsi qu'un support technique propre à chaque produit.

Intégration dans NetWare Remote Manager

Sur les serveurs NetWare version 5 ou ultérieure, un lien vers NetWare Remote Manager vous permet d'obtenir des informations de surveillance, de diagnostic et de dépannage basées sur le Web pour ces serveurs.

iMonitor s'intègre à NetWare Remote Manager comme suit :

- Le serveur Web léger de NetWare Remote Manager (httpstk.nlm) correspond à la première couche de l'architecture iMonitor sur la plate-forme NetWare.

- iMonitor s'enregistre auprès de NetWare Remote Manager (portal.nlm) afin que les liens vers iMonitor et vers d'autres informations spécifiques de eDirectory soient disponibles par le biais de l'interface de NetWare Remote Manager.

  Vous pouvez trouver ces liens à la section Manage eDirectory (Gérer eDirectory) de l'interface de Remote Manager. Des liens vers des informations sur l'état de santé de l'agent eDirectory sont également disponibles à la section Diagnose Server (Diagnostiquer le serveur) sous Health Monitor (Moniteur d'état de santé) dans les catégories relatives à eDirectory.

NetWare Remote Managers'enregistre également auprès de eDirectory, de sorte que iMonitor et NetWare Remote Managerpuissent établir des références croisées l'un vers l'autre et assurer ainsi un échange de données plus homogène entre les outils.

Fichiers de configuration

Des fichiers de configuration sont fournis avec iMonitor pour vous permettre de modifier ou de définir le comportement ou les valeurs par défaut de l'utilitaire.

Les fichiers de configuration sont des fichiers texte qui contiennent des balises de paramètres de configuration associées aux valeurs requises. Ces fichiers sont situés dans le même répertoire que l'exécutable iMonitor (qui se trouve généralement au même emplacement que les exécutables Novell eDirectory) sous NetWare et Windows, et dans le répertoire /etc sous Linux, Solaris, AIX et HP-UX.

- « ndsimon », page 199
- « ndsimonhealth », page 200

ndsimon

Le fichier de configuration ndsimon permet de modifier les paramètres des fichiers de trace, de contrôler l'accès au serveur, de définir le nombre maximal d'objets à afficher lors du listage d'un conteneur ou de l'affichage de résultats de recherche, mais aussi de spécifier le nombre de minutes d'inactivité autorisé avant d'arrêter une connexion.

Serveur	Fichier de configuration
NetWare	sys:\system\ndsimon.ini
Windows NT et Windows 2000	*répertoire_installation*\novell\NDS\ndsimon.ini
Linux, Solaris, AIX et HP-UX	/etc/opt/novell/eDirectory/conf/ndsimon.conf

Le fichier de configuration ndsimon permet de définir deux groupes de paramètres, à savoir:

- Paramètres relatifs au mode d'exécution du fichier exécutable de iMonitor

  Lors de son chargement sur des systèmes autres que NetWare, le fichier exécutable de iMonitor tente d'écouter sur le port HTTP traditionnel 80. Si ce port est déjà utilisé, il essaie le port 8028. Si ce port est également utilisé, iMonitor tente d'écouter un nouveau port, en augmentant à chaque fois la valeur du numéro de port de 2 : 8010, 8012, et ainsi de suite jusqu'à 8078.

  Lorsque le protocole SSL est configuré et disponible, le même schéma de tentative de liaison est appliqué. Dans un premier temps, une tentative est effectuée sur le port 81, puis sur les ports 8009, 8011, 8013 etc.

Ainsi, iMonitor peut coexister avec un serveur Web qui s'exécute sur le même serveur. Il se peut toutefois que, sur certaines plates-formes, iMonitor se charge avant le serveur Web installé ou que vous souhaitiez que iMonitor se lie à un port de votre choix. Les ports classiques et SSL peuvent être configurés respectivement à l'aide des paramètres HttpPort et HttpsPort. Le fichier de configuration d'origine contient des exemples de paramètres mis en commentaire. Par défaut, iMonitor se lie à toutes les adresses NIC sur le serveur où il se charge. Il existe cependant un paramètre Adresse que vous pouvez utiliser pour spécifier une liste d'adresses séparées par une virgule, auxquelles il devra se lier.

NetWare utilise des règles de sélection de port similaires. Elles sont toutefois contrôlées par la pile HTTP de NetWare Remote Manager (httpstk.nlm) et fonctionnent comme indiqué en détail dans la documentation de NetWare Remote Manager.

- Paramètres applicables à des fonctionnalités ou à des pages spécifiques

  Le fichier de configuration fourni avec iMonitor contient des exemples de paramètres que vous pouvez modifier. Ces paramètres sont précédés du caractère #. Il permet d'indiquer que ces paramètres font l'objet d'un commentaire et qu'ils ne sont pas utilisés lorsque iMonitor analyse le fichier de configuration. Concernant le fichier de configuration d'origine, iMonitor utilise l'ensemble des valeurs par défaut liées en interne pour ces paramètres. Pour activer l'un de ces paramètres, ou pour en ajouter, il suffit de supprimer le caractère # au début de la ligne.

ndsimonhealth

Le fichier de configuration ndsimonhealth vous permet de modifier les paramètres par défaut de la page d'informations sur l'état de santé de l'agent. Vous pouvez activer ou désactiver les options relatives à l'état de santé de l'agent, définir les niveaux de génération de rapports et les plages correspondantes pour les options, ainsi qu'établir les niveaux de génération de rapports des serveurs.

Serveur	Fichier de configuration
NetWare	sys:\system\ndsimonhealth.ini
Windows NT et Windows 2000	*répertoire_installation*\novell\NDS\ndsimonhealth.ini
Linux, Solaris, AIX et HP-UX	/etc/opt/novell/eDirectory/conf/ndsimonhealth.conf

Le fichier de configuration ndsimonhealth permet de définir trois types d'options.

- Options à activer/désactiver uniquement

  Pour désactiver une option, supprimez le signe # qui la précède et remplacez le niveau indiqué après le signe deux-points (:) par OFF. Pour définir le niveau de génération de rapports de ces options, supprimez le signe # qui les précède et indiquez un niveau de génération de rapports après le signe deux-points. Les niveaux autorisés sont WARN, MARGINAL et SUSPECT. Vous ne pouvez définir qu'un seul niveau de génération de rapports pour ces options.

- Options générales acceptant une plage de valeurs

  Ces options peuvent être activées ou désactivées, ou encore se voir affecter un niveau de génération de rapports avec les plages correspondantes.

  Pour définir le niveau de génération de rapports pour l'une de ces options, utilisez le nom de cette dernière suivi de « -active: », et le niveau de génération de rapports souhaité. Ainsi, pour activer time_delta (delta horaire), ajoutez la ligne suivante au fichier de configuration:

  ```
  time_delta-active: WARN
  ```

Pour désactiver time_delta, ajoutez la ligne suivante au fichier de configuration :

```
time_delta-active: OFF
```

Lors de la saisie de plages, la plage indiquée est celle pour laquelle le niveau de génération de rapports ne doit pas être affiché.

L'exemple de time_delta ci-dessous montre comment activer une option pour les trois niveaux de génération de rapports et définir les plages associées. Dans cet exemple, tout ce qui ne figure pas dans la plage -2 à 2 est au minimum marginal, tout ce qui n'est pas compris entre –5 et +5 est au moins suspect et tout ce qui ne figure pas entre -10 et 10 est un avertissement.

```
time_delta-active: WARN | SUSPECT | MARGINAL
time_delta-Min_Warn:      -10
time_delta-Min_Suspect:    -5
time_delta-Min_Marginal:   -2
time_delta-Max_Marginal:    2
time_delta-Max_Suspect:     5
time_delta-Max_Warn:        10
```

Pour obtenir de l'aide sur l'une de ces options, entrez l'URL suivante dans iMonitor :

```
http://XXX.XXX.XXX.XXX:PORT/nds/help?hbase=/nds/health/NOM_OPTION
```

XXX.XXX.XXX.XXX:*PORT* correspond à l'adresse IP et au port auxquels iMonitor peut être contacté, et *NOM_OPTION* est le nom de l'option sur laquelle vous souhaitez obtenir de l'aide (par exemple, time_delta).

Pour afficher les niveaux et plages actuellement définis, ouvrez avec votre navigateur la page d'état de santé qui contient l'option qui vous intéresse, puis ajoutez ce qui suit à la fin de la ligne d'URL :

```
&op=setup
```

- Options qui impliquent des paramètres personnalisés ou complexes

  Trois niveaux différents de génération de rapports du serveur peuvent être définis :

  - WARN détecte les serveurs qui exécutent une version de eDirectory devant être mise à niveau dès que possible.
  - SUSPECT détecte les serveurs exécutant une version de eDirectory dont la mise à niveau doit être planifiée.
  - MARGINAL détecte les serveurs exécutant une version de eDirectory qui n'est pas à jour.

  Ces options définissent le niveau de génération de rapports lorsque la version du serveur appartient à la plage spécifiée.

Fonctions de iMonitor

Cette section décrit brièvement les fonctions de iMonitor.

Pour obtenir des informations détaillées sur chaque fonction, accédez à l'aide en ligne fournie dans chaque section de iMonitor.

- « Affichage de l'état de santé des serveurs eDirectory », page 202
- « Affichage de l'état de synchronisation des partitions », page 203
- « Affichage des informations de connexion du serveur », page 203
- « Affichage des serveurs connus », page 204

Affichage de l'état de santé des serveurs eDirectory

La page Résumé de l'agent permet d'afficher des informations sur l'état de santé des serveurs eDirectory, notamment sur la synchronisation, l'état des processus de l'agent et le nombre total de serveurs reconnus par votre base de données.

1. Dans iMonitor, cliquez sur Résumé de l'agent  .
2. Choisissez parmi les options suivantes :

   Résumé de synchronisation de l'agent: permet d'afficher le type et le nombre de répliques que vous possédez, ainsi que le temps écoulé depuis leur dernière synchronisation. Vous pouvez également afficher le nombre d'erreurs pour chaque type de réplique. S'il n'y a qu'une réplique ou partition à afficher, l'intitulé devient État de synchronisation des partitions.

   Si le résumé de la synchronisation de l'agent n'apparaît pas, votre identité ne vous permet d'afficher aucune réplique.

   Ensemble des serveurs connus de la base de données permet d'afficher le type et le nombre de serveurs que la base de données reconnaît, qu'ils soient actifs ou non.

   Ensemble des états de processus de l'agent affiche l'état des processus exécutés sur un agent sans intervention de l'administrateur. En cas de problème ou d'ajout d'informations, un état est enregistré. La table augmente ou diminue en fonction du nombre d'états enregistrés.

Affichage de l'état de synchronisation des partitions

La page Synchronisation de l'agent permet d'afficher l'état de synchronisation de vos partitions. Vous pouvez filtrer ces informations à l'aide des options listées dans le cadre de l'Assistant, dans la partie gauche de la page.

1. Dans iMonitor, cliquez sur Synchronisation de l'agent dans le cadre de l'Assistant.
2. Choisissez parmi les options suivantes :

   État de la synchronisation des partitions permet d'afficher la partition, le nombre d'erreurs, la dernière synchronisation réussie et le delta d'anneau maximal.

   Partition permet d'afficher les liens vers la page de synchronisation des répliques de chaque partition.

   Dernière synchronisation réussie permet d'afficher le temps écoulé depuis la dernière synchronisation de toutes les répliques d'une partition à partir du serveur.

   Delta d'anneau maximal indique la quantité de données susceptibles de ne pas être synchronisées correctement par rapport à toutes les répliques de l'anneau. Par exemple, si un utilisateur a modifié son script de login au cours des 30 dernières minutes et que le delta d'anneau maximal est de 45 minutes, la synchronisation du login de l'utilisateur risque d'échouer. L'utilisateur risque de récupérer le script de login précédent lorsqu'il essaie de se loguer. Toutefois, s'il a modifié son script depuis plus de 45 minutes, il devrait systématiquement obtenir le nouveau script de login à partir de toutes les répliques.

   Si la valeur Inconnu apparaît dans les options de delta d'anneau maximal, le vecteur de transition synchronisé est incohérent et le delta d'anneau maximal ne peut pas être calculé en raison d'opérations de réplique/partition en cours ou d'autres problèmes.

Affichage des informations de connexion du serveur

La page Informations sur les agents vous permet d'afficher les informations de connexion relatives à votre serveur.

1. Dans iMonitor, cliquez sur Informations sur les agents dans le cadre de l'Assistant.
2. Choisissez parmi les options suivantes :

   Infos sur le ping indique que iMonitor a essayé un ping IP pour l'ensemble des adresses annoncées pour le serveur. Les résultats sont tels qu'indiqués.

   Nom DNS indique que iMonitor a tenté d'inverser les adresses IP gérées par le serveur et précise le nom DNS associé.

   En fonction du transport, de la configuration et de la plate-forme que vous utilisez, il se peut que ces informations ne s'affichent pas.

   L'option **Infos sur la connexion** permet d'afficher les informations de connexion relatives au serveur, notamment les adresses de renvoi du serveur, le delta horaire, la réplique maîtresse la plus proche de la racine et la profondeur de la réplique.

   En fonction du transport, de la configuration et de la plate-forme que vous utilisez, il se peut que ces informations ne s'affichent pas.

   L'option **Adresses de renvoi du serveur** permet d'afficher l'ensemble des adresses utilisables pour atteindre votre serveur.

   Heure synchronisée indique que l'heure synthétique ou future n'est utilisée que si le dernier tampon horaire émis par une réplique est postérieur à l'heure actuelle.

eDirectory considère que l'heure est suffisamment bien synchronisée pour émettre des tampons horaires en fonction de l'heure actuelle du serveur. Le protocole de synchronisation horaire peut ou non être dans un état synchronisé.

Delta horaire indique le décalage horaire (en secondes) entre iMonitor et le serveur à distance. Un entier négatif indique que l'heure de iMonitor avance par rapport à celle du serveur, et un entier positif indique qu'elle retarde.

Réplique maîtresse la plus proche de la racine indique que la réplique la plus élevée ou la plus proche de la racine de l'arborescence d'assignation de nom est une réplique maîtresse.

Profondeur de la réplique permet d'afficher la profondeur de la réplique la plus proche de la racine (c'est-à-dire le nombre de niveaux qui séparent la réplique la plus proche de la racine et la racine de l'arborescence).

Affichage des serveurs connus

La liste Serveurs connus indique les serveurs reconnus par la base de données du serveur source. Vous pouvez appliquer un filtre à la liste pour afficher tous les serveurs connus de la base de données ou tous les serveurs de l'anneau de répliques. Si une icône est affichée en regard d'un serveur, celui-ci fait partie d'un anneau de répliques.

1. Dans iMonitor, cliquez sur Serveurs connus dans le cadre de l'Assistant.
2. Choisissez parmi les options suivantes :

   ID de l'entrée liste l'identificateur d'un objet sur le serveur local. Les ID d'entrée ne peuvent pas être utilisés sur plusieurs serveurs.

   Révision NDS indique le numéro de révision ou de version de eDirectory mise en cache ou stockée sur le serveur avec lequel vous communiquez.

   État indique si le serveur est inconnu, actif ou inactif. L'état Inconnu signifie que le serveur n'a jamais eu besoin de communiquer avec le serveur signalé comme étant inconnu.

   Dernière mise à jour indique la dernière fois où ce serveur a tenté de communiquer avec le serveur et a détecté qu'il était inactif. Si cette colonne n'apparaît pas, tous les serveurs sont en service.

Affichage des informations relatives aux répliques

La page Partitions vous permet d'afficher des informations concernant les répliques du serveur avec lequel vous communiquez. Vous pouvez appliquer un filtre à cette page à l'aide des options du cadre de l'Assistant, dans la partie gauche de la page.

L'option **Informations sur la partition du serveur** permet notamment d'afficher l'ID de l'entrée, l'état de la réplique, la date et l'heure de la purge et celles de la dernière modification.

Partition permet d'afficher des informations relatives à l'objet Arborescence sur le serveur.

Date/heure de la purge indique l'heure à laquelle vous pouvez retirer les données supprimées précédemment de la base de données car ces suppressions ont déjà été répercutées sur toutes les répliques.

Date/heure de la dernière modification permet d'afficher le dernier tampon horaire émis des données écrites dans la base de données pour la réplique. Vous pouvez ainsi voir si le tampon horaire affiche une date/heure future et si l'heure synthétique est utilisée.

Synchronisation des répliques permet d'afficher la page de résumé de synchronisation de réplique qui se rapporte à cette partition. La page Synchronisation des répliques affiche des informations sur l'état de synchronisation des partitions et l'état des répliques. Vous pouvez également afficher les listes des partitions et des répliques.

Contrôle et configuration de l'agentDS

La page Configuration de l'agent permet de contrôler et de configurer l'agentDS. Les fonctions accessibles sur cette page dépendent des droits de l'identité actuelle et de la version de eDirectory utilisée.

1. Dans iMonitor, cliquez sur Configuration de l'agent  .
2. Choisissez parmi les options suivantes :

   L'option **Informations sur les agents** permet d'afficher les informations de connexion relatives à votre serveur.

   L'option **Partitions** permet d'afficher les répliques du serveur avec lequel vous communiquez.

   Filtres de réplication permet d'afficher les filtres de réplication configurés pour l'agent eDirectory spécifié. NDS eDirectory 8.5 (version d'intégration 8.5*.xx*) est la première version de eDirectory à mettre en oeuvre une fonction dite de « répliques filtrées ». Pour plus d'informations sur la définition, l'utilisation et la configuration des répliques filtrées, reportez-vous à la section « Répliques filtrées », page 56.

   Déclencheurs d'agent permet de lancer des processus d'arrière-plan. Ces déclencheurs ont la même fonction que la commande SET DSTRACE=**option*.

   Paramètres des processus en arrière-plan permet de modifier l'intervalle d'exécution en arrière-plan de certains processus. Ces paramètres ont la même fonction que la commande SET DSTRACE=!*option*.

   Synchronisation de l'agent permet de désactiver ou d'activer la synchronisation entrante ou sortante. Vous pouvez indiquer, en heures, le délai pendant lequel la synchronisation doit être désactivée.

   Cache de base de données permet de configurer la quantité de mémoire cache de base de données utilisée par le moteur de base de donnéesDS. Diverses statistiques de cache sont également disponibles pour vous aider à déterminer si la quantité de mémoire cache disponible est suffisante. Les performances du système peuvent être significativement ralenties si la quantité de mémoire cache disponible est insuffisante.

   Paramètres de login permet de désactiver la mise en file d'attente des mises à jour de login. Vous pouvez également augmenter ou réduire le délai entre les mises à jour, si ces dernières sont activées.

   La vitesse de login a été améliorée dans les dernières versions de eDirectory. Cette amélioration consiste à mettre en file d'attente les modifications qui, dans les versions antérieures de NDS, devaient impérativement être effectuées au moment du login, pendant que l'utilisateur attendait. Toute modification de la base de données eDirectory nécessite un verrouillage. Par conséquent, pendant les périodes d'utilisation intensive, les délais de login peuvent être longs et imprévisibles, selon le nombre de demandes exigeant un verrouillage de la base de données à un moment spécifique. En éliminant cet impératif de verrouillage et en mettant les mises à jour de login en file d'attente, le login est beaucoup plus rapide et prévisible.

   Cette option permet de contrôler le comportement de la mise en file d'attente dans les différents environnements eDirectory. Dans certains environnements, les données placées en file d'attente sont très importantes et doivent être immédiatement enregistrées dans la base de données. L'utilisateur doit alors attendre pendant que l'exécution des mises à jour. Dans d'autres environnements, ces données ne sont pas du tout utilisées et peuvent être omises. Le comportement par défaut convient généralement à la plupart des environnements.

Configuration des paramètres Trace

Vous pouvez configurer les paramètres de trace dans la page Configuration de Trace. La fonction DSTrace de Novell iMonitor est centrée sur le serveur. Cela signifie qu'elle ne peut être lancée que sur un serveur qui exécute iMonitor. Si vous voulez accéder à cette fonction sur un autre serveur, vous devez basculer vers l'application iMonitor exécutée sur ce serveur.

Pour accéder aux informations de la page Configuration de Trace, vous devez disposer de droits équivalents à ceux de l'administrateur du serveur ou à un opérateur de la console. Le système vous invite à entrer votre nom d'utilisateur et votre mot de passe afin de vérifier vos références avant que vous accédiez aux informations de cette page.

1. Dans iMonitor, cliquez sur Configuration de Trace  .
2. Choisissez parmi les options suivantes :

   Mettre à jour permet de soumettre des modifications aux options de Trace et aux préfixes de la ligne Trace. Si DSTraceest désactivé, cliquez sur Trace activée pour le mettre en fonction. Si DSTrace est déjà activé, cliquez sur Mettre à jour pour soumettre les modifications apportées à la trace actuelle.

   Trace activée/Trace désactivée active ou désactive DSTrace. Le texte du bouton change en fonction de l'état de DSTrace. Si DSTrace est activé, ce bouton s'intitule Trace désactivée. Cliquez sur ce bouton pour activer ou désactiver DSTrace. Lorsque DSTrace est désactivé, l'option Trace activée a la même fonction que l'option Mettre à jour.

   L'option **Préfixes de la ligne Trace** permet de choisir les éléments de données à ajouter au début des lignes Trace.

   L'option intitulée **Options de Trace DS** s'applique aux événements de l'agent DS local où l'opération Trace est lancée. Ces options affichent les erreurs, les problèmes éventuels et d'autres informations relatives à eDirectory sur votre serveur local. L'activation des options de Trace DS peut accroître l'utilisation des ressources du processeur et réduire les performances du système. Par conséquent, DSTrace ne doit pas être utilisé de façon systématique. Il sert généralement à effectuer des diagnostics. Ces options, plus pratiques, sont équivalentes à la commande SET DSTRACE=+*option*.

   Configuration de l'événement liste les options d'événement eDirectory à activer ou désactiver pour la surveillance dans DSTrace. Le système d'événements génère des événements pour les activités locales telles que l'ajout et la suppression d'objets, ou la modification de valeurs d'attributs. Pour chaque type d'événement, une structure contenant les informations qui lui sont propres est renvoyée.

   Historique de Trace permet d'afficher la liste des précédentes exécutions de Trace. Chaque journal de Trace antérieur est identifié par la période durant laquelle les données Trace ont été collectées.

   Déclencheurs de Trace permet d'afficher les drapeaux Trace qui doivent être définis pour pouvoir afficher les informations souhaitées sur l'agentDS dans DSTrace. Ils peuvent écrire de très grandes quantités de données de trace. En règle générale, nous vous recommandons d'activer ces déclencheurs à la demande du support technique de Novell uniquement.
3. Cliquez sur Trace activée pour activer DSTrace et soumettre les éventuelles modifications.
4. Cliquez sur le bouton  ou sur Trace Live pour faire apparaître DS Trace dans iMonitor.

Affichage des informations relatives à l'état des processus

La page État du processus de l'agent permet d'afficher les erreurs d'état des processus en arrière-plan, ainsi que des informations complémentaires sur chaque erreur survenue. Les options listées dans le cadre de l'Assistant à gauche de cette page permettent de filtrer les informations affichées.

1. Dans iMonitor, cliquez sur État du processus de l'agent dans le cadre de l'Assistant.

   Les états des processus en arrière-plan actuellement signalés sont les suivants :

   - Synchronisation du schéma
   - Traitement des notices nécrologiques
   - Référence externe/DRL
   - Contrôle de la connectivité (limber)
   - Réparation

Affichage de l'activité de l'agent

La page Activité de l'agent permet de déterminer des modèles de trafic et les éventuels goulots d'étranglement système. Cette page permet d'afficher les requêtes et les verbes actuellement gérés par eDirectory. Vous pouvez également voir quelles sont les requêtes qui tentent d'obtenir des verrousDIB afin d'écrire dans la base de données et leur nombre.

Si vous affichez un serveur qui exécute Novell eDirectory 8.6 ou version ultérieure, vous verrez également la liste des partitions et des serveurs de l'anneau de répliques, le serveur étant spécifié dans le cadre du navigateur. Avec Novell eDirectory 8.6, la synchronisation n'utilise plus un seul thread. Tout serveur 8.6 est susceptible de transmettre plusieurs partitions simultanément, et ce sur un ou plusieurs partenaires de réplication. La page Activité de synchronisation a par conséquent été créée pour vous permettre de surveiller plus facilement cette stratégie de synchronisation parallèle.

1. Dans iMonitor, cliquez sur Activité de l'agent dans le cadre de l'Assistant.
2. Choisissez parmi les options suivantes :

   Activité et statistiques du verbe permet de connaître le nombre total de verbes appelés et de requêtes effectuées depuis la dernière initialisation de eDirectory. Ces pages indiquent en outre le nombre de requêtes actuellement actives ainsi que la durée minimale, maximale et moyenne (en millisecondes) de traitement de ces requêtes.

   Synchronisation en cours et planifiée liste les heures des différentes synchronisations entrantes et sortantes. Si une synchronisation entrante ou sortante est en cours, une icône indiquant que le processus est actif apparaît. Des informations sur l'heure de début de la synchronisation ainsi que sur le serveur concerné sont également affichées.

   Si les synchronisations entrantes et sortantes sont désactivées, une icône vous en informe ; elle vous indique également l'heure prévue pour leur réactivation. Pour les synchronisations sortantes, l'heure de la prochaine synchronisation planifiée est indiquée.

   Activités permet d'afficher la liste des événements actifs, les statistiques des gestionnaires d'événements, un récapitulatif des statistiques des événements, ainsi que les fonctions Droits de l'événement en cours qui ont été invoquées.

   Planification des processus à l'arrière-plan permet d'afficher les processus en arrière-plan qui ont été planifiés, ainsi que leur état actuel et l'heure prévue pour leur prochaine exécution.

Affichage des modèles de trafic

La page Statistiques du verbe permet de déterminer des modèles de trafic et les éventuels goulots d'étranglement système. Cette page permet d'afficher le nombre de verbes invoqués et de requêtes effectuées depuis la dernière initialisation de eDirectory. Elle indique également le nombre de requêtes actuellement actives ainsi que les durées minimale, maximale et moyenne (en millisecondes) de leur traitement. Le suivi concerne tous les processus en arrière-plan et toutes les requêtes de Bindery et les requêtes eDirectory standard.

Si vous affichez cette page à l'aide d'une ancienne version de eDirectory, toutes les informations qui apparaissent dans eDirectory version 8.5 ou ultérieure risquent de ne pas être disponibles.

Affichage des processus en arrière-plan

La page Planification des processus à l'arrière-plan permet d'afficher les processus en arrière-plan planifiés, ainsi que leur état actuel et l'heure prévue pour leur prochaine exécution. La fonction de planification des processus à l'arrière-plan de NovelliMonitor est centrée sur le serveur. Cela signifie qu'elle ne peut être affichée que sur un serveur qui exécute iMonitor. Si souhaitez accéder à la planification des processus à l'arrière-plan sur un autre serveur, il vous faut basculer vers l'application iMonitor exécutée sur ce serveur. Au fur et à mesure que vous mettez des serveurs à niveau vers eDirectory 8.5, vous augmentez le nombre de fonctions iMonitor disponibles centrées sur le serveur. Les pages DSTrace et DSRepair comprennent d'autres fonctions centrées sur le serveur.

Pour accéder aux informations de la page Planification des processus à l'arrière-plan, vous devez disposez de droits équivalents à ceux de l'administrateur du serveur ou d'un opérateur de la console. Avant de pouvoir accéder aux informations de cette page, le système vous invite à vous loguer afin de vérifier vos références.

Affichage des erreurs relatives aux serveurs eDirectory

La page Index des erreurs permet d'afficher des informations concernant les erreurs détectées sur les serveurs eDirectory. Ces erreurs sont de deux types: les erreurs propres à eDirectory et les erreurs d'un autre ordre, susceptibles de vous intéresser. Chaque erreur listée est dotée d'un hyperlien qui mène à sa description. Cette dernière fournit une explication, la cause possible et des actions de dépannage.

1. Dans iMonitor, cliquez sur Index des erreurs dans le cadre de l'Assistant.

   La page Index des erreurs permet d'accéder à la documentation Novell la plus récente qui traite des erreurs et présente des informations techniques ainsi que des livres blancs.

Affichage des informations DSRepair

La page DSRepair permet d'afficher les problèmes et de sauvegarder ou de nettoyer les ensembles DIB. La fonction DSRepair de Novell iMonitor est centrée sur le serveur. Cela signifie qu'elle ne peut être lancée que sur un serveur qui exécute iMonitor. Si vous devez accéder aux informations DSRepair sur un autre serveur, il vous faut basculer vers l'application iMonitor exécutée sur ce serveur. Au fur et à mesure que vous mettez des serveurs à niveau vers des versions plus récentes de eDirectory, vous augmentez le nombre de fonctions iMonitor disponibles centrées sur le serveur. Les pages DSTrace et Planification des processus à l'arrière-plan comprennent d'autres fonctions centrées sur le serveur.

Pour accéder aux informations de cette page, vous devez disposer de droits équivalents à ceux de l'administrateur du serveur ou d'un opérateur de la console. Avant de pouvoir accéder aux informations de cette page, le système vous invite à vous loguer afin de vérifier vos références.

1. Dans iMonitor, cliquez sur le bouton DSRepair  .
2. Choisissez parmi les options suivantes :

   Téléchargements permet de récupérer des fichiers liés aux réparations sur le serveur de fichiers. Si l'utilitaire DSRepair est en cours d'exécution ou si vous avez lancé une réparation à partir de la page DSRepair de iMonitor, vous ne pouvez pas accéder au fichier dsrepair.log tant que l'opération n'est pas terminée.

   Supprimer les anciens ensembles DIB permet de supprimer un ancien ensemble DIB en cliquant sur la croix rouge (X).

   AVERTISSEMENT : cette opération est irréversible. Lorsque vous sélectionnez cette option, l'ancien ensemble DIB est purgé du système de fichiers.

   Paramètres avancés de réparation NDS permet de rechercher les problèmes, de les résoudre ou de créer une sauvegarde de la base de données. Vous ne devez pas compléter le champ Options de prise en charge sauf si le support technique de Novell vous le demande.
3. Cliquez sur Lancer la réparation pour exécuter DS Repair sur ce serveur.

Affichage d'informations sur l'état de santé de l'agent

La page État de santé de l'agent permet d'afficher des informations sur l'état de santé de l'agent eDirectory spécifié, ainsi que sur les partitions et les anneaux de répliques auxquels il participe.

1. Dans iMonitor, cliquez sur État de santé de l'agent dans le cadre de l'Assistant.
2. Cliquez sur les liens pour afficher des informations détaillées.

Accès aux objets de votre arborescence

La page Parcourir vous permet d'accéder à des objets de votre arborescence. La barre de navigation située dans la partie supérieure de la page vous permet de savoir à quel serveur appartient l'objet que vous visualisez et d'afficher le chemin d'accès à cet objet. Le cadre Réplique situé dans la partie gauche de la page permet d'afficher un objet ou d'y accéder sur n'importe quelle partition réelle. Cliquez sur un objet souligné dans la page afin d'afficher plus d'informations à son sujet. Vous pouvez également cliquer sur n'importe quelle portion du nom dans le cadre du navigateur afin de parcourir l'arborescence en amont.

Les informations affichées sur cette page dépendent des droits eDirectory avec lesquels vous vous êtes logué, du type d'objet que vous explorez, ainsi que de la version des NDS ou de eDirectory que vous utilisez. Cette page affiche des objets XRef si vous êtes logué avec des droits Superviseur. La liste des répliques permet d'atteindre une copie réelle de la réplique. Si vous recherchez des objets dans des groupes dynamiques, le tampon horaire n'est pas affiché pour les membres dynamiques.

Synchronisation des répliques affiche l'état de synchronisation de la réplique qui contient cet objet.

Synchronisation des entrées affiche les attributs qui, selon ce serveur, doivent être synchronisés.

Infos sur la connexion permet de savoir où iMonitor a obtenu les informations sur cet objet.

Informations sur les entrées affiche les informations relatives aux noms, aux drapeaux, à la classe de base, au tampon horaire de modification et au résumé des données de connexion de l'objet.

Envoyer l'entrée à toutes les répliques permet de renvoyer les attributs de cette entrée à toutes les autres répliques. Ce processus peut s'avérer très long si l'objet possède de nombreuses valeurs d'attribut. Il n'a pas pour effet de rendre toutes les copies de l'objet identiques. Il permet simplement aux autres répliques de reconsidérer chacun des attributs.

Tout envoyer (visible uniquement si l'objet parcouru est une racine de partition et si l'option Mode avancé est activée) renvoie toutes les entrées de cette partition à l'ensemble des serveurs qui possèdent des répliques de la partition. Ce processus n'a pas pour effet de rendre toutes les copies de l'objet identiques. Il permet simplement aux autres répliques de reconsidérer chaque objet et ses attributs.

Affichage des entrées à synchroniser ou à purger

La page Cache de changement permet d'afficher une liste d'entrées que ce serveur doit prendre en considération lors des opérations de synchronisation ou de purge. Cette option n'est disponible que si le serveur auquel vous accédez exécute eDirectory 8.6 ou version ultérieure et que l'objet affiché est une racine de partition. Vous devez disposer de droits Superviseur sur le serveur NCP pour afficher cette page.

Synchronisation des entrées permet de déterminer les raisons pour lesquelles une entrée doit être synchronisée.

Affichage des détails de Novell Nsure Identity Manager

La page DirXML - Résumé permet d'afficher la liste des pilotes DirXML exécutés sur votre serveur, l'état et les détails de chacun d'entre eux, ainsi que les associations en attente.

1. Dans iMonitor, cliquez le bouton sur DirXML – Résumé  .
2. Choisissez parmi les options suivantes :

   État affiche l'état actuel du pilote spécifié. Les états possibles sont: Arrêté, Démarrage, En cours d'exécution, Arrêt en attente et Obtention du schéma.

   Option de démarrage correspond à l'option de démarrage actuellement définie pour le pilote sélectionné.

   En attente affiche le nombre d'associations qui n'ont pas encore été réalisées.

   L'icône **Détail du pilote** affiche des détails relatifs à l'abonné et à l'éditeur, les règles XML, les filtres ainsi que les listes d'associations en attente pour les pilotes DirXML qui s'exécutent sur votre serveur. Elle affiche également des informations détaillées sur les 50 premiers objets en attente. Les détails relatifs à la règle XML fournis sur cette page peuvent être utilisés pour définir l'objet des recherches dans les objets en attente afin de permettre que leur création se poursuive pour le pilote DirXML spécifié.

Affichage de l'état de synchronisation d'une réplique

La page Synchronisation des répliques permet d'afficher l'état de synchronisation d'une réplique.

1. Dans iMonitor, cliquez sur Synchronisation de l'agent dans le cadre de l'Assistant.
2. Cliquez sur Synchronisation des répliques pour la partition à afficher.
3. Utilisez les liens figurant sur cette page et sur la barre de navigation située à gauche pour accéder à d'autres partitions et vous déplacer dans l'anneau de répliques.

Configuration et affichage de rapports

La page Rapports permet d'afficher et de supprimer les rapports exécutés directement sur ce serveur. L'exécution de certains rapports peut être longue et exiger une grande quantité de ressources système.

Rapports planifiés sans authentification de l'utilisateur (en tant que [Public]). Tous les rapports que vous exécutez portent votre identité. Toutes les données d'un rapport sont stockées sur le serveur à partir duquel ce rapport a été exécuté.

La page Configuration du rapport permet d'afficher la liste des rapports préconfigurés, personnalisés et planifiés. Elle permet également de modifier, d'exécuter des rapports et peut servir à créer des rapports personnalisés pour des pages iMonitor. Le tableau suivant présente les rapports préconfigurés inclus dans iMonitor 2.1.

Rapport	Description
Informations sur le serveur	Parcourt l'intégralité de l'arborescence, communique avec tous les serveurs NCP détectés et signale les erreurs trouvées. Utilisez ce rapport pour diagnostiquer les problèmes liés à la synchronisation horaire et au contrôle de connectivité (limber) ou pour savoir si le serveur actuel peut communiquer avec tous les autres serveurs. S'il a été sélectionné dans la page de configuration, ce serveur peut également générer des informations sur l'état de santé de l'agent NDS pour chaque serveur de l'arborescence.
Liste des notices nécrologiques	Liste l'ensemble des notices nécrologiques de ce serveur.
Statistiques d'objet	Analyse les objets d'une étendue donnée, puis liste ceux répondant aux critères demandés. Ces critères peuvent être des tampons horairesfuturs, des objets inconnus, des objets renommés, le nombre de classes de base, des conteneurs, des alias ou des références externes.
Annonce du service	Liste les annuaires et les serveurs connus du serveur actuel via SLP ou SAP.
État de santé de l'agent	Recueille des informations sur l'état de santé du serveur actuel.
Nombre de valeurs	Liste les objets avec des attributs dont le nombre de valeurs est supérieur à une valeur spécifiée par vos soins.

Affichage et suppression de rapports

1. Dans iMonitor, cliquez sur le bouton Rapports  .
2. Cliquez sur le bouton  pour supprimer un rapport, ou sur  pour afficher un rapport.

Exécution d'un rapport

1. Dans iMonitor, cliquez sur Rapports  > Configuration du rapport.
2. Cliquez sur le bouton  pour exécuter un rapport.

Configuration ou planification d'un rapport

1. Dans iMonitor, cliquez sur Rapports  > Configuration du rapport.
2. Cliquez sur le bouton  pour configurer et planifier un rapport.
3. Sélectionnez les options souhaitées, puis cliquez sur Enregistrer les valeurs par défaut pour enregistrer les options sélectionnées.
4. (Facultatif) Configurez le rapport afin de définir une exécution périodique ou ultérieure.
   - **4a** Indiquez une fréquence, ainsi qu'un jour et une heure de début.
   - **4b** Cliquez sur Planifier.
5. Cliquez sur Exécuter le rapport pour lancer le rapport.

Création d'un rapport personnalisé

Les rapports personnalisés permettent de lancer n'importe quelle page iMonitor en tant que rapport.

1. Dans iMonitor, cliquez sur Rapports  > Configuration du rapport.
2. Cliquez sur le bouton  sur la ligne Rapports personnalisés de la liste des rapports pouvant être exécutés.
3. Nommez le rapport, puis saisissez l'URL de la page iMonitor que vous souhaitez lancer sous forme de rapport.

   Lors de l'exécution d'un rapport personnalisé, entrez l'URL de la manière suivante :

   `/nds/page requise`
4. Indiquez le nombre de versions du rapport à conserver.
5. (Facultatif) Cliquez sur Enregistrer pour sauvegarder le rapport.
6. (Facultatif) Configurez le rapport afin de définir une exécution périodique ou ultérieure.
   - **6a** Indiquez une fréquence, ainsi qu'un jour et une heure de début.
   - **6b** Cliquez sur Planifier.
7. Cliquez sur Exécuter le rapport pour lancer le rapport.

Affichage des définitions d'un schéma, d'une classe et d'un attribut

La page Schéma permet d'afficher les définitions relatives à un schéma, une classe ou un attribut. Vous pouvez visualiser le schéma chargé dans votre arborescence, ses éventuelles extensions, ainsi que les informations qui lui sont spécifiques, telles que les modifications ou extensions effectuées.

1. Dans iMonitor, cliquez sur Schéma dans le cadre de l'Assistant.
2. Choisissez parmi les options suivantes :

   Liste des synchronisations liste les serveurs avec lesquels ce serveur sera synchronisé. Cette option n'est disponible que pour les serveurs qui exécutent NDS eDirectory 8.5 ou versionultérieure. Vous devez disposer de droits Superviseur sur le serveur pour afficher ces informations.

   Racine du schéma affiche des informations sur la réplique du schéma la plus proche de la racine de l'arborescence dans ce contexte.

   Chaque serveur eDirectory stocke une réplique du schéma dans sa totalité. Celle-ci est stockée séparément des partitions qui contiennent les objets Annuaire. Les modifications apportées à une réplique du schéma sont répercutées sur les autres répliques. Vous ne pouvez apporter des modifications au schéma que via un serveur qui stocke une réplique accessible en écriture de la partition racine. Les serveurs qui stockent des répliques Lecture seule de la partition racine peuvent lire les informations du schéma, mais pas les modifier.

   Définitions des attributs liste, pour chaque attribut, son nom, sa syntaxe et ses contraintes de fonctionnement. Utilisez la fenêtre de navigation située à gauche pour rechercher des attributs et y accéder.

   Définitions de classe liste le nom de chaque classe, ses règles et ses attributs. Utilisez la fenêtre de navigation située à gauche pour rechercher des attributs et y accéder.

Recherche d'objets

La page de recherche permet de rechercher des objets à l'aide de différents filtres et options de requête. Les options de requête et les filtres sont regroupés dans deux niveaux de requêtes de recherche: les requêtes élémentaires et les requêtes avancées. Les requêtes de recherche élémentaires sont destinées aux utilisateurs ordinaires de eDirectory souhaitant effectuer des recherches simples. En revanche, les requêtes de recherche avancées s'adressent plus particulièrement aux utilisateurs expérimentés et s'utilisent pour des recherches élaborées. Actuellement, seules les recherches au niveau du serveur sont prises en charge.

Toutes les options de recherche et tous les filtres des quatre sections sont conjonctifs. Les champs vierges (à l'exception de Nom distinctif relatif) seront ignorés. Utilisez la touche Ctrl pour désélectionner un élément ou sélectionner plusieurs éléments dans des listes autorisant les sélections multiples. Les listes autorisant les sélections multiples désélectionnées seront également ignorées.

1. Dans Novell iMonitor, cliquez sur le bouton Rechercher  .
2. Choisissez parmi les options suivantes :

   Les **Options d'étendue** permettent de spécifier l'étendue de la recherche.

   Les **Filtres d'entrée** permettent d'indiquer les filtres de requête de recherche liés aux informations entrées.

Les **Filtres d'attribut et de valeur** permettent d'indiquer les filtres de requête de recherche liés aux attributs et aux valeurs.

Les **Options d'affichage** permettent de spécifier les options qui contrôlent le format d'affichage des résultats de la recherche.

3. Cliquez sur le bouton Aide situé dans la partie inférieure du formulaire de recherche pour afficher des informations succinctes sur le formulaire, à l'intérieur même de ce dernier.

   Cliquez sur Recharger ou sur Rafraîchir pour effacer les informations d'aide.

Utilisation de la visionneuse de flux

La page Visionneuse de flux permet d'afficher le flux actuel dans l'un des formats suivants :

- Texte brut
- HTML
- GIF
- JPEG
- BMP
- WAV
- Dump hexadécimal
- Autre

Si vous souhaitez systématiquement afficher certains attributs de flux dans un format donné, vous pouvez utiliser la visionneuse de flux pour définir les paramètres d'affichage par défaut.

Configuration de l'attribut de flux NDS modifie le format d'affichage par défaut des flux dans votre navigateur. L'affichage correct du flux dépend exclusivement de votre navigateur ; il est donc possible que les paramètres que vous avez choisis ne soient pas toujours appliqués.

Vous devez être authentifié auprès du serveur pour pouvoir valider les modifications apportées aux paramètres par défaut. Vos modifications sont stockées dans le fichier streams.ini (pour les serveurs NetWare et Windows) ou streams.conf (pour les serveurs Solaris et Linux). Il est donc également possible de modifier manuellement les paramètres par défaut.

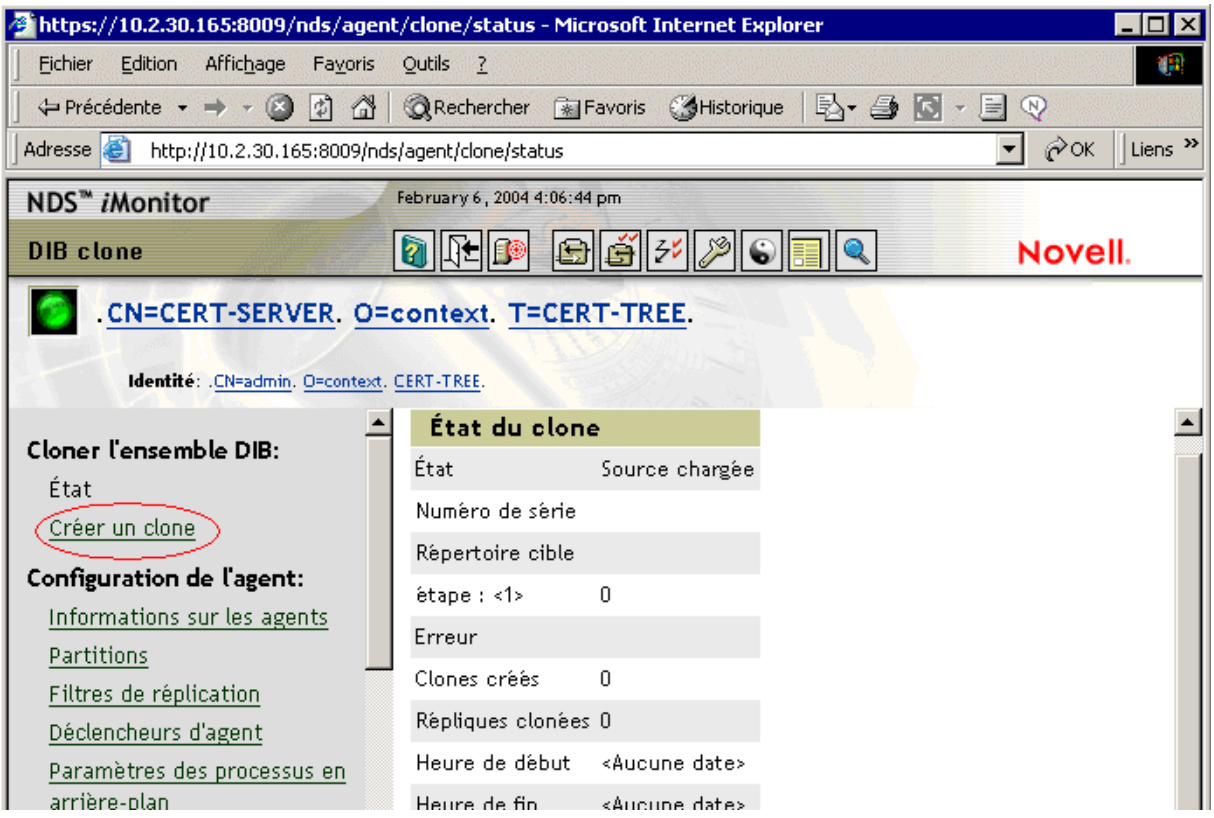
Cloner l'ensembleDIB

Cette option permet de dupliquer un ensemble complet de fichiers DIB d'une base de données eDirectory stockée sur un seul serveur (le serveur source). Ce clone peut ensuite être placé sur un autre serveur (le serveur cible). Lorsque le serveur cible lance eDirectory, il charge l'ensemble de fichiers DIB, accède à la réplique maîtresse de l'objet Serveur, résout son nom, puis synchronise les modifications éventuelles apportées à l'ensemble de fichiers DIB après la création du clone.

Vous devez placer le clone d'un ensemble DIB eDirectory sur un serveur qui exécute le même système d'exploitation que le serveur sur lequel le clone a été créé. Par exemple, si vous souhaitez restaurer un ensemble de fichiersDIB cloné sur un serveur Solaris, créez le clone sur un serveur Solaris, et non sur un serveur NetWare ou Windows.

Bien que l'interface dorsale de cette fonction soit livrée avec eDirectory 8.7, elle n'est prise en charge que depuis eDirectory 8.7.1 avec iMonitor 2.1 ou version ultérieure. Cette fonction ne s'applique pas aux versions de Novell eDirectory ou de NDS antérieures à 8.7.

Figure 32 Page Cloner l'ensemble DIB dans iMonitor



Cette section comprend les informations suivantes :

- « Utilisation de l'option Cloner l'ensemble DIB », page 216
- « Création d'un clone », page 216

Utilisation de l'option Cloner l'ensemble DIB

L'option Cloner l'ensemble DIB est employée dans les cas suivants :

- Création d'un serveur avec des partitions dont l'état est déjà « actif »

  Les avantages sont les suivants :

  - Tous les serveurs de l'anneau de doivent pas être en cours d'exécution pour pouvoir leur ajouter un nouveau serveur dans l'anneau de répliques.
  - Tout nouveau serveur disposera automatiquement de toutes les partitions sans qu'aucune synchronisation ne soit nécessaire.
  - Délai de récupération réduit.

- Reprise après sinistre

Avantages	Inconvénients
• Une seule copie de la partition est nécessaire à une exécution correcte. • Temps d'arrêt réduit sur des serveurs de grande taille comprenant plusieurs partitions.	• Au moins une copie correcte des partitions en question est nécessaire. • Les sauvegardes SSL ou de sécurité ne sont pas prises en charge. • Le système de fichiers n'est pas pris en compte.

- Sauvegarde et restauration

Avantages	Inconvénients
• Délai de récupération réduit notamment pour les bases de données volumineuses.	• Seuls les composants eDirectory de base sont ajoutés. Les composants LDAP, SNMP, SSL, etc. ne sont ni installés ni configurés. • Les dernières modifications ne sont pas récupérées. Seul un instantané est réalisé. Aucun fichier journal de transaction individuelle n'est exécuté.

En raison des inconvénients cités ci-dessus, nous vous déconseillons d'utiliser l'option Cloner l'ensemble DIB pour des opérations de sauvegarde et de restauration.

Création d'un clone

Vous pouvez créer un ensemble de fichiers DIB cloné alors que le serveur d'origine est en ligne ou hors ligne. La méthode hors ligne nécessite la mise hors service de eDirectory. Si vous utilisez le mode en ligne, eDirectory n'est pas verrouillé.

- « Méthode en ligne », page 217
- « Méthode hors ligne », page 218

Méthode en ligne

1 Étendez le schéma de l'arborescence.

Veillez à étendre le schéma afin d'éviter toute erreur. Utilisez le fichier dibclone.sch disponible dans le programme d'installation de eDirectory. Cette opération permet d'ajouter les attributs nécessaires au fonctionnement de l'utilitaire de clonage iMonitor.

Plate-forme	Pour étendre le schéma
NetWare	Utilisez NWConfig (NWConfig.nlm > Options de configuration > Annuaire > Étendre le schéma). Le fichier dibclone.sch se trouve dans le répertoire sys:\system\schema.
Windows	Utilisez le fichier NDSCons.exe [à partir de NDSCons.exe, chargez install.dlm, puis cliquez sur Install Additional Schema Files (Installer d'autres fichiers de schéma)]. Le fichier dibclone.sch se trouve dans le répertoire C:\Novell\NDS.
Linux, Solaris, AIX et HP-UX	Utilisez ndssch. Le fichier dibclone.sch se trouve dans le répertoire /opt/novell/eDirectory/lib/nds-schema. Pour plus d'informations, reportez-vous à la section « Utilisation de l'utilitaire ndssch pour étendre le schéma sur Linux, Solaris, AIX ou HP-UX », page 127.

2 Créez l'ensemble de fichiers DIB cloné.

2a Lancez Cloner la configuration du DIB dans iMonitor.

Cliquez sur Configuration de l'agent > Cloner l'ensemble DIB > Créer un clone.

2b Indiquez le nom complet du serveur cible et le chemin cible des fichiersDIB clonés, puis cochez les cases Créer un objet Clone et Cloner le DIB en ligne.

Le nom du serveur NCP (Objet Clone) du serveur cible doit correspondre au nom de serveur cible.

2c Cliquez sur Soumettre.

L'objet Clone NDS est créé et l'ensemble de fichiers DIB est copié à l'emplacement cible spécifié.

3 Déplacez l'ensemble de fichiers DIB cloné vers le serveur cible dans le répertoire approprié. Par ailleurs, sous les systèmes Linux, Solaris, AIX et HP-UX, transférez le fichier /etc/opt/novell/eDirectory/conf/nds.conf sur le serveur cible et remplacez toutes les références au nom du serveur source contenues dans le fichier par le nom du serveur cible.

4 Exécutez eDirectory sur le serveur source.

Assurez-vous que la réplique maîtresse de l'objet Serveur cible exécute eDirectory et qu'elle est disponible. Lors de son initialisation sur le serveur cible, eDirectory communique avec la réplique maîtresse sur laquelle le nom final du serveur cible est résolu.

Méthode hors ligne

1 Étendez le schéma de l'arborescence.

Veillez à étendre le schéma afin d'éviter toute erreur. Utilisez le fichier dibclone.sch disponible dans le programme d'installation de eDirectory. Cette opération permet d'ajouter les attributs nécessaires au fonctionnement de l'utilitaire de clonage iMonitor.

Plate-forme	Pour étendre le schéma
NetWare	Utilisez NWConfig (NWConfig.nlm > Options de configuration > Annuaire > Étendre le schéma). Le fichier dibclone.sch se trouve dans le répertoire sys:\system\schema.
Windows	Utilisez le fichier NDSCons.exe [à partir de NDSCons.exe, chargez install.dlm, puis cliquez sur Install Additional Schema Files (Installer d'autres fichiers de schéma)]. Le fichier dibclone.sch se trouve dans le répertoire C:\Novell\NDS.
Linux, Solaris, AIX et HP-UX	Utilisez ndssch. Le fichier dibclone.sch se trouve dans le répertoire *répertoire_installation*/opt/novell/eDirectory/lib/nds-schema. Pour plus d'informations, reportez-vous à la section « Utilisation de l'utilitaire ndssch pour étendre le schéma sur Linux, Solaris, AIX ou HP-UX », page 127.

2 Créez l'ensemble de fichiers DIB cloné.

2a Lancez Cloner la configuration du DIB dans iMonitor.

Cliquez sur Configuration de l'agent > Cloner l'ensemble DIB > Créer un clone.

2b Indiquez le nom complet du serveur cible, cochez la case Créer un objet Clone et désélectionnez la case Cloner le DIB en ligne.

Le nom du serveur NCP du serveur cible doit correspondre au nom de serveur cible.

2c Cliquez sur Soumettre.

L'objet Clone NDS est créé, eDirectory est mis hors service sur le serveur source et un message d'erreur indique que eDirectory est verrouillé.

2d Copiez manuellement les fichiers *.nds, nds* et nds.rfl/*.* dans un emplacement ou sur un support qui permettra de copier aisément l'ensemble sur le serveur cible. Par ailleurs, sous les systèmes Linux, Solaris, AIX et HP-UX, transférez le fichier /etc/opt/novell/eDirectory/conf/nds.conf sur le serveur cible et remplacez toutes les références au nom du serveur source contenues dans le fichier par le nom du serveur cible.

2e Mettez eDirectory en service sur le serveur source.

Le clone n'est pas valide si vous redémarrez eDirectory sur le serveur source avant que les fichiers soient copiés. Vous devrez alors supprimer l'objet Serveur NCP et recréer le clone.

3 Déplacez l'ensemble de fichiers DIB cloné vers le serveur cible dans le répertoire approprié.

4 Exécutez eDirectory sur le serveur cible.

Assurez-vous que la réplique maîtresse de l'objet Serveur cible exécute eDirectory et qu'elle est disponible. Lors de son initialisation sur le serveur cible, eDirectory communique avec la réplique maîtresse sur laquelle le nom final du serveur cible est résolu.

SDIKEY

1. Mettez eDirectory hors service sur le serveur cible.
2. Copiez le fichier NICISDI.KEY dans le répertoire approprié du serveur source sur le serveur cible.

Plate-forme	Chemin
NetWare	sys:\system\nici\NICISDI.KEY
Windows	C:\WINNT\System32\Novell\NICI\NICISDI.KEY
Linux, Solaris, AIX et HP-UX	/var/novell/nici/0/nicisdi.key

3. Démarrez eDirectory sur le serveur cible.

Configuration des services SAS, LDAP et SNMP

Sous les systèmes Linux, Solaris, AIX et HP-UX, les services listés ci-dessous peuvent être configurés simultanément en ajoutant la commande suivante à la ligne:

ndsconfig upgrade [-a *FDN_admin*]

SAS

Plate-forme	Commande ou outil
NetWare	Créez un objet Service SAS et des certificats à l'aide de iManager.
Windows	Créez un objet Service SAS et des certificats à l'aide de iManager.
Linux, Solaris, AIX et HP-UX	ndsconfig -t *nom_arborescence* -o *contexte_serveur* -m sas

LDAP

Plate-forme	Commande ou outil
NetWare	Créez des objets Serveur et Groupe LDAP à l'aide de iManager.
Windows	Créez des objets Serveur et Groupe LDAP à l'aide de iManager.
Linux, Solaris, AIX et HP-UX	ndsconfig -t *nom_arborescence* -o *contexte_serveur* -m ldap ou Créez des objets Serveur et Groupe LDAP à l'aide de iManager.

SNMP

Plate-forme	Commande ou outil
NetWare	SNMPINST -c *Contexte_admin mot_de_passe DN_serveur*
Windows	rundll32 snmpinst, snmpinst -c *createobj* -a *FDN_utilisateur* -p *mot_de_passe* -h *nom_hôte_ou_adresse_IP*
Linux, Solaris, AIX et HP-UX	ndsconfig -t *nom_arborescence* -o *contexte_serveur* -m snmp

Opérations iMonitor sécurisées

La sécurisation des accès à votre environnement iMonitor implique la procédure de protection suivante :

1. Utilisez un pare-feu et assurez un accès VPN (réseau privé virtuel). (Cela s'applique également à Novell iManager et aux autres services Web dont l'accès doit être restreint.)
2. Qu'un pare-feu soit ou non en place, limitez le type d'accès autorisé via iMonitor pour améliorer la protection contre les attaques de refus de service.

   Bien que des efforts considérables aient été entrepris pour s'assurer que iMonitor valide les données reçues via des requêtes d'URL, il est pratiquement impossible de garantir le rejet de toutes les entrées non valides éventuelles. Pour réduire le risque d'attaques de refus de service via des URL non valides, il existe trois niveaux d'accès que vous pouvez contrôler au moyen du fichier de configuration de iMonitor à l'aide de l'option LockMask.

Niveau d'accès	Description
0	Pas d'authentification requise avant le traitement des URL par iMonitor. Dans ce cas, les droits eDirectory de l'identité .[Public]. sont appliqués à toutes les requêtes et les informations affichées par iMonitor sont limitées par les droits de l'utilisateur .[Public]. Cependant, étant donné qu'aucune authentification n'est requise pour l'envoi d'URL à iMonitor, ce dernier peut être vulnérable aux attaques de refus de service basées sur la transmission d'informations incohérentes dans les URL.
1 (par défaut)	Authentification requise sous une identité eDirectory avant le traitement des URL par iMonitor. Dans ce cas, les droits eDirectory de cette identité sont appliqués à toutes les requêtes et sont donc restreints. Il existe une vulnérabilité aux attaques de refus de service identique à celle du niveau 0, à cette exception près que l'attaque doit être lancée par une personne qui s'est réellement authentifiée sur le serveur. Tant que l'authentification n'aboutit pas, iMonitor, lorsqu'il est configuré dans cet état, répond aux requêtes d'URL par une boîte de dialogue de login afin de se protéger contre les attaques lancées par des utilisateurs non authentifiés.
2	Avant le traitement des URL par iMonitor, authentification requise sous une identité eDirectory disposant de droits équivalents à ceux d'un superviseur sur le serveur auprès duquel iMonitor s'authentifie. Il existe une vulnérabilité aux attaques de refus de service identique à celle du niveau 1, à cette exception près que l'attaque doit être lancée par une personne qui s'est réellement authentifiée en tant que superviseur du serveur. Tant que l'authentification n'aboutit pas, iMonitor, lorsqu'il est configuré dans cet état, répond aux requêtes d'URL par une boîte de dialogue de login afin de se protéger contre les attaques lancées par des utilisateurs non authentifiés qui ne sont pas des superviseurs.

Le niveau 1 est le niveau par défaut car de nombreux administrateurs n'ont pas d'accès Superviseur à chaque serveur de l'arborescence, mais peuvent avoir besoin d'utiliser le service iMonitor sur un serveur qui interagit avec les leurs.

REMARQUE : plusieurs fonctions de iMonitor telles que Repair et Trace requièrent des droits équivalents à ceux de superviseur pour les accès, quel que soit le paramètre LockMask.

8 Fusion d'arborescences Novell eDirectory

L'utilitaire de fusion Novell® eDirectory™ permet de fusionner deuxarborescences Novell eDirectory distinctes pour n'en former plus qu'une seule. Seuls les objets Arborescence sont fusionnés ; les objets Conteneur et leurs objets Feuille gardent leur identité au sein de la nouvelle arborescence.

SUGGESTION : pour déplacer les objets Feuille ou fusionner des partitions, utilisez ConsoleOne® ou Novell iManager.

Les deux arborescences que vous fusionnez sont appelées arborescence source locale et arborescence cible. Avant la fusion de deux arborescences, il ne doit rester qu'une seule réplique de la partition racine dans l'arborescence cible, les autres doivent avoir été supprimées. Une fois cette opération effectuée, vous pouvez lancer la fusion. Après la fusion, deux répliques de la partition racine coexistent: celle de l'arborescence cible et celle qui se trouvait sur le serveur de l'arborescence source à l'origine de la fusion. Si vous avez besoin d'autres répliques de la partition racine dans votre arborescence, vous pouvez les intégrer après la fusion.

Si le serveur de l'arborescence cible contient plusieurs répliques de la partition racine au moment de la fusion, les serveurs ne disposant pas de la réplique maîtresse risquent d'avoir des difficultés à placer les objets de référence externe. Ces objets se trouvent dans des racines de partition de référence subordonnée qui doivent être placées sur les autres serveurs disposant d'une réplique de la partition racine afin de représenter les limites de la partition. Pour chaque partition subordonnée à la partition racine de l'arborescence source, une racine de partition de référence subordonnée doit être placée dans l'arborescence cible. En cas d'échec, le code d'erreur eDirectory -605, révélant un problème d'état de synchronisation, sera renvoyé. Dans ce cas, utilisez DSRepair pour réparer la base de données locale sur le serveur qui a généré l'erreur. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale », page 265.

DSMerge ne modifie pas les noms ou contextes eDirectory au sein des conteneurs. Les droits d'objets et de propriétés des objets fusionnés sont conservés.

Ce chapitre comprend les rubriques suivantes :

Fusion d'arborescences eDirectory

Pour fusionner des arborescences eDirectory, utilisez l'Assistant de fusion d'arborescence de Novell iManager. Celui-ci permet de fusionner les racines de deuxarborescences eDirectory distinctes. Seuls les objets Arborescence sont fusionnés ; les objets Conteneur et leurs objets Feuille gardent leur identité au sein de la nouvelle arborescence.

Les deuxarborescences que vous fusionnez sont appelées arborescence source et arborescence cible. L'arborescence cible est celle dans laquelle l'arborescence source sera fusionnée.

DSMerge ne modifie pas le nom des objets au sein des conteneurs. Les droits d'objets et de propriétés de l'arborescence fusionnée sont conservés.

Conditions préalables

- ❑ Novell eDirectory 8.8 doit être installé sur le serveur contenant la réplique maîtresse de la partition [Root] de l'arborescence source.
- ❑ Les autres serveurs de l'arborescence source doivent faire l'objet d'une mise à niveau vers eDirectory 8.6 ou version ultérieure pour offrir les fonctionnalités appropriées.

Exigences relatives à l'arborescence cible

- ❑ Novell eDirectory 8.8 doit être installé sur le serveur contenant la réplique maîtresse de la partition [Root] de l'arborescence cible. Si ce serveur exécute une autre version des services NDS® ou de eDirectory, la fusion échoue.
- ❑ Les autres serveurs de l'arborescence cible doivent faire l'objet d'une mise à niveau vers eDirectory 8.6 ou version ultérieure pour offrir les fonctionnalités appropriées.
- ❑ Vous ne pouvez pas conserver des conteneurs portant le même nom qui seraient subordonnés à l'objet Arborescence dans les arborescences source et cible. Avant de fusionner deux arborescences, vous devez renommer l'un de ces conteneurs.
- ❑ Si les arborescences source et cible contiennent un objet Sécurité, vous devez supprimer l'un de ces objets avant de fusionner les arborescences.

Exigences relatives au schéma

Avant de procéder à une fusion, vérifiez que le schéma des deux arborescences est strictement identique. Vous devez exécuter DSRepair sur le serveur contenant la réplique maîtresse de la partition [Racine] de chaque arborescence. Utilisez l'option Importer le schéma à distance afin de vous assurer que chaque arborescence prend en compte l'ensemble du schéma de l'autre arborescence.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Maintenance du schéma.
3. Indiquez quel serveur effectuera l'opération de maintenance du schéma, puis cliquez sur Suivant.
4. Authentifiez-vous auprès du serveur indiqué, puis cliquez sur Suivant.
5. Cliquez sur Importer le schéma à distance > Suivant.

6 Spécifiez le nom de l'arborescence à partir de laquelle le schéma doit être importé.

7 Cliquez sur Démarrer.

Il se peut que vous deviez exécuter cette option sur les arborescences source et cible jusqu'à ce qu'il n'y ait plus de différence entre les schémas. Sinon, la fusion échouera.

8 Lorsque le message « Terminé » contenant les informations renvoyées par l'opération de maintenance du schéma s'affiche, cliquez sur Fermer pour quitter le processus.

Fusion des arborescences source et cible

Lorsque vous fusionnez les arborescences, les serveurs de l'arborescence source sont intégrés à l'arborescence cible.

L'objet Arborescence cible devient le nouvel objet Arborescence des objets de l'arborescence source et l'arborescence de tous les serveurs de l'arborescence source prend le nom de l'arborescence cible.

Une fois la fusion terminée, le nom d'arborescence des serveurs de l'arborescence cible est conservé.

Les objets qui étaient subordonnés à l'objet Arborescence source deviennent subordonnés à l'objet Arborescence cible.

Modification des partitions

Au cours de la fusion, DSMerge sépare les objets situés sous l'objet Arborescence source en partitions distinctes.

Toutes les répliques de la partition Arborescence sont ensuite supprimées des serveurs dans l'arborescence source, à l'exception de la réplique maîtresse. Le serveur qui contenait la réplique maîtresse de l'arborescence source reçoit une réplique de la partition Arborescence de l'arborescence cible.

La Figure 33 et la Figure 34 illustrent les effets de la fusion de deux arborescences sur les partitions.

Figure 33 Arborescences eDirectory avant la fusion

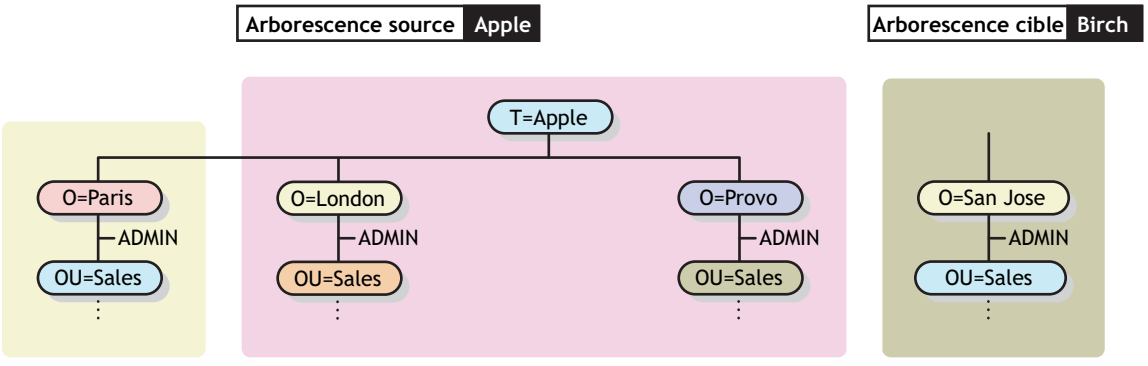
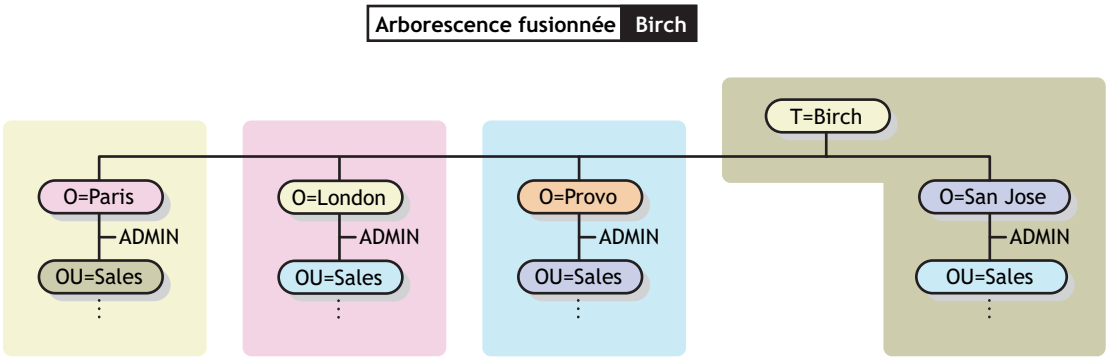


Figure 34 Arborescence eDirectory fusionnée



Préparation des arborescences source et cible

Avant d'effectuer une fusion, vérifiez que l'état de synchronisation de l'ensemble des serveurs concernés par cette opération est stable. Le tableau suivant indique les conditions préalables en vue de la préparation des arborescences source et cible à la fusion.

Condition préalable	Action requise
WANMAN doit être désactivé sur tous les serveurs qui contiennent une réplique de la partition Arborescence de l'arborescence source ou cible.	Contrôlez la règle WANMAN ; les restrictions de communication WAN ne doivent pas gêner la fusion. Au besoin, désactivez WANMAN avant de lancer la fusion.
Aucun alias ou objet Feuille ne peut exister sur l'objet Arborescence de l'arborescence source.	Supprimez tout alias ou objet Feuille de l'objet Arborescence de l'arborescence source.
Les arborescences source et cible ne doivent pas comporter de noms semblables.	Renommez les objets dont le nom est identique sur les arborescences source et cible. Si vous ne souhaitez pas renommer les objets Conteneur, déplacez-les vers un autre conteneur dans l'arborescence, puis supprimez le conteneur vide avant de lancer DSMerge. Pour plus d'informations, reportez-vous à la section Chapitre 3, « Gestion des objets », page 93. Des objets Conteneur identiques peuvent être présents dans les deux arborescences s'ils ne sont pas immédiatement subordonnés à l'objet Arborescence.
Aucune connexion de login ne doit exister dans l'arborescence source.	Fermez toutes les connexions dans l'arborescence source.
Les arborescences source et cible doivent utiliser la même version de eDirectory.	Mettez à niveau tous les serveurs qui contiennent une réplique de la partition racine sur lesquels eDirectory 8.8 n'est pas encore installé.
L'arborescence cible doit contenir une seule copie de la réplique racine.	Supprimez toutes les répliques de l'arborescence cible, à l'exception de la réplique maîtresse.
Le schéma des arborescences source et cible doit être identique.	Exécutez DSMerge. Si des rapports font état de problèmes au niveau du schéma, utilisez DSRepair pour les faire correspondre. (Pour plus d'informations, reportez-vous à la section « Importation du schéma à distance », page 276.) Exécutez de nouveau DSMerge.

Condition préalable	Action requise
Seule une des deuxarborescences peut posséder un conteneur de sécurité subordonné à la racine de larborescence.	Si les arborescences source et cible sont dotées d'un conteneur de sécurité, supprimez-en un en suivant les indications de l'« Remarques sur NMAS », page 565.

Étant donné que l'opération de fusion est une transaction unique, elle ne risque pas de subir de défaillance catastrophique due à une coupure de courant ou à une panne matérielle. Toutefois, avant d'utiliser DSMerge, effectuez une sauvegarde en bonne et due forme de la base de données eDirectory. Pour plus d'informations, reportez-vous à la section « Sauvegarde et restauration de Novell eDirectory », page 383.

Synchronisation des heures avant la fusion

IMPORTANT : la configuration correcte de la synchronisation horaire est un processus complexe. Prévoyez suffisamment de temps pour synchroniser les deuxarborescences avant de les fusionner.

Novell eDirectory ne fonctionnera pas correctement si les heures des différentes sources horaires utilisées ne concordent pas ou si les serveurs d'une arborescence ne sont pas tous synchronisés.

Avant d'effectuer la fusion, vérifiez que l'heure de tous les serveurs des deuxarborescences est synchronisée et qu'un seul serveur horaire fait office de source horaire. Toutefois, l'heure de l'arborescence cible peut avancer (de cinq minutes maximum) par rapport à celle de l'arborescence source.

En règle générale, une arborescence doit uniquement comporter un seul serveur de référence ou serveur horaire unique. Il en est de même dans l'arborescence après la fusion.

Si chacune des arborescences que vous fusionnez comporte un serveur de référence ou un serveur horaire unique, réassignez l'un d'eux pour qu'il fasse référence au serveur de référence ou au serveur horaire unique de l'autre arborescence afin d'obtenir un seul serveur de référence ou serveur horaire unique dans l'arborescence finale.

Pour plus d'informations sur les types de serveur horaire, consultez le manuel *Network Time Management Administration Guide* (Guide d'administration de la gestion de l'heure réseau) (http://www.novell.com/documentation/lg/nw65/time_enu/data/hl5k6r0y.html).

Fusion de deux arborescences

Pour que toutes les options de menu soient opérationnelles, exécutez DSMerge sur un serveur qui contient la réplique maîtresse de la partition Arborescence.

Si vous ne savez pas où est stockée la réplique maîtresse, un message vous indique le nom du serveur approprié lorsque vous tentez une opération qui requiert cette réplique maîtresse.

Pour effectuer une fusion, utilisez l'une des méthodes suivantes :

- Novell iManager
- Le client à ligne de commande eMBox

  Pour plus d'informations, reportez-vous à la section « Utilisation du client eMBox pour fusionner des arborescences », page 233.

Lors de la fusion d'arborescences volumineuses, vous gagnerez du temps à désigner comme arborescence source celle qui comporte le moins d'objets immédiatement subordonnés à l'objet Arborescence. Cela permet de minimiser le nombre de divisions en partitions lors de la fusion, puisque tous les objets subordonnés à l'objet Arborescence entraînent la création de nouvelles partitions au cours de cette opération.

Étant donné que le nom de l'arborescence source n'existe plus après la fusion, il est possible que vous ayez à modifier la configuration des postes de travail client. Pour le client Novell™ pour DOS/Windows, vérifiez les instructions Preferred Tree (Arborescence préférée) et Preferred Server (Serveur préféré) dans les fichiers net.cfg. Pour le client Novell pour Windows NT/2000 et Windows 95/98, vérifiez les instructions Preferred Tree et Preferred Server dans la page de propriétés du client.

Si l'instruction Preferred Server est utilisée, le client n'est pas affecté par une fusion ou un changement de nom des arborescences car il continue à se servir du nom pour se loguer au serveur. Si l'instruction Preferred Tree est utilisée et que l'arborescence est fusionnée ou renommée, le nom de l'arborescence disparaît. Seul le nom de l'arborescence cible est conservé après la fusion. Remplacez le nom de l'arborescence préférée par celui de la nouvelle arborescence.

SUGGESTION : pour réduire au maximum le nombre de postes de travail client à mettre à jour, désignez comme arborescence cible celle qui comporte le plus grand nombre de postes de travail client, car l'arborescence finale conserve le nom de l'arborescence cible. Vous pouvez également changer le nom de l'arborescence après la fusion pour que le nom de l'arborescence finale corresponde à l'arborescence possédant le plus grand nombre de postes de travail client. Pour plus d'informations, reportez-vous à la section « Changement du nom d'une arborescence », page 232.

La liste suivante de conditions préalables vous permet de savoir si vous êtes prêt à procéder à la fusion :

- ❑ Vous avez accès au serveur de l'arborescence source via iManager.
- ❑ Vous connaissez le nom et le mot de passe des objets Administrateur disposant de droits d'objet Superviseur sur l'objet Arborescence des deuxarborescences à fusionner.
- ❑ La base de données eDirectory des deuxarborescences a été sauvegardée.
- ❑ Tous les serveurs des deuxarborescences sont synchronisés à l'aide de la même source horaire.
- ❑ (Facultatif) Tous les serveurs de l'arborescence sont opérationnels (les serveurs hors service sont automatiquement mis à jour lorsqu'ils sont opérationnels.)
- ❑ Reportez-vous aux conditions préalables à la fusion énumérées à la section « Préparation des arborescences source et cible », page 224

Le processus de fusion en lui-même ne prend que quelques minutes, mais d'autres variables rallongent la durée d'exécution de cette opération :

- L'objet Arborescence contient de nombreux objets subordonnés qui doivent être divisés en partitions.
- L'arborescence source contient de nombreux serveurs qui requièrent la modification du nom de l'arborescence.

Pour fusionner deuxarborescences :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Fusionner l'arborescence.
3. Indiquez le serveur qui exécutera la fusion (il s'agit de l'arborescence source), puis cliquez sur Suivant.

4. Authentifiez-vous auprès du serveur, puis cliquez sur Suivant.
5. Spécifiez un nom d'utilisateur d'administrateur et un mot de passe pour l'arborescence source.
6. Spécifiez le nom de l'arborescence cible, le nom d'utilisateur de l'administrateur ainsi que son mot de passe, puis cliquez sur Démarrer.

   Une fenêtre d'état de l'Assistant de fusion d'arborescence s'ouvre et affiche la progression de la fusion.
7. Lorsque le message « Terminé » contenant les informations renvoyées par l'opération de fusion s'affiche, cliquez sur Fermer pour quitter le processus.

Tâches postérieures à la fusion

Après avoir fusionné deux arborescences, il peut s'avérer nécessaire d'exécuter également les tâches suivantes :

1. Vérifiez que tous les noms d'arborescence ont été correctement modifiés.
2. Vérifiez les nouvelles partitions créées au cours de la fusion.

   Si la nouvelle arborescence comporte un grand nombre de partitions peu volumineuses ou des partitions qui contiennent des informations connexes, il peut être intéressant de les fusionner. Pour plus d'informations, reportez-vous à la section « Fusion d'une partition », page 135.
3. Copiez une nouvelle réplique sur tous les serveurs non dotés de NetWare 5 si vous n'avez pas effectué la mise à niveau avant d'exécuter DSMerge.
4. Recréez dans l'arborescence tout objet Feuille ou tout alias supprimé avant l'exécution de DSMerge.
5. Évaluez le partitionnement de l'arborescence eDirectory.

   La fusion des arborescences peut changer les conditions de placement des répliques dans la nouvelle arborescence. Évaluez soigneusement le partitionnement et modifiez-le si nécessaire.
6. Mettez à jour la configuration des postes de travail client.

   Pour le client Novell pour DOS/Windows, vérifiez les instructions Preferred Tree et Preferred Server dans les fichiers net.cfg. Pour le client Novell pour Windows NT/2000 et Windows 95/98, vérifiez les instructions Preferred Tree et Preferred Server dans la page de propriétés du client, ou renommez l'arborescence cible.

   Si l'instruction Preferred Server est utilisée, le client n'est pas affecté par une fusion ou un changement de nom des arborescences car il continue à se servir du nom pour se loguer au serveur. Si l'instruction Preferred Tree est utilisée et que l'arborescence est fusionnée ou renommée, le nom de l'arborescence disparaît. Seul le nom de l'arborescence cible est conservé après la fusion. Remplacez le nom de l'arborescence préférée par celui de la nouvelle arborescence.

La liste ACL (Access Control ListListe de contrôle d'accès) pour l'objet Arborescence de l'arborescence source est conservée. Par conséquent, les droits de l'utilisateur Admin de l'arborescence source sur l'objet Arborescence restent valides.

Une fois la fusion terminée, les deux utilisateurs Admin existent toujours et sont identifiés de manière unique par des objets Conteneur différents.

Pour des raisons de sécurité, vous pouvez supprimer l'un des deux objets Utilisateur Admin ou restreindre leurs droits.

Greffe d'une arborescence à serveur unique

L'option Greffer l'arborescence permet de greffer l'objet Arborescence d'une arborescence source à serveur unique sous un conteneur spécifié dans l'arborescence cible. Une fois la greffe terminée, l'arborescence source prend le nom de l'arborescence cible.

Lors de la greffe, DSMerge modifie la classe de l'objet Arborescence de l'arborescence source par Domaine et crée une nouvelle partition. Le nouvel objet Domaine correspond à la racine de partition de la nouvelle partition. Tous les objets situés sous l'objet Arborescence de l'arborescence source se retrouvent désormais sous l'objet Domaine.

L'administrateur de l'arborescence cible possède des droits sur le conteneur racine de l'arborescence obtenue et, par conséquent, sur la racine greffée de l'arborescence source.

REMARQUE : il peut se passer plusieurs heures avant que les droits hérités ne soient recalculés et effectifs. Cette durée dépend de la complexité, de la taille et du nombre de partitions de l'arborescence.

L'administrateur de l'arborescence source possède uniquement des droits sur le nouvel objet Domaine.

La Figure 35 et la Figure 36, page 229 illustrent les effets de la greffe d'une arborescence sur un conteneur spécifique.

Figure 35 Arborescences eDirectory avant une greffe

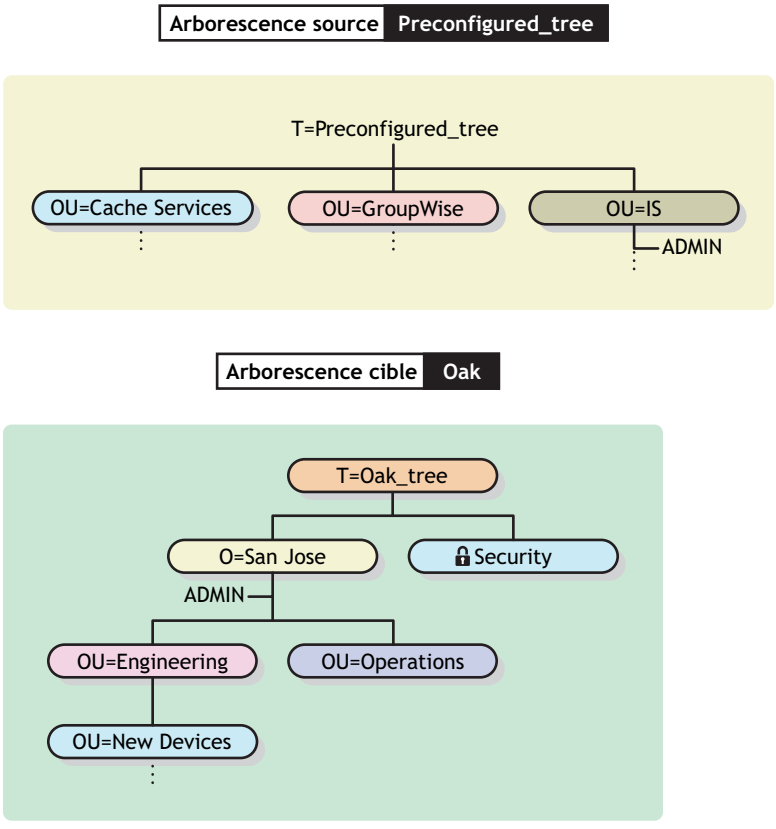
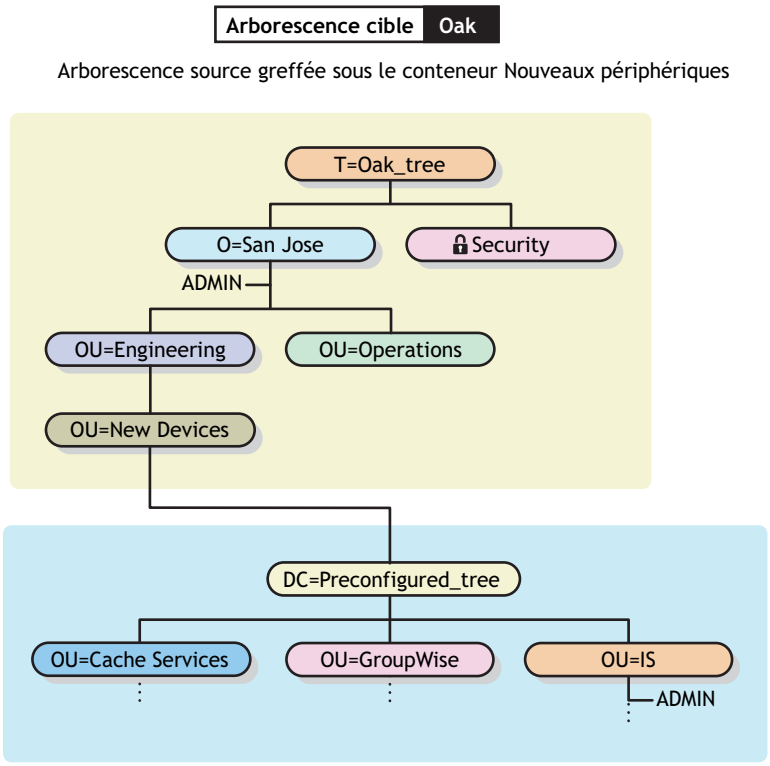


Figure 36 Arborescence eDirectory greffée



Cette section comprend les informations suivantes :

- « Changement des noms de contexte - Présentation », page 229
- « Préparation des arborescences source et cible », page 230
- « Exigences relatives à l'endiguement pour la greffe », page 231
- « Greffe des arborescences source et cible », page 232

Changement des noms de contexte - Présentation

Après la greffe de l'arborescence source sur le conteneur de l'arborescence cible, le nom de l'arborescence source, et le nom distinctif du nom du conteneur de l'arborescence cible dans laquelle l'arborescence source a été fusionnée, sont ajoutés dans cet ordre aux noms distinctifs des objets de l'arborescence source. Le nom distinctif relatif n'est pas modifié.

Par exemple, si vous utilisez des points comme séparateurs, le nom avec type pour Admin dans l'arborescence source Arbo_préconfigurée est

```
CN=Admin.OU=IS.T=Arbo_préconfigurée
```

Une fois l'arborescence Arbo_préconfigurée fusionnée dans le conteneur Nouveaux périphériques de l'arborescence Arbo_chêne, le nom avec type de l'Admin est

```
CN=Admin.OU=IS.DC=Arbo_préconfigurée.OU=Nouveauxpériphériques.
OU=Ingénierie.O=Bordeaux.T=Arbo_chêne.
```

REMARQUE : le nom distinctif peut contenir256 caractères au maximum. Cette limitation est particulièrement importante lorsque vous greffez la racine d'une arborescence sur un conteneur proche du bas de l'arborescence cible.

Le dernier point qui suit Arbo_chêne (Arbo_chêne.) indique que le dernier élément du nom distinctif est le nom de l'arborescence. Si vous ne mettez pas le point final, ne mettez pas non plus le nom de l'arborescence.

Préparation des arborescences source et cible

Avant de procéder à l'opération de greffe, vérifiez que l'état de l'ensemble des serveurs concernés par cette opération est stable. Le tableau suivant indique les conditions préalables pour préparer les arborescences source et cible à la greffe.

Condition préalable	Action requise
WANMAN doit être désactivé sur tous les serveurs qui contiennent une réplique de la partition Arborescence de l'arborescence source ou cible.	Contrôlez la règle WANMAN ; les restrictions de communication WAN ne doivent pas gêner la fusion. Au besoin, désactivez WANMAN avant de lancer la fusion.
L'arborescence source ne doit comporter qu'un serveur.	Ne conservez qu'un serveur dans l'arborescence source.
Aucun alias ou objet Feuille ne peut exister sur l'objet Arborescence de l'arborescence source.	Supprimez tout alias ou objet Feuille de l'objet Arborescence de l'arborescence source.
Le conteneur de greffage ne peut pas contenir plusieurs noms identiques.	Renommez les objets dans le conteneur de greffe de l'arborescence cible ou renommez l'arborescence source. Si vous ne souhaitez pas assigner de nouveaux noms, déplacez les objets d'un conteneur vers un conteneur différent de l'arborescence, puis supprimez le conteneur vide avant de lancer DSMerge. Pour plus d'informations, reportez-vous à la section Chapitre 3, « Gestion des objets », page 93. Des objets Conteneur identiques peuvent être présents dans les deuxarborescences s'ils ne sont pas immédiatement subordonnés au même objet parent. Les objets sont identifiés de manière unique par l'objet Conteneur immédiatement supérieur.
Le conteneur des arborescences source et cible doit exécuter eDirectory 8.5.1 SP2a ou version ultérieure.	DSMerge recherche la version appropriée de eDirectory. Si aucune version compatible ne peut être trouvée, DSMerge renverra une erreur. Pour obtenir la dernière version de eDirectory, consultez la page Web Novell Download page (page de téléchargement Novell) (http://download.novell.com).
Le conteneur pour la jonction de l'arborescence cible se trouve dans une partition qui ne comporte aucune réplique (partition à serveur unique).	Si le conteneur cible contient plusieurs répliques, effectuez *l'une* des opérations suivantes : ◆ Faites de la partition associée au conteneur la réplique maîtresse, puis supprimez les autres répliques. ◆ Divisez le conteneur de greffe de l'arborescence cible pour en faire une partition distincte, puis supprimez les répliques. Après la greffe, l'association de la partition peut être rétablie.
Le serveur possédant le conteneur cible doit également comporter une réplique de la partition racine.	Si le serveur ne comporte aucune réplique de cette partition, la greffe échoue et un message d'erreur -672 Pas d'accès s'affiche, car l'annuaire ne peut vérifier les droits Administrateur sur l'arborescence cible. Ajoutez une réplique de la partition racine à l'aide de iManager. Pour plus d'informations, reportez-vous à la section « Ajout d'une réplique », page 137.

Condition préalable	Action requise
Le schéma des arborescences source et cible doit être identique.	Exécutez l'option Greffer l'arborescence dans DSMerge. Si les rapports font état de problèmes relatifs au schéma, exécutez DSRepair sur l'arborescence cible afin d'importer le schéma à partir de l'arborescence source. L'opération de greffe importe automatiquement le schéma depuis l'arborescence source vers l'arborescence cible. Exécutez de nouveau DSMerge.
Seule une des deuxarborescences peut posséder un conteneur de sécurité subordonné à la racine de larborescence.	Si les arborescences source et cible possèdent un conteneur de sécurité, supprimez-en un en suivant les indications de l'.
La référence horaire de l'arborescence source doit être reconfigurée.	L'arborescence source doit généralement être définie comme serveur secondaire configuré pour obtenir sa source horaire d'un serveur de l'arborescence cible. Pour reconfigurer la synchronisation horaire (Timesync), reportez-vous à la section Configuring Timesync on Servers (Configuration de Timesync sur des serveurs) (http://www.novell.com/documentation/lg/nw65/time_enu/data/abzqzx2.html) dans le manuel *Network Time Management Administration Guide (Guide d'administration de la gestion de l'heure réseau)*.

Exigences relatives à l'endiguement pour la greffe

Pour greffer une arborescence source sur un conteneur de l'arborescence cible, celui-ci doit être préparé à accepter l'arborescence source. Le conteneur de l'arborescence cible doit pouvoir contenir un objet de la classe Domaine. En cas de problème d'endiguement, le message d'erreur `-611 Endiguement interdit` s'affiche pendant l'opération de greffe.

Utilisez les informations du tableau suivant afin de déterminer si vous devez exécuter DSRepair pour modifier les listes d'endiguement.

Exigences relatives au conteneur de l'arborescence cible	L'objet Domaine doit figurer dans la liste d'endiguement de l'objet Conteneur de l'arborescence cible. Vous pouvez le vérifier à l'aide de iMonitor > Schéma. Si l'objet Domaine ne figure pas dans la liste d'endiguement, exécutez DSRepair pour améliorer le schéma.
Exigences relatives à l'arborescence source	Avec la greffe, la classe de la racine de l'arborescence source passe de Racine de l'arborescence à Domaine. Toutes les classes d'objets qui sont subordonnées à l'arborescence doivent pouvoir appartenir à la classe Domaine conformément aux règles du schéma. Vous pouvez le vérifier à l'aide de iMonitor > Schéma. Si l'objet Domaine ne figure pas dans la liste d'endiguement, exécutez DSRepair pour améliorer le schéma.

Si les exigences liées à l'endiguement ne sont pas respectées, exécutez DSRepair pour corriger le schéma.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Maintenance du schéma.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Améliorations de schéma facultatives, puis sur Démarrer.
6. Suivez les instructions en ligne pour terminer l'opération.

Greffe des arborescences source et cible

Après avoir vérifié que les conditions préalables sont remplies, exécutez la greffe à l'aide de DSMerge.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Greffer l'arborescence.
3. Indiquez le serveur qui exécutera la greffe (il s'agit de l'arborescence source), puis cliquez sur Suivant.
4. Authentifiez-vous auprès du serveur, puis cliquez sur Suivant.
5. Spécifiez le nom et le mot de passe de l'administrateur de l'arborescence source. Indiquez le nom de l'arborescence cible, le nom et le mot de passe de son administrateur.
6. Cliquez sur Démarrer.

   Une fenêtre d'état de l'Assistant de greffe d'arborescence s'ouvre et affiche la progression de la greffe. Enfin, le message « Terminé » contenant les informations renvoyées par le processus de greffe s'affiche.
7. Cliquez sur Fermer pour quitter.

Changement du nom d'une arborescence

Si les deux arborescences à fusionner portent le même nom, vous devez en renommer une.

Vous ne pouvez renommer que l'arborescence source. Pour renommer l'arborescence cible, exécutez l'Assistant Renommer l'arborescence dans Novell iManager sur un serveur de l'arborescence cible.

Si vous renommez une arborescence, le contexte de Bindery ne change pas automatiquement. Étant donné que le contexte de Bindery défini dans le fichier autoexec.ncf contient également le nom de l'arborescence (par exemple, SET Bindery Context = O=n.*nom_arborescence_test*), un serveur contenant un nom d'arborescence récemment modifié ne se sert pas du contexte qu'il utilisait avant le changement de nom.

Par conséquent, la modification du nom d'une arborescence peut nécessiter que vous modifiiez la configuration des postes de travail client. Pour le client Novell pour DOS/Windows, vérifiez les instructions Preferred Tree et Preferred Server dans les fichiers net.cfg. Concernant le client Novell pour Windows NT/2000 et Windows 95/98, vérifiez les instructions Preferred Tree et Preferred Server dans la page des propriétés du client.

Si l'instruction Preferred Server est utilisée, le client n'est pas affecté par une fusion ou un changement de nom des arborescences car il continue à se servir du nom pour se loguer au serveur. Si l'instruction Preferred Tree est utilisée et que l'arborescence est fusionnée ou renommée, le nom de l'arborescence disparaît. Seul le nom de l'arborescence cible est conservé après la fusion. Remplacez le nom de l'arborescence préférée par celui de la nouvelle arborescence.

Lorsque vous fusionnez deux arborescences, pour réduire au maximum le nombre de postes de travail client à mettre à jour, désignez comme arborescence cible celle qui contient le plus grand nombre de postes de travail client, car l'arborescence finale conserve le nom de l'arborescence cible.

Vous pouvez également renommer l'arborescence après la fusion pour que le nom de l'arborescence finale corresponde à celui de l'arborescence qui comporte la majorité des postes de travail client.

Il est également possible de remplacer le nom de l'arborescence fusionnée par le nom de l'arborescence source d'origine. Si vous choisissez cette option, vous devez mettre à jour les fichiers net.cfg sur les postes de travail client de l'arborescence cible.

La liste suivante de conditions préalables vous permet de savoir si vous êtes prêt pour l'attribution d'un nouveau nom :

- Accès à une console de serveur dans l'arborescence source ou à une session RCONSOLE définie avec le serveur
- Droit d'objet Superviseur sur l'objet Arborescence de l'arborescence source
- (Facultatif) Tous les serveurs de l'arborescence sont opérationnels (les serveurs hors service sont automatiquement mis à jour lorsqu'ils sont opérationnels.)

Pour renommer l'arborescence :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Renommer l'arborescence.
3. Indiquez quel serveur doit exécuter l'Assistant Renommer l'arborescence (ce doit être un serveur de l'arborescence cible), puis cliquez sur Suivant.
4. Authentifiez-vous auprès du serveur, puis cliquez sur Suivant.
5. Indiquez un nouveau nom d'arborescence ainsi que le nom d'utilisateur et le mot de passe de l'administrateur.
6. Cliquez sur Démarrer.

   Une fenêtre d'état de l'Assistant Renommer l'arborescence s'ouvre et affiche la progression du processus de changement de nom.
7. Lorsque le message « Terminé » contenant les informations renvoyées par le processus de changement de nom s'affiche, cliquez sur Fermer pour quitter le processus.

Utilisation du client eMBox pour fusionner des arborescences

Le client eDirectory Management Toolbox (eMBox) est un client Java à ligne de commande qui permet d'accéder à distance à DSMerge. Le fichier emboxclient.jar est installé sur votre serveur comme élément de eDirectory. Vous pouvez l'exécuter sur toute machine dotée d'une JVM. Pour plus d'informations sur le client eMBox, reportez-vous à la section « Utilisation du client à ligne de commande eMBox », page 553.

Utilisation de l'outil eMTool DSMerge

1. Exécutez le client eMBox en mode interactif en entrant les éléments suivants dans la ligne de commande :

   java -cp *chemin_fichier*/emboxclient.jar embox -i

   (Si vous avez déjà placé le fichier emboxclient.jar dans votre chemin d'accès à la classe, il vous suffit d'entrer **java embox -i**.)

   L'invite du client eMBox apparaît :

   ```
   Client eMBox>
   ```

2. Pour vous loguer au serveur qui doit exécuter DSMerge (il s'agit de l'arborescence source), entrez la commande suivante :

   login -s*nom_ou_adresse_IP_serveur* -p*numéro_port*
   -u*nom_utilisateur.contexte* -w*mot_de_passe* -n

   Le numéro de port est généralement 80 ou 8028, à moins qu'il ne soit déjà utilisé par un serveur Web. L'option -n ouvre une connexion non sécurisée.

   Le client eMBox indique si le login a réussi.

3. Entrez une commande de fusion à l'aide de la syntaxe suivante :

   dsmerge.*options_ tâche*

   Par exemple :

   dsmerge.m -uadmin -ptest -TApple -Uadmin -Ptest fusionne l'arborescence cible Apple (en testant le nom d'utilisateur Admin et le mot de passe de l'utilisateur de l'arborescence cible) avec l'arborescence source à laquelle vous êtes actuellement logué (en testant le nom d'utilisateur Admin et le mot de passe de l'utilisateur de l'arborescence source).

   dsmerge.g -uadmin -ptest -TOrange -Uadmin -Ptest -CFruit greffe l'arborescence source à laquelle vous êtes actuellement logué (en testant le nom d'utilisateur Admin et le mot de passe de l'utilisateur de l'arborescence source) sur le conteneur Fruit de l'arborescence cible Orange (en testant le nom d'utilisateur Admin et le mot de passe de l'utilisateur de l'arborescence cible).

   Les paramètres doivent être séparés les uns des autres par un espace. L'ordre des paramètres n'a pas d'importance.

   Le client eMBox indique la réussite ou l'échec de la fusion.

   Pour plus d'informations sur les options de l'outil eMTool DSMerge, reportez-vous à la section « Options de l'outil eMTool DSMerge », page 235.

4. Déloguez-vous du client eMBox en entrant la commande suivante :

   logout

5. Quittez le client eMBox en entrant la commande suivante :

   exit

Options de l'outil eMTool DSMerge

Les tableaux suivants répertorient les options de l'outil eMTool DSMerge. Vous pouvez également utiliser la commande list -tdsmerge du client eMBox pour afficher une liste détaillée des options DSMerge. Pour plus d'informations, reportez-vous à la section « Liste des outils eMTools et de leurs services », page 557.

Opération de fusion	Commande du client eMBox
Vérifier si l'arborescence peut être renommée	dsmerge.pr -u*Utilisateur* -p*Mot_de_passe_utilisateur* –n*Nouveau_nom_arborescence*
Renommer l'arborescence	dsmerge.r -u*Utilisateur* -p*Mot_de_passe_utilisateur* –n*Nouveau_nom_arborescence*
Vérifier si deuxarborescences peuvent être fusionnées	dsmerge.pm -u*Utilisateur_arborescence_source*-p*Mot_de_passe_utilisateur_arborescence_source* –T*Nom_arborescence_cible* -U*Utilisateur_arborescence_cible* –P*Mot_de_passe_arborescence_cible*
Fusionner deuxarborescences	dsmerge.m -u*Utilisateur_arborescence_source*-p*Mot_de_passe_utilisateur_arborescence_source* –T*Nom_arborescence_cible*-U*Utilisateur_arborescence_cible* –P*Mot_de_passe_arborescence_cible*
Vérifier si l'arborescence source peut être greffée sur le conteneur de l'arborescence cible	dsmerge.pg -u*Utilisateur_arborescence_source* -p*Mot_de_passe_utilisateur_arborescence_source* –T*Nom_arborescence_cible* -U*Utilisateur_arborescence_cible* –P*Mot_de_passe_arborescence_cible* -C*Conteneur_arborescence_cible*
Greffer l'arborescence source sur le conteneur de l'arborescence cible	dsmerge.g -u*Utilisateur_arborescence_source* -p*Mot_de_passe_utilisateur_arborescence_source* –T*Nom_arborescence_cible* -U*Utilisateur_arborescence_cible* –P*Mot_de_passe_arborescence_cible* -C*Conteneur_arborescence_cible*
Annuler l'opération dsmerge en cours	cancel

9 Codage des données dans eDirectory

Novell® eDirectory™ 8.8 (ou version ultérieure) permet de coder certaines données lorsqu'elles sont stockées sur le disque et lorsqu'elles sont transmises entre plusieurs serveurs eDirectory 8.8, ce qui accroît la sécurité des données confidentielles.

Pour plus d'informations sur le cryptage de données et les scénarios dans lesquels vous pouvez effectuer cette opération, consultez le manuel *Novell eDirectory 8.8 What's New Guide* (http://www.novell.com/documentation/beta/edir88/index.html) (Guide des nouveautés de Novell eDirectory 8.8).

Pour protéger les données, vous pouvez coder les éléments suivants :

- les attributs : pour protéger les données confidentielles stockées sur le disque.

  Pour plus de détails, reportez-vous à la section « Attributs codés », page 237.

- la réplication : pour protéger les données confidentielles pendant la réplication entre des serveurs eDirectory 8.8.

  « Réplication codée », page 245.

Attributs codés

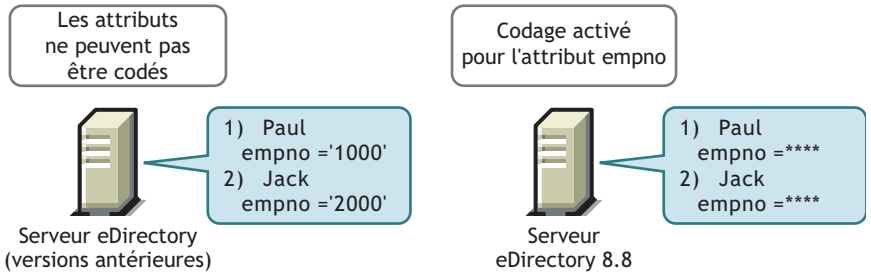
eDirectory 8.8 (ou version ultérieure) permet de coder les attributs pour protéger les données lorsqu'elles sont stockées sur le disque. Le codage d'attributs est une fonctionnalité propre au serveur.

Si vous codez un attribut, sa valeur est cryptée. Par exemple, vous pouvez coder un attribut Numéro_employé stocké dans la DIB. Si Numéro_employé=1000, la valeur de l'attribut (1000) n'est pas stockée comme du texte clair sur le disque. Vous ne pouvez lire cette valeur codée que lorsque vous accédez à l'annuaire par le biais d'un canal sécurisé.

Tous les attributs d'un schéma peuvent être activés pour le codage. Nous vous recommandons toutefois de ne pas activer l'attribut CN (nom commun) pour le codage et de n'activer pour le codage, que les données sensibles. Reportez-vous à la section « Règles de sécurité lors du codage de données », page 256 avant de décider de marquer des attributs pour le codage.

Il n'existe pas de limite d'accès aux attributs codés lisibles Public et Serveur. Autrement dit, un client peut accéder à ces attributs en texte clair, mais vous pouvez les marquer pour le codage au niveau de la DIB.

Figure 37 Attributs codés



Les données dans eDirectory peuvent être stockées selon l'une des méthodes suivantes :

- dans la DIB (Data Information Base) ou base de données ;
- sous la forme de données de sauvegarde ;
- sous la forme d'un fichier LDIF.

Pour coder des attributs, vous pouvez créer et appliquer des règles d'attributs codés aux serveurs.

Pour coder les attributs, effectuez les opérations suivantes dans iManager :

1. Créez et définissez une règle d'attributs codés.

   1a. Sélectionnez les attributs à coder.

   1b. Sélectionnez le modèle de codage pour les attributs.

   Pour plus d'informations, reportez-vous à la section « Création et définition des règles des attributs codés », page 240.

2. Appliquez la règle des attributs codés à un serveur.

   Pour plus d'informations, reportez-vous à la section « Application des règles des attributs codés », page 240.

Vous pouvez également coder des attributs par le biais de LDAP. Pour plus d'informations, reportez-vous à la section « Gestion des règles des attributs codés via LDAP », page 241.

Nous vous recommandons d'effectuer les opérations suivantes :

- Ne marquez pour le codage que les attributs sensibles et non l'ensemble des attributs (dont les attributs lisibles Public ou Serveur).
- Lors du marquage d'un attribut pour le codage, utilisez AES puisqu'il s'agit d'un algorithme de codage fort.

La suite de cette section fournit les informations ci-après :

- « Utilisation de modèles de codage », page 239
- « Accès aux attributs codés », page 243
- « Affichage des attributs codés », page 243
- « Gestion des règles des attributs codés », page 239
- « Migration vers des attributs codés », page 245

Utilisation de modèles de codage

eDirectory 8.8 offre les meilleurs niveaux de sécurité pour un attribut grâce à la prise en charge des modèles de codage suivants :

- norme de codage avancée (AES)
- norme de codage de données triple (3DES)
- norme de codage des données (DES)

Vous pouvez sélectionner des modèles de codage distincts pour différents attributs d'une même règle d'attributs codés. Par exemple, dans une règle d'attributs codés RC1, vous pouvez sélectionner AES comme modèle de codage pour un attribut Numéro_unité et 3DES pour un attribut Numéro_employé. Pour plus d'informations, reportez-vous à la section « Création et définition des règles des attributs codés », page 240.

Vous pouvez changer le modèle de codage d'un attribut codé en éditant la règle des attributs codés. Vous pouvez également supprimer le codage d'un attribut codé précédemment. Pour plus d'informations, reportez-vous à la section « Édition des règles des attributs codés », page 240.

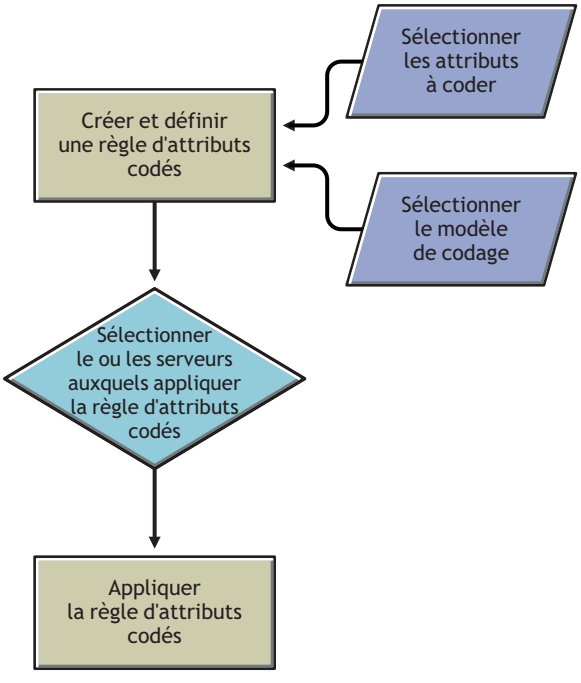
Vous pouvez décider d'affecter des modèles de codage distincts à différents serveurs de l'anneau de répliques. Par exemple, un attribut peut être activé pour le codage AES sur le serveur1, pour le codage 3DES sur le serveur 2 et pour aucun modèle de codage sur le serveur 3.

Gestion des règles des attributs codés

Pour gérer le codage des attributs, vous pouvez créer et définir des règles et les appliquer à des serveurs.

Vous définissez une règle d'attributs codés en sélectionnant les attributs à coder ainsi qu'un modèle de codage.

Figure 38 Codage d'attributs



Vous pouvez gérer les règles des attributs codés à l'aide de iManager. Cette section fournit les informations suivantes :

- « Gestion des règles des attributs codés via iManager », page 240
- « Gestion des règles des attributs codés via LDAP », page 241
- « Copie des règles des attributs codés », page 242
- « Opérations de partition », page 242

Gestion des règles des attributs codés via iManager

Cette section comprend les procédures suivantes :

- « Création et définition des règles des attributs codés », page 240
- « Édition des règles des attributs codés », page 240
- « Application des règles des attributs codés », page 240
- « Suppression des règles des attributs codés », page 241

Si le serveur eDirectory contient des attributs codés, iManager présente le comportement suivant :

1. La lecture, l'affichage ou la modification des attributs codés ne sont pas autorisés par le biais de canaux en texte clair ou sécurisés.
2. Une entrée qui possède des attributs non codés n'est pas autorisée à lire, afficher ou modifier des attributs via iManager par le biais de canaux en texte clair ou sécurisés, ce qui implique le blocage de l'entrée complète.

Création et définition des règles des attributs codés

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Codage eDirectory > Attributs.
3. Dans l'Assistant Gestion des règles d'attributs codés, sélectionnez Créer, éditer et appliquer la règle.
4. Suivez les instructions de l'Assistant Gestion des règles d'attributs codés pour créer et définir la règle.

   Vous pouvez obtenir de l'aide via l'Assistant.

Édition des règles des attributs codés

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Codage eDirectory > Attributs.
3. Dans l'Assistant Gestion des règles d'attributs codés, sélectionnez Éditer la règle.
4. Suivez les instructions de l'Assistant Gestion des règles d'attributs codés pour éditer la règle.

   Vous pouvez obtenir de l'aide via l'Assistant.

Application des règles des attributs codés

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Codage eDirectory > Attributs.

3 Dans l'Assistant Gestion des règles d'attributs codés, sélectionnez Appliquer la règle.

4 Suivez les instructions de l'Assistant Gestion des règles d'attributs codés pour appliquer la règle.

Vous pouvez obtenir de l'aide via l'Assistant.

Suppression des règles des attributs codés

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Codage eDirectory > Attributs.

3 Dans l'Assistant Gestion des règles d'attributs codés, sélectionnez Supprimer les règles.

4 Suivez les instructions de l'Assistant Gestion des règles d'attributs codés pour supprimer la règle.

Vous pouvez obtenir de l'aide via l'Assistant.

Gestion des règles des attributs codés via LDAP

IMPORTANT : il est vivement recommandé d'utiliser iManager plutôt que LDAP pour gérer les attributs codés.

Cette section comprend les procédures suivantes :

- « Création et définition des règles des attributs codés », page 241
- « Édition des règles des attributs codés », page 242
- « Application d'une règle d'attributs codés », page 242
- « Suppression d'une règle d'attributs codés », page 242

REMARQUE : lorsque vous marquez un attribut quelconque pour le cryptage via LDIF, vous devez spécifier la paire attribut/modèle, et non la liste des attributs et le modèle. Il s'agit là de l'actuelle contrainte pour les attributs codés.

