NetIQ® eDirectory™ 8.8 SP8

Guide des nouveautés

Septembre 2013

Mentions légales

Table des matières

À propos de ce guide et de la bibliothèque

Le *Guide des nouveautés* présente les nouvelles fonctionnalités de NetIQ eDirectory.

Pour obtenir la dernière version du *Guide des nouveautés de NetIQ eDirectory 8.8 SP8*, consultez le site Web de documentation en ligne de NetIQ eDirectory 8.8.

Public

Le guide est destiné aux administrateurs réseau.

Autres documents dans la bibliothèque

La bibliothèque propose les manuels suivants :

XDASv2 Administration Guide (Guide d'administration de XDASv2)

Décrit comment configurer et utiliser XDASv2 afin d'auditer eDirectory et NetIQ Identity Manager.

Guide d'installation

Décrit comment installer eDirectory. Il est destiné aux administrateurs réseau.

Guide d'administration

Décrit comment gérer et configurer eDirectory.

Guide de dépannage

Décrit comment résoudre les problèmes de eDirectory.

Tuning Guide for Linux Platforms (Guide de configuration de NetIQ eDirectory 8.8 SP8 pour plates-formes Linux)

Décrit comment analyser et configurer eDirectory sur les plates-formes Linux afin d'obtenir de meilleures performances dans tous les déploiements.

Ces guides sont disponibles sur le site Web de documentation de NetIQ eDirectory 8.8 (https://www.netiq.com/documentation/edir88/).

Pour plus d'informations sur l'utilitaire de gestion de eDirectory, voir le *Guide d'administration de NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/).

À propos de NetIQ Corporation

Fournisseur international de logiciels d'entreprise, nos efforts sont constamment axés sur trois défis inhérents à votre environnement (le changement, la complexité et les risques) et la façon dont vous pouvez les contrôler.

Notre point de vue

Adaptation au changement et gestion de la complexité et des risques : rien de neuf

Parmi les défis auxquels vous êtes confronté, il s'agit peut-être des principaux aléas qui vous empêchent de disposer du contrôle nécessaire pour mesurer, surveiller et gérer en toute sécurité vos environnements informatiques physiques, virtuels et en nuage (cloud computing).

Services métiers critiques plus efficaces et plus rapidement opérationnels

Nous sommes convaincus qu'en proposant aux organisations informatiques un contrôle optimal, nous leur permettons de fournir des services dans les délais et de manière plus rentable. Les pressions liées au changement et à la complexité ne feront que s'accroître à mesure que les organisations évoluent et que les technologies nécessaires à leur gestion deviennent elles aussi plus complexes.

Notre philosophie

Vendre des solutions intelligentes et pas simplement des logiciels

Pour vous fournir un contrôle efficace, nous veillons avant tout à comprendre les scénarios réels qui caractérisent les organisations informatiques telles que la vôtre, et ce jour après jour. De cette manière, nous pouvons développer des solutions informatiques à la fois pratiques et intelligentes qui génèrent assurément des résultats éprouvés et mesurables. En même temps, c'est tellement plus gratifiant que la simple vente de logiciels.

Vous aider à réussir, telle est notre passion

Votre réussite constitue le fondement même de notre manière d'agir. Depuis la conception des produits jusqu'à leur déploiement, nous savons que vous avez besoin de solutions informatiques opérationnelles qui s'intègrent en toute transparence à vos investissements existants. En même temps, après le déploiement, vous avez besoin d'une formation et d'un support continus. En effet, il vous faut un partenaire avec qui la collaboration est aisée... pour changer. En fin de compte, votre réussite est aussi la nôtre.

Nos solutions

- Gouvernance des accès et des identités
- Gestion des accès
- Gestion de la sécurité
- Gestion des systèmes et des applications

- Gestion des charges de travail
- Gestion des services

Contacter le support

Pour toute question concernant les produits, tarifs et fonctionnalités, contactez votre partenaire local. Si vous ne pouvez pas contacter votre partenaire, contactez notre équipe de support ventes.

Monde :	www.netiq.com/about_netiq/officelocations.asp
États-Unis et Canada :	1-888-323-6768
Courrier électronique :	info@netiq.com
Site Web :	www.netiq.com

Contacter le support technique

Pour tout problème spécifique au produit, contactez notre équipe du support technique.

Monde :	www.netiq.com/support/contactinfo.asp
Amérique du Nord et du Sud :	1-713-418-5555
Europe, Moyen-Orient et Afrique:	+353 (0) 91-782 677
Courrier électronique :	support@netiq.com
Site Web :	www.netiq.com/support

Contacter le support en charge de la documentation

Notre objectif est de vous proposer une documentation qui réponde à vos besoins. Si vous avez des suggestions d'améliorations, cliquez sur le bouton **Add Comment** (Ajouter un commentaire) au bas de chaque page dans les versions HTML de la documentation publiée à l'adresse www.netiq.com/documentation. Vous pouvez également envoyer un message électronique à l'adresse Documentation-Feedback@netiq.com. Nous accordons une grande importance à vos commentaires et sommes impatients de connaître vos impressions.

Contacter la communauté d'utilisateurs en ligne

La communauté en ligne de NetIQ, Qmunity, est un réseau collaboratif vous mettant en relation avec vos homologues et des spécialistes de NetIQ. En proposant des informations immédiates, des liens utiles vers des ressources et un accès aux experts NetIQ, Qmunity vous aide à maîtriser les connaissances nécessaires pour tirer pleinement parti du potentiel de vos investissements informatiques. Pour plus d'informations, consultez le site http://community.netiq.com.

1 Améliorations et fonctionnalités du Service Pack 8

Ce chapitre présente les fonctionnalités et améliorations de eDirectory 8.8 SP8.

1.1 Améliorations de l'évolutivité

Les améliorations de l'évolutivité disponibles dans eDirectory 8.8 SP8 et mentionnées dans les sections suivantes accélèrent la synchronisation des données et le traitement des notices nécrologiques, tout en réduisant l'encombrement de la mémoire lors du traitement des événements dans le journal.

Dans cette version, certains processus en arrière-plan ont été redéfinis afin de répondre aux besoins des environnements dynamiques de grande envergure. Il s'agit notamment de l'optimisation des processus en arrière-plan existants et fournit des options de configuration qui permettent de régler les systèmes en fonction de votre environnement.

1.1.1 Contrôle des processus en arrière-plan

Les administrateurs peuvent contrôler les processus en arrière-plan en configurant les stratégies Paramètres du délai des processus en arrière-plan suivantes, dans la fenêtre Paramètres des processus en arrière-plan de NetIQ iMonitor :

- **Processeur** : spécifie le pourcentage maximal de ressources de l'ordinateur et la durée de veille maximale d'un même processus (contrôleur de synchronisation [skulker]), purgeur ou notice nécrologique).
- **Limite stricte** : spécifie un paramètre de délai statique pour chacun des processus de contrôleur de synchronisation (skulker), purgeur et notice nécrologique.

Pour plus d'informations sur la configuration des processus en arrière-plan, consultez la section « Configuring Background Processes » (Configuration des processus en arrière-plan) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration NetIQ eDirectory 8.8 SP8).

1.1.2 Processus de contrôleur de synchronisation (skulker)

Pour augmenter le nombre de threads créés pour effectuer la réplication sur plusieurs serveurs simultanément, vous pouvez définir manuellement le nombre maximal de threads créés à l'aide des processus de contrôleur de synchronisation (skulker). Ce paramètre s'applique à toutes les partitions d'un serveur.

Pour plus d'informations sur la configuration du processus de contrôleur de synchronisation (skulker), consultez la section « Manually Configuring Synchronization Threads » (Configuration manuelle des threads de synchronisation) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

1.1.3 Réplication asynchrone

Pour réduire la durée de la réplication, les opérations suivantes s'exécutent désormais en parallèle :

- Traitement du cache des modifications
- Envoi de paquets à un serveur distant

La nouvelle option **Synchronisation sortante asynchrone (en millisecondes)** permet d'éviter de surcharger le serveur de réception. Par défaut, cette option est désactivée. Le paramètre dépend de votre environnement. Lorsque vous activez cette option, définissez-la sur la valeur `100`, puis augmentez ou réduisez-la en fonction des besoins.

Pour plus d'informations sur la configuration de la synchronisation sortante asynchrone, consultez la section « Configuring Asynchronous Outbound Synchronization » (Configuration de la synchronisation sortante asynchrone) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

1.1.4 Réplication basée sur des stratégies

Les administrateurs peuvent désormais créer une stratégie (fichier XML) pour spécifier le mode de réplication des modifications. Elle peut notamment être utile lorsqu'un anneau de réplique est réparti sur plusieurs emplacements. Si la stratégie contient une faute de frappe ou une syntaxe incorrecte, la réplication revient à la méthode par défaut.

Pour plus d'informations, consultez la section « Policy Based Replication » (Réplication basée sur les stratégies) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

1.1.5 Notice nécrologique

La notice nécrologique générée lorsqu'un objet est supprimé, renommé ou déplacé est traitée plus rapidement que dans les versions précédentes de eDirectory. Par exemple, une mise à jour qui nécessitait cinq cycles dans les versions précédentes peut désormais s'effectuer en deux cycles seulement.

En outre, le processus de génération de notice nécrologique peut désormais être exécuté parallèlement au processus de contrôleur de synchronisation (skulker).

1.1.6 Suivi du nombre de notices nécrologiques et de caches de changement par l'intermédiaire de iMonitor

iMonitor affiche le nombre d'objets avec notices nécrologiques dans chaque état. Il indique également le nombre d'objets dans le cache des modifications d'une partition lorsque vous affichez un objet Partition par le biais de iMonitor dans un serveur donné. Vous pouvez ainsi surveiller plus facilement l'état de synchronisation et le traitement des notices nécrologiques.

1.1.7 Liens de référence distribués

Afin d'optimiser le traitement des notices nécrologiques, eDirectory n'utilise plus les attributs de lien de référence distribué suivants :

- `UsedBy`
- `ObitUsedBy`

1.1.8 Caching des événements de journal

Le système des événements de journal est modifié pour vous permettre d'utiliser une combinaison de mémoire et de disque afin de gérer les événements dans la file d'attente. La forte augmentation en mémoire du processus ndsd est ainsi réduite.

Les améliorations apportées aux événements de journal sont les suivantes :

- **Caching**

  Lorsque la file d'attente des événements de journal augmente au-delà d'un certain point dans la mémoire (32 Mo = max. de 8 blocs de 4 Mo), eDirectory démarre à l'aide d'un cache sur le disque dur.

- **Variable**

  Les événements de journal comprennent les variables suivantes que les utilisateurs peuvent configurer :

  - NDSD_EVENT_DISK_CACHE
  - NDSD_EVENT_DISK_CACHE_DIR

- **Compression**

  La compression améliorée réduit la taille des données sur le disque dur. Le taux de compression est d'environ 20:1.

1.1.9 Prise en charge des disques SSD

Cette version prend en charge le disque SSD Enterprise qui améliore les opérations d'E/S.

1.1.10 Évaluation des coûts du renvoi avancé (ARC)

Dans cette version, l'ARC est activée par défaut.

Pour plus d'informations, consultez la section « Advanced Referral Costing » (Évaluation des coûts du renvoi avancé) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

1.1.11 Intervalle de mise à jour de la connexion

La nouvelle option Intervalle de mise à jour de la connexion permet aux administrateurs de spécifier un intervalle (en secondes) pendant lequel eDirectory ne met pas à jour les attributs de connexion.

REMARQUE : Cette option s'applique uniquement aux connexions NDS (NetIQ Directory Services).

Pour plus d'informations, reportez-vous à la section « Controlling and Configuring the DS Agent » (Contrôle et configuration de l'agent DS) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

1.2 Améliorations LDAP

Cette version inclut les améliorations LDAP suivantes :

1.2.1 Contrôle permissif des modifications

Vous pouvez étendre l'opération de modification LDAP à l'aide de cette option. Si vous tentez de supprimer un attribut qui n'existe pas ou d'ajouter une valeur à un attribut existant, l'opération s'effectue sans afficher de message d'erreur.

Pour plus d'informations, consultez la section « Configuring Permissive Modify Control » (Configuration du contrôle permissif de modification) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

1.2.2 Prise en charge de l'heure au format généralisé

La prise en charge de l'heure au format généralisé permet d'afficher l'heure au format `AAAAMMJJHHmmSS.0Z`.

Notez que la valeur `0Z` signifie la même prise en charge des fractions de seconde que dans Active Directory. Dans la mesure où eDirectory n'est pas compatible avec l'affichage des fractions de seconde, cette option affiche *0* afin de ne pas empêcher le fonctionnement dans un environnement coexistant.

Pour plus d'informations, consultez la section « Configuring Generalized Time Support » (Configuration de la prise en charge de l'heure au format généralisé) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

1.2.3 Contrôle de suppression des sous-arborescences

Cette version prend en charge le contrôle de suppression des sous-arborescences qui permet de supprimer tout objet Conteneur. Auparavant, seuls les objets Feuille pouvaient être supprimés. Toutefois, le contrôle de suppression des sous-arborescences ne gère pas la suppression des conteneurs de partition.

1.3 prise en charge d'IPv6

Cette version prend en charge les réseaux IPv4 et IPv6. IPv6 est automatiquement activé par défaut lors de l'installation de eDirectory. Lors de la mise à niveau à partir d'une version antérieure de eDirectory, vous devez activer manuellement la prise en charge de IPv6.

eDirectory 8.8 SP8 prend en charge les modes IPv6 suivants :

- Pile double
- Tunnelage
- IPv6 pur

eDirectory 8.8 SP8 ne prend pas en charge les types d'adresses IPv6 suivants :

- Adresses locales de lien
- Adresses IPv6 assignées IPv4
- Adresses IPv6 compatibles IPv4

eDirectory 8.8 SP8 prend en charge les formats d'adressage suivants :

- [::]
- [::1
- [2015::12]
- [2015::12]:524

1.4 Améliorations d'audit

Cette version améliore l'audit XDAS en prenant en charge l'adresse IP du client dans les événements.

2 Plates-formes prises en charge pour l'installation de eDirectory

eDirectory 8.8 SP8 est une version multi plate-forme visant à améliorer la stabilité de eDirectory.

2.1 Plates-formes obsolètes

eDirectory 8.8 SP8 ne prend pas en charge les plates-formes suivantes :

- NetWare
- eDirectory 32 et 64 bits sous Solaris
- eDirectory 32 bits sous AIX
- eDirectory 32 bits sous Linux
- eDirectory 32 bits sous Windows

2.2 Linux

Vous devez installer eDirectory sur l'une des plates-formes suivantes:

- SLES 11 SP1, SP2 et SP3 64 bits
- SLES 10 SP4 64 bits
- RHEL 5.7, 5.8 et 5.9
- RHEL 6.2, 6.3 et 6.4

Vous pouvez exécuter ces systèmes d'exploitation en mode virtuel sur les hyperviseurs suivants :

- VMware ESXi
- Xen (sur SLES 10 et SLES 11 et leurs Support Packs)

  REMARQUE : eDirectory 8.8 SP8 est pris en charge par le service de virtualisation SLES 10 XEN qui utilise le système d'exploitation invité SLES 10. Les mises à jour suivantes sont disponibles sur le site Web de mise à jour de NetIQ (https://update.novell.com) :

  - SUSE-Linux-Enterprise-Server-X86_64-10-0-20061011-020434
  - SLES10

  Pour enregistrer et mettre à jour SUSE Linux Enterprise 10, consultez la section Enregistrer SUSE Linux Enterprise avec le NetIQ Customer Center (http://www.suse.com/products/register.html). Après avoir installé la dernière mise à jour, assurez-vous que le niveau de correctif minimum de la mise à jour installée est 3.0.2_09763-0.8.

- Virtualisation Windows Server 2008 R2 avec Hyper-V

Pour déterminer la version de SUSE Linux que vous utilisez, consultez le fichier `/etc/SuSE-release`.

Veillez à ce que les correctifs glibc les plus récents soient appliqués à partir de Red Hat Errata (http://rhn.redhat.com/errata) sur les systèmes Red Hat. La version 2.1 est la version minimale requise pour la bibliothèque glibc.

2.3 Windows

Vous devez installer eDirectory sur l'une des plates-formes suivantes:

- Windows Server 2008 (x64) (Standard/Enterprise/Data Center Edition) et Service Packs
- Windows Server 2008 R2 (Standard/Enterprise/Data Center Edition) et Service Packs
- Serveur Windows 2012

IMPORTANT

- Vous devez utiliser un compte avec droits d'administrateur pour installer eDirectory 8.8 SP8 sur Windows Server 2008 R2.
- Les versions bureau de Windows ne sont pas prises en charge.

3 Améliorations relatives à l'installation et la mise à niveau

Ce chapitre traite des nouvelles fonctions et améliorations relatives à l'installation et à la mise à niveau de NetIQ eDirectory 8.8.

Le tableau ci-dessous liste les nouvelles fonctions et précise les plates-formes qui les prennent en charge.

