# NetIQ® eDirectory ™

## Guide d'installation

**Octobre 2019**

## Mentions légales

# À propos de ce guide et de la bibliothèque

Le *guide d'installation* explique comment installer eDirectory 9.2. Il est destiné aux administrateurs réseau.

Pour obtenir la dernière version du manuel *NetIQ eDirectory  Installation Guide (Guide d'installation de NetIQ eDirectory  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 :

**Guide d'administration**

Décrit comment gérer et configurer eDirectory.

**Guide d'optimisation pour les 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 9.2.

Pour plus d'informations sur l'utilitaire de gestion d'eDirectory, reportez-vous au *Guide d'administration de NetIQ 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 Fonctionnalités relatives à l'installation et à la mise à niveau

Ce chapitre décrit les fonctionnalités relatives à l'installation et à la mise à niveau de NetIQ eDirectory 9.2.

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 d'eDirectory 9.2 | ✓ | ✗ |
| 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-root | ✓ | ✗ |
| 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 :

# Formats de paquetage multiples pour l'installation d'eDirectory 9.2

Sous Linux, vous avez la possibilité de choisir entre plusieurs formats de fichier pendant l'installation d'eDirectory 9.2 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 à l'aide de fichiers Tarball, reportez-vous à la « Mise à niveau du déploiement du tarball d'eDirectory 9.2 » page 30.

# Installation d'eDirectory 9.2 dans un emplacement personnalisé

Avec eDirectory 9.2, vous avez la possibilité d'installer les fichiers d'application, de données et de configuration dans l'emplacement de votre choix.

Vous pouvez par exemple installer eDirectory 9.2 dans un emplacement personnalisé si une version antérieure d'eDirectory est déjà installée sur votre hôte et que vous souhaitez tester eDirectory 9.2 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 9.2.

**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 :


- « Indication d'un emplacement personnalisé pour les fichiers d'application » page 12
- « Indication d'un emplacement personnalisé pour les fichiers de données » page 13
- « Indication d'un emplacement personnalisé pour les fichiers de configuration » page 13


## 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 9.2 dans un emplacement personnalisé, vous pouvez utiliser le fichier d'installation tarball et décompresser eDirectory 9.2 dans 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 9.2 d'eDirectory.

## 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.<br>**REMARQUE :** cette option existait déjà avant la version 9.2 d'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.

## 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.

## Installation non-root

À partir de la version 9.2 d'eDirectory, l'installation et la configuration des serveurs eDirectory peuvent être effectuées par un utilisateur non-root. Les versions antérieures d'eDirectory ne pouvaient être installées et configurées que par un utilisateur root, avec une seule instance d'eDirectory qui s'exécutait sur un hôte.

À partir d'eDirectory 9.2, 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 des 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 à la « Mise à niveau de plusieurs instances » page 31.

La configuration et l'installation non-root s'appliquent uniquement aux plates-formes Linux. Pour plus d'informations sur l'installation et la configuration non-root, reportez-vous à la « Installation d'eDirectory 9.2 par un utilisateur non-root » page 36.

## Conformité aux normes

eDirectory 9.2 est conforme aux normes suivantes :


- « Conformité FHS » page 15
- « Conformité LSB » page 16

# Conformité FHS

Pour éviter les conflits avec les fichiers d'application d'autres produits, eDirectory 9.2 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 9.2, vous devez mettre à jour les variables d'environnement PATH et les exporter. Cela 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.

## Conformité LSB

eDirectory 9.2 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`.

# Vérifications de l’état de santé du serveur

NetIQ eDirectory propose des vérifications de l'état de santé du serveur qui permettent de s'assurer qu'il pourra bien être mis 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.

Pour plus d'informations sur les procédures régulières de vérification de l'état de santé, reportez-vous à la section Maintenance de NetIQ eDirectory du *Guide d'administration de NetIQ eDirectory*.

## 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.

## 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.

## Vérifications de l’état de santé

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


- « Avec la mise à niveau » page 16
- « Avec un utilitaire autonome » page 17


---

**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 1-1*** *Utilitaires de vérification de l'état de santé*

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

# 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 « Fichiers journaux » page 19.

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 « Catégorisation de l'état de santé » page 18.

### 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.

## 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 « Fichiers journaux » page 19.

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.

## 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 1-2*** *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`.<br><br>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 :<br><br>1. Si vous avez utilisé l'option `-h`, le fichier `ndscheck.log` est enregistré dans le répertoire privé de l'utilisateur.<br>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`* |

# Intégration de SecretStore dans eDirectory

eDirectory 9.2 permet de configurer Novell SecretStore 3.4 en même temps qu'eDirectory. Vous devez installer manuellement SecretStore avant eDirectory 9.0.

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).

# Installation de eDirectory Instrumentation

Les outils eDirectory précédents faisaient partie de Novell Audit. Vous devez installer eDirectory Instrumentation séparément.

Pour plus d'informations sur l'installation, la configuration et la désinstallation d'eDirectory Instrumentation, reportez-vous à la section Audit des événements eDirectory du *Guide d'administration de NetIQ eDirectory*.

# Pour plus d'informations

Pour plus d'informations sur l'une des fonctionnalités détaillées dans ce chapitre, consultez la documentation suivante :

- *Guide d'administration de NetIQ eDirectory*
- Sur Linux : pages du manuel `nds-install`, `ndsconfig` et `ndscheck`

# 2 Installation ou mise à niveau de NetIQ eDirectory sous Linux

Les informations suivantes permettent d'installer ou de mettre à niveau NetIQ eDirectory 9.2 sur un serveur Linux :



## Configuration système requise

Vous devez installer eDirectory sur l'une des plates-formes 64 bits suivantes :

- Mémoire
  - 300 Mo d’espace disque pour le serveur eDirectory
  - 150 Mo d’espace disque pour 50 000 utilisateurs
- Systèmes de virtualisation
  - VMWare ESXi
- L'un des systèmes d'exploitation suivants :

  Le tableau ci-après contient une liste des systèmes d'exploitation de serveur certifiés et pris en charge sur lesquels le coffre-fort d'identité peut s'exécuter.

  **IMPORTANT :** un système d'exploitation certifié est un système d'exploitation qui a été entièrement testé et qui est pris en charge. En revanche, un système d'exploitation simplement répertorié comme pris en charge est un système d'exploitation qui n'a pas encore été testé, mais qui devrait être compatible.

| Version certifiée du système d'exploitation du serveur | Systèmes d'exploitation pris en charge | Remarques |
|---|---|---|
| SUSE Linux Enterprise Server 12 (SLES) SP3 et SP4 | Pris en charge sous les versions ultérieures de Support Packs | Pour obtenir les dernières informations à propos de la configuration système requise, consultez les Notes de version. |

| Version certifiée du système d'exploitation du serveur | Systèmes d'exploitation pris en charge | Remarques |
|---|---|---|
| SUSE Linux Enterprise Server 15 et SLES 15 SP1 | Pris en charge sous les versions ultérieures de Support Packs | Pour obtenir les dernières informations à propos de la configuration système requise, consultez les Notes de version.<br><br>**REMARQUE :** pour utiliser les utilitaires `ndstrace` et `ldif2dib` sur SLES 15, installez la version 5 de `ncurses` à partir de l'espace de stockage SLES 15. |
| Red Hat Enterprise Linux (RHEL) 7.6, 7.7 | Pris en charge sous les versions ultérieures de Support Packs | Pour obtenir les dernières informations à propos de la configuration système requise, consultez les Notes de version.<br><br>**REMARQUE :** eDirectory 9.0 SP4 et ses versions ultérieures prennent en charge une installation non-root sous RHEL 7.x. |
| RHEL 8.0 | Pris en charge sous les versions ultérieures de Support Packs | Pour obtenir les dernières informations à propos de la configuration système requise, consultez les Notes de version.<br><br>**REMARQUE**<br>◆ pour utiliser les utilitaires `ndstrace` et `ldif2dib` sur RHEL 8, installez la version 5 de `ncurses` à partir de l'espace de stockage RHEL 8.<br>◆ Vous devez définir SELinux en mode « permissive » (permissif) sur RHEL 8. |

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

Veillez à ce que les correctifs `glibc` les plus récents (32 bits et 64 bits) soient appliqués à partir de Red Hat Errata (http://rhn.redhat.com/errata) sur les systèmes Red Hat. La version 2.4 est la version minimale requise pour la bibliothèque `glibc`.

**REMARQUE :** eDirectory ne prend pas en charge Btrfs (B-tree file system).

## Détermination de la version d'eDirectory

Pour déterminer la version d'eDirectory, suivez l'une des étapes mentionnées ci-dessous :

- Exécutez ndsstat.

  L'utilitaire ndsstat affiche des informations relatives aux serveurs eDirectory, par exemple le nom de l'arborescence eDirectory, le nom distinctif complet du serveur et la version de eDirectory. Dans l'exemple ci-dessous, eDirectory 9.2 est la version du produit (chaîne marketing) et 40201.12 la version binaire (numéro de version interne).

```
osg-dt-srv17:/>ndsstat
Tree Name: SNMP-HPUX-RASH
Server Name: .CN=osg-dt-srv17.O=novell.T=SNMP-HPUX-RASH.
Binary Version: 40201.12
Root Most Entry Depth: 0
Product Version: eDirectory for Linux x86_64 v9.2 [DS]
```

Pour plus d'informations sur l'exécution de ndsstat, reportez-vous à la section « Commandes et syntaxe de NetIQ eDirectory Linux » du Guide d'administration de NetIQ eDirectory ou à la page du manuel ndsstat (`ndsstat.1m`).

- Exécutez `ndsd --version`.

  Pour plus d'informations sur l'exécution de ndsd, reportez-vous à la section « Commandes et syntaxe de NetIQ eDirectory Linux » du Guide d'administration de NetIQ eDirectory ou à la page du manuel ndsd (`ndsd.1m`).

- Exécutez iMonitor.

  Dans la page Résumé de l'agent, cliquez sur Serveurs connus. Ensuite, sous Serveurs connus de la base de données, cliquez sur Serveurs connus. La colonne Révision de l'agent affiche le numéro de version interne de chaque serveur. Par exemple, un numéro de révision d'agent pour NetIQ eDirectory 9.2 pourrait être 40002.79.

  Pour plus d'informations sur l'exécution de iMonitor, reportez-vous à la section « Accessing iMonitor » (Accès à iMonitor) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

- Exécutez `rpm -qi NDSserv`.

  Cette commande permet d'afficher des informations identiques à `ndsd --version`.

# Conditions préalables

---

**IMPORTANT :** avant de mettre à niveau votre environnement eDirectory existant, vérifiez les applications NetIQ et tierces actuellement installées pour déterminer si ces produits sont pris en charge sur eDirectory 9.2. Les conditions préalables des autres produits NetIQ sont disponibles sur le site de documentation NetIQ (http://www.netiq.com/documentation/). Nous vous recommandons également de sauvegarder une instance eDirectory avant d'effectuer toute mise à niveau sur cette instance.

---

❒ Veillez à installer les RPM suivants en fonction de votre système d'exploitation :

- **RHEL 7.x :** `yum-utils` et `createrepo`
- **RHEL 8.x :** `dnf-utils` et `createrepo`
- **SLES :** Zypper

❒ (Conditionnel) NICI (Novell International Cryptographic Infrastructure) 3.2 et eDirectory 9.2 prennent en charge les tailles de clé allant jusqu'à 8 192 bits. Si vous souhaitez utiliser une taille de clé de 8 kilobits, chaque serveur doit être mis à niveau vers eDirectory 9.2. De plus, NICI 3.2 doit être installé sur chaque poste de travail qui utilise les utilitaires de gestion, par exemple iManager.

Lorsque vous mettez à niveau votre serveur d'autorité de certification (CA) vers eDirectory 9.2, la taille de clé reste inchangée (2 kilobits). La seule façon de créer une taille de clé de 8 kilobits est de recréer l'autorité de certification sur un serveur eDirectory 9.2. En outre, vous devrez remplacer la taille de clé par défaut (2 000 bits) par 8 000 bits lors de la création de l'autorité de certification.

Quand vous installez eDirectory, l'utilitaire nds-install installe automatiquement NICI. Pour en savoir plus sur l'installation de eDirectory, reportez-vous à la « Exécution de l'utilitaire nds-install pour installer des composants eDirectory » page 33. Cependant, si vous avez besoin d'installer uniquement NICI, et non eDirectory, sur un poste de travail qui est équipé des utilitaires de gestion, vous devez installer NICI manuellement. Pour en savoir plus sur l'installation manuelle de NICI, consultez « Installation de l'infrastructure NICI » page 37.

❒ (Conditionnel) Le service SLP (Service Location Protocol) doit être installé et configuré uniquement si vous envisagez de l'utiliser pour résoudre les noms d'arborescence lorsque DNS n'est pas disponible.

L'installation d'eDirectory 9.2 n'inclut pas celle de SLP.

Seul un utilisateur root peut installer SLP.

Pour plus d'informations sur l'installation de SLP, reportez-vous à la section « Utilisation de SLP avec eDirectory » page 32.

---

**REMARQUE :** le service SLP ne fonctionne pas avec eDirectory 9.1 et versions ultérieures.

---

❒ Hôte Linux activé pour le routage multidiffusion

Entrez la commande suivante afin de vérifier si l'hôte est activé pour le routage multidiffusion.

```
/bin/netstat -nr
```

L'entrée suivante doit être présente dans la table de routage :

```
224.0.0.0 0.0.0.0
```

Si l'entrée n'apparaît pas, connectez-vous en tant qu'utilisateur root, puis entrez la commande suivante pour activer le routage multidiffusion :

```
route add -net 224.0.0.0 netmask 240.0.0.0 dev interface
```

La valeur *interface* peut être une valeur telle que eth0, hme0, hme1 ou hme2, selon la carte d'interface réseau (NIC) installée et utilisée.

Pour plus d'informations sur les routages multidiffusion et de diffusion, consultez le site Web OpenSLP (http://www.openslp.org/doc/html/UsersGuide/Installation.html).

❒ Heure synchronisée sur le réseau de serveurs

Pour synchroniser l'heure de tous les serveurs du réseau, utilisez le module ntp du protocole NTP (Network Time Protocol).

❒ (Conditionnel) Si vous installez un serveur secondaire, toutes les répliques de la partition sur laquelle vous installez le produit doivent être activées.

❒ (Conditionnel) Si vous installez un serveur secondaire dans une arborescence existante en tant qu'utilisateur non administrateur, créez un conteneur, puis partitionnez-le. Vérifiez que vous disposez des droits suivants :

- droits de superviseur sur cette partition ;
- tous les droits d'attributs : droits de lecture, de comparaison et d'écriture sur l'objet W0.KAP.Security ;
- droits d'entrée : droits d'exploration sur l'objet Conteneur de sécurité ;

- tous les droits d'attributs : droits de lecture et de comparaison sur l'objet Conteneur de sécurité.
- (Conditionnel) Si l'objet W1.KAP.Security existe, vous disposez de tous les droits d'attribut sur cet objet : lecture, comparaison et écriture. Pour plus d'informations sur l'objet W1.KAP.Security, reportez-vous à la section Creating an AES 256-Bit Tree Key (Création d'une clé AES 256 bits) du *NICI Administration Guide* (Guide d'administration de NICI).

❒ (Conditionnel) Si vous installez un serveur secondaire dans une arborescence existante en tant qu'utilisateur non administrateur, assurez-vous qu'au moins l'un des serveurs de l'arborescence a la même version ou une version ultérieure de eDirectory par rapport à celle du serveur secondaire ajouté comme administrateur de conteneur. Dans le cas où le serveur secondaire ajouté possède une version ultérieure, le schéma doit alors être prolongé par l'administrateur de l'arborescence avant d'ajouter ledit serveur à l'aide de l'administrateur de conteneur.

❒ Lors de la configuration de eDirectory, vous devez activer les services SLP et un port de protocole NCP (NetWare Core Protocol) (port 524 par défaut) dans le pare-feu afin de permettre l'ajout du serveur secondaire. En outre, vous pouvez activer les ports de service suivant en fonction de vos exigences :

- LDAP texte clair - 389
- LDAP sécurisé - 636
- HTTP texte clair - 8028
- HTTP sécurisé - 8030

Si vous avez activé des ports définis par l'utilisateur, vous devez les mentionner pendant la configuration de eDirectory.

---

**REMARQUE :** Cette étape est requise uniquement si SLP est configuré dans votre système.

---

❒ Ne configurez pas les ports définis par l'utilisateur sur 8008 ou 8010 lors de la mise à niveau d'eDirectory 8.8 SP8 ou version ultérieure vers la version 9.2. Si les ports sont définis sur 8008 ou 8010, `ndsconfig` suppose que le serveur utilise une version d'eDirectory antérieure à 8.8.*x* et réinitialise automatiquement ces ports sur 8028 et 8030.

❒ Pendant la mise à niveau d'eDirectory, si SecretStore n'a pas été configuré avec les versions antérieures ou si vous ne souhaitez pas configurer SecretStore, utilisez l'option `-m no_ss` avec l'utilitaire `nds-install`.

❒ Si vous ne disposez pas de la version la plus récente de Platform Agent (PA) lors de la mise à niveau vers eDirectory 9.2, exécutez le fichier `novell-AUDTplatformagent-2.0.2-80.x86_64.rpm` à partir de l'emplacement d'installation `<dossier_extraction_version_eDirectory>/eDirectory/setup/`.

❒ L'outil NetIQ eMBox (eDirectory Management Toolbox) permet d'accéder à tous les principaux utilitaires d'eDirectory, à distance comme sur le serveur. Le client à ligne de commande est une application Java. Pour l'exécuter, vous devez installer la dernière version d'Oracle Java (1.8 ou version ultérieure). Vous devez également veiller à mettre à niveau toute version antérieure de Java en installant les mises à niveau de correctif disponibles. Une fois que la dernière version de Java est installée, exportez les variables d'environnement suivantes souhaitées :

- `EDIR_JAVA_HOME`
- `JAVA_HOME`
- `JRE_HOME`

**REMARQUE :**

- Si aucune des variables d'environnement mentionnées n'est détectée, le client à ligne de commande recherche le fichier binaire Java dans la variable d'environnement PATH par défaut.
- Si vous utilisez une version antérieure à eDirectory 9.0 SP4, pour exécuter le client à ligne de commande, vous devez avoir accès à l'environnement d'exécution Java, Oracle Java 1.8, qui est installé avec eDirectory.

### Configuration de l’adresse IP statique

L’adresse IP statique doit être configurée sur le serveur pour que eDirectory fonctionne efficacement. La configuration de eDirectory sur les serveurs dotés d’une adresse DHCP peut provoquer des résultats imprévisibles.

# Configuration matérielle requise

La configuration matérielle requise dépend de la mise en œuvre spécifique de eDirectory. Deux facteurs augmentent les performances : une mémoire cache plus importante et des processeurs plus rapides. Pour obtenir des résultats optimaux, mettez en cache autant de paramètres de l’ensemble DIB (Directory Information Base, base de données des informations de l’Annuaire) que le permet le matériel.

eDirectory fonctionne correctement avec un seul processeur. Cependant, NetIQ eDirectory 9.2 tire parti de la présence de plusieurs processeurs. L’ajout de processeurs améliore les performances dans certains cas, par exemple pour les connexions, et lorsque plusieurs fils d’exécution sont actifs sur plusieurs processeurs. eDirectory en lui-même n’est pas gourmand en ressources processeur, mais plutôt en E/S.

Le tableau suivant illustre les exigences système habituelles pour  eDirectory pour Linux :

| Objets | Mémoire | Disque dur |
|---|---|---|
| 100 000 | 2 Go et plus | 300 Mo |
| 1 million | 4 Go | 1,5 Go |
| 10 millions | 4 Go et plus | 15 Go |

# Exécution forcée du processus de liaison en amont

Étant donné que les identificateurs internes de eDirectory changent après la mise à niveau vers NetIQ eDirectory, le processus de liaison en amont (backlink) doit mettre à jour les objets liés en amont pour les rendre cohérents.

Les liens en amont sont utilisés pour assurer le suivi des références externes aux objets sur d’autres serveurs. Pour chaque référence externe sur un serveur, le processus de liaison en amont s’assure que l’objet réel existe dans l’emplacement correct et vérifie tous les attributs de liaison en amont sur la réplique maîtresse. Le processus de liaison en amont intervient deux heures après l’ouverture de la base de données, puis toutes les 780 minutes (13 heures). Vous pouvez paramétrer l’intervalle de 2 minutes à 10 080 minutes (7 jours).

Une fois la migration vers eDirectory effectuée, lancez le processus DSTrace à l'aide de la commande `ndstrace -l>log&` qui l'exécute en arrière-plan. Cela vous permet d'analyser correctement les résultats du processus de liaison en amont, ce qui prend entre 4 et 10 minutes. Vous pouvez ensuite forcer l'exécution de la liaison en amont à l'aide de la commande `ndstrace -c set ndstrace=*B'` à partir de l'invite de commande de l'OS DSTrace. Examinez les résultats du fichier journal créé à la première étape. Vous pouvez ensuite décharger le processus DSTrace au moyen de la commande `ndstrace -u`. Le processus de liaison en amont est particulièrement important sur les serveurs qui ne contiennent pas de réplique.

# Mise à niveau de eDirectory

Lors de la mise à niveau d'eDirectory, celle-ci peut-être effectuée à partir d'eDirectory 8.8.8.x 64 bits vers eDirectory 9.2 64 bits.

---

**REMARQUE :** pour effectuer une mise à niveau à partir d'une version 32 bits d'eDirectory vers une version 64 bits, vous devez d'abord mettre à niveau la version 32 bits vers la version 64 bits d'eDirectory 8.8.x, puis vers eDirectory 9.2. Vous pouvez suivre la même procédure pour la mise à niveau d'eDirectory 64 bits vers eDirectory 9.2.

---

Les sections suivantes fournissent des informations permettant de mettre à niveau votre installation eDirectory existante vers la version actuelle.


- « Vérifications de l'état de santé du serveur » page 27
- « Mettre à niveau sur des serveurs Linux autres qu'OES » page 28
- « Mise à niveau sans surveillance de eDirectory sous Linux » page 28
- « Mise à niveau du déploiement du tarball d'eDirectory 9.2 » page 30
- « Mise à niveau de plusieurs instances » page 31


---

**REMARQUE :** La commande `ndsconfig upgrade` permet de mettre à niveau la configuration nécessaire des différents composants tels que HTTP, LDAP, SNMP, SAS et NMAS (NetIQ Modular Authentication Service).

---

## Vérifications de l'état de santé du serveur

eDirectory 9.2 exécute par défaut une vérification de l'état de santé du serveur pour s'assurer qu'il est sain avant la mise à niveau :


- « État de santé des partitions et répliques » page 163


En fonction des résultats obtenus, la mise à niveau se poursuivra ou sera abandonnée :

- si toutes les vérifications de l'état de santé ont été menées avec succès, la mise à niveau se poursuivra ;
- en cas d'erreurs mineures, vous serez invité à poursuivre ou à quitter la mise à niveau ;
- en cas d'erreurs critiques, la mise à niveau sera abandonnée.

Reportez-vous à l'Annexe B, « Vérifications de l'état de santé de eDirectory », page 161 pour consulter la liste de conditions des erreurs mineures et critiques.

### Omission des vérifications de l'état de santé du serveur

Pour ignorer les vérifications de l'état de santé du serveur, exécutez `nds-install -j` ou `ndsconfig upgrade -j` à partir du dossier d'installation.

Pour plus d'informations, reportez-vous à la Annexe B, « Vérifications de l'état de santé de eDirectory », page 161.

## Mettre à niveau sur des serveurs Linux autres qu'OES

La mise à niveau de eDirectory est prise en charge à partir de eDirectory 8.8

Pour procéder à la mise à niveau, utilisez l'utilitaire nds-install. Cet utilitaire se trouve dans le répertoire `d'installation` du fichier téléchargé de la plate-forme Linux. Entrez la commande suivante à partir du répertoire `d'installation` :

```
./nds-install
```

Après la mise à niveau vers eDirectory 9.2, les emplacements par défaut des fichiers de configuration, des fichiers de données et des fichiers journaux sont respectivement déplacés vers `/etc/opt/novell/eDirectory/conf`, `/var/opt/novell/eDirectory/data` et `/var/opt/novell/eDirectory/log`.

Le nouveau répertoire `/var/opt/novell/eDirectory/data` utilise un lien symbolique vers le répertoire `/var/nds`.

L'ancien fichier de configuration `/etc/nds.conf` est migré vers le répertoire `/etc/opt/novell/eDirectory/conf`. L'ancien fichier de configuration `/etc/nds.conf` et les anciens fichiers journaux `/var/nds` sont conservés à des fins de référence.

---

**REMARQUE :** exécutez `ndsconfig upgrade` après `nds-install` si la mise à niveau de la DIB échoue et que `nds-install` vous invite à effectuer cette opération. Si les services eDirectory ne démarrent pas après avoir mis à niveau le système d'exploitation RHEL 6.8 vers la version 7.1, exécutez la commande `ndsconfig upgrade`.

---

**REMARQUE :** La vérification de l'état de santé échoue à cause de la synchronisation de l'heure. Pour résoudre ce problème, effectuez une synchronisation de l'heure entre les instances. Vous pouvez ignorer ce message d'avertissement pendant la mise à niveau.

---

## Mise à niveau sans surveillance de eDirectory sous Linux

Sous Linux, eDirectory fournit des commutateurs et des options, ainsi que le script d'installation et l'utilitaire de configuration qui simplifie la mise à niveau sans surveillance. Les sections suivantes abordent les diverses étapes de la mise à niveau sans surveillance de eDirectory sous Linux :

1. effectuez la vérification de l'état de santé de eDirectory :

   la vérification de l'état de santé de toutes les instances root planifiée pour la mise à niveau est réalisée manuellement à l'aide de l'utilitaire `ndscheck`.

   **1a** `exportez LD_LIBRARY_PATH vers l'<emplacement désarchivé de eDirectory>/eDirectory/setup/utils`

   **1b** Exécutez ndscheck à l'aide de l'une des commandes suivantes :

   ```
   <untarred location of eDirectory>/eDirectory/setup/utils/ndscheck -a <user name> -w passwd --config-file <nds.conf with absolute path>
   ```

**Passer le mot de passe dans la variable d'environnement :** `<emplacement désarchivé de 88SP8>/eDirectory/setup/utils/ndscheck -a <nom d'utilisateur> -w env:<variable d'environnement> --config-file <nds.conf avec chemin absolu>`

**Passer le mot de passe dans un fichier :** `<emplacement désarchivé de 88SP8>/eDirectory/setup/utils/ndscheck -a <nom d'utilisateur> -w file:<nom de fichier> --config-file <nds.conf avec chemin absolu>`

L'une des commandes ci-dessus peut être utilisée dans le script automatisé de la vérification de l'état de santé. Par exemple :

```
/Builds/eDirectory/utils/ndscheck -a admin.novell -w n
/Builds/eDirectory/utils/ndscheck -a admin.novell -w env:ADM_PASWD
/Builds/eDirectory/utils/ndscheck -a admin.novell -w file:adm_paswd
```

**2** Mettez à niveau les paquetages eDirectory 9.2 :

**2a** Exécutez le script nds-install pour mettre à niveau les paquetages tel qu'indiqué ci-dessous :

```
nds-install -u -i -j
```

**3** Mettez à jour les variables d'environnement suivantes :

```
PATH=/opt/novell/eDirectory/bin:/opt/novell/eDirectory/sbin:$PATH
LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/opt/novell/eDirectory/lib/nds-
modules:/opt/novell/lib:$LD_LIBRARY_PATH
MANPATH=/opt/novell/man:/opt/novell/eDirectory/man:$MANPATH
TEXTDOMAINDIR=/opt/novell/eDirectory/share/locale
```

**4** Mettez à niveau eDirectory à l'aide de l'utilitaire `ndsconfig` pour toutes les instances root en exécutant les commandes suivantes :

`ndsconfig upgrade -a <user name> -w passwd -c --config-file <nds.conf with absolute path> --configure-eba-now <yes/no>`

---

**REMARQUE :** pour activer l'authentification EBA, spécifiez *yes* pour le paramètre `--configure-eba-now` dans la commande ndsconfig upgrade. Dans le cas contraire, spécifiez *no* pour la configurer ultérieurement.

---

**Passer le mot de passe dans la variable d'environnement :** `ndsconfig upgrade -a <nom utilisateur> -w env:<variable environnement> -c --config-file <nds.conf avec chemin absolu> --configure-eba-now <yes/no>`

**Passer le mot de passe dans un fichier :** `ndsconfig upgrade -a <nom utilisateur> -w file:<nom fichier avec chemin absolu/relatif> -c --config-file <nds.conf avec chemin absolu> --configure-eba-now <yes/no>`

L'une des commandes ci-dessus peut être utilisée dans le script automatisé de la mise à niveau de eDirectory. Par exemple :

```
ndsconfig upgrade -a admin.novell -w n -c -–config-file /etc/opt/novell/
eDirectory/conf/nds.conf --configure-eba-now <yes/no>
```

```
ndsconfig upgrade -a admin.novell -w env:ADM_PASWD -c --config-file /etc/opt/
novell/eDirectory/conf/nds.conf --configure-eba-now <yes/no>
```

```
ndsconfig upgrade -a admin.novell -w <password file path>/adm_paswd -c --
config-file /etc/opt/novell/eDirectory/conf/nds.conf --configure-eba-now <yes/
no>
```

# Mise à niveau du déploiement du tarball d'eDirectory 9.2

Si vous souhaitez mettre à niveau le déploiement du tarball d'eDirectory 8.8 vers eDirectory 9.2, procédez comme suit :

1. Téléchargez la version du tarball.
2. Prenez une sauvegarde des fichiers de configuration suivants :
   - `$NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndsimon.conf`
   - `$NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ice.conf`
   - `$NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndsimonhealth.conf`
   - `$NDSHOME/eDirectory/etc/opt/novell/eDirectory/conf/ndssnmp/ndssnmp.cfg`
   - `$NDSHOME` est l'emplacement où eDirectory est installé.
3. Pour mettre à niveau des versions de eDirectory antérieures à 8.8 SP1, procédez comme suit :
   - Effectuez un contrôle de l'espace disque à l'aide de la commande `ndscheck -D --config-file conf_file_path`
   - Créez un fichier vide `upgradeDIB` sous l'emplacement DIB de chaque instance de serveur.

     La liste des instances peut être obtenue grâce à l'utilitaire `ndsmanage`.
4. Avant de procéder à la mise à niveau, exécutez une vérification de l'état de santé de toutes les instances à l'aide de l'utilitaire `ndscheck` et contrôlez le fichier `ndscheck.log` pour y détecter toute erreur.
5. Arrêtez toutes les instances à l'aide de l'utilitaire `ndsmanage`.
6. Désarchivez le tarball dans le même emplacement (`$NDSHOME`) que celui où est installé eDirectory. En désarchivant le tarball dans le même emplacement, vous écrasez les binaires et les bibliothèques.
7. Mettez à niveau le paquetage suivant, le cas échéant.

| Plate-forme | Commande | Paquetages |
|---|---|---|
| Linux | | ◆ `novell-NOVLsubag-9.2.0-0.x86_64.rpm`<br>◆ `nici64-3.2.0-0.00.x86_64.rpm`<br>**REMARQUE :** Pour plus d'informations sur l'installation de NICI 64 bits, reportez-vous à la section « Installation de l'infrastructure NICI » page 37. |

8. Restaurez les fichiers de configuration.
9. Exécutez `$NDSHOME/eDirectory/opt/novell/eDirectory/bin/ndspath` pour définir toutes les variables d'environnement.
10. Exécutez `ndsconfig upgrade -j` pour toutes les instances. Lors de l'exécution de `ndscongif upgrade`, suivez l'ordre dans lequel la réplique maîtresse est la première instance, puis est suivie des instances Lire/Écrire et des autres.

## Mise à niveau de plusieurs instances

Ce chapitre comprend les informations suivantes :



### L'utilisateur root possède plusieurs instances

Si vous exécutez nds-install après avoir mis à niveau le paquetage, il vous invite à mettre à niveau les fichiers DIB de toutes les instances du serveur eDirectory, ce qui peut durer longtemps. Si vous souhaitez effectuer la mise à niveau DIB en parallèle, vous pouvez le faire manuellement. Pour plus d'informations sur la mise à niveau manuelle de la DIB, consultez les Notes de version de NetIQ eDirectory. Si vous mettez à niveau la DIB de toutes les instances actives, une par une, la commande `ndsconfig upgrade` est exécutée séparément pour chaque instance. Si vous disposez d'une DIB plus volumineuse, vous pouvez sélectionner **Non** et exécuter `ndsconfig upgrade` en parallèle dans des shells distincts, ce qui réduit la durée de la mise à niveau de chaque instance.

### Instances d'utilisateur non root

Si vous avez des instances d'utilisateurs non root qui utilisent des binaires d'utilisateurs root, avant de procéder à la mise à niveau du paquetage, vous devez exécuter ndscheck pour lesdites instances et vous assurer que leur état de santé est correct en vous reportant au fichier `ndscheck.log`. Si vous exécutez nds-install, toutes les instances sont arrêtées, y compris les instances d'utilisateurs non root. Après avoir effectué la mise à niveau du paquetage, la commande `nds-install` n'appelle pas la commande `ndsconfig upgrade` pour les instances d'utilisateurs non-root. Pour démarrer ces instances, vous devez exécuter manuellement `ndsconfig upgrade` pour toutes les instances des utilisateurs non-root.

### Ordre de mise à niveau

Pendant l'exécution de `ndsconfig upgrade`, il est recommandé de suivre l'ordre dans lequel la réplique maîtresse arrive en premier, puis est suivie des répliques Lire//Écrire ou autres.

# Installation de eDirectory

Les sections suivantes fournissent des informations sur l'installation de NetIQ eDirectory sous Linux :

- « Configuration de SNMP par un utilisateur non-root » page 54
- « Localisation des fichiers journaux » page 55

## Utilisation de SLP avec eDirectory

Dans les précédentes versions de eDirectory, l'installation de SLP se faisait pendant celle de eDirectory. En revanche, avec eDirectory 9.2, vous devez d'abord installer SLP, puis eDirectory.

Si vous prévoyez d'utiliser SLP pour résoudre les noms d'arborescence, vous devez installer et configurer le protocole et les agents de répertoire (AR) SLP doivent être stables.

1. Installez OpenSLP si le programme n'est pas déjà installé.
2. Suivez les instructions affichées pour terminer l'installation de SLP.
3. Démarrez SLP manuellement comme suit :

   ```
   /etc/init.d/slpd start
   ```

Pour plus d'informations, reportez-vous à la Annexe C, « Configuration de OpenSLP pour eDirectory », page 167.

De la même manière, lorsque vous désinstallez le paquetage SLP, vous devez arrêter SLP manuellement en entrant la commande suivante :

```
/etc/init.d/slpd stop
```

Si vous ne souhaitez (ou ne pouvez) pas utiliser SLP, vous pouvez utiliser le fichier plat `host.nds` pour résoudre les noms d'arborescence en adresses de renvoi du serveur. Le fichier `hosts.nds` peut être utilisé pour éviter les retards liés à la multidiffusion SLP lorsqu'un agent Annuaire SLP est absent du réseau.

`hosts.nds` est une table de recherche statique utilisée par les applications eDirectory pour effectuer des recherches dans les partitions et les serveurs de eDirectory. Dans le fichier `hosts.nds`, pour chaque arborescence ou serveur, une ligne unique contient les informations suivantes :

- Nom d'arborescence/du serveur : les noms d'arborescence se terminent par un point final (.).
- Adresse Internet :il peut s'agir d'un nom DNS ou d'une adresse IP.
- Port serveur : facultatif, ajouté à l'adresse Internet via le signe deux-points (:).

Le serveur local n'a pas besoin d'entrée dans ce fichier sauf s'il écoute sur un port NCP non défini par défaut.

La syntaxe adoptée dans le fichier `hosts.nds` se présente comme suit :

```
<[partition name.]tree name>.  <host-name/ip-addr>[:<port>] <server name>  <dns-
addr/ip-addr>[:<port>]
```

Par exemple :

```
# This is an example of a hosts.nds file:
# Tree name             Internet address/DNS Resolvable Name
  CORPORATE.            myserver.mycompany.com
  novell.CORPORATE.     1.2.3.4:524

# Server name           Internet address
  CORPSERVER            myserver.mycompany.com
```

Pour plus d'informations, reportez-vous à la page d'aide (man page) de `hosts.nds`.

Si vous choisissez d'utiliser SLP pour résoudre le nom d'arborescence afin de déterminer si l'arborescence eDirectory est diffusée après l'installation de eDirectory et de SLP, entrez la ligne suivante :

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==[treename or *])"
```

Par exemple, pour rechercher les services dont l'attribut `svcname-ws` correspond à la valeur `EXEMPLE_ARBORESCENCE`, entrez la commande suivante :

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==SAMPLE_TREE)/"
```

Si vous avez un service dont l'attribut `svcname-ws` est enregistré comme `EXEMPLE_ARBORESCENCE`, le résultat sera similaire au suivant :

```
service:ndap.novell:///SAMPLE_TREE
```

Si vous n'avez pas de service dont l'attribut `svcname-ws` est enregistré comme `EXEMPLE_ARBORESCENCE`, vous n'obtiendrez aucun résultat.

Pour plus d'informations, reportez-vous à la Annexe C, « Configuration de OpenSLP pour eDirectory », page 167.

## Exécution de l'utilitaire nds-install pour installer des composants eDirectory

L'utilitaire nds-install permet d'installer les composants eDirectory sur les systèmes Linux. Cet utilitaire se trouve dans le répertoire `d'installation` du fichier téléchargé de la plate-forme Linux. L'utilitaire ajoute les logiciels nécessaires en fonction des composants que vous avez décidé d'installer.

1. Entrez la commande suivante au niveau du répertoire d'installation :

   ```
   ./nds-install
   ```

   Si vous n'indiquez pas les paramètres obligatoires sur la ligne de commande, l'utilitaire nds-install vous invite à les saisir.

   Le tableau suivant décrit les paramètres de l'utilitaire nds-install :

| Paramètre nds-install | Description |
|---|---|
| `-h` ou `--help` | Affiche l'aide de nds-install. |
| `-i` | Empêche le script nds-install d'appeler la commande `ndsconfig upgrade` si une DIB est détectée au moment de la mise à niveau. |
| `-j` | Ignore l'option de vérification de l'état de santé avant d'installer eDirectory. Pour plus d'informations sur les vérifications de l'état de santé, reportez-vous à l'Annexe B, « Vérifications de l'état de santé de eDirectory », page 161. |
| `-m` | Nom du module à configurer. Lors de la configuration d'une nouvelle arborescence, vous ne pouvez configurer que le module ds. Une fois le module ds configuré, vous pouvez ajouter les services NMAS, LDAP, SAS, SNMP, HTTP et NetIQ SecretStore (ss) à l'aide de la commande `add`. Si vous n'indiquez pas le nom du module, tous les modules sont installés. |
| `-u` | Option pour l'utilisation d'un mode d'installation sans surveillance. |
| `-f` | Option servant à forcer la mise à niveau vers une version ultérieure/antérieure vers n'importe quelle version d'eDirectory. |

Le programme d'installation installe les RPM suivants :

| Composant eDirectory | Logiciels installés | Description |
|---|---|---|
| Serveur eDirectory | ◆ novell-NDSbase<br>◆ novell-NDScommon<br>◆ novell-NDSmasv<br>◆ novell-NDSserv<br>◆ novell-NDSimon<br>◆ novell-NDSrepair<br>◆ novell-NDSdexvnt<br>◆ novell-NOVLsubag<br>◆ novell-NOVLsnmp<br>◆ novell-NOVLpkit<br>◆ novell-NOVLpkis<br>◆ novell-NOVLpkia<br>◆ novell-NOVLembox<br>◆ novell-NOVLlmgnt<br>◆ novell-NOVLxis<br>◆ novell-NLDAPsdk<br>◆ novell-NLDAPbase<br>◆ novell-NOVLsas<br>◆ novell-NOVLntls<br>◆ novell-NOVLnmas<br>◆ novell-NOVLldif2dib<br>◆ novell-NOVLncp<br>◆ novell-eba | Le serveur de répliques eDirectory est installé sur le serveur indiqué. |
| Utilitaires d'administration | ◆ novell-NOVLice<br>◆ novell-NDSbase<br>◆ novell-NLDAPbase<br>◆ novell-NLDAPsdk<br>◆ novell-NOVLpkia<br>◆ novell-NOVLxis<br>◆ novell-NOVLlmgnt | L'utilitaire d'importation, de conversion et d'exportation NetIQ ainsi que l'utilitaire d'administration des outils LDAP sont installés sur le poste de travail indiqué. |

**2** À l'invite du système, entrez le chemin d'accès complet au fichier de licence.

Le système vous invite à entrer le chemin d'accès complet au fichier de licence uniquement si le programme d'installation ne trouve pas le fichier à l'emplacement par défaut. L'emplacement par défaut est le répertoire `/var`, la disquette de licence montée ou le répertoire actuel.

Si le chemin d'accès saisi n'est pas valide, vous êtes invité à saisir le chemin d'accès correct.

**3** Une fois l'installation terminée, mettez à jour et exportez les variables d'environnement suivantes pour employer les utilitaires eDirectory pendant la session en cours :

```
export PATH=$PATH opt/novell/eDirectory/bin opt/novell/eDirectory/sbin
```

```
export MANPATH=$MANPATH opt/novell/man opt/novell/eDirectory/man

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/locale
```

L'utilitaire ndsconfig permet de configurer le serveur eDirectory après l'installation.

NMAS (NetIQ Modular Authentication Service) est installé conjointement avec le composant serveur. Par défaut, l'utilitaire ndsconfig configure NMAS. L'utilitaire nmasinst permet aussi de configurer le serveur NMAS après l'installation. Cette opération doit être réalisée après la configuration de eDirectory à l'aide de ndsconfig.

Par défaut, le serveur eDirectory s'exécute en mode FIPS. Pour désactiver le mode FIPS, transmettez `n4u.server.fips_tls=0` avec la commande `ndsconfig set`, puis redémarrez le serveur. Par exemple, `ndsconfig set n4u.server.fips_tls=0`.