Création et définition des règles des attributs codés

1 Créez une règle de codage des attributs.

Par exemple, si la règle des attributs codés est AE Policy- test-server, alors

```
dn: cn=AE Policy - test-server, o=novell
changetype: add
objectClass: encryptionPolicy
```

2 Ajoutez l'attribut attrEncryptionDefinition à l'objet Règle créé et marquez les attributs pour le codage.

Par exemple, si le nom de l'attribut à coder est CRID, spécifiez le modèle de codage et le nom de l'attribut comme indiqué ci-dessous :

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
add: attrEncryptionDefinition
attrEncryptionDefinition: aes$CRID
```

REMARQUE : le nom de l'attribut implique ici son nom NDS. Dans eDirectory, de nombreux attributs ont à la fois un nom LDAP et un nom NDS. Dans ce cas, vous devez spécifier le nom NDS de l'attribut.

3 Ajoutez l'attribut attrEncryptionRequiresSecure à la règle.

La valeur de cet attribut indique si un canal sécurisé est toujours requis pour accéder aux attributs codés. La valeur0 signifie que ce type de canal n'est pas toujours nécessaire. La valeur1 signifie qu'il est toujours indispensable.

Par exemple :

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
add: attrEncryptionRequiresSecure
attrEncryptionRequiresSecure: 0
```

4 Associez la règle à un serveur NCP.

Par exemple, si le serveur NCP est test-server :

```
dn: cn=test-server, o=novell
changetype: modify
add: encryptionPolicyDN
encryptionPolicyDN: cn=AE Policy - test-server, o=novell
```

Édition des règles des attributs codés

Le fichier LDIF suivant illustre l'édition d'une règle d'attributs codés par le changement de la valeur de l'attribut attrEncryptionRequireSecure :

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
replace: attrEncryptionRequiresSecure
attrEncrytionRequiresSecure: 1
```

Application d'une règle d'attributs codés

Le fichier LDIF suivant illustre l'application d'une règle d'attributs codés AEPolicy-test-server à un serveur test-server :

```
dn: cn=test-server, o=novell
changetype: modify
add: encryptionPolicyDN
encryptionPolicyDN: cn=AE Policy - test-server, o=novell
```

Suppression d'une règle d'attributs codés

Le fichier LDIF suivant illustre la suppression d'une règle d'attributs codés :

```
dn: cn=AE Policy - test-server, o=novell
changetype: delete
```

Copie des règles des attributs codés

eDirectory 8.8 (ou version ultérieure) permet de copier les règles des attributs codés pour disposer de configurations identiques sur plusieurs serveurs. Les règles sont stockées sous la forme d'objets dans eDirectory.

Pour une explication détaillée de la procédure de copie d'un objet Règle à l'aide de iManager, reportez-vous à la section « Copie d'objets », page 96.

Opérations de partition

Lorsque vous fusionnez deux partitions, les règles du parent sont conservées pour la partition résultante. Lorsque vous divisez une partition, la partition enfant hérite la règle de la partition parent.

Accès aux attributs codés

Si vous codez les attributs, vous protégez également leur accès, car eDirectory 8.8 (ou version ultérieure) peut limiter l'accès aux attributs codés par le biais d'un canal sécurisé (LDAP ou HTTP).

Par défaut, l'accès aux attributs codés est uniquement possible par canal sécurisé.

Toutefois, si vous souhaitez permettre aux clients d'accéder aux attributs codés en texte clair, désactivez l'option Toujours exiger un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair », page 243.

Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair

Vous pouvez activer ou désactiver l'accès aux attributs codés par le biais de canaux en texte clair en activant ou désactivant l'option Toujours exiger un canal sécurisé (autrement dit, l'attribut attrEncryptionRequireSecure) à l'aide de iManager ou LDAP.

Cette section comprend les informations suivantes :

- « Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair à l'aide de iManager », page 243
- « Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair à l'aide de LDAP », page 243

Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair à l'aide de iManager

Pour activer ou désactiver, à l'aide de iManager, l'accès aux attributs codés par le biais de canaux en texte clair, vous devez activer/désactiver l'option Toujours exiger un canal sécurisé dans l'Assistant Gestion des règles d'attributs codés lors de :

- la création et de la définition de règles d'attributs codés ;
- l'édition de règles d'attributs codés.

Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair à l'aide de LDAP

Pour activer ou désactiver, à l'aide de LDAP, l'accès aux attributs codés par le biais de canaux en texte clair, vous devez ajouter l'attribut suivant à la règle des attributs codés :

`attrEncryptionRequiresSecure`

Si vous définissez cet attribut sur 0, un canal sécurisé n'est pas toujours requis ; autrement dit, vous pouvez accéder aux attributs codés au moyen d'un canal en texte clair. Si vous le définissez sur 1, un canal sécurisé est toujours indispensable ; autrement dit, vous ne pouvez accéder aux attributs codés qu'à l'aide d'un canal sécurisé.

Pour plus d'informations, reportez-vous à la section Etape 3, page 241.

Affichage des attributs codés

L'affichage des attributs codés dépend de l'activation ou de la désactivation de l'option Toujours exiger un canal sécurisé, autrement dit de l'éventuelle nécessité d'un canal sécurisé pour y accéder.

- « Affichage des attributs codés avec iManager », page 244
- « Affichage des attributs codés avec DSBrowse », page 244
- « Trappes SNMP », page 244

Affichage des attributs codés avec iManager

Si l'option Toujours exiger un canal sécurisé est activée, vous ne pouvez pas afficher les attributs codés. Vous obtenez l'erreur -6089, ce qui signifie que vous avez besoin d'un canal sécurisé pour y accéder.

Dans le cas contraire, vous pouvez afficher les valeurs des attributs codés dans iManager.

Pour plus d'informations, reportez-vous à la section « Accès aux objets de votre arborescence », page 209.

Affichage des attributs codés avec DSBrowse

Si vous avez activé l'option Toujours exiger un canal sécurisé, autrement dit, si un canal sécurisé est indispensable pour accéder aux attributs codés, vous ne pouvez pas afficher les attributs de l'entrée qui sont marqués pour le codage. Vous pouvez toutefois voir ceux qui ne sont pas codés.

Trappes SNMP

Les événements Valeur NDS® sont bloqués si vous avez demandé de toujours exiger un canal sécurisé pour accéder aux attributs codés. Les trappes liées à des événements Valeur ont la donnée de valeur NULL et le résultat sera défini sur -6089, ce qui signifie que vous avez besoin d'un canal sécurisé pour obtenir la valeur d'attribut codé. Les trappes ayant la donnée de valeur NULL sont les suivantes :

- ndsAddValue
- ndsDeleteValue
- ndsDeleteAttribute

Codage et décodage des données de sauvegarde

Lors de la sauvegarde de données sur un serveur qui comporte des attributs marqués pour le codage, vous êtes invité à fournir un mot de passe pour le codage/décodage des données de sauvegarde. Ce mot de passe est défini par l'option -E dans l'utilitaire ndsbackup. Pour plus d'informations, reportez-vous aux pages du manuel ndsbackup.

Pour plus d'informations sur la sauvegarde de vos données, reportez-vous au.

Clonage de l'ensemble de fichiers DIB contenant des attributs codés

Lors du clonage, si la base de données eDirectory contient des attributs codés, les valeurs de ces attributs seront également codées dans l'ensemble de fichiers DIB cloné. Afin de sécuriser la clé utilisée par eDirectory pour le codage des valeurs dans cet ensemble, vous devez définir un mot de passe que vous devrez spécifier lorsque vous placerez l'ensemble cloné sur un autre serveur.

Pour plus d'informations, reportez-vous à la section « Cloner l'ensembleDIB », page 215.

Ajout de serveurs eDirectory 8.8 à des anneaux de répliques

Vous pouvez ajouter des serveurs eDirectory 8.8 à des anneaux de répliques indépendamment du fait que les attributs soient ou non marqués pour le codage sur l'un des serveurs hébergeant la réplique ou tous, et indépendamment de l'activation/la désactivation de l'option Toujours exiger un canal sécurisé.

Pour plus d'informations sur l'ajout du serveur eDirectory 8.8 à l'anneau de répliques, reportez-vous à la section « Ajout d'une réplique », page 137.

Compatibilité avec les versions précédentes

Pour accéder aux attributs codés, vous devez changer tous les utilitaires eDirectory, tels que iManager, SNMP, DirXML® et NSureAudit pour les rendre conformes à NCP™ sécurisé. Dans le cas contraire, vous devez indiquer qu'un canal sécurisé n'est pas toujours requis pour y accéder. Pour plus d'informations, reportez-vous à la section « Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair », page 243.

Migration vers des attributs codés

Lors d'une mise à niveau vers eDirectory 8.8 ou une version ultérieure, vous pouvez coder les attributs existants en créant et en définissant des règles d'attributs codés. Pour plus d'informations, reportez-vous à la section « Gestion des règles des attributs codés », page 239.

Réplication des attributs codés

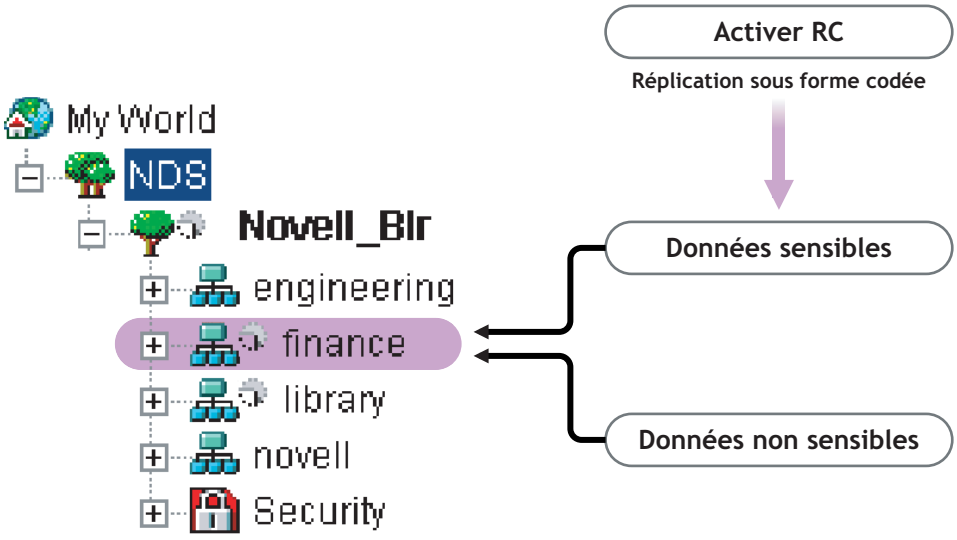
Par défaut, la réplication codée n'est pas activée même si le serveur comporte des attributs codés. Vous devez l'activer pour répliquer les attributs codés en toute sécurité. Pour la configuration de la réplication codée, reportez-vous à la section « Réplication codée », page 245.

Réplication codée

Novell eDirectory 8.8 (ou version ultérieure) permet de coder les données transmises entre des serveurs eDirectory 8.8, afin de garantir un niveau élevé de sécurité pendant la réplication puisque les données ne circulent pas en texte clair.

Pour plus d'informations sur l'utilité de la réplication codée et des exemples de scénarios de codage de données lors de la réplication, consultez le manuel *Novell eDirectory 8.8 What's New Guide* (http://www.novell.com/documentation/beta/edir88/edir88new/data/bqljql1.html#bqljql1) (Guide des nouveautés de Novell eDirectory 8.8).

Figure 39 Réplication codée



Dans l'illustration ci-dessus, « finances » et « bibliothèque » sont les partitions de l'arborescence. Il se peut que « finances » contienne des données sensibles à coder lors de la réplication. Vous pouvez dès lors activer la partition « finances » pour la réplication codée. Il n'est, par contre, pas nécessaire d'activer pour la réplication codée des partitions telles que « bibliothèque », qui ne risquent pas de contenir des données sensibles.

IMPORTANT : activer la réplication codée pour une partition peut ralentir le processus de réplication.

Vous pouvez activer ou désactiver la réplication codée à l'aide de iManager.

REMARQUE : la réplication codée n'est pas prise en charge sous Netware®.

Cette section fournit les informations suivantes :

- « Activation de la réplication codée », page 246
- « Ajout d'une nouvelle réplique à un anneau de répliques », page 250
- « Synchronisation et réplication codée », page 255
- « Affichage de l'état de la réplication codée », page 256

Activation de la réplication codée

Pour activer la réplication codée, vous devez lui configurer une partition. Les paramètres de configuration sont stockés dans l'objet Racine de la partition.

Vous pouvez choisir d'activer la réplication codée au niveau de la partition ou de la réplique.

Les configurations au niveau de la réplique priment sur celles au niveau de la partition. Cela signifie que si la réplication codée est :

- activée au niveau de la partition et désactivée pour des répliques spécifiques, la réplication entre les répliques spécifiques s'effectue en texte clair ;
- désactivée au niveau de la partition et activée pour des répliques spécifiques, la réplication entre les répliques spécifiques s'effectue sous forme codée ;

Tableau 2 **Remplacement de la configuration de la réplication codée au niveau de la partition**

Niveau de la partition	Niveau de la réplique	Réplication
Activée	Désactivée	Non codée
Désactivée	Activée	Codée

Cette section comprend les procédures suivantes :

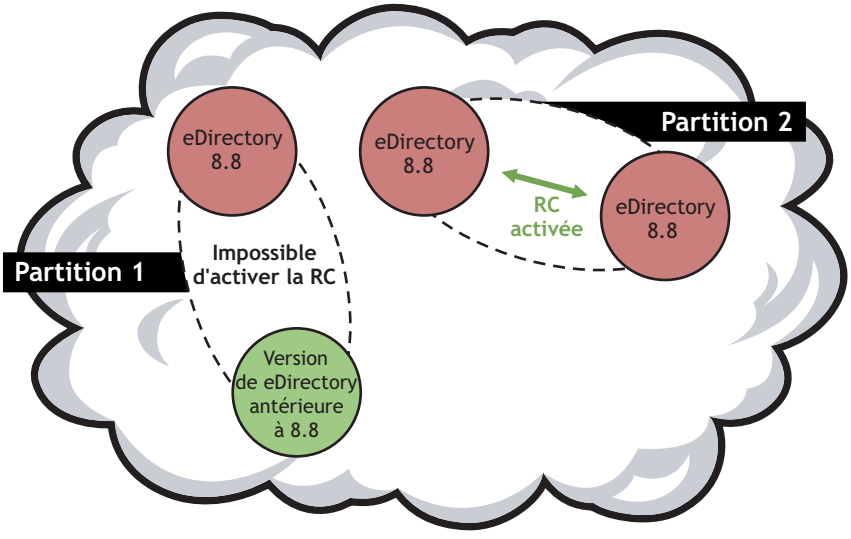
- « Activation de la réplication codée au niveau de la partition », page 247
- « Activation de la réplication codée au niveau de la réplique », page 249

Activation de la réplication codée au niveau de la partition

Lorsque vous activez la réplication codée au niveau d'une partition, la réplication entre toutes les répliques hébergeant la partition est codée. Imaginons, par exemple, que la partition P1 comporte les répliques R1, R2, R3 et R4. Vous pouvez coder la réplication entre toutes les répliques ; toutes les réplications, entrantes et sortantes, seront codées pour ces répliques.

Pour activer une partition pour la réplication codée, tous les serveurs hébergeant cette partition doivent exécuter eDirectory 8.8 ou une version ultérieure. Les autres partitions de l'arborescence qui ne sont pas activées pour la réplication codée peuvent avoir des serveurs antérieurs à eDirectory 8.8.

Figure 40 **Réplication codée au niveau de la partition**



Les configurations pour la réplication codée au niveau de la partition sont ignorées si vous disposez de configurations de ce type au niveau de la réplique. Reportez-vous à la Tableau 2, « Remplacement de la configuration de la réplication codée au niveau de la partition », page 247.

La compatibilité avec les versions précédentes dépend de l'activation/la désactivation de la réplication codée au niveau de la partition. Pour plus d'informations, reportez-vous à la section « Ajout d'une nouvelle réplique à un anneau de répliques », page 250.

Vous pouvez activer la réplication codée au niveau de la partition à l'aide de iManager ou de LDAP, comme expliqué aux sections suivantes :

- « Activation de la réplication codée au niveau de la partition avec iManager », page 248
- « Activation de la réplication codée au niveau de la partition avec LDAP », page 248
- « Opérations de partition », page 250

Activation de la réplication codée au niveau de la partition avec iManager

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Codage eDirectory > Réplication.
3. Dans l'Assistant de réplication codée, sélectionnez Coder toutes les synchronisations de répliques.

   Vous pouvez obtenir de l'aide via l'Assistant.

   REMARQUE : pour désactiver la réplication codée au niveau de la partition, désélectionnez Coder toutes les synchronisations de répliques.

Dans l'Assistant de réplication codée, si vous activez la réplication codée pour toute la partition, vous pouvez la désactiver pour des répliques spécifiques. Ces répliques ne recevront et n'enverront pas de données sous forme codée. Vous pouvez également désactiver le codage pour toute la partition en désélectionnant Coder toutes les synchronisations de répliques.

Activation de la réplication codée au niveau de la partition avec LDAP

IMPORTANT : il est vivement recommandé d'utiliser iManager pour activer la réplication codée.

Pour coder la réplication, vous devez utiliser l'attribut dsEncryptedReplicationConfig. La syntaxe est la suivante :

```
drapeau d'activation/de désactivation#numéro de réplique cible#numéro de
réplique source
```

Remplacez par l'un de ces drapeaux :

- 0 : désactive la réplication codée
- 1 : active la réplication codée

Les numéros de réplique source et cible représentent les numéros de réplique source et cible d'une partition. Ces numéros peuvent être spécifiés dans n'importe quel ordre, car si la réplication de A vers B est codée, celle de B vers A l'est également.

REMARQUE : si les numéros de réplique source et cible au niveau de la partition sont 0 et si le drapeau est 1, toutes les répliques sont considérées comme activées pour la réplication codée.

Pour activer la réplication codée au niveau de la partition, la valeur de l'attribut dsEncryptedReplicationConfig doit être 1#0#0.

Voici un exemple de fichier LDIF pour l'activation de la réplication codée au niveau de la partition:

```
dn: o=ou
changetype: modify
replace: dsEncryptedReplicationConfig
dsEncryptedReplicationConfig:1#0#0
```

Ces configurations au niveau de la réplique priment sur celles au niveau de la partition. Pour plus d'informations, reportez-vous à la section « Activation de la réplication codée au niveau de la réplique avec LDAP », page 250.

Activation de la réplication codée au niveau de la réplique

Lorsque vous activez la réplication codée au niveau de la réplique, la réplication, tant entrante que sortante, entre des répliques spécifiques est codée.

Imaginons, par exemple, que la partition P1 comporte les répliques R1, R2, R3 et R4. Vous pouvez coder la réplication entre les répliques R1 et R2 ou entre R2 et R4.

Pour activer la réplication codée entre des répliques d'une partition, vous devez définir entre elles un lien de codage. Pour plus d'informations, reportez-vous à la section « Activation de la réplication codée au niveau de la réplique avec iManager », page 249.

Si vous avez activé la réplication codée pour une réplique, cela signifie que :

- la synchronisation entrante d'un serveur vers cette réplique et
- la synchronisation sortante de cette réplique vers un autre serveur sont codées.

Les répliques activées pour la réplication codée doivent être situées sur des serveurs eDirectory 8.8. Les autres répliques de l'anneau, qui ne sont pas activées pour cette réplication, peuvent se trouver sur des serveurs exécutant des versions antérieures de eDirectory.

Si vous avez activé uniquement des répliques spécifiques pour la réplication codée, vous pouvez ajouter à l'anneau de répliques un serveur doté de eDirectory 8.8 ou d'une version antérieure.

Pour désactiver la réplication codée au niveau de la réplique, vous devez désactiver Coder le lien pour les répliques spécifiques à l'aide de l'Assistant de configuration de la réplication codée dans iManager.

Vous pouvez activer la réplication codée au niveau de la réplique à l'aide de iManager ou de LDAP, comme expliqué aux sections suivantes :

- « Activation de la réplication codée au niveau de la réplique avec iManager », page 249
- « Activation de la réplication codée au niveau de la réplique avec LDAP », page 250

Activation de la réplication codée au niveau de la réplique avec iManager

Vous pouvez activer la réplication codée au niveau de la réplique par le biais de iManager en créant des liens de codage. Ces derniers relient les répliques entre lesquelles la réplication doit être codée. Vous les créez lors de la configuration d'une réplique pour la réplication codée, en sélectionnant une réplique source et une ou plusieurs répliques cibles.

Imaginons, par exemple, que la partition P1 comporte les répliques R1, R2, R3 et R4. Pour coder la réplication entre les répliques R1 et R2, vous devez créer un lien de codage en identifiant l'une d'elles comme la source et l'autre comme la cible.

Une fois les liens de codage créés, vous pouvez choisir de coder ou pas ces liens pour des répliques spécifiques en (dé)sélectionnant Coder le lien dans l'Assistant de configuration de la réplication codée dans iManager. Pour plus d'informations, reportez-vous à la section « Activation de la réplication codée au niveau de la réplique avec iManager », page 249.

Pour activer la réplication codée au niveau de la réplique :

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Codage eDirectory > Réplication.

3 Dans l'Assistant de réplication codée, dans le tableau Synchronisations codées, sélectionnez Nouveau pour définir un lien de codage.

3a Sélectionnez une réplique source.

3b Sélectionnez une ou plusieurs répliques cibles.

3c Sélectionnez Coder le lien.

3d Cliquez sur OK.

4 Cliquez sur Terminer.

Activation de la réplication codée au niveau de la réplique avec LDAP

IMPORTANT : il est vivement recommandé d'utiliser iManager pour activer la réplication codée.

Pour coder la réplication, vous devez utiliser l'attribut dsEncryptedReplicationConfig. La syntaxe est la suivante :

```
drapeau d'activation/de désactivation#numéro de réplique cible#numéro de
réplique source
```

Pour plus d'informations sur la syntaxe, reportez-vous à la section « Activation de la réplication codée au niveau de la partition avec LDAP », page 248.

Lorsque vous spécifiez les numéros des répliques dans la syntaxe ci-dessus, vous activez la réplication codée entre celles-ci. Exemples de syntaxe :

- 1#0#1: la réplication codée est activée depuis et vers la réplique 1, ainsi que vers et depuis toutes les autres répliques de la partition.
- 0#3#1: la réplication codée est désactivée entre les répliques 1 et 3.
- 0#1#1: la réplication codée est désactivée pour la réplique 1.

Voici un exemple de fichier LDIF qui désactive la réplication codée entre les répliques 1 et 3 :

```
dn: o=ou
changetype: modify
replace: dsEncryptedReplicationConfig
dsEncryptedReplicationConfig: 0#3#1
```

Opérations de partition

Lorsque vous divisez une partition, la configuration de la réplication codée pour la partition parent est héritée par la partition enfant. Lorsque vous fusionnez une partition, cette configuration est conservée pour la partition résultante.

Ajout d'une nouvelle réplique à un anneau de répliques

L'ajout d'une nouvelle réplique à un anneau dépend de l'activation/la désactivation de la réplication codée pour la partition au niveau de cette dernière et de la réplique.

Pour plus d'informations sur l'ajout d'une réplique à un anneau de répliques, reportez-vous à la section « Gestion des répliques », page 137.

À chacun de ces niveaux, vous disposez de scénarios différents selon la version du serveur eDirectory à ajouter à l'anneau de répliques, comme expliqué aux sections suivantes :

- « Activation de la réplication codée au niveau de la partition », page 251
- « Activation de la réplication codée au niveau de la réplique », page 255

Activation de la réplication codée au niveau de la partition

Les scénarios varient en fonction de la version du serveur eDirectory à ajouter. Cette section comprend les informations suivantes :

- « Ajout à l'anneau de répliques de serveurs dotés d'une version de eDirectory antérieure à 8.8 », page 251
- « Ajout de serveurs eDirectory 8.8 à l'anneau de répliques », page 253

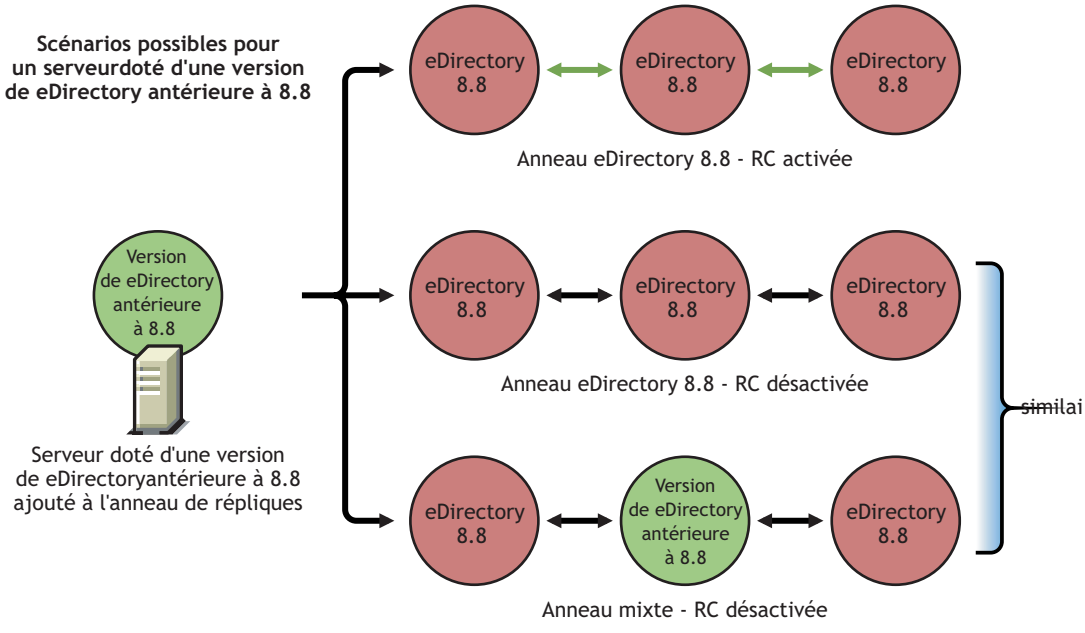
Ajout à l'anneau de répliques de serveurs dotés d'une version de eDirectory antérieure à 8.8

L'illustration suivante décrit les scénarios possibles lorsque vous ajoutez, à l'anneau de répliques, un serveur doté d'une version de eDirectory antérieure à 8.8 :

- Scénario A
- Scénario B
- Scénario C

REMARQUE : l'abréviationRC dans l'illustration ci-dessous désigne la réplication codée.

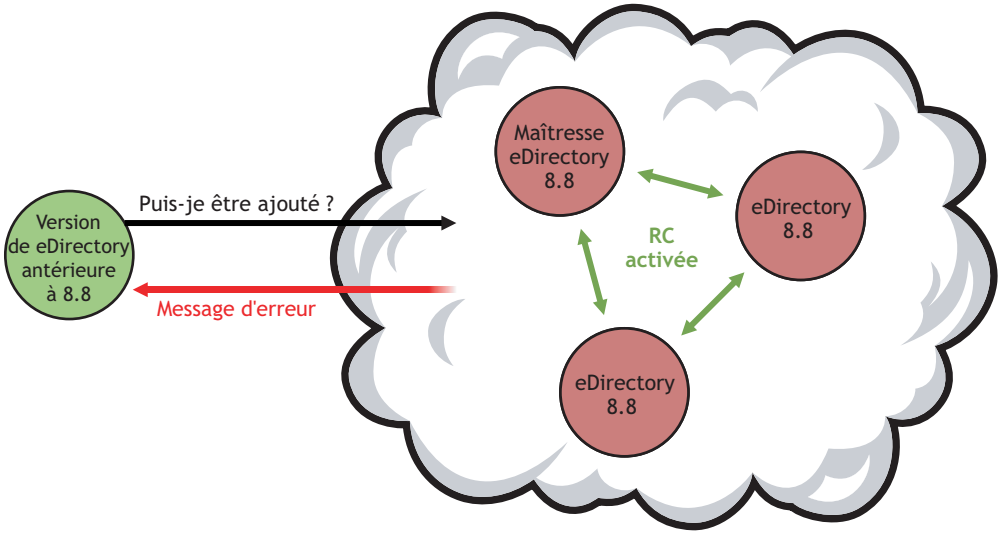
Figure 41 Scénarios possibles pour un serveur doté d'une version de eDirectory antérieure à 8.8



Scénario A : ajout d'un serveur doté d'une version de eDirectory antérieure à 8.8 à un anneau de répliques eDirectory 8.8 avec la réplication codée activée

Si vous essayez d'ajouter un serveur doté d'une version de eDirectory antérieure à 8.8 à un anneau de répliques eDirectory 8.8 pour lequel vous avez activé la réplication codée, l'erreur ERR_INCOMPATIBLE_DS est renvoyée. Vous pourrez ajouter le serveur à l'anneau, mais vous ne pourrez pas obtenir de réplique de la partition sur le serveur.

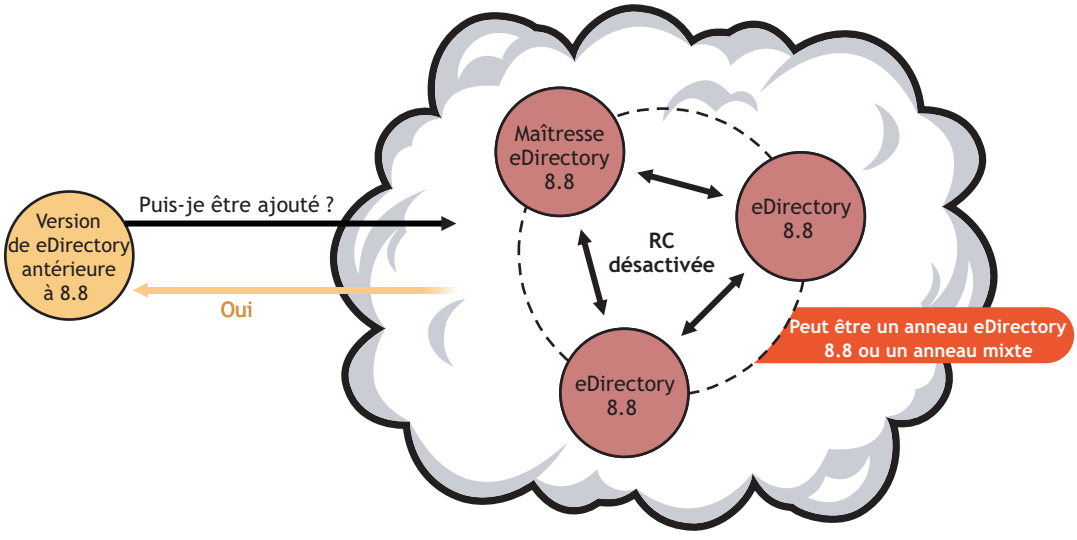
Figure 42 **Ajout d'un serveur doté d'une version de eDirectory antérieure à 8.8 à un anneau de répliques eDirectory 8.8 avec la réplication codée activée**



Scénario B : ajout d'un serveur doté d'une version de eDirectory antérieure à 8.8 à un anneau de répliques eDirectory 8.8 avec la réplication codée désactivée

Vous pouvez ajouter un serveur doté d'une version eDirectory antérieure à 8.8 à un anneau de répliques eDirectory 8.8 avec la réplication codée désactivée.

Figure 43 **Ajout d'un serveur doté d'une version de eDirectory antérieure à 8.8 à un anneau de répliques avec la réplication codée désactivée**



Scénario C : ajout d'un serveur doté d'une version de eDirectory antérieure à 8.8 à un anneau de répliques mixte avec la réplication codée désactivée

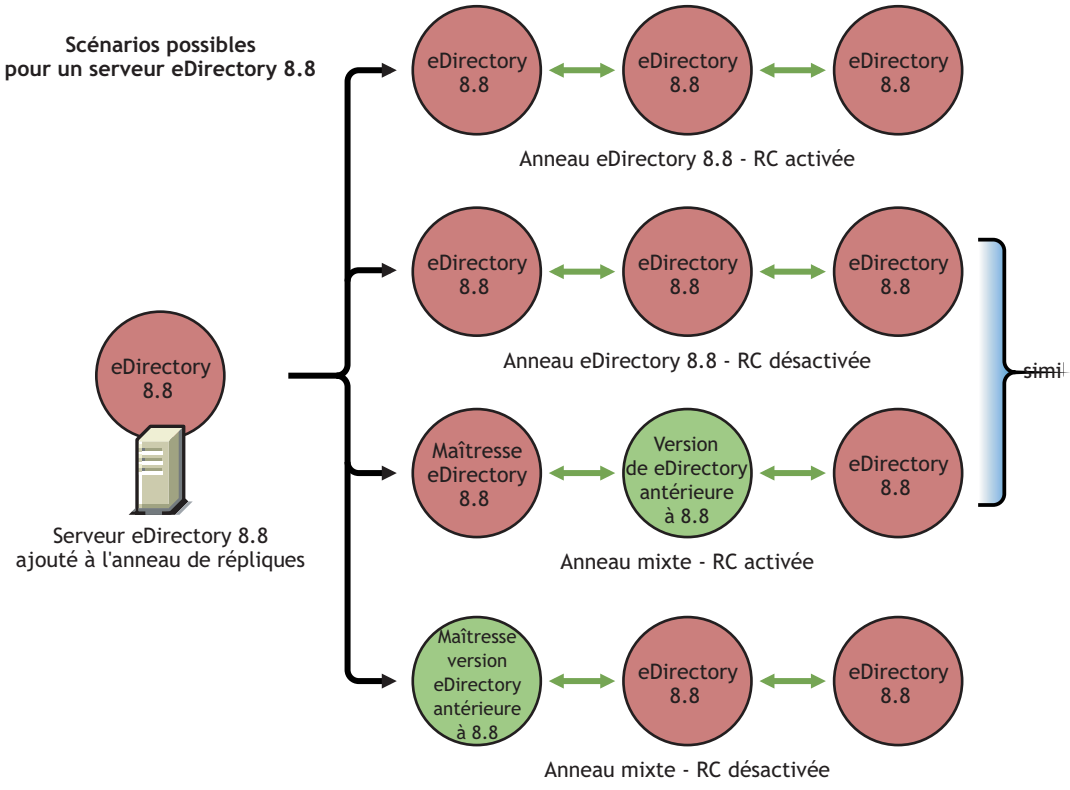
Vous pouvez ajouter un serveur doté d'une version eDirectory antérieure à 8.8 à un anneau de répliques comportant différentes versions de eDirectory avec la réplication codée désactivée. Reportez-vous à la figure 43 ci-dessus.

Ajout de serveurs eDirectory 8.8 à l'anneau de répliques

L'illustration suivante décrit les scénarios possibles lorsque vous ajoutez un serveur eDirectory 8.8 à l'anneau de répliques :

- ScénarioA
- ScénarioB
- ScénarioC
- ScénarioD

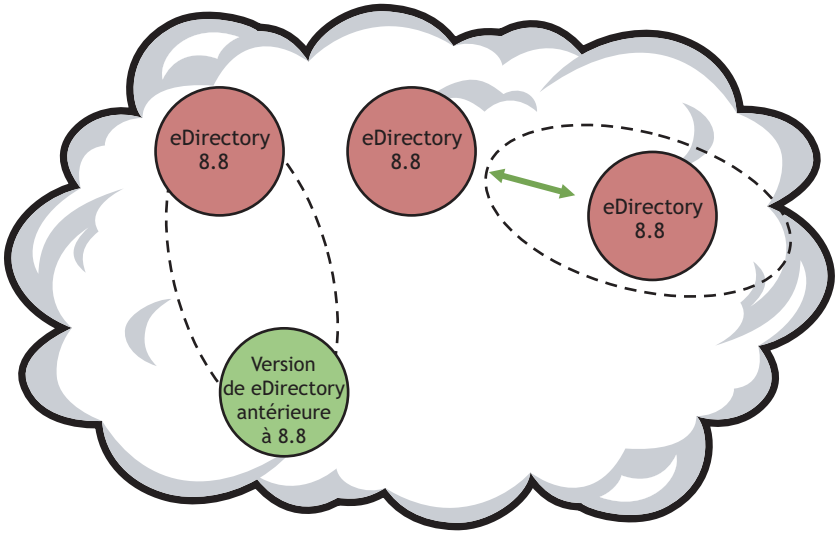
Figure 44 Scénarios possibles pour un serveur eDirectory 8.8



Scénario A : ajout de serveurs eDirectory 8.8 à un anneau de répliques eDirectory 8.8 avec la réplication codée activée

Dans ce cas, la réplication codée serait déjà activée sur le serveur eDirectory 8.8 ajouté.

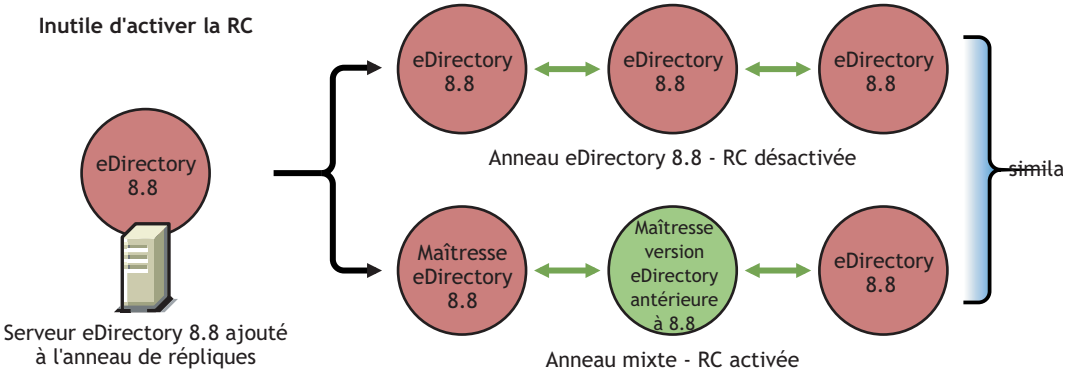
Figure 45 **Ajout d'un serveur eDirectory 8.8 à un anneau de répliques eDirectory avec la réplication codée activée**



Scénario B : ajout de serveurs eDirectory 8.8 à un anneau de répliques eDirectory 8.8 avec la réplication codée désactivée

Dans ce cas, la réplication codée sera désactivée sur le serveur eDirectory 8.8 ajouté.

Figure 46 **Ajout d'un serveur eDirectory 8.8 à des anneaux de répliques pour lesquels la réplication codée est désactivée**



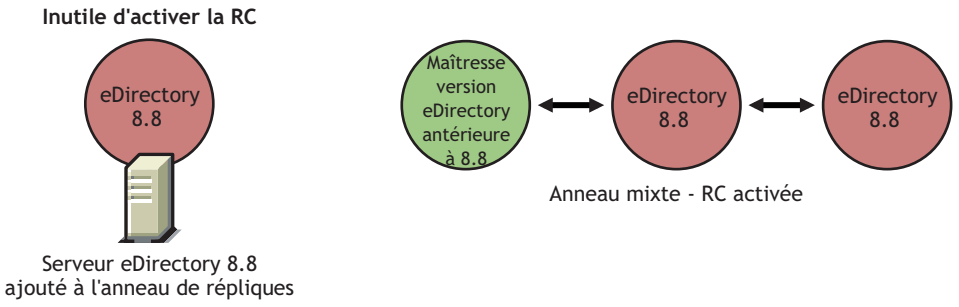
Scénario C : ajout de serveurs eDirectory 8.8 à un anneau de répliques mixte dans lequel la réplique maîtresse est un serveur eDirectory 8.8 et la réplication codée est désactivée

Dans ce cas, il n'est pas nécessaire d'activer la réplication codée sur le serveur eDirectory 8.8 à ajouter. Reportez-vous à la Figure 46, « Ajout d'un serveur eDirectory 8.8 à des anneaux de répliques pour lesquels la réplication codée est désactivée », page 254.

Scénario D : ajout de serveurs eDirectory 8.8 à un anneau de répliques mixte dans lequel la réplique maîtresse est un serveur doté d'une version de eDirectory antérieure à 8.8 et la réplication codée est désactivée

Dans ce cas, il n'est pas nécessaire d'activer la réplication codée sur le serveur eDirectory 8.8 à ajouter.

Figure 47 Ajout d'un serveur eDirectory 8.8 à un anneau de répliques dans lequel la réplique maîtresse est un serveur doté d'une version de eDirectory antérieure à 8.8



Activation de la réplication codée au niveau de la réplique

Si la réplication codée est activée entre une réplique source et des répliques cibles spécifiques, vous pouvez ajouter à l'anneau de répliques un serveur doté de eDirectory 8.8 ou d'une version antérieure.

Les scénarios varient si la réplication codée est activée entre une réplique source et toutes les autres répliques de l'anneau. C'est alors une situation similaire à l'ajout de répliques à un anneau pour lequel la réplication codée est activée ou désactivée au niveau de la partition. Pour plus d'informations, reportez-vous à la section « Activation de la réplication codée au niveau de la partition », page 251.

Activation de la réplication codée pour le serveur à ajouter

Si le serveur à ajouter fonctionne sous Linux ou UNIX, vous pouvez utiliser l'option-E de ndsconfig pour activer la réplication codée sur ce serveur. Pour plus d'informations, reportez-vous aux pages du manuel ndsconfig.

Si le serveur à ajouter fonctionne sous Windows, vous pouvez sélectionner l'option Activer la réplication codée dans l'Assistant d'installation.

Si le serveur à ajouter est sur des plates-formes autres que Linux et UNIX, vous pouvez activer la réplication codée à l'aide de iManager ou de LDAP. Pour plus d'informations, reportez-vous à la section « Activation de la réplication codée », page 246.

Synchronisation et réplication codée

Si une réplique est activée pour la réplication codée et que les changements de configuration ne sont pas synchronisés avec les autres serveurs, la réplication entre les répliques s'effectue sous forme codée. Celles qui ne sont pas synchronisées avec les changements de configuration pour la réplication codée continuent la synchronisation en texte clair.

Même si la configuration de la réplication codée n'a pas été synchronisée entre les répliques, la réplication entre ces dernières aura lieu sous forme codée.

Affichage de l'état de la réplication codée

Vous pouvez afficher l'état de la réplication codée via iMonitor de la manière suivante :

1. Dans iMonitor, cliquez sur Synchronisation de l'agent dans le cadre de l'Assistant.
2. Cliquez sur Synchronisation des répliques pour la partition à afficher.

   Les informations relatives à l'état des répliques s'affichent. Le champ État de codage indique si le lien de la réplique à laquelle vous êtes actuellement connecté est codé ou non.

   En fait, la réplication codée (RC) comporte trois scénarios :

   - **RC activée au niveau de la partition :** la réplique à laquelle vous êtes connecté indique que l'état de codage est Activé.

     Pour déterminer la réplique à laquelle vous êtes connecté, vous devez rechercher dans le cadre de la réplique celle qui n'a pas de lien hypertexte. Si vous parcourez les autres répliques, vous constatez que l'état de codage est également marqué comme Activé.
   - **RC activée au niveau de la réplique :** vous avez activé la RC pour toutes les répliques à partir d'une réplique spécifique (autrement dit, une vers toutes). Dans ce cas, lorsque vous êtes connecté à cette réplique, son état de codage est marqué comme Activé.
   - **RC activée/désactivée pour une combinaison de répliques :** RC activée/désactivée pour une combinaison de répliques – vous avez activé la RC pour l'ensemble de la partition, mais pas pour un groupe sélectionné de serveurs, ou inversement.

     Par exemple, vous avez activé la RC pour la partitionA qui compte trois répliques (1, 2 et 3) et l'avez désactivée pour 1 <–> 3. Dans ce cas, si vous êtes connecté à la réplique1, l'état de codage apparaît comme suit :

     Serveur 1 Activé

     Serveur 2

     Serveur 3 Désactivé

     Ce qui signifie que le serveur1 est activé pour la réplication codée vers tous les serveurs de l'anneau de répliques, mais que 1<–>3 est désactivé par l'administrateur.

Règles de sécurité lors du codage de données

La première règle de base à respecter avant de coder les données est la suivante :

Les informations qui seront codées ne doivent jamais apparaître en texte clair sur le disque dur (ou tout autre support).

Lorsque vous marquez pour le codage des données en texte clair existantes, elles seront certes codées mais il se peut que les données en texte clair restent présentes sur une partie du disque dur hébergeant la DIB.

Des données resteront en texte clair dans certains blocs de la base de données si vous tentez d'effectuer les opérations suivantes :

- Marquage de données en texte clair existantes pour le codage
- Modification du modèle de codage d'un attribut codé

Les sections suivantes présentent des scénarios de déploiement pour des données codées ainsi que des procédures permettant de garantir la sécurité de ce type de données :

Codage de données dans une toute nouvelle configuration

Dans le cas d'une nouvelle configuration, vous venez d'installer le système d'exploitation puis eDirectory. Vous êtes certain que le disque dur hébergeant la DIB ne contient pas de données en texte clair.

Respectez la procédure suivante pour garantir la sécurité des données codées dans eDirectory :

1. Déterminez à l'avance les attributs que vous souhaitez coder et le modèle à utiliser.

   En d'autres termes, vous devez décider à l'avance quels attributs vous allez coder avant de charger les données en texte clair dans eDirectory.

   AVERTISSEMENT : une fois que des données en texte clair sont chargées dans eDirectory, vous ne devriez plus marquer d'attribut pour le codage. Vous pouvez certes le faire, mais au risque d'entraîner des problèmes de sécurité.

2. Configurez eDirectory et définissez les modèles de codage désirés pour les attributs.

3. Chargez les données existantes sur le nouveau serveur.

   Les deux scénarios les plus probables sont le chargement par lots à partir d'un fichier LDIF ou la réplication avec un autre serveur. Si vous choisissez le chargement par lots, veillez à ne pas copier le fichier LDIF en texte clair sur le disque dur hébergeant la DIB. (N'oubliez pas la règle susmentionnée : aucune donnée en texte clair ne peut être écrite sur le disque.)

4. Détruisez toutes les données en texte clair existantes

   Tous les disques (ou autres supports) contenant les données en texte clair doivent être effacés de manière sûre. Il s'agit notamment du fichier LDIF en texte clair utilisé pour le chargement par lots sur le serveur, de tout autre serveur utilisé pour la réplication ou encore des bandes contenant d'anciennes sauvegardes.

Codage de données dans une configuration existante

Ce scénario inclut les opérations suivantes :

Conversion de données en texte clair existantes en données codées

Vous pouvez marquer pour le codage des données en texte clair et vous assurer de la sécurité des données en utilisant les méthodes suivantes :

La réplication :

1. Configurez le codage sur un nouveau serveur en respectant la procédure suivante :

   1a. Déterminez à l'avance les attributs que vous souhaitez coder et le modèle à utiliser.

   En d'autres termes, vous devez décider à l'avance quels attributs vous allez coder avant de charger les données en texte clair dans eDirectory.

   AVERTISSEMENT : une fois que des données en texte clair sont chargées dans eDirectory, vous ne devriez plus marquer d'attribut pour le codage. Vous pouvez certes le faire, mais au risque d'entraîner des problèmes de sécurité.

   1b. Commencez par une installation nette (incluant probablement le système d'exploitation) sur un disque récemment formaté et partitionné.

   Vous êtes ainsi certain qu'il ne contient pas de données en texte clair. En d'autres termes, vous ne pouvez pas vous contenter de réinstaller eDirectory sur un ordinateur ayant contenu des données en texte clair. Vous devez avoir effacé soigneusement toute trace de données sur le disque. Utilisez un logiciel d'effacement sécurisé, un démagnétiseur sur le disque ou tout autre programme de suppression de données avant d'installer eDirectory.

   1c. Configurez eDirectory et définissez les modèles de codage désirés pour les attributs.

2. Déplacez ce serveur dans un anneau de répliques contenant les données existantes à coder, effectuez la réplication, puis mettez l'ancien serveur hors ligne.

3. Détruisez toutes les données en texte clair existantes

   Tous les disques (ou autres supports) contenant les données en texte clair doivent être effacés de manière sûre. Il s'agit notamment du fichier LDIF en texte clair utilisé pour le chargement par lots sur le serveur, de tout autre serveur utilisé pour la réplication ou encore des bandes contenant d'anciennes sauvegardes.

La sauvegarde et la restauration :

1. Configurez le codage sur un nouveau serveur en respectant la procédure suivante :

   1a. Déterminez à l'avance les attributs que vous souhaitez coder et le modèle à utiliser.

   En d'autres termes, vous devez décider à l'avance quels attributs vous allez coder avant de charger les données en texte clair dans eDirectory.

   AVERTISSEMENT : une fois que des données en texte clair sont chargées dans eDirectory, vous ne devriez plus marquer d'attribut pour le codage. Vous pouvez certes le faire, mais au risque d'entraîner les problèmes de sécurité mentionnés à la remarque A.

   1b. Commencez par une installation nette (incluant probablement le système d'exploitation) sur un disque récemment formaté et partitionné.

   Vous êtes ainsi certain qu'il ne contient pas de données en texte clair. En d'autres termes, vous ne pouvez pas vous contenter de réinstaller eDirectory sur un ordinateur ayant contenu des données en texte clair. Vous devez avoir effacé soigneusement toute trace de données sur le disque. Utilisez un logiciel d'effacement sécurisé, un démagnétiseur sur le disque ou tout autre programme de suppression de données avant d'installer eDirectory.

   1c. Configurez eDirectory et définissez les modèles de codage désirés pour les attributs.

2. Restaurez la DIB sauvegardée (qui contient les données en texte clair existantes) sur le nouveau serveur. Vous pouvez sauvegarder la DIB en utilisant la fonction de clonage de la DIB ou de sauvegarde à chaud.

3 Détruisez toutes les données en texte clair existantes

   Tous les disques (ou autres supports) contenant les données en texte clair doivent être effacés de manière sûre. Il s'agit notamment du fichier LDIF en texte clair utilisé pour le chargement par lots sur le serveur, de tout autre serveur utilisé pour la réplication ou encore des bandes contenant d'anciennes sauvegardes.

Modification du modèle des données codées

Pour réaliser cette modification à l'aide de la sauvegarde et de la restauration, les opérations suivantes sont nécessaires :

1 Modifiez les algorithmes de codage d'un attribut.

2 Effectuez une sauvegarde de la DIB. Vous pouvez sauvegarder la DIB en utilisant la fonction de clonage de la DIB ou de sauvegarde à chaud.

3 Restaurez la DIB sauvegardée sur un nouveau serveur et supprimez l'ancien.

4 Détruisez toutes les données en texte clair existantes sur l'ancien serveur pour éviter que des données basées sur l'ancien modèle restent sur le disque dur.

   Tous les disques (ou autres supports) contenant les données en texte clair doivent être effacés de manière sûre. Il s'agit notamment du fichier LDIF en texte clair utilisé pour le chargement par lots sur le serveur, de tout autre serveur utilisé pour la réplication ou encore des bandes contenant d'anciennes sauvegardes.

Conclusion

Les scénarios mentionnés ici ne sont pas exhaustifs et le problème peut se poser dans d'autres scénarios. Tant que vous respectez la règle, *Les informations qui seront codées ne doivent jamais apparaître en texte clair sur le disque dur (ou tout autre support)*, les données codées seront parfaitement sécurisées.

10 Réparation de la base de données Novell eDirectory

L'utilitaire de réparation permet de mettre à jour et de réparer la base de données d'une arborescence Novell® eDirectory™. À l'aide de cet utilitaire, vous pouvez :

- corriger les problèmes de eDirectory tels que les enregistrements erronés, les discordances de schémas, les adresses de serveur incorrectes et les références externes ;
- apporter des changements complexes au schémaeDirectory ;
- vérifier automatiquement la structure de la base de données, sans fermer celle-ci et sans intervention de l'utilisateur ;
- vérifier les index opérationnels de la base de données ;
- récupérer de l'espace libre par suppression des enregistrements vides ;
- réparer la base de données locale ;
- réparer les répliques, les anneaux de répliques et les objets Serveur ;
- analyser chaque serveur dans chaque partition locale afin de détecter d'éventuelles erreurs de synchronisation ;
- repérer et synchroniser les objets de la base de données locale.

Un certain nombre de problèmes rencontrés par la base de données eDirectory ne sont pas fatals et n'empêchent pas le fonctionnement de eDirectory. Cependant, si la base de données est endommagée, un message apparaît sur la console ; il indique que le serveur n'a pas pu ouvrir la base de données locale. Dans ce cas, exécutez l'utilitaire de réparation ou contactez le support technique de Novell.

Novell déconseille l'exécution d'opérations de réparation, excepté en cas de problème avec eDirectory ou sur instruction du support technique. Néanmoins, vous êtes invité à faire appel aux fonctions de diagnostic de l'utilitaire de réparation et d'autres utilitaires, tels que Novell iMonitor. Pour plus d'informations, reportez-vous à la section Chapitre 7, « Utilisation de Novell iMonitor 2.1 », page 193.

Novell iManager propose les assistants de réparation suivants :

Assistant	Description
Assistant de réparation de base	Permet d'effectuer une réparation complète sans surveillance et de réparer la base de données locale ou un seul objet. Vous pouvez également rechercher d'éventuelles références externes et supprimer les objets Feuille inconnus.
Assistant Fichier journal	Permet d'ouvrir le fichier journal des réparations et d'en définir les options.
Réparer via iMonitor	Permet d'ouvrir iMonitor et d'utiliser les options de réparation proposées par ce programme.
Assistant de réparation des répliques	Permet de réparer toutes les répliques ou celles sélectionnées, de réparer les tampons horaires et de déclarer une nouvelle période, de désigner le serveur en cours comme nouvelle réplique maîtresse et de détruire la réplique sélectionnée, si nécessaire.
Assistant de réparation des anneaux de répliques	Permet de réparer tous les anneaux de répliques ou ceux sélectionnés, d'envoyer tous les objets vers chaque serveur de l'anneau, de recevoir tous les objets transmis de la réplique maîtresse vers la réplique sélectionnée et de supprimer le serveur actuel de l'anneau de répliques, si nécessaire.
Assistant de maintenance du schéma	Permet d'extraire un schéma de l'arborescence, de réinitialiser le schéma local, de déclarer une nouvelle période de schéma, d'apporter des améliorations facultatives au schéma, d'importer un schéma distant et de réaliser une mise à jour du schéma postérieure à NetWare® 5.
Assistant de réparation du serveur	Permet de réparer toutes les adresses réseau ou uniquement celles d'un serveur.
Assistant de réparation de la synchronisation	Permet de synchroniser la réplique sélectionnée sur le serveur actuel, d'indiquer l'état de synchronisation de ce serveur ou de tous les serveurs, d'effectuer une synchronisation horaire et de planifier une synchronisation immédiate.

Grâce aux assistants, vous pouvez réaliser les opérations suivantes :

- « Opérations de réparation de base », page 263
- « Affichage et configuration du fichier journal des réparations », page 267
- « Réalisation d'une réparation dans Novell iMonitor », page 268
- « Réparation des répliques », page 268
- « Réparation des anneaux de répliques », page 271
- « Maintenance du schéma », page 273
- « Réparation des adresses réseau du serveur », page 277
- « Opérations de synchronisation », page 278
- « Options DSRepair avancées », page 280
- « Utilisation du client eMBox pour réparer une base de données », page 284

Opérations de réparation de base

L'Assistant de réparation de base permet d'effectuer une réparation complète sans surveillance, ainsi qu'une réparation de la base de données locale ou d'un seul objet. Vous pouvez également rechercher d'éventuelles références externes et supprimer les objets Feuille inconnus.

Réalisation d'une réparation complète sans surveillance

Cette opération recherche et corrige les erreurs eDirectory les plus graves qui figurent dans les fichiers de base de données eDirectory d'un serveur donné. Cette réparation réalise huit opérations principales, dont aucune ne requiert l'intervention de l'administrateur. Pendant certaines de ces opérations, la base de données locale est verrouillée. La réparation complète sans surveillance génère un ensemble temporaire de fichiers de la base de données locale et effectue les corrections nécessaires par rapport à ces fichiers. De cette manière, en cas de problème grave, les fichiers d'origine demeurent intacts.

Nous vous recommandons d'appliquer ce type de réparation si vous ne maîtrisez pas les options interactives de réparation de la base de données locale. L'exécution de la réparation complète sans surveillance peut occuper le double de l'espace disque actuellement utilisé par les fichiers de la base de données. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale », page 265.

La reconstitution des index opérationnels utilisés par eDirectory n'est possible que lorsque la base de données locale est verrouillée.

Le tableau ci-dessous liste les opérations réalisées au cours d'une réparation complète sans surveillance :

Opération	Base de données verrouillée ?	Description
Vérifier la structure et l'index de la base de données	Oui	Analyse la structure et le format des enregistrements et des index de la base de données. Cette opération permet de s'assurer qu'aucune altération structurelle n'a été introduite dans l'environnement eDirectory au niveau de la base de données.
Reconstruire toute la base de données	Oui	Élimine les erreurs détectées lors de la vérification de la structure et de l'index. Les structures de données correctes sont rétablies et les fichiers de la base de données et de l'index eDirectory sont recréés.
Vérifier la structure de l'arborescence	Oui	Examine les liens entre les enregistrements de la base de données pour s'assurer qu'à chaque enregistrement enfant correspond un parent valide. Cette opération contribue à garantir la cohérence de la base de données. Les enregistrements non valides sont marqués pour pouvoir être restaurés à partir d'une autre réplique de partition lors de la synchronisation des répliques eDirectory.

Opération	Base de données verrouillée ?	Description
Réparer toutes les répliques locales	Oui	Élimine les incohérences de la base de données eDirectory en comparant chaque objet et attribut aux définitions du schéma. Vérifie également le format de toutes les structures de données internes. Cette opération peut également éliminer les incohérences détectées pendant la vérification de la structure de l'arborescence, via la suppression des enregistrements non valides de la base de données. Ainsi, tous les enregistrements enfants reliés par l'intermédiaire des enregistrements non valides sont marqués comme orphelins. Ces enregistrements orphelins ne sont pas perdus, mais cette opération peut générer de nombreuses erreurs pendant la reconstitution de la base de données. Tout cela est parfaitement normal. Les objets orphelins seront automatiquement réorganisés pendant la synchronisation des répliques.
Vérifier les références locales	Oui	Les références locales sont des pointeurs vers d'autres objets gérés dans la base de données eDirectory du serveur de fichiers actuel. Cette opération évalue les pointeurs internes de la base de données pour s'assurer qu'ils désignent les objets eDirectory appropriés. Si des références non valides sont trouvées, elles sont corrigées. Selon le nombre de relations existant entre les objets, cette opération peut prendre un certain temps.
Réparer les adresses réseau	Non	Compare les adresses réseau du serveur stockées dans eDirectory aux valeurs gérées dans les tables locales SAP, SLP ou DNS pour s'assurer que eDirectory dispose de données correctes. En cas d'incohérence, eDirectory est mis à jour avec les informations correctes.
Valider les fichiers de syntaxe de flux	Oui	Les fichiers de syntaxe de flux, tels que les scripts de login, sont stockés dans une zone réservée de la base de données eDirectory. Cette opération vérifie que chaque fichier de syntaxe de flux est associé à un objet eDirectory valide. Si tel n'est pas le cas, le fichier de syntaxe de flux est supprimé et son attribut de référence purgé.
Valider les rép. messagerie (NetWare uniquement)	Oui	Par défaut, eDirectory crée des répertoires de messagerie dans le répertoire sys:mail des serveurs NetWare® afin de prendre en charge les anciens utilisateurs de la Bindery. Les scripts de login des utilisateurs de la Bindery sont stockés dans leurs répertoires de messagerie. Cette opération vérifie que chaque répertoire de messagerie est associé à un objet Utilisateur eDirectory valide. Si tel n'est pas le cas, le répertoire de messagerie est supprimé.
Vérifier les objets Volume et les ayants droit (NetWare uniquement)	Non	Vérifie que chaque volume du serveur NetWare est associé à un objet Volume dans eDirectory. Si tel n'est pas le cas, elle recherche le contexte de résidence du serveur pour vérifier s'il existe un objet Volume. S'il n'en existe pas, un objet Volume est créé. Après validation des informations liées au volume, la liste des ID d'ayants droit est validée. Chaque objet eDirectory possède un ID unique d'ayant droit. Cet ID permet d'assigner des droits à d'autres objets, notamment les volumes NetWare, dans l'arborescence eDirectory. Cette opération vérifie que chaque ID d'ayant droit de la liste des volumes est un objet eDirectory valide. Si tel n'est pas le cas, l'ID de l'ayant droit est supprimé de la liste des volumes.

Pour effectuer une réparation complète sans surveillance :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de base.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparation complète sans surveillance, puis sur Démarrer.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation de la base de données locale

Cette option de réparation permet d'éliminer les incohérences dans la base de données locale afin que eDirectory puisse ouvrir cette dernière et y accéder.

Si vous le souhaitez, la réparation de la base de données locale peut s'effectuer sur un ensemble temporaire de fichiers. Sinon, la réparation a lieu sur la base de données active.

Pour que la réparation s'effectue sur un ensemble temporaire de fichiers de la base de données, vous devez fermer celle-ci pendant cette partie de l'opération. Si vous décidez de travailler sur un ensemble temporaire de fichiers, vous êtes invité à valider les modifications apportées lors de la réparation pour les rendre permanentes. Dans le cas contraire, les modifications sont appliquées immédiatement.

Après une réparation, vous pouvez afficher le journal des opérations de réparation pour déterminer si d'autres réparations sont nécessaires. Pour plus d'informations, reportez-vous à la section « Affichage et configuration du fichier journal des réparations », page 267.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de base.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparation de base de données locale, puis sur Suivant.
6. Spécifiez les options de l'opération de réparation locale, puis cliquez sur Démarrer.
7. Suivez les instructions en ligne pour terminer l'opération.

Vérification des références externes

Cette option vérifie chaque objet de référence externe afin de déterminer si une réplique contenant l'objet peut être localisée. Si tous les serveurs qui contiennent une réplique de la partition sur laquelle se trouve l'objet sont inaccessibles, l'objet est introuvable. Dans ce cas, un avertissement est publié.

Cette opération fournit également les informations de notice nécrologique.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de base.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.

4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Vérifier les références externes, puis sur Démarrer.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation d'un seul objet

Cette opération tente d'éliminer toutes les incohérences dans un objet eDirectory qui pourraient empêcher eDirectory d'accéder à ces données. Elle n'est possible que pour les partitions créées par l'utilisateur et pour la partition de référence externe.

Elle est exécutée sur les fichiers de base de données actifs. Si l'altération se situe au niveau physique, vous pouvez être amené à exécuter une vérification physique et structurelle avant de commencer à réparer l'objet.

Veillez à toujours disposer d'une copie de sauvegarde actualisée de la base de données eDirectory.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de base.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparation d'objet, puis sur Démarrer.
6. Spécifiez l'objet à réparer, puis cliquez sur Suivant.
7. Suivez les instructions en ligne pour terminer l'opération.

Suppression des objets Feuille inconnus

La réparation transforme les objets incohérents en objets inconnus lorsque des propriétés obligatoires font défaut ou lorsqu'ils ne sont pas valides pour d'autres raisons (leurs propriétés ne satisfont pas aux exigences minimales pour un type d'objet). Les objets inconnus sont des objets réels identifiés par eDirectory. Ils sont considérés comme « inconnus » car leur classe n'a pas pu être complètement validée. Vous pouvez supprimer des objets inconnus, représentés par des icônes en forme de point d'interrogation, mais il est difficile de leur rendre leur type d'origine.

Cette réparation supprime tous les objets de la base de données eDirectory locale qui appartiennent à la classe d'objet Inconnu et ne possèdent aucun objet subordonné. La suppression sera ensuite synchronisée avec d'autres répliques de l'arborescence eDirectory.

IMPORTANT : n'effectuez cette opération qu'en parfaite connaissance de cause ou sur instruction du support technique de Novell.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de base.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Supprimer les objets Feuille inconnus, puis sur Démarrer.
6. Suivez les instructions en ligne pour terminer l'opération.

Affichage et configuration du fichier journal des réparations

Le fichier journal des réparations contient des informations détaillées sur les partitions et serveurs locaux. Ces informations vous aident à diagnostiquer l'étendue des dommages causés à la base de données. L'Assistant Fichier journal permet d'ouvrir le fichier journal des réparations et d'en définir les options.

Cette section contient des informations sur les opérations suivantes :

- « Ouverture du fichier journal », page 267
- « Définition des options du fichier journal », page 267

Ouverture du fichier journal

Cette opération permet d'afficher le fichier journal des réparations. Le nom par défaut de ce fichier est dsrepair.log. Il contient les résultats des opérations réalisées par les réparations.

Vous pouvez activer ou désactiver le fichier journal, le supprimer, le réinitialiser ou le renommer. Pour plus d'informations, reportez-vous à la section « Définition des options du fichier journal », page 267.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Fichier journal.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Ouvrir le fichier journal, puis sur Démarrer.
6. Suivez les instructions en ligne pour terminer l'opération.

Définition des options du fichier journal

Ces options permettent de gérer le fichier journal des réparations. Vous pouvez activer ou désactiver le fichier journal, le supprimer, l'annexer au fichier journal existant ou le renommer.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Fichier journal.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Options de fichier journal, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Réalisation d'une réparation dans Novell iMonitor

Vous pouvez accéder aux fonctions de réparation à l'aide de l'option Réparer via iMonitor de Novell iManager. La page Réparer de iMonitor permet d'afficher les problèmes et de sauvegarder ou de nettoyer la base de données eDirectory.

Dans iMonitor, DSRepair est une fonction centrée sur le serveur. Autrement dit, cette fonction n'est disponible que sur le serveur local qui exécute iMonitor. Si vous voulez accéder à cette fonction sur un autre serveur, vous devez basculer vers l'application iMonitor exécutée sur ce serveur.

Vous devez être assimilé à l'administrateur du serveur ou à un opérateur de la console sur le serveur à partir duquel vous essayez d'accéder à la page DS Repair. De ce fait, vous devez d'abord vous loguer, afin que vos références puissent être vérifiées, avant de pouvoir accéder aux informations de cette page.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparer via iMonitor.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur OK.

   Pour ouvrir iMonitor et exécuter manuellement les options de réparation, cliquez sur Exécuter iMonitor et accéder à l'utilitaire de réparation, puis sur OK.
4. Spécifiez un nom d'utilisateur, un contexte et un mot de passe pour le serveur auquel vous essayez d'accéder, puis cliquez sur OK pour ouvrir la page Réparer de iMonitor.
5. Sélectionnez les options de réparation, puis cliquez sur Lancer la réparation.

Pour plus d'informations sur l'utilisation des fonctions de réparation disponibles dans iMonitor, reportez-vous à la section « Affichage des informations DSRepair », page 208.

Réparation des répliques

La réparation d'une réplique consiste à vérifier la cohérence de chacun des objets qu'elle contient par rapport au schéma et la cohérence de chaque attribut de ces objets par rapport au schéma et aux données en fonction de la syntaxe de l'attribut. D'autres structures de données internes associées à la réplique sont également vérifiées.

Utilisez l'Assistant de réparation des répliques pour effectuer les opérations suivantes :

- « Réparation de toutes les répliques », page 268
- « Réparation de répliques sélectionnées », page 269
- « Réparation des tampons horaires », page 269
- « Désignation d'un serveur comme la nouvelle réplique maîtresse », page 270
- « Destruction de la réplique sélectionnée », page 271

Réparation de toutes les répliques

Cette opération permet de réparer toutes les répliques figurant dans la table des répliques.

Si vous n'avez pas lancé d'opération Réparation de base de données locale sur la base de données eDirectory locale au cours des 30 dernières minutes, il est conseillé de le faire avant d'effectuer cette nouvelle opération. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale », page 265.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des répliques.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparer toutes les répliques, puis sur Démarrer.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation de répliques sélectionnées

Cette opération permet de ne réparer que la réplique sélectionnée dans l'affichage des répliques.

Si vous n'avez pas lancé d'opération Réparation de base de données locale sur la base de données eDirectory locale au cours des 30 dernières minutes, il est conseillé de le faire avant d'effectuer cette nouvelle opération. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale », page 265.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des répliques.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparer la réplique sélectionnée, puis sur Suivant.
6. Spécifiez la réplique à réparer, puis cliquez sur Démarrer.
7. Suivez les instructions en ligne pour terminer l'opération.

Réparation des tampons horaires

REMARQUE : avant d'effectuer cette opération, exécutez l'Assistant de réparation de la synchronisation pour vérifier que tous les serveurs de l'anneau de répliques communiquent convenablement. Pour plus d'informations, reportez-vous à la section « Opérations de synchronisation », page 278.

Cette opération fournit un nouveau point de référence à la réplique maîtresse afin que toutes les mises à jour appliquées aux répliques de la partition sélectionnée soient actualisées.

Cette opération est toujours effectuée sur la réplique maîtresse d'une partition. Cette réplique n'est pas obligatoirement la réplique locale sur ce serveur.

Les tampons horaires, placés sur les objets lors de leur création ou modification, doivent être uniques. Tous les tampons horaires d'une réplique maîtresse sont analysés. Si un tampon horaire est postérieur à l'heure réseau actuelle, il est remplacé par un nouveau. Si le tampon horaire est correct, aucun nouveau tampon n'est émis. Une fois tous les tampons horaires synchronisés, une nouvelle période est déclarée.

Effectuez cette opération si vous remarquez un écart entre les objets d'une réplique ou entre les propriétés d'un objet. Par exemple, si vous mettez à jour votre script de login mais que l'ancien apparaît toujours lorsque vous vous loguez, vérifiez que les répliques sont correctement synchronisées. Si l'écart entre les tampons horaires de l'heure future et de l'heure actuelle se compte en minutes, eDirectory le corrigera de lui-même. La déclaration d'une nouvelle période étant une opération extrêmement coûteuse, il est préférable de ne pas l'utiliser régulièrement.

Novell eDirectory constitue une base de données souple en matière de cohérence ; prévoyez donc cinq à dix minutes avant de vérifier la synchronisation des répliques. Les conséquences de cette opération sont les suivantes :

- Une nouvelle période est déclarée au niveau de la réplique maîtresse ; elle peut influer sur tous les objets de la réplique.
- Tous les tampons horaires sont examinés et réparés, si nécessaire.
- Les mises à jour ne sont pas acceptées de la part de répliques contenant des tampons horaires (périodes) postdatés tant que les répliques ne sont pas synchronisées.
- Une réplique reçoit une copie de tous les objets d'une réplique maîtresse ou de toute autre réplique pour laquelle une nouvelle période a été définie.
- La période de la réplique devient identique à celle de la réplique maîtresse.
- Les modifications d'une période précédente sont perdues.
- Il n'est pas nécessaire que la réplique maîtresse réside sur le serveur actuel, mais vous devez disposer du droit Superviseur sur cette réplique pour pouvoir effectuer la réparation.
- Les autres répliques passent dans un nouvel état.

Pour réparer les tampons horaires et déclarer une nouvelle période :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des répliques.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparer les tampons horaires et déclarer une nouvelle période, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Désignation d'un serveur comme la nouvelle réplique maîtresse

Cette opération désigne la réplique locale de la partition sélectionnée comme étant la réplique maîtresse. Vous pouvez ainsi désigner une nouvelle réplique maîtresse si l'original est perdu. Ce peut être le cas lorsque le serveur qui la contient présente une défaillance au niveau du disque dur et doit de ce fait être remplacé.

N'utilisez pas cette option pour réaliser les opérations classiques sur les partitions, disponibles dans Novell iManager. Pour plus d'informations, reportez-vous à la section Chapitre 5, « Gestion des partitions et des répliques », page 133.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des répliques.
3. Spécifiez le serveur à désigner comme nouvelle réplique maîtresse, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour authentifier le serveur, puis cliquez sur Suivant.
5. Cliquez sur Désigner ce serveur en tant que nouvelle réplique maîtresse, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Destruction de la réplique sélectionnée

Cette opération permet de supprimer la réplique sélectionnée du serveur actuel. La réplique est supprimée ou transformée en référence subordonnée.

N'utilisez pas cette option pour réaliser les opérations classiques sur les partitions, disponibles dans Novell iManager. Pour plus d'informations, reportez-vous à la section Chapitre 5, « Gestion des partitions et des répliques », page 133.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des répliques.
3. Spécifiez le serveur contenant la réplique à détruire, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour authentifier le serveur, puis cliquez sur Suivant.
5. Cliquez sur Détruire la réplique sélectionnée, puis sur Suivant.
6. Spécifiez la réplique à détruire, puis cliquez sur Suivant.
7. Suivez les instructions en ligne pour terminer l'opération.

Réparation des anneaux de répliques

La réparation d'un anneau de répliques consiste à vérifier les informations qui correspondent à cet anneau sur chacun des serveurs contenant une réplique et à valider les informations d'ID à distance.

Utilisez l'Assistant de réparation des anneaux de répliques pour effectuer les opérations suivantes :

- « Réparation de tous les anneaux de répliques », page 271
- « Réparation de l'anneau de répliques sélectionné », page 272
- « Envoi de tous les objets à chaque serveur de l'anneau », page 272
- « Réception de tous les objets de la réplique maîtresse sur la réplique sélectionnée », page 273
- « Suppression d'un serveur de l'anneau de répliques », page 273

Réparation de tous les anneaux de répliques

Cette opération permet de réparer l'anneau de toutes les répliques qui figurent dans l'affichage des répliques.

Si vous n'avez pas lancé d'opération Réparation de base de données locale sur la base de données eDirectory locale au cours des 30 dernières minutes, il est conseillé de le faire avant d'effectuer cette nouvelle opération. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale », page 265.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des anneaux de répliques.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparer tous les anneaux de répliques, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation de l'anneau de répliques sélectionné

Cette opération permet de réparer l'anneau de répliques de la réplique sélectionnée affichée dans la table des répliques.

Si vous n'avez pas lancé d'opération Réparation de base de données locale sur la base de données eDirectory locale au cours des 30 dernières minutes, il est conseillé de le faire avant d'effectuer cette nouvelle opération. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale », page 265.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des anneaux de répliques.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparer l'anneau de répliques sélectionné, puis sur Suivant.
6. Spécifiez la réplique à réparer, puis cliquez sur Suivant.
7. Suivez les instructions en ligne pour terminer l'opération.

Envoi de tous les objets à chaque serveur de l'anneau

Cette opération permet d'envoyer tous les objets du serveur sélectionné dans l'anneau de répliques vers tous les autres serveurs contenant une réplique de la partition.

Grâce à cette opération, vous pouvez vérifier si la réplique de la partition désignée sur le serveur sélectionné est synchronisée avec les autres serveurs de l'anneau de répliques. Vous ne pouvez pas exécuter cette opération sur un serveur ne contenant qu'une réplique de référence subordonnée de la partition.

Les modifications apportées à des répliques qui n'ont pas encore été synchronisées avec la réplique du serveur sélectionné sont perdues. Vérifiez l'état de synchronisation avant de lancer cette opération.

IMPORTANT : cette opération peut générer un trafic réseau très important lié à la nouvelle création des objets de la réplique. Il ne s'agit pas d'une opération de diagnostic.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des anneaux de répliques.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur, puis cliquez sur Suivant.
5. Cliquez sur Envoyer tous les objets à chaque serveur de l'anneau, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Réception de tous les objets de la réplique maîtresse sur la réplique sélectionnée

Cette opération permet de recevoir tous les objets de la réplique maîtresse sur la réplique des serveurs sélectionnés.

Grâce à cette opération, vous pouvez vérifier que la réplique de la partition désignée sur le serveur sélectionné dans l'anneau de répliques est synchronisée avec la réplique maîtresse. Vous ne pouvez pas exécuter cette opération sur un serveur contenant la réplique maîtresse.

IMPORTANT : cette opération risque de générer un trafic réseau particulièrement dense. Lorsque vous effectuez cette opération, la réplique actuelle se comporte comme si une nouvelle réplique était placée sur le serveur. Cette opération fait également passer la réplique dans un nouvel état.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des anneaux de répliques.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur, puis cliquez sur Suivant.
5. Cliquez sur Recevoir tous les objets de la réplique maîtresse sur la réplique sélectionnée, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Suppression d'un serveur de l'anneau de répliques

Cette option enlève un serveur spécifique de la réplique sélectionnée stockée sur le serveur actuel.

AVERTISSEMENT : si vous n'effectuez pas cette opération correctement, vous risquez d'endommager définitivement la base de données eDirectory. N'ayez recours à cette opération qu'à la demande du support technique de Novell.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation des anneaux de répliques.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur, puis cliquez sur Suivant.
5. Cliquez sur Enlever ce serveur de l'anneau de réplique, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Maintenance du schéma

Le schéma est un système de règles et de définitions pour les attributs d'objet. Il détermine le contenu et le format de chaque objet, ainsi que ses relations dans la base de données.

L'Assistant de maintenance du schéma comprend plusieurs opérations de schéma dont vous pouvez avoir besoin pour rendre un schéma de serveur eDirectory conforme à la réplique maîtresse de la racine. Toutefois, vous ne devez utiliser ces opérations que lorsque cela s'avère nécessaire. Les opérations de réparation locales et sans surveillance effectuent déjà une vérification du schéma.

Pour plus d'informations sur le schéma eDirectory, reportez-vous au Chapitre 4, « Gestion du schéma », page 121.

Utilisez l'Assistant de maintenance du schéma pour effectuer les opérations suivantes :

- « Demande du schéma de l'arborescence », page 274
- « Reconfiguration du schéma local », page 274
- « Mise à jour du schéma ultérieur à NetWare 5 », page 275
- « Améliorations de schéma facultatives », page 275
- « Importation du schéma à distance », page 276
- « Déclaration d'une nouvelle période de schéma », page 276

Demande du schéma de l'arborescence

Effectuez cette opération pour que la réplique maîtresse de la racine de l'arborescence synchronise son schéma avec ce serveur. Toutes les modifications apportées au schéma sont répercutées sur ce serveur depuis la réplique maîtresse de la racine pendant 24 heures.

IMPORTANT : Si tous les serveurs demandent ce schéma à la réplique maîtresse, le trafic réseau peut augmenter. Il est par conséquent recommandé d'utiliser cette option avec prudence.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Maintenance du schéma.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Demander le schéma de l'arborescence, puis sur Suivant
6. Suivez les instructions en ligne pour terminer l'opération.

Reconfiguration du schéma local

Cette opération provoque la réinitialisation du schéma qui efface les tampons horaires du schéma local et implique une synchronisation entrante du schéma.

Elle n'est pas disponible si elle est exécutée à partir de la réplique maîtresse de la partition [Root]. Cette restriction évite que tous les serveurs de l'arborescence soient réinitialisés en même temps.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Maintenance du schéma.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Reconfigurer le schéma local, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Mise à jour du schéma ultérieur à NetWare 5

Cette opération étend et modifie le schéma afin qu'il soit compatible avec les modifications DS effectuées dans des versions postérieures à NetWare 5.

En fonction de votre version de eDirectory, cette option peut être requise pour la mise à niveau vers une nouvelle version. Pour savoir si son utilisation est nécessaire, veuillez lire les notes de publication de la nouvelle version de eDirectory.

Cette opération implique que le serveur contient une réplique de la partition [Root] (de préférence, la maîtresse) et que l'état de la réplique est Actif.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Maintenance du schéma.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Mise à jour du schéma ultérieur à NetWare 5, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Améliorations de schéma facultatives

Cette opération étend et modifie le schéma pour des raisons d'endiguement et pour y apporter d'autres améliorations.

Pour cela, ce serveur doit contenir une réplique de la partition [Root] et l'état de la réplique doit être Actif. De plus, tous les serveurs NetWare 4 de l'arborescence doivent disposer des versions DS.NLM suivantes :

Serveur	Version
4.10	ds.nlm version 5.17 ou ultérieure
4.11 / 4.2	ds.nlm version 6.01 ou ultérieure

Les versions précédentes de eDirectory ne sont pas en mesure de synchroniser ces modifications.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Maintenance du schéma.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Améliorations de schéma facultatives, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Importation du schéma à distance

Cette opération permet de choisir une arborescence eDirectory qui contient le schéma à ajouter à celui de l'arborescence actuelle.

Une fois l'arborescence sélectionnée, le serveur contenant la réplique maîtresse de la partition [Root] est contacté. Le schéma de ce serveur est utilisé pour étendre le schéma sur l'arborescence actuelle.

Pour fusionner deux arborescences, vous devrez peut-être importer plusieurs fois le schéma d'une arborescence vers l'autre. Pour plus d'informations, reportez-vous à la section Chapitre 8, « Fusion d'arborescences Novell eDirectory », page 221.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Maintenance du schéma.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Importer le schéma à distance, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Déclaration d'une nouvelle période de schéma

Une période est un moment sélectionné de façon arbitraire comme point de référence. Elle équivaut à une ère ou à une nouvelle version. Une période contrôle la synchronisation des répliques. Lorsqu'une nouvelle période est déclarée, elle débute au niveau de la réplique maîtresse. Les autres répliques ne peuvent pas envoyer de mise à jour à une réplique d'une période plus récente, mais elles reçoivent des mises à jour de sa part jusqu'à ce qu'elles soient parfaitement synchronisées avec elle.

Lorsque d'autres répliques d'une partition donnée sont synchronisées avec la réplique mise à jour, c'est-à-dire lorsque les périodes de chaque réplique sont identiques, la synchronisation bidirectionnelle est à nouveau autorisée.

Lorsque vous déclarez une nouvelle période de schéma, la réplique maîtresse de la partition [Root] est contactée et les tampons horaires non autorisés sont réparés dans les enregistrements du schéma. Une nouvelle période de schéma est déclarée sur ce serveur, mais elle s'applique à l'ensemble de l'arborescence.

Tous les autres serveurs reçoivent une nouvelle copie du schéma, ainsi que les tampons horaires réparés.

Si le serveur récepteur contient un schéma non compris dans la nouvelle période, les objets et les attributs qui utilisent l'ancien schéma passent dans la classe ou l'attribut d'objet Inconnu.

IMPORTANT : n'effectuez cette opération que sur instruction du support technique de Novell.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Maintenance du schéma.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Déclarer une nouvelle période, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation des adresses réseau du serveur

L'Assistant de réparation du serveur permet de réparer toutes les adresses réseau de serveur figurant dans les anneaux de répliques ainsi que les objets Serveur de la base de données locale. Vous pouvez également réparer l'adresse réseau d'un serveur sélectionné dans les anneaux de répliques et les objets Serveur de la base de données locale.

Utilisez l'Assistant de réparation du serveur pour effectuer les opérations suivantes :

- « Réparation de toutes les adresses réseau », page 277
- « Réparation des adresses réseau d'un serveur », page 277

Réparation de toutes les adresses réseau

Cette opération permet de vérifier l'adresse réseau de tous les serveurs dans la base de données eDirectory locale. Le système recherche le nom de chaque serveur dans les tables SAP, auprès de l'agent Annuaire SLP et dans les informations DNS locales ou distantes, suivant le protocole de transport disponible.

Chaque adresse est ensuite comparée à l'attribut d'adresse réseau de l'objet Serveur eDirectory et à l'enregistrement d'adresse des attributs de réplique des objets [Root] de la partition. Si les adresses sont différentes, elles sont mises à jour de façon à être identiques.

Si l'adresse du serveur est introuvable dans les tables SAP, auprès de l'agent Annuaire SLP et dans les informations DNS locales ou distantes, aucune réparation n'est effectuée.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation du serveur.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Réparer toutes les adresses réseau, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation des adresses réseau d'un serveur

Cette opération permet de vérifier l'adresse réseau d'un serveur sélectionné dans les fichiers de la base de données eDirectory locale. Le système recherche le nom du serveur dans les tables SAP locales, auprès de l'agent Annuaire SLP ou dans les informations DNS locales ou distantes, suivant les protocoles de transport actuellement liés. L'adresse du serveur est ensuite comparée à l'attribut d'adresse réseau de l'objet Serveur eDirectory et à l'enregistrement d'adresse de chaque attribut de réplique des objets [Root] de la partition. Si les adresses sont différentes, elles sont mises à jour de façon à être identiques.

Si l'adresse du serveur est introuvable dans les tables SAP, auprès de l'agent Annuaire SLP et dans les informations DNS locales ou distantes, aucune autre réparation n'est effectuée.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation du serveur.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.

4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.

5 Cliquez sur Réparer les adresses réseau de ce serveur, puis sur Suivant.

6 Suivez les instructions en ligne pour terminer l'opération.

Problèmes

Novell SLP est un paquetage facultatif. La fonction d'authentification n'y est pas implémentée.

eDirectory est désormais exploitable avec OpenSLP, dont les fonctions d'authentification sont utilisées.

Opérations de synchronisation

L'Assistant de réparation de la synchronisation permet de synchroniser une réplique sélectionnée sur le serveur actuel, d'indiquer l'état de synchronisation de ce serveur et de tous les serveurs, d'effectuer une synchronisation horaire et de planifier une synchronisation immédiate.

Utilisez l'Assistant de réparation de la synchronisation pour effectuer les opérations suivantes :

- « Synchronisation de la réplique sélectionnée sur un serveur », page 278
- « Indication de l'état de synchronisation sur un serveur », page 279
- « Indication de l'état de la synchronisation sur tous les serveurs », page 279
- « Synchronisation horaire », page 279
- « Planification d'une synchronisation immédiate », page 280

Synchronisation de la réplique sélectionnée sur un serveur

Cette opération indique l'état de synchronisation complet de chaque serveur possédant une réplique de la partition sélectionnée.

Vous pouvez ainsi déterminer plus facilement l'état de santé d'une partition. Si tous les serveurs comportant une réplique de la partition se synchronisent correctement, la partition est considérée comme saine. Chaque serveur de l'anneau de répliques est contacté, puis chacun procède à une synchronisation immédiate avec les autres serveurs de l'anneau.

Les serveurs ne se synchronisent pas avec eux-mêmes. Par conséquent, l'état de la réplique du serveur actuel est Hôte.

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Utilitaires de maintenance eDirectory > Réparation de la synchronisation.

3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.

4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.

5 Cliquez sur Synchroniser la réplique sélectionnée sur ce serveur, puis sur Suivant.

6 Suivez les instructions en ligne pour terminer l'opération.

Indication de l'état de synchronisation sur un serveur

Cette opération indique l'état de synchronisation des répliques de chaque partition possédant une réplique sur le serveur actuel.

Cette opération obtient l'attribut État de synchronisation de l'objet [Root] de la réplique sur chacun des serveurs contenant des répliques des partitions. L'heure de la dernière synchronisation réussie avec tous les serveurs et les erreurs survenues depuis cette synchronisation sont affichées.

Un message d'avertissement apparaît également si la synchronisation n'est pas terminée dans un délai de 12 heures.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de la synchronisation.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Rapporter l'état de la synchronisation sur ce serveur, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Indication de l'état de la synchronisation sur tous les serveurs

Cette opération indique l'état de synchronisation des répliques de chacune des partitions possédant une réplique sur le serveur actuel.

Cette opération obtient l'attribut État de synchronisation de l'objet [Root] de la réplique sur chacun des serveurs contenant des répliques des partitions. L'heure de la dernière synchronisation réussie avec tous les serveurs et les erreurs survenues depuis cette synchronisation sont affichées.

Un message d'avertissement apparaît également si la synchronisation n'est pas terminée dans un délai de 12 heures.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de la synchronisation.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Rapporter l'état de la synchronisation sur tous les serveurs, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Synchronisation horaire

Cette opération contacte chaque serveur connu de la base de données eDirectory locale et demande des informations sur eDirectory et sur l'état de synchronisation horaire pour chaque serveur.

La version de eDirectory exécutée sur chaque serveur est indiquée dans le champ Version DS.

La valeur du champ Profondeur de la réplique est -1 si aucune réplique n'est stockée sur un serveur donné. La valeur0 indique que le serveur contient une réplique de la partition [Root]. Un nombre entier positif signale qu'une réplique existe sur un serveur donné. Il correspond au nombre d'objets qui séparent la racine de la réplique la plus proche.

Tous les serveurs d'une arborescence eDirectory doivent être synchronisés d'après la même source horaire. Si tous les serveurs ne sont pas synchronisés avec la même heure, la synchronisation d'objets entre répliques n'est pas gérée correctement lors de conflits.

L'Assistant de réparation de la synchronisation ne peut pas indiquer la source horaire de chaque serveur ; il signale en revanche le type de serveur horaire. Ces informations peuvent ensuite être utilisées pour déterminer si la synchronisation horaire est convenablement configurée.

IMPORTANT : il est préférable d'utiliser Novell iMonitor au lieu de DSRepair pour contrôler l'état « Presque en synchronisation » de la synchronisation horaire. Pour plus d'informations, reportez-vous à la section Chapitre 7, « Utilisation de Novell iMonitor 2.1 », page 193.

Pour plus d'informations, reportez-vous à la section « Synchronisation des heures réseau », page 90.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de la synchronisation.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Synchronisation horaire, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Planification d'une synchronisation immédiate

Cette opération permet de lancer immédiatement la synchronisation de toutes les répliques. Utilisez-la pour obtenir des informations sur la synchronisation sans attendre que le processus soit exécuté au moment prévu.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Réparation de la synchronisation.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur Suivant.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur Suivant.
5. Cliquez sur Planifier une synchronisation immédiate, puis sur Suivant.
6. Suivez les instructions en ligne pour terminer l'opération.

Options DSRepair avancées

Outre les fonctions de réparation disponibles dans Novell iManager, les utilitaires DSRepair de chaque plate-forme eDirectory offrent des fonctions avancées qu'une utilisation normale ne permet pas de déceler. Ces dernières sont activées par des paramètres spécifiques lors du chargement de l'utilitaire DSRepair sur ces différentes plates-formes.

- « Exécution de DSRepair sur le serveur eDirectory », page 281
- « Options de ligne de commande DSRepair », page 282
- « Utilisation des paramètres DSRepair avancés », page 283

Exécution de DSRepair sur le serveur eDirectory

NetWare

Pour exécuter DSRepair, entrez **`dsrepair.nlm`** sur la console du serveur.

Pour ouvrir DSRepair avec les options avancées, entrez **`dsrepair -a`** sur la console du serveur.

Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration > Services Novell eDirectory.
2. Cliquez sur dsrepair.dlm, puis sur Démarrer.

   Pour accéder à DSRepair avec les options avancées, entrez **`-a`** dans le champ Paramètres de démarrage de la consoleNovell eDirectory Services avant de lancer dsrepair.dlm.

Linux, Solaris, AIX et HP-UX

Pour exécuter DSRepair, entrez **`ndsrepair`** sur la console du serveur en utilisant la syntaxe suivante :

```
ndsrepair { -U | -E | -C | -P [-Ad] | -S [-Ad] | -N  | -T | -J ID_entrée | --version} [-F nom_fichier] [-A yes|no] [-O yes|no]
```

ou

```
ndsrepair -R [-l yes|no] [-u yes|no] [-m yes|no] [-i yes|no] [-f yes|no][-d yes|no] [-t yes|no] [-o yes|no][-r yes|no] [-v yes|no] [-c yes|no] [-F nom_fichier] [-A yes|no] [-O yes|no]
```

IMPORTANT : l'option -Ad ne doit pas être utilisée, sauf si le support technique de Novell vous le demande.

Exemples

Pour effectuer une réparation sans surveillance et consigner des événements dans le fichier /root/ndsrepair.log, ou pour annexer des événements au fichier journal existant, entrez la commande suivante :

```
ndsrepair -U  -A no -F /root/ndsrepair.log
```

Pour ouvrir DSRepair avec les options avancées, entrez la commande suivante :

```
ndsrepair -Ad
```

Pour afficher la liste de toutes les opérations globales du schéma et des options avancées, entrez la commande suivante :

```
ndsrepair -S -Ad
```

Pour réparer la base de données locale en imposant son verrouillage, entrez la commande suivante :

```
ndsrepair -R -l yes
```

REMARQUE : l'entrée de la commande ndsrepair peut être réacheminée à partir d'un fichier d'options. Il s'agit d'un fichier texte qui peut contenir des options et sous-options liées au fonctionnement des partitions et des répliques, qui n'exigent pas d'authentification auprès du serveur. Les options ou sous-options sont séparées par un retour à la ligne. Vérifiez que le contenu du fichier se présente dans le bon ordre. Si tel n'est pas le cas, le résultat est imprévisible.

Options de ligne de commande DSRepair

Option	Description
-U	Option Réparation complète sans surveillance. Commande l'exécution et l'arrêt de ndsrepair sans autre intervention de l'utilisateur. Cette méthode de réparation est conseillée ; il se peut néanmoins que le support technique de Novell vous demande d'effectuer certaines opérations manuellement. Vous pouvez consulter le fichier journal une fois la réparation terminée afin de connaître les modifications apportées par ndsrepair.
-P	Option Opérations de partition et de réplique. Liste les partitions dont des répliques sont stockées dans les fichiers de la base de données eDirectory du serveur actuel. Le menu des options de réplique permet de réparer les répliques, d'annuler une opération de partition, de planifier une synchronisation et de désigner la réplique locale comme réplique maîtresse.
-S	Option Opérations globales du schéma. Contient plusieurs opérations de schéma dont vous pouvez avoir besoin pour conformer le schéma du serveur à la réplique maîtresse de l'objet Arborescence. Toutefois, vous ne devez utiliser ces opérations que lorsque cela s'avère nécessaire. Les opérations de réparation locales et sans surveillance effectuent déjà une vérification du schéma.
-C	Option de vérification de l'objet de référence externe. Vérifie chaque objet de référence externe afin de déterminer si une réplique contenant l'objet peut être localisée. Si tous les serveurs qui contiennent une réplique de la partition sur laquelle se trouve l'objet sont inaccessibles, l'objet ne peut pas être trouvé. Dans ce cas, un avertissement est publié.
-E	Option de signalement de l'état de synchronisation des répliques. Indique l'état de synchronisation des répliques de chacune des partitions qui possède une réplique sur le serveur actuel. Cette opération lit l'attribut État de synchronisation de l'objet Arborescence de la réplique sur chacun des serveurs contenant des répliques des partitions. L'heure de la dernière synchronisation réussie avec tous les serveurs et les erreurs survenues depuis cette synchronisation sont affichées. Un message d'avertissement apparaît si la synchronisation n'est pas terminée dans les douze heures.
-N	Option Serveurs connus de cette base de données. Liste tous les serveurs connus de la base de données eDirectory locale. Si le serveur actuel contient une réplique de la partition Arborescence, il affiche la liste de tous les serveurs de l'arborescence eDirectory. Sélectionnez un serveur pour lancer l'exécution de ses options.
-J	Option de réparation d'un seul objet du serveur local. Vous devez fournir l'ID d'entrée (au format hexadécimal) de l'objet à réparer. Vous pouvez utiliser cette option à la place de Réparation sans surveillance (-U) pour réparer un objet spécifique altéré. L'exécution de l'option Réparation sans surveillance peut prendre plusieurs heures, selon la taille de la base de données. Cette option permet de gagner du temps.
-T	Option Synchronisation horaire. Contacte chaque serveur listé dans la base de données eDirectory locale pour lui demander des informations sur son état de synchronisation horaire. Si ce serveur contient une réplique de la partition Arborescence, chaque serveur de l'arborescence eDirectory est interrogé. Indique également la version de eDirectory qui est exécutée sur chaque serveur.
-A	Annexer au fichier journal existant. Les informations sont ajoutées au fichier journal existant. Par défaut, cette option est activée.

Option	Description
-O	Option de consignation de la sortie dans un fichier. Par défaut, cette option est activée.
-F *nom_fichier*	Consigne la sortie dans le fichier spécifié.
-R	Option de réparation de la base de données locale. Répare la base de données eDirectory locale. Cette option de réparation résout les incohérences existant dans la base de données locale afin d'en permettre l'ouverture et l'accès par eDirectory. Elle est associée à des sous-options qui facilitent les opérations de réparation réalisées sur la base de données. Cette option comporte des modificateurs de fonction qui sont décrits dans le tableau ci-dessous.

Les modificateurs de fonction utilisés avec l'option -R sont décrits ci-après :

Option	Description
-l	Verrouille la base de données eDirectory durant la réparation.
-u	Utilise une base de données eDirectory temporaire lors de la réparation.
-m	Conserve la base de données d'origine non réparée.
-i	Vérifie la structure et l'index de la base de données eDirectory.
-f	Récupère l'espace libre dans la base de données.
-d	Reconstitue l'ensemble de la base de données.
-t	Vérifie la structure de l'arborescence. Précisez Yes (Oui) pour vérifier la connectivité de tous les liens de structure d'arborescence dans la base de données. Indiquez No (Non) pour ignorer cette vérification. Valeur par défaut = Yes.
-o	Reconstitue le schéma opérationnel.
-r	Répare toutes les répliques locales.
-v	Valide les fichiers de flux.
-c	Vérifie les références locales.

Utilisation des paramètres DSRepair avancés

AVERTISSEMENT : les fonctions décrites dans cette section peuvent causer des dommages irréparables à votre arborescence eDirectory si elles ne sont pas correctement utilisées. N'exécutez ces fonctions que sur instruction du support technique de Novell.

Effectuez une sauvegarde complète de eDirectory sur le serveur avant d'utiliser ces fonctions dans un environnement de production. Pour plus d'informations, reportez-vous à la section « Sauvegarde et restauration de Novell eDirectory », page 383.

Sous NetWare, utilisez ces options sur la console du serveur lors du chargement de DSRepair (par exemple, dsrepair -XK2).

Sous Linux, Solaris, AIX et HP-UX, entrez **`ndsrepair -R -Ad -XK2`**.

Sous Windows, entrez ces options dans le champ Paramètres de démarrage de la console NDS avant de lancer dsrepair.dlm. Pour plus d'informations, reportez-vous à la section « Exécution de DSRepair sur le serveur eDirectory », page 281.

Paramètre	Description
-NLC	Si le paramètre STORE NETWARE 5 CONN SCL MLA USAGE IN NDS est activé sur un serveur NetWare, l'attribut NLS:CERT PEAK USED POOL risque d'avoir une valeur très élevée. L'exécution de DSRepair avec le paramètre -NLC permet de supprimer ces valeurs élevées.
-P	Marque tous les objets eDirectory de type Inconnu comme étant référencés. Les objets référencés ne participent pas à la synchronisation des répliques dans eDirectory.
-WM	Dans de nombreux cas, l'attribut WM: Registered Workstations prend une valeur très élevée sous ZENworks® 2.0. L'exécution de DSRepair avec le paramètre -WM supprime ces valeurs élevées.
-XK2	Élimine tous les objets eDirectory de la base de données eDirectory du serveur. Cette opération permet de détruire une réplique altérée qui ne peut être supprimée autrement.
-XK3	Élimine toutes les références externes de la base de données eDirectory du serveur. Cette opération permet de détruire toutes les références externes d'une réplique défectueuse. Si les références sont à l'origine du problème, eDirectory peut les recréer afin de rétablir le bon fonctionnement de la réplique.

Utilisation du client eMBox pour réparer une base de données

Le client eDirectory Management Toolbox (eMBox) est un client Java à ligne de commande qui permet d'accéder à DSRepair à distance. Le client eMBox peut être lancé en mode de traitement par lots (batch). Vous pouvez donc l'utiliser pour effectuer des réparations sans surveillance à l'aide de l'outil eMTool DSRepair de eDirectory.

Le fichier emboxclient.jar est installé sur votre serveur comme élément de eDirectory. Vous pouvez l'exécuter sur toute machine dotée d'une JVM. Pour plus d'informations sur le client eMBox, reportez-vous à la section « Utilisation du client à ligne de commande eMBox », page 553.

Utilisation de l'outil eMTool DSRepair

1. Exécutez le client eMBox en mode interactif en entrant les éléments suivants dans la ligne de commande :

   java -cp *chemin_fichier*/emboxclient.jar embox -i

   (Si le fichier emboxclient.jar figure déjà dans votre chemin d'accès à la classe, il vous suffit d'entrer la commande **java embox -i**.)

   L'invite du client eMBox apparaît :

   ```
   Client eMBox>
   ```

2. Loguez-vous au serveur à réparer en entrant la commande suivante :

   login -s*nom_ou_adresse_IP_serveur* -p*numéro_port*
   -u*nom_utilisateur.contexte* -w*mot_de_passe* -n

   Le numéro de port est généralement 80 ou 8028, à moins qu'il ne soit déjà utilisé par un serveur Web. L'option -n ouvre une connexion non sécurisée.

   Le client eMBox indique si le login a réussi.

3 Entrez une commande de réparation à l'aide de la syntaxe suivante :

dsrepair.*tâche options*

Par exemple :

dsrepair.ufr effectue une réparation complète sans surveillance.

dsrepair.rld -a -v répare la base de données locale à l'aide des options Réparer toutes les répliques locales et Vérifier les références locales.

Les paramètres doivent être séparés les uns des autres par un espace. L'ordre des paramètres n'a pas d'importance.

Le client eMBox indique la réussite ou l'échec de la réparation.

Pour plus d'informations sur les options de l'outil eMTool DSRepair, reportez-vous à la section « Options de l'outil eMTool DSRepair », page 285.

4 Déloguez-vous du client eMBox en entrant la commande suivante :

```
logout
```

5 Quittez le client eMBox en entrant la commande suivante :

```
exit
```

Options de l'outil eMTool DSRepair

Les tableaux suivants listent les options de l'outil eMTool DSRepair. Vous pouvez également utiliser la commande **`list -tdsrepair`** du client eMBox pour afficher les options DSRepair de manière détaillée. Pour plus d'informations, reportez-vous à la section « Liste des outils eMTools et de leurs services », page 557.

Option	Description
rso -o -d	Réparation d'objet ID d'objet au format hexadécimal DN d'objet
rts	Synchronisation horaire
rss	Signaler l'état de la synchronisation de toutes les partitions
rld -l -t -d -p -i -f -e -c -o -a -m -v	Réparer la base de données locale Verrouiller la base de données eDirectory pendant la réparation Utiliser la base de données temporaire de eDirectory pendant la réparation Maintenir les BdD non réparées d'origine Vérifier la structure de la BdD Vérifier la structure et l'index de la base de données Récupérer l'espace libre de la BdD Reconstruire toute la base de données Vérifier la structure de l'arborescence Reconstruire le schéma opérationnel Réparer toutes les répliques locales Valider les rép. messagerie / fichiers de flux Vérifier les références locales
ufr	Réparation complète sans surveillance

Option	Description
rsn -o -d	Réparer l'adresse réseau du serveur sélectionné ID d'objet au format hexadécimal DN d'objet
ran	Réparer toutes les adresses réseau
rsr -p -d	Réparer la réplique sélectionnée ID de partition DN de partition
rer	Réparation de toutes les répliques
ror -p -d	Réparer l'anneau de répliques sélectionné ID de partition DN de partition
rar	Réparer l'anneau, toutes les répliques
ssa -p -d	Signaler l'état de synchronisation des répliques de tous les serveurs ID de partition DN de partition
cer	Vérifier les références externes
rao -p -d -s -d	Recevoir tous les objets pour cette réplique ID de partition DN de partition ID de serveur DN de serveur
sao -p -d -s -d	Envoyer tous les objets à chaque réplique de l'anneau ID de partition DN de partition ID de serveur DN de serveur
dne -p -d	Réparer les tampons horaires et déclarer une nouvelle période ID de partition DN de partition
sri -p -d	Planifier une synchronisation immédiate ID de partition DN de partition ID de serveur DN de serveur
sks -p -d -s -d	Synchroniser les répliques sur le serveur sélectionné ID de partition DN de partition ID de serveur DN de serveur
ske -p -d	Synchroniser les répliques sur tous les serveurs ID de partition DN de partition
dsr -p -d	Détruire la réplique sélectionnée dans ce serveur ID de partition DN de partition

Option	Description
xsr	Enlever ce serveur de l'anneau de réplique
-p	ID de partition
-d	DN de partition
-s	ID de serveur
-d	DN de serveur
dnm	Désigner ce serveur en tant que nouvelle réplique maîtresse
-p	ID de partition
-d	DN de partition
dul	Supprimer les objets Feuille inconnus

11 Gestionnaire de trafic WAN

Le gestionnaire de trafic WAN (WTM – WAN Traffic Manager) permet de gérer le trafic de réplication via des liaisons WAN, afin de réduire les coûts sur le réseau. Installé en même temps que Novell® eDirectory™, il se compose des éléments suivants :

- WTM

  WTM réside sur chaque serveur de l'anneau de répliques. Avant que eDirectory ne génère du trafic de serveur à serveur, WTM lit une règle de trafic WAN et détermine si ce trafic doit être envoyé.

- Règles de trafic WAN

  Ces règles contrôlent la génération du trafic eDirectory. Elles sont stockées au format texte en tant que valeur de propriété eDirectory dans un objet Serveur, dans un objet Zone LAN ou dans les deux.

- Plug-in WANMAN Novell iManager

  Cette interface permet de créer ou de modifier des règles, de créer des objets Zone LAN et d'appliquer des règles à des zones LAN ou des serveurs. Lors de l'installation du gestionnaire de trafic WAN (dans le cadre de l'installation de eDirectory), le schéma inclut un objet Zone LAN et une page Gestionnaire de trafic WAN pour l'objet Serveur.

Le gestionnaire de trafic WAN (wtm.nlm sous NetWare® ou wtm.dlm sous Windows) doit résider sur chaque serveur dont vous souhaitez contrôler le trafic. Si l'anneau de répliques d'une partition comprend des serveurs aux deux extrémités d'une liaison WAN, vous devez installer le gestionnaire de trafic WAN sur tous ces serveurs.

IMPORTANT : le gestionnaire de trafic WAN n'est pas pris en charge sur les systèmes Linux, Solaris, AIX ou HP-UX.

Présentation du gestionnaire de trafic WAN

Les répertoires réseau, tels que eDirectory, génèrent du trafic de serveur à serveur. Si ce trafic traverse des liaisons de réseau étendu (WAN) non gérées, il peut augmenter les coûts inutilement et surcharger les liaisons WAN lentes pendant les périodes de pointe.

Le gestionnaire de trafic WAN permet de contrôler le trafic de serveur à serveur (sur des liaisons WAN) généré par eDirectory, ainsi que le trafic eDirectory entre les serveurs d'une arborescence eDirectory. Le gestionnaire de trafic WAN peut restreindre le trafic en fonction de son coût, de l'heure de la journée, du type d'opération eDirectory ou de plusieurs de ces éléments.

Par exemple, vous pouvez restreindre le trafic eDirectory sur une liaison WAN pendant les heures de forte utilisation. Les activités nécessitant une bande passante importante sont ainsi reportées aux heures creuses. Vous pouvez également autoriser le trafic de synchronisation des répliques uniquement aux périodes de tarif réduit afin de diminuer les coûts.

Le gestionnaire de trafic WAN contrôle uniquement les événements périodiques générés par eDirectory, comme la synchronisation des répliques. Il ne contrôle pas les événements générés sur l'initiative d'un administrateur ou d'un utilisateur, pas plus qu'il ne contrôle le trafic de serveur à serveur non eDirectory (synchronisation horaire).

Les processus eDirectory listés dans le tableau suivant génèrent du trafic de serveur à serveur.

Processus	Description
Synchronisation des répliques	Garantit la synchronisation des modifications apportées aux objets eDirectory dans toutes les répliques de la partition. Ainsi, tout serveur qui possède une copie d'une partition donnée doit communiquer avec les autres serveurs pour synchroniser une modification. Il existe deux types de synchronisation de répliques : ◆ La synchronisation immédiate se produit après la modification d'un objet eDirectory ou après l'ajout ou la suppression d'un objet dans l'arborescence Annuaire. ◆ La synchronisation lente se produit pour des modifications spécifiques apportées à un objet eDirectory, qui sont répétitives et communes à plusieurs objets, comme les modifications portant sur les propriétés de login. Exemple : la mise à jour des propriétés Heure de login, Heure du dernier login, Adresse réseau et Révision lorsqu'un utilisateur se logue ou se délogue. Le processus de synchronisation lente est exécuté uniquement en l'absence d'un processus de synchronisation immédiate. Par défaut, la synchronisation immédiate est exécutée 10secondes après l'enregistrement de toute modification et la synchronisation lente 22 minutes après l'ajout d'autres modifications.
Synchronisation du schéma	Garantit la cohérence du schéma sur les partitions de l'arborescence Annuaire et la mise à jour de toutes les modifications du schéma sur le réseau. Par défaut, ce processus est exécuté toutes les quatre heures.
Pulsation	Garantit la cohérence des objets Annuaire sur l'ensemble des répliques d'une partition. Ainsi, pour vérifier cette cohérence, tout serveur qui contient une copie d'une partition doit communiquer avec les autres serveurs comportant la partition. Ce processus est exécuté par défaut toutes les 30minutes sur chaque serveur qui comporte une réplique d'une partition.

Processus	Description
Contrôleur de connectivité	Garantit la mise à jour de la table des pointeurs de réplique d'un serveur en cas de modification du nom ou de l'adresse de ce serveur. Ces modifications ont lieu dans les cas suivants : ◆ Le serveur est redémarré avec un nouveau nom ou une nouvelle adresse IPX™ interne dans le fichier autoexec.ncf. ◆ Une adresse est ajoutée pour un protocole supplémentaire. Lors du démarrage d'un serveur, le processus de contrôle de la connectivité compare le nom du serveur et son adresse IPX avec ceux stockés dans la table des pointeurs de réplique. S'ils sont différents, eDirectory met automatiquement à jour toutes les tables de pointeurs de réplique qui contiennent la liste des données figurant sur ce serveur. Le processus de contrôle de la connectivité vérifie également que le nom d'arborescence est correct pour chacun des serveurs d'un anneau de répliques. Le contrôleur de connectivité s'exécute cinq minutes après l'initialisation du serveur et ensuite toutes les trois heures.
Lien en amont	Vérifie les références externes, c'est-à-dire les pointeurs vers les objets eDirectory qui ne sont pas stockés dans les répliques d'un serveur. Le processus de liaison en amont fonctionne habituellement deux heures après l'ouverture de la base de données locale, puis toutes les treize heures.
Gestion des connexions	Les serveurs d'un anneau de répliques requièrent une connexion hautement sécurisée pour le transfert des paquets NCP™. Ces connexions sécurisées, appelées connexions client virtuelles, sont établies par le processus de gestion des connexions. Celui-ci peut également avoir besoin d'établir une connexion client virtuelle pour la synchronisation du schéma ou les processus de liaison en amont. Le système de synchronisation horaire peut aussi nécessiter ce type de connexion, selon la configuration des services horaires.
Vérification de l'état du serveur	Chaque serveur qui ne contient pas de réplique déclenche une vérification de son état. Il établit une connexion au serveur le plus proche qui contient une réplique inscriptible de la partition sur laquelle l'objet Serveur est situé. La vérification de l'état du serveur est exécutée toutes les six minutes.

Objets Zone LAN

Un objet Zone LAN permet de gérer aisément les règles de trafic WAN d'un groupe de serveurs. Une fois que vous avez créé un objet Zone LAN, vous pouvez y ajouter des serveurs ou en supprimer. Lorsque vous appliquez une règle à la zone LAN, elle est appliquée à tous les serveurs compris dans cette zone.

Vous devez créer un objet Zone LAN lorsque plusieurs serveurs sont présents dans un LAN connecté à d'autres LAN par des liaisons WAN. Si vous ne créez pas d'objet Zone LAN, vous devez gérer le trafic WAN de chaque serveur séparément.

Création d'un objet Zone LAN

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Trafic WAN > Créer une zone LAN.
3. Sélectionnez Zone WANMAN-LAN dans la liste déroulante Classe d'objet.
4. Entrez le nom et le contexte de l'objet, puis cliquez sur Créer.

Continuez avec l'une des sections suivantes :

- « Ajout de serveurs à un objet Zone LAN », page 292
- « Application des règles WAN », page 293

Ajout de serveurs à un objet Zone LAN

Un serveur ne peut appartenir qu'à un seul objet Zone LAN. Si le serveur que vous ajoutez figure déjà dans un objet Zone LAN, le serveur est supprimé de cet objet et ajouté au nouveau.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Trafic WAN > Présentation du gestionnaire de trafic WAN.
3. Cliquez sur Afficher les zones LAN, puis sur l'objet Zone LAN souhaité.
4. Cliquez sur Liste de serveurs, puis sur le bouton Sélecteur d'objet  .
5. Sélectionnez le serveur de votre choix.
6. Répétez l'Etape 4 et l'Etape 5 pour chaque serveur à ajouter.

   Pour appliquer une règle WAN à l'objet Zone LAN, ce qui permet également d'appliquer cette règle à tous les serveurs du groupe, reportez-vous à la section « Application des règles WAN », page 293.
7. Cliquez sur Appliquer, puis sur OK.

Ajout d'informations supplémentaires à un objet Zone LAN

Vous pouvez ajouter à un objet Zone LAN des informations d'ordre descriptif à l'aide de ConsoleOne®. Cette fonction n'est pas disponible dans Novell iMonitor.

1. Dans ConsoleOne, cliquez avec le bouton droit sur un objet Zone LAN.
2. Cliquez sur Propriétés > Général.
3. Ajoutez les informations Propriétaire, Description, Emplacement, Service et Organisation de votre choix.
4. Cliquez sur Appliquer, puis sur OK.

Règles de trafic WAN

Les règles de trafic WAN contrôlent la génération du trafic eDirectory. Ces règles sont créées au format texte et stockées en tant que valeur de propriété eDirectory dans l'objet Serveur, dans l'objet Zone LAN ou dans les deux. Les règles sont interprétées grâce à un langage de traitement simple.

Vous pouvez appliquer des règles à des serveurs particuliers ou créer des objets Zone LAN et assigner plusieurs serveurs à l'un de ces objets. Toute règle appliquée à un objet Zone LAN est automatiquement appliquée à tous les serveurs assignés à cet objet.

Le gestionnaire de trafic WAN est livré avec plusieurs groupes de règles prédéfinies. Vous pouvez utiliser ces règles telles quelles, les modifier en fonction de vos besoins ou en écrire de nouvelles.

- « Application des règles WAN », page 293
- « Modification des règles WAN », page 294
- « Attribution d'un nouveau nom à une règle existante », page 295
- « Création de règles WAN », page 295

Groupes de règles prédéfinies

Le tableau suivant liste les groupes de règles prédéfinies qui ont des fonctions similaires :

Groupe de règles	Description
1-3am.wmg	Autorise l'envoi de données uniquement entre 1 heure et 3 heures du matin.
7am-6pm.wmg	Autorise l'envoi de données uniquement entre 7 heures et 18 heures.
costlt20.wmg	Autorise uniquement l'envoi du trafic dont le facteur de coût est inférieur à 20.
ipx.wmg	Autorise uniquement le trafic IPX.
ndsttyps.wmg	Fournit des exemples de règles pour différents types de trafic eDirectory.
onospoof.wmg	Autorise uniquement l'utilisation de connexions WAN existantes.
opnspoof.wmg	Autorise uniquement l'utilisation de connexions WAN existantes. Cette règle considère toutefois qu'une connexion inutilisée pendant 15 minutes fait l'objet d'une usurpation et ne doit par conséquent pas être utilisée.
samearea.wmg	Autorise le trafic uniquement dans la même zone réseau.
tcpip.wmg	Autorise uniquement le trafic TCP/IP.
timecost.wmg	Permet l'envoi de tout le trafic uniquement entre 1h00 et 1h30 du matin, les serveurs situés à un même emplacement pouvant continuer à communiquer librement.

Pour plus d'informations sur les groupes de règles prédéfinies et sur chacune de ces règles, reportez-vous à la section « Groupes de règles du gestionnaire de trafic WAN », page 299.

Application des règles WAN

Vous pouvez appliquer des règles WAN à un serveur donné ou à un objet Zone LAN. Les règles appliquées à un serveur particulier ne gèrent que le trafic eDirectory de ce serveur. Les règles appliquées à un objet Zone LAN gèrent le trafic de tous les serveurs appartenant à cet objet.

Dans wanman.ini, le gestionnaire de trafic WAN recherche une section des groupes de règles WAN contenant une instruction *clé* = *valeurs*. *Clé* est le nom de la règle qui apparaît dans le snap-in et *valeur* désigne le chemin d'accès aux fichiers texte contenant des règles délimitées.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Trafic WAN > Présentation du gestionnaire de trafic WAN.

3 Cliquez sur Afficher les zones LAN, puis sur l'objet Zone LAN souhaité.

   ou

   Cliquez sur Afficher les serveurs NCP, puis sur un objet Serveur NCP.

4 Cliquez sur Ajouter une règle, puis sélectionnez le groupe de règles de votre choix.

   Pour plus d'informations, reportez-vous à la section « Groupes de règles prédéfinies », page 293.

5 Cliquez sur OK.

   La liste des règles chargées à partir du groupe de règles s'affiche.

6 Cliquez sur OK.

   Vous pouvez ainsi connaître la fonctionnalité de cette règle ou modifier son contenu, mais aussi cliquer sur Vérifier une règle pour rechercher les éventuelles erreurs.

7 Pour supprimer une règle superflue, sélectionnez-la dans la liste déroulante Nom de la règle, puis cliquez sur Supprimer une règle.

8 Cliquez sur Appliquer, puis sur OK.

Modification des règles WAN

Vous pouvez modifier l'un des groupes de règles prédéfinies fournis avec le gestionnaire de trafic WAN afin qu'il réponde à vos besoins. Vous pouvez également modifier une règle que vous avez rédigée vous-même.

Modification des règles WAN appliquées à un serveur

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Trafic WAN > Présentation du gestionnaire de trafic WAN > Afficher les serveurs NCP.

3 Cliquez sur l'objet Serveur qui contient la règle à modifier.

4 Sélectionnez la règle à modifier dans la zone de liste déroulante Nom de la règle.

5 Dans la zone Règle, modifiez la règle selon vos besoins.

   Pour obtenir une présentation de la structure d'une règle WAN, reportez-vous à la section « Structure d'une règle WAN », page 313.

   Pour obtenir une présentation de la syntaxe d'une règle WAN, reportez-vous à la section « Blocs utilisés au sein de sections de règles », page 316.

6 Cliquez sur Vérifier une règle pour identifier les erreurs de syntaxe ou de structure.

   Le gestionnaire de trafic WAN n'exécute pas les règles contenant des erreurs.

7 Cliquez sur Appliquer si vous avez effectué des modifications.

8 Pour supprimer une règle superflue, sélectionnez-la dans la liste déroulante Nom de la règle, puis cliquez sur Supprimer une règle.

9 Cliquez sur Appliquer, puis sur OK.

Modification des règles WAN appliquées à un objet Zone LAN

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Trafic WAN > Présentation du gestionnaire de trafic WAN > Afficher les zones LAN.
3. Cliquez sur l'objet Zone LAN qui contient la règle à modifier.
4. Sélectionnez la règle à modifier dans la zone de liste déroulante Nom de la règle.
5. Dans la zone Règle, modifiez la règle selon vos besoins.

   Pour obtenir une présentation de la structure d'une règle WAN, reportez-vous à la section « Structure d'une règle WAN », page 313.

   Pour obtenir une présentation de la syntaxe d'une règle WAN, reportez-vous à la section « Blocs utilisés au sein de sections de règles », page 316.
6. Cliquez sur Vérifier une règle pour identifier les erreurs de syntaxe ou de structure.

   Le gestionnaire de trafic WAN n'exécute pas les règles contenant des erreurs.
7. Cliquez sur Appliquer si vous avez effectué des modifications.
8. Pour supprimer une règle superflue, sélectionnez-la dans la liste déroulante Nom de la règle, puis cliquez sur Supprimer une règle.
9. Cliquez sur Appliquer, puis sur OK.

Attribution d'un nouveau nom à une règle existante

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Trafic WAN > Présentation du gestionnaire de trafic WAN.
3. Cliquez sur Afficher les zones LAN, puis sur l'objet Zone LAN souhaité.

   ou

   Cliquez sur Afficher les serveurs NCP, puis sur un objet Serveur NCP.
4. Sélectionnez la règle à renommer dans la zone de liste déroulante Nom de la règle.
5. Cliquez sur Renommer une règle, puis saisissez le nouveau nom.

   Il doit s'agir d'un nom distinctif complet.
6. Cliquez sur OK, puis sur Appliquer et enfin sur OK.

Création de règles WAN

Vous pouvez rédiger une règle WAN destinée à un objet Serveur ou Zone LAN. Les règles rédigées pour un serveur particulier gèrent le trafic eDirectory de ce serveur uniquement, tandis que celles rédigées pour un objet Zone LAN gèrent le trafic de tous les serveurs appartenant à cet objet.

Création d'une règle WAN pour un objet Serveur

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Trafic WAN > Présentation du gestionnaire de trafic WAN > Afficher les serveurs NCP.
3. Cliquez sur l'objet Serveur pour lequel vous souhaitez créer une nouvelle règle, puis cliquez sur Créer une règle.

4 Spécifiez un nom pour cette règle, puis cliquez sur OK.

Il doit s'agir d'un nom distinctif complet.

5 Saisissez les informations nécessaires dans la zone de texte Règle.

Pour obtenir une présentation de la structure d'une règle WAN, reportez-vous à la section « Structure d'une règle WAN », page 313.

Pour obtenir une présentation de la syntaxe d'une règle WAN, reportez-vous à la section « Blocs utilisés au sein de sections de règles », page 316.

6 Cliquez sur Appliquer, puis sur OK.

Création d'une règle WAN pour un objet Zone LAN

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Trafic WAN > Présentation du gestionnaire de trafic WAN > Afficher les zones LAN.

3 Cliquez sur l'objet Zone LAN pour lequel vous souhaitez créer une règle WAN, puis cliquez sur Créer une règle.

4 Spécifiez un nom pour cette règle, puis cliquez sur OK.

Il doit s'agir d'un nom distinctif complet.

5 Saisissez les informations nécessaires dans la zone de texte Règle.

Pour obtenir une présentation de la structure d'une règle WAN, reportez-vous à la section « Structure d'une règle WAN », page 313.

Pour obtenir une présentation de la syntaxe d'une règle WAN, reportez-vous à la section « Blocs utilisés au sein de sections de règles », page 316.

6 Cliquez sur Appliquer, puis sur OK.

Limitation du trafic WAN

Le gestionnaire de trafic WAN est fourni avec deux groupes de règles WAN prédéfinies qui autorisent le trafic uniquement à certaines heures. (Pour plus d'informations, reportez-vous aux sections « 1-3am.wmg », page 299 et « 7am-6pm.wmg », page 299). Vous pouvez modifier ces règles afin de limiter le trafic à une plage horaire de votre choix.

Les instructions suivantes permettent de modifier le groupe qui autorise le trafic uniquement entre 1h00 et 3h00 du matin. Il vous suffit d'effectuer ces mêmes opérations pour modifier le groupe qui autorise le trafic uniquement entre 7h00 et 18h00.

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur Trafic WAN > Présentation du gestionnaire de trafic WAN.

3 Cliquez sur Afficher les zones LAN, puis sur l'objet Zone LAN souhaité.

ou

Cliquez sur Afficher les serveurs NCP, puis sur un objet Serveur NCP.

4 Cliquez sur Ajouter une règle.

5 Sélectionnez le fichier 1-3am.wmg dans la liste des règles prédéfinies, puis cliquez deux fois sur OK.

La règle apparaît dans la zone de texte Règle, dans laquelle vous pouvez effectuer vos modifications. Par exemple, si vous souhaitez que le trafic ne soit autorisé qu'entre 2h00 et 17h00 (et non entre 1h00 et 3h00), procédez comme suit :