Fonction	Linux	Windows
Formats de paquetage multiples pour l'installation de eDirectory 8.8	✓	✗
Emplacement personnalisé pour l'installation des fichiers d'application	✓	✓
Emplacement personnalisé pour l'installation des fichiers de données	✓	✓
Emplacement personnalisé pour l'installation des fichiers de configuration	✓	✗
Installation non racine	✓	✗
Amélioration de la prise en charge de l'installation sur des grappes haute disponibilité	✓	✓
Conformité FHS	✓	✗
Conformité LSB	✓	✗
Vérifications de l'état de santé du serveur	✓	✓
Intégration de SecretStore	✓	✓
Installation de eDirectory Instrumentation	✓	✓

Ce chapitre comprend les informations suivantes :

3.1 Formats de paquetage multiples pour l'installation de eDirectory 8.8

Sous Linux, vous avez la possibilité de choisir entre plusieurs formats de fichier pendant l'installation de eDirectory 8.8 sur l'hôte. Le tableau ci-dessous liste les différents formats de fichier.

Type d'utilisateur et emplacement de l'installation	Linux
Utilisateur root	
Emplacement par défaut	RPM
Emplacement personnalisé	Tarball
Utilisateur non root	
Emplacement personnalisé	Tarball

Pour plus d'informations sur l'installation des Tarballs, consultez le *Guide d'installation de NetIQ eDirectory 8.8 SP8*.

3.2 Installation de eDirectory 8.8 à un emplacement personnalisé

Avec eDirectory 8.8, vous avez la possibilité d'installer les fichiers d'application, de données et de configuration à un emplacement de votre choix.

Vous pouvez par exemple installer eDirectory 8.8 dans un emplacement personnalisé si une version antérieure de eDirectory est déjà installée sur votre hôte et que vous souhaitez tester eDirectory 8.8 avant d'effectuer la mise à niveau vers cette version. De cette manière, vous ne modifiez pas votre configuration eDirectory existante et pouvez néanmoins tester la nouvelle version. Vous pouvez ensuite décider si vous souhaitez conserver votre version existante ou procéder à une mise à niveau vers eDirectory 8.8.

REMARQUE : SLP et le sous-agent SNMP sont installés aux emplacements par défaut.

Cette section explique comment installer les différents fichiers à un emplacement personnalisé :

3.2.1 Indication d'un emplacement personnalisé pour les fichiers d'application

Pendant l'installation de eDirectory, vous pouvez installer vos fichiers d'application à un emplacement de votre choix.

Linux

Pour installer eDirectory 8.8 à un emplacement personnalisé, vous pouvez utiliser le fichier d'installation tarball et décompresser eDirectory 8.8 à l'emplacement de votre choix.

Windows

Vous aviez la possibilité de spécifier un emplacement personnalisé pour les fichiers d'application pendant la procédure d'installation, et ce même avant la version 8.8 de eDirectory.

3.2.2 Indication d'un emplacement personnalisé pour les fichiers de données

Pendant la configuration de eDirectory, vous pouvez enregistrer les fichiers de données à un emplacement de votre choix. Les fichiers de données incluent les répertoires `data`, `dib` et `log`.

Linux

Pour configurer les fichiers de données dans un emplacement personnalisé, vous pouvez utiliser l'option `-d` ou `-D` de l'utilitaire ndsconfig.

Option	Description
-d *emplacement_personnalisé*	Crée le répertoire `DIB` (base de données eDirectory) dans le chemin mentionné. **REMARQUE :** Cette option existait déjà avant la version 8.8 de eDirectory.
-D *emplacement_personnalisé*	Crée les répertoires `data` (contenant des données telles que les PID et les ID de socket), `dib` et `log` dans le chemin mentionné.

Windows

Sous Windows, vous êtes invité à entrer le chemin d'accès à la DIB pendant l'installation. Entrez le chemin de votre choix.

3.2.3 Indication d'un emplacement personnalisé pour les fichiers de configuration

Pendant la configuration de eDirectory, vous pouvez sélectionner l'emplacement de destination des fichiers de configuration.

Linux

Pour configurer le fichier de configuration `nds.conf` dans un autre emplacement, utilisez l'option `--config-file` de l'utilitaire ndsconfig.

Pour installer les autres fichiers de configuration (tels que `modules.conf`, `ndsimon.conf` et `ice.conf`) dans un autre emplacement, procédez comme suit :

1. Copiez tous les fichiers de configuration au nouvel emplacement.
2. Configurez le nouvel emplacement en entrant la commande suivante :

   ```
   ndsconfig set n4u.nds.configdir emplacement_personnalisé
   ```

Windows

Vous ne pouvez pas spécifier d'emplacement personnalisé pour les fichiers de configuration sous Windows.

3.3 Installation non racine

eDirectory 8.8 et les versions ultérieures prennent en charge l'installation et la configuration de serveurs eDirectory par un utilisateur non root. Les versions antérieures de eDirectory ne pouvaient être installées et configurées que par un utilisateur root, avec une seule instance de eDirectory qui s'exécutait sur un hôte.

À partir de eDirectory 8.8, tout utilisateur non root peut désormais utiliser une version Tarball pour installer eDirectory. Plusieurs installations binaires eDirectory peuvent être effectuées par le même utilisateur ou par des utilisateurs différents. Toutefois, même pour les installations effectuées par des utilisateurs non root, les services de niveau système tels que NICI (Novell International Cryptographic Infrastructure), SNMP et SLP ne peuvent être installés qu'avec des privilèges root. Le composant NICI est obligatoire pour le fonctionnement de eDirectory, tandis que les composants SNMP et SLP sont facultatifs. En outre, dans le cadre d'une installation par paquetage, l'utilisateur root ne peut installer qu'une seule instance.

Après l'installation, un utilisateur non root peut configurer les instances de serveur eDirectory à l'aide de sa propre installation Tarball ou à l'aide d'une installation binaire. Cela signifie que plusieurs instances de serveurs eDirectory peuvent s'exécuter sur un même hôte, car tout utilisateur, root ou non root, peut configurer différentes instances de serveur eDirectory sur un même hôte par installation par paquetage ou Tarball. Pour plus d'informations sur la fonctionnalité d'instances multiples, reportez-vous aux sections « Instances multiples » et « Mise à niveau d'instances multiples » du *Guide d'installation de NetIQ eDirectory 8.8 SP8*.

La configuration et l'installation non root s'appliquent uniquement aux plates-formes Linux. Pour plus d'informations sur la configuration et l'installation non root, reportez-vous à la section « Installation de eDirectory 8.8 en tant qu'utilisateur non root » du *Guide d'installation de NetIQ eDirectory 8.8 SP8*.

3.4 Amélioration de la prise en charge de l'installation sur des grappes haute disponibilité

eDirectory 8.8 SP8 simplifie l'installation et la gestion de eDirectory sur des grappes Linux et Windows, ce qui améliore la prise en charge de la mise en grappe et permet de bénéficier d'une disponibilité élevée. eDirectory permet également de bénéficier d'une disponibilité élevée grâce à la synchronisation des répliques, qui peut être associée à la mise en grappe afin d'améliorer le niveau de disponibilité.

Pour plus d'informations sur l'installation de eDirectory sur des grappes, consultez le *Guide d'installation de NetIQ eDirectory 8.8 SP8*.

3.5 Conformité aux normes

eDirectory 8.8 est conforme aux normes suivantes :

- Section 3.5.1, « Conformité FHS », page 23
- Section 3.5.2, « Conformité LSB », page 24

3.5.1 Conformité FHS

Pour éviter les conflits avec les fichiers d'application d'autres produits, eDirectory 8.8 respecte la norme FHS (Filesystem Hierarchy Standard). Cette fonction n'est disponible que sur Linux.

eDirectory respecte cette structure de répertoires uniquement si vous avez choisi de l'installer à l'emplacement par défaut. Si vous avez choisi un emplacement personnalisé, la structure de répertoires sera *emplacement_personnalisé/chemin_par_défaut*.

Par exemple, si vous choisissez d'effectuer l'installation dans le répertoire `eDir88`, la même structure de répertoires est utilisée dans ce répertoire `eDir88` ; par conséquent, les pages du manuel seront installées dans le répertoire `/eDir88/opt/novell/man`.

Le tableau suivant liste les changements au niveau de la structure de répertoires :

Types de fichiers stockés dans le répertoire	Nom et chemin du répertoire
Scripts de shell statiques et binaires exécutables	`/opt/novell/eDirectory/bin`
Binaires exécutables pour une utilisation root	`/opt/novell/eDirectory/sbin`
Binaires de bibliothèque statiques ou dynamiques	`/opt/novell/eDirectory/lib`
les fichiers de configuration.	`/etc/opt/novell/eDirectory/conf`
Données dynamiques d'exécution en lecture/ écriture, comme la DIB	`/var/opt/novell/eDirectory/data`
fichiers journaux	`/var/opt/novell/eDirectory /log`
Pages du manuel Linux	`/opt/novell/man`

Exportation de variables d'environnement

Avec la mise en oeuvre de FHS dans eDirectory 8.8, vous devez mettre à jour les variables d'environnement PATH et les exporter, ce qui entraîne les problèmes suivants :

- Vous devez vous rappeler tous les chemins exportés, de sorte que lorsque vous ouvrez un shell, vous devez exporter ces chemins avant de pouvoir utiliser les utilitaires.
- Si vous souhaitez utiliser plusieurs ensembles de binaires, vous devez ouvrir plusieurs shells ou encore affecter ou désaffecter fréquemment les chemins aux différents ensembles de binaires.

Pour résoudre ce problème, vous pouvez utiliser le script `/opt/novell/eDirectory/bin/ndspath` comme suit :

- Préfixez le script ndspath à l'utilitaire souhaité et exécutez-le comme suit :

  ```
  custom_location/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
  ```

- Exportez les chemins dans le shell actuel comme suit :

  ```
  . custom_location/opt/novell/eDirectory/bin/ndspath
  ```

- Après avoir entré la commande ci-dessus, exécutez les utilitaires comme d'habitude. Appelez le script bashrc dans votre profil ou des scripts similaires. Ainsi, lorsque vous vous connectez ou que vous ouvrez un nouveau shell, vous pouvez commencer à utiliser les utilitaires directement.

3.5.2 Conformité LSB

eDirectory 8.8 est désormais compatible LSB (Linux Standard Base). LSB recommande également la compatibilité FHS. Tous les paquetages eDirectory sous Linux portent le préfixe *novell*. Par exemple, `NDSserv` s'appelle désormais `novell-NDSserv`.

3.6 Vérifications de l'état de santé du serveur

eDirectory 8.8 propose des vérifications de l'état de santé du serveur qui permettent de s'assurer que l'état de santé du serveur est bon avant la mise à niveau.

Les vérifications de l'état de santé du serveur s'exécutent par défaut lors de chaque mise à niveau et s'opèrent avant la mise à niveau proprement dite du paquetage. Vous pouvez exécuter également l'outil de diagnostic ndscheck pour vérifier l'état de santé.

3.6.1 Avantage des vérifications de l'état de santé

Les versions antérieures de eDirectory ne vérifiaient pas l'état de santé du serveur avant de procéder à la mise à niveau. Si le serveur n'était pas en bonne condition, la mise à niveau risquait d'échouer et eDirectory pouvait se trouver dans un état instable. Dans certains cas, vous ne pouviez peut-être plus récupérer les paramètres existant avant la mise à niveau.

Grâce à ce nouvel outil, vous êtes désormais certain que votre serveur est prêt pour la mise à niveau.

3.6.2 État de santé d'un serveur

L'utilitaire de vérification de l'état de santé du serveur exécute certaines vérifications de l'état de santé pour garantir que l'arborescence est saine. L'arborescence est déclarée saine lorsque toutes ces vérifications de l'état de santé ont abouti.

3.6.3 Vérifications de l’état de santé

Vous pouvez vérifier l'état de santé du serveur de deux manières :

- « Avec la mise à niveau » page 25
- « Avec un utilitaire autonome » page 25

REMARQUE : pour exécuter l’utilitaire de vérification de l’état de santé, vous devez disposer de droits d’administrateur. Le droit minimal qui peut être défini pour l'exécution de l'utilitaire est le droit Public. Toutefois, avec le droit Public, certains objets NCP (NetWare Core Protocol) et certaines informations de partition ne sont pas disponibles.

Avec la mise à niveau

Les vérifications de l’état de santé sont exécutées par défaut à chaque mise à niveau de eDirectory.

Linux

Lors de chaque mise à niveau, l’état de santé est vérifié par défaut avant le début de la mise à niveau proprement dite.

Pour ignorer les vérifications de l'état de santé par défaut, vous pouvez utiliser l'option -j avec l'utilitaire nds-install.

Windows

Les vérifications de l'état de santé du serveur sont effectuées dans le cadre de la procédure d'installation à l'aide de l'Assistant. Vous pouvez activer ou désactiver ces vérifications lorsque vous y êtes invité.

Avec un utilitaire autonome

Vous pouvez à tout moment vérifier l'état de santé du serveur au moyen d'un utilitaire autonome. Le tableau suivant décrit les utilitaires de vérification de l'état de santé :

Tableau 3-1 *Utilitaires de vérification de l’état de santé*

Plate-forme	Nom de l’utilitaire
Linux	ndscheck Syntaxe : `ndscheck -h hostname:port -a admin_FDN -F logfile_path --config-file configuration_file_name_and_path` **REMARQUE :** Vous pouvez spécifier soit l'option `-h` soit l'option `--config-file`, mais pas les deux.
Windows	ndscheck

3.6.4 Types de vérifications de l’état de santé

Lorsque vous procédez à une mise à niveau ou que vous exécutez l'utilitaire ndscheck, les vérifications de l'état de santé suivantes sont effectuées :

- État de santé général du serveur
- État de santé des partitions et répliques

Si vous exécutez l'utilitaire ndscheck, le résultat des vérifications de l'état de santé est affiché à l'écran et consigné dans le fichier `ndscheck.log`. Pour plus d’informations sur les fichiers journaux, reportez-vous à la section Section 3.6.6, « Fichiers journaux », page 27.

Si l'état de santé est vérifié dans le cadre de la mise à niveau, au terme de la vérification, la mise à niveau pourra être poursuivie si vous y êtes invité ou sera abandonnée, et ce en fonction du caractère critique de l'erreur. Les erreurs sont détaillées à la section Section 3.6.5, « Catégorisation de l’état de santé », page 26.

État de santé général du serveur

Il s'agit de la première étape de la vérification de l'état de santé. L'utilitaire vérifie les points suivants :

1. Le service eDirectory est fonctionnel. La DIB est ouverte et capable de lire certaines informations de base sur l'arborescence, comme son nom.
2. Le serveur écoute sur les numéros de port respectifs.

   Pour LDAP, il obtient les numéros de port TCP et SSL et vérifie si le serveur écoute sur ces ports.

   De même, il obtient les numéros de port HTTP et HTTP sécurisé et vérifie si le serveur écoute sur ces ports.

État de santé des partitions et répliques

Après avoir vérifié l'état de santé général du serveur, l'étape suivante consiste à vérifier l'état de santé des partitions et répliques comme suit :

1. Vérifie l’état de santé des répliques des partitions locales.
2. Lit l'anneau de répliques de chacune des partitions gérées par le serveur et vérifie que tous les serveurs de l'anneau de répliques sont fonctionnels et que toutes les répliques ont l'état ACTIF.
3. Vérifie la synchronisation horaire de tous les serveurs de l'anneau de répliques afin d'afficher le décalage horaire entre les serveurs.

3.6.5 Catégorisation de l’état de santé

En fonction des erreurs détectées lors de la vérification de l'état de santé d'un serveur, on dénombre trois catégories d'état de santé. Le résultat des vérifications de l'état de santé est consigné dans un fichier journal. Pour plus d’informations, reportez-vous à la Section 3.6.6, « Fichiers journaux », page 27.

Les trois types d'état de santé sont Normal, Avertissement et Critique.

Normal

L'état de santé du serveur est normal lorsque toutes les vérifications ont abouti.

La mise à niveau se poursuit sans interruption.

Avertissement

L'état de santé du serveur relève de la catégorie Avertissement lorsque des erreurs mineures sont détectées pendant la vérification.

Si l'état de santé est vérifié dans le cadre de la mise à niveau, vous êtes invité à abandonner ou à continuer.

Des avertissements se présentent généralement dans les cas suivants :

1. Le serveur n'écoute pas sur les ports LDAP et HTTP (normal, sécurisé ou les deux).
2. Impossibilité de contacter un des serveurs non maîtres dans l'anneau de répliques.
3. Les serveurs de l'anneau de répliques ne sont pas synchronisés.

Critique

L'état de santé du serveur est critique lorsque des erreurs critiques ont été détectées pendant la vérification.

Si l'état de santé est vérifié dans le cadre de la mise à niveau de, la mise à niveau est abandonnée.

