opentext™

# OpenText™ eDirectory CE 24.4 (v9.3)

## Guide d'installation

**Janvier 2025**

## Mentions légales

**Copyright 2009 - 2024 Open Text Tous droits réservés.**

Les seules garanties pour les produits et services d'Open Text et de ses filiales et concédants de licence (« Open Text ») sont énoncées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucun élément du présent document ne doit être interprété comme constituant une garantie supplémentaire. Open Text ne pourra pas être tenu responsable des erreurs techniques ou éditoriales ou des omissions contenues dans le présent document. Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.

# Table des matières


**À propos de ce guide et de la bibliothèque 9**

**1 Migration d'OpenText eDirectory vers 24.4 (v9.3) 11**

Conditions préalables à la migration d'OpenText eDirectory . . . . . 11
Modifications importantes dans OpenText eDirectory après l'adoption d'OpenSSL 3.0 . . . . . 12
Migration d'OpenText eDirectory vers la version 9.3 . . . . . 14

**2 Fonctionnalités relatives à l'installation et à la mise à niveau 15**

Formats de paquetage multiples pour l'installation d'OpenText eDirectory 9.3 . . . . . 16
Installation d'OpenText eDirectory 9.3 dans un emplacement personnalisé. . . . . 17
Indication d'un emplacement personnalisé pour les fichiers d'application . . . . . 17
Indication d'un emplacement personnalisé pour les fichiers de données . . . . . 17
Indication d'un emplacement personnalisé pour les fichiers de configuration . . . . . 18
Installation non-root . . . . . 19
Conformité aux normes . . . . . 19
Conformité FHS . . . . . 19
Conformité LSB . . . . . 20
Vérifications de l'état de santé du serveur . . . . . 21
Avantage des vérifications de l'état de santé . . . . . 21
État de santé d'un serveur . . . . . 21
Vérifications de l'état de santé . . . . . 21
Types de vérifications de l'état de santé . . . . . 22
Catégorisation de l'état de santé . . . . . 23
Fichiers journaux . . . . . 24
Installation du correctif de pont sur le serveur avec EBA . . . . . 25
Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA sous Linux. . . . . 25
Installation d'un correctif de pont sur plusieurs serveurs de répliques avec EBA sous Windows. . . . . 26
Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA dans le conteneur . . . . . 27
Pour plus d'informations . . . . . 28

**3 Installation ou mise à niveau d'OpenText eDirectory CE 24.4 (v9.3) sous Linux 29**

Configuration système requise . . . . . 29
Conditions préalables . . . . . 31
Configuration matérielle requise . . . . . 35
Exécution forcée du processus de liaison en amont . . . . . 36
Ajout du groupe d'utilisateurs edirAdmin. . . . . 36
Mise à niveau d'OpenText eDirectory . . . . . 37
Vérifications de l'état de santé du serveur . . . . . 38
Mettre à niveau sur des serveurs Linux autres qu'OES. . . . . 38
Mise à niveau sans surveillance d'OpenText eDirectory sous Linux . . . . . 39
Mise à niveau du déploiement du tarball d'eDirectory 9.3 . . . . . 40
Mise à niveau d'OpenText eDirectory 9.3 par des utilisateurs non-root. . . . . 42

Mise à niveau de plusieurs instances . . . . . 42
Installation d'OpenText eDirectory . . . . . 43
Utilisation de SLP avec OpenText eDirectory . . . . . 44
Exécution de l'utilitaire nds-install pour installer des composants OpenText eDirectory . . . . . 45
Installation d'OpenText eDirectory 9.3 par un utilisateur non-root . . . . . 48
Configuration d'OpenText eDirectory par un utilisateur non-root à l'aide de l'installation root . . . . . 52
Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques OpenText eDirectory . . . . . 54
Utilisation de ndsconfig pour configurer plusieurs instances d'OpenText eDirectory 9.3 . . . . . 61
Utilisation de ndsconfig pour installer un serveur Linux dans une arborescence dont les noms de conteneur utilisent des points . . . . . 68
Exécution de l'utilitaire nmasinst pour configurer NMAS . . . . . 69
Configuration de SNMP par un utilisateur non-root . . . . . 70
Localisation des fichiers journaux . . . . . 70

**4 Installation ou mise à niveau d'OpenText eDirectory CE 24.4 (v9.3) sous Windows 73**

Configuration système requise . . . . . 73
Conditions préalables . . . . . 74
Configuration matérielle requise . . . . . 77
Exécution forcée du processus de liaison en amont . . . . . 77
Installation d'OpenText eDirectory sous Windows . . . . . 78
Installation ou mise à niveau d'OpenText eDirectory 9.3 sur un serveur Windows . . . . . 78
Vérifications de l'état de santé du serveur . . . . . 80
Communication avec OpenText eDirectory via LDAP . . . . . 81
Installation du logiciel NMAS Server . . . . . 82
Installation dans une arborescence comportant des conteneurs dont le nom utilise la notation à point . . . . . 82
Installation et configuration sans surveillance d'OpenText eDirectory 9.3 sous Windows . . . . . 83
Localisation des fichiers journaux . . . . . 90
Mise à niveau d'OpenText eDirectory sous Windows . . . . . 91
Extension de schéma NMAS avant la mise à niveau d'OpenText eDirectory . . . . . 91
Mise à niveau d'OpenText eDirectory à l'aide de Windows Installer . . . . . 92
Mise à niveau sans surveillance d'OpenText eDirectory sous Windows . . . . . 93

**5 Déploiement d'OpenText eDirectory dans Microsoft Azure 95**

Conditions préalables . . . . . 95
Procédure de déploiement . . . . . 95
Déploiement sur une plate-forme Linux . . . . . 95
Déploiement sur une plate-forme Windows . . . . . 110
Déploiement d'un conteneur OpenText eDirectory sur une instance de conteneur Microsoft Azure . . . . . 119
Liste de contrôle pour le déploiement du conteneur . . . . . 119

**6 Déploiement d'OpenText eDirectory sur Amazon Web Services EC2 127**

Conditions préalables . . . . . 127
Procédure de déploiement . . . . . 127
Préparation du cloud privé virtuel AWS . . . . . 129
Configuration des ACL réseau . . . . . 130
Configuration des groupes de sécurité . . . . . 132
Création d'une paire de clés SSH . . . . . 133

Création et déploiement d'instances . . . . . 134
Configuration d'un volume EBS pour le stockage des données OpenText eDirectory . . . . . 134
Installation d'OpenText eDirectory et d'OpenText Identity Console . . . . . 135
Déploiement des services d'audit . . . . . 139
Reprise après sinistre . . . . . 140
Guide de taille pour le déploiement d'OpenText eDirectory sur AWS . . . . . 141
Commencer avec la sélection d'instance AWS EC2 . . . . . 141
Détails des environnements de test des performances . . . . . 142
Détermination des exigences de taille . . . . . 144

**7 Déploiement d'OpenText eDirectory à l'aide d'un conteneur Docker 153**

Présentation de Docker . . . . . 153
Planification du déploiement d'OpenText eDirectory à l'aide d'un conteneur Docker . . . . . 153
Configuration système requise . . . . . 154
Conditions préalables . . . . . 154
Interface de ligne de commande (CLI) de Docker . . . . . 154
Déploiement d'un conteneur OpenText eDirectory . . . . . 154
Déploiement d'un conteneur OpenText eDirectory dans un réseau hôte . . . . . 157
Déploiement d'un conteneur OpenText eDirectory dans un réseau superposé défini par l'utilisateur . . . . . 159
Tâches de post-configuration . . . . . 161
Exécution de commandes sur un conteneur OpenText eDirectory en cours d'exécution . . . . . 161
Configuration d'OpenSLP pour le conteneur Docker pour OpenText eDirectory . . . . . 162
Installation des méthodes NMAS dans un conteneur Docker pour OpenText eDirectory . . . . . 163
Installation de nouveaux paquetages dans un conteneur Docker pour OpenText eDirectory . . . . 163
Configuration du fichier de propriétés CEF dans un conteneur Docker pour OpenText eDirectory . . . . . 164
Gestion du stockage des données OpenText eDirectory . . . . . 164
Mise à niveau d'OpenText eDirectory à l'aide d'un conteneur Docker . . . . . 165
Récupération d'un conteneur Docker pour OpenText eDirectory . . . . . 166

**8 Installation d'OpenText eDirectory sous Linux et Windows avec des adresses IPv6 167**

Configuration d'OpenText eDirectory sur Linux avec IPv6 . . . . . 168
Création d'une nouvelle arborescence OpenText eDirectory . . . . . 168
Ajout d’un serveur à une arborescence OpenText eDirectory existante . . . . . 168
Activation d’adresses IPv6 sur des serveurs OpenText eDirectory existants ou mis à niveau . . . . . 168
Ajout d'URL LDAP pour IPV6 sur l'objet Serveur LDAP . . . . . 169
Installation ou mise à niveau d’OpenText eDirectory sous Windows avec IPv6 . . . . . 169
Activation d’IPv6 lors de l’installation ou de la mise à niveau d'OpenText eDirectory . . . . . 170
Activation de IPv6 pour les serveurs existants . . . . . 170
Accès à OpenText iMonitor . . . . . 170

**9 Fonctionnement d'OpenText eDirectory en mode FIPS 171**

Configuration d'OpenText eDirectory en mode FIPS . . . . . 171

**10 Déplacement de la DIB 173**

Linux . . . . . 173
Windows . . . . . 174

**11 Conditions requises pour la mise à niveau d'OpenText eDirectory 9.3 175**

Changements de référence dans 8.8 SP1 ou versions ultérieures . . . . . 175
Procédure de mise à niveau dans la version 9.3 . . . . . 176

**12 Configuration d'OpenText eDirectory sous Linux 177**

Utilitaires de configuration . . . . . 177
Utilitaire ndsconfig . . . . . 177
Utilisation des outils LDAP pour configurer les objets Serveur LDAP et Groupe LDAP . . . . . 178
Utilisation de l'utilitaire nmasinst pour configurer le service NMAS (NetIQ Modular Authentication Service) . . . . . 178
Personnalisation d'OpenText eDirectory . . . . . 178
Paramètre de configuration . . . . . 180
Considérations relatives à la sécurité . . . . . 186

**13 Déploiement d'OpenText eDirectory sur les grappes haute disponibilité 187**

Mise en grappe des services OpenText eDirectory sur Linux . . . . . 188
Conditions préalables . . . . . 188
Installation et configuration d'OpenText eDirectory . . . . . 188
Configuration du serveur SNMP dans des environnements Linux en grappe . . . . . 191
Mise en grappe des services OpenText eDirectory sur Windows . . . . . 191
Conditions préalables . . . . . 191
Installation et configuration d'OpenText eDirectory . . . . . 192
Configuration du serveur SNMP dans des environnements Windows en grappe . . . . . 194
Dépannage des environnements en grappe . . . . . 194
Réparation ou mise à niveau d'OpenText eDirectory sur des noeuds en grappe . . . . . 194
Création de clés de registre Windows . . . . . 194
Options de l'utilitaire de configuration . . . . . 195

**14 Désinstallation d'OpenText eDirectory 197**

Désinstallation d'OpenText OpenText eDirectory sous Windows . . . . . 197
Désinstallation d'OpenText eDirectory, ConsoleOne et de l'agent Annuaire SLP . . . . . 197
Désinstallation sans surveillance d'OpenText eDirectory . . . . . 198
Désinstallation de NICI . . . . . 201
Désinstallation des bibliothèques d'exécution Microsoft Visual C++ 2005 et Visual C++ 2012 . . . 202
Désinstallation d'OpenText eDirectory sous Linux . . . . . 202
Désinstallation sans surveillance d'OpenText eDirectory sous Linux . . . . . 203
Avertissements concernant la désinstallation d'OpenText eDirectory . . . . . 204

**A Paquetages Linux pour OpenText eDirectory 205**

**B Vérifications de l'état de santé d'OpenText eDirectory 209**

Avantage des vérifications de l'état de santé . . . . . 209
Vérifications de l'état de santé . . . . . 209
Avec la mise à niveau . . . . . 209
Avec un utilitaire autonome . . . . . 210
Types de vérifications de l'état de santé . . . . . 210
État de santé général du serveur . . . . . 211
État de santé des partitions et répliques . . . . . 211

Catégorisation de l'état de santé . . . . . 211
Normal . . . . . 211
Avertissement . . . . . 211
Critique . . . . . 212
Fichiers journaux . . . . . 212

**C Configuration de OpenSLP pour OpenText eDirectory 215**

Protocole SLP . . . . . 215
Concepts fondamentaux de SLP . . . . . 215
Protocole SLP OpenText . . . . . 216
Agents Utilisateur . . . . . 217
Agents Service . . . . . 217
Paramètres de configuration . . . . . 218

**D Résolution des problèmes 221**

Résolution des problèmes d'installation . . . . . 221
Résolution des problèmes de configuration . . . . . 223
Résolution des problèmes liés à plusieurs instances d'OpenText eDirectory . . . . . 225
Utilitaire ndsconfig . . . . . 226
Résolution des problèmes d'installation de NMAS . . . . . 227
Dépannage durant l'installation du serveur de certificats . . . . . 227
Résolution des problèmes d'installation . . . . . 229

# À propos de ce guide et de la bibliothèque

Le *guide d'installation* explique comment installer OpenText™ eDirectory 9.3. Il est destiné aux administrateurs réseau.

Pour obtenir la dernière version du *guide d'installation d'OpenText eDirectory CE 24.4 (v9.3)*, consultez le site Web de documentation en ligne d'OpenText™ eDirectory (https://www.netiq.com/documentation/edirectory-93/).

## 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 OpenText eDirectory.

**Guide d'optimisation pour les plates-formes Linux)**

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

Ces guides sont disponibles sur OpenText™ eDirectory CE 24.4 (v9.3) (https://www.netiq.com/documentation/edirectory-93/).

Pour plus d'informations sur l'utilitaire de gestion OpenText eDirectory, consultez le guide d'administration d'OpenText™ Identity Console.

# 1 Migration d'OpenText eDirectory vers 24.4 (v9.3)

OpenText eDirectory 9.3 prend en charge OpenSSL 3.0. Vous devez suivre les étapes de migration pour transférer votre configuration OpenText eDirectory existante vers la version 9.3. Cette section décrit les étapes à suivre pour migrer OpenText eDirectory de la version 9.2 vers la 9.3.


- « Conditions préalables à la migration d'OpenText eDirectory » page 11
- « Modifications importantes dans OpenText eDirectory après l'adoption d'OpenSSL 3.0 » page 12
- « Migration d'OpenText eDirectory vers la version 9.3 » page 14


## Conditions préalables à la migration d'OpenText eDirectory

Avant de commencer la migration, veillez à procéder comme suit :

- ❒ **Sauvegarde:** effectuez une sauvegarde complète de votre instance d'OpenText eDirectory, y compris les fichiers de configuration et les données.
- ❒ **Compatibilité système** : OpenSSL 3.0 n'est pris en charge que sous SLES 15 SP3, SP4, SP5 et SP6 et RHEL 8.8, 8.9 et 8.10 et RHEL 9.2, 9.3 et 9.4. Assurez-vous que votre plate-forme répond à cette exigence.
- ❒ **Application de correctifs** : appliquez les derniers correctifs à votre installation OpenText eDirectory existante vers la version 9.2 ou une version ultérieure.
- ❒ **Correctif de pont** : si vous avez un environnement multiserveur et si EBA est activé sur l'un des serveurs ou sur leur ensemble, avant d'effectuer la mise à niveau vers OpenText eDirectory 9.3.0, **il est obligatoire de mettre à niveau tous les serveurs OpenText eDirectory vers les dernières versions 9.2.8 ou 9.2.9 d'OpenText eDirectory**. Une fois la mise à niveau effectuée, l'utilisateur doit appliquer le correctif de pont EBA à tous les serveurs de répliques sur lequel EBA est activé. Le correctif de pont EBA est disponible avec le build d'OpenText eDirectory dans les chemins suivants :
  - **Pour Linux :**

    ```
    <Untarred_edirectory_location>/eDirectory/eba_bridge_patch
    ```

  - **Pour Windows :**

    ```
    <extracted_patch>eDirectory\eba_bridge_patch
    ```

  - **Pour le conteneur :**

    ```
    <Untarred_edirectory_location>/eDirectory_930/eba_bridge_patch
    ```

  Exécutez la commande suivante pour vérifier si EBA est activé dans le système.

```
ndscheck -a  <admin_credentials> -w <tree_login_password>
```

Pour plus d'informations, reportez-vous aux sections « Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA sous Linux » page 25, « Installation d'un correctif de pont sur plusieurs serveurs de répliques avec EBA sous Windows » page 26 et « Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA dans le conteneur » page 27.