```
/* Cette règle autorise le trafic uniquement entre 2h00 et 17h00 */
LOCAL BOOLEAN Selected;
SELECTOR
  Selected := Now.hour >= 2 AND Now.hour < 17;
  IF Selected THEN
    RETURN 50; /* entre 2h00 et 17h00 cette règle a une
 priorité élevée */
  ELSE
    RETURN 1;  /* renvoie 1 au lieu de 0 s'il n'y a
 aucune règle */
               /* si aucune règle ne renvoie > 0, WanMan présuppose
 SEND */
  END
END
PROVIDER
  IF Selected THEN
    RETURN SEND; /* entre 2h00 et 17h00, SEND */
  ELSE
    RETURN DONT_SEND; /* autres horaires, pas de */
  END
END
```

Dans les lignes de commentaires (comprises entre /* et */), vous pouvez indiquer l'heure en spécifiant s'il s'agit du matin (a.m) ou de l'après-midi (p.m). Cependant, dans le code actif, vous devez utiliser le format 24heures. Dans ce cas, 5h00 p.m. devient 17.

Pour obtenir une présentation de la structure d'une règle WAN, reportez-vous à la section « Structure d'une règle WAN », page 313.

Pour obtenir une présentation de la syntaxe d'une règle WAN, reportez-vous à la section « Blocs utilisés au sein de sections de règles », page 316.

6 Après avoir modifié la syntaxe de la règle, cliquez sur Vérifier une règle pour identifier les erreurs de syntaxe ou de structure.

Les résultats de la vérification de la règle s'affichent.

Le gestionnaire de trafic WAN n'exécute pas les règles contenant des erreurs.

7 Si vous souhaitez conserver la règle initiale 1-3am, ajoutez la nouvelle règle sous un nom différent.

7a Cliquez sur Renommer une règle.

7b Attribuez un nom à la règle modifiée, puis cliquez sur OK.

8 Cliquez sur Appliquer, puis sur OK.

Assignation de facteurs de coût

Les facteurs de coût permettent au gestionnaire de trafic WAN de comparer le coût du trafic pour certaines destinations, puis de gérer le trafic à l'aide des règles WAN. Les règles WAN utilisent les facteurs de coût pour déterminer les dépenses relatives du trafic WAN. Vous pouvez ensuite utiliser ces informations pour décider de l'envoi du trafic.

Un facteur de coût est exprimé en termes de dépenses par unité de temps. Vous pouvez utiliser l'unité de votre choix à condition que ce soit la même dans chaque règle de trafic WAN. Vous pouvez, par

conséquent, exprimer la valeur en dollars par heure, en centimes par minute, en yens par seconde ou utiliser n'importe quel autre rapport dépense/temps, à condition de n'utiliser que ce rapport.

Vous pouvez assigner à des plages d'adresses particulières des facteurs de coût cible représentant les dépenses relatives du trafic. Par conséquent, vous pouvez assigner un coût à un groupe complet de serveurs dans une seule déclaration. Vous pouvez également assigner un facteur de coût par défaut, à utiliser lorsque aucun coût n'est indiqué pour une destination.

Si aucun coût n'est assigné à la destination, le coût par défaut est utilisé. Si aucun coût par défaut pour le serveur ou l'objet Zone LAN n'a été spécifié, la valeur -1 est utilisée.

Pour plus d'informations sur les règles limitant le trafic en fonction des facteurs de coût, reportez-vous à la section « Costlt20.wmg », page 299.

Pour plus d'informations sur la procédure de modification d'une règle, reportez-vous à la section « Modification des règles WAN », page 294.

Assignation de facteurs de coût par défaut

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Gestion du trafic WAN > Présentation du gestionnaire de trafic WAN.
3. Cliquez sur Afficher les zones LAN, puis sur l'objet Zone LAN souhaité.

   ou

   Cliquez sur Afficher les serveurs NCP, puis sur un objet Serveur NCP.
4. Cliquez sur Coûts, puis saisissez un coût dans le champ Coût par défaut.

   Le coût doit être un nombre entier non négatif. S'il est défini, le coût par défaut est assigné à toutes les destinations de l'objet Serveur ou Zone LAN, sauf si elles figurent dans l'une des plages d'adresses associées à un coût. Par exemple, vous pouvez indiquer le coût en unité monétaire, par exemple en dollars, ou en nombre de paquets par seconde.
5. Cliquez sur Appliquer, puis sur OK.

Assignation d'un coût à une plage d'adresses cible

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Gestion du trafic WAN > Présentation du gestionnaire de trafic WAN.
3. Cliquez sur Afficher les zones LAN, puis sur l'objet Zone LAN souhaité.

   ou

   Cliquez sur Afficher les serveurs NCP, puis sur un objet Serveur NCP.
4. Cliquez sur Coûts.
5. Cliquez sur le bouton Ajouter  .
6. Dans la fenêtre Créer un coût Wanman, sélectionnez Type d'adresse TCP/IP ou Type d'adresse IPX.
7. Indiquez les adresses de début et de fin de la plage, au format approprié pour les protocoles TCP/IP ou IPX.
8. Dans le champ de texte Coût, spécifiez un nombre entier non négatif.
9. Cliquez sur OK, puis sur Appliquer et enfin sur OK.

Groupes de règles du gestionnaire de trafic WAN

Le gestionnaire de trafic WAN est fourni avec les groupes de règles prédéfinies suivants.

Pour plus d'informations sur l'application des groupes de règles, reportez-vous à la section « Application des règles WAN », page 293.

1-3am.wmg

Les règles de ce groupe autorisent l'envoi du trafic uniquement entre 1h00 et 3h00 du matin. Il existe deux règles :

- 1 - 3 am, NA

  Limite la vérification des liens en amont, des références externes et des restrictions de login, l'exécution du nettoyeur ou du contrôleur de connectivité et la synchronisation du schéma aux heures définies.

- 1 - 3 am

  Autorise tout autre trafic uniquement à ces heures.

Pour limiter l'ensemble du trafic à ces heures, les deux règles doivent être appliquées.

7am-6pm.wmg

Les règles de ce groupe autorisent l'envoi du trafic uniquement entre 7h00 et 18h00. Il existe deux règles :

- 7 am - 6 pm, NA

  Limite la vérification des liens en amont, des références externes et des restrictions de login, l'exécution du nettoyeur ou du contrôleur de connectivité et la synchronisation du schéma aux heures définies.

- 7 am - 6 pm

  Autorise tout autre trafic uniquement à ces heures.

Pour limiter l'ensemble du trafic à ces heures, les deux règles doivent être appliquées.

CostIt20.wmg

Les règles de ce groupe autorisent uniquement l'envoi du trafic dont le facteur de coût est inférieur à 20. Il existe deux règles :

- Cost < 20, NA

  Permet uniquement de vérifier les liens en amont, les références externes et les restrictions de login, d'exécuter le nettoyeur ou le contrôleur de connectivité et de synchroniser le schéma si le facteur de coût est inférieur à 20.

- Cost < 20

  Interdit tout autre trafic à moins que le facteur de coût ne soit inférieur à 20.

Pour interdire tout trafic pour lequel le facteur de coût est égal ou supérieur à 20, les deux règles doivent être appliquées.

Ipx.wmg

Les règles de ce groupe n'autorisent que le trafic IPX. Il existe deux règles :

- IPX, NA

  Permet uniquement de vérifier les liens en amont, les références externes et les restrictions de login, d'exécuter le nettoyeur ou le contrôleur de connectivité et de synchroniser le schéma si le trafic généré est de type IPX.

- IPX

  Interdit tout autre trafic, sauf s'il s'agit d'un trafic IPX.

Pour interdire tous les trafics non IPX, les deux règles doivent être appliquées.

Ndsttyps.wmg

Les règles de ce groupe sont des exemples applicables à plusieurs types de trafic eDirectory. Elles contiennent les variables que eDirectory transmet dans une requête de ce type.

- « Exemple de règle: Catch All with Addresses », page 300
- « Exemple de règle: Catch All without Addresses », page 300
- « Exemple de règle: NDS_BACKLINK_OPEN », page 300
- « Exemple de règle: NDS_BACKLINKS », page 301
- « Exemple de règle: NDS_CHECK_LOGIN_RESTRICTION », page 303
- « Exemple de règle: NDS_CHECK_LOGIN_RESTRICTION_OPEN », page 304
- « Exemple de règle: NDS_JANITOR », page 305
- « Exemple de règle: NDS_JANITOR_OPEN », page 306
- « Exemple de règle: NDS_LIMBER », page 307
- « Exemple de règle: NDS_LIMBER_OPEN », page 308
- « Exemple de règle: NDS_SCHEMA_SYNC », page 309
- « Exemple de règle: NDS_SCHEMA_SYNC_OPEN », page 310
- « Exemple de règle: NDS_SYNC », page 311

Exemple de règle: Catch All with Addresses

Exemple de règle conçu pour les types de trafic avec adresses.

Exemple de règle: Catch All without Addresses

Exemple de règle conçu pour les types de trafic sans adresses.

Exemple de règle: NDS_BACKLINK_OPEN

NDS_BACKLINK_OPEN est un type de trafic utilisé uniquement si la valeur 1 a été assignée à CheckEachNewOpenConnection ou à CheckEachAlreadyOpenConnection lors de la requête NDS_BACKLINKS correspondante.

Cette requête est générée chaque fois que CheckEachNewOpenConnection correspond à 1 et que eDirectory doit ouvrir une nouvelle connexion pour l'établissement de liens en amont ou que CheckEachAlreadyOpenConnection correspond à 1 et que eDirectory doit réutiliser une connexion existante.

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Entrée et Sortie, type INTEGER)

  Si ConnectionIsAlreadyOpen correspond à TRUE (vrai), le système assigne à ExpirationInterval la valeur de l'intervalle d'expiration déjà définie pour la connexion existante. Sinon, cette variable reçoit la valeur ExpirationInterval assignée dans la requête NDS_BACKLINKS. Le paramètre 0 indique que la valeur par défaut (2 heures) doit être utilisée. À la fin de la procédure, la valeur de cette variable est assignée en tant qu'intervalle d'expiration de la connexion.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- ConnectionIsAlreadyOpen (Entrée uniquement, type BOOLEAN)

  Cette variable correspond à TRUE si eDirectory peut réutiliser une connexion existante et à FALSE s'il doit en créer une.

Valeur	Description
TRUE	eDirectory détecte qu'une connexion existe déjà pour cette adresse et peut la réutiliser.
FALSE	eDirectory n'a pas de connexion pour cette adresse et doit en créer une.

- ConnectionLastUsed (Entrée uniquement, type TIME)

  Si ConnectionIsAlreadyOpen correspond à TRUE, alors ConnectionLastUsed indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion. Sinon, la valeur correspond à 0.

Valeur	Description
TRUE	*ConnectionLastUsed* indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion.
FALSE	*ConnectionLastUsed* correspond à 0.

Exemple de règle: NDS_BACKLINKS

Avant de contrôler un lien en amont ou une référence externe, eDirectory interroge le gestionnaire de trafic WAN pour vérifier si le moment est propice à cette activité. NDS_BACKLINKS ne comportant pas d'adresse cible,une règle NO_ADDRESSES est requise. Si le gestionnaire de trafic WAN retourne DONT_SEND, la vérification du lien en amont est ajournée et reprogrammée. Les variables suivantes sont fournies :

- Last (Entrée uniquement, type TIME)

  Heure du dernier cycle de vérification des liens en amont depuis le démarrage de eDirectory. Au démarrage de eDirectory, la valeur *Last* correspond à 0. Si NDS_BACKLINKS renvoie SEND, cette valeur correspond à l'heure actuelle une fois que eDirectory a terminé le processus de liaison en amont.

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Sortie uniquement, type INTEGER)

  Intervalle d'expiration de toutes les connexions créées lors de l'établissement de liens en amont.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- Next (Sortie uniquement, type TIME)

  Indique à quel moment eDirectory doit programmer le prochain cycle de vérification des liens en amont.

Valeur	Description
In past, 0	Utilise la planification par défaut.
In future	Heure de planification du processus de liaison en amont.

- CheckEachNewOpenConnection (Sortie uniquement, type INTEGER)

  Indique à eDirectory la procédure à suivre si une connexion doit être créée au cours du processus de liaison en amont.

  CheckEachNewOpenConnection correspond à 0.

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

- CheckEachAlreadyOpenConnection (Sortie uniquement, type INTEGER)

  Indique à eDirectory la procédure à suivre si une connexion considérée comme déjà ouverte doit être réutilisée au cours du processus de liaison en amont. CheckEachAlreadyOpenConnection correspond à 0.

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

Exemple de règle: NDS_CHECK_LOGIN_RESTRICTION

Avant de vérifier une restriction de login, eDirectory interroge le gestionnaire de trafic WAN pour vérifier si le moment est propice à cette activité. Le type de trafic NDS_CHECK_LOGIN_RESTRICTIONS ne comportant pas d'adresse cible,une règle NO_ADDRESSES est requise. Si le gestionnaire de trafic WAN renvoie DONT_SEND, la vérification est annulée.

Les variables suivantessont fournies :

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- Result (Sortie uniquement, type INTEGER)

  Si le résultat de NDS_CHECK_LOGIN_RESTRICTIONS est DONT_SEND, les valeurs suivantes sont renvoyées au système d'exploitation.

Valeur	Description
0	Le login est autorisé.
1	Le login n'est pas autorisé pendant l'intervalle de temps actuel.
2	Le compte est désactivé ou a expiré.
3	Le compte a été supprimé.

- ExpirationInterval (Sortie uniquement, type INTEGER)

  Intervalle d'expiration devant être assigné à cette connexion.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- CheckEachNewOpenConnection (Sortie uniquement, type INTEGER)

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

- CheckEachAlreadyOpenConnection (Sortie uniquement, type INTEGER)

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

Exemple de règle: NDS_CHECK_LOGIN_RESTRICTION_OPEN

La règle NDS_CHECK_LOGIN_RESTRICTION_OPEN n'est utilisée que si la valeur 1 a été assignée à CheckEachNewOpenConnection ou à CheckEachAlreadyOpenConnection lors de la requête NDS_CHECK_LOGIN_RESTRICTIONS correspondante. Cette requête est générée chaque fois que CheckEachNewOpenConnection correspond à 1 et que eDirectory doit

- ouvrir une nouvelle connexion avant de lancer le contrôleur de connectivité ;
- ouvrir une nouvelle connexion avant de contrôler la restriction de login ;
- réutiliser une connexion existante.

Les variables suivantessont fournies :

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Entrée et Sortie, type INTEGER)

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- ConnectionIsAlreadyOpen (Entrée uniquement, type BOOLEAN)

Valeur	Description
TRUE	eDirectory détecte qu'une connexion existe déjà pour cette adresse et peut la réutiliser.
FALSE	eDirectory n'a pas de connexion pour cette adresse et doit en créer une.

- ConnectionLastUsed (Entrée uniquement, type TIME)

  Si ConnectionIsAlreadyOpen correspond à TRUE, alors ConnectionLastUsed indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion. Sinon, elle correspond à 0.

Valeur	Description
TRUE	*ConnectionLastUsed* indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion.
FALSE	*ConnectionLastUsed* correspond à 0.

Exemple de règle: NDS_JANITOR

Avant d'exécuter le nettoyeur, eDirectory interroge le gestionnaire de trafic WAN pour vérifier si le moment est propice à cette activité. NDS_JANITOR ne comportant pas d'adresse cible, une règle NO_ADDRESSES est requise. Si le gestionnaire de trafic WAN renvoie DONT_SEND, l'exécution du nettoyeur est ajournée et reprogrammée.

Les variables suivantessont fournies :

- Last (Entrée uniquement, type TIME)

  Heure du dernier cycle de nettoyage depuis le démarrage de eDirectory. Au démarrage de eDirectory, la valeur *Last* correspond à 0. Si NDS_JANITOR renvoie SEND, cette valeur est égale à l'heure actuelle une fois que eDirectory a terminé le nettoyage.

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Sortie uniquement, type INTEGER)

  Intervalle d'expiration de toutes les connexions créées lors de l'exécution du nettoyeur.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- Next (Sortie uniquement, type TIME)

  Indique à quel moment eDirectory doit planifier le prochain cycle de nettoyage.

Valeur	Description
In the past, 0	Utilise la planification par défaut.
In the future	Heure de planification du processus de nettoyage.

- CheckEachNewOpenConnection (Sortie uniquement, type INTEGER)

  Indique à eDirectory la procédure à suivre si une connexion doit être créée au cours du processus de nettoyage.

  CheckEachNewOpenConnection correspond à 0.

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

- CheckEachAlreadyOpenConnection (Sortie uniquement, type INTEGER)

  Indique à eDirectory la procédure à suivre si une connexion considérée comme déjà ouverte doit être réutilisée au cours du processus de nettoyage.

  CheckEachAlreadyOpenConnection correspond à 0.

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

Exemple de règle: NDS_JANITOR_OPEN

La règle NDS_JANITOR_OPEN n'est utilisée que si la valeur 1 a été assignée à CheckEachNewOpenConnection ou à CheckEachAlreadyOpenConnection lors de la requête NDS_JANITOR correspondante. Cette requête est générée chaque fois que CheckEachNewOpenConnection correspond à 1 et que eDirectory doit ouvrir une nouvelle connexion pour l'établissement de liens en amont ou que CheckEachAlreadyOpenConnection correspond à 1 et que eDirectory doit réutiliser une connexion existante.

Les variables suivantessont fournies :

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Entrée et Sortie, INTEGER)

  Si ConnectionIsAlreadyOpen correspond à TRUE (vrai), le système assigne à ExpirationInterval la valeur de l'intervalle d'expiration déjà définie pour la connexion existante. Sinon, cette variable reçoit la valeur ExpirationInterval assignée dans la requête NDS_JANITOR. Le paramètre 0 indique que la valeur par défaut (2heures, 10secondes) doit être utilisée. À la fin de la procédure, la valeur de cette variable est assignée en tant qu'intervalle d'expiration de la connexion.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- ConnectionIsAlreadyOpen (Entrée uniquement, type BOOLEAN)

  Cette variable correspond à TRUE si eDirectory doit réutiliser une connexion existante et à FALSE s'il doit en créer une.

Valeur	Description
TRUE	eDirectory détecte qu'une connexion existe déjà pour cette adresse et peut la réutiliser.
FALSE	eDirectory n'a pas de connexion pour cette adresse et doit en créer une.

- ConnectionLastUsed (Entrée uniquement, type TIME)

  Si ConnectionIsAlreadyOpen correspond à TRUE, alors ConnectionLastUsed indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion. Sinon, elle correspond à 0.

Valeur	Description
TRUE	ConnectionLastUsed indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion.
FALSE	ConnectionLastUsed correspond à 0.

Exemple de règle: NDS_LIMBER

Avant d'exécuter le contrôleur de connectivité, eDirectory interroge le gestionnaire de trafic WAN pour vérifier si le moment est propice à cette activité. Le type de trafic NDS_LIMBER ne comportant pas d'adresse cible, une règle NO_ADDRESSES est requise. Si le gestionnaire de trafic WAN renvoie DONT_SEND, l'exécution du contrôleur de connectivité est ajournée et reprogrammée.

Les variables suivantessont fournies :

- Last (Entrée uniquement, type TIME)

  Heure du dernier contrôle de connectivité depuis le démarrage de eDirectory.

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Sortie uniquement, type INTEGER)

  Intervalle d'expiration de toutes les connexions créées lors de l'exécution des contrôles de connectivité.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- CheckEachNewOpenConnection (Sortie uniquement, type INTEGER)

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

- CheckEachAlreadyOpenConnection (Sortie uniquement, type INTEGER)

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

- Next (Sortie uniquement, type TIME)

  Heure du prochain cycle de contrôle de la connectivité. Si cette valeur n'est pas définie, NDS_LIMBER utilise la valeur par défaut.

Exemple de règle: NDS_LIMBER_OPEN

La règle NDS_LIMBER_OPEN n'est utilisée que si la valeur 1 a été assignée à CheckEachNewOpenConnection ou à CheckEachAlreadyOpenConnection lors de la requête NDS_LIMBER correspondante. Cette requête est générée chaque fois que CheckEachNewOpenConnection correspond à 1 et que eDirectory doit ouvrir une nouvelle connexion avant l'exécution du processus de contrôle de la connectivité. Cette requête est générée chaque fois que CheckEachNewOpenConnection correspond à 1 et que eDirectory doit ouvrir une nouvelle connexion avant la synchronisation du schéma ou que CheckEachAlreadyOpenConnection correspond à 1 et que eDirectory doit réutiliser une connexion existante.

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Entrée et Sortie, type INTEGER)

  Intervalle d'expiration devant être assigné à cette connexion.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- ConnectionIsAlreadyOpen (Entrée uniquement, BOOLEAN)

Valeur	Description
TRUE	eDirectory détecte qu'une connexion existe déjà pour cette adresse et peut la réutiliser.
FALSE	eDirectory n'a pas de connexion pour cette adresse et doit en créer une.

- ConnectionLastUsed (Entrée uniquement, type TIME)

  Si ConnectionIsAlreadyOpen correspond à TRUE, alors ConnectionLastUsed indique la dernière instance d'un envoi de paquet par DS via cette connexion. Sinon, la valeur correspond à 0.

Valeur	Description
TRUE	ConnectionLastUsed indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion.
FALSE	ConnectionLastUsed correspond à 0.

Exemple de règle: NDS_SCHEMA_SYNC

Avant de synchroniser le schéma, eDirectory interroge le gestionnaire de trafic WAN pour vérifier si le moment est propice à cette activité. Le type de trafic NDS_SCHEMA_SYNC ne comportant pas d'adresse cible,une règle NO_ADDRESSES est requise. Si le gestionnaire de trafic WAN renvoie DONT_SEND, la synchronisation du schéma est ajournée et reprogrammée.

Les variables suivantessont fournies:

- Last (Entrée uniquement, type TIME)

  Heure de la dernière synchronisation de schéma réussie pour l'ensemble des serveurs.

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Sortie uniquement, type INTEGER)

  Intervalle d'expiration de toutes les connexions créées lors de la synchronisation du schéma.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- CheckEachNewOpenConnection (Sortie uniquement, type INTEGER)

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

- CheckEachAlreadyOpenConnection (Sortie uniquement, type INTEGER)

Valeur	Description
0	Renvoie un message de réussite sans appeler le gestionnaire de trafic WAN, ce qui permet à la connexion de se poursuivre normalement (valeur par défaut).
1	Appelle le gestionnaire de trafic WAN et permet aux règles d'autoriser ou non la connexion.
2	Renvoie ERR_CONNECTION_DENIED sans appeler le gestionnaire de trafic WAN et provoque l'interruption de la connexion.

Exemple de règle: NDS_SCHEMA_SYNC_OPEN

La règle NDS_SCHEMA_SYNC_OPEN n'est utilisée que si la valeur 1 a été assignée à CheckEachNewOpenConnection ou à CheckEachAlreadyOpenConnection lors de la requête NDS_SCHEMA_SYNC correspondante. Cette requête est générée chaque fois que CheckEachNewOpenConnection correspond à 1 et que eDirectory doit ouvrir une nouvelle connexion avant la synchronisation du schéma ou que CheckEachAlreadyOpenConnection correspond à 1 et que eDirectory doit réutiliser une connexion existante.

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Entrée et Sortie, INTEGER)

  Intervalle d'expiration devant être assigné à cette connexion.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

- ConnectionIsAlreadyOpen (Entrée uniquement, BOOLEAN)

Valeur	Description
TRUE	eDirectory détecte qu'une connexion existe déjà pour cette adresse et peut la réutiliser.
FALSE	eDirectory n'a pas de connexion pour cette adresse et doit en créer une.

- ConnectionLastUsed (Entrée uniquement, type TIME)

  Si ConnectionIsAlreadyOpen correspond à TRUE, alors ConnectionLastUsed indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion. Sinon, la valeur correspond à 0.

Valeur	Description
TRUE	*ConnectionLastUsed* indique la dernière instance d'un envoi de paquet par eDirectory via cette connexion.
FALSE	*ConnectionLastUsed* correspond à 0.

Exemple de règle: NDS_SYNC

Chaque fois que eDirectory doit synchroniser une réplique, il soumet une requête au gestionnaire de trafic WAN à l'aide du type de trafic NDS_SYNC. Les variables suivantes sont fournies par eDirectory. Elles sont destinées à être utilisées dans les règles WAN.

- Last (Entrée uniquement, type TIME)

  Heure de la dernière synchronisation réussie pour cette réplique.

- Version (Entrée uniquement, type INTEGER)

  Version de eDirectory.

- ExpirationInterval (Sortie uniquement, type INTEGER)

  Intervalle d'expiration de la connexion au serveur contenant la réplique mise à jour.

Valeur	Description
<0, 0	Utilise l'intervalle d'expiration par défaut (valeur par défaut).
>0	Intervalle d'expiration devant être assigné à cette connexion.

Onospoof.wmg

Les règles de ce groupe autorisent uniquement l'utilisation des connexions WAN existantes. Il existe deux règles :

- Already Open, No Spoofing, NA

  Permet de vérifier les liens en amont, les références externes et les restrictions de login, d'exécuter le nettoyeur ou le contrôleur de connectivité et de synchroniser le schéma uniquement sur les connexions WAN existantes.

- Already Open, No Spoofing

  Interdit tout autre trafic sur les connexions WAN existantes.

Pour interdire tout trafic sur les connexions existantes, les deux règles doivent être appliquées.

Opnspoof.wmg

Les règles de ce groupe autorisent uniquement l'utilisation des connexions WAN existantes. Elles considèrent toutefois qu'une connexion inutilisée pendant 15minutes fait l'objet d'une usurpation et ne doit par conséquent pas être utilisée. Il existe deux règles :

- Already Open, Spoofing, NA

  Cette règle permet de vérifier les liens en amont, les références externes et les restrictions de login, d'exécuter le nettoyeur ou le contrôleur de connectivité et de synchroniser le schéma uniquement sur les connexions WAN existantes ouvertes depuis moins de 15 minutes.

- Already Open, Spoofing

  Cette règle empêche tout autre trafic sur les connexions WAN existantes ouvertes depuis moins de 15 minutes.

Pour interdire tout trafic sur les connexions existantes ouvertes depuis moins de 15 minutes, les deux règles doivent être appliquées.

Samearea.wmg

Les règles de ce groupe autorisent le trafic uniquement dans la même zone réseau. Une zone réseau est déterminée par la section réseau d'une adresse. Le gestionnaire de trafic Wan considère que l'adresse TCP/IP est une adresse de classe C (c'est-à-dire que ses trois premières sections sont dans la même zone réseau). Dans une adresse IPX, toutes les adresses avec une portion de réseau identique sont considérées comme appartenant à la même zone réseau. Il existe trois règles :

- Same Network Area, NA

  Permet uniquement de vérifier les liens en amont, les références externes et les restrictions de login, d'exécuter le nettoyeur ou le contrôleur de connectivité et de synchroniser le schéma si le trafic est généré dans la même zone réseau.

- Same Network Area, TCPIP

  Autorise le trafic TCP/IP uniquement si le trafic est généré dans la même zone réseau TCP/IP.

- Same Network Area, IXP

  Autorise le trafic IPX uniquement si le trafic est généré dans la même zone réseau IPX.

Tcpip.wmg

Les règles de ce groupe autorisent uniquement le trafic TCP/IP. Il existe deux règles :

- TCPIP, NA

  Permet uniquement de vérifier les liens en amont, les références externes et les restrictions de login, d'exécuter le nettoyeur ou le contrôleur de connectivité et de synchroniser le schéma si le trafic généré est de type TCP/IP.

- TCPIP

  Interdit tout autre trafic, sauf s'il s'agit d'un trafic TCP/IP.

Pour interdire tous les trafics non TCP/IP, les deux règles doivent être appliquées.

Timecost.wmg

Les règles de ce groupe autorisent tout trafic uniquement entre 1h00 et 1h30 du matin, les serveurs situés à un même emplacement pouvant continuer à communiquer librement. Ce groupe utilise les règles suivantes qui doivent toutes être appliquées:

- COSTLT20

  Le trafic d'adresses et le paramètre NA ont une priorité de 40.

- Disallow Everything

  Interdit tout envoi de trafic. Si le gestionnaire de trafic WAN ne trouve aucune (0) règle alors que le sélecteur a renvoyé une valeur supérieure à 0, il prend par défaut la valeur SEND. Cette règle empêche cette situation.

- NDS Synchronization

  Autorise le trafic NDS_SYNC uniquement entre 1h00 et 1h30 du matin.

- Start Rest. Procs, NA.

  Autorise le démarrage à tout instant de l'ensemble des processus, mais le gestionnaire de trafic WAN doit être consulté pour chaque appel *_OPEN. Planifie l'exécution de ce processus quatre fois par jour, à 1h00, 7h00, 13h00 et 19h00.

- Start Unrest. Procs 1-1:30, NA

  Autorise le démarrage de tous les processus entre 1h00 et 1h30 du matin. Ils sont exécutés totalement sans envoi de requête supplémentaire au gestionnaire de trafic WAN. Les processus sont exécutés quatre fois par jour, toutes les six heures. Le processus qui a lieu à 1h00 est géré par cette règle, les autres par Start Rest. Procs, NA.

Structure d'une règle WAN

Une règle WAN se compose des trois sections suivantes :

- « Section de déclaration », page 313
- « Section du sélecteur », page 315
- « Section du fournisseur », page 316

Section de déclaration

La section de déclaration d'une règle contient les définitions des variables locales et de celles qui proviennent d'une requête client. Ces définitions sont utilisées dans les sections du sélecteur et du fournisseur. Ces variables sont stockées avec les variables système.

Les déclarations de variables sont séparées par des points-virgules (;). Vous pouvez combiner sur une même ligne plusieurs déclarations pour le même type ou passer à la ligne suivante ; le nombre de lignes est indifférent. Vous trouverez ci-dessous un exemple de section de déclaration :

```
REQUIRED INT R1;
REQUIRED TIME R2;
REQUIRED BOOLEAN R3,R4;
REQUIRED NETADDRESS R5,R6;
OPTIONAL INT P1 := 10;
OPTIONAL BOOLEAN := FALSE;
LOCAL INT L1 :=10;
LOCAL INT L2;
```

```
LOCAL TIME L3;
LOCAL BOOLEAN L4 :=TRUE, L5 :=FALSE;
LOCAL NETADDRESS L6;
```

Chaque type de trafic dispose de ses propres déclarations obligatoires et facultatives. Les règles qui ne comportent pas les variables obligatoires ne fonctionnent pas. Les déclarations facultatives doivent comporter une valeur qui sera utilisée comme valeur par défaut si aucune autre valeur n'est entrée. Le gestionnaire de trafic WAN fournit des symboles système (variables prédéfinies) à utiliser avec tous les types de trafic.

Chaque déclaration se compose de trois parties :

- Étendue
- Type
- Liste des paires nom/valeur facultative

Étendue

Les étendues valides sont présentées dans le tableau suivant.

Étendue	Description
REQUIRED	Les variables dont l'étendue est REQUIRED peuvent être utilisées dans plusieurs sections, mais elles ne peuvent apparaître qu'une fois dans la section de déclaration. Aucune valeur ne peut être définie pour une variable d'étendue REQUIRED. Sa valeur doit être issue de la requête GetWanPolicy.
OPTIONAL	Les variables dont l'étendue est OPTIONAL peuvent être utilisées dans plusieurs sections d'une règle, mais elles ne peuvent apparaître qu'une fois dans la section de déclaration. Les variables d'étendue OPTIONAL sont assignées à une valeur par défaut. Ces valeurs ne sont pas initialisées. Elles sont définies uniquement si aucune valeur n'est transmise. Si la requête de règle WAN ne fournit pas de nouvelle valeur au paramètre qui correspond au nom et au type, la valeur définie dans la déclaration est utilisée lors du traitement de la règle. Vous devez assigner une valeur aux variables dont l'étendue est OPTIONAL. Par conséquent, étant donné que les types TIME et NETADDRESS ne peuvent pas être initialisés dans la section de déclaration, n'utilisez pas une étendue OPTIONAL avec ces types de variables.
LOCAL	Les variables dont l'étendue est LOCAL peuvent être utilisées dans plusieurs sections, mais elles ne peuvent apparaître qu'une fois dans la section de déclaration. Les variables d'étendue LOCAL existent seulement pour une règle particulière : leurs valeurs ne sont pas renvoyées au client appelant. Tous les types de paramètres peuvent être définis. Toutefois, étant donné que les types TIME et NETADDRESS ne peuvent pas être initialisés dans la section de déclaration, ne leur assignez pas de valeur.
SYSTEM	Les variables dont l'étendue est SYSTEM peuvent être utilisées dans plusieurs sections, mais elles ne peuvent apparaître qu'une fois dans la section de déclaration.

Type

Les types valides sont présentés dans le tableau suivant.

Type	Description
INT	Représente le type de trafic de la requête GetWanPolicy pour laquelle la règle est exécutée. Par exemple, la règle suivante définit le type de trafic NDS_SYNC : IF TrafficType=NDS_SYNC THEN action END.
BOOLEAN	Utilisé pour les valeurs TRUE ou FALSE uniquement. La valeur sera indéterminée si elle n'est pas spécifiée dans une déclaration ou dans une requête de règle WAN.
TIME	Les variables d'étendue TIME doivent se voir attribuer leurs valeurs dans les sections du sélecteur ou du fournisseur, ou à partir de la requête de règle WAN. N'assignez pas de valeur aux variables d'étendue TIME dans la section de déclaration.
NETADDRESS	Les variables d'étendue NETADDRESS doivent se voir attribuer leurs valeurs dans les sections du sélecteur ou du fournisseur. N'assignez pas de valeur aux variables d'étendue NETADDRESS dans la section de déclaration.

Vous ne pouvez pas assigner de valeurs aux types Time et Netaddress dans la section de déclaration. Si ces types ne sont associés à aucune valeur, ils en reçoivent dans les sections du sélecteur ou du fournisseur. Seuls les types uniques sont initialisés dans la section de déclaration.

Paires nom/valeur facultative

Les noms de variables sont des chaînes sans limitation de longueur contenant des combinaisons de caractères alphanumériques. Étant donné que seuls les 31 premiers caractères sont utilisés, une variable doit commencer par une chaîne unique comprenant 31 caractères. Un nom de variable doit commencer par un caractère alphabétique, sinon le symbole est interprété en tant que constante numérique.

Les noms de variables tiennent compte de la casse. Par exemple, la variable *R1* est différente de la variable *r1*. Le caractère de soulignement (_) est autorisé dans les noms de variables.

Les valeurs d'une déclaration doivent être des constantes plutôt que des variables ou des expressions. Par conséquent, la déclaration `LOCAL INT L2:= L3;` n'est pas autorisée. Une valeur d'initialisation de variable dans la section de déclaration peut être modifiée dans les sections du sélecteur et du fournisseur de la règle.

Section du sélecteur

La section du sélecteur d'une règle commence par le mot-clé SELECTOR et se termine par le mot-clé END. Les sections du sélecteur sont évaluées afin de déterminer la règle chargée à utiliser.

Les sections du sélecteur de toutes les règles actuellement chargées sont exécutées afin d'identifier la règle prioritaire. Lors de cette évaluation, la section renvoie une priorité comprise entre 0 et 100. Une priorité 0 signifie que la règle ne doit pas être utilisée. Une priorité comprise entre 1 et 99 signifie que la règle est utilisée si aucune autre règle ne présente une valeur supérieure. Enfin, une priorité 100 signifie que la règle doit impérativement être utilisée.

Le résultat d'une section du sélecteur est indiqué dans une déclaration RETURN. Si aucune déclaration RETURN n'est générée, le système renvoie par défaut une valeur nulle. Voici un exemple de section du sélecteur :

```
SELECTOR
RETURN 49;
END
```

Lorsque les sections du sélecteur de différentes règles sont évaluées, plusieurs règles peuvent renvoyer la même valeur. Dans ce cas, il est impossible de déterminer la règle sélectionnée. Lorsque aucun autre élément ne les distingue, une règle de serveur est prioritaire par rapport à une règle WAN.

Pour plus d'informations sur la rédaction des déclarations, reportez-vous à la section « Blocs utilisés au sein de sections de règles », page 316. Reportez-vous également à la section « Section du fournisseur », page 316.

Section du fournisseur

La section du fournisseur commence par le mot-clé PROVIDER et se termine par le mot-clé END. La liste des déclarations constitue le corps de la section du fournisseur.

Cette liste de déclarations doit générer une valeur indiquant l'action suggérée pour la règle (SEND ou DONT_SEND).

Les résultats d'une section du fournisseur sont fournis dans une déclaration RETURN. Si aucune déclaration RETURN n'est générée, la valeur par défaut SEND est renvoyée.

Vous trouverez ci-dessous un exemple de section du fournisseur :

```
PROVIDER
RETURN SEND;
END
```

Pour plus d'informations sur la rédaction des déclarations, reportez-vous à la section « Blocs utilisés au sein de sections de règles », page 316.

Blocs utilisés au sein de sections de règles

Sauf indication contraire, les instructions et blocs suivants peuvent être utilisés dans les sections du sélecteur et du fournisseur d'une règle WAN. Pour plus d'informations sur la procédure à suivre pour créer la section de déclaration d'une règle, reportez-vous à la section « Section de déclaration », page 313.

Commentaires

Vous pouvez signaler les commentaires en plaçant les signes /* et */ respectivement en début et en fin de ligne. Par exemple :

```
/* Ceci est un commentaire. */
```

Vous pouvez également les signaler en insérant les symboles // à la fin d'une ligne, juste avant les commentaires. Par exemple :

```
IF L2> L3 THEN //Ceci est un commentaire.
```

Instruction IF-THEN

Les instructions IF-THEN sont utilisées pour exécuter un groupe de déclarations avec des conditions.

Exemples:

```
IF expression_booléenne THEN déclarations
END

IF expression_booléenne THEN déclarations
ELSE déclarations
END

IF expression_booléenne THEN déclarations
ELSIF expression_booléenne THEN déclarations
END
```

IF *expression_booléenne* THEN

Première clause d'une instruction IF-THEN. Une évaluation permet de savoir si l'expression booléenne est TRUE ou FALSE. Si elle est TRUE, les déclarations qui la suivent sont exécutées. Si elle est FALSE, le processus passe directement à la déclaration ELSE, ELSIF ou END suivante.

ELSE

Cette déclaration marque le début des déclarations exécutées lorsque toutes les instructions IF-THEN et ELSIF qui précèdent sont FALSE. Par exemple :

```
IF expression_booléenne THEN instructions
ELSIF expression_booléenne THEN instructions
ELSIF expression_booléenne THEN instructions
ELSE instructions
END
```

ELSIF *expression_booléenne* THEN

L'expression booléenne est évaluée si la déclaration IF-THEN qui précède renvoie une valeur FALSE. Une évaluation permet de savoir si la déclaration ELSIF est TRUE ou FALSE. Si elle est TRUE, les déclarations qui suivent sont exécutées. Si elle est FALSE, le processus passe directement à la déclaration ELSE, ELSIF ou END suivante.

Par exemple :

```
IF expression_booléenne THEN instructions
ELSIF expression_booléenne THEN instructions
ELSIF expression_booléenne THEN instructions
END
```

END

La déclaration END met fin à un bloc IF-THEN.

RETURN

La déclaration RETURN fournir les résultats des sections du sélecteur et du fournisseur.

Sélecteur

Dans une section du sélecteur, la déclaration RETURN fournit l'entier qui définit la priorité de la règle. La commande RETURN assigne à une règle une priorité comprise entre 0 et 100. Une priorité 0 signifie que la règlene doit pas être utilisée. Une priorité comprise entre 1 et 99 signifie que la règle est utilisée si aucune autre ne présente une valeur supérieure. Enfin, une priorité 100 signifie que la règle doit impérativement être utilisée. Si aucune déclaration RETURN n'est générée dans une section du sélecteur, le système renvoie par défaut une valeur nulle.

La déclaration doit obligatoirement se terminer par un point-virgule (;). Par exemple :

```
RETURN 49;
RETURN L2;
RETURN 39+7;
```

Fournisseur

Dans une section du fournisseur, la déclaration RETURN fournit le résultat SEND ou DONT_SEND. Si aucune déclaration RETURN n'est générée, la valeur par défaut SEND est renvoyée.

La déclaration doit obligatoirement se terminer par un point-virgule (;). Par exemple :

```
RETURN SEND;
RETURN DONT_SEND;
RETURN L1;
```

Assignation

La déclaration d'assignation modifie la valeur d'un symbole à l'aide des caractères :=. La variable définie par l'utilisateur ou par le système est indiquée en premier, suivie du signe := et de la valeur, de la variable ou de l'opération. La déclaration d'assignation doit se terminer par un point-virgule (;). Par exemple :

variable.champ:=*expression*; *variable*:=*expression*;

t1 et t2 sont du type TIME, i1 et i2 du type INTEGER, b1 et b2 sont des assignations booléennes valides:

```
t1 := t2;
b1 := t1 < t2;
i1 := t1.mday - 15;
b2 := t2.year < 2000
```

Assignations non valides:

```
b1 := 10 < i2 < 12;
```

(10 <i2) est de type BOOLEAN, or une valeur de ce type ne peut pas être comparée à une valeur INTEGER.

b1 := (10 < i2) AND (i2 < 12) ; peut être utilisée à la place. Par exemple :

```
  b2 := i1;
```

b2 est de type BOOLEAN et i1 de type INTEGER. Il s'agit donc de types incompatibles.

Vous pouvez utiliser b2 := i1 > 0 ; à la place.

Le système procède à une vérification stricte du type. Vous n'êtes pas autorisé à assigner une valeur INT à une variable TIME.

Opérateurs arithmétiques

Vous pouvez inclure des opérateurs arithmétiques dans des déclarations d'assignation, des déclarations RETURN ou des blocs IF. Les opérateurs valides sont les suivants :

- Adition (+)
- Soustraction (-)
- Division (/)
- Multiplication (*)
- Modulo (MOD)

Les opérateurs arithmétiques vous permettent uniquement d'utiliser des variables de type INT. N'utilisez pas de variables de type TIME, NETADDRESS ou BOOLEAN dans des expressions arithmétiques.

Évitez de procéder à des opérations générant un résultat inférieur à -2147483648 ou supérieur à +2147483648. Évitez également les divisions par zéro.

Opérateurs relationnels

Vous pouvez utiliser des opérateurs relationnels dans des blocs IF. Les opérateurs valides sont les suivants :

- Égal à (=)
- Différent de (< >)
- Supérieur à (>)
- Supérieur ou égal à (>=)
- Inférieur à (<)
- Inférieur ou égal à (<=)

Tous les opérateurs relationnels peuvent être utilisés avec les variables de type TIME et INT. Vous pouvez également utiliser < > et = avec des variables de type NET ADDRESS et BOOLEAN.

Opérateurs logiques

Les opérateurs valides sont les suivants :

- AND
- ou
- NOT
- Inférieur à (<)
- Supérieur à (>)
- Égal à (=)

Opérateurs de bits

Vous pouvez utiliser des opérateurs de bits sur des variables de type INT afin de renvoyer un entier. Les opérateurs valides sont les suivants :

- BITAND
- BITOR
- BITNOT

Opérations complexes

Les règles de priorité suivantes sont respectées lors du traitement d'expressions complexes. Les opérateurs présentant le même niveau de priorité sont traités de gauche à droite. L'ordrerespecté est le suivant :

- Parenthèse
- Unaire (+/-)
- BITNOT
- BITAND
- BITOR
- Multiplication, division, MOD
- Adition, soustraction
- Relationnel (>, >=, <, <=, =)
- NOT
- AND
- ou

Si vous n'êtes pas sûr de l'ordre de priorité, utilisez des parenthèses. Par exemple, si les valeurs A, B et C sont des entiers ou des variables, la combinaison A<B<C n'est pas autorisée. A<B renvoie une valeur booléenne, et non un entier. Cette valeur ne peut donc pas être comparée à l'entier C. En revanche, la syntaxe de l'instruction (A<B) AND (B<C) est correcte.

PRINT

Vous pouvez utiliser les déclarations PRINT pour envoyer du texte et des symboles vers l'écran d'affichage du gestionnaire de trafic WAN du serveur et dans le fichier journal.

Les instructions PRINT peuvent comporter autant d'arguments que nécessaire. Il peut s'agir de chaînes de constantes, de noms de symboles ou de membres, d'entiers ou de valeurs booléennes, séparés par des virgules.

Les chaînes de constantes doivent figurer entre guillemets ("). Les déclarations PRINT doivent se terminer par un point-virgule (;). Par exemple :

```
PRINT "INT=",10,"BOOL=",TRUE,"SYM=",R1;
```

Les variables TIME et NETADDRESS utilisent des déclarations PRINT formatées. Les symboles TIME sont imprimés de la manière suivante :

```
m:d:y h:m
```

Les variables NETADDRESS sont imprimées de la manière suivante :

Type longueur données

Le *type* peut être IP ou IPX, la *longueur* désigne le nombre d'octets et les *données* correspondent à la chaîne d'adresse hexadécimale.

12 Présentation des services LDAP pour Novell eDirectory

LDAP (Lightweight Directory Access Protocol) est un protocole de communications Internet qui permet aux applications client d'accéder aux informations sur l'annuaire. Basé sur le protocole DAP (Directory Access Protocol) X.500, il est moins complexe qu'un client traditionnel et peut être utilisé avec tout autre service d'annuaire répondant à la norme X.500.

LDAP est souvent utilisé en tant que protocole d'accès simplifié aux annuaires.

Les services LDAP pour Novell® eDirectory™ correspondent à une application serveur qui permet aux clients LDAP d'accéder aux informations stockées dans eDirectory.

Ils comportent les fonctions de eDirectory disponibles via LDAP :

- Provisioning
- Account Management (gestion des comptes)
- Authentification
- Autorisation
- Gestion des identités
- Notification
- Reporting
- Qualification
- Segmentation

Vous pouvez accorder à vos clients différents niveaux d'accès à l'annuaire ou y accéder par le biais d'une connexion sécurisée. Ces mécanismes de sécurité permettent de mettre certains types d'informations sur l'annuaire à la disposition du public, tandis que d'autres sont réservés à votre organisation, à des groupes ou à des personnes spécifiés.

Les fonctions d'annuaire accessibles aux clients LDAP dépendent des fonctions intégrées au client et au serveur LDAP. Les services LDAP pour eDirectory permettent, par exemple, aux clients LDAP de lire et d'écrire des données dans la base de données eDirectory s'ils disposent des autorisations nécessaires. Certains clients ont un accès en lecture et en écriture aux données de l'annuaire, d'autres n'ont qu'un accès en lecture.

Les fonctions client types permettent aux clients d'effectuer une ou plusieurs des opérations suivantes :

- rechercher des informations sur une personne spécifique, telles qu'une adresse électronique ou un numéro de téléphone ;
- rechercher des informations sur toutes les personnes répondant à un nom donné ou dont le nom commence par une certaine lettre ;
- rechercher des informations sur un objet ou une entrée eDirectory quelconque ;

- récupérer un nom, une adresse électronique, un numéro de téléphone professionnel ou un numéro de téléphone personnel ;
- récupérer un nom de société et un nom de ville.

Les sections suivantes fournissent des informations sur les services LDAP pour eDirectory :

- « Termes clés des services LDAP », page 322
- « Présentation du fonctionnement de LDAP avec eDirectory », page 324
- « Utilisation des outils LDAP sous Linux, Solaris, AIX ou HP-UX », page 334
- « Filtre de recherche de concordance extensible », page 344

Pour plus d'informations sur les services LDAP, reportez-vous à la documentation Novell LDAP Developer Documentation (documentation Novell du développeur LDAP) (http://developer.novell.com/ndk/doc_novell_edirectory.htm).

Pour plus d'informations sur LDAP, visitez les sites Web suivants :

- The University of Michigan (université du Michigan) (http://www.umich.edu/~dirsvcs/ldap/ldap.html)
- An LDAP Roadmap & FAQ (guide LDAP et FAQ) (http://www.kingsmountain.com/ldapRoadmap.shtml)
- LDAPzone.com (http://www.ldapzone.com)

Termes clés des services LDAP

Clients et serveurs

Client LDAP – Application (par exemple, Netscape* Communicator*, Internet Explorer ou utilitaire d'importation, de conversion et d'exportation Novell).

Serveur LDAP – Serveur sur lequel est exécuté nldap.nlm (pour NetWare®), nldap.dlm (pour Windows2000/NT), libnldap.so (pour systèmesLinux, Solaris et AIX) ou libnldap.sl (pour systèmes HP-UX).

Objets

Objet Groupe LDAP – Définit les propriétés LDAP Novell sur un serveur LDAP.

Cet objet est créé lors de l'installation de eDirectory. L'objet Groupe LDAP contient des informations de configuration pouvant être partagées par plusieurs serveurs LDAP.

Objet Serveur LDAP – Définit l'accès des clients LDAP aux informations figurant sur le serveur LDAP Novell et l'utilisation qu'ils en font.

Cet objet est créé lors de l'installation de eDirectory. L'objet Serveur LDAP représente des données de configuration propres au serveur.

La figure ci-après montre un objet Serveur LDAP dans Novell iManager.

Renvois

Renvoi – Message que le serveur LDAP envoie au client LDAP pour lui indiquer qu'il ne peut pas fournir de résultats complets et que des données complémentaires se trouvent peut-être sur un autre serveur LDAP.

Le renvoi contient toutes les informations nécessaires à la poursuite de l'opération.

Scénario : un client LDAP envoie une requête à un serveur LDAP, mais celui-ci ne trouve pas l'entrée cible localement. Grâce aux références de connaissances qu'il possède sur les partitions et les autres serveurs, le serveur LDAP identifie un autre serveur possédant plus d'informations sur l'entrée. Le serveur LDAP envoie ces informations au client.

Le client établit alors une nouvelle connexion LDAP avec le serveur identifié et tente à nouveau l'opération.

Les renvois présentent les avantages suivants :

- Le client LDAP conserve le contrôle de l'opération.

  Le client ayant toujours connaissance des opérations, il prend de meilleures décisions et transmet des commentaires à l'utilisateur. Le client peut également décider de ne pas suivre le renvoi ou de signaler à l'utilisateur qu'il s'apprête à le suivre.

- En général, les renvois permettent d'utiliser les ressources réseau plus efficacement que le chaînage.

  Le chaînage permet de transmettre deux fois une recherche à plusieurs entrées via le réseau. La première transmission passe du serveur qui détient les données à celui qui effectue le chaînage. La seconde passe du serveur qui effectue le chaînage au client.

  Le renvoi permet au client d'obtenir les données directement en provenance du serveur qui les détient, en une seule transmission.

- Lorsqu'un client connaît l'emplacement de stockage d'une entrée, il peut aller directement sur le serveur qui détient les données.

  Le chaînage masque les détails au client. S'il ne sait pas d'où proviennent les données, le client n'ira probablement pas directement sur le serveur qui les détient.

Les renvois présentent les inconvénients suivants :

- Le client doit savoir reconnaître et suivre les renvois.
- Les clients LDAPv2 ne savent pas reconnaître les renvois ou utilisent une méthode obsolète et non standard pour les détecter.
- Chaque partition eDirectory doit être gérée par un serveur LDAP.

  Sinon, aucun renvoi n'est transmis pour les données de cette partition.

Renvoi supérieur – Renvoi vers un serveur qui détient des données à un niveau de l'arborescence supérieur à celui du serveur avec lequel il communique. Pour plus de détails, reportez-vous à la section « Configuration des renvois supérieurs », page 373.

Les renvois supérieurs traitent les requêtes concernant des objets situés dans une partition non-eDirectory de niveau supérieur ou contiguë dans une arborescence multifournisseur.

Pour qu'un serveur eDirectory puisse participer à ce type d'arborescence, eDirectory classe les données hiérarchiques au-dessus de lui dans une partition marquée comme « non experte ». Les objets de la zone non experte sont uniquement les entrées nécessaires à la construction de la hiérarchie DN appropriée. Ces entrées sont similaires aux entrées de substitution « Glue » X.500.

eDirectory permet de placer dans la zone non experte des informations de connaissance sous la forme de données de renvoi LDAP. Ces informations servent à envoyer des renvois au client LDAP.

Lorsqu'une opération LDAP est effectuée dans une zone non experte de l'arborescence eDirectory, le serveur LDAP recherche les données de référence correspondantes et transmet un renvoi au client.

Chaînage – Protocole de résolution de nom basé sur un serveur.

Un client LDAP envoie une requête à un serveur LDAP, mais celui-ci ne trouve pas l'entrée cible localement. Grâce aux références de connaissances qu'il possède sur les partitions et sur d'autres serveurs de l'arborescence eDirectory, le serveur LDAP identifie un autre serveur LDAP possédant plus d'informations sur le DN. Le premier serveur LDAP contacte le serveur LDAP identifié (second).

Au besoin, ce processus se poursuit jusqu'à ce que le premier serveur en contacte un autre qui dispose d'une réplique de l'entrée. eDirectory gère alors tous les détails pour terminer l'opération. Ne connaissant pas les opérations serveur à serveur, le client suppose que le premier serveur a terminé la requête.

Sur un serveur LDAP, le chaînage présente les avantages suivants :

- Il masque tous les détails de résolution de nom au client.
- Il effectue automatiquement une nouvelle authentification.
- Il joue le rôle de proxy pour le client.
- Il fonctionne de manière transparente, même lorsque des serveurs de l'arborescence eDirectory ne prennent pas en charge les services LDAP.

Le chaînage présente les inconvénients suivants :

- Il est possible que la transmission des commentaires du serveur au client prenne du temps, pendant que le serveur effectue un chaînage pour résoudre le nom.
- Si l'opération exige du serveur LDAP qu'il envoie de nombreuses entrées via une liaison WAN, elle peut même s'avérer très longue.
- Si plusieurs serveurs sont capables d'effectuer l'opération, des serveurs distincts peuvent traiter deux requêtes pour gérer la même entrée.

  eDirectory essaie de classer les serveurs en fonction du coût encouru pour les contacter. Pour l'équilibrage des charges, eDirectory sélectionne de façon aléatoire un serveur à faible coût.

Présentation du fonctionnement de LDAP avec eDirectory

Cette section fournit les informations suivantes :

- « Connexion à eDirectory à partir de LDAP », page 325
- « Assignations de classes et d'attributs », page 328
- « Autorisation d'une sortie de schéma non standard », page 331
- « Différences de syntaxe », page 332
- « Contrôles et extensions LDAP Novell pris en charge », page 333

Connexion à eDirectory à partir de LDAP

Tous les clients LDAP se relient (se connectent) à Novell eDirectory en tant qu'un des types d'utilisateur suivants :

- Utilisateur [Public] (liaison anonyme)
- Utilisateur proxy (liaison anonyme d'utilisateur proxy)
- Utilisateur NDS ou eDirectory (liaison d'utilisateur NDS)

Le type de liaison avec lequel l'utilisateur s'authentifie détermine le contenu auquel le client LDAP peut accéder. Les clients LDAP accèdent à un annuaire en élaborant une requête qu'ils lui envoient. Lorsqu'un client LDAP envoie une requête via les services LDAP pour eDirectory, eDirectory traite la requête des seuls attributs pour lesquels le client LDAP dispose de droits appropriés.

Si le client LDAP fait, par exemple, porter sa requête sur une valeur d'attribut (nécessitant le droit Lire) mais que l'utilisateur dispose uniquement du droit Comparer sur cet attribut, la requête est rejetée.

Les restrictions de login et de mot de passe standard s'appliquent toujours. Toutefois, les restrictions sont tributaires de l'endroit où LDAP est exécuté. Les restrictions de temps et d'adresse sont respectées, mais les restrictions d'adresse sont tributaires de l'endroit où le login à eDirectory a été effectué ; dans ce cas, il s'agit du serveur LDAP.

Connexion en tant qu'utilisateur [Public]

Une liaison anonyme est une connexion qui ne contient pas de nom d'utilisateur ni de mot de passe. Si un client LDAP sans nom ni mot de passe se connecte aux services LDAP pour eDirectory et que le service n'est pas configuré pour utiliser un utilisateur proxy, l'utilisateur est authentifié auprès de eDirectory en tant qu'utilisateur [Public].

L'utilisateur [Public] est un utilisateur eDirectory non authentifié. Par défaut, l'utilisateur [Public] dispose du droit Parcourir sur les objets de l'arborescence eDirectory. Le droit Parcourir accordé par défaut à l'utilisateur [Public] permet de naviguer dans les objets eDirectory, mais verrouille l'accès à la majorité des attributs d'objets.

Les droits [Public] par défaut sont généralement trop limités pour la plupart des clients LDAP. Bien que vous puissiez modifier les droits [Public], leur modification confère ces droits à tous les utilisateurs. C'est la raison pour laquelle, il est recommandé d'utiliser plutôt une liaison anonyme d'utilisateur proxy. Pour plus d'informations, reportez-vous à la section « Connexion en tant qu'utilisateur proxy », page 325.

Pour conférer à un utilisateur [Public] un accès aux attributs des objets, vous devez transformer l'utilisateur [Public] en ayant droit du ou des conteneurs concernés, puis lui assigner les droits appropriés sur les objets et les attributs.

Connexion en tant qu'utilisateur proxy

Une liaison anonyme d'utilisateur proxy est une connexion anonyme liée à un nom d'utilisateur eDirectory. Si un client LDAP se lie anonymement aux services LDAP pour eDirectory et que le protocole est configuré pour utiliser un utilisateur proxy, l'utilisateur est authentifié auprès de eDirectory en tant qu'utilisateur proxy. Le nom est alors configuré à la fois dans les services LDAP pour et dans eDirectory.

En règle générale, la liaison anonyme se fait sur le port 389 dans les services LDAP. Vous pouvez cependant configurer manuellement d'autres ports lors de l'installation.

Les principaux concepts associés aux liaisons anonymes d'utilisateurs proxy sont présentés ci-dessous :

- Tous les accès d'un client LDAP par des liaisons anonymes sont assignés via l'objet Utilisateur proxy.
- Les clients LDAP ne fournissant pas de mot de passe lors des liaisons anonymes, l'utilisateur proxy doit avoir un mot de passe nul et ne doit avoir aucune restriction de mot de passe (intervalle de changement de mot de passe, par exemple). N'indiquez pas de date d'expiration du mot de passe et n'autorisez pas l'utilisateur proxy à changer de mot de passe.
- Vous pouvez limiter les emplacements depuis lesquels l'utilisateur peut se loguer en définissant des restrictions d'adresse pour l'objet Utilisateur proxy.
- L'objet Utilisateur proxy doit être créé dans eDirectory et des droits sur les objets eDirectory que vous souhaitez publier doivent lui être assignés. Les droits Utilisateur par défaut fournissent un accès en lecture sur un ensemble limité d'objets et d'attributs. Assignez les droits Lire et Rechercher de l'utilisateur proxy sur tous les objets et attributs de chaque sous-arborescence dans laquelle un accès est requis.
- L'objet Utilisateur proxy doit être activé dans la page Général de l'objet Groupe LDAP qui configure les services LDAP pour eDirectory. De ce fait, il n'existe qu'un objet Utilisateur proxy pour tous les serveurs d'un groupe LDAP. Pour plus d'informations, reportez-vous à la section « Configuration des objets LDAP », page 352.
- Vous pouvez accorder à un utilisateur proxy des droits d'objet sur toutes les propriétés (par défaut) ou sur des propriétés spécifiques.

Pour accorder à l'utilisateur proxy des droits sur les propriétés sélectionnées:

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Droits > Modifier les ayants droit.
3. Entrez le nom et le contexte du conteneur de niveau supérieur sur lequel l'utilisateur proxy a des droits ou cliquez sur  pour accéder au conteneur concerné, puis sur OK.
4. Dans l'écran Modifier les ayants droit, cliquez sur Ajouter un ayant droit.
5. Recherchez l'objet de l'utilisateur proxy et sélectionnez-le, puis cliquez sur OK.
6. Cliquez sur Droits assignés, à gauche de l'utilisateur proxy que vous venez d'ajouter.
7. Cochez les cases Tous les droits d'attribut et Droits d'entrée, puis cliquez sur Supprimer la propriété.
8. Cliquez sur Ajouter une propriété, puis cochez la case Afficher toutes les propriétés dans le schéma.
9. Sélectionnez un droit héritable pour l'utilisateur proxy, tel que Boîte postale (dans la section de la liste en minuscules) ou Titre, puis cliquez sur OK.

   Pour ajouter d'autres droits héritables, répétez les étapes 9 et 10.
10. Cliquez sur Terminé, puis sur OK.

Pour mettre en oeuvre les liaisons anonymes d'utilisateur proxy, vous devez créer l'objet Utilisateur proxy dans eDirectory et lui assigner les droits appropriés. Assignez les droits Lire et Rechercher de l'utilisateur proxy sur tous les objets et attributs de chaque sous-arborescence dans laquelle un accès est requis. Vous devez également activer l'utilisateur proxy dans les services LDAP pour eDirectory en spécifiant le même nom d'utilisateur proxy.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur LDAP > Présentation LDAP.
3. Cliquez sur le nom d'un objet Groupe LDAP à configurer.
4. Entrez le nom et le contexte d'un objet Utilisateur eDirectory dans le champ Utilisateur proxy.
5. Cliquez sur Appliquer, puis sur OK.

Utilisation de l'utilitaire ldapconfig sous Linux et UNIX

Par exemple, vous trouverez des informations sur la manière dont le serveur LDAP traite les renvois LDAP dans Utilisation de renvois lors d'une recherche pour LDAP.

1. À l'invite du système, entrez la commande suivante :

   ```
   ldapconfig -s "LDAP:otherReferralUsage=1"
   ```

2. Saisissez le nom distinctif complet de l'utilisateur pour eDirectory (FDN utilisateur) et le mot de passe de l'utilisateur.

Connexion en tant qu'utilisateur NDS ou eDirectory

Une liaison d'utilisateur eDirectory est une connexion établie par un client LDAP à l'aide d'un nom d'utilisateur eDirectory complet et d'un mot de passe. La liaison d'utilisateur eDirectory est authentifiée dans eDirectory et le client LDAP a accès à toutes les informations que l'utilisateur eDirectory est autorisé à consulter.

Les concepts clés des liaisons d'utilisateur eDirectory sont les suivants :

- Les liaisons d'utilisateur eDirectory sont authentifiées auprès de eDirectory à l'aide du nom d'utilisateur et du mot de passe saisis au niveau du client LDAP.
- Le nom d'utilisateur et le mot de passe eDirectory utilisés pour l'accès du client LDAP peuvent également être utilisés pour l'accès du client NetWare à eDirectory.
- Lors de connexions non-TLS, le mot de passe eDirectory est transmis en texte clair entre le client LDAP et les services LDAP pour eDirectory.
- Si les mots de passe en texte clair ne sont pas autorisés, toutes les requêtes de liaison eDirectory comportant un nom d'utilisateur ou un mot de passe sur des connexions non-TLS sont rejetées.
- En cas d'expiration du mot de passe d'un utilisateur eDirectory, les requêtes de liaison eDirectory de cet utilisateur sont rejetées.

Assignation de droits eDirectory aux clients LDAP

1. Déterminez le type de nom d'utilisateur que les clients LDAP vont utiliser pour accéder à eDirectory.
   - Utilisateur [Public] (liaison anonyme)
   - Utilisateur proxy (liaison anonyme d'utilisateur proxy)
   - Utilisateur NDS (liaison d'utilisateur NDS)

   Pour plus d'informations, reportez-vous à la section « Connexion à eDirectory à partir de LDAP », page 325.

2. Si les utilisateurs utilisent un nom d'utilisateur proxy ou plusieurs noms d'utilisateur eDirectory pour accéder aux services LDAP, utilisez iManager pour créer ces noms d'utilisateur dans eDirectory ou via les services LDAP.
3. Assignez les droits eDirectory correspondants aux noms d'utilisateur que les clients LDAP vont utiliser.

Les droits par défaut que la plupart des utilisateurs reçoivent comprennent des droits limités sur l'objet de l'utilisateur. Pour accorder l'accès à d'autres objets et à leurs attributs, vous devez changer les droits assignés dans eDirectory.

Lorsqu'un client LDAP demande l'accès à un objet et à un attribut eDirectory, eDirectory accepte ou refuse cette requête en fonction de l'identité eDirectory du client LDAP. Cette identité est définie à l'établissement de la liaison.

Assignations de classes et d'attributs

Une *classe* est un type d'objet dans un annuaire, par exemple un utilisateur, un serveur ou un groupe. Un attribut correspond à un élément d'annuaire qui définit des informations supplémentaires portant sur un objet spécifique. Par exemple, un objet Utilisateur peut avoir pour attribut un nom de famille ou un numéro de téléphone.

Un *schéma* est un ensemble de règles qui définit les classes et attributs autorisés dans un annuaire, ainsi que la structure de l'annuaire (des relations peuvent exister entre les classes). Étant donné que les schémas des annuaires LDAP et eDirectory sont parfois différents, l'assignation de classes et d'attributs LDAP aux objets et aux attributs eDirectory correspondants peut s'avérer nécessaire. Ces assignations définissent la conversion des noms du schéma LDAP au schéma eDirectory.

Les services LDAP pour eDirectory proposent des assignations par défaut. Dans de nombreux cas, la correspondance entre les classes et attributs LDAP et les types et propriétés d'objets eDirectory est logique et intuitive. Toutefois, en fonction de vos besoins en matière de mise en oeuvre, vous pouvez reconfigurer les assignations de classes et d'attributs.

Dans la plupart des cas, l'assignation d'une classe LDAP à un type d'objet eDirectory correspond à une relation de type un à un. Cependant, le schéma LDAP prend en charge les noms d'alias, tels que CN et commonName, qui font référence à un même attribut.

Assignation des attributs du groupe LDAP

La configuration par défaut des services LDAP pour eDirectory comprend un ensemble prédéfini d'assignations de classes et d'attributs. Celles-ci assignent un sous-ensemble d'attributs LDAP à un sous-ensemble d'attributs eDirectory. Si un attribut n'est pas encore assigné dans la configuration par défaut, une assignation générée automatiquement est assignée à l'attribut. De même, si le nom de schéma est un nom LDAP valide ne comportant ni espace ni deux points, aucune assignation n'est nécessaire. Examinez l'assignation de classes et d'attributs et reconfigurez-la si nécessaire.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur LDAP > Présentation LDAP > Afficher les groupes LDAP.
3. Cliquez sur un objet Groupe LDAP, puis sur Assignation d'attribut.

4 Ajoutez, supprimez ou modifiez les attributs de votre choix.

Étant donné que certains attributs LDAP peuvent disposer de noms de remplacement (comme CN et commonName), vous devrez peut-être assigner plusieurs attributs LDAP à un nom d'attribut eDirectory correspondant. Lorsque les services LDAP pour eDirectory renvoient les informations sur les attributs LDAP, ils renvoient la valeur du premier attribut correspondant repéré dans la liste.

Si vous assignez plusieurs attributs LDAP à un seul attribut eDirectory, vous devez réorganiser la liste afin de préciser l'attribut prioritaire, car l'ordre est important.

5 Cliquez sur Appliquer, puis sur OK.

Assignation des classes du groupe LDAP

Lorsqu'un client LDAP demande au serveur LDAP des informations sur les classes LDAP, le serveur renvoie les informations sur les classes eDirectory correspondantes. La configuration par défaut des services LDAP pour eDirectory comprend un ensemble prédéfini d'assignations de classes et d'attributs.

1 Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

2 Cliquez sur LDAP > Présentation LDAP.

3 Cliquez sur un objet Groupe LDAP, puis sur Assignation de classe.

4 Ajoutez, supprimez ou modifiez les classes de votre choix.

La configuration par défaut des services LDAP pour eDirectory comprend un ensemble prédéfini d'assignations de classes et d'attributs. Ces assignations assignent un sous-ensemble de classes et d'attributs LDAP à un sous-ensemble de classes et d'attributs eDirectory. Si un attribut ou une classe n'est pas encore assigné dans la configuration par défaut, une assignation générée automatiquement est assignée à l'attribut ou à la classe.

De même, si le nom de schéma est un nom LDAP valide ne comportant ni espace ni deux points, aucune assignation n'est nécessaire. Examinez l'assignation de classes et d'attributs et reconfigurez-la si nécessaire.

5 Cliquez sur Appliquer, puis sur OK.

Assignation de classes et d'attributs LDAP

Étant donné que les schémas des annuaires LDAP et eDirectory sont différents, il est nécessaire d'assigner des classes et attributs LDAP aux objets et attributs eDirectory correspondants. Ces assignations définissent la conversion des noms du schéma LDAP au schéma eDirectory.

Aucune assignation de schéma LDAP n'est requise pour une entrée de schéma si le nom est un nom de schéma LDAP valide. Dans LDAP, les seuls caractères autorisés dans un nom de schéma sont les caractères alphanumériques et les tirets (-). Le nom de schéma LDAP ne doit pas comporter d'espace.

Pour garantir le résultat d'une recherche par ID d'objet après une extension de schéma autre que LDAP, comme pour les fichiers .sch, vous devez actualiser la configuration du serveur LDAP si le schéma s'étend en dehors de LDAP.

Assignations de plusieurs éléments pour un seul

Pour prendre en charge LDAP depuis eDirectory, les services LDAP utilisent des assignations au niveau du protocole (plutôt qu'au niveau des services d'annuaire) pour effectuer la conversion entre les attributs et les classes LDAP et eDirectory. C'est pour cette raison que deux classes ou attributs LDAP peuvent être assignés à la même classe ou au même attribut eDirectory.

Par exemple, si vous créez un Cn via LDAP, puis recherchez CommonName=Value, vous pouvez obtenir un nom commun susceptible d'avoir la même valeur d'attribut que Cn.

Si vous demandez tous les attributs, vous obtenez le premier attribut de la liste des assignations correspondant à cette classe. Si vous demandez un attribut d'après son nom, vous obtenez le nom correct.

Assignations de plusieurs classes à une seule

Nom de classe LDAP	Nom de classe eDirectory
alias aliasObject	Alias
groupOfNames groupOfUniqueNames group	Groupe
mailGroup rfc822mailgroup	NSCP:mailGroup1

Assignations de plusieurs attributs à un seul

Nom d'attribut LDAP	Nom d'attribut eDirectory
c countryName	C
cn commonName	CN
uid userId	uniqueID
description multiLineDescription	Description
l localityname	L
member uniqueMember	Member
o organizationname	O
ou organizationalUnitName	OU
sn surname	Surname

Nom d'attribut LDAP	Nom d'attribut eDirectory
st stateOrProvinceName	S
certificateRevocationList;binary certificateRevocationList	certificateRevocationList
authorityRevocationList;binary authorityRevocationList	authorityRevocationList
deltaRevocationList;binary deltaRevocationList	deltaRevocationList
cACertificate;binary cACertificate	cACertificate
crossCertificatePair;binary crossCertificatePair	crossCertificatePair
userCertificate;binary userCertificate	userCertificate

REMARQUE : les attributs qui comportent « ;binary » concernent la sécurité. Ils se trouvent dans la table d'assignation, si votre application a besoin du nom récupéré avec la valeur « ;binary ». Sinon, vous pouvez modifier l'ordre des assignations.

Autorisation d'une sortie de schéma non standard

eDirectory comporte un commutateur de mode de compatibilité autorisant une sortie de schéma non standard que les clients ADSI actuels et les anciens clients Netscape peuvent lire. Pour le mettre en uvre, il convient de définir un attribut dans l'objet Serveur LDAP. Le nom de l'attribut concerné est nonStdClientSchemaCompatMode. L'objet Serveur LDAP est généralement créé dans le même conteneur que l'objet Serveur.

La sortie non standard n'est pas conforme aux normes IETF actuelles de LDAP, mais elle fonctionne avec la version actuelle des clients ADSI et les anciens clients Netscape.

Dans le format de sortie non standard:

- SYNTAX OID apparaît entre guillemets simples.
- Aucune limite supérieure n'apparaît en sortie.
- Aucune option X n'apparaît en sortie.
- S'il existe plusieurs noms, seul le premier détecté apparaît en sortie.
- Les attributs ou classes sans OID défini sortent sous la forme « attributename-oid » ou « classname-oid » en minuscules.
- Les attributs ou classes dont le nom comporte un tiret et ne possédant pas d'OID défini ne sont pas obtenus en sortie.

L'OID, ou identificateur d'objet, est une chaîne numérique d'octets nécessaire pour ajouter votre propre attribut ou classe d'objets à un serveur LDAP.

Pour autoriser la sortie de schéma non standard, procédez comme suit :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur LDAP > Présentation LDAP.
3. Cliquez sur Afficher les serveurs LDAP, puis sur un objet Serveur LDAP.
4. Cliquez sur Recherches, puis sur Autoriser la sortie de schéma pour les anciens clients ADSI et Netscape.

   La sortie non standard n'est pas conforme aux normes IETF actuelles définies pour LDAP, mais elle fonctionne avec les clients ADSI actuels et les anciens clients Netscape.
5. Cliquez sur Appliquer, puis sur Informations et sur Rafraîchir.

Différences de syntaxe

Les services LDAP et eDirectory n'utilisent pas la même syntaxe. Certaines différences importantes sont expliquées ci-dessous :

- « Virgules », page 332
- « Noms avec type », page 332
- « Caractère d'échappement », page 332
- « Attributs de dénomination multiples », page 333

Virgules

LDAP utilise la virgule et non le point comme séparateur. Exemple de nom distinctif (ou complet) dans eDirectory :

CN=JANEB.OU=MKTG.O=EMA

Le même nom distinctif avec la syntaxe LDAP :

CN=JANEB,OU=MKTG,O=EMA

Autres exemples de noms distinctifs LDAP:

CN=Bill Williams,OU=PR,O=Bella Notte Corp
CN=Susan Jones,OU=Humanities,O=University College London,C=GB

Noms avec type

eDirectory utilise aussi bien les noms sans type (.JOHN.MARKETING.ABCCORP) que les noms avec type (CN=JOHN.OU=MARKETING.O=ABCCORP). LDAP n'utilise que des noms avec type et la virgule comme délimiteur (CN=JOHN,OU=MARKETING,O=ABCCORP).

Caractère d'échappement

La barre oblique inverse (\) est utilisée comme caractère d'échappement dans les noms distinctifs LDAP. Si vous utilisez le signe plus (+) ou la virgule (,), vous pouvez utiliser une barre oblique inverse pour indiquer qu'ils font partie d'une séquence d'échappement.

Par exemple :

CN=praliné\+crème,OU=parfums,O=MFG (CN correspond à praliné+crème)

CN=DCardinal,O=Lionel\,Thomas et Catherine,C=US (O correspond à Lionel, Thomas et Catherine)

Pour plus d'informations, reportez-vous à la norme RFC 232 (http://www.ietf.org/rfc/rfc2253.txt?number=2253) d'IETF (Internet Engineering Task Force).

Attributs de dénomination multiples

Vous pouvez définir des objets en utilisant plusieurs attributs de dénomination dans le schéma. Dans les services LDAP comme dans eDirectory, l'objet Utilisateur en possède deux: CN et UID. Le signe plus (+) sépare les attributs de dénomination dans le nom distinctif. Si les attributs ne sont pas explicitement libellés, le schéma détermine la chaîne associée à chaque attribut (la première serait CN et la seconde UID pour eDirectory et LDAP). Vous pouvez les réorganiser en un nom distinctif en libellant manuellement chaque portion.

Par exemple, voici deux noms distinctifs relatifs :

Dupont (CN correspond à Dupont CN=Dupont)

Dupont+Lise (CN correspond à Dupont et OU correspond à Lise CN=Dupont UID=Lise)

Les deux noms distinctifs relatifs (Dupont et Dupont+Lise) peuvent exister dans le même contexte car ils doivent être référencés par deux noms distinctifs relatifs très différents.

Contrôles et extensions LDAP Novell pris en charge

Le protocole LDAP 3 permet aux clients et serveurs LDAP d'utiliser des contrôles et des extensions pour étendre une opération LDAP. Les contrôles et les extensions permettent d'indiquer des informations supplémentaires dans une requête ou une réponse. Chaque opération étendue est identifiée par un OID, ou identificateur d'objet, une chaîne numérique d'octets nécessaire pour ajouter votre propre attribut ou classe d'objet à un serveur LDAP. Les clients LDAP peuvent envoyer des requêtes d'opération étendue en indiquant l'OID de l'opération étendue à effectuer, ainsi que les données qui lui sont propres. Lorsque le serveur LDAP reçoit la requête, il effectue l'opération étendue et envoie au client une réponse contenant un OID et des données supplémentaires.

Par exemple, un client peut inclure un contrôle spécifiant un tri avec la requête de recherche qu'il envoie au serveur. Lorsque le serveur reçoit la requête de recherche, il trie les résultats de la recherche avant de les renvoyer au client. Les serveurs peuvent également envoyer des contrôles aux clients. Par exemple, un serveur peut envoyer un contrôle avec la requête d'authentification qui informe le client de l'expiration du mot de passe.

Par défaut, le serveur LDAP eDirectory charge toutes les extensions système, ainsi que les extensions et les contrôles facultatifs sélectionnés au démarrage du serveur LDAP. L'attribut extensionInfo de l'objet Serveur LDAP pour les extensions facultatives permet à l'administrateur système de sélectionner ou de désélectionner les extensions et les contrôles facultatifs.

Pour que le protocole LDAP 3 puisse activer les opérations étendues, les serveurs doivent fournir la liste des contrôles et des extensions pris en charge dans les attributs supportedControl et supportedExtension de l'entrée rootDSE. L'entrée rootDSE (entrée propre au DSA [Directory System Agent – Agent du système d'annuaire]) est située à la racine de l'arborescence qui contient les informations de l'annuaire (DIT – Directory Information Tree). Pour plus d'informations, reportez-vous à la section « Obtention d'informations sur le serveur LDAP », page 380.

Pour obtenir la liste des contrôles et extensions LDAP pris en charge, reportez-vous aux sections LDAP Controls (Contrôles LDAP) (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/cchbehhc.html) et LDAP Extensions (Extensions LDAP) (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html) du manuel *LDAP and NDS Integration Guide (Guide d'intégration LDAP et NDS)*.

Utilisation des outils LDAP sous Linux, Solaris, AIX ou HP-UX

eDirectory inclut les outils LDAP suivants, stockés dans /opt/novell/eDirectory/bin, afin de vous aider à gérer le serveur d'annuaire LDAP.

Outil	Description
ice	Importe les entrées d'un fichier dans un annuaire LDAP, modifie les entrées d'un fichier dans un annuaire, exporte les entrées vers un fichier et ajoute des définitions de classes et d'attributs à partir d'un fichier.
ldapadd	Ajoute de nouvelles entrées à un annuaire LDAP.
ldapdelete	Supprime les entrées d'un serveur d'annuaire LDAP. L'outil ldapdelete ouvre une connexion à un serveur LDAP, crée une liaison et supprime une ou plusieurs entrées.
ldapmodify	Ouvre une connexion à un serveur LDAP, crée une liaison et modifie ou ajoute des entrées.
ldapmodrdn	Modifie le nom distinctif relatif (RDN) d'entrées d'un serveur d'annuaire LDAP. Ouvre une connexion à un serveur LDAP, crée une liaison et modifie le nom distinctif relatif des entrées.
ldapsearch	Recherche des entrées dans un serveur d'annuaire LDAP. Ouvre une connexion à un serveur LDAP, crée une liaison et effectue une recherche à l'aide du filtre spécifié. Ce filtre doit correspondre à la représentation de type chaîne définie pour les filtres LDAP dans la norme RFC 2254 (http://www.ietf.org/rfc/rfc2254.txt).
ndsindex	Crée, liste, suspend, reprend ou supprime des index.

Pour plus d'informations, reportez-vous à LDAP Tools (Outils LDAP) (http://developer.novell.com/ndk/doc/cldap/ltoolenu/data/hevgtl7k.html) dans le manuel *LDAP Libraries for C Guide (Guide de LDAP Libraries for C)*.

Pour effectuer des opérations sécurisées avec les outils LDAP, reportez-vous à la section « Opérations eDirectory sécurisées sur les systèmes Linux, Solaris, AIX et HP-UX », page 86 et insérez le fichier DER dans toutes les opérations LDAP à ligne de commande qui établissent des connexions LDAP sécurisées à eDirectory.

OutilsLDAP

Les utilitaires LDAP permettent de supprimer, modifier et ajouter des entrées, d'étendre le schéma, de modifier les noms distinctifs relatifs, de déplacer des entrées vers de nouveaux conteneurs, de créer des index de recherche et d'effectuer des recherches.

ldapadd

L'utilitaire ldapadd ajoute de nouvelles entrées. Sa syntaxe est la suivante :

```
ldapadd [-c] [-C] [-l] [-M] [-P] [-r] [-n] [-v] [-F] [-l limite] [-M[M]] [-d
niveau_débogage] [-e nom_fichier_clé] [-D  DN_liaison] [[-W ]| [-w
mot_de_passe]] [-h  hôte_LDAP] [-p port_LDAP] [-P version] [-Z[Z]] [-f
fichier]
```

REMARQUE : sur les serveurs NetWare, cet utilitaire est appelé ladd.

Si l'option -f est spécifiée, ldapadd lit les modifications dans un fichier. Si elle n'est pas spécifiée, ldapadd lit les modifications dans stdin.

SUGGESTION : Le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier, par exemple ldapadd [options] > out.txt.

Option	Description
-a	Ajoute de nouvelles entrées. L'opération par défaut de ldapmodify consiste à modifier des entrées existantes. S'il est appelé sous la forme ldapadd, ce drapeau est toujours défini.
-r	Rétablit les valeurs par défaut.
-c	Mode de fonctionnement continu. Des erreurs sont signalées, mais ldapmodify continue les modifications. L'opération par défaut consiste à quitter chaque fois qu'une erreur est signalée.
-f *fichier*	Lit les informations de modification de l'entrée à partir d'un fichier LDIF et non de l'entrée standard. La longueur maximale d'un enregistrement est de 4096lignes.
-F	Impose l'application de toutes les modifications, quel que soit le contenu des lignes d'entrée qui commencent par replica: (réplique). (Par défaut, les lignes replica: sont comparées à l'hôte et au port du serveur LDAP utilisés pour savoir si un enregistrement replog doit être appliqué.)

Options communes à tous les outils LDAP

Certaines options sont communes à tous les outils LDAP. Elles sont présentées dans le tableau suivant :

Option	Description
-C	Active le suivi des renvois. (liaison anonyme)
-d *niveau_débogage*	Définit le niveau de débogage LDAP sur niveau_débogage. Pour que cette option ait un effet quelconque, l'outil ldapmodify doit être compilé avec LDAP_DEBUG défini.

Option	Description
-D *DN_liaison*	Utilise DN_liaison pour établir une liaison avec l'annuaire LDAP. *DN_liaison* doit être un nom distinctif représenté par une chaîne conformément à la norme RFC 1779.
-e *nom_fichier_clé*	Stocke le nom de fichier du certificat pour la liaison SSL.
-f *fichier*	Lit une série de lignes du fichier, en effectuant une recherche LDAP par ligne. Dans ce cas, le filtre spécifié dans la ligne de commande sert de modèle, la première occurrence de %s étant remplacée par une ligne du fichier. Si le fichier se résume à un tiret (-), les lignes sont lues depuis l'entrée standard.
-h *hôte_LDAP*	Définit un autre hôte sur lequel le serveur LDAP est exécuté.
-l *limite*	Définit le timeout de la connexion (en secondes).
-M	Active la commande Gérer DSA IT. (non critique)
-MM	Active la commande Gérer DSA IT. (critique)
-n	Affiche ce qui serait effectué, mais sans modifier réellement les entrées. Utile pour le débogage conjointement avec l'option -v.
-p *port_LDAP*	Indique un autre port TCP™ sur lequel le serveur LDAP écoute.
-P *version*	Spécifie la version de LDAP (2 ou 3).
-v	Utilise le mode verbeux, avec de nombreux diagnostics écrits sur la sortie standard.
-w *mot_de_passe*	Mot de passe utilisé pour l'authentification simple.
-W	Invite à une authentification simple. Cette option remplace l'utilisation du mot de passe dans la ligne de commande.
-Z	Démarre TLS avant la liaison pour effectuer l'opération. Toute erreur survenant au cours du démarrage de TLS est ignorée et l'opération se poursuit. Pour que l'opération s'arrête en cas d'erreur, il est conseillé d'utiliser l'option -ZZ. Si vous indiquez un port avec cette option, il doit accepter les connexions en texte clair. Pour que l'identité du serveur soit vérifiée, vous devez utiliser cette option conjointement avec -e pour spécifier un fichier de certificat de serveur. Ainsi, le certificat de racine approuvée du serveur est validé au démarrage de TLS. Si vous ne spécifiez pas l'option -e, tous les certificats du serveur sont acceptés.
-ZZ	Démarre TLS avant la liaison pour effectuer l'opération. Toute erreur survenant lors du démarrage de TLS entraîne l'interruption de l'opération. Si vous indiquez un port avec cette option, il doit accepter les connexions en texte clair. Pour que l'identité du serveur soit vérifiée, vous devez utiliser cette option conjointement avec -e pour spécifier un fichier de certificat de serveur. Ainsi, le certificat de racine approuvée du serveur est validé au démarrage de TLS. Si vous ne spécifiez pas l'option -e, tous les certificats du serveur sont acceptés.

Exemples

Supposons que le fichier /tmp/entrymods existe et contienne les éléments suivants :

```
dn: cn=Modify Me, o=University of Michigan, c=US

changetype: modify

replace: mail

mail: modme@terminator.rs.itd.umich.edu

-

add: title

title: Manager

-

add: jpegPhoto

jpegPhoto: /tmp/modme.jpeg

-

delete: description

-
```

Dans ce cas, la commande ldapmodify -b -r -f /tmp/entrymods remplace le contenu de l'attribut de messagerie de l'entrée Modify Me par la valeur modme@terminator.rs.itd.umich.edu, ajoute le titre Manager, ainsi que le contenu du fichier /tmp/modme.jpeg (jpegPhoto) et supprime complètement l'attribut de description.

Vous pouvez apporter les mêmes modifications que ci-dessus en utilisant l'ancien format d'entrée ldapmodify :

```
cn=Modify Me, o=University of Michigan, c=US

mail=modme@terminator.rs.itd.umich.edu

+title=Manager

+jpegPhoto=/tmp/modme.jpeg

-description

et la commande:

ldapmodify -b -r -f /tmp/entrymods

Supposons que le fichier /tmp/newentry existe et contienne les éléments
suivants :

dn: cn=Barbara Jensen, o=University of Michigan, c=US

objectClass: person

cn: Barbara Jensen

cn: B Jensen

sn: Jensen

title: Manager

mail: bjensen@terminator.rs.itd.umich.edu

uid: bjensen
```

Dans ce cas, la commande ldapadd -f /tmp/entrymods ajoute une nouvelle entrée pour B Jensen, en utilisant les valeurs du fichier /tmp/newentry.

Supposons que le fichier /tmp/newentry existe et contienne les éléments suivants :

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US

changetype: delete
```

Dans ce cas, la commande ldapmodify -f /tmp/entrymods supprime l'entrée B Jensen.

ldapdelete

L'utilitaire ldapdelete supprime l'entrée spécifiée. Il ouvre une connexion à un serveur LDAP, crée une liaison et supprime l'entrée. Sa syntaxe est la suivante :

```
ldapdelete [-n] [-v]  [-c]  [-r] [-l] [-C] [-M] [-d niveau_débogage] [-e
nom_fichier_clé] [-f fichier] [-D DN_liaison] [[-W]| [-w mot_de_passe]] [-h
hôte_LDAP] [-p port_LDAP] [-Z[Z]] [dn]...
```

REMARQUE : sur les serveurs NetWare, cet utilitaire est appelé ldelete.

Le paramètre dn est une liste des noms distinctifs des entrées à supprimer.

Il interagit avec l'option -f de l'une des façons suivantes, selon le cas :

- Si l'option -f est manquante dans la ligne de commande et que les dn y sont spécifiés, l'utilitaire supprime les entrées spécifiées.
- Si les dn et l'option -f sont spécifiés dans la ligne de commande, l'utilitaire recherche des dn à supprimer dans le fichier et ignore ceux de la ligne de commande.
- Si les dn et l'option -f sont manquants dans la ligne de commande, l'utilitaire lit le dn de stdin.

SUGGESTION : Le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier, par exemple ldapdelete [options] > out.txt.

Option	Description
-c	Mode de fonctionnement continu. Des erreurs sont signalées, mais ldapdelete continue les suppressions. L'opération par défaut consiste à quitter chaque fois qu'une erreur est signalée.
-f *fichier*	Lit une série de lignes dans le fichier, en effectuant une recherche LDAP par ligne. Dans ce cas, le filtre spécifié dans la ligne de commande sert de modèle, la première occurrence de %s étant remplacée par une ligne du fichier.
-r	Suppression récursive.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP », page 335.

Exemple

La commande ldapdelete "cn=Delete Me, o=University of Michigan, c=US" tente de supprimer l'entrée dont le nom commun est Delete Me directement sous l'entrée organisationnelle University of Michigan. Il sera probablement nécessaire de fournir un DN de liaison et un mot de passe pour autoriser la suppression (reportez-vous aux options -D et -w).

ldapmodify

L'utilitaire ldapmodify modifie les attributs d'une entrée existante ou ajoute de nouvelles entrées. Sa syntaxe est la suivante :

```
ldapmodify [-a] [-c] [-C] [-M] [-P] [-r] [-n] [-v] [-F] [-l limite] [-M[M]]
[-d niveau_débogage] [-e nom_fichier_clé] [-D DN_liaison] [[-W]|[-w
mot_de_passe]] [-h hôte_LDAP] [-p port_LDAP] [-P version] [-Z[Z]] [-f
fichier]
```

REMARQUE : sur les serveurs NetWare, cet utilitaire est appelé lmodify.

Si l'option -f est spécifiée, ldapmodify lit les modifications dans un fichier. Si elle n'est pas spécifiée, ldapmodify lit les modifications dans stdin.

SUGGESTION : Le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier, par exemple ldapmodify [options] > out.txt.

Option	Description
-a	Ajoute de nouvelles entrées. L'opération par défaut de ldapmodify consiste à modifier des entrées existantes. S'il est appelé sous la forme ldapadd, ce drapeau est toujours défini.
-r	Rétablit les valeurs par défaut.
-c	Mode de fonctionnement continu. Des erreurs sont signalées, mais ldapmodify continue les modifications. L'opération par défaut consiste à quitter chaque fois qu'une erreur est signalée.
-f *fichier*	Lit les informations de modification de l'entrée à partir d'un fichier LDIF et non de l'entrée standard. La longueur maximale d'un enregistrement est de 4096lignes.
-F	Impose l'application de toutes les modifications, quel que soit le contenu des lignes d'entrée qui commencent par replica : (réplique). (Par défaut, les lignes replica : sont comparées à l'hôte et au port du serveur LDAP utilisés pour savoir si un enregistrement replog doit être appliqué.)

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP », page 335.

ldapmodrdn

L'utilitaire ldapmodrdn modifie le nom distinctif relatif d'une entrée. L'entrée peut également être déplacée vers un nouveau conteneur. Sa syntaxe est la suivante :

```
ldapmodrdn [-r] [-n] [-v] [-c] [-C] [-l] [-M] [-s nouveau_supérieur] [-d
niveau_débogage] [-e nom_fichier_clé] [-D DN_liaison] [[-W]|[-w
mot_de_passe]]  [-h hôte_LDAP] [-p port_LDAP] [-Z[Z]] [-f fichier] [dn
nouveau_RDN]
```

REMARQUE : sur les serveurs NetWare, cet utilitaire est appelé lmodrdn dn <nouveau_RDN>).

Le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier, par exemple ldapmodrdn [options] > out.txt.

Option	Description
-c	Mode de fonctionnement continu. Des erreurs sont signalées, mais ldapmodify continue les modifications. L'opération par défaut consiste à quitter chaque fois qu'une erreur est signalée.
-f *fichier*	Lit les informations de modification de l'entrée à partir du fichier et non à partir de l'entrée standard ou de la ligne de commande. Veillez à ce qu'il n'y ait pas de ligne vide entre l'ancien et le nouveau RDN, sinon l'option f n'est pas prise en compte.
-r	Supprime les anciennes valeurs RDN de l'entrée. Par défaut, les anciennes valeurs sont conservées.
-s *nouveau_supérieur*	Nom distinctif du conteneur vers lequel l'entrée est déplacée.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP », page 335.

Exemple

Supposons que le fichier /tmp/entrymods existe et contienne les éléments suivants :

```
cn=Modify Me, o=University of Michigan, c=US

cn=The New Me
```

ldapsearch

L'utilitaire ldapsearch recherche dans l'annuaire les attributs et classes d'objet spécifiés. Sa syntaxe est la suivante :

```
ldapsearch [-n] [-u] [-v] [-t] [-A] [-T] [-C] [-V] [-M] [-P] [-L] [-d
niveau_débogage] [-e nom_fichier_clé] [-f fichier] [-D DN_liaison] [[-W]| [-
w mot_de_passe_liaison]] [-h hôte_LDAP] [-p port_LDAP] [-b base_recherche] [-
s étendue] [-a suppr_réf] [-l limite_temps] [-z limite_taille] [-Z[Z]] filter
[attributs....]
```

REMARQUE : sur les serveurs NetWare, cet utilitaire est appelé lsearch.

L'outil ldapsearch établit une connexion avec un serveur LDAP, crée une liaison et lance une recherche à l'aide du filtre. Ce filtre doit correspondre à la représentation de type chaîne définie pour les filtres LDAP dans la norme RFC 2254 (http://www.ietf.org/rfc/rfc2254.txt).

Si ldapsearch trouve des entrées, les attributs définis par attrs sont récupérés et les entrées et leurs valeurs sont affichées sur la sortie standard. Si aucun attribut n'est listé, tous les attributs sont renvoyés.

SUGGESTION : Le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier, par exemple ldapsearch [options] filter [liste d'attributs] > out.txt.

Option	Description
-a *suppr_réf*	Indique comment gérer la suppression des références aux alias. Les valeurs suivantes sont utilisées : ◆ Never : les références aux alias ne sont jamais supprimées lors de la localisation de l'objet de base ou de la recherche. ◆ Always : les références aux alias sont systématiquement supprimées lors de la localisation de l'objet de base et de la recherche. ◆ Search : les références aux alias ne sont pas supprimées lors de la localisation de l'objet de base, mais bien lors de la recherche de ses subordonnés. ◆ Find : les références aux alias sont supprimées lors de la localisation de l'objet de base, mais pas lors de la recherche de ses subordonnés.
-A	Récupère uniquement des attributs (aucune valeur). Cette fonction est utile lorsque vous voulez savoir si un attribut figure dans une entrée et que les valeurs proprement dites ne vous intéressent pas.
-CC	Active le suivi des renvois. (liaison authentifiée avec les mêmes DN et mot de passe de liaison)
-b *base_recherche*	Utilisez *base_recherche* comme point de départ de la recherche.
-L	Affiche les entrées au format LDIF.
-LL	Affiche les entrées au format LDIF sans commentaires.
-LLL	Affiche les entrées au format LDIF sans commentaires ni version.
-s *étendue*	Définit l'étendue de la recherche. L'étendue peut être « base », « one » ou « sub » pour spécifier une recherche portant respectivement sur un objet de base, sur un niveau ou sur une sous-arborescence. La valeur par défaut est « sub ».
-S *attribut*	Trie les entrées renvoyées selon l'attribut. Par défaut, les entrées renvoyées ne sont pas triées. Si l'attribut est une chaîne vide («»), les entrées sont triées sur la base des composants de leur nom distinctif. Pour plus d'informations, reportez-vous à ldap_sort. Notez que ldapsearch affiche normalement les entrées au fur et à mesure qu'il les reçoit. Lorsqu'elle est activée, l'option S annule ce comportement. Toutes les entrées sont alors récupérées, triées, puis affichées.
-t	Écrit les valeurs binaires récupérées dans un ensemble de fichiers temporaires. Cette fonction est utile pour traiter des valeurs non ASCII comme jpegPhoto ou audio.
-tt	Écrit toutes les valeurs dans des fichiers temporaires.
-T *chemin*	Écrit les fichiers dans le répertoire indiqué par path (chemin d'accès). Le répertoire par défaut est /tmp.
-u	Inclut dans la sortie la forme conviviale du nom distinctif (DN).
-V	Préfixe d'URL pour les fichiers.
-V *préfixe*	Préfixe d'URL pour les fichiers. Le préfixe par défaut est file://tmp/.
-z *limite_taille*	Essaie d'atteindre la valeur *limite_taille* avant d'arrêter la recherche.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP », page 335.

Exemples

La commande suivante :

```
ldapsearch "cn=mark smith" cn telephoneNumber
```

recherche dans une sous-arborescence (à l'aide de la base de recherche par défaut) les entrées dont la valeur commonName est mark smith. Les valeurs commonName et telephoneNumber sont récupérées et affichées sur la sortie standard. Si deux entrées sont détectées, cette sortie peut se présenter comme suit :

```
cn=Mark D Smith, ou="College of Literature, Science, and the Arts",
ou=Students, ou=People, o=University of Michigan, c=US

cn=Mark Smith

cn=Mark David Smith

cn=Mark D Smith 1

cn=Mark D Smith

telephoneNumber=+1 313930-9489

cn=Mark C Smith, ou=Information Technology Division, ou=Faculty and Staff,
ou=People,o=University of Michigan, c=US

cn=Mark Smith

cn=Mark C Smith 1

cn=Mark C Smith

telephoneNumber=+1 313764-2277
```

La commande :

```
ldapsearch -u -t "uid=mcs" jpegPhoto audio
```

recherche dans une sous-arborescence (à l'aide de la base de recherche par défaut) les entrées dont l'ID utilisateur est mcs. La forme conviviale du nom distinctif de l'entrée s'affiche dans la sortie après la ligne comportant le nom distinctif proprement dit et les valeurs jpegPhoto et audio sont récupérées et écrites dans des fichiers temporaires. Si la recherche permet d'obtenir une entrée avec une valeur pour chacun des attributs demandés, la sortie peut se présenter comme suit :

```
cn=Mark C Smith, ou=Information Technology Division, ou=Faculty and Staff,
ou=People, o=University of Michigan, c=US

Mark C Smith, Information Technology Division, Faculty and Staff, People,
University of Michigan, US

audio=/tmp/ldapsearch-audio-a19924

jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

La commande suivante effectue sur le niveau c=US une recherche à un niveau de toutes les organisations dont le nom commence par university :

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

Les résultats de cette recherche sont affichés au format LDIF. Les valeurs des attributs organizationName et description sont récupérées et affichées sur la sortie standard, ce qui donne un résultat semblable au suivant :

```
dn: o=University of Alaska Fairbanks, c=US

o: University of Alaska Fairbanks

description: Preparing Alaska for a brave new yesterday.
```

```
description: leaf node only
dn: o=University of Colorado at Boulder, c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research
dn: o=University of Colorado at Denver, c=US
o: University of Colorado at D
```

ndsindex

L'utilitaire ndsindex crée, liste, suspend, reprend ou supprime des index. Sa syntaxe est la suivante :

```
ndsindex list [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w
<mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] [<nom_index1>,
<nom_index2>.....]

ndsindex add [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w
<mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]]
<définition_index1> [<définition_index2>.....]

ndsindex delete [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w
<mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] <nom_index1>
[<nom_index2>.....]

ndsindex resume [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w
<mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] <nom_index1>
[<nom_index2>.....]

ndsindex suspend [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w
<mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] <nom_index1>
[<nom_index2>.....]
```

REMARQUE : sur les serveurs NetWare, cet utilitaire est appelé nindex.

Option	Description
list	Liste les index spécifiés. Si aucun index n'est spécifié, ndsindex liste tous les index existants sur le serveur.
add	Crée de nouveaux index.
delete	Supprime les index spécifiés.
resume	Reprend les index hors ligne spécifiés.
suspend	Suspend les index spécifiés en les mettant hors ligne.
-s *DN_serveur_eDirectory*	DN du serveur eDirectory.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP », page 335.

Exemples

Pour lister les index du serveur Mon_Hôte, entrez la commande suivante :

```
ndsindex list -h Mon_Hôte -D cn=admin, o=ma_société -w mot_de_passe -s
cn=Mon_Hôte, o=novell
```

Pour créer un index de sous-chaîne appelé Mon_Index sur l'attribut d'adresse électronique, entrez la commande suivante :

```
ndsindex add -h mon_hôte -D cn=admin, o=ma_société -w mot_de_passe -s
cn=mon_hôte, o=novell "Mon_Index;adresse électronique;substring"
```

Pour créer un index de valeur appelé Mon_Index sur l'attribut de ville, entrez la commande suivante :

```
ndsindex add -h mon_hôte -D cn=admin, o=ma_société -w mot_de_passe -s
cn=mon_hôte, o=novell "Mon_Index;ville;value"
```

Pour créer un index de sous-chaîne appelé Mon_Index sur l'attribut de numéro de téléphone personnel, entrez la commande suivante :

```
ndsindex add -h mon_hôte -D cn=admin, o=ma_société -w mot_de_passe -s
cn=mon_hôte, o=novell "Mon_Index;téléphone domicile;presence"
```

Pour supprimer l'index Mon_Index, entrez la commande suivante :

```
ndsindex delete -h mon_hôte -D cn=admin, o=ma_société -w mot_de_passe -s
cn=mon_hôte, o=novell Mon_Index
```

Pour suspendre l'index Mon_Index, entrez la commande suivante :

```
ndsindex suspend -h mon_hôte -D cn=admin, o=ma_société -w mot_de_passe -s
cn=mon_hôte, o=novell Mon_Index
```

Pour reprendre l'index Mon_Index, entrez la commande suivante :

```
ndsindex resume -h mon_hôte -D cn=admin, o=ma_société -w mot_de_passe -s
cn=mon_hôte, o=novell Mon_Index
```

Filtre de recherche de concordance extensible

Les spécifications du noyau du protocole LDAP 3 définies dans la norme RFC 2251 (http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2251.html) imposent aux serveurs LDAP de reconnaître un élément de recherche appelé « filtre de concordance extensible ». La concordance extensible permet à un client LDAP de définir les éléments suivants dans un filtre de recherche :

- un nom d'attribut facultatif ;
- une règle de concordance facultative ;
- un drapeau servant à préciser si les attributs dn doivent être traités comme faisant partie de l'entrée ;
- la valeur à utiliser pour la concordance.

Voici la représentation sous forme de chaîne du filtre de recherche de concordance extensible :

```
extensible = attr [":dn"] [":" matchingrule] ":=" value /
             [:dn"] ":" matchingrule ":=" value
```

Le tableau ci-dessous liste les paramètres du filtre de recherche de concordance extensible :

Paramètre	Description
attr	Définit l'attribut sur lequel établir la concordance.
[":dn"]	Indique que la règle de concordance doit être incluse dans la comparaison.
[":" règle_concordance]	Désigne la règle de concordance à utiliser.
":="	En l'absence de règle de concordance, entraîne une égalité.
valeur	Valeur de comparaison

ExtensibleMatch est un nouveau filtre fourni par LDAP 3. En l'absence du champ matchingRule, le champ d'attribut DOIT être présent, et la recherche d'égalité est effectuée pour cet attribut. Si le champ d'attribut est absent et la règle matchingRule présente, la valeur matchValue est comparée à tous les attributs d'une entrée prenant en charge cette règle, et cette dernière détermine la syntaxe de la valeur d'assertion.

Le résultat de l'élément de filtre :

- est TRUE (vrai) s'il correspond à au moins un attribut de l'entrée.
- est FALSE (faux) s'il ne correspond à aucun attribut de l'entrée.
- n'est pas défini si matchingRule n'est pas reconnue ou si assertionValue ne peut être analysée.

Si le champ de type et la règle matchingRule sont présents, matchingRule DOIT être une règle autorisée pour ce type. Dans le cas contraire, l'élément de filtre est indéfini. Si:dn est spécifié dans le filtre de recherche, la concordance est également effectuée pour tous les attributs du nom distinctif d'une entrée, et renvoie TRUE (vrai) s'il y a au moins un attribut de nom distinctif pour lequel l'élément de filtre donne la valeur TRUE (vrai). Le champ dnAttributes est présent afin d'éviter de faire appel à plusieurs versions des règles de concordance génériques, par exemple pour la correspondance de mots, l'une s'appliquant aux entrées et l'autre aux entrées et aux attributs dn.

Pour l'essentiel, un filtre de concordance extensible permet à un client LDAP d'atteindre deux objectifs :

- prendre en charge plusieurs règles de concordance pour le même type de données ;
- inclure des éléments DN dans les critères de recherche ;

  La spécification de DN permet la recherche de concordance sur certains éléments du DN.

Novell eDirectory 8.7.3 (ou version ultérieure) prend en charge le filtre de concordance extensible pour les recherches de correspondance sur des attributs de DN. Les autres éléments du filtre de recherche de concordance extensible, notamment la règle de concordance, sont traités comme indéfinis et ignorés. La recherche de concordance sur le DN permet à un client LDAP de réduire considérablement les recherches nécessaires pour localiser un objet dans une arborescence eDirectory. Par exemple, un filtre de recherche LDAP complexe, tel que

```
(&(ou:dn:=sales)(objectclass=user))
```

permet d'obtenir la liste de tous les objets Utilisateur appartenant à la fonction Ventes (c'est-à-dire situés n'importe où sous les conteneurs Ventes).

Exemples d'utilisation

Voici plusieurs exemples de représentations sous forme de chaîne du filtre de recherche de concordance extensible prises en charge dans eDirectory 8.7.3 (ou version ultérieure).

```
(o:dn:=Ace Industry)
```

Cet exemple illustre l'emploi de la notation :dn. Lorsque le système évalue la concordance, les attributs du nom distinctif d'une entrée sont considérés comme faisant partie de l'entrée. Dans cet exemple, le type de concordance est l'égalité.

```
(:dn:2.4.8.10:=Dino)
```

Cet exemple présente un filtre qui doit être appliqué à n'importe quel attribut d'une entrée. Les attributs contenus dans le DN et auxquels la règle de concordance 2.4.8.10 s'applique doivent également être pris en compte.

Voici quelques exemples de représentations sous forme de chaîne du filtre de recherche de concordance extensible qui ne sont *pas* prises en charge dans eDirectory 8.7.3 :

```
(cn:1.2.3.4.5:=John Smith)
```

Cet exemple présente un filtre qui indique le type d'attribut cn et la valeur John Smith. Il implique que le serveur d'annuaire établit la correspondance en fonction de la règle de concordance identifiée par l'oid 1.2.3.4.5.