Lorsque le mode FIPS est activé dans votre environnement eDirectory, toutes les applications et tous les modules eDirectory utilisant OpenSSL utilisent toujours OpenSSL en mode FIPS. Le fonctionnement d'eDirectory en mode FIPS n'autorise pas les communications sur SSLv3 et limite l'utilisation du chiffrement aux chiffrements forts. Pour plus d'informations, reportez-vous aux sections Configuration des objets LDAP et Configuration de l'objet Serveur HTTP du *Guide d'administration de NetIQ eDirectory*.

Pour plus d'informations sur l'utilitaire ndsconfig, reportez-vous à la section « Utilitaire ndsconfig » page 127.

Pour plus d'informations sur l'utilitaire nmasinst, reportez-vous à la section « Exécution de l'utilitaire nmasinst pour configurer NMAS » page 53.

---

**REMARQUE :** après avoir installé eDirectory, NetIQ vous recommande de ne pas inclure le répertoire DIB (présent sur votre serveur eDirectory) dans des processus liés à l'exécution d'antivirus ou de logiciels de sauvegarde. Utilisez l'outil de sauvegarde eDirectory pour sauvegarder votre répertoire DIB.

Pour plus d'informations sur la sauvegarde de eDirectory, consultez la section « Sauvegarder et restaurer NetIQ eDirectory » du *Guide d'administration NetIQ eDirectory* .

---

# Installation d'eDirectory 9.2 par un utilisateur non-root

Un utilisateur non-root peut installer eDirectory 9.2 à l'aide du tarball.

## Conditions préalables

- ❒ Si vous souhaitez installer eDirectory à l'aide du tarball plutôt qu'avec l'utilitaire nds-install, assurez-vous que NICI est installé. Pour plus d'informations sur l'installation de NICI, reportez-vous à la section « Installation de l'infrastructure NICI » page 37.
- ❒ Vérifiez que le sous-agent SNMP est installé en utilisant la commande `rpm --nodeps <chemin du rpm du sous-agent snmp>`.
- ❒ Si vous souhaitez utiliser SLP et SNMP, vérifiez qu'ils ont été installés par l'utilisateur root.
- ❒ Vous devez disposer de droits d'écriture sur le répertoire dans lequel vous souhaitez installer eDirectory.

  Si vous ne disposez pas des droits d'administrateur, vérifiez que vous jouissez des droits appropriés tels que mentionnés à la section « Conditions préalables » page 23.

## Installation de l’infrastructure NICI

NICI doit être installé avant eDirectory. Étant donné que les paquetages NICI requis sont utilisés sur l’ensemble du système, nous vous recommandons d’utiliser l’utilisateur root pour installer les paquetages nécessaires.

Avec eDirectory 9.2, les applications 32 et 64 bits peuvent coexister au sein d'un même système.

### Installation de NICI par un utilisateur root

Pour installer NICI 64 bits, entrez la commande suivante :

```
rpm -ivh chemin_absolu_RPM_NICI/nici64-3.2.0-0.00.x86_64.rpm
```

Pour vous assurer que NICI est défini en mode serveur, entrez la commande suivante en tant qu'utilisateur root :

```
/var/opt/novell/nici/set_server_mode64
```

## Configuration du service utilisateur sous SLES 12 ou version ultérieure

Pour prendre en charge les services d'utilisateurs non-root sur ces plates-formes, démarrez le système `systemd` spécifique de l'utilisateur (cette opération ne doit être réalisée qu'une seule fois).

Les avantages de démarrage des services en tant qu'utilisateur non-root sont les suivants :

- Un administrateur système peut contrôler un service.
- L'ordinateur démarre le service au redémarrage.

Pour démarrer le système `systemd` spécifique à un utilisateur, exécutez la commande suivante :

```
systemctl start user@<uid>.service
```

où `uid` est l'ID utilisateur.

Par exemple, `systemctl start user@1001.service`

Pour activer l'instance utilisateur `systemd` persistante, exécutez la commande suivante :

```
loginctl enable-linger user
```

---

**REMARQUE :** si vous déplacez `datadir` vers un nouvel emplacement après avoir configuré eDirectory sur SLES 12 ou version ultérieure, procédez comme suit :

- Mettez à jour le nouvel emplacement du fichier `ndsd.pid` dans le fichier de service qui se trouve dans l'emplacement `/usr/lib/systemd/system/`.

  Par exemple, si le fichier `nds.conf` se trouve dans `/etc/opt/novell/eDirectory`, un exemple de fichier de service est créé comme ci-dessous :

  `/usr/lib/systemd/system/ndsdtmpl-etc-opt-novell-eDirectory-conf-ds.conf@.service`.
- Rechargez le daemon à l'aide de la commande `systemctl daemon-reload`.
- Redémarrez le serveur eDirectory.

---

## Installation de eDirectory

1 Accédez au répertoire dans lequel vous souhaitez installer eDirectory.

2 Désarchivez le fichier tar comme suit :

```
tar xvf /tar_file_name
```

Les répertoires `etc`, `opt` et `var` sont créés.

3 Exportez les chemins comme suit :

- **Exportez manuellement les variables d'environnement en entrant les commandes suivantes :**

```
export LD_LIBRARY_PATH=custom_location/eDirectory/opt/novell/eDirectory/
lib64:custom_location/eDirectory/opt/novell/eDirectory/lib64/nds-
modules:custom_location/eDirectory/opt/novell/lib64:$LD_LIBRARY_PATH
```

```
export PATH=custom_location/eDirectory/opt/novell/eDirectory/
bin:custom_location/eDirectory/opt/novell/eDirectory/sbin:/opt/novell/
eDirectory/bin:$PATH
```

```
export MANPATH=custom_location/eDirectory/opt/novell/man:custom_location/
eDirectory/opt/novell/eDirectory/man:$MANPATH
```

```
export TEXTDOMAINDIR=custom_location/eDirectory/opt/novell/eDirectory/
share/locale:$TEXTDOMAINDIR
```

**Utilisez le script ndspath pour exporter les variables d'environnement en procédant comme suit :**

Si vous ne voulez pas exporter les chemins manuellement, préfixez le script ndspath sur l'utilitaire.

- Exécutez l'utilitaire voulu comme suit :

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

- Exportez les chemins dans le shell actuel comme suit :

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

---

**REMARQUE :** Veillez à entrer les commandes ci-dessus au niveau du répertoire *emplacement_personnalisé*/eDirectory/opt.

---

Après avoir entré les commandes 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.

4 Configurez eDirectory comme d'habitude.

Vous pouvez configurer eDirectory selon l'une des manières suivantes :

- Exécutez l'utilitaire ndsconfig comme suit :

```
ndsconfig new [-t <treename>] [-n <server_context>] [-a <admin_FDN>] [-w
<admin password>] [-i] [-S <server_name>] [-d <path_for_dib>] [-m <module>]
[e] [-L <ldap_port>] [-l <SSL_port>] [-o <http_port>] -O <https_port>] [-p
<IP address:[port]>] [-c] [-b <port_to_bind>] [-B <interface1@port1>,
<interface2@port2>,..] [-D <custom_location>] [--config-file
<configuration_file>] [--configure-eba-now <yes/no>]
```

Par exemple :

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /home/
mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/mary/
inst1/var --config-file /home/mary/inst1/nds.conf --configure-eba-now yes
```

Les numéros de port entrés doivent être compris entre 1 024 et 65 535. Ceux inférieurs à 1 024 sont normalement réservés à l'utilisateur privilégié et aux applications standard. Par conséquent, le port par défaut 524 ne peut pas être utilisé pour des applications eDirectory.

Les applications suivantes pourraient être interrompues :

- les applications ne permettant pas de spécifier le port du serveur cible ;
- les anciennes applications qui utilisent NCP et qui sont exécutées comme racine pour le port 524.

- Exécutez l'utilitaire ndsmanage pour configurer une nouvelle instance. Pour plus d'informations, consultez la « Création d'une instance via ndsmanage » page 49.

Pour activer l'authentification EBA, spécifiez *yes* pour le paramètre `--configure-eba-now` dans la commande ndsconfig upgrade. Dans le cas contraire, spécifiez *no* pour la configurer ultérieurement. Si vous ne transmettez pas le paramètre `--configure-eba-now` à la commande ndsconfig, eDirectory vous invite à indiquer votre choix. Par défaut, la configuration est définie sur `no`.

Suivez les instructions affichées pour terminer la configuration.

Pour plus d'informations, reportez-vous à la « Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques eDirectory » page 39.

---

**REMARQUE :** après avoir installé eDirectory, NetIQ vous recommande de ne pas inclure le répertoire DIB (présent sur votre serveur eDirectory) dans des processus liés à l'exécution d'antivirus ou de logiciels de sauvegarde. Utilisez l'outil de sauvegarde eDirectory pour sauvegarder votre répertoire DIB.

Pour plus d'informations sur la sauvegarde de eDirectory, consultez la section « Sauvegarder et restaurer NetIQ eDirectory » du *Guide d'administration NetIQ eDirectory* .

---

# Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques eDirectory

Après avoir installé eDirectory, configurez le serveur de répliques eDirectory à l'aide de l'utilitaire ndsconfig. Vous devez disposer de droits d'administrateur pour pouvoir exécuter l'utilitaire ndsconfig. Lorsque cet utilitaire est utilisé avec des arguments, il valide tous les arguments et invite l'utilisateur bénéficiant de droits Administrateur à entrer son mot de passe. Si l'utilitaire est utilisé sans arguments, ndsconfig affiche une description de l'utilitaire et des options disponibles. Vous pouvez également exécuter cet utilitaire pour supprimer le serveur de répliques eDirectory et modifier la configuration actuelle de l'objet Serveur eDirectory. Pour plus d'informations, reportez-vous à la « Utilitaire ndsconfig » page 127.

## Condition préalable pour la configuration de eDirectory dans des paramètres régionaux spécifiques

Si vous souhaitez configurer eDirectory dans des paramètres régionaux spécifiques, vous devez exporter au préalable LC_ALL et LANG vers ces paramètres donnés. Par exemple, pour configurer eDirectory dans des paramètres régionaux japonais, entrez la commande suivante :

```
export LC_ALL=ja
```

```
export LANG=ja
```

## Création d’une nouvelle arborescence

Utilisez la syntaxe suivante.

```
ndsconfig new [-m <modulename>] [-i] [-S <server name>] [-t <tree_name>] [-n
<server context>] [-d <path_for_dib>][-P <LDAP URL(s)>] [-L <ldap_port>] [-l
<ssl_port>] [-o http port] [-O https port] [-e] -a <admin FDN> [-R] [-c] [-w <admin
password>] [-b <port to bind>] [-B <interface1@port1, interface2@port2,..>] [-D
<path_for_data>] [--config-file <configuration file>] [--configure-eba-now <yes/
no>] [--pki-default-rsa-keysize <2048/4096/8192>] [--pki-default-ec-curve <P256/
P384/P521>] [--pki-default-cert-life <in years>]
```

Une nouvelle arborescence est installée avec les nom et contexte définis.

Le nombre de caractères des variables *nom_arborescence*, *FDN_admin* et *FDN_serveur* est limité. Le nombre maximum de caractères autorisé pour ces variables est le suivant :

- *nom_arborescence* : 32 caractères
- *FDN_admin* : 255 caractères
- *FND_serveur* : 255 caractères

---

**IMPORTANT :** bien qu'eDirectory permette de définir le FDN de l'objet Serveur NCP jusqu'à 256 caractères, NetIQ recommande de limiter la variable à une valeur bien inférieure étant donné qu'eDirectory crée d'autres objets de longueur supérieure en fonction de la longueur de cet objet.

---

Si vous n’avez défini aucun paramètre dans la ligne de commande, ndsconfig vous invite à saisir les valeurs de chaque paramètre manquant.

Vous pouvez également utiliser la syntaxe suivante :

```
ndsconfig def [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <admin
password>] [-c] [-i] [-S <server name>] [-d <path for dib>] [-m <module>] [-e] [-L
<ldap port>] [-l <SSL port>] [-o <http port>] [-O <https port>] [-D
<custom_location>] [--config-file <configuration_file>] [--configure-eba-now <yes/
no>]
```

Une nouvelle arborescence est installée avec les nom et contexte définis. Si vous n’avez défini aucun paramètre dans la ligne de commande, ndsconfig utilise les valeurs par défaut de chaque paramètre manquant.

Par exemple, pour créer une arborescence, vous pouvez entrer la commande suivante :

```
ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
```

---

**REMARQUE :** une nouvelle option nommée `--enable-pbkdf2` a été ajoutée à la commande `ndsconfig` dans eDirectory 9.2 lors de la création d'une arborescence. Si cette option est définie, une stratégie de mot de passe est créée et assignée automatiquement à l'ensemble de l'arborescence. Cette stratégie de mot de passe permet de synchroniser les mots de passe NDS avec les mots de passe PBKDF2 pour tous les utilisateurs de l'arborescence. Pour plus d'informations, reportez-vous à la section Présentation du stockage des mots de passe non réversibles dans le guide d'administration de NetIQ eDirectory.

---

### Spécification des paramètres par défaut pour les certificats de serveur par défaut

eDirectory offre la possibilité de spécifier la taille de la clé RSA par défaut, la courbe elliptique et la durée de vie des certificats de l'autorité de certification et des certificats de serveur par défaut lors de la configuration d'une nouvelle arborescence eDirectory. Vous pouvez utiliser les commandes suivantes pour spécifier les paramètres par défaut que les certificats de l'autorité de certification et les certificats de serveur par défaut doivent utiliser lors de la configuration d'une nouvelle arborescence eDirectory à l'aide la commande `ndsconfig new` :

- **pki-default-rsa-keysize :** permet de spécifier la taille de clé des certificats RSA. Les valeurs autorisées sont 2 048, 4 096 et 8 192 bits.
- **pki-default-ec-curve :** permet de spécifier la limite de courbe des certificats EC. Les valeurs autorisées sont P256, P384 et P521.
- **pki-default-cert-life :** permet de spécifier la durée de validité du certificat en nombre d'années.

Ces attributs peuvent être définis dans le cadre de la commande `ndsconfig new` pendant l'installation d'un nouveau serveur eDirectory.

Les valeurs spécifiées ici seront définies en fonction des attributs correspondants sur l'objet Autorité de certification organisationnelle lors de la configuration de la nouvelle arborescence.

Pour plus d'informations, reportez-vous à la section Création d'un objet Autorité de certification organisationnelle du *Guide d'administration de NetIQ eDirectory*.

## Ajout d’un serveur à une arborescence existante

Utilisez la syntaxe suivante.

```
ndsconfig add [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <admin
password>] [-e] [-P <LDAP URL(s)>][-L <ldap port>] [-l <SSL port>] [-o <http port>]
[-O <https port>] [-S <server name>] [-d <path for dib>] [-m <module>] [-p <IP
address:[port]>] [-R] [-c] [-b <port to bind>] [-B <interface1@port1>,
<interface2@port2>,..] [-D <custom_location>] [--config-file <configuration_file>]
[-E] [--configure-eba-now <yes/no>]
```

eDirectory ajoute un serveur à une arborescence existante dans le contexte spécifié. Si le contexte dans lequel l'utilisateur souhaite ajouter l'objet Serveur n'existe pas, ndsconfig le crée et ajoute le serveur.

Pour activer l'authentification EBA (Enhanced Background Authentication), spécifiez *yes* pour le paramètre `--configure-eba-now` dans la commande ndsconfig upgrade. Dans le cas contraire, spécifiez *no* pour la configurer ultérieurement. Si vous ne transmettez pas le paramètre `--configure-eba-now` à la commande ndsconfig, eDirectory vous invite à indiquer votre choix. Par défaut, la configuration est définie sur *no*.

Pour ajouter un serveur secondaire activé pour l'authentification EBA à l'arborescence, une autorité de certification EBA doit être configurée dans l'arborescence. Si aucune autorité de certification EBA n'est présente, commencez par ajouter le serveur sans activer l'authentification EBA, puis mettez à niveau le serveur pour qu'il héberge l'autorité de certification EBA. Dans le cas contraire, la configuration du serveur secondaire échoue.

Vous pouvez également ajouter des services LDAP et de sécurité une fois eDirectory installé dans l’arborescence existante.

Par exemple, pour ajouter un serveur à une arborescence existante, vous pouvez entrer la commande suivante :

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company -S srv1
```

L'option `-E` vous permet d'activer la réplication codée sur le serveur à ajouter. Pour plus d'informations sur la réplication codée, consultez la section « Réplication codée » du *Guide d'administration NetIQ eDirectory* .

## Suppression d'un objet Serveur et des services Annuaire d'une arborescence

Utilisez la syntaxe suivante.

```
ndsconfig rm [-a <admin FDN>] [-w <admin password>] [-p <IP address:[port]>] [-c]
```

eDirectory et sa base de données sont retirés du serveur.

---

**REMARQUE :** Les fichiers HTML créés à l'aide de iMonitor ne sont pas supprimés. Vous devez supprimer manuellement ces fichiers de `/var/opt/novell/eDirectory/data/dsreports` avant de supprimer eDirectory.

---

Par exemple, pour retirer l'objet Serveur eDirectory et les services Annuaire d'une arborescence, vous pouvez entrer la commande suivante :

```
ndsconfig rm -a cn=admin.o=company
```

## Paramètres de l'utilitaire ndsconfig

| Paramètre ndsconfig | Description |
|---|---|
| `nouveau` | Crée une arborescence eDirectory. Si vous n'avez défini aucun paramètre dans la ligne de commande, ndsconfig vous invite à saisir les valeurs de chaque paramètre manquant. |
| `def` | Crée une arborescence eDirectory. Si vous n'avez défini aucun paramètre dans la ligne de commande, ndsconfig utilise les valeurs par défaut de chaque paramètre manquant. |
| `ajouter` | Ajoute un serveur à une arborescence existante. Ajoute également les services LDAP et SAS après la configuration de eDirectory dans l'arborescence existante. |
| `rm` | Retire l'objet Serveur et les services Annuaire d'une arborescence.<br>**REMARQUE :** Cette option ne supprimer pas les objets matériels clés. Ces objets doivent être supprimés manuellement. |
| `mettre à niveau` | Met à niveau eDirectory vers une version ultérieure. |
| `-i` | Lors de la configuration d'une nouvelle arborescence, cette option permet de ne pas rechercher l'existence éventuelle d'une arborescence portant le même nom. Plusieurs arborescences portant le même nom peuvent coexister. |

| Paramètre ndsconfig | Description |
|---|---|
| `-S` *`nom_serveur`* | Nom du serveur. Ce nom peut également contenir des points (par exemple, netiq.com). Étant donné que ndsconfig est un utilitaire de ligne de commande, les points de ces noms exigent l'utilisation de caractères d'échappement et les paramètres qui contiennent ces contextes doivent être mis entre guillemets droits.<br><br>Par exemple, pour installer une nouvelle arborescence eDirectory sur un serveur Linux avec `netiq.com` en tant que nom du paramètre O, utilisez la commande suivante :<br><br>`ndsconfig new -a "admin.novell\\.com" -t netiq_tree -n "OU=servers.O=netiq\\.com"`<br><br>Le nom et contexte Admin et les paramètres de contexte du serveur sont entre guillemets, et seul le point ('.') de `netiq.com` est précédé d'une barre oblique inverse ('\') utilisée comme caractère d'échappement. Vous pouvez également utiliser ce format lorsque vous installez un serveur dans une arborescence existante.<br><br>**REMARQUE :** Un nom ne peut pas commencer par un point. Par exemple, vous ne pouvez pas installer un serveur appelé « .novell », car ce nom commence par un point (« . »). |
| `-t` *`nom_arborescence`* | Nom de l'arborescence à laquelle le serveur doit être ajouté. Il peut contenir un maximum de 32 caractères. S'il n'est pas spécifié, ndsconfig utilise le nom d'arborescence du paramètre `n4u.nds.tree-name` défini dans le fichier `/etc/opt/novell/eDirectory/conf/nds.conf`. Le nom d'arborescence par défaut est `$LOGNAME-$HOSTNAME-NDStree`. |
| `-n` *`contexte_serveur`* | Contexte du serveur auquel l'objet Serveur est ajouté. Il peut contenir un maximum de 64 caractères. Si le contexte n'est pas spécifié, ndsconfig utilise le contexte du paramètre de configuration `n4u.nds.server-context` défini dans le fichier `/etc/opt/novell/eDirectory/conf/nds.conf`. Le contexte de serveur doit être spécifié sous la forme d'un nom avec type. Le contexte par défaut est `org`. |
| `-d` *`chemin_de_DIB`* | Chemin d'accès au répertoire où les fichiers de base de données seront stockés. |
| `-r` | Cette option ajoute de force la réplique du serveur, quel que soit le nombre de serveurs déjà ajoutés au serveur. |
| `-L` *`port_ldap`* | Numéro du port TCP sur le serveur LDAP. Si le port par défaut 389 est déjà utilisé, vous êtes invité à indiquer un autre numéro de port. |
| `-l` *`port_ssl`* | Numéro du port SSL sur le serveur LDAP. Si le port par défaut 636 est déjà utilisé, vous êtes invité à indiquer un autre numéro de port. |
| `-a` *`FDN_admin`* | Nom distinctif complet de l'objet Utilisateur disposant des droits Superviseur sur le contexte dans lequel l'objet Serveur et les services Annuaire doivent être créés. Le nom admin doit être spécifié sous la forme d'un nom avec type. Il peut contenir un maximum de 64 caractères. Le nom par défaut est admin.org. |
| `-e` | Active les mots de passe en texte clair pour les objets LDAP. |

| Paramètre ndsconfig | Description |
|---|---|
| `-m` *`nom_module`* | Nom du module à configurer. Lors de la configuration d'une nouvelle arborescence, vous ne pouvez configurer que le module ds. Une fois le module ds configuré, vous pouvez ajouter les services NMAS, LDAP, SAS, SNMP, HTTP et NetIQ SecretStore (ss) à l'aide de la commande `add`. Si vous n'indiquez pas le nom du module, tous les modules sont installés.<br><br>**REMARQUE :** Si vous ne voulez pas configurer le SecretStore pendant la mise à niveau de eDirectory avec la commande `nds-install`, définissez la valeur `no_ss` sur cette option. Par exemple, `nds-install '-m no_ss'`. |
| `-o` | Indique le numéro de port en texte clair HTTP. |
| `-O` | Numéro de port sécurisé HTTP. |
| `-p` *`<Adresse_IP:[port]>`* | Cette option est utilisée pour ajouter un serveur secondaire (commande `add`) à une arborescence. Elle spécifie l'adresse IP de l'hôte distant qui contient une réplique de la partition à laquelle ce serveur est ajouté. Le numéro de port par défaut est 524. Cela permet de faire des recherches plus rapides de l'arborescence en évitant la recherche SLP. |
| `-R` | Par défaut, une réplique de la partition à laquelle est ajouté le serveur sera répliquée vers le serveur local. Cette option désactive l'ajout de répliques au serveur local. |
| `-c` | Cette option évite d'avoir des invites pendant l'opération ndsconfig, comme oui/non pour continuer l'opération, ou une invite pour ressaisir les numéros de port quand il y a un conflit, etc. L'utilisateur reçoit des invites uniquement pour ressaisir des paramètres obligatoires s'ils ne sont pas passés sur la ligne de commande. |
| `-w` *`<mot de passe admin>`* | Cette option permet de passer le mot de passe de l'utilisateur administrateur en texte clair.<br><br>**REMARQUE :** Comme le mot de passe est en texte clair, cela n'est pas une option de sécurité recommandée en raison du niveau élevé d'insécurité du mot de passe. |
| `-E` | Active la réplication codée pour le serveur que vous tentez d'ajouter. |
| `-j` | Ignore l'option de vérification de l'état de santé avant d'installer eDirectory. |
| `-b` *`port_à_connecter`* | Définit le numéro de port par défaut sur lequel une instance spécifique doit écouter. Cette commande définit le numéro de port par défaut sur les suivants : `n4u.server.tcp-port` et `n4u.server.udp-port`. Si un port NCP est renvoyé à l'aide de l'option `-b`, il est considéré comme le port par défaut et les paramètres TCP et UDP sont mis à jour en conséquence.<br><br>**REMARQUE :** Seuls `-b` et `-B` sont utilisés. |
| `-B` *`interface1@port1, interface2@port2,...`* | Indique le numéro de port ainsi que l'interface ou l'adresse IP. Par exemple :<br><br>`-B eth0@524`<br><br>ou<br><br>`-B 100.1.1.2@524`<br><br>**REMARQUE :** `-b` et `-B` s'excluent mutuellement. |
| `--config-file` *`fichier_configuration`* | Indiquez 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/`, entrez `--config-file /etc/opt/novell/eDirectory/nds.conf`. |

| Paramètre ndsconfig | Description |
|---|---|
| `-P <URL(s) LDAP>` | Permet aux URL LDAP de configurer l'interface LDAP sur l'objet Serveur LDAP.<br>Par exemple : `-P ldap://1.2.3.4:1389,ldaps://1.2.3.4:1636` |
| `-D chemin_des_données` | Crée le répertoire `DIB` ainsi que les répertoires des `journaux` et `données` dans le chemin mentionné. |
| `set liste_valeurs` | Définit la valeur des paramètres eDirectory configurables spécifiés. Cette option permet de définir les paramètres d'amorçage avant de configurer une arborescence. Lors de la modification de paramètres de configuration, ndsd doit être redémarré pour que les nouvelles valeurs soient prises en compte. Toutefois, certains paramètres de configuration ne nécessitent pas le redémarrage de ndsd.<br>Ces paramètres sont les suivants :<br>◆ `n4u.nds.inactivity-synchronization-interval`<br>◆ `n4u.nds.synchronization-restrictions`<br>◆ `n4u.nds.janitor-interval`<br>◆ `n4u.nds.backlink-interval`<br>◆ `n4u.nds.drl-interval`<br>◆ `n4u.nds.flatcleaning-interval`<br>◆ `n4u.nds.server-state-up-threshold`<br>◆ `n4u.nds.heartbeat-schema`<br>◆ `n4u.nds.heartbeat-data`<br>◆ `n4u.server.fips_tls`<br>◆ `n4u.server.eba_enabled` |
| `get help liste_paramètres` | Permet d'afficher les chaînes d'aide relatives aux paramètres eDirectory configurables qui ont été spécifiés. Si la liste des paramètres n'est pas spécifiée, ndsconfig liste les chaînes d'aide pour tous les paramètres eDirectory configurables. |
| `set liste_valeurs` | Définit la valeur des paramètres eDirectory configurables spécifiés. Cette option permet de définir les paramètres d'amorçage avant de configurer une arborescence.<br>Lors de la modification de paramètres de configuration, ndsd doit être redémarré pour que les nouvelles valeurs soient prises en compte. |
| `get liste_paramètres` | Permet d'afficher la valeur actuelle des paramètres eDirectory configurables qui ont été spécifiés. Si la liste des paramètres n'est pas spécifiée, ndsconfig liste tous les paramètres eDirectory configurables. |
| `configure-eba-now` | Utilisez ce paramètre pour configurer votre serveur eDirectory pour l'authentification EBA. |

# Utilisation de ndsconfig pour configurer plusieurs instances d'eDirectory 9.2

Vous pouvez configurer plusieurs instances d'eDirectory 9.2 sur un hôte unique. Désormais, grâce à la fonction d'instances multiples prise en charge par eDirectory 9.2, vous pouvez configurer les éléments suivants :

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

---

**AVERTISSEMENT :** la configuration de plusieurs arborescences pour le même utilisateur n'est pas prise en charge. NetIQ ne prend pas en charge les instances des serveurs dans différentes arborescences pour un utilisateur. Si vous souhaitez configurer des serveurs dans plusieurs arborescences, utilisez des comptes utilisateur différents.

---

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

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

La méthode de configuration de plusieurs instances est similaire à celle utilisée pour configurer une instance unique plusieurs fois. Chaque instance doit avoir des identificateurs d'instance qui lui sont propres tels que :

- Des données et un emplacement de fichier journal différents

  Pour ce faire, vous pouvez utiliser les options de ndsconfig `--config-file`, `-d` et `-D`.
- Un numéro de port unique sur lequel l'instance écoute

  Pour ce faire, vous pouvez utiliser les options de ndsconfig `-b` et `-B`.
- Un nom de serveur unique pour l'instance

  Vous pouvez utiliser l'option ndsconfig -S nom_serveur pour y procéder.

  ---

  **IMPORTANT :** Pendant la configuration de eDirectory, le nom de serveur NCP par défaut est défini comme nom du serveur hôte. Lorsque vous configurez plusieurs instances, vous devez modifier le nom du serveur NCP. Utilisez l'option de la ligne de commande `ndsconfig`, `-S <nom_serveur>` pour indiquer un nom de serveur différent.

  Lorsque vous configurez plusieurs instances, sur la même arborescence ou sur des arborescences différentes, le nom du serveur NCP doit être unique.

  ---

## 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.

## 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.

## Utilisation d'instances multiples

eDirectory 9.2 permet de configurer très facilement plusieurs instances. Pour pouvoir effectivement utiliser plusieurs instances, vous devez planifier la configuration, puis configurer les différentes instances.


- « Planification de la configuration » page 51
- « Configuration d'instances multiples » page 48


### 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 LDAP, LDAPS, HTTP et HTTP sécurisé) ;
- Nom de serveur unique pour chaque instance.

### 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`.<br><br>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.<br><br>**REMARQUE :** Seuls `-b` et `-B` sont utilisés. |
| -B | Indique le numéro de port ainsi que l'interface ou l'adresse IP. Par exemple :<br><br>`-B eth0@524`<br><br>ou<br><br>`-B 100.1.1.2@524`<br><br>**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 49.

## Gestion d'instances multiples

Cette section présente les informations suivantes :



### 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 2-1*** *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.

## Création d'une instance via ndsmanage

Pour créer une instance via ndsmanage :

1. Saisissez la commande suivante :

   ```
   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 :

Hormis les opérations répertoriées ci-dessous, 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 2-1*** *Écran de sortie de l'utilitaire ndsmanage avec options d'instance*

```
Les instances suivantes sont configurées par root

[1] /etc/opt/novell/eDirectory/conf/nds.conf : .LINUXS.ORG.TREE. : 10.20.118.76@524 : ACTIF

[2] /tmp/tree22.conf : .FREDS.ORG.TREE22. : 10.20.118.76@1524 : ACTIF

Entrée [r] pour rafraîchir la liste, [1 - 2] pour plus d'options, [c] pour créer une instance Ou [q] pour quitter : 1

INSTANCE SÉLECTIONNÉE :
[1] /etc/opt/novell/eDirectory/conf/nds.conf : .LINUXS.ORG.TREE. : 10.20.118.76@524 : ACTIF

[l] Lister les répliques sur le serveur
[s] Démarrer l'instance
[k] Arrêter l'instance
[t] Exécuter ndstrace
[d] Annuler la configuration
[b] Retour au menu précédent
[q] Quitter

Que voulez-vous faire de cette instance ? [Choisissez parmi les options susmentionnées] :
```

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 50).

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 50).

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 49.

## 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.

## 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
```

# Exemple de scénario pour des instances multiples

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

## 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` |

## 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
```

## 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.

## 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
  ```

# Utilisation de ndsconfig pour installer un serveur Linux dans une arborescence dont les noms de conteneur utilisent des points

ndsconfig permet d'installer un serveur Linux dans une arborescence eDirectory qui comporte des conteneurs dont le nom utilise la notation à point (par exemple, novell.com).

Étant donné que ndsconfig est un utilitaire de ligne de commande, les points de ces noms exigent l'utilisation de caractères d'échappement et les paramètres qui contiennent ces contextes doivent être mis entre guillemets droits. Par exemple, pour installer une nouvelle arborescence eDirectory sur un serveur Linux avec « O=netiq.com » en tant que nom du paramètre O, utilisez la commande suivante :

```
ndsconfig new -a 'admin.netiq.com' -t netiq_tree -n 'OU=servers.O=netiq.com'
```

Le nom et le contexte Admin ainsi que les paramètres de contexte du serveur sont mis entre guillemets et seul le point ('.') de novell.com est précédé d'une barre oblique inverse ('\') utilisée comme caractère d'échappement.

Vous pouvez également utiliser ce format lorsque vous installez un serveur dans une arborescence existante.

---

**REMARQUE :** Il convient d'utiliser ce format lors de la saisie du nom et du contexte Admin utilisant la notation à point avec des utilitaires tels que DSRepair, Backup, DSMerge, DSLogin et ldapconfig.

---

# Exécution de l'utilitaire nmasinst pour configurer NMAS

Par défaut, l'utilitaire ndsconfig configure NMAS. Vous pouvez également utiliser nmasinst pour configurer NMAS.

ndsconfig se charge uniquement de la configuration de NMAS ; il n'effectue pas l'installation des méthodes de connexion. Pour installer ces dernières, vous pouvez utiliser nmasinst.

---

**IMPORTANT :** Vous devez configurer eDirectory à l'aide de l'utilitaire ndsconfig avant d'installer les méthodes de connexion NMAS. Vous devez également disposer de droits d'administrateur sur l'arborescence.

---


- « Configuration de NMAS » page 53
- « Installation des méthodes de connexion » page 54


## Configuration de NMAS

Par défaut, l'utilitaire ndsconfig configure NMAS. Cependant, vous pouvez aussi utiliser l'utilitaire nmasinst.

Pour configurer NMAS et créer des objets NMAS dans eDirectory, entrez la commande suivante au niveau de la ligne de commande de la console du serveur :

```
nmasinst -i admin.context tree_name
```

nmasinst vous invite à indiquer votre mot de passe.

Cette commande crée les objets dans le conteneur Sécurité requis par NMAS et installe les extensions LDAP de NMAS dans l'objet Serveur LDAP de eDirectory.

Lorsqu'il est installé pour la première fois dans une arborescence, NMAS doit être déployé par un utilisateur disposant de droits suffisants pour créer des objets dans le conteneur Sécurité. Toutefois, les installations suivantes peuvent être réalisées par des administrateurs de conteneurs disposant de droits de lecture seule sur le conteneur Sécurité. nmasinst vérifie alors que les objets NMAS existent dans le conteneur Sécurité avant d'essayer de les créer.

nmasinst n'étend pas le schéma. Le schéma NMAS est installé en tant que composante du schéma eDirectory de base.

### Installation des méthodes de connexion

Pour installer les méthodes de connexion à l'aide de nmasinst, entrez la commande suivante sur la ligne de commande de la console du serveur :

```
nmasinst -addmethod admin.context tree_name config.txt_path
```

Le dernier paramètre spécifie le fichier `config.txt` de la méthode de connexion à installer. Un fichier `config.txt` est fourni avec chaque méthode de connexion.

Voici un exemple de commande `-addmethod` :

```
nmasinst -addmethod admin.netiq MY_TREE ./nmas-methods/novell/Simple Password/
config.txt
```

Si la méthode de connexion existe déjà, nmasinst la mettra à jour.

Pour plus d'informations, reportez-vous à la section Gestion de la connexion, méthodes de post-connexion et séquences du Guide d'administration de NetIQ eDirectory.

## Configuration de SNMP par un utilisateur non-root

`NICI` et `NOVLsubag` doivent être installés comme utilisateur root.

1. Installation de `NICI` par un utilisateur root. Reportez-vous à la section « Installation de NICI par un utilisateur root » page 37
2. Installation de `NOVLsubag` par un utilisateur root.

   Pour installer `NOVLsubag`, procédez comme suit :

   Saisissez la commande suivante :

   ```
   rpm -ivh --nodeps NOVLsubag_rpm_file_name_with_path
   ```

   Par exemple :

   ```
   rpm -ivh --nodeps novell-novell-NOVLsubag-9.2.0-0.x86_64.rpm
   ```

3. Exportez les chemins comme suit :

   Exportez manuellement les variables d'environnement.

   ```
   export LD_LIBRARY_PATH=custom_location/opt/novell/eDirectory/lib64:/opt/
   novell/eDirectory/lib64/nds-modules:/opt/novell/lib64:$LD_LIBRARY_PATH
   ```

   ```
   export   PATH=/opt/novell/eDirectory/bin:$PATH
   ```

   ```
   export MANPATH=/opt/novell/man:$MANPATH
   ```

# Localisation des fichiers journaux

## ndsd.log

Le fichier journal `ndsd.log` contient des informations sur les messages relatifs au serveur eDirectory, tels que les messages d'arrêt et de démarrage, généraux et propres aux services PKI et LDAP. Il se trouve par défaut dans le répertoire `/var/opt/novell/eDirectory/log`.

Vous pouvez augmenter le niveau de débogage du fichier `ndsd.log` en modifiant la variable suivante dans le fichier `nds.conf` du fichier `/etc/opt/novell/eDirectory/conf/nds.conf` .

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

Pour plus d'informations sur les niveaux des journaux ndsd, reportez-vous à la section Gestion de la consignation des erreurs dans eDirectory.

## Spécification de la taille du fichier journal sous Linux

Pour indiquer la taille du fichier journal, utilisez le paramètre `n4u.server.log-file-size` dans le fichier `nds.conf`. La taille maximale est de 2 Go et la valeur par défaut de 1 Mo. Vous pouvez toutefois également spécifier une taille de fichier inférieure à 1 Mo.

Ce paramètre ne s'applique pas au fichier `ndsd.log`.

Si la taille du fichier journal atteint la limite spécifiée, l'outil de consignation écrase le fichier journal à partir du début.

# 3 Installation ou mise à niveau de NetIQ eDirectory sous Windows

Les informations suivantes permettent d'installer ou de mettre à niveau NetIQ eDirectory 9.2 sur une plate-forme Windows :



**IMPORTANT :** NetIQ eDirectory 9.2 permet d'installer eDirectory pour Windows sans le client Novell. Si vous installez eDirectory 9.2 sur un ordinateur qui contient déjà le client Novell, eDirectory utilise le client existant. Pour plus d'informations, reportez-vous à la « Installation ou mise à niveau d'eDirectory 9.2 sur un serveur Windows » page 62.

## Configuration système requise

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

- Windows Server 2016 au minimum et Windows Server 2019

**IMPORTANT :** les versions bureau de Windows ne sont pas prises en charge.

eDirectory requiert également les éléments suivants :

Pour obtenir les dernières informations à propos de la configuration système requise, consultez les Notes de version.

- Une adresse IP assignée.
- Des droits d'administrateur sur le serveur Windows et sur toutes les portions de l'arborescence eDirectory qui contiennent des objets Utilisateur reconnaissant le domaine. Pour procéder à l'installation dans une arborescence existante, vous devez disposer de droits d'administrateur sur l'objet Arborescence afin de pouvoir étendre le schéma et créer des objets.

Reportez-vous aux exigences matérielles recommandées de l'OS pour votre serveur Windows.

# Conditions préalables

**IMPORTANT :** avant de mettre à niveau votre environnement eDirectory existant, assurez-vous que les applications NetIQ et tierces installées assurent la prise en charge d'eDirectory 9.2. Vous pouvez consulter l'état actuel des produits NetIQ dans le document TID 7003446 (http://www.novell.com/support/kb/doc.php?id=7003446). Il est également vivement recommandé de sauvegarder eDirectory avant toute mise à niveau.

- ❒ Dans la mesure où NTFS offre un processus de transaction plus sécurisé qu'un système de fichiers FAT, vous ne pouvez installer eDirectory que sur une partition NTFS. Ainsi, si vous disposez uniquement de systèmes de fichiers FAT, effectuez l'une des opérations suivantes :
  - Créez une partition et attribuez-lui le format NTFS.

    Utilisez l'Administrateur de disques. Pour plus d'informations, reportez-vous à la documentation Windows Server.
  - Convertissez un système de fichiers FAT existant au format NTFS à l'aide de la commande `CONVERT`.

    Pour plus d'informations, reportez-vous à la documentation Windows Server.

  Si votre serveur n'utilise que le système de fichiers FAT et que vous omettiez ce processus, le programme d'installation vous demande de fournir une partition NTFS.
- ❒ (Conditionnel) NICI 3.2 et eDirectory 9.2 prennent en charge les tailles de clé jusqu'à 8 192 bits pour le chiffrement RSA. Si vous souhaitez utiliser une taille de clé de 8 kilobits, chaque serveur doit être mis à niveau vers eDirectory 9.2. De plus, NICI 3.2 doit être installé sur chaque poste de travail qui utilise les utilitaires de gestion, par exemple iManager.

  Lorsque vous mettez à niveau votre serveur d'autorité de certification (CA) vers eDirectory 9.2, la taille de clé reste inchangée (2 kilobits). La seule façon de créer une taille de clé de 8 kilobits est de recréer l'autorité de certification sur un serveur eDirectory 9.2. En outre, vous devrez remplacer la taille de clé par défaut (2 kilobits) par 8 kilobits lors de la création de l'autorité de certification.

  **REMARQUE :** le programme d'installation en mode silencieux Windows nécessite que NICI 3.2 soit installé sur le système.
- ❒ Si vous effectuez une mise à niveau vers eDirectory 9.2, vérifiez que les derniers correctifs d'eDirectory sont installés sur tous les serveurs de l'arborescence autres que les serveurs eDirectory 9.2. Ces correctifs sont disponibles sur le site Web du support NetIQ (http://support.novell.com).
- ❒ La version 4.0 de .NET Management Framework ou une version ultérieure est requise.
- ❒ Vérifiez que les derniers Service Packs de Windows 2012 R2 sont installés. Le dernier Service Pack Windows mis à jour doit être installé après l'installation du service SNMP Windows.
- ❒ Si vous effectuez une mise à niveau à partir d'une version antérieure d'eDirectory, il doit s'agir au moins de la version 8.8.8.x ou d'une version ultérieure. Pour plus d'informations sur la détermination de la version d'eDirectory, reportez-vous à la section « Détermination de la version d'eDirectory » page 60.
- ❒ (Conditionnel) Si vous vous installez un serveur secondaire dans une arborescence existante sans posséder de droits d'administration d'eDirectory , vérifiez que vous disposez des droits suivants :
  - Droits Superviseur sur le conteneur dans lequel le serveur est installé ;
  - Droits Superviseur sur la partition dans laquelle ajouter le serveur.

**REMARQUE :** s'il existe moins de 3 répliques, ces droits sont obligatoires pour pouvoir en ajouter une.

- tous les droits d'attributs : droits de lecture, de comparaison et d'écriture sur l'objet W0.KAP.Security ;
- droits d'entrée : droits d'exploration sur l'objet Conteneur de sécurité ;
- tous les droits d'attributs : droits de lecture et de comparaison sur l'objet Conteneur de sécurité.
- (Conditionnel) Si l'objet W1.KAP.Security existe, vous disposez de tous les droits d'attribut sur cet objet : lecture, comparaison et écriture. Pour plus d'informations sur l'objet W1.KAP.Security, reportez-vous à la section Creating an AES 256-Bit Tree Key (Création d'une clé AES 256 bits) du *NICI Administration Guide* (Guide d'administration de NICI).