L'état critique se présente généralement dans les cas suivants :

1. Impossibilité de lire ou d'ouvrir la DIB. La DIB est peut-être verrouillée ou altérée.
2. Impossibilité de contacter tous les serveurs de l'anneau de répliques.
3. Les partitions locales sont occupées.
4. La réplique n'a pas l'état ACTIF.

3.6.6 Fichiers journaux

Chaque vérification de l'état de santé du serveur, qu'elle soit exécutée avec la mise à niveau ou en tant qu'utilitaire autonome, consigne l'état de santé dans un fichier journal.

Le contenu du fichier journal est similaire aux messages qui s'affichent à l'écran lors des vérifications.

Le fichier journal de vérification de l'état de santé contient les éléments suivants :

- Résultat des vérifications de l'état de santé (normal, avertissement ou critique).
- URL du site de support NetIQ.

Le tableau suivant indique les emplacements du fichier journal sur les différentes plates-formes :

Tableau 3-2 *Emplacements du fichier journal de l'état de santé*

Plate-forme	Nom du fichier journal	Emplacement du fichier journal
Linux	`ndscheck.log`	Dépend de l'emplacement spécifié avec l'option -F de l'utilitaire `ndscheck`. Si vous n'avez pas utilisé l'option `-F`, l'emplacement du fichier `ndscheck.log` est déterminé par les autres options mentionnées dans la ligne de commande de ndscheck comme suit : 1. Si vous avez utilisé l'option `-h`, le fichier `ndscheck.log` est enregistré dans le répertoire privé de l'utilisateur. 2. Si vous avez utilisé l'option `--config-file`, le fichier `ndscheck.log` est enregistré dans le répertoire des journaux de l'instance de serveur. Vous pouvez également sélectionner une instance dans la liste.
Windows	`ndscheck.log`	*`répertoire_installation`*

3.7 Intégration de SecretStore dans eDirectory

eDirectory 8.8 permet de configurer Novell SecretStore 3.4 en même temps que eDirectory. Vous devez installer manuellement SecretStore avant eDirectory 8.8.

SecretStore est une solution simple et sécurisée de gestion des mots de passe. Vous pouvez utiliser l'authentification unique auprès de eDirectory pour accéder à la plupart des applications Linux, Windows, Web et macroordinateur.

Lorsque vous êtes authentifié auprès de eDirectory, les applications compatibles SecretStore stockent et récupèrent les références de connexion appropriées. Lorsque vous utilisez SecretStore, vous évitez de devoir mémoriser ou synchroniser la multitude de mots de passe requis pour accéder aux applications, sites Web et gros systèmes protégés par mot de passe.

Pour configurer SecretStore 3.4 en même temps que eDirectory, procédez comme suit :

- **Linux :**

  Utilisez le paramètre `ndsconfig add -m ss`. Dans ce cas, `ss` fait référence à SecretStore et est un paramètre facultatif. Si vous ne mentionnez pas le nom du module, tous les modules sont installés. Si vous ne souhaitez pas configurer SecretStore, vous pouvez transmettre la valeur `no_ss` à cette option en spécifiant `-m no_ss`.

- **Windows :**

  Lors de l'installation de eDirectory, une option permet de spécifier si vous souhaitez configurer le module SecretStore. Par défaut, cette option est sélectionnée.

Pour plus d'informations sur l'utilisation de SecretStorage, consultez le manuel *Novell SecretStore 3.4 Administration Guide* (https://www.netiq.com/documentation/secretstore34/) (Guide d'administration de Novell SecretStore 3.4).

3.8 Installation de eDirectory Instrumentation

Les outils eDirectory précédents faisaient partie de Novell Audit. À partir de la version 8.8 SP3 de eDirectory, eDirectory Instrumentation doit être installé séparément.

Pour plus d'informations sur l'installation, la configuration et la désinstallation de eDirectory Instrumentation, reportez-vous à la section concernant eDirectory Instrumentation du *Guide d'installation de NetIQ eDirectory 8.8 SP8*.

3.9 Pour plus d'informations

Pour plus d'informations sur l'une des fonctions détaillées dans ce chapitre, consultez les références suivantes :

- *NetIQ eDirectory 8.8 SP8 Installation Guide (Guide d'installation de NetIQ eDirectory 8.8 SP8)*
- *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8)
- Sur Linux : pages du manuel `nds-install`, `ndsconfig` et `ndscheck`

4 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 clé de base de données nécessaire à l'ouverture du fichier DIB est encapsulée avec des clés NICI. Par conséquent, si la sauvegarde eDirectory est effectuée indépendamment de la sauvegarde NICI, elle n'est d'aucune utilité.

Modifications par l'intermédiaire du mécanisme précédent de sauvegarde et de restauration NICI

Auparavant, la sauvegarde et la restauration NICI devaient être réalisées manuellement. Une solution de sauvegarde et de restauration NICI a été ajoutée dans cette version. Le paramètre `-e` a été ajouté à la solution de sauvegarde eDirectory (sauvegarde eMBox et DSBK) ; il permet d'effectuer les opérations suivantes :

1. Sauvegarde des clés NICI lors de l'exécution d'une sauvegarde eDirectory
2. Restauration des clés NICI lors de l'exécution d'une restauration eDirectory

Reportez-vous à la section « Backing Up and Restoring NICI » (Sauvegarde et restauration NICI) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

5 Utilitaire ndspassstore

Le nouvel utilitaire ndspassstore permet de stocker le mot de passe codé de l'utilisateur sadmin ou eDirectory. Cet utilitaire est disponible sur les plates-formes Linux et Windows. Cet utilitaire se sert du nom d'utilisateur et du mot de passe en tant qu'entrées et les stocke sous forme de paires clé-valeur codées.

Dans cette version, cet utilitaire est utilisé pour définir le mot de passe sadmin.

Cet utilitaire est disponible par défaut dans les répertoires `C:\Novell\NDS` sous Windows et `/opt/novell/eDirectory/bin` sous Linux.

Synthèse de la commande

Vous pouvez utiliser l'utilitaire ndspassstore en saisissant la commande suivante sur la console du serveur :

```
ndspassstore -a <adminContext> -w <mot_de_passe>
```

Option	Utilisation
-a adminContext	Cette option permet d'accepter le contexte adminContext ; c'est le nom distinctif d'un utilisateur ayant des droits d'administrateur.
-w mot_de_passe	Cette option sert à accepter le mot de passe (mot de passe utilisateur) pour l'authentification.

6 Instances multiples

Auparavant, il n'était possible de configurer qu'une seule instance de NetIQ eDirectory sur un hôte unique. Désormais, grâce à la fonction d'instances multiples prise en charge par eDirectory 8.8, vous pouvez configurer les éléments suivants :

- plusieurs instances de eDirectory sur un hôte unique ;
- plusieurs arborescences sur un hôte unique ;
- plusieurs répliques de la même arborescence ou partition sur un hôte unique.

eDirectory 8.8 propose également un utilitaire (ndsmanage) qui permet de suivre aisément les instances.

Le tableau suivant liste les plates-formes prenant en charge les instances multiples :

Fonction	Linux	Windows
Prise en charge d'instances multiples	✓	✗

Ce chapitre comprend les informations suivantes :

6.1 Avantages des instances multiples

Les instances multiples ont été créées pour répondre à un besoin afin d'en tirer les avantages suivants :

- tirer parti d'un matériel haut de gamme en configurant plusieurs instances de eDirectory ;
- piloter votre configuration sur un hôte unique avant d'investir dans le matériel requis.

6.2 Exemples de scénarios pour le déploiement d'instances multiples

Des instances multiples appartenant à des arborescences identiques ou différentes peuvent en réalité être utilisées dans les scénarios suivants.

eDirectory dans une grande entreprise

- Dans les grandes entreprises, vous pouvez assurer un équilibrage de la charge et une disponibilité élevée des services eDirectory.

  Par exemple, si vous avez trois serveurs de répliques exécutant des services LDAP sur les ports 1 524, 2 524 et 3 524 respectivement, vous pouvez configurer une nouvelle instance de eDirectory et fournir un service LDAP hautement disponible sur un nouveau port 636.
- Vous pouvez tirer parti d'un matériel haut de gamme dans divers département d'une organisation en configurant plusieurs instances sur un hôte unique.

eDirectory dans un environnement d'évaluation

- **Universités :** grâce aux instances multiples, de nombreux (étudiants) enthousiastes peuvent évaluer eDirectory à partir du même hôte.
- **Formation sur l'administration de eDirectory :**
  - Des participants peuvent tester l'administration grâce aux instances multiples.
  - Des professeurs peuvent utiliser un hôte unique pour enseigner à une classe d'étudiants. Chaque étudiant peut ainsi disposer de sa propre arborescence.

6.3 Utilisation d'instances multiples

eDirectory 8.8 permet de configurer très facilement des instances multiples. Pour pouvoir effectivement utiliser plusieurs instances, vous devez planifier la configuration, puis configurer les différentes instances.

- Section 6.3.1, « Planification de la configuration », page 36
- Section 6.3.2, « Configuration d'instances multiples », page 36

6.3.1 Planification de la configuration

Pour utiliser cette fonction efficacement, nous vous recommandons de planifier les instances de eDirectory et de vous assurer que chaque instance a des identificateurs définis, comme le nom de l'hôte, le numéro de port, le nom de serveur ou le fichier de configuration.

Pendant la configuration des instances multiples, vous devez vérifier que vous avez bien planifié les éléments suivants :

- Emplacement du fichier de configuration ;
- Emplacement des données variables (par exemple les fichiers journaux) ;
- Emplacement de la DIB ;
- Interface NCP™, port d'identification unique pour chaque instance et ports d'autres services (comme les ports LDAP, LDAPS, HTTP et HTTP sécurisé)
- Un nom de serveur unique pour chaque instance

6.3.2 Configuration d'instances multiples

Vous pouvez configurer plusieurs instances de eDirectory à l'aide de l'utilitaire ndsconfig. Le tableau suivant liste les options ndsconfig à inclure lors de la configuration d'instances multiples.

REMARQUE : Toutes les instances partagent la même clé de serveur (NICI).

Option	Description
--config-file	Indique le chemin absolu et le nom du fichier de configuration `nds.conf`. Par exemple, pour stocker le fichier de configuration dans le répertoire `/etc/opt/novell/eDirectory/`, utilisez la commande `--config-file /etc/opt/novell/eDirectory/nds.conf`.
-b	Indique le numéro de port sur lequel la nouvelle instance doit écouter. **REMARQUE :** Seuls `-b` et `-B` sont utilisés.

-B	Indique le numéro de port ainsi que l'interface ou l'adresse IP. Par exemple :
	
	`-B eth0@524`
	
	ou
	
	`-B 100.1.1.2@524`
	
	REMARQUE : Seuls `-b` et `-B` sont utilisés.

-D	Crée les répertoires `data`, `dib` et `log` dans le chemin spécifié pour la nouvelle instance.
S	Nom du serveur.

Les options susmentionnées vous permettent de configurer une nouvelle instance de eDirectory.

Vous pouvez également configurer une nouvelle instance à l'aide de l'utilitaire ndsmanage. Pour plus d'informations, reportez-vous à la « Création d'une instance via ndsmanage » page 38.

6.4 Gestion d'instances multiples

Cette section présente les informations suivantes :

6.4.1 Utilitaire ndsmanage

L'utilitaire ndsmanage permet d'effectuer les opérations suivantes :

- Lister les instances configurées
- Créer une instance
- Effectuer les opérations suivantes pour une instance sélectionnée :
  - Lister les répliques sur le serveur
  - Démarrer l'instance
  - Arrêter l'instance

- Exécuter DSTrace (ndstrace) pour l'instance
- Annuler la configuration de l’instance

- Démarrer et arrêter toutes les instances

Liste des instances

Le tableau suivant décrit comment lister les instances eDirectory.

Tableau 6-1 *Utilisation de ndsmanage pour lister les instances*

Syntaxe	Description
ndsmanage	Liste toutes les instances que vous avez configurées.
ndsmanage -a|--all	Liste les instances de tous les utilisateurs d’une installation spécifique de eDirectory.
ndsmanage *nom_utilisateur*	Liste les instances configurées par un utilisateur spécifique

Les champs suivants sont affichés pour chaque instance :

- Chemin d’accès au fichier de configuration
- Port et FDN du serveur
- État (instance active ou inactive)

REMARQUE : Cet utilitaire liste toutes les instances configurées pour un seul binaire.

Reportez-vous à Figure 6-1 page 38 pour plus d’informations.

Création d’une instance via ndsmanage

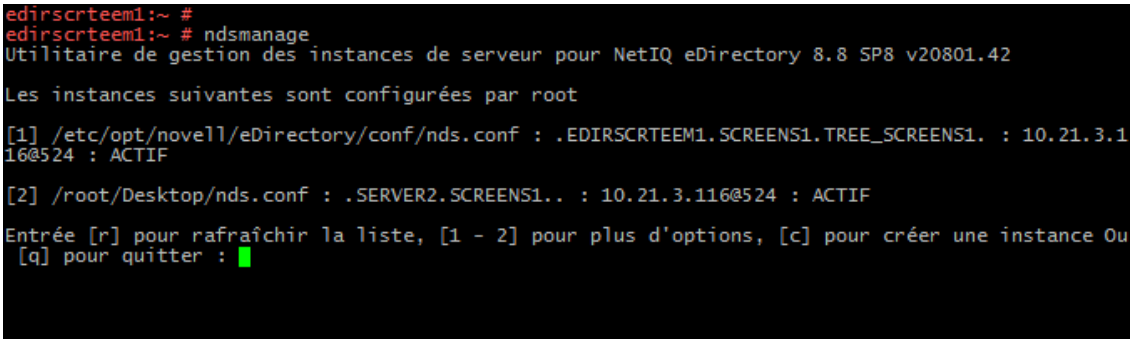
Pour créer une instance via ndsmanage :

1 Saisissez la commande suivante :

```
ndsmanage
```

Si deux instances sont configurées, l’écran suivant s’affiche :

Figure 6-1 *Écran de sortie de l’utilitaire ndsmanage*



2 Entrez c pour créer une instance.

Vous pouvez créer une arborescence ou ajouter un serveur à une arborescence existante. Suivez les instructions à l'écran pour créer une instance.

Exécution d'opérations pour une instance spécifique

Vous pouvez effectuer les opérations suivantes pour chaque instance :

- « Démarrage d'une instance spécifique » page 39
- « Arrêt d'une instance spécifique » page 40
- « Annulation de la configuration d'une instance » page 40

Hormis les opérations listées ci-dessus, vous pouvez également exécuter DSTrace pour une instance sélectionnée.

Démarrage d'une instance spécifique

Pour démarrer une instance que vous avez configurée, procédez comme suit :

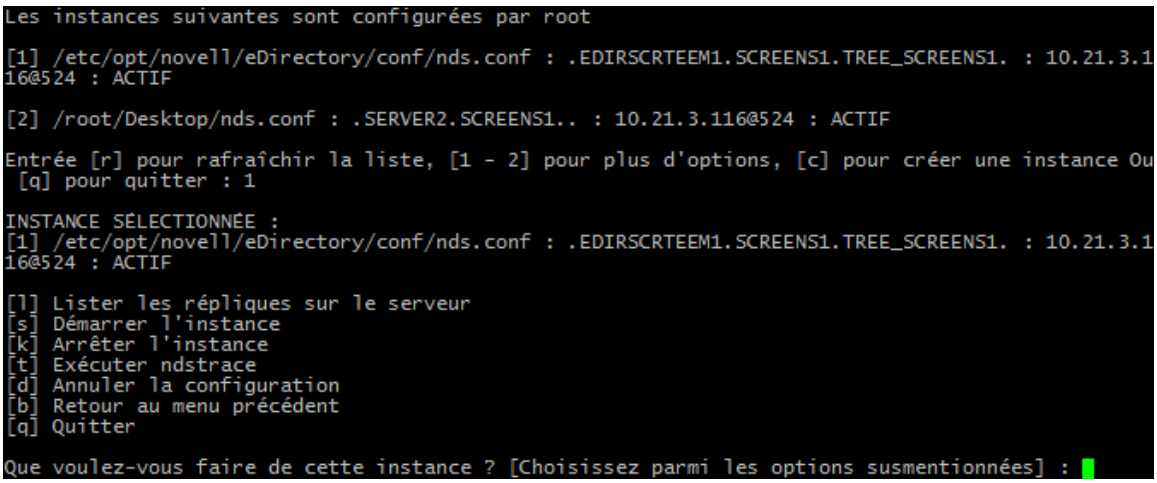
1 Saisissez la commande suivante :

```
ndsmanage
```

2 Sélectionnez l'instance à démarrer.

Le menu se développe pour inclure les options que vous pouvez exécuter sur une instance spécifique.