```
(sn:dn:2.4.6.8.10:=Barbara Jones)
```

Cet exemple illustre l'utilisation de la notation :dn pour indiquer que la règle de concordance 2.4.6.8.10 doit être utilisée lors des comparaisons et que les attributs du nom distinctif d'une entrée doivent être considérés comme faisant partie de cette dernière lors de l'évaluation de la correspondance.

13 Configuration des services LDAP pour Novell eDirectory

Le programme d'installation de eDirectory™ installe automatiquement les services LDAP pour Novell® eDirectory. Pour plus d'informations sur l'installation de eDirectory, reportez-vous au manuel *Novell eDirectory 8.8 Installation Guide* (Guide d'installation de Novell eDirectory 8.8).

Cette section fournit les informations suivantes :

Pour plus d'informations sur les outils LDAP, consultez le site Web LDAP Tools (http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html) (Outils LDAP).

Chargement et déchargement des services LDAP pour eDirectory

Pour charger les services LDAP pour eDirectory, entrez les commandes suivantes :

Serveur	Commande
NetWare®	À l'invite de la console, entrez **`load nldap.nlm`**
Windows	Dans l'écran DHOST (NDSCONS), cliquez sur Nldap.dlm > Démarrer.
Linux, Solaris, AIX ou HP-UX	À l'invite de Linux, Solaris, AIX ou HP-UX, entrez **`/opt/novell/eDirectory/sbin/nldap -l`**

Entrez les commandes suivantes pour décharger les services LDAP pour eDirectory :

Serveur	Commande
NetWare	À l'invite de la console, entrez **`unload nldap.nlm`**
Windows	Dans l'écran DHOST (NDSCONS), cliquez sur nldap.dlm > Arrêter.
Linux, Solaris, AIX et HP-UX	Pour décharger LDAP, dans la page de gestion à distance DHOST, cliquez sur l'icône *LDAP v3 pour Novell eDirectory 8.8* pour arrêter ce service. ou À l'invite de Linux, Solaris, AIX ou HP-UX, entrez **`/opt/novell/eDirectory/sbin/nldap -u`**

Vérification du chargement du serveur LDAP

Avant de configurer les objets LDAP, vérifiez que le serveur LDAP est chargé et qu'il fonctionne. Cette section explique comment vérifier que le serveur LDAP est chargé. Pour vous assurer que le serveur est en fonctionnement, reportez-vous à la section « Vérification du fonctionnement du serveur LDAP », page 349.

Sous NetWare

Pour savoir si nldap.nlm est chargé sur un serveur NetWare, entrez l'une des commandes suivantes dans la console du serveur :

- **`ldap display activity`**

  Si nldap.nlm n'est pas chargé, le serveur renvoie un message indiquant que la commande est inconnue `Unknown command`.

  Dans NetWare 6.*x*, l'affichage apparaît dans l'écran de l'outil de consignation et non dans celui de la console.

- **`ldap display config`**
- **`modules nldap.nlm`**

Vous pouvez également utiliser Novell iManager.

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Gestionnaire de services.
3. Sélectionnez une connexion, un serveur, un nom DNS ou une adresse IP, puis cliquez sur OK.
4. Spécifiez votre mot de passe, puis cliquez sur OK.
5. Cliquez sur LDAP Agent for Novell eDirectory 8.8
   (Agent LDAP pour Novell eDirectory 8.8).

   La section Informations sur le module affiche nldap.nlm dans le champ de nom du fichier.

Sous Windows 2000/NT

1. Sur un serveur Windows, ouvrez ndscons.exe.

   Cliquez sur Démarrer > Paramètres > Panneau de configuration > Services Novell eDirectory.

2. Dans l'onglet Services, faites défiler la liste pour atteindre nldap.dlm, puis affichez la colonne État.

   La colonne affiche En cours d'exécution.

Vous pouvez également utiliser Novell iManager.

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Gestionnaire de services.
3. Sélectionnez une connexion, un serveur, un nom DNS ou une adresse IP, puis cliquez sur OK.
4. Spécifiez votre mot de passe, puis cliquez sur OK.
5. Cliquez sur LDAP Agent for Novell eDirectory 8.8
   (Agent LDAP pour Novell eDirectory 8.8).

   La section Informations sur le module affiche nldap.nlm dans le champ de nom du fichier.

Vérification du chargement sous Linux et UNIX

Identifiez libnldap.so ou libnldap.sl. Ce nom peut être un lien symbolique vers un nom de fichier plus long, auquel s'ajoutent des informations de version.

De même, chaque fichier libnldap.so ou libnldap.sl correspond à un fichier binaire différent pour chaque plate-forme Linux et UNIX.

Vous pouvez également utiliser le fichier ndsd.log ou ndstrace pour vérifier que le serveur LDAP est chargé.

Vérification du fonctionnement du serveur LDAP

Une fois le serveur LDAP chargé, assurez-vous qu'il est exécuté. Vérifiez ensuite qu'un périphérique est à l'écoute.

- « Scénarios », page 349
- « Vérification du fonctionnement du serveur LDAP », page 350
- « Vérification de l'écoute d'un périphérique », page 352

Scénarios

En règle générale, le serveur LDAP s'exécute dès qu'il est chargé. Toutefois, deux scénarios peuvent empêcher le bon fonctionnement du serveur.

Scénario: le serveur est en état de veille. Le serveur LDAP se charge à condition que les chargeurs NetWare ou DHost puissent résoudre les dépendances externes. Toutefois, le serveur LDAP ne fonctionne correctement qu'après avoir été correctement configuré par les objets Serveur LDAP et Groupe LDAP.

Tant que le serveur LDAP est dans un état chargé mais non actif (état de veille), il tente régulièrement de trouver et de lire les objets de configuration. Si les objets sont mal configurés ou corrompus, le serveur LDAP reste en état de veille jusqu'à son déchargement ou sa désactivation (nldap.nlm, nldap.dlm, libnldap.so ou libnldap.sl).

Les chargeurs indiquent que le serveur LDAP est chargé. Toutefois, aucun port LDAP (389, 636) n'est ouvert par nldap.nlm (par nldap.dlm, libnldap.so ou libnldap.sl). En outre, aucune requête de client LDAP n'est satisfaite.

Des messages DSTrace signalent les tentatives régulières et la raison pour laquelle le serveur ne peut passer en mode d'exécution.

Scénario : refus de service. Chez Digital Airlines, le serveur traite une très longue recherche (d'au moins 20minutes). L'opération revient, dans les faits, à rechercher une aiguille dans une botte de foin.

Pendant la recherche, Henri effectue l'une des opérations suivantes :

- Il change un paramètre de configuration et met à jour un objet de configuration.
- Il clique sur Refresh Server Now (Rafraîchir le serveur maintenant).
- Il décharge le serveur LDAP (nldap.nlm, nldap.dlm, libnldap.so ou libnldap.sl).
- Il tente d'arrêter l'ensemble du serveur.

Le serveur LDAP attend la fin des opérations en cours avant d'appliquer une mise à jour. Il diffère également l'exécution de nouvelles opérations tant que la mise à jour n'est pas terminée. Avant d'avoir terminé sa recherche et d'avoir pu se rafraîchir, le serveur peut sembler ne plus répondre aux nouvelles requêtes. De même, il peut également sembler bloqué pendant le déchargement.

Lorsque la requête de recherche est longue, mais génère de nombreuses occurrences et qu'Henri souhaite commencer décharger le serveur LDAP, la recherche est annulée pour procéder rapidement au déchargement lorsque l'occurrence suivante est renvoyée au client. Toutefois, si en 20minutes, la recherche ne renvoie qu'un seul ou aucun résultat, le serveur LDAP ne peut pas renoncer à la requête NDS® ou eDirectory en cours.

La recherche ne sera pas abandonnée pour un rafraîchissement ou une mise à jour, même si elle renvoie de nombreuses occurrences au client.

Vérification du fonctionnement du serveur LDAP

Pour vérifier la bonne exécution du service LDAP, employez l'utilitaire d'importation, de conversion et d'exportation (ICE) de Novell. Sur un poste de travail, exécutez ice.exe à partir de la ligne de commande ou utilisez Novell iManager ou ConsoleOne®.

Dans la ligne de commande

1. Accédez au répertoire qui contient ice.exe (par exemple, c:\novell\consoleone\1.2\bin).
2. Exécutez ice.exe.

   Recherchez rootDSE. N'oubliez pas d'inclure les paramètres qui identifient les gestionnaires source et d'exportation. Par exemple, entrez

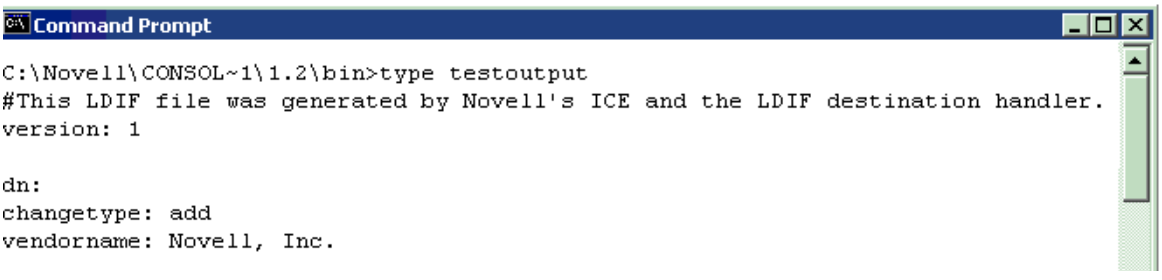
   ```
   ice -S LDAP -s 10.128.45.0 -p 389 -c base -a vendorname -D LDIF -f
   testoutput
   ```

Paramètre et valeur	Description
-S LDAP	Désigne LDAP comme gestionnaire source.
-s 10.128.45.0	Indique le nom DNS ou l'adresse IP du serveur.
-p 389	Spécifie le numéro de port du serveur LDAP identifié par le paramètre du gestionnaire source LDAP. La valeur par défaut est 389. Si le port installé n'est pas le 389, indiquez le numéro correct en texte clair.
-c base	Indique que l'étendue de la requête de recherche se limite uniquement à l'entrée de l'objet de base.
-a vendorname	Spécifie que la recherche doit récupérer l'attribut vendorname.
-D LDIF	Désigne LDIF comme gestionnaire cible.
-f testoutput	Indique le nom du fichier pouvant consigner les enregistrements LDIF.

Cet exemple envoie une sortie vers un fichier testoutput.

Pour plus d'informations sur l'utilisation de ICE, reportez-vous à la section « Utilitaire d'importation, de conversion et d'exportation Novell », page 147. Pour plus d'informations sur les gestionnaires source LDAP, reportez-vous à la section « Options du gestionnaire source LDAP », page 160. Pour plus d'informations sur les gestionnaires cible LDIF, reportez-vous à la section « Options du gestionnaire cible LDIF », page 160.

3 Affichez les résultats de la commande ICE.



L'exemple (étapes 2 et 3) limite la sortie de l'entrée rootDSE à l'attribut Vendor Name. Les données étant lues sur un serveur Novell eDirectory, Novell, Inc. s'affiche comme si Novell les fournissait.

Utilisation de Novell iManager

Pour vérifier que le serveur LDAP fonctionne avec Novell iManager, suivez la procédure mentionnée à la section « Exportation de données vers un fichier », page 149.

Si, après avoir saisi une adresse IP et un numéro de port, vous obtenez une connexion, le serveur est fonctionnel. Dans le cas contraire, vous obtenez un message d'erreur. Téléchargez (affichez) le fichier journal ou le fichier d'exportation.

Utilisation de ConsoleOne

Pour vérifier que le serveur LDAP fonctionne avec ConsoleOne, reportez-vous à la section « Exécution d'une exportationLDIF », page 169.

Indiquez un chemin et un nom de fichier dans le champ Sélectionner un fichier LDIF cible (par exemple, c:\ldap\textoutput.txt). Si vous saisissez uniquement un nom de fichier, le snap-in LDAP de ConsoleOne consigne le fichier dans le répertoire par défaut (généralement, c:\novell\consoleone\1.2\bin).

Vérification de l'écoute d'un périphérique

Vérifiez qu'un périphérique écoute le port 389.

Pour NetWare:

1. À l'invite de la console du serveur, entrez

   ```
   tcpcon
   ```

2. Sélectionnez Informations de protocole > TCP > Connexions TCP.
3. Sélectionnez 389 dans la colonne Port.

   Si la colonne État affiche Listen (Écouter), cela signifie qu'un périphérique est à l'écoute de ce port.

   Dans le cas contraire, le port est tout simplement manquant.

Pour Windows 2000/NT et UNIX

1. Dans la ligne de commande, entrez

   ```
   netstat -a
   ```

2. Localisez une ligne dans laquelle l'adresse locale est *nom_serveur*:389 et l'état LISTENING (Écoute).

Si l'une des situations suivantes se produit, lancez Novell iMonitor:

- Vous ne parvenez pas à obtenir d'informations de l'utilitaire ICE.
- Vous n'êtes pas certain que le serveur LDAP gère les requêtes LDAP.

Pour plus d'informations sur Novell iMonitor, reportez-vous aux sections « Fichiers de configuration », page 199 et « Configuration des paramètres Trace », page 206.

Pour plus d'informations sur les requêtes LDAP, reportez-vous à la section «Communicating with eDirectory through LDAP» (Communication avec eDirectory via LDAP) dans le manuel *Novell eDirectory 8.8 Installation Guide (Guide d'installation de Novell eDirectory 8.8)*.

Configuration des objets LDAP

Une installation eDirectory crée un objet Serveur LDAP et un objet Groupe LDAP. La configuration par défaut des services LDAP est consignée dans ces deux objets. Vous pouvez la modifier en utilisant soit le snap-in LDAP de ConsoleOne, soit la tâche de gestion LDAP de Novell iManager.

L'objet Serveur LDAP renferme des données de configuration propres au serveur.

L'objet Groupe LDAP contient des informations de configuration pouvant aisément être partagées par plusieurs serveurs LDAP. Cet objet fournit des données de configuration communes et représente un groupe de serveurs LDAP. Les serveurs ont des données communes.

Vous pouvez associer plusieurs objets Serveur LDAP à un objet Groupe LDAP. Tous les serveurs LDAP associés obtiennent alors la configuration spécifique à leur serveur de l'objet Serveur LDAP, mais reçoivent les informations communes ou partagées de l'objet Groupe LDAP.

Par défaut, le programme d'installation de eDirectory installe un seul objet Groupe LDAP et un seul objet Serveur LDAP pour chaque fichier nldap.nlm ou nldap.dlm. Par la suite, vous pouvez associer plusieurs objets Serveur LDAP à un objet Groupe LDAP unique.

IMPORTANT : bien qu'il soit possible de combiner les dernières versions d'un objet Serveur LDAP à des versions moins récentes d'objets Groupe LDAP, nous vous recommandons de ne pas le faire. Évitez par exemple d'associer un objet Groupe LDAP de eDirectory 8.5 à un objet Serveur LDAP de eDirectory 8.6.

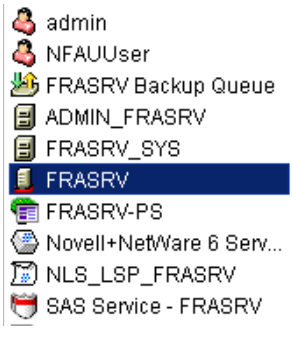
La quantité d'informations communes contenues dans un objet Groupe LDAP est limitée. Les données des attributs étant extrêmement courantes, LDAP n'a pas besoin de lire de nombreux attributs. De nombreux serveurs LDAP devront utiliser les mêmes données. En l'absence d'objet Groupe commun ou partagé, vous serez obligé de répliquer ces données sur chaque serveur LDAP.

En revanche, l'objet Serveur LDAP prend en charge davantage d'options et de données de configuration propres au serveur que l'objet Groupe LDAP.

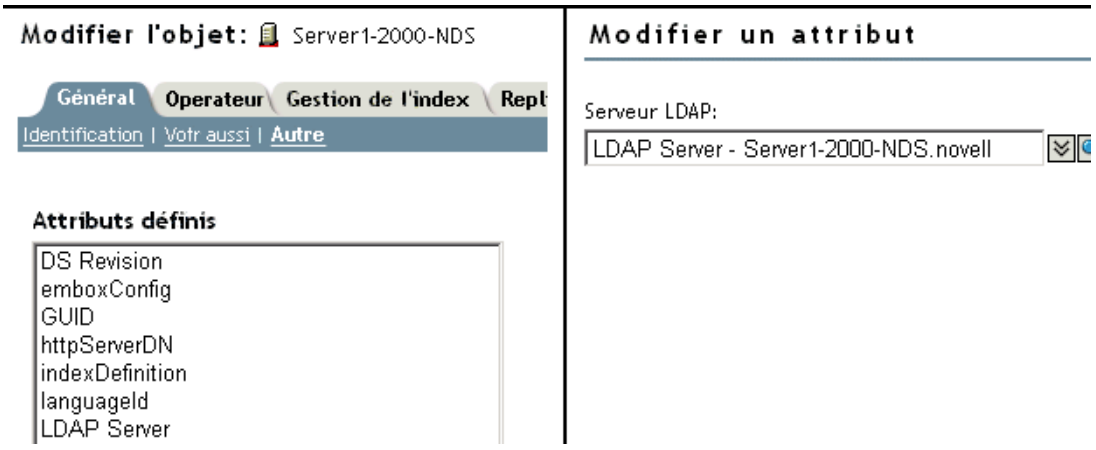
Les deux objets possèdent des attributs de syntaxe DN qui pointent les uns vers les autres.

Pour que le serveur LDAP puisse trouver ses données de configuration, une autre association est nécessaire. Elle est effectuée via le serveur NCP™, qui contient les données de configuration courantes de eDirectory. Elle est effectuée automatiquement par le programme d'installation de eDirectory.

Chaque serveur eDirectory possède un objet serveur NCP. Dans la figure suivante, le serveur Lundi illustre cet objet, tel qu'il s'affiche dans iManager :



Cet objet présente l'attribut Serveur LDAP, qui pointe vers l'objet Serveur LDAP d'un serveur hôte eDirectory en particulier. La figure suivante illustre cet attribut :



En règle générale, les objets Serveur LDAP, Groupe LDAP et Serveur NCP sont situés dans le même conteneur. Vous nommez ce conteneur pendant l'installation de eDirectory en même temps que le serveur et que le contexte Admin.

Si vous déplacez l'objet Serveur LDAP, vous devez le placer dans une réplique accessible en écriture.

Configuration d'objets Serveur LDAP et Groupe LDAP sur des systèmes Linux, Solaris, AIX ou HP-UX

L'utilitaire de configuration de LDAP est l'utilitaire ldapconfig. Vous pouvez l'utiliser sur des systèmes Linux, Solaris, AIX ou HP-UX pour modifier, afficher et rafraîchir les attributs des objets Serveur LDAP et Groupe LDAP.

Utilisez la syntaxe suivante pour afficher des valeurs d'attribut LDAP sur des systèmes Linux, Solaris, AIX et HP-UX :

```
ldapconfig get [...] | set liste_valeurs_attribut  [-t nom_arborescence | -p nom_hôte[:port]] [-w mot_de_passe] [-a FDN_utilisateur] [-f]
```

```
ldapconfig [-t nom_arborescence | -p nom_hôte[:port]] [-w mot_de_passe] [-a FDN_utilisateur] [-V] [-R] [-H] [-f] -v attribut,attribut2...
```

Utilisez la syntaxe suivante pour modifier des valeurs d'attributs LDAP sur des systèmes Linux, Solaris, AIX et HP-UX :

```
ldapconfig [-t nom_arborescence | -p nom_hôte[:port]] [-w mot_de_passe] [-a FDN_admin] -s attribut=valeur,...
```

Paramètre	Description
-t *nom_arborescence*	Nom de l'arborescence eDirectory sur laquelle installer le composant.
-p *nom_hôte*	Nom de l'hôte. Vous pouvez également indiquer le nom DNS ou l'adresse IP.
-w	Mot de passe de lutilisateur disposant des droits dadministrateur.

Paramètre	Description
-a	Nom distinctif complet de lutilisateur disposant des droits dadministrateur. Par exemple : cn=user.o=org1
get | -V	Permet d'afficher tous les attributs des objets Serveur/Groupe LDAP.
get | -v *liste d'attributs*	Affiche les valeurs actuelles des attributs dans la liste qui les contient.
set | -s *paires attribut-valeur*	Définit les attributs avec les valeurs spécifiées.
-v	Permet d'afficher la valeur de l'attribut LDAP.
-s	Définit une valeur pour un attribut des composants installés.
-R	Rafraîchit le serveur LDAP.
-V	Permet d'afficher les paramètres de configuration LDAP actuels.
-H	Permet d'afficher les chaînes de syntaxe et d'aide.
-f	Autorise les opérations sur une réplique filtrée.
attribut	Nom configurable des attributs Serveur ou Groupe LDAP. Pour plus d'informations, reportez-vous au « Attributs de l'objet Serveur LDAP », page 355 et à l'« Attributs de l'objet Groupe LDAP », page 357.

Exemples

Pour afficher la valeur de l'attribut dans la liste qui le contient, saisissez la commande suivante :

```
ldapconfig [-t nom_arborescence | -p nom_hôte[:port]]
  [-w mot_de_passe] [-a FDN_utilisateur] -v "Exiger TLS en cas de liaison
  simple avec mot de passe","searchTimeLimit"
```

Pour configurer le numéro de port TCP LDAP et la limite de taille de recherche à 1000, entrez la commande suivante :

```
ldapconfig [-t nom_arborescence | -p nom_hôte[:port]]
  [-w mot_de_passe] [-a FDN_admin] -s "Port TCP
  LDAP=389","searchSizeLimit=1000"
```

Attributs de l'objet Serveur LDAP

L'objet Serveur LDAP permet de configurer et de gérer les propriétés du serveur LDAP Novell.

Le tableau suivant décrit les attributs du serveur LDAP :

Attribut	Description
LDAP Server	Nom distinctif complet de l'objet Serveur LDAP de eDirectory.
LDAP Host Server	Nom distinctif complet du serveur hôte eDirectory sur lequel le serveur LDAP est exécuté.
LDAP Group	Objet Groupe LDAP de eDirectory auquel ce serveur LDAP appartient.

Attribut	Description
LDAP Server Bind Limit	Nombre de clients qui peuvent établir simultanément une liaison avec le serveur LDAP. La valeur 0 (zéro) indique qu'il n'existe aucune limite.
LDAP Server Idle Timeout	Période d'inactivité d'un client, à l'issue de laquelle le serveur LDAP interrompt la connexion avec ce client. La valeur 0 (zéro) indique qu'il n'existe aucune limite.
LDAP Enable TCP	Indique si les connexions TCP (non TLS) sont activées pour ce serveur LDAP. Valeur = 1 (oui), 0 (non)
LDAP Enable TLS	Indique si les connexions TLS sont activées pour ce serveur LDAP. Valeur = 1 (oui), 0 (non)
LDAP TCP Port	Numéro de port sur lequel le serveur LDAP reste à l'écoute de connexions TCP (non SSL). Plage = de 0 à 65535
LDAP TLS Port	Numéro de port sur lequel le serveur LDAP reste à l'écoute de connexions TLS. Plage = de 0 à 65535, nombre maximal de connexions autorisées sur le serveur LDAP.
keyMaterialName	Nom de l'objet Certificat de eDirectory associé à ce serveur LDAP et utilisé pour les connexions LDAP SSL.
searchSizeLimit	Nombre maximal d'entrées renvoyées par le serveur LDAP à un client LDAP en réponse à une recherche. La valeur 0 (zéro) indique qu'il n'existe aucune limite.
searchTimeLimit	Nombre maximal de secondes après lesquelles le serveur LDAP abandonne la recherche LDAP pour cause de dépassement de délai. La valeur 0 (zéro) indique qu'il n'existe aucune limite.
filteredReplicaUsage	Indique si le serveur LDAP doit utiliser une réplique filtrée pour une recherche LDAP. Valeurs = 1 (utiliser une réplique filtrée), 0 (ne pas utiliser de réplique filtrée)
sslEnableMutualAuthentication	Indique si l'authentification mutuelle SSL (authentification client basée sur un certificat) est activée sur le serveur LDAP.
ldapTLSVerifyClientCertificate	Active ou désactive la vérification du certificat du client pour une opération TLS qui passe par LDAP.
ldapNonStdAllUserAttrsMode	Active ou désactive les attributs opérationnels, non standard et de type Tous les utilisateurs.

Attribut	Description
ldapBindRestrictions	Applique les restrictions de liaison LDAP aux connexions client LDAP. Vous pouvez autoriser ou interdire les liaisons anonymes des clients LDAP. Valeurs = 0, 1 0 autorise les liaisons anonymes des clients. 1 empêche les clients d'établir des liaisons anonymes.
ldapEnablePSearch	Indique si la fonction de recherche persistante est activée ou non sur le serveur LDAP. Valeurs = true, false
ldapMaximumPSearchOperations	Nombre entier qui limite le nombre d'opérations de recherche persistante simultanées. La valeur zéro autorise un nombre illimité d'opérations de recherche persistante.
ldapIgnorePSearchLimitsForEvents	Indique si les limites de taille et de durée doivent être ignorées après que la requête de recherche persistante a envoyé le jeu de résultats initial. Valeurs = true, false Si la valeur False est sélectionnée pour cet attribut, l'ensemble des opérations de recherche persistante est soumis aux limites de recherche. Si l'une des limites est atteinte, la recherche échoue et le message d'erreur approprié apparaît.

Attributs de l'objet Groupe LDAP

L'objet Groupe LDAP permet de définir et de gérer le type d'accès autorisé pour les clients LDAP aux informations figurant sur le serveur LDAP Novell et l'utilisation qu'ils en font.

Pour exiger TLS en vue d'effectuer des liaisons simples, reportez-vous à la section « Utilisation de TLS en cas de liaison simple avec mot de passe », page 359. Cet attribut indique si le serveur LDAP autorise la transmission de mots de passe en texte clair de la part d'un client LDAP. Valeurs = 0 (non) ou 1 (oui).

Pour spécifier un renvoi par défaut ainsi que la méthode de traitement des renvois LDAP par les serveurs LDAP, reportez-vous à la section « Utilisation des renvois », page 367.

Rafraîchissement du serveur LDAP

Après avoir modifié une option ou un paramètre de configuration sur un serveur LDAP, vous devez rafraîchir le serveur pour que les changements soient pris en compte.

Vous ne pouvez cependant pas le rafraîchir lorsque des requêtes LDAP sont en cours de traitement. Par exemple, si une opération prend 15minutes pour parcourir l'arborescence eDirectory, le rafraîchissement n'aura lieu qu'à l'expiration de ce délai.

De même, vous ne pouvez pas arrêter le serveur LDAP lorsque ses threads sont en activité.

Lorsqu'un rafraîchissement est planifié, le serveur LDAP retarde le démarrage des nouvelles requêtes LDAP jusqu'à ce qu'il soit exécuté.

Par défaut, toutes les trente minutes, le serveur LDAP vérifie les tampons horaires sur les objets Serveur LDAP et Groupe LDAP afin de détecter les éventuels changements de paramètres. S'il en détecte, le serveur les applique.

S'il constate que les tampons horaires des paramètres n'ont pas changé, aucun rafraîchissement n'a lieu. (Si vous imposez un rafraîchissement, le serveur ignore les tampons horaires et applique les modifications.)

Pour rafraîchir le serveur LDAP, effectuez l'une des opérations ci-dessous :

- Avec Novell iManager.

  1. Dans la page Rôles et tâches, cliquez sur LDAP > Présentation LDAP > Afficher les serveurs LDAP.
  2. Cliquez sur Serveur LDAP, puis sur Rafraîchir.

- Attendez que le serveur se reconfigure durant l'intervalle de rafraîchissement.

- Déchargez puis rechargez le fichier nldap.nlm.

  Il n'est pas nécessaire de décharger des programmes NLM™ préalablement requis avant de décharger le fichier nldap.nlm.

  Nldap.nlm décharge, puis recharge les programmes dépendant de NLM.

- Dans la ligne de commande, modifiez l'intervalle de rafraîchissement.

  Cette option peut s'avérer utile si vos liaisons WAN ne sont pas actives en permanence. Vous pouvez au besoin augmenter ou réduire temporairement la pulsation du serveur.

  Cette modification n'est pas permanente. Vous devez entrer la commande lors de chaque chargement du fichier nldap.nlm.

  À l'invite de la console du serveur, entrez

  `ldap refresh [=] [`*`date`*`][`*`heure`*`][`*`intervalle`*`]`

  - Le format de la variable de date est mm:jj:aaaa. Si vous entrez des zéros dans tous les champs de date, la date actuelle est utilisée.
  - Le format de la variable d'heure est hh:mm:ss. Si vous entrez des zéros dans tous les champs d'heure, l'heure actuelle est utilisée.
  - Le format de l'intervalle est égal à 0 ou compris entre 1 et 2147483647 minutes. Si vous entrez zéro, la valeur par défaut utilisée est 30 minutes.

  Vous pouvez ajouter cette commande au fichier autoexec.ncf dans le répertoire sys:\system. Placez la commande après la ligne qui charge nldap.nlm.

Authentification et sécurité

Cette section fournit les informations suivantes :

- « Utilisation de TLS en cas de liaison simple avec mot de passe », page 359
- « Démarrage et arrêt de TLS », page 359
- « Configuration du serveur pour TLS », page 360
- « Configuration du client pour TLS », page 361
- « Exportation de la racine approuvée », page 362

- « Authentification auprès d'un certificat client », page 362
- « Utilisation d'autorités de certification de fournisseurs tiers », page 363
- « Utilisation de SASL », page 364

Utilisation de TLS en cas de liaison simple avec mot de passe

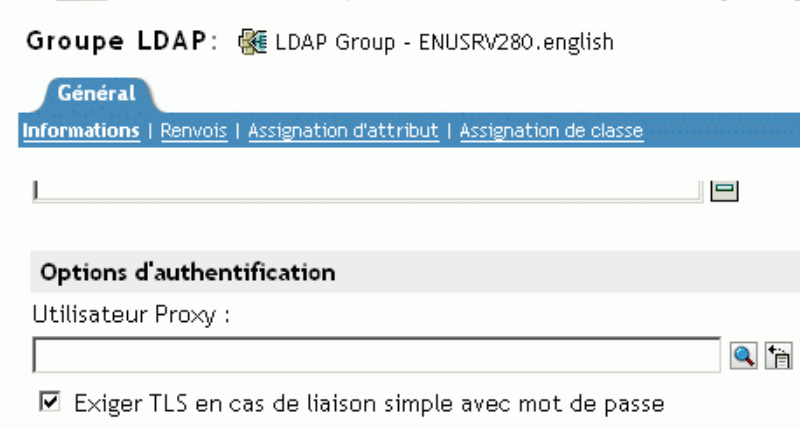
Le protocole SSL (Secure Socket Layer) 3.1 était à l'origine diffusé via Netscape. L'IETF s'est approprié cette norme en mettant en oeuvre TLS (Transport Layer Security) 1.0.

TLS permet de coder les connexions dans la couche Session. Il n'est pas nécessaire d'utiliser un port codé pour obtenir une connexion TLS. Il existe une autre façon de procéder : le port 636 est le port TLS implicite et le serveur LDAP lance automatiquement une session TLS lorsqu'un client se connecte au port sécurisé.

Un client peut également se connecter au port en texte clair et utiliser ultérieurement TLS pour passer d'une connexion en clair à une connexion codée.

Pour exiger TLS en cas de liaison simple avec mot de passe :

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur LDAP > Présentation LDAP > Afficher les groupes LDAP.
3. Cliquez sur l'objet Groupe LDAP, puis sur Informations dans l'onglet Général.
4. Cochez la case Exiger TLS en cas de liaison simple avec mot de passe.



5. Cliquez sur Appliquer, puis sur OK.

Démarrage et arrêt de TLS

L'opération étendue LDAP STARTTLS permet de passer d'une connexion en clair à une connexion codée. Cette fonction constituait une nouveauté de eDirectory 8.7.

Lorsque vous employez une connexion codée, c'est la totalité du paquet qui est codée. De ce fait, les analyseurs réseau (ou sniffers) sont dans l'impossibilité de diagnostiquer les données envoyées sur le réseau.

Scénario: avec STARTTLS – Vous créez une connexion en clair (sur le port 389) et effectuez quelques recherches anonymes. Toutefois, lorsque vous accédez à des données sécurisées, vous préférez lancer une session TLS. Vous exécutez donc une opération étendue STATTLS pour passer d'une connexion en clair à une connexion codée. Vos données sont alors sécurisées.

Vous arrêtez TLS pour passer d'une session codée à une session en clair. Avec les connexions en clair, la surcharge est moindre du fait qu'il n'est pas nécessaire de coder et décoder les données destinées au client et provenant de celui-ci. Les données sont donc acheminées plus rapidement. À ce stade, la connexion est rétrogradée à l'état Anonyme.

Pour vous authentifier, vous utilisez l'opération de liaison LDAP. La liaison établit votre ID en fonction des références que vous avez fournies. Lorsque vous arrêtez TLS, le service LDAP supprime les authentifications préalablement établies. Votre état d'authentification devient alors Anonyme. Par conséquent, pour passer à un autre état qu'Anonyme, vous devez de nouveau vous authentifier.

Scénario: nouvelle authentification – Henri lance STOPTLS. Son état devient Anonyme. Pour accéder à ses fichiers sur Internet et les utiliser, Henri exécute la commande Bind, fournit ses références de login et, après avoir été authentifié, se remet à travailler en texte clair sur Internet.

Configuration du serveur pour TLS

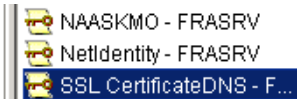
Lorsqu'une instance de session TLS est créée, un processus de reconnaissance mutuelle intervient. Le serveur et le client échangent des données. Le serveur détermine la façon dont cette reconnaissance se produit. Pour prouver qu'il est le serveur légitime, ce dernier envoie toujours son certificat au client. Cette reconnaissance garantit au client que le serveur est bien celui prévu.

Pour exiger que le client établisse également sa légitimité, vous définissez une valeur sur le serveur. Il s'agit de l'attribut ldapTLSVerifyClientCertificate.

Valeur	Description
0	Inactif. Pendant un processus de reconnaissance mutuelle, le serveur fournit un certificat au client. Il n'impose jamais au client d'envoyer un certificat. Ce dernier peut utiliser le certificat ou l'ignorer. Une session sécurisée est établie.
1	Pendant le processus de reconnaissance mutuelle, le serveur fournit au client un certificat et demande à ce dernier de lui en faire parvenir un. Le client peut choisir de retourner son certificat. Le certificat du client est validé. Si le serveur ne peut pas le valider, il met fin à la connexion. Si le client n'envoie aucun certificat, le serveur maintient la connexion.
2	Pendant le processus de reconnaissance mutuelle, le serveur impose au client de lui faire parvenir un certificat. S'il ne le fournit pas ou si le certificat ne peut pas être validé, le serveur met fin à la connexion.

Pour que le serveur puisse prendre en charge TLS, vous devez lui fournir un certificat X.509 qu'il utilisera pour établir sa légitimité.

Ce certificat est fourni automatiquement pendant l'installation de eDirectory. C'est au cours de cette procédure que des objets Matériel clé sont créés, dans le cadre de l'infrastructure PKI (Public Key Infrastructure) et des services NMAS™ (Novell Modular Authentication Services). La figure suivante présente ces objets dans iManager :



L'installation associe automatiquement l'un de ces certificats au serveur LDAP. Dans Novell iManager, l'onglet Connexions de l'objet Serveur LDAP affiche un DN. Il représente le certificat X.509. Le champ Certificat du serveur de la figure suivante illustre ce DN.

Dans Novell iManager, vous pouvez parcourir le système jusqu'aux certificats d'objet Matériel clé (KMO). La liste déroulante vous permet de changer de certificat. Le certificat DNS ou IP fonctionne.

Dans le cadre de la validation, le serveur doit contrôler le nom (adresse IP matérielle ou DN) qui figure dans le certificat.

Pour établir une connexion TLS, vérifiez ce qui suit :

- Le serveur LDAP doit connaître l'objet Matériel clé du serveur.
- Vous devez vous connecter au port sécurisé ou lancer TLS après vous être connecté au port en clair.

Une fois le serveur LDAP reconfiguré, rafraîchissez-le. Pour plus de détails, reportez-vous à la section « Rafraîchissement du serveur LDAP », page 357. ConsoleOne et Novell iManager rafraîchissent automatiquement le serveur.

Configuration du client pour TLS

Un client LDAP est une application (par exemple Netscape Communicator, Internet Explorer ou ICE). Il doit être en mesure de comprendre l'autorité de certification qu'emploie le serveur LDAP.

Lorsqu'un serveur est ajouté dans une arborescence eDirectory, l'installation crée par défaut :

- une autorité de certification pour l'arborescence (la CA de l'arborescence) ;
- un KMO à partir de la CA de l'arborescence.

Le serveur LDAP emploie ce fournisseur de certificat.

Le client doit importer un certificat dans lequel il a confiance, afin de valider la CA de l'arborescence que le serveur LDAP affirme utiliser. Cette importation est impérative pour que, lorsque le serveur envoie son certificat, le client puisse le valider et vérifier l'authenticité du serveur.

Pour pouvoir établir une connexion sécurisée, le client doit être configuré avant la connexion.

La méthode d'importation du certificat par le client diffère en fonction du type d'application utilisée. Chaque application doit avoir une méthode pour importer un certificat. Le navigateur Netscape possède la sienne, Internet Explorer également et ICE en utilise une troisième. Tous trois sont des clients LDAP différents. Chaque client possède sa méthode pour localiser les certificats dans lesquels il a confiance.

Exportation de la racine approuvée

Vous pouvez exporter automatiquement la racine approuvée tout en acceptant le serveur de certificats.

Pour exporter manuellement la racine approuvée, consultez le site Web Exporting a Trusted Root or Public Key Certificate (Exportation d'un certificat de racine approuvée ou de clé publique) (http://www.novell.com/documentation/lg/crt221ad/index.html).

La fonctionnalité d'exportation crée le fichier indiqué. Bien qu'il soit possible de modifier son nom, il peut s'avérer utile de garder DNS ou IP dans celui-ci, de manière à pouvoir reconnaître le type d'objet Matériel. Laissez également le nom du serveur.

Installez l'autorité de certification auto-assignée dans tous les navigateurs établissant des connexions LDAP sécurisées avec eDirectory.

Si vous utilisez le certificat avec des produits Microsoft (par exemple, Internet Explorer), conservez l'extension .der.

Si des applications ou des SDK requièrent le certificat, importez-le dans une base de données de certificats.

Internet Explorer 5 exporte automatiquement les certificats racine lors de chaque mise à jour du registre. L'extension classique .X509 utilisée par Microsoft est indispensable.

Authentification auprès d'un certificat client

L'authentification mutuelle exige une session TLS et un certificat client. Le serveur et le client doivent l'un et l'autre vérifier que leur correspondant est bien l'objet qu'il prétend être. Le certificat client a été validé au niveau de la couche Transport. Toutefois, au niveau de la couche du protocole LDAP, le client est anonyme jusqu'à ce qu'il effectue une requête de liaison LDAP.

À ce stade, le client a établi son authenticité vis-à-vis du serveur, mais pas de LDAP. Si un client souhaite s'authentifier à l'aide de l'identité mentionnée dans le certificat client, il exécute une opération de liaison en utilisant le mécanisme SASL EXTERNAL.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur LDAP > Présentation LDAP.
3. Cliquez sur Afficher les serveurs LDAP, puis cliquez sur le nom d'un objet Serveur LDAP.
4. Cliquez sur Connexions.
5. Dans la section TLS (Transport Layer Security), sélectionnez le menu déroulant Certificat client, puis cliquez sur Requis.

   L'authentification mutuelle est alors activée.
6. Cliquez sur Appliquer, puis sur OK.

Utilisation d'autorités de certification de fournisseurs tiers

Pendant l'installation de eDirectory, le serveur LDAP reçoit une autorité de certification (CA) de l'arborescence. L'objet Matériel clé LDAP repose sur cette CA. Tout certificat qu'un client envoie au serveur LDAP doit pouvoir être validé via cette CA de l'arborescence.

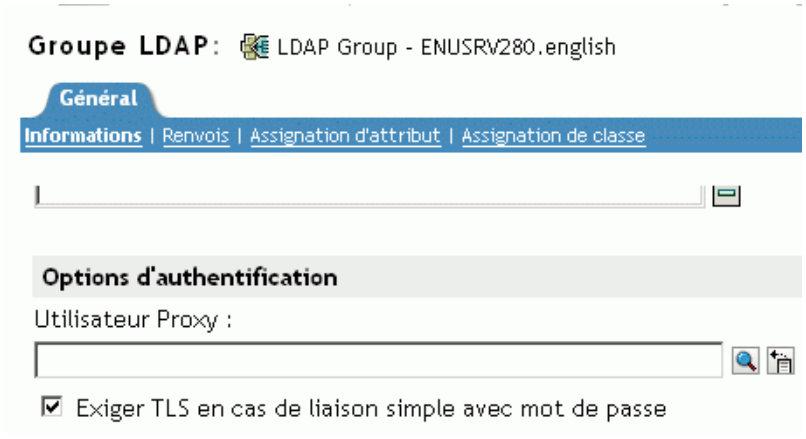
Les services LDAP pour eDirectory 8.8 prennent en charge plusieurs autorités de certification. L'autorité de certification d'arborescence Novell n'est que l'une d'entre elles. Le serveur LDAP peut en avoir d'autres (par exemple VeriSign*, une société externe). Ce type d'autorité de certification supplémentaire est également une racine approuvée.

Pour configurer le serveur LDAP afin qu'il utilise plusieurs autorités de certification, définissez l'attribut ldapTLSTrustedRootContainer sur l'objet Serveur LDAP. En faisant référence à plusieurs autorités de certification, le serveur LDAP permet à un client d'employer un certificat d'une autorité externe.

Création et emploi d'utilisateurs proxy LDAP

Novell eDirectory assigne l'identité [Public] aux utilisateurs qui ne sont pas authentifiés. Dans le protocole LDAP, un utilisateur non authentifié est un utilisateur anonyme. Par défaut, le serveur LDAP accorde aux utilisateurs anonymes les droits d'une identité [Public]. Grâce à ces droits, les utilisateurs eDirectory non authentifiés et les utilisateurs anonymes de LDAP peuvent parcourir eDirectory en utilisant les droits [Public].

Le serveur LDAP permet également aux utilisateurs anonymes de se servir des droits d'un autre utilisateur proxy. La valeur correspondante est située dans l'objet Groupe LDAP. Dans Novell iManager, cette valeur est le champ Utilisateur proxy. Dans ConsoleOne, elle correspond au champ Nom d'utilisateur proxy. La figure suivante illustre ce champ dans Novell iManager.



L'utilisateur proxy est un nom distinctif. Vous pouvez lui accorder d'autres droits que ceux dont bénéficie l'utilisateur Public. Avec l'utilisateur proxy, vous pouvez contrôler l'accès d'un client LDAP anonyme à des conteneurs spécifiques de l'arborescence eDirectory.

REMARQUE : n'imposez pas de restrictions de login à l'utilisateur proxy, sauf si vous souhaitez les voir appliquées à l'ensemble des utilisateurs LDAP anonymes.

Scénario: configuration d'un utilisateur proxy NLDAP – Digital Airlines a passé un contrat avec DataSure, un groupe de recherche. DataSure utilisera LDAP pour accéder aux résultats des enquêtes et les stocker sur DigitalAir43, serveur sous NetWare 6 de Digital Airlines. Vous ne souhaitez pas que DataSure dispose des droits Public sur les répertoires de DigitalAir43.

Vous pouvez donc créer un utilisateur proxy LDAP et lui assigner des droits spécifiques sur DataSure. Vous indiquez le Nom distinctif du proxy dans l'objet Groupe LDAP, et rafraîchissez le serveur. Le serveur emploie alors automatiquement les droits de l'utilisateur proxy pour tout utilisateur anonyme nouveau ou existant.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration eDirectory > Créer un objet et créez un utilisateur proxy (par exemple, LDAPProxy).
3. Affectez un mot de passe nul à cet utilisateur.
4. (Facultatif) Assignez à l'utilisateur proxy des droits sur les répertoires spécifiés.
5. Cliquez sur LDAP > Présentation LDAP > Afficher les groupes LDAP > objet Groupe LDAP.
6. Dans le champ Utilisateur Proxy, cliquez sur le bouton Parcourir, sélectionnez l'utilisateur LDAPProxy, puis cliquez sur OK.

Utilisation de SASL

SASL (Simple Authentication and Security Layer) définit divers mécanismes d'authentification qui doivent être enregistrés auprès de IANA (Internet Assigned Numbers Authority). Le serveur LDAP gère les mécanismes suivants :

- DIGEST-MD5
- EXTERNAL
- NMAS_LOGIN
- GSSAPI

Ces mécanismes sont déployés sur le serveur pendant une installation ou une mise à niveau de eDirectory. Toutefois, sous Linux et UNIX, vous devez exécuter l'utilitaire nmasinst pour installer les méthodes NMAS.

Le serveur LDAP interroge SASL pour connaître les mécanismes installés lors de sa configuration et prend automatiquement en charge les éléments installés. Le serveur LDAP signale également les mécanismes SASL pris en charge dans son entrée rootDSE à l'aide de l'attribut supportedSASLMechanisms.

Comme ces mécanismes sont enregistrés, vous devez les saisir entièrement en majuscules. Dans le cas contraire, le serveur LDAP ne les reconnaîtra pas.

Le protocole de liaison LDAP autorise le client à utiliser différents mécanismes SASL pour l'authentification. Lorsque l'application utilise l'API de liaison LDAP, elle doit choisir la liaison simple et fournir un DN et un mot de passe ou opter pour la liaison SASL et indiquer le nom du mécanisme SASL en majuscules, ainsi que toute référence SASL associée requise par le mécanisme.

DIGEST-MD5

Le mécanisme DIGEST-MD5 n'a pas besoin de TLS. Le serveur LDAP prend en charge DIGEST-MD5 sur les connexions en clair et sécurisées.

LDAP prend en charge les mécanismes SASL dans le cadre de la demande de liaison. Au lieu de demander une liaison LDAP simple (DN et mot de passe en texte clair), vous demandez une liaison LDAP SASL. Cette requête renvoie un DN et des références MD5.

MD5 fournit un hachage codé des mots de passe. Ces derniers sont codés même sur les connexions en clair. C'est la raison pour laquelle le serveur LDAP accepte les mots de passe utilisant MD5 sur le port en texte clair ou le port codé.

Si quelqu'un analyse cette connexion, le mot de passe ne peut pas être détecté. Toutefois, la connexion peut être simulée ou piratée.

Ce mécanisme est une liaison LDAP SASL (et non une liaison simple). Par conséquent, le serveur LDAP accepte ces requêtes, même si vous avez coché la case Exiger TLS en cas de liaison simple avec mot de passe pendant l'installation.

EXTERNAL

Le mécanisme EXTERNAL informe le serveur LDAP qu'un DN utilisateur et des références ont déjà été fournis au serveur. De ce fait, il n'est pas nécessaire que le DN et les références soient soumis à la demande de liaison.

La demande de liaison LDAP à l'aide du mécanisme SASL EXTERNAL demande au serveur d'effectuer les opérations suivantes :

- demander les références à la couche EXTERNAL ;
- authentifier l'utilisateur comme correspondant à ces références et à l'utilisateur concerné.

Une reconnaissance mutuelle sécurisée a eu lieu. Le serveur a demandé des références au client et ce dernier les lui a transmises. Le serveur LDAP a reçu le certificat envoyé par le client, l'a transmis au module NMAS et a authentifié l'utilisateur en fonction du DN transmis dans le certificat.

Pour disposer d'un certificat avec un DN utilisable, quelques opérations de configuration sont nécessaires sur le client. Pour plus d'informations sur la configuration du certificat, consultez la documentation en ligne NMAS (http://www.novell.com/documentation/beta/nmas30/index.html).

Même si le client envoie un mécanisme EXTERNAL, la requête peut ne pas être satisfaite par le serveur LDAP. Novell iMonitor peut fournir les raisons de cet échec :

- La connexion n'est pas sécurisée.
- Bien que la connexion soit sécurisée, le client n'a pas fourni le certificat requis pendant la procédure de reconnaissance mutuelle.
- Le module SASL est indisponible.
- Le client n'a pas vérifié rootDSE avant d'envoyer la requête.

NMAS_LOGIN

Le mécanisme NMAS_LOGIN permet au serveur LDAP d'accéder aux capacités biométriques de NMAS. Pour plus d'informations, consultez le Novell Developer Kit (NDK).

Lorsque le serveur est activé, le serveur LDAP s'initialise avec le module SASL et demande à ce dernier quels mécanismes sont à sa disposition.

Le client peut interroger rootDSE pour connaître l'attribut pris en charge par le mécanisme. Le serveur LDAP affiche ensuite les mécanismes pris en charge.

GSSAPI

Le mécanisme GSSAPI permet à un utilisateur Kerberos de s'authentifier auprès d'un serveur eDirectory à l'aide d'un ticket, sans devoir saisir de mot de passe utilisateur LDAP distinct.

Cette fonctionnalité est destinée aux utilisateurs d'applications LDAP dans des environnements disposant d'une infrastructure Kerberos existante. Ces utilisateurs doivent pouvoir utiliser des tickets délivrés par le serveur Kerberos afin de s'authentifier auprès du serveur LDAP sans devoir fournir de mot de passe utilisateur LDAP distinct.

Pour plus d'informations sur la configuration de GSSAPI, reportez-vous à la section « Configuration de GSSAPI avec eDirectory », page 583.

Utilisation du serveur LDAP pour effectuer des recherches dans l'annuaire

Cette section fournit les informations suivantes :

Définition de limites de recherche

Les attributs suivants de l'objet Serveur LDAP contrôlent la méthode de recherche du serveur LDAP dans l'annuaire:

- Limite d'entrées de recherche

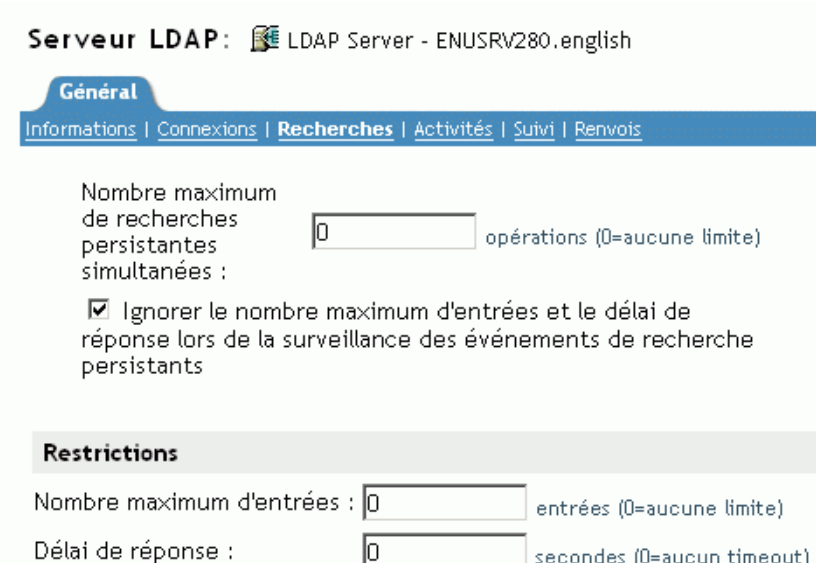
  Cette option limite la taille d'une recherche. La valeur par défaut est 0, indiquant qu'il n'y a pas de limite de taille. Afin d'éviter de surcharger le serveur LDAP, vous pouvez limiter le nombre d'entrées que le serveur LDAP renvoie lors d'une requête.

  Scénario: limitation de la taille d'une recherche – Henri lance une recherche qui peut renvoyer des milliers de réponses liées aux objets trouvés. Toutefois, vous avez défini une limite de dix résultats. Le serveur LDAP interrompt la recherche après avoir renvoyé dix résultats. Un message système informe Henri que la recherche a été arrêtée bien que d'autres données soient disponibles.

- Limite de temps de recherche

  Limite la durée de recherche du serveur. La valeur par défaut est 0, indiquant qu'il n'y a pas de limite de temps.

La figure suivante illustre ces attributs dans Novell iManager.



1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches.
2. Cliquez sur LDAP > Présentation LDAP > Afficher les serveurs LDAP.
3. Cliquez sur Objet Serveur LDAP > Recherches.
4. Faites défiler jusqu'à atteindre la section Restrictions, entrez des valeurs, puis cliquez sur OK.

Le client peut également définir des limites de temps pour les requêtes (par exemple, limiter la recherche à deux secondes). En cas de conflit entre la limite définie par le client et celle du serveur LDAP, ce dernier emploie la valeur la plus faible.

La recherche repose sur des ACL (Access Control Lists). De ce fait, une recherche anonyme peut renvoyer simplement quelques entrées, celles que l'utilisateur Public est autorisé à voir, même si l'annuaire en contient des milliers.

Utilisation des renvois

Un renvoi est une méthode qui permet au client de résoudre des noms. Un client LDAP envoie une requête à un serveur LDAP, qui tente de trouver localement l'entrée cible. Si le serveur ne parvient pas à trouver l'entrée cible, il utilise les références de connaissance dont il dispose pour générer un renvoi vers un second serveur qui possède plus d'informations sur l'entrée. Le premier serveur envoie les informations de renvoi au client LDAP.

Le client LDAP établit alors une connexion avec le second serveur LDAP et tente de nouveau l'opération. Si le second serveur LDAP possède l'entrée cible de l'opération, il l'exécute. Sinon, il transmet également un renvoi dans la réponse au client. Ce processus se poursuit jusqu'à ce que l'un des événements suivants se produise :

- Le client contacte un serveur qui possède l'entrée et peut effectuer l'opération voulue.
- Le serveur LDAP renvoie une erreur indiquant que l'entrée n'existe pas.
- Le serveur LDAP indique que plus aucun renvoi ne peut être suivi.

Une nouvelle fonctionnalité de LDAP pour eDirectory 8.7 occasionne un comportement légèrement différent des renvois par rapport aux anciennes versions de eDirectory et NDS. Ce changement de comportement influe sur la manière dont vous configurez les services LDAP.

Renvois par défaut

Généralement, une URL de renvoi par défaut contient une URL LDAP pointant vers un serveur qui contient la racine de l'arborescence. Une URL LDAP a la syntaxe suivante : ldap://*hôte*:*port*.

Entrez un renvoi par défaut dans le champ URL de renvoi par défaut:

Au départ, le serveur LDAP eDirectory envoyait le renvoi par défaut dans un certain nombre de situations de reprise après échec. De nombreux utilisateurs estimaient ce comportement étrange et parfois imprévisible. Les services LDAP pour eDirectory 8.8 vous permettent de contrôler le moment du renvoi par défaut pour n'importe quel type de renvoi subordonné.

La nouvelle option est une valeur (paramètre) qui réside dans l'attribut ldapDefaultReferralBehavior sur le serveur LDAP et les objets Groupe LDAP. Il s'agit d'un nombre entier qui est un masque binaire des bits ci-dessous.

Bits	Valeur
0x00000001	Le DN de base est introuvable.
0x00000002	Le DN de base est sur un serveur eDirectory non disponible.
0x00000004	Une entrée dans l'étendue de la recherche se trouve sur un serveur eDirectory non disponible.

Si pour l'opération, le serveur LDAP est configuré pour Toujours référer et si l'une des conditions indiquées est respectée et que la valeur correspondante est définie, le renvoi par défaut est exécuté.

Définition de renvois pour les opérations de recherche

Une fonctionnalité interagissant avec LDAP pour eDirectory 8.7 entraîne une légère modification du comportement des renvois par rapport aux anciennes versions de eDirectory et NDS. Ce changement de comportement influe sur la manière dont vous configurez les services LDAP.

Vous pouvez configurer le serveur LDAP eDirectory pour qu'il transmette les renvois à d'autres serveurs eDirectory de l'arborescence. Par défaut, le serveur LDAP chaîne toutes les opérations vers d'autres serveurs eDirectory pour le compte de l'utilisateur et aucun renvoi n'est jamais retourné.

Avant eDirectory 8.7, les options de renvoi n'existaient que comme paramètres de l'objet Groupe LDAP. Avec eDirectory 8.8, elles existent également pour l'objet Serveur LDAP. Tout paramètre de l'objet Serveur LDAP est prioritaire sur ceux de l'objet Groupe LDAP.

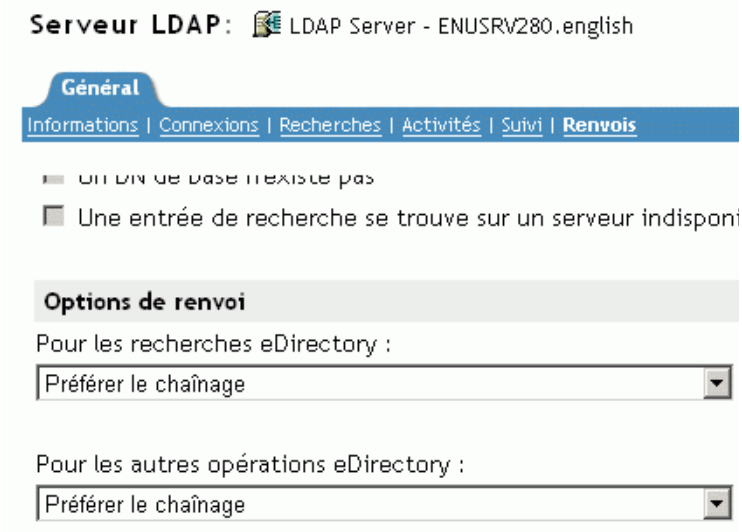
L'attribut ldapSearchReferralOption vous permet de définir l'option de renvoi. Dans les versions antérieures des services LDAP pour eDirectory 8.7, cet attribut pouvait être défini à l'aide des options suivantes :

- « Préférer le chaînage », page 370 (option par défaut)
- « Prefer Referrals (Préférer les renvois) », page 371
- « Toujours référer », page 371

Ces options de renvoi s'appliquent uniquement à la référence et au chaînage à d'autres serveurs eDirectory de l'arborescence eDirectory. Ces paramètres de configuration ne contrôlent pas les renvois provenant d'une partition non experte. Ainsi, même si vous sélectionnez une option (par exemple Toujours chaîner) dans la liste déroulante Options de renvois, les renvois parviendront toujours aux autres serveurs depuis des partitions non expertes.

Pour prendre en charge les renvois supérieurs vers des DSA non-eDirectory, les services LDAP pour eDirectory 8.7.a disposent d'une option Toujours chaîner. Pour plus de détails, reportez-vous à la section « Toujours chaîner », page 369.

La figure ci-dessous illustre les listes déroulantes de renvoi LDAP destinées aux recherches et aux autres opérations.



Les «autres» opérations eDirectory incluent des renvois pour les opérations d'ajout, de suppression, de modification et de liaison.

Toujours chaîner

L'option Toujours chaîner est une option indiquant qu'aucun renvoi ne sera jamais effectué. Si vous sélectionnez cette option, le serveur LDAP eDirectory ne retourne jamais les renvois à d'autres serveurs eDirectory de l'arborescence eDirectory. Le serveur LDAP effectue une vérification auprès des autres serveurs LDAP pour le compte du client demandeur et transmet le renvoi à celui-ci.

L'option Toujours chaîner s'avère très utile si eDirectory est déployé dans une arborescence fédérée globale sous la forme de serveurs subordonnés.

Ces options de renvoi s'appliquent uniquement à la méthode de gestion des renvois dans l'arborescence eDirectory. Elles n'ont aucun effet sur le comportement des renvois sur les serveurs non-eDirectory.

La raison du blocage des renvois sur d'autres serveurs eDirectory est subtile, mais peut s'avérer précieuse. Si les données non expertes d'un serveur eDirectory 8.7 ou ultérieur sont répliquées sur un autre serveur eDirectory, plus ancien, un renvoi au serveur plus ancien risque de fournir à une application client une vue déformée de l'arborescence globale.

Par exemple, imaginons qu'un client LDAP mette en cache les renvois vers les serveurs LDAP et envoie des requêtes au dernier serveur avec lequel il a communiqué. Si le client est configuré pour envoyer des requêtes à un serveur eDirectory prenant en charge les renvois supérieurs, l'arborescence globale devrait s'afficher normalement pour ce client.

Toutefois, les serveurs LDAP antérieurs à eDirectory 8.7 ne prennent pas en charge les zones non expertes et les renvois supérieurs. Par conséquent, si le client fait suivre un renvoi vers un serveur équipé d'une version plus ancienne de eDirectory dans l'arborescence eDirectory et continue à envoyer des requêtes à ce serveur plus ancien, le serveur ayant la version plus ancienne de LDAP présentera les données non expertes comme s'il s'agissait des données réelles de l'arborescence Annuaire.

Un client intelligent doit, cependant, interroger l'attribut supportedFeatures de RootDSE pour vérifier si le serveur prend ou non en charge les renvois supérieurs.

Préférer le chaînage

L'option Préférer le chaînage indique que les résultats de recherche ne comprennent généralement pas de renvois. Au lieu de cela, le serveur LDAP fait progresser l'opération de recherche sur l'ensemble des DSA eDirectory pour la compléter.

En revanche, les opérations de recherche accompagnées du contrôle de recherche persistante constituent une exception. Dans ce cas, comme la mise en oeuvre Novell de la recherche persistante ne prend pas en charge le chaînage, les renvois sont transmis si l'étendue de la recherche ne reste pas totalement locale.

Le serveur LDAP reçoit une opération de recherche. Si l'entrée de l'arborescence n'est pas stockée localement, le serveur effectue automatiquement un chaînage vers les autres serveurs. Une fois l'entrée localisée, le serveur LDAP joue le rôle de proxy pour le client LDAP. En utilisant la même identité que celle à laquelle le client LDAP est lié, le serveur LDAP s'authentifie auprès du serveur distant et continue l'opération de recherche sur celui-ci.

Le serveur LDAP qui a reçu la demande de recherche initiale envoie au client LDAP l'ensemble des entrées de recherche et le résultat. Comme le serveur LDAP se charge intégralement de la demande, le client LDAP ne sait pas que d'autres serveurs étaient impliqués.

Grâce au chaînage de eDirectory, un serveur LDAP qui contient peu d'informations peut sembler contenir les données de la totalité de l'arborescence.

L'option Préférer le chaînage est importante en ce qui concerne les partitions.

Scénario : recherche d'informations dans une autre partition – Dans la société Digital Airlines, Luc sélectionne l'option Préférer le chaînage pour le serveur LDAP DAir43. DAir43 se trouve dans la partitionA. La partitionB est une sous-partition deA et contient le serveur LDAP DAir44.

Un client LDAP lance une recherche. DAir43 recherche l'entrée localement mais ne trouve qu'une partie des données. DAir43 effectue automatiquement un chaînage vers DigitalAir44, qui contient l'entrée nécessaire. DAir44 envoie les données à DAir43, et ce dernier envoie l'entrée au client LDAP.

Avec l'option Préférer le chaînage, le serveur LDAP effectue un chaînage vers d'autres serveurs pour traiter les requêtes de recherche (le cas échéant), sauf si l'opération est une recherche persistante. Pour plus d'informations sur la recherche persistante, reportez-vous à la section « Recherche persistante : configuration en fonction des événements eDirectory », page 378.

Prefer Referrals (Préférer les renvois)

L'option Préférer les renvois indique que les opérations de recherche doivent retourner des renvois à d'autres serveurs eDirectory de l'arborescence le cas échéant. Des renvois sont émis seulement si le serveur local peut assurer que le serveur qui contient les données est opérationnel et que le service LDAP est exécuté. Dans le cas contraire, l'opération est chaînée à un autre serveur ou échoue si cet autre serveur est inutilisable.

Vous disposez de deux partitions et vous exécutez une recherche de sous-arborescence. Vous en arrivez à un stade où les entrées recherchées ne figurent plus sur le serveur local. La recherche doit donc porter sur un autre serveur. Si le serveur qui contient la réplique de ces données (de cette partition) exécute aussi le fichier nldap.nlm, le serveur LDAP crée un renvoi LDAP et le retourne au client LDAP.

Si le serveur contenant la réplique n'exécute pas nldap.nlm, le serveur LDAP chaîne la requête vers l'autre serveur, terminant ainsi la recherche.

Lorsque nldap.nlm démarre, le serveur LDAP indique à eDirectory que le serveur LDAP est un point de renvoi. Si un client a reçu des renvois mais que ceux-ci cessent, le serveur LDAP n'est pas en service.

Toujours référer

L'option Toujours référer suit la même logique que Préférer les renvois, si ce n'est que le renvoi par défaut est envoyé dans différentes situations de reprise après échec (par exemple si l'objet est introuvable ou si le serveur est hors service).

Si un autre serveur contenant le reste des données n'exécute pas le service LDAP, le premier serveur LDAP ne chaîne alors pas la requête au deuxième.

Si vous activez l'option Toujours référer, vous êtes autorisé à saisir un renvoi par défaut. Le champ Renvoi par défaut est utile pour associer deux serveurs LDAP de fournisseurs différents et constituer votre propre arborescence Annuaire.

Scénario: utilisation d'un serveur par défaut – Vous disposez d'une arborescence LDAP. Une partie de cette arborescence est gérée par eDirectory. Une partition subordonnée est gérée par iPlanet. Dans le champ Renvoi par défaut, vous placez une URL renvoyant au serveur iPlanet. Un client LDAP lance une recherche.

Incapable de résoudre le DN de base, le serveur LDAP envoie au client la chaîne qui figure dans le champ Renvoi par défaut. Le renvoi indique au client LDAP de rechercher à l'endroit indiqué dans l'URL. Le client LDAP contacte le serveur iPlanet, qui exécute la recherche.

Si un renvoi par défaut est configuré et que le serveur ne trouve pas le DN de base recherché, le client reçoit ce renvoi par défaut.

Le renvoi présente la forme d'une URL LDAP (par exemple, LDAP://123.23.45.6:389).

Lorsque le serveur LDAP transmet un renvoi par défaut à un client (parce que le DN de base est indisponible), il ajoute une barre oblique (/) et le DN recherché par le client. Le renvoi par défaut et les informations ajoutées sont transmis au client. Le client envoie la requête de recherche au serveur spécifié dans le renvoi par défaut.

L'objet Groupe LDAP comporte un champ de chaîne destiné au renvoi par défaut. Le serveur LDAP traite ces données comme une chaîne. Aucune validation n'a lieu. Tout ce qui est saisi est inséré au début du renvoi. Certaines données sont ajoutées à la fin de celui-ci. Le serveur LDAP s'attend à recevoir une chaîne semblable à une URL.

Lorsqu'ils reçoivent des renvois désignant d'autres serveurs eDirectory qui exécutent LDAP, les clients obtiennent deux renvois par serveur.

- un renvoi qui dirige le client vers le port en texte clair ;
- un renvoi qui dirige le client vers le port sécurisé.

Pour faire la différence entre les deux renvois, le renvoi en texte clair commence par ldap:// et le port sécurisé par ldaps//.

En cas de renvoi provenant du serveur, le numéro de port est ajouté.

Définition de renvois pour d'autres opérations

Le paramétrage initial de l'option de renvoi ne s'appliquait qu'à l'opération de recherche. Pour fournir à d'autres opérations une option comparable, l'attribut ldapOtherReferralOption est utilisé. Cet attribut autorise les mêmes valeurs et contrôle le comportement des opérations qui ne comprennent pas de recherche (à l'exception de la liaison, qui n'émet jamais de renvois).

Pas de prise en charge de la gestion de DSA IT

Dans les services LDAP pour eDirectory 8.8, les relations distribuées entre les serveurs eDirectory d'une arborescence eDirectory sont gérées par d'autres moyens que la commande Gérer DSA IT. La commande Gérer DSA IT n'autorise pas le client LDAP à interroger ou à mettre à jour les références eDirectory subordonnées ou croisées.

Fonctionnalité non prise en charge

Les services LDAP pour eDirectory 8.8 ne prennent pas en charge les références subordonnées. Il n'est pas possible de créer de façon fiable une partition non experte qui soit subordonnée à une partition experte et de lui faire émettre des renvois. Si optez pour ce cas de figure, les renvois ne sont transmis que lors de la résolution du DN de base pour une opération. Les références SearchResultReferences ne sont pas envoyées.

Il n'existe aucune prise en charge des mises à jour distribuées de données dans la zone non experte. Si un changement de nom se produit sur le serveur racine, il n'existe aucun mécanisme intégré permettant de copier cette modification sur le serveur eDirectory qui contient les mêmes données dans une zone non experte.

Recherche de répliques filtrées

Un filtre limite la quantité de données que contient la réplique. De ce fait, une réplique filtrée n'affiche pas l'ensemble des données réelles contenues dans l'annuaire. Voici quelques exemples de filtres appliqués à une réplique :

- La réplique contient uniquement des objets Utilisateur.
- La réplique contient tous les objets Utilisateur, mais ces derniers ne contiennent que des numéros de téléphone et des adresses d'expédition.

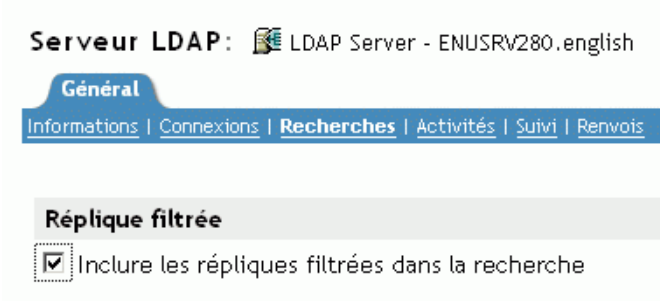
Comme les données d'une réplique filtrée sont incomplètes, une recherche LDAP peut donner lieu à des résultats tronqués. Par conséquent, une requête de recherche LDAP n'examine pas, par défaut, les répliques filtrées.

Lorsque vous effectuez une recherche dans les répliques filtrées, celle-ci peut ne pas retourner les résultats par filtre de réplique dans les cas suivants :

- Si les objets correspondant au filtre de recherche ne sont pas présents sur le serveur de répliques filtrées locales, les résultats peuvent ne pas correspondre au filtre de la réplique locale, dans la mesure où les résultats peuvent être trouvés par un serveur de répliques complètes.
- Lorsque la base de recherche ne se trouve pas en local sur le serveur de répliques filtrées, les objets correspondant au filtre de recherche peuvent être obtenus sur un serveur de répliques complètes, mais peuvent ne pas correspondre au filtre de la réplique locale.

Vous pouvez cependant configurer un serveur LDAP pour rechercher dans les répliques filtrées si vous êtes certain que ces dernières contiennent les données dont vous avez besoin.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur LDAP > Présentation LDAP.
3. Cliquez sur Afficher les serveurs LDAP, puis cliquez sur le nom d'un serveur LDAP.
4. Cliquez sur Recherches.
5. Sélectionnez Inclure les répliques filtrées dans la recherche et cliquez sur Appliquer.



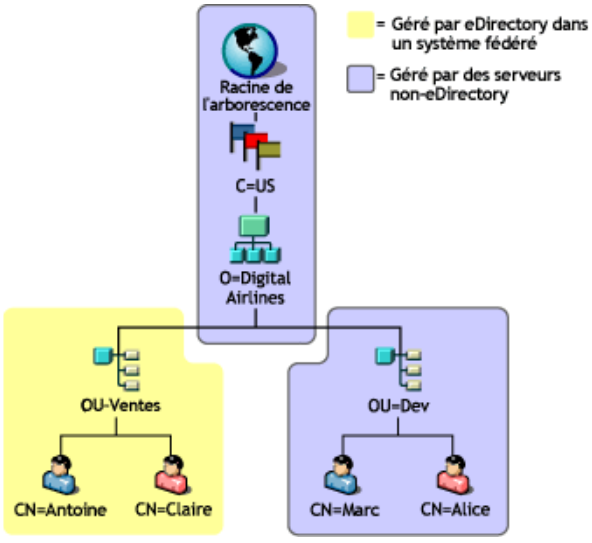
Configuration des renvois supérieurs

Il arrive souvent que les déploiements importants nécessitent une arborescence Annuaire utilisant des logiciels Serveur LDAP de différents fournisseurs. Elle est alors appelée arborescence fédérée globale. Les services LDAP pour eDirectory 8.8 ont la capacité de retourner des renvois à un DSA supérieur de l'arborescence fédérée.

Scénario : renvois supérieurs dans une arborescence fédérée

Luc est responsable des réseaux de Digital Airlines. Un serveur OpenLDAP est utilisé pour gérer la racine d'une arborescence Annuaire de Digital Airlines (de la racine de l'arborescence à O=Digital Airlines). Une organisation (OU=Ventes) est gérée par un serveur eDirectory, et une autre (OU=Dév) réside sur un serveur iPlanet.

La figure suivante illustre cette arborescence :



eDirectory ne gère que les données de la partition pour OU=Ventes. Les données des autres zones sont gérées sur des DSA non-eDirectory. Luc configure les services LDAP de telle sorte qu'ils retournent des renvois supérieurs à chaque fois qu'une opération prend racine sur O=Digital Airlines ou au-dessus, ou à n'importe quel point sous O=Digital Airlines qui ne fait pas partie de la hiérarchie OU=Ventes.

Une opération est envoyée au serveur LDAP eDirectory, avec le DN de base OU=Dév, O=Digital Airlines, C=US. Le renvoi retourné pointe vers les serveurs qui contiennent cette entrée ou vers ceux qui savent quels serveurs la contiennent.

De même, lors d'une recherche dans la sous-arborescence ayant comme racine O=Digital Airlines, C=US débouche sur un renvoi au DSA racine. Ce dernier retourne à son tour des renvois vers les DSA qui gèrent OU=Ventes et OU=Dév.

Pour que le serveur eDirectory puisse intégrer cette arborescence, les services LDAP permettent à eDirectory de disposer des données hiérarchiques supérieures dans une partition marquée comme non experte. Les objets de la zone non experte sont seulement les entrées nécessaires à l'élaboration d'une hiérarchie DN correcte. Ces entrées sont similaires aux entrées de substitution « Glue » X.500.

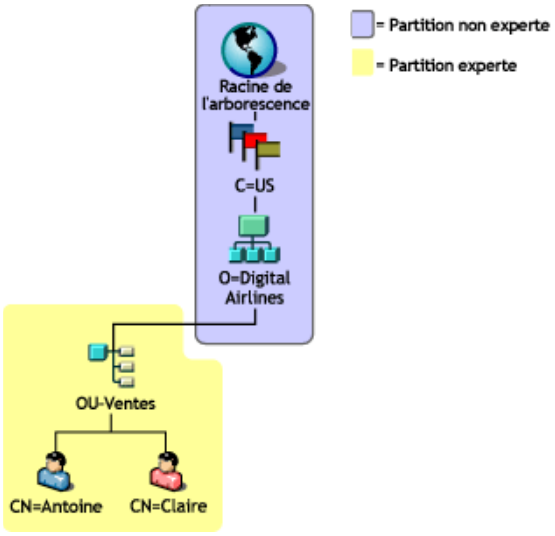
Dans ce scénario, les objets Racine, C=US et O=Digital Airlines résident sur le serveur eDirectory dans une zone non experte.

eDirectory permet de placer des informations de connaissance (données de renvoi) à l'intérieur de zones non expertes. Ces informations servent à retourner les renvois au client LDAP.

Lorsqu'une opération LDAP est effectuée dans une zone non experte de l'arborescence eDirectory, le serveur LDAP recherche les données de référence correspondantes et transmet un renvoi au client.

Création d'une zone non experte

La figure suivante illustre les données réelles de l'arborescence fédérée sur le serveur eDirectory présentée à la section « Scénario : renvois supérieurs dans une arborescence fédérée », page 373.



Notez que des entrées sont situées au-dessus de OU=Ventes, même si elles sont gérées par un autre DSA. Ce placement est nécessaire pour fournir les DN corrects aux entrées gérées par le serveur eDirectory.

Pour créer une zone non experte :

1. Séparez les données non expertes des données expertes.

   Créez une limite de partition au sommet de la zone experte. Un serveur eDirectory se considère expert pour toutes les données qu'il contient, sauf indication contraire.

2. Marquez la partition racine comme non experte.

   2a Ajoutez l'attribut expert à l'entrée la plus proche de la racine dans la partition.

   2b Attribuez la valeur zéro à l'attribut expert.

3. Tracez une limite au bas de la zone non experte.

   Créez des racines de partition dans les zones de la sous-arborescence pour lesquelles ce serveur doit être expert. Par exemple, dans la figure ci-dessus, l'entrée OU=Ventes est une racine de partition. Dans les nouvelles partitions, l'attribut expert n'est pas défini sur zéro. Par conséquent, le serveur sera expert pour les partitions.

4. Rafraîchissez le serveur LDAP.

   Le serveur LDAP met en cache les limites des zones experte et non experte à chaque rafraîchissement de sa configuration. Si vous n'actualisez pas manuellement la configuration du serveur, celui-ci le fait automatiquement en arrière-plan lors d'une tâche déclenchée à un intervalle de 30minutes.

   Plusieurs partitions peuvent être empilées en une chaîne de zones non expertes. Toutefois, les services LDAP pour eDirectory 8.8 nécessitent que toutes les partitions non expertes soient contiguës et présentes dans des répliques locales.

Spécification des données de référence

Quand le serveur LDAP détermine qu'une opération s'effectue dans une zone non experte, il recherche les informations qu'il peut utiliser pour retourner un renvoi au client. Ces informations de renvoi peuvent figurer aux emplacements suivants :

- sur n'importe quelle entrée de la zone non experte ou sur toutes ces entrées ;
- sur l'objet Serveur LDAP ou Groupe LDAP qui contient les données de configuration du serveur, sous forme de renvoi par défaut.

Les informations de renvoi présentes dans les entrées de la zone non experte constituent une référence supérieure immédiate. Ces informations de renvoi consistent en un attribut ref à valeurs multiples. (Pour consulter la description de cet attribut, consultez le site Web RFC 3296 (http://www.ietf.org/rfc/rfc3296.txt). Les informations de renvoi présentes dans le paramètre de configuration Renvoi par défaut constituent une référence supérieure et ne contiennent qu'une seule valeur. (Reportez-vous aux types de DSE immSupr et supr dans X.501.)

Les données de référence sont consignées sous la forme d'une URL LDAP, mais n'indiquent que l'hôte et (de façon facultative) le port des DSA faisant l'objet de la référence. L'exemple suivant illustre ces données de référence :

```
ldap://ldap.digital_airlines.com:389
```

Le serveur LDAP observe le DN de base de l'opération (ou s'il est introuvable, le DN correspondant). Si le DN de base contient des informations de référence, le serveur LDAP renvoie celles-ci sous la forme d'un renvoi.

Si aucune information de référence n'est trouvée, le serveur LDAP parcourt l'arborescence vers le haut à la recherche d'informations de référence. S'il n'en trouve aucune après avoir essayé toutes les entrées, le serveur LDAP renvoie la référence supérieure. (Cette référence figure dans le paramètre de renvoi par défaut de l'objet Groupe LDAP ou Serveur LDAP.)

Ajout d'une référence supérieure immédiate

Vous pouvez ajouter une classe d'objet auxiliaire appelée immeditateSuperiorReference (référence supérieure immédiate) à une entrée de la zone non experte. Cette classe auxiliaire ajoute un attribut ref indiqué avec une ou plusieurs URL LDAP. Chaque URL indique le nom d'hôte et (éventuellement) le port d'un DSA.

Ajout d'une référence supérieure

À l'origine, l'objet Groupe LDAP comportait un attribut ldapReferral. Cet attribut contenait une référence par défaut qui était utilisée pour diverses situations de reprise après erreur lors du retour de renvois à d'autres serveurs eDirectory d'une arborescence eDirectory. Dans les services LDAP pour eDirectory 8.8, cet attribut est utilisé pour contenir un seul renvoi par défaut vers un DSA supérieur au sein d'une arborescence fédérée.

Par ailleurs, l'attribut ldapReferral a été ajouté à l'objet Serveur LDAP. Si l'attribut ldapReferral contient une valeur de l'objet Serveur LDAP, ce paramètre remplace la valeur contenue dans le même attribut de l'objet Groupe LDAP. Ce comportement vous permet de configurer tous les serveurs LDAP d'un groupe pour qu'ils aient un renvoi donné par défaut, en ne laissant qu'un ou deux serveurs remplacer cette valeur par un autre renvoi par défaut.

La valeur de l'attribut ldapReferral est une URL LDAP. Cette URL contient l'hôte et le port facultatif du DSA auquel le renvoi fait référence.

Mise à jour des informations de références par l'intermédiaire de LDAP

Si vous avez suivi les procédures ci-dessus dans l'ordre et utilisé LDAP pour exécuter les tâches, vous n'avez probablement pas pu ajouter une référence supérieure immédiate. En effet, comme la partition racine a déjà été marquée comme non experte, LDAP émet des renvois pour toute opération agissant sur les données de cette partition.

Pour permettre la mise à jour ou l'interrogation des informations d'une zone non experte, la commande Gérer DSA IT doit accompagner la requête LDAP. Pour plus d'informations sur ce contrôle, consultez le site Web RFC 3296 (http://www.ietf.org/rfc/rfc3296.txt). Ce contrôle pousse effectivement le serveur LDAP à considérer l'ensemble de la zone non experte comme si elle l'était.

REMARQUE : la fonction de référence supérieure est seulement accessible via LDAP. Les autres protocoles (par exemple, NDAP) ne sont pas influencés par la présence de l'attribut expert. Par conséquent, rien ne vient entraver le fonctionnement de ConsoleOne ou de Novell iManager lors de l'interrogation ou de la mise à jour de données dans la zone non experte.

Opérations affectées

Les zones non expertes et les renvois supérieurs agissent sur les opérations LDAP suivantes :

- Rechercher et comparer
- Modifier et ajouter

  Les valeurs des attributs de syntaxe du DN ne sont pas vérifiées. Par conséquent, un attribut membre du groupe peut contenir des DN qui pointent vers des entrées d'une zone non experte.
- Supprimer
- Renommer (moddn)
- Déplacer (moddn)

  Si le DN parent se situe dans une zone non experte, une erreur affectsMultipleDSAs doit être renvoyée.
- Opérations étendues

Prise en charge des références supérieures

Seuls les services LDAP pour eDirectory 8.7 et versions ultérieures prennent en charge les renvois supérieurs. Pour savoir si un serveur eDirectory prend en charge cette fonctionnalité, consultez l'attribut supportedFeatures sur le DSE racine. Si l'attribut supportedFeatures liste l'OID 2.16.840.1.113719.1.27.99.1, ces fonctions sont disponibles. Les autres modifications de l'objet DSE racine liées à l'identification de la prise en charge sont notamment les suivantes :

- namingContexts

  Cet attribut ne liste que les racines de la partition figurant sur le DSA local sur lequel le serveur a autorité. Aucune racine de partition non experte n'est listée.
- altServer

  Cet attribut ne liste pas les autres serveurs eDirectory qui partagent seulement des partitions non expertes avec le serveur local.
- superiorReference

  Cet attribut annonce le renvoi supérieur pour le DSA. Cette valeur est administrée par la mise à jour de l'attribut ldapReferral sur l'objet Serveur LDAP ou Groupe LDAP.

Recherche persistante : configuration en fonction des événements eDirectory

Novell eDirectory dispose d'un service d'événements permettant de signaler aux applications les événements importants qui se produisent au sein de l'annuaire. Certains d'entre eux sont des événements généraux qui peuvent relever de n'importe quel service d'annuaire. D'autres événements sont spécifiques à eDirectory et à ses fonctions spéciales.

Les événements eDirectory sont exposés aux applications par l'intermédiaire de deux extensions distinctes du protocole LDAP:

- Mise en oeuvre du contrôle de la recherche persistante

  La fonction Recherche persistante de Novell eDirectory est une opération de recherche qui se poursuit après le renvoi initial de l'ensemble des entrées correspondantes. La recherche persistante est une extension de l'opération de recherche LDAP v3 qui permet de faire basculer la tâche de recherche de mises à jour dans un ensemble de résultats du client vers le serveur. Le contrôle Recherche persistante permet au client d'effectuer une recherche LDAP normale (en spécifiant le nom distinctif de base, l'étendue et le filtre de la recherche, etc.) et, au lieu que le serveur renvoie un message SearchResultDone à la fin de la recherche, l'opération maintient une connexion afin que le client reçoive chaque fois une mise à jour des entrées de l'ensemble de résultats lors de leur modification. Ainsi, le client peut gérer un cache des entrées qui l'intéressent ou déclencher une opération logique dès qu'une mise à jour se produit.

  Consultez le document « Persistent Search » (Recherche persistante) sur Internet (http://www.ietf.org/proceedings/01mar/I-D/ldapext-psearch-03.txt) pour obtenir une description plus détaillée de cette extension.

- Surveillance des événements (une fonction LDAP étendue propre à eDirectory)

Les applications qui utilisent les services d'événements eDirectory peuvent représenter une lourde charge de traitement pour l'annuaire. Divers paramètres d'administration permettent de déterminer la manière dont les services d'événements sont employés sur chaque serveur eDirectory. Ces paramètres sont stockés dans l'objet Serveur LDAP. Vous pouvez les définir à l'aide de ConsoleOne ou de Novell iManager.

Pour certaines applications qui emploient le service d'événements, il peut être nécessaire d'affecter des valeurs spécifiques à ces paramètres. La documentation de ces applications indique leurs besoins propres.

Pour plus d'informations, consultez le site Web Understanding and Using Persistent Search in Novell eDirectory (Présentation et utilisation de la recherche persistante dans Novell eDirectory) (http://developer.novell.com/research/appnotes/2003/february/04/a030204.htm).

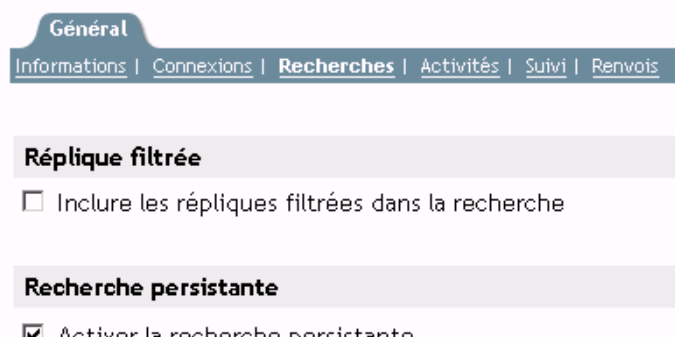
Gestion des recherches persistantes

Novell iManager vous permet d'afficher ou de modifier les recherches persistantes.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Administration de eDirectory > Modifier un objet.

3 Spécifiez le nom et le contexte de l'objet Serveur LDAP à modifier ou cliquez sur pour rechercher ou accéder à l'objet Serveur LDAP.

4 Cliquez sur OK, puis sur Recherches dans l'onglet Général.



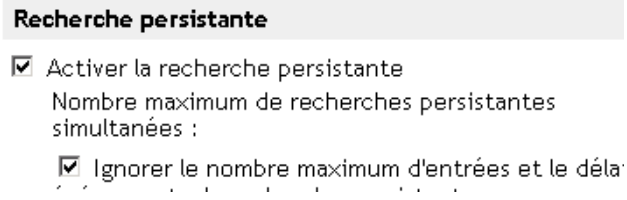
5 Activez les recherches persistantes.

Par défaut, la case Activer la recherche persistante est cochée. Pour désactiver et empêcher les recherches persistantes sur ce serveur, désélectionnez la case à cocher.

REMARQUE : si vous désactivez une opération de recherche persistante précédemment établie, il se peut que la recherche continue, même après la désactivation de l'option et le rafraîchissement du serveur.

6 Déterminez le nombre de recherches persistantes simultanées à effectuer sur le serveur concerné.

Entrez une valeur dans le champ Nombre maximum de recherches persistantes simultanées. La valeur zéro autorise un nombre illimité de recherches persistantes simultanées.



7 Déterminez si vous souhaitez ignorer les limites de taille et de temps.

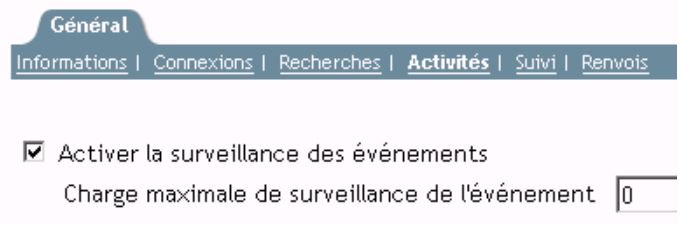
Pour déterminer si les limites de taille et de temps doivent être ignorées après l'envoi de l'ensemble initial de résultats de recherche par la recherche persistante, cochez la case Ignorer le nombre maximum d'entrées et le délai de réponse lors de la surveillance des événements de recherche persistants.

Si vous ne sélectionnez pas cette option, la totalité de l'opération de recherche persistante est soumise aux restrictions de recherche. Si l'une des limites est atteinte, la recherche échoue et le message d'erreur correspondant s'affiche.

8 Cliquez sur Appliquer, puis sur OK.

Contrôle de l'emploi de l'opération étendue de surveillance des événements

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches .
2. Cliquez sur LDAP > Présentation LDAP.
3. Cliquez sur Afficher les serveurs LDAP, puis cliquez sur le nom d'un serveur LDAP.
4. Cliquez sur Événements.



5. Déterminez si les applications client peuvent surveiller les événements de ce serveur LDAP.

   Pour leur permettre de surveiller les événements de ce serveur LDAP, cochez la case Activer la surveillance des événements.

   Pour désactiver la surveillance des événements, désélectionnez cette case.

6. Déterminez la charge maximale que les applications de surveillance des événements peuvent placer sur le serveur.

   Entrez une valeur dans le champ Charge maximale de surveillance de l'événement.

   Le traitement de données et l'envoi de notifications d'événements à des applications de surveillance impliquent une importante charge de traitement pour le serveur LDAP. Pour chaque événement, la charge précise du serveur dépend de la fréquence à laquelle survient l'événement surveillé, des données associées à ce dernier et du nombre d'applications client qui le surveillent.

   La charge maximale de surveillance des événements est une valeur relative indiquant la proportion de charge que l'extension de surveillance des événements est autorisée à placer sur le serveur. La valeur zéro indique qu'aucune limite n'a été définie. Pour déterminer la valeur appropriée de cet attribut, faites des essais.

7. Cliquez sur Appliquer, puis sur OK.

Obtention d'informations sur le serveur LDAP

Pour obtenir des informations sur un serveur LDAP, vous devez utiliser une recherche LDAP ou ICE. Les utilitaires correspondants ont besoin d'informations de rootDSE (Directory Service Agent, entrée spécifique).

RootDSE est un pseudo-objet d'une arborescence Annuaire. Il s'agit d'une entrée sans nom à la racine de l'arborescence. RootDSE contient des informations relatives au serveur auquel vous êtes connecté. À titre d'exemple, rootDSE sait où se trouvent les extensions et le schéma, et vérifie la prise en charge de ce dernier.

rootDSE n'étant pas une entrée nommée de l'arborescence, un serveur LDAP ne le retourne pas au client dans le cadre d'une opération de recherche normale.

Le tableau ci-dessous liste les informations provenant de rootDSE.

Informations et description	Exemple
Emplacement du schéma: subschemaSubentry vous indique l'emplacement du schéma de l'arborescence ou du serveur LDAP. Pour eDirectory, cn=schema constitue la base de la recherche.	subschemaSubentry: cn=schema
Extensions prises en charge: les extensions permettent de gérer le serveur (par exemple, de créer ou de fusionner les contextes, d'ajouter ou de supprimer de nouvelles répliques, de rafraîchir le serveur LDAP, de modifier la réplique maîtresse en réplique de type Lecture/écriture ou Lecture seule) et les identités. Les extensions sont au format ASN.1OID. Pour consulter les noms des extensions, reportez-vous au site Web LDAP Extensions (Extensions LDAP) (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html).	supportedExtension: 2.16.840.1.113719.1.27.100.12 supportedExtension: 2.16.840.1.113719.1.27.100.7 supportedExtension: 2.16.840.1.113719.1.27.100.8
Nom du fournisseur du serveur LDAP.	vendorName: Novell, Inc.
Version d'annuaire prise en charge par le serveur LDAP.	vendorVersion: eDirectory v8.7.0 (10410.29)
Version de eDirectory en cours d'exécution.	vendorVersion: eDirectory v8.7.0 (10410.29)
Nom du serveur d'annuaire et nom de l'arborescence Annuaire.	dsaName: cn=WestWindNDS,o=westwind directoryTreeName: t=WESTWINDTREE
Mécanismes SASL pris en charge.	supported SASLMechanisms: EXTERNAL supported SASLMechanisms: DIGEST-MD5 supported SASLMechanisms: NMAS LOGIN
Versions du serveur LDAP prises en charge.	supportedLDAPVersion: 2 supportedLDAPVersion: 3
Statistiques du serveur: RootDSE fournit une quantité de statistiques sur le serveur LDAP (par exemple, le nombre de liaisons d'authentification renforcée).	errors: 0 securityErrors: 0 chainings: 3 referralsReturned: 6 extendedOps: 0 abandonOps: 0 wholeSubtreeSearchOps: 1

Les informations fournies par rootDSE sont utiles aux développeurs d'application.

Scénario : développement d'une application – Henri écrit une application qui crée une nouvelle réplique. Il lit rootDSE et trouve supportedExtension: 2.16.840.1.113719.1.27.100.7 dans la liste. Il sait que le serveur prend en charge l'appel de création d'une réplique.

De plus, Novell iManager vérifie quelles fonctionnalités sont disponibles dans rootDSE et tient compte de ces informations.

Pour rechercher rootDSE, entrez les données suivantes sur un poste de travail :

ldapsearch -h *nom_hôte* -p 389 -b "" -s base "objectclass=*"

Cette recherche peut être effectuée par n'importe quelle application utilisant les API ldap_search.

Pour pouvoir effectuer votre recherche, la base doit être nulle et le filtre doit être défini sur objectclass=*. (dans le cas de ce client, la base correspond à -b).

Pour plus d'informations sur la lecture de rootDSE, reportez-vous à l'une des références suivantes :

- LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html)
- LDAP Classes for Java (http://developer.novell.com/ndk/doc/jldap/jldapenu/data/hevgtl7k.html)

Pour plus d'informations sur les filtres de recherche LDAP, consultez le site LDAP Search Filters (Filtres de recherche LDAP) (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a3saoeg.html). Cette section figure dans la section relative à l'intégration LDAP et NDS de la documentation NDK.

14 Sauvegarde et restauration de Novell eDirectory

Novell® eDirectory™ est conçu pour assurer la tolérance aux pannes au moyen dun système de réplication. Ainsi, si un serveur n'est pas disponible, d'autres serveurs peuvent fournir les accès requis. La réplication est la principale méthode de protection de eDirectory.

Elle ne peut toutefois pas être mise en oeuvre dans un environnement qui comprend un seul serveur. De plus, la réplication ne garantit pas la restauration complète de serveurs individuels en cas de défaillance matérielle ou autre d'un serveur ou encore de sinistre tel qu'un incendie ou une inondation entraînant la perte de plusieurs machines. La sauvegarde de eDirectory sur chaque serveur augmente la tolérance aux pannes de votre réseau.

eDirectory 8.7 a introduit un nouvel utilitaire de sauvegarde et de restauration, eDirectory Backup eMTool, destiné à sauvegarder la base de données eDirectory sur des serveurs individuels. Ses avantages sont les suivants :

- **Même outil pour toutes les plates-formes.**
- **Sauvegarde continue à chaud.** Vous pouvez sauvegarder votre serveur sans fermer la base de données eDirectory, tout en disposant d'une sauvegarde complète.
- **Possibilité de restauration rapide d'un serveur individuel.** Ceci s'avère particulièrement utile en cas de défaillance matérielle.
- **Évolutivité.** Vous pouvez sauvegarder un serveur dont la base de données eDirectory contient des dizaines voire des centaines de millions d'objets. La vitesse du processus de sauvegarde est principalement limitée par la bande passante du canal d'E/S.
- **Capacité de restauration rapide de l'arborescence, en association avec la planification de répliques et les serveurs DSMASTER.** Même si vous n'utilisez pas de serveurs DSMASTER, vous devez être en mesure de restaurer une partie de l'arborescence. Pour plus de détails, reportez-vous à la section « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre », page 397.
- **Possibilité d'exécution à distance des tâches.** Vous pouvez effectuer la plupart des tâches de sauvegarde et de restauration dans un navigateur, à l'aide de iManager, à l'intérieur ou à l'extérieur du pare-feu. Il est également possible d'exécuter des tâches avancées à distance, à l'aide du client eMBox, client Java à ligne de commande qui permet un accès derrière le pare-feu ou via un réseau privé virtuel (VPN).
- **Possibilité de sauvegarder des fichiers connexes.** Vous pouvez sauvegarder des fichiers du serveur liés à la base de données, tels que les fichiers de sécurité NICI, les fichiers de flux, ainsi que tous ceux (tels que autoexec.ncf) listés dans un fichier d'inclusion.
- **Possibilité de restaurer eDirectory dans létat où il se trouvait avant son arrêt,** en utilisant la fonction de consignation continue de transactions individuelles par fichier. Pour plus de détails, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

- **Simplification de la mise à niveau du matériel.** En effectuant une sauvegarde à froid, puis en restaurant la base de données eDirectory, vous pouvez transférer facilement l'identité du serveur sur une nouvelle machine, ou la protéger pendant que vous effectuez des modifications telles qu'un ajout de mémoire vive. Pour plus de détails, reportez-vous à la section « Mise à niveau du matériel ou remplacement d'un serveur », page 534.
- **Fonctionnement adapté à l'environnement distribué de eDirectory.** Vous pouvez vous assurer qu'un serveur restauré possède l'état de synchronisation qu'attendent les autres serveurs de l'arborescence en activant la consignation continue de transactions individuelles par fichier.
- **Possibilité de sauvegardes sans surveillance.** Vous pouvez créer des fichiers de traitement par lots pour exécuter des sauvegardes sans surveillance au moyen du client eMBox.

Le nouveau programme eDirectory Backup eMTool est conçu pour effectuer la sauvegarde et la restauration complètes de la base de données et des fichiers associés présents sur un serveur. Il ne prend pas en charge la sauvegarde ni la restauration de sections ou d'objets individuels de l'arborescence.

De plus, il doit être utilisé en association avec les sauvegardes du système de fichiers, afin d'enregistrer sur bande les fichiers de sauvegarde de eDirectory, par mesure de sécurité.

Ce chapitre comprend les rubriques suivantes :

Liste de contrôle pour la sauvegarde de eDirectory

Pour vous assurer de l'accessibilité des objets d'une arborescence multiserveur, même lorsqu'un serveur est arrêté :

- ❑ Pour les arborescences multiserveurs, vérifiez que toutes les partitions eDirectory sont répliquées sur plusieurs serveurs, afin d'assurer la tolérance aux pannes.

  Pour plus d'informations sur la création de répliques, reportez-vous à la section « Ajout d'une réplique », page 137.

Pour permettre une restauration rapide et complète de serveurs individuels (après une défaillance matérielle, par exemple) :

- ❑ Effectuez régulièrement une sauvegarde complète de la base de données eDirectory (une fois par semaine, par exemple).
- ❑ Effectuez régulièrement une sauvegarde incrémentielle (toutes les nuits, par exemple).
- ❑ Effectuez des sauvegardes sur bande complètes et incrémentielles du système de fichiers peu après les sauvegardes complètes ou incrémentielles de la base de données eDirectory.

  L'outil Backup eMTool enregistre les fichiers de sauvegarde dans le répertoire du serveur que vous indiquez, mais ne peut pas les enregistrer directement sur bande. C'est pourquoi la sauvegarde du système de fichiers doit être configurée pour s'exécuter après la sauvegarde de eDirectory, afin d'enregistrer les fichiers de sauvegarde de la base de données sur bande pour en assurer le stockage sécurisé.
- ❑ Activez et configurez la consignation de transactions individuelles par fichier, si elle est nécessaire dans votre environnement.

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Si vous ne le faites pas, des erreurs se produisent lors de la restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvre pas. Avec la restauration par défaut, une base de données qui partage des répliques avec d'autres serveurs n'est pas ouverte tant qu'elle n'a pas été restaurée dans l'état où elle se trouvait au moment de l'arrêt du système.

  Dans un environnement monoserveur, la consignation de transactions individuelles par fichier n'est pas nécessaire au processus de vérification de la restauration, mais vous pouvez l'utiliser si vous souhaitez pouvoir restaurer eDirectory dans l'état où il se trouvait avant son arrêt, au lieu de bénéficier simplement de l'état enregistré dans la dernière sauvegarde.

  Lorsque vous activez la fonction de consignation de transactions individuelles par fichier, vous devez avant tout prendre les précautions suivantes. Pour plus d'informations, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

  - Spécifiez un nouvel emplacement pour les fichiers journaux de transactions individuelles (n'utilisez pas la valeur par défaut).

    Les fichiers journaux doivent se trouver dans un répertoire local du serveur. Pour des raisons de tolérance aux pannes, ils ne doivent pas être stockés sur le même volume/partition de disque ou périphérique de stockage que eDirectory. Vous pouvez éventuellement réserver une partition/un volume aux fichiers journaux de transactions individuelles.
  - Prenez note de l'endroit où se trouvent les fichiers journaux de transactions individuelles, afin de pouvoir les retrouver en cas de défaillance.

    Pour localiser cet emplacement lorsque le serveur est sain, vous pouvez utiliser l'option Configuration de la sauvegarde dans iManager ou getconfig dans le client eMBox. Toutefois, si le serveur connaît une défaillance affectant eDirectory (une panne matérielle, par exemple), vous ne pouvez pas rechercher l'emplacement des fichiers journaux de transactions individuelles.
  - Surveillez l'espace disque sur la partition ou le volume qui reçoit les fichiers journaux de transactions individuelles afin d'éviter une saturation.

    Si les fichiers journaux de transactions individuelles ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné.

- Limitez l'accès à l'emplacement où les fichiers journaux de transactions individuelles sont conservés, afin que les utilisateurs non autorisés ne puissent pas les visualiser.
- Si une restauration est nécessaire, veillez à reconfigurer les fichiers journaux de transactions individuelles sur le serveur une fois la restauration terminée. En effet, les paramètres reprennent leur valeur par défaut durant une restauration. Après avoir activé les fichiers journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

- ❑ Si vous utilisez l'infrastructure NICI, assurez-vous que les sauvegardes de eDirectory incluent les fichiers de sécurité NICI.

  En l'absence de ces fichiers, vous ne pouvez pas restaurer les clés de codage ni lire les données codées. Pour plus d'informations sur la sécurité NICI, consultez le manuel *NICI Administration Guide (Guide d'administration de NICI)* (http://www.novell.com/documentation/beta/nici27x/index.html) et le document TID sur la sauvegarde des fichiers NICI (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098087.htm).

- ❑ Pour les arborescences multiserveurs, si vous utilisez Backup eMTool pour sauvegarder un serveur, vous devez mettre à niveau tous les serveurs qui partagent des répliques avec ce dernier en installant eDirectory 8.5 ou une version ultérieure.

  Le processus de vérification de la restauration est rétrocompatible avec eDirectory 8.5 et versions ultérieures uniquement. Pour plus d'informations sur la vérification de la restauration, reportez-vous aux sections « Présentation du processus de restauration avec Backup eMTool », page 391 et « Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement », page 399.

- ❑ (NetWare® uniquement) Prenez connaissance des problèmes liés aux droits du système de fichiers à la section « Préservation des droits lors de la restauration des données du système de fichiers sous NetWare », page 400. Recherchez les problèmes éventuels et prenez des mesures préventives au besoin.

- ❑ Vérifiez périodiquement le fichier journal des sauvegardes pour vous assurer de la réussite des sauvegardes sans surveillance.

- ❑ Effectuez une sauvegarde à froid avant de mettre à niveau un serveur, comme expliqué dans la section « Mise à niveau du matériel ou remplacement d'un serveur », page 534.

- ❑ Pour les arborescences multiserveurs, vérifiez que toutes les partitions eDirectory sont répliquées sur plusieurs serveurs, afin d'assurer la tolérance aux pannes.

  La réplication de vos partitions permet non seulement de rendre les objets disponibles lorsqu'un serveur est arrêté, à des fins de maintenance par exemple, mais aussi d'assurer une tolérance aux pannes pour protéger vos informations en cas de perte d'un serveur, à la suite d'une défaillance matérielle. Si un serveur d'une arborescence multiserveur contenant une partition non répliquée connaît une défaillance, vous risquez de ne pas pouvoir récupérer la partition en question. Il est préférable de s'assurer que toutes les partitions sont répliquées. Pour plus d'informations sur les raisons pour lesquelles vous risquez de ne pas pouvoir récupérer une partition non répliquée dans une arborescence multiserveur, reportez-vous aux sections « Présentation du processus de restauration avec Backup eMTool », page 391, « Utilisation des fichiers journaux de transactions individuelles », page 401 et « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442.

  Pour plus d'informations sur la réplication, reportez-vous à la section « Répliques », page 52 et au Chapitre 5, “Gestion des partitions et des répliques”, page 133.

- ❑ Veillez à stocker en lieu sûr les bandes qui contiennent les sauvegardes de eDirectory et du système de fichiers.

- ❑ Testez régulièrement votre stratégie de sauvegarde pour vous assurer qu'elle répond à vos objectifs.
- ❑ (Facultatif) Si vous envisagez d'accéder à distance aux serveurs pour effectuer des sauvegardes à froid (une sauvegarde complète avec la base de données fermée) ou des tâches avancées de sauvegarde et de restauration, installez le client eMBox sur la machine que vous prévoyez d'utiliser. Pensez également aux accès (accès par un réseau privé virtuel, par exemple) derrière le pare-feu.

  iManager vous permet d'effectuer des sauvegardes et des restaurations à distance, à l'extérieur du pare-feu, mais il ne prend en charge ni la sauvegarde à froid ni les tâches avancées.

  Le client eMBox est installé avec eDirectory sur le serveur. Vous pouvez aussi l'utiliser sur des postes de travail avec Sun JVM1.3.1. Pour plus dinformations sur l'installation et la configuration du client eMBox, reportez-vous à la section.

Pour vous préparer à un sinistre dans lequel vous perdez plusieurs serveurs :

- ❑ Tenez compte des considérations ci-dessus.
- ❑ Pour les arborescences multiserveurs, prévoyez de créer des serveurs DSMASTER afin d'être prêt en cas de sinistre.

  Pour plus de détails, reportez-vous à la section « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre », page 397.
- ❑ Testez régulièrement votre stratégie de reprise après sinistre afin de vous assurer qu'elle répond à vos objectifs.

Présentation des services de sauvegarde et de restauration

À propos de l'outil eDirectory Backup eMTool

Backup eMTool permet d'effectuer une sauvegarde continue à chaud de la base de données eDirectory sur un serveur individuel. Si vous sauvegardez eDirectory sur votre serveur sans fermer la base de données, vous obtenez néanmoins d'une sauvegarde complète, image fidèle de l'état de la base au début de la sauvegarde. Grâce à cette fonction, vous pouvez lancer une sauvegarde à tout moment, eDirectory restant accessible tout au long du processus. (La sauvegarde continue à chaud

est adoptée par défaut. Vous pouvez, si nécessaire, demander une sauvegarde «à froid» lorsque la base de données est fermée.)

La nouvelle fonction de sauvegarde permet également d'activer la consignation de transactions individuelles par fichier, pour conserver un enregistrement des transactions dans la base de données depuis la dernière sauvegarde. Vous pouvez ainsi restaurer un serveur dans l'état où il se trouvait avant son arrêt. Vous devez activer cette consignation pour les serveurs qui font partie d'un anneau de répliques, afin de rendre à un serveur l'état de synchronisation attendu par les autres serveurs. Si vous ne le faites pas, des erreurs se produisent lors de la restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvre pas. Par défaut, la consignation de transactions individuelles par fichier est désactivée. Pour plus d'informations, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

Backup eMTool ne sauvegarde pas tous les objets de eDirectory à la fois, mais seulement les partitions d'un serveur individuel. Cela permet une meilleure restauration du serveur et des sauvegardes plus rapides qu'avec l'utilitaire de sauvegarde classique TSA pour NDS®. (Celui-ci continue de fonctionner comme expliqué dans eDirectory 8.6 ; vous pouvez l'employer avec la nouvelle fonction de sauvegarde, si nécessaire.) Pour une comparaison, reportez-vous à la section « Quelles sont les différences des fonctions de sauvegarde et de restauration de eDirectory 8.7.3 ? », page 389.

Le nouvel outil de sauvegarde de eDirectory doit être utilisé en association avec les sauvegardes du système de fichiers, afin d'enregistrer sur bande les fichiers de sauvegarde de eDirectory, par mesure de sécurité. Novell a établi des partenariats avec plusieurs grands fournisseurs de solutions de sauvegarde. Vous trouverez une liste à la page NetWare Partner Products : Backup, Restore, & Recovery (http://www.novell.com/partnerguide/p100004.html) (Produits partenaires NetWare : sauvegarde, restauration et reprise après sinistre).

Sous NetWare, vous devrez peut-être également utiliser l'outil de sauvegarde eDirectory en association avec les sauvegardes des droits du système de fichiers. Pour plus d'informations, reportez-vous à la section « Préservation des droits lors de la restauration des données du système de fichiers sous NetWare », page 400.

Dans iManager, vous pouvez employer toutes les fonctions, exception faite de la sauvegarde à froid, des sauvegardes sans surveillance et des options de restauration avancées, comme expliqué dans la section « Utilisation de Novell iManager pour la sauvegarde et la restauration », page 410. Toutes les tâches de sauvegarde et de restauration, y compris les sauvegardes sans surveillance, peuvent être exécutées à partir du client Java à ligne de commande eMBox, comme expliqué dans la section « Utilisation du client eMBox pour la sauvegarde et la restauration », page 419.

Pour obtenir une description des options de sauvegarde et de restauration dans iManager, consultez l'aide en ligne. Pour une description des options du client eMBox, reportez-vous à la section « Options de ligne de commande pour la sauvegarde et la restauration », page 431.

Pour obtenir une description du processus de restauration, reportez-vous à la section « Présentation du processus de restauration avec Backup eMTool », page 391.

eDirectory Backup eMTool fait partie du jeu d'outils eMBox. Installé sur le serveur, eMBox est un service qui fait partie de eDirectory.

Backup eMTool comprend les fichiers suivants :

Nom de fichier	Description
backupcr	Bibliothèque principale contenant toutes les fonctionnalités de sauvegarde et de restauration. Cette bibliothèque ne possède pas d'interface utilisateur ; elle est chargée et liée dynamiquement par le programme backuptl.
backuptl	Interface eMTool avec la bibliothèque backupcr. Offre des fonctionnalités de sauvegarde et de restauration qui mettent en oeuvre l'architecture eMBox. backuptl est accessible par l'intermédiaire du plug-in iManager ou du client Java à ligne de commande eMBox.
dsbackup_en.xlf	Fichier de langue contenant les messages renvoyés par Backup eMTool.

Pour obtenir une description du format des fichiers de sauvegarde et des fichiers journaux créés par Backup eMTool, reportez-vous aux sections « Format du fichier journal de sauvegarde », page 396 et « Format de l'en-tête des fichiers de sauvegarde », page 392.

IMPORTANT : Le processus de vérification de la restauration est rétrocompatible avec eDirectory 8.5 et versions ultérieures uniquement. Si vous souhaitez utiliser le nouvel outil de sauvegarde et de restauration sur des serveurs qui font partie d'un anneau de répliques, veillez à les mettre à niveau vers eDirectory 8.5 ou une version ultérieure. (Reportez-vous également à la section « Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement », page 399.)

Quelles sont les différences des fonctions de sauvegarde et de restauration de eDirectory 8.7.3 ?

Dans les versions précédentes de eDirectory, les fonctions de sauvegarde et de restauration étaient axées sur la sauvegarde de l'arborescence, objet par objet.

Le nouvel outil Backup eMTool de eDirectory 8.7 a introduit une méthode totalement différente, ainsi qu'une nouvelle architecture. En effet, il est axé sur le serveur, et non sur l'arborescence. Vous sauvegardez la base de données eDirectory individuellement sur chaque serveur. De plus, il est beaucoup plus rapide que l'utilitaire de sauvegarde classique TSA pour NDS.

Vous pouvez continuer d'utiliser celui-ci pour sauvegarder l'arborescence, mais nous vous conseillons d'employer le nouvel outil.

La sauvegarde des informations propres au serveur a été mise en oeuvre à l'aide de Backup eMTool. Pour plus de détails, reportez-vous à la section « Modifications apportées à la sauvegarde des informations propres au serveur (NetWare uniquement) », page 440.

Pour plus d'informations, consultez le tableau ci-dessous.

Critère	Utilitaire de sauvegarde classique TSA pour NDS	Outil Backup eMTool « Sauvegarde continue à chaud »
Objectif	Conçu pour sauvegarder l'arborescence, objet par objet. Pour plus d'informations sur les utilitaires de sauvegarde classiques (qui sont toujours pris en charge dans eDirectory 8.7 ; les deux types de sauvegarde peuvent au besoin être utilisés), reportez-vous à la section «Backing Up and Restoring Novell eDirectory (Sauvegarde et restauration de Novell eDirectory)» (http://www.novell.com/documentation/lg/ndsedir86/taoenu/data/a2n4mb6.html) dans le manuel *Novell eDirectory 8.6 Administration Guide (Guide d'administration de Novell eDirectory 8.6)*.	Conçu pour sauvegarder la base de données eDirectory sur chaque serveur pris individuellement. La tolérance aux pannes de l'arborescence complète doit être en premier lieu assurée par la réplication, mais le fait de sauvegarder chaque serveur permet de la renforcer. Lorsque vous devez prévoir une stratégie de restauration de l'arborescence à la suite d'un sinistre ayant entraîné la perte de nombreux serveurs, pensez à employer des serveurs DSMASTER avec la fonction de planification de répliques, comme expliqué dans la section « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre », page 397.
Vitesse	Non applicable	Considérablement accrue. La vitesse est l'une des caractéristiques les plus importantes du nouvel outil de sauvegarde.
Emplacement de la sauvegarde	Permet de placer la sauvegarde directement sur une bande magnétique.	Les fichiers de sauvegarde sont placés dans le système de fichiers. Vous devez sauvegarder ce dernier pour les enregistrer sur bande, afin de les stocker en lieu sûr.
Multiplate-forme	Fonctionne différemment sur chaque plate-forme.	Fonctionne de manière identique sur toutes les plates-formes.
Possibilité de restaurer des serveurs individuels	Non conçu pour cela.	Offre la possibilité de restaurer un serveur individuel après une défaillance de disque dur, ou d'utiliser la sauvegarde pour transférer un serveur d'une machine vers une autre. Il est également possible de mettre en oeuvre la consignation de transactions individuelles par fichier afin de rendre à un serveur l'état qu'il avait avant son arrêt, de sorte qu'il retrouve l'état de synchronisation attendu par les autres serveurs dans un anneau de répliques. Permet de sauvegarder des fichiers liés à eDirectory sur un serveur individuel. Vous pouvez, par exemple, sauvegarder et restaurer des fichiers NICI. Vous pouvez aussi créer votre propre liste de fichiers à inclure dans la sauvegarde.

Critère	Utilitaire de sauvegarde classique TSA pour NDS	Outil Backup eMTool « Sauvegarde continue à chaud »
Possibilité de restaurer des fichiers NICI pour un serveur	Non conçu pour cela.	Permet de sauvegarder et de restaurer les fichiers NICI, afin de pouvoir accéder aux données codées après une restauration. Vous pouvez ainsi gagner beaucoup de temps lors de la restauration.
Consignation de transactions individuelles par fichier pour un serveur individuel	Non conçu pour cela.	Permet de conserver un enregistrement des transactions dans la base de données depuis la dernière sauvegarde, afin de restaurer un serveur dans l'état où il se trouvait avant son arrêt. Dans un environnement multiserveur, cela vous permet de rendre à un serveur l'état de synchronisation attendu par les autres serveurs. Par défaut, la consignation de transactions individuelles par fichier est désactivée. Pour plus d'informations, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

Présentation du processus de restauration avec Backup eMTool

Avant d'effectuer la restauration, vous devez collecter tous les fichiers de sauvegarde en suivant les instructions contenues dans la section « Préparation d'une restauration », page 406. Lorsque vous demandez à l'outil Backup eMTool de commencer la restauration, à laide de iManager ou du client eMBox, celui-ci exécute la procédure suivante :

1. Il ferme l'agent DS.
2. Il transforme l'ensemble DIB (Data Information Base) actif nommé NDS en un nouvel ensemble DIB nommé RST.

   (La base de données NDS existante est conservée sur le serveur ; si la vérification de la restauration échoue, elle redevient l'ensemble DIB actif.)
3. Il effectue la restauration dans l'ensemble DIB nommé RST.
4. Il désactive l'ensemble DIB.

   Il applique l'attribut de login désactivé sur le pseudo-serveur, ce qui empêche l'agent DS de s'ouvrir avec cet ensemble DIB.
5. Il rétablit les paramètres par défaut des fichiers journaux de transactions individuelles.

   Ainsi, après une restauration, la consignation de transactions individuelles par fichier est toujours désactivée. De plus, l'emplacement par défaut des fichiers journaux de transactions individuelles est rétabli.

   (Si vous souhaitez activer la consignation de transactions individuelles par fichier sur le serveur, vous devez prévoir de recréer la configuration appropriée après une restauration afin de vous assurer que cette fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les fichiers journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.)
6. Il vérifie la base de données RST restaurée.

Le serveur tente de vérifier la cohérence des données restaurées. Pour ce faire, il contacte chaque serveur avec lequel il partage une réplique et compare les vecteurs de transition.

Le résultat de ce processus de vérification est enregistré dans le fichier journal.

Si le vecteur de transition du serveur distant est en avance par rapport au vecteur local, il manque alors des données dans la restauration et la vérification échoue.

Voici un exemple des informations enregistrées dans le fichier journal en cas d'échec de la vérification pour l'une des répliques. Il montre les vecteurs de transition qui ont été comparés :

```
Server: \T=LONE_RANGER\O=novell\CN=CHIP
   Replica: \T=LONE_RANGER\O=novell
      Status: ERROR = -6034
         Local TV              Remote TV
         s3D35F377 r02 e002    s3D35F3C4 r02 e002
         s3D35F370 r01 e001    s3D35F370 r01 e001
         s3D35F363 r03 e001    s3D35F363 r03 e001
         s3D35F31E r04 e004    s3D35F372 r04 e002
         s3D35F2EE r05 e001    s3D35F2EE r05 e001
         s3D35F365 r06 e003    s3D35F365 r06 e003
```

Pour plus d'informations, reportez-vous à la section « Vecteurs de transition et processus de vérification de la restauration », page 399.

7. Si la vérification réussit, l'ensemble DIB RST est renommé NDS et l'attribut de login désactivé est effacé, de sorte que la base de données eDirectory concernée devient la base de données active sur le serveur. Si la vérification échoue, l'ensemble DIB RST n'est pas renommé, et NDS redevient l'ensemble DIB actif.

   En cas d'échec de la vérification, reportez-vous à la section « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442 pour savoir comment récupérer le serveur. (Il est possible de forcer l'activation et le déverrouillage de la base de données RST à l'aide des options de restauration avancées, mais cela n'est pas conseillé, sauf si Novell vous le propose.)

Format de l'en-tête des fichiers de sauvegarde

Les fichiers de sauvegarde comportent un en-tête que vous pouvez lire pour accéder à des informations importantes, notamment:

- Le nom assigné au fichier de sauvegarde lors de sa création.

  Cela est utile si le fichier a été renommé depuis la création de la sauvegarde.

- Le nom du fichier journal de transaction individuelle utilisé au moment de la sauvegarde.

  S'il s'agit de la dernière sauvegarde du jeu à partir duquel vous effectuez la restauration (par exemple la dernière sauvegarde incrémentielle d'un ensemble constitué d'une sauvegarde complète et de trois sauvegardes incrémentielles), cette information vous est utile puisqu'elle indique le premier fichier journal de transaction individuelle dont vous avez besoin pour effectuer une restauration complète.

- Les répliques que contenait le serveur.

  Cette information est utile si vous n'avez pas noté l'emplacement de vos répliques. Si vous êtes confronté à un sinistre impliquant la perte de nombreux serveurs, la liste des répliques figurant dans l'en-tête du fichier de sauvegarde peut vous aider à choisir les serveurs à restaurer en premier.

- Les noms des fichiers inclus dans la sauvegarde, listés dans un fichier d'inclusion utilisateur.
- Le nombre de fichiers figurant dans le jeu de sauvegarde.

Pour chaque sauvegarde individuelle, l'en-tête du fichier est au format XML. Immédiatement après l'en-tête viennent les données de sauvegarde de la base de données exprimées en code binaire. (Étant donné que des données binaires sont incluses à la fin du fichier, l'analyse de ce dernier produirait des erreurs. Toutefois, l'en-tête est conforme au standard XML.) Si la sauvegarde s'étend sur plusieurs fichiers, les informations d'en-tête sont incluses dans chacun d'eux.

AVERTISSEMENT : lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car il pourrait alors devenir tronqué. La plupart des applications ne peuvent pas enregistrer correctement les données binaires.

Voici la partie DTD de l'en-tête XML. (Elle est incluse également dans l'en-tête du fichier de sauvegarde, pour référence).

```
<?xml version=”1.0” encoding=”UTF-8” standalone=”yes” ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
    backup_type (full|incremental) #REQUIRED
    idtag CDATA #REQUIRED
    time CDATA #REQUIRED
    srvname CDATA #REQUIRED
    dsversion CDATA #REQUIRED
    compression CDATA “none”
    os CDATA #REQUIRED
    current_log CDATA #REQUIRED
    number_of_files CDATA #IMPLIED
    backup_file CDATA #REQUIRED
    incremental_file_ID CDATA #IMPLIED
    next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
    name CDATA #REQUIRED
    encoding CDATA “base64”
    type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
    modification_time CDATA #REQUIRED
    replica_type (MASTER|SECONDARY|READONLY|SUBREF|
    SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
    replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED|
    CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA|
    BEGIN_ADD|MASTER_START|MASTER_DONE|
    FEDERATED|SS_0|SS_1|JS_0|JS_1|MS_0|MS_1|
    Unknown) #REQUIRED>
]>
```

Le tableau ci-dessous décrit les attributs que contient cette partie.

Attribut	Explication
backup version	Version de l'outil de sauvegarde.
backup backup_type	Type de sauvegarde exécuté (sauvegarde complète ou incrémentielle). (Une sauvegarde à froid est une sauvegarde complète.)

Attribut	Explication
backup idtag	Identificateur GUID attribué selon l'heure de la sauvegarde. Il permet d'identifier la sauvegarde, même si le fichier de sauvegarde est renommé.
backup time	Date et heure à laquelle la sauvegarde a débuté.
backup srvname	Nom distinctif du serveur sauvegardé.
backup dsversion	Version de eDirectory exécutée sur le serveur.
backup compression	Indique si Backup eMTool a comprimé les données de sauvegarde. La compression ne s'applique qu'aux données ; l'en-tête n'est jamais comprimé.
backup os	Système d'exploitation sur lequel la sauvegarde a été exécutée. Nous vous recommandons de ne restaurer que le même système d'exploitation.
backup current_log	Premier fichier journal de transaction individuelle nécessaire pour restaurer la sauvegarde. Cette information vous permet de collecter l'ensemble de fichiers approprié pour une restauration.
backup number_of_files	Nombre de fichiers faisant partie du jeu de sauvegarde. Cette valeur figure uniquement dans le premier fichier de sauvegarde.
backup backup_file	Nom de fichier de la sauvegarde actuelle. Si la sauvegarde s'étend sur plusieurs fichiers, l'en-tête de chaque fichier indique le nom du fichier ainsi que son numéro d'ordre dans le jeu de sauvegarde. Pour un exemple de noms de fichiers de sauvegarde, voir -s *f ile_size*.
backup incremental_file_ID	S'il s'agit d'une sauvegarde incrémentielle, cet attribut représente l'ID du fichier incrémentiel.
backup next_inc_file_ID	ID attribué au fichier de sauvegarde incrémentielle suivant lors de sa création. Cette information vous permet de collecter l'ensemble de fichiers approprié pour une restauration.
file size	Taille des données qui figurent entre les balises <file> du fichier.
file name	Nom et emplacement du fichier au moment de la sauvegarde.
file encoding	Algorithme de codage utilisé pour le fichier.
file type	Indique s'il s'agit d'un fichier NICI ou utilisateur.
replica partition_DN	Nom distinctif de la partition. Cette information est utile si vous n'avez pas noté l'emplacement de vos répliques. Si vous êtes confronté à un sinistre impliquant la perte de nombreux serveurs, la liste des répliques figurant dans l'en-tête du fichier de sauvegarde peut vous aider à choisir les serveurs à restaurer en premier.

Attribut	Explication
replica modification_time	Vecteur de transition de la réplique au moment de la sauvegarde.
replica replica_type	Type de réplique (maîtresse ou lecture seule, par exemple).
replica_state	État de la réplique au moment de la sauvegarde (active ou nouvelle réplique, par exemple).

Voici un exemple d'en-tête de fichier de sauvegarde d'un serveur Windows NT. Les fichiers de sécurité NICI sont inclus dans la sauvegarde.