❒ (Conditionnel) Si vous installez un serveur secondaire dans une arborescence existante en tant qu'utilisateur non administrateur, assurez-vous qu'au moins l'un des serveurs de l'arborescence a la même version ou une version ultérieure de eDirectory par rapport à celle du serveur secondaire ajouté comme administrateur de conteneur. Dans le cas où le serveur secondaire ajouté possède une version ultérieure, le schéma doit alors être prolongé par l'administrateur de l'arborescence avant d'ajouter ledit serveur à l'aide de l'administrateur de conteneur.

❒ Lors de la configuration de eDirectory, vous devez activer les services SLP et un port de protocole NCP (NetWare Core Protocol) (port 524 par défaut) dans le pare-feu afin de permettre l'ajout du serveur secondaire. Le port NCP doit être configuré afin d'autoriser le trafic entrant et sortant.

En outre, vous pouvez activer les ports de service suivant en fonction de vos exigences :

- LDAP texte clair - 389
- LDAP sécurisé - 636
- HTTP texte clair - 8028
- HTTP sécurisé - 8030

Si vous avez activé des ports définis par l'utilisateur, vous devez les mentionner pendant la configuration de eDirectory.

❒ Si vous installez eDirectory sur une machine virtuelle dotée d'une adresse DHCP ou sur une machine physique ou virtuelle sur laquelle SLP n'est pas diffusé, vérifiez que l'agent Annuaire est configuré sur votre réseau.

❒ Si vous ne disposez pas de la version la plus récente de Platform Agent (PA) lors de la mise à niveau vers eDirectory 9.2, exécutez le fichier `Novell_Audit_PlatformAgent_Win64.exe` à partir de l'emplacement d'installation `C:\NetIQ\eDirectory\auditds/`.

❒ L'outil NetIQ eMBox (eDirectory Management Toolbox) permet d'accéder à tous les principaux utilitaires d'eDirectory, à distance comme sur le serveur. Le client à ligne de commande est une application Java. Pour l'exécuter, vous devez installer la dernière version d'Oracle Java (1.8 ou version ultérieure). Vous devez également veiller à mettre à niveau toute version antérieure de Java en installant les mises à niveau de correctif disponibles. Une fois que la dernière version de Java est installée, exportez les variables d'environnement suivantes souhaitées :

- `EDIR_JAVA_HOME`
- `JAVA_HOME`
- `JRE_HOME`

**REMARQUE :** si vous utilisez une version antérieure à eDirectory 9.0 SP4, pour exécuter le client à ligne de commande, vous devez avoir accès à l'environnement d'exécution Java, Oracle Java 1.8, qui est installé avec eDirectory.

### Détermination de la version d'eDirectory

Pour déterminer la version d'eDirectory, suivez l'une des étapes mentionnées ci-dessous :

- Exécutez iMonitor.

  Dans la page Résumé de l'agent, cliquez sur Serveurs connus. Ensuite, sous Serveurs connus de la base de données, cliquez sur Serveurs connus. La colonne Révision de l'agent affiche le numéro de version interne de chaque serveur. Par exemple, un numéro de révision de l'agent pour eDirectory 9.2 pourrait être 40101.x.

  Pour plus d'informations sur l'exécution de iMonitor, reportez-vous à la section « Accessing iMonitor » (Accès à iMonitor) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

- Exécutez `NDSCons.exe`.

  Dans le Panneau de configuration de Windows, double-cliquez sur Services NetIQ eDirectory. Dans la colonne Services, sélectionnez ds.dlm, puis cliquez sur Configurer. L'onglet Agent affiche la chaîne marketing (par exemple, NetIQ eDirectory 9.2) et le numéro de version interne (par exemple, 40101.x).

- Affichez les propriétés d'un fichier `ds.dlm`.

  Cliquez avec le bouton droit sur le fichier `.dlm` dans l'Explorateur Windows, puis cliquez sur l'onglet Version dans la boîte de dialogue Propriétés. Le système affiche alors le numéro de version de l'utilitaire. L'emplacement par défaut des fichiers `ds.dlm` est `C:\NetIQ\eDirectory`.

### Configuration de l’adresse IP statique

L’adresse IP statique doit être configurée sur le serveur pour que eDirectory fonctionne efficacement. La configuration de eDirectory sur les serveurs dotés d’une adresse DHCP peut provoquer des résultats imprévisibles.

## Configuration matérielle requise

La configuration matérielle requise dépend de la mise en œuvre spécifique de eDirectory.

Par exemple, une installation de base de eDirectory avec le schéma standard requiert environ 74 Mo d’espace disque pour chaque groupe de 50 000 utilisateurs. Cependant, si vous ajoutez un nouvel ensemble d’attributs ou si vous paramétrez tous les attributs existants, la taille de l’objet augmente. Ces ajouts affectent l’espace disque, le processeur et la mémoire nécessaires.

Deux facteurs augmentent les performances : une mémoire cache plus importante et des processeurs plus rapides.

Pour obtenir des résultats optimaux, mettez en cache autant de paramètres de l’ensemble DIB que le permet le matériel.

eDirectory fonctionne correctement avec un seul processeur. Cependant, NetIQ eDirectory 9.2 tire parti de la présence de plusieurs processeurs. L’ajout de processeurs améliore les performances dans certains cas, par exemple pour les connexions, et lorsque plusieurs fils d’exécution sont actifs sur plusieurs processeurs. eDirectory en lui-même n’est pas gourmand en ressources processeur, mais plutôt en E/S.

Le tableau suivant illustre les exigences système habituelles pour NetIQ eDirectory pour Windows :

| Objets | Mémoire | Disque dur |
|---|---|---|
| 10 000 | 384 Mo | 144 Mo |
| 1 million | 2 Go | 1,5 Go |
| 10 millions | 2 Go et plus | 15 Go |

Les exigences relatives aux processeurs dépendent des services supplémentaires disponibles sur l'ordinateur, ainsi que du nombre d'authentifications, de lectures et d'écritures gérées par l'ordinateur. Certains traitements, tels que le chiffrement et l'indexation, peuvent nécessiter des ressources importantes au niveau du processeur.

# Exécution forcée du processus de liaison en amont

Étant donné que les identificateurs internes de eDirectory changent après la mise à niveau vers eDirectory, le processus de liaison en amont (backlink) doit mettre à jour les objets liés en amont pour les rendre cohérents.

Les liens en amont sont utilisés pour assurer le suivi des références externes aux objets sur d'autres serveurs. Pour chaque référence externe sur un serveur, le processus de liaison en amont s'assure que l'objet réel existe dans l'emplacement correct et vérifie tous les attributs de liaison en amont sur la réplique maîtresse. Le processus de liaison en amont intervient deux heures après l'ouverture de la base de données, puis toutes les 780 minutes (13 heures). Vous pouvez paramétrer l'intervalle de 2 minutes à 10 080 minutes (7 jours).

Une fois la migration vers eDirectory effectuée, nous vous recommandons de forcer l'exécution de la liaison en amont en effectuant la procédure suivante. Le processus de liaison en amont est particulièrement important sur les serveurs qui ne contiennent pas de réplique.

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**
2. Dans l'onglet **Services**, sélectionnez **ds.dlm**.
3. Cliquez sur **Configurer**.
4. Dans l'onglet **Déclencheur**, cliquez sur **Liaison en amont**.

# Installation d'eDirectory sous Windows

Cette section comprend les informations suivantes :

# Installation ou mise à niveau d'eDirectory 9.2 sur un serveur Windows

Vous pouvez installer eDirectory 9.2 pour Windows sans le client Novell. Si vous installez eDirectory 9.2 sur une machine qui contient déjà le client Novell, eDirectory utilise le client existant ou le met à jour s'il ne s'agit pas de la version la plus récente.

1. Sur le serveur Windows, connectez-vous en tant qu'administrateur ou en tant qu'utilisateur doté de droits d'administration.
2. Si la fonction d'exécution automatique est désactivée, exécutez le fichier `eDirectory_920_Windows_x86_64.exe` à partir du dossier `windows` sur le CD-ROM eDirectory 9.2 ou à partir du fichier téléchargé.
3. (Nouvelles installations uniquement) Sélectionnez un type d'installation eDirectory sous l'onglet **De base** :
   - **Créer une nouvelle arborescence eDirectory** Permet de créer une arborescence. Utilisez cette option s'il s'agit du premier serveur à placer dans l'arborescence ou si ce serveur requiert une arborescence distincte. Les ressources de la nouvelle arborescence ne seront pas accessibles aux utilisateurs connectés à une autre arborescence.
   - **Installer eDirectory dans une arborescence existante** Permet d'intégrer le serveur concerné au réseau eDirectory. Le serveur peut être installé à un niveau quelconque de l'arborescence.
4. Fournissez des informations dans l'écran d'installation d'eDirectory :
   - Si vous installez un nouveau serveur eDirectory, indiquez un nom d'arborescence, le contexte de l'objet Serveur ainsi que le nom et le mot de passe Admin pour la nouvelle arborescence.

     **IMPORTANT :** bien qu'eDirectory permette de définir le FDN de l'objet Serveur NCP jusqu'à 256 caractères, NetIQ recommande de limiter la variable à une valeur bien inférieure étant donné qu'eDirectory crée d'autres objets de longueur supérieure en fonction de la longueur de cet objet.
   - Si vous effectuez l'installation dans une arborescence existante, indiquez l'adresse IP, le nom de l'arborescence, le contexte de l'objet Serveur ainsi que le nom et le mot de passe d'administration de l'arborescence existante.
   - Si vous effectuez la mise à niveau d'un serveur eDirectory, entrez le mot de passe Admin.

     **REMARQUE :** eDirectory 9.2 vous permet d'utiliser des mots de passe sensibles à la casse pour tous les utilitaires.

   Pour plus d'informations sur l'utilisation des points dans les noms de conteneurs, reportez-vous à « Installation dans une arborescence comportant des conteneurs dont le nom utilise la notation à point » page 65.
5. Indiquez ou confirmez le chemin d'installation. L'emplacement par défaut est `C:\NetIQ\eDirectory`.
6. Indiquez ou confirmez le chemin des fichiers DIB. L'emplacement par défaut est `C:\NetIQ\eDirectory\DIBFiles`.
7. Sous l'onglet **Avancé**, indiquez les informations suivantes :
   - Si vous souhaitez utiliser des adresses IPv6, sélectionnez **Activer IPv6**.

**REMARQUE :** si vous n'activez pas les adresses IPv6 pendant la procédure d'installation et que vous décidez de les utiliser par la suite, vous devez réexécuter le programme d'installation.

- Si vous souhaitez activer l'authentification EBA, sélectionnez **Activer EBA**.

  **REMARQUE :** si vous n'activez pas EBA pendant la procédure d'installation et que vous décidez d'utiliser cette authentification par la suite, vous devez réexécuter le programme d'installation.

  Pour ajouter un serveur secondaire activé pour l'authentification EBA à l'arborescence, une autorité de certification EBA doit être configurée dans l'arborescence. Si aucune autorité de certification EBA n'est présente, commencez par ajouter le serveur sans activer l'authentification EBA, puis mettez à niveau le serveur pour qu'il héberge l'autorité de certification EBA. Dans le cas contraire, la configuration du serveur secondaire échoue.

- Spécifiez les **ports de pile HTTP** à utiliser pour le serveur HTTP d'administration d'eDirectory.

  **IMPORTANT :** Veillez à ce que les ports de la pile HTTP que vous avez définis pendant l'installation de eDirectory soient différents de ceux que vous avez utilisés ou allez utiliser pour NetIQ iManager. Pour plus d'informations, reportez-vous au *Guide d'administration de iManager* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html).

- Indiquez les **ports LDAP** à utiliser.

  Pour plus d'informations, reportez-vous à la section « Communication avec eDirectory via LDAP » page 64.

8 Cliquez sur **Installer**.

  Le programme d'installation vérifie les composants suivants avant d'installer eDirectory. Si un composant est manquant ou si sa version est incorrecte, le programme d'installation lance automatiquement l'installation du composant.

  - NICI 3.2

    Pour plus d'informations sur NICI (Novell International Cryptographic Infrastructure), consultez le manuel *NICI Administration Guide* (Guide d'administration de NICI).

9 eDirectory installera et configurera tous les composants requis automatiquement.

10 Lorsque le programme d'installation a terminé, cliquez sur **Terminer** pour quitter l'assistant.

**IMPORTANT :** seul l'administrateur d'eDirectory doit pouvoir se connecter au serveur sur lequel eDirectory est installé.

**REMARQUE :** Après avoir installé eDirectory, nous vous recommandons d'exclure le répertoire DIB présent sur votre serveur eDirectory de la portée de tout antivirus ou processus de logiciels de sauvegarde. Utilisez l'outil de sauvegarde eDirectory pour sauvegarder votre répertoire DIB.

Pour plus d'informations sur la sauvegarde de eDirectory, consultez la section « Sauvegarder et restaurer NetIQ eDirectory » du *Guide d'administration NetIQ eDirectory* .

# Vérifications de l’état de santé du serveur

eDirectory 9.2 exécute par défaut une vérification de l'état de santé du serveur pour s'assurer qu'il est sain avant la mise à niveau.

- « État de santé des partitions et répliques » page 163

En fonction des résultats obtenus, la mise à niveau se poursuivra ou sera abandonnée :

- si toutes les vérifications de l’état de santé ont été menées avec succès, la mise à niveau se poursuivra ;
- en cas d’erreurs mineures, vous serez invité à poursuivre ou à quitter la mise à niveau ;
- en cas d’erreurs critiques, la mise à niveau sera abandonnée.

Reportez-vous à l’Annexe B, « Vérifications de l’état de santé de eDirectory », page 161 pour consulter la liste de conditions des erreurs mineures et critiques.

# Communication avec eDirectory via LDAP

Lorsque vous installez eDirectory, vous devez sélectionner un port que le serveur LDAP surveille afin de traiter les demandes LDAP. Le tableau suivant liste les options pour différentes installations :

| Installation | Option | Résultat |
|---|---|---|
| eDirectory 9.2 | Port 389 en texte clair | Sélectionne le port 389. |
| eDirectory 9.2 | Port 636 codé | Sélectionne le port 636. |

## Port 389, le port LDAP standard non codé

La connexion via le port 389 n’est pas codée. Toutes les données envoyées lors d’une connexion établie via ce port se présentent en clair, ce qui constitue un risque en matière de sécurité. Ainsi, les mots de passe LDAP peuvent être affichés en cas de demande de liaison simple.

Une liaison simple LDAP nécessite seulement un DN et un mot de passe. Le mot de passe se présente en texte clair. Si vous employez le port 389, l’ensemble du paquet est en texte clair. Par défaut, cette option est désactivée pendant l’installation de eDirectory.

Du fait que le port 389 autorise le texte clair, les services du serveur LDAP lisent et écrivent les demandes adressées à l’annuaire via ce port. Cette ouverture est adaptée aux environnements de confiance où aucune simulation n’a lieu et dans lesquels aucun utilisateur ne peut intercepter les paquets qui ne lui sont pas destinés.

Si vous établissez une connexion sécurisée avec le port 636 et disposez d’une liaison simple, la connexion est déjà codée. Personne ne peut voir les mots de passe, les paquets de données ou les demandes de liaison.

## Port 636, le port sécurisé standard

La connexion via le port 636 est codée. TLS (anciennement SSL) gère le chiffrement. Par défaut, le programme d’installation de eDirectory sélectionne ce port.

La connexion au port 636 lance automatiquement une procédure de reconnaissance mutuelle. Si celle-ci échoue, la connexion est refusée.

**IMPORTANT :** Cette sélection par défaut peut poser un problème pour le serveur LDAP. Si un service déjà chargé sur le serveur hôte (avant l'installation de eDirectory) utilise le port 636, vous devez spécifier un autre port.

Le programme d'installation charge le fichier `nldap.nlm`, publie un message d'erreur dans le fichier `dstrace.log` et s'exécute sans le port sécurisé.

**Scénario : le port 636 est déjà utilisé :** Votre serveur exécute Active Directory. et exécute un programme LDAP qui utilise le port 636. Vous installez eDirectory. Le programme d'installation détecte alors que le port 636 est en cours d'utilisation et n'affecte pas de numéro de port au serveur LDAP NetIQ. Le serveur LDAP se charge et semble s'exécuter. Toutefois, comme le serveur LDAP ne peut pas dupliquer un port ni en utiliser un qui est déjà ouvert, il ne traite pas les requêtes de service sur un port dupliqué.

En cas de doute sur le port affecté au serveur NetIQ LDAP (389 ou 636) lancez l'utilitaire ICE. Si le champ **Version du fournisseur** n'indique pas NetIQ, vous devez reconfigurer le serveur LDAP pour eDirectory et sélectionner un port différent. Pour plus d'informations, consultez la section « Vérifier que le serveur LDAP est en cours d'exécution » du *Guide d'administration NetIQ eDirectory* .

**Scénario : Active Directory est en cours d'exécution** Active Directory est en cours d'exécution. Le port non codé 389 est ouvert. Vous exécutez la commande `ICE` sur le port 389 et demandez la version du fournisseur. Le résultat affiché est `Microsoft*`. Vous reconfigurez alors le serveur NetIQ LDAP en sélectionnant un autre port, afin que le serveur LDAP eDirectory puisse répondre aux requêtes LDAP.

NetIQ iMonitor peut également signaler que le port 389 ou 636 est déjà ouvert. Si le serveur LDAP ne fonctionne pas, utilisez NetIQ iMonitor pour identifier les détails. Pour plus d'informations, consultez la section « Vérifier que le serveur LDAP est en cours d'exécution » du *Guide d'administration NetIQ eDirectory* .

## Installation du logiciel NMAS Server

Les composants du serveur NMAS (NetIQ Modular Authentication Service) sont automatiquement installés lorsque vous lancez le programme d'installation de eDirectory. La méthode de connexion NDS est configurée par défaut.

Pour plus d'informations sur les méthodes de connexion, reportez-vous à la section Gestion de la connexion, méthodes de post-connexion et séquences du Guide d'administration de NetIQ eDirectory.

## Installation dans une arborescence comportant des conteneurs dont le nom utilise la notation à point

Vous pouvez installer un serveur Windows dans une arborescence eDirectory qui comporte des conteneurs dont le nom utilise la notation à point (par exemple, O=netiq.com ou C=e.u). Lors de l'utilisation de ce type de conteneurs, ces points exigent l'emploi d'une barre oblique inverse comme caractère d'échappement. Dès lors, insérez une barre oblique inverse devant chaque point du nom du conteneur.

Un nom ne peut pas commencer par un point. Il est, par exemple, impossible de créer un conteneur nommé « .netiq ».

**IMPORTANT :** S'il existe dans votre arborescence des conteneurs dont les noms comportent des points, vous devez précéder ces derniers de caractères d'échappement lorsque vous vous connectez à des utilitaires tels que iMonitor, iManager et DHost iConsole. Par exemple, si votre arborescence contient « netiq.com » comme nom pour O, entrez *nom_utilisateur*.netiq\.com dans le champ **Nom d'utilisateur** lorsque vous vous connectez à iMonitor.

# Installation et configuration sans surveillance d'eDirectory 9.2 sous Windows

eDirectory 9.2 automatise l'installation et la mise à niveau d'eDirectory de sorte qu'eDirectory soit installé et mis à niveau en mode silencieux sur les serveurs Windows, sans intervention humaine.

Sur Windows, l'installation sans surveillance de eDirectory utilise les fichiers texte prédéfinis qui simplifient l'installation ou la mise à niveau sans surveillance. Vous pouvez réaliser l'une des configurations suivantes en utilisant l'installation sans surveillance de eDirectory :

- Installation ou mise à niveau autonome de eDirectory selon s'il s'agit ou non d'une installation complète de eDirectory. Le processus de mise à niveau autonome met à niveau les fichiers installés uniquement.
- Configuration de la version de eDirectory installée. Si vous installez eDirectory, une configuration complète de eDirectory est réalisée. Sinon, lorsque vous mettez à niveau eDirectory, le programme d'installation configure uniquement les fichiers mis à niveau.

Pour plus d'informations sur comment mentionner la configuration correspondant à l'installation sans surveillance, consultez la section « Ajout de fonctionnalités à l'installation automatisée » page 67.

## Conditions préalables

- La version 4.0 de .NET Management Framework ou une version ultérieure est requise.
- Assurez-vous que Windows Server 2012 R2 est mis à jour avec le dernier correctif Windows.

Les sections suivantes abordent les différentes fonctionnalités qui peuvent être utilisées pour configurer l'installation sans surveillance, y compris l'emplacement d'installation, aucun affichage des écrans de démarrage, les configurations de port, les autres méthodes NMAS, l'arrêt et le démarrage des services SNMP, etc.


- « Fichiers de réponse » page 66
- « Ajout de fonctionnalités à l'installation automatisée » page 67
- « Contrôle de l'installation automatisée » page 71
- « Installation sans surveillance de eDirectory à l'aide du fichier de réponses » page 72


## Fichiers de réponse

L'installation ou la mise à niveau vers eDirectory 9.2 sur un système d'exploitation Windows peut être réalisée en mode silencieux et de manière plus flexible en utilisant un fichier de réponses pour les tâches suivantes :

- Installation complète sans surveillance avec toutes les données utilisateur requises
- Configuration par défaut des composants
- Ignorer toutes les invites pendant l'installation

Un fichier de réponses est un fichier texte qui contient des sections et des clés (comme un fichier `Windows.ini`). Pour le créer et le modifier, vous pouvez utiliser tout éditeur de texte ASCII. La mise à niveau eDirectory lit directement les paramètres d'installation depuis le fichier de réponses et remplace les valeurs d'installation par défaut par celles du fichier de réponses. Le programme d'installation accepte les valeurs du fichier de réponses et poursuit l'installation sans émettre d'invite.

### Sections et clés du fichier de réponses

L'installation d'eDirectory 9.2 nécessite de modifier les sections du fichier de réponses afin d'ajouter des informations sur l'instance eDirectory à installer, notamment le nom d'arborescence, le contexte administrateur, les références de l'administrateur (y compris le nom d'utilisateur et les mots de passe), les emplacements d'installation, etc. Une liste complète des clés et de leurs valeurs par défaut est disponible dans les fichiers d'exemples de réponses fournis avec l'installation d'eDirectory. Il existe quatre fichiers de réponses disponibles dans `<Chemin_Installation_eDirectory>\NetIQ\eDirectory\Sample_Response_File` lors de l'installation d'eDirectory :

- `newTree.ni` : ce fichier permet de configurer une nouvelle arborescence eDirectory.
- `existingtree.ni` : ce fichier permet d'ajouter un serveur à une arborescence eDirectory existante.
- `upgrade.ni` : ce fichier permet de mettre à niveau le serveur eDirectory.
- `deconfigure.ni` : ce fichier permet d'annuler la configuration d'une arborescence eDirectory.

---

**REMARQUE :** lors de l'installation d'eDirectory, vous devez utiliser l'un des fichiers de réponses fournis. En effet, des paramètres essentiels sont définis par défaut dans ces fichiers. Lorsque vous modifiez ces fichiers, veillez à ce qu'il n'y ait aucun espace entre la clé, les valeurs et le signe égal (« = ») dans chaque paire clé-valeur.

---

## Ajout de fonctionnalités à l'installation automatisée

La plupart des détails portant sur la configuration du programme d'installation de eDirectory ont des paramètres par défaut prévus pour l'installation manuelle. Cependant, pendant l'installation sans surveillance, chaque paramètre de configuration doit être explicitement configuré. Cette section aborde les paramètres de base à configurer, peu importe la séquence d'installation ou les fonctionnalités supplémentaires.

### Détails sur le serveur eDirectory

Peu importe s'il s'agit d'une mise à niveau ou de l'installation d'un serveur primaire/secondaire, les détails du serveur à installer ou mettre à niveau doivent être fournis au programme d'installation. La plupart de ces informations sont configurées dans la balise `[NWI : NDS]`.

`[NWI:NDS]`

- **mode :** par défaut, la clé du mode est définie sur configurer. Cela configure eDirectory.
- **Nom de l'arborescence :** Pour l'installation d'un serveur primaire, il s'agit du nom de l'arborescence qui doit être installée. Pour l'installation d'un serveur secondaire, il s'agit de l'arborescence à laquelle ce serveur doit être ajouté.
- **Nom du serveur:** Le nom du serveur actuellement installé.
- **Conteneur de serveurs :** Tout serveur ajouté à une arborescence possède un objet Serveur contenant tous les détails de la configuration spécifiques au serveur. Ce paramètre est l'objet Conteneur de l'arborescence à laquelle l'objet Serveur sera ajouté. Pour des installations de serveur primaire, ce conteneur sera créé avec l'objet Serveur.

- **Nom de connexion d'admin. :** Le nom (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté. Toutes les opérations ayant lieu dans l'arborescence seront réalisées sous cet utilisateur.
- **Contexte d'admin. :** Tout utilisateur ajouté à une arborescence possède un objet Utilisateur qui contient tous les détails spécifiques à l'utilisateur. Ce paramètre est l'objet Conteneur de l'arborescence à laquelle l'objet Administrateur sera ajouté. Pour des installations de serveur primaire, ce conteneur sera créé avec l'objet Serveur.
- **Mot de passe de l'administrateur :** Le mot de passe de l'objet Administrateur créé dans les paramètres précédents. Ce mot de passe sera configuré sur l'objet Administrateur pendant les installations du serveur primaire. Pour les installations de serveur secondaire, le mot de passe de l'objet Administrateur du serveur primaire doit détenir les droits sur le contexte auquel le nouveau serveur est ajouté.

  Nous vous recommandons de définir le mot de passe d'administration dans une variable d'environnement et de mentionner le nom de la variable d'environnement dans le fichier de réponses. Une fois que la configuration silencieuse est terminée, supprimez le mot de passe de la variable d'environnement.

  ---

  **IMPORTANT :** vous indiquez les références de l'administrateur dans le fichier de réponses en vue d'une installation sans surveillance. Par conséquent, vous devez supprimer définitivement le fichier après l'installation pour éviter de compromettre les références de l'administrateur.

  ---

- **DataDir :** par défaut, la DIB est installée dans le sous-dossier `Files` à l'emplacement NDS, mais les administrateurs peuvent modifier ce paramètre et indiquer un autre emplacement. Si aucune valeur n'est fournie pour ce paramètre, la valeur sera définie sur `<Emplacement Installation>/DIBFiles` par défaut.
- **EBA :** fournit un protocole en arrière-plan de meilleure qualité et plus sécurisé pour s'authentifier auprès des serveurs NCP de l'arborescence. eDirectory offre la possibilité d'activer EBA lors de la configuration de l'arborescence eDirectory. Par défaut, EBA n'est pas configuré dans eDirectory, à moins d'un changement dans le fichier de réponses. Pour activer l'authentification EBA, définissez Require EBA (Exiger EBA) sur Yes (Oui).
- **FIPS :** NetIQ prend en charge l'exécution d'eDirectory en mode FIPS (Federal Information Processing Standard). Pour activer eDirectory en mode FIPS, définissez Require FIPS for TLS (Exiger FIPS pour TLS) sur Yes (Oui).
- **Enable PBKDF2 (Activer PBKDF2) :** un nouveau paramètre de configuration, `Enable PBKDF2` (Activer PBKDF2), a été ajouté au fichier de réponses `newtree.ni` dans eDirectory 9.2. Si cette option a la valeur yes (oui), une stratégie de mot de passe est créée et assignée automatiquement à l'ensemble de l'arborescence. Cette stratégie de mot de passe permet de synchroniser les mots de passe NDS avec les mots de passe PBKDF2 pour tous les utilisateurs de l'arborescence. Pour plus d'informations, reportez-vous à la section Présentation du stockage des mots de passe non réversibles dans le guide d'administration de NetIQ eDirectory.

Ce qui suit est un exemple de texte inclus dans le fichier de réponses pour tous les paramètres de base décrits ci-dessus :

```
[NWI:NDS]
mode=configure
New Tree=Yes
Tree Name=ENEWTREE
Server Name=ENEWSERVER
Server Container=myorg
Admin Context=myorg
Admin Login Name=Admin
Admin Password=env: PASSWORD_VAR
Require IPV6=NO
Require EBA=NO
Require FIPS for TLS=NO
DataDir=C:\NetIQ\eDirectory\DIBFiles
LDAP TCP Port=389
LDAP SSL Port=636
Require TLS=No
Require SS=YES
Enable PBKDF2=No
```

## Ajout de méthodes NMAS

eDirectory prend en charge l'installation de plusieurs méthodes NMAS, à la fois pendant l'installation et la mise à niveau. Pendant des installations manuelles, vous pouvez sélectionner les méthodes NMAS à installer et configurer. Cela peut également être réalisé dans le cadre d'installations automatisées.

Les paramètres de configuration associés à NMAS sont fournis dans la balise `[NWI:NMAS]`. La balise possède deux clés à configurer, et les deux sont obligatoires :

- **Options possibles :** Cette clé informe le composant d'installation de eDirectory sur le nombre de méthodes NMAS qui doit être installé.
- **Méthodes :** Cette clé liste les options de méthode NMAS qui doivent être installées. Actuellement, il existe 6 méthodes NMAS prises en charge. Les noms de méthode et leurs types sont les suivants :

***Tableau 3-1*** *Méthodes NMAS*

| Nom de la méthode | Type de méthode |
|---|---|
| CertMutual | Méthode de connexion Certificate Mutual |
| Réponse de vérification d'identité | La méthode NMAS de réponse de vérification d'identité NetIQ |
| DIGEST-MD5 | Méthode de connexion Digest MD5 |
| SAML | Méthode d'authentification Secuity Assertion Markup Language (SAML) |
| NDS | Méthode de connexion NDS (par défaut) |
| Mot de passe simple | Méthode de connexion NMAS par mot de passe simple |
| SCRAM | La méthode d'authentification SCRAM (Salt Challenge Response Authentication Mechanism) utilise les mots de passe basés sur le hachage PBKDF2. |

**REMARQUE :** Les noms de méthode doivent correspondre exactement à ceux listés dans le tableau ci-dessus, en tant qu'options de la clé Méthodes. Le programme d'installation fait correspondre la chaîne exacte (casse incluse) pour choisir les méthodes NMAS à installer.

La méthode NMAS NDS est obligatoire et sera installée automatiquement si aucune liste de méthodes NMAS n'est fournie. Toutefois, si vous créez une liste explicite, ne supprimez pas cette méthode de la liste.

Si les méthodes NMAS sont configurées à l'aide de cette méthodologie dans le fichier de réponses, eDirectory affiche un message d'état pendant l'installation, sans inviter l'utilisateur à entrer des données.

Ce qui suit est un exemple de texte inclus dans le fichier de réponses permettant de choisir les méthodes NMAS :

```
[NWI:NMAS]
Methods=CertMutual,Challenge Response,DIGEST-MD5,NDS,Simple Password,SAML
```

## Ports HTTP

eDirectory écoute sur les ports HTTP préconfigurés pour un accès via le Web. Par exemple, iMonitor accède à eDirectory par le biais d'interfaces Web. Certaines doivent être spécifiées dans l'ordre afin d'accéder aux applications adéquates. Deux clés peuvent être définies avant d'installer et de configurer eDirectory sur des ports spécifiques :

- **Port HTTP en texte clair :** Le numéro de port correspondant aux opérations HTTP en texte clair.
- **Port HTTP SSL :** Le numéro de port HTTP correspondant aux opérations SSL (Secure Socket Layer).

Ce qui suit est un exemple de texte inclus dans le fichier de réponses permettant de configurer les numéros de port HTTP :

```
[eDir:HTTP]

Clear Text HTTP Port=8028

SSL HTTP Port=8030
```

## Configuration LDAP

eDirectory prend en charge les opérations LDAP. Il écoute les requêtes LDAP en texte clair et en SSL sur deux ports différents. Ces ports peuvent être configurés dans le fichier de réponses avant l'installation, de sorte qu'au démarrage de eDirectory, le programme écoute sur ces ports configurés.

Il y a trois clés dans la balise `[NWI:NDS]` qui configurent les ports LDAP :

- **Port TCP LDAP:** Le port sur lequel eDirectory doit écouter les requêtes LDAP en texte clair. Si aucun port n'est mentionné, `389` sera celui utilisé par défaut.
- **Port SSL LDAP:** Le port sur lequel eDirectory doit écouter les requêtes LDAP en SSL. Vous pouvez également utiliser une clé pour configurer le fait que eDirectory doive rendre obligatoire ou non les connexions sécurisées lorsque des requêtes de liaison envoient le mot de passe en texte clair. Si aucun port n'est mentionné, `636` sera celui utilisé par défaut.
- **Exiger TLS :** Si eDirectory doit rendre obligatoire ou non TLS lors de la réception de requêtes LDAP en texte clair. Si aucune valeur n'est renseignée pour ce paramètre, la valeur par défaut sera `Yes` (Oui).

Ce qui suit est un exemple de texte inclus dans le fichier de réponses pour la configuration LDAP :

```
[NWI:NDS]

Require TLS=Yes
```

```
LDAP TLS Port=389

LDAP SSL Port=636
```

## Contrôle de l’installation automatisée

Le fichier de réponses peut également être modifié afin de contrôler le flux de l’installation automatisée.

### Arrêt des services SNMP

Cette fonction est spécifique à une installation de eDirectory sur Windows. La plupart des serveurs Windows ont un service SNMP configuré et en cours d’exécution. Lors de l’installation de eDirectory, les services SNMP doivent être arrêtés puis redémarrés après l’installation. Dans le cas d’une installation manuelle, le programme d’installation invite l’utilisateur actif à arrêter les services SNMP avant de poursuivre l’installation. Cette invite peut être évitée pendant l’automatisation en définissant la clé dans la balise `[NWI:SNMP]` :

- **Arrêter le service :** Définissez la valeur sur Oui pour arrêter les services SNMP sans recevoir d’invite. La propriété d’état apparaît à l’écran.

Ce qui suit est un exemple de texte inclus dans le fichier de réponses permettant d’arrêter les services SNMP :

```
[NWI:SNMP]

Stop service=yes
```

### Services SLP

eDirectory utilise les services SLP pour identifier d’autres serveurs ou arborescences dans le sous-réseau pendant l’installation ou la mise à niveau. Si les services SLP avaient déjà été installés sur votre serveur dans le cadre d'une installation précédente d'eDirectory, la version actuelle d'eDirectory les détecte et les met à niveau vers la version la plus récente. Si aucun service SLP n'est installé, eDirectory installe les services SLP pendant l'installation silencieuse.

### Spécification des paramètres par défaut pour les certificats de serveur par défaut

eDirectory permet de spécifier la taille de la clé RSA par défaut, la courbe elliptique et la durée de vie des certificats de l'autorité de certification et des certificats de serveur par défaut lors de la configuration d'une nouvelle arborescence eDirectory. Vous pouvez spécifier les paramètres par défaut suivants concernant les certificats de l'autorité de certification et ceux du serveur par défaut lors de l'installation silencieuse d'une nouvelle arborescence eDirectory dans le fichier de réponses :

- **Taille de la clé RSA :** permet de spécifier la taille de clé des certificats RSA. Les valeurs autorisées sont 2 048, 4 096 et 8 192 bits.
- **EC Curve (Courbe EC) :** permet de spécifier la limite de courbe des certificats EC. Les valeurs autorisées sont P256, P384 et P521.
- **Certificate Life (Durée de vie du certificat) :** permet de spécifier la durée de validité du certificat en nombre d'années.

Les valeurs spécifiées ici seront définies en fonction des attributs correspondants sur l'objet Autorité de certification organisationnelle lors de la configuration de la nouvelle arborescence.

Ces attributs peuvent être définis dans la balise [NWI:PKI] du fichier `newtree.in` lors de l'installation d'un nouveau serveur eDirectory, comme illustré ci-dessous :

```
[NWI:PKI]
RSA KeySize=4096
EC Curve=P521
Certificate Life=4
```

Pour plus d'informations, reportez-vous à la section Création d'un objet Autorité de certification organisationnelle du *Guide d'administration de NetIQ eDirectory*.

### Installation d'un serveur primaire/secondaire

Le programme d'installation eDirectory fournit des options qui permettent d'installer sans surveillance un serveur primaire ou secondaire dans un réseau. Il existe une clé qui aide le programme d'installation à décider s'il s'agit de l'installation d'un serveur primaire ou secondaire.

- **Serveur primaire :** utilisez la clé `New Tree` (Nouvelle arborescence) dans la balise `[NWI:NDS]` et définissez-la sur `Yes` (Oui) dans le cadre de l'installation d'une nouvelle arborescence ou d'une arborescence primaire dans le fichier `newtree.ni` ou dans un fichier de réponses similaire requis pour la configuration d'un nouveau serveur.
- **Serveur secondaire :** utilisez la clé `New Tree` (Nouvelle arborescence) dans la balise `[NWI:NDS]` et définissez-la sur `No` (Non) dans le cadre de l'installation d'une arborescence secondaire dans le fichier `existingtree.ni` ou dans un fichier de réponses similaire requis pour la configuration d'un serveur secondaire.

Par exemple, les clés permettant d'installer un serveur primaire dans une nouvelle arborescence seraient les suivantes :

```
[NWI:NDS]

New Tree=Yes
```

et pour l'installation d'un serveur secondaire dans une arborescence existante :

```
[NWI:NDS]

New Tree=No
```

## Installation sans surveillance de eDirectory à l'aide du fichier de réponses

Il est facile de lancer le programme d'installation eDirectory sur Windows. Le fichier `eDirectory_920_Windows_x86_64.exe` fourni avec la version d'eDirectory est invoqué dans la ligne de commande avec quelques autres paramètres.

Selon le mode de configuration choisi, utilisez l'une des commandes suivantes :

### Installer

```
<chemin_emplacement_téléchargement>\eDirectory_920_Windows_x86_64.exe /qn
```

Par exemple : `D:\builds\eDirectory_920_Windows_x86_64.exe /qn`

---

**REMARQUE :** exécutez la commande suivante pour installer eDirectory dans un emplacement personnalisé :

```
eDirectory_920_Windows_x86_64.exe /qn INSTALLDIR="C:\<emplacement_installation>
```

---

### Configuration

```
<emplacement installation eDirectory> ./EConfig.ps1 -rfile
<emplacement_Exemple_Fichiers_Réponses>\newtree.ni
```

Par exemple, `C:\NetIQ\eDirectory>./EConfig.ps1 -rfile C:\Sample_Response_Files\newtree.ni`

---

**REMARQUE :** les fichiers journaux sont accessibles à partir des emplacements suivants :

- `C:\Program Files\NetIQ\eDirectory\installlogs`
- `C:\Program Files\NetIQ\eDirectory\logs`

---

## Localisation des fichiers journaux

### dsinstall.log

La première partie du fichier `dsinstall.log` disponible à l'emplacement `<Unité Windows>\NetIQ\eDirectory` répertorie les variables d'environnement définies. La seconde partie contient les messages d'état qui se rapportent au processus d'installation de eDirectory.

# Mise à niveau d'eDirectory sous Windows

Lors de la mise à niveau d'eDirectory, celle-ci peut-être effectuée à partir d'eDirectory 8.8.8.x 64 bits vers eDirectory 9.2 64 bits.

---

**REMARQUE :** pour effectuer une mise à niveau à partir d'une version 32 bits d'eDirectory vers une version 64 bits, vous devez d'abord mettre à niveau la version 32 bits vers la version 64 bits d'eDirectory 8.8.x, puis vers eDirectory 9.2. Vous pouvez suivre la même procédure pour la mise à niveau d'eDirectory 64 bits vers eDirectory 9.2.

---

Les sections suivantes fournissent des informations permettant de mettre à niveau votre installation eDirectory existante vers la version actuelle.


- « Mise à niveau d'eDirectory à l'aide de Windows Installer » page 73
- « Mise à niveau sans surveillance d'eDirectory sous Windows » page 74


## Mise à niveau d'eDirectory à l'aide de Windows Installer

Vous pouvez mettre à niveau votre serveur eDirectory à l'aide de Windows Installer. Procédez comme suit pour mettre à niveau votre serveur eDirectory :

1. Sur le serveur Windows, connectez-vous en tant qu'administrateur ou en tant qu'utilisateur doté de droits d'administration.
2. Exécutez `eDirectory_920_Windows_x86_64.exe` à partir du dossier windows sur le CD-ROM eDirectory 9.2 ou à partir du fichier téléchargé.

3 L'écran du programme d'installation affiche ensuite le nom de l'arborescence eDirectory et le FDN du serveur dans l'onglet **De base**. Entrez les informations d'identification de l'administrateur de l'arborescence, puis cliquez sur le bouton **Mettre à niveau** pour procéder à la mise à niveau.

4 Dans l'onglet **Avancé**, vous pouvez modifier les paramètres existants définis lors de l'installation d'eDirectory. Pour plus d'informations, reportez-vous à la section « Installation ou mise à niveau d'eDirectory 9.2 sur un serveur Windows » page 62.

## Mise à niveau sans surveillance d'eDirectory sous Windows

Vous pouvez effectuer la mise à niveau d'eDirectory sous Windows en mode silencieux.

Sous Windows, avant d'effectuer la mise à niveau, vous devez mentionner le nom de l'arborescence, le nom du serveur et les informations d'identification de l'administrateur du serveur eDirectory existant dans le fichier de réponses `upgrade.ni`.

Vous trouverez ci-dessous un exemple de fichier de réponses `upgrade.ni` avec la configuration de la mise à niveau :

```
[NWI:NDS]
mode=configure
Tree Name=enewtree
Server Name=enewserver
Server Container=org
Admin Context=org
Admin Login Name=Admin
Admin Password=env:PASSWORD_VAR
Require IPV6=NO
Require EBA=NO
Require FIPS for TLS=YES
LDAP TCP Port=389
LDAP SSL Port=636
Require TLS=Yes
Require SS=Yes
Existing Server=172.65.156.167
Existing Server Port=524

[NWI:SNMP]
Stop service=No

[NWI:NMAS]
Methods=CertMutual,Challenge Response,DIGEST-MD5,NDS,Simple Password,SAML
```

Une fois le fichier de réponses `upgrade.ni` mis à jour avec les détails du serveur eDirectory nécessaires, exécutez la commande suivante pour mettre à niveau votre serveur eDirectory :

```
<emplacement_installation_eDirectory> ./EConfig.ps1 -rfile
<emplacement_exemples_fichiers_réponses>\upgrade.ni
```

Par exemple, `C:\NetIQ\eDirectory> ./EConfig.ps1 -rfile C:\exemples_fichiers_réponses\upgrade.ni`.