- **Compatibilité Same Box** : si une ancienne version d'Identity Console est installée sur le même système qu'OpenText eDirectory, mettez à niveau Identity Console vers la version 1.9 ou ultérieure. Au cours de la mise à niveau, l'installation d'OpenText eDirectory se terminera si une ancienne version d'Identity Console est détectée sur la même machine.

---

**REMARQUE**

- Au cours de l'installation, le programme d'installation d'OpenText eDirectory recherche le correctif de pont appliqué à tous les serveurs de répliques EBA et met fin à l'installation si le correctif n'est appliqué à aucune réplique. La vérification de la présence d'EBA ne fonctionne pas sur l'utilisateur et le conteneur non-root.
- À partir d'OpenText eDirectory 9.3.0 et des versions ultérieures, s'il s'agit du serveur maître 9.3.0, l'ajout de versions antérieures d'OpenText eDirectory en tant que réplique n'est pas pris en charge, avec ou sans EBA.
- Si OpenText eDirectory 9.2.9 ou 9.2.8 coexiste avec OpenText Identity Console 1.8, il est recommandé de mettre à niveau OpenText Identity Console vers la version 1.9 avant de mettre à niveau OpenText eDirectory vers 9.3 sous Linux.

---

# Modifications importantes dans OpenText eDirectory après l'adoption d'OpenSSL 3.0

Vous devez comprendre les changements importants suivants avant de commencer la migration.

## Protocoles TLS et méthodes de chiffrement

- Le produit prend désormais en charge TLS 1.3 avec TLS 1.2.
- Les méthodes de chiffrement ont été mises à jour pour s'aligner sur OpenSSL 3.0 et incluent les méthodes de chiffrement TLS 1.3 suivantes :
  - TLS_AES_256_GCM_SHA384.
  - TLS_CHACHA20_POLY1305_SHA256 (non-FIPS uniquement).
  - TLS_AES_128_GCM_SHA256.
- Les chiffrements TLS 1.2 continuent avec une combinaison d'options de chiffrement AES et RSA.

---

**IMPORTANT :** Configurez les environnements qui nécessitent TLS 1.3 en conséquence. Veillez à retirer ou à mettre à jour les méthodes de chiffrement obsolètes ou dépassées.

---

### Paramètres FIPS et NICI

- Dans OpenText eDirectory 9.3, le mode FIPS est désactivé par défaut. Toutefois, vous pouvez l'activer en fonction de la configuration NICI (Novell International Cryptographic Infrastructure). Cela s'applique aux normes FIPS TLS et FIPS NICI. Dans la version précédente du produit, TLS FIPS est activé par défaut.
- Le fichier de configuration NICI, `nici64.cfg`, devient le point de référence pour activer TLS FIPS et NICI FIPS. Pour plus d'informations, voir Fonctionnement d'eDirectory en mode FIPS (https://www.netiq.com/documentation/edirectory-93/edir_install/data/b1gnsxb4.html).

---

**IMPORTANT :** Pour les systèmes nécessitant la conformité FIPS, examinez les configurations NICI. Si vous effectuez une mise à niveau à partir de la version 9.2, attendez-vous à des comportements par défaut différents dans les paramètres TLS-FIPS.

---

### Certificat RSA et algorithmes de chiffrement

OpenText eDirectory 9.3 ne prend plus en charge les données suivantes :

- Certificats RSA avec des tailles de clé de 512, 768 ou 1 024 bits en mode FIPS.
- Certificats SHA-1 en mode FIPS dans OpenText eDirectory 9.3. Toutefois, ces paramètres sont pris en charge dans les configurations non-FIPS.
- DES et RC2-40 dans les environnements FIPS ou non-FIPS. Toutefois, 3DES reste pris en charge en mode FIPS.

---

**IMPORTANT :** Vérifiez et mettez à jour les certificats et les configurations de chiffrement, en particulier si des certificats DE petite taille ou SHA-1 sont utilisés.

---

### Comportement de la clé d'arborescence NICI

Une nouvelle installation d'OpenText eDirectory 9.3 crée automatiquement une clé d'arborescence AES 256 bits (CN=W1.CN=KAP.CN=Security). Toutefois, lors de la mise à niveau à partir d'anciennes versions d'OpenText eDirectory, la clé d'arborescence existante reste inchangée et continue de fonctionner comme prévu. Pour plus d'informations sur les clés NICI, voir Description des clés NICI (https://www.netiq.com/documentation/edirectory-9/nici_admin_guide/data/agtbw4b.html)

### Compatibilité avec les versions précédentes et intégrations

OpenText eDirectory 9.3 ne prend en charge que les versions suivantes de ces produits. Effectuez une mise à niveau si vous utilisez des versions antérieures.

- OpenText Identity Console 24.4 (v1.9)
- OpenText Identity Manager 24.4 (v4.10)

---

**IMPORTANT :** Vérifiez que les intégrations avec ces produits sont compatibles avec les versions avant la mise à niveau. Les versions antérieures peuvent provoquer des échecs d'installation ou des problèmes de communication.

---

# Migration d'OpenText eDirectory vers la version 9.3

Mettez à niveau les composants associés à la migration du produit vers la version 9.3.

1 Compatibilité avec OpenText Identity Console :

OpenText eDirectory 9.3 ne prend en charge que les versions suivantes d'OpenText Identity Console et d'OpenText Identity Manager :

- OpenText Identity Console 24.4 (v1.9)
- OpenText Identity Manager 24.4 (v4.10)

Si des versions non prises en charge de ces produits sont installées, mettez-les à niveau vers les versions prises en charge.

2 Gestion des méthodes NMAS après la mise à niveau

OpenText eDirectory 9.3.0 intègre les méthodes NMAS à la dernière version de NICI, conçue sur OpenSSL 3.0.15.

- **Environnement à serveur unique :**

  **Aucune action n'est nécessaire :** si vous avez une seule instance d'OpenText eDirectory 9.3.0 avec les méthodes NMAS, aucune étape supplémentaire n'est requise dans Linux. Pour Windows, il est nécessaire d'étendre le schéma NMAS. Pour plus d'informations, reportez-vous à la section « Extension de schéma NMAS avant la mise à niveau d'OpenText eDirectory » page 91.

- **Environnement à serveurs multiples** : si vous avez des serveurs de configuration à serveurs multiples avec des versions mixtes, l'ajout d'une nouvelle méthode NMAS à OpenText eDirectory 9.3.0 n'est pas impacté. Toutefois, si la réplique utilise une version d'OpenText eDirectory inférieure ou égale à la version 9.2.9, ajoutez la méthode NMAS dans OpenText eDirectory 9.2.9, puis à 9.3.0.

---

**REMARQUE :**

- **Aucune étape manuelle n'est nécessaire :** une fois tous les serveurs mis à niveau vers OpenText eDirectory 9.3.0, l'ajout manuel de méthodes NMAS ne sera plus nécessaire.
- Pour plus d'informations sur les méthodes NMAS, consultez le guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3) (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/a53vifw.html).

---

# 2 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 d'OpenText eDirectory CE 24.4 (v9.3).

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'OpenText eDirectory 9.3 | ✓ | ✗ |
| 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 d'OpenText eDirectory Instrumentation | ✓ | ✓ |

**REMARQUE**

- À partir d'OpenText eDirectory CE 24.4 (v9.3)9.2.3, la clé d'arborescence AES 256 bits est activée par défaut. Cependant, si nous effectuons une mise à niveau à partir de la version 9.2.x, vous devez ajouter l'objet W1.KAP.Security manuellement après la mise à niveau d'OpenText eDirecotry.
- Dans la configuration avec EBA activé, assurez-vous que tous les serveurs de répliques sont sur eDirectory 9.2.8 ou 9.2.9 si vous effectuez la mise à niveau de l'un de vos serveurs vers OpenText eDirectory CE 24.4 (v9.3) avec EBA. Avant de mettre à niveau la réplique vers la version 9.3.0, appliquez le correctif de pont. Le correctif de pont ne peut pas être appliqué sur OpenText eDirectory 9.2.7 et les versions antérieures.

Ce chapitre comprend les informations suivantes :


- « Formats de paquetage multiples pour l'installation d'OpenText eDirectory 9.3 » page 16
- « Installation d'OpenText eDirectory 9.3 dans un emplacement personnalisé » page 17
- « Installation non-root » page 19
- « Conformité aux normes » page 19
- « Vérifications de l'état de santé du serveur » page 21
- « Installation du correctif de pont sur le serveur avec EBA » page 25
- « Pour plus d'informations » page 28


# Formats de paquetage multiples pour l'installation d'OpenText eDirectory 9.3

Sous Linux, vous avez la possibilité de choisir entre plusieurs formats de fichier pendant l'installation d'OpenText eDirectory 9.3 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 section « Mise à niveau du déploiement du tarball d'eDirectory 9.3 » page 40.

# Installation d'OpenText eDirectory 9.3 dans un emplacement personnalisé

Avec OpenText eDirectory 9.3, 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 OpenText eDirectory 9.3 dans un emplacement personnalisé si une version antérieure d'OpenText eDirectory est déjà installée sur votre hôte et que vous souhaitez tester OpenText eDirectory 9.3 avant d'effectuer la mise à niveau vers cette version. De cette manière, vous ne modifiez pas votre configuration OpenText 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 OpenText eDirectory 9.3.

---

**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 17
- « Indication d'un emplacement personnalisé pour les fichiers de données » page 17
- « Indication d'un emplacement personnalisé pour les fichiers de configuration » page 18


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

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

### Linux

Pour installer OpenText eDirectory 9.3 dans un emplacement personnalisé, vous pouvez utiliser le fichier d'installation tarball et décompresser OpenText eDirectory 9.3 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 OpenText eDirectory version 9.3.

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

Pendant la configuration d'OpenText 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 OpenText eDirectory) dans le chemin mentionné. |
| -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 d'OpenText 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

OpenText eDirectory 9.1 et versions ultérieures prennent en charge l'installation et la configuration de serveurs OpenText eDirectory par un utilisateur non-root. Les versions antérieures d'OpenText eDirectory ne pouvaient être installées et configurées que par un utilisateur root, avec une seule instance d'OpenText eDirectory qui s'exécutait sur un hôte.

À partir d'OpenText eDirectory 9.3, tout utilisateur non-root peut désormais utiliser une version Tarball pour installer OpenText eDirectory. Plusieurs installations binaires OpenText 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 d'OpenText 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 OpenText eDirectory à l'aide de sa propre installation Tarball ou à l'aide d'une installation binaire. Cela signifie que plusieurs instances de serveurs OpenText eDirectory peuvent s'exécuter sur un même hôte, car tout utilisateur, root ou non root, peut configurer différentes instances de serveur OpenText 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 section « Mise à niveau de plusieurs instances » page 42.

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 section « Installation d'OpenText eDirectory 9.3 par un utilisateur non-root » page 48.

# Conformité aux normes

OpenText eDirectory 9.3 est conforme aux normes suivantes :


- « Conformité FHS » page 19
- « Conformité LSB » page 20


## Conformité FHS

Pour éviter les conflits avec les fichiers d'application d'autres produits, OpenText eDirectory 9.3 respecte la norme FHS (Filesystem Hierarchy Standard, norme de hiérarchie du système de fichiers). Cette fonction n'est disponible que sur Linux.

OpenText 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 `eDir93`, la même structure de répertoires est utilisée dans ce répertoire `eDir93` ; par conséquent, les pages du manuel seront installées dans le répertoire `/eDir93/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 OpenText eDirectory 9.3, 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

OpenText eDirectory 9.3 est désormais compatible LSB (Linux Standard Base). LSB recommande également la compatibilité FHS. Tous les paquetages OpenText eDirectory sous Linux portent le préfixe *novell*. Par exemple, `NDSserv` s'appelle désormais `novell-NDSserv`.

# Vérifications de l'état de santé du serveur

OpenText eDirectory CE 24.4 (v9.3) 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 d'OpenText eDirectory du *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

## Avantage des vérifications de l'état de santé

Les versions antérieures d'OpenText 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 OpenText 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 21
- « Avec un utilitaire autonome » page 22

---

**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 d'OpenText 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 2-1*** *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 24.

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 23.

### 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 OpenText 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 section « Fichiers journaux » page 24.

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 OpenText.

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

***Tableau 2-2*** *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`* |

# Installation du correctif de pont sur le serveur avec EBA


- « Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA sous Linux » page 25
- « Installation d'un correctif de pont sur plusieurs serveurs de répliques avec EBA sous Windows » page 26
- « Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA dans le conteneur » page 27


## Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA sous Linux

---

**IMPORTANT :** Avant d'effectuer la mise à niveau vers OpenText eDirectory 9.3.0, assurez-vous que tous les serveurs de répliques ou maîtres utilisent la version 9.2.8 ou 9.2.9 d'OpenText eDirectory. Pour mettre à niveau l'un de ces serveurs, installez le correctif de pont EBA fourni avec la version 9.3.0 d'OpenText eDirectory. OpenText eDirectory 9.3.0 ne démarre pas si l'extension de schéma n'est pas appliquée avant le correctif de pont.

---

Lorsqu'OpenText eDirectory 9.3.0 est installé sur un nouveau serveur et ajouté à un anneau de répliques dans lequel le serveur maître est OpenText eDirectory 9.2.8 ou 9.2.9, et qu'EBA est activé, appliquez le correctif de pont EBA aux serveurs OpenText eDirectory 9.2.8 ou 9.2.9 avant d'installer OpenText eDirectory 9.3.0.

- **Pour installer le correctif de pont sous Linux pour un utilisateur root, suivez les étapes ci-dessous**.

1 Téléchargez et désarchivez le build d'OpenText eDirectory, accédez à l'emplacement désarchivé `<emplacement_edirectory_désarchivé>/eDirectory/correctif_pont_eba` et exécutez les étapes suivantes. Après le désarchivage, localisez le fichier `eba_bridge.sch` dans cet emplacement. Élargissez le schéma de correctif de pont à l'aide de la commande ci-dessous.

```
ndssch [-h <hostname>[:<port>]][-t <treename>] <admin-FDN> <schemafile>
```

Par exemple :

```
ndssch  -h 10.10.10.10:524 -t tree1 admin.novell eba_bridge.sch
```

2 Pour appliquer la connexion au correctif de pont en tant qu'utilisateur root, exécutez la commande suivante :

```
rpm -ivh --force novell-eba-9.2.8.0000.x86_64.rpm
```

3 Redémarrez les services ndsd.

- **Pour installer le correctif de pont sous Linux pour un utilisateur non-root, suivez les étapes ci-dessous**.

1 Téléchargez et désarchivez le build d'OpenText eDirectory, accédez à l'emplacement désarchivé <emplacement_edirectory_désarchivé>/eDirectory/correctif_pont_eba et exécutez les étapes suivantes. Après le désarchivage, localisez le fichier eba_bridge.sch dans cet emplacement. Élargissez le schéma de correctif de pont à l'aide de la commande ci-dessous.

```
ndssch [-h <hostname>[:<port>]][-t <treename>] <admin-FDN> <schemafile>
```

Par exemple :

```
ndssch  -h 10.10.10.10:524 -t tree1 admin.novell eba_bridge.sch
```

2 Copiez les fichiers de bibliothèque ci-dessous dans /home/nuser/eDirectory/opt/novell/eDirectory/lib64, où /home/nuser est un chemin spécifique à l'utilisateur.

```
libebacli.so, libebasrv.so, libebassl_cli.so, libebassl_srv.so and libgssapi.so
```

3 Redémarrez les services ndsd.

---

**REMARQUE :** OpenText eDirectory ne démarre pas si l'extension de schéma n'est pas appliquée avant d'appliquer le correctif de pont.

---

## Installation d'un correctif de pont sur plusieurs serveurs de répliques avec EBA sous Windows

Pour installer le correctif de pont sous Windows, procédez comme suit.

1 Dézippez le build d'OpenText eDirectory situé dans <correctif_extrait>eDirectory\correctif_pont_eba

2 Mettez à jour le fichier upgrade.ni présent dans le dossier preUpgrade_930. Indiquez 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=10.10.10.10
Existing Server Port=524
[NWI:SNMP]
Stop service=No
[NWI:NMAS]
Methods=CertMutual,Challenge Response,DIGEST-MD5,NDS,Simple
Password,SAML
```

3 Exécutez la commande ci-dessous à partir de powershell.