```
<?xml version=”1.0” encoding=”UTF-8” standalone=”yes” ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
    backup_type (full|incremental) #REQUIRED
    idtag CDATA #REQUIRED
    time CDATA #REQUIRED
    srvname CDATA #REQUIRED
    dsversion CDATA #REQUIRED
    compression CDATA “none”
    os CDATA #REQUIRED
    current_log CDATA #REQUIRED
    number_of_files CDATA #IMPLIED
    backup_file CDATA #REQUIRED
    incremental_file_ID CDATA #IMPLIED
    next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
    name CDATA #REQUIRED
    encoding CDATA “base64”
    type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
    modification_time CDATA #REQUIRED
    replica_type (MASTER|SECONDARY|READONLY|SUBREF|
    SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
    replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED|
    CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA|
    BEGIN_ADD|MASTER_START|MASTER_DONE|
    FEDERATED|SS_0|SS_1|JS_0|JS_1|MS_0|MS_1|
    Unknown) #REQUIRED>
]>

<backup version=”2” backup_type=”full” idtag=”3D611DA2” time=”2002-8-
19'T10:32:35” srvname=”\T=MY_TREE\O=novell\CN=DSUTIL-DELL-NDS”
dsversion=”1041081” compression=”none” os=”windows”
current_log=”00000003.log” next_inc_file_ID=”2” number_of_files=”0000001”
backup_file=”c:\backup\header.bak”><replica partition_DN=”\T=MY_TREE”
modification_time=”s3D611D95_r1_e2” replica_type=”MASTER” replica_state=”ON”
/><replica partition_DN=”\T=MY_TREE\O=part1”
modification_time=”s3D611D95_r1_e2” replica_type=”MASTER” replica_state=”ON”
/><replica partition_DN=”\T=MY_TREE\O=part2”
modification_time=”s3D611D95_r1_e2” replica_type=”MASTER” replica_state=”ON”
/><replica partition_DN=”\T=MY_TREE\O=part3”
modification_time=”s3D611D96_r1_e2” replica_type=”MASTER” replica_state=”ON”
/><file size=”190”
```

```
name="C:\WINNT\system32\novell\nici\bhawkins\XARCHIVE.001"
encoding="base64" type="nici">the data is included here</file>

<file size="4228" name="C:\WINNT\system32\novell\nici\bhawkins\XMGRCFG.KS2"
encoding="base64" type="nici">the data is included here</file>

<file size="168" name="C:\WINNT\system32\novell\nici\bhawkins\XMGRCFG.KS3"
encoding="base64" type="nici">the data is included here</file>

<file size="aaac" name="C:\WINNT\system32\novell\nici\nicintacl.exe"
encoding="base64" type="nici">the data is included here</file>

<file size="150" name="C:\WINNT\system32\novell\nici\NICISDI.KEY"
encoding="base64" type="nici">the data is included here
</file>

<file size="4228" name="C:\WINNT\system32\novell\nici\system\Xmgrcfg.ks2"
encoding="base64" type="nici">the data is included here
</file>

<file size="168" name="C:\WINNT\system32\novell\nici\system\Xmgrcfg.ks3"
encoding="base64" type="nici">the data is included here
</file>

<file size="1414" name="C:\WINNT\system32\novell\nici\xmgrcfg.wks"
encoding="base64" type="nici">the data is included here
</file>

</backup>
```

Les données binaires de la sauvegarde de la base de données sont ajoutées dans le fichier de sauvegarde à la suite de len-tête.

Format du fichier journal de sauvegarde

eDirectory Backup eMTool tient à jour un journal qui présente une vue d'ensemble de son activité et comporte des informations sur les sauvegardes antérieures. Le fichier journal contient un historique de toutes les sauvegardes et consigne l'heure de début et de fin de chacune d'entre elles. Il fournit également des informations sur les erreurs survenues éventuellement pendant le processus de sauvegarde. Ce fichier est complété à chaque sauvegarde. Il est également enregistré à l'emplacement que vous désignez.

Le fichier journal permet de s'assurer de la réussite des sauvegardes sans surveillance. Le résultat (réussite ou échec) est indiqué sur la dernière ligne avec le code d'erreur éventuel.

Le fichier journal de Backup eMTool mentionne également l'ID des sauvegardes effectuées, ce qui facilite la collecte des fichiers de sauvegarde complète et incrémentielle corrects en vue d'une restauration. Les quatre premières lignes reprennent les informations de l'en-tête du fichier de sauvegarde.

Les autres fichiers inclus dans la sauvegarde de la base de données, tels que les fichiers NICI ou ceux listés dans un fichier d'inclusion, sont également consignés dans le fichier journal.

Pour une restauration, ce dernier enregistre aussi les fichiers inclus qui ont été restaurés.

Voici deux exemples d'entrées de fichier journal :

```
|=================DSBackup Log: Backup===============|
Backup type: Full
Log file name: sys:/backup/backup.log
Backup started: 2002-6-21'T19:53:5GMT
Backup file name: sys:/backup/backup.bak
Server name: \T=VIRTUALNW_TREE\O=novell\CN=VIRTUALNW
Current Roll Forward Log: 00000001.log
DS Version: 1041072
Backup ID: 3D138421
Backing up security file: sys:/system/nici/INITNICI.LOG
Backing up security file: sys:/system/nici/NICISDI.KEY
Backing up security file: sys:/system/nici/XARCHIVE.000
Backing up security file: sys:/system/nici/XARCHIVE.001
Backing up security file: sys:/system/nici/XMGRCFG.KS2
Backing up security file: sys:/system/nici/XMGRCFG.KS3
Backing up security file: sys:/system/nici/XMGRCFG.NIF
Starting database backup...
Database backup finished
Completion time 00:00:03
Backup completed successfully

|=================DSBackup Log: Restore==============|
Log file name: sys:/save/doc.log
Restore started: 2002-7-19'T19:1:34GMT
Restore file name: sys:/backup/backup.bak
Starting database restore...
Restoring file sys:/backup/backup.bak
Restoring file sys:/system/nici/INITNICI.LOG
Restoring file sys:/system/nici/NICISDI.KEY
Restoring file sys:/system/nici/XARCHIVE.000
Restoring file sys:/system/nici/XARCHIVE.001
Restoring file sys:/system/nici/XMGRCFG.KS2
Restoring file sys:/system/nici/XMGRCFG.KS3
Restoring file sys:/system/nici/XMGRCFG.NIF
Database restore finished
Completion time 00:00:15
Restore completed successfully
```

Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre

Si vous possédez un environnement multiserveur et souhaitez planifier la reprise après un sinistre entraînant la perte de tous vos serveurs, vous pouvez utiliser des serveurs DSMASTER dans le cadre du plan de restauration de votre arborescence.

L'outil Backup eMTool s'emploie pour sauvegarder chaque serveur séparément ; il est axé sur le serveur, et non sur l'arborescence. Si toutefois, vous créez des serveurs DSMASTER, vous pouvez utiliser les fonctionnalités de Backup eMTool pour sauvegarder toute la structure de votre arborescence. Un exemple de sauvegarde impliquant des serveurs DSMASTER est présenté à la section « Scénario : perte de tous les serveurs dans un environnement multiserveur », page 451.

Lors d'une restauration après un sinistre, l'un des principaux problèmes consiste à éviter de restaurer des répliques de la même partition qui ne concordent pas. Si, à la suite d'un sinistre, vous perdez les fichiers journaux de transactions individuelles de vos serveurs, vous ne pouvez pas restaurer ces derniers au même point dans le temps. Sans ces fichiers journaux, les répliques qui se trouvent dans vos sauvegardes ne concordent pas. Cela entraîne des problèmes si elles sont

toutes restaurées au même moment et intégrées ensemble à l'arborescence. (Le processus de vérification de la restauration a pour but d'éviter ces problèmes : par défaut, une base de données eDirectory restaurée ne s'ouvre pas après une restauration si elle ne concorde pas avec les autres répliques.)

Vous pouvez recourir à des serveurs DSMASTER pour vous préparer à cette situation, en créant une copie maîtresse de l'arborescence que vous utiliserez comme point de départ.

Pour utiliser des serveurs DSMASTER en prévision d'un éventuel sinistre :

- Organisez vos répliques pour qu'un serveur contienne une réplique de chaque partition de l'arborescence. Ainsi, vous pouvez disposer d'une copie de l'ensemble de l'arborescence dans la base de données eDirectory d'un seul serveur (si l'arborescence est trop grande, vous pouvez utiliser deux serveurs clés). Ce type de serveur est souvent appelé serveur DSMASTER. Les répliques du serveur DSMASTER doivent être de type maîtresse ou Lecture/écriture.

  REMARQUE : si vous utilisez deux serveurs DSMASTER clés, gardez à l'esprit que chacun doit en principe disposer d'un ensemble unique de répliques de partitions. Il ne doit pas y avoir de chevauchement pour éviter les incohérences entre les répliques lors de la restauration après un sinistre.

  Si un sinistre entraîne la perte de vos serveurs, vous n'aurez pas accès aux derniers fichiers journaux de transactions individuelles pour la restauration ; en effet, ceux-ci sont enregistrés localement sur le serveur, de sorte qu'il sera probablement impossible de restaurer tous les serveurs DSMASTER au même point dans le temps. Si la même réplique est stockée sur deux serveurs DSMASTER, les deux copies ne seront probablement pas identiques, ce qui entraînera des incohérences dans l'arborescence. Pour préparer une reprise après sinistre, il est donc préférable qu'une même partition ne soit pas répliquée sur plusieurs serveurs DSMASTER.

  Pour obtenir des informations générales sur les répliques, reportez-vous à la section « Répliques », page 52.

- Sauvegardez régulièrement les serveurs DSMASTER pour créer une copie de sauvegarde de votre arborescence. Il peut, en outre, être judicieux de prendre des précautions supplémentaires pour le stockage des sauvegardes des serveurs DSMASTER dans le cadre de votre plan de reprise après sinistre.

Si vous concevez votre arborescence de cette façon, en cas de sinistre, la structure de l'arborescence pourra rapidement redevenir opérationnelle ; il vous suffira de restaurer le serveur concerné (ou le petit groupe de serveurs clés) et de vous assurer que les répliques qu'il contient sont bien celles désignées comme maîtresses.

Une fois la structure de l'arborescence redevenue opérationnelle, vous pourrez restaurer les autres serveurs perdus en utilisant uniquement les fichiers de sauvegarde complète et incrémentielle. Cependant, comme vous ne disposez pas des fichiers journaux de transactions individuelles, la vérification de la restauration échoue pour ces autres serveurs. Pour les réintégrer dans l'arborescence, vous devrez les supprimer de l'anneau de répliques, changer en références externes toutes les informations concernant leurs répliques à l'aide de DSRepair, puis leur ajouter de nouveau les répliques en effectuant la réplication à partir de la copie figurant sur le serveur DSMASTER. Ces opérations sont décrites à la section « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442.

Si, lors d'un sinistre, vous perdez une grande partie de vos serveurs, la procédure liée aux répliques risque d'être complexe. Dans ce cas, nous vous conseillons de contacter le support technique de Novell.

Vecteurs de transition et processus de vérification de la restauration

Un vecteur de transition est un tampon horaire pour une réplique. Ce tampon est constitué d'une représentation du nombre de secondes écoulées depuis un point de référence historique commun (1erjanvier1970), du numéro de réplique et du numéro d'événement en cours. En voici un exemple :

```
s3D35F377 r02 e002
```

Dans le contexte de la sauvegarde et de la restauration, le vecteur de transition est important car il sert à vérifier que le serveur restauré est synchronisé avec les anneaux de répliques auxquels il participe.

Les serveurs qui contiennent des répliques dune même partition communiquent entre eux pour que celles-ci restent synchronisées en permanence. Chaque fois qu'un serveur communique avec un autre serveur de l'anneau de répliques, il conserve un enregistrement du vecteur de transition de l'autre serveur au moment de la communication. Les vecteurs de transition permettent aux serveurs d'un anneau de répliques de savoir quelles informations ils doivent envoyer à chacune des répliques de l'anneau pour assurer leur synchronisation. Lorsqu'un serveur s'arrête, il cesse de communiquer. Les autres serveurs ne lui envoient plus de mises à jour et ne modifient plus le vecteur de transition qu'ils ont enregistré pour lui jusqu'à ce qu'il recommence à communiquer.

Lorsque vous restaurez eDirectory sur un serveur, le processus de vérification de la restauration compare le vecteur de transition du serveur en cours de restauration et celui des autres serveurs de l'anneau de répliques. Cela permet de s'assurer que les répliques restaurées sont dans l'état attendu par les autres serveurs.

Si le vecteur de transition du serveur distant est en avance par rapport au vecteur local, il manque alors des données dans la restauration et la vérification échoue. (Par exemple, des données peuvent être manquantes pour les raisons suivantes : vous n'avez pas activé la consignation continue de transactions individuelles par fichier avant la dernière sauvegarde complète ou incrémentielle, vous n'avez pas inclus les fichiers journaux de transactions individuelles dans la restauration ou l'ensemble de fichiers journaux que vous avez fourni pour la restauration est incomplet.)

Par défaut, la base de données eDirectory restaurée n'est pas ouverte si elle est incohérente par rapport aux autres répliques.

Pour obtenir un exemple d'entrée de fichier journal lorsque les vecteurs de transition ne concordent pas, reportez-vous à la section « Présentation du processus de restauration avec Backup eMTool », page 391.

Pour obtenir une description des problèmes de compatibilité pouvant faire échouer la vérification de la restauration, reportez-vous à la section « Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement », page 399.

Pour plus d'informations sur la procédure à suivre en cas d'échec de la vérification de la restauration, reportez-vous à la section « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442.

Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement

Le processus de vérification de la restauration est rétrocompatible avec eDirectory 8.5 et versions ultérieures uniquement. Si le serveur que vous restaurez partage une réplique avec un serveur qui exécute une version de eDirectory antérieure à 8.5, le journal de restauration indique l'erreur 666 (version DS incompatible) pour cette réplique. Cela n'indique pas si les répliques sont

désynchronisées ; cette erreur signifie simplement que le processus de vérification de la restauration ne peut pas comparer les vecteurs de transition étant donné que la version de eDirectory est antérieure à 8.5.

Par défaut, la base de données ne s'ouvre pas car la vérification de la restauration ne s'est pas déroulée correctement. Dans ce cas, faites appel à votre bon sens. Si la seule erreur provient d'un serveur8.5 et si les autres serveurs ont été correctement vérifiés, vous pouvez choisir d'ouvrir la base de données en sélectionnant l'option de remplacement de la restauration, disponible dans le client eMBox.

Vous pouvez aussi supprimer de l'anneau de répliques le serveur exécutant une version antérieure, puis recommencer la restauration.

Pour plus d'informations sur le processus de restauration et les vecteurs de transition, reportez-vous aux sections « Présentation du processus de restauration avec Backup eMTool », page 391 et « Vecteurs de transition et processus de vérification de la restauration », page 399.

Préservation des droits lors de la restauration des données du système de fichiers sous NetWare

Sous NetWare uniquement, la restauration des droits du système de fichiers (appelés aussi assignations d'ayant droit) dépend de l'objet qui est l'ayant droit actuel dans eDirectory. Compte tenu de cette relation, vous devez procéder avec précaution lorsque vous restaurez eDirectory et les données du système de fichiers sous NetWare, afin de préserver les droits du système de fichiers.

Si vous restaurez eDirectory *avant* les données du système de fichiers, les droits du système de fichiers devraient normalement être préservés lors de la restauration des données. Vous devez néanmoins être conscient des problèmes Recherchez les problèmes éventuels et prenez des mesures préventives au besoin.

Impact éventuel d'une restauration sur les droits du système de fichiers

Dans le cadre de votre préparation à la restauration de eDirectory, vous devez procéder à une nouvelle installation de eDirectory en créant une arborescence temporaire, soit sur un nouveau périphérique de stockage destiné à remplacer l'unité défaillante qui contenait le volume sys:, soit sur une nouvelle machine, si vous faites migrer un serveur d'une machine vers une autre.

Une nouvelle installation de eDirectory ne contient pas les objets auxquels des droits d'ayant droit ont été assignés. (Il va de soi que les objets seront restaurés lors de la restauration de eDirectory.)

Lors de la restauration des données du système de fichiers, le processus de restauration recherche les objets ayants droit dans eDirectory. Si un objet désigné comme ayant droit n'existe pas dans la base de données eDirectory (comme dans le cas d'une nouvelle installation avant la restauration de eDirectory), il se peut que les assignations de droits de cet objet soient supprimées du système de fichiers.

Comment procéder en cas de problème

Pour résoudre les problèmes liés aux restaurations et aux droits du système de fichiers/assignations d'ayant droit, vous disposez de plusieurs méthodes différentes :

- Le pus important est de restaurer eDirectory avant le système de fichiers.

Vous pouvez effectuer une nouvelle installation et restaurer eDirectory sans prendre de mesures particulières, puis, une fois eDirectory restauré, prévoir d'effectuer une restauration du système de fichiers pour tous les fichiers pour lesquels vous devez rétablir des droits/assignations d'ayant droit.

- Dans le cadre de votre stratégie de sauvegarde, vous pouvez utiliser trustbar.nlm pour sauvegarder et restaurer les droits/assignations d'ayant droit du système de fichiers, ou un logiciel tiers comparable. De cette manière, vous pouvez au besoin rétablir des assignations d'ayant droit sur le système de fichiers, une fois eDirectory restauré.

  Vous pouvez planifier des sauvegardes des droits/assignations d'ayant droit du système de fichiers à intervalles réguliers, comme vous le faites pour eDirectory et le système de fichiers.

  REMARQUE : vous pouvez planifier la sauvegarde des droits du système de fichiers à l'aide d'un logiciel tiers, ou de cron.nlm (http://support.novell.com/servlet/tidfinder/2939440), disponible sur le site Web du support Novell.

- Vous pouvez reconfigurer votre système de stockage afin de réduire les risques de défaillances nécessitant la restauration de eDirectory et des données du système de fichiers. Ainsi, en utilisant un système RAID ou une autre configuration, vous pouvez réduire le risque de perte de données en cas de défaillance d'un périphérique de stockage. Si vous disposez d'un volume sys: redondant et qu'un périphérique est défaillant, il y a plus de chances qu'une nouvelle installation de eDirectory et une restauration du système de fichiers ne soient pas nécessaires.

- Si, pour l'une ou l'autre raison, vous restaurez les données du système de fichiers avant eDirectory et que vous perdez des droits, vous pouvez recommencer la restauration du système de fichiers après celle de eDirectory.

- Vous pouvez faire en sorte qu'aucun volume, à l'exception de sys:, ne soit monté tant que eDirectory n'est pas restauré, par exemple, dans le cas où la défaillance d'un périphérique de stockage affecterait le volume sys:, les autres périphériques de stockage du serveur restant opérationnels.

  Pour cela, vous pouvez déconnecter les périphériques de stockage du serveur avant la nouvelle installation de NetWare et de eDirectory, puis les reconnecter une fois eDirectory restauré.

  Après la restauration de eDirectory, vous pouvez, au besoin, restaurer le système de fichiers du volume sys:, pour récupérer les droits sur ce volume.

Utilisation des fichiers journaux de transactions individuelles

La consignation de transactions individuelles par fichier s'apparente à la journalisation dans d'autres produits de bases de données. Les fichiers journaux de transactions individuelles enregistrent toutes les modifications opérées dans la base de données.

L'intérêt de la consignation de transactions individuelles par fichier est qu'elle fournit un historique des modifications depuis la dernière sauvegarde complète ou incrémentielle, de sorte que vous pouvez restaurer eDirectory dans l'état où il se trouvait avant une défaillance. Sans les fichiers journaux de transactions individuelles, vous ne pouvez restaurer eDirectory que dans l'état où il se trouvait au moment de la dernière sauvegarde complète ou incrémentielle.

eDirectory enregistre les transactions dans un fichier journal avant de les appliquer à la base de données. Par défaut, ce fichier journal est réutilisé continuellement (occupant ainsi peu d'espace disque) et l'historique des changements apportés à la base de données eDirectory n'est pas enregistré.

Lorsque vous activez la consignation continue de transactions individuelles par fichier, l'historique des modifications est enregistré dans un jeu de fichiers journaux de transactions individuelles consécutifs. La consignation de transactions individuelles par fichier ne réduit pas les performances du serveur ; elle enregistre simplement les entrées du fichier journal que eDirectory est déjà en train de créer.

Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Si vous ne le faites pas, des erreurs se produisent lors de la restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvre pas. Avec la restauration par défaut, une base de données qui partage des répliques avec d'autres serveurs n'est pas ouverte tant qu'elle n'a pas été restaurée dans l'état où elle se trouvait au moment de l'arrêt du système. (En l'absence de fichiers journaux de transactions individuelles, vous devez suivre une procédure distincte pour tenter de récupérer ce qui a été perdu, comme expliqué dans la section « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442.)

Par défaut, la consignation de transactions individuelles par fichier est désactivée. Vous devez l'activer pour pouvoir l'utiliser sur un serveur. Elle est également désactivée lorsque vous restaurez un serveur, et les paramètres reprennent leur valeur par défaut. Après une restauration, vous devez donc la réactiver et recréer votre configuration. (Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.)

Dans un environnement monoserveur, la consignation de transactions individuelles par fichier n'est pas nécessaire. Vous pouvez néanmoins l'utiliser si vous souhaitez pouvoir restaurer eDirectory dans l'état où il se trouvait avant son arrêt, au lieu de bénéficier simplement de l'état enregistré dans la dernière sauvegarde.

Pensez à contrôler l'espace disque lorsque la consignation de transactions individuelles par fichier est activée. Pour plus d'informations, reportez-vous à la section « Sauvegarde et suppression des fichiers journaux de transactions individuelles », page 405.

Cette section fournit les informations suivantes :

Vous pouvez activer et configurer la consignation de transactions individuelles par fichier à l'aide de iManager ou du client eMBox. Reportez-vous à la section « Configuration des fichiers journaux de transactions individuelles avec iManager », page 413 ou « Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox », page 426.

Considérations utiles concernant la consignation de transactions individuelles par fichier

Si vous décidez d'utiliser la fonction de consignation de transactions individuelles par fichier, vous devez tenir compte des considérations suivantes :

- **Activez la consignation de transactions individuelles par fichier avant d'effectuer une sauvegarde** si vous souhaitez pouvoir l'utiliser pour restaurer la base de données.
- **Pour assurer une tolérance aux pannes, veillez à placer les fichiers journaux de transactions individuelles sur un périphérique de stockage différent de celui de eDirectory.** Par mesure de sécurité, veillez également à restreindre les droits d'accès aux fichiers journaux des utilisateurs. Pour plus d'informations, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles », page 404.
- **Notez l'emplacement des fichiers journaux de transactions individuelles.** Pour plus d'informations, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles », page 404.
- **Contrôlez l'espace disque disponible à l'emplacement de stockage des fichiers journaux.** Pour plus d'informations, reportez-vous à la section « Sauvegarde et suppression des fichiers journaux de transactions individuelles », page 405.
- **Si les fichiers journaux ont été désactivés ou perdus, réactivez-les, puis effectuez une nouvelle sauvegarde complète** afin de pouvoir effectuer une récupération totale. Cette opération est nécessaire dans les cas suivants :
  - Après une restauration. La consignation de transactions individuelles par fichier est désactivée et les paramètres reprennent leur valeur par défaut dans le cadre du processus de restauration.
  - Si vous perdez le répertoire contenant les fichiers journaux de transactions individuelles en raison de la défaillance d'un périphérique de stockage ou d'une autre panne.
  - Si les fichiers journaux de transactions individuelles ont été désactivés par inadvertance.
- **Si vous activez la consignation des fichiers de flux, les fichiers journaux de transactions individuelles consomment l'espace disque plus rapidement.** Lorsque vous activez la consignation des fichiers de flux (les scripts de login, par exemple), le fichier de flux complet est copié dans le fichier journal de transaction individuelle à chaque modification. La taille des fichiers journaux augmentera moins rapidement si vous désactivez la consignation des fichiers de flux et ne sauvegarder ces derniers que lors d'une sauvegarde complète ou incrémentielle.
- **La phase la plus lente de la restauration de la base de données est la lecture des fichiers journaux de transactions individuelles.** La taille de ces fichiers journaux dépend du nombre de modifications apportées à l'arborescence et de la consignation éventuelle des fichiers de flux (tels que les scripts de login).

  Si votre base de données change fréquemment, vous pouvez envisager d'effectuer des sauvegardes de eDirectory plus souvent pour réduire le nombre de changements à traiter à partir des fichiers journaux de transactions individuelles durant une restauration.
- **Ne renommez pas un fichier journal de transaction individuelle.** Si un fichier journal porte un nom différent de celui qu'il avait lors de sa création, il ne peut pas être utilisé dans une restauration.

- **N'oubliez pas que la suppression de eDirectory entraîne celle de tous les fichiers journaux de transactions individuelles.** Si vous souhaitez pouvoir utiliser les fichiers journaux pour une restauration ultérieure, vous devez les copier à un autre emplacement avant de supprimer eDirectory.
- **Si une restauration est nécessaire, veillez à reconfigurer les fichiers journaux de transactions individuelles sur le serveur une fois la restauration terminée** afin de vous assurer qu'ils sont activés et qu'ils se trouvent à un emplacement assurant la tolérance aux pannes. Après avoir activé les fichiers journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

  Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Emplacement des fichiers journaux de transactions individuelles

Si vous activez la consignation de transactions individuelles par fichier, veillez à changer l'emplacement du répertoire des fichiers journaux de transactions individuelles afin d'utiliser un périphérique de stockage différent de celui de eDirectory.

Voici quelques points importants à prendre en compte lors du choix de l'emplacement :

- **Ne laissez pas les fichiers journaux à l'emplacement par défaut ; veillez à les enregistrer sur un périphérique de stockage différent de celui de eDirectory.** Ainsi, si eDirectory est perdu en raison de la défaillance d'un périphérique de stockage, vous pouvez quand même accéder aux fichiers journaux de transactions individuelles pour le restaurer.

  Par exemple, sous NetWare, l'emplacement par défaut est sys:_netware\nds.rfl\. Toutefois, si vous activez la consignation de transactions individuelles par fichier, vous ne devez pas utiliser cet emplacement. Les fichiers journaux ne doivent pas résider sur le volume sys: car ce dernier contient la base de données eDirectory.

  Si votre serveur ne comprend qu'un seul périphérique de stockage, les fichiers journaux de transactions individuelles ne permettent pas d'assurer la tolérance aux pannes de eDirectory en cas de défaillance de ce périphérique. Dans ce cas, il est préférable de ne pas les utiliser.

  Vous pouvez modifier l'emplacement des fichiers journaux de transactions individuelles à l'aide des options Configuration de la sauvegarde dans iManager ou setconfig dans le client eMBox. Ces fichiers journaux doivent se trouver dans un répertoire local du serveur.
- **Notez l'emplacement des fichiers journaux.** Vous devez noter l'emplacement de stockage des fichiers journaux de transactions individuelles de manière à pouvoir les retrouver si vous devez restaurer la base de données sur un serveur. Il est important de le faire lorsque le serveur est sain, avant qu'un incident ne survienne.

  Pour localiser cet emplacement lorsque le serveur est sain, vous pouvez utiliser l'option Configuration de la sauvegarde dans iManager ou getconfig dans le client eMBox. Toutefois, si le serveur connaît une défaillance affectant eDirectory (une panne matérielle, par exemple), vous ne pouvez pas rechercher l'emplacement des fichiers journaux de transactions individuelles.

  Si vous tentez de restaurer un serveur qui a déjà subi une défaillance, sachez qu'à chaque nouvelle installation de eDirectory, c'est l'emplacement par défaut des fichiers journaux de transactions individuelles qui est indiqué. Par conséquent, si vous venez de réinstaller eDirectory lors de la première étape d'un processus de restauration, eDirectory n'indique pas l'emplacement où étaient stockés les fichiers journaux avant la défaillance du serveur. Vous devez vous reporter à vos notes pour savoir où ils se trouvent.

La configuration des fichiers journaux de transactions individuelles est également enregistrée dans le fichier _ndsdb.ini, mais celui-ci figure sur le même volume/partition de disque que eDirectory. Par conséquent, si vous perdez le périphérique de stockage sur lequel se trouve eDirectory, vous ne pourrez pas employer ce fichier pour rechercher l'emplacement des fichiers journaux.

- **Limitez les droits d'accès pour l'emplacement de stockage des fichiers journaux de transactions individuelles.** C'est une question de sécurité. Les informations ne sont pas facilement lisibles, mais il est possible de décoder les fichiers journaux pour accéder à des données sensibles.
- **Contrôlez si l'espace disque disponible est suffisant.** Pour plus de détails, reportez-vous à la section « Sauvegarde et suppression des fichiers journaux de transactions individuelles », page 405.
- **Il est recommandé de réserver un volume/une partition de disque aux fichiers journaux de transactions individuelles.** Il est ainsi plus facile de contrôler les privilèges de sécurité et l'espace disque.
- **Le dernier répertoire du chemin d'accès est créé par eDirectory.** Il correspond au nom de la base de données eDirectory actuelle.

  Ainsi, si l'emplacement spécifié correspond à d:\Novell\NDS\DIBFiles\ et le nom de votre base de données eDirectory à NDS, l'emplacement des fichiers journaux de transactions individuelles est alors d:\Novell\NDS\DIBFiles\nds.rfl\. Si vous renommez la baseNDS en ND1, le répertoire des fichiers journaux devient d:\Novell\NDS\DIBFiles\nd1.rfl.

  Le répertoire est créé immédiatement après le changement d'emplacement, mais aucun fichier journal de transaction individuelle n'est créé tant qu'aucune transaction n'a lieu dans la base de données.
- **Lors de la restauration, tous les fichiers journaux de transactions individuelles nécessaires doivent figurer dans le même répertoire.** Pour plus d'informations, reportez-vous à la section « Préparation d'une restauration », page 406.

Sauvegarde et suppression des fichiers journaux de transactions individuelles

S'ils ne sont pas surveillés, les fichiers journaux de transactions individuelles peuvent saturer le volume/la partition de disque qui les reçoit. Si ces fichiers journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Il est conseillé de sauvegarder périodiquement les fichiers journaux et de supprimer du serveur ceux qui ne sont pas utilisés afin de libérer de l'espace disque.

Pour identifier, sauvegarder et supprimer les fichiers journaux de transactions individuelles dont la suppression ne pose pas de problème, procédez comme suit :

1. Notez le nom du dernier fichier journal de transaction individuelle inutilisé.

   Pour trouver le nom de ce fichier journal, vous avez plusieurs possibilités :

   - Dans iManager, cliquez sur Maintenance de eDirectory > Configuration de la sauvegarde et consultez le nom de fichier affiché.
   - Dans le client eMBox, entrez la commande de sauvegarde getconfig. Pour plus d'informations, reportez-vous à la section « Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox », page 426.

Le dernier fichier journal de transaction individuelle inutilisé correspond au fichier le plus récent que la base de données a renseigné et qu'elle n'utilise plus pour enregistrer des transactions. Il s'agit du dernier fichier journal de transaction individuelle inutilisé puisque la base de données a fini d'y enregistrer des informations et a créé un nouveau fichier journal, de sorte qu'elle n'a plus besoin de le maintenir ouvert. (Le fichier journal actuellement utilisé pour l'enregistrement des transactions est toujours nécessaire à la base de données.)

2. Sauvegardez les fichiers journaux de transactions individuelles à partir du système de fichiers, afin de les enregistrer sur bande par mesure de sécurité.
3. Supprimez les fichiers journaux de transactions individuelles plus anciens que le dernier inutilisé.

   AVERTISSEMENT : faites preuve de précaution lorsque vous supprimez des fichiers journaux de transactions individuelles du serveur. Assurez-vous que vous avez bien sauvegardé sur bande tous les fichiers journaux que vous supprimez.

   Le dernier fichier journal de transaction individuelle inutilisé indique le nom du fichier que la base de données vient de compléter et de fermer. Il ne précise pas si vous pouvez supprimer ce fichier du serveur en toute sécurité. Veillez à ne supprimer que les fichiers que vous avez sauvegardés sur bande.

Si vous devez récupérer certains fichiers journaux de transactions individuelles sauvegardés sur bande afin de les utiliser dans une restauration, tenez compte des points suivants :

- Comme tous les fichiers journaux de transactions individuelles utilisés pour une restauration, ceux récupérés à partir d'une bande de sauvegarde du système de fichiers doivent être placés dans le même dossier que les autres fichiers journaux, sur le serveur en cours de restauration.
- Comparez les tampons horaires des fichiers dupliqués sur la bande et sur le serveur. Si les tampons horaires diffèrent, utilisez le fichier le plus récent, c'est-à-dire celui du serveur. Par exemple, le fichier journal de transaction individuelle que la base de données utilisait au moment de la sauvegarde du système de fichiers est incomplet sur la bande ; la version complète et la plus récente de ce fichier se trouve sur le serveur.

Avertissement : la suppression de eDirectory entraîne également celle des fichiers journaux de transactions individuelles.

Si vous supprimez eDirectory de votre serveur, le répertoire des fichiers journaux de transactions individuelles et son contenu sont également supprimés. Si vous souhaitez utiliser les fichiers journaux ultérieurement pour restaurer le serveur, vous devez les copier à un autre emplacement avant de supprimer eDirectory.

Préparation d'une restauration

Lors de la restauration de la base de données eDirectory, le plus important est de s'assurer qu'elle est complète. Avant de restaurer une base de données eDirectory sur un serveur, assurez-vous que les conditions préalables ont été remplies, comme expliqué dans la section « Conditions préalables à la restauration », page 407. En cas de doutes concernant la collecte des fichiers de sauvegarde appropriés, reportez-vous à la section « Localisation des fichiers de sauvegarde requis pour une restauration », page 408.

Conditions préalables à la restauration

- ❑ Tous les serveurs qui partagent une réplique avec le serveur à restaurer doivent être en service et communiquer. Le processus de vérification de la restauration peut ainsi effectuer un contrôle auprès des serveurs qui font partie d'un même anneau de répliques.
- ❑ Vous avez collecté tous les fichiers de sauvegarde requis :
  - Le fichier de sauvegarde complète et les fichiers incrémentiels consécutifs ont été copiés dans un répertoire du serveur à restaurer.
  - Tous les fichiers journaux de transactions individuelles depuis la dernière sauvegarde se trouvent dans un répertoire du serveur à restaurer.

    Si le serveur fait partie d'un anneau de répliques, vous devez vous assurer que tous les fichiers journaux de transactions individuelles créés depuis la dernière sauvegarde figurent dans un même répertoire du serveur, sous le nom qu'ils avaient au moment de leur création.

  Pour plus de détails, reportez-vous à la section « Localisation des fichiers de sauvegarde requis pour une restauration », page 408.

  REMARQUE : si vous ne disposez pas de fichiers de sauvegarde pour le serveur, utilisez XBrowse pour tenter de récupérer des informations sur ce dernier en sondant eDirectory. Effectuez cette opération avant de supprimer l'objet Serveur ou tout objet associé de l'arborescence. Vous trouverez XBrowse ainsi que des informations supplémentaires sur le siteWeb du support Novell, solution 2960653 (http://support.novell.com/servlet/tidfinder/2960653).
- ❑ Vous avez installé eDirectory dans une nouvelle arborescence temporaire.

  Il est nécessaire, dans un premier temps, de rétablir le serveur dans une nouvelle arborescence car vous allez le créer sous le nom qu'il avait avant la défaillance, mais vous devez éviter la confusion qu'entraînerait son intégration dans l'arborescence originale avant que la restauration n'ait recréé son identité complète. Une fois le processus de restauration de la base de données terminé, le serveur est rétabli dans son arborescence d'origine.
- ❑ (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier sur ce serveur, prévoyez de recréer la configuration appropriée à l'issue de la restauration, afin d'être certain que la fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les fichiers journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

  Le processus de restauration désactive la fonction de consignation et rétablit la configuration par défaut pour cette dernière.

  Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.
- ❑ (Conditionnel) Si des applications ou des objets doivent rechercher le serveur par son adresse IP, prévoyez d'utiliser la même adresse IP pour le serveur restauré.
- ❑ (NetWare uniquement) Assurez-vous que le nom du serveur sur lequel vous effectuez la restauration est identique à celui du serveur défaillant. Si les noms diffèrent, des erreurs peuvent se produire, par exemple des objets Volume incorrects après la restauration.

  Pour changer le nom du serveur NetWare sur lequel vous effectuez la restauration, remplacez le nom qui figure dans le fichier autoexec.ncf et redémarrez le serveur.

- ❑ (NetWare uniquement) Tenez compte des problèmes liés à la préservation des droits du système de fichiers lors de la restauration des données du système de fichiers et de eDirectory. Nous vous conseillons de restaurer eDirectory avant les données du système de fichiers. Vous devrez peut-être effectuer des opérations supplémentaires, comme expliqué dans la section « Préservation des droits lors de la restauration des données du système de fichiers sous NetWare », page 400.

eDirectory Backup eMTool restaure d'abord la sauvegarde complète. Une fois cette opération terminée, il vous invite à saisir les noms des fichiers de sauvegarde incrémentielle. Il vous indique l'ID du fichier suivant. Une fois tous ces fichiers restaurés, Backup eMTool passe aux fichiers journaux de transactions individuelles. (Reportez-vous également à la section « Présentation du processus de restauration avec Backup eMTool », page 391.)

Après avoir collecté tous les fichiers nécessaires, effectuez la restauration à l'aide de iManager ou du client eMBox. Reportez-vous à la section « Restauration à partir de fichiers de sauvegarde avec le client eMBox », page 428 ou « Restauration à partir de fichiers de sauvegarde avec iManager », page 415.

Localisation des fichiers de sauvegarde requis pour une restauration

1. À partir de la bande de sauvegarde du système de fichiers, copiez les fichiers de la dernière sauvegarde complète de eDirectory dans un répertoire du serveur.

   Pour vérifier l'ID de la dernière sauvegarde complète, consultez le fichier journal de Backup eMTool.

2. À partir de la bande de sauvegarde du système de fichiers, copiez également chaque fichier de sauvegarde incrémentielle consécutif dans le même répertoire du serveur.

   Pour vérifier que vous disposez des fichiers de sauvegarde incrémentielle appropriés, consultez l'en-tête du fichier de sauvegarde complète. Il contient l'ID du fichier de sauvegarde incrémentielle suivant, dans l'attribut next_inc_file_ID. L'ID mentionné dans next_inc_file_ID est identique à celui enregistré dans l'en-tête du fichier de sauvegarde incrémentielle, dans l'attribut incremental_file_number (Pour obtenir une description de l'en-tête, reportez-vous à la section « Format de l'en-tête des fichiers de sauvegarde », page 392.)

   AVERTISSEMENT : lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car il pourrait alors devenir tronqué. La plupart des applications ne peuvent pas enregistrer correctement les données binaires.

   Chaque fichier de sauvegarde incrémentielle contient également l'ID du prochain fichier de sauvegarde incrémentielle.

   Vous pouvez aussi rechercher l'ID de sauvegarde incrémentielle dans le fichier journal de Backup eMTool.

   Les ID sont importants car il se peut que vos fichiers de sauvegarde aient reçu le même nom au moment de leur création (par exemple, si vous utilisez le même fichier de traitement par lots pour les sauvegardes incrémentielles sans surveillance, le nom du fichier de sauvegarde spécifié est toujours identique). Il peut alors être nécessaire de changer les noms de fichiers afin de pouvoir enregistrer toutes les sauvegardes dans le même répertoire. L'ID qui figure dans l'en-tête vous permet de trouver les fichiers appropriés, même si vous les avez renommés.

3 (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier sur ce serveur, assurez-vous que tous les fichiers journaux de transactions individuelles créés depuis la dernière sauvegarde figurent dans un répertoire du serveur, sous le nom de fichier qu'ils avaient au moment de leur création.

Si votre serveur fait partie d'un anneau de répliques, vous devez le restaurer en utilisant tous les fichiers journaux de transactions individuelles. Si vous ne les incluez pas tous et si le serveur partage des répliques avec d'autres serveurs, le processus de vérification de la restauration échoue parce que les vecteurs de transition ne correspondent pas à ceux des autres répliques de l'anneau. Par défaut, la base de données eDirectory restaurée n'est pas ouverte à l'issue de la restauration si elle est incohérente par rapport aux autres répliques.

Identifiez le premier journal de transaction individuelle dont vous avez besoin en ouvrant le dernier fichier de sauvegarde dans un éditeur de texte et en consultant l'attribut current_log dans l'en-tête. Vous devez collecter ce fichier journal ainsi que tous les suivants.

AVERTISSEMENT : lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car il pourrait alors devenir tronqué. La plupart des applications ne peuvent pas enregistrer correctement les données binaires.

Les fichiers journaux de transactions individuelles nécessaires peuvent ne pas tous figurer au même emplacement lorsque vous souhaitez les utiliser pour une restauration. Vous devez donc vous assurer que vous en avez collecté un jeu complet et les avez placés dans le même répertoire. Les fichiers journaux de transactions individuelles peuvent se trouver à différents emplacements pour les raisons suivantes :

- Vous avez modifié l'emplacement du répertoire des fichiers journaux de transactions individuelles depuis la dernière sauvegarde complète ou incrémentielle.
- Vous les avez enregistrés sur bande à l'aide de la sauvegarde du système de fichiers, puis supprimés du serveur pour libérer de l'espace disque.

  Si vous devez récupérer des fichiers journaux de transactions individuelles à partir d'une sauvegarde sur bande, assurez-vous que vous disposez du jeu de fichiers le plus récent. Comparez les tampons horaires des fichiers dupliqués sur la bande et sur le serveur. Le fichier journal de transaction individuelle utilisé par la base de données au moment de la sauvegarde du système de fichiers est incomplet sur la bande ; la version complète et la plus récente de ce fichier figure sur le serveur.
- Vous avez renommé la base de données eDirectory depuis la dernière sauvegarde (NDS est devenu ND1, par exemple). Cela modifie le dernier nom de répertoire dans le chemin d'accès aux fichiers journaux de transactions individuelles.

  Par exemple, si l'emplacement spécifié correspondait à d:\novell\nds\dibfiles\ et le nom de votre base de données eDirectory à NDS, l'emplacement des fichiers journaux de transactions individuelles correspondait à d:\novell\nds\dibfiles\nds.rfl\. Si vous avez renommé la base de données NDS en ND1, le répertoire des fichiers journaux de transactions individuelles est devenu d:\novell\nds\dibfiles\nd1.rfl\.

IMPORTANT : veillez à fournir tous les fichiers journaux de transactions individuelles requis. Backup eMTool ne peut pas déterminer si le jeu de fichiers journaux dont vous disposez est complet. Il les ouvre et les utilise dans l'ordre. S'il ne trouve pas le fichier journal suivant dans le répertoire indiqué, il met fin au processus de restauration. Si vous n'avez pas fourni tous les fichiers journaux nécessaires, la restauration est incomplète.

Utilisation de Novell iManager pour la sauvegarde et la restauration

Les tâches de sauvegarde, de configuration de la sauvegarde et de restauration de Novell iManager vous donnent accès à la plupart des fonctions de eDirectory Backup eMTool. En outre, iManager vous permet d'effectuer des tâches sur vos serveurs depuis un navigateur, même si vous êtes à l'extérieur du pare-feu. Pour plus d'informations sur Novell iManager, consultez le manuel *Novell iManager 2.5 Administration Guide (Guide d'administration de Novell iManager 2.5)* (http://www.novell.com/documentation/imanager25/index.html).

Les tâches non disponibles dans iManager sont la sauvegarde à froid (sauvegarde complète lorsque la base de données est fermée), la sauvegarde sans surveillance et les options de restauration avancées. Pour celles-ci, vous devez utiliser le client eMBox, comme expliqué dans la section « Utilisation du client eMBox pour la sauvegarde et la restauration », page 419.

Avant d'exécuter des tâches de sauvegarde et de restauration, consultez la « Liste de contrôle pour la sauvegarde de eDirectory », page 384 pour une vue d'ensemble des éléments à considérer lors de la préparation d'une stratégie de sauvegarde efficace pour eDirectory.

Cette section fournit les informations suivantes :

- « Sauvegarde manuelle avec iManager », page 410
- « Configuration des fichiers journaux de transactions individuelles avec iManager », page 413
- « Restauration à partir de fichiers de sauvegarde avec iManager », page 415

Sauvegarde manuelle avec iManager

Utilisez la fonction Sauvegarder de iManager à partir d'un navigateur pour sauvegarder les données d'une base de données eDirectory dans un ou plusieurs fichiers du serveur sur lequel la sauvegarde a lieu. Vous pouvez exécuter une sauvegarde complète ou incrémentielle.

Les fichiers de sauvegarde contiennent les informations nécessaires pour restaurer eDirectory dans l'état où il se trouvait au moment de la sauvegarde. Les résultats de la sauvegarde sont consignés dans le fichier journal que vous indiquez.

Les sauvegardes effectuées à l'aide de iManager sont des sauvegardes continues à chaud. Cela signifie que la base de données eDirectory est ouverte et accessible pendant le processus, mais que vous obtenez néanmoins une sauvegarde complète, image fidèle de l'état de la base au début de la sauvegarde.

Notez que pour effectuer une sauvegarde à froid (avec la base de données fermée) ou sans surveillance, vous devez employer le client eMBox. Reportez-vous aux sections « Sauvegarde manuelle à l'aide du client eMBox », page 419 et « Sauvegardes sans surveillance à l'aide d'un fichier de traitement par lots et du client eMBox », page 422.

Avant d'exécuter des tâches de sauvegarde et de restauration, consultez la « Liste de contrôle pour la sauvegarde de eDirectory », page 384 pour une vue d'ensemble des éléments à considérer lors de la préparation d'une stratégie de sauvegarde efficace pour eDirectory.

Conditions préalables

- Déterminez les autres fichiers à sauvegarder avec eDirectory et créez au besoin un fichier d'inclusion.

  Vous pouvez sauvegarder les fichiers NICI et de flux en cochant les cases correspondantes dans iManager. Nous vous recommandons de sauvegarder systématiquement les fichiers NICI.

  Pour inclure d'autres fichiers, tels que autoexec.ncf, vous devez indiquer leur chemin d'accès complet dans un fichier d'inclusion. Séparez les chemins d'accès par un point-virgule, sans inclure de retour chariot ni d'espace (Par exemple, sys:\system\autoexec.ncf;sys:\etc\hosts;).

- Prévoyez d'effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory si vous devez enregistrer les fichiers de sauvegarde de eDirectory sur bande (Backup eMTool les place uniquement sur le serveur.)

  SUGGESTION : pour faciliter le transfert des fichiers de sauvegarde eDirectory sur un autre périphérique de stockage, vous pouvez spécifier la taille maximale de ces fichiers. Vous pouvez également utiliser un logiciel tiers pour les compresser après leur création. Le taux de compression atteint environ 80%.

- Si vous prévoyez d'utiliser des fichiers journaux de transactions individuelles pour le serveur concerné, veillez à les activer avant d'effectuer une sauvegarde.

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Si vous ne le faites pas, des erreurs se produisent lors de la restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvre pas.

  Pour plus d'informations sur les fichiers journaux de transactions individuelles, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401. Pour savoir comment les activer, reportez-vous à la section « Configuration des fichiers journaux de transactions individuelles avec iManager », page 413.

- Pour les arborescences multiserveurs, nous vous conseillons de mettre à niveau tous les serveurs qui partagent des répliques avec le serveur concerné en installant eDirectory 8.5 ou une version ultérieure.

  Pour plus d'informations, reportez-vous à la section « Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement », page 399.

Procédure

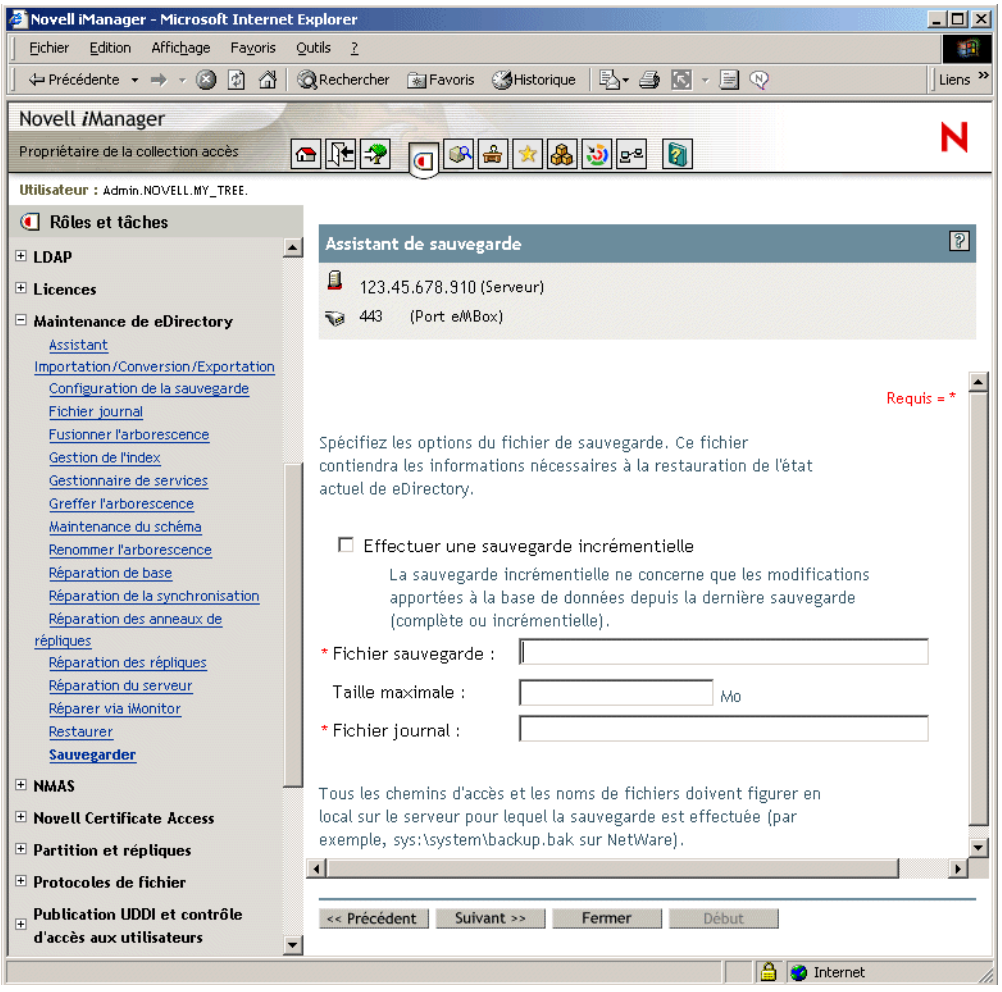
Pour sauvegarder la base de données eDirectory sur un serveur à l'aide de iManager, procédez comme suit :

SUGGESTION : l'aide en ligne fournit une description des options disponibles dans iManager.

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Sauvegarder.
3. Spécifiez le serveur qui effectuera la sauvegarde, puis cliquez sur Suivant.
4. Entrez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel la sauvegarde doit être effectuée, puis cliquez sur Suivant.
5. Spécifiez les options relatives au fichier de sauvegarde, puis cliquez sur Suivant.

   Pour ne sauvegarder que les modifications apportées à la base de données depuis la dernière sauvegarde, cliquez sur Effectuer une sauvegarde incrémentielle.

Voici un exemple d'écran.

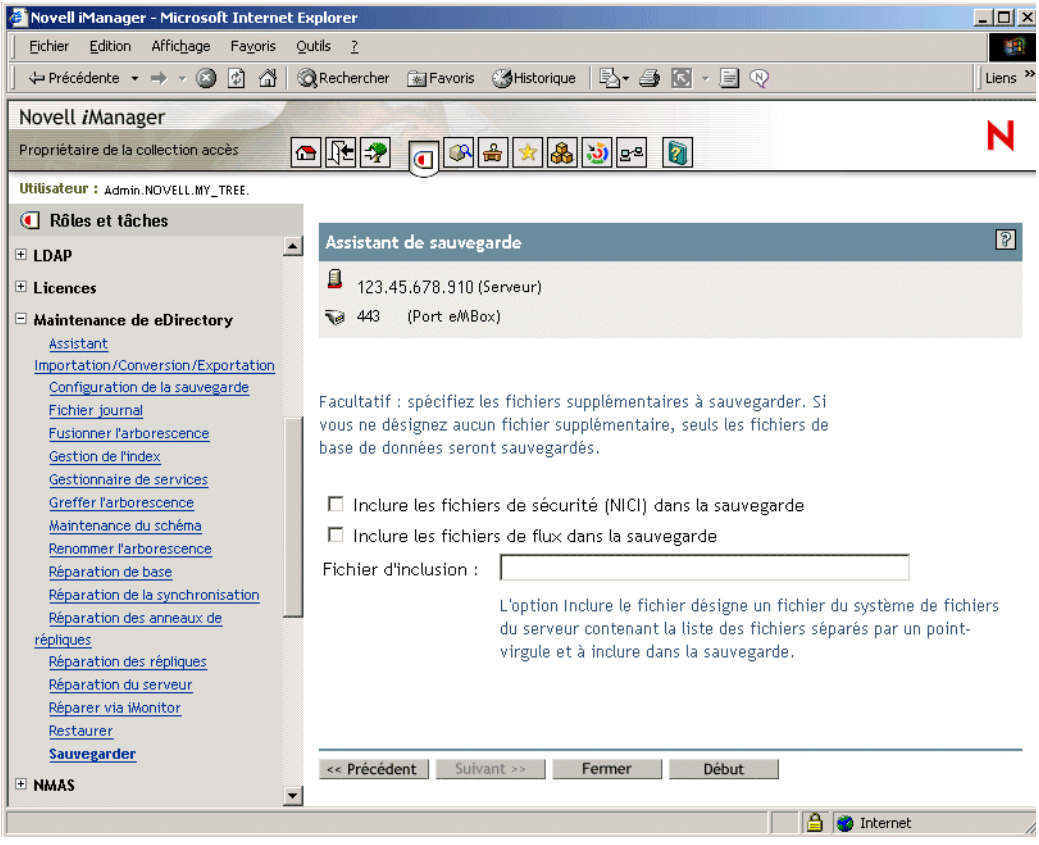


6 Désignez d'autres fichiers à sauvegarder.

Si aucun fichier supplémentaire n'est désigné, seule la base de données eDirectory est sauvegardée.

Nous vous conseillons de sauvegarder systématiquement les fichiers de sécurité NICI.

Voici un exemple d'écran.



7 Suivez les instructions en ligne pour terminer la sauvegarde.

8 Veillez à effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory, afin d'enregistrer les fichiers de sauvegarde sur bande par mesure de sécurité. (Backup eMTool les place uniquement sur le serveur.)

Configuration des fichiers journaux de transactions individuelles avec iManager

Utilisez l'option Configuration de la sauvegarde à partir d'un navigateur pour modifier les paramètres des fichiers journaux de transactions individuelles. Vous pouvez effectuer les tâches suivantes :

- activer ou désactiver la fonction de consignation de transactions individuelles par fichier ;

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Si vous ne le faites pas, des erreurs se produisent lors de la restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvre pas.

- modifier le répertoire des fichiers journaux de transactions individuelles ;
- définir la taille minimale et maximale des fichiers journaux de transactions individuelles ;
- déterminer le fichier journal de transaction individuelle actuel ainsi que le dernier fichier journal utilisé ;
- activer ou désactiver la consignation des fichiers de flux pour les fichiers journaux de transactions individuelles.

Pour plus d'informations sur les fichiers journaux de transactions individuelles, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

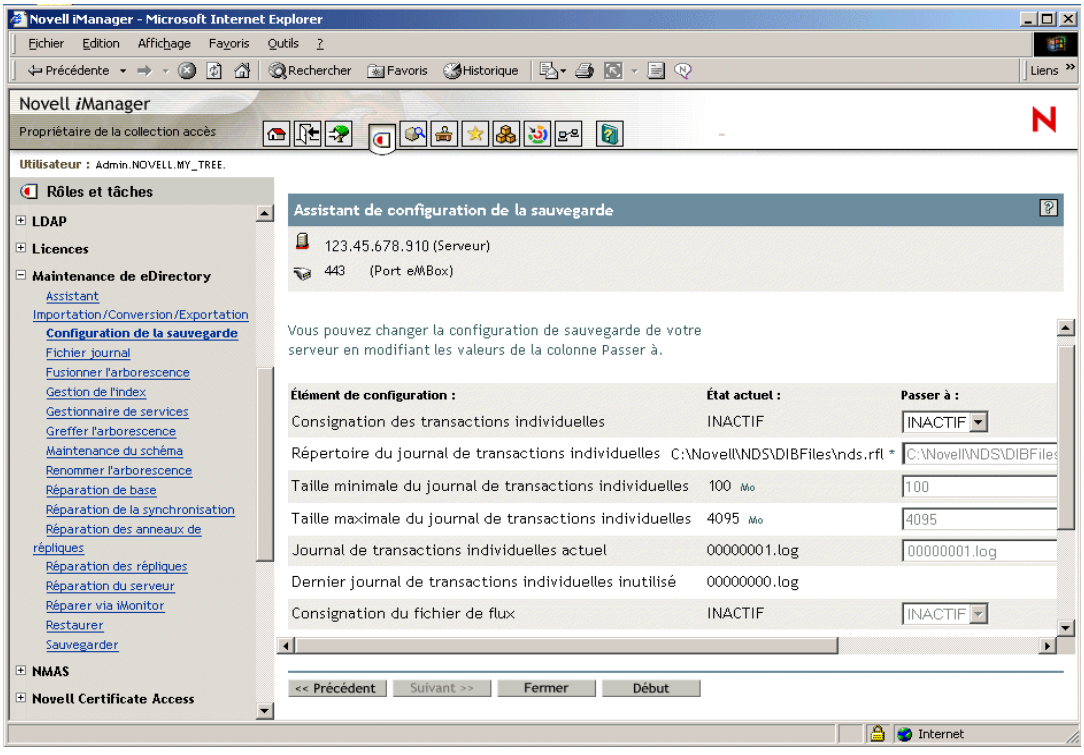
SUGGESTION : l'aide en ligne fournit une description des options disponibles dans iManager.

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Configuration de la sauvegarde.
3. Sélectionnez le serveur qui modifiera la configuration, puis cliquez sur Suivant.
4. Entrez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel la configuration sera modifiée, puis cliquez sur Suivant.
5. Apportez les modifications requises à la configuration de sauvegarde du serveur.

   AVERTISSEMENT : si vous activez la consignation de transactions individuelles par fichier, n'utilisez pas l'emplacement par défaut. Pour assurer une tolérance aux pannes, placez le répertoire sur un volume/une partition de disque et un périphérique de stockage différents de ceux de eDirectory. Le répertoire des fichiers journaux de transactions individuelles doit résider sur le serveur sur lequel vous modifiez la configuration de sauvegarde.

   IMPORTANT : si vous activez la consignation de transactions individuelles par fichier, vous devez surveiller l'espace disque sur le volume où vous placez les fichiers journaux de transactions individuelles. Si vous ne le surveillez pas, le répertoire des fichiers journaux s'étend jusqu'à saturer le volume/la partition de disque. Si ces fichiers journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Nous vous conseillons de sauvegarder et de supprimer périodiquement du serveur les fichiers journaux de transactions individuelles inutilisés. Pour plus de détails, reportez-vous à la section « Sauvegarde et suppression des fichiers journaux de transactions individuelles », page 405.

   Voici un exemple d'écran.



6 Suivez les instructions en ligne pour terminer l'opération.

Restauration à partir de fichiers de sauvegarde avec iManager

Utilisez l'option Restaurer dans un navigateur pour restaurer une base de données eDirectory à partir des données enregistrées dans des fichiers de sauvegarde. Les résultats de la restauration sont consignés dans le fichier journal que vous indiquez.

Pour obtenir une description du processus de restauration, reportez-vous à la section « Présentation du processus de restauration avec Backup eMTool », page 391.

Notez que pour accéder aux options de restauration avancées, vous devez employer le client eMBox, comme expliqué dans la section « Utilisation du client eMBox pour la sauvegarde et la restauration », page 419.

Conditions préalables

- Placez tous les fichiers de sauvegarde dont vous avez besoin pour la restauration dans un répertoire du serveur sur lequel vous effectuez cette opération.

  Reportez-vous aux sections « Préparation d'une restauration », page 406 et « Localisation des fichiers de sauvegarde requis pour une restauration », page 408.

- Vérifiez que eDirectory est déjà installé sur le serveur sur lequel vous effectuez la restauration, et qu'il fonctionne.

Par exemple, si la restauration est nécessaire en raison de la défaillance d'un périphérique de stockage, vous devez réinstaller eDirectory sur le nouveau périphérique. Si vous restaurez un serveur défaillant sur une nouvelle machine, ou transférez simplement un serveur d'une machine à une autre, vous devez installer le système d'exploitation ainsi que eDirectory sur la nouvelle machine.

- Consultez la description du processus de restauration à la section « Présentation du processus de restauration avec Backup eMTool », page 391.
- (NetWare uniquement) Tenez compte des problèmes liés à la préservation des droits du système de fichiers lors de la restauration des données du système de fichiers et de eDirectory. Nous vous conseillons de restaurer eDirectory avant les données du système de fichiers. Vous devrez peut-être effectuer des opérations supplémentaires, comme expliqué dans la section « Préservation des droits lors de la restauration des données du système de fichiers sous NetWare », page 400.

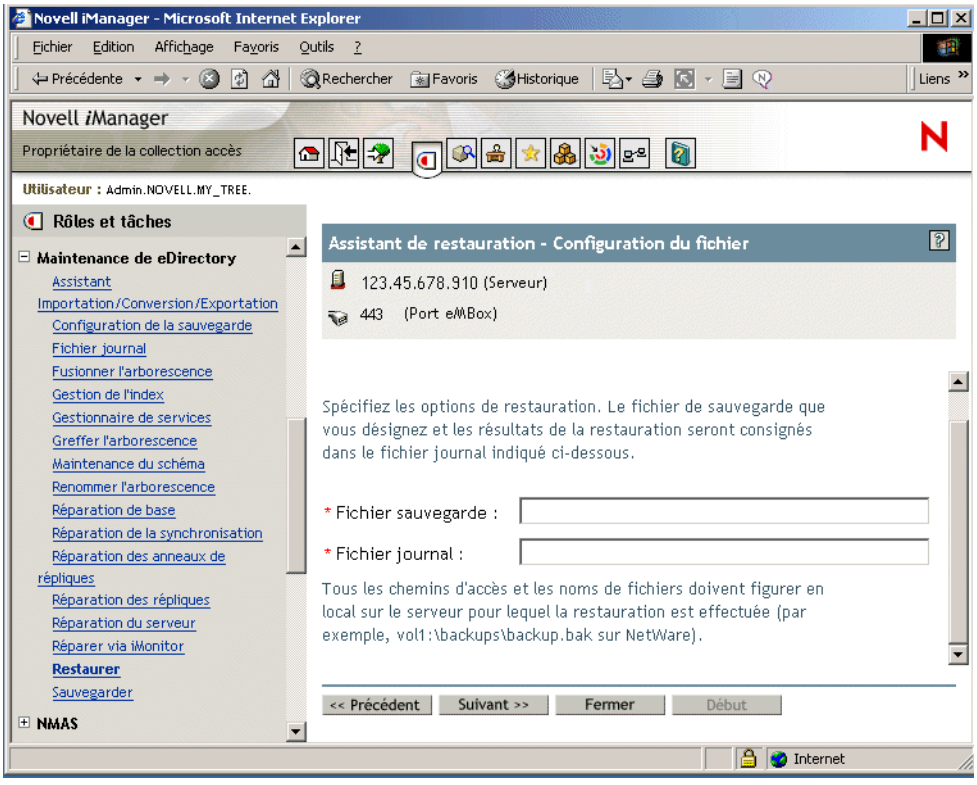
Procédure

SUGGESTION : l'aide en ligne fournit une description des options disponibles dans iManager.

Pour restaurer la base de données eDirectory sur un serveur à l'aide de iManager, procédez comme suit :

1. Vérifiez que vous avez collecté les fichiers de sauvegarde nécessaires, comme expliqué dans la section « Préparation d'une restauration », page 406.
2. Cliquez sur le bouton Rôles et tâches  .
3. Cliquez sur Maintenance de eDirectory > Restaurer.
4. Spécifiez le serveur qui effectuera la restauration, puis cliquez sur Suivant.
5. Entrez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel la restauration sera effectuée, puis cliquez sur Suivant.
6. Indiquez les noms des fichiers de sauvegarde et des fichiers journaux à utiliser, puis cliquez sur Suivant.

   Voici un exemple d'écran.



7 Spécifiez d'autres options de restauration, puis cliquez sur Suivant.

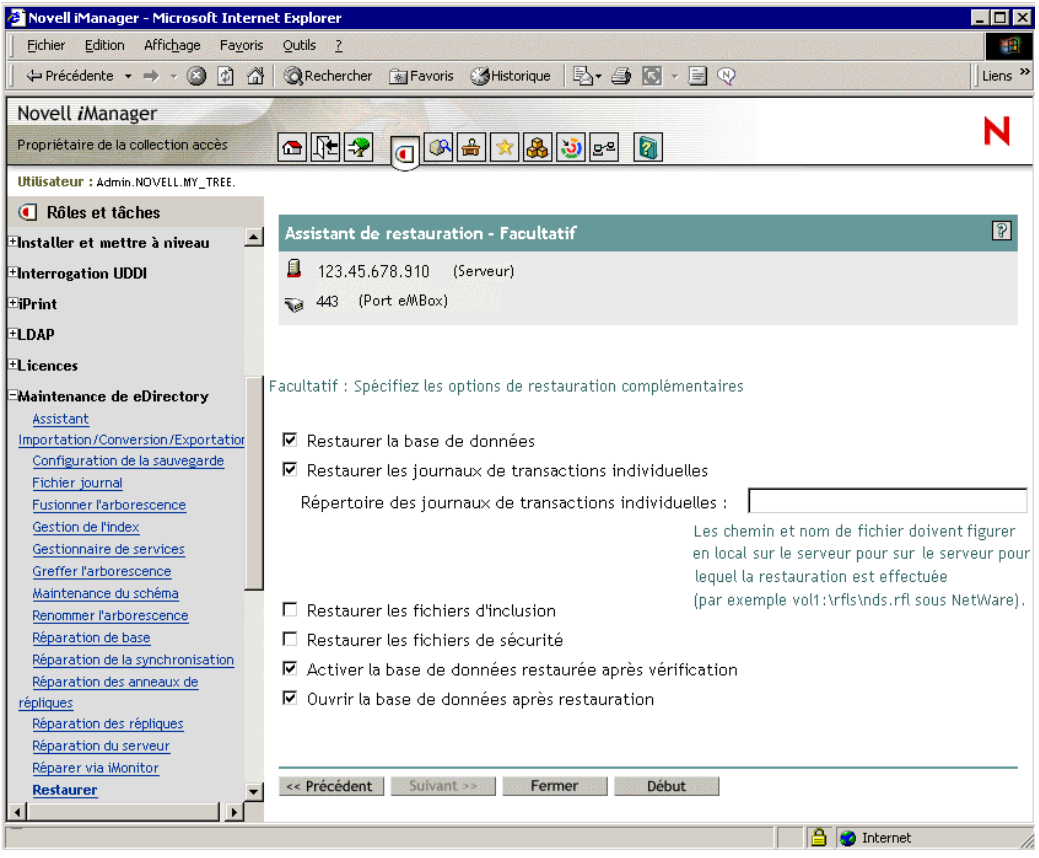
Dans la plupart des cas, vous devez au moins cocher les cases relatives à

- la restauration de la base de données ;
- l'activation de la base de données restaurée après vérification ;
- l'ouverture de la base de données après exécution de la restauration ;
- la restauration des fichiers de sécurité (NICI).

Nous vous recommandons de sauvegarder systématiquement les fichiers NICI afin de pouvoir lire les informations codées après une restauration.

Si vous restaurez des fichiers journaux de transactions individuelles, veillez à inclure leur chemin d'accès complet, y compris le répertoire créé automatiquement par eDirectory, généralement dénommé \nds.rfl. (Pour plus d'informations sur ce répertoire, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles », page 404.)

Voici un exemple d'écran.



8 Suivez les instructions en ligne pour terminer la restauration.

Si la vérification de la restauration échoue, reportez-vous à la section « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442.

REMARQUE : si le serveur que vous restaurez partage une réplique avec un serveur qui exécute une version de eDirectory antérieure à 8.5, le journal de restauration indique l'erreur 666 (version DS incompatible) pour cette réplique. Pour plus d'informations sur cette situation et la façon de procéder, reportez-vous à la section « Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement », page 399.

9 Si vous avez restauré les fichiers de sécurité NICI, redémarrez le serveur pour réinitialiser NICI une fois la restauration terminée.

10 Vérifiez que le serveur fonctionne normalement.

11 (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier sur ce serveur, vous devez recréer la configuration de votre choix afin d'être certain que la fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les fichiers journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Pour plus d'informations sur les fichiers journaux de transactions individuelles et leur emplacement, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

La restauration est à présent terminée et NICI réinitialisé avec les fichiers correspondants restaurés, ce qui vous permet d'accéder aux informations codées. Si vous utilisez la fonction de consignation de transactions individuelles par fichier, vous vous êtes préparé contre toute nouvelle défaillance en réactivant cette fonction à l'issue de la restauration, puis en effectuant une nouvelle sauvegarde complète.

Utilisation du client eMBox pour la sauvegarde et la restauration

Le client eMBox est un client Java à ligne de commande qui donne accès aux outils eMBox tels que eDirectory Backup eMTool. Il vous permet d'effectuer, à partir d'une seule machine, des tâches de sauvegarde, de restauration et de configuration de la consignation de transactions individuelles par fichier pour plusieurs serveurs, si vous disposez d'un accès derrière le pare-feu.

Étant donné que le client eMBox peut être exécuté en mode de traitement par lots,vous pouvez l'utiliser pour effectuer des sauvegardes sans surveillance à l'aide de eDirectory Backup eMTool.

Le fichier eMBoxClient.jar est installé sur votre serveur en tant qu'élément de eDirectory. Vous pouvez également copier ce fichier et l'exécuter sur toute machine équipée de Sun JVM1.3.1. Pour plus d'informations, reportez-vous aux sections et.

Avant d'exécuter des tâches de sauvegarde et de restauration, consultez la « Liste de contrôle pour la sauvegarde de eDirectory », page 384 pour une vue d'ensemble des éléments à considérer lors de la préparation d'une stratégie de sauvegarde efficace pour eDirectory.

Cette section fournit les informations suivantes :

Sauvegarde manuelle à l'aide du client eMBox

Le client eMBox vous permet de sauvegarder les données d'une base de données eDirectory dans un fichier que vous indiquez, sur le serveur sur lequel la sauvegarde est en cours d'exécution. Le fichier de sauvegarde (ou le jeu de fichiers) contient les informations nécessaires pour restaurer eDirectory dans l'état où il se trouvait au moment de la sauvegarde. Les résultats de la sauvegarde sont consignés dans le fichier journal que vous indiquez.

Avant d'exécuter des tâches de sauvegarde et de restauration, consultez la « Liste de contrôle pour la sauvegarde de eDirectory », page 384 pour une vue d'ensemble des éléments à considérer lors de la préparation d'une stratégie de sauvegarde efficace pour eDirectory.

Le client eMbox vous permet d'effectuer un certain nombre de tâches, notamment :

- effectuer une sauvegarde complète ou incrémentielle lorsque la base de données est ouverte (sauvegarde continue à chaud) ;

  Cela signifie que la base de données eDirectory est ouverte et accessible pendant le processus, mais que vous obtenez néanmoins une sauvegarde complète, image fidèle de l'état de la base au début de la sauvegarde.

- effectuer une sauvegarde à froid (la base de données est fermée et une sauvegarde complète est créée) ;

  Cette option est utile lors de la mise à niveau d'une machine, ou du déplacement d'un serveur vers une nouvelle machine équipée du même système d'exploitation (comme expliqué dans la section).

- paramétrer la base de données pour qu'elle reste fermée et verrouillée après une sauvegarde ;
- définir la taille maximale du fichier de sauvegarde.

Pour exécuter ces tâches sans surveillance, reportez-vous à la section « Sauvegardes sans surveillance à l'aide d'un fichier de traitement par lots et du client eMBox », page 422.

Conditions préalables

- ❑ Assurez-vous que le fichier eMBoxClient.jar se trouve sur la machine à partir de laquelle vous souhaitez lancer la sauvegarde.

  Ce fichier est installé sur votre serveur en tant qu'élément de eDirectory. Vous pouvez le copier afin de l'utiliser sur un autre ordinateur équipé de Sun JVM1.3.1. Il vous permet d'effectuer à partir d'une même machine des sauvegardes pour plusieurs serveurs, si vous disposez d'un accès derrière le pare-feu. Pour plus d'informations, reportez-vous à la section.

- ❑ Si vous prévoyez d'utiliser des fichiers journaux de transactions individuelles pour le serveur concerné, veillez à les activer avant d'effectuer une sauvegarde.

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Si vous ne le faites pas, des erreurs se produisent lors de la restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvre pas.

  Pour plus d'informations sur les fichiers journaux de transactions individuelles, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401. Pour savoir comment les activer, reportez-vous à la section « Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox », page 426.

- ❑ Déterminez les autres fichiers à sauvegarder avec eDirectory et créez au besoin un fichier d'inclusion.

  Vous pouvez sauvegarder les fichiers NICI et de flux à l'aide des paramètres appropriés. Nous vous recommandons de sauvegarder systématiquement les fichiers NICI.

  Pour inclure d'autres fichiers, tels que autoexec.ncf, vous devez indiquer leur chemin d'accès complet dans un fichier d'inclusion. Séparez les chemins d'accès par un point-virgule, sans inclure de retour chariot ni d'espace (Par exemple, sys:\system\autoexec.ncf;sys:\etc\hosts;).

- ❑ Prévoyez d'effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory pour enregistrer les fichiers de sauvegarde de eDirectory sur bande. (Backup eMTool les place uniquement sur le serveur.)

SUGGESTION : pour faciliter le transfert des fichiers de sauvegarde sur un autre périphérique de stockage, vous pouvez spécifier la taille maximale de ces fichiers dans la commande de sauvegarde (utilisez l'option s suivie d'un nombre indiquant la taille en octets). Vous pouvez également utiliser un logiciel tiers pour les compresser après leur création. Le taux de compression atteint environ 80%.

- Consultez la description des options de la ligne de commande à la section « Options de ligne de commande pour la sauvegarde et la restauration », page 431.
- Pour les arborescences multiserveurs, nous vous conseillons de mettre à niveau tous les serveurs qui partagent des répliques avec le serveur concerné en installant eDirectory 8.5 ou une version ultérieure.

  Pour plus d'informations, reportez-vous à la section « Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement », page 399.

Procédure

Pour sauvegarder la base de données eDirectory sur un serveur à l'aide du client eMBox, procédez comme suit :

1. Lancez le client eMBox en mode interactif.

   - NetWare et UNIX : dans la ligne de commande, entrez **`edirutil -i`**.
   - Windows : exécutez
     ***`lecteur`*`\novell\nds\edirutil.exe -i`**

   Le fichier edirutil est un raccourci pour l'exécution du client eMBox. Il pointe vers l'exécutable Java et l'emplacement par défaut où le client eMBox est installé avec eDirectory ; pour NetWare, il comprend l'option-ns qui est nécessaire. (Vous pouvez également entrer les informations manuellement, comme expliqué dans la section « Configuration du chemin et du chemin de classe pour le client eMBox », page 555.)

   Lorsque le client eMBox s'ouvre, l'invite correspondante s'affiche : Client eMBox>

2. Loguez-vous au serveur à sauvegarder. Pour ce faire, entrez

   `login -s` ***`nom_serveur_ou_adresse_IP`*** **`-p`** ***`numéro_port`*** **`-u`** ***`nom_utilisateur.contexte`*** **`-w`** ***`mot_de_passe`***

   Par exemple, sous Windows, vous entrez

   `login -s 151.155.111.1 -p 8009 -u admin.ma_société -w mon_mot_de_passe`

   Si un message d'erreur indique qu'il est impossible d'établir une connexion sécurisée, vérifiez si votre machine possède les fichiers JSSE listés à la section « Établissement d'une connexion sécurisée avec le client eMBox », page 561.

   Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory », page 561.

   Le client eMBox indique si le login a réussi.

3. Entrez la commande de sauvegarde à l'invite du client eMBox, en suivant le modèle général ci-dessous :

   backup -b -f *nom_et_chemin_fichier_de_sauvegarde* -l *nom_et_chemin_fichier_journal_sauvegarde* -u *nom_et_chemin_fichier_inclusion* -t -w

   Les paramètres doivent être séparés les uns des autres par un espace. L'ordre des paramètres n'a pas d'importance.

   Par exemple, sous Windows, vous entrez

backup -b -f c:\backups\8_20_2001.bak -l c:\backups\backup.log -u c:\backups\mon_fichier_inclusion.txt -t -w

Cet exemple de commande permet d'effectuer une sauvegarde complète (-b), le fichier de sauvegarde étant enregistré sous c:\ backups\8_20_2001.bak et le fichier journal correspondant sous c:\backups\backup.log. Cette commande indique que d'autres fichiers doivent être sauvegardés avec la base de données :

- les fichiers mentionnés dans un fichier d'inclusion (-u c:\backups\mon_fichier_inclusion.txt), préalablement créé par l'administrateur ;
- les fichiers de flux (-t).

Cet exemple de commande indique que le fichier de sauvegarde doit être remplacé (-w). Par conséquent, si un fichier portant le même nom existe, Backup eMTool le remplace.

Le client eMBox indique si la sauvegarde a réussi.

4. Déloguez-vous du serveur. Pour ce faire, entrez la commande suivante :

   ```
   logout
   ```

5. Quittez le client eMBox en entrant la commande suivante :

   ```
   exit
   ```

6. Veillez à effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory, afin d'enregistrer les fichiers de sauvegarde sur bande par mesure de sécurité. (Backup eMTool les place uniquement sur le serveur.)

Sauvegardes sans surveillance à l'aide d'un fichier de traitement par lots et du client eMBox

Pour exécuter des sauvegardes de eDirectory sans surveillance avec le client eMBox, vous devez utiliser un fichier de traitement par lots. Supposons que vous souhaitiez effectuer une sauvegarde complète de eDirectory toutes les semaines et une sauvegarde incrémentielle toutes les nuits.

Vous pouvez, dans ce cas, exécuter le client eMBox en mode de traitement par lots en utilisant un fichier système, un fichier propre au client eMBox, ou encore une combinaison des deux. Pour plus d'informations, reportez-vous à la section « Exécution du client à ligne de commande eMBox en mode de traitement par lots », page 558.

La procédure ci-dessous met en oeuvre un fichier système de traitement par lots.

Conditions préalables

- ❑ Pour des instructions sur l'exécution de fichiers de traitement par lots sans surveillance, consultez la documentation de votre système d'exploitation ou de votre logiciel de planification tiers.

  REMARQUE : sous NetWare, vous pouvez utiliser un logiciel de planification tiers ou cron.nlm (http://support.novell.com/servlet/tidfinder/2939440), disponible sur le site Web du support Novell.

- ❑ Assurez-vous que le fichier eMBoxClient.jar se trouve sur la machine à partir de laquelle vous souhaitez lancer la sauvegarde.

  Ce fichier est installé sur votre serveur en tant qu'élément de eDirectory. Vous pouvez le copier afin de l'utiliser sur un autre ordinateur équipé de Sun JVM1.3.1. Il vous permet d'effectuer à partir d'une même machine des sauvegardes pour plusieurs serveurs, si vous disposez d'un accès derrière le pare-feu. Pour plus d'informations, reportez-vous à la section « Utilisation du client à ligne de commande eMBox », page 553.

- Si vous prévoyez d'utiliser des fichiers journaux de transactions individuelles pour le serveur concerné, veillez à les activer avant d'effectuer une sauvegarde.

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Si vous ne le faites pas, des erreurs se produisent lors de la restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvre pas.

  Pour plus d'informations sur les fichiers journaux de transactions individuelles, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401. Pour savoir comment les activer, reportez-vous à la section « Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox », page 426.

- Déterminez les autres fichiers à sauvegarder avec eDirectory et créez au besoin un fichier d'inclusion.

  Vous pouvez sauvegarder les fichiers NICI et de flux à l'aide des paramètres appropriés. Nous vous recommandons de sauvegarder systématiquement les fichiers NICI.

  Pour inclure d'autres fichiers, tels que autoexec.ncf, vous devez indiquer leur chemin d'accès complet dans un fichier d'inclusion. Séparez les chemins d'accès par un point-virgule, sans inclure de retour chariot ni d'espace (Par exemple, sys:\system\autoexec.ncf;sys:\etc\hosts;).

- Prévoyez d'effectuer des sauvegardes du système de fichiers peu après avoir sauvegardé eDirectory, afin d'enregistrer les fichiers de sauvegarde de eDirectory sur bande par mesure de sécurité. (Backup eMTool les place uniquement sur le serveur.)

  SUGGESTION : pour faciliter le transfert des fichiers de sauvegarde eDirectory sur un autre périphérique de stockage, vous pouvez spécifier la taille maximale de ces fichiers. Vous pouvez également utiliser un logiciel tiers pour les compresser après leur création. Le taux de compression atteint environ 80%.

- Consultez la description des options de la ligne de commande à la section « Options de ligne de commande pour la sauvegarde et la restauration », page 431.

Procédure

1. Créez un fichier système de traitement par lots pour sauvegarder les serveurs et suivez le modèle général ci-dessous, c'est-à-dire avec une ligne par serveur.

   Voici le modèle général pour Windows et UNIX :

   ```
   java -cp chemin/eMBoxClient.jar embox -s nom_serveur -p numéro_port -u
   nom_utilisateur.contexte -w mot_de_passe -t backup.backup -b -f
   nom_et_chemin_fichier_de_sauvegarde -l
   nom_et_chemin_fichier_journal_sauvegarde -u
   nom_et_chemin_fichier_inclusion -t -w
   ```

   Sous NetWare, vous suivez le même modèle général, auquel s'ajoute `-nsac`, que vous ne devez pas utiliser sur d'autres plates-formes :

   ```
   java -nsac -cp chemin/eMBoxClient.jar embox -s nom_serveur -p numéro_port
   -u nom_utilisateur.contexte -w mot_de_passe -t backup.backup -b -f
   nom_et_chemin_fichier_de_sauvegarde -l
   nom_et_chemin_fichier_journal_sauvegarde -u
   nom_et_chemin_fichier_inclusion -t -w
   ```

   Pour obtenir des exemples et des explications supplémentaires, reportez-vous à la section « Exemples de fichiers système de traitement par lots pour les sauvegardes sans surveillance », page 424.

Pour les sauvegardes incrémentielles effectuées toutes les nuits, vous pouvez utiliser le même fichier que pour les sauvegardes complètes, mais en remplaçant l'option b par i. Vous obtenez ainsi une sauvegarde incrémentielle au lieu d'une sauvegarde complète. Il est également judicieux d'utiliser des noms de fichiers de sauvegarde différents pour les sauvegardes incrémentielles et pour la sauvegarde complète.

Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory », page 561. Si vous voulez utiliser une connexion sécurisée, reportez-vous à la section « Établissement d'une connexion sécurisée avec le client eMBox », page 561. Pour plus d'informations sur l'utilisation d'un fichier de traitement par lots propre au client eMBox, reportez-vous à la section « Exécution du client à ligne de commande eMBox en mode de traitement par lots », page 558.

2. Exécutez les fichiers de traitement par lots sans surveillance, conformément aux instructions de la documentation de votre système d'exploitation ou du logiciel tiers.
3. Prévoyez d'effectuer des sauvegardes du système de fichiers peu après avoir sauvegardé eDirectory, afin d'enregistrer les fichiers de sauvegarde de eDirectory sur bande par mesure de sécurité.

   Backup eMTool les place uniquement sur le serveur.
4. Vérifiez périodiquement les résultats consignés dans le fichier journal que vous avez spécifié, pour vous assurer de la réussite des sauvegardes sans surveillance.

Exemples de fichiers système de traitement par lots pour les sauvegardes sans surveillance

Voici deux exemples :

- « Exemple de fichier de traitement par lots pour NetWare », page 424
- « Exemple de fichier de traitement par lots pour Windows », page 425

Exemple de fichier de traitement par lots pour NetWare

```
java -nsac -cp sys:\system\embox\eMBoxClient.jar embox -s 10.10.1.200 -p 8008
-u admin.mon_conteneur -w mon_mot_de_passe -n -t backup.backup -b -f
sys:\system\backup\backup.bak -l sys:\system\backup\backup.log -u
sys:\system\backup\fichier_inclusion.txt -t -w
```

Les options suivantes figurent dans cet exemple de fichier de traitement par lots.

- Sous NetWare uniquement, ajoutez `-nsac` après la commande java. (N'utilisez pas `-nsac` sur une autre plate-forme).

  AVERTISSEMENT : sur un serveur NetWare uniquement: pour éviter un abend, vous devez ajouter `-ns`.

  L'option -ns ouvre un nouvel écran.

  L'option ac ferme automatiquement l'écran lorsque la tâche du fichier de traitement par lots a été exécutée. Si vous n'introduisez pas cette option dans les fichiers de traitement par lots pour NetWare, un écran reste ouvert sur le serveur chaque fois que le fichier de traitement par lots est exécuté sans surveillance.
- Une sauvegarde complète est demandée (-b).
- Un fichier d'inclusion est désigné (-u). Cette option est facultative. Le fichier d'inclusion vous permet d'introduire dans la sauvegarde d'autres fichiers de votre choix. Il doit avoir été créé auparavant.
- Les fichiers de flux (-t) sont également sauvegardés.

- L'option d'écrasement d'un fichier de sauvegarde du même nom est spécifiée (-w).

  IMPORTANT : si un fichier de sauvegarde portant le même nom existe déjà (ce qui est probable si vous utilisez régulièrement le même fichier de traitement par lots), votre sauvegarde aboutit uniquement si vous employez l'option -w pour remplacer le fichier de sauvegarde existant.

  En mode de traitement par lots, si un fichier du même nom existe et si l'option -w n'est pas spécifiée, le comportement par défaut consiste à ne pas écraser le fichier, ce qui empêche la création d'une sauvegarde. (En mode interactif, si vous n'utilisez pas l'option -w, le client eMBox vous demande si vous souhaitez écraser le fichier.)

  Si vous effectuez une sauvegarde du système de fichiers peu après chaque sauvegarde complète ou incrémentielle de eDirectory, les fichiers de sauvegarde précédents doivent avoir été copiés sur une bande. Vous pouvez donc écraser le fichier de sauvegarde existant sans crainte.

- Comme un port non sécurisé est utilisé dans cet exemple (-p 8008), une connexion non sécurisée est spécifiée (-n).

Exemple de fichier de traitement par lots pour Windows

```
java -cp c:\novell\nds\embox\eMBoxClient.jar embox -s mon_serveur -p 8008 -u
admin.mon_org -w mon_mot_de_passe -n -t backup.backup -b -f
c:\backup\backup.bak -u c:\backup\includes\fichier_inclusion.txt -l
c:\backup\backup.log -e -t -w
```

Les options suivantes figurent dans cet exemple de fichier de traitement par lots.

- Une sauvegarde complète est demandée (-b).
- Un fichier d'inclusion est désigné (-u). Cette option est facultative. Le fichier d'inclusion vous permet d'introduire dans la sauvegarde d'autres fichiers de votre choix. Il doit avoir été créé auparavant.
- Les fichiers de flux (-t) sont également sauvegardés.
- L'option d'écrasement d'un fichier de sauvegarde du même nom est spécifiée (-w).

  IMPORTANT : si un fichier de sauvegarde portant le même nom existe déjà (ce qui est probable si vous utilisez régulièrement le même fichier de traitement par lots), votre sauvegarde aboutit uniquement si vous employez l'option -w pour remplacer le fichier de sauvegarde existant.

  En mode de traitement par lots, si un fichier du même nom existe et si l'option -w n'est pas spécifiée, le comportement par défaut consiste à ne pas écraser le fichier, ce qui empêche la création d'une sauvegarde. (En mode interactif, si vous n'utilisez pas l'option -w, le client eMBox vous demande si vous souhaitez écraser le fichier.)

  Si vous effectuez une sauvegarde du système de fichiers peu après chaque sauvegarde complète ou incrémentielle de eDirectory, les fichiers de sauvegarde précédents doivent avoir été copiés sur une bande. Vous pouvez donc écraser le fichier de sauvegarde existant sans crainte.

- Comme un port non sécurisé est utilisé dans cet exemple (-p 8008), une connexion non sécurisée est spécifiée (-n).

REMARQUE : les options -ns et ac présentées dans les exemples de fichier de traitement par lots pour NetWare doivent être utilisées dans cet environnement uniquement. Ne vous en servez pas sous Windows ou UNIX.

Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox

Le client eMBox vous permet de modifier les paramètres des fichiers journaux de transactions individuelles. Vous pouvez effectuer les tâches suivantes :

- rechercher la configuration actuelle ;
- activer ou désactiver la fonction de consignation de transactions individuelles par fichier ;

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Si vous ne le faites pas, des erreurs se produisent lors de la restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvre pas.
- modifier le répertoire des fichiers journaux de transactions individuelles ;
- définir la taille minimale et maximale des fichiers journaux de transactions individuelles ;
- rechercher le fichier journal de transaction individuelle actuel ainsi que le dernier fichier journal utilisé ;
- activer ou désactiver la consignation des fichiers de flux pour les fichiers journaux de transactions individuelles.

Pour plus d'informations sur la consignation de transactions individuelles par fichier, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

Conditions préalables

- ❑ Assurez-vous que le fichier eMBoxClient.jar se trouve sur la machine à partir de laquelle vous souhaitez modifier la configuration.

  Ce fichier est installé sur votre serveur en tant qu'élément de eDirectory. Vous pouvez le copier afin de l'utiliser sur un autre ordinateur équipé de Sun JVM1.3.1. Il vous permet d'effectuer à partir d'une même machine des sauvegardes pour plusieurs serveurs, si vous disposez d'un accès derrière le pare-feu. Pour plus d'informations, reportez-vous à la section.
- ❑ Consultez la description des options de la ligne de commande à la section « Options de ligne de commande pour la sauvegarde et la restauration », page 431.

Procédure

1. Lancez le client eMBox en mode interactif :
   - NetWare et UNIX: dans la ligne de commande, entrez **`edirutil -i`**.
   - Windows: exécutez ***`lecteur`*`\novell\nds\edirutil.exe -i`**.

   Le fichier edirutil est un raccourci pour l'exécution du client eMBox. Il pointe vers l'exécutable Java et l'emplacement par défaut où le client eMBox est installé avec eDirectory ; pour NetWare, il comprend l'option-ns qui est nécessaire. (Vous pouvez également entrer les options manuellement, comme expliqué dans la section « Exécution du client eMBox sur un poste de travail », page 555.)

   Lorsque le client eMBox s'ouvre, l'invite correspondante s'affiche : Client eMBox>
2. Loguez-vous au serveur sur lequel vous souhaitez configurer la consignation de transactions individuelles par fichier. Pour ce faire, entrez

   `login -s` ***`nom_serveur_ou_adresse_IP`*** **`-p`** ***`numéro_port`*** **`-u`** ***`nom_utilisateur.contexte`*** **`-w`** ***`mot_de_passe`***

Par exemple, sous Windows, vous entrez

```
login -s 151.155.111.1 -p 8009 -u admin.ma_société -w mon_mot_de_passe
```

Si un message d'erreur indique qu'il est impossible d'établir une connexion sécurisée, vérifiez si votre machine possède les fichiers JSSE listés à la section « Établissement d'une connexion sécurisée avec le client eMBox », page 561.

Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory », page 561.

Le client eMBox indique si le login a réussi.

3 (Facultatif) Recherchez la configuration actuelle. Pour ce faire, entrez

```
getconfig
```

Aucun paramètre n'est nécessaire.

Voici un exemple des informations que vous recevez :

```
Roll forward log status OFF
Stream file logging status OFF
Current roll forward log directory vol1:/rfl/nds.rfl
Minimum roll forward log size (bytes) 104857600
Maximum roll forward log size (bytes) 4294705152
Last roll forward log not used 00000000.log
Current roll forward log 00000001.log
*** END ***
```

4 Modifiez les paramètres à l'aide de la commande setconfig et suivez le modèle général ci-dessous :

setconfig [-L|-l] [-T|-t] -r *chemin_fichiers_journaux_transactions_individuelles* -n *taille_minimale_fichier* -m *taille_maximale_fichier*

Les paramètres doivent être séparés les uns des autres par un espace. L'ordre des paramètres n'a pas d'importance.

Par exemple, sous NetWare, vous entrez

setconfig -L -r rflvolume:\logs

Cet exemple active la consignation de transactions individuelles par fichier (paramètre-L) et spécifie que les fichiers journaux sont enregistrés dans rflvolume:\logs. (En principe, vous devriez réserver un volume/une partition de disque à ces fichiers journaux, afin de faciliter le contrôle de l'espace disque et des droits.) L'exemple n'inclut pas l'option d'activation de la consignation des fichiers de flux.

AVERTISSEMENT : si vous activez la consignation de transactions individuelles par fichier, n'utilisez pas l'emplacement par défaut. Pour assurer une tolérance aux pannes, placez le répertoire sur un volume/une partition de disque et un périphérique de stockage différents de ceux de eDirectory. Le répertoire des fichiers journaux de transactions individuelles doit résider sur le serveur sur lequel vous modifiez la configuration de sauvegarde.

IMPORTANT : si vous activez la consignation de transactions individuelles par fichier, vous devez surveiller l'espace disque sur le volume où vous placez les fichiers journaux de transactions individuelles. Si vous ne le surveillez pas, le répertoire des fichiers journaux s'étend jusqu'à saturer le volume/la partition de disque. Si ces fichiers journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Nous vous conseillons de sauvegarder et de supprimer périodiquement du serveur les fichiers journaux de transactions individuelles inutilisés. Pour plus de détails, reportez-vous à la section « Sauvegarde et suppression des fichiers journaux de transactions individuelles », page 405.

5 Déloguez-vous du serveur. Pour ce faire, entrez la commande suivante :

```
logout
```

6 Quittez le client eMBox en entrant la commande suivante :