# 4 Déploiement d'eDirectory dans Microsoft Azure

Il est possible de déployer eDirectory sur des machines virtuelles Microsoft Azure.

eDirectory prend en charge les systèmes d'exploitation suivants sur Azure :

- SUSE Linux Enterprise Server (SLES) 12 SP3
- SUSE Linux Enterprise Server (SLES) 12 SP4
- SUSE Linux Enterprise Server (SLES) 15
- Red Hat Enterprise Linux (RHEL) 7.5
- Red Hat Enterprise Linux (RHEL) 7.6

## Conditions préalables

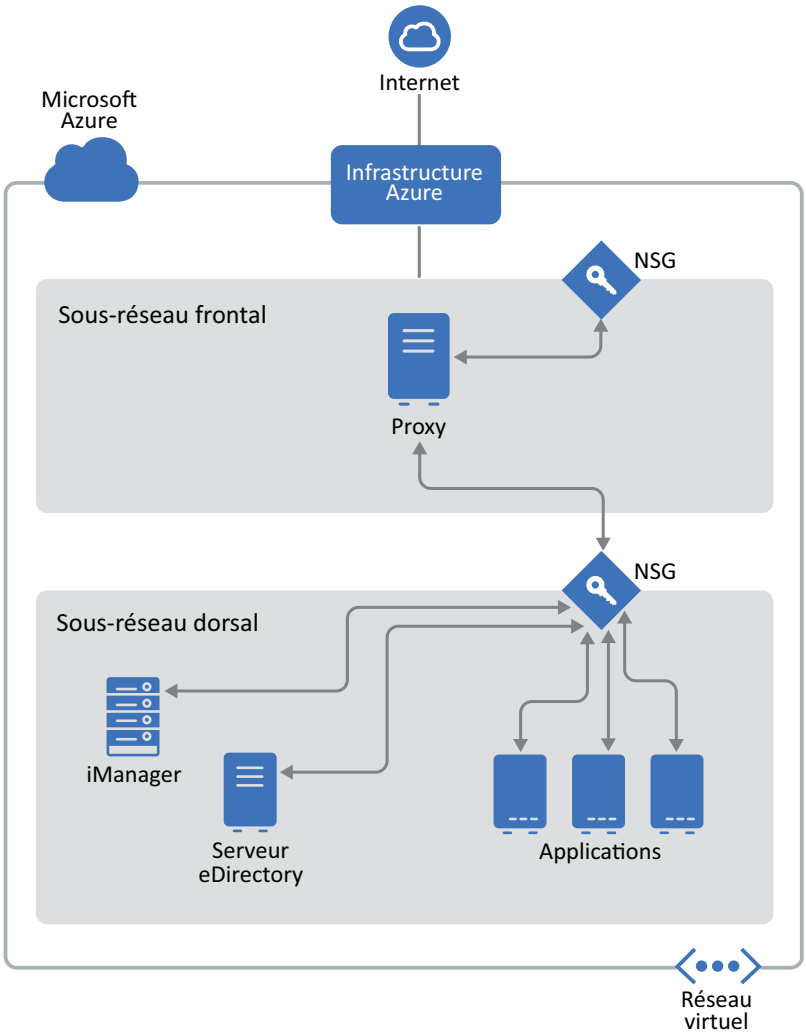
En plus de la configuration système d'eDirectory, veillez à respecter les exigences suivantes :

- Un compte d'administration dans Azure.
- Le programme d'installation d'eDirectory (tarball) a été téléchargé et extrait et est disponible pour être copié sur les machines virtuelles.
- Un client SSH permettant de se connecter aux machines virtuelles Azure à partir de la machine cliente.

## Procédure de déploiement

eDirectory ne doit être déployé que dans un sous-réseau dorsal du service Réseau virtuel Azure. La Figure 4-1 illustre un exemple de déploiement utilisé dans les sections suivantes.

*Figure 4-1 Déploiement d'eDirectory dans Azure*




**REMARQUE**

- Un proxy est un hôte bastion du sous-réseau frontal auquel l'administrateur se connecte à l'aide de SSH et se connecte aux autres instances du sous-réseau dorsal à l'aide du réacheminement de l'agent SSH.
- Les applications qui ont besoin d'accéder à eDirectory doivent être déployées dans le sous-réseau dorsal. Si ces applications doivent être accessibles à partir d'Internet, configurez un équilibreur de charge Azure dans le sous-réseau frontal pour activer l'accès. Pour plus d'informations, reportez-vous à la section Créer un équilibreur de charge de base public.

La procédure de déploiement comporte les étapes suivantes :


- « Préparation des services Azure » page 77
- « Configuration de groupes de sécurité d'application (ASG) » page 77
- « Configuration de groupes de sécurité réseau (NSG) pour les sous-réseaux » page 78
- « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 80
- « Création d'une paire de clés SSH » page 83

# Préparation des services Azure

Cette section décrit les étapes générales à suivre pour créer les services Azure à utiliser avec eDirectory, notamment la création de groupes de ressources, de réseaux virtuels (VNet) et de sous-réseaux.

---

**IMPORTANT :** lors de la création de services (réseau virtuel, groupes de sécurité, machines virtuelles, etc.), veillez à spécifier la même valeur d'**emplacement**.

---

## Création de groupes de ressources

Un groupe de ressources est un conteneur qui renferme des ressources associées pour une solution Azure. Le groupe de ressources peut comprendre toutes les ressources de la solution ou uniquement celles que vous voulez gérer en tant que groupe. Par exemple, lors du déploiement d'eDirectory sur Azure, les groupes de ressources doivent contenir des machines virtuelles, un réseau virtuel, des groupes de sécurité d'application, des groupes de sécurité réseau, une adresse IP publique, une interface réseau et des disques. Pour plus d'informations sur la création d'un groupe de ressources, reportez-vous à l'article Gérer des ressources Azure à l'aide du portail Azure.

---

**REMARQUE :** les administrateurs peuvent ne pas tous être autorisés à créer un groupe de ressources.

---

## Création d'un réseau virtuel

Le service Réseau virtuel Azure permet à de nombreux types de ressources Azure, comme les machines virtuelles (VM) Azure, de communiquer en toute sécurité entre eux, avec Internet et avec les réseaux locaux. Pour plus d'informations, reportez-vous à l'article Présentation du réseau virtuel Azure.

Dans le cadre de la création d'un réseau virtuel, un sous-réseau est créé par défaut. Si vous souhaitez créer plusieurs sous-réseaux, accédez au nouveau **Réseau virtuel** > **Sous-réseau** > **Ajouter un sous-réseau**.

# Configuration de groupes de sécurité d'application (ASG)

Grâce aux groupes de sécurité d'application, vous pouvez configurer la sécurité réseau en tant qu'extension naturelle de la structure d'une application. Vous pouvez également regrouper des machines virtuelles et définir des stratégies de sécurité réseau en fonction de ces groupes. Pour plus d'informations, reportez-vous à la section Groupes de sécurité d'application.

Avant de configurer les groupes de sécurité réseau, vous devez créer les groupes de sécurité d'application suivants :

*Tableau 4-1 Groupes de sécurité d'application*

| Nom | Description |
|---|---|
| SSH_Proxy | Contient l'interface réseau de la machine virtuelle sur laquelle SSH_Proxy sera configuré. |
| eDirectory | Contient l'interface réseau de toutes les machines virtuelles sur lesquelles eDirectory sera configuré. |
| eDirectory_CA | Contient l'interface réseau de la machine virtuelle sur laquelle le serveur eDirectory qui héberge l'autorité de certification de l'arborescence sera configuré. |
| iManager | Contient l'interface réseau de la machine virtuelle sur laquelle iManager sera configuré. |

## Configuration de groupes de sécurité réseau (NSG) pour les sous-réseaux

Vous pouvez filtrer le trafic réseau entrant et sortant pour un sous-réseau à l'aide d'un groupe de sécurité réseau (NSG). Les NSG contiennent des règles de sécurité qui filtrent le trafic réseau par adresse IP, port et protocole.

Cette section décrit les règles qui permettent de créer un NSG pour le sous-réseau frontal. Configurez les règles suivantes sur les règles de sécurité par défaut :

- Règles entrantes :

*Tableau 4-2 Règles entrantes pour le sous-réseau frontal*

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | SSH | TCP 22 | N'importe laquelle | SSH_Proxy (ASG) | ALLOW | Autorise la connexion SSH au serveur proxy à partir d'Internet. |
| 110 | Allow Subnet Traffic (Autoriser le trafic de sous-réseau) | N'importe laquelle | Tout | Sous-réseau frontal | ALLOW | (Conditionnel) Autorise tout le trafic intra-sous-réseau.<br>**REMARQUE :**<br>Ne définissez cette règle que si d'autres machines virtuelles du sous-réseau frontal doivent communiquer entre eux. |

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 120 | All Traffic (Tout le trafic) | Toutes | Tout | Tout | DENY | Refuse tout le trafic entrant qui n'est pas géré par une règle précédente. |

Cette section décrit les règles qui permettent de créer des NSG dans le sous-réseau dorsal. Configurez les règles suivantes pour les groupes de sécurité réseau :

- Règles entrantes :

***Tableau 4-3*** *Règles entrantes pour le sous-réseau dorsal*

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | SSH | TCP 22 | Proxy (ASG) | Sous-réseau dorsal | ALLOW | Autorise le trafic SSH entrant depuis le proxy SSH. |
| 110 | iManager | TCP 8443 | Proxy (ASG) | iManager (ASG) | ALLOW | Autorise le trafic HTTPS pour l'accès à iManager à partir d'un proxy SSH. |
| 120 | HTTP CRL | TCP 8028 | Réseau virtuel | eDirectory_CA (ASG) | ALLOW | Nécessaire pour accéder à la liste de révocation de certificats (CRL) de l'arborescence eDirectory à partir du réseau virtuel lorsque des services du réseau virtuel sont configurés avec des certificats émis par l'autorité de certification de l'arborescence. |

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 130 | Allow Subnet Traffic (Autoriser le trafic de sous-réseau) | N'importe laquelle | Sous-réseau dorsal | Sous-réseau dorsal | ALLOW | Autorise tout le trafic intra-sous-réseau. |
| 140 | All Traffic (Tout le trafic) | Toutes | Tout | Tout | DENY | Refuse tout le trafic entrant. |

## Configuration de groupes de sécurité réseau pour une machine virtuelle

Un groupe de sécurité est un ensemble de règles de pare-feu virtuel qui peuvent être assignées à une ou plusieurs machines virtuelles du réseau virtuel.

Par défaut, un nouveau groupe de sécurité autorise uniquement le trafic entrant sur le port 22, ce qui ne vous permet de vous connecter à l'instance qu'à l'aide de SSH.

Pour plus d'informations, reportez-vous à l'article Groupes de sécurité.

Pour déployer eDirectory dans Azure, créez les groupes de sécurité réseau suivants : eDirectory_NSG_1, eDirectory_NSG_2 et iManager_NSG. Créez ces groupes de sécurité à l'aide des règles de port suivantes sur les règles de sécurité par défaut :

1. **eDirectory_NSG_1 :** ce groupe NSG doit être associé à la machine virtuelle qui héberge l'autorité de certification de l'arborescence eDirectory.

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | SSH | TCP 22 | SSH Proxy (ASG) | eDirectory (ASG) | ALLOW | Autorise le trafic SSH depuis le proxy SSH. |
| 110 | NCP | TCP 524 | Sous-réseau dorsal | eDirectory (ASG) | ALLOW | Autorise le trafic NCP pour eDirectory dans le sous-réseau dorsal. |

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 120 | HTTP CRL | TCP 8028 | Réseau virtuel | eDirectory_CA (ASG) | ALLOW | Nécessaire pour accéder à la liste de révocation de certificats (CRL) de l'arborescence eDirectory à partir du réseau virtuel lorsque des services du réseau virtuel sont configurés avec des certificats émis par l'autorité de certification de l'arborescence. |
| 130 | LDAPS | TCP 636 | Sous-réseau dorsal | eDirectory (ASG) | ALLOW | Autorise le trafic LDAP sécurisé dans le sous-réseau dorsal. |
| 140 | SLP | N'importe laquelle (427) | Sous-réseau dorsal | eDirectory (ASG) | ALLOW | Autorise le trafic SLP dans le sous-réseau dorsal. |
| 150 | All Traffic (Tout le trafic) | Toutes | Tout | Tout | DENY | Refuse tout le trafic entrant. |

**REMARQUE :** les serveurs eDirectory ne doivent pas être configurés pour écouter le port LDAP 389 et l'accès au port 389 ne doit pas être autorisé dans le groupe de sécurité assigné à eDirectory. En outre, l'accès au port HTTP doit uniquement être autorisé dans le groupe de sécurité assigné au serveur eDirectory qui héberge l'autorité de certification de l'arborescence.

2. **eDirectory_NSG_2 :** ce groupe NSG doit être associé à toutes les machines virtuelles qui hébergent des serveurs eDirectory autres que l'autorité de certification de l'arborescence eDirectory.

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | SSH | TCP 22 | SSH Proxy (ASG) | eDirectory (ASG) | ALLOW | Autorise le trafic SSH depuis le proxy SSH. |
| 110 | NCP | TCP 524 | Sous-réseau dorsal | eDirectory (ASG) | ALLOW | Autorise le trafic NCP pour eDirectory dans le sous-réseau dorsal. |
| 120 | LDAPS | TCP 636 | Sous-réseau dorsal | eDirectory (ASG) | ALLOW | Autorise le trafic LDAP sécurisé dans le sous-réseau dorsal. |
| 130 | SLP | N'importe laquelle (427) | Sous-réseau dorsal | eDirectory (ASG) | ALLOW | Autorise le trafic SLP dans le sous-réseau dorsal. |
| 140 | All Traffic (Tout le trafic) | Toutes | Tout | Tout | DENY | Refuse tout le trafic entrant. |

3. **iManager_NSG :** ce groupe NSG doit être associé à la machine virtuelle qui héberge iManager. Les règles NSG suivantes autorisent l'accès au serveur iManager à partir du serveur proxy uniquement.

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | SSH | TCP 22 | SSH Proxy (ASG) | iManager (ASG) | ALLOW | Autorise le trafic SSH depuis le proxy. |
| 110 | HTTPS | TCP 8443 | SSH Proxy (ASG) | iManager (ASG) | ALLOW | Autorise le trafic HTTP sécurisé pour l'accès à iManager à partir du proxy. |
| 120 | All Traffic (Tout le trafic) | Toutes | Tout | Tout | DENY | Refuse tout le trafic entrant. |

## Création d'une paire de clés SSH

Vous devez créer une paire de clés SSH avant de configurer les machines virtuelles Azure. Pour créer une paire de clés, procédez comme suit :

1. Créez une paire de clés SSH RSA 4 096 bits sur le client à l'aide de la commande suivante :

   ```
   ssh-keygen -t rsa -b 4096
   ```

   `ssh-keygen` place la nouvelle clé publique dans `~/.ssh/id_rsa.pub`.

2. Fournissez la clé publique SSH ci-dessus à votre compte Azure. Pour plus d'informations, reportez-vous à la section Fournir une clé publique SSH.

---

**IMPORTANT :** vous pouvez vous connecter à vos machines virtuelles et les gérer uniquement à l'aide de la clé privée SSH. Par conséquent, veillez à ne pas perdre la clé privée SSH.

---

## Création et déploiement de machines virtuelles

Créez et lancez vos machines virtuelles (VM) sur l'une des plates-formes prises en charge. Pour plus d'informations sur la création et sur le lancement de machines virtuelles, reportez-vous à la section Créer et lancer votre machine virtuelle Linux. Dans le cadre de la création et du lancement des instances, vous devez également effectuer les étapes suivantes :

1. Associez eDirectory_NSG_1 aux machines virtuelles sur lesquelles le premier serveur eDirectory sera configuré, eDirectory_NSG_2 à la machine virtuelle sur laquelle tous les autres serveurs eDirectory seront configurés et iManager_NSG avec la machine virtuelle sur laquelle iManager sera configuré. Pour plus d'informations sur les groupes de sécurité, reportez-vous à la section « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 80.
2. Associez la clé publique créée à la section « Création d'une paire de clés SSH » page 83 à vos instances.

---

**REMARQUE :** lorsque plusieurs zones de disponibilité sont disponibles pour l'emplacement Azure sélectionné, les serveurs de répliques ne doivent pas être déployés dans la même zone de disponibilité que le serveur eDirectory maître.

---

## Configuration d'un disque de données pour le stockage des données eDirectory

La configuration d'un disque de données est nécessaire pour éviter la perte des données et de la configuration d'eDirectory en cas de crash de la machine virtuelle Azure. Pour plus d'informations sur la récupération des données et de la configuration d'eDirectory, reportez-vous à la section « Reprise après sinistre » page 89. Une fois la machine virtuelle créée, procédez comme suit pour préparer la machine virtuelle pour le déploiement d'eDirectory :

1. Créez et attachez un disque de données. Pour cela, suivez la procédure décrite dans l'article Utiliser le portail pour attacher un disque de données à une machine virtuelle Linux.
2. Connectez-vous à la machine virtuelle, formatez le disque de données avec le système de fichiers `ext4`, puis montez ce disque. Pour plus d'informations sur le formatage et sur le montage du disque de données, reportez-vous à la section Se connecter à la machine virtuelle Linux afin de monter le nouveau disque.

3 Effectuez un montage de liaison des répertoires du disque de données vers les répertoires de données eDirectory/NICI. Procédez comme suit en tant qu'utilisateur root pour effectuer le montage de liaison :

**3a** Créez le répertoire de données eDirectory à l'aide de la commande suivante :

```
mkdir <mount_point>/eDirectory_data
```

**3b** Créez le répertoire de données NICI à l'aide de la commande suivante :

```
mkdir <mount_point>/nici_data
```

**3c** Créez les répertoires de configuration NICI et eDirectory à l'aide de la commande suivante :

```
mkdir <mount_point>/eDirectory_nici_conf
```

**3d** Créez les répertoires nécessaires pour eDirectory à l'aide des commandes suivantes :

```
mkdir --parents /var/opt/novell/eDirectory
mkdir –-parents /var/opt/novell/nici
mkdir –-parents /etc/opt/novell/eDirectory
```

**3e** Pour effectuer le montage de liaison des répertoires, ajoutez les éléments suivants à `/etc/fstab` :

```
<mount_point>/eDirectory_data /var/opt/novell/eDirectory none
defaults,bind 0 0

<mount_point>/nici_data /var/opt/novell/nici none defaults,bind 0 0

<mount_point>/eDirectory_nici_conf /etc/opt/novell/eDirectory none
defaults,bind 0 0
```

---

**REMARQUE :** toutes les opérations dans la machine virtuelle doivent être effectuées en tant qu'utilisateur root.

---

# Installation d'eDirectory et d'iManager

## Conditions préalables

- ❒ Veillez à respecter la configuration requise indiquée à la section Configuration système requise.
- ❒ Créez des groupes de sécurité comme indiqué à la section « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 80.
- ❒ La machine virtuelle proxy doit être un serveur renforcé et sécurisé. La clé privée SSH requise pour accéder aux machines virtuelles du sous-réseau dorsal et à la machine virtuelle proxy ne doit pas être stockée sur le réseau virtuel, mais uniquement sur le client. Choisissez une taille de machine virtuelle dont les performances et la mémoire sont adaptées à cette instance.
- ❒ Créez une interface réseau supplémentaire pour la machine virtuelle proxy et assignez une adresse IP publique statique à cette interface.
- ❒ Configurez le serveur VNC dans la machine virtuelle proxy. Le serveur VNC doit être renforcé par un mot de passe fort adapté. Connectez-vous au serveur VNC via un tunnel SSH afin de permettre des communications sécurisées. Le serveur VNC doit être configuré pour écouter uniquement les connexions depuis l'hôte local. Désactivez le verrouillage de l'écran pour éviter le verrouillage de la session. Après avoir utilisé le serveur VNC, mettez fin à la session.

- ❒ Mettez à jour manuellement le fichier `/etc/hosts` des machines virtuelles avec l'entrée `IP-Address Full-Qualified-Hostname Short-Hostname`. Cette mise à jour permet de contourner la limitation liée à Azure pour effectuer une recherche DNS inverse.
- ❒ Connectez-vous à la machine virtuelle du sous-réseau dorsal sur laquelle eDirectory/iManager sera configuré à l'aide du proxy SSH :

  ```
  ssh -i edir_key.pem -A -J azureuser@<ssh_proxy_ip>
  azureuser@<instance_private_ip>
  ```

  **REMARQUE**

  - Dans les exemples de commandes ci-dessus, `edir_key.pem` correspond à un exemple de nom de fichier contenant la clé de serveur.
  - Vous pouvez également ajouter le fichier d'identité dans l'agent à l'aide de la commande `SSH-Add` pour éviter d'utiliser le fichier d'identité à chaque connexion.

  Pour afficher l'adresse IP privée d'une machine virtuelle, cliquez sur **Instances** > *[instance]* > **Description**.
- ❒ Configurez un serveur Agent Annuaire (DA) SLP dans une machine virtuelle du sous-réseau dorsal. Ouvrez le port 427 dans la règle entrante du groupe NSG pour la machine virtuelle sur laquelle le DA SLP est déployé. Activez l'opération DA en éditant le fichier `slp.conf`. Pour plus d'informations, reportez-vous à la section Configuration de OpenSLP pour eDirectory du *guide d'administration de NetIQ eDirectory*.

## Procédure d'installation et de configuration

Cette section fournit les instructions détaillées à suivre pour installer et configurer eDirectory et iManager dans un environnement Azure. Une fois eDirectory installé, assurez-vous que les conditions suivantes sont respectées :

- EBA est activé.
- SNMP est désactivé.
- eDirectory n'écoute pas le port 389.
- Les services LDAP et HTTP sont configurés pour utiliser les certificats ECDSA uniquement.
- L'accès au port SSH des machines virtuelles Azure du sous-réseau dorsal doit être désactivé lorsqu'il n'est pas utilisé.
- Désactivez les modules iMonitor, eMBox et DHost afin de renforcer la sécurité. Une fois qu'ils sont désactivés, toutes les activités impliquant ces modules doivent être effectuées à l'aide des utilitaires NDS uniquement.

### Installation et configuration d'eDirectory

1. Copiez le fichier `eDirectory_<version>_Linux_x86_64.tar.gz` à l'aide de Secure Copy (scp) vers la machine virtuelle du sous-réseau dorsal sur laquelle eDirectory sera configuré à l'aide du proxy SSH :

   ```
   scp -i <keyname> -o ProxyJump=vm-user@<ssh_proxy_ip>
   eDirectory_<version>_Linux_x86_64.tar.gz vm-user@<instance_ip>:/<directory>
   ```

2. Installez eDirectory. Pour plus d'informations, reportez-vous à la section Exécution de l'utilitaire nds-install pour installer des composants eDirectory.

3 Configurez eDirectory. Pour plus d'informations, reportez-vous à la section Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques eDirectory. Voici un exemple de commande qui permet d'installer et de configurer eDirectory :

```
ndsconfig  new [-t <tree_name>] [-n <server context>] -a <admin FDN> [-w <admin
password>] -P ldaps://<instance_ip> --configure-eba-now yes
```

4 Installez `openslp-server`, puis démarrez le service SLPD.

### Installation et configuration d'iManager

Grâce à la console d'administration d'iManager, vous pouvez gérer les opérations eDirectory dans votre environnement Azure. iManager doit être installé sur votre machine virtuelle Azure après l'installation d'eDirectory.

1 Copiez le fichier `iMan_<version>_linux_x86_64.tgz` à l'aide de Secure Copy (scp) vers l'instance du sous-réseau dorsal sur laquelle iManager sera configuré à l'aide du proxy SSH :

```
scp -i <keyname> -o ProxyJump=vm-user@<ssh_proxy_ip>
iMan_<version>_linux_x86_64.tgz vm-user@<instance_ip>:/<directory>
```

2 Installez et configurez iManager. Pour plus d'informations, reportez-vous à la section Installation d'iManager Server sous Linux. Avant d'installer iManager, reportez-vous à la section Configuration système requise dans le *guide d'installation d'iManager*.

3 Téléchargez le certificat de l'autorité de certification EBA sur la machine virtuelle sur laquelle iManager est exécuté. Pour plus d'informations, reportez-vous à la section Gestion de l'autorité de certification EBA à l'aide d'iManager dans le *guide d'administration de NetIQ eDirectory*.

4 Remplacez les certificats auto-signés dans la machine virtuelle exécutant iManager par des certificats signés par une autorité de certification. Pour plus d'informations, reportez-vous à la section Remplacement des certificats auto-signés temporaires pour iManager.

---

**REMARQUE :** veillez à configurer le serveur iManager pour qu'il n'utilise que des certificats ECDSA. Après avoir installé iManager, spécifiez un utilisateur autorisé ainsi que le nom de l'arborescence eDirectory appropriée que cet utilisateur va gérer.

---

### Lancement d'iManager

Procédez comme suit pour lancer iManager :

1 Connectez-vous au serveur VNC exécuté sur l'hôte local de la machine virtuelle proxy via le tunnel SSH.

2 Installez et lancez un navigateur dans la même instance.

3 Lancez l'arborescence eDirectory et connectez-vous à l'aide de l'adresse IP ou du nom de l'arborescence.

## Tâches de post-configuration

1 Pour vérifier si EBA est activé, reportez-vous à la section Affichage des informations relatives à l'authentification EBA dans le *guide d'administration de NetIQ eDirectory*.

2 Activez SuiteB dans Certificate Server. Pour plus d'informations, reportez-vous à la section Activation de SuiteB dans Certificate Server dans le *guide d'administration de NetIQ eDirectory*.

3 Configurez la clé d'arborescence AES 256 bits pour le premier serveur eDirectory. Pour plus d'informations, reportez-vous à la section Creating an AES 256-Bit Tree Key (Création d'une clé d'arborescence AES 256 bits) dans le document *NICI Administration Guide* (Guide d'administration de NICI).

4 Supprimez les points de distribution CRL sur le premier serveur eDirectory. L'accès LDAP non sécurisé sur le port 389 étant désactivé sur tous les serveurs eDirectory, la CRL pour l'autorité de certification de l'arborescence devrait être disponible au téléchargement par HTTP uniquement. Procédez comme suit pour supprimer les points de distribution CRL :

   **4a** Connectez-vous à iManager en tant qu'administrateur.

   **4b** Sélectionnez **Rôles et tâches** > **NetIQ Certificate Server** > **Configure Certificate Authority** (Configurer l'autorité de certification).

   **4c** Cliquez sur **CRL**.

   **4d** Cliquez sur **One**. Sélectionnez et supprimez tous les **points de distribution CRL**, à l'exception du point de distribution CRL HTTP (http://<IP_instance>:8028/crl/one.crl).

   **4e** Cliquez sur **Appliquer**, puis sur **Fermer**.

   **4f** Cliquez sur **OneEC**. Sélectionnez et supprimez tous les **points de distribution CRL**, à l'exception du point de distribution CRL HTTP (http://<IP_instance>:8028/crl/oneec.crl).

   **4g** Cliquez sur **Appliquer**, puis sur **OK**.

5 Réparez les certificats par défaut du serveur à l'aide du plug-in iManager Certificate Server. Pour cela, procédez comme suit :

   **5a** Connectez-vous à iManager en tant qu'administrateur.

   **5b** Sélectionnez **Rôles et tâches** > **NetIQ Certificate Server** > **Réparer les certificats par défaut**.

   **5c** Sélectionnez le ou les serveurs qui possèdent les certificats, puis cliquez sur **Suivant**.

   **5d** Sélectionnez **Tous les certificats par défaut sont écrasés**, puis cliquez sur **Suivant**.

   **5e** Examinez les tâches à effectuer, puis cliquez sur **Terminer**.

6 Configurez les services LDAP et HTTP pour qu'ils utilisent les certificats ECDSA et les Ciphers SuiteB. Pour plus d'informations, reportez-vous à la section Configuration des services LDAP et HTTP pour qu'ils utilisent les certificats ECDSA et les Ciphers SuiteB dans le *guide d'administration de NetIQ eDirectory*. Une fois l'opération terminée, redémarrez eDirectory.

7 Pour plus d'informations pour vérifier si le sous-agent SNMP est déchargé, reportez-vous à la section Chargement et déchargement du module serveur SNMP dans le *guide d'administration de NetIQ eDirectory*.

8 Assurez-vous qu'eDirectory n'écoute pas le port 389.

9 Désactivez iMonitor, eMBox, DHost et la pile HTTP.

   **9a** Procédez comme suit pour désactiver iMonitor, eMBox et DHost sur le serveur eDirectory qui héberge l'autorité de certification de l'arborescence :

      **9a1** Éditez le fichier `ndsmodules.conf` en commentant `hconserv`, `imon` et `embox`.

      **9a2** Redémarrez eDirectory.

   **9b** Procédez comme suit pour désactiver la pile HTTP dans les serveurs de répliques eDirectory :

      **9b1** Éditez le fichier `ndsmodules.conf` en commentant `httpstk`, `hconserv`, `imon` et `embox`.

      **9b2** Redémarrez eDirectory.

**REMARQUE :** `httpstk` doit être placé au-dessus de `nds` dans le fichier `ndsmodules.conf` avant les commentaires. Le module `nds` cesse alors d'activer la pile HTTP.

10 Configurez SLP pour forcer eDirectory à utiliser la monodiffusion comme méthode d'annonce. Éditez le fichier `slp.conf` en indiquant l'adresse IP du serveur DA dans le sous-réseau dorsal. Pour plus d'informations, reportez-vous à la section Paramètres de configuration du *guide d'administration de NetIQ eDirectory*.

**REMARQUE :** après avoir configuré toutes les machines virtuelles eDirectory et iManager, configurez les règles de sécurité du sous-réseau dorsal Azure pour interdire l'accès au port SSH et l'autoriser uniquement si nécessaire.

# Déploiement des services d'audit

Vous pouvez déployer le service d'audit Common Event Format (CEF) sur Azure pour auditer divers événements eDirectory. Procédez comme suit pour déployer les services d'audit CEF :

1 Installez un serveur d'audit dans le réseau virtuel.

2 Configurez le serveur d'audit pour qu'il écoute un port.

**REMARQUE :** il est recommandé d'utiliser Sentinel comme serveur d'audit.

3 Créez une règle de groupe de sécurité réseau dans le sous-réseau frontal avec la configuration suivante et associez-la à la machine virtuelle sur laquelle le serveur d'audit s'exécute :

| Nom | Port | Source | Destination | Description |
|---|---|---|---|---|
| Port du serveur d'audit | TCP (port du serveur d'audit) | Sous-réseau dorsal | IP du serveur d'audit | Autorise la réception des événements provenant des serveurs eDirectory. |

4 Mettez à jour les éléments suivants dans le fichier `/etc/opt/novell/eDirectory/conf/auditlogconfig.properties` sur toutes les instances d'eDirectory :

```
log4j.appender.S.Host=<Auditing server ip>
log4j.appender.S.Port=<auditing server port>
```

5 Activez les événements CEF correspondants à partir d'iManager. Pour plus d'informations, reportez-vous à la section Configuration des événements CEF pour l'audit. Les événements activés sont transmis au serveur d'audit.

# Reprise après sinistre

La reprise après sinistre est effectuée en cas de crash d'une machine virtuelle sur laquelle eDirectory était exécuté. Procédez comme suit pour effectuer une reprise après sinistre :

1. Arrêtez la machine virtuelle qui a subi un crash et dissociez le disque de données de cette machine. Pour plus d'informations, reportez-vous à l'article Comment détacher un disque de données d'une machine virtuelle Linux.
2. Configurez une nouvelle machine virtuelle avec le même système d'exploitation que la machine virtuelle qui a subi le crash.
3. Installez la même version d'eDirectory dans la nouvelle machine virtuelle.
4. Attachez le disque de données à la nouvelle machine virtuelle et montez le système de fichiers. Pour plus d'informations, reportez-vous à l'article Utiliser le portail pour attacher un disque de données à une machine virtuelle Linux.
5. Effectuez le montage de liaison des répertoires.

   Pour effectuer le montage de liaison des répertoires, mettez à jour les éléments suivants dans `/etc/fstab` :

   ```
   <mount_point>/eDirectory_data /var/opt/novell/eDirectory none defaults,bind 0 0
   ```

   ```
   <mount_point>/nici_data /var/opt/novell/nici none defaults,bind 0 0
   ```

   ```
   <mount_point>/eDirectory_nici_conf /etc/opt/novell/eDirectory none defaults,bind 0 0
   ```

6. Remplacez l'adresse IP dans `/etc/opt/novell/eDirectory/conf/nds.conf` par l'adresse IP de la machine virtuelle actuelle.
7. Mettez à niveau eDirectory en ignorant la vérification de l'état de santé. Pour plus d'informations, reportez-vous à la section *Mise à niveau d'eDirectory* dans le guide d'installation de NetIQ eDirectory.
8. Réparez les adresses réseau à l'aide de l'utilitaire `ndsrepair`. Pour plus d'informations, reportez-vous à la section*Options DSRepair* du guide d'administration de NetIQ eDirectory.
9. Modifiez l'adresse?  IP du point de distribution CRL si l'adresse IP de l'autorité de certification de l'arborescence a changé. Pour plus d'informations sur la modification de l'adresse IP, reportez-vous à la section Affichage et modification des propriétés d'un objet Configuration CRL dans le guide d'administration de NetIQ eDirectory.
10. Réparez les certificats par défaut du serveur à l'aide du plug-in iManager Certificate Server. Pour cela, procédez comme suit :

    **10a** Connectez-vous à iManager en tant qu'administrateur.

    **10b** Sélectionnez **Rôles et tâches** > **NetIQ Certificate Server** > **Réparer les certificats par défaut**.

    **10c** Sélectionnez le ou les serveurs qui possèdent les certificats, puis cliquez sur **Suivant**.

    **10d** Sélectionnez **Tous les certificats par défaut sont écrasés**, puis cliquez sur **Suivant**.

    **10e** Examinez les tâches à effectuer, puis cliquez sur **Terminer**.
11. Configurez les services LDAP et HTTP pour qu'ils utilisent les nouveaux certificats ECDSA.

# 5 Déploiement d'eDirectory sur Amazon Web Services EC2

eDirectory peut être déployé sur des instances Amazon Web Services (AWS) EC2.

eDirectory prend en charge les systèmes d'exploitation suivants sur AWS EC2 :

- SUSE Linux Enterprise Server (SLES) 12 SP3
- SUSE Linux Enterprise Server (SLES) 12 SP4
- SUSE Linux Enterprise Server 15
- Red Hat Enterprise Linux (RHEL) 7.5
- Red Hat Enterprise Linux (RHEL) 7.6

## Conditions préalables

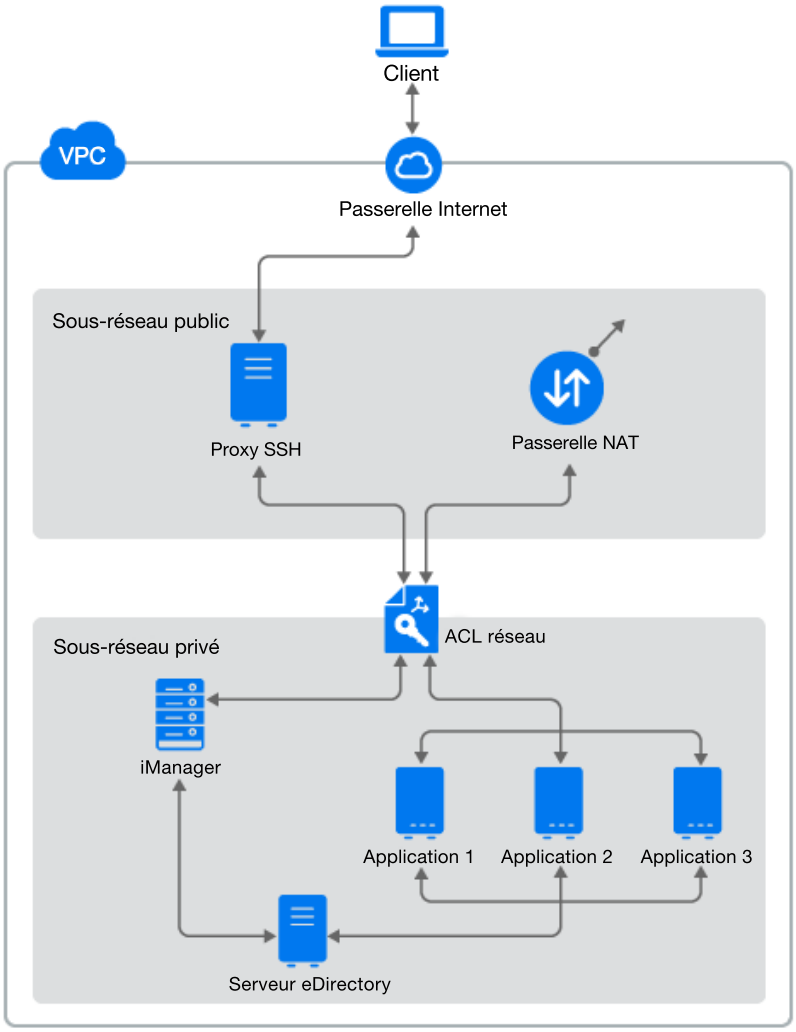
En plus de la configuration système requise pour eDirectory, veillez à respecter les exigences suivantes :

- Un compte d'administration dans AWS EC2.
- Le programme d'installation d'eDirectory (tarball) a été téléchargé et extrait et est disponible pour être copié sur les instances.
- Un client SSH permettant de se connecter aux instances AWS EC2 à partir de la machine cliente.

## Procédure de déploiement

eDirectory ne doit être déployé que dans un sous-réseau privé dans Amazon VPC. La Figure 4-1 illustre un exemple de déploiement utilisé dans les sections suivantes.

*Figure 5-1 Déploiement d'eDirectory dans AWS EC2*




**REMARQUE**

- Un proxy SSH est un hôte bastion du sous-réseau public auquel l'administrateur se connecte à l'aide de SSH et se connecte aux autres instances du sous-réseau privé à l'aide du réacheminement de l'agent SSH.
- Les applications qui ont besoin d'un accès à eDirectory doivent être déployées dans le sous-réseau privé. Si ces applications doivent être accessibles à partir d'Internet, configurez un équilibreur de charge AWS EC2 dans le sous-réseau public pour activer l'accès. Pour plus d'informations, reportez-vous à l'article Create an Application Load Balancer (Créer un équilibreur de charge d'application).

La procédure de déploiement comporte les étapes suivantes :


- « Préparation d'AWS Virtual Private Cloud » page 93
- « Configuration des ACL réseau » page 94
- « Configuration des groupes de sécurité » page 95
- « Création d'une paire de clés SSH » page 97
- « Création et déploiement d'instances » page 97

# Préparation d'AWS Virtual Private Cloud

Cette section décrit les étapes générales à suivre pour configurer AWS VPC à utiliser avec eDirectory. Pour plus d'informations, reportez-vous à la documentation Amazon Elastic Compute Cloud.

Procédez comme suit pour créer les services AWS VPC :

1. Connectez-vous à AWS Management Console.
2. Créez les services suivants :

| Service | Description |
|---|---|
| **VPC** | Vous pouvez créer un service VPC à l'aide de la console Amazon VPC. Pour plus d'informations sur la création d'un service VPC, reportez-vous à l'article Creating a VPC (Création d'un VPC).<br><br>Pour obtenir une présentation de VPC, reportez-vous à la Documentation Amazon Virtual Private Cloud. |
| **IMPORTANT :** lors de la création d'un service VPC à l'aide de l'**Assistant de démarrage d'un VPC**, deux sous-réseaux, des passerelles Internet, une table de routage et une passerelle NAT sont créés pour le VPC. Vous pouvez afficher ou éditer ces éléments comme suit : | |
| **Sous-réseaux** | Dans le cadre de la création d'un VPC, deux sous-réseaux sont créés : un sous-réseau public et un privé. eDirectory doit être déployé dans le sous-réseau privé. Comme illustré à la Figure 4-1, toutes les applications qui accèdent à eDirectory doivent être déployées dans le même sous-réseau privé. L'accès SSH aux instances du sous-réseau privé doit s'effectuer via le proxy SSH du sous-réseau public. Pour plus d'informations, reportez-vous à l'article VPC et sous-réseaux. |
| **Passerelles Internet** | Une passerelle Internet est nécessaire pour activer la connexion SSH au proxy SSH, comme illustré à la Figure 4-1. Pour plus d'informations sur la création et sur l'attachement de passerelles Internet avec VPC, reportez-vous à l'article Passerelles Internet. |
| **Table de routage** | Pour plus d'informations sur la création d'une table de routage, reportez-vous à l'article Tables de routage. |
| **Passerelle NAT** | Une passerelle NAT est nécessaire pour que les instances qui se trouvent dans le sous-réseau privé puissent télécharger les mises à jour du système d'exploitation. Pour plus d'informations sur la création d'une passerelle NAT, reportez-vous à l'article Passerelles NAT. |
| **Adresse IP Elastic** | Une adresse IP Elastic est une adresse IP statique publique qui doit être assignée à l'instance qui exécute le proxy SSH et la passerelle NAT. Pour plus d'informations sur la création d'une adresse IP Elastic, reportez-vous à la section Utilisation d'adresses IP Elastic. |

# Configuration des ACL réseau

Une liste de contrôle d'accès (ACL) est une couche de sécurité facultative pour le VPC qui sert de pare-feu pour contrôler le trafic entrant et sortant d'un ou de plusieurs sous-réseaux. Pour plus d'informations, reportez-vous à l'article ACL réseau.