```
preUpgrade.ps1 -rfile <path_for_Configuration>/upgrade.ni
```

4 Arrêtez les services OpenText eDirectory avant de copier les DLL `ebacli.dll`, `ebai18n.dll`, `ebaldap.dll`, `ebassl_cli.dll`, `ebasym.dll` depuis `<correctif_extrait>eDirectory\correctif_pont_eba vers C:\NetIQ\eDirectory` (emplacement binaire d'OpenText eDirectory).

5 Démarrez les services `ndsd`.

## Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA dans le conteneur

Pour installer le correctif de pont sur le conteneur, procédez comme suit.

1 Téléchargez et désarchivez le build d'OpenText eDirectory, accédez à l'emplacement désarchivé `<emplacement_edirectory_désarchivé>/eDirectory_930/correctif_pont_eba` et exécutez les étapes suivantes.

2 Après le désarchivage,

**2a** Copiez le fichier `eba_brdge.sch` dans le conteneur et exécutez la commande suivante.

```
docker cp eba_brdge.sch <eDirectory Container name>:/config
```

**2b** Copiez le fichier `novell-eba-9.2.8.0000.x86_64.rpm` dans le conteneur, puis exécutez la commande ci-dessous.

```
docker cp novell-eba-9.2.8.0000.x86_64.rpm <eDirectory Container
name>:/config
```

3 Connectez-vous au conteneur, accédez au répertoire dans lequel vous avez copié le fichier de schéma à l'Étape 2a page 27, puis exécutez la commande ci-dessous.

Extension d'un schéma

```
ndssch [-h <hostname>[:<port>]][-t <treename>] <admin-FDN> <schemafile>
```

Par exemple :

```
ndssch  -h 10.10.10.10:524 -t tree1 admin.novell eba_bridge.sch
```

4 Pour installer le RPM du correctif de pont EBA, exécutez les étapes ci-dessous.

**4a** Connectez-vous au conteneur en tant qu'utilisateur root.

```
docker exec -it -u root <eDirectory Container name> /bin/bash
```

**4b** Accédez au répertoire dans lequel vous avez copié le RPM à l'étape 2b, page 146, et exécutez la commande ci-dessous.

```
rpm -ivh --force novell-eba-9.2.8.0000.x86_64.rpm
```

5 Pour redémarrer les services ndsd, redémarrez le conteneur OpenText eDirectory à l'aide de la commande ci-dessous.

```
docker restart <eDirectory Container name>
```

# Pour plus d'informations

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

- *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*
- Sous Linux : consultez les pages du manuel pour `nds-install` `ndsconfig`et `ndscheck`.

  Exemple : `man nds-install`

# 3 Installation ou mise à niveau d'OpenText eDirectory CE 24.4 (v9.3) sous Linux

Les informations suivantes permettent d'installer ou de mettre à niveau OpenText eDirectory CE 24.4 (v9.3) sur un serveur Linux :


- « Configuration système requise » page 29
- « Conditions préalables » page 31
- « Configuration matérielle requise » page 35
- « Exécution forcée du processus de liaison en amont » page 36
- « Ajout du groupe d'utilisateurs edirAdmin » page 36
- « Mise à niveau d'OpenText eDirectory » page 37
- « Installation d'OpenText eDirectory » page 43


## Configuration système requise

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

- Mémoire
  - 2 Mo d'espace disque pour le serveur OpenText eDirectory
  - 2 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 15 SP3, SP4, SP5 et SP6 | 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 |
|---|---|---|
| RHEL 8.8 et versions ultérieures | 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>**REMARQUE**<br>◆ Vous devez définir SELinux en mode « permissive » (permissif) sur RHEL 8.8 et versions ultérieures. |
| RHEL 9.2 et versions ultérieures | 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>**REMARQUE :**<br>◆ Vous devez définir `SELinux` en mode « permissive » (permissif) sur RHEL 9.2 et versions ultérieures.<br>◆ Si `SELNIUX` est défini sur `ENFORCING` , suivez les étapes présentées dans « Conditions préalables » page 31. |

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`.

Assurez-vous qu'une entrée appropriée pour la machine Linux est disponible dans le fichier `/etc/hosts`.

**REMARQUE :**

- OpenText eDirectory ne prend pas en charge BTRFS (B-tree file system).

## Détermination de la version d'OpenText eDirectory

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

- Exécutez ndsstat.

L'utilitaire ndsstat affiche des informations relatives aux serveurs OpenText eDirectory, par exemple le nom de l'arborescence OpenText eDirectory, le nom distinctif complet du serveur et la version d'OpenText eDirectory. Dans l'exemple ci-dessous, OpenText eDirectory 9.3 est la version du produit (chaîne marketing) et 40201.12 la version binaire (numéro de version interne).

```
osg-dt-srv17:/>ndsstat
Tree Name: EDR93E
Server Name: .CN=Master.O=server.T=EDR93E.
Binary Version: 40301.00
Root Most Entry Depth: 0
Product Version: eDirectory for Linux x86_64 v9.3 [DS]
```

Pour plus d'informations sur l'exécution de ndsstat, reportez-vous à la section « Commandes et syntaxe d'OpenText eDirectory pour Linux » du Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3) 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 d'OpenText eDirectory pour Linux » du Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3) 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 De l'agent pour OpenText™ eDirectory CE 24.4 (v9.3) pourrait être 40301.00.

  Pour plus d'informations sur l'exécution d'iMonitor, voir « Accès à OpenText iMonitor » dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

- 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 OpenText eDirectory existant, vérifiez les applications OpenText et tierces actuellement installées pour déterminer si ces produits sont pris en charge sur OpenText eDirectory 9.3. Les conditions préalables des autres produits OpenText sont disponibles sur le site de documentation OpenText (http://www.netiq.com/documentation/) . Nous vous recommandons également de sauvegarder une instance OpenText 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 8.x et RHEL 9 :** `dnf-utils` et `createrepo`

  Exécutez la procédure suivante pour installer RHEL 8.x RPM

  1. Installez le paquetage `yum-utils`

     yum install `createrepo yum-utils`

  2. Installez les bibliothèques suivantes requises pour OpenText eDirectory.

     yum install libgcc*.i686 libncurses*

3. Accédez au fichier de configuration SELinux situé à l'emplacement `/etc/selinux/config` et définissez SELinux en mode « permissive » (permissif) comme suit :

   `SELINUX=permissive`

- **Versions minimales RHEL :** `ncurses, libxcrypt-compat, iproute, initscripts, procps` et `net-tools`.
- **SLES :** Zypper

❒ Si la mise à niveau du système d'exploitation RHEL échoue lors de l'installation d'OpenText eDirectory, procédez comme suit.

- Utilisez la commande ci-dessous pour supprimer le paquetage avant la mise à niveau du système d'exploitation RHEL.

  `rpm -e --nodeps novell-NLDAPsdk`

- Mise à niveau du système d'exploitation RHEL de la version 8.x vers la version 9.x ou ultérieure.
- Après la mise à niveau du système d'exploitation, installez le paquetage à l'aide de la commande ci-dessous.

  `rpm -ivh ./novell-NLDAPsdk*`

- Redémarrez le service OpenText eDirectory.

❒ Exécutez les étapes suivantes pour installer OpenText eDirectory, si SELINUX est réglé sur Appliquer :

1. Téléchargez et désarchivez la version d'OpenText eDirectory.
2. Installez les paquetages OpenText eDirectory, exécutez `./nds-install` situé dans `untared_location/eDirectory/setup`.
3. Avant de configurer l'arborescence, créez le répertoire de données à l'emplacement de la dib OpenText eDirectory par défaut`/var/opt/novell/eDirectory`.

   Désormais, l'emplacement de la dib sera `/var/opt/novell/eDirectory/data`

   (Pour un emplacement personnalisé, indiquez le chemin personnalisé `ex/home/edirectory/data`)
4. Exécutez les commandes suivantes :
   - `touch /var/opt/novell/eDirectory/data/ndsd.pid`
   - `semanage fcontext -a -t var_run_t '/var/opt/novell/eDirectory/data/ndsd.pid'`
   - `restorecon -v '/var/opt/novell/eDirectory/data/ndsd.pid'`
5. À présent, configurez l'arborescence à l'aide de la nouvelle commande `ndsconfig`.

❒ (Conditionnel) NICI (Novell International Cryptographic Infrastructure) 3.3 et OpenText eDirectory 9.3 prennent en charge les tailles de clé allant jusqu'à 8 192 bits. Si vous souhaitez utiliser une taille de clé de 8 Ko, chaque serveur doit être mis à niveau vers OpenText eDirectory 9.3. De plus, NICI 3.3 doit être installé sur chaque poste de travail qui utilise les utilitaires de gestion, par exemple Identity Console.

Lorsque vous mettez à niveau votre serveur d'autorité de certification (CA) vers OpenText eDirectory 9.3, la taille de clé reste inchangée (2 Ko). La seule façon de créer une taille de clé de 8 Ko est de recréer l'autorité de certification sur un serveur OpenText eDirectory 9.3. 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 OpenText eDirectory, l'utilitaire nds-install installe automatiquement NICI. Pour en savoir plus sur l'installation d'OpenText eDirectory, reportez-vous à la section « Exécution de l'utilitaire nds-install pour installer des composants OpenText eDirectory » page 45. Cependant, si vous avez besoin d'installer uniquement NICI, et non OpenText 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 49.

- ❒ Veillez à obtenir la clé d'arborescence 3DES 168 bits pour vos serveurs OpenText eDirectory.
- ❒ (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'OpenText eDirectory 9.3 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 OpenText eDirectory » page 44.
- ❒ 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 W1.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 d'OpenText 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 d'OpenText 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 d'OpenText 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'OpenText 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'OpenText 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`.

❒ L'outil OpenText 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 OpenText 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.

### Signature RPM : clé publique pour valider la signature

Avant d'installer les composants OpenText eDirectory sur les systèmes Linux à partir d'OpenText eDirectory 9.2.7 et versions ultérieures, exécutez la procédure suivante pour effectuer la vérification de la signature RPM :

1. Accédez à l'emplacement suivant pour la clé publique :

   ```
   <untarred location of eDirectory>/eDirectory/license/
   MicroFocusGPGPackageSign.pub
   ```

2. Exécutez la commande suivante pour importer la clé publique :

   ```
   rpm --import MicroFocusGPGPackageSign.pub
   ```

3. (Facultatif) Exécutez la commande suivante pour vérifier la signature RPM :

   ```
   rpm --checksig -v <RPM Name>
   ```

   Par exemple :

   ```
   rpm --checksig -v novell-NDSbase-9.2.x.0000.x86_64.rpm
   ```

**REMARQUE :** OpenText eDirectory 9.3.0 doit être installé sur un système d'exploitation FIPS avec les versions RHEL 8 ou ultérieures et RHEL 9 ou ultérieures, SLES 12 SP5 et SLES 15 SP3, SP4, SP5 et SP6.

### Configuration de l'adresse IP statique

L'adresse IP statique doit être configurée sur le serveur pour qu'OpenText eDirectory fonctionne efficacement. La configuration d'OpenText 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 d'OpenText 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.

OpenText eDirectory fonctionne correctement avec un seul processeur. Cependant, OpenText eDirectory 9.3 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. OpenText 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 OpenText 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 d'OpenText eDirectory changent après la mise à niveau vers OpenText 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 OpenText 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.

# Ajout du groupe d'utilisateurs edirAdmin

Dans la version 9.3 d'OpenText eDirectory, le nom de groupe fixe eDirAdmin a été retiré. Il a été modifié pour incorporer le comportement actuel. Il est flexible, configurable, modifiable et facultatif (non obligatoire). La nouvelle installation ne crée pas de groupe edirAdmin. Il permet d'entrer un nom de groupe, s'il est donné, il sera utilisé à la place d'edirAdmin. Vous pouvez définir le nom du groupe à l'aide de l'option -g dans l'option `ndsconfig new/add/upgrade`. L'utilisateur doit entrer un nom de groupe valide et existant dans l'option `-g`. Il ne doit pas y avoir d'écart entre -g et le nom de groupe (-g <groupname>). Le nom de groupe indiqué sera stocké dans le fichier de configuration en tant que « `n4u.server.osgroup-name` ». S'il est vide, il ne sera pas utilisé, sinon il sera utilisé pour définir des restrictions sur les répertoires sélectionnés. L'utilisateur qui crée l'instance doit faire partie du groupe pour définir les restrictions. Il est facultatif et, s'il n'est pas donnée, on suppose qu'aucun paramètre de groupe n'est à définir. Pour la mise à niveau/migration à partir de la version 9.2.5/9.2.6, edirAdmin est déjà le propriétaire, l'utilisateur configurant doit également faire partie de ce groupe.

**REMARQUE :** Les paramètres de groupe d'utilisateurs edirAdmin suivants s'appliquent aux versions 9.2.5 et 9.2.6 d'OpenText eDirectory.

Dans la version 9.2.5 d'OpenText eDirectory, un nouveau groupe d'utilisateurs edirAdmin est ajouté à OpenText eDirectory au cours de l'installation. Ce groupe d'utilisateurs dispose des autorisations d'accès aux répertoires dans lequel les fichiers de données, de journal et de configuration sont installés. Tout utilisateur ajouté à ce groupe aura les autorisations de groupe assignées à ces répertoires.

Lors de l'installation et de la configuration root, le programme d'installation crée par défaut le groupe d'utilisateurs edirAdmin. Toutefois, pour une installation et une configuration non-root, ce groupe doit être créé manuellement avant de mettre à niveau ou d'installer la dernière version d'OpenText eDirectory. Après avoir créé le groupe, vous devez vous assurer que l'utilisateur est ajouté à ce groupe pour pouvoir configurer les instances du serveur OpenText eDirectory à l'aide de son installation tarball individuelle ou à l'aide d'une installation binaire. Par contre, lorsqu'un utilisateur non-root effectue la configuration d'OpenText eDirectory installé en root, le groupe est ajouté dans le cadre de l'installation. Vous devez vous assurer que l'utilisateur est ajouté à ce groupe, sinon il peut rencontrer des erreurs lors de la configuration d'OpenText eDirectory à l'aide de l'utilitaire `ndsconfig`.

Sur le serveur sur lequel OpenText eDirectory est installé, ouvrez un terminal et exécutez les commandes suivantes :

- Pour ajouter le groupe edirAdmin, exécutez `groupadd edirAdmin`
- Pour ajouter un utilisateur au groupe edirAdmin, exécutez `usermod -a -G edirAdmin <username>`.

  où `username` est le nom de l'utilisateur. Par exemple, pour ajouter l'utilisateur John au groupe edirAdmin, vous devez exécuter la commande :