Figure 6-2 *Écran de sortie de l'utilitaire ndsmanage avec options d'instance*



3 Entrez s pour démarrer l'instance.

Sinon, vous pouvez également entrer la commande suivante à l'invite :

```
ndsmanage start --config-file
fichier_configuration_instance_configurée_par_vos_soins
```

Arrêt d'une instance spécifique

Pour arrêter une instance que vous avez configurée, procédez comme suit :

1. Saisissez la commande suivante :

   ```
   ndsmanage
   ```

2. Sélectionnez l'instance à arrêter.

   Le menu se développe pour inclure les options que vous pouvez exécuter sur une instance spécifique. Pour plus d'informations, reportez-vous à la Écran de sortie de l'utilitaire ndsmanage avec options d'instance (page 39).

3. Entrez `k` pour arrêter l'instance.

Sinon, vous pouvez également entrer la commande suivante à l'invite :

```
ndsmanage stop --config-file
fichier_configuration_instance_configurée_par_vos_soins
```

Annulation de la configuration d'une instance

Pour annuler la configuration d'une instance, procédez comme suit :

1. Saisissez la commande suivante :

   ```
   ndsmanage
   ```

2. Sélectionnez l'instance dont vous souhaitez annuler la configuration.

   Le menu se développe pour inclure les options que vous pouvez exécuter sur une instance spécifique. Pour plus d'informations, reportez-vous à la Écran de sortie de l'utilitaire ndsmanage avec options d'instance (page 39).

3. Entrez `d` pour annuler la configuration de l'instance.

Démarrage et arrêt de toutes les instances

Vous pouvez démarrer et arrêter toutes les instances que vous avez configurées.

Démarrage de toutes les instances

Pour démarrer toutes les instances que vous avez configurées, entrez la commande suivante à l'invite :

```
ndsmanage startall
```

Pour démarrer une instance spécifique, reportez-vous à la section « Démarrage d'une instance spécifique » page 39.

Arrêt de toutes les instances

Pour arrêter toutes les instances que vous avez configurées, entrez la commande suivante à l'invite :

```
ndsmanage stopall
```

Pour arrêter une instance spécifique, reportez-vous à la section « Arrêt d'une instance spécifique » page 40.

6.4.2 Identification d'une instance spécifique

Pendant que vous configurez plusieurs instances, vous assignez à chaque instance un nom d'hôte, un numéro de port et un chemin d'accès unique au fichier de configuration. Le nom d'hôte et le numéro de port sont les identificateurs de l'instance.

La plupart des utilitaires intègrent l'option `-h` *`nom_hôte:port`* ou `--config-file` *`emplacement_fichier_configuration`* qui permet d'indiquer une instance spécifique. Pour plus d'informations, consultez les pages du manuel relatives à ces utilitaires.

6.4.3 Appel d'un utilitaire pour une instance spécifique

Si vous souhaitez exécuter un utilitaire pour une instance spécifique, vous devez inclure l'identificateur de cette instance dans la commande de l'utilitaire. Les identificateurs d'instance sont le chemin d'accès au fichier de configuration, le nom d'hôte et le numéro de port. Pour ce faire, vous pouvez utiliser l'option `--config-file` *`emplacement_fichier_configuration`* ou `-h` *`nom_hôte:port`*.

Si vous n'incluez pas les identificateurs d'instance dans la commande, l'utilitaire affiche les différentes instances dont vous êtes propriétaire et vous invite à sélectionner l'instance pour laquelle vous souhaitez exécuter l'utilitaire.

Par exemple, afin d'exécuter DSTrace pour un utilitaire spécifique à l'aide de l'option `--config-file`, vous devez entrer la commande suivante :

```
ndstrace --config-file configuration_filename_with_location
```

6.5 Exemple de scénario pour des instances multiples

Utilisateur non root, Marie souhaite configurer deux arborescences sur une seule machine hôte pour un binaire unique.

6.5.1 Planification de la configuration

Marie spécifie les identificateurs d'instance suivants.

- **Instance 1 :**

Numéro de port sur lequel l'instance doit écouter	1 524
Chemin d'accès au fichier de configuration	`/home/marieinst1/nds.conf`
Répertoire de la DIB	`/home/marie/inst1/var`

- **Instance 2 :**

Numéro de port sur lequel l'instance doit écouter	2 524
Chemin d'accès au fichier de configuration	`/home/marie/inst2/nds.conf`
Répertoire de la DIB	`/home/marie/inst2/var`

6.5.2 Configuration des instances

Pour configurer les instances en fonction des identificateurs d'instance susmentionnés, Marie doit entrer les commandes suivantes.

- **Instance 1 :**

  ```
  ndsconfig new -t mytree -n o=novell -a cn=admin.o=company -b 1524 -D
  /home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
  ```

- **Instance 2 :**

  ```
  ndsconfig new -t corptree -n o=novell -a cn=admin.o=company -b 2524 -D
  /home/mary/inst2/var --config-file /home/mary/inst2/nds.conf
  ```

6.5.3 Appel d'un utilitaire pour une instance

Si Marie souhaite exécuter l'utilitaire DSTrace pour l'instance 1 qui écoute sur le port 1 524 et dont le fichier de configuration se trouve à l'emplacement `/home/marie/inst1/nds.conf` et le fichier DIB dans le répertoire `/home/marie/inst1/var`, elle peut exécuter l'utilitaire comme suit :

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

ou

```
ndstrace -h 164.99.146.109:1524
```

Si elle ne spécifie pas d'identificateur d'instance, l'utilitaire affiche toutes les instances appartenant à Marie et l'invite à en sélectionner une.

6.5.4 Liste des instances

Si Marie souhaite plus d'informations sur les instances de l'hôte, elle peut exécuter l'utilitaire ndsmanage.

- Pour afficher toutes les instances appartenant à Marie :

  ```
  ndsmanage
  ```

- Pour afficher toutes les instances appartenant à John (dont le nom d'utilisateur est john) :

  ```
  ndsmanage john
  ```

- Pour afficher toutes les instances de tous les utilisateurs d'une installation spécifique de eDirectory :

  ```
  ndsmanage -a
  ```

6.6 Pour plus d'informations

Pour plus d'informations sur la prise en charge des instances multiples, consultez les documents suivants :

- *NetIQ eDirectory 8.8 SP8 Installation Guide (Guide d'installation de NetIQ eDirectory 8.8 SP8)*
- Pour Linux : pages du manuel ndsconfig et ndsmanage

7 Authentification auprès de eDirectory via SASL-GSSAPI

Le mécanisme SASL-GSSAPI pour NetIQ eDirectory 8.8 vous permet de vous authentifier auprès de eDirectory via LDAP à l'aide d'un ticket Kerberos, sans devoir entrer le mot de passe utilisateur de eDirectory. Le ticket Kerberos peut être obtenu en s'authentifiant auprès d'un serveur Kerberos.

Cette fonctionnalité est surtout utile aux utilisateurs d'applications LDAP dans des environnements disposant d'une infrastructure Kerberos existante. Ces utilisateurs peuvent ainsi s'authentifier auprès du serveur LDAP sans devoir fournir un mot de passe utilisateur LDAP distinct.

C'est dans cette optique que eDirectory intègre désormais le mécanisme SASL-GSSAPI.

La mise en oeuvre actuelle de SASL-GSSAPI est compatible avec la convention RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222) et ne prend en charge que le mécanisme d'authentification Kerberos v5.

Ce chapitre comprend les informations suivantes :

7.1 Concepts

7.1.1 Définition de Kerberos

Kerberos est un protocole standard qui permet d'authentifier des entités sur un réseau. Basé sur un modèle tiers approuvé, il inclut des secrets partagés et utilise la cryptographie à clé symétrique.

Pour plus d'informations, reportez-vous à la section RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

7.1.2 Définition de SASL

SASL (Simple Authentication and Security Layer) offre aux applications une couche d'abstraction d'authentification. Il s'agit d'un cadre auquel les modules d'authentification peuvent être connectés.

Pour plus d'informations, reportez-vous à la section RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.1.3 Définition de GSSAPI

L'interface GSSAPI (Generic Security Services Application Program Interface) propose des services d'authentification et autres services de sécurité via un ensemble standard d'API. Elle prend en charge différents mécanismes d'authentification, le plus courant étant Kerberos v5.

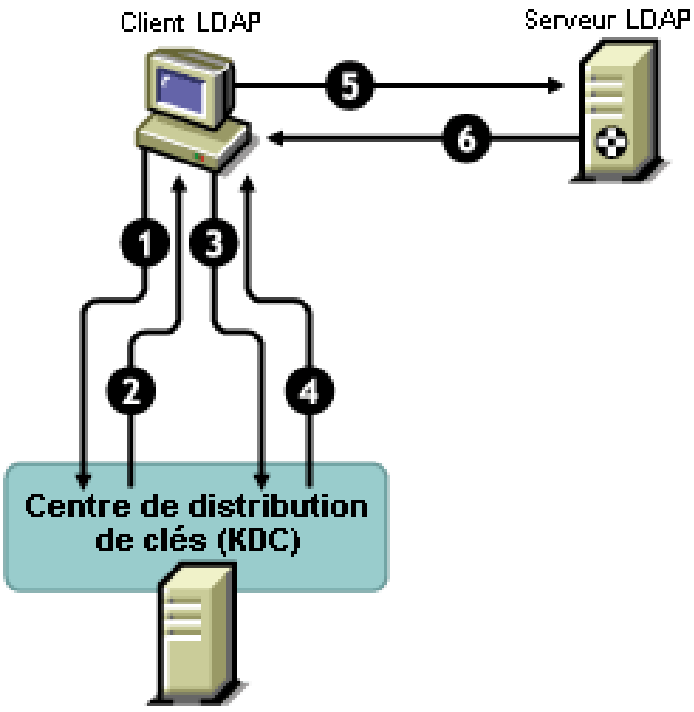
Pour plus d'informations sur les API GSS, reportez-vous à la section RFC 1964 (http://www.ietf.org/rfc/rfc1964.txt?number=1964).

Cette mise en oeuvre de SASL-GSSAPI commence à la section 7.2 de RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.2 Fonctionnement de GSSAPI avec eDirectory

Le schéma ci-dessous illustre le fonctionnement de GSSAPI avec un serveur LDAP.

Figure 7-1 *Fonctionnement de GSSAPI*



Dans la figure ci-dessus, les numéros correspondent aux éléments suivants :

1. Un utilisateur eDirectory envoie une requête via un client LDAP au serveur KDC (Key Distribution Center) Kerberos concernant un ticket initial appelé TGT (Ticket Granting Ticket).

Un KDC Kerberos peut être de type MIT ou Microsoft*.

2. En réponse, le KDC envoie un TGT au client LDAP.
3. Le client LDAP renvoie le TGT au KDC et demande un ticket de service LDAP.
4. En réponse, le KDC envoie le ticket de service LDAP au client LDAP.
5. Le client LDAP établit une liaison ldap_sasl_bind avec le serveur LDAP et envoie le ticket de service LDAP.
6. Le serveur LDAP valide le ticket de service LDAP à l'aide du mécanisme GSSAPI et, en fonction du résultat, renvoie la liaison ldap_sasl_bind réussie ou échouée au client LDAP.

7.3 Configuration de 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 la clé principale et les clés maîtresses du domaine.

   iManager est généralement configuré par défaut pour une connexion à eDirectory de type SSL/TLS. Si vous souhaitez configurer la méthode de connexion Kerberos pour GSSAPI sur une arborescence autre que celle qui héberge la configuration de iManager, vous devez configurer iManager pour une connexion à eDirectory de type SSL/TLS.

   Pour plus d'informations sur la configuration de iManager avec connexion SSL/TLS à eDirectory, reportez-vous au manuel *NetIQ iManager 2.7 Administration Guide* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html) (Guide d'administration de NetIQ iManager 2.7).

   Le plug-in iManager pour SASL-GSSAPI (`kerberosPlugin.npm`) est disponible dans le cadre des deux fichiers `eDir_88_iMan26_Plugins.npm` et `eDir_88_iMan27_Plugins.npm`. Téléchargez les fichiers NPM depuis le site Web de téléchargement de Novell (http://download.novell.com).
2. Pour utiliser un ticket Kerberos pour s'authentifier auprès d'un serveur eDirectory :
   - **2a** Étendez le schéma Kerberos.
   - **2b** Créez un conteneur de domaine.
   - **2c** Extrayez une clé de principal de service ou une clé partagée du KDC.
   - **2d** Créez l'objet Principal de service LDAP.
   - **2e** Associez un nom de principal Kerberos à l'objet Utilisateur.

Pour plus d'informations sur les étapes ci-dessus, reportez-vous à la section « Configuring GSSAPI with eDirectory » (Configuration GSSAPI avec eDirectory) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

7.4 Utilisation de GSSAPI par LDAP

Une fois le mécanisme GSSAPI configuré, il est ajouté avec les autres méthodes SASL à l'attribut `supportedSASLMechanisms` dans `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 « Understanding How LDAP Works with eDirectory » (Présentation du fonctionnement de LDAP avec eDirectory) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