Cette section décrit les règles qui permettent de créer des ACL réseau dans le sous-réseau privé. Configurez les règles suivantes pour les ACL réseau dans le sous-réseau privé :

- Règles entrantes :

***Tableau 5-1***

| Règle | Type | Plage de ports | Source | Opération | Description |
|---|---|---|---|---|---|
| 10 | SSH | TCP 22 | *<Adresse_IP_proxy_SSH>*/32 | ALLOW | Autorise le trafic SSH entrant à partir de l'adresse IP du proxy SSH dans le sous-réseau public. |
| 15 | HTTPS | TCP 8443 | *<Adresse_IP_proxy_SSH>*/32 | ALLOW | Autorise le trafic HTTPS entrant à partir de l'adresse IP du proxy SSH dans le sous-réseau public. |
| 20 | Règle TCP personnalisée | TCP 32768-65535 | 0.0.0.0/0 | ALLOW | Autorise le trafic de retour entrant depuis les hôtes sur Internet qui répondent aux requêtes provenant du sous-réseau. |
| * | All Traffic (Tout le trafic) | Toutes | 0.0.0.0/0 | DENY | Refuse tout le trafic IPv4 entrant qui n'est pas géré par une règle précédente (non modifiable). |

- Règles sortantes :

*Tableau 5-2*

| Règle | Type | Plage de ports | Destination | Opération | Description |
|---|---|---|---|---|---|
| 10 | Règle TCP personnalisée | TCP 32768-65535 | *<Adresse_IP_proxy_SSH>*/32 | ALLOW | Autorise le trafic SSH sortant depuis le sous-réseau privé vers le proxy SSH du sous-réseau public. |
| 12 | Règle TCP personnalisée | TCP 32768-65535 | *<Adresse_IP_proxy_SSH>*/32 | ALLOW | Autorise le trafic sortant pour l'accès à iManager à partir du sous-réseau public. |
| 15 | HTTPS | TCP 443 | 0.0.0.0/0 | ALLOW | Autorise le trafic HTTPS sortant depuis le sous-réseau privé vers Internet. |
| 20 | HTTP | TCP 80 | 0.0.0.0/0 | ALLOW | Autorise le trafic HTTP sortant depuis le sous-réseau privé vers Internet. |
| 25 | HTTPS | Numéro de port écouté par le serveur d'audit. | *<Adresse_IP_serveur_audit>* | ALLOW | Autorise l'audit des événements eDirectory.<br>**REMARQUE :**<br>cette règle ne s'applique que si le serveur d'audit se trouve en dehors du sous-réseau privé. |
| * | All Traffic (Tout le trafic) | Toutes | 0.0.0.0/0 | DENY | Refuse tout le trafic IPv4 sortant qui n'est pas géré par une règle précédente (non modifiable). |

# Configuration des groupes de sécurité

Un groupe de sécurité est un ensemble de règles de pare-feu virtuel qui peuvent être assignées à une ou plusieurs instances du VPC.

Par défaut, un nouveau groupe de sécurité autorise uniquement le trafic entrant sur le port 22, ce qui ne vous permet de vous connecter à l'instance qu'à l'aide de SSH.

Pour plus d'informations, reportez-vous à l'article Groupes de sécurité Amazon EC2 pour les instances Linux.

Pour déployer eDirectory sur AWS, créez trois groupes de sécurité. Par exemple, Groupe de sécurité 1, Groupe de sécurité 2 et Groupe de sécurité 3. Créez ces groupes de sécurité avec les règles de port suivantes :

1. **Groupe de sécurité 1 (pour eDirectory) :**

| Port | Source | Description |
|---|---|---|
| TCP 22 | Sous-réseau public | Autorise le trafic SSH depuis le sous-réseau public. |
| TCP 636 | Sous-réseau privé | Autorise le trafic LDAPS dans le sous-réseau privé. |
| TCP 524 | Sous-réseau privé | Autorise le trafic NCP pour eDirectory dans le sous-réseau privé. |
| UDP 427 | Sous-réseau privé | Autorise le trafic SLP dans le sous-réseau privé. |

**REMARQUE :** le port LDAP 389 ne doit pas être activé dans le groupe de sécurité assigné à eDirectory. Le port HTTP ne doit être activé que dans le groupe de sécurité assigné au serveur eDirectory qui héberge l'autorité de certification de l'arborescence.

2. **Groupe de sécurité 2 (pour eDirectory) :**

| Port | Source | Description |
|---|---|---|
| TCP 8028 | VPC | Nécessaire pour accéder à la liste de révocation de certificats (CRL) de l'arborescence eDirectory à partir du VPC lorsque des services du VPC sont configurés avec des certificats émis par l'autorité de certification de l'arborescence. Ce groupe de sécurité est assigné au serveur eDirectory qui héberge l'autorité de certification de l'arborescence. |

3. **Groupe de sécurité 3 (pour iManager) :**

| Port | Source | Description |
|---|---|---|
| TCP 22 | Sous-réseau public | Autorise le trafic SSH depuis le sous-réseau public. |
| TCP 8443 | Sous-réseau·public | Autorise le trafic HTTPS pour l'accès à iManager à partir du sous-réseau public. |

## Création d'une paire de clés SSH

Vous devez créer une paire de clés SSH avant de configurer les instances Amazon EC2. Pour créer une paire de clés, procédez comme suit :

1. Créez une paire de clés SSH RSA 4 096 bits sur le client à l'aide de la commande suivante :

   ```
   ssh-keygen -t rsa -b 4096
   ```

   `ssh-keygen` place la nouvelle clé publique dans `~/.ssh/id_rsa.pub`.

2. Importez la clé publique SSH vers votre compte Amazon EC2.
   Pour·plus·d'informations,·reportez-vous·à·la·section Importation de votre propre clé publique dans Amazon EC2.

---

**IMPORTANT :** vous pouvez vous connecter à vos instances et les gérer uniquement à l'aide de la clé privée SSH. Par conséquent, veillez à ne pas perdre la clé privée SSH.

---

## Création et déploiement d'instances

Créez et lancez vos instances EC2 sur l'une des plates-formes prises en charge. Pour plus d'informations sur la création et le lancement d'instances, reportez-vous à l'article Créer vos ressources EC2 et lancer votre instance EC2. Dans le cadre de la création et du lancement des instances, vous devez également effectuer les étapes suivantes :

1. Associez le groupe de sécurité 1 aux instances dans lesquelles le premier serveur eDirectory sera configuré, le groupe de sécurité 2 à l'instance dans laquelle tous les autres serveurs eDirectory seront configurés et le groupe de sécurité 3 à l'instance dans laquelle iManager sera configuré. Pour plus d'informations sur les groupes de sécurité, reportez-vous à la section « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 80.
2. Associez la clé publique créée à la section « Création d'une paire de clés SSH » page 83 à vos instances.

## Configuration d'un volume EBS pour le stockage des données eDirectory

La configuration d'un volume EBS est nécessaire pour éviter la perte des données et de la configuration d'eDirectory en cas de crash d'une instance EC2. Pour plus d'informations sur la récupération des données et de la configuration d'eDirectory, reportez-vous à la section « Reprise après sinistre » page 89. Une fois l'instance EC2 créée, procédez comme suit pour préparer l'instance pour le déploiement d'eDirectory :

1. Créez un volume EBS. Pour cela, suivez la procédure décrite dans l'article Création d'un volume Amazon EBS.
2. Associez le volume EBS à l'instance EC2. Pour plus d'informations, reportez-vous à l'article Attacher un volume Amazon EBS à une instance.
3. Connectez-vous à l'instance, formatez le volume EBS avec le système de fichiers `ext4`, puis montez ce volume. Pour plus d'informations sur le formatage et sur le montage du volume EBS, reportez-vous à l'article Rendre un volume Amazon EBS disponible à l'utilisation sur Linux.

4 Effectuez un montage de liaison des répertoires du volume EBS vers les répertoires de données eDirectory/NICI. Procédez comme suit en tant qu'utilisateur root pour effectuer le montage de liaison :

**4a** Créez le répertoire de données eDirectory à l'aide de la commande suivante :

```
mkdir <mount_point>/eDirectory_data
```

**4b** Créez le répertoire de données NICI à l'aide de la commande suivante :

```
mkdir <mount_point>/nici_data
```

**4c** Créez les répertoires de configuration NICI et eDirectory à l'aide de la commande suivante :

```
mkdir <mount_point>/eDirectory_nici_conf
```

**4d** Créez les répertoires nécessaires pour eDirectory à l'aide des commandes suivantes :

```
mkdir –-parents /var/opt/novell/eDirectory
mkdir –-parents /var/opt/novell/nici
mkdir –-parents /etc/opt/novell/eDirectory
```

**4e** Pour effectuer le montage de liaison des répertoires, ajoutez les éléments suivants à `/etc/fstab` :

```
<mount_point>/eDirectory_data /var/opt/novell/eDirectory none
defaults,bind 0 0

<mount_point>/nici_data /var/opt/novell/nici none defaults,bind 0 0

<mount_point>/eDirectory_nici_conf /etc/opt/novell/eDirectory none
defaults,bind 0 0
```

---

**REMARQUE :** toutes les opérations dans l'instance doivent être effectuées en tant qu'utilisateur root.

---

# Installation d'eDirectory et d'iManager

## Conditions préalables

- ❒ Veillez à respecter la configuration requise indiquée à la section Configuration système requise.
- ❒ Créez des groupes de sécurité comme indiqué à la section « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 80.
- ❒ L'instance du proxy SSH doit être un serveur renforcé et sécurisé. Ouvrez uniquement le port SSH 22 pour cette instance et sélectionnez un type d'instance AWS dont les performances et la mémoire sont adaptées. La clé privée SSH requise pour accéder aux instances du sous-réseau privé et à l'instance dans laquelle le proxy SSH est exécuté ne doit pas être stockée dans le VPC, mais uniquement sur le client. Associez une adresse IP Elastic au serveur proxy SSH afin de disposer d'une adresse IP publique statique.
- ❒ Configurez le serveur VNC dans l'instance du proxy SSH. Le serveur VNC doit être renforcé par un mot de passe fort adapté. Connectez-vous au serveur VNC via un tunnel SSH uniquement afin de permettre des communications sécurisées. Le serveur VNC doit être configuré pour écouter uniquement les connexions depuis l'hôte local. Désactivez le verrouillage de l'écran pour éviter le verrouillage de la session. Après avoir utilisé le serveur VNC, mettez fin à la session.

❒ Connectez-vous à l'instance du sous-réseau privé dans laquelle eDirectory/iManager sera configuré à l'aide du proxy SSH :

```
ssh -i edir_key.pem -A -J ec2-user@<ssh_proxy_ip> ec2-
user@<instance_private_ip>
```

**REMARQUE**

- Dans les exemples de commandes ci-dessus, `edir_key.pem` correspond à un exemple de nom de fichier contenant la clé de serveur.
- Vous pouvez également ajouter le fichier d'identité dans l'agent à l'aide de la commande `SSH-Add` pour éviter d'utiliser le fichier d'identité à chaque connexion.

Pour afficher l'adresse IP privée d'une instance, cliquez sur **Instances** > *[instance]* > **Description**.

❒ Configurez un serveur Agent Annuaire (DA) SLP dans une machine virtuelle du sous-réseau dorsal. Ouvrez le port 427 dans la règle entrante du groupe NSG pour la machine virtuelle sur laquelle le DA SLP est déployé. Activez l'opération DA en éditant le fichier `slp.conf`. Pour plus d'informations, reportez-vous à la section Configuration de OpenSLP pour eDirectory du *guide d'administration de NetIQ eDirectory*.

## Procédure d'installation et de configuration

Cette section fournit les instructions détaillées à suivre pour installer et configurer eDirectory et iManager dans un environnement AWS EC2. Une fois eDirectory installé, assurez-vous que les conditions suivantes sont respectées :

- EBA est activé.
- SNMP est désactivé.
- eDirectory n'écoute pas le port 389.
- Les services LDAP et HTTP sont configurés pour utiliser les certificats ECDSA uniquement.
- L'accès au port SSH de l'instance privée AWS EC2 doit être désactivé lorsqu'il n'est pas utilisé.
- Désactivez les modules iMonitor, eMBox et DHost afin de renforcer la sécurité. Une fois qu'ils sont désactivés, toutes les activités impliquant ces modules doivent être effectuées à l'aide des utilitaires NDS uniquement.

### Installation et configuration d'eDirectory

1. Copiez le fichier `eDirectory_<version>_Linux_x86_64.tar.gz` à l'aide de Secure Copy (scp) vers l'instance du sous-réseau privé dans laquelle eDirectory sera configuré à l'aide du proxy SSH :

   ```
   scp -i <keyname> -o ProxyJump=ec2-user@<ssh_proxy_ip>
   eDirectory_<version>_Linux_x86_64.tar.gz ec2-user@<instance_ip>:/<directory>
   ```

2. Installez eDirectory. Pour plus d'informations, reportez-vous à la section Exécution de l'utilitaire nds-install pour installer des composants eDirectory.
3. Configurez eDirectory. Pour plus d'informations, reportez-vous à la section Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques eDirectory. Voici un exemple de commande qui permet d'installer et de configurer eDirectory :

```
ndsconfig  new [-t <tree_name>] [-n <server context>] -a <admin FDN> [-w <admin
password>] -P ldaps://<instance_ip> --configure-eba-now yes
```

4 Installez `openslp-server`, puis démarrez le service SLPD.

### Installation et configuration d'iManager

Grâce à la console d'administration d'iManager, vous pouvez gérer les opérations eDirectory dans votre environnement AWS. iManager doit être installé sur votre instance AWS après l'installation d'eDirectory.

1 Copiez le fichier `iMan_<version>_linux_x86_64.tgz` à l'aide de Secure Copy (scp) vers l'instance du sous-réseau privé dans laquelle iManager sera configuré à l'aide du proxy SSH :

```
scp -i <keyname> -o ProxyJump=ec2-user@<ssh_proxy_ip>
iMan_<version>_linux_x86_64.tgz ec2-user@<instance_ip>:/<directory>
```

2 Installez et configurez iManager. Pour plus d'informations, reportez-vous à la section Installation d'iManager Server sous Linux. Avant d'installer iManager, reportez-vous à la section Configuration système requise dans le *guide d'installation d'iManager*.

3 Téléchargez le certificat de l'autorité de certification EBA sur l'instance dans laquelle iManager est exécuté. Pour plus d'informations, reportez-vous à la section Gestion de l'autorité de certification EBA à l'aide d'iManager dans le *guide d'administration de NetIQ eDirectory*.

4 Remplacez les certificats auto-signés dans la machine virtuelle exécutant iManager par des certificats signés par une autorité de certification. Pour plus d'informations, reportez-vous à la section Remplacement des certificats auto-signés temporaires pour iManager.

---

**REMARQUE :** veillez à configurer le serveur iManager pour qu'il n'utilise que des certificats ECDSA. Après avoir installé iManager, spécifiez un utilisateur autorisé ainsi que le nom de l'arborescence eDirectory appropriée que cet utilisateur va gérer.

---

### Lancement d'iManager

Procédez comme suit pour lancer iManager :

1 Connectez-vous au serveur VNC exécuté sur l'hôte local du proxy SSH via le tunnel SSH.

2 Installez et lancez un navigateur dans la même instance.

3 Lancez iManager et connectez-vous à l'arborescence eDirectory à l'aide de l'adresse IP ou du nom de l'arborescence.

## Tâches de post-configuration

1 Pour vérifier si EBA est activé, reportez-vous à la section Affichage des informations relatives à l'authentification EBA dans le *guide d'administration de NetIQ eDirectory*.

2 Activez SuiteB dans Certificate Server. Pour plus d'informations, reportez-vous à la section Activation de SuiteB dans Certificate Server dans le *guide d'administration de NetIQ eDirectory*.

3 Configurez la clé d'arborescence AES 256 bits pour le premier serveur eDirectory. Pour plus d'informations, reportez-vous à la section Creating an AES 256-Bit Tree Key (Création d'une clé d'arborescence AES 256 bits) dans le document *NICI Administration Guide* (Guide d'administration de NICI).

4 Supprimez les points de distribution CRL sur le premier serveur eDirectory. L'accès LDAP non sécurisé sur le port 389 étant désactivé sur tous les serveurs eDirectory, la CRL pour l'autorité de certification de l'arborescence devrait être disponible au téléchargement par HTTP uniquement. Procédez comme suit pour supprimer les points de distribution CRL :

   4a Connectez-vous à iManager en tant qu'administrateur.

   4b Sélectionnez **Rôles et tâches** > **NetIQ Certificate Server** > **Configure Certificate Authority** (Configurer l'autorité de certification).

   4c Cliquez sur **CRL**.

   4d Cliquez sur **One**. Sélectionnez et supprimez tous les **points de distribution CRL**, à l'exception du point de distribution CRL HTTP (http://<IP_instance>:8028/crl/one.crl).

   4e Cliquez sur **Appliquer**, puis sur **Fermer**.

   4f Cliquez sur **OneEC**. Sélectionnez et supprimez tous les **points de distribution CRL**, à l'exception du point de distribution CRL HTTP (http://<IP_instance>:8028/crl/oneec.crl).

   4g Cliquez sur **Appliquer**, puis sur **OK**.

5 Réparez les certificats par défaut du serveur à l'aide du plug-in iManager Certificate Server. Pour cela, procédez comme suit :

   5a Connectez-vous à iManager en tant qu'administrateur.

   5b Sélectionnez **Rôles et tâches** > **NetIQ Certificate Server** > **Réparer les certificats par défaut**.

   5c Sélectionnez le ou les serveurs qui possèdent les certificats, puis cliquez sur **Suivant**.

   5d Sélectionnez **Tous les certificats par défaut sont écrasés**, puis cliquez sur **Suivant**.

   5e Examinez les tâches à effectuer, puis cliquez sur **Terminer**.

6 Configurez les services LDAP et HTTP pour qu'ils utilisent les certificats ECDSA et les Ciphers SuiteB. Pour plus d'informations, reportez-vous à la section Configuration des services LDAP et HTTP pour qu'ils utilisent les certificats ECDSA et les Ciphers SuiteB dans le *guide d'administration de NetIQ eDirectory*. Une fois l'opération terminée, redémarrez eDirectory.

7 Pour plus d'informations pour vérifier si le sous-agent SNMP est déchargé, reportez-vous à la section Chargement et déchargement du module serveur SNMP dans le *guide d'administration de NetIQ eDirectory*.

8 Assurez-vous qu'eDirectory n'écoute pas le port 389.

9 Désactivez iMonitor, eMBox, DHost et la pile HTTP.

   9a Procédez comme suit pour désactiver iMonitor, eMBox et DHost sur le serveur eDirectory qui héberge l'autorité de certification de l'arborescence :

      9a1 Éditez le fichier `ndsmodules.conf` en commentant `hconserv`, `imon` et `embox`.

      9a2 Redémarrez eDirectory.

   9b Procédez comme suit pour désactiver la pile HTTP dans les serveurs de répliques eDirectory :

      9b1 Éditez le fichier `ndsmodules.conf` en commentant `httpstk`, `hconserv`, `imon` et `embox`.

      9b2 Redémarrez eDirectory.

**REMARQUE :** `httpstk` doit être placé au-dessus de `nds` dans le fichier `ndsmodules.conf` avant les commentaires. Le module `nds` cesse alors d'activer la pile HTTP.

10 Configurez SLP pour forcer eDirectory à utiliser la monodiffusion comme méthode d'annonce. Éditez le fichier `slp.conf` en indiquant l'adresse IP du serveur DA dans le sous-réseau dorsal. Pour plus d'informations, reportez-vous à la section Paramètres de configuration du *guide d'administration de NetIQ eDirectory*.

**REMARQUE :** après avoir configuré toutes les instances eDirectory et iManager, configurez la liste ACL réseau du sous-réseau privé AWS pour interdire l'accès au port SSH et l'autoriser uniquement si nécessaire.

# Déploiement des services d'audit

Vous pouvez déployer le service d'audit Common Event Format (CEF) dans AWS EC2 pour auditer divers événements eDirectory. Procédez comme suit pour déployer les services d'audit CEF :

1 Installez un serveur d'audit dans le VPC.

2 Configurez le serveur d'audit pour qu'il écoute un port.

**REMARQUE :** il est recommandé d'utiliser Sentinel comme serveur d'audit.

3 Créez un groupe de sécurité réseau avec la configuration suivante et associez-le à l'instance dans laquelle le serveur d'audit s'exécute :

| Port | Source | Description |
|---|---|---|
| TCP (port du serveur d'audit) | Sous-réseau privé | Autorise la réception des événements provenant des serveurs eDirectory. |

4 Mettez à jour les éléments suivants dans le fichier `/etc/opt/novell/eDirectory/conf/auditlogconfig.properties` sur toutes les instances d'eDirectory :

```
log4j.appender.S.Host=<Auditing server ip>
log4j.appender.S.Port=<auditing server port>
```

5 Activez les événements CEF correspondants à partir d'iManager. Pour plus d'informations, reportez-vous à la section Configuration des événements CEF pour l'audit. Les événements activés sont transmis au serveur d'audit.

# Reprise après sinistre

La reprise après sinistre est effectuée en cas de crash d'une instance dans laquelle eDirectory était exécuté. Procédez comme suit pour effectuer une reprise après sinistre :

1 Arrêtez l'instance qui a subi un crash et dissociez le volume EBS de cette instance. Pour plus d'informations, reportez-vous à l'article Détacher un volume Amazon EBS d'une instance.

2 Configurez une nouvelle instance EX2 avec le même système d'exploitation que l'instance qui a subi le crash.

3 Installez la même version d'eDirectory dans la nouvelle instance EC2.

4 Attachez le volume EBS à la nouvelle instance et montez le système de fichiers. Pour plus d'informations, reportez-vous à l'article Attacher un volume Amazon EBS à une instance.

5 Effectuez le montage de liaison des répertoires.

Pour effectuer le montage de liaison des répertoires, mettez à jour les éléments suivants dans `/etc/fstab` :

```
<mount_point>/eDirectory_data /var/opt/novell/eDirectory none defaults,bind 0
0
```

```
<mount_point>/nici_data /var/opt/novell/nici none defaults,bind 0 0
```

```
<mount_point>/eDirectory_nici_conf /etc/opt/novell/eDirectory none
defaults,bind 0 0
```

6 Remplacez l'adresse IP dans `/etc/opt/novell/eDirectory/conf/nds.conf` par l'adresse IP de l'instance actuelle.

7 Mettez à niveau eDirectory en ignorant la vérification de l'état de santé. Pour plus d'informations, reportez-vous à la section *Mise à niveau d'eDirectory* dans le guide d'installation de NetIQ eDirectory.

8 Réparez les adresses réseau à l'aide de l'utilitaire `ndsrepair`. Pour plus d'informations, reportez-vous à la section*Options DSRepair* du guide d'administration de NetIQ eDirectory.

9 Modifiez l'adresse?  IP du point de distribution CRL si l'adresse IP de l'autorité de certification de l'arborescence a changé. Pour plus d'informations sur la modification de l'adresse IP, reportez-vous à la section Affichage et modification des propriétés d'un objet Configuration CRL dans le guide d'administration de NetIQ eDirectory.

10 Réparez les certificats par défaut du serveur à l'aide du plug-in iManager Certificate Server. Pour cela, procédez comme suit :

**10a** Connectez-vous à iManager en tant qu'administrateur.

**10b** Sélectionnez **Rôles et tâches** > **NetIQ Certificate Server** > **Réparer les certificats par défaut**.

**10c** Sélectionnez le ou les serveurs qui possèdent les certificats, puis cliquez sur **Suivant**.

**10d** Sélectionnez **Tous les certificats par défaut sont écrasés**, puis cliquez sur **Suivant**.

**10e** Examinez les tâches à effectuer, puis cliquez sur **Terminer**.

11 Configurez les services LDAP et HTTP pour qu'ils utilisent les nouveaux certificats ECDSA.

# 6 Déploiement d'eDirectory à l'aide d'un conteneur Docker

Ce chapitre explique comment déployer eDirectory à l'aide d'un conteneur Docker.



## Présentation de Docker

Docker est la technologie de conteneurisation d'applications la plus courante. Il s'agit d'une plate-forme conçue pour faciliter la création, le déploiement et l'exécution des applications à l'aide de conteneurs. Un conteneur encapsule une application et son propre système d'exploitation et toutes les autres dépendances, comme les bibliothèques et les paquetages. Le déploiement d'eDirectory à l'aide de conteneurs Docker présente les avantages suivants :

- **Portabilité élevée :** toute application exécutée dans des conteneurs peut être facilement déployée sur les plates-formes matérielles et les systèmes d'exploitation pris en charge par Docker.
- **Facilité de déploiement :** les conteneurs permettent de déployer, de mettre à niveau et de mettre à l'échelle les applications plus rapidement à l'aide d'outils d'orchestration.
- **Cohérence :** il n'y a pas d'impact sur la fonctionnalité d'eDirectory, quel que soit l'endroit où les conteneurs sont déployés.

Pour plus d'informations sur Docker et sur ses composants, reportez-vous à la section Docker Overview (Présentation de Docker).

## Planification du déploiement d'eDirectory à l'aide d'un conteneur Docker

Cette section décrit la configuration système requise et les conditions préalables nécessaires au déploiement d'un conteneur Docker pour eDirectory.

### Configuration système requise

#### Configuration requise de la plate-forme

❒ Docker Community Edition version 18.06 ou ultérieure est suffisant pour déployer le conteneur Docker pour eDirectory.

- ❒ `overlay2` est le pilote de stockage Docker recommandé. BTRFS n'est pas un système de fichiers pris en charge de l'hôte sur lequel Docker peut être installé.
- ❒ Kernel Linux version 3.10 ou ultérieure.

### Configuration matérielle requise

- ❒ Un minimum de 4 Go de mémoire RAM et de 30 Go d'espace disque doit être prévu sur la machine hôte Docker.

---

**REMARQUE :** les exigences en matière de mémoire, de processeur et de disque dur varient en fonction du type de déploiement et du nombre de conteneurs à déployer. Prévoyez toujours plus de ressources que celles requises pour garantir une évolutivité future.

---

## Conditions préalables

- ❒ Les machines hôtes Docker doivent être configurées avec une adresse IP statique.
- ❒ Docker doit être installé. Pour plus d'informations sur les plates-formes prises en charge, reportez-vous à la documentation relative à Docker.
- ❒ Le daemon Docker doit être actif et en cours d'exécution.
- ❒ Le tarball de l'image Docker pour eDirectory doit être téléchargé à partir du site Web de téléchargement NetIQ.
- ❒ Les utilisateurs souhaitant effectuer l'administration des conteneurs dans Docker doivent être ajoutés au groupe `docker`.

## Interface de ligne de commande (CLI) de Docker

Vous trouverez ici les explications des différentes commandes utilisées dans l'interface de ligne de commande (CLI) de Docker.

# Déploiement d'un conteneur eDirectory

L'image de base du système d'exploitation de l'image Docker pour eDirectory est openSUSE Leap 15.1. Le fichier tar de l'image eDirectory doit être téléchargé sur la machine hôte Docker. Une fois le tarball téléchargé, l'image doit être chargée dans le registre Docker local à l'aide des commandes suivantes :

```
# tar xf eDirectory_920.tar.gz
# docker load --input edir920.tar
```

Le conteneur Docker pour eDirectory accepte tous les paramètres de l'utilitaire `ndsconfig` avec la commande docker run. Pour plus d'informations sur l'utilitaire `ndsconfig`, reportez-vous à la section « Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques eDirectory » page 39.

**REMARQUE :** il n'est pas recommandé de définir le mot de passe à l'aide de l'option `-w` de l'utilitaire `ndsconfig` dans la commande docker run. En effet, un mot de passe défini à l'aide de cette option peut être affiché en texte brut avec la commande docker inspect. La spécification du FDN et du mot de passe administrateur dans l'invite permet de configurer les informations d'identificateur de l'administrateur en toute sécurité.

Le conteneur Docker pour eDirectory utilise les valeurs par défaut pour les paramètres `ndsconfig` ci-dessous. Par conséquent, vous ne devez pas configurer ces paramètres dans la commande docker run :

- **Fichier de configuration :** /config/eDirectory/inst/conf/nds.conf
- **Emplacement de l'instance :** /config/eDirectory/inst/data/data
- **Emplacement de la DIB :** /config/eDirectory/inst/data/data/dib

**REMARQUE :** il est important que les données et la configuration de l'instance soient remplies dans le dossier `/config` du conteneur afin d'activer les fonctionnalités de mise à niveau et de stockage persistant des conteneurs eDirectory. Pour plus d'informations, reportez-vous à la section « Gestion du stockage des données eDirectory » page 113.

L'emplacement par défaut du fichier journal du conteneur eDirectory est `/config/eDirectory/inst/data/log`.

Avant de déployer eDirectory, vous devez tenir compte des recommandations suivantes :

- Aucune contrainte de ressources n'est définie par défaut pour les conteneurs Docker. Ainsi, chaque conteneur dispose d'un accès à toutes les ressources de l'UC et mémoire fournies par le kernel de l'hôte. Vous devez également vous assurer qu'un conteneur en cours d'exécution ne consomme pas plus de ressources et n'épuise pas les autres conteneurs en cours d'exécution en définissant des limites pour le volume de ressources utilisables par un conteneur.
  - Le conteneur Docker doit veiller à ce qu'une limite fixe soit appliquée à la mémoire utilisée par le conteneur à l'aide du drapeau `--memory` dans la commande docker run.
  - Le conteneur Docker doit veiller à ce qu'une limite soit appliquée à la quantité d'UC utilisée par un conteneur en cours d'exécution à l'aide du drapeau `--cpuset-cpus` dans la commande docker run.
  - Le drapeau `--pids-limit` doit avoir la valeur 300 pour restreindre le nombre de threads du kernel générés à tout moment dans le conteneur. Ceci permet d'éviter les attaques par déni de service (DoS).
- Vous devez définir la stratégie de redémarrage de conteneur en cas d'échec sur la valeur 5 à l'aide du drapeau `--restart` dans la commande docker run.
- Vous ne devez utiliser le conteneur eDirectory qu'une fois que l'état de santé est **Healthy** (Sain) lorsque le conteneur est activé. Pour vérifier l'état de santé du conteneur, exécutez la commande suivante :

  ```
  docker ps <container_name/ID>
  ```

- Les conteneurs Docker comprennent généralement une liste par défaut de fonctions Linux activées. Veillez à ne conserver que les fonctions suivantes activées pour le conteneur eDirectory et à supprimer les autres fonctions :
  - AUDIT_WRITE
  - CHOWN
  - DAC_OVERRIDE

- SETGID
- SETUID
- NET_BIND_SERVICE
- SYS_CHROOT (uniquement en cas d'activation du service SLP)
- SYS_PTRACE (uniquement en cas d'utilisation d'utilitaires faisant appel à la fonction Linux `ptrace`, comme `gdb`)

Pour plus d'informations sur l'ajout et la suppression de fonctions, reportez-vous à la section Runtime privilege and Linux capabilities (Privilège d'exécution et fonctions Linux).

- Le conteneur eDirectory démarre toujours en tant qu'utilisateur non-root (`nds`). Par mesure de sécurité supplémentaire, activez la réassignation de l'espace de noms utilisateur sur le daemon pour éviter les attaques par élévation de privilèges à partir du conteneur. Pour plus d'informations sur la réassignation de l'espace de noms utilisateur, reportez-vous à la section Isolate containers with a user namespace (Isoler les conteneurs avec un espace de noms).

---

**REMARQUE :** si vous utilisez une version autonome antérieure d'eDirectory, vous ne pouvez pas migrer la configuration vers l'environnement Docker à l'aide d'un conteneur Docker pour eDirectory 9.2.

---

Le conteneur Docker pour eDirectory prend en charge les pilotes de réseau hôte (Host) et superposé (Overlay) pour le déploiement dans un environnement Docker multi-hôte :


- « Déploiement d'un conteneur eDirectory dans un réseau hôte » page 108
- « Déploiement d'un conteneur eDirectory dans un réseau superposé défini par l'utilisateur » page 109


# Déploiement d'un conteneur eDirectory dans un réseau hôte

Les conteneurs eDirectory peuvent être déployés dans un environnement hybride à l'aide du pilote de réseau hôte sous Linux uniquement. Pour plus d'informations sur les réseaux Docker, reportez-vous à la section Configure networking (Configurer la mise en réseau).

---

**REMARQUE :** le réseau hôte n'est pas pris en charge sous Windows.

---

Un environnement hybride est une combinaison de déploiements hérités et basés sur les conteneurs de serveurs eDirectory dans une même arborescence. Un réseau hybride permet d'introduire des conteneurs Docker pour eDirectory en toute transparence dans un environnement de production existant qui héberge déjà un déploiement eDirectory hérité. Dans le cadre de la mise en réseau hôte Docker, les ports de service ne peuvent pas être réutilisés, car la pile réseau de l'hôte est partagée par les déploiements eDirectory hérités et conteneurisés. En outre, un serveur eDirectory conteneurisé apparaît en tant que serveur eDirectory hérité pour les clients et les autres serveurs de l'arborescence.

L'exemple suivant indique comment créer une arborescence à l'aide d'un conteneur eDirectory :

```
docker run -it --name eDir-container-1 --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --network=host
edirectory:9.2.0 new -t docker-tree1 -n novell -S m1 -B 164.99.1.1@1524 -o 1028 -O
1030 -L 1389 -l 1636 --configure-eba-now yes
```

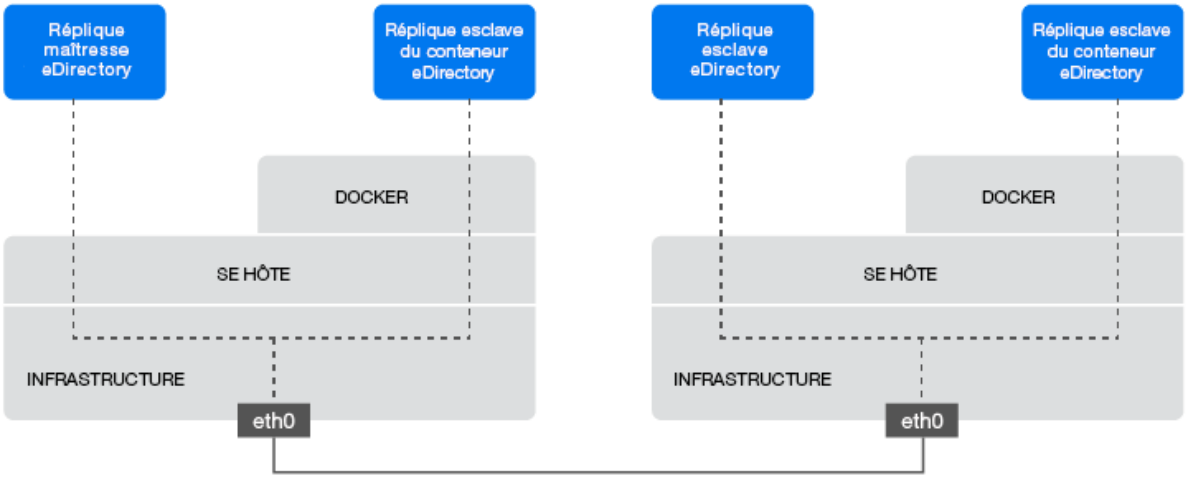
L'exemple suivant indique comment ajouter un serveur de répliques d'un conteneur eDirectory à une arborescence existante :

```
docker run -it --name eDir-container-2 --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume2:/config --network=host
edirectory:9.2.0 add -t docker-tree1 -n novell -S m2 -B 164.99.10.10@2524 -o 2028 -
O 2030 -L 2389 -l 2636 --configure-eba-now yes -p 164.99.1.1@1524
```

**REMARQUE**

- Le drapeau `--network` sert à déployer le conteneur à l'aide du pilote de réseau hôte.
- Les numéros de port des services ne doivent pas être répétés entre les conteneurs eDirectory exécutés sur un même hôte Docker.
- Les adresses IP utilisées dans les commandes ci-dessus sont celles de l'ordinateur hôte Docker sur lequel le conteneur doit s'exécuter.

***Figure 6-1*** *Déploiement d'un conteneur eDirectory dans un réseau hôte*




# Déploiement d'un conteneur eDirectory dans un réseau superposé défini par l'utilisateur

Vous pouvez utiliser un réseau superposé défini par l'utilisateur pour créer un réseau distribué de conteneurs eDirectory qui s'exécutent sur plusieurs hôtes de daemon Docker. Un conteneur eDirectory dans un réseau superposé défini par l'utilisateur peut être déployé sous Linux et Windows. Le service Docker Swarm doit être utilisé pour joindre les hôtes Docker à un essaim. Les conteneurs eDirectory qui y sont exécutés peuvent ainsi communiquer en toute transparence. Pour plus d'informations sur le pilote de réseau superposé Docker, reportez-vous à la section Use overlay networks (Utiliser des réseaux superposés).

**REMARQUE :** les opérations de mise à l'échelle et de planification des fonctions d'un essaim Docker ne sont pas certifiées avec les conteneurs eDirectory. De plus, la migration des conteneurs eDirectory sur les hôtes par le service Swarm n'est pas prise en charge.

## Conditions préalables

- ❒ Un essaim Docker doit être créé avec au moins un hôte Docker configuré en tant que `manager` (gestionnaire) et les autres hôtes en tant que `workers` (travailleurs).
- ❒ Créez un réseau superposé attachable nommé `myOverlay`.

- ❒ Ouvrez les ports suivants sur le pare-feu entre les hôtes Docker pour la gestion des grappes et la communication au sein d'un essaim Docker :
  - Port TCP 2377
  - Port TCP et UDP 7946
  - Port UDP 4789
- ❒ Vous devez assigner aux conteneurs déployés dans un réseau superposé une adresse IP interne statique appartenant au sous-réseau `myOverlay`.

Pour plus d'informations sur le déploiement d'un essaim et sur la création d'un réseau superposé défini par l'utilisateur, reportez-vous à la section Networking with overlay networks (Mise en réseau avec des réseaux superposés).

Avant de déployer un conteneur eDirectory dans un réseau superposé défini par l'utilisateur, vous devez tenir compte des recommandations suivantes :

- Le serveur de répliques maîtresses du conteneur eDirectory et ses répliques R/W doivent être déployés au sein d'un même réseau superposé. Les communications avec d'autres serveurs eDirectory autonomes ou des conteneurs exécutés en dehors du réseau superposé ne sont pas prises en charge.
- Il est recommandé de déployer le conteneur Docker pour iManager dans le même réseau superposé défini par l'utilisateur à des fins d'administration d'eDirectory. Pour plus d'informations sur le déploiement des conteneurs Docker pour iManager, reportez-vous à la section Déploiement d'iManager à l'aide d'un conteneur Docker.
- Pour obtenir les informations détaillées du réseau superposé défini par l'utilisateur, exécutez la commande suivante :

  ```
  docker inspect myOverlay
  ```

La commande suivante indique comment créer une arborescence à l'aide d'un conteneur eDirectory :

```
docker run -it --name eDir-container-1 --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --
network=myOverlay --ip=10.0.0.5 edirectory:9.2.0 new -t docker-tree1 -n novell -S
m1 –b 524 -o 8028 -O 8030 -L 389 -l 636 --configure-eba-now yes
```

La commande suivante indique comment obtenir l'adresse IP du conteneur eDirectory créé ci-dessus :

```
docker inspect eDir-container-1 --format
{{.NetworkSettings.Networks.myOverlay.IPAddress}}
```

Vous pouvez utiliser l'adresse IP affichée en tant qu'`adresse_IP_distante` lors de l'ajout d'un serveur de répliques de conteneur eDirectory à l'arborescence.

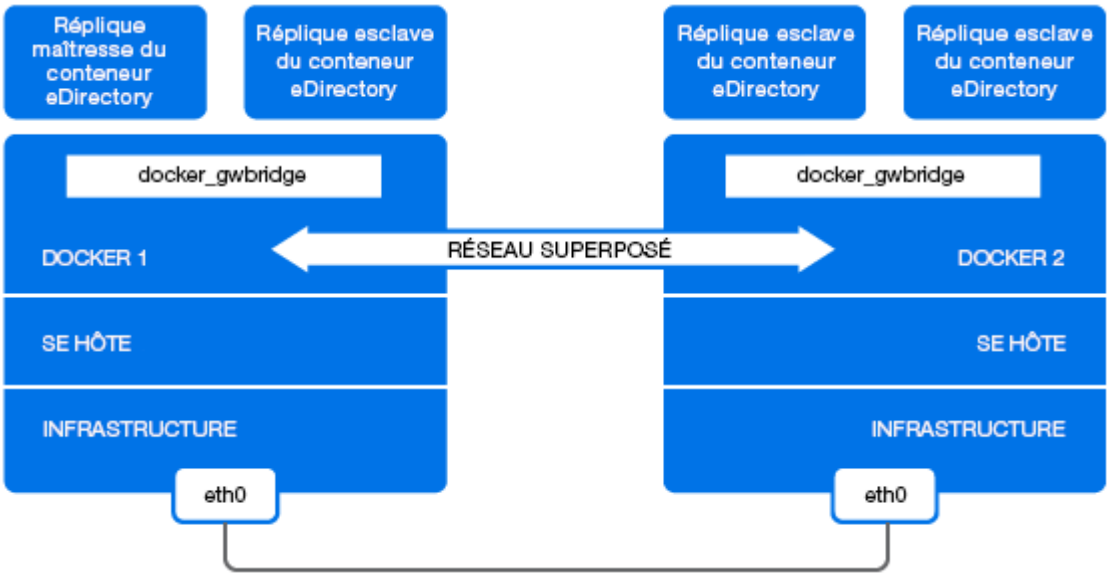
La commande suivante indique comment ajouter un serveur de répliques d'un conteneur eDirectory à une arborescence existante :

```
docker run -it --name eDir-container-2 --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="300" --volume eDir-volume2:/config --
network=myOverlay --ip=10.0.0.6 edirectory:9.2.0 add -t docker-tree1 -n novell -S
m2 –b 524 -o 8028 -O 8030 -L 389 -l 636 --configure-eba-now yes -p
<remote_IP_Address>
```

**REMARQUE**

- Le drapeau `--network` sert à déployer le conteneur dans le réseau superposé défini par l'utilisateur nommé `myOverlay` à l'aide du pilote de réseau superposé.
- Dans les exemples ci-dessus, le drapeau `--ip` sert à assigner une adresse IP interne statique au conteneur appartenant au sous-réseau `myOverlay`.

***Figure 6-2*** *Déploiement d'un conteneur eDirectory dans un réseau superposé défini par l'utilisateur*




# Tâches de post-configuration

Vous devez effectuer les tâches suivantes après avoir déployé les conteneurs eDirectory.


- « Exécution de commandes sur un conteneur eDirectory en cours d'exécution » page 111
- « Configuration d'OpenSLP pour le conteneur Docker pour eDirectory » page 112
- « Installation des méthodes NMAS dans un conteneur Docker pour eDirectory » page 112


## Exécution de commandes sur un conteneur eDirectory en cours d'exécution

Exécutez la commande suivante sur la machine hôte Docker pour obtenir un shell bash dans le conteneur Docker pour eDirectory :

```
bash# docker exec -it eDir-container-1 /bin/bash
```

La commande ci-dessus permet de définir le chemin d'accès binaire eDirectory sur `/opt/novell/eDirectory/bin`.