  ```
  $ usermod -a -G edirAdmin john
  ```

---

**REMARQUE :** Avant d'ajouter l'utilisateur au groupe d'utilisateurs OpenText edirAdmin, l'administrateur doit s'assurer qu'il n'est pas connecté au serveur via une session de terminal. Une fois ajouté, l'utilisateur peut se connecter et configurer OpenText eDirectory à l'aide de l'utilitaire ndsconfig.

---

# Mise à niveau d'OpenText eDirectory

Il est recommandé de ne pas mettre directement à niveau OpenText eDirectory de la version 8.8SP1 vers la version 9.3. Vous devez passer par la version 9.2, puis par la version 9.3. La mise à niveau d'OpenText eDirectory à partir d'une version antérieure de 8.8 SP1 vers la version 9.2 a une incidence sur les performances de votre serveur OpenText eDirectory.

---

**REMARQUE :** Pour effectuer une mise à niveau à partir d'une version 32 bits d'OpenText eDirectory vers une version 64 bits, vous devez d'abord mettre à niveau la version 32 bits vers la version 64 bits d'OpenText eDirectory 8.8.x, puis vers OpenText eDirectory 9.2. Vous pouvez suivre la même procédure pour la mise à niveau d'OpenText eDirectory 64 bits vers OpenText eDirectory 9.3.

---

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


- « Vérifications de l'état de santé du serveur » page 38
- « Mettre à niveau sur des serveurs Linux autres qu'OES » page 38

- « Mise à niveau sans surveillance d'OpenText eDirectory sous Linux » page 39
- « Mise à niveau du déploiement du tarball d'eDirectory 9.3 » page 40
- « Mise à niveau d'OpenText eDirectory 9.3 par des utilisateurs non-root » page 42
- « Mise à niveau de plusieurs instances » page 42

---

**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

OpenText eDirectory 9.3 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 211

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 d'OpenText eDirectory », page 209 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 l'Annexe B, « Vérifications de l'état de santé d'OpenText eDirectory », page 209.

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

La mise à niveau d'OpenText eDirectory est prise en charge à partir d'OpenText eDirectory 9.20.

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 OpenText 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 OpenText 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 d'OpenText eDirectory sous Linux

Sous Linux, OpenText 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 d'OpenText eDirectory sous Linux :

1. effectuez la vérification de l'état de santé d'OpenText 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 OpenText eDirectory 9.3 :

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 OpenText 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 9.3

Si vous souhaitez mettre à niveau le déploiement du tarball d'OpenText eDirectory 9.20 vers OpenText eDirectory 9.3, 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 OpenText eDirectory est installé.

3 Pour mettre à niveau des versions d'OpenText 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 OpenText 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>• `netiq-openssl-3.0.15.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 49. |

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 d'OpenText eDirectory 9.3 par des utilisateurs non-root

Un utilisateur non-root peut mettre à niveau OpenText eDirectory à l'aide de la nouvelle version du tarball. Pour mettre à niveau OpenText eDirectory en tant qu'utilisateur non-root, procédez comme suit :

1. Connectez-vous à la machine sur laquelle OpenText eDirectory est installé en tant qu'utilisateur non-root à l'aide de ssh.
2. Accédez au répertoire dans lequel vous souhaitez installer OpenText eDirectory.
3. Désarchivez la nouvelle version du fichier tar comme suit :

   ```
   tar xvf /tar_file_name
   ```

   Les répertoires `etc`, `opt` et `var` sont créés.
4. Arrêtez tous les serveurs eDirectory comme suit :

   ```
   ndsmanage stopall
   ```
5. Mettez à niveau OpenSSL et NICI en tant qu'utilisateur root à l'aide des commandes suivantes :
   - OpenSSL doit être mis à niveau avant de mettre à niveau NICI. Pour installer OpenSSL, entrez la commande suivante :

     ```
     rpm -Uvh openssl_rpm_absolute_path/netiq-openssl-3.0.15.x86_64.rpm
     ```
   - Pour mettre à niveau NICI 64 bits, entrez la commande suivante :

     ```
     rpm -Uvh NICI_rpm_absolute_path/nici64-3.3.0-0.00.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
     ```
6. Exécutez la commande suivante pour mettre à niveau les serveurs OpenText eDirectory :

   ```
   ndsconfig upgrade
   ```

# Mise à niveau de plusieurs instances

Ce chapitre comprend les informations suivantes :


- « L'utilisateur root possède plusieurs instances » page 42
- « Instances d'utilisateur non root » page 43
- « Ordre de mise à niveau » page 43


## 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 OpenText 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

d'OpenText 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.

---

**REMARQUE :** Pour mettre à niveau le serveur de répliques avec EBA dans Linux pour eDirectory 9.2.8 et 9.2.9, voir « Installation du correctif de pont sur plusieurs serveurs de répliques avec EBA sous Linux » page 25.

---

# Installation d'OpenText eDirectory

Les sections suivantes fournissent des informations sur l'installation d'OpenText eDirectory sous Linux :


- « Utilisation de SLP avec OpenText eDirectory » page 44
- « Exécution de l'utilitaire nds-install pour installer des composants OpenText eDirectory » page 45
- « Installation d'OpenText eDirectory 9.3 par un utilisateur non-root » page 48
- « Configuration d'OpenText eDirectory par un utilisateur non-root à l'aide de l'installation root » page 52
- « Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques OpenText eDirectory » page 54
- « Utilisation de ndsconfig pour configurer plusieurs instances d'OpenText eDirectory 9.3 » page 61
- « Utilisation de ndsconfig pour installer un serveur Linux dans une arborescence dont les noms de conteneur utilisent des points » page 68
- « Exécution de l'utilitaire nmasinst pour configurer NMAS » page 69
- « Configuration de SNMP par un utilisateur non-root » page 70
- « Localisation des fichiers journaux » page 70

## Utilisation de SLP avec OpenText eDirectory

Dans les précédentes versions d'OpenText eDirectory, l'installation de SLP se faisait pendant celle d'OpenText eDirectory. En revanche, avec eDirectory 9.1 et versions ultérieures, vous devez d'abord installer SLP, puis OpenText 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 l'Annexe C, « Configuration de OpenSLP pour OpenText eDirectory », page 215.

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 OpenText eDirectory pour effectuer des recherches dans les partitions et les serveurs d'OpenText 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 l'Annexe C, « Configuration de OpenSLP pour OpenText eDirectory », page 215.

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

L'utilitaire nds-install permet d'installer les composants OpenText 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 OpenText 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 d'OpenText eDirectory », page 209. |
| `-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 OpenText 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'OpenText 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 OpenText 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 OpenText 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 OpenText 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 OpenText 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 d'OpenText eDirectory à l'aide de ndsconfig.

Par défaut, le serveur OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

Pour plus d'informations sur l'utilitaire ndsconfig, reportez-vous à la section « Utilitaire ndsconfig » page 177.

Pour plus d'informations sur l'utilitaire nmasinst, reportez-vous à la section « Exécution de l'utilitaire nmasinst pour configurer NMAS » page 69.

---

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

Pour plus d'informations sur la sauvegarde d'OpenText eDirectory, voir « Sauvegarde et restauration d'OpenText eDirectory », dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

---

# Installation d'OpenText eDirectory 9.3 par un utilisateur non-root

Un utilisateur non-root peut installer eDirectory 9.3 à l'aide du tarball.

## Conditions préalables

- ❒ Si vous souhaitez installer OpenText eDirectory à l'aide du tarball plutôt qu'avec l'utilitaire nds-install, assurez-vous qu'OpenSSL est installé avant d'installer NICI. Pour plus d'informations sur l'installation d'OpenSSL, reportez-vous à la section « Installation d'OpenSSL » page 49.

- ❒ Si vous souhaitez installer OpenText 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 49.
- ❒ 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 OpenText 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 31.

## Installation d'OpenSSL

OpenSSL doit être installé, puis NICI avant d'installer OpenText eDirectory.

### Installation d'OpenSSL par un utilisateur root

Pour installer OpenSSL, entrez la commande suivante :

```
rpm -ivh openssl_rpm_absolute_path/netiq-openssl-3.0.15.x86_64.rpm
```

## Installation de l'infrastructure NICI

NICI doit être installé avant OpenText 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 OpenText eDirectory 9.3, les applications 32 et 64 bits peuvent coexister au sein d'un même système. Pour l'installation de NICI, reportez-vous aux sections suivantes.

### Installation de NICI par un utilisateur root

Pour installer NICI 64 bits, entrez la commande suivante :

```
rpm -ivh NICI_rpm_absolute_path/nici64-3.3.0.0000.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 de l'utilisateur sous SLES 15 et versions ultérieures

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 un démarrage de systemd spécifique à un utilisateur, connectez-vous à la machine sur laquelle OpenText eDirectory est installé en tant qu'utilisateur root et 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 OpenText eDirectory sur SLES 15 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 OpenText eDirectory.

---

## Installation d'OpenText eDirectory

1. Connectez-vous à la machine sur laquelle OpenText eDirectory est installé en tant qu'utilisateur non-root à l'aide de ssh.
2. Accédez au répertoire dans lequel vous souhaitez installer OpenText eDirectory.
3. Désarchivez le fichier tar comme suit :

   ```
   tar xvf /tar_file_name
   ```

   Les répertoires etc et opt sont créés.
4. 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
  ```

- Vous pouvez également exporter les chemins dans le shell actuel en fournissant explicitement l'emplacement du tarball OpenText eDirectory vers l'utilitaire ndspath :

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

  ---

  **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.

**5** Configurez OpenText eDirectory comme d'habitude.

Vous pouvez configurer OpenText 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 1024 et 65535. Ceux inférieurs à 1024 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 65.

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, OpenText 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 section « Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques OpenText eDirectory » page 54.

---

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

Pour plus d'informations sur la sauvegarde d'OpenText eDirectory, voir « Sauvegarde et restauration d'OpenText eDirectory », dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

---

## Configuration d'OpenText eDirectory par un utilisateur non-root à l'aide de l'installation root

Plusieurs menaces de sécurité sont associées lorsqu'un utilisateur non-root installe et configure OpenText eDirectory à l'aide du tarball d'installation. L'utilisateur non-root qui configure OpenText eDirectory est propriétaire des binaires qui le rendront vulnérable aux attaques externes. Pour des raisons de sécurité, nous vous recommandons d'exécuter le service `ndsd` en tant qu'utilisateur non-root, après avoir installé OpenText eDirectory à l'aide du script d'installation en tant qu'utilisateur root. L'utilisateur non-root doit être un utilisateur non privilégié et ne doit pas posséder/disposer d'autorisations en écriture sur les binaires OpenText eDirectory placés lors de l'installation root, ce qui réduit le risque de menaces de sécurité. Cela vous permet également d'utiliser l'utilitaire `nds-install` pour maintenir ou mettre à niveau le serveur OpenText eDirectory :

1. En tant qu'utilisateur root, utilisez l'utilitaire `nds-install` pour installer les composants OpenText eDirectory sur les systèmes Linux :

   ```
   ./nds-install
   ```

   Acceptez l'accord de licence.

   Pour plus d'informations, reportez-vous à la section « Exécution de l'utilitaire nds-install pour installer des composants OpenText eDirectory » page 45.

2. Exportez les chemins comme suit :

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

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

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

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

export TEXTDOMAINDIR=/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 :

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

- Exportez les chemins dans le shell actuel comme suit :

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

  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.

**3** En tant qu'utilisateur non-root, utilisez l'utilitaire `ndsconfig` ou `ndsmanage` pour configurer le serveur eDirectory après l'installation root d'OpenText eDirectory. Voici un exemple de commande :

```
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
```

---

**REMARQUE**

- OpenText eDirectory ne peut pas être configuré à l'aide des ports standard. La plage de ports doit être entre comprise entre 1 024 et 65 535.
- L'utilisateur non-root doit avoir les autorisations requises pour l'emplacement où est stocké le fichier de configuration OpenText eDirectory, sauf si la configuration échoue.

---

Pour un démarrage de `systemd` spécifique à un utilisateur, connectez-vous à la machine sur laquelle OpenText eDirectory est installé en tant qu'utilisateur root et 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
```

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

Après avoir installé OpenText eDirectory, configurez le serveur de répliques OpenText 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 OpenText eDirectory et modifier la configuration actuelle de l'objet Serveur OpenText eDirectory. Pour plus d'informations, reportez-vous à la section « Utilitaire ndsconfig » page 177.

---

**REMARQUE :** À partir d'OpenText eDirectory 9.3.0 et des versions ultérieures, s'il s'agit du serveur maître 9.3.0, l'ajout de versions antérieures d'OpenText eDirectory en tant que réplique n'est pas pris en charge, avec ou sans EBA.

---

## Condition préalable pour la configuration d'OpenText eDirectory dans des paramètres régionaux spécifiques

Si vous souhaitez configurer OpenText eDirectory dans des paramètres régionaux spécifiques, vous devez exporter au préalable LC_ALL et LANG vers ces paramètres donnés. Par exemple, pour configurer OpenText 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'OpenText eDirectory permette de définir le FDN de l'objet Serveur NCP jusqu'à 256 caractères, nous vous recommandons de limiter la variable à une valeur bien inférieure étant donné qu'OpenText 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 OpenText 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 du Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).

---

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

OpenText 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 OpenText 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 OpenText 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 OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

## 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>]
```

OpenText 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, OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

---

**REMARQUE :** Nous avons supprimé la prise en charge de la réplication codée dans la version 9.2.7 d'OpenText 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 OpenText eDirectory.

---

Par exemple, pour retirer l'objet Serveur OpenText 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 OpenText 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 OpenText 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 d'OpenText eDirectory dans l'arborescence existante. |
| `rm` | Retire l'objet Serveur et les services Annuaire d'une arborescence.<br><br>**REMARQUE :** Cette option ne supprimer pas les objets matériels clés. Ces objets doivent être supprimés manuellement. |
| `mettre à niveau` | Met à niveau OpenText 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 OpenText 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 OpenText 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 d'OpenText 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 OpenText 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. Si l'administrateur spécifie uniquement `@<port-number>` pour cette option, les services NCP, http et https se lient à toutes les interfaces disponibles. |

| Paramètre ndsconfig | Description |
|---|---|
| `--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`. |
| `-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 OpenText 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 OpenText 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 OpenText eDirectory configurables. |
| `set` `liste_valeurs` | Définit la valeur des paramètres OpenText 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 OpenText eDirectory configurables qui ont été spécifiés. Si la liste des paramètres n'est pas spécifiée, ndsconfig liste tous les paramètres OpenText eDirectory configurables. |

| Paramètre ndsconfig | Description |
|---|---|
| `configure -eba-now` | Utilisez ce paramètre pour configurer votre serveur eDirectory pour l'authentification EBA. |

## Utilisation de ndsconfig pour configurer plusieurs instances d'OpenText eDirectory 9.3

Vous pouvez configurer plusieurs instances d'OpenText eDirectory 9.3 sur un hôte unique. Désormais, grâce à la fonction d'instances multiples prise en charge par OpenText eDirectory 9.3, vous pouvez configurer les éléments suivants :

- plusieurs instances d'OpenText 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. OpenText 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 d'OpenText 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 d'OpenText 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 haute disponibilité des services OpenText 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 d'OpenText 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.

### OpenText eDirectory dans un environnement d'évaluation

- **Universités :** grâce aux instances multiples, de nombreux (étudiants) enthousiastes peuvent évaluer OpenText eDirectory à partir du même hôte.
- **Formation à l'administration d'OpenText 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

OpenText eDirectory 9.3 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 67
- « Configuration d'instances multiples » page 63

## Planification de la configuration

Pour utiliser cette fonction efficacement, nous vous recommandons de planifier les instances d'OpenText 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 d'OpenText 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 d'OpenText eDirectory.

Vous pouvez également configurer une nouvelle instance à l'aide de l'utilitaire ndsmanage. Pour plus d'informations, reportez-vous à la section « Création d'une instance via ndsmanage » page 65.

## Gestion d'instances multiples

Cette section présente les informations suivantes :

- « Utilitaire ndsmanage » page 64
- « Identification d'une instance spécifique » page 66
- « Appel d'un utilitaire pour une instance spécifique » page 67

### 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 3-1*** *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 :

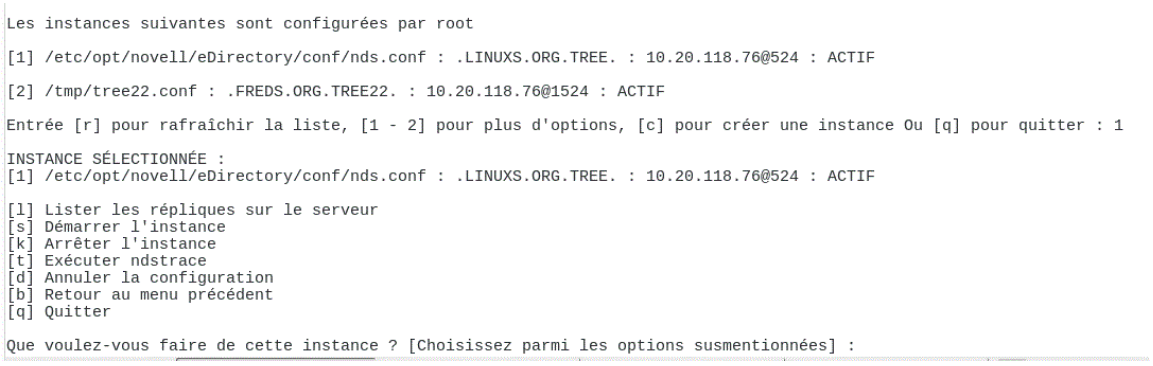
1. Saisissez la commande suivante :

   ```
   ndsmanage
   ```

2. Sélectionnez l'instance à démarrer.

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

***Figure 3-1*** *Écran de sortie de l'utilitaire ndsmanage avec options d'instance*




3. Entrez s pour démarrer l'instance.

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

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

### Arrêt d'une instance spécifique

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

1. Saisissez la commande suivante :