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
```

7.5 Terminologie courante

Le tableau suivant définit les termes couramment utilisés avec Kerberos et GSSAPI.

Tableau 7-1 *Terminologie Kerberos/GSSAPI*

Terme	Définition
KDC (Key Distribution Center)	Serveur Kerberos qui authentifie des utilisateurs et délivre des tickets.
Principal	Entité (instance service ou utilisateur) enregistrée auprès du KDC.
Domaine	Domaine ou groupe de principaux desservis par un ensemble de KDC.
ST (Service Ticket)	Enregistrement contenant des informations sur le client et le service ainsi qu'une clé de session codée avec la clé partagée du principal d'un service spécifique
TGT (Ticket Granting Ticket)	Type de ticket permettant au client d'obtenir d'autres tickets Kerberos.

8 Application de mots de passe universels respectant la casse

Dans NetIQ eDirectory 8.8, vous pouvez activer la fonctionnalité de mot de passe universel et rendre votre mot de passe sensible à la casse lorsque vous accédez au serveur eDirectory 8.8 via les clients et utilitaires suivants :

- Novell Client 4.9 et versions ultérieures ;
- Utilitaires d'administration mis à niveau vers eDirectory 8.8 ;
- NetIQ iManager 2.7 et versions ultérieures, sauf s'il s'exécute sous Windows.

Vous pouvez utiliser n'importe quelle version du SDK LDAP pour obtenir des mots de passe respectant la casse.

Le tableau suivant liste les plates-formes prenant en charge la fonction des mots de passe respectant la casse :

Fonction	Linux	Windows
Application de mots de passe universels respectant la casse	✓	✓

Ce chapitre comprend les informations suivantes :

8.1 Avantage des mots de passe respectant la casse

Les mots de passe respectant la casse augmentent la sécurité du login à l'annuaire. Par exemple, si vous avez un mot de passe aBc respectant la casse, toutes les tentatives de login avec des combinaisons telles que abc, Abc ou ABC échoueront.

Depuis eDirectory 8.8, vous pouvez définir les mots de passe comme devant respecter la casse pour tous les clients mis à niveau vers eDirectory 8.8.

En imposant l'utilisation de mots de passe respectant la casse, vous pouvez empêcher les anciens clients Novell d'accéder au serveur eDirectory 8.8. Reportez-vous à Section 8.4, « Interdiction aux anciens clients Novell d'accéder au serveur eDirectory 8.8 », page 50 pour plus d’informations.

8.2 Déploiement des mots de passe respectant la casse

Dans eDirectory 8.8 (ou version ultérieure), vous pouvez rendre les mots de passe sensibles à la casse pour tous les clients en activant la fonction du mot de passe universel qui est désactivée par défaut.

8.2.1 Conditions préalables

Par défaut, les utilitaires LDAP et autres utilitaires côté serveur utilisent d'abord le login NDS et, en cas d'échec, le login avec mot de passe simple. Pour que les mots de passe respectent la casse, vous devez d'abord vous connecter via NMAS (Novell Modular Authentication Service). Par conséquent, vous devez définir la variable d'environnement `NDSD_TRY_NMASLOGIN_FIRST` sur Vrai pour que la fonctionnalité de mot de passe respectant la casse soit disponible.

Effectuez la procédure suivante pour rendre la fonction des mots de passe respectant la casse disponible :

1. Définissez la variable d'environnement
   - Linux :

     Ajoutez à la fin les informations suivantes dans `/opt/novell/eDirectory/sbin/pre_ndsd_start`.

     ```
     NDSD_TRY_NMASLOGIN_FIRST=true
     export NDSD_TRY_NMASLOGIN_FIRST
     ```

   - Windows :

     Cliquez avec le bouton droit sur Poste de travail et sélectionnez Propriétés. Dans l'onglet Avancé, cliquez sur Variables d'environnement. Sous Variables système, ajoutez la variable et définissez la valeur sur Vrai.
2. Redémarrez le serveur eDirectory.

REMARQUE : L'utilisation de NMAS pour l'authentification augmente le temps nécessaire à la connexion.

8.2.2 Procédure pour rendre votre mot de passe sensible à la casse

1. Connectez-vous à eDirectory en utilisant le mot de passe existant.

   Dans le cas d'une nouvelle installation, le mot de passe existant est celui que vous avez défini pendant la configuration de eDirectory 8.8.

   Par exemple, votre mot de passe est “novell”.

   REMARQUE : Ce mot de passe n'est pas sensible à la casse.
2. Activer le mot de passe universel.

   Pour plus d'informations, reportez-vous à la section « Deploying Universal Password » (Déploiement de mot de passe universel) du manuel *Novell Password Management 3.3 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guide d'administration de Novell Password Management 3.3).
3. Déloguez-vous de eDirectory.
4. Connectez-vous à eDirectory en saisissant le mot de passe existant dans la casse de votre choix.

   Le mot de passe que vous venez d'entrer sera désormais sensible à la casse.

Par exemple, entrez “NoVELL”.

Votre mot de passe sera désormais “NoVELL”. Par conséquent, “novell” ou toute autre combinaison de majuscules et de minuscules autre que “NoVELL” ne sera pas valide.

Si vous migrez vers des mots de passe respectant la casse, reportez-vous à la section Section 8.3.1, « Migration vers des mots de passe respectant la casse », page 49.

Tout nouveau mot de passe que vous définissez sera sensible à la casse selon le niveau (objet ou partition) auquel vous avez activé la fonction du mot de passe universel.

8.2.3 Gestion des mots de passe respectant la casse

Vous pouvez gérer le respect de la casse de vos mots de passe en activant ou en désactivant la fonction du mot de passe universel via iManager. Pour plus d'informations, reportez-vous à la section « Deploying Universal Password » (Déploiement de mot de passe universel) du manuel *NetIQ Password Management 3.3 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guide d'administration de NetIQ Password Management 3.3).

8.3 Mise à niveau des anciens clients et utilitaires Novell

Les dernières versions des clients Novell et utilitaires NetIQ sont les suivantes :

- Novell Client 4.9 ;
- Utilitaires d'administration avec eDirectory 8.8 ;
- NetIQ iManager 2.7 et versions ultérieures

Les clients et utilitaires antérieurs aux versions susmentionnés sont d'anciens clients Novell.

Pour obtenir des mots de passe respectant la casse pour les anciens clients Novell, vous devez d'abord mettre ces derniers à niveau vers leur dernière version. Grâce à eDirectory 8.8, la migration de vos mots de passe existants vers des mots de passe respectant la casse est aisée et souple. Reportez-vous à Section 8.3.1, « Migration vers des mots de passe respectant la casse », page 49 pour plus d’informations.

Si vous ne mettez pas à niveau les anciens clients vers leur dernière version, leur utilisation de eDirectory 8.8 peut être bloquée au niveau du serveur. Reportez-vous à Section 8.4, « Interdiction aux anciens clients Novell d'accéder au serveur eDirectory 8.8 », page 50 pour plus d’informations.

8.3.1 Migration vers des mots de passe respectant la casse

La fonction du mot de passe universel étant désactivée par défaut, vos mots de passe existants ne seront pas affectés tant que vous n'activez pas cette fonction dans iManager. Pour des instructions pas à pas, reportez-vous à la section Section 8.2, « Déploiement des mots de passe respectant la casse », page 48.

L'exemple suivant explique la migration vers des mots de passe respectant la casse :

Ouverture de session 1 : le mot de passe universel est désactivé par défaut.

- Vous vous connectez en utilisant votre mot de passe existant. Supposons, par exemple, que vous utilisez le mot de passe netiq.

- Ce mot de passe n'est pas sensible à la casse. Par conséquent, netiq et NetIQ sont tous deux des mots de passe valides.
- Après vous être connecté, vous activez la fonction de mot de passe universel. Reportez-vous à la section « Deploying Universal Password » (Déploiement de mot de passe universel) du manuel *NetIQ Password Management 3.3 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guide d'administration de NetIQ Password Management 3.3).

Ouverture de session 2 : la fonction de mot de passe universel a été activée lors de la session précédente.

- Vous vous connectez en utilisant votre mot de passe existant. Supposons, par exemple, que vous tapez le mot de passe noVell.
- Lorsque la fonction du mot de passe universel est activée, ce mot de passe devient sensible à la casse. Vous devez donc vous rappeler comment vous avez entré votre mot de passe la première fois.

Session de connexion 3 et connexions suivantes.

- Si vous vous connectez en utilisant le mot de passe netIQ, il est valide.
- Si vous vous connectez en utilisant le mot de passe NetIQ (ou toute autre variante, à l'exception de noVell), il n'est pas valide.

8.4 Interdiction aux anciens clients Novell d'accéder au serveur eDirectory 8.8

Dans eDirectory 8.7.1 et 8.7.3, vous pouviez empêcher les anciens clients Novell de définir ou modifier le mot de passe NDS. Avec eDirectory 8.8, vous pouvez également les empêcher de se connecter à eDirectory 8.8 et de vérifier les mots de passe.

Pour autoriser ou interdire l'utilisation de eDirectory 8.8 aux anciens clients Novell, vous devez configurer le login aux NDS via iManager ou LDAP.

Cette section présente les informations suivantes :

8.4.1 Nécessité d'interdire aux anciens clients Novell l'accès au serveur eDirectory 8.8

Les mots de passe des anciens clients Novell ne sont pas sensibles à la casse. Par conséquent, dans eDirectory 8.8 (ou version ultérieure), si vous souhaitez imposer l'utilisation de mots de passe respectant la casse, vous devrez peut-être bloquer l'accès des anciens clients à l'annuaire.

Les versions antérieures à Novell Client 4.9 ne prenaient pas en charge la fonction du mot de passe universel. En effet, les modifications au niveau du login et du mot de passe étaient envoyées directement aux NDS plutôt qu'à NMAS. Désormais, si vous utilisez la fonction du mot de passe

universel, la modification des mots de passe via d'anciens clients peut engendrer un problème de type « password drift », ce qui signifie que le mot de passe NDS et le mot de passe universel ne sont pas synchronisés. Une solution à ce problème consiste à bloquer les modifications de mot de passe à partir des clients antérieurs à la version 4.9.

Reportez-vous à la section suivante, Gestion des configurations de login aux NDS, pour plus d'informations sur le blocage des clients existants afin qu'ils n'accèdent pas au serveur eDirectory 8.8.

8.4.2 Gestion des configurations de login aux NDS

En configurant le login aux NDS, vous pouvez autoriser ou interdire l'accès des anciens clients Novell au serveur eDirectory 8.8. Vous pouvez gérer les configurations de login aux NDS via iManager 2.6 et LDAP.

Dans eDirectory 8.8 (ou version ultérieure), vous pouvez configurer la définition et la modification des mots de passe via LDAP et iManager.

Cette section fournit les informations suivantes :

Configurations des NDS à différents niveaux

Vous pouvez configurer le login aux NDS à un des niveaux suivants, voire tous :

- Niveau partition ;
- Niveau objet.

Si vous ne spécifiez pas le niveau, la configuration de login aux NDS est activée à tous les niveaux.

La configuration au niveau de l'objet est toujours prioritaire sur celle au niveau de la partition, comme décrit dans le tableau suivant :

Tableau 8-1 *Configuration des NDS*

Configuration au niveau de l'objet	Configuration au niveau de la partition	Configuration
Non spécifiée	Activé	Activé
Activé	Non spécifiée	Activé
Non spécifiée	Désactivé	Désactivé
Désactivé	Non spécifiée	Désactivé
Activé	Activé	Activé
Activé	Désactivé	Activé
Désactivé	Activé	Désactivé
Désactivé	Désactivé	Désactivé

À tous les niveaux (objet et partition), vous pouvez configurer le login aux NDS pour les opérations suivantes :

- Login à l'annuaire à l'aide d'un mot de passe NDS ou vérification du mot de passe NDS ;
- Définition d'un nouveau mot de passe et modification du mot de passe existant.

Login à l'annuaire ou vérification du mot de passe NDS

Connexion/vérification du mot de passe NDS signifie :

- Login à l'annuaire en utilisant un mot de passe NDS ;
- Vérification du mot de passe existant dans l'annuaire.

L'option de connexion/vérification du mot de passe NDS est activée par défaut. Si vous désactivez cette option, vous ne pourrez plus vous connecter à la dernière version d'eDirectory ni vérifier les mots de passe. Vous pouvez activer ou désactiver l'option de connexion/vérification du mot de passe NDS au niveau de la partition et de l'objet. Si elle est désactivée, vous ne pourrez pas définir ni modifier de mot de passe NDS.

Vous pouvez configurer l'option de connexion/vérification du mot de passe NDS via iManager et LDAP. Pour plus d'informations, reportez-vous aux sections « Gestion des configurations des NDS via iManager » page 52 et « Gestion des configurations des NDS via LDAP » page 53.

Définition d'un nouveau mot de passe ou modification du mot de passe NDS

Définition/modification d'un mot de passe NDS signifie :

- Définition d'un nouveau mot de passe pour un objet ;
- Modification du mot de passe existant pour un objet.

L'option Définition/modification du mot de passe NDS est activée par défaut. Si vous désactivez la clé de définition/modification, vous ne pourrez plus définir un nouveau mot de passe ou modifier le mot de passe existant dans eDirectory. Vous pouvez activer ou désactiver l'option Définition/modification du mot de passe NDS au niveau de la partition et de l'objet. Si l'option de connexion/vérification est désactivée, vous ne pourrez pas définir/modifier de mot de passe.

Précédemment, vous pouviez définir/modifier les mots de passe NDS via LDAP uniquement. Désormais, vous pouvez également le faire via iManager. Pour plus d'informations, reportez-vous aux sections « Gestion des configurations des NDS via iManager » page 52 et « Gestion des configurations des NDS via LDAP » page 53.

Gestion des configurations des NDS via iManager

Cette section présente les informations suivantes :

Vous pouvez activer la cléde login/vérification ou la cléde définition/modification dans la configuration de login aux NDS.

Activation/désactivation de la configuration des NDS pour une partition

Pour activer la connexion à NDS pour les clients utilisant une version antérieure à eDirectory 8.8 :

1. Dans iManager, cliquez sur le bouton *Rôles et tâches*  .
2. Sélectionnez *NMAS* > *Application du mot de passe universel*.
3. Dans le plug-in Application du mot de passe universel, sélectionnez *Configuration des NDS pour une partition*.
4. Suivez les instructions de l'Assistant Configuration des NDS pour une partition afin de configurer la gestion de mot de passe et de login au niveau d'une partition.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

Activation/désactivation de la configuration des NDS pour un objet

Pour activer la connexion à NDS pour les clients utilisant une version antérieure à eDirectory 8.8 :

1. Dans iManager, cliquez sur le bouton *Rôles et tâches*  .
2. Sélectionnez *NMAS* > *Application du mot de passe universel*.
3. Dans l'Assistant, sélectionnez *Configuration des NDS pour un objet*.
4. Suivez les instructions de l'Assistant Configuration des NDS pour un objet afin de configurer la gestion de mot de passe et de login au niveau d'un objet.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

Gestion des configurations des NDS via LDAP

IMPORTANT : il est vivement recommandé d'utiliser iManager plutôt que LDAP pour gérer les configurations des NDS.

Vous pouvez gérer les configurations des NDS via LDAP à l'aide d'un attribut eDirectory sur un conteneur racine de partition ou d'objet. Les attributs font partie du schéma dans eDirectory 8.7.1 ou versions ultérieures, mais ne sont pas pris en charge dans eDirectory 8.7 ou versions antérieures.

La méthode utilisée par les anciens clients pour définir les configurations de la connexion NDS est appelée « gestion de la connexion NDAP », et celle utilisée pour les configurations de mot de passe NDS, « gestion des mots de passe NDAP ».

Cette section comprend les informations suivantes :

Activation/désactivation de la configuration des NDS pour une partition

Gestion de la connexion/vérification du mot de passe

Utilisez l'attribut `ndapPartitionLoginMgmt` pour activer ou désactiver la gestion de connexion NDS et de vérification du mot de passe pour une partition.

Valeur de l'attribut ndapPartitionLoginMgmt	Description
Absente ou non spécifiée	La gestion de la connexion NDAP est activée.
0	La gestion de la connexion NDAP est désactivée.
1	La gestion de la connexion NDAP est activée.

Définition et modification du mot de passe NDS

Utilisez l'attribut `ndapPartitionPasswordMgmt` pour activer ou désactiver la définition et la modification d'un mot de passe NDS pour une partition.

Valeur de l'attribut ndapPartitionPasswordMgmt	Description
Absente ou non spécifiée	La gestion de mot de passe NDAP est activée.
0	La gestion de mot de passe NDAP est désactivée.
1	La gestion de mot de passe NDAP est activée.

Activation/désactivation des configurations des NDS pour un objet

Login et vérification du mot de passe NDS

Utilisez l'attribut `ndapLoginMgmt` pour activer ou désactiver la gestion de connexion NDS et de vérification d'un objet.

Valeur de l'attribut ndapLoginMgmt	Description
Absente ou non spécifiée	La gestion de la connexion NDAP dépend de la configuration au niveau de la partition.
0	La gestion de la partition NDAP est désactivée si elle l'est également au niveau de la partition.
1	La gestion de la connexion NDAP est activée quel que soit le paramètrage défini au niveau de la partition.

Définition et modification du mot de passe NDS

Utilisez l'attribut `ndapPasswordMgmt` pour activer ou désactiver la définition et la modification d'un mot de passe NDS pour un objet.

Valeur de l'attribut ndapPasswordMgmt	Description
Absente ou non spécifiée	La gestion de mot de passe NDAP dépend de la configuration au niveau de la partition.
0	La gestion de mot de passe NDAP est désactivée si elle l'est également au niveau de la partition.
1	La gestion de mot de passe NDAP est activée quel que soit le paramètre de configuration au niveau de la partition.

REMARQUE : Pour plus d'informations sur la création et la gestion des stratégies de synchronisation de priorité, reportez-vous aux sections « Using LDAP Tools on Linux » (Utilisation des outils LDAP sur Linux) et « NetIQ Import Conversion Export Utility » (Utilitaire NetIQ Import Conversion Export) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

8.4.3 Opérations de partition

Lorsque vous divisez une partition, la partition enfant n'hérite pas des configurations des NDS. Lorsque vous fusionnez des partitions, les configurations des NDS du parent sont conservées par la partition résultante.

8.4.4 Application de mots de passe respectant la casse dans une arborescence mixte

Si une arborescence contient un serveur eDirectory 8.8 (ou version ultérieure) et un serveur eDirectory 8.7 (ou version antérieure), et que les deux serveurs partagent une partition, la désactivation de la configuration de login aux NDS sur cette partition entraînera des résultats non fiables. Le serveur 8.8 appliquera le paramètre, empêchant ainsi les clients d'accéder à l'annuaire. Quant au serveur 8.7, il n'appliquera pas le paramètre et vous pourrez donc accéder à l'annuaire via ce serveur.

8.5 Pour plus d'informations

Pour plus d'informations sur les mots de passe respectant la casse, consultez les références suivantes :

- Aide en ligne de iManager
- Reportez-vous à la section « Deploying Universal Password » (Déploiement de mot de passe universel) du manuel *NetIQ Password Management 3.3 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html) (Guide d'administration de NetIQ Password Management 3.3).

9 Prise en charge de la stratégie de mot de passe de Microsoft Windows Server 2008

Dans les versions précédentes de eDirectory, les utilisateurs pouvaient utiliser la stratégie de complexité de Microsoft par défaut ou la syntaxe Novell héritée. NetIQ eDirectory 8.8 SP8 prend désormais en charge l'utilisation de stratégies de mot de passe qui sont conformes aux exigences en matière de complexité des stratégies de mot de passe de Microsoft Windows Server 2008 et qui diffèrent de la configuration requise dans la stratégie de complexité Microsoft précédente. Vous pouvez utiliser iManager pour créer une stratégie à l'aide de la nouvelle option de syntaxe de stratégie de mot de passe de Microsoft Server 2008 et configurer cette stratégie en fonction de votre environnement.

Ce chapitre comprend les informations suivantes :

9.1 Création de stratégies de mot de passe Windows Server 2008

Vous pouvez utiliser iManager pour créer des stratégies de mot de passe qui utilisent la configuration requise en matière de complexité de Microsoft Windows Server 2008 et assigner des utilisateurs de votre environnement eDirectory à la nouvelle stratégie. Pour obtenir des instructions détaillées sur la création de stratégies de mot de passe, reportez-vous au manuel *NetIQ Password Management 3.3.2 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html) (Guide d'administration de NetIQ Password Management 3.3.2).