Vous pouvez exécuter les commandes de l'utilitaire NDS à l'invite du conteneur. Voici un exemple :

```
nds@abbae7c93b1c:~> ndsstat
```

```
[1] Instance at /config/eDirectory/inst/conf/nds.conf:  m1.O=novell.DOCKER-TREE1
Tree Name: DOCKER-TREE1
Server Name: .CN=m1.O=novell.T=DOCKER-TREE1.
Binary Version: 40201.14
Root Most Entry Depth: 0
Product Version: eDirectory for Linux x86_64 v9.2 [DS]
```

Vous pouvez exécuter la commande ci-dessus directement à partir de la machine hôte. Voici un exemple :

```
bash# docker exec -it eDir-container-1 /opt/novell/eDirectory/bin/ndsstat
```

```
[1] Instance at /config/eDirectory/inst/conf/nds.conf:  m1.O=novell.DOCKER-TREE1
Tree Name: DOCKER-TREE1
Server Name: .CN=m1.O=novell.T=DOCKER-TREE1.
Binary Version: 40201.14
Root Most Entry Depth: 0
Product Version: eDirectory for Linux x86_64 v9.2 [DS]
```

## Configuration d'OpenSLP pour le conteneur Docker pour eDirectory

Procédez comme suit pour démarrer le serveur SLP dans un conteneur eDirectory en cours d'exécution :

1. Démarrez `slpd` en exécutant la commande suivante :

   ```
   docker exec --user root eDir-container-1 /usr/sbin/slpd
   ```

2. Redémarrez eDirectory en exécutant les commandes suivantes :

   ```
   docker exec eDir-container-1 /opt/novell/eDirectory/bin/ndsmanage stopall
   ```

   ```
   docker exec eDir-container-1 /opt/novell/eDirectory/bin/ndsmanage startall
   ```

---

**REMARQUE**

- L'arrêt et le redémarrage du conteneur arrêtent le daemon SLP. Vous devez le redémarrer manuellement. Si un fichier PID caduc se trouve dans `/var/run/slpd.pid`, vous devez le supprimer avant de lancer le daemon.
- Un fichier PID caduc est un fichier dont le PID est un processus arrêté ou terminé (dans ce cas, le processus du daemon SLP).
- Dans un environnement superposé, le DA SLP doit être exécuté dans le même réseau superposé.

---

## Installation des méthodes NMAS dans un conteneur Docker pour eDirectory

Effectuez les tâches suivantes pour installer les méthodes NMAS dans un conteneur eDirectory :

---

**REMARQUE :** par défaut, les méthodes NMAS sont disponibles dans `/home/nds/eDirectory/nmas`.

---

1. Connectez-vous au conteneur eDirectory à l'aide de la commande suivante :

```
docker exec -it eDir-container-1 bash
```

2 Ajoutez la méthode NMAS :

```
cd /home/nds/eDirectory/nmas/NmasMethods/Novell/<method-name>
```

```
nmasinst -addmethod admin.novell docker-tree1 ./config.txt
```

---

**REMARQUE :** pour plus d'informations sur l'ajout d'une méthode NMAS, reportez-vous à la section Installation d'une méthode de connexion à l'aide de l'utilitaire nmasinst dans le *guide d'administration de NetIQ eDirectory*.

---

3 Quittez la console du conteneur :

```
exit
```

4 Redémarrez le conteneur eDirectory :

```
docker restart eDir-container-1
```

# Gestion du stockage des données eDirectory

Docker Volume est le mécanisme de stockage persistant privilégié pour les données et la configuration d'eDirectory. Pour plus d'informations sur le stockage persistant, reportez-vous à la section Manage data in Docker (Gérer les données dans Docker).

Les données d'application eDirectory qui nécessitent un stockage persistant sont placées dans le répertoire `/config` du conteneur pendant le démarrage. Un volume Docker doit être monté dans le chemin `/config` du conteneur eDirectory pour assurer le stockage persistant des données sur le système de fichiers de l'hôte Docker en dehors du conteneur. Ainsi, les données d'application dans le volume sont conservées même en cas d'arrêt ou de suppression d'un conteneur à des fins d'administration.

Cette pratique est utile pour conserver l'ancienne configuration et les anciennes données lors d'une mise à niveau d'un conteneur eDirectory. Pour plus d'informations sur la mise à niveau d'un conteneur eDirectory, reportez-vous à la section « Mise à niveau d'eDirectory à l'aide d'un conteneur Docker » page 114.

L'exemple suivant montre comment créer un volume Docker nommé `eDir-volume-1` :

```
docker volume create eDir-volume-1
```

L'exemple ci-dessous indique comment démarrer un conteneur eDirectory avec un volume monté à des fins de stockage :

```
docker run -it --name eDir1-Host --restart on-failure:5 --memory="700M" --cpuset-
cpus="1" --pids-limit="300" --volume eDir-volume1:/config --network=host
edir920:latest new -t docker-tree1 -n novell -S m1 -B 164.99.179.213@1524 -o 1028 -
O 1030 -L 1389 -l 1636 --configure-eba-now yes
```

Dans la commande ci-dessus, `eDir-volume1` correspond au volume Docker créé et monté dans l'emplacement `/config` du conteneur eDirectory.

# Mise à niveau d'eDirectory à l'aide d'un conteneur Docker

Quand une nouvelle version de l'image eDirectory est disponible, l'administrateur peut effectuer une mise à niveau pour déployer le conteneur à l'aide de la dernière version d'eDirectory. Veillez à assurer le stockage persistant de toutes les données nécessaires liées à l'application dans les volumes Docker avant d'effectuer une mise à niveau. Procédez comme suit pour effectuer la mise à niveau d'eDirectory à l'aide d'un conteneur Docker :

1. Arrêtez et supprimez le conteneur eDirectory en cours d'exécution. Étant donné qu'ils ne peuvent pas utiliser la nouvelle image, les conteneurs en cours d'exécution doivent être arrêtés et supprimés avant une mise à niveau.
2. Démarrez un nouveau conteneur à l'aide de la nouvelle image Docker pour eDirectory et des données d'application de l'ancien conteneur stockées dans le volume Docker :

   L'exemple ci-dessous indique comment démarrer un conteneur eDirectory avec un volume monté à des fins de stockage :

   ```
   docker run -it --name eDir1-Host --restart on-failure:5 --memory="700M" --
   cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --
   network=host <eDirectory_image> new -t docker-tree1 -n novell -S m1 -B
   <Host_IP_Address>@1524 -o 1028 -O 1030 -L 1389 -l 1636 --configure-eba-now yes
   ```

   L'exemple suivant indique comment mettre à niveau le conteneur eDirectory créé à l'étape 2 :

   ```
   docker run -it --name eDir1-Host --restart on-failure:5 --memory="700M" --
   cpuset-cpus="1" --pids-limit="300" --volume eDir-volume1:/config --
   network=host <Latest_eDirectory_image> upgrade
   ```

   `eDir-volume1` correspond au même volume que celui qui conserve les données d'application de l'ancien conteneur eDirectory.

---

**REMARQUE**

- Le conteneur eDirectory ne doit être mis à niveau qu'après la suppression du conteneur qui exécute l'ancienne version de l'image.
- Il n'est pas recommandé d'utiliser les options `-a` et `-w` de la commande `ndsconfig`. Vous devez utiliser l'invite à l'écran pour entrer les informations d'identification de l'administrateur pour mettre à niveau le conteneur.

---

# Récupération d'un conteneur Docker pour eDirectory

Si un conteneur eDirectory en cours d'exécution est inaccessible, supprimé ou inutilisable pour une raison inconnue, vous devez effectuer une récupération de conteneur. Dans ce cas, vous devez arrêter et supprimer le conteneur concerné. Vous devez démarrer un nouveau conteneur en utilisant la même image eDirectory et le volume Docker du conteneur concerné. Procédez comme suit pour récupérer un conteneur eDirectory :

1. Arrêtez et supprimez le conteneur concerné.
2. Éditez le tampon horaire de période dans le fichier `nds.version` dans le chemin `/var/lib/docker/volumes/eDir-volume1/_data/eDirectory/inst/conf` de la machine hôte pour lui assigner une valeur inférieure.
3. Démarrez un nouveau conteneur avec la même image eDirectory et le volume du conteneur concerné. L'exemple suivant montre comment récupérer un conteneur concerné :

```
docker run -it --name eDir1-Host --restart on-failure:5 --memory="700M" --
cpuset-cpus="1" --pids-limit="150" --volume eDir-volume1:/config --
network=host <same_eDirectory_image> upgrade
```

`eDir-volume1` correspond au même volume que celui qui conserve les données d'application du conteneur eDirectory concerné.

# 7 Installation d'eDirectory sous Linux et Windows avec des adresses IPv6

eDirectory 9.2 prend en charge les adresses IPv4 et IPv6. Vous pouvez activer les adresses IPv6 au cours du processus d'installation de eDirectory. Lors de la mise à niveau à partir d'une version antérieure, vous devez activer manuellement la prise en charge des adresses IPv6.

eDirectory 9.2 prend en charge les méthodes de transition Dual IP stack, Tinneling et Pure IPv6. Seules les adresses IP globales sont prises en charge. Par exemple,

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

La fonctionnalité eDirectory est la même pour les adresses IPv6 et IPv4, à ceci près que vous devez spécifier les adresses IPv6 entre crochets `[]`. Vous pouvez également utiliser le nom d'hôte au lieu d'une adresse IP. Si vous utilisez le nom d'hôte, vous devez le spécifier dans le fichier `etc\hosts` et l'associer à l'adresse IPv6.

Les exemples suivants font référence à des utilitaires eDirectory avec adresses IPv6 :

```
ndsstat -h [6015:abc:def:123:456:12:0:123]
```

```
ndsstat -h [6015:abc:def:123:456:12:0:123]:524
```

```
ndslogin -h [2015::4] admin.organization
```

```
ndscheck -h [6015:abc:def:123:456:12:0:123] -a admin.organization -w password
```

```
ldapadd -h [2015::4] -p 389 -D cn=admin,o=organization -w password -f adduser.ldif
```

```
ldapdelete -h [6015:abc:def:123:456:12:0:123] -p 389 -D cn=admin,o=organization -w
password cn=user21,o=organization
```

```
ldapmodify -h [2015::4] -p 389 -D cn=admin,o=organization -w password -f
modify.ldif
```

```
ldapsearch -h [6015:abc:def:123:456:12:0:123] -p 389 -D cn=admin,o=organization -w
password -b o=organization objectclass=inetorgperson
```

```
http://[2015::3]:8028/nds
```

eDirectory 9.2 ne prend pas en charge les adresses link-local, IPv6 mappées vers IPv4 et IPv6 compatibles IPv4.

Les sections suivantes décrivent comment installer et configurer NetIQ eDirectory 9.2 sur Linux et Windows où les adresses IPv6 sont déjà configurées :


- « Configuration de eDirectory sur Linux avec IPv6 » page 118
- « Installation ou mise à niveau d'eDirectory sous Windows avec IPv6 » page 119


Pour plus d'informations sur les différences entre les plates-formes Linux et Windows pour IPv6, consultez la section « Récepteurs d'adresses IPv6 non spécifiées dans Linux et Windows » du *Guide de dépannage NetIQ eDirectory* .

# Configuration de eDirectory sur Linux avec IPv6

Cette section fournit des informations sur la configuration de eDirectory sur un ordinateur Linux prenant déjà en charge les adresses IPv6 :

## Création d'une nouvelle arborescence eDirectory

Vous pouvez configurer une nouvelle arborescence eDirectory avec une adresse IPv6 en transmettant l'adresse IPv6 avec l'option `-B` dans la commande `ndsconfig`. Par exemple :

```
ndsconfig new -t CORP-TREE -B [2015::3]@524 -P ldap://[2015::3]:389,ldaps://
[2015::3]:636
```

Pour que les récepteurs LDAP commencent automatiquement à écouter les adresses IPv6, vous devez spécifier les URL LDAP avec l'option `-P` lors de la configuration de eDirectory. Si vous ne les spécifiez pas lors de la configuration initiale, vous pouvez les ajouter par la suite dans l'attribut `ldapInterfaces` à l'aide de la commande `ldapconfig` ou de iManager. Pour plus d'informations, reportez-vous à la « Ajout d'URL LDAP pour IPV6 sur l'objet Serveur LDAP » page 119.

## Ajout d'un serveur à une arborescence eDirectory existante

Vous pouvez ajouter un serveur à une arborescence existante avec IPv6 en transmettant l'adresse IPv6 à l'aide de l'option `-B` dans la commande `ndsconfig`. Par exemple :

```
ndsconfig add -t CORP-TREE -B [2015::4]@524 -P ldap://[2015::4]:389,ldaps://
[2015::4]:636
```

Pour que les récepteurs LDAP commencent automatiquement à écouter les adresses IPv6, vous devez spécifier les URL LDAP avec l'option `-P` lors de la configuration de eDirectory. Si vous ne les spécifiez pas lors de la configuration initiale, vous pouvez les ajouter par la suite dans l'attribut `ldapInterfaces` à l'aide de la commande `ldapconfig` ou de iManager. Pour plus d'informations, reportez-vous à la « Ajout d'URL LDAP pour IPV6 sur l'objet Serveur LDAP » page 119.

## Activation d'adresses IPv6 sur des serveurs eDirectory existants ou mis à niveau

1. Ajoutez une adresse d'interface IPv6 avec le numéro de port dans le fichier `/etc/opt/novell/eDirectory/conf/nds.conf`. Vous devez l'ajouter dans chaque fichier de configuration si plusieurs instances sont configurées sur l'ordinateur.

   Voici quelques exemples :

   ```
   n4u.server.interfaces=164.99.90.148@524,[2015::4]@524,[2015:1234:2345:3456:abc
   d:bcde:cdef:aaaa]@524
   ```

   ```
   http.server.interfaces=164.99.90.148@8028,[2015::4]@8028,[2015:1234:2345:3456:
   abcd:bcde:cdef:aaaa]@8028
   ```

   ```
   https.server.interfaces=164.99.90.148@8030,[2015::4]@8030,[2015:1234:2345:3456
   :abcd:bcde:cdef:aaaa]@8030
   ```

2. Redémarrez ndsd à l'aide des commandes suivantes :

   ```
   ndsmanage stopall
   ndsmanage startall
   ```

## Ajout d’URL LDAP pour IPV6 sur l’objet Serveur LDAP

Si vous ne spécifiez pas les URL LDAP lors de la configuration initiale d'eDirectory, vous pouvez utiliser la commande `ldapconfig` ou iManager pour les ajouter à l'attribut `ldapInterfaces`.

Les exemples suivants illustrent l'utilisation des commandes `ldapconfig set` et `ldapconfig -s` :

```
ldapconfig set "ldapInterfaces=ldap://[2015::3]:389,ldaps://[2015::3]:636"
```

```
ldapconfig -s
"ldapInterfaces=ldap://[2015::3]:389,ldapInterfaces=ldaps://[2015::3]:636"
```

Pour ajouter des URL LDAP dans iManager :

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **LDAP** > **Options LDAP**.
3. Cliquez sur **Afficher les serveurs LDAP**, puis sur le nom d’un objet Serveur LDAP à configurer.
4. Cliquez sur **Connexions** et **ajoutez des URL LDAP** dans le champ **Interfaces LDAP**.
5. Cliquez sur **Appliquer**, puis sur **OK**.

# Installation ou mise à niveau d’eDirectory sous Windows avec IPv6

Cette section fournit des informations sur la configuration de eDirectory sur un ordinateur Windows prenant déjà en charge les adresses IPv6 :

## Activation d’IPv6 lors de l’installation ou de la mise à niveau de eDirectory

Si vous souhaitez utiliser des adresses IPv6, veillez à cocher la case **Activer IPv6** dans **Préférence IPv6** lors de l’installation de eDirectory. Si vous sélectionnez cette option, l’hôte DHost commence à écouter les adresses IPv6. Si vous n’activez pas les adresses IPv6 pendant le processus d’installation et que vous décidez ultérieurement de les utiliser, vous devez exécuter à nouveau le programme de configuration.

## Activation de IPv6 pour les serveurs existants

Si vous souhaitez utiliser des adresses IPv6 pour un serveur eDirectory déjà configuré, vous devez réexécuter l’installation et cocher la case **Activer IPv6** dans **Préférence IPv6**. Cette option active les protocoles NCP, HTTP et HTTPS pour les adresses IPv6.

## Accès à iMonitor

Vous pouvez accéder à iMonitor sur les adresses IPv6 à l’aide du lien suivant :

```
http://[2015::3]:8028/nds
```

# 8 Fonctionnement d'eDirectory en mode FIPS

eDirectory 9.2 tire parti des fonctionnalités compatibles FIPS pour répondre aux exigences de sécurité des agences fédérales américaines et des clients dont les environnements sont hautement sécurisés. Ce chapitre fournit des informations sur la configuration et le fonctionnement d'eDirectory en mode FIPS.

Vous pouvez exécuter eDirectory en mode FIPS 140-2 pris en charge par les modules NICI et OpenSSL.



## Configuration d'eDirectory en mode FIPS pour OpenSSL

Lorsque le mode FIPS est activé sur votre serveur eDirectory, toutes les applications et tous les modules en cours d'exécution dans eDirectory à l'aide d'OpenSSL utilisent toujours OpenSSL en mode FIPS. Par exemple, les opérations LDAP, HTTP ainsi que toutes les opérations de chiffrement utilisent l'authentification EBA. Le fonctionnement d'eDirectory en mode FIPS n'autorise pas les communications sur SSLv3 et limite l'utilisation du chiffrement aux chiffrements forts. Pour plus d'informations, reportez-vous aux sections Configuration des objets LDAP et Configuration de l'objet Serveur HTTP du *Guide d'administration de NetIQ eDirectory*.

Tous les serveurs eDirectory 9.2 s'exécutent en mode FIPS pour OpenSSL par défaut sur les plates-formes Linux et Windows. eDirectory fournit des paramètres pour configurer le mode FIPS en fonction de vos besoins.

Pour activer le mode FIPS pour OpenSSL :

- **Windows :** le mode FIPS est activé par défaut dans votre environnement eDirectory, tous les modules/applications eDirectory utilisant OpenSSL utilisent toujours OpenSSL en mode FIPS. Le fonctionnement d'eDirectory en mode FIPS n'autorise pas les communications sur SSLv3 et limite l'utilisation du chiffrement aux chiffrements forts. Pour plus d'informations, reportez-vous aux sections Configuration des objets LDAP et Configuration de l'objet Serveur HTTP du *Guide d'administration de NetIQ eDirectory*.
- **Linux :** aucune configuration supplémentaire n'est nécessaire pour l'exécution d'eDirectory en mode FIPS sous Linux. Le mode FIPS est activé par défaut lors de l'installation d'eDirectory.

Pour désactiver le mode FIPS pour OpenSSL :

- **Windows :** accédez à la valeur de registre `HKLM\SOFTWARE\Novell\NDS\FipsMode` et définissez **FipsMode** sur **0**.
- **Linux :** transmettez **n4u.server.fips_tls=0** avec la commande `ndsconfig set` et redémarrez le serveur.

  Par exemple, `ndsconfig set n4u.server.fips=0`.

# 9 Déplacement de la DIB

Après avoir installé et configuré NetIQ eDirectory, vous pouvez déplacer la DIB si nécessaire. Vous voudrez peut-être déplacer votre DIB pour diverses raisons, par exemple si le nombre d'objets dans l'arborescence doit augmenter mais que le système de fichiers actuel hébergeant la DIB ne dispose pas d'un espace suffisant.

## Linux

Exécutez la procédure suivante pour déplacer votre DIB :

1. Vérifiez l'état du serveur en entrant la commande suivante sur la ligne de commande :

   `ndscheck`

2. Arrêtez le service eDirectory à l'aide de ndsmanage en procédant comme suit :

   **2a** À l'invite, entrez la commande `ndsmanage`.

   **2b** Sélectionnez l'instance à arrêter.

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

   **2c** Entrez `k` pour arrêter l'instance.

3. Recherchez l'emplacement actuel de la DIB en entrant la commande suivante :

   `ndsconfig get n4u.nds.dir`

4. Copiez la DIB vers son nouvel emplacement en entrant la commande suivante :

   `cp -rp` *`current__location new__location`*

   Par exemple, pour copier la DIB dans le répertoire `/home/nds`, entrez la commande suivante :

   `cp -rp /var/opt/novell/eDirectory/data//* /home/nds//`

5. Éditez le fichier de configuration `nds.conf` spécifique à l'instance et modifiez la valeur du paramètre de `n4u.nds.dir` comme suit :

   `n4u.nds.dir=`*`new__location`*

   Par exemple, si vous déplacez la DIB de `/var/nds/` vers `/home/nds/`, entrez la commande suivante :

   `n4u.nds.dir=/home/nds/`

6. Démarrez le service eDirectory comme suit :

   **6a** À l'invite, entrez la commande `ndsmanage`.

   **6b** Sélectionnez l'instance à démarrer.

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

   **6c** Entrez s pour démarrer l'instance.

7 Vérifiez l'état du serveur en entrant la commande suivante :

```
ndscheck
```

# Windows

Le déplacement de la DIB vers un nouvel emplacement n'est actuellement pas pris en charge. Toutefois, vous pouvez enregistrer la DIB à un emplacement personnalisé pendant l'installation de eDirectory.

# 10 Conditions requises pour la mise à niveau d'eDirectory 9.2

L'une des fonctionnalités uniques de eDirectory est sa capacité à maintenir l'intégrité référentielle stricte. Tout objet Classes issu de Top aura un attribut de référence dans sa définition de classe. Il s'agit d'un attribut masqué ajouté à tous les objets référencés qui sont maintenus en interne par eDirectory. Les processus en arrière-plan continuent de fonctionner pour vérifier les liens entre l'objet référencé et les objets de référencement.

Si l'objet référencé provient d'une partition différente de celle détenue localement dans le serveur, une référence externe à cet objet sera créée localement dans la partition de référence externe. Une référence externe est une représentation d'un objet existant dans l'arborescence de eDirectory. Cependant, il ne s'agit pas d'une copie de l'objet et de ses attributs assignés.

S'il est possible de supprimer l'attribut Référence de eDirectory, les définitions de classe sont actuellement préservées afin de conserver la compatibilité avec les versions précédentes dans l'arborescence.

Ce chapitre explique les modifications et les scénarios de mise à niveau possibles dans eDirectory 9.2.



## Changements de référence dans 9.2 ou versions ultérieures

L'attribut de référence est un attribut masqué et est conservé sur chaque objet référencé. Il est créé et conservé par DS. Le nouveau code de référencement dans DS est basé sur un index du gestionnaire Flexible Adaptable Information Manager (FLAIM) appelé`LocalEntryIDIndex` créé par DS. Bien que FLAIM maintienne l'index, l'utilisation est déterminée par DS. FLAIM met automatiquement à jour l'index quand une valeur DN est ajoutée ou supprimée. Chaque clé de l'index est une clé composée, c.-à-d. DN de l'objet référencé + ID de l'entrée de l'objet de référencement. Par exemple, si un objet a l'ID d'entrée 343, et que sa valeur de « membre » dirige vers l'objet #899, FLAIM génèrera automatiquement la clé 899+343 dans l'index. DS peut désormais faire des recherches dans l'index pour trouver tous les objets pointant vers l'objet #899. Il n'est pas nécessaire que l'objet #899 conserve un attribut de référence sur lui pour se souvenir de tous les objets qui y font référence. En fait, FLAIM maintient l'index sans savoir comment ce dernier est utilisé, mais DS détient le code qui sait comment utiliser l'index.

La nouvelle façon de maintenir les références nécessite néanmoins de mettre à niveau la base de données si l'instance d'eDirectory existante est mise à niveau vers la version 9.2 ou ultérieure. La mise à niveau requiert la création d'un nouvel index, ce qui nécessitera de parcourir chaque entrée dans la base de données. Cela requiert également de supprimer tous les attributs de « référence » dans chaque entrée de la base de données. En outre, certains attributs internes de chaîne d'octets utilisés par DS et ayant des DN incorporés nécessiteront de générer de nouvelles valeurs DN qui seront stockées avec la valeur de chaîne d'octets. Pour une base de données volumineuse, cela représente un processus très long. Étant donné que DS a changé afin de réaliser l'intégrité référentielle avec la nouvelle fonctionnalité FLAIM et que cela dépend du nouvel index, il est

impossible que DS puisse vraiment fonctionner avant la fin de la conversion. Par conséquent, à la première ouverture d'une base de données existante, tous les attributs de référence doivent être changés et dirigés vers un nouvel index. Pour une base de données volumineuse, cela peut prendre des heures avant qu'elle ne s'ouvre vraiment et que des applications puissent l'utiliser.

# Procédure de mise à niveau dans la version 9.2

La commande `ndsconfig upgrade` permet de mettre à niveau la configuration nécessaire des composants tels que HTTP, LDAP, SNMP, SAS et NMAS. La base de données eDirectory est mise à niveau vers un nouveau format si les versions eDirectory antérieures à eDirectory 8.8 SP1 sont mises à niveau vers eDirectory 9.2.

## Utilisation de l'option Force pour mettre à niveau eDirectory à partir de versions antérieures sur Linux

eDirectory 9.2 ne prend en charge que les mises à niveau à partir de la version 8.8.8 ou ultérieure sur Linux.

Pour effectuer la mise à niveau de la version 8.7.3 à la version 8.8.8 d'eDirectory, effectuez l'une des étapes suivantes :

- Effectuez tout d'abord une mise à niveau vers eDirectory 8.8.8, puis vers eDirectory 9.2.

ou

- Mettez directement à niveau en utilisant la commande de force `switch -f`.

  Avec cette option, certaines vérifications comme la vérification de l'état de santé et de l'espace disque aux fins de mise à niveau de la DIB n'auront pas lieu. De plus, les anciens RPM sont supprimés et les nouveaux RPM sont installés.

---

**IMPORTANT :** si le module du journal des modifications (changelog) d'Identity Manager est déjà installé, vous devez définir la variable d'environnement `NDSD_IGNORE_IDM_CHECK` sur 1 lors de la mise à niveau d'eDirectory vers la version 9.2. Par exemple :

- Sous Linux : `NDSD_IGNORE_IDM_CHECK=1./nds-install`
- Sous Windows : définissez `NDSD_IGNORE_IDM_CHECK` sur `true` (vrai) avant d'exécuter le fichier `setup.exe`.

---

# 11 Configuration de NetIQ eDirectory sous Linux

NetIQ eDirectory contient des utilitaires qui simplifient la configuration de différents composants de eDirectory sous Linux. Les sections suivantes traitent des fonctionnalités et de l'utilisation des composants de configuration de eDirectory :



## Utilitaires de configuration

Cette section traite de l'utilisation des utilitaires de configuration eDirectory suivants :



### Utilitaire ndsconfig

L'utilitaire ndsconfig permet de configurer eDirectory. Vous pouvez également l'utiliser pour ajouter le serveur de répliques eDirectory à une arborescence existante ou pour créer une arborescence. Pour plus d'informations, reportez-vous à la « Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques eDirectory » page 39.

---

**REMARQUE**

- vérifiez que le nom du serveur NCP est unique au sein du réseau.
- L'utilitaire `ndsconfig` échoue sous SLES 12 SP2 et RHEL 7.2. Ce problème se produit de manière aléatoire. Pour plus d'informations sur la façon de résoudre ce problème, consultez le document TID 7018366.

---

Pour changer la configuration actuelle des composants installés, utilisez la syntaxe suivante :

`ndsconfig {set value_list | get [parameter_list] | get help [parameter_list]}`

Pour obtenir la description des paramètres `ndsconfig`, reportez-vous à la section « Paramètres de configuration » page 130.

**IMPORTANT :** Après l'installation, assurez-vous d'exécuter l'utilitaire ndsconfig à partir de l'emplacement installé sur le serveur, qui est `/opt/novell/eDirectory/bin` par défaut. N'exécutez pas ndsconfig à partir du paquetage d'installation.

# Utilisation des outils LDAP pour configurer les objets Serveur LDAP et Groupe LDAP

Vous pouvez utiliser les outils LDAP inclus avec eDirectory sous Linux pour modifier, afficher et rafraîchir les attributs des objets Groupe et Serveur LDAP.

Pour plus d'informations, reportez-vous à la section « Using LDAP Tools on Linux » (Utilisation d'outils LDAP sur Linux) du manuel *NetIQ eDirectory Administration Guide* (Guide d'administration de NetIQ eDirectory 8.8 SP8).

# Utilisation de l'utilitaire nmasinst pour configurer le service NMAS (NetIQ Modular Authentication Service)

Pour eDirectory 9.2, l'utilitaire ndsconfig configure NMAS par défaut. Vous pouvez également utiliser nmasinst pour configurer NMAS.

ndsconfig se charge uniquement de la configuration de NMAS ; il n'effectue pas l'installation des méthodes de connexion. Pour installer ces dernières, vous pouvez utiliser nmasinst. Pour plus d'informations, reportez-vous à la « Exécution de l'utilitaire nmasinst pour configurer NMAS » page 53.

# Personnalisation d'eDirectory



## Utilisation du script d'initialisation de ndsd

Le script d'initialisation de ndsd lance le daemon au démarrage du système, avec les paramètres de configuration du fichier de configuration par défaut (`/etc/opt/novell/eDirectory/conf/nds.conf`).

**REMARQUE :** vous ne devez pas utiliser le script `/etc/init.d/ndsd` dans l'environnement `systemd`. `systemd` est actuellement uniquement pris en charge avec les plates-formes SLES 12 et RHEL 7. Pour plus d'informations, reportez-vous à la section « Utilisation d'eDirectory sur les plates-formes SLES 12 et RHEL 7 » page 129.

Avant de démarrer ndsd, assurez-vous qu'un agent SLP (Service Location Protocol) est en cours d'exécution sur l'hôte. Vous pouvez installer OpenSLP, un SLP natif disponible avec votre système d'exploitation ou encore NetIQ SLP.

**REMARQUE :** pour démarrer eDirectory, employez l'utilitaire ndsmanage.

Pour démarrer ndsd, exécutez `/etc/init.d/ndsd start`.

Pour arrêter ndsd, exécutez `/etc/init.d/ndsd stop`.

---

**REMARQUE :** exécutez les commandes suivantes pour démarrer et arrêter eDirectory sous SLES 12 et RHEL 7 ou version ultérieure :

- Pour démarrer ndsd, exécutez `systemctl start ndsd*`
- Pour arrêter ndsd, exécutez `systemctl stop ndsd*`

---

La configuration d'eDirectory crée les scripts de shell suivants à l'emplacement `/opt/novell/eDirectory/sbin` :

- `pre_ndsd_start`
- `post_ndsd_start`
- `pre_ndsd_stop`
- `post_ndsd_stop`

Comme son nom l'indique, le script `pre_ndsd_start` est exécuté avant que le script `/etc/init.d/ndsd` ne démarre le binaire ndsd. Le script `post_ndsd_start` est exécuté après que le script `/etc/init.d/ndsd` ne démarre le binaire ndsd. De la même manière, les scripts `pre_ndsd_stop` et `post_ndsd_stop` sont exécutés respectivement avant et après l'arrêt du processus ndsd.

Vous pouvez ajouter les commandes de votre choix à ces scripts pour les exécuter. Par défaut le script `post_ndsd_start` possède des commandes pour garantir que le script `/etc/init.d/ndsd` est exécuté après avoir vérifié que les services LDAP sont fonctionnels et en cours d'exécution.

---

**REMARQUE :** vous devez ajouter toutes les variables d'environnement requises pour le service eDirectory dans le script `env_custom` qui se trouve dans le répertoire `/etc/opt/novell/eDirectory/conf`. L'exportation des variables d'environnement sur les terminaux ou le script `/etc/init.d/ndsd` n'est pas utilisée par eDirectory. Pour plus d'informations sur les variables d'environnement, consultez le document TID 7018431.

---

## Utilisation d'eDirectory sur les plates-formes SLES 12 et RHEL 7

eDirectory lance le daemon au démarrage du système, avec les paramètres de configuration du fichier de configuration par défaut (`/etc/opt/novell/eDirectory/conf/nds.conf`).

Avant de démarrer ndsd, assurez-vous qu'un agent SLP (Service Location Protocol) est en cours d'exécution sur l'hôte. Vous pouvez installer OpenSLP, un SLP natif disponible avec votre système d'exploitation ou encore NetIQ SLP.

Pour démarrer ou arrêter eDirectory, employez l'utilitaire `ndsmanage`.

La configuration d'eDirectory crée les scripts de shell suivants à l'emplacement `/opt/novell/eDirectory/sbin` :

- `pre_ndsd_start_custom` : utilisez ce script pour l'ajout personnalisé de commandes avant l'exécution d'eDirectory.
- `post_ndsd_start_custom` : utilisez ce script pour l'ajout personnalisé de commandes après l'exécution d'eDirectory.
- `post_ndsd_stop_custom` : utilisez ce script pour l'ajout personnalisé de commandes après l'arrêt d'eDirectory.

**REMARQUE**

- n'utilisez aucun des scripts d'usine à partir de l'emplacement `/opt/novell/eDirectory/sbin`. La configuration d'eDirectory utilise les scripts d'usine. Pour inclure les commandes supplémentaires de votre choix, utilisez des scripts personnalisés.
- après la mise à niveau du système d'exploitation, exécutez l'utilitaire `ndsconfig upgrade`.

### Activation des instances non-root d'eDirectory pour qu'elles se lancent au démarrage du serveur

À partir d'une installation non-root, les instances eDirectory ne démarrent pas automatiquement. Pour permettre aux instances non-root d'eDirectory de se lancer automatiquement lors du redémarrage du serveur procédez comme suit :

1. Créez un script de démarrage.
2. Dans le script, entrez la commande suivante :

   ```
   su - user1 -c"/home/user1/eDirectory/opt/novell/eDirectory/bin/ndsmanage
   startall
   ```

   Dans l'exemple ci-dessus, eDirectory est exécuté par un utilisateur non-root (`user1`) à l'aide du script `ndsmanage` disponible via le chemin `/home/user1/eDirectory/opt/novell/eDirectory/bin/ndsmanage`.
3. Enregistrez le fichier.
4. Donnez l'autorisation nécessaire à l'utilisateur root pour exécuter le script.
5. Créez des liens symboliques vers le script de démarrage à l'aide des commandes suivantes :

   ```
   ln -s /etc/init.d/ndsstart /sbin/rcndsstart
   ln -s /etc/init.d/ndstart /etc/init.d/rc2.d/S10ndsstart
   ln -s /etc/init.d/ndstart /etc/init.d/rc3.d/S10ndsstart
   ln -s /etc/init.d/ndsstart /etc/init.d/rc5.d/S10ndsstart
   ```

Désormais, si le serveur est redémarré, toutes les instances non-root d'eDirectory seront lancées automatiquement.

## Paramètres de configuration

Les paramètres de configuration de eDirectory sont stockés dans le fichier `nds.conf`..

Lors de la modification de paramètres de configuration, ndsd doit être redémarré pour que les nouvelles valeurs soient prises en compte. Vous devez utiliser ndsmanage pour redémarrer ndsd.

Toutefois, certains paramètres de configuration ne nécessitent pas le redémarrage de ndsd. Ces paramètres sont les suivants :

- `n4u.nds.inactivity-synchronization-interval`
- `n4u.nds.synchronization-restrictions`
- `n4u.nds.janitor-interval`
- `n4u.nds.backlink-interval`
- `n4u.nds.drl-interval`

- `n4u.nds.flatcleaning-interval`
- `n4u.nds.server-state-up-thresholdn4u.nds.heartbeat-scheman4u.nds.heartbeat-data`

Le tableau suivant décrit les paramètres de l'utilitaire nds-install :

| Paramètre | Description |
|---|---|
| `n4u.nds.preferred-server` | Nom d'hôte de la machine qui héberge le service eDirectory.<br><br>Valeur par défaut = aucune valeur |
| `n4u.base.tree-name` | Nom de l'arborescence utilisée par Account Management. Il s'agit d'un paramètre obligatoire défini par le programme d'installation de Account Management. Vous ne pouvez pas définir ce paramètre. |
| `n4u.base.dclient.use-udp` | DClient peut utiliser UDP en plus de TCP pour communiquer avec les serveurs eDirectory. Ce paramètre active le transport UDP.<br><br>Valeur par défaut = 0<br><br>Plage = 0, 1 |
| `n4u.base.slp.max-wait` | Timeout des appels d'API du protocole SLP (Service Location Protocol).<br><br>Valeur par défaut = 30<br><br>Plage = 3 à 100<br><br>Cette valeur est exprimée en secondes.<br><br>Cette option est prise en charge uniquement par NetIQ SLP et non par OpenSLP. |
| `n4u.nds.advertise-life-time` | eDirectory se réenregistre lui-même auprès de l'agent Annuaire après ce laps de temps.<br><br>Valeur par défaut = 3600<br><br>Plage = 1 à 65535<br><br>Cette valeur est exprimée en secondes. |
| `n4u.server.signature-level` | Désigne le niveau de prise en charge de la sécurité étendue. L'augmentation de cette valeur accroît la sécurité mais réduit les performances.<br><br>Valeur par défaut = 1<br><br>Plage = 0 à 3 |

| Paramètre | Description |
| --- | --- |
| `n4u.nds.dir` | Base de données des informations de l'annuaire eDirectory.<br><br>Par défaut :<br><br>`/var/opt/novell/eDirectory/data/`<br><br>Ce paramètre ne peut pas être défini en utilisant la commande `ndsconfig set`. Vous pouvez modifier ce paramètre manuellement si vous souhaitez déplacer votre DIB. Mais nous vous le déconseillons. |
| `n4u.nds.server-guid` | Identificateur unique global du serveur eDirectory.<br><br>Valeur par défaut = aucune valeur |
| `n4u.nds.server-name` | Nom du serveur eDirectory.<br><br>Valeur par défaut = aucune valeur |
| `n4u.nds.bindery-context` | Chaîne du contexte de Bindery.<br><br>Valeur par défaut = aucune valeur |
| `n4u.nds.server-context` | Contexte auquel est ajouté le serveur eDirectory. Ce paramètre ne peut être ni défini, ni modifié. |
| `n4u.nds.external-reference-life-span` | Temps (en heures) pendant lequel les références externes non utilisées sont conservées avant d'être retirées.<br><br>Valeur par défaut = 192<br><br>Plage = 1 à 384 |
| `n4u.nds.inactivity-synchronization-interval` | Intervalle (en minutes) au terme duquel une synchronisation complète des répliques est exécutée, suite à une période d'absence de modification des informations conservées dans eDirectory sur le serveur.<br><br>Valeur par défaut = 60<br><br>Plage = 2 à 1440 |
| `n4u.nds.synchronization-restrictions` | La valeur Off (Inactif) permet d'exécuter une synchronisation avec n'importe quelle version de eDirectory. La valeur On (Actif) limite la synchronisation aux numéros de version que vous spécifiez en tant que paramètres (par exemple, `ON,420,421`).<br><br>Par défaut=désactivé |
| `n4u.nds.janitor-interval` | Intervalle (en minutes) au terme duquel est exécuté le processus de nettoyage (Janitor) de eDirectory.<br><br>Valeur par défaut = 2<br><br>Plage = 1 à 10080 |

| Paramètre | Description |
| --- | --- |
| `n4u.nds.backlink-interval` | Intervalle (en minutes) au terme duquel est exécuté le contrôle de cohérence des liens en amont de eDirectory.<br><br>Valeur par défaut = 780<br><br>Plage = 2 à 10080 |
| `n4u.nds.drl-interval` | Intervalle (en minutes) au terme duquel est exécuté le contrôle de cohérence des liens de référence distribués de eDirectory.<br><br>Valeur par défaut = 780<br><br>Plage = 2 à 10080 |
| `n4u.nds.flatcleaning-interval` | Intervalle (en minutes) au terme duquel le processus du gestionnaire d'attributs (flat cleaner) lance automatiquement la purge et la suppression des entrées de la base de données.<br><br>Valeur par défaut = 720<br><br>Plage = 1 à 720 |
| `n4u.nds.server-state-up-threshold` | Seuil de vérification de l'état du serveur, en minutes. Il s'agit du délai à l'issue duquel eDirectory vérifie l'état du serveur avant de renvoyer des erreurs -625.<br><br>Valeur par défaut = 30<br><br>Plage = 1 à 720 |
| `n4u.nds.heartbeat-schema` | Intervalle de synchronisation du schéma de base de pulsation, en minutes.<br><br>Valeur par défaut = 240<br><br>Plage = 2 à 1440 |
| `n4u.nds.heartbeat-data` | Intervalle de synchronisation de pulsation, en minutes.<br><br>Valeur par défaut = 60<br><br>Plage = 2 à 1440 |
| `n4u.nds.dofsync` | Si ce paramètre est défini sur 0, les performances de mise à jour augmentent considérablement pour les bases de données volumineuses, mais il existe un risque d'altération de la base de données en cas de panne du système. |
| `n4u.server.configdir` | Les fichiers de configuration de eDirectory sont stockés ici.<br><br>Valeur par défaut = `/etc` |
| `n4u.server.vardir` | Les fichiers journaux de eDirectory et des utilitaires sont stockés ici.<br><br>Emplacement par défaut = `/var/opt/novell/eDirectory/log` |

| Paramètre | Description |
| --- | --- |
| `n4u.server.libdir` | Les bibliothèques propres à eDirectory sont stockées ici, dans le répertoire `nds-modules`.<br><br>Emplacement par défaut = `/opt/novell/eDirectory/lib` |
| `n4u.server.sid-caching` | Active le caching de l'ID de session SSL. Pour plus d'informations sur le caching de l'ID de session dans SSL, reportez-vous au document SSL v3.0 RFC. |
| `n4u.server.tcp-port` | Port utilisé par défaut si aucun numéro de port n'est spécifié dans le paramètre `n4u.server.interfaces`. |
| `n4u.server.interfaces` | Adresse IP et numéro de port sur lequel le serveur eDirectory est à l'écoute des connexions client. La valeur peut être une liste de combinaisons de paramètres possibles séparées par une virgule. Par exemple :<br>`n4u.server.interfaces=101.1.2.3@524,100.1.2.3@1524` |
| `n4u.server.max-interfaces` | Ce paramètre définit le nombre maximal d'interfaces qu'utilisera eDirectory.<br><br>Valeur par défaut = 128<br><br>Plage = 1 à 2048 |
| `n4u.server.max-openfiles` | Ce paramètre spécifie le nombre maximal de descripteurs de fichier pouvant être utilisés par eDirectory.<br><br>Valeur par défaut = nombre maximal autorisé par l'administrateur |
| `n4u.server.max-threads` | Nombre maximal de threads que peut démarrer le serveur eDirectory. Il s'agit du nombre d'opérations simultanées susceptibles d'être exécutées au niveau du serveur eDirectory.<br><br>Valeur par défaut = 64<br><br>Plage = 32 à 512<br><br>Consultez le *Guide de dépannage NetIQ eDirectory* pour définir une valeur optimale. |
| `n4u.server.idle-threads` | Nombre maximal de threads inactifs autorisés dans le serveur eDirectory.<br><br>Valeur par défaut = 8<br><br>Plage = 1 à 128 |
| `n4u.server.start-threads` | Nombre initial de threads au démarrage.<br><br>Valeur par défaut = 8 |

| Paramètre | Description |
|---|---|
| `n4u.server.log-levels` | Ce paramètre permet de configurer les paramètres de consignation des erreurs pour les messages côté serveur. Il règle le niveau de consignation des messages sur LogFatal, LogWarn, LogErr, LogInfo ou LogDbg. |
| `n4u.server.log-file` | Ce paramètre spécifie l'emplacement du fichier journal dans lequel consigner les messages. Par défaut, les messages sont consignés dans le fichier `ndsd.log`. |
| `n4u.ldap.lburp.transize` | Nombre d'enregistrements envoyés via le client d'importation/exportation NetIQ au serveur LDAP dans un même paquet LBURP. Vous pouvez augmenter la taille de la transaction pour être sûr que les opérations d'ajout multiples puissent être exécutées en une seule requête.<br><br>Valeur par défaut = 25<br><br>Plage = 1 à 250 |
| `n4u.server.listen-on-loopback` | Il s'agit d'un paramètre booléen activé par défaut. Dans certaines distributions Linux récentes, le nom d'hôte dans le fichier `/etc/hosts` est associé à l'adresse de bouclage. Bien que l'adresse commune donnée dans les systèmes SLES soit 127.0.0.2, elle peut être comprise entre 127.0.0.0 et 127.255.255.255 (adresses de bouclage valides). |
| `http.server.interfaces` | Liste d'interfaces séparées par une virgule que le serveur HTTP doit utiliser. |
| `http.server.request-io-buffer-size` | Taille par défaut du tampon d'E/S. |
| `http.server.request_timeout-seconds` | Timeout de requête envoyée au serveur. |
| `http.server.keep-timeout-seconds` | Nombre de secondes d'attente de la requête suivante du même client sur la même connexion. |
| `http.server.threads-per-processor` | Taille du pool de threads HTTP par processeur. |
| `http.server.session-exp-seconds` | Délai d'expiration de la session, en secondes. |
| `http.server.sadmin-passwd` | Mot de passe de session de l'administrateur. |
| `http.server.module-base` | Webroot du serveur HTTP. |
| `https.server.cached-cert-dn` | DN de certificat mis en cache du serveur HTTP. |
| `https.server.cached-server-dn` | DN mis en cache du serveur HTTPS. |
| `http.server.trace-level` | Niveau de trace de diagnostic du serveur HTTP. |
| `http.server.auth-req-tls` | L'authentification du serveur HTTP requiert TLS. |
| `http.server.clear-port` | Port du serveur pour le protocole HTTP. |
| `http.server.tls-port` | Port du serveur pour le protocole HTTPS. |

| Paramètre | Description |
| --- | --- |
| `n4u.server.fips` | Indique si le serveur Directory est exécuté en mode FIPS.<br><br>Valeur par défaut = 1. Cela signifie qu'eDirectory est exécuté en mode FIPS.<br><br>Pour désactiver le mode FIPS, transmettez n4u.server.fips=0 avec la commande ndsconfig set, puis redémarrez le serveur. |

**REMARQUE :** Pour plus d'informations détaillées sur les paramètres de configuration de eDirectory, consultez la page du manuel `nds.conf`.