```
ndsmanage
```

2. Sélectionnez l'instance à arrêter.

   Le menu se développe pour inclure les options que vous pouvez exécuter sur une instance spécifique. Pour plus d'informations, reportez-vous à la section Écran de sortie de l'utilitaire ndsmanage avec options d'instance (page 65).

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 section Écran de sortie de l'utilitaire ndsmanage avec options d'instance (page 65).

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 65.

## 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 d'OpenText 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 OpenText 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 OpenText 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 69
- « Installation des méthodes de connexion » page 69


## 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 d'OpenText 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 composant du schéma OpenText 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 des méthodes et des séquences de connexion et de post-connexion du Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).

# 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 49
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 OpenText 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 OpenText 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.

# 4 Installation ou mise à niveau d'OpenText eDirectory CE 24.4 (v9.3) sous Windows

Les informations suivantes permettent d'installer ou de mettre à niveau OpenText eDirectory 9.3 sur une plate-forme Windows :


- « Configuration système requise » page 73
- « Conditions préalables » page 74
- « Configuration matérielle requise » page 77
- « Exécution forcée du processus de liaison en amont » page 77
- « Installation d'OpenText eDirectory sous Windows » page 78
- « Mise à niveau d'OpenText eDirectory sous Windows » page 91


---

**IMPORTANT :** OpenText eDirectory 9.3 permet d'installer OpenText eDirectory pour Windows sans le client Novell. Pour plus d'informations, reportez-vous à la section « Installation ou mise à niveau d'OpenText eDirectory 9.3 sur un serveur Windows » page 78.

---

## Configuration système requise

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

- Windows Server 2016 au minimum et Windows Server 2022

---

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

---

OpenText 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 OpenText 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 OpenText eDirectory existant, assurez-vous que les applications NetIQ et tierces installées assurent la prise en charge d'OpenText eDirectory 9.3. Vous pouvez consulter l'état actuel des produits OpenText dans le document TID 7003446 (http://www.novell.com/support/kb/doc.php?id=7003446). Il est également vivement recommandé de sauvegarder OpenText eDirectory avant toute mise à niveau.

- ❒ Dans la mesure où un système NTFS offre un processus de transaction plus sécurisé qu'un système de fichiers FAT, vous ne pouvez installer OpenText 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 ne dispose que d'un système de fichiers FAT et que vous omettez ce processus, le programme d'installation vous demande de fournir une partition NTFS.
- ❒ (Conditionnel) NICI 3.3 et OpenText eDirectory 9.3 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 Ko, chaque serveur doit être mis à niveau vers OpenText eDirectory 9.3. De plus, NICI 3.3 doit être installé sur chaque poste de travail qui utilise les utilitaires de gestion, par exemple Identity Console.

  Lorsque vous mettez à niveau votre serveur d'autorité de certification (CA) vers OpenText eDirectory 9.3, la taille de clé reste inchangée (2 Ko). La seule façon de créer une taille de clé de 8 Ko est de recréer l'autorité de certification sur un serveur OpenText eDirectory 9.3. 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 3.3 soit installé sur le système.
- ❒ Veillez à obtenir la clé d'arborescence 3DES 168 bits pour vos serveurs OpenText eDirectory.
- ❒ Si vous effectuez une mise à niveau vers OpenText eDirectory 9.3, vérifiez que les derniers correctifs d'OpenText eDirectory sont installés sur tous les serveurs de l'arborescence autres que les serveurs OpenText eDirectory 9.3. Ces correctifs sont disponibles sur le site Web du support OpenText (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 Server sont installés. Le dernier Service Pack Windows Server mis à jour doit être installé après l'installation du service SNMP Windows.
- ❒ Si vous effectuez la mise à niveau à partir d'une ancienne version d'OpenText eDirectory, il doit s'agir de la version 9.3.0 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'OpenText eDirectory » page 76.

- ❒ (Conditionnel) Si vous vous installez un serveur secondaire dans une arborescence existante sans posséder de droits d'administration d'OpenText 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 et W1.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 d'OpenText 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 indiquer pendant la configuration d'OpenText eDirectory.
- ❒ Si vous installez OpenText 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 OpenText eDirectory 9.3, exécutez le fichier `Novell_Audit_PlatformAgent_Win64.exe` à partir de l'emplacement d'installation `<C:\NetIQ\eDirectory\auditds/`.

- ❒ L'outil OpenText 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 ou Azul 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 OpenText eDirectory 9.0 SP4, pour exécuter le client à ligne de commande, vous devez avoir accès à l'environnement d'exécution Java.
  - L'installation d'Identity Manager 4.8.7 permet de mettre à niveau les paquetages dépendants Java dans OpenText eDirectory de JRE 8 vers JRE 11.

## Détermination de la version d'OpenText eDirectory

Pour déterminer la version d'OpenText 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 d'agent pour eDirectory 9.3 pourrait être 40301.00.

  Pour plus d'informations sur l'exécution d'OpenText iMonitor, voir « Accès à OpenText iMonitor » dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

- Exécutez `NDSCons.exe`.

  Dans le Panneau de configuration de Windows, double-cliquez sur Services OpenText eDirectory. Dans la colonne Services, sélectionnez ds.dlm, puis cliquez sur Configurer. L'onglet Agent affiche la chaîne marketing (par exemple, OpenText eDirectory 9.3) et le numéro de version interne (par exemple, 40301.00).

- 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 qu'OpenText 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 d'OpenText eDirectory.

Par exemple, une installation de base d'OpenText 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.

OpenText eDirectory fonctionne correctement avec un seul processeur. Cependant, OpenText eDirectory 9.3 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. OpenText 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 OpenText 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 d'OpenText eDirectory changent après la mise à niveau vers OpenText 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 OpenText 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** > **OpenText 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'OpenText eDirectory sous Windows

Ce chapitre comprend les informations suivantes :


- « Installation ou mise à niveau d'OpenText eDirectory 9.3 sur un serveur Windows » page 78
- « Vérifications de l'état de santé du serveur » page 80
- « Communication avec OpenText eDirectory via LDAP » page 81
- « Installation du logiciel NMAS Server » page 82
- « Installation dans une arborescence comportant des conteneurs dont le nom utilise la notation à point » page 82
- « Installation et configuration sans surveillance d'OpenText eDirectory 9.3 sous Windows » page 83
- « Localisation des fichiers journaux » page 90


## Installation ou mise à niveau d'OpenText eDirectory 9.3 sur un serveur Windows

Vous pouvez installer OpenText eDirectory 9.3 pour Windows sans le client Novell. Si vous installez OpenText eDirectory 9.3 sur une machine qui contient déjà le client Novell, OpenText 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_930_Windows_x86_64.exe` à partir du dossier `windows` sur le CD-ROM eDirectory 9.3 ou à partir du fichier téléchargé.
3. (Nouvelles installations uniquement) Sélectionnez un type d'installation OpenText 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'OpenText 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'OpenText eDirectory permette de définir le FDN de l'objet Serveur NCP jusqu'à 256 caractères, OpenText vous recommande de limiter la variable à une valeur bien inférieure étant donné qu'OpenText 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 :** OpenText eDirectory 9.3 vous permet d'utiliser des mots de passe qui respectent la casse pour tous les utilitaires.

Pour plus d'informations sur l'utilisation des points dans les noms de conteneurs, reportez-vous à la section « Installation dans une arborescence comportant des conteneurs dont le nom utilise la notation à point » page 82.

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'OpenText eDirectory.

**IMPORTANT :** Veillez à ce que les ports de la pile HTTP que vous avez définis pendant l'installation d'OpenText eDirectory soient différents de ceux que vous avez utilisés ou allez utiliser pour OpenText Identity Console. Pour plus d'informations, consultez le *Guide d'administration d'OpenText Identity Console* (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/bookinfo.html).

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

  Pour plus d'informations, reportez-vous à la section « Communication avec OpenText eDirectory via LDAP » page 81.

8 Cliquez sur **Installer**.

  Le programme d'installation vérifie les composants suivants avant d'installer OpenText eDirectory. Si un composant est manquant ou si sa version est incorrecte, le programme d'installation lance automatiquement l'installation du composant. L'invite de commande apparaît avec le message - **INSTALL PASSED.** Ce message disparaît automatiquement après la réussite de l'installation de NICI et l'installation d'eDirectory se poursuit.

  - NICI 3.3

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

9 OpenText 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'OpenText eDirectory doit pouvoir se connecter au serveur sur lequel OpenText eDirectory est installé.

**REMARQUE :** Après avoir installé OpenText 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 d'OpenText eDirectory pour sauvegarder votre répertoire DIB.

Pour plus d'informations sur la sauvegarde d'OpenText eDirectory, voir « Sauvegarde et restauration d'OpenText eDirectory », dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

## Vérifications de l'état de santé du serveur

OpenText eDirectory 9.3 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 211

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 d'OpenText eDirectory », page 209 pour consulter la liste de conditions des erreurs mineures et critiques.

# Communication avec OpenText eDirectory via LDAP

Lorsque vous installez OpenText 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 9.3 | Port 389 en texte clair | Sélectionne le port 389. |
| eDirectory 9.3 | 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 OpenText 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 d'OpenText eDirectory 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. Active Directory s'exécute sur 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 OpenText LDAP. 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 OpenText LDAP (389 ou 636) lancez l'utilitaire ICE. Si le champ **Version du fournisseur** n'indique pas OpenText, vous devez reconfigurer le serveur LDAP pour OpenText eDirectory et sélectionner un port différent. Pour plus d'informations, reportez-vous à la section « Vérification de l'exécution du serveur LDAP » du *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

**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 OpenText LDAP en sélectionnant un autre port, afin que le serveur LDAP OpenText eDirectory puisse répondre aux requêtes LDAP.

OpenText iMonitor peut également signaler que le port 389 ou 636 est déjà ouvert. Si le serveur LDAP ne fonctionne pas, utilisez OpenText iMonitor pour identifier les détails. Pour plus d'informations, reportez-vous à la section « Vérification de l'exécution du serveur LDAP » du *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

## 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 des méthodes et des séquences de connexion et de post-connexion du Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).

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

Vous pouvez installer un serveur Windows dans une arborescence OpenText 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 OpenText iMonitor, OpenText Identity Console 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'OpenText eDirectory 9.3 sous Windows

OpenText eDirectory 9.3 automatise l'installation et la mise à niveau d'OpenText 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 d'OpenText eDirectory selon s'il s'agit ou non d'une installation complète d'OpenText eDirectory. Le processus de mise à niveau autonome met à niveau les fichiers installés uniquement.
- Configuration de la version d'OpenText eDirectory installée. Si vous installez OpenText eDirectory, une configuration complète d'eDirectory est réalisée. Sinon, lorsque vous mettez à niveau OpenText 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 84.

### Conditions préalables

- La version 4.0 de .NET Management Framework ou une version ultérieure est requise.
- Assurez-vous que Windows Server  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 83
- « Ajout de fonctionnalités à l'installation automatisée » page 84
- « Contrôle de l'installation automatisée » page 88
- « Installation sans surveillance d'OpenText eDirectory à l'aide du fichier de réponses » page 90


## Fichiers de réponse

L'installation ou la mise à niveau vers OpenText eDirectory 9.3 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 9.3 nécessite de modifier les sections du fichier de réponses afin d'ajouter des informations sur l'instance OpenText 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'OpenText eDirectory :

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

---

**REMARQUE :** Lors de l'installation d'OpenText 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 OpenText 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 permet de configurer OpenText 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. OpenText eDirectory offre la possibilité d'activer EBA lors de la configuration de l'arborescence OpenText eDirectory. Par défaut, EBA n'est pas configuré dans OpenText 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 :** OpenText prend en charge l'exécution d'eDirectory en mode FIPS (Federal Information Processing Standard). Pour activer OpenText 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 OpenText eDirectory 9.3. 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 du Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).

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

OpenText 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 d'OpenText 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 4-1*** *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 OpenText |
| 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, OpenText 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

OpenText eDirectory écoute sur les ports HTTP préconfigurés pour un accès via le Web. Par exemple, iMonitor accède à OpenText 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

OpenText 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 d'OpenText 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 OpenText 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 OpenText eDirectory doit écouter les requêtes LDAP en SSL. Vous pouvez également utiliser une clé pour configurer le fait qu'OpenText 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 OpenText 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 d'OpenText eDirectory sur Windows. La plupart des serveurs Windows ont un service SNMP configuré et en cours d'exécution. Lors de l'installation d'OpenText 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
```

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

OpenText 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 OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

### Installation d'un serveur primaire/secondaire

Le programme d'installation OpenText 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 d'OpenText eDirectory à l'aide du fichier de réponses

Il est facile de lancer le programme d'installation OpenText eDirectory sur Windows. Le fichier `eDirectory_930_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

Exécutez la commande suivante à l'invite de commande Windows :

`<chemin_emplacement_téléchargement>\eDirectory_930_Windows_x86_64.exe /qn`

Par exemple : `D:\builds\eDirectory_930_Windows_x86_64.exe /qn`

---

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

```
eDirectory_930_Windows_x86_64.exe /qn
INSTALLDIR="C:\<emplacement_installation>
```

---

### Configuration

Exécutez la commande suivante dans Windows PowerShell :

```
<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 d'OpenText Directory.

# Mise à niveau d'OpenText eDirectory sous Windows

Il est recommandé de ne pas mettre directement à niveau eDirectory de la version 8.8 SP1 vers la version 9.3. Vous devez passer à la version 9.2, puis à la version 9.3. Si vous avez un serveur EBA, vous devez être sous OpenText eDirectory 9.2.8 ou 9.2.9 avant d'effectuer la mise à niveau vers OpenText eDirectory 9.3.0.

Si la méthode NMAS est déjà installée, pour mettre à niveau OpenText eDirectory 9.30, vous devez étendre le schéma NMAS avant la mise à niveau. Pour plus d'informations, reportez-vous à la section « Extension de schéma NMAS avant la mise à niveau d'OpenText eDirectory » page 91.

---

**REMARQUE :** Pour effectuer une mise à niveau à partir d'une version 32 bits d'OpenText eDirectory vers une version 64 bits, vous devez d'abord mettre à niveau la version 32 bits vers la version 64 bits d'OpenText eDirectory 8.8.x, puis vers OpenText eDirectory 9.2. Vous pouvez suivre la même procédure pour la mise à niveau d'OpenText eDirectory 64 bits vers OpenText eDirectory 9.3.

---

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


- « Extension de schéma NMAS avant la mise à niveau d'OpenText eDirectory » page 91
- « Mise à niveau d'OpenText eDirectory à l'aide de Windows Installer » page 92
- « Mise à niveau sans surveillance d'OpenText eDirectory sous Windows » page 93


## Extension de schéma NMAS avant la mise à niveau d'OpenText eDirectory

Lorsque `eDirectory_930_Windows_x86_64.exe` est téléchargé et extrait, un fichier `preUpgrade_930` est présent avec le programme d'installation. Accédez au fichier `preUpgrade_930` pour afficher les fichiers ci-dessous.

- `preUpgrade_930/preUpgrade.ps`
- `preUpgrade_930/upgrade.ni`
- `preUpgrade_930/nmas.sch`

**Extension de schéma dans les fenêtres :**

Avant de mettre à niveau OpenText eDirectory vers la version 9.3.0, procédez comme suit pour étendre le schéma.

1 Mettez à jour le fichier `upgrade.ni` présent dans le dossier preUpgrade_930. Indiquez 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=10.10.10.10
Existing Server Port=524
[NWI:SNMP]
Stop service=No
[NWI:NMAS]
Methods=CertMutual,Challenge Response,DIGEST-MD5,NDS,Simple
Password,SAML
```

2 Exécutez la commande ci-dessous à partir de powershell.

```
preUpgrade.ps1 -rfile <path_for_Configuration>/upgrade.ni
```

3 Une fois l'extension du schéma réussie, poursuivez la mise à niveau d'eDirectory vers la version 9.3.0.

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

Vous pouvez mettre à niveau votre serveur OpenText 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_930_Windows_x86_64.exe` à partir du dossier windows sur le CD-ROM eDirectory 9.3 ou à partir du fichier téléchargé.

3 L'écran du programme d'installation affiche ensuite le nom de l'arborescence OpenText 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'OpenText eDirectory. Pour plus d'informations, reportez-vous à la section « Installation ou mise à niveau d'OpenText eDirectory 9.3 sur un serveur Windows » page 78.

---

**REMARQUE :** Pour mettre à niveau le serveur de répliques avec EBA dans Windows pour eDirectory 9.2.8 et 9.2.9, voir « Installation d'un correctif de pont sur plusieurs serveurs de répliques avec EBA sous Windows » page 26

---

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

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

Sous Windows, vous devez installer la dernière version d'OpenText eDirectory avant d'utiliser la commande suivante :

```
<Download Location Path>\eDirectory_930_Windows_x86_64.exe /qn
```

Exemple

```
D:\builds\eDirectory_930_Windows_x86_64.exe /qn
```

Pour plus d'informations, reportez-vous à la section « Installation et configuration sans surveillance d'OpenText eDirectory 9.3 sous Windows » page 83.