REMARQUE

- Avant de créer une nouvelle stratégie de mot de passe à l'aide de la syntaxe des stratégies de mot de passe de Microsoft Server 2008, veillez à installer la dernière version du plug-in Novell iManager Password Management. Pour plus d'informations sur l'installation des modules de plug-in iManager, consultez le manuel *NetIQ iManager 2.7 Administration Guide* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html) (Guide d'administration de NetIQ iManager 2.7).
- Vous devez également vous assurer que les règles de mot de passe universel et de mot de passe avancé sont activées pour la stratégie que vous souhaitez créer ou configurer.

9.2 Gestion des stratégies de mot de passe de Windows Server 2008

Vous pouvez gérer les stratégies qui utilisent les exigences de complexité de stratégie de mot de passe Windows Server 2008 à l'aide de iManager. Pour plus d'informations, reportez-vous à la section « Managing Passwords by Using Password Policies » (Gestion des mots de passe à l'aide des stratégies de mot de passe) du manuel *Novell Password Management 3.3.2 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/ampxjj0.html) (Guide d'administration de Novell Password Management 3.3.2).

9.3 Pour plus d'informations

Reportez-vous aux détails ci-dessous pour plus d'informations sur les stratégies de mot de passe de eDirectory :

- Aide en ligne de iManager
- *Novell Password Management 3.3.2 Administration Guide* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html) (Guide d'administration de Novell Password Management 3.3.2)
- *Novell Modular Authentication Services Administration Guide* (http://www.netiq.com/documentation/nmas33/admin/data/a20gkue.html) (Guide d'administration de Novell Modular Authentication Services)

10 Synchronisation de priorité

Nouvelle fonction de NetIQ eDirectory 8.8, la synchronisation de priorité vient compléter le processus de synchronisation actuel dans eDirectory. Grâce à la synchronisation de priorité, vous pouvez synchroniser immédiatement les données critiques modifiées, telles que les mots de passe.

Vous pouvez synchroniser vos données critiques à l'aide de la synchronisation de priorité si vous ne pouvez pas attendre la synchronisation normale. La synchronisation de priorité est plus rapide que la synchronisation normale. Elle est prise en charge uniquement entre plusieurs serveurs eDirectory 8.8 (ou versions ultérieures) hébergeant la même partition.

Le tableau suivant liste les plates-formes prenant en charge la synchronisation de priorité :

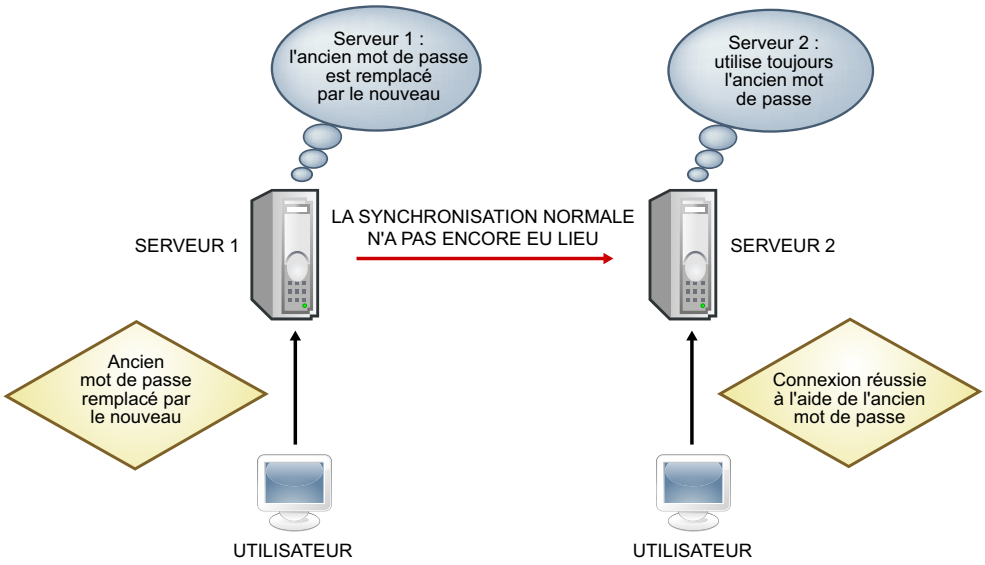
Fonction	Linux	Windows
Synchronisation de priorité	✓	✓

Ce chapitre comprend les informations suivantes :

10.1 Avantage de la synchronisation de priorité

La synchronisation normale peut prendre un certain temps, pendant lequel les données modifiées ne sont pas disponibles sur d'autres serveurs. Supposons, par exemple, que votre configuration contienne différentes applications qui communiquent avec l'annuaire. Vous modifiez votre mot de passe sur le Serveur1. Avec la synchronisation normale, un certain temps s'écoule avant que ce changement ne soit synchronisé avec le Serveur2. Par conséquent, un utilisateur pourra toujours s'authentifier à l'annuaire via une application dialoguant avec le Serveur2, à l'aide de l'ancien mot de passe.

Figure 10-1 *Avantage de la synchronisation de priorité*



Dans les déploiements à grande échelle, lorsque les données critiques d'un objet sont modifiées, les changements doivent être synchronisés immédiatement. Le processus de synchronisation de priorité résout ce problème.

10.2 Utilisation de la synchronisation de priorité

Pour synchroniser des modifications de données via la synchronisation de priorité, vous devez procéder comme suit :

1. Activez la synchronisation de priorité, configurez le nombre de threads et la taille de la file d'attente de la synchronisation de priorité via iMonitor.
2. Définissez les règles de synchronisation de priorité en identifiant les attributs critiques via iManager.
3. Appliquez les règles de synchronisation de priorité aux partitions via iManager.

10.3 Pour plus d'informations

Pour plus d'informations sur la synchronisation de priorité, consultez les références suivantes :

- *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8)
- Aide en ligne de iManager et iMonitor

11 Codage de données

NetIQ eDirectory 8.8 (ou versions ultérieures) permet de coder certaines données lorsqu'elles sont stockées sur le disque et qu'elles sont transmises entre plusieurs serveurs eDirectory 8.8. Vous bénéficiez ainsi d'une plus grande sécurité pour les données confidentielles.

Le tableau suivant liste les plates-formes prenant en charge le codage des données :

Fonction	Linux	Windows
Attributs codés	✓	✓
Réplication codée	✓	✓

Ce chapitre comprend les informations suivantes :

11.1 Codage d'attributs

eDirectory 8.8 vous permet de coder des données sensibles stockées sur le disque. Le codage d'attributs est une fonctionnalité propre au serveur.

Vous ne pouvez accéder à des attributs codés que par le biais de canaux sécurisés à moins que vous ne choisissiez de prévoir un accès par le biais de canaux en texte clair également. Reportez-vous à Section 11.1.3, « Accès aux attributs codés », page 62 pour plus d'informations.

Cette section présente les informations suivantes :

La fonction du codage d'attributs n'est prise en charge que sur les serveurs eDirectory 8.8 et version ultérieure.

11.1.1 Besoin d'attributs codés

Avant eDirectory 8.8, les données étaient stockées sur le disque en texte clair. Il était alors nécessaire de protéger les données et de n'en autoriser l'accès que par le biais de canaux sécurisés.

Vous pouvez utiliser cette fonction lorsque vous souhaitez protéger des données confidentielles, par exemple les numéros de carte de crédit des clients d'une banque.

11.1.2 Procédure pour le codage des attributs

Pour coder des attributs, vous pouvez créer et définir des règles d'attributs codés pour ensuite les appliquer aux serveurs. Vous pouvez créer, définir, appliquer et gérer des règles d'attributs codés via iManager et LDAP.

1. Créez et définissez une règle d'attributs codés :
   - **1a** Sélectionnez les attributs à coder.
   - **1b** Définissez le modèle de codage des attributs.
2. Appliquez la règle des attributs codés à un serveur.

11.1.3 Accès aux attributs codés

Vous ne pouvez accéder aux attributs codés que par le biais de canaux sécurisés, tels que le port SSL LDAP ou le port HTTP sécurisé. Vous pouvez autoriser l'accès aux attributs codés par le biais de canaux en texte clair à l'aide du plug-in iManager. Pour plus d'informations, reportez-vous au manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

11.2 Codage de la réplication

La réplication codée consiste à coder des données transmises entre plusieurs serveurs eDirectory 8.8.

La réplication codée complète la synchronisation normale dans eDirectory.

Cette section présente les informations suivantes :

11.2.1 Avantage de la réplication codée

Avant eDirectory 8.8, les données étaient transmises sur le réseau pendant la réplication en texte clair. Il convenait alors de protéger les données confidentielles sur le réseau en les codant, surtout si les répliques étaient séparées géographiquement et connectées via Internet.

Cette fonction peut être utilisée dans les scénarios suivants :

- Si les serveurs d'annuaire sont répartis sur différents sites géographiques via WAN et Internet et qu'il est nécessaire de coder les données sensibles sur le réseau.
- Si vous ne souhaitez protéger que certaines partitions de votre arborescence, vous pouvez sélectionner les partitions contenant les données sensibles à coder pour la réplication.
- Si vous avez besoin d'une réplication codée entre certaines répliques d'une partition qui contiennent des données sensibles.
- Si vous pensez que le réseau de votre installation est hostile, vous pouvez protéger les données sensibles pendant la réplication.

11.2.2 Activation de la réplication codée

Vous pouvez activer la réplication codée à l'aide de iManager. Vous pouvez l'activer au niveau de la partition et de la réplique.

IMPORTANT : Avant d'activer la réplication codée, assurez-vous que les serveurs source et cible disposent des certificats par défaut. Si vous avez modifié les certificats, par exemple, si vous les avez renommés, la réplication codée échouera.

11.3 Pour plus d'informations

Pour plus d'informations sur le codage de données dans eDirectory, consultez les références suivantes :

- *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8)
- Aide en ligne de iManager et iMonitor

12 Performances de chargement par lots

NetIQ eDirectory 8.8 intègre des améliorations qui accroissent les performances du chargement en bloc.

Pour plus d'informations sur l'augmentation des performances du chargement en bloc, reportez-vous aux sections suivantes du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8) :

- « Paramètres du cache eDirectory »
- « Définition de la taille de transaction LBURP »
- « Augmentation du nombre de requêtes asynchrones dans ICE »
- « Augmentation du nombre de threads d'écriture LDAP »
- « Désactivation de la validation de schéma dans ICE »
- « Désactivation des modèles ACL »
- « Processus de liaison en amont »
- « Activation/désactivation du cache en ligne »
- « Augmentation du timeout de LBURP »
- « Utilitaire de chargement en bloc hors connexion »

13 Plug-ins ICE dans iManager

Dans les versions antérieures à NetIQ eDirectory 8.8, certaines des options de ligne de commande de l'utilitaire ICE (importation, conversion et exportation) de Novell n'avaient pas d'options correspondantes dans le plug-in iManager.

Le tableau suivant liste les plates-formes prenant en charge cette fonction :

Fonction	Linux	Windows
Améliorations ICE dans iManager	✓	✓

L'Assistant ICE dans iManager 2.7 avec eDirectory 8.8 intègre les fonctions suivantes :

- Ajout de schéma manquant
- Comparaison de schémas
- Génération d'un fichier de commande

13.1 Ajout d'un schéma manquant

Dans eDirectory 8.8, iManager intègre des options permettant d'ajouter un schéma manquant au schéma d'un serveur. Ce processus implique une comparaison d'une source et d'une cible. Si le schéma source contient un schéma supplémentaire, ce dernier est ajouté au schéma cible. La source peut être un fichier ou un serveur LDAP, et la destination doit être un serveur LDAP.

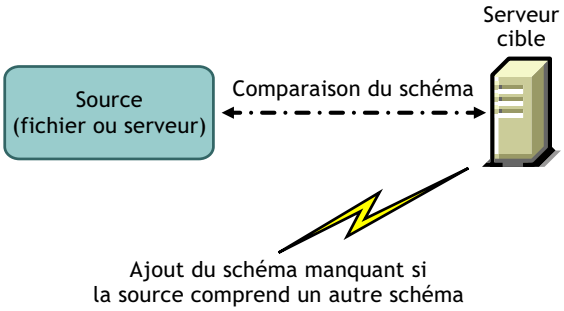
L'Assistant ICE dans iManager permet d'ajouter le schéma manquant à l'aide des options suivantes :

- Ajouter un schéma depuis un fichier
- Ajouter un schéma depuis un serveur

13.1.1 Ajouter un schéma depuis un fichier

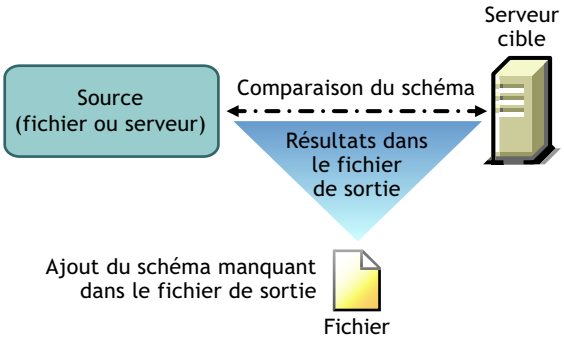
ICE peut comparer le schéma dans la source et la cible. La source est un fichier ou serveur LDAP ; la cible, un serveur LDAP. Le fichier du schéma source peut être au format LDIF ou SCH.

Figure 13-1 *Comparaison et ajout du schéma depuis un fichier*



Si vous souhaitez simplement comparer le schéma sans ajouter de schéma supplémentaire au serveur de destination, sélectionnez l'option *Ne pas ajouter mais comparer le schéma*. 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.

Figure 13-2 *Comparaison du schéma et consignation des résultats dans un fichier de sortie*



Pour plus d'informations, reportez-vous à la section « NetIQ eDirectory Management Utilities » (Utilitaires de gestion de NetIQ eDirectory) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

13.1.2 Ajouter un schéma depuis un serveur

La source et la cible sont des serveurs LDAP.

Si vous souhaitez simplement comparer le schéma sans ajouter de schéma supplémentaire au serveur de destination, sélectionnez l'option *Ne pas ajouter mais comparer le schéma*. 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.

Pour plus d'informations, reportez-vous à la section « NetIQ eDirectory Management Utilities » (Utilitaires de gestion de NetIQ eDirectory) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

13.2 Comparaison du schéma

iManager permet de comparer le schéma entre une source et une cible. La source peut être un fichier ou un serveur, et la destination doit être un fichier LDIF.

iManager compare le schéma entre une source et une cible, puis consigne les résultats dans un fichier de sortie.

L'Assistant ICE dans iManager permet de comparer le schéma à l'aide des options suivantes :

- Comparer les fichiers de schéma
- Comparer un schéma entre serveur et fichier

13.2.1 Comparer les fichiers de schéma

L'option *Comparer les fichiers de schéma* compare le schéma d'un fichier source à celui d'un fichier de destination, puis consigne le résultat dans un fichier de sortie. Pour ajouter le schéma manquant au fichier cible, appliquez-lui les enregistrements du fichier de sortie.

Pour plus d'informations, reportez-vous à la section « NetIQ eDirectory Management Utilities » (Utilitaires de gestion de NetIQ eDirectory) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

13.2.2 Comparer un schéma entre serveur et fichier

L'option *Comparer un schéma entre serveur et fichier* compare le schéma d'un serveur source et celui d'un fichier de destination, puis consigne le résultat dans un fichier de sortie. Pour ajouter le schéma manquant au fichier cible, appliquez-lui les enregistrements du fichier de sortie.

Pour plus d'informations, reportez-vous à la section « NetIQ eDirectory Management Utilities » (Utilitaires de gestion de NetIQ eDirectory) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

13.3 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.

Pour plus d'informations, reportez-vous à la section « NetIQ eDirectory Management Utilities » (Utilitaires de gestion de NetIQ eDirectory) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

13.4 Pour plus d'informations

Pour plus d'informations sur cette fonction, consultez les références suivantes :

- *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8)
- Aide en ligne de iMonitor

14 Sauvegarde LDAP

Nouvelle fonction de NetIQ eDirectory 8.8, la sauvegarde LDAP permet de sauvegarder les attributs et leurs valeurs, un objet à la fois.

Le tableau suivant liste les plates-formes prenant en charge cette fonction :

Fonction	Linux	Windows
Sauvegarde LDAP	✓	✓

Cette fonction permet d'effectuer une sauvegarde incrémentielle dans laquelle l'objet n'est sauvegardé que s'il est modifié.

Elle comprend une série d'interfaces pour la sauvegarde et la restauration d'objets eDirectory exposés via LDAP Libraries for C, via des opérations étendues LDAP.

Pour plus d'informations sur le SDK LDAP Libraries for C, reportez-vous à la documentation concernant LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

Pour savoir comment effectuer la sauvegarde et la restauration d'objets eDirectory via LDAP, consultez l'exemple de code backup.c (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html).

14.1 Avantage de la sauvegarde LDAP

La sauvegarde LDAP tente de résoudre les problèmes liés à la sauvegarde et restauration actuelles.

Les problèmes résolus par cette fonction sont les suivants :

- Intègre une interface cohérente permettant aux développeurs ou aux applications de sauvegarde tierces de sauvegarder eDirectory sur toutes les plates-formes prises en charge.
- Permet de sauvegarder les objets de manière incrémentielle.

14.2 Pour plus d'informations

Pour plus d'informations sur cette fonction, consultez les références suivantes :

- LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html)
- Exemple de code : backup.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html)

15 Liste LDAP d'obtention des privilèges efficaces

L'API Liste LDAP d'obtention des privilèges efficaces a été intégrée dans NetIQ eDirectory 8.8 SP6.

Le tableau suivant liste les plates-formes prenant en charge cette fonction :

Fonction	Linux	Windows
Liste LDAP d'obtention des privilèges efficaces	✓	✓

Cette fonctionnalité permet d'obtenir les privilèges efficaces d'un DN d'objet sur un DN cible et pour un jeu d'attributs. L'interface permet d'obtenir la liste des privilèges par l'intermédiaire de LDAP Libraries for C via les opérations étendues LDAP.

Pour plus d'informations sur le SDK LDAP Libraries for C, reportez-vous à la documentation concernant LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

15.1 Besoin de l'interface Liste LDAP d'obtention des privilèges efficaces

L'interface Liste LDAP d'obtention des privilèges efficaces essaie de résoudre les problèmes liés à l'API d'obtention des privilèges efficaces.

Les problèmes résolus par cette fonction sont les suivants :

- Une seule requête auprès de l'Annuaire permet d'obtenir les droits effectifs pour plusieurs attributs.
- Réduit le temps d'aller-retour avec l'Annuaire pour l'obtention des droits effectifs pour plusieurs attributs.
- Identifie les défaillances dans les entrées de la requête ou dans l'Annuaire.

15.2 Pour plus d'informations

Pour plus d'informations sur cette fonction, consultez les références suivantes :

- LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html).
- Exemple de code : getpriv.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html).

16 Gestion de la consignation des erreurs dans eDirectory 8.8

De nombreux clients ont signalé que la consignation des erreurs dans NetIQ eDirectory ne permettait pas vraiment d'identifier ni de résoudre les problèmes courants. La consignation des erreurs démarre automatiquement pendant l'installation de eDirectory.

Ce chapitre comprend les sections suivantes :

16.1 Niveaux de gravité des messages

Tous les messages sont associés à un niveau de gravité qui permet de déterminer leur caractère critique. Par ordre décroissant de gravité, les niveaux sont les suivants :

16.1.1 Fatal

Un message fatal indique un problème important, comme la perte de données ou de fonctionnalité.

Exemples :

- Si le serveur eDirectory ne parvient pas à charger des modules système comme NCPEngine et DSLoader pendant le chargement de modules, une erreur fatale est signalée et consignée.
- Si le serveur eDirectory ne parvient pas à établir une connexion sur le port sécurisé 636, une erreur fatale est signalée et consignée.

16.1.2 Avertissement

Message qui n'est pas nécessairement grave, mais qui peut engendrer un problème ultérieurement.

Exemples :

- Échecs de connexion entre deux serveurs quelconques de l'arborescence, engendrant l'ajout d'un serveur dans un cache d'adresses erronées. Le serveur peut quitter cet état spécifique après réinitialisation du cache d'adresses erronées.
- Si l'application client LDAP établit une liaison et met fin à la connexion sans annuler la liaison, le serveur LDAP consigne un avertissement avec le message correspondant.
- Si le serveur eDirectory a utilisé tous les descripteurs de fichier et a atteint la limite Seuil, il ne peut pas traiter les requêtes entrantes ni y répondre, ce qui entraîne un échec de l'application.

16.1.3 Erreur

Message qui peut être dû à une opération non valide, mais qui ne cause aucun problème.

Exemples :

- Lorsqu'une application client tente d'ajouter un objet pour lequel les attributs ne sont pas définis dans le schéma, le serveur eDirectory signale l'erreur ERR_NO_SUCH_ATTRIBUTE.
- Lorsqu'un utilisateur tente de se connecter avec un mot de passe non valide, le serveur eDirectory renvoie l'erreur ERR_FAILED_AUTHENTICATION.

16.1.4 Informations

Message qui décrit l'aboutissement d'une opération ou d'un événement dans le serveur eDirectory.

Exemples :

- Lorsque le chargement/déchargement d'un module aboutit, il peut s'avérer approprié de consigner un message d'information concernant l'opération.
- Si la configuration du cache de base de données est modifiée, un message d'information devrait être consigné lors de la réussite de l'enregistrement de cette configuration.

16.1.5 Débogage

Message contenant des informations qui aideront les développeurs à déboguer un programme.

Exemples :

Lors d'une recherche de groupe dynamique, le message affiche tous les membres de ce groupe avec des informations sur l'ID d'entrée, l'ID de partition et le DN des membres. Ces informations contribuent à déterminer si tous les membres sont renvoyés au niveau eDirectory.

16.2 Configuration de la consignation des erreurs

16.2.1 Linux

Afin de configurer les paramètres de consignation des erreurs pour les messages côté serveur, vous pouvez utiliser les paramètres `n4u.server.log-levels` et `n4u.server.log-file` du fichier de configuration `/etc/opt/novell/eDirectory/conf/nds.conf`.

Définition du niveau de gravité

Les niveaux de gravité disponibles sont `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` et `LogDbg` (par ordre décroissant de gravité). Pour plus d'informations sur les niveaux de gravité, reportez-vous à la section Section 16.1, « Niveaux de gravité des messages », page 75.

Le niveau de gravité par défaut est `LogFatal`. Dès lors, seuls les messages dont le niveau de gravité est fatal seront consignés.

Pour définir le niveau de gravité, utilisez le paramètre `n4u.server.log-levels` dans le fichier `nds.conf` comme suit :