# Considérations relatives à la sécurité

Les considérations suivantes relatives à la sécurité sont recommandées :

- Assurez-vous que seuls les utilisateurs authentifiés disposent des droits Parcourir sur l'arborescence. Pour restreindre cela, procédez comme suit :
  - Supprimez les droits Parcourir de [Public] sur la racine de l'arborescence.
  - Assignez les droits Parcourir [Root] sur la racine de l'arborescence.
- Définissez l'attribut `ldapBindRestrictions` de l'objet Serveur LDAP sur `Interdire toute liaison simple anonyme`. Cela empêche les clients de faire des liaisons anonymes.

# 12 Migration vers eDirectory 9.2

Le présent document vous guide pour migrer votre serveur NetIQ eDirectory 8.8.8.x vers eDirectory 9.2 lorsque vous devez aussi mettre à niveau votre système d'exploitation.

Depuis le changement survenu au niveau des systèmes d'exploitation pris en charge par eDirectory 9.2, certaines versions ne sont plus prises en charge par eDirectory 9.2 alors qu'elles l'étaient par eDirectory 8.8.8.x.

Deux scénarios sont possibles lors d'une migration vers eDirectory 9.2 :

- **Migrer vers eDirectory 9.2 lorsqu'une mise à niveau de la plate-forme est possible**

  Dans ce scénario, vous mettez à niveau votre système d'exploitation vers une version prise en charge, puis mettez à niveau eDirectory vers eDirectory 9.2.
- **Migrer vers eDirectory 9.2 lorsqu'une mise à niveau de la plate-forme n'est pas possible**

  Dans ce scénario, vous ne pouvez pas mettre à niveau votre système d'exploitation vers une version prise en charge, car le chemin de migration du système d'exploitation n'est pas possible.

## Migration vers eDirectory 9.2 tout en mettant à niveau le système d'exploitation

Dans ce scénario, vous pouvez migrer vers eDirectory 9.2 après avoir mis à niveau le système d'exploitation. Par exemple, vous pouvez effectuer une mise à niveau à partir d'un système d'exploitation 32 bits vers un système d'exploitation 64 bits. Le tableau ci-dessous décrit le chemin de migration.

**IMPORTANT**

- Assurez-vous d'avoir mis à niveau eDirectory 8.7.3 avec l'ensemble de correctifs le plus récent.
- Si vous utilisez BTRFS, il est recommandé d'effectuer une migration vers un système de fichiers pris en charge. Pour plus d'informations sur la migration, reportez-vous à la section « Migration vers eDirectory 9.2 sans mettre à niveau le système d'exploitation » page 138.

***Tableau 12-1*** *Chemin de migration*

| Système d'exploitation | État de démarrage | État intermédiaire | État intermédiaire | État désiré |
|---|---|---|---|---|
| Windows | Windows 2008 SP2 + eDirectory 8.8 SP8 | Windows 2012 + eDirectory 8.8 SP8 | | Windows 2012 R2 + eDirectory 9.2 |
| | Précautions : avant de mettre à niveau eDirectory sous Linux, vérifiez que le nom d'hôte est configuré sur une adresse IP valide et non sur une adresse de bouclage dans le fichier `/etc/hosts`. | | | |
| Linux | SLES 10 + eDirectory 8.8.8.x | SLES 11 SP4 + eDirectory 8.8.8.x | SLES 12 + eDirectory 8.8 SP8 | SLES 12 + eDirectory 9.2.x |

**IMPORTANT :** veillez à exécuter la commande `ndsconfig upgrade` après la mise à niveau d'eDirectory 8.8 SP8 vers la version 9.2.

### Recommandations

1. Sauvegardez vos fichiers eDirectory 8.8.8.x avant de mettre à niveau le système d'exploitation. Arrêtez eDirectory et sauvegardez les fichiers suivants :
   - Répertoire `dib`
   - Répertoire `nds.rfl` (par défaut ce répertoire est présent sous le répertoire `dib`)
   - Fichier `nds.conf`
   - Répertoire `nici` (dans le cas d'un utilisateur root, le répertoire situé dans `/var/opt/novell/nici/0` correspond au répertoire utilisateur NICI)
   - Fichiers journaux
2. Si la version eDirectory n'est pas prise en charge sur un système d'exploitation spécifique à l'état intermédiaire, n'effectuez aucune autre opération que la mise à niveau d'eDirectory.

## Migration vers eDirectory 9.2 sans mettre à niveau le système d'exploitation

Cette méthode est utilisée dans des scénarios où il n'y a aucun chemin de mise à niveau du système d'exploitation vers la version d'eDirectory 9.2 prise en charge.

Par exemple, eDirectory 8.8 est installé sous SLES 10. Un client qui utilise SLES 10 souhaite passer à eDirectory 9.2 sous SLES 12 alors qu'il n'existe aucun chemin de mise à niveau de SLES 10 vers SLES 12.

Procédez comme suit pour effectuer la migration vers eDirectory 9.2 :

1. Arrêtez le serveur eDirectory.
2. Effectuez une sauvegarde des fichiers eDirectory 8.8 suivants :
   - Répertoire `dib`
   - Répertoire `nds.rfl` (par défaut, ce répertoire est présent sous le répertoire `dib`)
   - Fichier `nds.conf`
   - Répertoire utilisateur NICI (dans le cas d'un utilisateur root, le répertoire situé dans `/var/opt/novell/nici/0` correspond au répertoire utilisateur NICI)
   - Fichiers journaux
3. Installez le système d'exploitation.
4. Installez eDirectory 9.2 sur le serveur (nouvelle installation).
5. Restaurez le répertoire utilisateur NICI dans `/var/opt/novell`.

   Pour plus d'informations sur le répertoire utilisateur NICI, reportez-vous à la section Configuring the Settings for NICI User Directory (Configuration des paramètres pour le répertoire utilisateur NICI) dans le document *NICI Administration Guide* (Guide d'administration de NICI).
6. Restaurez les répertoires `dib` et `nds.rfl`.
7. Restaurez le fichier `nds.conf` sur l'emplacement indiqué par l'utilisateur.
8. Modifiez `/etc/opt/novell/eDirectory/conf/.edir/instances.0` et définissez le chemin absolu sur `nds.conf file`.

9 Modifiez le fichier `nds.conf` et ajoutez ce qui suit:

```
n4u.nds.dir=_file_location
n4u.server.libdir=/opt/novell/eDirectory/lib
n4u.server.vardir=var_directory
n4u.server.configdir=/etc/opt/novell/eDirectory/conf
http.server.module-base=http_server_module_base_directory
```

10 Définissez le chemin comme suit :

Utilisez l'utilitaire `/opt/novell/eDirectory/bin/ndspath`.

11 Exécutez `ndsconfig upgrade` après avoir défini le chemin.

# 13 Déploiement de eDirectory sur les grappes haute disponibilité

Configurer plusieurs serveurs via la synchronisation représente la méthode principale grâce à laquelle NetIQ eDirectory prend en charge la haute disponibilité. Cependant, la mise en grappe peut être une alternative plus viable pour atteindre la haute disponibilité dans certains environnements.

La présente section fournit des instructions pour configurer eDirectory sur des grappes haute disponibilité à l'aide du stockage partagé. Les informations de cette section sont générales, elles s'appliquent aux grappes de disponibilité élevée avec stockage partagé sur les plates-formes Windows et Linux prises en charge ; elles ne sont pas spécifiques d'un gestionnaire de grappes particulier.

Les données d'état de eDirectory doivent être situées sur le stockage partagé de sorte qu'elles soient disponibles sur le noeud de grappe qui exécute actuellement les services. Cela signifie que la DIB de eDirectory doit être située sur le stockage partagé de la grappe. L'instance root eDirectory sur chaque noeud de grappe doit être configurée pour utiliser la DIB sur le stockage partagé.

Outre la DIB, il faut partager les données NICI (NetIQ International Cryptographic Infrastructure) pour que les clés spécifiques du serveur soient répliquées sur les noeuds de grappe. Les données NICI utilisées par tous les noeuds de grappe doivent être situées sur le stockage partagé de grappe.

D'autres données de configuration et de journaux eDirectory doivent également résider sur le stockage partagé.

eDirectory 9.2 inclut un utilitaire destiné aux serveurs Linux et Windows qui configure automatiquement eDirectory dans votre environnement en grappe, y compris en copiant des données vers un emplacement de stockage partagé spécifié, en mettant à jour les paramètres de configuration appropriés et en configurant des services eDirectory sur les noeuds de grappe autres que le noeud primaire.

Les procédures décrites dans les sections ci-après reposent sur les suppositions suivantes :

- Vous connaissez les procédures d'installation de eDirectory.
- Vous utilisez une grappe à deux noeuds.

---

**REMARQUE :** Une grappe à deux noeuds est la configuration minimale utilisée pour la haute disponibilité. Cependant, les concepts de cette section peuvent facilement être appliqués à une grappe comprenant des noeuds supplémentaires. Notez que eDirectory ne prend pas en charge l'équilibrage de la charge en utilisant plusieurs noeuds de grappe.

---

Cette section comprend les rubriques suivantes :

# Mise en grappe des services eDirectory sur Linux

Cette section explique comment configurer eDirectory 9.2 en utilisant la mise en grappe haute disponibilité sur Linux.



## Conditions préalables

- Deux serveurs Linux ou plus équipés d'un logiciel de grappe
- Stockage partagé externe pris en charge par le logiciel de grappe, avec un espace disque suffisant pour stocker toutes les données de eDirectory et NICI
- Adresse IP virtuelle
- NetIQ eDirectory 9.1 ou version ultérieure

---

**REMARQUE :** L'utilitaire nds-cluster-config prend uniquement en charge la configuration de l'instance eDirectory root. eDirectory ne prend pas en charge la configuration de plusieurs instances et les installations non root de eDirectory dans un environnement de grappe.

---

## Installation et configuration de eDirectory

1. Installez et configurez eDirectory sur le serveur que vous souhaitez utiliser comme noeud de grappe primaire. Pour plus d'informations sur les procédures d'installation et de configuration, consultez la « Exécution de l'utilitaire nds-install pour installer des composants eDirectory » page 33.

   ---

   **REMARQUE**

   - Pendant la configuration de eDirectory, le nom de serveur NCP par défaut est le nom de serveur hôte de l'ordinateur sur lequel vous avez installé eDirectory. Comme eDirectory est hébergé sur plusieurs hôtes dans un environnement en grappe, vous devez toutefois indiquer un nom de serveur NCP qui est unique sur la grappe au lieu d'utiliser le nom par défaut. Par exemple, vous pouvez indiquer le nom `clusterserver` pour le serveur NCP lorsque vous configurez eDirectory sur le noeud de grappe primaire.
   - Pendant le processus de configuration, assurez-vous de définir l'adresse IP virtuelle de votre installation de eDirectory. Dans un environnement en grappe, eDirectory écoute uniquement sur l'adresse IP virtuelle et non sur l'adresse IP du système.

   ---

2. Après avoir installé et configuré eDirectory, accédez au fichier `nds.conf`, qui se trouve dans le répertoire `/etc/opt/novell/eDirectory/conf`.
3. Modifiez le fichier `nds.conf` pour définir la valeur du paramètre `n4u.nds.preferred-server` sur l'adresse IP virtuelle de l'installation en grappe, puis enregistrez et fermez le fichier.
4. Vérifiez l'installation de eDirectory en utilisant la commande `ndsstat`.

   eDirectory doit être fonctionnel et en cours d'exécution sur le noeud de grappe primaire.
5. Montez le système de fichiers partagé à l'aide du gestionnaire de grappes.

6 Avant d'exécuter l'utilitaire de configuration, sauvegardez toutes les données dans les répertoires suivants :

- `/var/opt/novell/nici`
- `/var/opt/novell/eDirectory/data` (`n4u.server.vardir`)
- `/var/opt/novell/eDirectory/data/dib` (`n4u.nds.dibdir`)
- `/etc/opt/novell/eDirectory/conf` (`n4u.server.configdir`)
- `/var/opt/novell/eDirectory /log`

---

**REMARQUE :** Si vous installez eDirectory dans un emplacement non défini par défaut, vous pouvez utiliser la commande `ndsconfig get` pour trouver les chemins `vardir`, `dir` utilisés dans votre installation. `nds.conf` doit être dans l'emplacement par défaut, qui est `/etc/opt/novell/eDirectory/conf/nds.conf`.

---

7 Sur le serveur de noeud en grappe primaire, ouvrez un terminal et exécutez la commande suivante pour arrêter le service eDirectory :

```
ndsmanage stopall
```

8 Dans le terminal, accédez à l'emplacement de l'utilitaire de configuration, `nds-cluster-config`. L'utilitaire est situé dans le répertoire `/opt/novell/eDirectory/bin`.

9 Exécutez la commande suivante :

```
nds-cluster-config -s /<sharedfilesystem>
```

où *<sharedfilesystem>* représente l'emplacement à utiliser pour les données de grappe partagées de eDirectory.

---

**REMARQUE :** Vous pouvez également exécuter l'utilitaire en mode sans surveillance à l'aide de l'option `-u`. Si vous utilisez cette option, l'utilitaire ne demande pas de confirmation lorsque vous configurez eDirectory sur une grappe.

Si vous utilisez l'option sans surveillance, vous devez également utiliser l'option `-s` et indiquer le système de fichiers en grappe partagé.

---

10 Après que l'utilitaire a vérifié la validité du stockage partagé en grappe, cliquez sur **y** pour poursuivre la configuration sur la grappe.

L'utilitaire de configuration déplace les données des répertoires susmentionnés vers les emplacements suivants sur le système de fichiers partagé :

- *<système_fichiers_partagé>*/nici
- *<système_fichiers_partagé>*/data
- *<système_fichiers_partagé>*/data/
- *<système_fichiers_partagé>*/conf
- *<système_fichiers_partagé>*/log

11 Démarrez les services de eDirectory en exécutant la commande suivante :

```
ndsmanage startall
```

12 Vérifiez l'état de eDirectory en utilisant ndsstat. Les services de eDirectory doivent être fonctionnels et en cours d'exécution.

13 Arrêtez les services de eDirectory en exécutant la commande suivante :

```
ndsmanage stopall
```

14 Connectez-vous au serveur que vous souhaitez utiliser comme noeud secondaire de la grappe.

15 Utilisez le gestionnaire de grappes pour déplacer le stockage partagé vers le noeud secondaire.

16 Installez la même version de eDirectory sur le noeud de grappe secondaire que celle installée sur le noeud de grappe primaire, mais ne configurez pas eDirectory.

17 Dans le terminal, accédez à l'emplacement de l'utilitaire de configuration sur le noeud secondaire. L'utilitaire est situé dans le répertoire `/opt/novell/eDirectory/bin`.

18 Ouvrez un terminal et exécutez la commande suivante :

```
nds-cluster-config -s /<sharedfilesystem>
```

Où *<système_fichiers_partagé>* représente le stockage partagé en grappe. Le chemin du *<système_fichiers_partagé>* doit être le même que l'emplacement de chemin indiqué lors de la configuration du noeud primaire.

L'utilitaire nds-cluster-config relie le noeud en grappe secondaire aux données partagées de eDirectory situées sur le système de fichiers en grappe.

19 Démarrez les services de eDirectory en exécutant la commande suivante :

```
ndsmanage startall
```

Vérifiez l'état de eDirectory en utilisant la commande `ndsstat`.

20 Arrêtez les services de eDirectory sur le noeud secondaire en exécutant la commande `ndsmanage stopall`.

21 Après avoir configuré avec succès eDirectory sur les deux noeuds de la grappe, vous devez aussi modifier le mode de démarrage du service ndsd sur chaque noeud en utilisant la commande suivante :

```
chkconfig -d ndsd
```

22 Une fois que l'utilitaire de configuration a terminé de configurer le noeud secondaire, vous pouvez utiliser le gestionnaire de grappes pour ajouter les services de eDirectory dans la grappe.

Pour plus d'informations sur les Cluster Services sous Linux, reportez-vous à la documentation suivante :

- SUSE Linux Enterprise Server (SLES 12 et versions ultérieures)
- SLES 11 SP4

---

**IMPORTANT :** Idéalement, le gestionnaire de grappes vérifie que deux noeuds ou plus n'accèdent pas simultanément à la même DIB. Vous devez toutefois vous assurer que ndsd n'est pas exécuté simultanément à partir de deux noeuds de grappe ou plus. Cela est dû au fait que l'accès à la même DIB par le biais de deux noeuds ou plus provoque la corruption de la DIB.

---

## Configuration du serveur SNMP dans des environnements Linux en grappe

1 Sur tous les noeuds, modifiez le fichier `snmpd.conf`. Pour plus d'informations, consultez la section « Installer et configurer les services SNMP pour eDirectory » du *Guide d'administration de NetIQ eDirectory* .

2 Démarrez ndssnmpsa.

3 Sélectionnez Oui pour l'option `Mémoriser le mot de passe`.

4 Pour démarrer le service SNMP, effectuez l'une des actions suivantes :
   - Ajoutez `/etc/init.d/ndssnmpsa start` au script `post_ndsd_start` et `/etc/init.d/ndssnmpsa stop` au script `pre_ndsd_stop`.
   - Ajoutez `ndssnmpsa` comme ressource en grappe avec une dépendance sur la ressource eDirectory.

---

**REMARQUE :** Étant donné que eDirectory écoute sur une adresse IP virtuelle, les trappes ont l'adresse IP de l'hôte, qui est l'adresse IP de l'agent.

---

# Mise en grappe des services eDirectory sur Windows

Cette section explique comment configurer eDirectory 9.2 en utilisant la mise en grappe haute disponibilité sur Windows.


- « Conditions préalables » page 145
- « Installation et configuration de eDirectory » page 145
- « Configuration du serveur SNMP dans des environnements Windows en grappe » page 147


## Conditions préalables

- Deux serveurs Windows ou plus équipés d'un logiciel de grappe
- Stockage partagé externe pris en charge par le logiciel de grappe
- Adresse IP virtuelle
- NetIQ eDirectory 9.2

## Installation et configuration de eDirectory

1 Installez et configurez eDirectory sur le serveur que vous souhaitez utiliser comme noeud de grappe primaire. Pour plus d'informations sur les procédures d'installation et de configuration, consultez la « Installation ou mise à niveau d'eDirectory 9.2 sur un serveur Windows » page 62.

2 Montez le volume partagé à l'aide du gestionnaire de grappes.

3 Sauvegardez tous les fichiers de la DIB et les données NICI avant d'exécuter l'utilitaire de configuration.

4 Sur le noeud de grappe primaire, ouvrez un terminal et accédez à l'utilitaire `NDSCons.exe`. L'utilitaire est situé dans le dossier *<dossier d'installation eDirectory>* par défaut.

5 Dans le terminal, exécutez la commande suivante :

```
NDSCons.exe
```

6 Dans l'utilitaire NDSCons, cliquez sur **Arrêter** pour arrêter tous les services eDirectory.

7 Cliquez sur **Oui** pour confirmer.

8 Dans le terminal, accédez à l'emplacement de l'utilitaire de configuration, `dsclusterconfig.exe`. L'utilitaire est situé dans le dossier <dossier d'installation eDirectory> par défaut.

9 Exécutez la commande suivante :

```
dsclusterconfig.exe -s /<sharedfilesystem>
```

où *<sharedfilesystem>* représente l'emplacement à utiliser pour les données de grappe partagées de eDirectory.

---

**REMARQUE**

- Vous pouvez également exécuter l'utilitaire en mode sans surveillance à l'aide de l'option -s incluant `-u`.
- Vous devez indiquer un dossier au sein du lecteur partagé monté sur le noeud de grappe primaire. Vous ne pouvez indiquer qu'un seul nom de lecteur. Par exemple, au lieu d'indiquer `E:`, vous devez indiquer `E:\Novell`.

---

**10** Après que l'utilitaire a vérifié la validité du stockage partagé en grappe, cliquez sur **y** pour poursuivre la configuration sur la grappe.

L'utilitaire de configuration déplace les données des répertoires susmentionnés vers les emplacements suivants sur le système de fichiers partagé :

- *<système_fichiers_partagé>*`/nici`
- *<système_fichiers_partagé>*`/Files`

Outre le déplacement des données eDirectory vers le système de fichiers partagé, l'utilitaire copie la clé du registre des services eDirectory sur le volume partagé, en enregistrant la clé en tant que fichier `ndsConfigKey`.

L'utilitaire change également le type de démarrage du service `Serveur NDS` sur l'ordinateur du noeud primaire en le passe du mode `Automatique` au mode `Manuel`.

**11** Dans l'utilitaire NDSCons, cliquez sur **Démarrer** pour démarrer tous les services eDirectory.

**12** Vérifiez que tous les services eDirectory sont en cours d'exécution, puis utilisez l'utilitaire NDSCons pour arrêter à nouveau les services.

**13** Fermez l'utilitaire NDSCons.

**14** Connectez-vous au serveur que vous souhaitez utiliser comme noeud secondaire de la grappe.

**15** Utilisez le gestionnaire de grappes pour déplacer le stockage partagé vers le noeud secondaire.

**16** Utilisez le programme d'installation de eDirectory pour réaliser une installation sans surveillance de eDirectory sur le noeud secondaire. Assurez-vous que le mode d'installation est `install`.

**17** Dans le terminal, accédez à l'emplacement de l'utilitaire de configuration sur le noeud secondaire. L'utilitaire est situé dans le dossier d'installation eDirectory par défaut.

**18** Exécutez la commande suivante :

```
dsclusterconfig.exe -s /<sharedfilesystem>
```

Où *<système_fichiers_partagé>* représente le stockage partagé en grappe. Le chemin du *<système_fichiers_partagé>* doit être le même que l'emplacement de chemin indiqué lors de la configuration du noeud primaire.

**19** L'utilitaire dsclusterconfig met à jour le registre sur le noeud de grappe secondaire vers les données partagées de eDirectory situées sur le système de fichiers en grappe.

**20** Une fois que l'utilitaire de configuration a terminé la configuration du noeud secondaire, ouvrez l'utilitaire NDSCons.

**21** Dans l'utilitaire NDSCons, cliquez sur **Démarrer**.

**22** Cliquez sur **Oui** pour confirmer.

**23** Quand NDSCons démarre tous les services eDirectory, vérifiez eDirectory, puis cliquez sur **Arrêter**.

**24** Cliquez sur **Oui** pour confirmer.

25 Pour configurer eDirectory dans le groupe Ressource de la grappe, créez une nouvelle ressource dans le groupe Ressource à utiliser pour eDirectory.

Vous devez fournir les détails suivants :

- Type de ressource - Service générique
- Dépend de - Adresse IP et disque partagé dans le groupe Ressource
- Nom du service - `NDS Server0`
- Aucun paramètre de démarrage
- Clés de registre - `SYSTEM\CurrentControlSet\Services\NDS Server0`

---

**REMARQUE :** Idéalement, le gestionnaire de grappes vérifie que deux noeuds ou plus n'accèdent pas simultanément à la même DIB. Vous devez toutefois vous assurer que ndsd n'est pas exécuté simultanément à partir de deux noeuds de grappe ou plus. Cela est dû au fait que l'accès à la même DIB par le biais de deux noeuds ou plus provoque la corruption de la DIB.

---

## Configuration du serveur SNMP dans des environnements Windows en grappe

1 Sur le noeud de grappe primaire, configurez l'agent maître et définissez le type de démarrage sur automatique. Pour plus d'informations, consultez la section « Installer et configurer les services SNMP pour eDirectory » du *Guide d'administration de NetIQ eDirectory* .

2 Enregistrez le mot de passe de eDirectory quand vous êtes invité à le saisir.

3 Démarrez le sous-agent.

4 Effectuez l'Étape 1 à l'Étape 3 sur les autres noeuds.

# Dépannage des environnements en grappe

## Réparation ou mise à niveau de eDirectory sur des noeuds en grappe

Lorsque vous effectuez une réparation ou une mise à niveau sur l'un des noeuds de grappe, les autres noeuds de grappe peuvent être mis sur pause ou en attente pour éviter toute reprise après échec automatique.

## Création de clés de registre Windows

Dans le cadre du processus de configuration dans les environnements en grappe Windows, l'utilitaire de configuration crée automatiquement une clé de registre, `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NDS Server0\ImagePath`, sur le système de fichiers partagé de la grappe. eDirectory a besoin de la clé de registre pour démarrer le service `Serveur NDS x86` sur les noeuds de grappe.

Si l'utilitaire ne peut pas créer la clé de registre et renvoie un message d'erreur pendant la configuration, vous devez utiliser l'éditeur de registre pour créer manuellement la clé de registre sur tous les noeuds de grappe, même si l'utilitaire de configuration semble avoir terminé avec succès la configuration.

Créez la clé de registre suivante sur tous les noeuds :

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NDS Server0\ImagePath`

Assignez la valeur suivante à la clé `ImagePath` :

`"<primarynodeinstallfolder>\NDS\ndsserv.exe" /DataDir="<sharedstorage>\Files" ds`

Où *<primarynodeinstallfolder>* représente le dossier où vous avez installé eDirectory sur le noeud primaire et *<sharedstorage>* représente le chemin vers l'emplacement du système de fichiers partagé.

# Options de l'utilitaire de configuration

Les options pouvant être utilisées dans l'utilitaire de configuration sont les suivantes :

`<configuration utility> [-h] [-u] [-s /<sharedfilesystem>]`

Où *<configuration utility>* représente `nds-cluster-config` ou `dsclusterconfig.exe`, selon la plate-forme, et *<sharedfilesystem>* représente l'emplacement à utiliser pour les données de grappe partagées de eDirectory.

| Paramètre | Description |
|---|---|
| `-h` | Affiche l'aide de l'utilitaire de configuration. |
| `-s` | Indique le chemin du répertoire partagé de la grappe. |
| `-u` | Permet à l'utilitaire de configurer eDirectory sur la grappe en mode sans surveillance.<br><br>Si vous exécutez l'utilitaire à l'aide de l'option `-u`, vous devez également utiliser l'option `-s` et indiquer le chemin de répertoire partagé. Par exemple :<br><br>`nds-cluster-config -u -s <sharedfilesystem>` |

# 14 Désinstallation de NetIQ eDirectory

Ce chapitre développe les informations suivantes :



## Désinstallation de eDirectory sous Windows

Pour supprimer eDirectory, ConsoleOne, l'agent Annuaire SLP et NICI sur des serveurs Windows, utilisez le Panneau de configuration de Windows.

---

**IMPORTANT :** La suppression de eDirectory entraîne également celle du répertoire des journaux de transactions individuelles et de leur contenu. Pour être en mesure d'utiliser les journaux afin de restaurer ultérieurement eDirectory sur le serveur, vous devez les copier dans un autre emplacement avant de supprimer eDirectory. Pour plus d'informations sur les journaux de transactions individuelles, reportez-vous à la section « Utilisation des journaux de transactions individuelles » du *Guide d'administration de NetIQ eDirectory* .

---



---

**REMARQUE :** Les fichiers HTML créés à l'aide de iMonitor ne sont pas supprimés. Vous devez supprimer manuellement ces fichiers du `<répertoire d'installation>\novell\NDS\ndsimon\dsreports` avant de supprimer eDirectory.

---

### Désinstallation de eDirectory, ConsoleOne et de l'agent Annuaire SLP

1. Sur le serveur Windows où est installé eDirectory, cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **Ajout/Suppression de programmes**.
2. Sélectionnez **eDirectory**, **ConsoleOne** ou l'**agent Annuaire SLP** dans la liste, puis cliquez sur **Ajouter/Supprimer**.
3. Confirmez la suppression en cliquant sur **Oui**.

   L'Assistant d'installation supprime le programme du serveur.

# Désinstallation sans surveillance de eDirectory

Sur Windows, la désinstallation sans surveillance de eDirectory utilise des fichiers texte prédéfinis qui facilitent ledit processus. Vous pouvez effectuer les actions suivantes en utilisant le mode de désinstallation sans surveillance de eDirectory :

- Déconfiguration du eDirectory installé.
- Désinstallation autonome de eDirectory.
- Désinstallation et déconfiguration de eDirectory.

Les sections suivantes abordent les diverses fonctionnalités de la désinstallation sans surveillance de eDirectory :



## Fichiers de réponse

La désinstallation de eDirectory sur un système d'exploitation Windows peut être réalisée en mode silencieux et de façon plus flexible en utilisant un fichier de réponses (`remove.rsp`) pour effectuer les tâches suivantes :

- Désinstallation complète sans surveillance avec toutes les données utilisateur requises
- Configuration par défaut des composants
- Ignorez toutes les invites pendant l'installation

Un fichier de réponses est un fichier texte qui contient des sections et des clés (comme un fichier `Windows.ini`). Pour le créer et le modifier, vous pouvez utiliser tout éditeur de texte ASCII. La mise à niveau eDirectory lit directement les paramètres de désinstallation depuis le fichier de réponses et remplace les valeurs de désinstallation par défaut par celles du fichier de réponses. Le programme de désinstallation accepte les valeurs du fichier de réponses et poursuit la désinstallation sans émettre d'invite.

## Sections et clés du fichier remove.rsp

La désinstallation de eDirectory nécessite de modifier les sections dans le fichier de réponses en vue d'ajouter des informations comme le nom de l'arborescence, le contexte administrateur, les références de l'administrateur (nom d'utilisateur et mots de passe), etc. Une liste complète des clés et de leurs valeurs par défaut est disponible dans l'exemple de fichier `remove.rsp` fourni avec l'installation de eDirectory.

---

**REMARQUE :** Vous devez utiliser le fichier `remove.rsp` fourni. Vous le trouverez sous `eDirectory\windows\x64\NDSonNT\remove.rsp` dans le dossier d'installation de eDirectory. Les paramètres essentiels sont définis par défaut dans ce fichier. Lorsque vous modifiez le fichier `remove.rsp`, vérifiez qu'il n'y a aucun espace entre la clé et les valeurs accompagnées du signe égal (« = ») dans chaque paire clé-valeur.

---

Vous fournissez les références de l'utilisateur administrateur dans le fichier `remove.rsp` en vue d'une désinstallation sans surveillance. Par conséquent, vous devez supprimer définitivement le fichier après la désinstallation pour éviter de compromettre les références de l'administrateur.

## Ajouter des fonctionnalités à la désinstallation automatisée

La plupart des détails portant sur la configuration du programme de désinstallation de eDirectory ont des paramètres par défaut prévus pour la désinstallation manuelle. Cependant, pendant la désinstallation sans surveillance, chaque paramètre de configuration doit être explicitement configuré. Cette section aborde les paramètres de base à déconfigurer.

### Détails sur le serveur eDirectory

Les détails du serveur à désinstaller doivent être fournis au programme de désinstallation. La plupart de ces informations sont configurées dans trois balises : `[Novell:NDSforNT:1.0.0]`, `[Initialization]` et `[Selected Nodes]`.

Prenez toutes les valeurs mentionnées dans `[Initialization]` et `[Selected Nodes]` vers `remove.rsp` telles quelles.

### [Novell:NDSforNT:1.0.0]

**Nom de l'arborescence :** Nom de l'arborescence à partir de laquelle le serveur sera désinstallé.

**Nom de connexion d'admin. :** Le nom (RDN) de l'objet Administrateur de l'arborescence qui possède les droits complets, au moins sur le contexte auquel ce serveur est ajouté. Toutes les opérations ayant lieu dans l'arborescence seront réalisées sous cet utilisateur.

**Contexte d'admin. :** Tout utilisateur ajouté à une arborescence possède un objet Utilisateur qui contient tous les détails spécifiques à l'utilisateur. Ce paramètre est l'objet Conteneur de l'arborescence à laquelle l'objet Administrateur sera ajouté. Pour des installations de serveur primaire, ce conteneur sera créé avec l'objet Serveur.

**Mot de passe de l'administrateur :** Le mot de passe de l'objet Administrateur créé dans les paramètres précédents. Ce mot de passe sera configuré sur l'objet Administrateur pendant les installations du serveur primaire. Pour les installations de serveur secondaire, le mot de passe de l'objet Administrateur du serveur primaire doit détenir les droits sur le contexte auquel le nouveau serveur est ajouté.

**Emplacement NDS :** L'emplacement d'installation de eDirectory dans le système local sur lequel les bibliothèques et binaires sont copiés. Par défaut, eDirectory est installé dans `C:\Novell\NDS` sauf si cela est modifié dans le fichier réponses.

**DataDir :** Jusqu'à la version 9.2 d'eDirectory, la DIB était installée dans l'emplacement NDS en tant que sous-dossier. Plus tard, les administrateurs ont eu la possibilité de fournir un emplacement de DIB différent car il risquait d'y avoir trop de données stockées dans la DIB pour pouvoir les insérer dans l'emplacement NDS. Actuellement, la DIB est installée par défaut dans le sous-dossier `Fichier` dans l'emplacement NDS, mais les administrateurs peuvent modifier ce paramètre et fournir un emplacement différent.

**mode :** Le type de configuration sur eDirectory. Les trois types de configuration sont :

- configure : effectue la déconfiguration de eDirectory.
- uninstall : effectue la désinstallation de eDirectory.
- full : effectue la désinstallation et la déconfiguration de eDirectory.

**REMARQUE :** Si vous choisissez le mode de configuration complet pendant la désinstallation sans surveillance, vous ne pouvez pas choisir l'option de déconfiguration et de désinstallation individuelle pendant la désinstallation configuration de eDirectory.

**ConfigurationMode :** Si la configuration mentionnée dans la clé mode est deconfigure, vérifiez alors que vous ne modifiez pas la valeur `RestrictNodeRemove` de la clé `ConfigurationMode`.

**Prompt :** Le type de mode de désinstallation doit être mentionné dans cette variable. Il sera défini par défaut sur « silent » dans le cas d'une désinstallation sans surveillance. Si une autre valeur est définie, une désinstallation normale sera alors réalisée.

Ce qui suit est un exemple de texte inclus dans le fichier de réponses pour tous les paramètres de base décrits ci-dessus :

```
[Novell:NDSforNT:1.0.0]

  Tree Name=SILENTCORP-TREE

  Admin Context=Novell

  Admin Login Name=Admin

  Admin Password=novell

  prompt=silent
```

## Supprimer les modifications du fichier de configuration

Dans le fichier `remove.cfg` situé dans `<Lecteur d'installation Windows>\Program Files\Common Files\novell\ni\bin`, remplacez

```
[PARAMETERS]0/OUTPUT_TO_FILE
```

par

```
[PARAMETERS]0/OUTPUT_TO_FILE /SILENT
```

## Désinstallation sans surveillance de eDirectory à l'aide du fichier de réponses

Copiez le fichier modifié ci-dessus `remove.rsp` dans `<Lecteur d'installation Windows>\Program Files\Common Files\novell\ni\data`.

L'exécutable `install.exe` installé dans la version de eDirectory est invoqué dans la ligne de commande avec d'autres paramètres. Selon la configuration requise, vous devez utiliser l'une des commandes suivantes :

### Deconfigure

```
<Windows Installed Drive>\Program Files\Common Files\novell\ni\bin>install.exe -
remove /restrictnoderemove /nopleasewait ..\data\ip.db ..\data\remove.rsp
Novell:NDSForNT:1.0.0 0 NDSonNT
```

### Uninstall

1. Renommez le fichier `ip.db` présent dans le répertoire `<Lecteur Windows>\Program Files\Common Files\novell\ni\data`.
2. Copiez le fichier `ip_conf.db` du dossier `<Lecteur Windows>\Program Files\Common Files\novell\ni\data` vers `ip.db`.
3. Exécutez la commande suivante :

   ```
   <Lecteur installé Windows>\Program Files\Common
   Files\novell\ni\bin>install.exe -remove /nopleasewait ..\data\ip.db
   ..\data\remove.rsp Novell:NDSForNT:1.0.0 0 NDSonNT
   ```

### Déconfiguration et désinstallation de eDirectory

```
<Windows Installed Drive>\Program Files\Common Files\novell\ni\bin>install.exe -
remove /nopleasewait ..\data\ip.db ..\data\remove.rsp Novell:NDSForNT:1.0.0 0
NDSonNT
```

Après avoir réalisé la désinstallation de eDirectory ou la configuration combinée, supprimez les dossiers suivants :

- `C:\Novell\NDS` (emplacement par défaut, ou un autre depuis le répertoire installé de eDirectory)
- `C:\Novell\NDS\Files` (emplacement par défaut, ou un autre depuis l'emplacement de la DIB de eDirectory)
- `<Lecteur installé Windows>:\Program Files\Common Files\Novell\ni`
- `<Lecteur installé Windows>:\Windows\system32\NDScpa.cpl`

## Désinstallation de NICI

1. Sur le serveur Windows où est installé eDirectory, cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **Ajout/Suppression de programmes**.
2. Sélectionnez **NICI** dans la liste, puis cliquez sur **Ajouter/Supprimer**.
3. Confirmez la suppression de NICI en cliquant sur **Oui**.

   L'Assistant d'installation retire NICI du serveur.

Après avoir désinstallé NICI, si vous souhaitez supprimer complètement NICI de votre système, effacez le sous-répertoire `C:\Windows\system32\novell\nici` (32 bits) et `C:\Windows\SysWOW64\novell\nici` (64 bits). Il est possible que vous deviez être propriétaire de certains fichiers et répertoires pour les supprimer.

---

**AVERTISSEMENT :** Une fois le sous-répertoire `nici` supprimé, les données précédemment codées à l'aide de NICI seront perdues.

---

## Désinstallation des bibliothèques d'exécution Microsoft Visual C++ 2005 et Visual C++ 2012

Si les bibliothèques d'exécution Microsoft Visual C++ 2005 et Visual C++ 2012 ne sont pas utilisées par d'autres produits que eDirectory, désinstallez-les en suivant la procédure ci-dessous :

1. Accédez à *Ajouter/supprimer des programmes* ou **Programmes et fonctionnalités** sur le serveur Windows où est installé eDirectory.
2. Supprimez le paquetage de redistribution suivant Microsoft Visual C++ 2005 :

   `Microsoft Visual C++ 2012 Redistributable` et `Microsoft Visual C++ 2005 Redistributable (x64)`

# Désinstallation de eDirectory sous Linux

Utilisez l'utilitaire `nds-uninstall` pour désinstaller les composants de eDirectory installés sur les ordinateurs Linux. Cet utilitaire désinstalle eDirectory de l'hôte local. Vous devez déconfigurer le serveur eDirectory avant d'exécuter `nds-uninstall`. Exécutez `ndsconfig rm -a <FDN admin>` pour supprimer le serveur eDirectory. Cet utilitaire est disponible à l'emplacement `/opt/novell/eDirectory/sbin/nds-uninstall`.

Notez que vous ne devez pas exécuter `ndsconfig rm` sur un serveur OES.