Après avoir mis à jour toutes les bibliothèques, indiquez 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=10.10.10.10
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 OpenText eDirectory nécessaires, exécutez la commande suivante pour mettre à niveau votre serveur OpenText 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`.

# 5 Déploiement d'OpenText eDirectory dans Microsoft Azure

Il est possible de déployer OpenText eDirectory sur des machines virtuelles Microsoft Azure. Pour plus d'informations sur les systèmes d'exploitation pris en charge, voir « Configuration système requise » page 29 pour Linux ou « Configuration système requise » page 73 pour Windows.

## Conditions préalables

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

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

## Procédure de déploiement

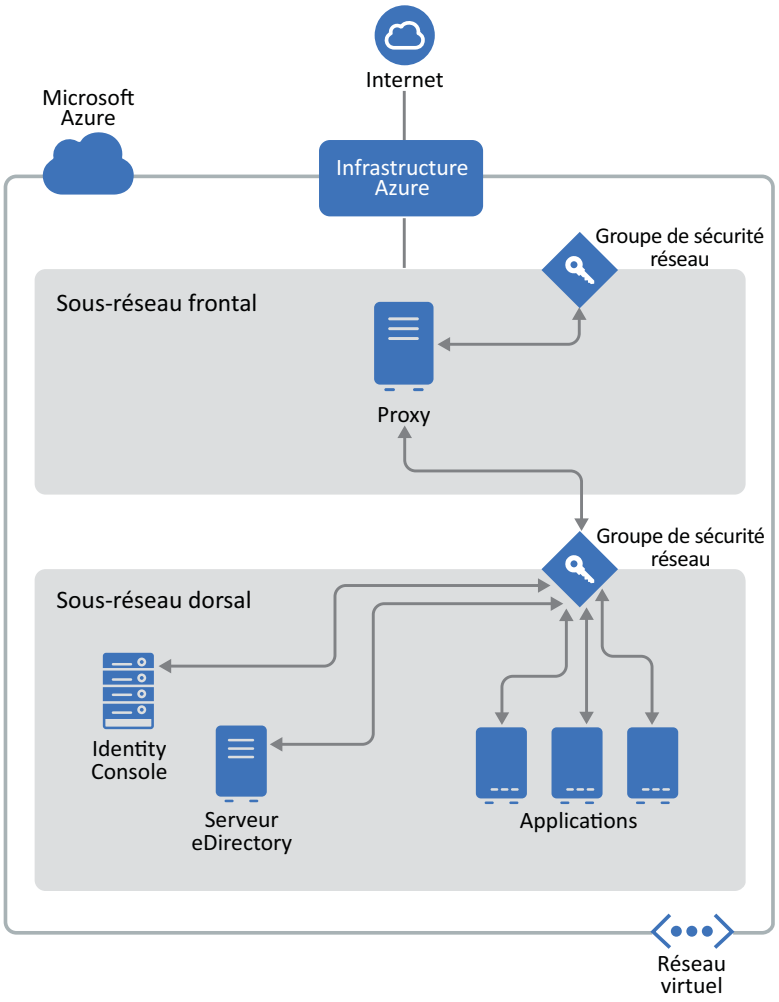
La section suivante fournit des instructions pour le déploiement d'OpenText eDirectory sur Microsoft Azure en fonction du système d'exploitation qui s'exécute sur les machines virtuelles.


- « Déploiement sur une plate-forme Linux » page 95
- « Déploiement sur une plate-forme Windows » page 110


### Déploiement sur une plate-forme Linux

OpenText eDirectory ne doit être déployé que dans un sous-réseau dorsal du service Réseau virtuel Azure. La Figure 5-1 illustre un exemple de déploiement utilisé dans les sections suivantes.

***Figure 5-1*** *Déploiement d'OpenText 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 OpenText 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.
- L'installation hybride, c'est-à-dire l'installation sur site et la réplique maître d'OpenText eDirectory sur la machine virtuelle Azure, et inversement, n'est pas prise en charge.

La procédure de déploiement comporte les étapes suivantes :


- « Préparation des services Azure » page 97
- « Configuration de groupes de sécurité d'application (ASG) » page 98
- « Configuration de groupes de sécurité réseau (NSG) pour les sous-réseaux » page 98
- « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 100

- « Création d'une paire de clés SSH » page 103
- « Création et déploiement de machines virtuelles » page 103
- « Configuration d'un disque de données pour le stockage des données OpenText eDirectory » page 104
- « Installation d'OpenText eDirectory et d'OpenText Identity Console » page 105
- « Déploiement des services d'audit » page 109
- « Reprise après sinistre » page 109


## Préparation des services Azure

Cette section décrit les étapes générales à suivre pour créer les services Azure à utiliser avec OpenText 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'OpenText 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 Azure 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 5-1*** *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 OpenText eDirectory sera configuré. |
| eDirectory_CA | Contient l'interface réseau de la machine virtuelle sur laquelle le serveur OpenText eDirectory qui héberge l'autorité de certification de l'arborescence sera configuré. |
| OpenText Identity Console | Contient l'interface réseau de la machine virtuelle sur laquelle OpenText Identity Console 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 5-2*** *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. |

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 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. |
| 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 5-3*** *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 | Identity Console | TCP 9000 | Proxy (ASG) | OpenText Identity Console (ASG) | ALLOW | Autorise le trafic HTTPS pour accéder à OpenText Identity Console à partir du proxy SSH |

| 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 OpenText 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 | 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 OpenText eDirectory dans Azure, créez les groupes de sécurité réseau suivants : eDirectory_NSG_1, eDirectory_NSG_2 et IdentityConsole_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) | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic SSH depuis le proxy SSH. |
| 110 | NCP | TCP 524 | Sous-réseau dorsal | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic NCP pour OpenText eDirectory dans le sous-réseau dorsal. |
| 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 OpenText 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 | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic LDAP sécurisé dans le sous-réseau dorsal. |
| 140 | SLP | N'importe laquelle (427) | Sous-réseau dorsal | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic SLP dans le sous-réseau dorsal. |

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 150 | All Traffic (Tout le trafic) | Toutes | Tout | Tout | DENY | Refuse tout le trafic entrant. |

**REMARQUE :** Les serveurs OpenText 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 OpenText eDirectory. En outre, l'accès au port HTTP doit uniquement être autorisé dans le groupe de sécurité assigné au serveur OpenText 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 OpenText eDirectory autres que l'autorité de certification de l'arborescence OpenText eDirectory.

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | SSH | TCP 22 | SSH Proxy (ASG) | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic SSH depuis le proxy SSH. |
| 110 | NCP | TCP 524 | Sous-réseau dorsal | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic NCP pour OpenText eDirectory dans le sous-réseau dorsal. |
| 120 | LDAPS | TCP 636 | Sous-réseau dorsal | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic LDAP sécurisé dans le sous-réseau dorsal. |
| 130 | SLP | N'importe laquelle (427) | Sous-réseau dorsal | OpenText 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. **IdentityConsole_NSG :** ce groupe NSG doit être associé à la machine virtuelle qui héberge Identity Console. Les règles NSG suivantes autorisent l'accès au serveur Identity Console à partir du serveur proxy uniquement.

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | SSH | TCP 22 | SSH Proxy (ASG) | OpenText Identity Console (ASG) | ALLOW | Autorise le trafic SSH depuis le proxy. |
| 110 | HTTPS | TCP 9000 | SSH Proxy (ASG) | OpenText Identity Console (ASG) | ALLOW | Autorise le trafic HTTP sécurisé pour l'accès à Identity Console 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 OpenText eDirectory sera configuré, eDirectory_NSG_2 à la machine virtuelle sur laquelle tous les autres serveurs OpenText eDirectory seront configurés et IdentityConsole_NSG avec la machine

virtuelle sur laquelle Identity Console 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 100.

2 Associez la clé publique créée à la section « Création d'une paire de clés SSH » page 103 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 OpenText eDirectory maître.

---

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

La configuration d'un disque de données est nécessaire pour éviter la perte des données et de la configuration d'OpenText eDirectory en cas de crash de la machine virtuelle Azure. Pour plus d'informations sur la récupération des données et de la configuration d'OpenText eDirectory, reportez-vous à la section « Reprise après sinistre » page 109. Une fois la machine virtuelle créée, procédez comme suit pour préparer la machine virtuelle pour le déploiement d'OpenText 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 OpenText eDirectory/NICI. Procédez comme suit en tant qu'utilisateur root pour effectuer le montage de liaison :

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

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

**3d** Créez les répertoires nécessaires pour OpenText 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'OpenText eDirectory et d'OpenText Identity Console

### Conditions préalables

- ❒ Veillez à respecter la configuration requise indiquée à la section « Configuration système requise » page 29.
- ❒ Créez des groupes de sécurité comme indiqué à la section « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 100.
- ❒ 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 OpenText eDirectory/ OpenText Identity Console 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, consultez Configuration d'OpenSLP pour OpenText eDirectory dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

## Procédure d'installation et de configuration

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

- EBA est activé.
- SNMP est désactivé.
- OpenText 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 OpenText 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'OpenText 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 OpenText 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 OpenText eDirectory. Pour plus d'informations, reportez-vous à la section Exécution de l'utilitaire nds-install pour installer des composants OpenText eDirectory.
3. Configurez OpenText eDirectory. Pour plus d'informations, reportez-vous à la section Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques OpenText eDirectory. Voici un exemple de commande qui permet d'installer et de configurer OpenText 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'Identity Console***

Grâce à Identity Console, vous pouvez gérer les opérations OpenText eDirectory dans votre environnement Azure. OpenText Identity Console doit être installé sur votre machine virtuelle Azure après avoir installé OpenText eDirectory.

1. Copiez le fichier `IdentityConsole_170_Containers.tar.gz` à l'aide de Secure Copy (scp) vers l'instance du sous-réseau dorsal sur laquelle OpenText Identity Console sera configuré à l'aide du proxy SSH :

   ```
   scp -i <keyname> -o ProxyJump=vm-user@<ssh_proxy_ip>
   IdentityConsole_170_Containers.tar.gz vm-user@<instance_ip>:/<directory>
   ```

2. Installez et configurez OpenText Identity Console. Pour plus d'informations, voir Installation du poste de travail OpenText Identity Console sous Windows. Avant d'installer OpenText Identity Console, consultez la section Configuration système requise et conditions préalables concernant l'installation en mode Poste de travail du Guide d'installation d'OpenText™ Identity Console.
3. Remplacez les certificats auto-signés dans la machine virtuelle exécutant Identity Console par des certificats signés par une autorité de certification sécurisée. Pour plus d'informations, reportez-vous à la section Remplacement des certificats auto-signés temporaires pour OpenText iManager.

***Lancement d'OpenText Identity Console***

Pour lancer OpenText Identity Console, procédez comme suit :

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 et connectez-vous à l'arborescence OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.
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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.
3. Configurez la clé d'arborescence AES 256 bits pour le premier serveur OpenText 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 OpenText eDirectory. L'accès LDAP non sécurisé sur le port 389 étant désactivé sur tous les serveurs OpenText 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 OpenText Identity Console en tant qu'administrateur.
   - **4b** Accédez à **Gestion des certificats** > **Gestion des AC** > **CRL** > Créer les CRL .

**4c** 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).

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

**4e** 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).

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

**5** Réparez les certificats par défaut du serveur à l'aide du gestionnaire de certificats OpenText Identity Console. Pour cela, procédez comme suit :

**5a** Connectez-vous à OpenText Identity Console en tant qu'administrateur.

**5b** Accédez à **Gestion des certificats > > Certificat 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** > **OK**.

**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 Suite B dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*. Une fois l'opération terminée, redémarrez OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

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

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

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

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

**9a2** Redémarrez OpenText eDirectory.

**9b** Procédez comme suit pour désactiver la pile HTTP dans les serveurs de répliques OpenText 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 OpenText 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, consultez Paramètres de configuration dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

**REMARQUE :** après avoir configuré toutes les machines virtuelles OpenText eDirectory et OpenText Identity Console, 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 OpenText 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 OpenText eDirectory. |

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

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

5. Activez les événements CEF correspondants à partir d'OpenText Identity Console. Pour plus d'informations, reportez-vous à la section Configuration des événements CEF pour l'audit (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/t44e7j6b8ufi.html#t44e7j6cx14i). 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 OpenText 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'OpenText 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 OpenText eDirectory en ignorant la vérification de l'état de santé. Pour plus d'informations, voir *Mise à niveau d'OpenText eDirectory*.

8 Réparez les adresses réseau à l'aide de l'utilitaire `ndsrepair`. Pour plus d'informations, consultez *Options DSRepair* dans le Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).

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 (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/b1j4tpo3.html#b1j581ua) dans le Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).

10 Réparez les certificats par défaut du serveur à l'aide du gestionnaire de certificats OpenText Identity Console. Pour cela, procédez comme suit :

**10a** Connectez-vous à OpenText Identity Console en tant qu'administrateur.

**10b** Accédez à **Gestion des certificats > > Certificat 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** > **OK**.

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

## Déploiement sur une plate-forme Windows

La première étape du déploiement nécessite la préparation des services Azure en vue de leur utilisation avec OpenText eDirectory. Pour plus d'informations, reportez-vous à la section « Préparation des services Azure » page 97. Après avoir créé les services Azure, procédez comme suit :

- « Configuration de groupes de sécurité d'application (ASG) » page 111
- « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 111
- « Création et déploiement de machines virtuelles » page 114

- « Configuration d'un disque de données pour le stockage des données OpenText eDirectory » page 114
- « Installation d'OpenText eDirectory et d'OpenText Identity Console » page 115
- « Reprise après sinistre » page 117

## 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 5-4*** *Groupes de sécurité d'application*

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

## 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.

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

Pour déployer OpenText eDirectory dans Azure, créez les groupes de sécurité réseau suivants : eDirectory_NSG_1, eDirectory_NSG_2 et IdentityConsole_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 OpenText eDirectory.

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | NCP | TCP 524 | Sous-réseau OpenText eDirectory | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic NCP pour OpenText eDirectory dans le sous-réseau OpenText eDirectory. |
| 110 | HTTP CRL | TCP 8028 | Réseau virtuel | eDirectory_CA (ASG) | ALLOW | Nécessaire pour accéder à la liste de révocation de certificats (CRL) de l'arborescence OpenText 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. |
| 120 | LDAPS | TCP 636 | Sous-réseau OpenText eDirectory | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic LDAP sécurisé dans le sous-réseau OpenText eDirectory. |
| 130 | SLP | N'importe laquelle (427) | Sous-réseau OpenText eDirectory | OpenText eDirectory (ASG) | ALLOW | Autorise le trafic SLP dans le sous-réseau OpenText eDirectory. |

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 140 | All Traffic (Tout le trafic) | Toutes | Tout | Tout | DENY | Refuse tout le trafic entrant. |

**REMARQUE**

- Le sous-réseau OpenText eDirectory fait référence à la machine virtuelle sur laquelle OpenText eDirectory est installé.
- Les serveurs OpenText 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 OpenText eDirectory. En outre, l'accès au port HTTP doit uniquement être autorisé dans le groupe de sécurité assigné au serveur OpenText 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 OpenText eDirectory autres que l'autorité de certification de l'arborescence OpenText eDirectory.

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

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

| Priorité | Nom | Plage de ports | Source | Destination | Opération | Description |
|---|---|---|---|---|---|---|
| 100 | HTTPS | TCP 9000 | Réseau virtuel - Sous-réseau | OpenText Identity Console (ASG) | ALLOW | Autorise le trafic HTTP sécurisé pour l'accès au proxy dans le sous-réseau. |
| 110 | All Traffic (Tout le trafic) | Toutes | Tout | Tout | DENY | Refuse tout le trafic entrant. |

## 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 Windows. 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 OpenText eDirectory sera configuré, eDirectory_NSG_2 à la machine virtuelle sur laquelle tous les autres serveurs OpenText eDirectory seront configurés et IdentityConsole_NSG avec la machine virtuelle sur laquelle Identity Console 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 111.

2 Créez un hôte Bastion pour vous connecter à la machine virtuelle Windows.

Pour accéder à la machine virtuelle Windows sur Azure, créez Bastion. Pour plus d'informations sur la configuration de Bastion et la connexion à une machine virtuelle Windows, voir Configuration de Bastion.