```
n4u.server.log-levels=niveau_gravité
```

Par exemple :

- Pour définir la gravité sur le niveau `LogInfo` et les niveaux supérieurs, entrez la commande suivante :

  ```
  n4u.server.log-levels=LogInfo
  ```

  Avec cette configuration, les messages de niveaux de gravité `LogInfo` et supérieurs (c'est-à-dire `LogFatal`, `LogWarn` et `LogErr`) sont consignés dans le fichier journal.
- Pour définir la gravité sur le niveau `LogWarn` et les niveaux supérieurs, entrez la commande suivante :

  ```
  n4u.server.log-levels=LogWarn
  ```

  Avec cette configuration, les messages de niveaux de gravité `LogWarn` et supérieurs (`LogFatal`) sont consignés dans le fichier journal.

Indication du nom du fichier journal

Pour spécifier l'emplacement du fichier journal où les messages sont consignés, utilisez le paramètre `n4u.server.log-file` dans le fichier `nds.conf`. Par défaut, les messages sont consignés dans le fichier `ndsd.log`.

Par exemple, pour consigner les messages dans le fichier `/tmp/edir.log`, entrez la commande suivante :

```
n4u.server.log-file=/tmp/edir.log
```

Pour consigner les messages dans le journal système, utilisez le paramètre `n4u.server.log-file` comme suit :

```
n4u.server.log-file=syslog
```

16.2.2 Windows

- « Définition du niveau de gravité » page 78
- « Indication du nom du fichier journal et du chemin » page 78
- « Indication de la taille du fichier journal » page 78

Définition du niveau de gravité

Les niveaux de gravité disponibles sont `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` et `LogDbg` (par ordre décroissant de gravité). Pour plus d'informations sur les niveaux de gravité, reportez-vous à la section Section 16.1, « Niveaux de gravité des messages », page 75.

Pour définir le niveau de gravité, procédez comme suit :

1. Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration* > *NetIQ eDirectory Services*
2. Dans l'onglet *Services*, sélectionnez *dhlog.dlm*.
3. Entrez le niveau de consignation dans la zone *Paramètres de démarrage*.

   Par exemple, pour définir la consignation sur le niveau `LogErr` et les niveaux supérieurs, entrez la commande suivante :

   ```
   LogLevels=LogErr
   ```
4. Cliquez sur *Configurer*
5. Dans l'onglet *Configuration ACS*, cliquez sur le signe plus de *DHostLogger*.

   Le paramètre `LogLevel` est actualisé avec la valeur configurée.

Indication du nom du fichier journal et du chemin

1. Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration* > *NetIQ eDirectory Services*
2. Dans l'onglet *Services*, sélectionnez *dhlog.dlm*.
3. Entrez le chemin du fichier journal dans la zone *Paramètres de démarrage* comme suit :

   ```
   LogFile=file_path
   ```

   Par exemple, pour définir le chemin du fichier journal sur `/tmp/Err.log`, entrez la commande suivante dans la zone Paramètres de démarrage :

   ```
   LogFile=/tmp/Err.log
   ```
4. Cliquez sur *Configurer*
5. Dans l'onglet *Configuration ACS*, cliquez sur le signe plus de *DHostLogger*.

   Le paramètre `LogFile` est actualisé avec la valeur configurée.

Indication de la taille du fichier journal

1. Cliquez sur *Démarrer* > *Paramètres* > *Panneau de configuration* > *NetIQ eDirectory Services*
2. Dans l'onglet *Services*, sélectionnez *dhlog.dlm*.
3. Entrez le chemin du fichier journal dans la zone *Paramètres de démarrage* comme suit :

   ```
   LogSize=size
   ```

   La taille du fichier par défaut est de 1 Mo.
4. Cliquez sur *Configurer*
5. Dans l'onglet *Configuration ACS*, cliquez sur le signe plus de *DHostLogger*.

   Le paramètre `LogSize` est actualisé avec la valeur configurée.

16.3 Messages DSTrace

Vous pouvez filtrer les messages de trace en fonction de leur ID de thread, de leur ID de connexion et de leur gravité.

Après avoir spécifié un filtre pour les messages, seuls les messages qui lui correspondent sont affichés à l'écran. Tous les autres messages pour les balises activées sont consignés dans le fichier `ndstrace.log` s'il est défini sur ON.

Vous ne pouvez appliquer qu'un seul filtre à la fois. Il doit être spécifié pour chaque session de DSTrace.

Par défaut, le niveau de gravité est défini sur INFO, ce qui signifie que tous les messages de niveau supérieur à INFO sont affichés. Pour afficher le niveau de gravité, activez la balise `svty`.

Pour filtrer les messages de trace, vous pouvez également utiliser iMonitor. Pour plus d'informations, reportez-vous à la Section 16.4, « Filtrage des messages de iMonitor », page 81.

16.3.1 Linux

Pour filtrer les messages de trace, procédez comme suit :

1. Activez le filtrage à l'aide de la commande suivante :

   ```
   ndstrace tag filter_value
   ```

   Pour désactiver le filtrage, entrez la commande suivante :

   ```
   ndstrace tag
   ```

   Exemples d'activation du filtrage :

   - Pour activer le filtre pour l'ID de thread 35, entrez la commande suivante :

     ```
     ndstrace thrd 35
     ```

   - Pour activer le filtre pour le niveau de gravité FATAL, entrez la commande suivante :

     ```
     ndstrace svty fatal
     ```

     Les niveaux de gravité sont `FATAL`, `WARN`, `ERR`, `INFO` et `DEBUG`.

   - Pour activer le filtre pour l'ID de connexion 21, entrez la commande suivante :

     ```
     ndstrace conn 21
     ```

   Exemples de désactivation du filtrage :

   - Pour désactiver le filtre basé sur l'ID de thread, entrez la commande suivante :

     ```
     ndstrace thrd
     ```

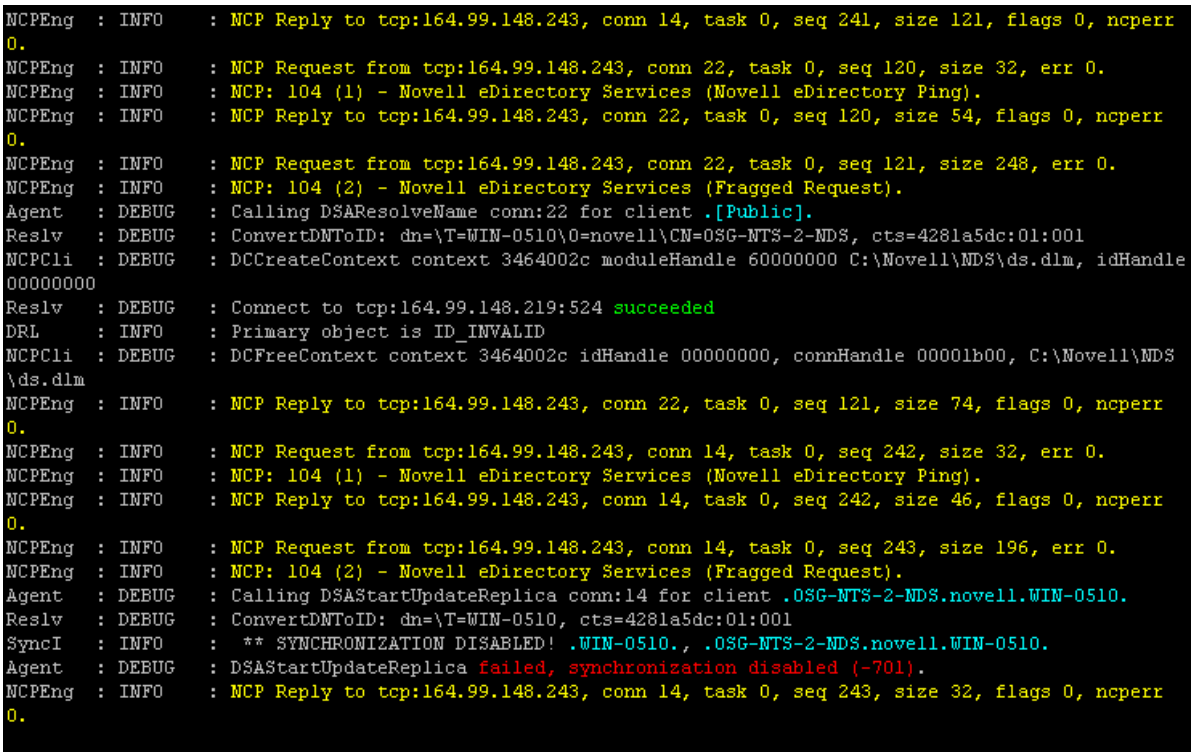
   - Pour désactiver le filtre basé sur l'ID de connexion, entrez la commande suivante :

     ```
     ndstrace conn
     ```

   - Pour désactiver le filtre basé sur la gravité, entrez la commande suivante :

     ```
     ndstrace svty
     ```

Figure 16-1 *Exemple d'écran des messages de trace avec filtres*



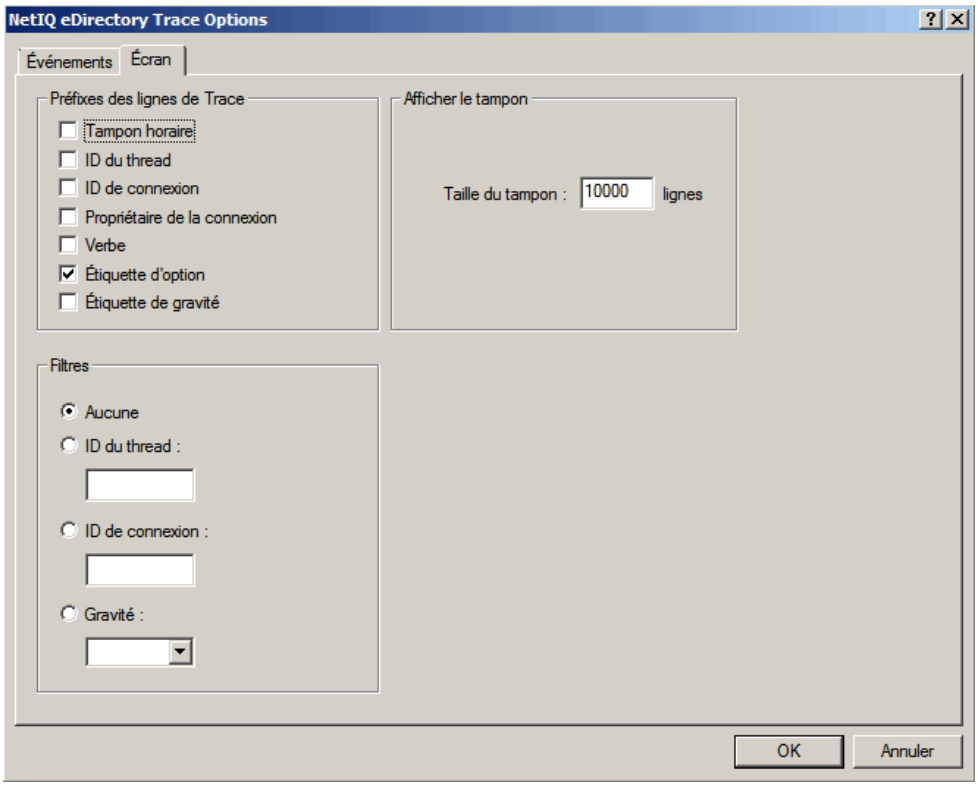
16.3.2 Windows

Pour filtrer les messages de trace, procédez comme suit :

1. Sélectionnez *Démarrer-> Panneau de configuration -> Services eDirectory*.
2. Dans l'onglet *Services*, sélectionnez *dstrace.dlm*.
3. Cliquez sur *Éditer* > *Options* dans la fenêtre de Trace.

   La boîte de dialogue Options de DS Trace de NetIQ eDirectory apparaît.

Figure 16-2 *Écran des options de trace sous Windows*



4 Cliquez sur l'onglet *Écran*.

5 Sélectionnez l'option de filtrage dans le groupe *Filtres* et saisissez la valeur du filtre.

Vous pouvez filtrer les messages en fonction des éléments suivants :

- ID du thread
- ID de connexion
- Gravité

Avant de sélectionner l'un des filtres, assurez-vous qu'il est activé sous *Préfixes des lignes de Trace*.

Vous pouvez également désactiver le filtrage en sélectionnant *Aucun* ou en désélectionnant l'option de filtre.

REMARQUE : si vous avez sélectionné l'option de filtre *ID de thread* ou *ID de connexion* et saisissez une valeur qui n'existe pas, les messages ne s'affichent pas à l'écran. Toutefois, tous les autres messages continuent à être consignés dans le fichier `ndstrace.log`.

16.4 Filtrage des messages de iMonitor

Vous pouvez filtrer les messages de trace de iMonitor en fonction de leur ID de connexion, de leur ID de thread ou de leur numéro d'erreur.

Pour filtrer selon les deux premiers éléments, veillez à ce qu'ils soient activés dans l'onglet Configuration de Trace.

Pour plus d'informations, consultez l'aide en ligne de iMonitor.

16.5 Filtrage des messages de SAL

SAL a fait l'objet d'améliorations pour permettre la consignation d'informations détaillées sur les erreurs à la demande. Les appels de fonction peuvent être suivis avec des arguments dans les versions de débogage.

16.5.1 Configuration des niveaux de gravité

Pour configurer les niveaux de gravité des messages de SAL, vous pouvez utiliser le paramètre `SAL_LogLevels`. Cette liste `SAL_LogLevels` répertorie les niveaux de consignation souhaités, séparés par une virgule.

Les niveaux de consignation sont expliqués dans le tableau ci-dessous :

Tableau 16-1 *Paramètres de filtrage des messages de SAL*

Nom du paramètre	Description
`LogCrit`	Messages critiques. Ce niveau est activé par défaut. Après la consignation d'une erreur critique, le système s'arrête.
`LogErr`	Tous les messages d'erreur. Le système continue à fonctionner, mais les résultats sont imprévisibles.
`LogWarn`	Messages d'avertissement. Il s'agit simplement d'un avertissement qui vous informe d'une erreur imminente.
`LogInfo`	Messages d'information.
`LogDbg`	Messages utilisés à des fins de débogage au moment du développement. Ils sont compilés à partir d'une version diffusée pour réduire la taille du binaire.
`LogCall`	Suit les appels de fonction. Il s'agit d'un sous-ensemble des messages de débogage.
`LogAll`	Active tous les messages sauf `LogCall`.

Un signe « - » au début d'un niveau de consignation spécifique désactive ce niveau.

Exemples

Pour effectuer le filtrage en fonction de tous les niveaux du journal, à l'exception de `LogInfo` et de `LogDbg`, procédez comme suit :

Linux

1. Arrêtez `ndsd`.
2. Saisissez la commande suivante :