```
exit
```

Restauration à partir de fichiers de sauvegarde avec le client eMBox

Le client eMBox vous permet de restaurer une base de données eDirectory à partir des données stockées dans les fichiers de sauvegarde que vous avez créés manuellement ou à l'aide d'un fichier de traitement par lots. Les résultats de la restauration sont consignés dans le fichier journal que vous indiquez.

Le client eMBox vous permet en outre d'utiliser des options de restauration avancées qui ne sont pas disponibles dans iManager. Ces options sont présentées à la section « Options de ligne de commande pour la sauvegarde et la restauration », page 431, sous restore et restadv.

Conditions préalables

- Assurez-vous que le fichier eMBoxClient.jar se trouve sur la machine à partir de laquelle vous souhaitez lancer la restauration.

  Ce fichier est installé sur votre serveur en tant qu'élément de eDirectory. Vous pouvez le copier afin de l'utiliser sur un autre ordinateur équipé de Sun JVM1.3.1. Il vous permet d'effectuer à partir d'une même machine des restaurations pour plusieurs serveurs, si vous disposez d'un accès derrière le pare-feu. Pour plus d'informations, reportez-vous à la section.

- Placez tous les fichiers de sauvegarde dont vous avez besoin pour la restauration dans un répertoire du serveur sur lequel vous effectuez cette opération.

  Reportez-vous aux sections « Préparation d'une restauration », page 406 et « Localisation des fichiers de sauvegarde requis pour une restauration », page 408.

- Assurez-vous que eDirectory est installé et en service sur le serveur sur lequel vous effectuez la restauration.

  Par exemple, si la restauration est nécessaire en raison de la défaillance d'un périphérique de stockage, vous devez réinstaller eDirectory sur le nouveau périphérique. Si vous restaurez un serveur défaillant sur une nouvelle machine, ou transférez simplement un serveur d'une machine à une autre, vous devez installer le système d'exploitation ainsi que eDirectory sur la nouvelle machine.

- Consultez la description des options de la ligne de commande à la section « Options de ligne de commande pour la sauvegarde et la restauration », page 431.

- Consultez la description du processus de restauration à la section « Présentation du processus de restauration avec Backup eMTool », page 391.

- (NetWare uniquement) Tenez compte des problèmes liés à la préservation des droits du système de fichiers lors de la restauration des données du système de fichiers et de eDirectory. Nous vous conseillons de restaurer eDirectory avant les données du système de fichiers. Vous devrez peut-être effectuer des opérations supplémentaires, comme expliqué dans la section « Préservation des droits lors de la restauration des données du système de fichiers sous NetWare », page 400.

Procédure

Pour restaurer une base de données eDirectory sur un serveur à l'aide du client eMBox, procédez comme suit :

1. Vérifiez que vous avez collecté les fichiers de sauvegarde nécessaires, comme expliqué dans la section « Préparation d'une restauration », page 406.

2. Lancez le client eMBox en mode interactif :

   - NetWare et UNIX: dans la ligne de commande, entrez **`edirutil -i`**.
   - Windows: exécutez
     ***`lecteur`*`\novell\nds\edirutil.exe -i`**

   Le fichier edirutil est un raccourci pour l'exécution du client eMBox. Il pointe vers l'exécutable Java et l'emplacement par défaut où le client eMBox est installé avec eDirectory ; pour NetWare, il comprend l'option-ns qui est nécessaire. (Vous pouvez également entrer les informations manuellement, comme expliqué dans la section « Exécution du client eMBox sur un poste de travail », page 555.)

   Lorsque le client eMBox s'ouvre, l'invite correspondante s'affiche : <Client eMBox>

3. Loguez-vous au serveur à restaurer. Pour ce faire, entrez

   `login -s `*`nom_serveur_ou_adresse_IP`*` -p `*`numéro_port`*` -u `*`nom_utilisateur.contexte`*` -w `*`mot_de_passe`

   Par exemple, sous Windows, vous entrez

   `login -s 151.155.111.1 -p 8009 -u admin.ma_société -w mon_mot_de_passe`

   Si un message d'erreur indique qu'il est impossible d'établir une connexion sécurisée, vérifiez si votre machine possède les fichiers JSSE listés à la section « Établissement d'une connexion sécurisée avec le client eMBox », page 561.

   Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory », page 561.

   Le client eMBox indique si le login a réussi.

4. Entrez la commande de restauration à l'invite du client eMBox, en suivant le modèle général ci-dessous :

   restore -r -a -o -f *chemin_et_nom_de_fichier_de_sauvegarde_complète* -d *emplacement_fichiers_journaux_transactions_individuelles* -l *chemin_et_nom_de_fichier_journal_de_restauration*

   Les paramètres doivent être séparés les uns des autres par un espace. L'ordre des paramètres n'a pas d'importance. Veillez à utiliser le paramètre -r afin de restaurer la base de données eDirectory proprement dite ; sinon, seuls les autres types de fichiers sont restaurés. Si vous souhaitez qu'à la fin de la restauration, la base de données soit ouverte et active, veillez à spécifier les paramètres -a et -o.

   Si vous restaurez des fichiers journaux de transactions individuelles, veillez à inclure leur chemin d'accès complet, y compris le répertoire créé automatiquement par eDirectory, généralement dénommé \nds.rfl. (Pour plus d'informations sur ce répertoire, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles », page 404.)

   Par exemple :

   restore -r -a -o -f sys:/backup/nds.bak -d vol1:/rfldir/nds.rfl -l sys:/backups/backup.log

Cet exemple de commande indique que la base de données proprement dite doit être restaurée (-r), et qu'elle doit être activée (-a) et ouverte (-o) une fois la vérification de la restauration effectuée correctement. Le paramètre -f indique où se trouve le fichier de sauvegarde complète, le paramètre -d désigne l'emplacement des fichiers journaux de transactions individuelles et le paramètre -l, le fichier journal dans lequel les résultats de la restauration sont consignés.

Le client eMBox restaure la sauvegarde complète, puis vous invite à indiquer les fichiers de sauvegarde incrémentielle.

5. (Conditionnel) Si vous restaurez des fichiers de sauvegarde incrémentielle, indiquez le chemin d'accès et le nom de chaque fichier lorsque le client eMBox vous invite à désigner le fichier incrémentiel suivant.

   Il vous fournit l'ID du fichier suivant, que vous pouvez trouver dans l'en-tête du fichier de sauvegarde incrémentielle.

   Le client eMBox indique si la restauration a réussi.

6. (Conditionnel) Si la restauration échoue, consultez les erreurs dans le fichier journal.

   Si la vérification de la restauration échoue, reportez-vous à la section « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442.

   REMARQUE : si le serveur que vous restaurez partage une réplique avec un serveur qui exécute une version de eDirectory antérieure à 8.5, le journal de restauration indique l'erreur 666 (version DS incompatible) pour cette réplique. Pour plus d'informations sur cette situation et la façon de procéder, reportez-vous à la section « Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement », page 399.

7. Déloguez-vous du serveur. Pour ce faire, entrez la commande suivante :

   ```
   logout
   ```

8. Quittez le client eMBox en entrant la commande suivante :

   ```
   exit
   ```

9. (Conditionnel) Si vous avez restauré les fichiers de sécurité NICI, redémarrez le serveur pour réinitialiser NICI une fois la restauration terminée.

10. Vérifiez que le serveur fonctionne normalement.

11. (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier sur ce serveur, vous devez recréer la configuration de votre choix afin d'être certain que la fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les fichiers journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

    Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

    Pour plus d'informations sur les fichiers journaux de transactions individuelles et leur emplacement, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

La restauration est à présent terminée et NICI réinitialisé avec les fichiers correspondants restaurés, ce qui vous permet d'accéder aux informations codées. Si vous utilisez la fonction de consignation de transactions individuelles par fichier, vous vous êtes préparé contre toute nouvelle

défaillance en réactivant cette fonction à l'issue de la restauration, puis en effectuant une nouvelle sauvegarde complète.

Options de ligne de commande pour la sauvegarde et la restauration

Les options de ligne de commande de eDirectory Backup eMTool sont réparties en six fonctions : backup, restore, restadv, getconfig, setconfig et cancel.

Les paramètres peuvent être introduits dans n'importe quel ordre dans la commande, après le nom de la fonction. Ils doivent cependant être séparés par un espace.

Option et paramètres	Description
backup	**Effectue une sauvegarde de la base de données et des fichiers associés.**
-f *nom_fichier*	(Obligatoire) Nom et chemin d'accès du fichier de sauvegarde Indique le nom et l'emplacement du fichier de sauvegarde que Backup eMTool doit créer. Ce fichier doit figurer sur le serveur que vous sauvegardez. Par exemple, backup -f vol1:\backup\ndsbak.bak sauvegarde la base de données dans vol1:\backup\ndsbak.bak.
-l *nom_fichier*	(Obligatoire) Nom et chemin d'accès du fichier journal Indique le fichier journal dans lequel consigner les résultats de la sauvegarde.
-b	(Facultatif) Effectuer une sauvegarde complète Effectue une sauvegarde complète de la base de données eDirectory. Il s'agit de l'option par défaut. Si vous n'indiquez ni -i ni -c, une sauvegarde complète est effectuée.
-i	(Facultatif) Effectuer une sauvegarde incrémentielle Effectue une sauvegarde incrémentielle de la base de données eDirectory. Toutes les modifications apportées à la base de données depuis la dernière sauvegarde complète ou incrémentielle sont sauvegardées.
-t	(Facultatif) Sauvegarder les fichiers de flux Inclut les fichiers de flux lors de la sauvegarde de la base de données eDirectory.

Option et paramètres	Description
-u *nom_fichier*	(Facultatif) Nom et chemin d'accès du fichier d'inclusion utilisateur Indique un fichier d'inclusion qui contient les fichiers supplémentaires à sauvegarder. Vous pouvez créer ce fichier de configuration afin d'inclure dans la sauvegarde d'autres fichiers importants pour la restauration de la base de données eDirectory du serveur. Dans le fichier d'inclusion, indiquez le chemin d'accès complet de chaque fichier à sauvegarder, suivi d'un point-virgule (;). Par exemple, si, en tant qu'administrateur, vous souhaitez inclure les fichiers autoexec.ncf et hosts dans la sauvegarde pour un serveur NetWare, le fichier d'inclusion utilisateur peut se présenter comme suit : `sys:\system\autoexec.ncf;sys:\etc\hosts;` N'incluez pas d'espace ni de retour chariot dans la liste des fichiers. Pour vous assurer que les fichiers indiqués ont bien été sauvegardés, consultez le fichier journal de sauvegarde ou l'en-tête du fichier de sauvegarde. (Reportez-vous aux sections « Format du fichier journal de sauvegarde », page 396 et « Format de l'en-tête des fichiers de sauvegarde », page 392.) **Avertissement :** lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car il pourrait alors devenir tronqué. La plupart des applications ne peuvent pas enregistrer correctement les données binaires.

Option et paramètres	Description
-s *taille_fichier*	(Facultatif) Taille limite des fichiers de sauvegarde (octets) Indique la taille maximale (en octets) du fichier de sauvegarde. Vous pouvez utiliser cette option si la taille des fichiers risque de poser un problème avec le support servant à enregistrer les fichiers de sauvegarde après leur création. Si la taille maximale est atteinte, un nouveau fichier de sauvegarde est créé avec le même nom, mais une extension de cinq chiffres hexadécimaux est ajoutée pour indiquer de quel fichier il s'agit. Cette extension est incrémentée pour chaque nouveau fichier. Par exemple, vous pouvez fixer la taille maximale des fichiers de sauvegarde à 1 Mo en utilisant les paramètres suivants dans la commande : backup -f vol1:/backup/mydib.bak -s 1000000. Si la taille de la base de données est de 3,5 Mo, vous obtenez le jeu de fichiers de sauvegarde suivant : vol1:/backup/mydib.bak, la taille correspond à 1 Mo vol1:/backup/mydib.bak.00001, la taille correspond à 1 Mo vol1:/backup/mydib.bak.00002, la taille correspond à 1 Mo vol1:/backup/mydib.bak.00003, la taille correspond à 0,5 Mo La taille minimale correspond à 500Ko. Le premier fichier peut être plus volumineux, selon le nombre de fichiers inclus dans la sauvegarde. Il contient, sous l'étiquette backup, un attribut nommé number_of_files (nombre de fichiers). Il s'agit du nombre total de fichiers qui composent le jeu de sauvegarde. Dans l'exemple ci-dessus, ce nombre est4. De plus, l'en-tête de chaque fichier de sauvegarde contient l'attribut backup_file. Il s'agit du nom original du fichier. (Pour plus d'informations, reportez-vous à la section « Format de l'en-tête des fichiers de sauvegarde », page 392.) Pour restaurer un ensemble de fichiers de sauvegarde comme dans l'exemple ci-dessus, la commande est la suivante : restore -f vol1:/backup/mydib.bak -l *chemin_et_nom_du_fichier_journal* Backup eMTool identifie la présence de plusieurs fichiers et les recherche dans le même répertoire que le premier, mais prend en compte les modifications de nom indiquées plus haut. **Suggestion :** en utilisant un logiciel de compression tiers, vous pouvez également réduire considérablement la taille des fichiers de sauvegarde. Le taux de compression atteint environ 80%.

Option et paramètres	Description
-w	(Facultatif) Écraser le fichier de sauvegarde portant le même nom Écrase le fichier de sauvegarde avec le paramètre f si un fichier du même nom existe déjà. Si cette option n'est pas utilisée et qu'un fichier du même nom existe déjà, Backup eMTool vous demande si vous souhaitez écraser ce fichier (en mode interactif). En mode de traitement par lots, si un fichier du même nom existe déjà et si le paramètre -w n'est pas spécifié, le comportement par défaut consiste à ne pas écraser le fichier, ce qui empêche la création d'une sauvegarde. Si vous effectuez une sauvegarde du système de fichiers peu après chaque sauvegarde complète ou incrémentielle de eDirectory, les fichiers de sauvegarde précédents doivent avoir été copiés sur une bande. Vous pouvez donc écraser le fichier de sauvegarde existant sans crainte. **Important :** utilisez cette option dans vos fichiers de traitement par lots pour les sauvegardes sans surveillance. si un fichier de sauvegarde portant le même nom existe déjà (ce qui est probable si vous utilisez régulièrement le même fichier de traitement par lots), votre sauvegarde aboutit uniquement si vous employez l'option -w pour remplacer le fichier de sauvegarde existant. En mode de traitement par lots, si un fichier du même nom existe et si l'option -w n'est pas spécifiée, le comportement par défaut consiste à ne pas écraser le fichier, ce qui empêche la création d'une sauvegarde. (En mode interactif, si vous n'utilisez pas l'option -w, le client eMBox vous demande si vous souhaitez écraser le fichier.)
-c	(Facultatif) Effectuer une sauvegarde à froid Exécute une sauvegarde complète de la base de données fermée. Une fois la sauvegarde terminée, la base de données est rouverte, sauf si les paramètres -o ou -o et -d sont utilisés.
-o	(Facultatif) Laisser la base de données fermée après la sauvegarde à froid Ne peut être utilisé que si le paramètre c est également spécifié. Laisse la base de données fermée après une sauvegarde à froid. Cette option est utile lors de la mise à niveau d'une machine, ou du déplacement d'un serveur vers une nouvelle machine équipée du même système d'exploitation (comme expliqué dans la section).
-d	(Facultatif) Désactiver l'agent DS après la sauvegarde à froid Ne peut être utilisé que si les paramètres -c et -o sont également spécifiés. Désactive l'agent DS après une sauvegarde à froid. Cette option est utile lors de la mise à niveau d'une machine, ou du déplacement d'un serveur vers une nouvelle machine équipée du même système d'exploitation (comme expliqué dans la section). L'utilisation de l'attribut Login désactivé sur le pseudo-serveur permet de désactiver l'agent DS, ce qui entraîne l'erreur -663 au démarrage de eDirectory.
restore	**Effectue une restauration de la base de données et des fichiers associés.**

Option et paramètres	Description
-f *nom_fichier*	(Obligatoire) Nom et chemin d'accès du fichier de sauvegarde Indique la sauvegarde complète à partir de laquelle effectuer la restauration. Le fichier doit se trouver sur le serveur en cours de restauration. Par exemple, restore -f vol1:/backup/ndsbak.bak effectue la restauration à partir du fichier vol1:/backup/ndsbak.bak. Si la sauvegarde est constituée de plusieurs fichiers, tous les fichiers du jeu doivent être copiés dans le même répertoire du serveur.
-l *nom_fichier*	(Obligatoire) Nom et chemin d'accès du fichier journal Indique le fichier journal dans lequel consigner les résultats de la restauration.
-r	(Facultatif) Restaurer l'ensemble DIB Indique que la base de données eDirectory doit être restaurée. **Avertissement :** si cette option n'est pas définie, la base de données eDirectory proprement dite n'est pas restaurée. Seuls les autres types de fichiers spécifiés seront restaurés.
-d *nom_rép*	(Facultatif) Répertoire des fichiers journaux de transactions individuelles Indique le répertoire où sont stockés les fichiers journaux de transactions individuelles. Le chemin d'accès complet doit être indiqué et le répertoire doit se trouver sur le serveur restauré. Tous les fichiers journaux de transactions individuelles doivent se trouver dans le répertoire spécifié et porter le même nom que lors de leur création. Une fois la base de données restaurée, les modifications enregistrées dans ces fichiers journaux sont réappliquées afin de mettre à jour la base de données. Si le paramètre -d n'est pas utilisé, Backup eMTool ne réapplique aucune modification, même si la consignation de transactions individuelles par fichier était activée au moment de la sauvegarde. Pour identifier le premier fichier de transaction individuelle requis, ouvrez dans un éditeur de texte le dernier fichier de sauvegarde restauré et lisez l'attribut current_log de l'étiquette Backup. Le dernier fichier de sauvegarde restauré est le fichier de sauvegarde complète spécifié par l'option -f ou le dernier fichier de sauvegarde incrémentielle qui doit être appliqué pendant la restauration. (Pour plus d'informations sur les attributs listés dans l'en-tête, reportez-vous à la section « Format de l'en-tête des fichiers de sauvegarde », page 392.) **Avertissement :** lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car il pourrait alors devenir tronqué. La plupart des applications ne peuvent pas enregistrer correctement les données binaires.
-u	(Facultatif) Restaurer les fichiers utilisateur Restaure les fichiers utilisateur inclus dans la sauvegarde de la base de données. Dans le cadre de la sauvegarde, vous pouvez créer un fichier texte contenant la liste des fichiers à sauvegarder avec la base de données, et le définir comme fichier d'inclusion utilisateur. Les fichiers concernés ne peuvent être restaurés que s'ils ont été inclus dans la sauvegarde.

Option et paramètres	Description
-a	(Facultatif) Activer DIB après vérification Renomme la base de données RST en NDS une fois la restauration correctement vérifiée. (Pour obtenir une vue d'ensemble du processus, reportez-vous à la section « Présentation du processus de restauration avec Backup eMTool », page 391.)
-o	(Facultatif) Ouvrir la base de données à la fin de l'opération Indique à Backup eMTool d'ouvrir la base de données une fois la restauration achevée. Si la vérification se déroule correctement, la base de données restaurée s'ouvre. Sinon, cette option entraîne l'ouverture de la base de données présente sur le serveur avant la restauration. (Pour obtenir une vue d'ensemble du processus, reportez-vous à la section « Présentation du processus de restauration avec Backup eMTool », page 391.)
-n	(Facultatif) Ne pas vérifier la base de données après la restauration Indique à Backup eMTool de restaurer la base de données sans effectuer de vérification. Le vecteur de transition du serveur n'est pas comparé à celui qu'attendent les autres serveurs de l'anneau de répliques dont il fait partie. (Pour plus d'informations sur les vecteurs de transition, reportez-vous à la section « Vecteurs de transition et processus de vérification de la restauration », page 399). La base de données RST n'est pas renommée en NDS, sauf si une autre option est définie à cet effet. **Important :** nous vous recommandons de ne pas utiliser cette option à moins d'y être invité par le support technique de Novell.
-v	(Facultatif) Remplacer la restauration Renomme la base de données RST en NDS sans tenter de vérification. **Important :** nous vous recommandons de ne pas utiliser cette option à moins d'y être invité par le support technique de Novell.
-k	(Facultatif) Supprimer le verrouillage de la base de données Supprime le verrouillage de la base de données NDS.
restadv	**Options de restauration avancées. (REMARQUE : l'agent DS est fermé pour toutes les options de restauration avancées.)**
-l *nom_fichier*	(Obligatoire) Nom et chemin d'accès du fichier journal Indique le fichier journal dans lequel consigner les résultats de la restauration.
-o	(Facultatif) Ouvrir la base de données à la fin de l'opération Indique à Backup eMTool d'ouvrir la base de données une fois la restauration achevée. Si la vérification se déroule correctement, la base de données restaurée s'ouvre. Sinon, cette option entraîne l'ouverture de la base de données présente sur le serveur avant la restauration. (Pour obtenir une vue d'ensemble du processus, reportez-vous à la section « Présentation du processus de restauration avec Backup eMTool », page 391.)
-n	(Facultatif) Tenter de vérifier une restauration qui a précédemment échoué Tente de vérifier une base de données RST restaurée précédemment.

Option et paramètres	Description
-m	(Facultatif) Supprimer les fichiers DIB restaurés Supprime la base de données RST éventuellement présente.
-v	(Facultatif) Remplacer la restauration Renomme la base de données RST en NDS sans tenter de vérification. **Important :** nous vous recommandons de ne pas utiliser cette option à moins d'y être invité par le support technique de Novell.
-k	(Facultatif) Supprimer le verrouillage de la base de données Supprime le verrouillage de la base de données NDS.
getconfig	**Récupère la configuration actuelle des fichiers journaux de transactions individuelles.**

	Aucune option n'est nécessaire.
	
	Affiche la configuration actuelle. Par exemple, sur un serveur pour lequel la consignation de transactions individuelles par fichier est désactivée, la commande getconfig renvoie des informations semblables aux suivantes :
	
	`Roll forward log status OFF`
	`Stream file logging status OFF`
	`Current roll forward log directory vol1:/rfl/nds.rfl`
	`Minimum roll forward log size (bytes) 104857600`
	`Maximum roll forward log size (bytes) 4294705152`
	`Last roll forward log not used 00000000.log`
	`Current roll forward log 00000001.log`
	`*** END ***`

setconfig	**Définit la configuration des fichiers journaux de transactions individuelles.**
-L	(Facultatif) Début de l'enregistrement des fichiers journaux de transactions individuelles Active la consignation de transactions individuelles par fichier (désactivée par défaut). La consignation continue de transactions individuelles par fichier vous permet de rendre à un serveur l'état qu'il avait avant son arrêt, plutôt que celui de la dernière sauvegarde complète ou incrémentielle. Vous devez activer cette fonction pour les serveurs qui font partie d'un anneau de répliques afin de pouvoir restaurer un serveur dans l'état de synchronisation attendu par les autres serveurs. L'administrateur doit intervenir une fois que la consignation de transactions individuelles par fichier a été activée. Si vous ne les surveillez pas, les fichiers journaux de transactions individuelles s'étendent jusqu'au point de saturer le volume/la partition de disque. Si ces fichiers journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Il est donc nécessaire de sauvegarder et de supprimer périodiquement les fichiers journaux inutilisés. Pour plus de détails, reportez-vous à la section « Sauvegarde et suppression des fichiers journaux de transactions individuelles », page 405. Pour plus d'informations, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

Option et paramètres	Description
-l	(Facultatif) Arrêt de l'enregistrement des fichiers journaux de transactions individuelles Désactive la consignation de transactions individuelles par fichier (désactivée par défaut). La base de données réutilise le fichier journal de transaction individuelle actuel, au lieu d'enregistrer un ensemble de fichiers journaux consécutifs. Si la consignation de transactions individuelles par fichier est désactivée, vous ne pouvez restaurer eDirectory qu'au point de la dernière sauvegarde complète ou incrémentielle. Si elle a été désactivée par mégarde, vous devez la réactiver puis effectuer une nouvelle sauvegarde de la base de données pour pouvoir effectuer une restauration complète. Pour plus d'informations, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.
-T	(Facultatif) Début du chargement des fichiers de flux (Ne s'applique que si la fonction de consignation de transactions individuelles par fichier est activée.) Si un fichier de flux est modifié, il est intégralement copié dans le fichier journal de transaction individuelle. Les fichiers de flux sont des fichiers d'informations supplémentaires liés à la base de données. Les scripts de login en font partie, par exemple. Les fichiers journaux de transactions individuelles occupent l'espace disque plus rapidement lorsque les fichiers de flux sont consignés. Veillez, par conséquent, à contrôler l'espace libre sur le volume/la partition de disque où sont stockés les fichiers journaux de transactions individuelles. Si ces fichiers journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné.
-t	(Facultatif) Arrêt de l'enregistrement des fichiers de flux Arrête la copie du fichier de flux entier dans le fichier journal de transaction individuelle en cas de modification. Si la consignation des fichiers de flux est désactivée, vous pouvez utiliser les options de sauvegarde pour enregistrer ces fichiers lors des sauvegardes complètes et incrémentielles. Cette solution peut être suffisante si vos fichiers de flux changent peu souvent. Si vous désactivez la consignation des fichiers de flux, la taille des fichiers journaux de transactions individuelles augmentera moins rapidement.

Option et paramètres	Description
-r *nom_rép*	(Facultatif) Définition du répertoire du fichier journal de transaction individuelle Modifie le répertoire où sont stockés les fichiers journaux de transactions individuelles. Par exemple, si la commande utilisée est setconfig -r vol2:\rfl, un répertoire est créé sous vol2:\rfl et les fichiers journaux de transactions individuelles y sont enregistrés. Le nom de ce répertoire est défini en fonction du nom de la base de données eDirectory actuelle. Pour les installations standard, il s'agit de « NDS ».Le nom du répertoire résultant est donc vol2:\rfl\nds.rfl\. Si vous renommez la base de données eDirectory NDS en ND1, le répertoire des fichiers journaux de transactions individuelles devient vol2:\rfl\nd1.rfl\. Vous pouvez trouver l'emplacement actuel des fichiers journaux à l'aide de la commande getconfig. Le répertoire est créé immédiatement après le changement d'emplacement, mais aucun fichier journal de transaction individuelle n'est créé tant qu'aucune transaction n'a lieu dans la base de données. **Important :** l'outil de sauvegarde ne permet pas de suivre les changements apportés au répertoire des fichiers journaux de transactions individuelles. Lorsque vous restaurez la base de données, vous devez collecter tous les fichiers journaux de transactions individuelles sur le serveur, dans un même répertoire. Pour plus d'informations, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.
-n *_fichier*	(Facultatif) Définition de la taille minimale du fichier journal de transaction individuelle Définit la taille minimale des fichiers journaux de transactions individuelles (en octets). Lorsque la taille minimale est atteinte, la base de données commence un nouveau fichier journal de transaction individuelle dès que la transaction en cours est terminée.
-m *taille_fichier*	(Facultatif) Définition de la taille maximale du fichier journal de transaction individuelle Définit la taille maximale des fichiers journaux de transactions individuelles (en octets). Si cette limite est atteinte et qu'une transaction est en cours, cette dernière se poursuit dans le fichier suivant. Cette valeur doit toujours être supérieure à la taille minimale.
-s	(Facultatif) Création d'un nouveau fichier journal de transaction individuelle Lance un nouveau fichier journal de transaction individuelle à la fin de la transaction en cours. Le nouveau fichier est créé au début de la transaction suivante.
cancel	**Annule toute opération de sauvegarde ou de restauration en cours. Aucune option n'est nécessaire.**

Utilisation de DSBK.NLM sous NetWare

Dsbk est un analyseur de ligne de commande léger qui effectue les mêmes opérations que l'outil Backup eMTool, mais vous permet de lancer une sauvegarde à partir de la console du serveur sans vous loguer au préalable ni devoir configurer la fonction RBS (voir). Il s'exécute comme un fichier NLM sur le serveur, en utilisant les mêmes options de ligne de commande que l'outil Backup eMTool. Cet utilitaire peut également être utilisé pour créer des scripts de sauvegarde à l'aide de fichiers NCF sur le serveur.

IMPORTANT : Dsbk ne restaurera pas les sauvegardes incrémentielles. Vous ne pouvez l'utiliser que pour restaurer des sauvegardes complètes.

Au terme d'une opération dsbk, les résultats sont écrits dans un fichier (dsbk.err) dont vous pouvez programmer l'ouverture et l'affichage des résultats. Les quatre premiers octets de ce fichier contiennent les éventuels codes d'erreur générés pendant l'opération. En l'absence d'erreurs, ces quatre octets contiennent des zéros.

Pour utiliser dsbk.nlm :

1. Téléchargez et installez eDirectory 8.7.3 IR3 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2969860.htm).
2. Vérifiez que le fichier dsbk.nlm se trouve dans le répertoire sys:\system.

   Dsbk doit se trouver dans le même répertoire que backupcr.nlm, la bibliothèque principale qui contient toutes les fonctionnalités de sauvegarde et de restauration. Cette bibliothèque ne possède pas d'interface utilisateur ; elle est chargée et liée dynamiquement par l'utilitaire dsbk.
3. Sur la console du serveur, exécutez la commande suivante avec l'une des options figurant dans la section « Options de ligne de commande pour la sauvegarde et la restauration », page 431 :

   ```
   load dsbk
   ```

   .

Modifications apportées à la sauvegarde des informations propres au serveur (NetWare uniquement)

Les administrateurs ont mis en place des sauvegardes des informations propres au serveur dans un grand nombre d'installations NetWare. Or, avec l'introduction de eDirectory 8.6, la structure du schéma eDirectory a changé. Des modifications supplémentaires ont été apportées dans eDirectory 8.7. Cependant, les sauvegardes des informations propres au serveur, créées par l'agent TSA du système de fichiers ou un outil de sauvegarde tiers, n'ont pas été prises en charge dans le cadre de ces modifications. Un nouvel outil de sauvegarde «à chaud» a été fourni en remplacement. Il est accessible par Backup eMTool, dans Novell iManager, ou par le client eMBox. La prise en charge de la sauvegarde des informations propres au serveur avec TSA n'était pas disponible à l'époque. Elle l'est aujourd'hui dans eDirectory 8.7.3, avec la fonction de sauvegarde à chaud. Comme dans les versions précédentes, l'agent TSA du système de fichiers appelle dsbacker.nlm pour créer la sauvegarde. Désormais, dsbacker.nlm appelle backupcr.nlm, qui créé une sauvegarde à l'aide de la fonctionnalité Backup eMTool.

Vous pouvez ainsi effectuer des sauvegardes et les restaurer en suivant les recommandations ci-dessous selon les versions de NetWare et de eDirectory utilisées.

Version eDirectory	Version NetWare	Recommandations relatives aux méthodes de sauvegarde/restauration
8.6 ou versions antérieures	Toutes versions	Pour restaurer une sauvegarde des informations propres au serveur (SSI) à l'aide de l'agent TSA du système de fichiers : ◆ Ne supprimez pas le volume ou les objets associés au serveur arrêté. ◆ Contactez le support technique de Novell pour obtenir des instructions détaillées.
8.7	5.1 & 6.0	Effectuez la sauvegarde et la restauration avec Backup eMTool uniquement. (Il est impossible de restaurer les sauvegardes effectuées à l'aide de l'agent TSA du système de fichiers.)
8.7.1 ou versions ultérieures	5.1	Effectuez la sauvegarde et la restauration avec Backup eMTool uniquement. (Il est impossible de restaurer les sauvegardes SSI effectuées à l'aide de l'agent TSA du système de fichiers.)
8.7.1 ou versions ultérieures	6.0 avec SP3 (Requis pour eDirectory 8.7.1)	Vous pouvez utiliser Backup eMTool, l'agent TSA du système de fichiers ou des outils tiers. La restauration s'effectue à l'aide de Backup eMTool.

Voici les principales différences relatives aux informations propres au serveur dans NetWare 6.0 avec eDirectory 8.7.1 :

- **Le fichier de sauvegarde est plus volumineux :** avec la méthode précédente, la sauvegarde SSI ne contenait qu'une infime partie de la base de données. Désormais, étant donné que le fichier de sauvegarde contient toutes les informations relatives à tous les objets d'annuaire du serveur, il est beaucoup plus volumineux. Il a approximativement la même taille que la base de données.
- **L'emplacement d'un fichier est défini par l'utilisateur :** dans les versions antérieures des sauvegardes des informations propres au serveur, un seul fichier, servedata.nds, était créé dans le répertoire système sys:. Comme le fichier était plus petit, l'emplacement des données avant leur copie sur bande n'avait pas d'importance. Avec eDirectory 8.7.3, vous pouvez utiliser l'agent TSA du système de fichiers pour créer des sauvegardes complètes de la base de données. Trois fichiers sont impliqués. L'emplacement de l'un d'eux, ssiback.bak, est défini par l'utilisateur.

Fichier	Description	Emplacement
ssiback.bak	Ce fichier de sauvegarde est identique à la « sauvegarde à chaud » complète créée avec Backup eMTool. Pour plus de détails, reportez-vous à la section « À propos de l'outil eDirectory Backup eMTool », page 387.	Défini par l'utilisateur. L'emplacement par défaut est sys:system. Étant donné la taille du fichier, nous vous conseillons de le transférer sur un volume autre que sys:.
ssiback.ini	Fichier texte contenant le chemin d'accès au fichier ssiback.bak. L'emplacement par défaut du fichier de sauvegarde est sys:system. Par exemple : vol1:/backups/ssibackup.bak.	sys:\system
ssiback.log	Fichier journal contenant des informations sur les sauvegardes précédentes. Le fichier journal contient un historique de toutes les sauvegardes et consigne l'heure de début et de fin de chacune d'entre elles. Il fournit également des informations sur les erreurs survenues éventuellement pendant le processus de sauvegarde.	sys:\system

- **Restauration avec Backup eMTool :** les informations propres au serveur ne peuvent être restaurées qu'avec Backup eMTool.

Récupération de la base de données en cas d'échec de la vérification de la restauration

Le processus de restauration comprend une étape de vérification qui consiste à comparer la base de données eDirectory sur le serveur en cours de restauration et celles des autres serveurs de l'anneau de répliques, par rapprochement des vecteurs de transition. (Pour plus d'informations sur le processus de restauration, reportez-vous aux sections « Présentation du processus de restauration avec Backup eMTool », page 391 et « Vecteurs de transition et processus de vérification de la restauration », page 399.)

Si les vecteurs de transition ne correspondent pas, la vérification échoue. Il faut généralement en déduire qu'il manque des données dans les fichiers utilisés pour la restauration. Les raisons peuvent notamment être les suivantes :

- Vous n'avez pas activé la consignation de transactions individuelles par fichier avant d'effectuer la dernière sauvegarde.
- Vous n'avez pas introduit les fichiers journaux de transactions individuelles dans l'opération de restauration.
- Le jeu de fichiers journaux de transactions individuelles fourni pour la restauration est incomplet.

REMARQUE : la vérification de la restauration peut également échouer si l'anneau de répliques comprend un serveur qui exécute une version de eDirectory antérieure à 8.5. Pour plus d'informations sur cette situation et la façon de procéder, reportez-vous à la section « Rétrocompatibilité du processus de vérification de la restauration avec eDirectory 8.5 et versions ultérieures uniquement », page 399.

Par défaut, la base de données eDirectory restaurée n'est pas ouverte à l'issue de la restauration si elle est incohérente par rapport aux autres répliques.

Si vous possédez tous les fichiers de sauvegarde et tous les fichiers journaux de transactions individuelles nécessaires à une restauration complète, mais avez oublié de les fournir pendant le processus, vous pouvez vous contenter d'exécuter de nouveau la restauration avec l'ensemble complet de fichiers. Si la restauration est complète lors du second essai, la vérification réussit et la base de données restaurée s'ouvre.

Si vous ne possédez pas tous les fichiers de sauvegarde et fichiers journaux de transactions individuelles nécessaires pour effectuer une restauration complète et garantir la réussite de la vérification, vous devez suivre les instructions de cette section pour restaurer le serveur. Voici un récapitulatif des éléments récupérables en cas d'échec de la vérification :

- Vous pouvez toujours récupérer l'identité du serveur et les droits du système de fichiers.
- Vous ne pouvez pas récupérer les répliques qui figuraient sur le serveur à partir de la sauvegarde, mais vous pouvez utiliser ce dernier pour ces répliques après avoir exécuté la procédure de récupération présentée ici. Vous devez enlever le serveur de l'anneau de répliques et utiliser les options de restauration avancées ainsi que l'outil DSRepair pour remettre le serveur dans un état qui permette sa réintégration dans l'anneau de répliques. Vous pouvez ensuite réinstaller les répliques de votre choix.
- Néanmoins, si le serveur détenait l'unique copie d'une partition de la base de données (absence d'autres répliques), celle-ci ne peut pas être récupérée.

Si la vérification a échoué, suivez les instructions ci-dessous pour rétablir l'identité du serveur et les droits du système de fichiers, ainsi que pour enlever le serveur de l'anneau de répliques et l'y réintégrer. Une fois cette procédure exécutée et la réplication terminée, le serveur doit fonctionner comme avant la défaillance (exception faite des partitions qui n'étaient pas répliquées et qui ne peuvent donc pas être rétablies).

Reportez-vous d'abord à la section « Nettoyage de l'anneau de répliques », page 443. Consultez ensuite la section « Réparation du serveur défaillant et réinstallation des répliques », page 445.

Nettoyage de l'anneau de répliques

Cette procédure explique comment effectuer les tâches suivantes :

- **Réassigner des répliques maîtresses.** Si le serveur défaillant contient la réplique maîtresse d'une partition, utilisez DSRepair pour désigner une nouvelle réplique maîtresse sur un autre serveur de la liste des répliques.
- **Supprimer de la liste des répliques les références au serveur défaillant.** Tous les serveurs faisant partie des anneaux de répliques qui incluaient le serveur défaillant doivent être informés de l'indisponibilité de ce dernier.

Conditions préalables

- ❑ eDirectory est installé sur la machine sur laquelle vous tentez de restaurer le serveur défaillant.
- ❑ Une restauration a été tentée, mais la vérification a échoué.

- ❑ La base de données NDS est ouverte et en service, et la base de données RST se trouve toujours sur la machine (elle y a été laissée par le processus de restauration).
- ❑ Vous savez quelles partitions répliquées ont été stockées sur le serveur défaillant. Les répliques que contenait le serveur sont listées dans l'en-tête du fichier de sauvegarde.

Procédure

Pour nettoyer l'anneau de répliques :

1. Depuis la console de l'un des serveurs qui partageaient une réplique avec le serveur défaillant, chargez DSRepair avec le paramètre permettant d'accéder aux options avancées.
   - NetWare et Windows : utilisez le paramètre -a.
   - UNIX : utilisez le paramètre -Ad.

   Pour plus d'informations sur l'exécution de DSRepair avec le paramètre -a ou -Ad, reportez-vous à la section « Options DSRepair avancées », page 280.

   AVERTISSEMENT : si vous utilisez DSRepair avec le paramètre -a ou -Ad, certaines des options avancées peuvent endommager votre arborescence. Pour plus d'informations sur ces options, consultez le site Web du support Novell, Solution 2938493 (http://support.novell.com/servlet/tidfinder/2938493).
2. Sélectionnez Opérations de partition et de réplique.
3. Sélectionnez la partition à modifier, afin de pouvoir enlever le serveur défaillant de l'anneau de répliques pour cette partition.
4. Sélectionnez Afficher l'anneau de répliques pour afficher la liste des serveurs disposant de répliques de la partition.
5. (Conditionnel) Si le serveur défaillant contenait la réplique maîtresse, choisissez un autre serveur pour cette réplique en sélectionnant Désigner ce serveur en tant que nouvelle réplique maîtresse.

   L'anneau de répliques comporte désormais une nouvelle réplique maîtresse. Toutes les répliques faisant partie de l'anneau sont informées de son existence.
6. Patientez pendant la mise en place de la réplique maîtresse. Avant de poursuivre, vérifiez que les autres serveurs de l'anneau ont bien enregistré le changement.
7. Revenez à Afficher l'anneau de répliques. Sélectionnez le nom du serveur défaillant, puis Enlever ce serveur de l'anneau de répliques.

   Si vous n'avez pas chargé DSRepair avec le paramètre -a ou -Ad (selon la plate-forme) pour accéder aux options avancées, cette option ne figure pas dans la liste.

   AVERTISSEMENT : veillez à ne pas effectuer cette opération si le serveur défaillant est désigné comme réplique maîtresse. Cette information est indiquée dans la liste des serveurs de l'anneau. S'il s'agit de la réplique maîtresse, désignez un autre serveur en tant que maître, comme expliqué à l'Etape 5. Revenez ensuite à cette étape et enlevez le serveur défaillant de l'anneau de répliques.
8. Loguez-vous en tant qu'utilisateur Admin.
9. Après avoir lu le message d'explication, indiquez que vous souhaitez poursuivre.
10. Quittez DSRepair.

    Tous les serveurs qui font partie de l'anneau de répliques sont notifiés.
11. Répétez cette procédure sur un serveur pour chaque anneau de répliques dont le serveur défaillant faisait partie.

Pour finir de préparer le serveur défaillant en vue de charger de nouvelles copies des répliques, poursuivez avec la procédure ci-dessous, « Réparation du serveur défaillant et réinstallation des répliques », page 445.

Réparation du serveur défaillant et réinstallation des répliques

Cette procédure vous permet de changer en références externes les informations relatives aux répliques qui figurent sur le serveur, de sorte que celui-ci ne se considère plus comme faisant partie de l'anneau de répliques. Une fois que vous avez appliqué cette méthode pour enlever les répliques du serveur, vous pouvez déverrouiller la base de données.

Après avoir retiré les répliques, vous terminez la procédure en les réinstallant sur le serveur. Celui-ci reçoit ainsi une nouvelle copie actualisée de chaque réplique. Après la réinstallation de chaque réplique, le serveur doit fonctionner de la même façon qu'avant la défaillance.

Pour enlever les répliques à l'aide de DSRepair, puis les réinstaller à l'aide de la fonction de réplication :

1. Assurez-vous d'avoir terminé la procédure « Nettoyage de l'anneau de répliques », page 443.
2. Remplacez la restauration sur le serveur en utilisant l'option de restauration avancée appropriée du client eMBox.

   2a Lancez le client eMBox en mode interactif :

   - NetWare et UNIX : dans la ligne de commande, entrez **`edirutil -i`**.
   - Windows : exécutez **`lecteur\novell\nds\edirutil.exe -i`**

   Le fichier edirutil est un raccourci pour l'exécution du client eMBox. Il pointe vers l'exécutable Java et l'emplacement par défaut où le client eMBox est installé avec eDirectory ; pour NetWare, il comprend l'option-ns qui est nécessaire. (Vous pouvez également entrer les informations manuellement, comme expliqué dans la section « Exécution du client eMBox sur un poste de travail », page 555.)

   Lorsque le client eMBox s'ouvre, l'invite correspondante s'affiche : Client eMBox>

   2b Loguez-vous au serveur à restaurer. Pour ce faire, entrez

   `login -s nom_serveur_ou_adresse_IP -p numéro_port -u nom_utilisateur.contexte -w mot_de_passe`

   Par exemple, sous Windows, vous entrez

   ```
   login -s 151.155.111.1 -p 8008 -u admin.ma_société -w
     mon_mot_de_passe
   ```

   Si un message d'erreur affiche qu'il est impossible d'établir une connexion sécurisée, vérifiez si votre machine possède les fichiers JSSE mentionnés dans la section « Établissement d'une connexion sécurisée avec le client eMBox », page 561.

   Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory », page 561.

   Le client eMBox indique si le login a réussi.

   2c Utilisez l'option de restauration avancée permettant de remplacer la restauration et précisez un nom de fichier journal :

   `restadv -v -l nomfichierjournal`

   Cette option de restauration avancée renomme la base de données RST (la base de données qui a été restaurée, mais dont la vérification a échoué) en NDS, mais la laisse verrouillée.

3 Depuis la console du serveur, changez en références externes toutes les informations relatives aux répliques figurant sur le serveur, à l'aide des options avancées de DSRepair.

- NetWare : entrez **`dsrepair -XK2 -rd`**
- Windows : Cliquez sur Démarrer > Paramètres > Panneau de configuration > Services Novell eDirectory. Sélectionnez dsrepair.dlm. Dans le champ Paramètres de démarrage, tapez **`-XK2 -rd`**. Cliquez sur Démarrer.
- UNIX : entrez **`ndsrepair -R -Ad -xk2`**

Le paramètre -rd ou R permet de réparer la base de données locale et la réplique.

AVERTISSEMENT : l'utilisation incorrecte des options avancées de DSREPAIR risque d'endommager votre arborescence. Pour plus d'informations sur ces options, consultez le site Web du support Novell, Solution 2938493 (http://support.novell.com/servlet/tidfinder/2938493).

4 Lorsque la réparation est terminée, supprimez le verrouillage et ouvrez la base de données à l'aide des options de restauration avancées suivantes du client eMBox :

`restadv -o -k -l` ***`nomfichierjournal`***

Le paramètre -o permet d'ouvrir la base de données et le paramètre -k de supprimer le verrouillage.

5 Utilisez iManager pour réintroduire le serveur dans l'anneau de répliques :

5a Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .

5b Cliquez sur Partition et répliques > Affichage des répliques.

5c Spécifiez le nom et le contexte de la partition à répliquer, puis cliquez sur OK.

5d Cliquez sur Ajouter une réplique.

5e En regard du champ Nom du serveur, cliquez sur le bouton Parcourir  , puis sélectionnez le serveur que vous venez de restaurer.

5f Sélectionnez le type de réplique désiré, cliquez sur OK puis sur Terminé.

5g Répétez cette procédure pour chaque anneau de répliques dont le serveur faisait partie.

6 Attendez la fin du processus de réplication.

Le processus de réplication est terminé lorsque les répliques passent de l'état Nouveau à Actif. Vous pouvez vérifier l'état dans iManager. Pour plus d'informations, reportez-vous à la section « Affichage des informations sur une réplique », page 144.

7 Si vous avez restauré les fichiers de sécurité NICI, redémarrez le serveur pour réinitialiser NICI une fois la restauration et la réplication terminées.

8 (Conditionnel) Si vous souhaitez utiliser la consignation de transactions individuelles par fichier sur le serveur, vous devez recréer votre configuration afin de vous assurer que cette fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les fichiers journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Pour plus d'informations sur les fichiers journaux de transactions individuelles et leur emplacement, reportez-vous à la section « Utilisation des fichiers journaux de transactions individuelles », page 401.

Scénarios de sauvegarde et de restauration

Scénario : perte d'un disque dur contenant eDirectory dans un réseau monoserveur

Ingrid est l'administrateur d'un réseau monoserveur chez Stationery Supply, Inc. Elle ne peut pas recourir à la réplication pour la tolérance aux pannes, car son environnement ne comporte qu'un seul serveur. La nouvelle fonctionnalité Backup eMTool de eDirectory 8.7.3 offre à Ingrid une solution simple pour sauvegarder et restaurer eDirectory. Cette solution est centrée sur le serveuret, qui plus est, rapide.

Après avoir mis à niveau son serveur WindowsNT en passant de eDirectory 8.6.2 à eDirectory 8.7.3, Ingrid configure des sauvegardes sans surveillance pour ce serveur, à l'aide de fichiers de traitement par lots qui exécutent Backup eMTool.

Ingrid souhaite effectuer une sauvegarde complète de eDirectory chaque dimanche soir, et une sauvegarde incrémentielle chaque nuit, en semaine. Elle configure les sauvegardes sans surveillance pour qu'elles s'exécutent chaque nuit, peu avant ses sauvegardes complètes et incrémentielles du système de fichiers. Ainsi, les sauvegardes sur bande contiennent les fichiers de sauvegarde de eDirectory en même temps que ceux du système de fichiers. Elle a passé un contrat avec une société de stockage de données à distance afin d'envoyer les sauvegardes sur bande hors site.

Tous les lundis matin, Ingrid vérifie le journal de sauvegarde pour s'assurer de la réussite de la sauvegarde. Pendant la semaine, elle contrôle occasionnellement les fichiers journaux pour vérifier que les sauvegardes incrémentielles ont abouti.

Ingrid décide de ne pas activer les fichiers journaux de transactions individuelles pour les raisons suivantes :

- Comme elle ne possède pas de périphérique de stockage distinct sur son serveur, l'activation des fichiers journaux de transactions individuelles ne lui permet pas d'effectuer des sauvegardes supplémentaires de eDirectory. Une défaillance du périphérique de stockage entraînerait la perte des fichiers journaux en même temps que celle de eDirectory. Créer des journaux ne présente donc aucun intérêt.
- L'arborescence ne change pas beaucoup. Ingrid se contente de pouvoir la restaurer dans l'état qu'elle avait lors de la sauvegarde de la dernière nuit. Elle n'a pas besoin de pouvoir restaurer eDirectory dans l'état où il se trouvait avant la défaillance.
- Étant donné que le serveur ne fait pas partie d'un anneau de répliques comprenant d'autres serveurs, les fichiers journaux de transactions individuelles ne sont pas nécessaires à la réussite du processus de vérification de la restauration.

Stationery Supply, Inc. décide de réorganiser les ressources humaines. Ingrid fait donc une sauvegarde manuelle avant d'apporter des changements importants à l'arborescence et après les avoir appliqués. Sa stratégie consiste à faire une nouvelle sauvegarde des changements un jour de la semaine, lorsque cela s'avérera nécessaire, au lieu d'exécuter en permanence des fichiers journaux de transactions individuelles.

Pour s'assurer que sa stratégie de sauvegarde sera prête à fonctionner lorsqu'elle en aura besoin, Ingrid la teste de temps à autre. Comme elle ne dispose pas du budget requis pour acquérir un second serveur afin d'effectuer les tests, elle passe un accord avec un laboratoire de test local. Sur un serveur du laboratoire comparable au sien, elle installe son système d'exploitation et son système de fichiers pour obtenir un environnement proche de celui de sa base de données eDirectory. Elle restaure ses sauvegardes et vérifie que la restauration de eDirectory correspond à ses attentes.

Un mercredi matin, le disque dur qui contient eDirectory sur le serveur tombe en panne. Ingrid se procure un nouveau disque dur et réunit les fichiers de la sauvegarde complète du dimanche soir, de la sauvegarde incrémentielle du lundi soir et de celle du mardi soir. Elle met en place le nouveau disque dur et installe eDirectory sur ce dernier. Elle restaure ensuite les sauvegardes complète et incrémentielles. Les modifications apportées à l'arborescence le mercredi matin, avant la défaillance du disque dur, sont perdues puisque Ingrid n'effectuait pas de consignation de transactions individuelles par fichier sur le serveur. Toutefois, le fait de pouvoir effectuer la restauration jusqu'à la sauvegarde de la dernière nuit seulement convient à Ingrid ; pour elle, l'exécution de fichiers journaux de transactions individuelles, compte tenu de la surcharge administrative que cela représenterait, ne présente pas d'intérêt.

Scénario : perte d'un disque dur contenant eDirectory dans un environnement multiserveur

Chez Outdoor Recreation, Inc., Georges dispose de dix serveurs qui exécutent eDirectory. Il effectue des sauvegardes complètes chaque dimanche soir et des sauvegardes incrémentielles toutes les nuits. La sauvegarde de eDirectory a lieu peu avant la sauvegarde sur bande du système de fichiers.

Tous les serveurs font partie d'anneaux de répliques. Georges utilise la consignation de transactions individuelles par fichier sur chacun d'eux. Pour chaque serveur, il a placé les fichiers journaux de transactions individuelles sur un périphérique de stockage différent de celui de eDirectory. Il surveille l'espace disponible afin de s'assurer que les fichiers journaux de transactions individuelles ne le saturent pas. Il contrôle en outre les droits sur le périphérique de stockage. De temps à autre, il sauvegarde sur bande les fichiers journaux de transactions individuelles, puis les supprime tous, à l'exception de celui utilisé par eDirectory, afin de libérer de l'espace.

Pour Georges, la surcharge administrative liée à la mise en oeuvre de la consignation continue de transactions individuelles par fichier est compensée par le fait qu'il dispose d'une sauvegarde jusqu'à la dernière minute, ce qui est nécessaire pour des serveurs faisant partie d'anneaux de répliques. S'il doit restaurer un serveur, celui-ci retrouve l'état de synchronisation qu'attendent les autres serveurs de l'anneau de répliques.

Dans son laboratoire de test, Georges teste périodiquement les fichiers de sauvegarde pour s'assurer que sa stratégie de sauvegarde répond à ses objectifs.

Un jeudi à 14heures, le serveur Linux Stocks_DB1 subit une défaillance de disque dur, sur l'unité qui contient eDirectory.

Georges doit se procurer la dernière sauvegarde complète et les sauvegardes incrémentielles effectuées depuis celle-ci. Il peut ainsi restaurer la base de données dans l'état où elle se trouvait avant la sauvegarde incrémentielle réalisée la nuit précédente à une heure du matin. Les fichiers journaux de transactions individuelles ayant enregistré les modifications apportées à la base depuis la sauvegarde de la dernière nuit, Georges les introduit dans la restauration. Il peut ainsi rétablir la base dans l'état où elle se trouvait juste avant la défaillance du disque dur.

Georges procède de la façon suivante :

1. Il se procure un disque dur de rechange pour le serveur.
2. Il récupère la bande de la sauvegarde complète du serveur, effectuée le dimanche précédent.

   Le fichier de traitement par lots qu'il utilise pour effectuer des sauvegardes complètes chaque dimanche soir place le fichier de sauvegarde dans /adminfiles/backup/backupfull.bk.

   Comme il avait spécifié une taille limite de 200Mo dans les paramètres de configuration de la sauvegarde, il y a deux fichiers de sauvegarde :

   backupfull.bk.00001 (250 Mo)
   backupfull.bk.00002 (32 Mo)
3. Il se procure également les bandes qui contiennent les sauvegardes incrémentielles de lundi, mardi et mercredi soir.

   Le fichier de traitement par lots qu'il utilise pour effectuer des sauvegardes incrémentielles tous les soirs en semaine place le fichier de sauvegarde dans /adminfiles/backup/backupincr.bk.

   Étant donné qu'il exécute le même fichier de traitement par lots chaque soir de la semaine pour les sauvegardes incrémentielles de eDirectory, celles-ci ont toutes le même nom de fichier. Il doit leur assigner un nouveau nom lorsqu'il les recopie sur le serveur car elles doivent toutes être placées dans le même répertoire pendant la restauration.
4. Georges installe le disque dur de remplacement.

   Comme le système d'exploitation du serveur n'était pas sur le disque dur défaillant, il n'a pas besoin d'installer Linux.
5. Georges restaure le système de fichiers depuis la sauvegarde sur bande, pour les partitions de disque affectées.
6. Il réinstalle eDirectory et place le serveur dans une nouvelle arborescence temporaire (le processus de restauration le replace dans l'arborescence d'origine par la suite).
7. Georges crée le répertoire /adminfiles/restore sur le serveur, pour y stocker les fichiers à restaurer.
8. Il copie les deux fichiers de sauvegarde complète dans ce répertoire.
9. Ensuite, il y copie les sauvegardes incrémentielles de lundi, mardi et mercredi soirs.

   Elles se nomment toutes backupincr.bk. Par conséquent, lorsqu'il les copie dans le répertoire, il doit modifier les noms de fichiers en

   backupincr.lun.bk
   backupincr.mar.bk
   backupincr.mer.bk

   REMARQUE : les sauvegardes complètes et incrémentielles ne doivent pas toutes se trouver dans un même répertoire. Cependant, toutes les sauvegardes incrémentielles doivent être placées dans le même répertoire.

10. Il utilise iManager pour restaurer eDirectory :

    a. Il ouvre iManager et clique sur Utilitaires de maintenance eDirectory > Restaurer.

    b. Il se connecte au serveur, en utilisant le contexte de la nouvelle arborescence temporaire.

    c. Dans l'écran Assistant de restauration- Configuration du fichier, il effectue les opérations suivantes :

       Il entre /adminfiles/restore comme emplacement des fichiers de sauvegarde.

       Il entre /adminfiles/restore/restore.log pour l'emplacement du journal de restauration.

    d. Dans l'écran Assistant de restauration- Facultatif, il effectue les opérations suivantes :

       Il coche Restaurer la base de données.

       Il coche aussi Restaurer les fichiers journaux de transactions individuelles.

       Il entre l'emplacement des fichiers journaux de transactions individuelles.

       (Il s'agit de l'emplacement distinct qu'il a créé spécifiquement pour stocker les fichiers journaux de transactions individuelles. Comme il les a placés sur un disque dur différent de celui de eDirectory, la panne qui s'est produite ne les a pas affectés et ils sont toujours disponibles.)

       Il coche Restaurer les fichiers de sécurité.

       Il coche Activer la base de données restaurée après vérification.

       Il coche Ouvrir la base de données après restauration.

       Il souhaite que eDirectory s'ouvre si la vérification de la restauration réussit.

11. Il lance la restauration et entre les noms des fichiers de sauvegarde incrémentielle lorsqu'il y est invité.

12. La vérification de la restauration réussit, de sorte que la base de données s'ouvre avec l'arborescence originale.

    Elle a réussi parce que les fichiers journaux de transactions individuelles étaient en service sur le serveur lors de la défaillance du disque dur, et que Georges les a inclus dans la restauration.

13. Une fois la restauration terminée, Georges recrée la configuration des fichiers journaux de transactions individuelles sur le serveur. Il effectue ensuite une nouvelle sauvegarde complète.

    Comme les paramètres reprennent leur valeur par défaut durant une restauration, la consignation de transactions individuelles par fichier est désactivée. Il doit la réactiver. Il doit, en outre, effectuer une nouvelle sauvegarde complète afin de se prémunir contre toute défaillance survenant avant la prochaine sauvegarde complète sans surveillance.

Georges vérifie le fonctionnement du serveur. Celui-ci semble être normal.

Scénario : perte d'un serveur complet dans un environnement multiserveur

Bruno est l'administrateur de 15 serveurs chez GK Designs Company. Il effectue des sauvegardes complètes chaque samedi soir et des sauvegardes incrémentielles toutes les nuits. La sauvegarde de eDirectory a lieu peu avant la sauvegarde sur bande du système de fichiers.

Tous les serveurs font partie d'anneaux de répliques. Bruno utilise la consignation de transactions individuelles par fichier sur chacun d'eux.

Un incendie d'origine électrique détruit l'un des serveurs d'une succursale située de l'autre côté de la ville. Heureusement, toutes les partitions de ce serveur, sauf une, sont répliquées sur d'autres serveurs. Bruno avait activé les fichiers journaux de transactions individuelles sur ce serveur, mais ils ont été perdus avec toutes les autres données. Il ne peut donc pas restaurer la base de données eDirectory du serveur dans l'état où elle se trouvait juste avant que ce dernier tombe en panne.

Il peut cependant recréer l'identité eDirectory du serveur en le restaurant à partir des fichiers de sauvegarde existants. Étant donné que Bruno ne peut pas inclure les fichiers journaux de transactions individuelles dans la restauration, le serveur ne correspond pas à l'état de synchronisation attendu par les autres serveurs (voir « Vecteurs de transition et processus de vérification de la restauration », page 399). Par conséquent, le processus de vérification de la restauration échoue. Cela signifie que, par défaut, la base de données eDirectory n'est pas ouverte après la restauration.

Pour résoudre ce problème, Bruno enlève le serveur des anneaux de répliques en utilisant DSRepair pour changer en références externes toutes les informations périmées relatives aux répliques qui figurent sur le serveur. Ensuite, il ajoute une nouvelle copie de chaque partition du serveur en effectuant une réplication à partir des autres serveurs contenant les répliques à jour. (Ces opérations sont décrites dans la section « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442.)

La seule partition du serveur que Bruno n'avait pas répliquée était un conteneur dans lequel figuraient des objets Impression en réseau de la succursale, tels qu'une imprimante/fax et une imprimante couleur grand format. Les informations de cette partition ne peuvent pas être récupérées avec la méthode indiquée ci-dessus, puisque aucun autre serveur n'en possède de réplique. Bruno doit donc recréer les objets de la partition. Cette fois, il choisit de les répliquer sur d'autres serveurs pour assurer, à l'avenir, une meilleure tolérance aux pannes.

Bruno recrée également la configuration des fichiers journaux de transactions individuelles après la remise en ligne du serveur (car la restauration désactive la fonction de consignation et rétablit les paramètres par défaut), puis il crée une nouvelle sauvegarde complète qui servira de point de départ.

Scénario : perte de plusieurs serveurs dans un environnement multiserveur

Julien administre 20 serveurs sur trois sites. Sur l'un de ces sites, la rupture d'une canalisation d'eau détruit cinq des huit serveurs.

Julien dispose de sauvegardes de eDirectory pour tous les serveurs. Toutefois, ceux-ci font partie d'anneaux de répliques. Le problème est de les réinstaller dans l'arborescence sans fichiers journaux de transactions individuelles, puisque ces derniers ont aussi été perdus. Il ne sait pas sur quels serveurs il doit restaurer eDirectory d'abord, ni comment gérer les incohérences entre les répliques. En raison de la complexité de ces problèmes, il appelle le support technique de Novell afin d'être conseillé sur le choix de la méthode de restauration.

Scénario : perte de tous les serveurs dans un environnement multiserveur

Dolorès et son équipe de Human Resources Consulting, Inc. gèrent 50 serveurs sur un site.

Pour assurer la tolérance aux pannes dans les conditions normales d'exploitation, ils ont créé trois répliques de chaque partition de leur arborescence. Si un serveur est arrêté, les objets des partitions qu'il contient restent ainsi disponibles sur d'autres serveurs. Ils ont également prévu la récupération de serveurs individuels en sauvegardant régulièrement tous leurs serveurs avec Backup eMTool, en activant la consignation de transactions individuelles par fichier et en stockant les bandes de sauvegarde sur un site distant.

Dans le cadre d'un plan de reprise après sinistre, Dolorès et son équipe ont également désigné deux de leurs serveurs comme serveurs DSMASTER. Deux serveurs sont nécessaires en raison de la taille de l'arborescence. Un seul serveur DSMASTER ne suffit pas à accueillir les répliques de toutes les partitions. Chaque partition de l'arborescence est répliquée sur l'un des deux serveurs DSMASTER. Les deux serveurs DSMASTER ne contiennent aucune réplique de la même partition, de sorte qu'il n'y a pas de chevauchement entre eux. Il s'agit là d'un aspect important de leur plan de reprise après sinistre.

Dans leur laboratoire de test, Dolorès et son équipe testent périodiquement les sauvegardes afin de s'assurer que la stratégie de sauvegarde répond à leurs objectifs.

Une nuit, le bâtiment abritant Human Resources Consulting, Inc. est endommagé par un ouragan, et tous les serveurs de l'infocentre sont détruits.

À la suite de ce sinistre, Dolorès et son équipe commencent par restaurer les deux serveurs DSMASTER, qui contiennent les répliques de toutes les partitions. Ils utilisent la dernière sauvegarde complète et les sauvegardes incrémentielles consécutives, mais ils ne peuvent pas inclure les fichiers journaux de transactions individuelles dans la restauration du fait qu'ils ont été perdus lors de la destruction des serveurs. Dolorès et son équipe ont structuré les serveurs DSMASTER afin qu'ils ne partagent pas de répliques. De ce fait, le processus de vérification de la restauration réussit sur les deux serveurs, même si les fichiers journaux de transactions individuelles ne sont pas inclus dans la restauration. Une fois les deux serveurs DSMASTER restaurés, tous les objets de l'arborescence de Human Resources Consulting, Inc. sont à nouveau disponibles.

Les serveurs DSMASTER sont importants, car Dolorès et son équipe peuvent les utiliser pour recréer une arborescence sans incohérences à la suite d'un sinistre.

Ils utilisaient des fichiers journaux de transactions individuelles afin de pouvoir restaurer un serveur dans l'état où il se trouvait avant son arrêt et rétablir l'état de synchronisation attendu par les autres serveurs de l'anneau de répliques. Le serveur pouvait ainsi reprendre les communications là où elles avaient été interrompues et recevoir des autres répliques les mises à jour nécessaires à la synchronisation de l'ensemble de l'anneau.

Dans le cas du présent sinistre, cependant, Dolorès et son équipe ne disposent pas des fichiers journaux de transactions individuelles. En leur absence, seul un serveur peut être restauré sans erreurs dans un anneau de répliques,à savoir le premier. Pour les autres serveurs, la vérification de la restauration échoue parce que les états de synchronisation ne correspondent pas à ce qui est attendu (voir « Vecteurs de transition et processus de vérification de la restauration », page 399). Si la vérification de la restauration échoue, le processus de restauration n'active pas la base de données eDirectory restaurée.

Dolorès et son équipe ont prévu cette situation et se sont organisés en conséquence. Ils utilisent comme point de départ les deux serveurs DSMASTER et ne disposent donc que d'une réplique de chaque partition. Il est possible de restaurer ces serveurs sans erreurs, et les répliques qu'ils contiennent peuvent servir de répliques maîtresses qui seront copiées sur tous les autres serveurs.

Après la restauration des serveurs DSMASTER, la restauration des autres serveurs nécessite quelques opérations supplémentaires. Dolorès et son équipe doivent restaurer chacun des serveurs restants en procédant comme suit :

- Ils vérifient que les répliques placées sur les serveurs DSMASTER sont désignées comme répliques maîtresses.
- Ils enlèvent tous les serveurs des anneaux de répliques, à l'exception des serveurs DSMASTER.

- Ils restaurent les sauvegardes complètes et incrémentielles pour chacun des autres serveurs.

  Dolorès et son équipe savent que le processus de vérification de la restauration va échouer pour le reste des serveurs parce qu'ils n'ont pas pu utiliser les fichiers journaux de transactions individuelles durant leur restauration. Ils obtiennent donc une base de données restaurée mais non activée.

- Ils activent la base de données restaurée, à l'aide des options de restauration avancées, mais la maintiennent verrouillée.

- Ils utilisent DSREPAIR pour modifier en références externes toutes les informations sur les répliques.

- Ils déverrouillent la base de données restaurée.

  À ce stade, le serveur a la même identité qu'auparavant, mais il ne tente pas de synchroniser les informations de réplique. Il est toutefois prêt à recevoir une nouvelle copie des répliques qu'il contenait précédemment.

  Pour les serveurs NetWare, Dolorès et son équipe s'assurent que la restauration du système de fichiers intervient une fois eDirectory restauré.

- Ils réinstallent les répliques sur chacun des serveurs en les dupliquant à partir de la copie qui figure sur le serveur DSMASTER.

  Dolorès et son équipe savent assez précisément quelles répliques étaient détenues par chaque serveur, mais ils peuvent consulter l'en-tête des fichiers de sauvegarde de chacun d'eux pour voir la liste des répliques qu'ils contenaient au moment de la dernière sauvegarde.

- Ils recréent la configuration des fichiers journaux de transactions individuelles après la remise en ligne des serveurs (puisque la restauration désactive la fonction de consignation et rétablit les paramètres par défaut), puis effectuent une nouvelle sauvegarde complète qui servira de base pour faire face aux défaillances susceptibles de survenir avant la prochaine sauvegarde complète sans surveillance.

(Ces étapes sont décrites plus en détail dans la section « Récupération de la base de données en cas d'échec de la vérification de la restauration », page 442.)

Dolorès et son équipe ont beaucoup de travail en vue, mais ils peuvent remettre l'arborescence en service assez rapidement et peuvent s'attendre à récupérer l'identité eDirectory de tous leurs serveurs.

Sauvegarde et restauration de NICI

L'infrastructure cryptographique internationale de Novell (NICI) stocke des clés et des données utilisateur dans le système de fichiers et dans les répertoires et fichiers spécifiques au système et à l'utilisateur. Pour protéger ces fichiers et répertoires, ils sont associés aux autorisations adéquates à l'aide du mécanisme fourni par le système d'exploitation. Cette opération est effectuée par le programme d'installation de NICI.

Désinstaller NICI du système ne supprime pas les fichiers et répertoires utilisateur ou système. Par conséquent, la seule raison justifiant la restauration de ces fichiers à un état antérieur est la récupération après une panne système catastrophique ou une erreur humaine. Il importe de comprendre que le fait d'écraser un ensemble existant de fichiers et de répertoires utilisateur NICI risque d'interrompre une application existante.

La sauvegarde et la restauration de NICI exige deux opérations :

1. la sauvegarde et la restauration des fichiers et répertoires ;
2. la sauvegarde et la restauration des droits d'utilisateur spécifiques sur ces fichiers et répertoires.

L'ordre exact des événements requis dépend de la plate-forme que vous utilisez.

Il est primordial pour la sauvegarde et la restauration de maintenir des autorisations exactes sur les fichiers et répertoires. Le fonctionnement de NICI et la sécurité ainsi fournie dépendent de la définition correcte de ces autorisations.

Les logiciels de sauvegarde classiques disponibles dans le commerce devraient préserver les autorisations sur le système NICI et les fichiers et répertoires utilisateur. Vérifiez si votre logiciel de sauvegarde effectue l'opération avant de réaliser une sauvegarde personnalisée de NICI.

Veillez bien à sauvegarder la structure de répertoires NICI existante et, le cas échéant, son contenu avant d'effectuer une restauration. La perte de la clé machine est irréparable. Étant donné qu'elle permet de coder les clés et données utilisateur, son égarement entraîne une perte permanente des données utilisateur.

La restauration de NICI uniquement exige une certaine connaissance de votre part afin de déterminer les fichiers à restaurer. Pendant la restauration, il importe de restaurer les droits d'accès exacts correspondant au propriétaire. Sur les systèmes UNIX et Windows, le nom du répertoire spécifique à l'utilisateur reflète l'ID du propriétaire, mais sur ces deux systèmes, l'ID du propriétaire peut changer entre le moment de la sauvegarde et celui de la restauration. Pour des raisons de sécurité, l'opérateur doit savoir quel compte est en cours de restauration et déterminer si les droits d'accès et le nom du répertoire sont assignés en conséquence. La simple existence sur le système d'un compte utilisateur possédant le même ID que celui sauvegardé ne signifie pas que le compte actuel est le véritable propriétaire des informations restaurées.

Pour plus d'informations, consultez les documents TID10098087, How to Backup NICI 2.7.x and 2.6.x (Procédure de sauvegarde de NICI 2.7.x et 2.6.x) (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098087.htm) et TID10096647, How to Backup the eDirectory Database and Associated Security Services Files (Procédure de sauvegarde de la base de données eDirectory et des fichiers de services de sécurité associés) (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10096647.htm) dans la base de connaissances Novell.

UNIX

Dans NICI 2.6.5 et versions antérieures, le répertoire /var/novell/nici contient tous les fichiers et répertoires utilisateur et système. Dans NICI 2.7.0 et versions ultérieures, /var/novell/nici est un lien symbolique vers le répertoire /var/opt/novell/nici qui contient les fichiers.

Pour identifier la version de NICI que vous utilisez, consultez le fichier /etc/nici.cfg.

Réalisation d'une sauvegarde

Les répertoires et fichiers suivants doivent être sauvegardés. Veillez à préserver les droits sur tous les fichiers et répertoires.

Pour les versions de NICI antérieures à 2.7.0

Nom du fichier/répertoire	Type de fichier et instructions spéciales
/etc/nici.cfg	Fichier de configuration.
/usr/lib/libccs2.so	Lien symbolique vers la bibliothèque proprement dite dans /usr/lib/.
/usr/lib/libccs2.so.*	Bibliothèque NICI (le nom est complété par la version de la bibliothèque).
/var/novell/nici	Ce répertoire contient toutes les clés système, les répertoires et fichiers/clés utilisateur, ainsi que les programmes utilisés pour initialiser NICI.

Pour les versions NICI 2.7.0 et ultérieures

Nom du fichier/répertoire	Type de fichier et instructions spéciales
/etc/nici.cfg	Lien symbolique vers le fichier de configuration /etc/opt/novell/nici.cfg.
/etc/opt/novell/nici.cfg	Fichier de configuration.
/usr/lib/libccs2.so	Lien symbolique vers la bibliothèque proprement dite dans /opt/novell/lib/.
/opt/novell/lib/libccs2.so.*	Bibliothèque NICI (le nom est complété par la version de la bibliothèque).
/var/novell/nici	Lien symbolique vers le répertoire /var/opt/novell/nici.
/var/opt/novell/nici	Ce répertoire contient toutes les clés système, les répertoires et fichiers/clés utilisateur, ainsi que les programmes utilisés pour initialiser NICI.

Restauration de NICI

Pour restaurer les fichiers de configuration NICI, vérifiez d'abord que NICI est déjà installé sur la machine en recherchant le lien ou le fichier /etc/nici.cfg.

1. Si NICI est déjà installé sur le système, sauvegardez la configuration existante comme expliqué ci-dessus.
2. Désinstallez NICI et supprimez la structure de répertoires /var/novell/nici ou /var/opt/novell/nici.

   Cette opération permet de vérifier que les clés système existantes ne sont pas en conflit avec l'ensemble restauré.
3. Restaurez toute la structure de la zone de stockage de sauvegarde (selon la version de NICI), en n'oubliant pas de restaurer les droits d'accès.

Nous vous recommandons de respecter la procédure ci-dessus, mais un opérateur averti peut choisir de restaurer des fichiers ou répertoires spécifiques, en changeant éventuellement les noms des fichiers ou des répertoires et en assignant de nouveaux droits d'accès. Cette opération est possible si les fichiers nicifk et xmgrcfg.wks sont identiques à ceux de la zone de stockage de sauvegarde.

Les recommandations suivantes pour chaque fichier/répertoire s'appliquent à la restauration lors d'une installation NICI existante :

Nom du fichier	Procédure
xmgrcfg.nif	Peut être restauré sur un fichier existant.
xarchive.000	Peut être restauré sur un fichier existant.
Répertoires et fichiers spécifiques à l'utilisateur	Veillez à ce que l'ID utilisateur dans la sauvegarde soit identique à celui sur la machine. Si le répertoire utilisateur existe déjà, déterminez si l'utilisateur souhaite conserver les fichiers actuels ou les restaurer dans un état antérieur. Normalement, les fichiers de configuration utilisateur doivent être restaurés en groupe et non individuellement. Veillez à restaurer les fichiers utilisateur avec l'ID approprié et à restaurer les droits sur le répertoire utilisateur et son contenu. Par exemple, si Bruno avait l'ID utilisateur 1000 au moment de la sauvegarde et a désormais l'ID 5000, les fichiers du répertoire sauvegardé 1000 doivent être restaurés dans le répertoire 5000, ou il convient de rendre à Bruno son ancien ID (1000). Le processus de restauration ne doit pas être une restauration aveugle des répertoires utilisateur, il nécessite une intervention de l'opérateur. Dans tous les cas, le répertoire utilisateur NICI existant doit être sauvegardé.

NetWare

Avant NICI 2.*x*, les fichiers de configuration étaient conservés dans le répertoire sys:_NetWare et différentes procédures s'appliquaient. Ces instructions ne concernent que les versions NICI 2.*x* ou ultérieures.

Réalisation d'une sauvegarde

Sauvegardez le répertoire sys:\system\NICI, les éventuels sous-répertoires ainsi que les droits d'accès. Étant donné que sous NetWare, il n'existe qu'un seul utilisateur, la complication liée à la sauvegarde et la restauration des répertoires utilisateur comme sous UNIX et Windows n'existe pas.

Restauration de NICI

Si NICI n'est pas installé, restaurez le répertoire sys:\system\NICI et son contenu.

S'il est installé (comme l'indique la présence du fichier sys:\system\NICI\nici.cfg), sauvegardez la configuration existante et supprimez NICI. Copiez toute la structure de sauvegarde de la zone de stockage de sauvegarde en vue de la restauration.

Une restauration sélective n'est possible que si le fichier nicifk est resté identique à celui de la zone de stockage de sauvegarde. S'il n'a pas changé, restaurez les fichiers souhaités dans le répertoire sys:\system\NICI. Généralement, les fichiers doivent être restaurés en groupe, mais un opérateur averti peut choisir de ne restaurer que certains fichiers ou sous-répertoires.

Windows

Les informations de configuration sont stockées dans le registre système sous la clé suivante :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NICI.
```

Une deuxième clé identifie la version de NICI actuellement installée. Par exemple :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NICI (Shared) U.S./Worldwide (128 bit)
```

Réalisation d'une sauvegarde

1. Sauvegardez les informations de registre sous HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NICI*

   NICI* indique toutes les clés de registre qui commencent par NICI. Il peut y en avoir plusieurs.

2. Sauvegardez le répertoire, y compris les sous-répertoires, identifiés par HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NICI\ConfigDirectory.

   Comme pour les systèmes UNIX, n'oubliez pas les droits d'accès sur ce répertoire et tous les sous-répertoires. Pour plus d'informations, reportez-vous à la section « Réalisation d'une sauvegarde », page 454.

Si un logiciel disponible dans le commerce est utilisé pour la sauvegarde, assurez-vous que le programme de sauvegarde proprement dit s'exécute comme un processus système et qu'il peut donc accéder à tous les répertoires et sous-répertoires.

Restauration de NICI

1. Si NICI n'est pas installé, restaurez d'abord toutes les informations de registre.

   ou

   s'il est installé, supprimez NICI et écrasez les informations de registre de la zone de stockage de sauvegarde.

2. Restaurez les fichiers et répertoires dans HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NICI\ConfigDirectory conformément à la sélection de l'opérateur.

Comme pour UNIX, nous recommandons de restaurer tous les fichiers en groupe. Un opérateur avisé peut toutefois choisir de restaurer des entrées spécifiques. Cette opération n'est possible que si les fichiers nicifk et xmgrcfg.wks sont identiques à ceux de la zone de stockage de sauvegarde. Dans ce cas, veillez à configurer les droits d'accès en fonction du nouveau propriétaire des répertoires de configuration de l'utilisateur. Les répertoires spécifiques portent le nom de leur propriétaire, mais les droits d'accès sont contrôlés par l'identificateur de sécurité (SID). Le simple fait qu'un sous-répertoire soit nommé Bruno n'implique pas automatiquement que l'utilisateur actuel, en l'occurrence Bruno, soit le propriétaire des informations restaurées.

Cas particulier pour Windows

Il est possible de configurer la valeur de registre HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NICI\UserDirectoryRoot pour indiquer que les fichiers de configuration utilisateur doivent être stockés dans le répertoire de configuration personnel de l'utilisateur. Dans ce cas, soyez prêt à sauvegarder et restaurer les informations utilisateur indépendamment dans le cadre d'opérations normales de sauvegarde et de restauration.

Si NICI a été configuré de cette manière, vous devez en être informé et être prêt à réaliser des sauvegardes spécifiques.

Pour profiter de cette possibilité pour le répertoire utilisateur de Windows, créez la valeur de registre EnableUserProfileDirectory au lieu de pointer simplement en direction du chemin du répertoire. Si Windows est configuré pour créer et supprimer automatiquement des comptes utilisateur, il se peut que le répertoire soit automatiquement supprimé à l'activation du répertoire du profil utilisateur. Dans ce cas, la sauvegarde et la restauration ne sont nécessaires que pour les utilisateurs spécifiques permanents. Le chemin par défaut sera la branche du répertoire Application Data\Novell\Nici du répertoire de l'utilisateur dans Mes documents et paramètres.

15 Prise en charge du protocole SNMP pour Novell eDirectory

Le protocole SNMP (Simple Network Management Protocol) correspond au protocole Internet standard d'exploitation et de maintenance. Il permet l'échange de données de gestion entre les applications de console de gestion et les périphériques qu'elles gèrent. Les applications de console de gestion sont des applications telles que HP* Openview, Novell® NMS, IBM* NetView ou Sun* Net Manager. Les périphériques gérés comprennent les hôtes, les routeurs, les passerelles et les hubs ainsi que des applications réseau telles que Novell eDirectory™.

Cette section décrit les services SNMP pour Novell eDirectory 8.8. Elle contient les rubriques suivantes :

SNMP: définitions et terminologie

Le tableau suivant contient la terminologie employée dans ce chapitre.

Terminologie	Définition
EMANATE	EMANATE (Enhanced Management Agent Through Extensions) est un produit de SNMP Research International, Inc.
SNMP	Simple Network Management Protocol. Protocole utilisé pour l'échange de données sur l'activité du réseau.
NAA	Native Agent Adapter (Adaptateur d'agent natif)
NMS	Network Management Station (Station d'administration réseau)
MA	Management Agent (Agent de gestion)
SA	Sous-agent
MIB	Management Information Base (Base d'informations de gestion)
NCP™	NetWare® Core Protocol™ (Protocole NCP)
NMA	Network Management Application (Application de gestion réseau)

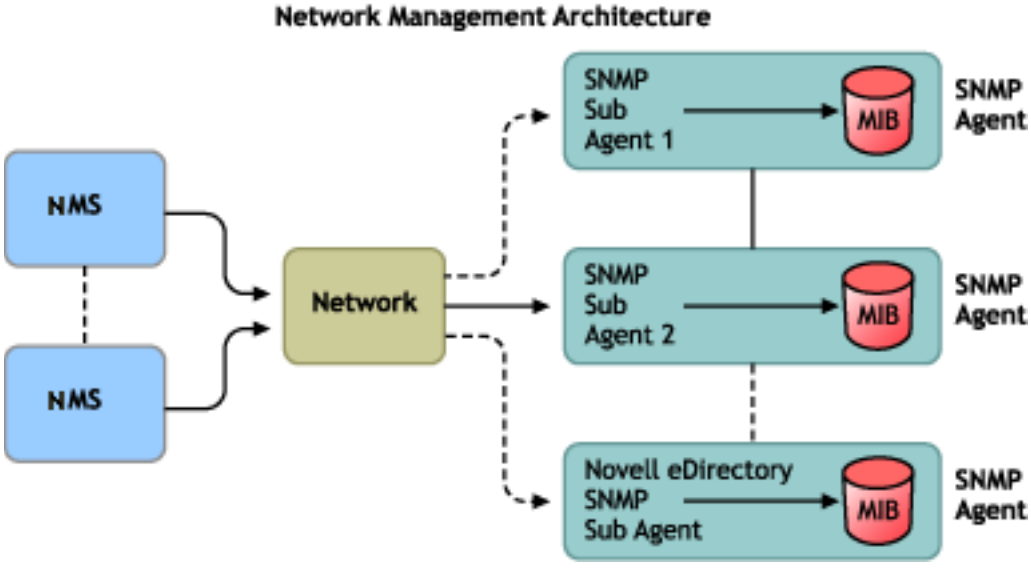
Terminologie	Définition
edir.mib	MIB de surveillance du serveur Novell eDirectory qui contient les trappes et objets MIB appropriés pour Novell eDirectory.
Trappes	Alertes générées par des agents sur un périphérique géré lorsque des événements eDirectory se produisent sur le serveur. Ces conditions sont définies dans la MIB (base d'informations de gestion) fournie par Novell.

Présentation des services SNMP

SNMP repose sur une architecture gestionnaire/agent. L'architecture de gestion réseau SNMP comprend les éléments suivants :

- Station d'administration réseau (NMS)
- Périphérique géré
- Agent principal
- Sous-agent
- Base d'informations de gestion (MIB)
- Protocole de gestion réseau

Figure 48 Architecture de gestion réseau



Station de gestion réseau

Une station de gestion réseau est un poste de travail qui comporte une ou plusieurs applications de gestion réseau installées permettant d'afficher en mode graphique des informations sur les périphériques gérés.

Fonctions NMS :

- Elle fournit l'interface utilisateur à l'ensemble du système de gestion réseau et offre ainsi un outil de gestion réseau puissant, souple et simple à utiliser.

- Elle permet d'exécuter les opérations SNMP Get, Get Next, Get Response et Set. La station de gestion réseau permet également de capturer les trappes SNMP envoyées sur le réseau par les périphériques gérés.
- Elle surveille une ou plusieurs applications de gestion réseau (NMA) simultanément et affiche en mode graphique des informations sur les périphériques gérés, les tables et la consignation.
- Elle permet de compiler le fichier MIB à l'aide du compilateur MIB disponible dans la NMS.

Périphériques gérés

Un périphérique géré est un périphérique sur lequel est installé SNMP. Il peut s'agir d'un hôte, d'un routeur, d'une passerelle, d'un hub, etc. La NMS les surveille et communique avec eux.

Les informations circulant entre la NMS et le périphérique géré sont transférées via deux types d'agent: le sous-agent et l'agent principal.

Sous-agent

Le sous-agent collecte les informations relatives au périphérique géré et les transmet à l'agent principal.

Agent principal

L'agent principal prend en charge l'échange d'informations entre les différents sous-agents et la NMS. Il est exécuté sur la même machine hôte que les sous-agents avec lesquels il communique.

Base d'informations de gestion

SNMP permet d'échanger des informations sur le réseau sous forme de PDU (Protocol Data Units). Les PDU contiennent des informations sur les variables stockées sur le périphérique géré. Ces variables, appelées objets gérés, possèdent des valeurs et des intitulés qui sont renvoyés à la NMS. Tous les objets gérés sont définis dans la base d'informations de gestion. La MIB est une base de données virtuelle de type arborescence.

Protocole de gestion réseau SNMP

Le tableau ci-dessous liste les fonctions de base de SNMP.

Fonction	Description
Get	Commande utilisée par le gestionnaire pour demander des informations à un agent.
Get Next	Commande employée par le gestionnaire pour obtenir des informations depuis un tableau ou une table.
Get Response	Commande employée par l'agent interrogé pour répondre à la demande du gestionnaire.
Set	Commande employée par le gestionnaire pour modifier la valeur de la variable qui réside dans la MIB de l'agent.
Trap	Notification utilisée par l'agent pour informer le gestionnaire qu'un événement donné s'est produit.

Pour plus d'informations sur SNMP, consultez les sites Web suivants :

- NET-SNMP Home Page (Page d'accueil NET-SNMP) (http://net-snmp.sourceforge.net)
- SNMP FAQ (FAQ sur SNMP) (http://www.faqs.org/faqs/snmp-faq/part1)
- RFC 1157 (http://www.ietf.org/rfc/rfc1157.txt)
- SNMPLink (liaison SNMP) (http://www.snmplink.org)
- SNMPInfo (Infos sur SNMP) (http://www.snmpinfo.com)
- SNMP RFC Standard MIBs and Informative Links (Liens d'information et MIB standard RFC SNMP (http://www.wtcs.org/snmp4tpc/snmp_rfc.htm)
- RFC 2605 (http://ietf.org/rfc/rfc2605.txt?number=2605)

eDirectory et SNMP

eDirectory peut stocker et gérer des millions d'objets, tels que des utilisateurs, des applications, des périphériques réseau et des données. Plus les objets sont nombreux, plus il est nécessaire de suivre les ajouts et les modifications effectués dans eDirectory. SNMP apporte une solution à ce problème: il vous aide à surveiller les serveurs eDirectory en assurant le suivi des modifications.

Avantages de l'instrumentation de SNMP sur eDirectory

- Surveillance en temps réel d'un serveur eDirectory
- Surveillance de eDirectory depuis un navigateur MIB SNMP tiers
- Suivi du statut de eDirectory pour vérifier les opérations standard
- Identification et traitement des problèmes potentiels après leur détection
- Configuration de trappes et de statistiques en vue d'une surveillance sélective
- Définition d'une tendance pour l'accès à eDirectory
- Enregistrement et analyse des données historiques obtenues via SNMP
- Prise en charge des statistiques pour les opérations SNMP Get, GetNext
- Utilisation de l'agent principal natif SNMP sur l'ensemble de la plate-forme

Présentation du fonctionnement de SNMP avec eDirectory

L'implémentation de SNMP dans eDirectory fournit des informations utiles sur eDirectory en matière de statistiques sur les accès, les opérations, les erreurs et les performances du cache. Des trappes relatives à l'occurrence d'événements peuvent également être envoyées via une implémentation de SNMP. Les trappes et statistiques sont définies dans la MIB.

REMARQUE : Il se peut que vous deviez accéder aux attributs codés en utilisant un canal sécurisé, si vous avez spécifié qu'il convient d'utiliser un canal sécurisé pour accéder à ces attributs. Pour plus d'informations, reportez-vous à la section « Attributs codés », page 237.

MIB de surveillance du service d'annuaire

La MIB eDirectory définit les statistiques et les trappes qui servent à surveiller eDirectory. Les OID suivants sont assignés à cette MIB:

iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).novell(23).mibDoc(2).ndsMIB(98)

Statistiques

La MIB eDirectory est divisée en quatre tables distinctes d'objets gérés :

- **Table Statistiques de la base de données mise en cache – ndsDbCacheTable :** contient une description des serveurs d'annuaire ainsi que des statistiques globales sur les entrées mises en cache par ces serveurs.
- **Table Statistiques de la base de données configurée – ndsDbConfigTable :** contient une description des serveurs d'annuaire ainsi que des statistiques globales sur les entrées configurées par ces serveurs.
- **Table Statistiques de protocole – ndsProtoIfOpsTable :** fournit des statistiques globales sur les accès, les opérations et les erreurs pour chaque interface de protocole d'application d'un serveur d'annuaire.
- **Table Statistiques d'interaction – ndsServerIntTable :** effectue un suivi du dernier serveur d'annuaire « N » avec lequel l'annuaire surveillé est entré ou a tenté d'entrer en interaction. « N » est une constante définie localement.

REMARQUE : pour plus d'informations sur les statistiques, reportez-vous à « Statistiques », page 505.

Trappes – ndsTrapVariables

La MIB eDirectory définit 119trappes, dont 117 sont assignées à des événements eDirectory. Les deux trappes supplémentaires, ndsServerStart et ndsServerStop, sont directement générées par le sous-agent SNMP. Ces 2 trappes ne peuvent pas être configurées.

REMARQUE : pour plus d'informations sur les trappes, reportez-vous à la section « Trappes », page 479.

Pour plus d'informations sur les statistiques et les trappes, reportez-vous au fichier edir.mib.

Il réside dans les répertoires suivants :

NetWare : sys:\etc

Windows : <répertoire_installation>\SNMP

Linux et UNIX : /etc/opt/novell/eDirectory/conf/ndssnmp/

Objet Groupe SNMP

L'objet Groupe SNMP permet de configurer et de gérer les trappes SNMP eDirectory. Durant l'installation, un objet Groupe SNMP appelé « Groupe SNMP – *nom_serveur* » est créé (*nom_serveur* étant le nom du serveur sur lequel les services SNMP pour eDirectory sont installés). L'objet Groupe SNMP est créé dans le même conteneur que l'objet Serveur. Cet utilitaire de configuration SNMP permet de configurer les trappes SNMP.

Sous Windows

Pour créer un objet Groupe SNMP, entrez la commande suivante :

```
rundll32 snmpinst, snmpinst -c <createobj> -a <FDN_utilisateur> -
p <mot_de_passe> -h <nom_hôte ou adresse _IP>
```

Paramètre	Description
-c <*createobj*>	Commande de trappe spécifiant la création d'un objet
-a <*FDN_utilisateur*>	Nom distinctif complet d'un utilisateur disposant de droits d'administrateur
-p <*mot_de_passe*>	Mot de passe d'authentification du FDN utilisateur
-h <*nom_hôte ou adresse_IP*>	Nom d'hôte DNS ou adresse IP

Exemple :

rundll32 snmpinst, snmpinst -c createobj -a admin.mon_contexte -p mon_mot_de_passe -h 160.98.146.26

Pour supprimer un objet Groupe SNMP, entrez la commande suivante :

rundll32 snmpinst, snmpinst -c < deleteobj> -a *<FDN_utilisateur>* -p *<mot_de_passe>* -h *<nom_hôte ou adresse _IP>*

Pour plus d'informations, consultez le tableau ci-dessus.

Exemple :

rundll32 snmpinst, snmpinst -c deleteobj -a admin.mon_contexte -p mon_mot_de_passe -h 160.98.146.26

Sous NetWare

L'utilitaire snmpinst permet de créer et de supprimer un objet Groupe SNMP. Il réside dans le répertoire sys:\system\.

Pour créer un objet Groupe SNMP, entrez la commande suivante :

SNMPINST -c *<contexte_admin> <mot_de_passe> <DN_serveur>*

Paramètre	Description
-c	Commande de trappe spécifiant la création d'un objet La commande de suppression correspond à -d.
<*Contexte_admin*>	Nom distinctif complet d'un utilisateur disposant de droits d'administrateur
<*Mot_de_passe*>	Mot de passe d'authentification du FDN utilisateur
<*DN_serveur*>	Nom d'hôte DNS

Exemple :

SNMPINST -c admin.mon_contexte.nom_arborescence mon_mot_de_passe mon_serveur

Pour supprimer un objet Groupe SNMP, entrez la commande suivante :

SNMPINST -d *<contexte_admin> <mot_de_passe> <DN_serveur>*

Pour plus d'informations, reportez-vous au tableau ci-dessus.

Exemple :

SNMPINST -d admin.mon_contexte.nom_arborescence mon_mot_de_passe mon_serveur

Sous Linux et UNIX

Pour créer un objet Groupe SNMP, entrez la commande suivante :

ndsconfig add -m *<nom_module>* -a *< FDN_utilisateur>*

Exemple :

ndsconfig add -m snmp -a admin.mon_contexte

Installation et configuration des services SNMP pour eDirectory

L'installation des services SNMP pour eDirectory s'effectue simultanément avec celle de eDirectory. Vous pouvez modifier la configuration par défaut des services SNMP pour eDirectory à l'aide de iManager. Pour plus d'informations, reportez-vous à la section « Configuration dynamique », page 467.

Un nouvel objet appelé Groupe SNMP est ajouté à l'arborescence Annuaire lors de l'installation de eDirectory. Cet objet permet de configurer et de gérer les trappes SNMP de Novell eDirectory. Pour plus d'informations, reportez-vous à la section « Objet Groupe SNMP », page 463.

Installation de SNMP après l'installation de eDirectory sous Windows

Si les services SNMP ne sont pas installés avec eDirectory, le programme d'installation de eDirectory copie uniquement les fichiers de sous-agents SNMP requis et ne met pas à jour le registre.

Si vous souhaitez par la suite utiliser les services SNMP sur eDirectory, vous pouvez en effectuer l'installation et mettre à jour le registre via la commande suivante :

```
rundll32 snmpinst, snmpinst -c createreg
```

Chargement et déchargement du module serveur SNMP

Vous pouvez charger et décharger manuellement le module serveur SNMP. Par défaut, ce module est chargé automatiquement sur toutes les plates-formes. Toutefois, vous pouvez le charger manuellement sur les plates-formes Windows et Linux et UNIX.

Pour charger le module serveur SNMP, entrez les commandes suivantes :

Serveur	Commande
NetWare	Non applicable
Windows	Dans l'écran DHOST (NDSCONS), sélectionnez Ndssnmp.dlm > cliquez sur Démarrer.
Linux, Solaris, AIX et HP-UX	Pour charger le serveur de trappes SNMP, dans la page de gestion à distance DHOST, cliquez sur l'icône Serveur de trappes SNMP pour Novell eDirectory 8.8 pour démarrer. ou À l'invite, entrez `/opt/novell/eDirectory/bin/ndssnmp -l`.

Pour décharger le module serveur SNMP, entrez les commandes suivantes :

Serveur	Commande
NetWare	Non applicable
Windows	Dans l'écran DHOST (NDSCONS), sélectionnez ndssnmp.dlm, puis cliquez sur Arrêter.

Serveur	Commande
Linux, Solaris, AIX et HP-UX	Pour décharger le serveur de trappes SNMP, dans la page de gestion à distance DHOST, cliquez sur l'icône SNMP Trap Server (Serveur de trappes SNMP) pour Novell eDirectory 8.8 pour arrêter. ou À l'invite, entrez **`/opt/novell/eDirectory/bin/ndssnmp -u`**.

Configuration du sous-agent

Configuration statique

La configuration statique est employée avant la mise en service du sous-agent. Vous pouvez le configurer manuellement en modifiant le fichier ndssnmp.cfg sous Windows, Solaris, Linux, AIX ou le fichier dssnmp.cfg sous NetWare. Le fichier ndssnmp.cfg réside dans les répertoires suivants :

Windows : *répertoire_installation*\SNMP\

NetWare : sys:\etc\

Linux et UNIX : /etc/opt/novell/eDirectory/conf/ndssnmp/

REMARQUE : si vous apportez des modifications au fichier ndssnmp.cfg, vous devez redémarrer le sous-agent.

Vous pouvez fournir au sous-agent des informations de configuration telles que :

- INTERACTIVE *état*

  Où *état* peut correspondre à « on » (activé) ou « off » (désactivé). Si l'état correspond à « on », vous êtes invité à entrer le nom d'utilisateur et le mot de passe lors du démarrage du sous-agent. Si l'état est « off », le nom d'utilisateur et le mot de passe sont extraits de l'emplacement de stockage sécurisé. Valeur par défaut = off.

  Exemples:

  INTERACTIVE on

  INTERACTIVE off

- INTERACTION *valeur*

  Où le paramètre *valeur* correspond au nombre d'entrées de la table d'interaction. Plage = de 1 à 10. Valeur par défaut= 4. Exemples: INTERACTION 4 INTERACTION 2

- MONITOR *état*

  Où *état* peut correspondre à «on» (activé) ou «off» (désactivé). Valeur par défaut = On. Exemples : MONITOR on MONITOR off

- SSLKEY *fichier_certificat*

  Où le paramètre *fichier_certificat* correspond au certificat exporté avec son chemin d'accès. Vous devez saisir le chemin d'accès au certificat exporté. Exemples: SSLKEY /home/guest/snmp-cert.der (Linux and UNIX) SSLKEY c:\home\guest\snmp-cert.der (WindowsNT et NetWare)

- SERVER *nom_hôte/adresse_ip*

  Où *nom_hôte* correspond au nom de l'hôte sur lequel le serveur eDirectory est installé et configuré. Seul le serveur installé en local est pris en charge. Il s'agit d'une commande obligatoire dans le fichier. Dans le cas contraire, aucun des serveurs n'est surveillé. Valeur par défaut: nom d'hôte du serveur local. Exemples: SERVER mon_serveurSERVER mon_serveur:1524

  Sous Linux et UNIX, si vous disposez de plusieurs instances de eDirectory, vous pouvez inclure tous les serveurs eDirectory à surveiller comme suit :

  SERVER myserver:1524

  SERVER myserver:2524

  SERVER myserver:6524

  REMARQUE : n'insérez pas d'espace avant ou après «:» dans la commande du serveur.

Configuration dynamique

Une fois le service d'annuaire activé et en cours d'exécution, la configuration dynamique peut s'effectuer à tout moment à l'aide des méthodes suivantes :

Ligne de commande

Un utilitaire de ligne de commande de configuration des trappes peut être utilisé pour configurer les trappes SNMP de eDirectory.

L'utilitaire de ligne de commande de configuration permet:

- d'activer ou de désactiver les trappes ; de définir l'intervalle des trappes ; d'activer ou de désactiver les trappes d'échec ; de lister les trappes activées, désactivées ou toutes les trappes.

REMARQUE : pour plus de détails, reportez-vous à la section « Configuration des trappes », page 494.

Plug-in iManager

Vous pouvez également utiliser Novell iManager pour configurer les trappes. Novell iManager est un outil basé sur un navigateur qui permet d'administrer, de gérer et de configurer les objets eDirectory. Novell iManager vous donne la possibilité d'assigner des tâches ou des responsabilités particulières aux utilisateurs, et de leur présenter uniquement les outils (et les droits associés) qui leur sont nécessaires.

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Gestion SNMP > Présentation de SNMP.
3. Cliquez sur Afficher des objets Groupe SNMP: cliquez sur le nom de l'objet Groupe SNMP à configurer.
4. Entrez les paramètres configurables dans la page Général/Trappes.
5. Cliquez sur Appliquer, puis sur OK pour enregistrer les nouveaux paramètres de configuration.

   REMARQUE : pour plus d'informations, reportez-vous à l'aide en ligne de Novell iManager.

Configuration des services SNMP pour eDirectory

Pour configurer les services SNMP pour eDirectory, exécutez la procédure suivante :

1. Configuration de l'agent principal
2. Démarrage de l'agent principal
3. Configuration du sous-agent
4. Démarrage du sous-agent

NetWare

Sous NetWare, l'agent principal natif (snmp.nlm) est installé par défaut avec le système d'exploitation.

SUGGESTION : NetWare fournit l'agent principal SNMP par défaut. Pour plus d'informations, consultez le site Web SNMP Developers Components (Composants pour développeurs SNMP) (http://developer.novell.com/ndk/snmpcomp.htm).

Configuration de l'agent principal

Nom de communauté

1. À l'invite, entrez la commande **inetcfg**:
2. Sélectionnez l'option Manage Configuration (Gérer la configuration).
3. Sélectionnez l'option Configure SNMP parameters (Configurer les paramètres SNMP).
4. Modifiez en conséquence la chaîne de communauté.

Emplacement cible des trappes

1. Éditer le fichier sys:\etc\traptarg.cfg et entrez l'adresse IP ou le nom d'hôte de l'ordinateur cible auquel les trappes doivent être envoyées.

Démarrage de l'agent principal

L'agent principal snmp.nlm est lancé par défaut.

Chargement du sous-agent

1. Pour charger le sous-agent, entrez **dssnmpsa** à l'invite de commande.

   Vous accédez à une boîte de dialogue contenant les options Login et Quitter.
2. Cliquez sur Login pour poursuivre et sur Quitter pour arrêter.
3. (Conditionnel) Si vous sélectionnez Login, vous devez indiquer les informations correspondantes. Entrez le nom d'utilisateur et le mot de passe.
4. Entrez **o** dans le champ Mémoriser le mot de passe pour enregistrer le mot de passe. Au prochain lancement du sous-agent, vous ne serez plus invité à entrer le mot de passe. Si vous tapez n, vous devrez indiquer le mot de passe au prochain démarrage du sous-agent.
5. Appuyez sur Entrée après avoir saisi « o » ou « n ».
6. Appuyez sur la touche F10 pour vous loguer à l'arborescence.
7. Appuyez sur Entrée pour continuer.
8. Le sous-agent est lancé.

REMARQUE : si la valeur ON est définie pour le paramètre INTERACTION dans le fichier sys:\etc\ndssnmp.cfg, cette boîte de dialogue saffiche. Si la valeur correspond à OFF, elle ne s'affiche pas.

Windows

Configuration de l'agent principal

REMARQUE : l'agent principal SNMP doit être installé avant eDirectory. Pour plus d'informations, consultez le site Web SNMP Installation on Windows (Installation de SNMP sous Windows) (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winntas/maintain/featusability/getting.asp).

1. Dans la boîte de dialogue SNMP Properties (Propriétés de SNMP) de Microsoft, cliquez sur l'onglet Agent.
2. Entrez les informations relatives au contact et à lemplacement.
3. Cliquez sur Traps (Interruptions), puis entrez les informations relatives au nom de communauté et à l'emplacement cible des trappes.
   - **3a** Entrez le nom de communauté, puis cliquez sur Ajouter.
   - **3b** Entrez l'adresse IP ou le nom d'hôte de l'ordinateur cible pour lequel sont générées les trappes.
   - **3c** Cliquez sur Ajouter pour ajouter l'adresse IP ou le nom d'hôte.
4. Activez l'option Allow Service to Interact with Desktop (Autoriser le service à interagir avec le Bureau).

   Si elle n'est pas activée, vous ne pourrez pas vous connecter à SNMP sous Windows.

   - Sous Windows NT : cliquez sur Start (Démarrer) > Paramètres (Settings) > Panneau de configuration (Control Panel) > Services. Sélectionnez ensuite SNMP > Startup (Démarrage), puis l'option Allow Service to Interact with Desktop (Autoriser le service à interagir avec le Bureau).
   - Sous Windows 2000 : cliquez sur Start (Démarrer) > Settings (Paramètres) > Control Panel (Panneau de configuration) > Administrative Tools (Outils d'administration) > Services. Puis cliquez avec le bouton droit sur SNMP et sélectionnez Properties (Propriétés). Dans l'onglet Log On (Connexion), sélectionnez l'option Allow Service to Interact with Desktop (Autoriser le service à interagir avec le Bureau).

Démarrage de l'agent principal

Pour démarrer l'agent principal, procédez comme suit :

- Sous Windows NT : cliquez sur Start (Démarrer) > Settings (Paramètres) > Control Panel (Panneau de configuration) > Services > SNMP > Start (Démarrer).

  Sous Windows 2000 : cliquez sur Start (Démarrer) > Settings (Paramètres) > Control Panel (Panneau de configuration) > Administrative Tools (Outils d'administration) > Services > SNMP > Start (Démarrer).
- À l'invite, entrez la commande suivante :

  ```
  Net start SNMP
  ```

Arrêt de l'agent principal

Pour arrêter l'agent principal, procédez comme suit :

- Sous Windows NT : cliquez sur Start (Démarrer) > Settings (Paramètres) > Control Panel (Panneau de configuration) > Services > SNMP > Stop (Arrêter).

  Sous Windows 2000 : cliquez sur Start (Démarrer) > Settings (Paramètres) > Control Panel (Panneau de configuration) > Administrative Tools (Outils d'administration) > Services > SNMP > Stop (Arrêter).
- À l'invite, entrez la commande suivante :

  ```
  Net stop SNMP
  ```

Démarrage du sous-agent

Lorsque l'agent principal est lancé sous Windows, le sous-agent démarre également.

IMPORTANT : le dernier Service Pack mis à jour doit être installé consécutivement au service SNMP.

Linux

Sous Linux (excepté SLES 9 ou Linux OES), le RPM net-snmp-5.0.9-4.rh73.i386.rpm doit être installé. Sous SLES 9 (Linux OES), l'agent principal par défaut du système (net-snmp-5.1-80.xx) est utilisé.

La procédure de configuration de SLES 9 (Linux OES) et d'autres variantes de Linux est différente. Pour plus d'informations, reportez-vous aux sections :

- « Configuration des services SNMP sous SLES 9 ou Linux OES », page 470
- « Configuration des services SNMP sous Linux (excepté SLES 9 ou OES) », page 471
- « Problèmes survenant au démarrage du sous-agent », page 473

Configuration des services SNMP sous SLES 9 ou Linux OES

- « Configuration de l'agent principal », page 470
- « Démarrage de l'agent principal », page 471
- « Démarrage du sous-agent », page 471
- « Arrêt du sous-agent », page 471

Configuration de l'agent principal

Pour configurer l'agent principal sous SLES 9 ou Linux OES, modifiez le fichier snmpd.conf comme expliqué dans la section « Modifications de Snmpd.conf », page 470.

Le fichier snmpd.conf se trouve dans le répertoire /etc/snmp sous Linux OES ou SLES9 et dans le répertoire /etc sur les autres plates-formes Linux.

Modifications de Snmpd.conf

Dans le fichier snmpd.conf, entrez le nom d'hôte

```
trapsink mon_serveur public
```

Où *mon_serveur* correspond au nom d'hôte de l'emplacement cible des trappes.

Dans le fichier snmpd.conf, ajoutez la ligne suivante :

```
master agentx
```

Apportez également les modifications suivantes :

Texte original	Texte modifié
com2sec notConfigUser default public	com2sec demouser default public
group notConfigGroup v1 notConfigUser	group demogroup v1 demouser
view systemview included system	view all included .1
access notConfigGroup "" any noauth exact systemview none none	access demogroup "" any noauth exact all all all

Si le texte ci-dessus ne figure pas dans le fichier snmpd.conf, ajoutez-le.

IMPORTANT : si des fichiers de configuration sont modifiés, il convient de redémarrer l'agent principal et le sous-agent.

Démarrage de l'agent principal

Pour démarrer l'agent principal, exécutez la commande suivante :

```
/usr/sbin/snmpd -C -c /etc/snmpd.conf
```

Démarrage du sous-agent

Pour démarrer le sous-agent, exécutez la commande suivante :

```
/etc/init.d/ndssnmpsa start
```

REMARQUE : Si vous obtenez une erreur «undefined symbol: EVP_md5» au démarrage du sous-agent, reportez-vous à la section « Problèmes survenant au démarrage du sous-agent », page 473.

Entrez le nom d'utilisateur et le mot de passe lorsque le système vous y invite. Une fois l'authentification effectuée, le message suivant s'affiche si le paramètre INTERACTION a la valeur ON dans le fichier /etc/ndssnmp/ndssnmp.cfg :

```
Souhaitez-vous mémoriser le mot de passe? (o/n)
```

Entrez **o** pour le mémoriser. Au prochain lancement du sous-agent, vous ne serez plus invité à entrer le mot de passe.

Si vous entrez **n**, vous devrez indiquer le mot de passe au prochain démarrage du sous-agent.

IMPORTANT : Pour SLES 9 ou Linux OES, reportez-vous au fichier lisezmoi qui mentionne les problèmes connus survenant au démarrage du sous-agent.

Arrêt du sous-agent

Pour arrêter le sous-agent, exécutez la commande suivante :

```
/etc/init.d/ndssnmpsa stop
```

Configuration des services SNMP sous Linux (excepté SLES 9 ou OES)

- « Configuration de l'agent principal », page 471
- « Démarrage de l'agent principal », page 472
- « Démarrage du sous-agent », page 473
- « Arrêt du sous-agent », page 473

Configuration de l'agent principal

Téléchargez-le à l'adresse http://sourceforge.net/projects/net-snmp (http://sourceforge.net/projects/net-snmp).

Net-snmp-5.0.9-4.rh73.i386.rpm requiert rpm-4.0.4-7x.i386.rpm pour être installé sur le système. Vous pouvez le télécharger à l'adresse http://rpmfind.net/linux/RPM/rpm.org/rpm/dist/rpm-4.0.x/rpm-4.0.4-7x.i386.html (http://rpmfind.net/linux/RPM/rpm.org/rpm/dist/rpm-4.0.x/rpm-4.0.4-7x.i386.html).

En outre, vous devez modifier le fichier snmpd.conf comme expliqué dans la section « Modifications de Snmpd.conf », page 470.

Démarrage de l'agent principal

Pour démarrer l'agent principal, vous devez d'abord installer et configurer net-snmp-5.0.9-4.rh73.i386.rpm.

Pour ce faire, utilisez l'une des deux solutions expliquées ci-dessous. Nous vous recommandons toutefois d'utiliser la première étant donné que dans la seconde, vous devrez désinstaller les paquetages SNMP du système et peut-être également tous les RPM qui y sont associés.

Solution 1

1. Installez les RPM net-snmp-5.0.9-4.rh73.i386.rpm et rpm-4.0.4-7x.i386.rpm à un emplacement personnalisé, par exemple, /home/ndssnmp.

   Installez-le premier RPM comme suit :

   ```
   # cd /home/ndssnmp
   # rpm2cpio net-snmp-5.0.9-4.rh73.i386.rpm | cpio -ivd
   ```

2. Installez le second RPM (il s'agit du RPM associé requis par le daemon SNMP)

   ```
   # cd /home/ndssnmp
   # rpm2cpio  rpm-4.0.4-7x.i386.rpm | cpio -ivd
   ```

3. Exportez le chemin comme suit :

   ```
   # export LD_LIBRARY_PATH=/home/ndssnmp/usr/lib
   ```

4. Démarrez l'agent principal comme suit :

   ```
   # /home/ndssnmp/usr/sbin/snmpd -C -c snmpd.conf
   ```

   Par exemple, si votre fichier snmpd.conf figure dans le répertoire /etc, la commande sera similaire à celle-ci :

   ```
   # /home/ndssnmp/usr/sbin/snmpd -C -c /etc/snmpd.conf
   ```

   REMARQUE : vérifiez que le fichier snmpd.conf contient les informations pertinentes nécessaires au démarrage de ndssnmpsa. Pour plus d'informations, reportez-vous à la section « Configuration des services SNMP sous SLES 9 ou Linux OES », page 470.

5. (Conditionnel) Il se peut que l'erreur suivante soit renvoyée au démarrage de l'agent principal:

   ```
   snmpd: error while loading shared libraries:libcrypto.so.2: cannot open
   shared object file: No such file or directory (snmpd: erreur au chargement
   des bibliothèques partagées:libcrypto.so.2: impossible d'ouvrir le
   fichier d'objet partagé: aucun fichier ou répertoire de ce type)
   ```

   Cette erreur sera renvoyée si libcrypto.so.2 n'est pas installé sur votre système.

   Par conséquent, vous devez établir un lien explicite vers la bibliothèque crypto installée sur le système comme mentionné ci-dessous :

   ```
   # cd /usr/lib
   ```

   Ajoutez en outre l'un des éléments ci-dessous en fonction de votre version de Linux :

   - **Pour Red Hat Advanced Server 3.0 :**

     ```
     # ln -s libcrypto.so libcrypto.so.2
     ```

   - **Pour SUSE Linux Enterprise Server 8 :**

     ```
     # ln -s libcrypto.so.0.9.6 libcrypto.so.2
     ```

6. (Conditionnel) Si l'agent principal SNMP est déjà configuré sur un port par défaut 161, démarrez-le sur un autre port tel que :

   ```
   # /home/ndssnmp/usr/sbin/snmpd -C -c /etc/snmpd.conf 1161
   ```

Solution 2

1. Désinstallez le paquetage SNMP de votre système.
2. Si le paquetage SNMP est déjà installé et qu'il s'agit d'une autre version que net-snmp-5.0.9-4.rh73.i386.rpm, désinstallez-le et installez net-snmp-5.0.9-4.rh73.i386.rpm.

   REMARQUE : Si des RPM associés sont requis, téléchargez-les et installez-les également.
3. Démarrez l'agent principal comme suit :

   ```
   /usr/sbin/snmpd -C -c /etc/snmpd.conf
   ```

Démarrage du sous-agent

Pour démarrer le sous-agent, exécutez la commande suivante :

`/etc/init.d/ndssnmpsa start`

REMARQUE : Si vous obtenez une erreur «undefined symbol: EVP_md5» au démarrage du sous-agent, reportez-vous à la section « Problèmes survenant au démarrage du sous-agent », page 473.

Entrez le nom d'utilisateur et le mot de passe lorsque le système vous y invite. Une fois l'authentification effectuée, le message suivant s'affiche si le paramètre INTERACTION a la valeur ON dans le fichier /etc/ndssnmp/ndssnmp.cfg :

```
Souhaitez-vous mémoriser le mot de passe? (o/n)
```

Entrez **`o`** pour le mémoriser. Au prochain lancement du sous-agent, vous ne serez plus invité à entrer le mot de passe.

Si vous entrez **`n`**, vous devrez indiquer le mot de passe au prochain démarrage du sous-agent.

Arrêt du sous-agent

Pour arrêter le sous-agent, exécutez la commande suivante :

`/etc/init.d/ndssnmpsa stop`

Problèmes survenant au démarrage du sous-agent

Au démarrage du sous-agent, il se peut que le message d'erreur suivant s'affiche :

```
 /opt/novell/eDirectory/bin/ndssnmpsa: error while loading shared libraries:
/usr/lib/libnetsnmp.so.5: undefined symbol: EVP_md5.
```

Pour résoudre ce problème, vous devez exporter le chemin d'accès libcrypto. Par exemple :

`export LD_PRELOAD=/lib/libcrypto.so.0.9.7a:/usr/lib/libwrap.so.0`

Le chemin d'accès libcrypto.so.0.9.7a peut porter un autre nom sur votre système. Cela dépend de la version crypto installée.

Solaris

Configuration de l'agent principal

Avant de charger le paquetage SNMP, vous devez installer l'agent principal Solstice Enterprise 1.0.3 dans le système. S'il n'est pas installé, téléchargez-le sur le site Solstice Enterprise Agents (Agents Solstice Enterprise) (http://wwws.sun.com/software/entagents).

1. Dans le fichier /etc/snmp/conf/snmpd.conf, identifiez un nom d'hôte. Ajoutez l'entrée de trappe suivante :

   `trap` ***`mon_serveur`***

   Où *mon_serveur* correspond au nom d'hôte de l'emplacement cible des trappes.

2 Dans le fichier /etc/snmp/conf/snmpdx.acl, ajoutez la commande suivante dans la section destinée aux paramètres de trappes :

communauté_trappes = public
hosts = *mon_serveur* {
enterprise = "*Novell eDirectory*"
num_trappes = 1-117, 2001, 2002 }

où *communauté_trappes* correspond au nom de la communauté utilisé dans les trappes, *mon_serveur* au nom d'hôte de l'emplacement cible des trappes, *Novell eDirectory* à la MIB de l'entreprise et *num_trappes* à la plage de trappes.

IMPORTANT : si des fichiers de configuration sont modifiés, il convient de redémarrer l'agent principal et le sous-agent.

Démarrage de l'agent principal

Pour démarrer l'agent principal, exécutez la commande suivante :

```
/usr/lib/snmp/snmpdx -y -c /etc/snmp/conf/
```

Configuration du sous-agent

Sous Solaris, le sous-agent ndssnmpsa est un processus de daemon.

La configuration du sous-agent nécessite l'utilisation des fichiers de configuration suivants (enregistrés sous /etc/snmp/conf/):

- **ndsmib.reg** correspond au fichier d'enregistrement du sous-agent
- **ndsmib.acl** est le fichier de configuration du sous-agent SNMP.

Démarrage du sous-agent

Pour démarrer le sous-agent, exécutez la commande suivante :

```
/etc/init.d/ndssnmpsa start
```

Entrez le nom d'utilisateur et le mot de passe lorsque le système vous y invite. Une fois l'authentification effectuée, le message suivant s'affiche si le paramètre INTERACTION a la valeur ON dans le fichier /etc/ndssnmp/ndssnmp.cfg :

```
Souhaitez-vous mémoriser le mot de passe? (o/n)
```

Entrez **o** pour le mémoriser. Au prochain lancement du sous-agent, vous ne serez plus invité à entrer le mot de passe.

Si vous entrez **n**, vous devrez indiquer le mot de passe au prochain démarrage du sous-agent.

Arrêt du sous-agent

Pour arrêter le sous-agent, exécutez la commande suivante :

```
/etc/init.d/ndssnmpsa stop
```

AIX

Configuration de l'agent principal

Dans le fichier /etc/snmpd.conf, ajoutez l'entrée cible suivante pour les trappes :

trap *communauté mon_serveur nom_vue masque_trappe*

où

- *communauté* correspond au nom de la communauté qui sera codée dans le paquet de trappes ;
- *mon_serveur* correspond au nom d'hôte de l'emplacement cible des trappes
- *nom_vue* correspond à l'identificateur d'objet unique dans la notation numérique séparée par des points.

  Par exemple : 1.3.6.1.4.1.23.2.98. Ce paramètre est facultatif. S'il n'est pas ajouté, la vue s'applique par défaut à l'ensemble de l'arborescence MIB.
- *masque_trappe* correspond au format hexadécimal

  Les bits, de gauche à droite, correspondent aux trappes coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss et enterpriseSpecific. Dans l'exemple, la valeur « 98 » figurant à droite n'a aucune signification. La valeur «1» permet l'envoi de la trappe correspondante. Une valeur différente entraîne le blocage de la trappe.

Exemple :

fe ne bloque aucune trappe (1111 1110)

7e bloque la trappe coldStart (0111 1110)

be bloque la trappe warmStart (1011 1110)

3e bloque les trappes coldStart et warmStart (0011 1110)

Démarrage de l'agent principal

Pour démarrer l'agent principal, exécutez la commande suivante :

/usr/sbin/snmpdv1

Démarrage du sous-agent

Pour démarrer le sous-agent, exécutez la commande suivante :

/etc/ndssnmpsa start

Entrez le nom d'utilisateur et le mot de passe lorsque le système vous y invite. Une fois l'authentification effectuée, le message suivant s'affiche si le paramètre INTERACTION a la valeur ON dans le fichier /etc/ndssnmp/ndssnmp.cfg :

```
Souhaitez-vous mémoriser le mot de passe? (o/n)
```

Entrez **o** pour le mémoriser. Au prochain lancement du sous-agent, vous ne serez plus invité à entrer le mot de passe.

Si vous entrez **n**, vous devrez indiquer le mot de passe au prochain démarrage du sous-agent.

Arrêt du sous-agent

Pour arrêter le sous-agent, exécutez la commande suivante :

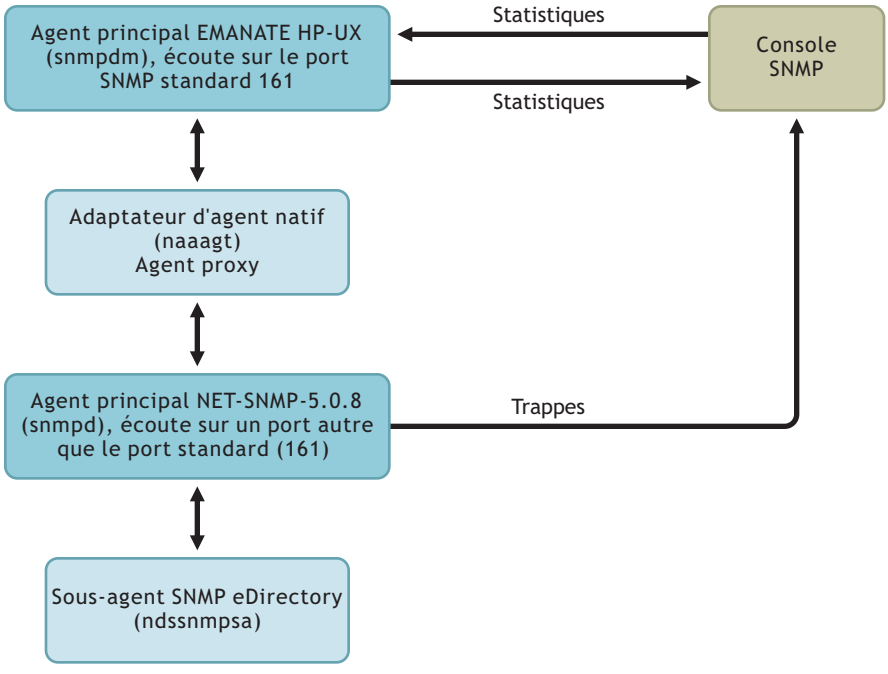
/etc/ndssnmpsa stop

Sous HP-UX, l'agent principal natif est EMANATE SNMP. La configuration de l'agent principal sous HP-UX implique également la configuration de l'agent SNMP proxy. Cette dernière s'effectue via l'adaptateur d'agent natif (NAA). Celui-ci permet aux agents SNMP tiers de travailler avec l'agent principal SNMP HP-UX (snmpdm). L'agent SNMP tiers est, dans ce cas, l'agent principal NET-SNMP. Ce dernier doit utiliser le même port UDP non standard que celui sur lequel l'adaptateur d'agent natif a été configuré pour écouter.

Pour plus de détails, reportez-vous aux sections « Démarrage/configuration de l'adaptateur d'agent natif (NAA) », page 476 et « Démarrage/configuration de l'agent principal NET-SNMP », page 477.

La figure suivante présente le flux de données entre le sous-agent SNMP de eDirectory, l'agent principal NET-SNMP, l'agent NAA, l'agent principal EMANATE HP-UX et la console SNMP.

Figure 49 Flux de données SNMP



Démarrage de l'agent principal SNMP HP-UX

Pour démarrer l'agent principal SNMP HP-UX, exécutez la commande suivante :

```
/etc/snmpd
```

ou

```
/usr/sbin/snmpdm
```

REMARQUE : pour arrêter l'agent principal SNMP HP-UX, entrez etc/snmpd -k

Démarrage/configuration de l'adaptateur d'agent natif (NAA)

Avant de lancer l'agent NAA (naaagt), vous devez exporter les variables d'environnement suivantes :

- HP_NAA_CNF – fichier de configuration NAA ;
- HP_NAA_PORT – port UDP non standard que l'agent principal NET-SNMP écoute ;
- HP_NAA_GET_COMMUNITY – nom de communauté à utiliser dans les requêtes SNMP transférées de NAA à l'agent principal NET-SNMP.

Par exemple :

```
export HP_NAA_CNF=/etc/ndssnmp/ndssnmpNAA.cfg

export HP_NAA_PORT=8161 ## Spécifiez un port UDP non standard

export HP_NAA_GET_COMMUNITY=public
```

Pour plus de détails sur l'agent NAA, reportez-vous à la page du manuel naaagt.

Pour lancer l'agent NAA, entrez la commande suivante :

/usr/sbin/naaagt

REMARQUE : vous devez accéder à la racine pour lancer l'agent NAA.

Démarrage/configuration de l'agent principal NET-SNMP

Pour pouvoir configurer l'agent principal NET-SNMP, vous devez d'abord le télécharger et l'installer.

1. Téléchargez le fichier TAR NET-SNMP version 5.0.8 (net-snmp-5.0.8-HP-UX_B.11.00_9000_712.tar.gz) à l'adresse SorceForge.net (http://sourceforge.net/project/showfiles.php?group_id=12694).
2. Installez les binaires NET-SNMP version 5.0.8. Pour ce faire, désarchivez le fichier TAR mentionné ci-dessus.

   Une fois cette opération effectuée, les binaires NET-SNMP version 5.0.8 sont installés dans le *répertoire_de_travail_actuel*/usr/local.

Pour configurer l'agent principal NET-SNMP :

- dans le fichier /etc/ndssnmp/snmpd-net-snmp.conf, entrez le nom d'hôte

  trapsink *mon_serveur* public

  où *mon_serveur* correspond au nom d'hôte de l'emplacement cible des trappes.

- Dans le fichier /etc/ndssnmp/snmpd-net-snmp.conf, ajoutez la ligne suivante si elle n'y figure pas déjà:

  master agentx

REMARQUE : aucun modèle de fichier de configuration d'agent principal n'est téléchargé avec les binaires NET-SNMP-5.0.8. Par conséquent, l'exemple de fichier correspondant est regroupé avec le composant SNMP de eDirectory. Après avoir installé eDirectory, vous pouvez accéder au modèle de fichier de configuration NET-SNMP (snmpd-net-snmp.conf file) dans le répertoire /etc/ndssnmp.

Pour démarrer l'agent principal NET-SNMP-5.0.8, utilisez la syntaxe suivante :

```
répertoire_NET-SNMP_installé/usr/local/sbin/snmpd -C -c /etc/ndssnmp/snmpd-
net-snmp.conf 8161
```

IMPORTANT : si des fichiers de configuration sont modifiés, il convient de redémarrer l'agent principal et le sous-agent.

Démarrage du sous-agent

Pour démarrer le sous-agent, exécutez la commande suivante :

```
/sbin/init.d/ndssnmpsa start
```

Entrez le nom d'utilisateur et le mot de passe lorsque le système vous y invite. Une fois l'authentification effectuée, le message suivant s'affiche si le paramètre INTERACTION a la valeur ON dans le fichier /etc/ndssnmp/ndssnmp.cfg :

```
Souhaitez-vous mémoriser le mot de passe? (o/n)
```

Entrez **o** pour le mémoriser. Au prochain lancement du sous-agent, vous ne serez plus invité à entrer le mot de passe.

Si vous entrez **n**, vous devrez indiquer le mot de passe au prochain démarrage du sous-agent.

Arrêt du sous-agent

Pour arrêter le sous-agent, exécutez la commande suivante :