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

La configuration d'un disque de données est nécessaire pour éviter la perte des données et de la configuration d'OpenText eDirectory en cas de crash de la machine virtuelle Azure. Pour plus d'informations sur la récupération des données et de la configuration d'OpenText eDirectory,

reportez-vous à la section « Reprise après sinistre » page 117. Une fois la machine virtuelle créée, procédez comme suit pour préparer la machine virtuelle pour le déploiement d'OpenText 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 Windows.
2. Connectez-vous à la machine virtuelle, formatez le disque de données avec le système de fichiers NTFS, puis montez ce disque. Pour plus d'informations sur le formatage et le montage du disque de données, voir Initialiser un nouveau disque de données.

## Installation d'OpenText eDirectory et d'OpenText Identity Console

### Conditions préalables

- ❒ Veillez à respecter la configuration requise indiquée à la section « Configuration système requise » page 73.
- ❒ Créez des groupes de sécurité comme indiqué à la section « Configuration de groupes de sécurité réseau pour une machine virtuelle » page 111.
- ❒ Choisissez une taille de machine virtuelle dont les performances et la mémoire sont adaptées à cette instance.
- ❒ Configurez le disque de données pour le stockage des données OpenText eDirectory.
- ❒ Configurez Bastion pour qu'il se connecte à la machine virtuelle Windows.

### Procédure d'installation et de configuration

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

- EBA est activé.
- SNMP est désactivé.
- OpenText eDirectory n'écoute pas le port 389.
- Les services LDAP et HTTP sont configurés pour utiliser les certificats ECDSA uniquement.
- L'accès au port RDP du sous-réseau des machines virtuelles Azure doit être désactivé lorsqu'il n'est pas utilisé.
- Désactivez les modules OpenText 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'OpenText eDirectory*

1. Téléchargez le fichier `eDirectory_<version>_Windows_x86_64.exe`.
2. Installez eDirectory. Pour plus d'informations, voir Installation ou mise à niveau d'OpenText eDirectory CE 24.4 (v9.3) sous Windows.

***Installation et configuration d'OpenText Identity Console***

Grâce à console d'administration OpenText Identity Console, vous pouvez gérer les opérations OpenText eDirectory dans votre environnement Azure. Identity Console doit être installé sur votre machine virtuelle Azure après avoir installé OpenText eDirectory.

1. Téléchargez le fichier `IdentityConsole_<version>_win_x86_64.zip`.
2. Installez et configurez OpenText Identity Console. Pour plus d'informations, voir Installation d'OpenText Identity Console sous Windows (https://www.netiq.com/documentation/identity-console/identity_console-install/data/t4j68b4oo7x1.html). Avant d'installer OpenText Identity Console, consultez la section Configuration système requise (https://www.netiq.com/documentation/identity-console/identity_console-install/data/t4ja6mu8vquv.html) du Guide d'installation d'OpenText Identity Console. (https://www.netiq.com/documentation/identity-console/identity_console-install/data/bookinfo.html)

***Lancement d'OpenText Identity Console***

Pour lancer OpenText Identity Console, procédez comme suit :

1. Ouvrez l'interface utilisateur hôte Bastion.
2. Lancez OpenText Identity Console dans un nouvel onglet de navigateur.
3. Entrez le port et l'URL d'OpenText Identity Console.

## 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.
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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.
3. Configurez la clé d'arborescence AES 256 bits pour le premier serveur OpenText 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 OpenText eDirectory. L'accès LDAP non sécurisé sur le port 389 étant désactivé sur tous les serveurs OpenText 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 OpenText Identity Console en tant qu'administrateur.
   - **4b** Accédez à **Gestion des certificats** > **Gestion des AC** > **CRL** > Créer les CRL .
   - **4c** 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).
   - **4d** Cliquez sur **Enregistrer**, puis sur **OK**.
   - **4e** 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).
   - **4f** Cliquez sur **Enregistrer**, puis sur **OK**.

5 Réparez les certificats par défaut du serveur à l'aide du gestionnaire de certificats OpenText Identity Console. Pour cela, procédez comme suit :

   **5a** Connectez-vous à OpenText Identity Console en tant qu'administrateur.

   **5b** Accédez à **Gestion des certificats > > Certificat 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** > **OK**.

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 Suite B dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*. Une fois l'opération terminée, redémarrez OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

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

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

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

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

      **9a2** Redémarrez OpenText eDirectory.

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

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

      **9b2** Redémarrez OpenText 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 OpenText 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, consultez Paramètres de configuration dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

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

## Reprise après sinistre

Procédez comme suit pour effectuer une reprise après sinistre sur une machine virtuelle Windows :

**REMARQUE :** Il est recommandé de sauvegarder les fichiers nici à l'aide de la sauvegarde dsbk après la configuration d'une arborescence. Pour plus d'informations, reportez-vous à la section Plan de reprise d'activité sous Windows.

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 Windows.
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'OpenText eDirectory dans la nouvelle machine virtuelle.
4. Copiez les fichiers de sauvegarde dsbk avec la sauvegarde nici sur la nouvelle machine virtuelle. Arrêtez les services ndsd et exécutez la restauration dsbk avec nici.
5. 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 Windows.
6. Démarrez les services ndsd sur la nouvelle machine virtuelle.
7. Mettez à niveau OpenText eDirectory. Pour plus d'informations, voir *Mise à niveau d'OpenText eDirectory* dans le Guide d'installation d'OpenText™ eDirectory CE 24.4 (v9.3).
8. Réparez les adresses réseau à l'aide de l'utilitaire `ndsrepair`. Pour plus d'informations, consultez Options DSRepair dans le Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).
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 (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/b1j4tpo3.html#b1j581ua) dans le Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).
10. Réparez les certificats par défaut du serveur à l'aide du gestionnaire de certificats OpenText Identity Console. Pour cela, procédez comme suit :
    - **10a** Connectez-vous à OpenText Identity Console en tant qu'administrateur.
    - **10b** Accédez à **Gestion des certificats > > Certificat 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** > **OK**.
11. Configurez les services LDAP et HTTP pour qu'ils utilisent les nouveaux certificats ECDSA.

# Déploiement d'un conteneur OpenText eDirectory sur une instance de conteneur Microsoft Azure

OpenText eDirectory prend en charge le déploiement de conteneurs OpenText eDirectory sur une instance de conteneur Microsoft Azure. Le processus de déploiement est simple et rapide. Le conteneur OpenText eDirectory est distribué dans le registre en tant qu'image Docker autonome et capable de s'exécuter seule. Cette section vous guide tout au long du processus de déploiement de l'image Docker d'OpenText eDirectory sous Azure.

## Liste de contrôle pour le déploiement du conteneur

Pour configurer le conteneur Azure pour le déploiement, nous vous recommandons d'effectuer les étapes de la liste de contrôle suivante :

| | **Éléments de la liste de vérifications** |
|---|---|
| ❑ | 1. Vous devez créer un registre de conteneurs Azure pour stocker et gérer l'image du conteneur Docker pour OpenText eDirectory. Connectez-vous au portail Azure sur https://portal.azure.com/ et suivez les étapes du processus Créer un registre de conteneurs Azure à l'aide du portail Azure pour créer un registre de conteneurs. |
| ❑ | 2. Vous devez ensuite configurer un compte de stockage Azure. Ce compte stocke toutes vos données accessibles à partir de n'importe quel endroit dans le monde via HTTP ou HTTPS. Connectez-vous au portail Azure et suivez les étapes du processusCréer un compte de stockage pour créer un compte de stockage Azure. |
| ❑ | 3. Après avoir créé le compte de stockage, créez un partage de fichiers Azure. Un système de fichiers partagé est requis pour permettre aux conteneurs d'accéder au système de fichiers, quelle que soit l'instance sur laquelle ils s'exécutent. Pour plus d'informations sur les considérations et le processus à suivre lors de la création d'un partage de fichiers Azure, consultez Créer un partage de fichiers Azure. |
| ❑ | 4. Vous devez créer 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 Azure Internet et avec les réseaux locaux. Suivez les étapes du processus Création d'un réseau virtuel. |
| ❑ | 5. Ensuite, distribuez l'image Docker d'OpenText eDirectory vers le registre des conteneurs. Pour plus d'informations, reportez-vous à la section « Distribuez l'image Docker vers le registre de conteneurs Azure » page 120. |
| ❑ | 6. Éditez et enregistrez le fichier YAML fourni avec le tarball d'image Docker pour OpenText eDirectory. Pour plus d'informations, reportez-vous à la section « Édition du fichier de configuration YAML » page 120. |
| ❑ | 7. Enfin, créez une instance de conteneur Azure à l'aide du fichier YAML. Pour plus d'informations, reportez-vous à la section « Création d'une instance de conteneur Azure » page 125. |

## Distribuez l'image Docker vers le registre de conteneurs Azure

**Pour distribuer l'image Docker dans le registre des conteneurs Azure :**

1. Téléchargez le tarball d'image Docker pour OpenText eDirectory à partir du portail Licence de logiciel et téléchargement.
2. Désarchivez le build téléchargé, extrayez l'image Docker, puis chargez-la dans le registre Docker local à l'aide des commandes suivantes :

   ```
   tar -xvf eDirectory_93x_Container.tar.gz
   docker load --input eDirectory_93x/eDirectory_93x.tar.gz
   ```

   La commande de chargement de Docker charge l'image Docker nommée `edirectory:9.3.x` à partir de l'archive tar.
3. Marquez l'image Docker avec le nom de votre registre à l'aide de la commande suivante :

   ```
   Docker tag edirectory:<image-id> <registry-name>.azurecr.io/
   <repository-name-tag>
   ```

   Où

   `edirectory :<image-id>` est 'ID d'image Docker local.

   `<registry-name>` est le nom de votre registre privé.

   `<repository-name-tag>` est la balise que vous voulez assigner à l'image Docker.

   Par exemple, `docker tag edirectory:93x myazureregistry.azurecr.io/edir93`
4. Distribuez l'image Docker vers le registre à l'aide de la commande suivante :

   ```
   docker push <registry-name>.azurecr.io/<repository-name-tag>
   ```

   Où

   `<registry-name>` est le nom de votre registre privé.

   `<repository-name-tag>` est la balise que vous avez assignée à l'image Docker.

   Par exemple, `docker push myazureregistry.azurecr.io/edir93x`

## Édition du fichier de configuration YAML

Un fichier YAML est un moyen simple et rapide de créer ou de mettre à jour un groupe de conteneurs. La commande `az container create` dans l'interface de ligne de commande Azure lit les configurations de groupe à partir d'un fichier YAML. Vous devez éditer et télécharger le fichier YAML fourni avec le tarball de l'image Docker pour OpenText eDirectory avant de créer une instance de conteneur Azure.

La section suivante présente le schéma d'un fichier YAML, y compris les commentaires (indiqués par le symbole #) qui mettent en surbrillance les propriétés des clés. Pour obtenir une description des propriétés de ce schéma, consultez la section Valeurs des propriétés.

```
name:  # Provide the name of the container group
apiVersion: '2019-12-01'
properties: # Properties of container group
  containers: # The containers within the container group
  - name: test-edir93 # Provide a name of container instance
    properties: # Properties of a container instance
      image: myazureregistry.azurecr.io/edir93 # Provide the name of the
container image used to create the container instance
      command:
      - /start.sh #Not optional
      - 'new -t 93edir1 -n novell -a admin.novell -w xx -S server1 -i -B
@1524 -o 1028 -O 1030 -L 1389 -l 1636 --configure-eba-now no' #Sample
command
     ports: # External-facing ports exposed on the instance, must also be
set in group ipAddress property
      - protocol: tcp
       port: 1030 #HTTPS port. Depends on the parameter provided in command
for -O
      - protocol: tcp
       port: 1389 #LDAP port. Depends on the parameter provided in command
for -L
      environmentVariables:
      - name: YAML_MODE #Mandatory variable. Required if yaml file is used
for configuring edirectory
        value: '1'
      resources: # Minimum resource requirements of the instance
        requests:
          memoryInGB: 2
          cpu: 1.5
      volumeMounts: # Array of volume mounts for the instance
      - name: configvolume
        mountPath: /config #Mandatory. Do not change this path.
  imageRegistryCredentials: # Credentials to pull a private image
  - server: myazureregistry.azurecr.io #Provide the image registry server
name
    username: myazureregistry #Provide the image registry username
password: xxxx #Provide the image registry password
  #restartPolicy: Never #Optional
  ipAddress: # IP address configuration of container group
    ports:
    - protocol: tcp
      port: 1030 #HTTPS port. Depends on the parameter provided in command
for -O
    - protocol: tcp
      port: 1389 #LDAP port. Depends on the parameter provided in command
for -L
    type: Private
  networkProfile: # Virtual network profile for container group
```

```
    id: subscriptions/xxx-xxx-xxx/resourceGroups/myresourcegroup/
providers/Microsoft.Network/networkProfiles/aci-network-profile-
VirtualNetmy-containersubnet
#Can be found by running the command, az network profile list --resource-
group myResourceGroup --query [0].id --output tsv, if no output then run
the first time using azure cloud shell
  osType: Linux
  volumes: # Array of volumes available to the instances
  - name: configvolume
    azureFile:
      shareName: testshare  #Provide the name of the Azure File share to be
mounted as a volume
      storageAccountName: myfileshare  #Provide name of the storage account
       storageAccountKey: xxx_xxx #Provide storage account access key
```

## Valeurs des propriétés

Les tableaux suivants décrivent les valeurs à définir dans le schéma.

| Nom | Type | Requis | Valeur |
|---|---|---|---|
| Objet **`containerGroups`** | | | |
| Nom | Chaîne | Oui | Nom du groupe de conteneurs. Vous pouvez également fournir un nom de conteneur. |
| apiVersion | énuméré | Oui | Version d'API de ressource. Par exemple, « 2019-12-01 ». |
| propriétés | objet | Oui | Propriétés d'un groupe de conteneurs. Recherchez l'objet `ContainerGroupProperties` dans cette table pour trouver les valeurs prises en charge pour les propriétés. |
| Objet **`ContainerGroupProperties`** | | | |
| conteneurs | tableau | Oui | Conteneurs dans le groupe de conteneurs. Recherchez l'objet `Container` dans cette table pour trouver les valeurs prises en charge pour les conteneurs. |
| imageRegistryCredentials | tableau | Non | Informations d'identification du registre d'images à partir des lesquelles le groupe de conteneurs est créé. Recherchez l'objet `ImageRegistryCredential` dans cette table pour trouver les valeurs prises en charge pour imageRegistryCredentials. |
| restartPolicy | énuméré | Non | Redémarrez la stratégie pour tous les conteneurs au sein du groupe de conteneurs :<br>◆ - Always : toujours redémarrer<br>◆ - OnFailure : redémarre en cas d'échec<br>◆ - Never : ne jamais redémarrer |

| Nom | Type | Requis | Valeur |
|---|---|---|---|
| ipAddress | objet | Non | Type d'adresse IP du groupe de conteneurs. Recherchez l'objet `IPAddress` dans cette table pour trouver les valeurs prises en charge pour ipAddress. |
| osType | énuméré | Oui | Type de système d'exploitation requis par les conteneurs du groupe de conteneurs. - Windows ou Linux |
| le faire | tableau | Non | Liste des volumes qui peuvent être montés par des conteneurs dans ce groupe de conteneurs. Recherchez l'objet `Volume` dans cette table pour trouver les valeurs prises en charge pour les volumes. |
| **Objet Conteneur** | | | |
| name | chaîne | Oui | Nom fourni par l'utilisateur de l'instance de conteneur. Par exemple, `test-edir93`. |
| propriétés | objet | Oui | Propriétés de l'instance de conteneur. Recherchez l'objet `ContainerProperties` dans cette table pour trouver les valeurs prises en charge pour les propriétés. |
| Objet **`ContainerProperties`** | | | |
| Image | chaîne | Oui | Nom de l'image utilisée pour créer l'instance de conteneur. Par exemple, `myazureregistry.azurecr.io/edir93` (Étape 3). |
| command | tableau | Non | Commandes à exécuter dans l'instance de conteneur sous la forme exec. Le conteneur Docker pour OpenText eDirectory accepte les paramètres de l'utilitaire `ndsconfig` avec la commande Docker. Pour plus d'informations sur l'utilitaire `ndsconfig`, reportez-vous à la section « Utilitaire ndsconfig » page 177. |
| ports | tableau | Non | Ports exposés sur l'instance de conteneur. Recherchez l'objet `ContainerPort` dans cette table pour trouver les valeurs prises en charge pour les ports. |
| environmentVariables | tableau | Non | Variables d'environnement à définir dans l'instance de conteneur. Recherchez l'objet `EnvironmentVariable` dans cette table pour trouver les valeurs prises en charge pour environmentVariables. |
| ressources | objet | Oui | Les exigeznces de ressource pour l'instance de conteneur. Recherchez l'objet `ResourceRequirements` dans cette table pour trouver les valeurs prises en charge pour les ressources. |