```
export SAL_LogLevels=LogAll,-LogInfo,-LogDbg
```

3 Démarrez `ndsd`.

Windows

1 Arrêtez `DHost`.

2 À l'invite de commande, saisissez la commande suivante :

```
set SAL_LogLevels=LogAll,-LogInfo,-LogDbg
```

```
c:\novell\nds>dhost.exe /datadir=c:\novell\nds\DIBFiles\
```

3 Redémarrez `DHost`.

16.5.2 Définition du chemin de fichier journal

La variable d'environnement `SAL_LogFile` permet de définir l'emplacement du fichier journal. Il peut s'agir d'un nom de fichier valide avec un chemin valide ou de l'une des options suivantes.

- Console : tous les messages sont consignés sur la console.
- Syslog : sous Linux, les messages sont placés dans le journal système. Sous Windows, les messages sont consignés dans un fichier nommé syslog. C'est le comportement par défaut de la consignation.

  Toutes les erreurs critiques sont toujours consignées dans syslog sauf en cas de désactivation spécifique.

17 Utilitaire de chargement en bloc en mode hors connexion : ldif2dib

ldif2dib est un nouvel utilitaire de NetIQ eDirectory 8.8 destiné au chargement en bloc des données dans la base de données eDirectory à partir des fichiers LDIF. Cet utilitaire en mode hors connexion permet d'atteindre des chargements en bloc plus rapides qu'avec les autres outils en ligne.

Le tableau suivant répertorie les plates-formes sur lesquelles l'utilitaire ldif2dib est pris en charge.

Fonction	Linux	Windows
ldif2dib	✓	✓

17.1 Utilité de ldif2dib

L'utilitaire ldif2dib est nécessaire lorsqu'une base de données utilisateur volumineuse doit être renseignée avec les entrées d'un fichier LDIF. Les outils en ligne tels que ice ou ldapmodify sont plus lents que ldif2dib en raison des surcharges associées au chargement en bloc en ligne telles que la vérification du schéma, la traduction du protocole et les vérifications du contrôle d'accès. ldif2dib permet d'accélérer le temps de fonctionnement lorsqu'une base de données utilisateur volumineuse doit être remplie et que le temps d'arrêt initial n'est pas un problème.

17.2 Pour plus d'informations

Pour plus d'informations sur cet utilitaire, reportez-vous à la section « Offline Bulkload Utility » (Utilitaire de chargement en bloc hors connexion) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

18 Sauvegarde eDirectory avec SMS

La structure API Services de gestion de stockage (SMS) de Novell est utilisée par les applications de sauvegarde pour proposer une solution complète de sauvegarde. La structure SMS est implémentée par deux composants principaux :

- Requêteur de données de gestion de stockage (SMDR)
- Agent de service cible (TSA)

L'Agent de service cible (TSA) pour les services eDirectory (`tsands`) cible et fournit une implémentation de l'API Services de gestion de stockage (SMS) de Novell pour les arborescences de répertoires. Les applications peuvent être écrites sur l'`API SMS` pour fournir une solution de sauvegarde complète.

Le TSA pour NDS est pris en charge sous Linux.

19 Audit LDAP

L'audit est l'une des principales fonctionnalités qui intéresseront l'administrateur pour l'évaluation d'un annuaire. Le mécanisme d'événements eDirectory facilite l'audit eDirectory. Étant donné que les applications adoptent largement le protocole LDAP pour accéder aux répertoires, il est désormais essentiel que les opérations LDAP soient auditées.

Ce chapitre comprend les sections suivantes :

19.1 Nécessité d'un audit LDAP

L'absence de ce mécanisme d'événement sur le serveur LDAP eDirectory existant était particulièrement notable, car les informations LDAP fournies n'étaient pas suffisantes. Le système d'événements NDS produisait des événements pour toutes les opérations eDirectory, mais la plupart de ces informations étaient insuffisantes ou inadaptées pour qu'une application puisse auditer le serveur LDAP. Les informations concernant le protocole et la liaison, l'adresse réseau, les méthodes et types d'authentification, la recherche et les transactions LDAP, etc., sont essentielles à l'audit d'un serveur LDAP, mais elles n'étaient pas disponibles avec les événements NDS. Pour les développeurs d'applications, il était compliqué d'écrire dans des applications d'audit LDAP en fonction de ces événements.

Le protocole LDAP est une interface importante de eDirectory, car ce mécanisme permet aux applications d'auditer le serveur LDAP eDirectory. Un nouveau sous-système d'événements LDAP a par conséquent été introduit dans la version NetIQ eDirectory 8.8 SP3. Ce sous-système génère des événements LDAP spécifiques, avec toutes les informations pertinentes, pour qu'une application puisse auditer un serveur LDAP. Il s'intitule « audit LDAP ».

19.2 Utilisation de l'audit LDAP

L'audit LDAP permet aux applications de surveiller/auditer les opérations LDAP, notamment l'ajout, la modification et la recherche, et extrait du serveur LDAP des informations utiles telles que les informations de connexion, l'IP du client auquel le serveur était connecté au moment de l'opération LDAP, l'ID du message, le code de résultat de l'opération, etc.

L'audit LDAP peut être exercé par le biais de LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html), qui fournissent l'interface côté client de cette fonctionnalité par l'intermédiaire de nouveaux événements et structures LDAP.

19.3 Pour plus d'informations

Reportez-vous aux informations ci-dessous pour plus de détails sur les événements d'audit LDAP :

- « Configuring LDAP Services for NetIQ eDirectory » (Configuration des services LDAP pour NetIQ eDirectory) du manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).
- NDK : Outils LDAP (http://developer.novell.com/documentation/cldap/ltoolenu/data/hevgtl7k.html) dans la documentation LDAP Libraries for C.

Pour plus d'informations sur les outils LDAP, reportez-vous à la section LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html).

20 Audit avec XDASv2

La spécification XDASv2 fournit une classification standardisée pour les événements d'audit. Elle définit un ensemble d'événements génériques à un niveau système distribué global. XDASv2 offre un format d'enregistrement d'audit portable courant pour faciliter la fusion et l'analyse d'informations d'audit provenant de plusieurs composants au niveau système distribué. Les événements XDASv2 sont encapsulés dans un système de notation hiérarchique qui permet d'étendre l'ensemble d'identificateurs d'événements standard ou existants.

Avec eDirectory 8.8 SP8, si l'agent XDASv2 ne peut pas communiquer avec le serveur syslog, il peut être configuré pour mettre dans le cache local les événements d'audit consignés, ce qui évite la perte des données d'audit. L'agent tente ensuite de renvoyer les événements d'audit stockés, jusqu'à ce que la communication soit rétablie. Le caching des événements XDAS est désactivé par défaut.

Pour plus d'informations, reportez-vous au manuel *NetIQ XDASv2 Administration Guide* (Guide d'administration de NetIQ XDASv2).

21 Divers

Ce chapitre présente de nouvelles fonctionnalités de NetIQ eDirectory 8.8.

21.1 Rapport de vidage de cache de iMonitor

La page Cache de changement de iMonitor affiche un seul objet à la fois, ce qui complique la navigation dans l'intégralité de ce cache. eDirectory 8.8 SP8 ajoute un nouveau rapport de vidage du cache de changement aux rapports par défaut inclus dans iMonitor. Grâce à ce rapport, vous pouvez afficher en une seule fois l'intégralité du cache de changement. Ce rapport permet également à l'administrateur de mieux comprendre les modifications apportées à un serveur.

Lorsque vous exécutez un rapport de vidage du cache de changement, iMonitor génère également un vidage XML complet de tous les objets du cache, ainsi que des attributs et valeurs qui doivent être synchronisés entre les serveurs.

Pour plus d'informations sur les rapports iMonitor, reportez-vous au manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

21.2 Prise en charge dans iManager de la syntaxe des nombres entiers longs de Microsoft

eDirectory 8.8 SP8 propose une nouvelle syntaxe permettant de prendre en charge la syntaxe des nombres entiers longs de Microsoft. Cette syntaxe permet de stocker les valeurs entières longues ou les dates antérieures à 1970 ou ultérieures à 2038. Vous pouvez utiliser LDAP ou iManager pour créer ou gérer des attributs avec cette syntaxe.

REMARQUE : eDirectory utilise toujours sa syntaxe existante et les valeurs 32 bits pour les tampons horaires internes.

21.3 Caching des objets Sécurité

Créé au niveau de la partition racine lors de l'installation du premier serveur dans l'arborescence, le conteneur Sécurité contient des informations telles que des données générales, des règles de sécurité et des clés.

Après l'introduction du mot de passe universel, chaque fois qu'un utilisateur se connectait à eDirectory via NMAS®, NMAS accédait aux informations du conteneur Sécurité pour authentifier la connexion. Si la partition renfermant le conteneur Sécurité n'était pas présente au niveau local, NMAS accédait au serveur qui contenait cette partition. Cela affectait les performances de l'authentification NMAS. C'était encore pire lorsqu'il fallait accéder au serveur qui contenait la partition disposant du conteneur Sécurité par le biais de liaisons WAN.

Pour y remédier, eDirectory 8.8 met en cache les données du conteneur Sécurité sur le serveur local. Ainsi, NMAS ne doit pas accéder au conteneur Sécurité situé sur une autre machine à chaque login d'un utilisateur ; il peut facilement le faire au niveau local, ce qui améliore les performances. L'ajout au serveur local de la partition disposant du conteneur Sécurité augmente les performances, mais n'est pas toujours possible si les serveurs sont trop nombreux.

Si les données du conteneur Sécurité changent sur le serveur qui contient la partition renfermant le conteneur Sécurité, le cache local est rafraîchi par un processus en arrière-plan appelé « liaison en amont ». Par défaut, une liaison en amont est exécutée toutes les treize heures pour extraire les données modifiées du serveur distant. Dans ce cas, les données doivent être synchronisées immédiatement et vous pouvez planifier un processus de liaison en amont sur le serveur local par l'intermédiaire de iMonitor, ndstrace sous Linux ou ndscons sous Windows. Pour plus d'informations, consultez l'aide en ligne de iMonitor ou la page du manuel ndstrace.

La fonction de caching des objets Sécurité est activée par défaut. Si vous ne souhaitez pas que le processus de liaison en amont mette des données en cache, retirez `CachedAttrsOnExtRef` de l'objet Serveur NCP.

21.4 Amélioration des performances de recherche dans les sous-arborescences

Les performances de recherche dans les sous-arborescences de eDirectory demeurent piètres dans les arborescences de grande taille présentant une structure fortement imbriquée, et ce quel que soit le DN de base de la recherche. Ce problème a été résolu par l'utilisation de l'attribut `AncestorID`. L'attribut `AncestorID` répertorie les ID d'entrée de tous les ancêtres, associés à chaque entrée. Utilisé en interne pendant la recherche dans les sous-arborescences, l'attribut `AncestorID` limite l'étendue de la recherche.

Il est complété lors de l'ajout d'une entrée et après une mise à niveau pour toutes les entrées de la DIB, et est recomplété pour toutes les entrées de la sous-arborescence après le déplacement de celle-ci. Toutefois, la recherche dans les sous-arborescences n'utilise pas l'attribut `AncestorID` pendant que l'attribut est complété après une mise à niveau et un déplacement de sous-arborescence. Les performances de recherche dans les sous-arborescences restent donc similaires à celles qui existaient avant eDirectory 8.8.

Pour vérifier si les attributs `AncestorID` sont actualisés après une mise à niveau :

Une fois les attributs `AncestorID` complétés, la version de mise à niveau de l'objet NDS passe à 6 ou plus. Pour le vérifier, utilisez iMonitor dans la section *Historique de la DIB* de la page Informations sur les agents.

Pour vérifier si les attributs `AncestorID` sont actualisés après le déplacement d'une sous-arborescence :

Pendant que les attributs `AncestorID` sont complétés, l'attribut `UpdateInProgress` dans l'objet `Pseudo serveur` détient la liste des ID d'entrée de la racine de partition de la sous-arborescence. Une fois les attributs `AncestorID` complétés, l'attribut est absent de l'objet `Pseudo serveur`.

DSRepair met à jour l'attribut `AncestorID` s'il n'est pas valide.

21.5 Changements d'hôte local

Les serveurs eDirectory 8.8 n'écoutent pas sur l'adresse en boucle. Les utilitaires qui utilisent l'hôte local doivent être reconfigurés pour utiliser la résolution du nom d'hôte ou de l'adresse IP.

Si un utilitaire ou un outil tiers assure la résolution par le biais de l'hôte local, il doit être reconfiguré pour l'effectuer grâce au nom d'hôte ou à l'adresse IP et non via l'adresse de l'hôte local.

21.6 256 gestionnaires de fichiers sous Solaris

Auparavant, l'implémentation des flux stdio Solaris 2.*x* pouvait utiliser un maximum de 256 descripteurs de fichiers. ce qui ne suffisait pas pour un bon fonctionnement de eDirectory. eDirectory 8.8 fournit une bibliothèque stub pour éviter ce problème.

21.7 Gestionnaire de mémoire sous Solaris

Les précédentes versions de eDirectory sous Solaris utilisaient comme gestionnaire de mémoire le produit tiers Geodesic*. En revanche, eDirectory 8.8 ne comporte plus d'allocateur de mémoire tiers, mais emploie le gestionnaire de mémoire natif.

Les performances de eDirectory ne sont pas affectées. Dans la plupart des cas, celles-ci sont identiques, voire meilleures, que dans les versions avec allocateur tiers.

21.8 Groupes imbriqués

eDirectory 8.8 SP2 prend en charge le regroupement de groupes, ce qui constitue une forme de regroupement plus structurée. Cette fonctionnalité est appelée « groupes imbriqués ». Actuellement, l'imbrication est autorisée pour les groupes statiques.

Elle peut comporter plusieurs niveaux, jusqu'à 200.

Pour plus d'informations sur les groupes imbriqués, reportez-vous au manuel *NetIQ eDirectory 8.8 SP8 Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).