---

**IMPORTANT :** La suppression de eDirectory entraîne également celle du répertoire des journaux de transactions individuelles et de leur contenu. Pour être en mesure d'utiliser les journaux afin de restaurer ultérieurement eDirectory sur le serveur, vous devez les copier dans un autre emplacement avant de supprimer eDirectory. Pour plus d'informations sur les journaux de transactions individuelles, reportez-vous à la section « Utilisation des journaux de transactions individuelles » du *Guide d'administration de NetIQ eDirectory* .

---

1. Exécutez la commande `nds-uninstall`.
2. Utilisez la syntaxe suivante.

   ```
   nds-uninstall [-s][-h]
   ```

   Si vous n'indiquez pas les paramètres requis sur la ligne de commande, l'utilitaire nds-install vous invitera à les saisir.

| Paramètre | Description |
|---|---|
| `-h` | Affiche les chaînes d'aide. |
| `-s` | Supprime les paquetages et binaires de eDirectory, même quand les instances sont configurées. Néanmoins, cette option ne supprime pas le répertoire DIB et le fichier de configuration NDS.<br><br>**IMPORTANT :** Veillez à utiliser cette option sans affecter les autres services pendant une trop longue période. |

nds-uninstall ne désinstalle pas les paquetages suivants :

| Paquetage | Raisons expliquant la non-désinstallation |
|---|---|
| `Paquetage NICI` | Il se peut que `NICI` soit utilisé par :<br>◆ Toutes les autres mises à jour de produit<br>◆ eDirectory installé à un emplacement personnalisé ;<br>◆ eDirectory installé par un utilisateur non-root. |
| `NOVLsubag` | Il se peut que `NOVLsubag` soit utilisé par :<br>◆ eDirectory installé à un emplacement personnalisé ;<br>◆ eDirectory installé par un utilisateur non-root. |

# Désinstallation sans surveillance de eDirectory sous Linux

1. Supprimez les instances de eDirectory :

   ```
   ndsconfig rm -a <user name> -w passwd -c
   ```

2. Utilisez l'un des scripts automatisés suivants pour déconfigurer eDirectory :

   **Passer le mot de passe dans la variable d'environnement :** `ndsconfig rm -a <nom d'utilisateur> -w env:<variable d'environnement> -c`

   **Passer le mot de passe dans un fichier :** `ndsconfig rm -a <nom d'utilisateur> -w file:<nom de fichier avec chemin absolu/relatif> -c`

3. (Optionnel) Dans le cas d'instances multiples, exécutez la commande suivante pour chaque instance :

   ```
   ndsconfig rm -a <user name> -w passwd  --config-file <absolute path for configuration file>
   ```

   Par exemple :

   ```
   ndsconfig rm -a admin.novell -w n -c
   ndsconfig rm -a admin.novell -w env:ADM_PASWD -c
   ndsconfig rm -a admin.novell -w file:/Builds/88SP8/adm_paswd -c
   ```

4. Pour désinstaller les paquetages eDirectory, exécutez le script nds-uninstall pour supprimer les paquetages eDirectory :

   ```
   nds-uninstall -u
   ```

# Avertissements concernant la désinstallation de eDirectory

Quand vous désinstallez eDirectory et le réinstallez, le serveur eDirectory ne peut pas être accessible aux autres serveurs du réseau. Toutes les opérations distribuées telles que la synchronisation et le traitement des notices nécrologiques n'ont pas lieu sur les partitions dont les répliques sont présentes sur le serveur eDirectory. Si cet état persiste un moment, cela peut avoir des incidences sur tous les serveurs et sur les processus en cours sur ces derniers.

Évitez de désinstaller une version plus récente de eDirectory et d'installer une version précédente, car :

- cela ne rétablit pas les mises à niveau associées au schéma ;
- eDirectory risque de ne pas être fonctionnel si la DIB est mise à niveau vers la version plus récente ;
- cela supprime tous les fichiers de configuration existants, sauf le fichier `nds.conf`.

Néanmoins, prenez en compte ce qui suit quand vous désinstallez une version plus récente de eDirectory installez une version précédente :

- mettez à niveau la DIB vers la version la plus récente, sinon eDirectory risque de ne pas fonctionner ;
- sauvegardez les fichiers de configuration existants, sauf le fichier `nds.conf` et procédez à la restauration quand eDirectory est réinstallé ;
- cela ne rétablit pas les mises à niveau associées au schéma ;

# A Paquetages Linux pour NetIQ eDirectory

NetIQ eDirectory contient un système de paquetages Linux. Il s'agit d'une collection d'outils visant à simplifier l'installation et la désinstallation de différents composants de eDirectory. Ces paquetages contiennent des fichiers « makefile » qui décrivent les paramètres à prendre en compte pour installer un composant défini de eDirectory. Ces paquetages contiennent également des fichiers de configuration, des utilitaires, des bibliothèques, des daemons et des pages du manuel qui utilisent les outils standard Linux installés avec l'OS.

Le tableau suivant fournit des informations sur les paquetages Linux inclus dans NetIQ eDirectory.

**REMARQUE :** Sous Linux, tous les paquetages ont comme préfixe *novell-* sauf **eba**. Par exemple, NDSserv s'appelle novell-NDSserv.

| Paquetage | Description |
|---|---|
| NOVLice | Contient l'utilitaire d'importation, de conversion et d'exportation NetIQ et dépend des paquetages NOVLlmgnt, NOVLxis et NLDAPbase. |
| NDSbase | Représente l'agent Utilisateur/Annuaire. Ce paquetage dépend du paquetage NICI.<br>Le logiciel NDSbase contient les éléments suivants :<br>◆ Boîte à outils contenant l'authentification RSA nécessaire à eDirectory<br>◆ Bibliothèque indépendante de la plate-forme et du système, bibliothèque contenant toutes les fonctions définies de l'agent utilisateur d'annuaire et bibliothèque d'extension du schéma<br>◆ Utilitaire de configuration combiné et utilitaire de test de l'agent utilisateur d'annuaire<br>◆ Fichier de configuration et pages de manuel de eDirectory |
| NDScommon | Contient les pages du manuel du fichier de configuration et des utilitaires d'installation et de désinstallation de eDirectory. Ce paquetage dépend du paquetage NDSbase. |
| NDSmasv | Contient les bibliothèques requises pour le service MASV (Mandatory Access Control). |

| Paquetage | Description |
|---|---|
| NDSserv | Contient tous les binaires et bibliothèques nécessaires à eDirectory Server. Il contient également les utilitaires de gestion de eDirectory Server sur le système. Ce paquetage dépend des paquetages de NDSbase, NDScommon, NDSmasv, NLDAPsdk, NOVLpkia et NOVLpkit.<br><br>Le logiciel NDSserv contient les éléments suivants :<br><br>◆ Bibliothèque d'installation NDS, bibliothèque FLAIM, bibliothèque de trace, bibliothèque NDS, bibliothèque de serveur LDAP, bibliothèque d'installation LDAP, bibliothèque d'éditeur d'index, bibliothèque DNS, bibliothèque de fusion et bibliothèque d'extension LDAP pour SDK LDAP<br>◆ Daemon eDirectory Server<br>◆ Valeur binaire pour DNS et valeur binaire pour le chargement ou le déchargement de LDAP<br>◆ L'utilitaire nécessaire pour créer l'adresse MAC, l'utilitaire de trace du serveur et de modification de certaines variables globales du serveur, l'utilitaire de sauvegarde et de restauration de eDirectory et l'utilitaire de fusion des arborescences eDirectory<br>◆ Scripts de démarrage de DNS, NDSD et NLDAP<br>◆ Pages du manuel |
| NDSimon | Contient les bibliothèques d'exécution ainsi que les utilitaires permettant de rechercher et de récupérer des données à partir des services eDirectory. Ce paquetage dépend du paquetage NDSbase. |
| NDSrepair | Contient les bibliothèques d'exécution ainsi que l'utilitaire permettant de corriger les problèmes liés à la base de données eDirectory. Ce paquetage dépend du paquetage NDSbase. |
| NLDAPbase | Contient les bibliothèques LDAP, leurs extensions et les outils LDAP suivants :<br><br>◆ ldapdelete<br>◆ ldapmodify<br>◆ ldapmodrdn<br>◆ ldapsearch<br><br>Ce paquetage dépend du paquetage NLDAPsdk. |
| NOVLnmas | Contient l'ensemble des bibliothèques NMAS, ainsi que les fichiers binaires nmasinst requis par le serveur NMAS. Ce paquetage dépend des paquetages NICI et NDSmasv. |
| NLDAPsdk | Contient les extensions NetIQ du module d'exécution LDAP et des bibliothèques de sécurité (Client NICI). |
| NOVLsubag | Contient les utilitaires et bibliothèques d'exécution du sous-agent SNMP de eDirectory. Ce paquetage dépend des paquetages NICI, NDSbase et NLDAPbase. |
| NOVLpkit | Fournit des services PKI indépendants de eDirectory. Ce paquetage dépend des paquetages NICI et NLDAPsdk. |
| NOVLpkis | Fournit le service PKI Server. Ce paquetage dépend des paquetages NICI, NDSbase et NLDAPsdk. |
| NOVLsnmp | Utilitaires et bibliothèques d'exécution pour SNMP. Ce paquetage dépend du paquetage NICI. |

| Paquetage | Description |
|---|---|
| NDSdexvnt | Contient la bibliothèque qui gère les événements générés dans NetIQ eDirectory vers d'autres bases de données. |
| NOVLpkia | Fournit des services PKI. Ce paquetage dépend des paquetages NICI, NDSbase et NLDAPsdk. |
| NOVLembox | Fournit l'infrastructure eMBox et les outils eMTools. |
| NOVLlmgnt | Contient les bibliothèques d'exécution relatives à NetIQ Language Management. |
| NOVLxis | Contient les bibliothèques d'exécution relatives à NetIQ XIS. |
| NOVLsas | Contient les bibliothèques SAS de NetIQ. |
| NOVLntls | Contient la bibliothèque TLS de NetIQ.<br>Ce paquetage est identifié sous le nom ntls sous Linux. |
| NOVLldif2 | Contient l'utilitaire NetIQ Offline Bulkload et dépend des paquetages NDSbase, NDSserv, NOVLntls, NOVLlmgnt et NICI. |
| NOVLncp | Contient les services NCP chiffrés de NetIQ pour Linux. Ce paquetage dépend du paquetage NDScommon. |
| novell-eba | Contient les bibliothèques pour la prise en charge d'EBA. Ce paquetage dépend des paquetages NICI, NDSbase et NDSServ. |

# B Vérifications de l’état de santé de eDirectory

NetIQ eDirectory 9.2 intègre un outil de diagnostic qui permet de déterminer si l'état de santé d'eDirectory est bon. Cet outil sert principalement à vérifier l’état de santé du serveur avant une mise à niveau.

Les vérifications de l’état de santé de eDirectory s’exécutent par défaut lors de chaque mise à niveau et s’opèrent avant la mise à niveau proprement dite du paquetage. Néanmoins, vous pouvez exécuter l’outil de diagnostic `ndscheck` pour vérifier l’état de santé.

## 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.

## Vérifications de l’état de santé

Vous pouvez vérifier l’état de santé de eDirectory de deux manières :

---

**REMARQUE :** pour exécuter l’utilitaire de vérification de l’état de santé, vous devez disposer de droits d’administrateur.

---


- « Avec la mise à niveau » page 161
- « Avec un utilitaire autonome » page 162


### 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 `nds-install`.

### Windows

Les vérifications de l'état de santé de eDirectory 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 de eDirectory au moyen d'un utilitaire autonome. Le tableau suivant liste les noms d'utilitaires de vérification de l'état de santé pour chaque plate-forme.

***Tableau B-1*** *Utilitaires de vérification de l'état de santé*

| Plate-forme | Nom de l'utilitaire |
|---|---|
| Linux | `ndscheck`<br><br>Syntaxe :<br><br>`ndscheck [--help \| -?] Display command usage ndscheck [--version \| -v] Display version information ndscheck [-h <hostname port]>] [-a <admin FDN>] [-F <log file>] [-D] [-q] [--config-file <file name>]` |
| Windows | `ndscheck`<br><br>Syntaxe :<br><br>`ndscheck [--help \| -?] Display command usage ndscheck [--version \| -v] Display version information ndscheck [-h <hostname port]>] [-a <admin FDN>] [-F <log file>] [-D] [-q] [--config-file <file name>]` |

# Types de vérifications de l'état de santé

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

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

Lorsque vous exécutez l'utilitaire `ndscheck`, les résultats sont affichés à l'écran et consignés dans le fichier `ndscheck.log`. Pour plus d'informations sur les fichiers journaux, reportez-vous à la section « Fichiers journaux » page 164.

Si l'état de santé est vérifié dans le cadre de la mise à niveau, vous êtes invité à poursuivre la mise à niveau ou à l'interrompre en fonction des types d'erreurs détectés (le cas échéant). Les types d'erreur sont décrits dans la « Catégorisation de l'état de santé » page 163.

## État de santé général du serveur

Il s'agit de la première étape de la vérification de l'état de santé, celle où l'utilitaire vérifie les points suivants :

1. Le service eDirectory est fonctionnel. La DIB est ouverte et capable de lire certaines informations élémentaires sur l'arborescence de base, 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, il vérifie ensuite celui 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 gardées 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.

# Catégorisation de l'état de santé

Il existe trois types d'état de santé qui dépendent des erreurs détectées pendant la vérification de l'état de santé du serveur eDirectory :

- Normal (page 163)
- Avertissement (page 163)
- Critique (page 164)

Le résultat des vérifications de l'état de santé est consigné dans un fichier journal. Pour plus d'informations, reportez-vous à la « Fichiers journaux » page 164.

## Normal

Toutes les vérifications de l'état de santé ont abouti et l'état de santé du serveur est normal.

La mise à niveau se poursuit sans interruption.

## Avertissement

Des erreurs mineures ont été détectées pendant la vérification de l'état de santé du serveur.

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 :

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

### Critique

Des erreurs critiques ont été détectées pendant la vérification de l'état de santé de eDirectory.

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

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

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

## Fichiers journaux

Chaque vérification de l'état de santé de eDirectory, 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).
- Adresses URL proposant des solutions possibles.
  - Forums de support (http://forums.novell.com/netiq/netiq-product-discussion-forums/edirectory/)
  - Documentation de dépannage (https://www.netiq.com/documentation/edir88/edir88tshoot/data/bookinfo.html)
  - Codes d'erreur (http://www.novell.com/documentation/nwec/)
  - Correctifs (http://support.novell.com/patches.html)
  - Cool Solutions (http://www.novell.com/communities/coolsolutions/edirectory)

Le tableau suivant donne l'emplacement par défaut du fichier journal sur plusieurs plates-formes :

***Tableau B-2*** *Emplacement du fichier journal de l'état de santé*

| Plate-forme | Nom du fichier de consignation | Emplacement |
|---|---|---|
| Linux | `ndscheck.log` | 1. Si vous utilisez l'option `-h`, le fichier `ndscheck.log` est enregistré dans le répertoire privé de l'utilisateur.<br>2. Si vous utilisez 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 | `nsdcheck.log` | Le fichier journal sera enregistré à l'emplacement *`répertoire_installation`*`\novell nds\`.<br>**REMARQUE :** *`répertoire_installation`* est indiqué par l'utilisateur. |

# C Configuration de OpenSLP pour eDirectory

Destinée aux administrateurs, cette annexe contient des informations sur la configuration des installations OpenSLP pour NetIQ eDirectory sans Novell Client.



## Protocole SLP

OpenSLP est une mise en œuvre open-source de la convention IETF Service Location Protocol version 2.0, documentée sur le site IETF Request-For-Comments (RFC) 2608 (http://www.ietf.org/rfc/rfc2608.txt?number=2608).

Outre la mise en œuvre du protocole SLP v2, l'interface fournie par le code source OpenSLP est une implémentation d'une autre norme de l'IETF concernant l'accès par programme à la fonctionnalité SLP, documentée sous RFC 2614 (http://www.ietf.org/rfc/rfc2614.txt?number=2614).

Pour comprendre parfaitement les travaux de SLP, il est important de lire ces documents et de les assimiler. Leur lecture peut s'avérer laborieuse, mais ils sont essentiels pour procéder à une configuration correcte de SLP sur un intranet.

Pour plus d'informations sur le projet OpenSLP, consultez les sites Web OpenSLP (http://www.OpenSLP.org) et SourceForge (http://sourceforge.net/projects/openslp). Le site Web OpenSLP contient plusieurs documents qui offrent de précieux conseils de configuration. Un grand nombre de ces documents sont encore incomplets à la date de rédaction de la présente documentation.

## Concepts fondamentaux de SLP

Le protocole SLP spécifie trois composants :

- L'agent Utilisateur (UA)
- L'agent de service (SA)
- L'agent Annuaire (DA)

La fonction de l'agent Utilisateur est de fournir une interface par programmation aux clients pour leurs requêtes de services, et aux services pour leur permettre de publier leurs annonces. Un agent Utilisateur contacte un agent Annuaire pour interroger des services enregistrés d'une classe de service et d'une étendue spécifiées.

La fonction de l'agent Service consiste à fournir des points de stockage et de maintenance persistants pour des services locaux s'étant enregistrés auprès de SLP. L'agent de service a pour tâche principale de gérer une base de données en mémoire des services locaux enregistrés. En fait, un service ne peut pas s'enregistrer auprès de SLP tant qu'un agent de service local n'est pas présent. Les clients peuvent identifier les services au moyen d'une seule bibliothèque d'agent

Utilisateur, mais l'enregistrement nécessite obligatoirement un agent de service (SA), principalement parce que cet agent doit régulièrement vérifier l'existence de services enregistrés pour maintenir l'enregistrement des agents Annuaire à l'écoute.

Le fonction de l'agent Annuaire consiste à fournir un cache persistant à long terme pour les services annoncés, ainsi qu'un point d'accès permettant aux agents Utilisateur de rechercher des services. En tant que cache, l'agent Annuaire reste à l'écoute de l'annonce de nouveaux services par les agents de service et met en cache ces notifications. À court terme, le cache d'un agent Annuaire se complète. Les agents Annuaire utilisent un algorithme d'expiration pour faire expirer les entrées de cache. Lorsqu'un agent Annuaire s'active, il lit le cache du stockage persistant (en général un disque dur), puis commence à faire expirer les entrées selon l'algorithme. Lorsqu'un nouvel agent Annuaire arrive ou lorsqu'un cache a été supprimé, l'agent Annuaire détecte cette condition et envoie une notification spéciale à tous les agents Service à l'écoute pour qu'ils vident leurs bases de données locales, de manière à ce que l'agent Annuaire puisse rapidement créer son cache.

En l'absence d'agents Annuaire, l'agent Utilisateur effectue une requête de multidiffusion générale à laquelle les agents de service peuvent répondre listant ainsi les services demandés de la même manière que les agents Annuaire créent leur cache. La liste des services renvoyée par une telle requête est incomplète et bien plus localisée que celle fournie par un agent Annuaire, notamment en présence d'un filtrage multidiffusion mis en œuvre par un grand nombre d'administrateurs réseaux, lesquels limitent les diffusions et les multidiffusions au sous-réseau local seulement.

En bref, tout s'articule autour de l'agent Annuaire trouvé par un agent Utilisateur dans une étendue donnée.

## Protocole SLP NetIQ

La version NetIQ de SLP prend certaines libertés vis-à-vis de la norme SLP afin de fournir un environnement d'annonce de service renforcé, mais au prix d'une certaine évolutivité.

Par exemple, pour améliorer l'évolutivité d'une structure d'annonce de service, vous pouvez limiter le nombre de paquets diffusés ou multidiffusés sur un sous-réseau. La norme SLP gère ce facteur en imposant des limitations aux agents de service et Utilisateur concernant les requêtes à l'agent Annuaire. Le premier agent Annuaire identifié qui dessert l'étendue souhaitée est celui qu'un agent de service (et par conséquent des agents Utilisateur locaux) utilisera pour toutes les requêtes futures sur cette étendue.

La mise en œuvre de NetIQ SLP permet d'analyser tous les agents Annuaire connus, à la recherche des informations de la requête. Un acheminement AR de 300 millisecondes étant considéré comme trop long, 10 serveurs peuvent être analysés en 3 à 5 secondes. Il n'est pas nécessaire d'effectuer cette opération si SLP est configuré correctement sur le réseau et que OpenSLP considère le réseau comme configuré correctement pour le trafic SLP. Les valeurs de timeout de réponse de OpenSLP sont supérieures à celles du fournisseur de services SLP de NetIQ et cela limite le nombre d'agents Annuaire au premier qui répond, que les informations de celui-ci soient ou non précises et complètes.

## Agents Utilisateur

Un agent utilisateur prend la forme physique d'une bibliothèque statique ou dynamique liée à une application. Il permet à l'application d'émettre des requêtes de services SLP.

Les agents Utilisateur suivent un algorithme pour obtenir l'adresse d'un agent Annuaire auquel les requêtes seront envoyées. Une fois qu'ils ont obtenu une adresse d'agent Annuaire sur une étendue spécifiée, ils continuent à utiliser cette adresse pour cette étendue jusqu'à ce qu'elle ne réponde plus. Là, ils se procurent une autre adresse pour l'étendue. Les agents Utilisateur localisent l'adresse d'un agent Annuaire sur une étendue spécifiée en :

1. vérifiant si l'identificateur de socket de la requête en cours est connecté à un agent Annuaire pour l'étendue indiquée ; S'il se trouve que la requête fait partie d'une requête en plusieurs parties, elle peut déjà contenir une connexion en cache.
2. recherchant dans le cache de l'agent Annuaire connu un agent Annuaire correspondant à l'étendue indiquée ;
3. recherchant auprès de l'agent de service un agent Annuaire de l'étendue spécifiée (et en ajoutant de nouvelles adresses au cache) ;
4. interrogeant DHCP pour obtenir des adresses d'agents Annuaire configurées pour le réseau et correspondant à l'étendue indiquée (et en ajoutant de nouvelles adresses au cache) ;
5. envoyant une requête d'identification d'agent Annuaire par multidiffusion sur un port connu (et en ajoutant de nouvelles adresses au cache).

Sauf spécification contraire, l'étendue indiquée est celle « par défaut ». Cela signifie que si aucune étendue n'est définie de façon statique dans le fichier de configuration SLP et qu'aucune étendue n'est indiquée dans la requête, l'étendue utilisée est le mot « default ». Notez également que eDirectory n'indique jamais d'étendue dans ses enregistrements. Cela ne signifie pas pour autant que l'étendue utilisée avec eDirectory soit toujours « default ». En fait, s'il existe une étendue configurée statiquement, celle-ci devient l'étendue par défaut pour les requêtes à l'agent Utilisateur local et les enregistrements de l'agent Service en l'absence d'une étendue spécifiée.

## Agents Service

Les agents de service prennent la forme physique d'un processus distinct exécuté sur l'ordinateur hôte. Dans le cas de Windows, `slpd.exe` s'exécute en tant que service sur l'ordinateur local. Des agents utilisateur interrogent l'agent de service local en envoyant des messages à l'adresse de bouclage sur un port connu.

Un agent de service localise et met en cache les agents Annuaire et la liste de l'étendue qu'ils prennent en charge en envoyant directement une requête d'identification d'agent Annuaire à des adresses d'agent Annuaire potentielles en :

1. vérifiant toutes les adresses d'agent Annuaire configurées statiquement (et en ajoutant de nouvelles au cache d'agent Annuaire connu de l'agent de service) ;
2. demandant la liste des agents Annuaire et des étendues à DHCP (et en en ajoutant de nouveaux au cache d'agent Annuaire connu de l'agent de service) ;
3. envoyant une requête d'identification d'agent Annuaire par multidiffusion sur un port connu (et en en ajoutant de nouvelles au cache d'agent Annuaire connu de l'agent de service) ;
4. recevant les paquets d'annonce régulièrement diffusés par les agents Annuaire (et en ajoutant les nouveaux au cache d'agent Annuaire connu de l'agent de service).

Puisqu'un agent utilisateur interroge toujours l'agent de service local en premier, cela est important, car la réponse de l'agent de service local détermine si l'agent utilisateur passe ou non à l'étape suivante de la découverte (dans ce cas, DHCP-- voir étapes 3 et 4 de la section « Agents Utilisateur » page 169).

# Paramètres de configuration

Certains paramètres de configuration du fichier `%systemroot%/slp.conf` contrôlent également la découverte d'agents Annuaire :

```
net.slp.useScopes = <comma delimited scope list>
net.slp.DAAddresses = <comma delimited address list>
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

L'option `useScopes` indique à quelles étendues l'agent Service va s'annoncer et à quelles étendues les requêtes seront adressées en l'absence d'une étendue spécifique lors de l'enregistrement ou de la requête effectuée par le service ou l'application client. Comme eDirectory envoie toujours ses annonces et requêtes à partir de l'étendue par défaut, cette liste sera considérée comme la liste d'étendues par défaut pour l'ensemble des enregistrements et des requêtes de eDirectory.

L'option `DAAddresses` est une liste d'adresses IP décimales avec points, séparées par une virgule, qui doivent être préférées à toutes les autres. Si cette liste des agents Annuaire configurés ne prend pas en charge l'étendue d'un enregistrement ou d'une requête, les agents de service et Utilisateur font alors appel à l'identification d'agent Annuaire multidiffusion, sauf si cette fonction a été désactivée.

L'option `passiveDADetection` a par défaut la valeur Vrai. Les agents Annuaire annoncent régulièrement leur existence sur le sous-réseau au moyen d'un port connu si celui-ci est configuré à cet effet. Ils s'intitulent paquets DAAdvert. Si cette option a pour valeur `Faux`, tous les paquets DAAdvert diffusés sont ignorés par l'agent de service.

L'option `activeDADetection` a également par défaut la valeur Vrai. Elle permet à l'agent de service de diffuser régulièrement une requête à tous les agents Annuaire pour qu'ils répondent au moyen d'un paquet DAAdvert dirigé. Un paquet dirigé n'est pas diffusé, mais envoyé directement à l'agent de service en réponse à ces requêtes. Si cette option a pour valeur `False` (faux), aucune requête régulière de découverte d'agents Annuaire n'est diffusée par l'agent de service.

L'option `DAActiveDiscoveryInterval` est un paramètre de vérification d'état. La valeur par défaut est `1`. Cela signifie que l'agent de service doit seulement envoyer une requête de découverte d'agent Annuaire à l'initialisation. Si vous attribuez la valeur `0` à cette option, cela revient à attribuer la valeur `false` à l'option `activeDADetection`. Toute autre valeur indique un nombre de secondes entre les diffusions d'identification.

Employées correctement, ces options assurent une utilisation appropriée de la bande passante du réseau pour l'annonce de services. En fait, les paramètres par défaut sont conçus pour optimiser l'évolutivité d'un réseau moyen.

# D Résolution des problèmes

Cette section fournit des informations utiles pour la résolution des problèmes rencontrés lors de l'installation et de la configuration d'eDirectory.

## Résolution des problèmes d'installation

Le tableau suivant répertorie les problèmes que vous risquez de rencontrer et les actions suggérées pour les résoudre. Si le problème persiste, contactez votre représentant NetIQ.

| Problèmes connus | Actions suggérées |
|---|---|
| L'installation dure longtemps.<br><br>Lorsque vous installez eDirectory dans une arborescence existante, si l'installation prend trop de temps, consultez l'écran DSTrace sur le serveur. Si le message `-625 Échec de transport` s'affiche, vous devez réinitialiser le cache d'adresses | Pour réinitialiser le cache des adresses, entrez la commande suivante sur la console système :<br><br>`set dstrace = *A` |
| L'installation de eDirectory échoue pour les administrateurs de conteneurs<br><br>Le programme d'installation d'eDirectory 9.0 prend en charge les installations effectuées par les administrateurs disposant de droits Superviseur sur le conteneur dans lequel réside le serveur. Pour ce faire, le premier serveur sur lequel eDirectory 9.0 est installé doit disposer de droits Superviseur sur la racine ([Root]) pour étendre le schéma. De ce fait, il n'est pas nécessaire que les autres serveurs disposent de droits sur la racine [Root]. Cependant, selon la plate-forme sur laquelle est installé eDirectory 9.0 en premier lieu, il se peut que les schémas ne soient pas tous étendus, ce qui nécessite des droits Superviseur sur la racine pour l'installation des autres serveurs sur des plates-formes différentes. | Si eDirectory 9.0 doit être installé sur plusieurs plates-formes, assurez-vous de disposer de droits Superviseur sur [Racine] pour le premier serveur sur lequel eDirectory sera installé pour CHACUNE des plates-formes. Par exemple, si le premier serveur sur lequel eDirectory 9.0 doit être installé fonctionne sous Linux et que eDirectory 9.0 doit également être installé sur Solaris, le premier serveur de chaque plate-forme doit disposer de droits Superviseur sur [Racine]. Les autres serveurs de chacune des plates-formes devront seulement disposer de droits Administrateur des conteneurs sur le conteneur où le serveur est installé.<br><br>Pour plus d'informations, reportez-vous à la solution NOVL83874 (http://support.novell.com/docs/Tids/Solutions/10073723.html) *du eDirectory 8.7.x Readme Addendum (Addendum au fichier Lisezmoi de Novell eDirectory 8.7.x* |
| Modules d'écoute par défaut pour la nouvelle interface réseau | Sous Windows, eDirectory écoute sur toutes les interfaces configurées sur l'ordinateur pour les protocoles NCP, HTTP, HTTPS, LDAP et LDAPS par défaut. Après l'ajout de la nouvelle adresse d'interface réseau à l'ordinateur et le redémarrage d'eDirectory, le programme commencera automatiquement à écouter sur cette adresse et à avoir des renvois ajoutés en conséquence.<br><br>**REMARQUE :** sous Linux, des interfaces doivent être ajoutées manuellement au paramètre `n4u.server.interfaces`. |

| Problèmes connus | Actions suggérées |
| --- | --- |
| Problèmes de réplication après la mise à niveau<br><br>Lorsque vous effectuez une mise à niveau de vers eDirectory 9.0 et activez la réplication codée, il se peut que la réplication échoue, même si ce scénario est plutôt rare. | Pour résoudre ce problème :<br><br>1. Dans NetIQ iManager, sélectionnez **Modifier un objet**, puis l'objet Serveur NCP.<br>2. Sous l'onglet Général, sélectionnez **Autre**.<br>3. Sélectionnez **NCPKeyMaterialName** dans la liste des attributs non définis et ajoutez-le à la liste des attributs définis avec le nom de certificat (p. ex., **SSL CertificateDNS**).<br>4. Exécutez le contrôleur de connectivité (limber) sur le serveur où l'attribut a changé à l'Étape 3. Pour plus d'informations sur l'utilisation du contrôleur de connectivité (limber), reportez-vous au manuel NetIQ eDirectory Administration Guide (Guide d'administration de NetIQ eDirectory 8.8 SP8). |

# Résolution des problèmes de configuration

Le tableau suivant répertorie les problèmes que vous risquez de rencontrer et les actions suggérées pour les résoudre. Si le problème persiste, contactez votre représentant NetIQ.

| Problèmes connus | Actions suggérées |
| --- | --- |
| Le serveur Annuaire retourne des renvois de boucle | Lorsque eDirectory est configuré pour écouter des adresses de boucle, ces adresses sont stockées et retournées aux clients lorsqu'ils effectuent des recherches et d'autres opérations. Les renvois ne s'appliquent pas aux clients qui essaient de se connecter à partir de machines autres que le serveur. Par conséquent, ces renvois de boucle ne permettent pas aux clients de se connecter. Toutefois, les autres renvois retournés par le serveur continuent à fonctionner pour les clients.<br><br>Si vous essayez de vous connecter à chaque renvoi de boucle et choisissez ensuite les renvois corrects, les performances des clients risquent d'être altérées. |
| Échec de recherche de nom d'arborescence : erreur -632 lors de la configuration de eDirectory 9.0 sous Linux | Lors de la configuration de eDirectory 9.0 sous Linux, la recherche du nom de l'arborescence peut échouer et renvoyer l'erreur -632. Pour résoudre ce problème, procédez comme suit :<br><br>1. Après avoir installé le paquetage SLP, veillez à démarrer manuellement SLP comme suit :<br>`/etc/init.d/slpuasa start`<br>2. Après avoir désinstallé le paquetage SLP, veillez à arrêter manuellement SLP comme suit :<br>`/etc/init.d/slpuasa stop` |

| Problèmes connus | Actions suggérées |
| --- | --- |
| L'ajout d'un serveur secondaire activé pour l'authentification EBA à un serveur non activé pour EBA entraîne un échec de la configuration | Pour résoudre ce problème, commencez par configurer le serveur secondaire sans les paramètres EBA, puis procédez à la mise à niveau vers l'authentification EBA à l'aide des paramètres de configuration EBA. |
| Exclusion du répertoire DIB des processus de sauvegarde ou antivirus<br><br>Après avoir installé eDirectory, vous devez configurer votre environnement pour exclure le répertoire DIB stocké sur votre serveur eDirectory de tous les processus antivirus ou de sauvegarde. Si vous n'excluez pas le répertoire DIB des processus de ce type, les fichiers DIB risquent d'être endommagés ou vous pouvez rencontrer des erreurs d'incohérence de base de données `-618 FFFFFD96 INCONSISTENT DATABASE`. | Utilisez l'outil de sauvegarde eDirectory pour sauvegarder votre répertoire DIB. Pour plus d'informations sur la sauvegarde d'eDirectory, reportez-vous à la section Backing Up and Removing Roll-Forward Logs (Sauvegarde et suppression des journaux de transactions individuelles) du NetIQ Certificate Server Administration Guide (Guide d'administration du serveur de certificats NetIQ). |
| Le certificat IP AG n'est pas créé sur la plate-forme SLES 11 64 bits | Envisagez un scénario où les interfaces IPv4 et IPv6 sont configurées sur eDirectory 9.0 , mais où une seule (IPv4 par exemple) dispose d'une entrée dans le fichier `/etc/hosts`, l'autre interface étant accessible à partir d'une machine distante. Si vous configurez eDirectory pour écouter les deux adresses IP, le certificat IP AG est généré uniquement pour l'adresse IP répertoriée dans le fichier `/etc/hosts`. Dans cet exemple, il est généré pour IPv4 |
| Chemin d'accès d'instance par défaut pour plusieurs instances.<br><br>Lorsque vous configurez la deuxième instance de eDirectory sur votre hôte, vous êtes invité à utiliser le chemin par défaut. | Sélectionnez un chemin différent et poursuivez. |

# Résolution des problèmes liés à plusieurs instances d'eDirectory

Le tableau suivant répertorie les problèmes que vous risquez de rencontrer et les actions suggérées pour les résoudre. Si le problème persiste, contactez votre représentant NetIQ.

| Problèmes connus | Actions suggérées |
|---|---|
| Si la première instance est inactive, HTTP ne fonctionne pas<br><br>Sur les plates-formes Linux, si eDirectory est configuré sur du matériel équipé de plusieurs cartes d'interface réseau et si HTTP est relié à plusieurs interfaces, la mise à l'arrêt de la première interface bloque l'accès HTTP aux autres interfaces.<br><br>En effet, dans ce cas, les autres interfaces redirigent la requête vers la première, laquelle est inactive. | Pour résoudre ce problème, si la première interface est désactivée, redémarrez eDirectory. |
| ndsd se connecte au port par défaut si l'interface indiquée est incorrecte | Lorsque vous utilisez la commande `ndsconfig new` ou `ndsmanage` pour créer une deuxième instance de l'annuaire, nds essaie d'utiliser l'interface par défaut si l'interface spécifiée est incorrecte. Si vous spécifiez un port différent du port par défaut (1524 par exemple), l'interface spécifiée est incorrecte ; la commande utilise alors l'interface par défaut et le port par défaut 524.<br><br>Pour `n4u.server.interfaces`, si l'interface spécifiée est incorrecte, `ndsd` tente d'écouter sur la première interface et le numéro de port est celui indiqué dans `n4u.server.tcp-port`. |
| Recréation du répertoire .edir | Le répertoire `.edir` est utilisé pour effectuer le suivi de plusieurs instances de eDirectory. Pour recréer le fichier d'instances perdues on endommagées (fichier `instances.$uid`, où `$uid` spécifie l'ID de l'utilisateur dans le système), vous devez créer le fichier de ses différentes instances.<br><br>Ces fichiers doivent contenir l'emplacement absolu des fichiers `nds.conf` de toutes les instances configurées par l'utilisateur. Par exemple, un utilisateur dont l'`uid` est égal à 1000 doit créer un fichier d'instances `/etc/opt/novell/eDirectory/conf/.edir/instances.1000` avec les entrées suivantes :<br><br>`/home/user1/instance1/nds.conf`<br><br>`/home/user1/instance2/nds.conf` |

# Utilitaire ndsconfig

Le tableau suivant répertorie les problèmes que vous risquez de rencontrer et les actions suggérées pour les résoudre. Si le problème persiste, contactez votre représentant NetIQ.

| Problèmes connus | Actions suggérées |
|---|---|
| Configuration de ndsconfig pour une exécution à partir d'un emplacement différent de l'emplacement par défaut | Si vous recevez une erreur lorsque vous exécutez l'utilitaire ndsconfig à partir d'un emplacement différent du répertoire par défaut `/opt/novell/eDirectory/bin`, veillez à exporter la commande ndspath avant d'exécuter ndsconfig. Utilisez la commande suivante :<br>`source /opt/novell/eDirectory/bin/ndspath`<br>Après avoir exporté la commande, entrez `ndsconfig` pour exécuter l'utilitaire ndsconfig au lieu de `./ndsconfig`. |
| ndsconfig ne vérifie pas convenablement la validité du chemin d'accès au fichier de configuration | Pour créer le fichier de configuration nécessaire, ndsconfig a besoin du chemin d'accès complet et du nom du fichier de configuration. Lorsque le même nom de chemin d'accès est transmis pour le fichier de configuration et le répertoire d'instance, ndsconfig ne peut pas créer le fichier de configuration et abandonne l'opération. |
| ndsconfig get affiche des caractères indésirables à la place des caractères non anglais | La commande `ndsconfig get` génère des caractères indésirables sous Linux pour certains paramètres contenant des caractères d'une autre langue que l'anglais.<br>Pour éviter ce problème, saisissez le nom du paramètre à obtenir comme suit :<br>`ndsconfig get <paramètre_à_afficher>`<br>Pour une liste des paramètres, consultez la page du manuel `nds.conf`. |

# Résolution des problèmes d'installation de NMAS

- Si vous désinstallez le client Novell, vous devez désinstaller et réinstaller le client NMAS s'il est utilisé par une autre application.
- NMAS doit être installé sur un serveur qui contient une réplique inscriptible de l'objet Utilisateur pour que l'utilisateur puisse utiliser NMAS.
- Le client NICI (Novell International Cryptographic Infrastructure) doit être installé sur chaque poste de travail client qui exécute le logiciel NMAS.
- Si vous ne redémarrez pas le serveur après l'installation de NMAS et tentez de réinitialiser les mots de passe, un message d'erreur s'affiche.
- Veillez à maintenir la méthode de connexion à jour. Il se peut que les installations eDirectory sous OES/Linux ne fournissent aucun moyen pour mettre à niveau la méthode.

# Dépannage durant l'installation du serveur de certificats

## Conflit des données de fichier lors de l'installation

Si un message indique que l'installation précédente contient un fichier plus récent, vous devez choisir de toujours écraser le fichier plus récent.

## Liste non exhaustive des serveurs

La liste des serveurs affichée au cours de l'installation ne peut pas répertorier les serveurs qui sont uniquement configurés pour utiliser IP. Vous pouvez installer le serveur de certificats NetIQ sur un serveur non répertorié lorsque vous entrez son nom dans la zone de texte.

## Échecs pendant l'installation

Si l'installation échoue lors de la création de l'autorité de certification organisationnelle ou du certificat de serveur, ou lors de l'exportation du certificat de racine approuvée, il est inutile de recommencer l'installation. L'installation du logiciel a réussi à ce stade. Vous pouvez utiliser iManager pour créer une autorité de certification organisationnelle et des certificats de serveur et exporter la racine approuvée.

## Le plug-in PKI rencontre une erreur lorsqu'il est installé sur iManager 2.7.6 Patch1 et versions antérieures

Pour résoudre ce problème, créez un lien symbolique libntls.so.8 pointant vers libntls.so comme suit :

```
ln -sf /var/opt/novell/iManager/nps/WEB-INF/bin/linux/libntls.so
```

```
/var/opt/novell/iManager/nps/WEB-INF/bin/linux/libntls.so.8
```

## Le certificat IP généré automatiquement n'est pas créé sur la plate-forme SLES 11 64 bits

Envisagez un scénario où les interfaces IPv4 et IPv6 sont configurées sur eDirectory 9.0 , mais où une seule (IPv4 par exemple) dispose d'une entrée dans le fichier /etc/hosts, l'autre interface étant accessible à partir d'une machine distante. Si vous configurez eDirectory pour écouter les deux adresses IP, le certificat IP AG est généré uniquement pour l'adresse IP répertoriée dans le fichier /etc/hosts. Dans cet exemple, il est généré pour IPv4.

## Le certificat IPv6 généré automatiquement n'est pas créé lorsque la longueur du nom RDN de l'objet Certificat dépasse la limite maximale

Lors de l'installation d'eDirectory 9.0, qui écoute sur les adresses IPv4 et IPv6, le certificat IP AG < IPv6 > (KMO) n'est pas créé.

Cela se produit lorsque la longueur du nom RDN de l'objet Certificat dépasse la limite maximale de 64 caractères. Pour résoudre ce problème, un format compressé d'adresse IPv6 est utilisé afin que même si la longueur dépasse la limite maximale, l'adresse soit raccourcie pour répondre à la requête. L'adresse est raccourcie à partir du troisième signe deux-points (à partir de la fin) de l'adresse.

Par exemple, si l'adresse IPv6 est 2508:f0g0:1003:0061:0000:0000:0000:0002, l'adresse tronquée est la suivante : 0000:0000:0002. De cette manière, l'hôte est identifiable même si l'adresse est tronquée.

### Le serveur HTTP s'associe avec le certificat IP AG lors de la recréation des certificats de serveur par défaut pour un serveur n'hébergeant aucun autorité de certification

Utilisez iManager pour modifier manuellement l'association par défaut.

Connectez-vous à iManager > Modifier > Sélectionnez l'objet Serveur http > Sélectionnez l'attribut httpKeyMaterialObject, puis modifiez l'association de l'objet Serveur HTTP sur SSL CertificateDNS.