```
/sbin/init.d/ndssnmpsa stop
```

Surveillance de eDirectory à l'aide de SNMP

eDirectory est surveillé à l'aide des trappes et de la fonctionnalité de statistiques de SNMP.

Pour surveiller un serveur eDirectory à laide de SNMP, vous devez disposer des droits suivants sur les objets Serveur NCP, Groupe LDAP et Serveur LDAP :

- droits Superviseur sur l'objet Serveur NCP ;
- droits de lecture sur l'attribut LDAP Autoriser les mots de passe en texte clair de l'objet Groupe LDAP
- droits de lecture sur les attributs LDAP Port TCP et Port SSL de l'objet Serveur LDAP.

Par défaut, un utilisateur qui se logue avec les droits d'administrateur ne rencontre aucun problème pour surveiller un serveur eDirectory qui exécute SNMP.

Trappes

Le composant SNMP génère au total 119trappes dont ndsServerStart (2001) et ndsServerStop (2002) qui ne peuvent pas être configurées. Ces trappes sont activées par défaut.

Vous pouvez utiliser un navigateur MIB pour vérifier les trappes générées.

REMARQUE : les numéros de trappe 42, 92 et 100 sont spécifiques à NetWare.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
1	ndsCreateEntry	Un nouvel objet est ajouté dans l'annuaire. Exemple : Création d'un objet à l'aide des outils LDAP, ICE, ConsoleOne® ou iManager.
2	ndsDeleteEntry	Un objet existant est supprimé. Exemple : Création d'un objet à l'aide des outils LDAP, ICE, ConsoleOne ou iManager.
3	ndsRenameEntry	Un objet existant est renommé. Exemple : Attribution dun nouveau nom à un objet à l'aide des outils LDAP, ICE, ConsoleOne ou iManager.
4	ndsMoveSourceEntry	Un objet est déplacé vers un autre contexte. La trappe donne alors le contexte de l'objet avant son déplacement. Exemple : Déplacement d'un objet via ldapmodrdn ou ldapsdk.
5	ndsAddValue	Une valeur est ajoutée à un attribut d'objet. Exemple : Ajout de nouvelles valeurs à des attributs à l'aide des outils LDAP, ICE, ConsoleOne ou iManager. **Remarque :** Si la valeur renvoyée est nulle, vous devrez peut-être accéder au répertoire via un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Accès aux attributs codés », page 493.
6	ndsDeleteValue	Une valeur est supprimée d'un attribut d'objet. Exemple : Suppression de nouvelles valeurs d'attribut à l'aide des outils LDAP, ICE, ConsoleOne ou iManager. **Remarque :** Si la valeur renvoyée est nulle, vous devrez peut-être accéder au répertoire via un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Accès aux attributs codés », page 493.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
7	ndsCloseStream	Un attribut de flux est modifié.
8	ndsDeleteAttribute	Une valeur est supprimée d'un attribut à valeur unique. Exemple : Suppression d'un attribut à l'aide des outils LDAP, ICE, ConsoleOne ou iManager. **Remarque :** Si la valeur renvoyée est nulle, vous devrez peut-être accéder au répertoire via un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Accès aux attributs codés », page 493.
9	ndsCheckSecurityEquiv	Le vecteur d'équivalence de sécurité d'une entrée spécifique est contrôlé. Exemple : Modification de l'attribut d'équivalence de sécurité à l'aide des outils LDAP, ICE, ConsoleOne ou iManager.
10	ndsUpdateSecurityEquiv	Le vecteur d'équivalence de sécurité d'une entrée spécifique est modifié. Exemple : Modification de l'attribut d'équivalence de sécurité à l'aide des outils LDAP, ICE, ConsoleOne ou iManager.
11	ndsMoveDestEntry	Un objet est déplacé vers un autre contexte. La trappe donne alors le contexte vers lequel l'objet est déplacé. Exemple : Déplacement d'objets via ldapmodrdn ou ldapsdk.
12	ndsDeleteUnusedExtref	Un objet Lien en amont est supprimé.
13	ndsAgentOpenLocal	L'agent Annuaire local est ouvert. Exemple : Exécution d'une réparation sans surveillance.
14	ndsAgentCloseLocal	L'agent Annuaire local est fermé. Exemple : Exécution d'une réparation sans surveillance.
15	ndsDSABadVerb	Un numéro de verbe incorrect est associé à une requête DSAgent. Exemple : Envoi d'une requête de verbe erronée à eDirectory à l'aide d'appels DClient.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
16	ndsMoveSubtree	Un conteneur et son objet subordonné sont déplacés. Exemple : Déplacement d'une partition vers un autre contexte à l'aide des outils LDAP, ICE, ConsoleOne ou iManager.
17	ndsNoReplicaPointer	Aucun pointeur de réplique n'est associé à une réplique donnée.
18	ndsSyncInEnd	La synchronisation entrante est terminée.
19	ndsBacklinkSecurEquiv	Une opération de liaison en amont a mis à jour le vecteur d'équivalence de sécurité d'un objet. Exemple : Modification de l'attribut d'équivalence de sécurité à l'aide des outils LDAP, ICE, ConsoleOne ou iManager.
20	ndsBacklinkOperPrivChg	Une opération de liaison en amont a modifié les privilèges de l'opérateur de la console d'un objet.
21	ndsDeleteSubtree	Un conteneur et ses objets subordonnés ont été supprimés.
22	ndsReferral	Un renvoi est créé.
23	ndsUpdateClassDef	Une définition de classe de schéma est mise à jour. Exemple : Cette trappe est générée lorsqu'une nouvelle classe ou un nouvel attribut sont ajoutés à un objet primaire, lui-même synchronisé avec un objet secondaire à l'aide des outils LDAP, ICE, ConsoleOne ou iManager.
24	ndsUpdateAttributeDef	Une définition d'attribut de schéma est mise à jour. Exemple : Cette trappe est générée lorsqu'un nouvel attribut est ajouté à un objet primaire, lui-même synchronisé avec un objet secondaire à l'aide des outils LDAP, ICE, ConsoleOne ou iManager.
25	ndsLostEntry	eDirectory identifie une entrée perdue. Une entrée perdue est une entrée pour laquelle vous recevez des mises à jour bien qu'elle n'existe pas sur le serveur local.
26	ndsPurgeEntryFail	L'opération de purge a échoué.
27	ndsPurgeStart	L'opération de purge a commencé. Exemple : Run dstrace et Set ndstrace=*j.
28	ndsPurgeEnd	L'opération de purge est terminée. Exemple : Run dstrace et Set ndstrace=*j.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
29	ndsLimberDone	L'opération de contrôle de connectivité est terminée. Exemple : Configuration de dstrace en vue du lancement du contrôleur de connectivité (limber) après une période donnée.
30	ndsPartitionSplitDone	L'opération de division de la partition est terminée. Exemple : Création d'une partition à l'aide de ConsoleOne ou de iManager.
31	ndsSyncServerOutStart	La synchronisation sortante à partir d'un serveur particulier est lancée. Exemple : Configuration de dstrace en vue du lancement de la synchronisation sortante après une période donnée.
32	ndsSyncServerOutEnd	La synchronisation sortante à partir d'un serveur particulier est terminée. Exemple : Configuration de dstrace en vue de l'arrêt de la synchronisation sortante après une période donnée.
33	ndsSyncPartitionStart	La synchronisation de la partition est lancée. Exemple : Première partition des conteneurs.
34	ndsSyncPartitionEnd	La synchronisation de la partition est terminée. Exemple : Première partition des conteneurs.
35	ndsMoveTreeStart	Le déplacement d'une sous-arborescence est lancé. Une sous-arborescence est déplacée en même temps qu'une partition. Exemple : Création et déplacement d'une partition vers un autre conteneur à l'aide de ConsoleOne ou de iManager.
36	ndsMoveTreeEnd	Le déplacement d'une sous-arborescence est terminé. Une sous-arborescence est déplacée lors de la fusion d'une partition. Exemple : Création et déplacement d'une partition vers un autre conteneur à l'aide de ConsoleOne ou de iManager.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
37	ndsJoinPartitionDone	La jonction des partitions est terminée. Exemple : Création et fusion d'une partition à l'aide de ConsoleOne ou de iManager.
38	ndsPartitionLocked	Une partition est verrouillée (par exemple, avant la fusion des partitions). Exemple : Création d'une partition à l'aide de ConsoleOne ou de iManager.
39	ndsPartitionUnlocked	Une partition est déverrouillée (par exemple, après la fusion des partitions). Exemple : Création d'une partition à l'aide de ConsoleOne ou de iManager.
40	ndsSchemaSync	Les schémas sont synchronisés. Exemple : Planification de la synchronisation du schéma via ldapsdk schsync.
41	ndsNameCollision	Deux objets résidant sur des serveurs différents portent le même nom (ils *entrent en collision*). Exemple : Désactivation de la synchronisation sortante des serveurs primaire et secondaire d'une arborescence via iMonitor. Ajoutez des objets Utilisateur aux deux serveurs à l'aide des outils LDAP. Puis, activez la synchronisation sortante des deux serveurs via iMonitor.
42	ndsNLMLoaded	Un programme NLM™ est chargé dans NetWare. Cette trappe est uniquement applicable à NetWare. Exemple : chargement ou déchargement de nldap.nlm.
43	ndsChangeModuleState	Un module eDirectory (NLM/DLM) est chargé ou déchargé. Exemple : Chargement ou déchargement du module nldap.
44	ndsLumberDone	Le processus en arrière-plan de contrôle de la connectivité est lancé.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
45	ndsBacklinkProcDone	Le processus de liaison en amont est terminé. Exemple : Configuration de dstrace en vue du lancement de la liaison en amont après une période donnée.
46	ndsServerRename	Un serveur est renommé. Exemple : Utilisation de ldapmodrdn ou ldapsdk pour renommer le serveur.
47	ndsSyntheticTime	Des objets sont créés avec des tampons horaires futurs. Pour synchroniser les serveurs eDirectory, il convient d'utiliser l'heure synthétique. Exemple : Ajout d'un serveur secondaire à l'arborescence via ndsconfig.
48	ndsServerAddressChange	Le contrôleur de connectivité (limber) modifie une adresse de renvoi du serveur. Exemple : modification de l'adresse IP du serveur et redémarrage de ndsd.
49	ndsDSARead	Une entrée est lue. Cette trappe est générée pour toutes les opérations exécutées sur eDirectory. Exemple : Utilisation de ldapsearch pour générer des trappes.
50	ndsLogin	Un utilisateur se logue à eDirectory. Exemple : Login à l'arborescence via ndslogin.
51	ndsChangePassword	Un mot de passe est modifié. Exemple : Modification du mot de passe d'un objet Utilisateur via ldapmodify.
52	ndsLogout	Un utilisateur se délogue de eDirectory. Exemple : Déconnexion de l'arborescence à l'aide du client Novell.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
53	ndsAddReplica	Une réplique est ajoutée à une partition de serveur. Exemple : Ajout d'une réplique à l'arborescence via ndsconfig.
54	ndsRemoveReplica	Une réplique est supprimée. Exemple : Suppression d'une réplique de l'un des serveurs à l'aide de ConsoleOne ou de iManager.
55	ndsSplitPartition	Une partition est divisée. Exemple : Création d'une partition à l'aide de ConsoleOne ou de iManager.
56	ndsJoinPartition	Une partition parente est associée à une partition enfant. Exemple : Création et jonction d'une partition à l'aide de ConsoleOne ou de iManager.
57	ndsChangeReplicaType	Le type de réplique d'une partition est modifié. Exemple : Modification du type de réplique de « réplique maîtresse » en « réplique de type Lecture-écriture ».
58	ndsAddEntry	Un nouvel objet est ajouté. Exemple : Ajout d'un objet Utilisateur à l'aide de ConsoleOne ou de iManager.
59	ndsAbortPartitionOp	Une opération de partition est abandonnée. Exemple : Partitionnement d'un conteneur et abandon de l'opération de partitionnement.
60	ndsRecvReplicaUpdates	Une réplique reçoit une mise à jour lors de la synchronisation. Exemple : Un serveur eDirectory dans une configuration d'arborescence multiserveur demande des mises à jour sur la réplique qu'il détient. Cette opération peut s'effectuer à l'aide de ConsoleOne ou de iManager.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
61	ndsRepairTimeStamps	Les tampons horaires d'une réplique font l'objet d'une réparation. Exemple : Exécution d'une opération de réparation de la DIB pour les tampons horaires à l'aide de dsrepair (ndsrepair sous Linux et UNIX ou NDSCons sous Windows.)
62	ndsSendReplicaUpdates	Une réplique est mise à jour lors de la synchronisation. Exemple : un serveur eDirectory dans une configuration d'arborescence multiserveur envoie des mises à jour sur la réplique qu'il détient. Cette opération peut s'effectuer à l'aide de ConsoleOne ou de iManager.
63	ndsVerifyPass	Un mot de passe est vérifié. Exemple : Lorsque le mot de passe expire, saisissez-le de nouveau pour confirmation à l'invite de modification du mot de passe.
64	ndsBackupEntry	Une entrée est sauvegardée. Exemple : Sauvegarde d'objets Annuaire à l'aide de l'utilitaire dsbackup (ndsbackup sous Linux et UNIX ou NDSCons sous Windows).
65	ndsRestoreEntry	Une entrée est restaurée. Exemple : Restauration des objets Annuaire sauvegardés à l'aide de l'utilitaire dsbackup (ndsbackup sous Linux et UNIX ou NDSCons sous Windows).
66	ndsDefineAttributeDef	Une définition d'attribut est ajoutée au schéma. Exemple : Extension du schéma de l'arborescence eDirectory par l'ajout d'une définition d'attribut. Le schéma peut être étendu lors de l'installation d'une application dépendante de eDirectory, telle que ZENWorks® ou NMAS™. L'extension du schéma peut également s'effectuer via ConsoleOne, iManager ou l'utilitaire d'extension de schéma ndssch sous Linux et UNIX.
67	ndsRemoveAttributeDef	Une définition d'attribut est supprimée du schéma. Exemple : Suppression d'une définition d'attribut du schéma de l'arborescence eDirectory. La suppression du schéma peut également s'effectuer via ConsoleOne, iManager ou l'utilitaire d'extension de schéma ndssch sous Linux et UNIX.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
68	ndsRemoveClassDef	Une définition de classe est supprimée du schéma. Exemple : Suppression d'une définition de classe d'objet du schéma de l'arborescence eDirectory. La suppression de la classe peut également s'effectuer via ConsoleOne, iManager ou l'utilitaire d'extension de schéma ndssch sous Linux et UNIX.
69	ndsDefineClassDef	Une définition de classe est ajoutée au schéma. Exemple : Extension du schéma de l'arborescence eDirectory par l'ajout d'une classe. Le schéma peut être étendu lors de l'installation d'une application dépendante de eDirectory, telle que ZENWorks ou NMAS. L'extension du schéma peut également s'effectuer via ConsoleOne, iManager ou l'utilitaire d'extension de schéma ndssch sous Linux et UNIX.
70	ndsModifyClassDef	Une définition de classe est modifiée. Exemple : Modification d'une classe d'objet ou de définitions d'attribut.
71	ndsResetDSCounters	Les compteurs internes de eDirectory sont réinitialisés.
72	ndsRemoveEntryDir	Un répertoire de fichiers associé à une entrée est supprimé.
73	ndsCompAttributeValue	Les valeurs des attributs sont comparées. Exemple : Comparaison d'une valeur d'attribut à un objet. Exécution d'une opération de recherche LDAP par rapport à un objet Utilisateur pour vérifier si son numéro de téléphone correspond à la valeur entrée.
74	ndsOpenStream	Un attribut de flux est ouvert ou fermé. Exemple : Création ou ouverture d'un flux pour des opérations de lecture ou d'écriture. Création d'un script de login pour un objet Utilisateur. La génération de cette trappe résulte de la création d'un fichier sous le répertoire DIB.
75	ndsListSubordinates	Une opération consistant à lister les entrées subordonnées est exécutée sur un objet Conteneur. Il s'agit d'une recherche sur un niveau. Exemple : À l'aide de ConsoleOne ou de iManager, cliquez sur un objet Conteneur pour lister ses objets subordonnés.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
76	ndsListContainerClasses	Une opération Lister les classes pouvant être contenues est exécutée sur une entrée. Exemple : Pour un objet donné, énumération des classes de conteneurs susceptibles de contenir l'objet. Lorsque la requête porte sur un objet Utilisateur, les classes de conteneurs listées peuvent être les suivantes : Organisation, Unité organisationnelle et Domaine.
77	ndsInspectEntry	Une opération Inspecter l'entrée est exécutée sur une entrée. Exemple : Inspection d'une entrée pour obtenir des informations la concernant et vérifier si des erreurs se sont produites à ce niveau. Cet événement est généré dans le cadre du processus d'arrière-plan Gestionnaire d'attributs (Flat Cleaner) de eDirectory, qui entraîne la génération de cette trappe.
78	ndsResendEntry	Une opération Envoyer à nouveau l'entrée est exécutée sur une entrée. Exemple : Durant une opération de réplication, lors du renvoi d'une entrée en raison de l'échec de l'envoi précédent à cause de la connexion entre les serveurs.
79	ndsMutateEntry	Une opération Muter l'entrée est exécutée sur une entrée. Exemple : Mutation d'une classe d'objet Bindery en classe d'objet Utilisateur.
80	ndsMergeEntries	Deux entrées sont fusionnées. Exemple : Fusion de deux objets Utilisateur. Fusion de l'entrée 2 (ndsEntryName2) avec l'entrée (ndsEntryName).
81	ndsMergeTree	Deux arborescences eDirectory sont fusionnées. Exemple : Fusion de deux arborescences eDirectory via dsmerge (ndsmerge sous Linux et UNIX ou NDSCons sous Windows).
82	ndsCreateSubref	Une référence subordonnée est créée. Exemple : Lorsque vous supprimez la réplique de la partition enfant d'un serveur, la réplique de référence subordonnée est créée automatiquement, ce qui entraîne la génération de cette trappe.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
83	ndsListPartitions	Une opération Répertorier les partitions est exécutée. Exemple : À l'aide de ConsoleOne ou de iManager, dans la vue Partition et schéma, cliquez sur l'objet Serveur eDirectory pour lister les partitions que contient le serveur.
84	ndsReadAttribute	Une valeur d'attribut est lue. Exemple : Exécution d'une opération de recherche sur l'arborescence.
85	ndsReadReferences	Les références d'une entrée sont lues.
86	ndsUpdateReplica	Une opération Mettre à jour la réplique est exécutée sur une réplique de partition. Exemple : Si vous supprimez un utilisateur de l'un des serveurs, l'autre réplique est mise à jour de façon à prendre en compte l'opération de suppression.
87	ndsStartUpdateReplica	Une opération Début de la mise à jour de la réplique est exécutée sur une réplique de partition. Exemple : Si vous supprimez un utilisateur de l'un des serveurs, l'autre réplique est mise à jour de façon à prendre en compte l'opération de suppression.
88	ndsEndUpdateReplica	Une opération Fin de la mise à jour de la réplique est exécutée sur une réplique de partition. Exemple : Si vous supprimez un utilisateur de l'un des serveurs, l'autre réplique est mise à jour de façon à prendre en compte l'opération de suppression.
89	ndsSyncPartition	Une opération Sync. – Partition est exécutée sur une réplique de partition. Exemple : Suppression d'un utilisateur de l'une des partitions, La synchronisation peut être observée à l'aide de ndstrace.
90	ndsSyncSchema	La réplique maîtresse de la racine est invitée à synchroniser son schéma avec le serveur. Exemple : Ajout d'une nouvelle classe via ConsoleOne > Assistant > Schéma, outils LDAP ou utilitaires ndssch.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
91	ndsCreateBackLink	Un lien en amont est créé. (Ce type de lien est créé lorsqu'il est fait référence à un objet qui n'est pas présent au niveau local.) Exemple : dans un scénario multiserveur, création d'une partition contenant certains utilisateurs. La suppression de cette partition de l'un des serveurs entraîne la création d'une référence subordonnée. Un lien en amont est créé pour tous les utilisateurs présents dans la partition supprimée.
92	ndsCheckConsoleOperator	Le processus de liaison en amont vérifie les privilèges de l'opérateur de la console. Cette trappe est uniquement applicable à NetWare.
93	ndsChangeTreeName	Le nom de l'arborescence est modifié. Exemple : Exécution de l'utilitaire de fusion dsmerge/ndsmerge pour renommer l'arborescence.
94	ndsStartJoinPartition	Une opération Début de la jonction est exécutée pour fusionner des partitions. Exemple : Fusion ou jonction de partitions à l'aide de ConsoleOne ou des outils LDAP.
95	ndsAbortJoinPartition	Une opération Joindre les partitions est abandonnée pour arrêter la fusion des partitions. Exemple : Fusion ou jonction de partitions à l'aide de ConsoleOne ou des outils LDAP.
96	ndsUpdateSchema	Une opération Mettre à jour le schéma est exécutée. Exemple : Ajout d'une classe via ConsoleOne > Assistant > Schéma, outils LDAP ou ndssch.
97	ndsStartUpdateSchema	Une opération Début de la mise à jour du schéma est exécutée. Exemple : Ajout d'une classe via ConsoleOne > Assistant > Schéma, outils LDAP ou ndssch.
98	ndsEndUpdateSchema	Une opération Fin de la mise à jour du schéma est exécutée. Exemple : Ajout d'une classe via ConsoleOne > Assistant > Schéma, outils LDAP ou ndssch.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
99	ndsMoveTree	Une opération Déplacer l'arborescence est exécutée. Exemple : déplacement d'une partition d'un conteneur à un autre.
100	ndsReloadDS	DS est de nouveau chargé. Cette trappe est uniquement applicable à NetWare. Exemple : set dstrace=*.
101	ndsConnectToAddress	Une connexion est établie avec une adresse particulière. Exemple : Parcours de larborescence à l'aide de ConsoleOne ou de iManager.
102	ndsSearch	Une opération Rechercher est exécutée. Exemple : Exécution de ldapsearch sur l'arborescence à l'aide des outils LDAP.
103	ndsPartitionStateChange	Une partition est créée ou supprimée. Exemple : Création d'une partition.
104	ndsRemoveBacklink	Des références externes inutilisées sont supprimées et le serveur envoie une requête de suppression de lien en amont au serveur contenant l'objet.
105	ndsLowLevelJoinPartition	Une jonction de faible niveau est exécutée durant les opérations de fusion des partitions. Exemple : fusion ou jonction de partitions à l'aide de ConsoleOne, de iManager ou des outils LDAP.
106	ndsCreateNameBase	Une base de noms eDirectory est créée.
107	ndsChangeSecurityEquals	L'attribut Équivalents de sécurité est modifié. Exemple : Modification de l'équivalent de sécurité d'un utilisateur pour le rendre équivalent à Admin à l'aide de ConsoleOne ou de iManager.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
108	ndsRemoveEntry	Une entrée est supprimée de eDirectory. Exemple : Suppression d'un utilisateur à l'aide de ConsoleOne ou de iManager.
109	ndsCRCFailure	Un échec CRC se produit au cours de la reconstitution de requêtes NCP fragmentées.
110	ndsModifyEntry	Une entrée de eDirectory est modifiée. Exemple : Modification des attributs d'un utilisateur à l'aide de ConsoleOne ou de iManager.
111	ndsNewSchemaEpoch	Le schéma est réinitialisé via DSRepair. Exemple : Création d'une période de schéma à l'aide de ndsrepair -S -Ad sous Linux et UNIX.
112	ndsLowLevelSplitPartition	Une division de faible niveau est exécutée lors de la création d'une partition. Exemple : Création d'une partition à l'aide de ConsoleOne, de iManager ou des outils LDAP.
113	ndsReplicaInTransition	Une réplique est ajoutée ou supprimée.
114	ndsAclModify	L'ayant droit d'un objet est modifié [un objet ACL (Liste de contrôle d'accès) est modifié]. Exemple : Ajout, modification ou suppression de l'ayant droit d'un objet via les outils LDAP, ICE, ConsoleOne ou iManager.
115	ndsLoginEnable	Le serveur reçoit une requête visant à activer le compte utilisateur. Exemple : Activation de l'attribut Compte désactivé via les outils LDAP, ICE, ConsoleOne ou iManager.
116	ndsLoginDisable	Le serveur reçoit une requête visant à désactiver le compte utilisateur. Exemple : Désactivation de l'attribut Compte désactivé via les outils LDAP, ICE, ConsoleOne ou iManager.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
117	ndsDetectIntruder	Un compte utilisateur est verrouillé suite à la détection d'un intrus. Exemple : Verrouillage au moyen de l'attribut Intrus via les outils LDAP, ICE, ConsoleOne ou iManager.
2001	ndsServerStart	Le sous-agent réussit à se reconnecter au serveur eDirectory. Cette trappe comporte deux variables : ◆ ndsTrapTime: variable contenant le nombre total de secondes depuis minuit (24:00) du 1er janvier 1970 GMT (TU), date à laquelle le sous-agent a réussi à se reconnecter au serveur eDirectory. ◆ ndsServerName: serveur eDirectory auquel le sous-agent a réussi à se reconnecter. Exemple : arrêt et démarrage du serveur eDirectory alors que le sous-agent est en cours d'exécution.
2002	ndsServerStop	Le sous-agent perd sa connexion au serveur eDirectory. Cette trappe comporte deux variables : ◆ ndsTrapTime: variable contenant le nombre total de secondes depuis minuit (24:00) du 1er janvier 1970 GMT (TU), date à laquelle le sous-agent a perdu sa connexion au serveur eDirectory. ◆ ndsServerName: serveur eDirectory dont le sous-agent s'est déconnecté. Exemple : arrêt du serveur eDirectory alors que le sous-agent est en cours d'exécution.

Accès aux attributs codés

eDirectory 8.8 (ou version ultérieure) permet de coder des données sensibles spécifiques pour les protéger lorsqu'elles sont stockées sur le disque et lorsque vous tentez d'y accéder sur le réseau. Vous pouvez spécifier si vous souhaitez toujours accéder aux attributs codés via un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Accès aux attributs codés », page 243.

Les événements Valeur NDS sont bloqués si vous avez demandé de toujours exiger un canal sécurisé pour accéder aux attributs codés. Les trappes liées à des événements Valeur auront la donnée de valeur NULL et une erreur -6089 sera renvoyée indiquant que vous avez besoin d'un canal sécurisé pour obtenir la valeur d'attribut codé. Les trappes qui auront la donnée de valeur NULL sont les suivantes :

- ndsAddValue
- ndsDeleteValue
- ndsDeleteAttribute

Configuration des trappes

La méthode de configuration des trappes diffère d'une plate-forme à l'autre.

Plate-forme	Utilitaire
NetWare	dssnmpsa
Windows	ndssnmpcfg
Linux et UNIX	ndssnmpconfig

NetWare

L'utilitaire dssnmpsa permet de configurer les trappes sous NetWare. Il réside dans le répertoire sys:\etc\. Cet utilitaire permet d'activer et de désactiver les trappes, de définir l'intervalle de temps des trappes individuelles, de définir un intervalle de temps par défaut, d'activer des trappes pour les opérations en échec et de lister toutes les trappes.

Pour obtenir de l'aide sur l'utilisation de dssnmpsa, entrez **`help dssnmpsa`** dans la ligne de commande.

Syntaxe :

dssnmpsa *commandes de trappes*

Pour plus d'informations sur les commandes de trappes sous NetWare, reportez-vous à la section « Commandes de trappes NetWare », page 494.

Commandes de trappes NetWare

Commandes de trappes	Description	Syntaxe
DISABLE	La désactivation d'une trappe signifie que la NMS ne reçoit pas les trappes, bien que ces dernières soient générées.	dssnmpsa “DISABLE *Spécification_trappe*" Il peut s'agir de l'une des spécifications suivantes : Pour désactiver des trappes spécifiques, par exemple les trappes10, 11 et 100 : dssnmpsa "DISABLE 10, 11, 100" Pour désactiver toutes les trappes, excepté les trappes10,11 et100 : dssnmpsa "DISABLE ID != 10, 11, 100" Pour désactiver toutes les trappes comprises dans la plage allant de 20 à 30 : dssnmpsa "DISABLE 20-29" Pour désactiver toutes les trappes : dssnmpsa "DISABLE ALL"

Commandes de trappes	Description	Syntaxe
ENABLE	L'activation d'une trappe signifie que la NMS reçoit les trappes lorsqu'elles sont générées.	dssnmpsa " ENABLE *Spécification_trappe*" Il peut s'agir de l'une des spécifications suivantes : Pour activer des trappes spécifiques, par exemple les trappes10,11 et 100 : dssnmpsa "ENABLE 10, 11, 100" Pour activer toutes les trappes, excepté les trappes10, 11 et 100 : dssnmpsa "ENABLE ID != 10, 11, 100" Pour activer toutes les trappes comprises dans la plage allant de 20 à 30 : dssnmpsa "ENABLE 20-29" Pour activer toutes les trappes : dssnmpsa "ENABLE ALL"
INTERVAL	Cet utilitaire permet de définir et d'afficher l'intervalle de temps. Celui-ci correspond au nombre de secondes précédant l'envoi de trappes en double. Sa valeur doit être comprise entre 0 et 2592000 secondes. Si ce n'est pas le cas, l'intervalle de temps par défaut est pris en compte. S'il présente la valeur zéro, toutes les trappes sont envoyées.	Pour afficher l'intervalle de temps : dssnmpsa"213,240,79 INTERVAL" Pour définir l'intervalle de temps entre plusieurs trappes (par exemple, pour définir un intervalle de temps de 5 entre les trappes 12, 17 et 101) : dssnmpsa "12 17 101 INTERVAL 5" Pour afficher l'intervalle de temps par défaut : dssnmpsa "DEFAULT INTERVAL" Pour définir l'intervalle de temps par défaut : dssnmpsa "DEFAULT INTERVAL = 10"

Commandes de trappes	Description	Syntaxe
LIST	Cet utilitaire permet d'afficher des listes de numéros de trappe répondant à des critères spécifiés.	dssnmpsa LIST *Spécification_trappe* La valeur *Spécification_trappe* permet de spécifier des groupes de numéros de trappe et peut être suivie de l'un des mots-clés suivants : ALL, ENABLED, DISABLED, FAILED ou une expression logique Exemples : Pour lister toutes les trappes activées par leur nom : dssnmpsa LIST ENABLED Pour lister toutes les trappes désactivées par nom : dssnmpsa LIST DISABLED Pour lister toutes les trappes (117) par nom : dssnmpsa LIST ALL Pour lister des trappes spécifiques telles que 12, 224 et300 par nom : dssnmpsa LIST ID = 12,224,300 Pour lister toutes les trappes, excepté celles sélectionnées, telles que 12, 224 et 300 par nom : dssnmpsa LIST ID != 12,224,300 Pour lister toutes les trappes mises en échec par nom : dssnmpsa LIST FAILED

Commandes de trappes	Description	Syntaxe
READ_CFG	Cette commande permet de modifier la configuration de l'annuaire à partir du fichier de configuration ndstrap.cfg. Toutes les modifications spécifiées dans ce fichier sont alors appliquées. Cet utilitaire sert principalement à regrouper plusieurs commandes dans le fichier ndstrap.cfg et à exécuter l'opération en une fois. Le fichier ndstrap.cfg réside dans le répertoire sys:\etc\. Il indique les paramètres opérationnels à utiliser pour configurer les trappes et constitue un moyen de configurer le fonctionnement des trappes SNMP. Ce fichier est lu à chaque fois que l'utilitaire de configuration de trappes dssnmpsa est exécuté avec la commande READ_CFG.	dssnmpsa "READ_CFG"
FAILURE	Cette commande permet de lister toutes les trappes activées pour être mises en échec. Lorsqu'un événement échoue, une trappe d'échec est générée. **Remarque :** si la trappe est mise en échec, puis désactivée avant d'être à nouveau activée via la commande enable trapid, elle est alors activée en cas de réussite, et non d'échec.	dssnmpsa " FAILURE *Spécification_trappe*" La valeur *Spécification_trappe* comporte un ou plusieurs numéros de trappe séparés par une virgule ou un espace, du mot-clé ALL ou d'une expression logique. Exemples : Pour mettre plusieurs trappes en échec : dssnmpsa "FAILURE 10,11,100" Pour mettre toutes les trappes en échec, à l'exception de celles mentionnées : dssnmpsa "FAILURE ID != 24,30" Pour mettre toutes les trappes en échec : dssnmpsa "FAILURE ALL"

Windows

L'utilitaire ndssnmpcfg permet de configurer les trappes sous Windows. Il réside dans le répertoire *chemin_installation*\snmp\. Cet utilitaire permet d'activer et de désactiver les trappes, de définir l'intervalle de temps des trappes individuelles, de définir un intervalle de temps par défaut, d'activer des trappes pour les opérations en échec et de lister toutes les trappes.

Syntaxe:

ndssnmpcfg -h [*nom_hôte*[*:port*]] -p *mot_de_passe* -a *FDN_utilisateur* -c *commande*

Paramètre	Description
-h	Nom d'hôte DNS ou adresse IP
-p	Mot de passe d'authentification du FDN utilisateur
-a	Nom distinctif complet d'un utilisateur disposant de droits d'administrateur
-c	Commandes de trappes (Reportez-vous à la section « Commandes de trappes Windows », page 498.)

Commandes de trappes Windows

Commandes de trappes	Description	Syntaxe
DISABLE	La désactivation d'une trappe signifie que la NMS ne reçoit pas de trappes, bien que ces dernières soient générées.	Pour désactiver des trappes spécifiques, par exemple les trappes 10, 11 et 100 : ndssnmpcfg "DISABLE 10, 11, 100" Pour désactiver toutes les trappes, excepté les trappes 10, 11 et 100 : ndssnmpcfg "DISABLE ID != 10, 11, 100" Pour désactiver toutes les trappes comprises dans la plage allant de 20 à 30 : ndssnmpcfg "DISABLE 20-29" Pour désactiver toutes les trappes : ndssnmpcfg "DISABLE ALL"

Commandes de trappes	Description	Syntaxe
ENABLE	L'activation d'une trappe signifie que la NMS reçoit les trappes lorsqu'elles sont générées.	ndssnmpcfg "ENABLE *Spécification_trappe*" Il peut s'agir de l'une des spécifications suivantes : Pour activer des trappes spécifiques, par exemple les trappes10, 11 et 100 : ndssnmpcfg "ENABLE 10, 11, 100" Pour activer toutes les trappes, excepté les trappes10,11 et 100 : ndssnmpcfg "ENABLE ID != 10, 11, 100" Pour activer toutes les trappes comprises dans la plage allant de 20 à 30 : ndssnmpcfg "ENABLE 20-29" Pour activer toutes les trappes : ndssnmpcfg "ENABLE ALL"
INTERVAL	Cet utilitaire permet de définir et d'afficher l'intervalle de temps. Celui-ci correspond au nombre de secondes précédant l'envoi de trappes en double. Sa valeur doit être comprise entre 0 et 2592000 secondes. Si ce n'est pas le cas, l'intervalle de temps par défaut est pris en compte. S'il présente la valeur zéro, toutes les trappes sont envoyées.	Pour afficher l'intervalle de temps : ndssnmpcfg "213,240,79 INTERVAL" Pour définir l'intervalle de temps entre plusieurs trappes (par exemple, pour définir un intervalle de temps de 5 entre les trappes 12, 17 et 101) : ndssnmpcfg "12 17 101 INTERVAL 5" Pour afficher l'intervalle de temps par défaut : ndssnmpcfg "DEFAULT INTERVAL" Pour définir l'intervalle de temps par défaut : ndssnmpcfg "DEFAULT INTERVAL=10"

Commandes de trappes	Description	Syntaxe
LIST	Cet utilitaire permet d'afficher des listes de numéros de trappe répondant à des critères spécifiés.	ndssnmpcfg LIST *Spécification_trappe* La valeur *Spécification_trappe* permet de spécifier des groupes de numéros de trappe et peut être suivie de l'un des mots-clés suivants : ALL, ENABLED, DISABLED, FAILED ou une expression logique Exemples : Pour lister toutes les trappes activées par leur nom : ndssnmpcfg LIST ENABLED Pour lister toutes les trappes désactivées par nom : ndssnmpcfg LIST DISABLED Pour lister toutes les trappes (117) par nom : ndssnmpcfg LIST ALL Pour lister des trappes spécifiques telles que 12, 224 et 300 par nom : ndssnmpcfg LIST ID = 12,224,300 Pour lister toutes les trappes, excepté celles sélectionnées, telles que 12, 224 et 300 par nom : ndssnmpcfg LIST ID != 12,224,300 Pour lister toutes les trappes mises en échec par nom : ndssnmpcfg LIST FAILED

Commandes de trappes	Description	Syntaxe
READ_CFG	Cette commande permet de modifier la configuration de l'annuaire à partir du fichier de configuration ndstrap.cfg. Toutes les modifications spécifiées dans ce fichier sont alors appliquées. Cet utilitaire sert principalement à regrouper plusieurs commandes dans le fichier ndstrap.cfg et à exécuter l'opération en une fois. Le fichier ndstrap.cfg réside à l'emplacement *répertoire_installation*\SNMP Il indique les paramètres opérationnels à utiliser pour configurer les trappes et constitue un moyen de configurer le fonctionnement des trappes SNMP. Ce fichier est lu à chaque fois que l'utilitaire de configuration de trappes ndssnmpcfg est exécuté avec la commande READ_CFG.	ndssnmpcfg "READ_CFG"
FAILURE	Cette commande permet de lister toutes les trappes activées pour être mises en échec. Lorsqu'un événement échoue, une trappe d'échec est générée. **Remarque :** si la trappe est mise en échec, puis désactivée avant d'être à nouveau activée via la commande enable trapid, elle est alors activée en cas de réussite, et non d'échec.	ndssnmpcfg "FAILURE *Spécification_trappe*" La valeur *Spécification_trappe* comporte un ou plusieurs numéros de trappe séparés par une virgule ou un espace, du mot-clé ALL ou d'une expression logique. Exemples : Pour mettre plusieurs trappes en échec : ndssnmpcfg "FAILURE 10,11,100" Pour mettre toutes les trappes en échec, à l'exception de celles mentionnées : ndssnmpcfg "FAILURE ID != 24,30" Pour mettre toutes les trappes en échec : ndssnmpcfg "FAILURE ALL"

Linux et UNIX

L'utilitaire ndssnmpconfig permet de configurer des trappes sous Linux et UNIX. Il réside dans le répertoire /etc/ndssnmp/. Cet utilitaire permet d'activer et de désactiver les trappes, de définir l'intervalle de temps des trappes individuelles, de définir un intervalle de temps par défaut, d'activer des trappes pour les opérations en échec et de lister toutes les trappes.

Syntaxe :

ndssnmpconfig -h [*nom_hôte*[*:port*]] -p *mot_de_passe* -a *FDN_utilisateur* -c *commande*

Paramètre	Description
-h	Nom d'hôte DNS ou adresse IP
-p	Mot de passe d'authentification du FDN utilisateur
-a	Nom distinctif complet d'un utilisateur disposant de droits d'administrateur
-c	Commandes de trappes (Reportez-vous à la section « Commandes de trappes Linux et UNIX », page 502.)

Commandes de trappes Linux et UNIX

Commandes de trappes	Description	Syntaxe
DISABLE	La désactivation d'une trappe signifie que la NMS ne reçoit pas de trappes, bien que ces dernières soient générées.	Pour désactiver des trappes spécifiques, par exemple les trappes 10, 11 et 100 : ndssnmpconfig "DISABLE 10, 11, 100" Pour désactiver toutes les trappes, excepté les trappes 10, 11 et 100 : ndssnmpconfig "DISABLE ID != 10, 11, 100" Pour désactiver toutes les trappes comprises dans la plage allant de 20 à 30 : ndssnmpconfig "DISABLE 20-29" Pour désactiver toutes les trappes : ndssnmpconfig "DISABLE ALL"

Commandes de trappes	Description	Syntaxe
ENABLE	L'activation d'une trappe signifie que la NMS reçoit les trappes lorsqu'elles sont générées.	ndssnmpconfig "ENABLE *Spécification_trappe*" Il peut s'agir de l'une des spécifications suivantes : Pour activer des trappes spécifiques, par exemple les trappes 10, 11 et 100: ndssnmpconfig "ENABLE 10, 11, 100" Pour activer toutes les trappes, excepté les trappes 10, 11 et 100: ndssnmpconfig "ENABLE ID != 10, 11, 100" Pour activer toutes les trappes comprises dans la plage allant de 20 à 30 : ndssnmpconfig "ENABLE 20-29" Pour activer toutes les trappes : ndssnmpconfig "ENABLE ALL"
INTERVAL	Cet utilitaire permet de définir et d'afficher l'intervalle de temps. Celui-ci correspond au nombre de secondes précédant l'envoi de trappes en double. Sa valeur doit être comprise entre 0 et 2592000 secondes. Si ce n'est pas le cas, l'intervalle de temps par défaut est pris en compte. S'il présente la valeur zéro, toutes les trappes sont envoyées.	Pour afficher l'intervalle de temps : ndssnmpconfig "213,240,79 INTERVAL" Pour définir l'intervalle de temps entre plusieurs trappes (par exemple, pour définir un intervalle de temps de 5 entre les trappes12,17 et101): ndssnmpconfig "12 17 101 INTERVAL 5" Pour afficher l'intervalle de temps par défaut : ndssnmpconfig "DEFAULT INTERVAL" Pour définir l'intervalle de temps par défaut : ndssnmpconfig "DEFAULT INTERVAL=10"

Commandes de trappes	Description	Syntaxe
LIST	Cet utilitaire permet d'afficher des listes de numéros de trappe répondant à des critères spécifiés.	ndssnmpconfig LIST <*Spécification_trappe*> La valeur *Spécification_trappe* permet de spécifier des groupes de numéros de trappe et peut être suivie de l'un des mots-clés suivants : ALL, ENABLED, DISABLED, FAILED ou une expression logique Exemples : Pour lister toutes les trappes activées par leur nom : ndssnmpconfig LIST ENABLED Pour lister toutes les trappes désactivées par nom : ndssnmpconfig LIST DISABLED Pour lister toutes les trappes (117) par nom : ndssnmpconfig LIST ALL Pour lister des trappes spécifiques telles que 12, 224 et300 par nom : ndssnmpconfig LIST ID = 12,224,300 Pour lister toutes les trappes, excepté celles sélectionnées, telles que 12, 224 et300 par nom : ndssnmpconfig LIST ID != 12,224,300 Pour lister toutes les trappes mises en échec par nom : ndssnmpconfig LIST FAILED

Commandes de trappes	Description	Syntaxe
READ_CFG	Cette commande permet de modifier la configuration de l'annuaire à partir du fichier de configuration ndstrap.cfg. Toutes les modifications spécifiées dans ce fichier sont alors appliquées. Cet utilitaire sert principalement à regrouper plusieurs commandes dans le fichier ndstrap.cfg et à exécuter l'opération en une seule fois. Ce fichier est enregistré dans /etc/ndssnmp/. Il indique les paramètres opérationnels à utiliser pour configurer les trappes et constitue un moyen de configurer le fonctionnement des trappes SNMP. Ce fichier est lu à chaque fois que l'utilitaire de configuration de trappes ndssnmpcfg est exécuté avec la commande READ_CFG.	ndssnmpconfig "READ_CFG"
FAILURE	Cette commande permet de lister toutes les trappes activées pour être mises en échec. Lorsqu'un événement échoue, une trappe d'échec est générée. **Remarque :** si la trappe est mise en échec, puis désactivée avant d'être à nouveau activée via la commande enable trapid, elle est alors activée en cas de réussite, et non d'échec.	ndssnmpconfig "FAILURE *Spécification_trappe*" La valeur *Spécification_trappe* comporte un ou plusieurs numéros de trappe séparés par une virgule ou un espace, du mot-clé ALL ou d'une expression logique. Exemples : Pour mettre plusieurs trappes en échec : ndssnmpconfig "FAILURE 10,11,100" Pour mettre toutes les trappes en échec, à l'exception de celles mentionnées : ndssnmpconfig "FAILURE ID != 24,30" Pour mettre toutes les trappes en échec : ndssnmpconfig "FAILURE ALL"

Statistiques

- « ndsDbCache », page 506
- « ndsDbConfig », page 507
- « ndsProtoIfOps », page 507
- « ndsServerInt », page 509

Objets gérés dans l'Annuaire	Description
ndsDbSrvApplIndex	Index permettant d'identifier de façon unique l'application serveur eDirectory.
ndsDbDibSize	Taille actuelle en Ko de la base de données eDirectory.
ndsDbBlockSize	Taille des blocs en Ko de la base de données eDirectory.
ndsDbEntryCacheMaxSize	Informations relatives à la taille maximale en Ko du cache d'entrées.
ndsDbBlockCacheMaxSize	Informations relatives à la taille maximale en Ko du cache de blocs.
ndsDbEntryCacheCurrentSize	Informations relatives à la taille actuelle du cache d'entrées.
ndsDbBlockCacheCurrentSize	Informations relatives à la taille actuelle du cache de blocs.
ndsDbEntryCacheCount	Informations relatives au nombre d'entrées du cache.
ndsDbBlockCacheCount	Informations relatives au nombre de blocs du cache.
ndsDbEntryCacheOldVerCount	Informations relatives aux entrées de la version précédente du cache.
ndsDbBlockCacheOldVerCount	Informations relatives aux blocs de la version précédente du cache.
ndsDbEntryCacheOldVerSize	Informations relatives à la taille de la version précédente du cache d'entrées.
ndsDbBlockCacheOldVerSize	Informations relatives à la taille de la version précédente du cache de blocs.
ndsDbEntryCacheHits	Informations relatives au nombre d'occurrences d'entrées.
ndsDbBlockCacheHits	Informations relatives au nombre d'occurrences de blocs.
ndsDbEntryCacheHitLooks	Informations relatives au nombre d'entrées examinées pour trouver des occurrences.
ndsDbBlockCacheHitLooks	Informations relatives au nombre de blocs examinés pour trouver des occurrences.
ndsDbEntryCacheFaults	Informations relatives au nombre de pannes d'entrées.
ndsDbBlockCacheFaults	Informations relatives au nombre de pannes de blocs.
ndsDbEntryCacheFaultLooks	Informations relatives au nombre d'entrées examinées pour déterminer les occurrences manquantes.
ndsDbBlockCacheFaultLooks	Informations relatives au nombre de blocs examinés pour déterminer les occurrences manquantes.

ndsDbConfig

Objets gérés dans l'Annuaire	Description
ndsDbCfgSrvApplIndex	Index permettant d'identifier de façon unique l'application serveur eDirectory.
ndsDbCfgDynamicCacheAdjust	Informations indiquant si l'ajustement dynamique du cache est activé ou désactivé. 0 = désactivé 1 = activé
ndsDbCfgDynamicCacheAdjustPercent	Informations sur le paramètre de pourcentage d'ajustement dynamique du cache de mémoire disponible.
ndsDbCfgDynamicCacheAdjustMin	Informations sur le paramètre de valeur minimale d'ajustement dynamique du cache. Il s'agit des valeurs de contraintes relatives à la taille du cache exprimées en Ko.
ndsDbCfgDynamicCacheAdjustMinToLeave	Informations relatives à la valeur minimale de l'ajustement dynamique du cache exprimée en Ko à soustraire de la taille totale de la mémoire disponible exprimée en Ko.
ndsDbCfgHardLimitCacheAdjust	Informations indiquant si l'ajustement de la limite stricte du cache est activé ou désactivé. 0 = désactivé 1 = activé
ndsDbCfgHardLimitCacheAdjustMax	Informations relatives à la taille maximale du cache exprimée en Ko. Il s'agit d'un paramètre de limite stricte.
ndsDbCfgBlockCachePercent	Informations relatives au pourcentage du cache de blocs.
ndsDbCfgCacheAdjustInterval	Informations relatives à l'intervalle d'ajustement du cache en secondes.
ndsDbCfgCacheCleanupInterval	Informations relatives à l'intervalle de nettoyage du cache en secondes.
ndsDbCfgPermanentSettings	Informations indiquant si les paramètres permanents sont activés ou désactivés. 0 = désactivé 1 = activé

ndsProtoIfOps

Objets gérés dans l'Annuaire	Description
ndsProtoIfSrvApplIndex	Index permettant d'identifier de façon unique l'application serveur eDirectory.
ndsProtoIfIndex	Index permettant d'identifier de façon unique une entrée correspondant à une interface de protocole du serveur eDirectory.
ndsProtoIfDescription	Informations relatives au port utilisé par l'interface de protocole DS.
ndsProtoIfUnauthBinds	Nombre de requêtes de liaison non authentifiées/ anonymes reçues.

Objets gérés dans l'Annuaire	Description
ndsProtoIfSimpleAuthBinds	Nombre de requêtes de liaison qui ont été authentifiées à l'aide de procédures simples d'authentification avec lesquelles le mot de passe est envoyé sur le réseau en format codé ou en texte clair.
ndsProtoIfStrongAuthBinds	ndsProtoIfStrongAuthBinds Nombre de requêtes de liaison authentifiées à l'aide des procédures d'authentification supérieures SASL et X.500. Ceci englobe les liaisons qui ont été authentifiées à l'aide de procédures d'authentification externes.
ndsProtoIfBindSecurityErrors	Nombre de requêtes de liaison qui ont été rejetées en raison d'une authentification inappropriée ou de références non valides.
ndsProtoIfInOps	Nombre de requêtes reçues des agents utilisateurs d'annuaire ou d'autres serveurs eDirectory.
ndsProtoIfReadOps	Nombre de requêtes de lecture reçues.
ndsProtoIfCompareOps	Nombre de requêtes de comparaison reçues.
ndsProtoIfAddEntryOps	Nombre de requêtes addEntry reçues.
ndsProtoIfRemoveEntryOps	Nombre de requêtes removeEntry reçues.
ndsProtoIfModifyEntryOps	Nombre de requêtes modifyEntry reçues.
ndsProtoIfModifyRDNOps	Nombre de requêtes modifyRDN reçues.
ndsProtoIfListOps	Nombre de requêtes de liste reçues.
ndsProtoIfSearchOps	Nombre de requêtes de recherche (portant sur un objet de base, sur un niveau ou sur l'ensemble de la sous-arborescence) reçues.
ndsProtoIfOneLevelSearchOps	Nombre de requêtes de recherche reçues portant sur un niveau.
ndsProtoIfWholeSubtreeSearchOps	Nombre de requêtes de recherche reçues portant sur l'ensemble de la sous-arborescence.
ndsProtoIfExtendedOps	Nombre d'opérations avancées.
ndsProtoIfReferrals	Nombre de renvois retournés comme réponse aux requêtes d'opérations.
ndsProtoIfChainings	Nombre d'opérations réacheminées par ce serveur eDirectory aux autres serveurs eDirectory.
ndsProtoIfSecurityErrors	Nombre de requêtes reçues qui ne répondent pas aux conditions de sécurité requises.
ndsProtoIfErrors	Nombre de requêtes qui n'ont pas pu être traitées en raison d'erreurs autres que celles liées à la sécurité et aux renvois. Une opération partiellement traitée n'est pas comptabilisée comme une erreur. Les erreurs portent sur l'attribution des noms, les mises à jour, les attributs et les services.

Objets gérés dans l'Annuaire	Description
ndsProtoIfReplicationUpdatesIn	Nombre de mises à jour de réplications récupérées ou reçues par les serveurs eDirectory.
ndsProtoIfReplicationUpdatesOut	Nombre de mises à jour de réplication envoyées aux serveurs eDirectory ou exécutées par les eDirectory.
ndsProtoIfInBytes	Trafic entrant, en octets, sur l'interface. Cela comprend les requêtes des agents utilisateurs d'annuaire ainsi que les réponses des autres serveurs eDirectory.
ndsProtoIfOutBytes	Trafic sortant, en octets, sur l'interface. Comprend les réponses aux agents utilisateurs d'annuaire et aux serveurs eDirectory ainsi que les requêtes adressées à d'autres serveurs eDirectory.

ndsServerInt

Objets gérés dans l'Annuaire	Description
ndsSrvIntSrvApplIndex	Index permettant d'identifier de façon unique une application serveur eDirectory.
ndsSrvIntProtoIfIndex	Index permettant d'identifier de façon unique une entrée correspondant à une interface de protocole du serveur eDirectory.
ndsSrvIntIndex	Associé aux objets ndsSrvIntSrvApplIndex et ndsSrvIntProtoIfIndex, cet objet constitue une clé unique permettant d'identifier la ligne conceptuelle qui contient des informations utiles l'interaction (la tentative d'interaction) entre le serveur eDirectory (correspondant à applIndex) et un serveur eDirectory homologue utilisant un protocole particulier.
ndsSrvIntURL	URL du serveur eDirectory homologue.
ndsSrvIntTimeOfCreation	Nombre total de secondes depuis minuit (24:00) du 1er janvier 1970 GMT (TU), date à laquelle cette ligne a été créée.
ndsSrvIntTimeOfLastAttempt	Nombre total de secondes depuis minuit (24:00) du 1er janvier 1970 GMT (TU), date à laquelle la dernière tentative de contact avec le serveur eDirectory homologue a été effectuée.
ndsSrvIntTimeOfLastSuccess	Nombre total de secondes depuis minuit (24:00) du 1er janvier 1970 GMT (TU), date à laquelle la dernière tentative de contact avec le serveur eDirectory homologue a abouti.
ndsSrvIntFailuresSinceLastSuccess	Nombre d'échecs depuis la dernière tentative réussie de contact avec le serveur eDirectory homologue. Si aucune tentative n'a abouti, ce compteur totalise le nombre d'échecs depuis que cette entrée a été créée.

Objets gérés dans l'Annuaire	Description
ndsSrvIntFailures	Échecs cumulés des tentatives de contact du serveur eDirectory homologue depuis la création de cette entrée.
ndsSrvIntSuccesses	Réussites cumulées des tentatives de contact du serveur eDirectory homologue depuis la création de cette entrée.

Dépannage

Les fichiers journaux sont mis à jour et permettent ainsi de résoudre les problèmes qui se présentent. Ils contiennent des informations sur les erreurs qui se produisent et peuvent vous aider à résoudre les problèmes.

Pour plus d'informations, reportez-vous à « Troubleshooting SNMP » (Dépannage du protocole SNMP).

Plate-forme	Sous-agent	Serveur	Agent principal
Windows NT/2000	*répertoire_installation*\nds\dssnmpsa.log	r*épertoire_installation*\nds\dssnmpsrv.log	Non applicable
Solaris	/var/opt/novell/eDirectory/log/ndssnmpsa.log	/var/opt/novell/eDirectory/log/ndsd.log	/var/adm/messages
Linux	/var/opt/novell/eDirectory/log/ndssnmpsa.log	/var/opt/novell/eDirectory/log/ndsd.log	/var/log/messages
AIX	/var/opt/novell/eDirectory/log/ndssnmpsa.log	/var/opt/novell/eDirectory/log/ndsd.log	/var/adm/messages
HP-UX	/var/opt/novell/eDirectory/log/ndssnmpsa.log	/var/opt/novell/eDirectory/log/ndsd.log	Agent principal net-snmp-5.0.8 : /usr/adm/snmpd.log Agent NAA : /var/adm/snmpd.log

16 Gestion de Novell eDirectory

Pour que Novell® eDirectory™ fonctionne de manière optimale, il est impératif de tenir à jour l'annuaire en vérifiant régulièrement son état de santé et de mettre à niveau ou de remplacer le matériel lorsque cela s'avère nécessaire.

Ce chapitre traite des sujets de gestion suivants :

Performances

- « Amélioration des performances de eDirectory », page 511
- « Amélioration des performances de eDirectory sur les systèmes Linux, Solaris, AIX et HP-UX », page 520
- « Amélioration des performances de chargement par lots », page 526

Vérifications de l'état de santé

- « Vérification de l'état de santé de eDirectory », page 531
- « Ressources de surveillance », page 534

Remplacements de matériel

- « Mise à niveau du matériel ou remplacement d'un serveur », page 534

Récupération de eDirectory

- « Restauration de eDirectory après une panne matérielle », page 542

Amélioration des performances de eDirectory

Le paramètre le plus important en matière de performances de eDirectory est le cache. Dans les versions antérieures des NDS®, vous pouviez spécifier une limite de cache de blocs pour réguler la quantité de mémoire utilisée par l'annuaire pour le cache. La valeur par défaut était de 8 Mo de RAM pour le cache.

Avec eDirectory 8.5 ou version ultérieure, vous pouvez spécifier une limite de cache de blocs et une limite de cache d'entrées. Disponible dans les versions précédentes des NDS, le cache de blocs met uniquement en cache des blocs physiques de la base de données. Nouvelle fonction de eDirectory 8.5, le cache d'entrées met en cache les entrées logiques de la base de données. Le caching des entrées réduit la durée de traitement nécessaire à l'instanciation des entrées en mémoire depuis le cache de blocs.

Bien que ces deux caches soient parfois redondants, chacun est conçu pour améliorer l'exécution d'opérations particulières. Le cache de blocs s'avère plus utile dans les opérations de mise à jour. Le cache d'entrées est plus utile dans des opérations qui exigent que l'arborescence eDirectory soit parcourue par lecture des entrées, par exemple lors d'une résolution de nom.

Les caches d'entrées et de blocs sont tous deux utiles pour améliorer l'exécution des requêtes. Le cache de blocs accélère la recherche dans les index. Le cache d'entrées accélère la récupération des entrées référencées dans un index.

Vous trouverez ci-après les paramètres par défaut de eDirectory 8.8 :

- Si le serveur sur lequel vous installez eDirectory ne dispose pas d'une réplique, la valeur par défaut est limitée à 16 Mo de mémoire, dont 8 Mo pour le cache de blocs et 8 Mo pour le cache d'entrées.

  Pour plus d'informations, reportez-vous à la section « Présentation de la limite de mémoire stricte », page 513.

- Si le serveur comporte une réplique, la valeur par défaut correspond à une limite de mémoire disponible de 51 %, ajustée de manière dynamique. Le seuil minimal est de 8 Mo et le seuil maximal de 24 Mo disponibles.

  Pour plus d'informations, reportez-vous à la section « Présentation de la limite à ajustement dynamique », page 512.

Répartition de la mémoire entre caches d'entrées et de blocs

Avec un cache d'entrées et un cache de blocs, la mémoire totale disponible pour le caching est partagée par les deux caches. Il s'agit par défaut d'une répartition égale. Pour conserver la quantité de cache de blocs disponible dans les versions antérieures des NDS 8, vous devez doubler la taille totale du cache de eDirectory. Si vous utilisez le cache pour améliorer les performances d'importation LDIF par exemple, vous pouvez doubler la taille totale du cache ou modifier les paramètres par défaut du cache. Pour modifier les paramètres par défaut du cache, reportez-vous à la section « Configuration des limites à ajustement dynamique et de mémoire stricte », page 513.

Plus le nombre de blocs et d'entrées susceptibles d'être mis en cache est élevé, meilleures sont les performances globales. L'idéal est de mettre en cache la base de données entière dans les caches de blocs et d'entrées, bien que cette procédure soit impossible pour les bases de données volumineuses. En règle générale, essayez, autant que possible, de vous rapprocher d'un rapport 1:1 entre cache de blocs et ensemble DIB. Concernant le cache d'entrées, il convient d'approcher le plus possible un rapport 1:2 ou 1:4. Pour obtenir des performances optimales, dépassez ces rapports.

Utilisation des paramètres par défaut du cache

eDirectory propose deux méthodes pour contrôler la consommation de mémoire cache : une limite à ajustement dynamique et une limite de mémoire stricte. Les deux méthodes peuvent être utilisées, mais pas simultanément car elles s'excluent mutuellement. La dernière méthode utilisée remplace systématiquement les paramètres définis précédemment.

Présentation de la limite à ajustement dynamique

Avec la limite à ajustement dynamique, eDirectory ajuste périodiquement sa consommation de mémoire en réponse au niveau de consommation de mémoire des autres processus. Vous indiquez la limite sous la forme d'un pourcentage de la mémoire physique disponible. Sur la base de ce pourcentage, eDirectory permet de calculer la nouvelle limite de mémoire à intervalles définis. La nouvelle limite de mémoire correspond au pourcentage de mémoire physique disponible à ce moment.

Outre le pourcentage, vous pouvez définir un seuil maximal et minimal. Le seuil correspond au nombre d'octets auxquels eDirectory s'ajuste. Il peut représenter le nombre d'octets à utiliser ou à laisser disponibles. Le seuil minimal par défaut est de 16 Mo. Le seuil maximal par défaut est de 4 Go.

Si les limites de seuil minimal et maximal sont incompatibles, c'est le seuil minimal qui prévaut. Vous pouvez, par exemple, indiquer les paramètres suivants :

Seuil minimal :	8 Mo
Pourcentage de mémoire physique disponible :	75
Seuil maximal :	Conserver 10 Mo disponibles

Lorsque eDirectory ajuste sa limite de cache, la mémoire physique disponible est de 16 Mo. eDirectory calcule une nouvelle limite de 12 Mo et vérifie si elle est comprise dans l'intervalle délimité par les seuils minimal et maximal. Dans cet exemple, le seuil maximal indique que 10 Mo doivent rester disponibles et eDirectory fixe donc la limite à 6 Mo. Cependant, le seuil minimal est de 8 Mo, c'est pourquoi eDirectory adopte cette valeur comme limite finale.

La limite à ajustement dynamique nécessite également la définition d'un intervalle. L'intervalle par défaut est de 15 secondes. Plus l'intervalle est court, plus la consommation de mémoire se base sur les conditions réelles. Cependant, des intervalles trop courts ne sont pas nécessairement avantageux, dans la mesure où le calcul du pourcentage alloue et libère davantage de mémoire.

Présentation de la limite de mémoire stricte

La limite de mémoire stricte est la méthode utilisée dans les versions antérieures de eDirectory pour réguler la consommation de mémoire. Choisissez l'une des méthodes suivantes pour définir la limite de mémoire stricte :

- Nombre fixe d'octets
- Pourcentage de mémoire physique

  Le pourcentage de mémoire physique pour l'intervalle correspond à un nombre fixe d'octets.
- Pourcentage de mémoire physique disponible

  Le pourcentage de mémoire physique disponible pour l'intervalle correspond à un nombre fixe d'octets.

Élimination des données superflues du cache

Les NDS 8 créent plusieurs versions des blocs et des entrées dans leur cache afin de préserver l'intégrité des transactions. Les versions antérieures des NDS 8 ne supprimaient pas ces blocs et entrées lorsqu'ils n'étaient plus nécessaires. Dans eDirectory 8.8, un processus d'arrière-plan parcourt périodiquement le cache et élimine les anciennes versions. Cette procédure permet de réduire la consommation de mémoire cache. L'intervalle d'analyse par défaut est de 15 secondes.

Configuration des limites à ajustement dynamique et de mémoire stricte

Vous pouvez configurer dynamiquement les limites à ajustement dynamique et de mémoire stricte en utilisant l'une des deux méthodes suivantes :

- « Utilisation de Novell iMonitor », page 514
- « Utilisation du fichier _ndsdb.ini », page 515

Utilisation de Novell iMonitor

1. Cliquez sur Configuration de l'agent  .
2. Cliquez sur Cache de base de données et consultez les informations suivantes :

Informations sur le cache de base de données	Description
Taille maximale	Taille maximale (en Ko) que peut avoir le cache spécifié.
Taille actuelle	Taille actuelle (en Ko) du cache spécifié.
Éléments mis en cache	Nombre d'éléments contenus dans le cache spécifié.
Anciennes versions mises en cache	Nombre d'anciennes versions contenues dans le cache spécifié. Les anciennes versions des éléments contenus dans le cache sont conservées par souci de cohérence des transactions de lecture dans la base de données. Autrement dit, si un thread se trouve dans une transaction de lecture et un autre dans une transaction d'écriture, les anciennes versions des blocs modifiés par l'opération d'écriture sont conservées à l'intention de l'utilisateur qui effectue la lecture. Cet utilisateur a ainsi la garantie d'obtenir des résultats cohérents durant toute sa transaction de lecture, même si des modifications sont effectuées dans l'intervalle.
Taille des anciennes versions	Taille (en Ko) des anciennes versions des éléments contenus dans le cache.
Correspondances	Nombre d'accès réussis à un élément à partir du cache spécifié.
Recherches des correspondances	Nombre d'éléments examinés avant un accès réussi à un élément à partir du cache spécifié. Le rapport de recherche de correspondances permet de mesurer l'efficacité de la recherche dans le cache. Normalement, il doit avoisiner 1:1.
Anomalies	Nombre de fois où un élément introuvable dans le cache spécifié a dû être obtenu dans un cache de niveau inférieur ou à partir du disque.
Recherches des anomalies	Nombre d'éléments examinés avant qu'il soit établi que l'élément voulu ne se trouvait pas dans le cache spécifié. Le rapport de recherche d'anomalies permet de mesurer l'efficacité de la recherche dans le cache. Normalement, il doit avoisiner 1:1.

3 Choisissez parmi les options suivantes :

Option	Description
Ajustement dynamique	Permet à la base de données eDirectory d'ajuster dynamiquement la quantité de mémoire système qu'il convient de réserver au cache, compte tenu des besoins estimés et des paramètres indiqués ci-dessous.
Pourcentage d'ajustement du cache	Pourcentage de la mémoire disponible qui peut être utilisé à la fois pour les caches d'enregistrement et de blocs.
Contraintes de taille de cache	Lors de l'ajustement dynamique, veillez à respecter les contraintes spécifiées. N'utilisez pas pour le cache une quantité de mémoire inférieure au chiffre indiqué, ni supérieure à la quantité totale de mémoire disponible moins le chiffre indiqué.
Limite stricte	Quantité exacte de mémoire système à utiliser pour le cache.
Taille maximale du cache	Taille (en Ko) des caches d'enregistrement et de blocs combinés.
Pourcentage du cache de blocs	Pourcentage de la mémoire système disponible pour le caching à affecter au cache de blocs. Le pourcentage restant est alloué au cache d'enregistrement.
Intervalle d'ajustement du cache	Cet intervalle ne s'applique que si l'ajustement dynamique est activé. Il détermine la fréquence d'ajustement de la taille du cache, en fonction du pourcentage et des contraintes spécifiés.
Intervalle de nettoyage du cache	Détermine à quelle fréquence les anciennes versions inutilisées sont supprimées du cache.
Paramètres de cache permanents	Lorsque cette option est sélectionnée, toutes les modifications soumises par le biais de iMonitor deviennent définitives et remplacent les paramètres précédemment enregistrés ainsi que les valeurs par défaut du système.

4 Cliquez sur Soumettre.

Utilisation du fichier _ndsdb.ini

1 Ouvrez _ndsdb.ini dans un éditeur de texte.

Sous NetWare®, ce fichier se trouve dans sys:\netware. Sous Windows NT et Windows 2000, il se trouve généralement dans \Novell\NDS\DIBfiles.

2 Ajoutez la syntaxe appropriée au fichier :

Commande	Explication de la variable	Définition
cache=*octets_cache*	Nombre fixe d'octets à utiliser.	Définit une limite de mémoire stricte. Par exemple, pour définir une limite stricte de 8 Mo, entrez cache=8000000
cache=*options_cache*	Vous pouvez préciser plusieurs options, dans l'ordre de votre choix, en les séparant par une virgule. ◆ DYN Définit une limite à ajustement dynamique. ◆ HARD Définit une limite de mémoire stricte. ◆ %:*pourcentage* Pourcentage de mémoire disponible ou physique à utiliser. ◆ AVAIL ou TOTAL Pourcentage de mémoire physique disponible ou totale (réservé à la limite de mémoire stricte). ◆ MIN:*nombre_octets* Nombre minimum d'octets. ◆ MAX:*nombre_octets* Nombre maximum d'octets. ◆ LEAVE:*nombre_octets* Nombre minimum d'octets à laisser.	Définit une limite de mémoire stricte ou à ajustement dynamique. Par exemple, pour définir une limite à ajustement dynamique de 75 % de la mémoire disponible et un minimum de 16 Mo, entrez cache=DYN, %:75,MIN:16000000 Ou, pour définir une limite stricte de 75 % de la mémoire physique totale et un minimum de 16 Mo, entrez cache=HARD,%:75,MIN: 16000000

3 (Facultatif) Pour préciser l'intervalle de la limite à ajustement dynamique, ajoutez la ligne suivante :

cacheadjustinterval=*nombre_secondes*

4 (Facultatif) Pour préciser l'intervalle de nettoyage des anciennes versions des entrées et des blocs, ajoutez la ligne suivante :

cachecleanupinterval=*nombre_secondes*

5 (Facultatif) Pour modifier la répartition du pourcentage entre cache de blocs et cache d'entrées, ajoutez la ligne suivante :

blockcachepercent=*pourcentage*

La variable *pourcentage* doit être comprise entre 0 et 100. Le pourcentage spécifié correspond au pourcentage de mémoire cache utilisé pour le cache de blocs. Le pourcentage restant est utilisé pour le cache d'entrées. Il est recommandé de ne pas choisir le pourcentage 0.

6 Redémarrez le serveur eDirectory pour que les modifications soient prises en compte.

Configuration de limites à l'aide de DSTrace

Si vous utilisez eDirectory pour NetWare, vous pouvez configurer la limite à ajustement dynamique et la limite de mémoire stricte via DSTrace. Vous n'avez pas besoin de redémarrer le serveur pour que les modifications soient prises en compte.

1 (Facultatif) Pour définir une limite stricte, entrez la commande suivante sur la console du serveur :

SET DSTRACE=!MB*quantité_de_RAM_à_utiliser_en_octets*

Par exemple, pour définir une limite stricte de 8 Mo, entrez

```
SET DSTRACE=!MB8388608
```

2 (Facultatif) Pour définir une limite stricte calculée, entrez la commande suivante sur la console du serveur. N'entrez que les options souhaitées :

SET DSTRACE=!MHARD,AVAIL OR TOTAL,%:*pourcentage*,MIN:*nombre_octets*,MAX:*nombre_octets*,LEAVE:*nombre_octets_à_laisser*,NOSAVE

Par exemple, pour définir une limite stricte de 75 % de la mémoire physique totale et un minimum de 16 Mo, et pour indiquer de ne pas enregistrer ces options dans le fichier de démarrage, entrez

```
SET DSTRACE=!MHARD,%:75,MIN:16777216,NOSAVE
```

3 (Facultatif) Pour définir une limite à ajustement dynamique, entrez la commande suivante sur la console du serveur :

SET DSTRACE=!MDYN,%:*pourcentage*,MIN:*nombre_octets*,MAX:*nombre_octets*,LEAVE:*nombre_octets_à_laisser*, NOSAVE

Par exemple, pour définir une limite dynamique de 75 % de la mémoire disponible et un minimum de 8 Mo, entrez

```
SET DSTRACE=!MDYN,%:75,MIN:8388608
```

Réglage des services LDAP pour eDirectory

Pour plus d'informations sur la configuration matérielle et logicielle de base du serveur LDAP, les paramètres de réglage et les conseils en matière d'organisation d'annuaire, consultez le site Web How to Configure and Optimize eDirectory LDAP Servers (Configuration et optimisation des serveurs LDAP eDirectory) (http://developer.novell.com/research/appnotes/2000/septembe/04/a000904.htm).

eDirectory utilise de la mémoire pour le cache de la base de données et pour l'utilisation de l'annuaire. Il s'agit de réserves de mémoire allouées distinctes. Le moteur de l'annuaire utilise au besoin la mémoire des réserves de mémoire allouées dans le système d'exploitation. La base de données utilise une réserve de cache définie par les paramètres ci-dessous. En général, plus la quantité de cache de base de données allouée à eDirectory est grande, plus les performances sont optimales. Cependant, étant donné que eDirectory utilise la mémoire système disponible pour ses tampons, si des clients effectuent des requêtes qui nécessitent le renvoi d'ensembles de données volumineux, il peut être nécessaire de réduire la taille du cache de la base de données afin de disposer de suffisamment de mémoire système pour que l'annuaire puisse gérer l'élaboration des réponses aux requêtes.

Le moteur de base de données utilise le cache de base de données pour stocker les blocs les plus récemment utilisés. Ce cache possède initialement une taille fixe de 16 Mo. Sa taille peut être modifiée à partir de la ligne de commande dans les versions d'origine de eDirectory. Par exemple, la commande suivante définit une taille de 80 Mo pour le cache de base de données de eDirectory :

```
set dstrace=!mb 80000000
```

Vous pouvez également définir un fichier nommé _ndsdb.ini dans le répertoire sys:_netware d'un serveur NetWare ou dans le répertoire contenant les fichiers de base de données eDirectory des environnements Windows (normalement, *épertoire_installation*>\nds\dbfiles) ainsi que Linux et UNIX (normalement \var\nds\dib). Ce fichier texte doit simplement contenir une ligne telle que :

```
cache=80000000
```

N'ajoutez aucun espace autour du signe égal (=).

Le cache de eDirectory 8.8 peut être initialisé avec une limite stricte, comme c'était le cas dans les versions précédentes. De plus, les limites supérieure et inférieure peuvent être définies soit sous forme de nombres fixes soit sous forme de pourcentage de la mémoire disponible. Les paramètres de contrôle d'allocation dynamique permettent à la taille du cache d'augmenter ou de diminuer selon l'utilisation. Si les paramètres de configuration appropriés sont définis, le cache de base de données augmente ou diminue de façon dynamique, selon les besoins des autres ressources système.

L'édition du fichier _ndsdb.ini permet de contrôler manuellement l'utilisation de la mémoire de la base de données. Le format de commandes du fichier INI est le suivant :

```
cache=octets_cache # Set a hard memory limit
```

D'autres formats sont présentés dans le tableau suivant :

Commande	Description
cache=*options_cache*	Définit une limite stricte ou à ajustement dynamique. Vous pouvez préciser plusieurs options de cache, dans l'ordre de votre choix, en les séparant par une virgule. Elles sont toutes facultatives. Ces options sont les suivantes :
DYN ou HARD	Limite dynamique ou stricte.
AVAIL ou TOTAL	Ces options ne s'appliquent que si une limite stricte a été choisie. Omettez ces options pour une limite dynamique.
%:*pourcentage*	Pourcentage de mémoire physique disponible ou totale à utiliser.

Commande	Description
MIN:*octets*	Nombre minimum d'octets.
MAX:*octets*	Nombre maximum d'octets.
LEAVE:*octets*	Nombre minimum d'octets à laisser au système d'exploitation.
blockcachepercent=*pourcentage*	Divise le cache entre le cache de blocs et le cache d'enregistrement.

Si une limite stricte est indiquée et que l'administrateur souhaite définir le cache de base de données en fonction d'un pourcentage de mémoire, il peut choisir entre un pourcentage de mémoire totale ou de mémoire disponible. Les limites dynamiques font toujours référence à un pourcentage de mémoire disponible. Voici des exemples de commandes valides dans le fichier _ndsdb.ini.

L'exemple de limite dynamique suivant équivaut à 75 % de la mémoire disponible, avec un minimum de 16 Mo, et 32 Mo pour le système d'exploitation :

```
cache=DYN,%:75,MIN:16000000, LEAVE 32000000
```

L'exemple de limite stricte suivant équivaut à 75 % de la mémoire physique totale, avec un minimum de 18 Mo et un maximum de 512 Mo :

```
cache=HARD, TOTAL,%:75,MIN:18000000, MAX 512000000
```

L'exemple suivant est un exemple de format ancien de limite stricte équivalant à 8 Mo :

```
cache=8000000
```

Le cache de base de données est réparti entre le cache de blocs et le cache d'enregistrement. Le cache de blocs contient des blocs de données et d'index qui mettent en miroir le stockage sur le disque. Le cache d'enregistrement garde en mémoire des représentations des objets et des attributs de l'annuaire. Si vous effectuez des mises à jour ou des ajouts dans l'annuaire, utilisez le paramètre du cache de blocs. Si vous effectuez principalement des lectures, utilisez le cache d'enregistrement. Vous risquez d'endommager les deux caches si vous effectuez de nombreuses mises à jour séquentielles sans allouer une taille de cache correcte. À moins que vous n'apportiez des modifications spécifiques, le cache est alloué pour 50 % au cache de blocs et pour 50 % au cache d'enregistrement. L'option blockcachepercent peut être incluse dans le fichier _ndsdb.ini pour indiquer le pourcentage de cache alloué à la mise en cache des blocs d'index et de données. (La valeur par défaut est 50 %.) Le cache restant est utilisé pour les entrées.

Par exemple, pour indiquer 60 % de cache de blocs et 40 % de cache d'enregistrement, entrez :

```
blockcachepercent=60
```

Ne choisissez pas l'intégralité du cache pour le cache de blocs ou le cache d'enregistrement, au détriment de l'autre type de cache. En règle générale, n'allouez pas plus de 75 % de votre mémoire cache à l'un des deux types de cache.

La configuration du cache de base de données peut également être contrôlée à l'aide de Novell iMonitor.

Bien que la taille du cache soit dynamique selon la quantité de mémoire disponible, la commande DSTRACE peut quand même être utilisée dans des environnements personnalisés.

Amélioration des performances de eDirectory sur les systèmes Linux, Solaris, AIX et HP-UX

Les sections suivantes fournissent des informations sur l'amélioration des performances de eDirectory sur des systèmes Linux et UNIX :

Optimisation du serveur eDirectory

Novell eDirectory sous Linux et Solaris utilise une réserve de threads à ajustement dynamique pour répondre aux requêtes des clients. La réserve de threads s'ajuste automatiquement et fournit des performances optimales dans la plupart des cas. Cependant, vous pouvez éviter le retard provoqué par le démarrage des threads en cas de charge soudaine sur le serveur, en configurant les paramètres suivants dans le fichier /etc/opt/novell/eDirectory/conf/nds.conf.

Paramètre	Description et paramètres recommandés
n4u.server.idle-threads	Nombre minimum de threads (indépendamment de l'activité). La valeur de ce paramètre doit être fixée en fonction de la charge moyenne du client, afin de réduire le délai nécessaire à la production de nouveaux threads en condition d'activité normale du client.
n4u.server.max-threads	Nombre maximum de threads. La valeur de ce paramètre doit être fixée en fonction du nombre maximum de clients qui doivent être pris en charge simultanément, ainsi que des recommandations suivantes : ◆ eDirectory requiert 16 threads au minimum. ◆ Un thread pour 255 connexions LDAP (thread de surveillance). ◆ Un thread pour 4 clients simultanés (thread de travail).
n4u.server.start-threads	Nombre de threads qui démarrent en même temps que eDirectory. La valeur de ce paramètre doit être fixée en fonction de la charge moyenne du client, afin de réduire le délai nécessaire à la production de nouveaux threads en condition d'activité normale du client.

Optimisation du cache de eDirectory

Novell eDirectory utilise un caching persistant, afin que les modifications apportées à un serveur soient conservées dans un vecteur. Si le serveur se bloque lors de modifications, eDirectory se charge plus rapidement et synchronise les modifications en quelques secondes dès que le serveur a redémarré. Novell eDirectory utilise un modèle de retour à l'état initial avec un fichier journal pour exécuter un repositionnement avec restauration actualisée sur les transactions en cas de défaillance du système.

Les paramètres de eDirectory commencent avec 16 Mo de cache, dont 50 % sont alloués au caching de blocs et le reste au cache d'enregistrement. Après un délai de 15 minutes, eDirectory modifie ses seuils de cache afin d'initialiser jusqu'à 51% de la mémoire disponible pour le cache, en laissant au moins 24 Mo pour le système d'exploitation. Cet algorithme n'est utilisé que si le système d'exploitation de l'hôte prend en charge l'appel qui vous permet de déterminer la quantité de mémoire libre disponible.

Vous pouvez optimiser votre cache eDirectory par les moyens suivants :

- « Utilisation d'une quantité fixe de RAM pour les systèmes Linux et UNIX », page 521
- « Définition des paramètres de cache », page 523

Pour plus d'informations sur l'optimisation du cache de eDirectory, reportez-vous à la section « Amélioration des performances de chargement par lots », page 526.

Utilisation d'une quantité fixe de RAM pour les systèmes Linux et UNIX

Bien que l'algorithme ci-dessus fonctionne correctement avec Windows et NetWare, il n'en va pas de même avec les systèmes Linux et UNIX. Dans les systèmes Linux et UNIX, la mémoire libre disponible indiquée par le système d'exploitation est inférieure à celle des autres systèmes d'exploitation en raison de la manière dont Linux et UNIX utilisent la mémoire libre pour le caching interne des blocs du système de fichiers, l'exécution fréquente de programmes, de bibliothèques, etc. En outre, sous Linux et UNIX, les bibliothèques ne restituent généralement pas au système d'exploitation la mémoire libérée.

C'est pourquoi nous vous recommandons d'allouer une quantité fixe de RAM au cache.

Fixez la quantité de RAM pour les systèmes Linux et UNIX en utilisant l'une des méthodes suivantes :

- « Création manuelle d'un fichier .ini », page 521
- « Utilisation de Novell iMonitor », page 522

Création manuelle d'un fichier .ini

1. Créez un fichier appelé _ndsdb.ini dans le répertoire qui contient déjà les fichiers de la base de données eDirectory (ensemble DIB) ; il s'agit généralement du répertoire /var/opt/novell/eDirectory/data/dib.
2. Ajoutez au fichier _ndsdb.ini les paramètres listés ci-dessous :

Paramètre	Description
blockcachepercent=50	Définit le pourcentage de cache alloué au caching de blocs de base de données.
cacheadjustinterval=15	Définit l'intervalle, en secondes, utilisé par eDirectory pour évaluer son utilisation de la mémoire libre et ajuster la taille globale du cache.
cachecleanupinterval=15	Définit l'intervalle, en secondes, utilisé par eDirectory pour écrire les blocs de cache altérés sur le disque.
cache=16777216	Définit la limite stricte (en octets).

Utilisation de Novell iMonitor

1. Cliquez sur Configuration de l'agent  .
2. Cliquez sur Cache de base de données et consultez les informations suivantes :

Informations sur le cache de base de données	Description
Taille maximale	Taille maximale (en Ko) que peut avoir le cache spécifié.
Taille actuelle	Taille actuelle (en Ko) du cache spécifié.
Éléments mis en cache	Nombre d'éléments contenus dans le cache spécifié.
Anciennes versions mises en cache	Nombre d'anciennes versions contenues dans le cache spécifié. Les anciennes versions des éléments contenus dans le cache sont conservées par souci de cohérence des transactions de lecture dans la base de données. Autrement dit, si un thread se trouve dans une transaction de lecture et un autre dans une transaction d'écriture, les anciennes versions des blocs modifiés par l'opération d'écriture sont conservées à l'intention de l'utilisateur qui effectue la lecture. Cet utilisateur a ainsi la garantie d'obtenir des résultats cohérents durant toute sa transaction de lecture, même si des modifications sont effectuées dans l'intervalle.
Taille des anciennes versions	Taille (en Ko) des anciennes versions des éléments contenus dans le cache.
Correspondances	Nombre d'accès réussis à un élément à partir du cache spécifié.
Recherches des correspondances	Nombre d'éléments examinés avant un accès réussi à un élément à partir du cache spécifié. Le rapport de recherche de correspondances permet de mesurer l'efficacité de la recherche dans le cache. Normalement, il doit avoisiner 1:1.
Anomalies	Nombre de fois où un élément introuvable dans le cache spécifié a dû être obtenu dans un cache de niveau inférieur ou à partir du disque.
Recherches des anomalies	Nombre d'éléments examinés avant qu'il soit établi que l'élément voulu ne se trouvait pas dans le cache spécifié. Le rapport de recherche d'anomalies permet de mesurer l'efficacité de la recherche dans le cache. Normalement, il doit avoisiner 1:1.

3 Choisissez parmi les options suivantes :

Option	Description
Ajustement dynamique	Permet à la base de données eDirectory d'ajuster dynamiquement la quantité de mémoire système qu'il convient de réserver au cache, compte tenu des besoins estimés et des paramètres indiqués ci-dessous.
Pourcentage d'ajustement du cache	Pourcentage de la mémoire disponible qui peut être utilisé à la fois pour les caches d'enregistrement et de blocs.
Contraintes de taille de cache	Lors de l'ajustement dynamique, veillez à respecter les contraintes spécifiées. N'utilisez pas pour le cache une quantité de mémoire inférieure au chiffre indiqué, ni supérieure à la quantité totale de mémoire disponible moins le chiffre indiqué.
Limite stricte	Quantité exacte de mémoire système à utiliser pour le cache.
Taille maximale du cache	Taille (en Ko) des caches d'enregistrement et de blocs combinés.
Pourcentage du cache de blocs	Pourcentage de la mémoire système disponible pour le caching à affecter au cache de blocs. Le pourcentage restant est alloué au cache d'enregistrement.
Intervalle d'ajustement du cache	Cet intervalle ne s'applique que si l'ajustement dynamique est activé. Il détermine la fréquence d'ajustement de la taille du cache, en fonction du pourcentage et des contraintes spécifiés.
Intervalle de nettoyage du cache	Détermine à quelle fréquence les anciennes versions inutilisées sont supprimées du cache.
Paramètres de cache permanents	Lorsque cette option est sélectionnée, toutes les modifications soumises par le biais de iMonitor deviennent définitives et remplacent les paramètres précédemment enregistrés ainsi que les valeurs par défaut du système.

4 Cliquez sur Soumettre.

Définition des paramètres de cache

Par défaut, eDirectory utilise un cache dynamique. Si vous disposez de suffisamment de mémoire vive pour augmenter la taille du cache eDirectory, vous pouvez considérablement améliorer les performances de eDirectory pour les bases de données volumineuses en allouant plus de mémoire vive au cache eDirectory.

Les paramètres listés dans le tableau suivant peuvent être ajustés en vue d'améliorer les performances de eDirectory :

Paramètre du cache eDirectory	Description
blockcachepercent=*valeur*	Définit le pourcentage de cache alloué au caching de blocs de base de données. La valeur par défaut est 50.
cachecleanupinterval=*valeur*	Définit l'intervalle, en secondes, utilisé par eDirectory pour écrire les blocs de cache altérés sur le disque. La valeur par défaut est 15.
cacheadjustinterval=*valeur*	Définit l'intervalle, en secondes, utilisé par eDirectory pour évaluer son utilisation de la mémoire libre et ajuster la taille globale du cache. La valeur par défaut est 15.
cache=*valeur*	Définit la limite stricte, en octets, de la mémoire que eDirectory peut utiliser pour le caching.
cache=leave:*valeur*	Indique le nombre minimal d'octets à laisser.
min:*valeur*	Indique la taille minimale du cache en octets.
max:*valeur*	Indique la taille maximale du cache en octets.

Selon l'algorithme, le paramètre par défaut de Novell eDirectory est le suivant :

```
cache=dyn,%:51,min:16777216,max:0,leave:0
```

En d'autres termes :

- La taille minimale du cache est 16 Mo.
- Aucune limite maximale n'est définie.
- Jusqu'à 51 % de la mémoire disponible seront utilisés dynamiquement.
- 24 Mo seront laissés au système d'exploitation.

  eDirectory fonctionne avec une limite stricte de 16 Mo afin que toutes les applications soient lancées et que le système soit stabilisé.

Vous pouvez également configurer eDirectory pour qu'il utilise un pourcentage de la mémoire totale. Pour ce faire, spécifiez le cache comme illustré ci-dessous :

```
cache=hard,total,%:pourcentage_de_mémoire_totale_en_octets
```

Réglage du système d'exploitation Solaris pour Novell eDirectory

Les sections suivantes expliquent comment régler le kernel, le réseau et le système de fichiers Solaris :

IMPORTANT : avant de commencer, vérifiez que vous avez appliqué les correctifs recommandés au système d'exploitation Solaris. Pour plus d'informations, reportez-vous à la section « Installing or Upgrading Novell eDirectory on Solaris (Installation ou mise à niveau de Novell eDirectory sous Solaris) » dans le manuel Novell eDirectory 8.8 Installation Guide (Guide d'installation de Novell eDirectory 8.8).

- « Réglage du kernel Solaris », page 525
- « Réglage du réseau Solaris », page 525
- « Optimisation du système de fichiers Solaris », page 526

Réglage du kernel Solaris

Pour optimiser les performances de eDirectory sous Solaris, définissez les variables kernel suivantes dans le fichier /etc/system :

Paramètre	Description
set maxphys=1048576	Nombre maximum d'octets pouvant être transférés par transaction SCSI.
set md_maxphys=1048576	Nombre maximum d'octets pouvant être transférés par transaction SCSI si vous utilisez disksuite, vol_maxio ou vxvm.
set ufs:ufs_LW=*1/128e_de_la_mémoire_disponible*	Pour chaque fichier, nombre limite d'octets en deçà duquel la valeur de la variable conditionnelle qui régit les processus en attente est permutée.
set ufs:ufs_HW=*1/64e_de_la_mémoire_disponible*	Pour chaque fichier, valeur maximale autorisée d'octets en attente.
ctcp:*taille_hachage_conn_tcp*=8192	Nombre d'entrées de hachage de connexion allouées pour localiser rapidement les structures de données du kernel associées à la connexion TCP. (Il est possible de porter cette valeur à 262 144 selon le nombre de clients LDAP.)

Réglage du réseau Solaris

Vous pouvez améliorer les performances de recherche LDAP à l'aide de la commande ndd de Solaris. La syntaxe de commande suivante vous permet d'analyser et de modifier les paramètres réglables qui influent sur les opérations et le comportement du réseau :

```
ndd -set /dev/tcp nom_variable valeur_variable
```

Les valeurs recommandées pour les variables sont listées dans le tableau ci-dessous :

Paramètre	Description
tcp_conn_req_max_q : 1024	Le « q » correspond ici à la file d'attente dans laquelle sont conservés les sockets complets jusqu'à l'émission d'une acceptation par l'application.
tcp_time_wait_interval : 60000	Définit (dans ce cas-ci réduit) le délai d'attente.
tcp_xmit_hiwat : 64000 tcp_xmit_lowat : 64000	Ajuste la taille minimale et maximale de la fenêtre d'envoi TCP.
tcp_slow_start_initial : 2	Change de 1 en 2 le nombre de premiers paquets de transmission.

Optimisation du système de fichiers Solaris

Les performances de Novell eDirectory sous Solaris peuvent être améliorées si le système de fichiers Solaris est correctement réglé, surtout pour les opérations de chargement par lots de données dans l'annuaire. Le réglage du système de fichiers pour eDirectory est similaire à celui d'une base de données. Pour plus d'informations sur le système de fichiers Solaris, consultez le site Web Sunworld* (http://www.sunworld.com/sunworldonline).

Amélioration des performances de chargement par lots

eDirectory 8.8 propose de nouvelles options pour accroître les performances de chargement par lots.

Les paramètres réglables pour les performances de chargement par lots avec l'utilitaire ICE d'importation/de conversion/d'exportation Novell sont les suivants :

- « Paramètres du cache eDirectory », page 526
- « Définition de la taille de transaction LBURP », page 527
- « Augmentation du nombre de requêtes asynchrones dans ICE », page 528
- « Augmentation du nombre de threads d'écriture LDAP », page 528
- « Désactivation de la validation de schéma dans ICE », page 529
- « Désactivation des modèles ACL », page 529
- « Liaison en amont », page 531
- « Activation/désactivation du cache en ligne », page 531
- « Augmentation du timeout de LBURP », page 531

Reportez-vous également aux différents paramètres réglables de votre système d'exploitation.

Paramètres du cache eDirectory

Les principaux facteurs sont la gestion inadaptée des entrées/sorties de disque et l'allocation de mémoire insuffisante pour le cache eDirectory. Si eDirectory est la seule application du serveur, vous pouvez régler le cache sur des valeurs supérieures, avec une limite maximale de 2,5 Go. Tout cache alloué est finalement utilisé. Une taille de mémoire cache supérieure améliorera les performances de eDirectory sur les données non rémanentes.

La plage de réglage du cache va de 100 Mo à 2,5 Go. En règle générale, vous n'aurez pas besoin de plus de trois à quatre fois la taille de l'ensemble DIB. Pour les ensembles DIB volumineux, limitez le cache à 2 Go.

La plus petite taille de cache testée est 0 et la plus grande 2,5 Go. Pour déterminer la taille appropriée du cache, vous devez connaître les besoins en mémoire des autres processus exécutés sur le serveur, ainsi que la quantité de mémoire cache sur disque nécessaire. Nous vous conseillons d'essayer différentes tailles pour trouver le meilleur équilibre.

Pour optimiser les performances de chargement par lots, allouez un pourcentage supérieur du cache eDirectory pour le cache de bloc. Nous recommandons de choisir une valeur de 90 %. Cette valeur peut être réinitialisée, une fois l'opération terminée.

L'utilisation de iMonitor est le moyen le plus rapide de modifier le paramètre blockcachepercentage. Pour ce faire, suivez les instructions figurant dans la section « Utilisation de Novell iMonitor 2.1 », page 193.

Pour plus d'informations, reportez-vous à la section « Tuning the cache subsystem » (Réglage du sous-système de cache) sur le site Web *Novell® eDirectory 8.7.1 : Performance Tuning for Linux* and UNIX* (Novell® eDirectory 8.7.1 : optimisation des performances pour Linux* et UNIX*)* (http://www.novell.com/collateral/4621373/4621373.pdf).

Définition de la taille de transaction LBURP

La taille de transaction LBURP définit le nombre d'enregistrements qui sont envoyés au serveur LDAP par l'utilitaire ICE, durant une même transaction. En augmentant cette valeur, vous pouvez améliorer les performances de chargement par lots, en supposant toutefois que vous avez défini une mémoire suffisante et que l'augmentation n'entraîne pas de conflit d'entrées/sorties.

La taille de transaction par défaut est 25, ce qui est suffisant pour les petits fichiers LDIF (moins de 100 000 opérations), mais non pour un nombre important d'enregistrements. La taille de transaction LBURP peut être définie entre 1 et 350.

Modification de la taille de transaction

Pour modifier la taille de transaction, changez la valeur requise dans le paramètre n4u.ldap.lburp.transize du fichier /etc/opt/novell/eDirectory/conf/nds.conf. Dans les situations idéales, une taille de transaction plus élevée assure des performances supérieures. Cependant, vous ne devez pas attribuer des valeurs arbitrairement élevées à la taille de transaction pour les raisons suivantes :

- Une taille de transaction plus élevée exige que le serveur alloue plus de mémoire à l'exécution de la transaction. Si le système commence à manquer de mémoire, cela peut provoquer un ralentissement dû aux échanges.
- Le fichier LDIF doit être exempt d'erreurs et toutes les entrées préexistantes dans eDirectory doivent être mises en commentaire. Si la transaction présente ne serait-ce qu'une seule erreur (y compris les cas où l'objet à ajouter existe déjà dans l'annuaire), eDirectory ne tient pas compte du paramètre de la transaction LBURP et effectue une validation après chaque opération pour garantir l'intégrité des données.

  Pour plus d'informations, reportez-vous à « Debugging LDIF Files » (Débogage de fichiers LDIF).
- L'optimisation LBURP ne fonctionne que pour les objets Feuille. Si la transaction renferme à la fois un conteneur et les objets qui lui sont subordonnés, eDirectory la traite comme une erreur. Pour éviter ce problème, nous recommandons de charger les objets Conteneur d'abord à l'aide d'un fichier LDIF distinct ou d'activer l'utilisation des références en aval.

  Pour plus d'informations, reportez-vous à la section « Enabling Forward References » (Activation des références en aval) dans le manuel *Novell eDirectory 8.8 Troubleshooting Guide* (Guide de dépannage de Novell eDirectory 8.8).

Augmentation du nombre de requêtes asynchrones dans ICE

Il s'agit du nombre d'entrées que le client ICE peut envoyer au serveur LDAP en mode asynchrone avant d'attendre l'envoi des résultats par le serveur.

Le nombre de requêtes asynchrones peut être défini entre 10 et 200. La valeur par défaut est 100. Toute valeur inférieure au minimum (10) est ramenée à la valeur par défaut. La valeur minimale est suffisante pour les petits fichiers LDIF.

Idéalement, une taille de fenêtre plus élevée assure de meilleures performances. Vous ne devez toutefois pas attribuer des valeurs arbitrairement élevées à la taille de fenêtre car une taille de fenêtre élargie oblige le client à allouer plus de mémoire au traitement des entrées dans le fichier LDIF. Si le système commence à manquer de mémoire, cela peut provoquer un ralentissement dû aux échanges.

Vous pouvez modifier le nombre de requêtes asynchrones dans ICE à l'aide de l'option de ligne de commande ICE ou de iManager.

Avec l'option de ligne de commande ICE

Il est possible de spécifier le nombre de requêtes asynchrones à l'aide de l'option de ligne de commande -Z de ICE. Elle est disponible dans le gestionnaire cible LDAP.

Pour définir 50 comme nombre de requêtes asynchrones envoyées au client ICE, entrez la commande suivante :

```
ice -SLDIF -f fichier_LDIF -a -c -DLDAP -d cn=admin,o=novell -Z50 -w
mot_de_passe
```

Avec l'Assistant ICE de iManager

Pour définir le nombre de requêtes asynchrones envoyées par le client ICE via iManager, procédez comme suit :

1. Cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Maintenance de eDirectory > Assistant Importation/Conversion/Exportation.
3. Tapez la valeur dans le champ Taille de la fenêtre LBURP des écrans du gestionnaire cible LDAP pour les tâches Importation de données à partir d'un fichier et Migration de données entre des serveursLDAP.
4. Cliquez sur Suivant.

   Pour plus d'informations, consultez l'aide de l'Assistant.

Augmentation du nombre de threads d'écriture LDAP

Le serveur LDAP comporte désormais plusieurs threads d'écriture. Utilisez l'option de ligne de commande -F de ICE pour activer les références en aval afin d'éviter toute erreur possible due à un traitement concurrent, en entrant la commande suivante :

```
ice -SLDIF -f fichier_LDIF -a -c -DLDAP -d cn=admin,o=novell -w mot_de_passe  -F
```

Désactivation de la validation de schéma dans ICE

Utilisez les options de ligne de commande -C et -n de ICE pour désactiver la validation de schéma au niveau du client ICE en entrant la commande suivante :

```
ice -C -n -SLDIF -f fichier_LDIF -a -c -DLDAP -d cn=admin,o=novell -w
mot_de_passe
```

Désactivation des modèles ACL

Vous pouvez désactiver les modèles ACL (Access Control List - liste de contrôle d'accès) pour accroître les performances de chargement par lots. Certaines ACL risquent alors d'être manquantes, mais vous pouvez résoudre ce problème en ajoutant les ACL nécessaires au fichier LDIF ou en les appliquant ultérieurement.

1. Exécutez la commande suivante :

   ldapsearch -D *cn_admin* -w *mot_de_passe* -b cn=schema -s base objectclasses=inetorgperson

   Cette commande donne le résultat suivant :

   ```
   dn: cn=schemaobjectClasses: ( 2.16.840.1.113730.3.2.2 NAME
   'inetOrgPerson' SUP
    organizationalPerson STRUCTURAL MAY ( groupMembership $ ndsHomeDirectory
    $ loginAllowedTi meMap $ loginDisabled $ loginExpirationTime $
    loginGraceLimit $ loginGraceRem aining $ loginIntruderAddress $
    loginIntruderAttempts $ loginIntruderResetTim e $
    loginMaximumSimultaneous $ loginScript $ loginTime $
    networkAddressRestri ction $ networkAddress $ passwordsUsed $
    passwordAllowChange $ passwordExpirationInterval $
    passwordExpirationTime $passwordMinimumLength $ passwordRequired $
    passwordUniqueRequired $ printJobConfiguration $ privateKey $ Profile $
    publicKey $ securityEquals $ accountBalance $ allowUnlimitedCredit $
    minimum AccountBalance $ messageServer $ Language $ UID $
    lockedByIntruder $ serverHolds $ lastLoginTime $ typeCreatorMap $
    higherPrivileges $ printerControl $ securityFlags $ profileMembership $
    Timezone $ sASServiceDN $ sASSecretStore $ sASSecretStoreKey $
    sASSecretStoreData $ sASPKIStoreKeys $ userCertificate
    $nDSPKIUserCertificateInfo $ nDSPKIKeystore $ rADIUSActiveConnections $
    rADIUS AttributeLists $ rADIUSConcurrentLimit $ rADIUSConnectionHistory
    $ rADIUSDefa ultProfile $ rADIUSDialAccessGroup $ rADIUSEnableDialAccess
    $ rADIUSPassword $ rADIUSServiceList $ audio $ businessCategory $
    carLicense $ departmentNumbe r $ employeeNumber $ employeeType $
    givenName $ homePhone $ homePostalAddress  $ initials $ jpegPhoto $
    labeledUri $ mail $ manager $ mobile $ pager $ ldap Photo $
    preferredLanguage $ roomNumber $ secretary $ uid $ userSMIMECertifica te
    $ x500UniqueIdentifier $ displayName $ userPKCS12 ) X-NDS_NAME 'User' X
   -NDS_NOT_CONTAINER '1' X-NDS_NONREMOVABLE '1' X-NDS_ACL_TEMPLATES (
   '2#subtree#[Self]#[All Attributes Rights]' '6#entry#[Self]#loginScript'
   '1#subtree#[Root Template]#[Entry Rights]'
   '2#entry#[Public]#messageServer' '2#entry#[Root
   Template]#groupMembership' '6#entry#[Self]#printJobConfiguration'
   '2#entry#[Root  Template]#networkAddress') )
   ```

2. Dans le résultat obtenu à l'étape précédente, supprimez les informations figurant en gras.

3. Enregistrez le résultat révisé sous la forme d'un fichier LDIF.

4 Ajoutez les informations suivantes dans le nouveau fichier LDIF :

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113730.3.2.2 )

-

add:objectclasses
```

Votre fichier LDIF devrait à présent ressembler à ceci :

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113730.3.2.2 )

-

add:objectclasse

sobjectClasses: ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' SUP
 organization alPerson STRUCTURAL MAY ( groupMembership $ ndsHomeDirectory
 $ loginAllowedTimeMap $ loginDisabled $ loginExpirationTime $
 loginGraceLimit $ loginGraceRem aining $ loginIntruderAddress $
 loginIntruderAttempts $ loginIntruderResetTime $
 loginMaximumSimultaneous $ loginScript $ loginTime $
 networkAddressRestri ction $ networkAddress $ passwordsUsed $
 passwordAllowChange $ passwordExpirationInterval $
 passwordExpirationTime $ passwordMinimumLength $ passwordRequired
 $passwordUniqueRequired $ printJobConfiguration $ privateKey $ Profile $
 publicKey $ securityEquals $ accountBalance $ allowUnlimitedCredit $
 minimum AccountBalance $ messageServer $ Language $ UID $
 lockedByIntruder $ serverHolds $ lastLoginTime $ typeCreatorMap $
 higherPrivileges $ printerControl $ securityFlags $ profileMembership $
 Timezone $ sASServiceDN $ sASSecretStore $ sASSecretStoreKey $
 sASSecretStoreData $ sASPKIStoreKeys $ userCertificate $
 nDSPKIUserCertificateInfo $ nDSPKIKeystore $ rADIUSActiveConnections $
 rADIUSAttributeLists $ rADIUSConcurrentLimit $ rADIUSConnectionHistory $
 rADIUSDefa ultProfile $ rADIUSDialAccessGroup $ rADIUSEnableDialAccess
 $rADIUSPassword $ rADIUSServiceList $ audio $ businessCategory $
 carLicense
 $ departmentNumbe r $ employeeNumber $ employeeType $ givenName $
 homePhone $ homePostalAddress  $ initials $ jpegPhoto $ labeledUri $ mail
 $ manager $ mobile $ pager $ ldap Photo $ preferredLanguage $ roomNumber
 $ secretary $ uid $ userSMIMECertifica te $ x500UniqueIdentifier $
 displayName $ userPKCS12 ) X-NDS_NAME 'User' X-ND S_NOT_CONTAINER '1' X
-NDS_NONREMOVABLE '1' )
```

5 Entrez la commande suivante :

ldapmodify -D *cn_admin* -w *mot_de_passe* -f *nom_fichier_ NDIF*

Liaison en amont

La liaison en amont est un processus d'arrière-plan qui vérifie notamment l'intégrité référentielle dans le cadre des vérifications effectuées 50 minutes après l'activation du serveur eDirectory. Cette vérification s'effectue de nouveau après 13 heures. Veillez à ce que la liaison en amont ne s'exécute pas pendant le chargement par lots, qui risquerait alors d'être perturbé selon la durée du chargement et le nombre d'objets chargés.

Activation/désactivation du cache en ligne

Le cache de changement en ligne peut être activé ou désactivé pour un serveur. Cette option ne peut toutefois être désactivée que si la synchronisation sortante est elle-même désactivée. Si la synchronisation sortante est activée, le cache de changement en ligne l'est également.

La désactivation du cache de changement en ligne rend ce cache non valide pour la réplique concernée ; il apparaît avec un drapeau non valide dans Configuration de l'agent > Partitions. Si le cache de changement en ligne est réactivé, le drapeau non valide est supprimé lors de la reconstruction du cache.

Augmentation du timeout de LBURP

Par défaut, le timeout pour un client est de 20 minutes (1 200 secondes). Mais pendant le chargement par lots, lorsque la taille de la transaction LBURP est de l'ordre de 250, que les objets comportent un grand nombre d'attributs dont les valeurs sont élevées et qu'un traitement LBURP est activé simultanément sur le serveur, le serveur est occupé à traiter les données provenant du client ICE sans lui répondre dans le délai imparti entraînant ainsi l'expiration de ce dernier.

Dès lors, nous vous recommandons d'augmenter le timeout. Pour ce faire, vous pouvez exporter la variable d'environnement LBURP_TIMEOUT avec des valeurs élevées (en secondes).

Par exemple, pour exporter la variable LBURP_TIMEOUT avec 1 200 secondes, entrez la commande suivante :

```
export ICE_LBURP_TIMEOUT=1200
```

Vérification de l'état de santé de eDirectory

L'état de santé des services d'annuaire est essentiel à toute organisation. Des vérifications régulières de l'état de santé à l'aide de Novell iMonitor assurent le bon fonctionnement de votre annuaire et facilitent les mises à niveau et les opérations de dépannage.

Fréquence des vérifications de l'état de santé

En règle générale, si votre réseau ne change pas souvent (si vous n'ajoutez des serveurs et des partitions que tous les deux mois et ne réalisez habituellement que de simples modifications), la vérification de l'état de santé doit être effectuée une fois par mois.

En revanche, si votre réseau est plus dynamique (si vous ajoutez toutes les semaines des partitions ou des serveurs, ou que votre entreprise est en pleine restructuration), il est recommandé de réaliser ce contrôle une fois par semaine.

Ajustez la fréquence des contrôles en fonction de l'évolution de votre environnement. Les facteurs qui influent sur la fréquence des contrôles sont notamment les suivants :

- le nombre de partitions et de répliques ;

- la stabilité des serveurs qui contiennent des répliques ;
- la quantité d'informations contenue dans une partition eDirectory ;
- la taille et la complexité des objets ;
- le nombre d'erreurs lors de précédentes exécutions de DSRepair.

Lorsque vous effectuez une vérification de l'état de santé, iMonitor rassemble des informations provenant de tous les serveurs, en fonction de droits donnés. Sachez que l'exécution de rapports sur l'état de santé augmente le trafic réseau et consomme de l'espace disque.

Présentation de la vérification de l'état de santé

Une vérification complète de l'état de santé couvre les aspects suivants :

- Version de eDirectory

  L'exécution de différentes versions des NDS ou de eDirectory sous la même version de NetWare peut entraîner des problèmes de synchronisation. Si votre version des NDS ou de eDirectory est obsolète, téléchargez le dernier correctif logiciel à partir de Novell Directory Services Patches and Files (Correctifs et fichiers NDS) (http://support.novell.com/filefinder/5069/index.html).

- Synchronisation horaire

  Tous les serveurs eDirectory doivent prendre en charge l'heure exacte. Des tampons horaires associés à chaque objet et propriété garantissent que les mises à jour de ces objets et propriétés sont classées dans le bon ordre. Ils permettent à eDirectory de déterminer les répliques à synchroniser.

- Tolérances de synchronisation

  Périodes depuis lesquelles un serveur s'est synchronisé en intégrant les changements de données entrantes et sortantes, les quantités de données en attente, etc.

- Processus d'arrière-plan

  Processus qui effectuent différentes tâches, notamment la réplication des changements et la mise à jour des informations système.

  - Références externes
  - Notices nécrologiques
  - Schéma eDirectory

Pour connaître la procédure détaillée permettant d'effectuer ces contrôles, reportez-vous à la section suivante, « Contrôle de l'état de santé de eDirectory à l'aide de iMonitor »..

Contrôle de l'état de santé de eDirectory à l'aide de iMonitor

En fonction de vos préférences, vous pouvez effectuer une vérification de l'état de santé du serveur eDirectory en utilisant l'une ou l'autre des méthodes proposées dans iMonitor :

- Utilisation du cadre du navigateur
- Utilisation du cadre de l'Assistant

Utilisation du cadre du navigateur

1. Accédez à iMonitor

   Pour plus de détails, reportez-vous à la section « Accès à iMonitor », page 195.
2. Dans le cadre du navigateur, cliquez sur l'icône Rapports  .
3. Dans le cadre de l'Assistant, cliquez sur le lien Configuration du rapport.

   La liste des rapports pouvant être exécutés s'affiche dans le cadre des données.
4. Cliquez sur l'icône Configurer le rapport  pour obtenir les informations requises sur le serveur.

   Un rapport d'information sur le serveur s'affiche dans le cadre des données. Utilisez-le pour sélectionner les options souhaitées pour votre rapport.
5. Cochez la case Sous-rapport de santé.
6. Pour exécuter le rapport à intervalles donnés, sélectionnez les options requises dans la section Planifier le rapport du cadre des données.

   IMPORTANT : si vous exécutez un rapport planifié, il s'exécute comme public et risque de ne pas rassembler autant d'informations que s'il s'exécutait comme utilisateur authentifié.
7. Cliquez sur Exécuter le rapport pour traiter le rapport.

Utilisation du cadre de l'Assistant

1. Accédez à iMonitor

   Pour plus de détails, reportez-vous à la section « Accès à iMonitor », page 195.
2. Dans le cadre de l'Assistant, cliquez sur État de santé de l'agent.

   Les informations sur la vérification de l'état de santé s'affichent dans le cadre des données correspondant au serveur sur lequel iMonitor lit ces informations (qui n'est pas nécessairement celui auquel vous êtes connecté).

Examen des informations du rapport

Une fois le rapport généré, le cadre des données affiche les résultats. Si l'état de santé de certains serveurs de votre arborescence laisse à désirer, le rapport est divisé en trois catégories (en commençant par les serveurs en moins bonne santé) :

- Serveurs avec signalement d'avertissements
- Serveurs présentant des signes suspects
- Serveurs en bonne santé

Si aucun de vos serveurs n'affiche d'avertissement ou ne présente de signes suspects, ces catégories n'apparaissent pas.

Pour les serveurs qui ne sont pas en bonne santé, vous pouvez cliquer sur le lien Sous-rapport d'état de santé de l'agent  situé en regard de chaque serveur. Utilisez l'aide contextuelle en ligne pour résoudre les problèmes. Cette aide vous permet de connaître la signification et l'importance de chacune des options, de résoudre les problèmes éventuels, d'ajuster les plages et de déterminer si vous souhaitez inclure certaines options dans la vérification de l'état de santé.

IMPORTANT : si des avertissements sont signalés pour un serveur, il est vivement recommandé de résoudre les problèmes correspondants. Ce conseil s'applique également aux serveurs qui présentent des signes suspects.

Complément d'informations

Les outils et techniques utilisés pour contrôler eDirectory sont listés dans le cours Novell Certified Directory Engineer Course 991 : Advanced eDirectory Tools and Diagnostics (Cours 991 – Ingénieur d'annuaire certifié : Outils et diagnostics eDirectory avancés). Dans ce cours, vous apprendrez à :

- effectuer des vérifications de l'état de santé de eDirectory ;
- effectuer correctement les opérations eDirectory ;
- diagnostiquer, dépanner et résoudre les problèmes eDirectory ;
- exécuter les outils et utilitaires de dépannage de eDirectory.

Pour plus d'informations sur ce cours, visitez le site Web Novell Training Services (services de formation Novell) (http://www.novell.com/training/index.html).

Ressources de surveillance

L'utilitaire Novell DSTrace s'exécute sous NetWare, Windows NT, Linux, Solaris, AIX et HP-UX. Cet outil permet de surveiller toutes les ressources de eDirectory. Pour plus dinformations sur DSTrace, reportez-vous aux sources suivantes :

- « Configuration des paramètres Trace », page 206
- Looking Into the Directory Services Trace (DSTrace) Options (Étude des options DSTrace) (http://developer.novell.com/research/sections/netmanage/dirprimer/2001/august/spv.htm)
- More on Using the DSTrace Command (Complément d'informations sur l'utilisation de la commande DSTrace) (http://developer.novell.com/research/sections/netmanage/dirprimer/2001/septembe/p010901.htm)

Vous pouvez également investir dans des produits tiers qui offrent des solutions complémentaires de gestion de l'environnement eDirectory. Pour plus d'informations, visitez les sites Web suivants :

- BindView (http://www.bindview.com)
- Blue Lance (http://www.bluelance.com)
- NetPro* (http://www.netpro.com)

Si vous devez surveiller ou auditer certaines caractéristiques de eDirectory non proposées par nos partenaires, les services de conseil Novell Consulting peuvent vous aider grâce au système Novell Event pour procéder à une évaluation ou un audit personnalisés.

Mise à niveau du matériel ou remplacement d'un serveur

Cette section explique comment transférer et protéger eDirectory sur un serveur spécifique, lorsque vous effectuez une mise à niveau du matériel ou remplacez celui-ci. Elle se fonde sur des informations figurant dans la section « Sauvegarde et restauration de Novell eDirectory », page 383.

L'outil Backup eMTool vous permet de préparer les informations eDirectory sur un serveur pour effectuer les opérations suivantes :

- « Mise à niveau planifiée du matériel ou d'un périphérique de stockage sans remplacement du serveur », page 535
- « Remplacement planifié d'un serveur », page 539

Mise à niveau planifiée du matériel ou d'un périphérique de stockage sans remplacement du serveur

Si vous envisagez de mettre à niveau le matériel, par exemple un périphérique de stockage ou de la mémoire RAM, commencez par effectuer une sauvegarde à froid de eDirectory à l'aide de Backup eMTool, ainsi qu'une sauvegarde du système de fichiers. Vous pourrez ainsi sauvegarder l'identité eDirectory du serveur et les données du système de fichiers, ce qui présente les avantages suivants :

- Si vous remplacez des périphériques de stockage, les sauvegardes vous permettent de transférer des informations des anciens périphériques vers les nouveaux.
- Si vous remplacez le périphérique de stockage qui contient le volume/la partition de disque où est stocké eDirectory, les informations de sauvegarde vous permettent également d'utiliser le processus de restauration pour recréer la base de données eDirectory sur le nouveau périphérique.
- En effectuant une sauvegarde à froid de eDirectory et en gardant la base de données fermée ensuite, vous pouvez mettre à niveau le matériel et transférer la base de données sans vous préoccuper de savoir si elle a changé depuis la dernière sauvegarde.
- En cas de problème, vous disposez de sauvegardes pour la récupération des données.

Pour la sauvegarde à froid de eDirectory, vous devez utiliser les options de verrouillage et de désactivation de eDirectory sur le serveur pour empêcher toute modification des données après la sauvegarde. Pour les autres serveurs qui communiquent normalement avec ce serveur, le serveur semble être arrêté. Toutes les informations eDirectory qui sont normalement envoyées au serveur sont stockées dans l'arborescence jusqu'à ce que les communications avec le serveur reprennent. Les informations stockées servent à synchroniser le serveur lors de sa remise en ligne.

REMARQUE : étant donné que d'autres serveurs de l'arborescence eDirectory attendent la remise en ligne rapide du serveur, vous devez effectuer la mise à niveau et ouvrir la base de données eDirectory sur le serveur dès que possible.

Pour effectuer une mise à niveau planifiée du matériel, procédez comme suit :

1. Si vous pensez que la mise à niveau risque d'entraîner un problème pour votre serveur, vous pouvez préparer une autre machine en vue d'une éventuelle utilisation.

   Pour plus de détails, reportez-vous à la section « 1. Préparation du remplacement d'un serveur », page 539.

2. Utilisez une commande du client eMBox similaire à la suivante pour effectuer une sauvegarde à froid de la base de données eDirectory et maintenir celle-ci fermée et verrouillée une fois l'opération terminée. Si vous utilisez NICI, veillez également à sauvegarder les fichiers de sécurité au moyen de l'option -e.

   ```
   backup -f nom_et_chemin_fichier_de_sauvegarde
     -l nom_et_chemin_fichier_journal -e -t -c -o -d
   ```

   Si vous utilisez NICI, veillez à sauvegarder les fichiers NICI au moyen du paramètre -e. (Pour plus d'informations sur l'utilisation du client eMBox et des paramètres, reportez-vous aux sections « Sauvegarde manuelle à l'aide du client eMBox », page 419 et « Options de ligne de commande pour la sauvegarde et la restauration », page 431.)

   La base de données eDirectory est à présent verrouillée. Vous devez la laisser verrouillée pour empêcher toute modification des données sur ce serveur, tant que la procédure n'est pas terminée.

   Terminez rapidement la procédure afin de réduire au maximum le temps d'indisponibilité du serveur.

3 Sauvegardez le système de fichiers au moyen de l'outil de votre choix. (Pour NetWare, vous pouvez utiliser SMS™.)

Il est important de le faire *après* la sauvegarde de la base de données afin que les fichiers de sauvegarde eDirectory soient enregistrés sur bande avec le reste du système de fichiers.

4 Arrêtez le serveur et remplacez le matériel.

5 Après avoir remplacé le matériel, suivez les instructions correspondant à la modification apportée :

Si vous…	Exécutez ces procédures générales
N'avez pas modifié les périphériques de stockage	Démarrez le serveur et déverrouillez la base de données.
Avez remplacé des périphériques de stockage, sans modifier le volume/la partition de disque contenant eDirectory	1. Démarrez le serveur et eDirectory. 2. Restaurez le système de fichiers uniquement pour les volumes/partitions de disque qui se trouvaient sur les périphériques de stockage remplacés. 3. Déverrouillez la base de données eDirectory.

Si vous…	Exécutez ces procédures générales
Avez remplacé le périphérique de stockage qui contenait eDirectory sur un système d'exploitation autre que NetWare	1. Installez le système d'exploitation, si nécessaire. 2. Restaurez le système de fichiers sur les partitions de disque concernées par le changement de périphérique de stockage. 3. Installez eDirectory sur le nouveau périphérique de stockage, dans une nouvelle arborescence temporaire. 4. Restaurez eDirectory à partir de la sauvegarde (ce qui rétablit l'arborescence d'origine), en spécifiant l'option qui permet de le maintenir fermé et verrouillé après la restauration. Utilisez une commande similaire à la suivante : restore -r -f *nom_et_chemin_fichier_sauvegarde* -l *nom_et_chemin_fichier_journal*-e Utilisez l'option -e si vous avez sauvegardé des fichiers NICI. Ajoutez l'option -u si vous avez sauvegardé des fichiers listés dans un fichier d'inclusion. 5. Déverrouillez la base de données eDirectory. 6. Si vous avez restauré les fichiers de sécurité NICI, après avoir terminé la restauration, redémarrez le serveur pour réinitialiser le système de sécurité. 7. Vérifiez que le serveur répond comme d'habitude. Utilisez ConsoleOne® pour contrôler le serveur et sa synchronisation. Vérifiez que les scripts de login et l'impression fonctionnent correctement. 8. Si vous avez utilisé la consignation de transactions individuelles par fichier sur ce serveur, veillez à recréer la configuration des fichiers journaux de transactions individuelles, une fois la restauration terminée. Après avoir activé les fichiers journaux de transactions individuelles, vous devez effectuer une nouvelle sauvegarde complète. Étant donné que les paramètres reprennent leur valeur par défaut après une restauration, la consignation de transactions individuelles par fichier est désactivée. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Si vous…	Exécutez ces procédures générales
Avez remplacé le périphérique de stockage qui contenait le volume sys : et eDirectory sous NetWare	Lorsque vous restaurez les données du système de fichiers sous NetWare, tenez compte des problèmes liés à la préservation des droits du système de fichiers. Vous devez restaurer eDirectory avant le système de fichiers. Il se peut aussi que vous deviez effectuer des opérations supplémentaires, comme expliqué dans la section « Préservation des droits lors de la restauration des données du système de fichiers sous NetWare », page 400. 1. Installez NetWare et eDirectory sur le nouveau périphérique de stockage en créant un nouveau volume sys : dans une nouvelle arborescence temporaire. 2. Placez les fichiers de sauvegarde eDirectory sur ce volume en les copiant à partir de la sauvegarde sur bande. 3. Restaurez eDirectory à partir de la sauvegarde (ce qui rétablit l'arborescence d'origine), en spécifiant l'option qui permet de le maintenir fermé et verrouillé après la restauration. Utilisez une commande similaire à la suivante : restore -r -f *nom_et_chemin_fichier_sauvegarde* -l *nom_et_chemin_fichier_journal*-e Utilisez l'option -e si vous avez sauvegardé des fichiers NICI. Ajoutez l'option -u si vous avez sauvegardé des fichiers listés dans un fichier d'inclusion. 4. Restaurez le système de fichiers sur tous les volumes concernés par le changement de périphérique de stockage. 5. Déverrouillez la base de données eDirectory. 6. Si vous avez restauré les fichiers de sécurité NICI, après avoir terminé la restauration, redémarrez le serveur pour réinitialiser le système de sécurité. 7. Vérifiez que le serveur répond comme d'habitude. Utilisez iMonitor pour contrôler le serveur et sa synchronisation. Vérifiez que les scripts de login et l'impression fonctionnent correctement. 8. Si vous avez utilisé la consignation de transactions individuelles par fichier sur ce serveur, veillez à recréer la configuration des fichiers journaux de transactions individuelles, une fois la restauration terminée. Après avoir activé les fichiers journaux de transactions individuelles, vous devez effectuer une nouvelle sauvegarde complète. Étant donné que les paramètres reprennent leur valeur par défaut après une restauration, la consignation de transactions individuelles par fichier est désactivée. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Si le serveur ne répond pas comme d'habitude, vous devrez peut-être procéder à une récupération en appliquant l'une des deux méthodes ci-après :

- Recréez la configuration matérielle précédente, puisqu'elle fonctionnait avant le changement.
- Transférez l'identité du serveur vers une autre machine au moyen des sauvegardes du système de fichiers et de eDirectory que vous avez effectuées. Pour plus de détails, reportez-vous à la section « Remplacement planifié d'un serveur », page 539.

Remplacement planifié d'un serveur

Les instructions suivantes concernent les cas où le remplacement du serveur s'opère par le déplacement de son identité eDirectory et des données de son système de fichiers vers une autre machine. L'ancien serveur est appelé serveur A et le nouveau serveur, ou serveur de remplacement, serveur B.

Il convient, au préalable, d'effectuer une sauvegarde à froid de eDirectory (c'est-à-dire pendant que la base de données est fermée) à l'aide de l'outil Backup eMTool, ainsi qu'une sauvegarde du système de fichiers à l'aide de l'outil de votre choix. Ces données de sauvegarde vous permettent d'utiliser le processus de restauration pour recréer le serveur sur la nouvelle machine.

Pour la sauvegarde à froid de eDirectory, vous devez utiliser les options de verrouillage et de désactivation de eDirectory sur le serveur A pour empêcher toute modification des données après la sauvegarde. Pour les autres serveurs qui communiquent normalement avec ce serveur, le serveur semble être arrêté. Toutes les informations eDirectory qui sont normalement envoyées au serveur sont stockées dans l'arborescence jusqu'à ce que les communications avec le serveur reprennent. Les informations stockées servent à synchroniser le serveur lorsque vous le remettez en ligne sur la nouvelle machine, à savoir le serveur B.

REMARQUE : étant donné que d'autres serveurs de l'arborescence eDirectory attendent la remise en ligne rapide du serveur, vous devez effectuer le changement et la restauration des informations eDirectory sur le serveur dès que possible.

Suivez la procédure générale suivante pour remplacer un serveur :

1. Pour réduire le temps d'arrêt du serveur A durant son remplacement, il est préférable de préparer le serveur B du mieux possible avant de commencer la procédure, en installant le système d'exploitation, etc., comme indiqué à l'étape « 1. Préparation du remplacement d'un serveur », page 539.
2. Effectuez les sauvegardes de eDirectory et du système de fichiers sur le serveur A, comme expliqué à l'étape « 2. Création d'une sauvegarde de eDirectory », page 540.
3. Transférez les informations vers le serveur B, comme expliqué à l'étape « 3. Restauration des informations eDirectory pour le remplacement d'un serveur », page 541.

1. Préparation du remplacement d'un serveur

Utilisez, pour les serveurs A et B, les listes de contrôle suivantes afin de déterminer si vous êtes prêt à remplacer le serveur A. En préparant préalablement le serveur B, vous réduirez le temps d'inactivité du serveur durant le transfert d'une machine vers l'autre.

Préparation du serveur A

- ❑ Assurez-vous que la dernière version du système d'exploitation est installée sur le serveur A.
- ❑ Vérifiez l'état de santé de l'arborescence du serveur A en exécutant DSRepair sur le serveur contenant la réplique maîtresse de la partition Arborescence et en exécutant une synchronisation horaire.
- ❑ Exécutez DSRepair sur la base de données du serveur A. Vérifiez que celui-ci est entièrement synchronisé.

Préparation du serveur B

- ❑ Installez la dernière version du système d'exploitation. Il doit s'agir du même système d'exploitation que celui du serveur A.
- ❑ Installez eDirectory en plaçant le serveur B dans une nouvelle arborescence temporaire.

  (Si vous restaurez eDirectory durant l'étape « 3. Restauration des informations eDirectory pour le remplacement d'un serveur », page 541, le serveur B sera placé dans l'arborescence d'origine qui était celle du serveur A.)
- ❑ (NetWare uniquement) Lorsque vous restaurez les données du système de fichiers dans le cadre du remplacement d'un serveur, tenez compte des problèmes liés à la préservation des droits du système de fichiers. Prévoyez de restaurer eDirectory avant le système de fichiers. Il se peut aussi que vous deviez effectuer des opérations supplémentaires, comme expliqué dans la section « Préservation des droits lors de la restauration des données du système de fichiers sous NetWare », page 400.

Passez à l'étape suivante, « 2. Création d'une sauvegarde de eDirectory ».

2. Création d'une sauvegarde de eDirectory

Vous devez créer une sauvegarde de eDirectory avant de remplacer un serveur. Après avoir réalisé la procédure « 1. Préparation du remplacement d'un serveur », page 539, utilisez le client eMBox pour effectuer une sauvegarde à froid de la base de données eDirectory sur le serveur A, au moyen des options avancées pour désactiver et verrouiller cette base après la sauvegarde.

Pour effectuer une sauvegarde à froid de eDirectory (c'est-à-dire pendant que la base de données est fermée) et maintenir ensuite la base de données fermée, procédez comme suit :

1. Assurez-vous d'avoir terminé la procédure « 1. Préparation du remplacement d'un serveur », page 539.
2. Utilisez une commande de sauvegarde similaire à la suivante dans le client eMBox, en précisant les paramètres -c, -o et -d pour effectuer une sauvegarde à froid de la base de données eDirectory sur le serveur A et maintenir ensuite cette base fermée et verrouillée :

   backup -f *nom_et_chemin_fichier_de_sauvegarde*
   -l *nom_et_chemin_fichier_journal* -e -t -c -o -d

   Si vous utilisez NICI, veillez à sauvegarder les fichiers NICI au moyen du paramètre -e. (Pour plus d'informations sur l'utilisation du client eMBox et des paramètres, reportez-vous aux sections « Sauvegarde manuelle à l'aide du client eMBox », page 419 et « Options de ligne de commande pour la sauvegarde et la restauration », page 431.)

   La base de données eDirectory du serveur A est à présent verrouillée. Vous devez la maintenir verrouillée afin qu'aucune nouvelle modification de données n'intervienne sur ce serveur, jusqu'à ce que vous le replaciez dans l'arborescence en le restaurant sur le serveur B.

   Terminez rapidement la procédure de mise à niveau/remplacement du serveur afin de réduire au maximum le temps d'indisponibilité de ce dernier.
3. Effectuez une sauvegarde complète du système de fichiers du serveur A. (Pour NetWare, vous pouvez utiliser SMS.)

   Il est important d'effectuer cette sauvegarde *après* celle de la base de données afin que les fichiers de sauvegarde de eDirectory soient enregistrés sur bande avec le reste du système de fichiers.

Pour plus d'informations sur l'utilisation de SMS, consultez le manuel *Storage Management Services Administration Guide (Guide d'administration SMS)* (http://www.novell.com/documentation/lg/nw65/smsadmin/data/hjc2z4tu.html).

4 Verrouillez la base de données eDirectory sur le serveur A et déconnectez celui-ci du réseau.

Continuez en suivant la procédure « 3. Restauration des informations eDirectory pour le remplacement d'un serveur », page 541.

3. Restauration des informations eDirectory pour le remplacement d'un serveur

Pour transférer le système de fichiers et l'identité eDirectory du serveur A vers le serveur B :

1 Assurez-vous d'avoir terminé les procédures « 1. Préparation du remplacement d'un serveur », page 539 et « 2. Création d'une sauvegarde de eDirectory », page 540.

2 Vérifiez que le serveur B et eDirectory fonctionnent.

3 Utilisez la fonction de restauration pour transférer le système de fichiers et l'identité eDirectory du serveur A vers le serveur B :

3a Copiez les fichiers de sauvegarde à froid eDirectory du serveur A vers le serveur B.

En utilisant un outil de compression tiers, vous pouvez sensiblement réduire la taille des fichiers de sauvegarde, car ceux-ci offrent un taux de compression élevé. Cela peut vous aider à accélérer la copie.

3b Restaurez la base de données eDirectory du serveur A vers le serveur B à l'aide des fichiers de sauvegarde que vous avez copiés. Sur la ligne de commande du client eMBox, entrez une commande similaire à la suivante :

restore -r -f *nom_et_chemin_fichier_sauvegarde*
-l *nom_et_chemin_fichier_journal* -e

Si vous utilisez NICI, veillez à restaurer les fichiers NICI au moyen du paramètre -e. Ajoutez l'option -u si vous avez sauvegardé des fichiers listés dans un fichier d'inclusion. (Pour plus d'informations sur l'utilisation du client eMBox et des paramètres, reportez-vous aux sections « Restauration à partir de fichiers de sauvegarde avec le client eMBox », page 428 et « Options de ligne de commande pour la sauvegarde et la restauration », page 431.)

Il est inutile d'inclure des fichiers journaux de transactions individuelles dans la restauration, puisque vous avez effectué une sauvegarde à froid et maintenu ensuite la base de données fermée. Aucune transaction n'est intervenue dans la base de données, puisque celle-ci était fermée ; aucun fichier journal de transaction individuelle n'a donc été créé depuis la sauvegarde.

IMPORTANT : sous NetWare, il est particulièrement important de restaurer eDirectory avant le système de fichiers, afin de préserver les droits et assignations d'ayant droit lors de la restauration des données du système de fichiers. Pour plus d'informations, reportez-vous à la section « Préservation des droits lors de la restauration des données du système de fichiers sous NetWare », page 400.

3c Transférez les données du système de fichiers du serveur A vers le serveur B à partir de la sauvegarde.

4 (NetWare uniquement) Renommez le serveur B en utilisant l'adresse IP et le nom du serveur A dans autoexec.ncf.

5 Si vous utilisez NICI, redémarrez le serveur pour réinitialiser NICI afin qu'il utilise les fichiers de sécurité restaurés.

6 Déverrouillez la base de données eDirectory.

7 Une fois la restauration terminée, vérifiez que le serveur B a adopté l'identité du serveur A et qu'il répond normalement. Utilisez ConsoleOne pour vérifier le serveur et sa synchronisation. Vérifiez que les scripts de login, l'impression et la sécurité NICI fonctionnent correctement.

   Si le serveur répond normalement, la procédure de remplacement est terminée. Vous pouvez maintenant désinstaller eDirectory du serveur A en supprimant l'identité eDirectory de ce dernier, puis utiliser la machine à d'autres fins. Ne refaites pas fonctionner le serveur A tant que vous n'avez pas supprimé eDirectory. Sinon, la synchronisation de eDirectory risquerait de perturber le réseau, car les serveurs A et B entreraient en concurrence pour obtenir la même identité.

8 (Conditionnel) Si vous avez utilisé la consignation de transactions individuelles par fichier sur ce serveur, veillez à recréer la configuration des fichiers journaux de transactions individuelles, une fois la restauration terminée. Après avoir activé les fichiers journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

   Comme ces paramètres reprennent leur valeur par défaut après une restauration, la consignation de transactions individuelles par fichier est désactivée. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Si le serveur B ne fonctionne pas correctement et que l'identité et le système de fichiers du serveur A doivent être immédiatement disponibles, procédez comme suit :

1 Débranchez le câble réseau du serveur B ou arrêtez le serveur.

2 Reconnectez le serveur A au réseau, démarrez-le, puis ouvrez la base de données eDirectory.

   Ignorez les messages système vous invitant à exécuter DSREPAIR.

3 Supprimez eDirectory du serveur B et tentez à nouveau la mise à niveau.

Restauration de eDirectory après une panne matérielle

Une panne de disque dur impliquant le volume/la partition de disque contenant eDirectory correspond à une suppression de eDirectory du serveur. (Heureusement, dans un environnement multiserveur, un serveur peut s'arrêter, alors que les autres serveurs de l'anneau de répliques restent intacts.)

Pour restaurer eDirectory après une panne affectant le volume/la partition de disque où celui-ci réside, respectez les procédures de restauration à partir des fichiers de sauvegarde comme expliqué dans les sections « Préparation d'une restauration », page 406 et « Restauration à partir de fichiers de sauvegarde avec iManager », page 415 (ou « Restauration à partir de fichiers de sauvegarde avec le client eMBox », page 428).

Durant la nouvelle installation, suivez les instructions du fabricant pour vérifier le bon fonctionnement des disques durs du serveur. Le nouveau disque dur doit avoir une capacité de stockage au moins égale à celle du disque qu'il remplace. Utilisez les fichiers contenant les informations locales du serveur pour vérifier les informations de configuration.

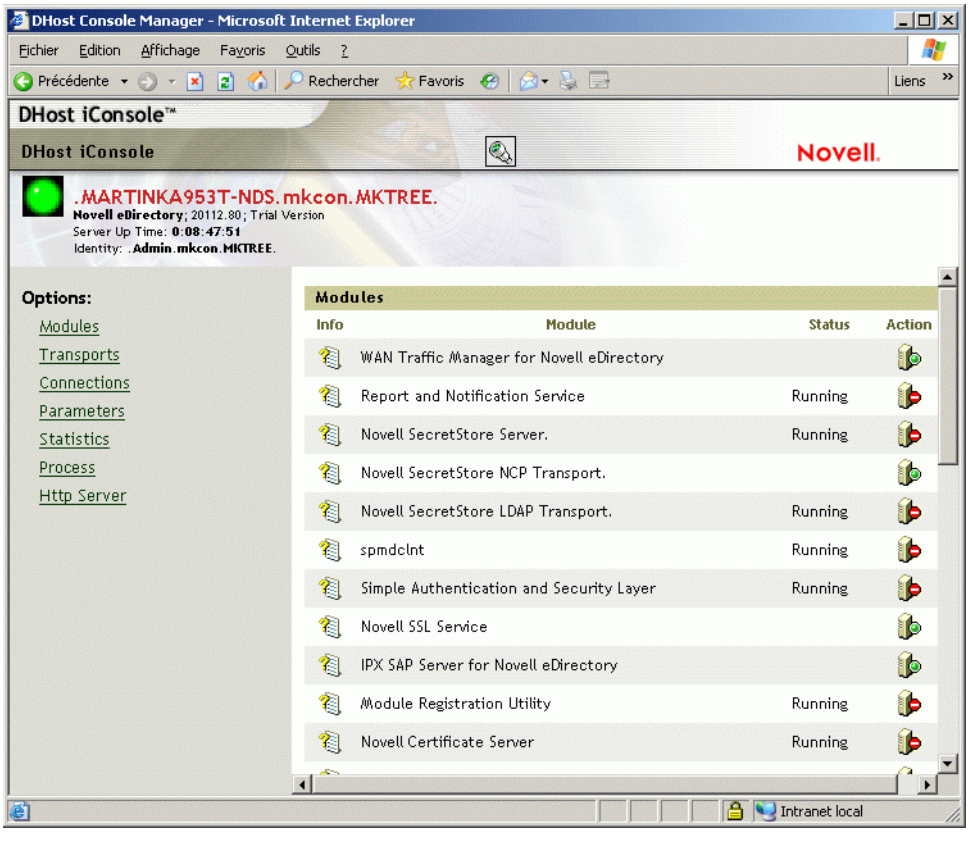
REMARQUE : si vous ne disposez pas de fichiers de sauvegarde pour le serveur, utilisez l'outil XBrowse pour interroger eDirectory et ainsi récupérer les informations du serveur. Effectuez cette opération avant de supprimer l'objet Serveur ou tout objet associé de l'arborescence. Vous trouverez XBrowse et des informations complémentaires auprès du support technique de Novell, Document d'informations techniques n° 2960653 (http://support.novell.com/servlet/tidfinder/2960653).

17 Gestionnaire DHost iConsole

Outil d'administration basé sur le Web, le gestionnaire DHost iConsole est un navigateur qui permet de :

- gérer les modules Dhost ;
- rechercher les paramètres de configuration Dhost ;
- consulter les informations de connexion Dhost ;
- visualiser les statistiques de réserves de threads ;
- consulter des informations détaillées sur les protocoles enregistrés auprès du gestionnaire de piles de protocoles Dhost.

Figure 50 Gestionnaire DHost iConsole



Le gestionnaire DHost iConsole est également un outil de diagnostic et de débogage qui permet d'accéder au serveur HTTP lorsque le serveur eDirectory ne fonctionne pas correctement. (Pour plus d'informations, reportez-vous à la section « Définition du mot de passe SAdmin », page 550.)

Ce chapitre développe les informations suivantes :

Définition de DHost

Le logiciel Novell® eDirectory pour Windows, Solaris, Linux, AIX et HP-UX repose sur le même code de base que eDirectory pour NetWare®. Pour que eDirectory pour Windows, Linux et UNIX interagisse correctement avec les autres versions de eDirectory, un sous-ensemble de services NCP™ (NetWare Core Protocol™) est pris en charge. Il est géré par un programme appelé DHost. DHost réside sous eDirectory et fournit aux plates-formes non-NetWare des fonctionnalités que le système d'exploitation NetWare propose normalement.

DHost fournit les services orientés NetWare suivants :

Service	Description
Moteur NCP	Protocole basé sur des paquets qui permet à un client d'envoyer des requêtes à un serveur NetWare et de recevoir les réponses de ce dernier. Pour plus d'informations, consultez le site Web NetWare Core Protocols (NCP) (http://developer.novell.com/ndk/doc/ncp/ncp__enu/data/hc4lztgy.html).
Surveillance	Paquets utilisés pour vérifier que les postes de travail sont toujours connectés au serveur NetWare. Pour plus d'informations, consultez le site Web Watchdog Packet Spoofing (Simulation de paquets de surveillance) (http://www.novell.com/documentation/lg/nw65/ipx_enu/data/h0cufuir.html).
Table de connexions	Numéro unique assigné à un processus, à un serveur d'impression, à une application, à un poste de travail ou à toute autre entité qui s'attache à un serveur NetWare. Ce numéro peut être différent pour chaque attache. Les numéros de connexion sont utilisés pour mettre en oeuvre la sécurité et la facturation réseau. Ils indiquent la place des objets dans la table de connexions des serveurs de fichiers. De plus, ils facilitent l'identification et l'obtention d'informations concernant les objets logués sur le réseau.
Système d'événements	Permet aux applications de surveiller l'activité d'un serveur.
Réserve de threads	Séquence d'instructions exécutée comme une entité indépendante et programmée par le logiciel système.

Service	Description
Extensions NCP	Permettent aux développeurs d'applications serveur d'écrire des NLM™ à mettre en oeuvre dans le SE NetWare en tant que NCP. Pour plus d'informations, consultez le site Web NCP Extension Concepts (Concepts d'extensions NCP) (http://developer.novell.com/ndk/doc/ncp/index.html?page=/ndk/doc/ncp/ncp__enu/data/a1wftl8.html).
Message Digest	Forme compressée ou condensée d'un document, ou extrait d'un document, qui sert d'«empreinte digitale numérique» pour un document de plus grande taille. Un message digest permet de créer une signature numérique unique propre à un document.

Exécution de DHost iConsole

- « Exécution de DHost iConsole sous NetWare », page 545
- « Exécution de DHost iConsole sous Windows », page 545
- « Exécution de DHost iConsole sous Linux, Solaris, AIX et HP-UX », page 546

Exécution de DHost iConsole sous NetWare

Sous NetWare, vous pouvez accéder à DHost iConsole via NetWare Remote Manager. Si vous voulez définir ou modifier le mot de passe SAdmin, httpstk.nlm doit être en cours d'exécution sur le serveur eDirectory.

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez:

   http://*adresse_TCP/IP_du_serveur*:*port*

   Par exemple :

   http://137.65.123.11:8028

   REMARQUE : l'autre numéro de port par défaut est8028. Si vous avez changé cette valeur dans la page Configuration de NetWare Remote Manager, veillez à entrer le nouveau numéro de port.

   Si des DNS (Domain Name Services - services de noms de domaines) sont installés sur votre réseau pour la résolution de noms de serveur en adresses IP, vous pouvez également entrer le nom DNS du serveur plutôt que son adresseIP.
3. Entrez un nom d'utilisateur, un contexte et un mot de passe.

Exécution de DHost iConsole sous Windows

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez :

   http://*nom.serveur*:*port*/dhost

   Par exemple :

   `http://MonServeur:80/dhost`

Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

```
http://137.65.135.150:80/dhost
```

3 Entrez un nom d'utilisateur, un contexte et un mot de passe.

Exécution de DHost iConsole sous Linux, Solaris, AIX et HP-UX

1 Ouvrez un navigateur Web.

2 Dans le champ de l'adresse URL, saisissez :

http://*nom.serveur*:*port*/dhost

Par exemple :

```
http://MonServeur:80/dhost
```

Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

```
http://137.65.135.150:80/dhost
```

3 Entrez un nom d'utilisateur, un contexte et un mot de passe.

Gestion des modules eDirectory

La page Modules de DHost iConsole fournit des informations sur les services eDirectory disponibles et sur leurs états. Elle permet également de démarrer et d'arrêter (de charger et de décharger) ces services.

Vous pouvez uniquement charger ou décharger des modules non interactifs tels que LDAP, SNMP et HTTPSTK.

La page Modules comporte les attributs suivants :

Attribut	Description
Info (Infos)	Cliquez sur  pour afficher la description, le nom de fichier, l'identificateur, les attributs et le nom d'objet partagé du module sélectionné.
Module	Affiche le nom du module.
Status (État)	Indique si le module est en cours d'exécution ou non.
Action	Indique si le module peut être démarré ou non. Les trois états possibles d'un module sont les suivants :  indique qu'il s'agit d'un module système qui ne peut pas être déchargé.  indique que le module peut être chargé et qu'il est prêt à être chargé.  indique que le module est en cours d'exécution.

- « Chargement et déchargement de modules sous NetWare », page 547
- « Chargement et déchargement de modules sous Windows », page 547
- « Chargement et déchargement de modules sous Linux, Solaris, AIX et HP-UX », page 548

Pour plus d'informations sur l'utilisation de Novell iManager pour le chargement et le déchargement de services eDirectory, reportez-vous à la section « Gestionnaire de services eDirectory », page 190.

Chargement et déchargement de modules sous NetWare

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez :

   `http://adresse_TCP/IP_du_serveur:port`

   Par exemple :

   http://137.65.123.11:8028

   REMARQUE : l'autre numéro de port par défaut est8028. Si vous avez changé cette valeur dans la page Configuration de NetWare Remote Manager, veillez à entrer le nouveau numéro de port.

   Si des DNS (Domain Name Services – services de noms de domaines) sont installés sur votre réseau pour la résolution de noms de serveur en adresses IP, vous pouvez également entrer le nom DNS du serveur plutôt que son adresse IP.
3. Entrez un nom d'utilisateur, un contexte et un mot de passe.
4. Cliquez sur Lister les modules dans la liste Gérer les applications.
5. Pour charger un module, entrez son nom puis cliquez sur Charger le module.

   Pour vérifier si le module est chargé, cochez la case Afficher la console système pour le chargement de modules.

Chargement et déchargement de modules sous Windows

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez:

   `http://nom.serveur:port/dhost`

   Par exemple :

   `http://MonServeur:80/dhost`

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   `http://137.65.135.150:80/dhost`
3. Entrez un nom d'utilisateur, un contexte et un mot de passe.
4. Cliquez sur Modules.
5. Cliquez sur  pour charger un module, ou sur  pour en décharger un.

Chargement et déchargement de modules sous Linux, Solaris, AIX et HP-UX

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez :

   http://*nom.serveur*:*port*/dhost

   Par exemple :

   ```
   http://MonServeur:80/dhost
   ```

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   ```
   http://137.65.135.150:80/dhost
   ```
3. Entrez un nom d'utilisateur, un contexte et un mot de passe.
4. Cliquez sur Modules.
5. Cliquez sur  pour charger un module, ou sur  pour en décharger un.

Demande d'informations DHost

Grâce au gestionnaire DHost iConsole, vous pouvez demander les informations suivantes :

- paramètres de configuration ;
- protocoles enregistrés avec le gestionnaire PSTACK ;
- propriétésde connexion ;
- résuméde la réserve de threads.

Affichage des paramètres de configuration

Les paramètres de configuration sont uniquement spécifiques aux plates-formes Linux et UNIX.

Dans le gestionnaire DHost iConsole, cliquez sur Paramètres. Pour plus d'informations, reportez-vous à la section « Exécution de DHost iConsole sous Linux, Solaris, AIX et HP-UX », page 546.

Les paramètres de configuration affichent les informations suivantes :

Option	Description
Parameter name (Nom de paramètre)	Affiche le nom du paramètre de configuration.
Default value (Valeur par défaut)	Affiche la valeur par défaut du paramètre.
Set value (Valeur définie)	Affiche la valeur actuellement définie.
Minimum value (Valeur minimum)	Affiche la valeur minimale qui peut être définie pour le paramètre.
Maximum value (Valeur maximum)	Affiche la valeur maximale qui peut être définie pour le paramètre.
Type	Affiche le type de valeur qui peut être défini pour le paramètre.

Pour plus d'informations, reportez-vous à la section Configuration Parameters (Paramètres de configuration) du manuel *Novell eDirectory 8.8 Installation Guide (Guide d'installation de Novell eDirectory 8.8)*.

Affichage des informations sur le protocole

Dans le gestionnaire DHost iConsole, cliquez sur Transports.

Les informations de protocole suivantes s'affichent :

- ID
- Protocol (Protocol)
- Transports

Affichage des propriétés de connexion

Dans le gestionnaire DHost iConsole, cliquez sur Connexions.

Les propriétés de connexion suivantes s'affichent :

- Conn
- Flags (Drapeaux)
- Identity (Identité)
- Display Name (Nom d'affichage)
- Transport
- Authentication Name (Nom d'authentification)
- SEV Count (Nombre SEV)
- Last Access (Dernier accès)
- Locked (Verrouillée)

Affichage des statistiques de réserves de threads

Dans le gestionnaire DHost iConsole, cliquez sur Statistiques.

Les statistiques de réserves de threads s'affichent :

- Spawned Threads (Threads générés)
- Dead Threads (Threads morts)
- Idle Threads (Threads inactifs)
- Worker Thread (Thread de travail)
- Peak Worker Thread (Thread de travail maximum)
- Ready for Work Thread (Thread prêt pour le travail)
- Ready Queue Peak Worker Threads (Threads de travail maximum prêts dans la file d'attente)
- Ready Queue Max Wait Time (Délai d'attente maximal prêt dans la file d'attente)
- Schedule Delay Minimum Time (Durée d'attente minimale planifiée)
- Schedule Delay Maximum Time (Durée d'attente maximale planifiée)

- Schedule Delay Average Time (Durée d'attente moyenne planifiée)
- Waiting For Work (En attente de travail)
- Peaking Waiting For Work (Attente de travail maximale)

Pile de processus

La pile de processus contient la liste des threads en cours d'exécution dans l'espace de processus DHost. Pour obtenir des informations détaillées sur un thread, cliquez sur son ID. Cette fonction sert généralement d'outil de débogage de niveau inférieur aux ingénieurs et au personnel du support technique de Novell.

Cette option n'est disponible que sous Windows.

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez:

   http://*nom.serveur*:*port*/dhost

   Par exemple :

   ```
   http://MonServeur:80/dhost
   ```

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   ```
   http://137.65.135.150:80/dhost
   ```
3. Entrez un nom d'utilisateur, un contexte et un mot de passe.
4. Cliquez sur Processus.
5. Pour afficher la pile d'appel d'un thread, cliquez sur l'ID de ce dernier.

Définition du mot de passe SAdmin

Vous pouvez définir un utilisateur Admin préconfiguré qui permet d'accéder à HTTPSTK (pile de protocoles HTTP) lorsque eDirectory n'est pas chargé. Cet utilisateur, SAdmin, a des droits équivalents à ceux de l'objet Utilisateur Admin eDirectory. Si l'état du serveur ne permet pas à eDirectory de fonctionner correctement, vous pouvez vous loguer au serveur sous l'identité de cet utilisateur et effectuer toutes les tâches de diagnostic et de débogage nécessaires qui ne requièrent pas eDirectory.

- « Définition du mot de passe SAdmin sous NetWare », page 550
- « Définition du mot de passe SAdmin sous Windows », page 551
- « Définition du mot de passe SAdmin sous Linux, Solaris, AIX et HP-UX », page 551

Définition du mot de passe SAdmin sous NetWare

Utilisez NetWare Remote Manager pour activer l'objet Utilisateur SAdmin, ainsi que pour définir ou modifier le mot de passe associé à cet objet. Pour ces deux dernières opérations, httpstk.nlm doit être en cours d'exécution sur le serveur eDirectory.

1. Ouvrez un navigateur Web.

2 Dans le champ de l'adresse URL, saisissez :

http://*adresse_TCP/IP_du_serveur*:*port*

Par exemple :

http://137.65.123.11:8028

REMARQUE : l'autre numéro de port par défaut est8028. Si vous avez changé cette valeur dans la page Configuration de NetWare Remote Manager, veillez à entrer le nouveau numéro de port.

Si des DNS (Domain Name Services - services de noms de domaines) sont installés sur votre réseau pour la résolution de noms de serveur en adresses IP, vous pouvez également entrer le nom DNS du serveur plutôt que son adresse IP.

3 Entrez un nom d'utilisateur, un contexte et un mot de passe.

4 Cliquez sur le bouton Configurer  > Activer le compte d'urgence (utilisateur SADMIN) et définir le mot de passe.

5 Entrez un mot de passe SAdmin et vérifiez-le.

6 Cliquez sur Définir.

Définition du mot de passe SAdmin sous Windows

Utilisez la page du gestionnaire à distance DHOST (accessible via l'URL /dhost ou à partir de la page racine) pour définir le mot de passe SAdmin. Si vous voulez définir ou modifier le mot de passe SAdmin, dhost.exe doit être en cours d'exécution sur le serveur eDirectory.

1 Ouvrez un navigateur Web.

2 Dans le champ de l'adresse URL, saisissez:

http://*nom.serveur*:*port*/dhost

Par exemple :

`http://MonServeur:80/dhost`

Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

`http://137.65.135.150:80/dhost`

3 Entrez un nom d'utilisateur, un contexte et un mot de passe.

4 Cliquez sur Serveur HTTP, puis entrez un mot de passe SAdmin.

5 Vérifiez le mot de passe que vous venez d'entrer, puis cliquez sur Soumettre.

Définition du mot de passe SAdmin sous Linux, Solaris, AIX et HP-UX

Vous pouvez définir le mot de passe SAdmin sur les systèmes Solaris, Linux, AIX ou HP-UX au moyen de l'un des éléments suivants :

- « Page de gestion à distance de DHOST », page 552
- « Ndsconfig », page 552

Page de gestion à distance de DHOST

La page du gestionnaire à distance DHOST (accessible via l'URL /dhost ou à partir de la page racine) permet de définir le mot de passe SAdmin. Si vous voulez définir ou modifier ce mot de passe, Novell eDirectory Server doit être en cours d'exécution sur le serveur eDirectory.

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez:

   http://*nom.serveur*:*port*/dhost

   Par exemple :

   ```
   http://MonServeur:80/dhost
   ```

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   ```
   http://137.65.135.150:80/dhost
   ```
3. Entrez un nom d'utilisateur, un contexte et un mot de passe.
4. Cliquez sur Serveur HTTP, puis entrez un mot de passe SAdmin.
5. Vérifiez le mot de passe que vous venez d'entrer, puis cliquez sur Soumettre.

Ndsconfig

L'utilitaire ndsconfig permet de définir le mot de passe SAdmin. Si vous voulez définir ou modifier ce mot de passe, ndsd doit être en cours d'exécution sur le serveur eDirectory.

Entrez la commande suivante sur la console du serveur :

ndsconfig set http.server.sadmin-pwd=*mot_de_passe*

où *mot_de_passe* représente le nouveau mot de passe SAdmin.

Pour plus d'informations sur l'utilisation de l'utilitaire ndsconfig, reportez-vous à la section ndsconfig Utility Parameters (Paramètres de l'utilitaire ndsconfig) dans le manuel *Novell eDirectory 8.8 Installation Guide (Guide d'installation de Novell eDirectory 8.8)*.

18 eDirectory Management Toolbox

L'outil eMBox (Novell® eDirectory™ Management Toolbox) permet d'accéder à tous les utilitaires de l'interface dorsale de eDirectory, à distance comme sur le serveur.

Combiné à Novell iManager, eMBox fournit un accès via le Web à des utilitaires eDirectory tels que DSRepair, DSMerge, le gestionnaire de services et l'utilitaire de sauvegarde et de restauration.

IMPORTANT : pour pouvoir exécuter les tâches eMBox, les services basés sur le rôle doivent être configurés via iManager pour l'arborescence à administrer.

Toutes les fonctions sont accessibles, sur le serveur local ou à distance, via un client à ligne de commande. Grâce au client eMBox, vous pouvez effectuer des tâches pour plusieurs serveurs à partir d'un seul serveur ou poste de travail.

Pour exécuter tous les outils eMTools (eDirectory Management Tools), tels que Backup (Sauvegarde), DSRepair, DSMerge, Schema Operations (Opérations sur le schéma) et eDirectory Service Manager (Gestionnaire de services eDirectory), eMBox doit être chargé et en cours d'exécution sur le serveur eDirectory.

Cette section fournit les informations suivantes :

Utilisation du client à ligne de commande eMBox

Il est entre autres possible d'accéder à eMBox à l'aide de son client Java à ligne de commande. Ce client propose deux modes: interactif et traitement par lots. En mode interactif, vous exécutez une commande eMBox à la fois. En mode de traitement par lots, vous pouvez exécuter automatiquement un groupe de commandes. Le client à ligne de commande possède un service de consignation pour les deux modes.

Ce client est une application Java. Pour l'activer, vous devez avoir accès à l'environnement d'exécution Java (Java Runtime Environment), JVM1.3.1 de Sun, installé avec eDirectory. Vous devez aussi pouvoir accéder derrière le pare-feu aux serveurs que vous voulez gérer. Vous pouvez effectuer des tâches pour plusieurs serveurs à partir d'un même serveur ou poste de travail.

Cette section fournit les informations suivantes :

Affichage de l'aide sur la ligne de commande

Pour afficher l'aide générale sur la ligne de commande eMBox avant d'accéder au client eMBox, procédez comme suit :

- NetWare®, Linux et UNIX: sur la ligne de commande, entrez `edirutil -?`.
- Windows: exécutez
  `lecteur\novell\nds\embox\edirutil.exe -?`

Pour obtenir de l'aide sur la ligne de commande eMBox en mode interactif, entrez un point d'interrogation(?) à l'invite du client eMBox. Par exemple,

```
Client eMBox> ?
```

L'aide affiche des informations sur les options de ligne de commande similaires à celles de la section « Options du client à ligne de commande eMBox », page 560.

Exécution du client à ligne de commande eMBox en mode interactif

Le mode interactif permet d'exécuter les commandes eMBox l'une après l'autre.

Cette section fournit les informations suivantes :

Exécution du client eMBox sur un serveur eDirectory

Le client eMBox et JVM1.3.1 de Sun sont installés avec eDirectory. Pour ouvrir le client eMBox en mode interactif sur un serveur eDirectory, procédez comme suit :

- NetWare, Linux et UNIX: dans la ligne de commande, entrez `edirutil -i`.
- Windows: exécutez
  `lecteur\novell\nds\edirutil.exe -i`

Le fichier edirutil est un raccourci pour l'exécution du client eMBox. Il pointe vers l'exécutable Java et l'emplacement d'installation par défaut du client eMBox avec eDirectory. Pour NetWare, il comprend l'option requisens. Il s'agit d'une option Java sous NetWare qui signifie « new screen » (« nouvel écran »). (Vous pouvez également entrer les informations manuellement, comme expliqué dans la section « Configuration du chemin et du chemin de classe pour le client eMBox », page 555.)

L'utilisation du client à ligne de commande eMBox nécessite un accès derrière le pare-feu pour les serveurs que vous voulez gérer. Si vous êtes à distance, vous devez donc disposer d'un accès via un réseau privé virtuel (VPN).

Exécution du client eMBox sur un poste de travail

Pour exécuter le client eMBox sur une machine autre qu'un serveur eDirectory:

- Copiez le fichier eMBoxClient.jar depuis un serveur eDirectory vers votre machine.
  - NetWare : sys:\system\embox\eMBoxClient.jar
  - Windows : \novell\nds\embox\eMBoxClient.jar
  - Linux et UNIX : /opt/novell/eDirectory/lib/nds-modules/embox/eMBoxClient.jar
- Assurez-vous que JVM1.3.1 de Sun est installé sur la machine.
- Vérifiez que l'accès derrière le pare-feu est possible afin d'utiliser le client à ligne de commande eMBox pour les serveurs que vous voulez gérer.

Contrairement à un serveur, un poste de travail ne permet pas d'employer la commande edirutil comme raccourci pour accéder au client eMBox en mode interactif. Vous devez soit configurer l'environnement après avoir accédé à votre chemin et votre chemin de classe, soit l'entrer chaque fois manuellement. Pour plus de détails, reportez-vous à la section « Configuration du chemin et du chemin de classe pour le client eMBox », page 555.

Configuration du chemin et du chemin de classe pour le client eMBox

Si vous exécutez le client eMBox sur un serveur eDirectory sans avoir modifié l'emplacement de Java ou du fichier eMBoxClient.jar, vous pouvez utiliser `edirutil` comme raccourci pour l'exécution. (Reportez-vous à la section « Exécution du client eMBox sur un serveur eDirectory », page 554.)

En revanche, si vous avez modifié les emplacements par défaut, si vous exécutez le fichier eMBoxClient.jar sur une machine autre qu'un serveur ou encore si vous voulez entrer le chemin de classe manuellement, vous devez configurer le chemin et le chemin de classe pour le client eMBox conformément aux indications de cette section.

Vous pouvez exécuter le client eMBox à partir de n'importe quel emplacement sur votre ordinateur si vous suivez la procédure ci-après :

- Ajoutez à votre chemin l'emplacement de l'exécutable Java (par exemple java.exe) ou vérifiez que Java est déjà en cours d'exécution.

  Si vous êtes sur un serveur, cette opération a probablement déjà été effectuée pour vous. Sur des serveurs Windows, Linux et UNIX, le répertoire doit se trouver dans votre chemin. Sous NetWare, il n'est pas nécessaire d'ajouter le répertoire à un chemin d'accès, mais Java doit être en cours d'exécution.

  Sur un poste de travail, il se peut que vous deviez effectuer vous-même cette opération. Par exemple, sous Windows, cliquez sur Démarrer > Paramètres > Panneau de configuration > Système. Dans l'onglet Avancé, cliquez sur Variables d'environnement et ajoutez le chemin à la variable Path.

  Pour procéder manuellement: si le chemin d'accès à l'exécutable Java n'a pas été ajouté à votre chemin, vous devez d'abord accéder, via la ligne de commande, au répertoire contenant cet exécutable avant de lancer eMBox. Par exemple, sous Windows, entrez
  `cd c:\novell\nds\embox\jre\bin`
- Ajoutez le chemin du fichier eMBoxClient.jar à votre chemin de classe.

  Serveur NetWare :
  `set ENVSET=`*`chemin`*`\eMBoxClient.jar`

  Serveur ou poste de travail Windows :
  `set CLASSPATH=`*`chemin`*`\eMBoxClient.jar`

  Serveur ou poste de travail Linux ou Unix:
  `export CLASSPATH=`*`chemin`*`/eMBoxClient.jar`

Pour procéder manuellement : un autre moyen de spécifier le chemin de classe consiste à utiliser le drapeau-cp pour Java chaque fois que vous voulez exécuter eMBox.

```
java -cp chemin/eMBoxClient.jar embox -i
```

Par exemple, sous Windows, entrez

```
java -cp c:\novell\nds\embox\eMBoxClient.jar embox -i
```

AVERTISSEMENT : sur les serveurs NetWare uniquement, pour éviter un abend, vous *devez* inclure `-ns` (option Java sous NetWare signifiant « new screen », soit « nouvel écran »). Par exemple,

```
java -ns -cp sys:\system\embox\eMBoxClient.jar embox -i
```

Une fois ces deux opérations effectuées, vous pouvez exécuter le client en mode interactif à partir de n'importe quel emplacement de votre machine en utilisant la commande suivante :

```
java embox -i
```

AVERTISSEMENT : sur les serveurs NetWare uniquement, pour éviter un abend, vous *devez* inclure `-ns` (option Java sous NetWare signifiant « new screen », soit « nouvel écran »). Par exemple,

```
java -ns embox -i
```

Pour plus d'informations sur les commandes Java, consultez la documentation Java sur le site Web de Sun (http://java.sun.com).

Login à un serveur

Pour vous loguer à un serveur, vous devez indiquer son nom ou son adresseIP, ainsi que le numéro du port de connexion spécifique. Pour les logins publics, il est inutile de préciser un nom d'utilisateur et un mot de passe.

Par exemple, une fois que le client eMBox est ouvert en mode interactif, entrez

```
login -s 137.65.123.244 -p 8028 -u admin.ma_société
-w mon_mot_de_passe -n
```

Pour plus d'informations sur les numéros de port, reportez-vous à la section « Recherche des numéros de port eDirectory », page 561.

Définition des préférences de langue, de timeout et de fichier journal

La langue par défaut est la langue du système client. Ainsi, dans la plupart des cas, vous n'avez pas besoin de définir explicitement une langue. De même, le timeout par défaut convient le plus souvent. Pour définir le fichier journal, indiquez son nom et son mode d'ouverture (annexer ou écraser).

Le tableau ci-après fournit des exemples de commandes.

Commande	Description
`set -L en,de`	Définit l'anglais et l'allemand comme langues préférées (dans cet ordre).
`set -T 100`	Définit un timeout de 100secondes. Le paramètre de timeout indique le délai d'attente des réponses du serveur.
`set -l monjournal.txt o`	Utilise monjournal.txt comme fichier journal et l'écrase (overwrite) à l'ouverture. Valeur par défaut=append (annexer)

Liste des outils eMTools et de leurs services

Une fois logué à un serveur, vous pouvez utiliser la commande list pour afficher la liste des services disponibles sur ce serveur.

La commande list affiche dynamiquement tous les outils eMTools suivants et leurs services.

eMTool	Description
backup	Novell eDirectory Backup eMTool
dsmerge	Novell eDirectory Merge eMTool
dsrepair	Novell eDirectory Repair eMTool
dsschema	Novell eDirectory Schema Operations eMTool
service	Novell eDirectory Service Manager eMTool

Utilisez -r pour forcer le rafraîchissement de la liste. Utilisez -t pour lister les détails des services. Utilisez -f pour lister uniquement le format de la commande.

Le tableau ci-après fournit des exemples de commandes.

Commande	Description
`list`	Liste les outils eMTools disponibles sur le serveur.
`list -r`	Rafraîchit la liste des outils eMTools.
`list -t backup`	Liste les services de sauvegarde (Backup) de manière détaillée.
`list -t dsrepair`	Liste les services DSRepair de manière détaillée.
`list -t dsmerge -f`	Liste les services DSMerge de manière détaillée.

Exécution d'un service spécifique

Une fois logué à un serveur, vous pouvez effectuer des tâches au moyen des différents services eMTool. Par exemple :

Commande	Description
`dsrepair.rld`	Réparer la base de données locale
`backup.getconfig`	Obtenir des informations sur la configuration de la sauvegarde.

Pour plus d'informations, reportez-vous aux sections suivantes :

- « Utilisation du client eMBox pour la sauvegarde et la restauration », page 419
- « Utilisation du client eMBox pour fusionner des arborescences », page 233
- « Utilisation du client eMBox pour réparer une base de données », page 284
- « Utilisation de l'outil Service Manager eMTool du client eMBox », page 190

Logout du serveur en cours

Pour vous déloguer de la session en cours, utilisez la commande suivante :

logout

Si vous vous loguez à un autre serveur, vous n'avez pas besoin d'utiliser cette commande, car vous vous déloguez automatiquement du serveur actuel.

Fermeture du client

Pour quitter le client, utilisez l'une des commandes suivantes :

exit

ou

quit

Exécution du client à ligne de commande eMBox en mode de traitement par lots

Il existe trois méthodes d'exécution du client eMBox en mode de traitement par lots :

- « Tâches uniques », page 558
- « Fichier interne de traitement par lots », page 558
- « Fichier système de traitement par lots », page 560

Pour une souplesse accrue et pour organiser et réutiliser les commandes fréquemment exécutées, vous pouvez combiner des fichiers système et internes de traitement par lots.

Tâches uniques

Dans la ligne de commande, vous pouvez n'exécuter qu'une seule tâche eMBox en mode de traitement par lots. Il suffit d'entrer la commande avec l'option-t pour spécifier l'outil et la tâche sans sélectionner l'option-i (mode interactif). Par exemple,

```
java embox -s 137.65.123.244 -p 8028 -u admin.ma_société
-w mon_mot_de_passe -l monjournal.txt -t dsrepair.rld -n
```

AVERTISSEMENT : sous NetWare uniquement: pour éviter un abend, vous *devez* inclure `-ns` (option Java sous NetWare signifiant «new screen», soit «nouvel écran»). Par exemple,

```
java -ns embox -s 137.65.123.244 -p 8028 -u admin.ma_société -w mon_mot_de_passe -l
monjournal.txt -t dsrepair.rld -n
```

Pour des tâches multiples sur plusieurs serveurs, ou des tâches que vous exécutez fréquemment, il est recommandé d'utiliser un fichier interne de traitement par lots. Pour plus d'informations, reportez-vous à la section suivante, “Fichier interne de traitement par lots.”

Fichier interne de traitement par lots

Pour exécuter le client eMBox en mode de traitement par lots à l'aide d'un fichier de traitement par lots propre au client eMBox, vous devez créer un fichier contenant le groupe des commandes eMBox que vous exécuteriez en mode interactif.

Un fichier de traitement par lots propre au client eMBox permet l'exécution automatique de toutes les commandes qu'il contient. Vous pouvez effectuer des tâches multiples à l'aide de plusieurs outils eMBox sur le même serveur sans avoir à vous loguer et vous déloguer pour chaque tâche.

À partir d'un serveur, vous pouvez également exécuter plusieurs tâches au moyen d'outils eMBox sur plusieurs serveurs.

Les fichiers internes de traitement par lots aident à organiser et à réutiliser les commandes fréquemment exécutées, ce qui évite de les entrer à chaque fois manuellement dans la ligne de commande.

Vous pouvez accéder à la ligne de commande et exécuter le fichier interne de traitement par lots à l'aide d'une commande du client eMBox. Par exemple, la commande suivante effectue le login à un serveur et exécute les commandes listées dans le fichier monlot.mbx:

```
java embox -s 137.65.123.244 -p 8028 -u admin.ma_société -w mon_mot_de_passe
-l monjournal.txt -o -b monlot.mbx -n
```

AVERTISSEMENT : sous NetWare uniquement: pour éviter un abend, vous *devez* inclure `-ns` (option Java sous NetWare signifiant «new screen», soit «nouvel écran»). Par exemple,

```
java -ns embox -s 137.65.123.244 -p 8028 -u admin.ma_société -w mon_mot_de_passe -l
monjournal.txt -o -b monlot.mbx -n
```

Une autre solution consiste à inclure le même type de commande dans un fichier système de traitement par lots, ce qui permet de planifier l'exécution sans surveillance de ce fichier sur le serveur. Pour plus de détails, reportez-vous à la section « Fichier système de traitement par lots », page 560.

Voici un exemple de fichier interne de traitement par lots eMBox. Il contient des exemples de commandes exécutables et un exemple de login à un autre serveur. Dans cet exemple, nous partons du principe que vous êtes logué à un serveur lors de l'ouverture du client eMBox. (Chaque commande doit figurer sur une ligne distincte. Les lignes qui commencent par le signe# sont des commentaires.)

```
# Le nom de ce fichier est monlot.mbx.
# Il s'agit d'un exemple de commandes utilisables dans
# un fichier interne de traitement par lots eMBox.

# Commandes Backup
backup.getconfig
backup.backup -b -f masauvegarde.bak -l backup.log -t -e -w

# Commandes DSRepair
dsrepair.rld

# Login à un autre serveur
login -s 137.65.123.255 -p 8028 -u admin.ma_société -w mon_mot_de_passe -n

# Commandes DSMerge
dsmerge.pr -u admin.ma_société -p admin.ma_société -n mon_mot_de_passe #
Opérations sur le schéma
dsschema.rst
dsschema.dse
dsschema.rls
dsschema.gsu
dsschema.scc
dsschema.irs -n Arborescence_Locale

# Commandes DSService
service.serviceList

# Fin de l'exemple.
```

Fichier système de traitement par lots

Comme avec d'autres outils de ligne de commande, vous pouvez créer des fichiers système de traitement par lots qui contiennent des commandes du client eMBox, et les exécuter manuellement dans la ligne de commande ou planifier leur exécution sans surveillance sur le serveur. Par exemple, vous pouvez effectuer des sauvegardes sans surveillance en utilisant des fichiers système de traitement par lots similaires à ceux des exemples décrits à la section « Sauvegardes sans surveillance à l'aide d'un fichier de traitement par lots et du client eMBox », page 422.

À partir d'un seul serveur, vous pouvez exécuter des tâches multiples à l'aide de plusieurs outils eMBox sur différents serveurs.

Dans un fichier système de traitement par lots, vous pouvez combiner des commandes individuelles du client eMBox et des fichiers internes de traitement par lots pour bénéficier d'une souplesse accrue et pour organiser et réutiliser les commandes que vous exécutez fréquemment. Pour plus d'informations, reportez-vous à la section « Fichier interne de traitement par lots », page 558 ci-dessus.

Pour des instructions sur l'exécution de fichiers de traitement par lots sans surveillance, consultez la documentation de votre système d'exploitation ou de votre logiciel de planification tiers.

REMARQUE : sous NetWare, vous pouvez utiliser un logiciel de planification tiers ou CRON.NLM (http://support.novell.com/servlet/tidfinder/2939440), un outil non pris en charge que vous pouvez télécharger sur le site du support technique de Novell.

Options du client à ligne de commande eMBox

Option	Description
-? ou -h	Affiche l'aide.
-i	Exécute les commandes eMBox l'une après l'autre en mode interactif.
-s *serveur*	Nom ou adresseIP du serveur eMBox. Valeur par défaut=127.0.0.1
-p *port*	Numéro de port du serveur eMBox. Valeur par défaut=80
-u *utilisateur*	DN utilisateur. Par exemple, admin.ma_société. Valeur par défaut=anonymous (anonyme)
-w *mot_de_passe*	Mot de passe associé à l'utilisateur spécifié par -u.
-m *mode*	Mode de login. Valeur par défaut=dclient
-n	Ne tente pas d'établir une connexion SSL sécurisée. Utilise une connexion non sécurisée. Si vous n'utilisez pas cette option, le client eMBox tente d'établir une connexion SSL et une erreur est renvoyée si vous ne disposez pas des fichiers JSSE dans votre chemin de classe. Pour plus d'informations, reportez-vous à la section « Établissement d'une connexion sécurisée avec le client eMBox », page 561.

Option	Description
-l *fichier_journal*	Nom du fichier journal.
-o	Écrase le fichier journal à son ouverture.
-T *timeout*	Délai d'attente (en secondes) des réponses du serveur.
-L *langue*	Liste des langues admises classées par ordre de préférence et séparées par des virgules. Par exemple : en-US,de_DE. L'option par défaut est la langue du système client.
-t [*outil*.]*options_ tâche*	Exécute un service unique avec cette connexion. La chaîne qui suit l'option -t doit être une commande eMBox valide.
-b *fichier_traitement_par_lots_ eMBox*	Exécute un groupe de services tel qu'il est spécifié dans le fichier de traitement par lots. Les commandes eMBox du fichier de traitement par lots doivent être placées sur des lignes distinctes. Les lignes précédées du signe# sont des commentaires.

Établissement d'une connexion sécurisée avec le client eMBox

Si vous utilisez une connexion non sécurisée, toutes les informations que vous entrez, telles que les noms d'utilisateur et mots de passe, sont envoyées en texte clair sur le réseau.

Si vous voulez établir une connexion sécurisée au moyen de SSL, procédez comme suit :

- Veillez à ne pas utiliser l'option-n dans votre commande lors du login à un serveur. Cette option spécifie en effet une connexion non sécurisée. La valeur par défaut est une connexion sécurisée.
- Vérifiez que les fichiers JSSE (Java Secure Socket Extension) suivants figurent dans votre chemin de classe:
  - jsse.jar
  - jnet.jar
  - jcert.jar

  Si ce n'est pas le cas, le client eMBox renvoie une erreur indiquant qu'il ne parvient pas à établir de connexion sécurisée.

  Pour obtenir ces fichiers, ainsi que des informations sur JSSE, reportez-vous au site Web de Sun (http://java.sun.com/products/jsse).

Recherche des numéros de port eDirectory

Lorsque vous vous loguez à un serveur du client eMBox, vous devez spécifier un numéro de port.

Si vous avez déjà indiqué un numéro de port lors de l'installation de eDirectory, utilisez ce numéro.

Les ports par défaut sont les suivants :

- Pour NetWare, par défaut, le port non sécurisé est8028 et le port sécurisé8009.
- Pour les autres plates-formes, par défaut, le port non sécurisé est8028, et le port sécurisé8010.

Les sections suivantes fournissent des conseils supplémentaires pour trouver le port assigné à eDirectory :

- « Sous Windows », page 562
- « Sous NetWare », page 562
- « Sous Linux et UNIX », page 562

Sous Windows

1. Cliquez sur Démarrer > Paramètres > Panneau de configuration.
2. Double-cliquez sur l'icône Services Novell eDirectory, puis cliquez sur l'onglet Transport.
3. Recherchez le port sécurisé ou non sécurisé.
   - Pour le port non sécurisé, cliquez sur le signe plus placé en regard de HTTP.
   - Pour le port sécurisé, cliquez sur le signe plus placé en regard de HTTPS.

   Cliquez sur le signe plus placé en regard de Transports liés pour afficher le numéro de port.

Sous NetWare

La propriété Adresse réseau d'un objet Serveur affiche les ports.

Vous pouvez consulter cette propriété dans les outils suivants :

- Dans iManager, consultez l'objet Serveur sous Administration de eDirectory > Modifier un objet, et recherchez l'adresse réseau dans la liste déroulante de l'onglet Général.
- Dans ConsoleOne®, cliquez avec le bouton droit sur l'objet Serveur ou sélectionnez-le, cliquez sur Objet > Propriétés, puis recherchez l'adresse réseau dans la liste déroulante.

Recherchez les adresses qui commencent par http: ou https: et finissent par « /portal ». Ce sont les ports non sécurisés et sécurisés utilisés par les outils eMBox.

Pour déterminer le numéro de port :

- Si un numéro de port apparaît dans l'adresse réseau, il s'agit du numéro qui a été assigné.

  Par exemple, http://137.65.188.1:8028/portal signifie que le port8028 est utilisé pour les outils eMBox.
- Si aucun numéro de portail n'apparaît et que seule l'adresse IP du serveur est visible, cela signifie que les numéros de port par défaut sont utilisés.

  Par exemple, https://137.65.188.1/portal n'affiche pas de numéro de port après l'adresse IP. Cela signifie que le numéro de portail sécurisé par défaut est utilisé pour les outils eMBox : 8009 sous NetWare, 8010 sur les autres plates-formes.

Sous Linux et UNIX

Vous pouvez utiliser la commande suivante pour afficher une liste de ports :

```
ndsconfig get | grep http
```

Recherchez les lignes qui contiennent http.server.interface suivi d'un numéro de port.

Vous pouvez également chercher le numéro de port dans iManager ou ConsoleOne, toujours en utilisant la méthode décrite à la section « Sous NetWare », page 562.

Utilisation de l'outil de consignation eMBox

L'outil de consignation eMBox est un module d'infrastructure qui consigne tous les événements pour l'ensemble des outils eMTools tels que DSBackup, DSMerge et DSRepair. Cette version est livrée avec un seul fichier journal dans lequel tous les outils eMTools consignent leurs opérations.

L'outil de consignation eMBox est différent du service de consignation du client qui est fourni via les fichiers journaux que vous spécifiez lorsque vous exécutez le client eMBox (par exemple, lorsque vous indiquez `-l monfichierjournal.txt` dans une commande du client eMBox ou que vous entrez `monfichierjournal.txt` en tant que nom de fichier journal dans iManager). Il enregistre tous les messages du serveur pour les tâches exécutées par eMBox, en affichant davantage de détails. Le service de consignation du client, quant à lui, enregistre les messages envoyés et reçus par le client, fournissant ainsi un rapport général sur la progression.

La consignation est asynchrone et toutes les opérations sont consignées par défaut.

Cette version de l'outil de consignation eMBox présente les caractéristiques suivantes :

- Possibilité de changer le nom et l'emplacement du fichier journal.

  Par défaut, les fichiers journaux sont créés dans le répertoire embox\log situé dans le répertoire d'installation de eDirectory.

- Possibilité de changer la taille maximale du fichier journal, après quoi ce fichier est réinitialisé.

  La taille maximale du fichier est 8Mo.

- Possibilité de changer de mode de consignation.

  Vous pouvez choisir d'annexer tous les nouveaux messages au fichier journal ou d'écraser un fichier journal existant. L'option Annexer (append) est définie par défaut.

- Possibilité de lancer et d'arrêter la consignation.

  Par défaut, l'outil de consignation est en mode Démarrage au lancement de eMBox. Par opposition, aucun message n'est consigné en mode Arrêt.

- Possibilité de réinitialiser le contenu du fichier journal.

- Possibilité de lire le fichier journal à partir d'un poste client.

Cette section fournit les informations suivantes :

- « Utilisation du client à ligne de commande « outil de consignation eMBox » », page 564
- « Utilisation de la fonction « outil de consignation eMBox » dans Novell iManager », page 564

Utilisation du client à ligne de commande « outil de consignation eMBox »

Le tableau suivant liste les options du client à ligne de commande « outil de consignation eMBox » :

Option	Description
logstart	Démarre l'outil de consignation eMBox.
logstop	Arrête l'outil de consignation eMBox.
readlog	Affiche le fichier journal en cours.
getlogstate	Affiche l'état actuel de l'outil de consignation eMBox (Démarrage/Arrêt).
getloginfo	Affiche le nom, le mode de consignation (Annexer/Écraser) et les tailles maximale et actuelle du fichier journal eMBox.
setloginfo [-f *nom_fichier*] [-s *taille_en_kilo-octets*] [-a | -o]	Permet de définir le nom, la taille et le mode de consignation (Annexer/Écraser) du fichier journal eMBox à l'aide des paramètres suivants : ◆ -f *nom_fichier* Nom du fichier journal eMBox. ◆ -s *taille_en_Ko* Taille maximale du fichier journal. ◆ -a Les nouveaux messages de journal sont annexés au journal actuel. ◆ -o Le fichier journal est écrasé.
emptylog	Efface le contenu du fichier journal du serveur.

Utilisation de la fonction « outil de consignation eMBox » dans Novell iManager

1. Dans Novell iManager, cliquez sur le bouton Rôles et tâches  .
2. Cliquez sur Utilitaires de maintenance eDirectory > Fichiers journaux.
3. Indiquez quel serveur effectuera l'opération de fichier journal, puis cliquez sur Suivant.
4. Authentifiez-vous auprès du serveur, puis cliquez sur Suivant.
5. Sélectionnez l'opération de fichier journal à effectuer.

   Cliquez sur Aide pour obtenir des détails.

A Remarques sur NMAS

Cette annexe comprend les rubriques suivantes :

Configuration d'un conteneur Sécurité en tant que partition distincte

NMAS™ (Novell® Modular Authentication Services) repose sur le stockage de règles qui s'appliquent à la totalité de l'arborescence Novell eDirectory™. L'arborescence eDirectory représente en réalité le domaine de sécurité. Les règles de sécurité doivent être accessibles à tous les serveurs de l'arborescence.

NMAS place les règles d'authentification et les données de configuration des méthodes de login dans le conteneur Sécurité créé au niveau de la racine dans les arborescences eDirectory sous NetWare® version 5.1 ou ultérieure. Ces informations doivent être facilement accessibles pour tous les serveurs qui utilisent NMAS. Le conteneur Sécurité sert à regrouper les règles globales relatives aux propriétés de sécurité, telles que le login, l'authentification et la gestion des clés.

Avec NMAS, il est recommandé de créer le conteneur Sécurité en tant que partition distincte et de le répliquer largement. Cette partition doit être répliquée en tant que partition Lecture/écriture uniquement sur les serveurs de votre arborescence qui sont approuvés.

REMARQUE : étant donné que le conteneur Sécurité contient des règles globales, soyez attentifs à l'emplacement des répliques accessibles en écriture car ces serveurs peuvent modifier les règles de sécurité générales spécifiées dans l'arborescence eDirectory. Pour que les utilisateurs se loguent avec NMAS, les répliques des objets Utilisateur doivent se trouver sur le serveur NMAS.

Fusion d'arborescences avec plusieurs conteneurs Sécurité

Il convient d'être particulièrement prudent lors de la fusion d'arborescences eDirectory si l'une d'elles au moins comporte un conteneur Sécurité. Vérifiez qu'il s'agit bien d'une opération que vous souhaitez vraiment réaliser. Cette procédure peut en effet être longue et fastidieuse.

IMPORTANT : les instructions suivantes concernent des arborescences avec Novell Certificate Server™ versions 2.21 et antérieures, Novell Single Sign-on version 2.*x* et NMAS 2.*x*.

Pour fusionner des arborescences avec plusieurs conteneurs Sécurité :

1. Dans iManager, identifiez les arborescences à fusionner.
2. Identifiez les arborescences source et cible.

Tenez compte des remarques suivantes concernant la sécurité pour les arborescences source et cible :

- Tous les certificats signés par l'autorité de certification organisationnelle de l'arborescence source doivent être supprimés.
- Cette autorité doit elle-même être supprimée.
- Tous les secrets d'utilisateur enregistrés dans Novell SecretStore® sur l'arborescence source doivent être supprimés.
- Toutes les méthodes de login NMAS de l'arborescence source doivent être supprimées et réinstallées dans l'arborescence cible.
- Tous les utilisateurs NMAS de l'arborescence source doivent être réinscrits une fois les arborescences fusionnées.
- Tous les utilisateurs et serveurs qui se trouvaient dans l'arborescence source doivent disposer de nouveaux certificats créés après la fusion des arborescences.
- Les secrets de tous les utilisateurs qui se trouvaient dans l'arborescence source doivent être réinstallés dans SecretStore.

S'il n'existe pas de conteneur appelé Sécurité à la racine des arborescences source et cible, ou s'il en existe un dans une seule des deux arborescences, aucune autre action n'est nécessaire. Sinon, poursuivez la procédure.

Opérations à effectuer par produit avant une fusion d'arborescences

Cette section comprend les informations suivantes :

- « Novell Certificate Server », page 566
- « Novell Single Sign-on », page 568
- « NMAS », page 568
- « Infrastructure du domaine de sécurité Novell », page 569
- « Autres opérations de sécurité », page 569

Novell Certificate Server

Si Novell Certificate Server, anciennement appelé PKIS (Public Key Infrastructure Services), est installé sur un ou plusieurs serveurs de l'arborescence source, procédez comme suit.

REMARQUE : selon l'utilisation du produit, les objets et éléments auxquels il est fait référence peuvent ne pas être présents. Si les objets et éléments cités dans une étape donnée ne sont pas présents dans l'arborescence source, vous pouvez ignorer l'étape.

1. Tous les certificats de racine approuvée dans l'arborescence source doivent être installés dans l'arborescence cible.

   Les certificats de racine approuvée sont stockés dans des objets Racine approuvée, eux-mêmes placés dans des conteneurs Racine approuvée. Les conteneurs Racine approuvée peuvent être créés à n'importe quel endroit de l'arborescence. Cependant, seuls les certificats Racine approuvée se trouvant dans les conteneurs Racine approuvée du conteneur Sécurité doivent être déplacés manuellement depuis l'arborescence source vers l'arborescence cible.

2 Installez les certificats de racine approuvée dans l'arborescence cible.

2a Sélectionnez un conteneur Racine approuvée dans le conteneur Sécurité de l'arborescence source.

2b Créez un conteneur Racine approuvée dans le conteneur Sécurité de l'arborescence cible en conservant le nom exact utilisé dans l'arborescence source (étape2a).

2c Dans l'arborescence source, ouvrez un objet Racine approuvée dans le conteneur du même nom sélectionné et exportez le certificat.

IMPORTANT : notez l'emplacement et le nom du fichier utilisé ; vous en aurez besoin à la prochaine étape.

2d Dans l'arborescence cible, créez un objet Racine approuvée dans le conteneur créé à l'étape 2b. Indiquez le même nom que pour l'arborescence source et, lorsque vous êtes invité à préciser le certificat, spécifiez le fichier créé à l'étape 2c.

2e Supprimez l'objet Racine approuvée de l'arborescence source.

2f Répétez la procédure de l'étape 2c à l'étape 2e jusqu'à ce que tous les objets Racine approuvée du conteneur Racine approuvée sélectionné soient installés dans l'arborescence cible.

2g Supprimez le conteneur Racine approuvée de l'arborescence source.

2h Répétez la procédure de l'étape 2a à l'étape 2f jusqu'à ce que tous les conteneurs Racine approuvée soient supprimés de l'arborescence source.

3 Supprimez l'autorité de certification organisationnelle dans l'arborescence source.

L'objet Autorité de certification organisationnelle se trouve dans le conteneur Sécurité.

IMPORTANT : après cette étape, tous les certificats signés par l'autorité de certification organisationnelle de l'arborescence source sont inutilisables. C'est notamment le cas des certificats utilisateur et de serveur signés par l'autorité de certification organisationnelle de l'arborescence source.

4 Supprimez tous les objets Matériel clé (KMO Key Material Object) de l'arborescence source possédant un certificat signé par l'autorité de certification organisationnelle de l'arborescence source.

Les objets Matériel clé de l'arborescence source possédant des certificats signés par d'autres autorités de certification restent valides et n'ont pas à être supprimés.

Si vous n'êtes pas sûr de l'identité de l'autorité de certification apposant sa signature pour un objet Matériel clé, consultez la section Certificat de racine approuvée de l'onglet Certificats sur la page de propriétés de l'objet Matériel clé.

5 Supprimez tous les certificats utilisateur de l'arborescence source signés par l'autorité de certification organisationnelle de cette arborescence.

Si les utilisateurs de l'arborescence source ont déjà exporté leurs certificats et clés privées, ces derniers restent utilisables. Les clés privées et les certificats restant dans eDirectory ne peuvent par contre plus être utilisés une fois l'étape 3 effectuée.

Pour chaque utilisateur disposant de certificats, ouvrez les propriétés de l'objet Utilisateur. La liste de tous les certificats pour l'utilisateur s'affiche dans la section Certificats de l'onglet Sécurité. Tous les certificats émis par l'autorité de certification organisationnelle doivent être supprimés.

Les certificats utilisateur ne seront présents dans l'arborescence source que si Novell Certificate Server version 2.0 ou ultérieure est installé sur le serveur qui héberge l'autorité de certification organisationnelle de cette arborescence.

Novell Single Sign-on

Si Novell Single Sign-on est installé sur un ou plusieurs serveurs de l'arborescence source, vous devez supprimer tous les secrets Novell Single Sign-on pour les utilisateurs de l'arborescence source.

Pour chaque utilisateur qui emploie Novell Single Sign-on dans l'arborescence source, ouvrez les propriétés de l'objet Utilisateur. Tous les secrets de l'utilisateur sont listés dans la section SecretStore de l'onglet Sécurité. Supprimez tous les secrets de la liste.

REMARQUE : selon l'utilisation du produit, les objets et éléments auxquels il est fait référence peuvent ne pas être présents. S'ils ne se trouvent pas dans l'arborescence source, vous pouvez ignorer cette étape.

NMAS

Si NMAS est installé sur un ou plusieurs serveurs de l'arborescence source, procédez comme suit.

REMARQUE : selon l'utilisation du produit, les objets et éléments auxquels il est fait référence peuvent ne pas être présents. S'ils ne se trouvent pas dans l'arborescence source, vous pouvez ignorer cette étape.

1. Dans l'arborescence cible, installez toutes les méthodes de login NMAS qui se trouvaient dans l'arborescence source et pas dans l'arborescence cible.

   Pour vous assurer que tous les composants de login client et serveur nécessaires sont correctement installés dans l'arborescence cible, nous vous recommandons d'installer les nouvelles méthodes de login en utilisant des sources Novell d'origine ou des sources proposées par le fournisseur.

   Bien que les méthodes *puissent* être réinstallées à partir des fichiers serveur existants, il est généralement plus simple et plus fiable de procéder à une installation à partir de paquetages fournis par Novell ou par le fournisseur.

2. Pour garantir que les séquences de login précédemment établies dans l'arborescence source sont disponibles dans l'arborescence cible, migrez les séquences de login souhaitées.

   2a Dans ConsoleOne, sélectionnez le conteneur Sécurité de l'arborescence source.

   2b Cliquez avec le bouton droit sur l'objet Règle de login, puis sélectionnez Propriétés.

   2c Pour chaque séquence de login figurant dans la liste déroulante Séquences de login définies, notez les méthodes de login utilisées (affichées dans le volet droit).

   2d Sélectionnez le conteneur Sécurité dans l'arborescence cible et répliquez les séquences de login en utilisant les mêmes méthodes de login qu'à l'étape2c.

   2e Cliquez sur OK lorsque vous avez terminé.

3. Supprimez les attributs de sécurité de login NMAS dans l'arborescence source.

   3a Dans le conteneur Sécurité de l'arborescence source, supprimez l'objet Règle de login.

   3b Dans le conteneur Méthodes de login autorisées de l'arborescence source, supprimez toutes les méthodes de login.

   3c Supprimez le conteneur Méthodes de login autorisées de l'arborescence source.

   3d Dans le conteneur Méthodes de post-login autorisées de l'arborescence source, supprimez toutes les méthodes de login.

   3e Supprimez ensuite le conteneur Méthodes de post-login autorisées de l'arborescence source.

Infrastructure du domaine de sécurité Novell

Si Novell Certificate Server version2.x ou ultérieure, Novell Single Sign-on, NMAS, NetWare version5.1 ou ultérieure ou eDirectory version8.5 ou ultérieure est installé sur un ou plusieurs serveurs de l'arborescence source, l'infrastructure du domaine de sécurité Novell (SDI Security Domain Infrastructure) est installée. Dans ce cas, procédez comme suit.

REMARQUE : selon l'utilisation du produit, les objets et éléments auxquels il est fait référence peuvent ne pas être présents. S'ils ne se trouvent pas dans l'arborescence source, vous pouvez ignorer cette étape.

1. Supprimez l'objetW0 et le conteneur KAP de l'arborescence source.

   Le conteneur KAP se trouve dans le conteneur Sécurité. L'objet W0 se trouve dans le conteneur KAP.

2. Sur tous les serveurs de l'arborescence source, effacez les clés SDI en supprimant le fichier sys:\system\nici\nicisdi.key.

   IMPORTANT : veillez à supprimer ce fichier sur tous les serveurs de l'arborescence source.

Autres opérations de sécurité

Si un conteneur Sécurité existe dans l'arborescence source, supprimez-le avant de fusionner les arborescences.

Fusion des arborescences

L'utilitaire ndsmerge permet de fusionner les arborescences eDirectory. Pour plus d'informations, reportez-vous au Chapitre 8, « Fusion d'arborescences Novell eDirectory », page 221 et à l'Annexe B, « Commandes Novell eDirectory pour Linux et UNIX et syntaxe correspondante », page 571.

Opérations à effectuer par produit après la fusion

Cette section comprend les informations suivantes :

Infrastructure du domaine de sécurité Novell

Si l'objet W0 existait dans l'arborescence cible avant la fusion, les clésSDI utilisées par les serveurs résidant précédemment dans l'arborescence cible doivent être installées sur les serveurs qui résidaient précédemment dans l'arborescence source.

La solution la plus simple consiste à installer Novell Certificate Server version 2.52 ou ultérieure sur tous les serveurs précédemment installés dans l'arborescence source, qui possédaient des clés SDI (fichier sys:\system\nici\nicisdi.key). Cette opération doit être réalisée même si Novell Certificate Server est déjà installé sur le serveur.

Si l'objet W0 n'existait pas dans l'arborescence cible avant la fusion mais existait dans l'arborescence source, la SDI doit être réinstallée dans l'arborescence obtenue.

La solution la plus simple consiste à installer Novell Certificate Server version 2.52 ou ultérieure sur les serveurs de la nouvelle arborescence. Novell Certificate Server doit être installé sur tous les serveurs se trouvant précédemment dans l'arborescence source, qui hébergeaient les clés SDI (fichier sys:\system\nici\nicisdi.key). Il peut aussi être installé sur d'autres serveurs de la nouvelle arborescence.

Pour plus d'informations sur l'installation de Novell Certificate Server, consultez le manuel *Novell Certificate Server Administration Guide (Guide d'administration du serveur de certificats Novell)* (http://www.novell.com/documentation/beta/crt30/index.html).

Novell Certificate Server

Si vous utilisez Novell Certificate Server, après la fusion des arborescences, émettez de nouveau, si nécessaire, des certificats pour les serveurs et les utilisateurs qui se trouvaient auparavant dans l'arborescence source.

Nous vous recommandons d'installer Novell Certificate Server version 2.52 ou ultérieure sur tous les serveurs qui comportent une réplique de la partition contenant un objet Utilisateur.

Pour que vous puissiez émettre un certificat pour un serveur, Novell Certificate Server version 2.52 ou ultérieure doit être installé.

Novell Certificate Server version 2.52 ou ultérieure doit être installé sur le serveur qui héberge l'autorité de certification organisationnelle. Pour plus d'informations, consultez le manuel *Novell Certificate Server Administration Guide (Guide d'administration du serveur de certificats Novell)* (http://www.novell.com/documentation/beta/crt30/index.html).

Novell Single Sign-On

Si vous utilisez Novell Single Sign-on, après la fusion des arborescences, recréez si nécessaire des secrets SecretStore pour les utilisateurs qui se trouvaient auparavant dans l'arborescence source.

NMAS

Si vous utilisez NMAS, après la fusion des arborescences, réinscrivez si nécessaire les utilisateurs NMAS qui se trouvaient auparavant dans l'arborescence source.

Pour plus d'informations, consultez le manuel *Novell Modular Authentication Service Administration Guide (Guide d'administration de Novell Modular Authentication Service)* (http://www.novell.com/documentation/beta/nmas30/index.html).

B Commandes Novell eDirectory pour Linux et UNIX et syntaxe correspondante

Ce chapitre présente les utilitaires pour Novell® eDirectory™8.8 sous Linux, Solaris, AIX et HP-UX, ainsi que leur syntaxe:

Utilitaires généraux

Cette section contient la liste des utilitaires eDirectory pour Linux et UNIX et décrit leur syntaxe.

REMARQUE : pour plus d'informations sur l'utilisation de ces utilitaires, reportez-vous aux pages du manuel des utilitaires.

Commande	Description	Syntaxe
nds-install	Utilitaire d'installation des composants Novell eDirectory.	`nds-install [-c composant1 [-c composant2]...] [-h] [--help] [-i] [-j] [-u]`

Commande	Description	Syntaxe
ndsconfig	Configure Novell eDirectory	ndsconfig new [-m <nom_module>] [-i] [-S <nom_serveur>] [-t <nom_arborescence>] [-n <contexte_serveur>] [-d <chemin_DIB>] [-L <port_ldap>] [-l <port_ssl>] [-o port_http] [-O port_https] [-e] -a <FDN_admin> [-b <port_à_connecter>] [-B <interface1@port1, interface2@port2,..>] [-D <emplacement_personnalisé>] [--config-file <fichier_configuration>] ndsconfig def [-m <nom_module>] [-i] [-S <nom_serveur>] [-t <nom_arborescence>] [-n <contexte_serveur>] [-d <chemin_DIB>] [-L <port_ldap>] [-l <port_ssl>] [-o port_http] [-O port_https] [-e] -a <FDN_admin> [-D <emplacement_personnalisé>] [--config-file <fichier_configuration>] ndsconfig add [-m <nom_module>] [-S <nom_serveur>] [-t <nom_arborescence>] [-p <adresse_IP:port>] [-n <contexte_serveur>] [-d <chemin_DIB>] [-L <port_ldap>] [-l <port_ssl>] [-o port_http] [-O port_https] [-e] -a <FDN_admin> [-b <port_à_connecter>] [-B <interface1@port1, interface2@port2,..>] [-D <emplacement_personnalisé>] [-E] [--config-file <fichier_configuration>] ndsconfig rm [-a <FDN_admin>] [-b <port_à_connecter>] [--config-file <fichier_configuration>] ndsconfig upgrade [-a <FDN_admin>] [-j] [--config-file <fichier_configuration>] ndsconfig {set <liste_valeurs> | get [<liste_paramètres>] | get help [<liste_paramètres>]}
ndscheck	Utilitaire qui vérifie l'état de santé de l'arborescence.	ndscheck [-h <nom_hôte:port>] [-a <FDN_admin>] [-F <nom_fichier_journal>] [--config-file <nom_et_chemin_fichier_configuration>] --version
ndsmanage	Utilitaire listant les instances eDirectory.	ndsmanage [-a] ndsmanage [<nom_utilisateur>]

Commande	Description	Syntaxe
ndsbackup	Crée des archives d'objets eDirectory et ajoute ou extrait des objets eDirectory	`ndsbackup c [fevwXR] [fichier_ndsbackup] [fichier_exclusion] [nom_serveur_réplique] [-a utilisateur_admin] [-I fichier_inclusion] [-E mot_de_passe] [--config-file <chemin_fichier_configuration>]... [objet_eDirectory]` `ndsbackup r [fevwXR] [fichier_ndsbackup] [fichier_exclusion] [nom_serveur_réplique] [-a utilisateur_admin] [-I fichier_inclusion] [-E mot_de_passe] [--config-file <chemin_fichier_configuration>]... [objet_eDirectory]` `ndsbackup t [fevwXR] [fichier_ndsbackup] [fichier_exclusion] [nom_serveur_réplique] [-a utilisateur_admin] [-I fichier_inclusion] [-E mot_de_passe] [--config-file <chemin_fichier_configuration>]... [objet_eDirectory]` `ndsbackup x [fevwXR] [fichier_ndsbackup] [fichier_exclusion] [nom_serveur_réplique] [-a utilisateur_admin] [-I fichier_inclusion] [-E mot_de_passe] [--config-file <chemin_fichier_configuration>]... [eDirectoryobject]ndsbackup s [evXR] [fichier_exclusion] [nom_serveur_réplique] [-a utilisateur_admin] [-I fichier_inclusion] [-E mot_de_passe] [--config-file <chemin_fichier_configuration>]... [objet_eDirectory]`  `ndsbackup --version`
ndslogin	Utilitaire de diagnostic pour la vérification de l'authentification Novell eDirectory	`ndslogin [-t <nom_arborescence>] [-h nom_hôte[:port]] [-p mot_de_passe] [-s] <FDN_utilisateur> [--config-file <chemin_fichier_configuration>]`
ndsd	Daemon NDS®	`/opt/novell/eDirectory/sbin/ndsd [--config-file` *`fichier_config`*`]` **Remarque :** vous devez arrêter ndsd avant de redémarrer Solaris. Entrez **`/etc/init.d/ndsd stop`**. Pour une installation non racine ou à un emplacement personnalisé, utilisez ndsmanage pour arrêter l'instance.
ndsimonitor	Surveille et diagnostique les serveurs de l'arborescence Novell eDirectory à l'aide de HTTP	`/opt/novell/eDirectory/bin/ndsimonitor [-l [-d <chemin_fichiers_configuration_ndsimonitor> ] | u] [-h <interface_locale:port>] [--config-file <chemin_fichier_configuration>]`

Commande	Description	Syntaxe
ndsmerge	Utilitaire de fusion de deux arborescences Novell eDirectory	`ndsmerge [-m arborescence_cible admin_cible admin_source [conteneur_cible]] [-c] [-t] [-r arborescence_cible admin_source] [-h <interface_locale:port>] [--config-file <chemin_fichier_configuration>]`

ndsrepair	Utilitaire de réparation et de résolution des problèmes de la base de données Novell eDirectory, au niveau des enregistrements, du schéma, des objets de Bindery et des références externes	`ndsrepair {-U |-E |-C |-P [Ad] |-S [Ad]|-N |-T |-J <id_entrée>} [-A <oui/non>] [-O <oui/non>][-F nom_fichier] [-h <interface_locale:port>] [--config-file <chemin_fichier_configuration>]`
		
		`ndsrepair -R [-l <oui/non>][-u <oui/non>][-m <oui/non>][-i <oui/non>][-f <oui/non>][-d <oui/non>][-t <oui/non>][-o <oui/non>][-r <oui/non>][-v <oui/non>][-c <oui/non>][-A <oui/non>][-O <oui/non>][-F nom_fichier] [-h <interface_locale>] [--config-file <chemin_fichier_configuration>]`

ndssch	Utilitaire d'extension de schéma Novell eDirectory	`ndssch [-h <nom_hôte>[:<port>]][-t <nom_arborescence>] <FDN_admin> <fichier_schéma> ...`
		
		`ndssch [-h <nom_hôte>[:<port>]][-t <nom_arborescence>] [-d] <FDN_admin> <fichier_schéma> [description_schéma] ...`

ndssnmp	Module de services SNMP pour Novell eDirectory	`/opt/novell/eDirectory/bin/ndssnmp`
ndssnmpconfig	Utilitaire de configuration des trappes SNMP	`ndssnmpconfig -h [nom_hôte[:port]] -p <mot_de_passe> -a <FDN_utilisateur> -c <commande>`
ndssnmpsa	Daemon de sous-agent SNMP eDirectory	`/opt/novell/eDirectory/bin/ndssnmpsa`
ndsstat	Utilitaire d'affichage des informations sur le serveur	`ndsstat [-h nom_hôte[:port]] { -r -s } [--config-file <chemin_fichier_configuration>]`
ndstrace	Utilitaire d'affichage des messages de débogage du serveur	`ndstrace [-l|-u|-c "commande1;....."|--version] [-h <interface_locale:port>] [--config-file <chemin_fichier_configuration>]`
nds-uninstall	Utilitaire de désinstallation de Novell eDirectory	`nds-uninstall -c <composant1> [[-c <composant2>]...] [-h]`
nldap	Services LDAP pour le daemon NDS	`/opt/novell/eDirectory/sbin/nldap`

nmasinst	Utilitaire de configuration de NMAS™	`nmasinst -i <FDN_admin> <nom_arborescence> [-h <nom_hôte>[:port]]`
		
		`nmasinst -addmethod <FDN_admin> <nom_arborescence> >fichier_config.txt< [-h <nom_hôte>[:port]]`

npki	Services PKI de Novell	`/opt/novell/eDirectory/sbin/npki`

Commandes spécifiques de LDAP

Commande	Description	Syntaxe

ldapconfig	Utilitaire de configuration des objets Serveur LDAP et Groupe LDAP	`ldapconfig get [...] | set <liste_valeurs_attribut> [-t nom_arborescence | -p nom_hôte[:port] | --config-file <fichier_configuration>] [-w mot_de_passe] [-a <FDN_utilisateur>] [-f]`
		
		`ldapconfig [-t nom_arborescence | -p nom_hôte[:port]] [-w mot_de_passe | --config-file <fichier_configuration>] [-a <FDN_utilisateur>] [-V] [-R] [-H] [-f] -v <attribut>,<attribut2>...`
		
		`ldapconfig [-t nom_arborescence | -p nom_hôte[:port] | --config-file <fichier_configuration>] [-w mot_de_passe] [-a <FDN_admin>] [-V] [-R] [-H] [-f] -s <attribut>=<valeur>,...`

ldapadd
ldapmodify
	Ajoute ou modifie des entrées d'un serveur LDAP	`ldapmodify [-a] [-c] [-C] [-M] [-P] [-r] [-n] [-v] [-F] [-l limite] [-M[M]] [-d niveau_débogage] [-e nom_fichier_clé] [-D DN_liaison] [[-W]|[-w mot_de_passe]] [-h hôte_LDAP] [-p port_LDAP] [-P version] [-Z[Z]] [-f fichier]`
		
		`ldapadd [-c] [-C] [-l] [-M] [-P] [-r] [-n] [-v] [-F] [-l limite] [-M[M]] [-d niveau_débogage] [-e nom_fichier_clé] [-D DN_liaison] [[-W ]| [-w mot_de_passe]] [-h hôte_ldap] [-p port_ldap] [-P version] [-Z[Z]] [-f fichier]`

ldapdelete	Supprime les entrées d'un serveur LDAP	`ldapdelete [-n] [-v] [-c] [-r] [-l] [-C] [-M] [-d niveau_débogage] [-e nom_fichier_clé] [-f fichier] [-D DN_liaison] [[-W]| [-w mot_de_passe]] [-h hôte_LDAP] [-p port_LDAP] [-Z[Z]] [dn]...`
ldapmodrdn	Outil de modification du nom distinctif relatif (RDN) des entrées LDAP	`ldapmodrdn [-r] [-n] [-v] [-c] [-C] [-l] [-M] [-s nouveau_supérieur] [-d niveau_débogage] [-e nom_fichier_clé] [-D DN_liaison] [[-W]|[-w mot_de_passe]] [-h hôte_LDAP] [-p port_LDAP] [-Z[Z]] [-f fichier] [dn nouveau_RDN]`
ldapsearch	Outil de recherche LDAP	`ldapsearch [-n] [-u] [-v] [-t] [-A] [-T] [-C] [-V] [-M] [-P] [-L] [-d niveau_débogage] [-e nom_fichier_clé] [-f fichier] [-D DN_liaison] [[-W]| [-w mot_de_passe_liaison]] [-h hôte_LDAP] [-p port_LDAP] [-b base_recherche] [-s étendue] [-a suppr_réf] [-l limite_temps] [-z limite_taille] [-Z[Z]] filter [attributs....]`

Commande	Description	Syntaxe

ndsindex	Utilitaire permettant de créer, de lister, de suspendre, de reprendre ou de supprimer des index de base de données Novell eDirectory	`ndsindex list [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w <mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] [<nom_index1>, <nom_index2>.....]`
		
		`ndsindex add [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w <mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] <définition_index1> [<définition_index2>.....]`
		
		`ndsindex delete [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w <mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] <nom_index1> [<nom_index2>.....]`
		
		`ndsindex resume [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w <mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] <nom_index1> [<nom_index2>.....]`
		
		`ndsindex suspend [-h <nom_hôte>] [-p <port>] -D <DN_liaison> -W|[-w <mot_de_passe>] [-l limite] -s <DN_serveur_eDirectory> [-Z[Z]] <nom_index1> [<nom_index2>.....]`

C Configuration de OpenSLP pour eDirectory

Destinée aux administrateurs réseau, cette annexe contient des informations sur la configuration des installations OpenSLP pour Novell® eDirectory™, sans le client Novell®.

Protocole SLP (Service Location Protocol)

OpenSLP est une mise en oeuvre open-source de la norme IETF Service Location Protocol version2.0, documentée sur le site IETF Request-For-Comments (RFC)2608 (http://www.ietf.org/rfc/rfc2608.txt?number=2608).

Outre la mise en oeuvre du protocole SLPv2, l'interface fournie par le code source OpenSLP est une implémentation d'une autre norme de l'IETF concernant l'accès par programme à la fonctionnalité SLP, documentée sous RFC 2614 (http://www.ietf.org/rfc/rfc2614.txt?number=2614).

Pour bien comprendre le fonctionnement de SLP, il est recommandé de lire ces deux documents et de les assimiler. Leur lecture peut s'avérer laborieuse, mais ils sont essentiels pour procéder à une configuration correcte de SLP sur un intranet.

Pour plus d'informations sur le projet OpenSLP, consultez les sites Web OpenSLP (http://www.OpenSLP.org) et SourceForge (http://sourceforge.net/projects/openslp). Le site Web OpenSLP contient plusieurs documents qui offrent de précieux conseils de configuration. Un grand nombre de ces documents sont encore incomplets à la date de rédaction de la présente documentation.

Concepts fondamentaux de SLP

Le protocole SLP spécifie trois composants:

- L'agent Utilisateur (UA)
- L'agent de service (SA)
- L'agent Annuaire (DA)

La fonction de l'agent utilisateur est de fournir une interface par programmation aux clients pour les requêtes de services, et aux services pour leur permettre de s'annoncer. Un agent Utilisateur contacte un agent Annuaire pour émettre des requêtes pour des services enregistrés d'une classe de service et d'une étendue spécifiées.

La tâche de l'agent de service consiste à fournir des points de stockage et de maintenance constants pour les services locaux enregistrés auprès de SLP. L'agent de service a pour tâche principale de gérer une base de données en mémoire des services locaux enregistrés. En fait, un service ne peut pas s'enregistrer auprès de SLP tant qu'un agent de service local n'est pas présent. Les clients ne peuvent identifier les services qu'au moyen d'une bibliothèque d'agent Utilisateur, mais l'enregistrement requiert un agent de service, principalement parce que ce dernier doit régulièrement vérifier l'existence de services enregistrés pour maintenir l'enregistrement avec des agents Annuaire à l'écoute.

Le travail de l'agent Annuaire consiste à fournir un cache persistant à long terme pour les services annoncés ainsi qu'un point d'accès permettant aux agents Utilisateur de rechercher des services. En tant que cache, l'agent Annuaire reste à l'écoute de l'annonce de nouveaux services par les agents de service et met en cache ces notifications. À court terme, le cache d'un agent Annuaire se complète. Les agents Annuaire utilisent un algorithme d'expiration pour faire expirer les entrées de cache. Lorsqu'un agent Annuaire s'active, il lit le cache du stockage persistant (en général un disque dur), puis commence à faire expirer les entrées selon l'algorithme. Lorsqu'un nouvel agent Annuaire arrive ou lorsqu'un cache a été supprimé, l'agent Annuaire détecte cette condition et envoie une notification spéciale à tous les agents Service à l'écoute pour qu'ils vident leurs bases de données locales, de manière à ce que l'agent Annuaire puisse rapidement créer son cache.

En l'absence d'agents Annuaire, l'agent Utilisateur effectue une requête de multidiffusion générale à laquelle les agents de service peuvent répondre listant ainsi les services demandés de la même manière que les agents Annuaire créent leur cache. La liste des services renvoyée par une telle requête est incomplète et bien plus localisée que celle fournie par un agent Annuaire, notamment en présence d'un filtrage multidiffusion mis en uvre par un grand nombre d'administrateurs réseaux, lesquels limitent les diffusions et les multidiffusions au sous-réseau local seulement.

En bref, tout s'articule autour de l'agent Annuaire trouvé par un agent Utilisateur dans une étendue donnée.

Protocole SLP Novell

La version Novell de SLP prend certaines libertés vis-à-vis de la norme SLP afin de fournir un environnement d'annonce de service renforcé, mais au prix d'une certaine évolutivité.

Par exemple, pour améliorer l'évolutivité d'une structure d'annonce de service, nous cherchons à limiter le nombre de paquets diffusés ou multidiffusés sur un sous-réseau. La norme SLP gère ce facteur en imposant des limitations aux agents de service et Utilisateur concernant les requêtes à l'agent Annuaire. Le premier agent Annuaire identifié qui dessert l'étendue souhaitée est celui qu'un agent de service (et par conséquent des agents Utilisateur locaux) utilisera pour toutes les requêtes futures sur cette étendue.

La mise en oeuvre de Novell SLP permet d'analyser tous les agents Annuaire connus, à la recherche des informations de la requête. Un aller-retour de 300millisecondes étant considéré comme trop long, 10 serveurs peuvent être balayés en 3à 5secondes. Il n'est pas nécessaire d'effectuer cette opération si SLP est configuré correctement sur le réseau et que OpenSLP considère le réseau comme configuré correctement pour le trafic SLP. Les valeurs de timeout de réponse de OpenSLP sont supérieures à celles du prestataire de services SLP de Novell, ce qui limite le nombre d'agents Annuaire au premier qui répond, que ses informations soient ou non précises et complètes.

Agents Utilisateur

Un agent Utilisateur prend la forme physique d'une bibliothèque statique ou dynamique liée à une application. Il permet à l'application d'émettre des requêtes de services SLP.

Les agents Utilisateur suivent un algorithme pour obtenir l'adresse d'un agent Annuaire auquel envoyer les requêtes. Une fois qu'ils ont obtenu une adresse d'agent Annuaire sur une étendue spécifiée, ils continuent à utiliser cette adresse pour cette étendue jusqu'à ce qu'elle ne réponde plus. Là, ils se procurent une autre adresse pour l'étendue. Les agents Utilisateur localisent l'adresse d'un agent Annuaire sur une étendue spécifiée en :

1. vérifiant si l'identificateur de socket de la requête en cours est connecté à un agent Annuaire pour l'étendue indiquée. (S'il se trouve que la requête fait partie d'une requête en plusieurs parties, il peut déjà exister une connexion en cache dans la requête.) ;
2. recherchant dans le cache de l'agent Annuaire connu un agent Annuaire correspondant à l'étendue indiquée ;
3. recherchant auprès de l'agent de service un agent Annuaire de l'étendue spécifiée (et en ajoutant de nouvelles adresses au cache) ;
4. interrogeant DHCP pour obtenir des adresses d'agents Annuaire configurées pour le réseau et correspondant à l'étendue indiquée (et en ajoutant de nouvelles adresses au cache) ;
5. envoyant une requête d'identification d'agent Annuaire par multidiffusion sur un port connu (et en ajoutant de nouvelles adresses au cache).

L'étendue indiquée est celle « par défaut », sauf spécification contraire. Cela signifie que si aucune étendue n'est définie de façon statique dans le fichier de configuration SLP et qu'aucune étendue n'est indiquée dans la requête, alors l'étendue utilisée est le mot « default ». Notez également que eDirectory n'indique jamais d'étendue dans ses enregistrements. Cela ne signifie pas pour autant que l'étendue utilisée avec eDirectory soit toujours « default ». En fait, si aucune étendue n'est spécifiée, mais qu'il en existe une configurée statiquement, cette dernière devient l'étendue par défaut pour toutes les requêtes à l'agent Utilisateur local et les enregistrements de l'agent de service.

Agents de service

Les agents de service prennent la forme physique d'un processus distinct exécuté sur la machine hôte. Dans le cas de Win32, slpd.exe s'exécute en tant que service sur l'ordinateur local. Des agents Utilisateur interrogent l'agent de service local en envoyant des messages à l'adresse de bouclage sur un port connu.

Un agent de service localise et met en cache les agents Annuaire et la liste de l'étendue qu'ils prennent en charge en envoyant directement une requête d'identification d'agent Annuaire à des adresses d'agent Annuaire potentielles en :

1. vérifiant toutes les adresses d'agent Annuaire configurées statiquement (et en ajoutant de nouvelles au cache d'agent Annuaire connu de l'agent de service) ;
2. demandant une liste des agents Annuaire et des étendues de DHCP (et en en ajoutant de nouveaux au cache d'agent Annuaire connu de l'agent de service) ;
3. envoyant une requête d'identification d'agent Annuaire par multidiffusion sur un port connu (et en en ajoutant de nouvelles au cache d'agent Annuaire connu de l'agent de service) ;
4. recevant les paquets d'annonce régulièrement diffusés par les agents Annuaire (et en ajoutant les nouveaux au cache d'agent Annuaire connu de l'agent de service).

Le fait qu'un agent Utilisateur interroge toujours l'agent de service local en premier lieu revêt toute son importance, car la réponse de l'agent de service local détermine si l'agent Utilisateur passe ou non à l'étape suivante de l'identification (en l'occurrence, DHCP-- reportez-vous aux étapes 3 et 4 de la section « Agents Utilisateur », page 579).

Paramètres de configuration

Certains paramètres de configuration du fichier %systemroot%/slp.conf contrôlent également l'identification d'agent Annuaire :

```
net.slp.useScopes= <liste d'étendues séparées par des virgules>
net.slp.DAAddresses = <liste d'adresses séparées par des virgules>
net.slp.passiveDADetection = <« true » ou « false »>
net.slp.activeDADetection = <« true » ou « false »>
net.slp.DAActiveDiscoveryInterval = <0, 1 ou un nombre de secondes>
```

L'option useScopes indique à quelles étendues l'agent Service va s'annoncer et à quelles étendues les requêtes seront adressées en l'absence d'une étendue spécifique lors de l'enregistrement ou de la requête effectuée par le service ou l'application client. Comme eDirectory émet toujours ses annonces et ses interrogations sur l'étendue par défaut, cette liste sera considérée comme la liste d'étendues par défaut pour l'ensemble des enregistrements et des requêtes de eDirectory.

L'option DAAddresses fait référence à une liste d'adresses IP d'agents Annuaires dont les adresses sont séparées par des virgules et utilisent la notation décimale pointée et qui doivent prévaloir sur toutes les autres. Si cette liste des agents Annuaire configurés ne prend pas en charge l'étendue d'un enregistrement ou d'une requête, les agents de service et Utilisateur font alors appel à l'identification d'agent Annuaire multidiffusion, sauf si cette fonction a été désactivée.

L'option passiveDADetection a par défaut la valeur Vrai. Les agents Annuaire annoncent régulièrement leur existence sur le sous-réseau au moyen d'un port connu si celui-ci est configuré à cet effet. Ces paquets prennent le nom de paquets DAAdvert. Si cette option a pour valeur Faux, tous les paquets DAAdvert diffusés sont ignorés par l'agent de service.

L'option activeDADetection a également par défaut la valeur Vrai. Elle permet à l'agent de service de diffuser régulièrement une requête à tous les agents Annuaire pour qu'ils répondent au moyen d'un paquet DAAdvert dirigé. Un paquet dirigé n'est pas diffusé, mais envoyé directement à l'agent de service en réponse à ces requêtes. Si cette option est définie sur Faux, aucune requête régulière d'identification d'agent Annuaire n'est diffusée par l'agent de service.

L'option DAActiveDiscoveryInterval est un paramètre de vérification d'état. La valeur par défaut est 1. Elle indique que l'agent de service ne doit envoyer une requête d'identification d'agent Annuaire qu'à l'initialisation. Si vous attribuez la valeur0 à cette option, cela revient à attribuer la valeur « false » à l'option activeDADetection. Toute autre valeur indique un nombre de secondes entre les diffusions d'identification.

Utilisées correctement, ces options peuvent assurer une utilisation appropriée de la bande passante du réseau pour l'annonce de services. En fait, les paramètres par défaut sont conçus pour optimiser l'évolutivité d'un réseau moyen.

D Fonctionnement de Novell eDirectory avec DNS

Si un client demande à un serveur de résoudre un nom complet (par exemple, admin.novell.novell_inc) qui n'existe pas dans l'arborescence Novell® eDirectory™, ou si vous utilisez une application autonome telle que Novell iManager pour Linux et UNIX ou l'application d'installation de eDirectory pour résoudre un nom dans l'arborescence et que vous n'avez encore aucun serveur à contacter, eDirectory utilise des protocoles d'identification de services pour la résolution. Ces protocoles correspondent à une classe d'applications réseau qui permettent à des composants distribués de rechercher et d'utiliser les services appropriés sur un réseau.

eDirectory utilisait jusqu'à présent SAP et SLP pour rechercher et annoncer les services réseau. Le protocole d'identification DNS a été intégré à eDirectory 8.7.1. Grâce à cette nouvelle fonctionnalité, si vous demandez un nom d'arborescence que eDirectory ne comprend pas (parce que vous communiquez avec un serveur qui ne détient pas de copie de l'arborescence ou que vous utilisez une application autonome), la machine qui tente l'identification (qu'il s'agisse d'une machine exécutant une application autonome, d'une application JClient telle que Novell iManager ou ConsoleOne®, ou d'un serveur) utilise les protocoles d'identification de eDirectory dans l'ordre suivant :

1. Protocole DNS (Domain Name System)
2. Protocole SLP (Service Location Protocol)
3. Protocole SAP (Service Advertising Protocol)

Lorsqu'il utilise le protocole DNS, eDirectory considère le nom tel qu'il a été transmis (par exemple, le nom de serveur prod_server4.provo.novell.novell_inc) et tente de résoudre le nom complet tel quel. Il ajoute alors chaque nom à la liste de recherche DNS de la machine d'identification et demande au serveur DNS de cette dernière s'il dispose d'une adresse pour ce nom. Par exemple, si la liste de recherche DNS contient dev.novell.com et test.novell.com, eDirectory recherche prod_server4.provo.novell.novell_inc.dev.novell.com et prod_server4.provo.novell.novell_inc.test.novell.com.

eDirectory considère ensuite les composants du nom qui lui a été transmis. Par exemple, lors de la résolution de prod_server4.provo.novell.novell_inc, eDirectory essaie d'abord provo.novell.novell_inc, puis novell.novell_inc, puis novell_inc. Il procède ainsi pour chacun des contextes de recherche et essaie pour finir le composant unique qui constitue la racine de l'arborescence. Le client essaie chacune des adresses jusqu'à ce qu'il parvienne à établir une connexion. Il effectue les tentatives en suivant l'ordre des enregistrements renvoyés par le serveur DNS. La révision de code exécutée par les serveurs de l'anneau de répliques importe peu, l'essentiel étant que la version eDirectory 8.7.1 (ou une version ultérieure) soit installée sur la machine qui tente d'effectuer l'identification.

Nous vous recommandons de placer le nom de votre arborescence eDirectory dans DNS au moyen d'un enregistrement de ressource de type A, AAAA ou service (SRV) sous le domaine DNS que les clients vont utiliser pour résoudre les noms. Dans le cas d'enregistrements A ou AAAA, les serveurs eDirectory doivent utiliser le port par défaut524. S'ils utilisent un autre port, vous devez recourir à un enregistrement SRV.

Dans les exemples d'enregistrements de ressources ci-dessous, novell_inc est le nom de l'arborescence et provo.novell.com, le contexte de recherche DNS :

Enregistrement	Exemple
A	novell_inc.provo.novell.com. EN A 192.168.1.2
AAAA	novell_inc.provo.novell.com. EN AAAA 4321:0:1:2:3:4:567:89ab
SRV	_ldap._tcp.novell_inc.provo.novell.com. SRV 0 0 389 server1.novell_inc.provo.novell.com SRV 10 0 389 server2.novell_inc.provo.novell.com

Pour assurer la redondance ou pour spécifier plusieurs hôtes (serveurs de l'anneau de répliques) pour l'enregistrement A, créez plusieurs enregistrements de ce type. eDirectory les examinera tous. Pour plus d'informations sur les enregistrements A, AAAA et SRV, consultez le site Web DNS Resource Records (Enregistrements de ressources DNS) (http://www.dns.net/dnsrd/rr.html).

L'entrée de l'enregistrement du serveur DNS ne doit pas nécessairement pointer sur un élément qui détient une racine de partition correspondante. Dès que la machine d'identification parvient à contacter un serveur qui connaît l'arborescence, elle peut parcourir cette dernière pour résoudre le nom. Par exemple, si vous placez novell_inc dans votre DNS, vous ne devez pas inclure les serveurs contenant la racine novell_inc. Il vous suffit de pointer sur n'importe quel serveur de l'arborescence novell_inc car, après avoir accédé à ce dernier dans l'arborescence, celui-ci vous fera connaître dans l'ensemble de l'arborescence.

E Configuration de GSSAPI avec eDirectory

Le mécanisme SASL-GSSAPI pour Novell® eDirectory™ permet de s'authentifier auprès de eDirectory via LDAP à l'aide d'un ticket Kerberos. Il n'est pas nécessaire de saisir le mot de passe utilisateur de eDirectory. Le ticket Kerberos peut être obtenu en s'authentifiant auprès d'un serveur Kerberos.

Pour des informations conceptuelles sur SASL-GSSAPI, consultez le manuel *Novell eDirectory 8.8 What's New Guide* (Guide des nouveautés de Novell eDirectory 8.8) (http://www.novell.com/documentation/beta/edir88/index.html).

REMARQUE : le mécanisme SASL-GSSAPI est compatible avec eDirectory 8.7.1 et versions ultérieures.

Les sections suivantes expliquent comment configurer GSSAPI, décrivent les différentes tâches pouvant être effectuées avec Kerberos dans eDirectory et fournissent d'autres informations utiles :

Conditions préalables

La configuration de GSSAPI implique d'effectuer préalablement les opérations suivantes :

- **Méthode SASL-GSSAPI :** installez la méthode SASL-GSSAPI. Reportez-vous à la section Installing a Login Method (Installation d'une méthode de login) du manuel *NMAS 3.0 Administration Guide* (Guide d'administration de NMAS 3.0) (http://www.novell.com/documentation/beta/nmas30/admin/data/a49tuwk.html#a49tuwk).

  REMARQUE : pour installer la méthode de login SASL-GSSAPI sous NetWare, suivez la même procédure que dans Windows.

  Pour vérifier que SASL-GSSAPI est installé sur votre machine, entrez la commande suivante :

  ```
  ldapsearch -x -h osg-dt-srv9 -b " " -s base | grep -i sasl
  ```

  Si SASL-GSSAPI est installé, la commande donne un résultat similaire à celui-ci:

  ```
  supportedSASLMechanisms: NMAS_LOGIN
  ```

- **Plug-in Kerberos pour iManager :** installez le plug-in Kerberos pour iManager. Pour plus d'informations, reportez-vous à la section « Installation du plug-in Kerberos pour iManager. », page 584.

- **KDC :** installez le centre de distribution de clés KDC Kerberos [MIT, Microsoft (Active Directory) ou Heimdal] sur le réseau.

  Les outils Kerberos doivent être installés pour le KDC Microsoft (Active Directory). Ils font partie de l'installation de Windows et peuvent être installés en exécutant le fichier \support\tools\setup.exe du CD d'installation Windows.

- **Synchronisation horaire :** pour que cette méthode fonctionne, synchronisez l'heure du poste client NMAS™, du serveur NMAS et de la machine KDC. Pour plus d'informations sur la synchronisation de l'heure réseau, reportez-vous à la section « Synchronisation des heures réseau », page 90.

- **LDAP Libraries for C :** installez les dernières bibliothèques LDAP libraries for C à l'emplacement par défaut (excepté sous Windows). Pour plus d'informations, consultez le site Web LDAP Libraries for C (http://developer.novell.com/ndk/cldap.htm) .

- **Extensions LDAP Kerberos :** ajoutez les extensions LDAP Kerberos. Pour plus d'informations, reportez-vous à la section « Ajout d'extensions LDAP Kerberos », page 586.

  IMPORTANT : toutes les informations Kerberos collectées auprès de votre système d'administration Kerberos tiennent compte de la casse et doivent la respecter.

Hypothèses concernant les caractéristiques réseau

Le mécanisme SASL-GSSAPI se base sur les hypothèses suivantes :

- La synchronisation horaire de toutes les machines du réseau présente une souplesse relative, ce qui signifie que les heures des différentes machines diffèrent tout au plus de plus de cinq minutes.
- Le mécanisme SASL-GSSAPI est censé être utilisé principalement dans un environnement LAN vu la difficulté à respecter l'exigence de synchronisation horaire, mentionnée ci-dessus, dans des environnements MAN et/ou WAN. Ce mécanisme ne se limite toutefois pas au LAN.
- Vous faites entièrement et systématiquement confiance aux serveurs et administrateurs Kerberos.
- Une attaque de refus de service n'est pas contrée. Pour plus d'informations, consultez le site Web RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

Installation du plug-in Kerberos pour iManager.

1. Ouvrez le navigateur.
2. Saisissez l'URL suivante dans le champ Adresse de la fenêtre du navigateur:

   `http://nom_hôte/nps/iManager.html`

   où *nom_hôte* est le nom ou l'adresse IP du serveur iManager sur lequel installer le plug-in iManager pour SASL-GSSAPI.

   REMARQUE : en cas de problèmes, vérifiez que les serveurs Web et Tomcat sont configurés correctement. Pour plus d'informations, consultez le manuel iManager 2.5 Administration Guide (Guide d'administration de iManager 2.5) (http://www.novell.com/documentation/beta/imanager25/index.html).

3. Indiquez un nom d'utilisateur et un mot de passe pour vous loguer à eDirectory, puis cliquez sur Login.
4. Cliquez sur le bouton Configurer  dans la barre d'outils de iManager.
5. Dans le volet gauche, cliquez sur Configuration du module > Installer le progiciel du module.

6 Indiquez l'emplacement du fichier kerberosPlugin.npm ou cliquez sur Parcourir pour le sélectionner.

L'ensemble des plug-ins se trouve à l'emplacement suivant :

dossier_extrait/<plate-forme(Linux, Solaris)>/nmas/NmasMethods/Novell/GSSAPI/plugins/, où *dossier_extrait* est le répertoire où vous avez extrait le fichier edir88.zip. Si vous avez déplacé le fichier kerberosPlugin.npm, accédez à son nouvel emplacement et sélectionnez le fichier.

7 Cliquez sur Installer.

Cette installation prendra quelques minutes.

REMARQUE : il se peut que le message d'erreur « Unexpected end of part » (Fin de partie inattendue) s'affiche pendant l'installation du progiciel du module si vous exécutez iManager sur un serveur Web IIS Windows avec Tomcat. Cela est dû à un problème connu lié au téléchargement de fichiers via le redirecteur Tomcat pour IIS. Pour effectuer correctement l'installation d'un progiciel de module, connectez-vous à iManager directement via Tomcat (par exemple, via le port 8080).

Par exemple, http://nom_hôte:8080/nps/iManager.html

Pour plus d'informations, consultez le manuel *iManager 2.5 Administration Guide* (Guide d'administration de iManager 2.5) (http://www.novell.com/documentation/beta/imanager25/index.html).

8 Redémarrez le serveur iManager après avoir reçu un message indiquant la réussite de l'enregistrement du module.

Si vous exécutez iManager en mode Accès illimité (aucune collection RBS dans l'arborescence), ignorez les étapes 9 à 15.

REMARQUE : pour plus d'informations sur le redémarrage du serveur iManager, consultez le manuel iManager 2.5 Administration Guide (Guide d'administration de iManager 2.5) (http://www.novell.com/documentation/beta/imanager25/index.html).

9 Loguez-vous à iManager, puis cliquez sur le bouton Configurer  .

10 Dans le volet gauche, cliquez sur Configuration RBS > Configurer iManager.

11 (Conditionnel) Si vous avez déjà créé une collection RBS, sélectionnez Mettre à niveau des collections, puis cliquez sur Suivant > Suivant.

12 (Conditionnel) Si vous n'avez pas de collection RBS, procédez comme suit :

12a Sélectionnez Créer une nouvelle collection, puis cliquez sur Suivant.

12b Sélectionnez le conteneur dans lequel vous souhaitez créer les services basés sur le rôle, puis cliquez sur Suivant.

13 Sélectionnez le plug-in Kerberos Novell, assignez une étendue (nom d'arborescence ou n'importe quel conteneur), puis cliquez sur Démarrer pour terminer l'installation du plug-in iManager pour la configuration Kerberos.

REMARQUE : cette opération conférera des droits Superviseur à l'étendue sélectionnée pour le rôle Kerberos Management (Gestion Kerberos).

14 Lorsque le message Terminé s'affiche, cliquez sur Fermer.

15 Rafraîchissez la page.

Le rôle Kerberos Management s'affiche dans le volet gauche.

Si ce n'est pas le cas, redémarrez le serveur iManager comme indiqué à l'étape8 ci-dessus.

REMARQUE : si le serveur iManager est exécuté sur les services Web Windows (IIS), une collection RBS doit être créée avant d'installer le plug-in iManager pour Kerberos NMAS.

Ajout d'extensions LDAP Kerberos

Les extensions LDAP Kerberos permettent de gérer les clés Kerberos.

L'utilisation des extensions LDAP Kerberos nécessite l'installation de LDAP libraries for C. Pour plus d'informations, consultez le site Web *LDAP Libraries for C* (http://developer.novell.com/ndk/cldap.htm).

Pour ajouter ou supprimer des extensions LDAP Kerberos, employez l'utilitaire krbldapconfig disponible aux emplacements suivants :

- **Linux :** dossier_extrait/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Linux/krbldapconfig

  Par exemple :

  /misc/eDir88/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Linux/krbldapconfig

- **Solaris :** dossier_extrait/Solaris/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Solaris/krbldapconfig

  Par exemple :

  /misc/eDir88/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Linux/krbldapconfig

- **NetWare® et Windows :**
  Sous NetWare, vous pouvez exécuter le fichier krbldapconfig sur n'importe quelle autre plate-forme.

  dossier_extrait/Windows/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Windows/krbldapconfig

  Par exemple :

  /misc/eDir88/Linux/nmas/NmasMethods/Novell/GSSAPI/Kerberos_ldap_extensions/Windows/krbldapconfig

Pour ajouter les extensions LDAP Kerberos, utilisez la syntaxe suivante :

```
krbldapconfig {-i | -u} -D DN_liaison [-w mot_de_passe_DN_liaison] [-h
hôte_ldap] [-p port_ldap] [-e certificat_racine_approuvée]
```

Le tableau suivant décrit les paramètres de l'utilitaire krbldapconfig :

Paramètre	Description
-i	Ajoute les extensions LDAP Kerberos à eDirectory.
-u	Supprime les extensions LDAP Kerberos de eDirectory.
-D FDN_liaison	Indique le FDN de l'administrateur ou de l'utilisateur disposant de droits équivalents. Il doit avoir le format suivant cn=admin,o=org.
-w mot_de_passe_FDN_liaison	Indique le mot de passe du FDN de liaison (FDN_liaison).
-h serveur_ldap	Indique le nom d'hôte ou l'adresse IP du serveur LDAP où doivent être installées les extensions LDAP Kerberos.

Paramètre	Description
-p port	Indique le port sur lequel est exécuté le serveur LDAP.
-e fichier_racine_approuvée	Indique le nom du fichier de certificat de racine approuvée pour la liaison SSL. Si vous utilisez un port SSL, spécifiez l'option -e. Pour plus d'informations, reportez-vous à la section « Exportation du certificat de racine approuvée », page 587.

REMARQUE : si l'option -h n'est pas spécifiée, le nom de l'hôte local à partir duquel le fichier krbldapconfig est appelé est utilisé par défaut.

Si aucun port de serveur LDAP ni certificat de racine approuvée ne sont spécifiés, le port 389 est utilisé par défaut.

Si aucun port de serveur LDAP n'est spécifié, mais qu'un certificat de racine approuvée est indiqué, le port 636 est utilisé par défaut.

Par exemple, entrez la commande suivante pour ajouter les extensions :

```
krbldapconfig -i -D cn=admin,o=org -w mot_de_passe -h serveur_ldap -p 389
```

Entrez la commande suivante pour supprimer des extensions :

```
krbldapconfig -u -D cn=admin,o=org -w mot_de_passe -h serveur_ldap -p 389
```

IMPORTANT : le serveur LDAP doit être actualisé manuellement pour que les modifications apportées à l'installation soient prises en compte. Pour plus d'informations, reportez-vous à la section « Rafraîchissement du serveur LDAP », page 357.

Exportation du certificat de racine approuvée

1. Dans iManager, cliquez sur Administration de eDirectory > Modifier un objet pour ouvrir la page correspondante.
2. Cliquez sur Objet unique, puis sélectionnez l'objet Certificat de serveur du serveur.
3. Cliquez sur OK.
4. Cliquez sur l'onglet Certificats, puis sélectionnez Certificat de racine approuvée pour afficher les informations relatives au certificat.
5. Cliquez sur Exporter pour lancer l'Assistant d'exportation du certificat.
6. Indiquez si vous souhaitez ou non exporter la clé privée, puis cliquez sur Suivant.
7. Sélectionnez Fichier au format DER binaire, puis cliquez sur Suivant.
8. Cliquez sur Enregistrer le certificat exporté dans un fichier.
9. Cliquez sur Fermer.

Configuration de la méthode SASL-GSSAPI

1. Le plug-in iManager pour SASL-GSSAPI ne fonctionnera pas si iManager n'est pas configuré pour utiliser une connexion à eDirectory de type SSL/TLS. Une connexion sécurisée est obligatoire pour protéger les clés de principal et la clé maîtresse du domaine.

   iManager est généralement configuré par défaut pour une connexion à eDirectory de type SSL/TLS. Vous devez toutefois lui ajouter les certificats de racine approuvée SSL du serveur LDAP que vous utilisez pour l'administration Kerberos.

   Pour plus d'informations sur la configuration de iManager avec une connexion à eDirectory de type SSL/TLS, consultez le manuel *iManager 2.0 Administration Guide* (Guide d'administration de iManager 2.5) (http://www.novell.com/documentation/lg/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/am4ajce.html#bow4dv4).

2. Effectuez les procédures suivantes dans l'ordre indiqué:

   2a Étendez le schéma Kerberos.

   2b Créez un conteneur de domaine.

   2c Créez le principal de service LDAP.

   2d Extrayez une clé de principal de service ou une clé partagée du KDC.

   2e Créez un objet Principal de service dans eDirectory.

   2f Associez un nom de principal Kerberos à un objet Utilisateur.

Fusion d'arborescences eDirectory configurées avec la méthode SASL-GSSAPI

Lorsque vous fusionnez deux arborescences, dont l'une ou les deux ont été configurées avec la méthode SASL-GSSAPI, vous devez créer manuellement tous les objets Kerberos de l'arborescence source dans l'arborescence cible.

Gestion de la méthode SASL-GSSAPI

iManager vous permet d'effectuer les opérations Kerberos suivantes :

- « Extension du schéma Kerberos », page 588
- « Gestion de l'objet Domaine Kerberos », page 589
- « Gestion d'un principal de service », page 590
- « Édition de principaux étrangers », page 594

Extension du schéma Kerberos

Cette tâche permet d'étendre votre schéma eDirectory en ajoutant des définitions d'attributs et une classe d'objet Kerberos.

1. Si le schéma n'a pas encore été étendu, cliquez sur OK pour l'étendre.
2. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > Extend Schema (Étendre le schéma) pour ouvrir la page correspondante.

   Si le schéma a été étendu, un message affiche son état.
3. Cliquez sur Fermer.

Gestion de l'objet Domaine Kerberos

Un domaine est un réseau logique desservi par un ensemble de centres de distribution de clés (KDC - Key Distribution Center). En d'autres termes, un domaine est un espace ou un groupement de principaux desservis par un ensemble de KDC. L'usage veut que les noms de domaine Kerberos soient en lettres majuscules pour les distinguer des domaines Internet. Pour plus d'informations, consultez le site Web RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

Cette section fournit les informations suivantes :

- « Création d'un objet Domaine », page 589
- « Édition d'un objet Domaine », page 589
- « Suppression d'un objet Domaine », page 590

Création d'un objet Domaine

Le type de codage par défaut pris en charge est DES-CBC-CRC.

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > New Realm (Nouveau domaine) pour ouvrir la page correspondante.
2. Indiquez un nom pour le domaine Kerberos à créer.

   Le nom de domaine doit être identique à celui que vous voulez utiliser pour configurer cette méthode de login et doit être conforme aux conventions RFC 1510.
3. Indiquez un mot de passe principal pour le domaine, puis confirmez-le.

   REMARQUE : veillez à utiliser un mot de passe principal complexe.
4. Indiquez la sous-arborescence avec laquelle vous souhaitez configurer le domaine Kerberos ou utilisez l'icône Sélecteur d'objet pour la sélectionner.

   Il s'agit du FDN de la sous-arborescence ou du conteneur qui renferme les principaux de service eDirectory de ce domaine. Cette sous-arborescence n'est pas applicable aux principaux Utilisateur.

   Si vous ne sélectionnez pas de sous-arborescence ni de conteneur, la racine de l'arborescence est utilisée par défaut.
5. Indiquez l'étendue de la recherche dans la sous-arborescence:
   - One-level (Un niveau) : recherche dans les subordonnés immédiats de la sous-arborescence du domaine.
   - Subtree (Sous-arborescence) : recherche dans l'ensemble de la sous-arborescence en commençant par la sous-arborescence du domaine.
6. Cliquez sur OK.

REMARQUE : KDC Services n'est pas utilisé dans SASL-GSSAPI.

Édition d'un objet Domaine

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) >Edit Realm (Éditer le domaine) pour ouvrir la page correspondante.
2. Indiquez un nom pour le domaine Kerberos à éditer ou utilisez l'icône Sélecteur d'objet pour le sélectionner.
3. Cliquez sur OK.

4 Indiquez la sous-arborescence avec laquelle vous souhaitez configurer le domaine Kerberos ou utilisez l'icône Sélecteur d'objet pour la sélectionner.

Il s'agit du FDN de la sous-arborescence ou du conteneur qui renferme les principaux de service eDirectory de ce domaine. Cette sous-arborescence n'est pas applicable aux principaux Utilisateur.

Si vous ne sélectionnez pas de sous-arborescence ni de conteneur, la racine de l'arborescence est utilisée par défaut.

5 Indiquez l'étendue de la recherche de la sous-arborescence.

- One-level (Un niveau) : recherche dans les subordonnés immédiats de la sous-arborescence du domaine.
- Subtree (Sous-arborescence) : recherche dans l'ensemble de l'arborescence en commençant par la sous-arborescence du domaine.

6 Cliquez sur OK.

7 (Facultatif) Pour éditer un autre domaine, cliquez sur Repeat Task (Répéter la tâche).

REMARQUE : KDC Services n'est pas utilisé dans SASL-GSSAPI.

Suppression d'un objet Domaine

1 Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) >Delete Realm (Supprimer le domaine) pour ouvrir la page correspondante.

2 Sélectionnez les domaines à supprimer.

Pour en sélectionner plusieurs, appuyez sur la touche Maj et sélectionnez les domaines ou appuyez sur Maj et sur les touches fléchées.

3 Cliquez sur OK.

4 Cliquez de nouveau sur OK pour confirmer la suppression ou sur Annuler pour annuler cette opération.

IMPORTANT : la suppression d'un objet Domaine efface également tous les objets Principal de service qu'il contient.

Gestion d'un principal de service

Cette section fournit les informations suivantes :

Création d'un principal de service pour un serveur LDAP

L'outil d'administration Kerberos disponible avec votre KDC permet de créer le principal de service eDirectory avec DES-CBC-CRC comme type de codage et Normal comme type de valeur aléatoire (salt).

Le nom du principal doit être ldap/*MONHÔTE.MONDOMAINEDNS@NOMDOMAINE*.

Par exemple, si vous utilisez un KDC MIT, exécutez la commande suivante :

```
kadmin:addprinc -randkey -e des-cbc-crc:normal ldap/
server.novell.com@DOMAINEMIT
```

Par exemple, si vous utilisez un KDC Heimdal, exécutez la commande suivante :

```
kadmin -lkadmin> add --random-key ldap/
server.novell.com@DOMAINEMIT
```

Pour supprimer les types de codage non pris en charge pour le principal de service, exécutez la commande suivante :

```
kadmin> del_enctype ldap/MONHÔTE.MONDOMAINEDNS@MONDOMAINE des-
cbc-md4kadmin> del_enctype ldap/MONHÔTE.MONDOMAINEDNS@MONDOMAINE
des-cbc-md5kadmin> del_enctype ldap/
MONHÔTE.MONDOMAINEDNS@MONDOMAINE des3-cbc-sha1
```

où *MONHÔTE.MONDOMAINEDNS* est le nom d'hôte et *MONDOMAINE*, le domaine Kerberos.

Recommandation

Il est recommandé de changer régulièrement les clés de principal de service LDAP. Lors de leur changement, veillez à mettre à jour l'objet Principal dans eDirectory.

Extraction de la clé du principal de service pour eDirectory

L'outil d'administration Kerberos disponible avec votre KDC permet d'extraire la clé du principal de service LDAP créé à la section « Création d'un principal de service pour un serveur LDAP », page 590, puis de la stocker dans le système de fichiers local. Votre administrateur Kerberos peut vous aider à effectuer cette opération.

Par exemple, si vous utilisez un KDC MIT, exécutez la commande suivante :

```
kadmin: ktadd -k /chemin_répertoire/nom_fichier_keytab -e des-cbc-
crc:normal ldap/server.novell.com@DOMAINEMIT
```

Par exemple, si vous utilisez un KDC Microsoft, créez un utilisateur ldapMONHÔTE dans Active Directory, puis exécutez la commande suivante :

```
ktpass -princ ldap/MONHÔTE.MONDOMAINEDNS@MONDOMAINE -mapuser
ldapMONHÔTE -pass mon_mot_de_passe -out MONHÔTE.keytab
```

Cette commande assigne le principal (ldap/MONHÔTE.MONDOMAINEDNS@MONDOMAINE) au compte utilisateur (ldapMONHÔTE), définit le mot de passe de principal hôte en mon_mot_de_passe et extrait la clé dans le fichier MONHÔTE.keytab.

Par exemple, si vous utilisez un KDC Heimdal, exécutez la commande suivante :

```
kadmin> ext_keytab -k /chemin_répertoire/nom_fichier_keytab ldap/
server.novell.com@DOMAINEMIT
```

où *nom_fichier_keytab* est le nom du fichier qui contient la clé extraite.

Création d'un objet Principal de service dans eDirectory.

Vous devez créer un principal de service Kerberos avec un nom identique (ldap/*MONHÔTE.MONDOMAINEDNS@MONDOMAINE*) à celui indiqué à la section « Création d'un principal de service pour un serveur LDAP », page 590.

Recommandation

Les principaux de service pour eDirectory doivent être aisément accessibles à tous les serveurs activés pour le mécanisme SASL-GSSAPI. S'ils ne sont pas créés sous le conteneur Domaine Kerberos dans le conteneur Sécurité, il est vivement recommandé de créer le conteneur qui les renferme en tant que partition distincte et de le répliquer largement.

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > New Principal (Nouveau principal) pour ouvrir la page correspondante.
2. Indiquez le nom du principal à créer.

   Le nom du principal doit avoir le format suivant : ldap/*MONDOMAINEDNS@NOMDOMAINE*.
3. Indiquez le nom du conteneur qui renfermera l'objet Principal créé ou utilisez l'icône Sélecteur d'objet pour le sélectionner.
4. Indiquez le nom du domaine.

   Si vous l'avez déjà spécifié à l'étape2, laissez ce champ vide.
5. Effectuez l'une des opérations suivantes :
   - Indiquez le nom du fichier keytab ou cliquez sur Parcourir pour sélectionner son emplacement de stockage.

     Il s'agit du fichier qui contient la clé extraite à la section « Extraction de la clé du principal de service pour eDirectory », page 591.
   - Spécifiez le mot de passe, confirmez-le, puis sélectionnez les types de codage et de valeur aléatoire (salt).

     Le mot de passe et la combinaison types de codage/de valeur aléatoire doivent être identiques à ceux spécifiés lors de la création du principal de service dans la base de données KDC.
6. Cliquez sur OK.

Affichage des clés de principal de service Kerberos

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > View Principal Keys (Afficher les clés de principal) pour ouvrir la page correspondante.
2. Indiquez le nom de la clé de principal à afficher ou utilisez l'icône Sélecteur d'objet pour le sélectionner.

   Les informations suivantes sur les clés de principal s'affichent :
   - Principal name (Nom du principal)
   - Key Table (Table de clés)
     - Number (Numéro) : numéro de série de la clé dans la table
     - Version : version de la clé
     - Key Type (Type de clé) : type de la clé de principal
     - Salt Type (Type de valeur aléatoire) : type de valeur aléatoire de la clé de principal
3. Cliquez sur OK.

Suppression d'un objet Principal de service Kerberos

Vous pouvez supprimer un ou plusieurs objets, ou encore, effectuer une sélection avancée des objets Principal à effacer.

Pour supprimer un seul objet Principal :

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > Delete Principal (Supprimer le principal) pour ouvrir la page correspondante.
2. Cliquez sur Select a Single Object (Sélectionner un seul objet).
3. Indiquez le nom de l'objet Principal à supprimer ou utilisez l'icône Sélecteur d'objet pour le sélectionner.
4. Cliquez sur OK.
5. Cliquez de nouveau sur OK pour confirmer la suppression ou sur Annuler pour annuler cette opération.

Pour supprimer plusieurs objets Principal :

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > Delete Principal (Supprimer le principal) pour ouvrir la page correspondante.
2. Cliquez sur Select Multiple Objects (Sélectionner plusieurs objets).
3. Indiquez le nom des objets Principal à supprimer ou utilisez l'icône Sélecteur d'objet pour les sélectionner.
4. Sélectionnez les objets Principal à supprimer.
5. Cliquez sur OK.
6. Cliquez de nouveau sur OK pour confirmer la suppression ou sur Annuler pour annuler cette opération.

Pour supprimer un principal en utilisant la sélection avancée :

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > Delete Principal (Supprimer le principal) pour ouvrir la page correspondante.
2. Cliquez sur Advanced Selection (Sélection avancée).
3. Sélectionnez la classe d'objet.
4. Indiquez le conteneur qui renferme l'objet Principal ou utilisez l'icône Sélecteur d'objet pour le sélectionner.
5. Cliquez sur Include subcontainers (Inclure les sous-conteneurs) pour englober les sous-conteneurs du conteneur spécifié à l'étape3.
6. Cliquez sur le bouton  pour ouvrir la fenêtre Advanced Selection Criteria (Critères de sélection avancés).
7. Sélectionnez le type d'attribut et l'opérateur dans la liste déroulante, puis fournissez les valeurs correspondantes.
8. Cliquez sur le bouton Add Row (Ajouter une ligne)  pour inclure d'autres groupes logiques dans la sélection.
9. Cliquez sur OK pour définir le filtre.
10. Cliquez sur Show Preview (Afficher l'aperçu) pour afficher un aperçu de la sélection avancée.
11. Cliquez sur OK.
12. Cliquez de nouveau sur OK pour confirmer la suppression ou sur Annuler pour annuler cette opération.

Définition d'un mot de passe pour le principal de service Kerberos

Si la clé de principal de service eDirectory a été réinitialisée dans votre KDC, vous devez également la mettre à jour dans eDirectory.

Pour plus d'informations sur l'extraction de clé, reportez-vous à la section « Extraction de la clé du principal de service pour eDirectory », page 591.

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > Set Principal Password (Définition de mot de passe de principal) pour ouvrir la page correspondante.
2. Indiquez le nom de l'objet Principal pour lequel définir un mot de passe individuel ou utilisez l'icône Sélecteur d'objet pour le sélectionner.
3. Indiquez le nom du fichier keytab ou cliquez sur Parcourir pour accéder à son emplacement de stockage.
4. Effectuez l'une des opérations suivantes :
   - Indiquez le nom du fichier keytab qui contient la clé de principal ou cliquez sur Parcourir pour sélectionner son emplacement de stockage.

     Pour plus d'informations sur la création de principaux de service et l'extraction de clés, reportez-vous aux sections « Création d'un principal de service pour un serveur LDAP », page 590 et « Extraction de la clé du principal de service pour eDirectory », page 591.
   - Spécifiez le mot de passe, confirmez-le, puis sélectionnez les types de codage et de valeur aléatoire.
5. Cliquez sur OK pour définir le mot de passe.
6. (Facultatif) Pour définir le mot de passe d'un autre principal, cliquez sur Repeat Task (Répéter la tâche).

Édition de principaux étrangers

iManager permet d'ajouter des noms de principaux Kerberos aux utilisateurs de eDirectory.

1. Dans iManager, cliquez sur Kerberos Management (Gestion Kerberos) > Edit Foreign Principals (Éditer les principaux étrangers) pour ouvrir la page correspondante.
2. Indiquez le FDN d'un objet Utilisateur valide ou utilisez l'icône Sélecteur d'objet pour sélectionner la référence à l'objet Utilisateur.
3. Cliquez sur OK.
4. Indiquez les noms de principaux étrangers, puis cliquez sur le bouton Add (Ajouter)  .

   Le nom du principal doit avoir le format nomdeprincipal@*NOMDOMAINE*.

   Pour supprimer le nom de principal étranger, sélectionnez-le, puis cliquez sur le bouton Delete (Supprimer)  .
5. Cliquez sur OK.

Création d'une séquence de login

Pour plus d'informations sur la création d'une séquence de login, reportez-vous à la section Managing Login Sequences (Gestion de séquences de login) du manuel *NMAS 3.0 Administration Guide* (Guide d'administration de NMAS3.0) (http://www.novell.com/documentation/beta/nmas30/index.html?page=/documentation/beta/nmas30/admin/data/a49tuwk.html#a4).

Utilisation de SASL-GSSAPI par LDAP

Après avoir configuré la méthode SASL-GSSAPI, elle est ajoutée avec d'autres méthodes SASL à l'attribut supportedSASLMechanisms dans rootDSE.

Le serveur LDAP interroge SASL pour connaître les mécanismes installés lors de sa configuration et prend automatiquement en charge les éléments installés. Le serveur LDAP signale également les mécanismes SASL pris en charge dans son entrée rootDSE à l'aide de l'attribut supportedSASLMechanisms.

Par conséquent, une fois configuré, GSSAPI devient le mécanisme par défaut.

Toutefois, pour effectuer spécifiquement une opération LDAP sur le mécanisme SASL-GSSAPI, vous pouvez mentionner GSSAPI dans la ligne de commande.

Par exemple, pour effectuer une recherche à l'aide du mécanisme GSSAPI dans OpenLDAP, entrez la commande suivante :

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

Messages d'erreur

Les messages d'erreur SASL-GSSAPI sont consignés aux emplacements suivants :

- Linux et UNIX: ndsd.log
- NetWare: écran de l'outil de consignation
- Windows: c:\temp\saslgss.log

Pour plus d'informations, reportez-vous à la section « Error messages » (Messages d'erreur) dans le manuel *eDirectory 8.8 Troubleshooting Guide* (Guide de dépannage de eDirectory 8.8) (http://www.novell.com/documentation/beta/edir88/index.html).