| Nom | Type | Requis | Valeur |
|---|---|---|---|
| volumeMounts | tableau | Non | Les montages de volume à la disposition de l'instance de conteneur. Recherchez l'objet `VolumeMount` dans cette table pour trouver les valeurs prises en charge pour volumeMounts. |
| Objet **`ContainerPort`** | | | |
| protocole | énuméré | Non | Protocole associé au port. - TCP ou UDP |
| port | entier | Oui | Numéro de port. |
| Objet **`EnvironmentVariable`** | | | |
| name | chaîne | Oui | Nom de la variable d'environnement. |
| value | chaîne | Non | Valeur de la variable d'environnement. |
| Objet **`ResourceRequirements`** | | | |
| requêtes | objet | Oui | Requêtes de ressource de cette instance de conteneur. Recherchez l'objet `ResourceRequests` dans cette table pour trouver les valeurs prises en charge pour les requêtes. |
| Objet **`ResourceRequests`** | | | |
| memoryInGB | number | Oui | Requête de mémoire en Go de cette instance de conteneur. |
| cpu | number | Oui | Requête d'UC de cette instance de conteneur. |
| Objet **`VolumeMount`** | | | |
| name | chaîne | Oui | Nom du montage de volume. |
| mountPath | chaîne | Oui | Chemin d'accès au conteneur dans lequel le volume doit être monté. Ne doit pas contenir de signe deux-points (:). |
| Objet **`ImageRegistryCredential`** | | | |
| server | chaîne | Oui | Le serveur de registre d'images Docker sans protocole tel que « http » et « https ». Entrez le nom du registre créé à l'étape 1 de la liste de contrôle (voir Liste de contrôle pour le déploiement du conteneur). |
| username | chaîne | Non | Nom d'utilisateur pour le registre privé. Pour plus d'informations, voir Comment rechercher des informations sur le nom d'utilisateur. |
| password | chaîne | Non | Mot de passe pour le registre privé. Pour plus d'informations, voir Comment rechercher le mot de passe du registre Azure. |
| Objet **`Adresse IP`** | | | |
| ports | tableau | Oui | Liste des ports exposés sur le groupe de conteneurs. Recherchez l'objet `Port` dans cette table pour trouver les valeurs prises en charge pour les ports. |

| Nom | Type | Requis | Valeur |
|---|---|---|---|
| type | énuméré | Oui | Indique si l'adresse IP est exposée à l'Internet public ou au réseau VNET privé. - Public ou Privé |
| Objet **`Port`** | | | |
| protocole | énuméré | Non | Protocole associé au port. - TCP ou UDP |
| port | entier | Oui | Numéro de port. |
| **objet Volume** | | | |
| name | chaîne | Oui | Nom du volume. |
| azureFile | objet | Non | Volume de fichiers Azure. Recherchez l'objet `AzureFileVolume` dans ce tableau pour trouver les valeurs prises en charge pour azureFile. |
| Objet **`AzureFileVolume`** | | | |
| shareName | chaîne | Oui | Nom du partage de fichiers Azure à monter en tant que volume. Entrez le nom du partage de fichiers de stockage créé à l'étape 3 de la liste de contrôle (voir Liste de contrôle pour le déploiement du conteneur). |
| storageAccountName | chaîne | Oui | Nom du compte de stockage qui contient le partage de fichiers Azure. |
| storageAccountKey | chaîne | Non | Clé d'accès au compte de stockage utilisée pour accéder au partage de fichiers Azure. Pour trouver la clé de compte de stockage, voir Afficher les clés d'accès au compte. |

## Création d'une instance de conteneur Azure

Exécutez la commande suivante pour créer un conteneur dans un groupe de conteneurs à l'aide du fichier YAML que vous avez modifié précédemment :

```
az container create --resource-group <MyResourceGroup> --name <container-instance-name>  --file <containerGroup.yaml>
```

Où

`<MyResourceGroup>` représente le nom du groupe de ressources. Champ obligatoire.

`<container-instance-name>` représente le nom de l'instance de conteneur dans un groupe de conteneurs.

`<containerGroup.yaml>` représente le chemin d'accès au fichier d'entrée.

Par exemple, `az container create --resource-group MyResourcegroup --name edir93 --file edir-azure-conf.yaml`

# 6 Déploiement d'OpenText eDirectory sur Amazon Web Services EC2

OpenText eDirectory peut être déployé sur des instances Amazon Web Services (AWS) EC2. Pour plus d'informations sur les systèmes d'exploitation pris en charge, reportez-vous à la section « Configuration système requise » page 29.

Les sections suivantes expliquent les différentes conditions préalables et la procédure de déploiement d'OpenText eDirectory sur AWS :


- « Conditions préalables » page 127
- « Procédure de déploiement » page 127
- « Guide de taille pour le déploiement d'OpenText eDirectory sur AWS » page 141


## Conditions préalables

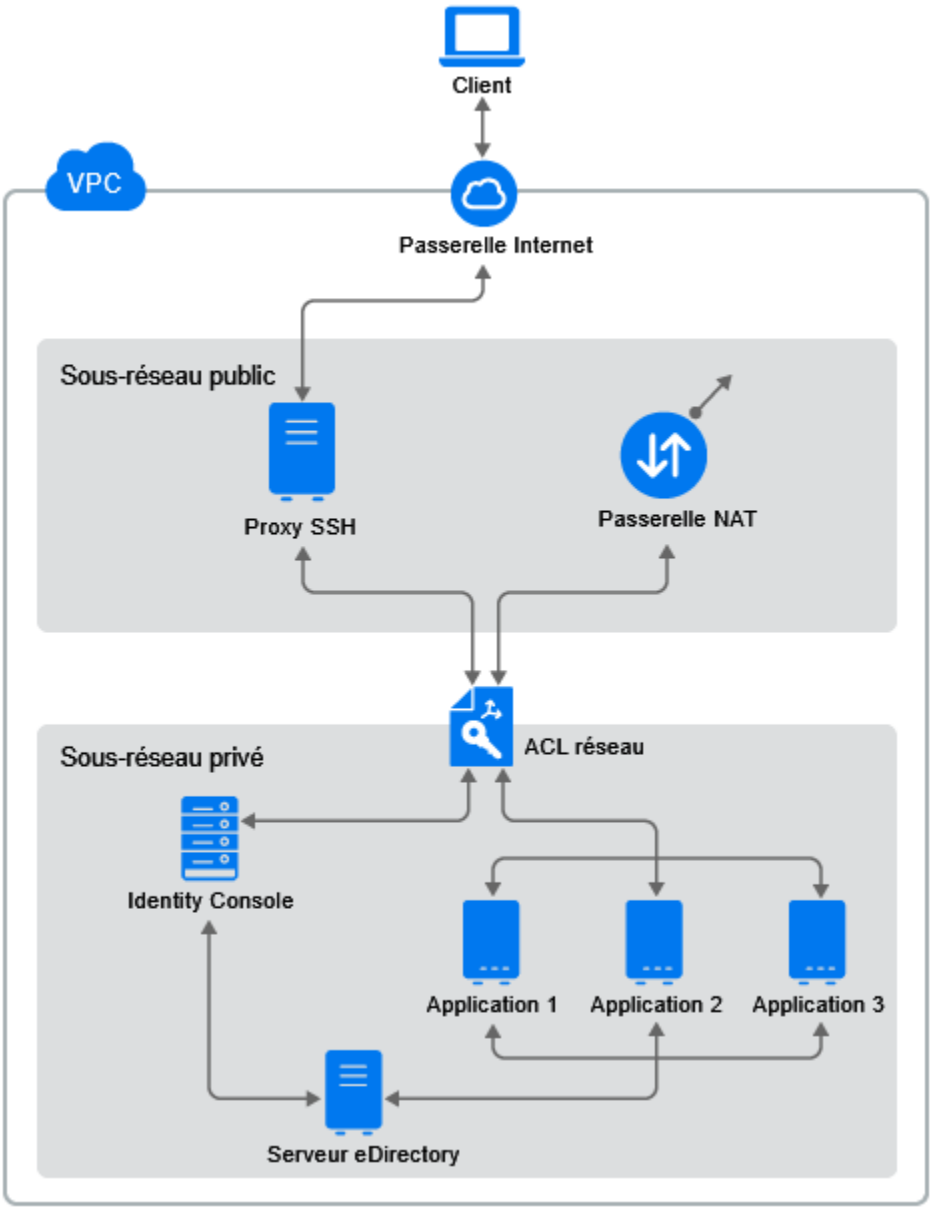
En plus de la configuration système d'OpenText eDirectory, veillez à respecter les exigences suivantes :

- Vous disposez d'un compte administratif sur AWS EC2.
- Le programme d'installation d'OpenText 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

OpenText eDirectory ne doit être déployé que dans un sous-réseau privé dans Amazon VPC. La Figure 5-1 illustre un exemple de déploiement utilisé dans les sections suivantes.

***Figure 6-1*** *Déploiement d'OpenText 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'accéder à OpenText 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 du cloud privé virtuel AWS » page 129
- « Configuration des ACL réseau » page 130
- « Configuration des groupes de sécurité » page 132
- « Création d'une paire de clés SSH » page 133
- « Création et déploiement d'instances » page 134
- « Configuration d'un volume EBS pour le stockage des données OpenText eDirectory » page 134
- « Installation d'OpenText eDirectory et d'OpenText Identity Console » page 135
- « Déploiement des services d'audit » page 139
- « Reprise après sinistre » page 140


## Préparation du cloud privé virtuel AWS

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

Effectuez les étapes suivantes pour créer des 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. OpenText eDirectory doit être déployé dans le sous-réseau privé. Comme illustré à la Figure 5-1, toutes les applications qui accèdent à OpenText 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 (https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html). |
| **Passerelles Internet** | Une passerelle Internet est nécessaire pour activer la connexion SSH au proxy SSH, comme illustré à la Figure 5-1. 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. |

| Service | Description |
|---|---|
| **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, voir Association d'adresses IP Elastic à des ressources dans votre VPC (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-eips.html#WorkWithEIPs). |

## 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 6-1***

| 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 9000 | *<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. |

| Règle | Type | Plage de ports | Source | Opération | Description |
|---|---|---|---|---|---|
| * | 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 6-2***

| 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 Identity Console 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. |

| Règle | Type | Plage de ports | Destination | Opération | Description |
|---|---|---|---|---|---|
| 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 au document Amazon EC2 Security Groups for Linux Instances (Groupes de sécurité Amazon EC2 pour les instances Linux).

Pour déployer OpenText 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 OpenText eDirectory. Le port HTTP ne doit être activé que dans le groupe de sécurité assigné au serveur OpenText 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 OpenText 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 OpenText eDirectory qui héberge l'autorité de certification de l'arborescence. |

3. **Groupe de sécurité 3 (pour Identity Console) :**

| Port | Source | Description |
|---|---|---|
| TCP 22 | Sous-réseau public | Autorise le trafic SSH depuis le sous-réseau public. |
| TCP 9000 | Sous-réseau public | Autorise le trafic HTTPS pour l'accès à Identity Console 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 (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-key-pairs.html).

**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 OpenText eDirectory sera configuré, le groupe de sécurité 2 à l'instance dans laquelle tous les autres serveurs OpenText 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 100.
2. Associez la clé publique créée à la section « Création d'une paire de clés SSH » page 103 à vos instances.

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

La configuration d'un volume EBS est nécessaire pour éviter la perte des données et de la configuration d'OpenText eDirectory en cas de crash d'une instance EC2. Pour plus d'informations sur la récupération des données et de la configuration d'OpenText eDirectory, reportez-vous à la section « Reprise après sinistre » page 140. Une fois l'instance EC2 créée, procédez comme suit pour préparer l'instance pour le déploiement d'OpenText 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 OpenText eDirectory/NICI. Procédez comme suit en tant qu'utilisateur root pour effectuer le montage de liaison :
   - **4a** Créez le répertoire de données OpenText 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 OpenText eDirectory à l'aide de la commande suivante :

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

   - **4d** Créez les répertoires nécessaires pour OpenText 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'OpenText eDirectory et d'OpenText Identity Console

## 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 100.
- ❒ 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 OpenText eDirectory/OpenText Identity Console 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, consultez Configuration d'OpenSLP pour OpenText eDirectory dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

## Procédure d'installation et de configuration

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

- EBA est activé.
- SNMP est désactivé.
- OpenText 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 OpenText 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'OpenText 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 OpenText 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 OpenText eDirectory. Pour plus d'informations, reportez-vous à la section Exécution de l'utilitaire nds-install pour installer des composants OpenText eDirectory.
3. Configurez OpenText eDirectory. Pour plus d'informations, reportez-vous à la section Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques OpenText eDirectory. Voici un exemple de commande qui permet d'installer et de configurer OpenText 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'OpenText Identity Console

Grâce à la console d'administration d'OpenText Identity Console, vous pouvez gérer les opérations OpenText eDirectory dans votre environnement AWS. OpenText Identity Console doit être installé sur votre instance AWS après avoir installé OpenText eDirectory.

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

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

2. Installez et configurez OpenText Identity Console. Pour plus d'informations, voir Installation d'OpenText Identity Console en mode autonome (non-Docker). Avant d'installer OpenText Identity Console, consultez la section Configuration système requise et conditions préalables concernant l'installation en mode Poste de travail du Guide d'installation d'OpenText™ Identity Console.
3. Remplacez les certificats auto-signés dans la machine virtuelle exécutant Identity Console par des certificats signés par une autorité de certification sécurisée. Pour plus d'informations, reportez-vous à la section Remplacement des certificats auto-signés temporaires pour iManager.

---

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

---

### Lancement d'OpenText Identity Console

Pour lancer OpenText Identity Console, procédez comme suit :

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 OpenText Identity Console et connectez-vous à l'arborescence OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.
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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.
3. Configurez la clé d'arborescence AES 256 bits pour le premier serveur OpenText 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 OpenText eDirectory. L'accès LDAP non sécurisé sur le port 389 étant désactivé sur tous les serveurs OpenText 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 OpenText Identity Console en tant qu'administrateur.

   **4b** Accédez à **Gestion des certificats** > **Gestion des AC** > **CRL** > Créer les CRL .

   **4c** 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).

   **4d** Cliquez sur **Enregistrer**, puis sur **OK**.

   **4e** 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).

   **4f** Cliquez sur **Enregistrer**, puis sur **OK**.

5 Réparez les certificats par défaut du serveur à l'aide du gestionnaire de certificats OpenText Identity Console. Pour cela, procédez comme suit :

   **5a** Connectez-vous à OpenText Identity Console en tant qu'administrateur.

   **5b** Accédez à **Gestion des certificats > > Certificat 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** > **OK**.

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 Suite B dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*. Une fois l'opération terminée, redémarrez OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

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

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

   **9a** Procédez comme suit pour désactiver OpenText 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 OpenText 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 OpenText 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 OpenText 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, consultez Paramètres de configuration dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

**REMARQUE :** Après avoir configuré toutes les instances OpenText eDirectory et OpenText Identity Console, 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 OpenText 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 OpenText eDirectory. |

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

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

5 Activez les événements CEF correspondants à partir d'OpenText Identity Console. Pour plus d'informations, reportez-vous à la section Configuration des événements CEF pour l'audit (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/t44e7j6b8ufi.html#t44e7j6cx14i). 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 OpenText 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'OpenText 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 OpenText eDirectory en ignorant la vérification de l'état de santé. Pour plus d'informations, voir *Mise à niveau d'OpenText eDirectory*.
8. Réparez les adresses réseau à l'aide de l'utilitaire `ndsrepair`. Pour plus d'informations, consultez *Options DSRepair* dans le Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).
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 (https://www.netiq.com/documentation/edirectory-93/edir_admin/data/b1j4tpo3.html#b1j581ua) dans le Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).
10. Réparez les certificats par défaut du serveur à l'aide du plug-in du serveur de certificats OpenText Identity Console. Pour cela, procédez comme suit :
    - **10a** Connectez-vous à OpenText Identity Console en tant qu'administrateur.
    - **10b** Accédez à **Gestion des certificats > > Certificat 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** > **OK**.
11. Configurez les services LDAP et HTTP pour qu'ils utilisent les nouveaux certificats ECDSA.

# Guide de taille pour le déploiement d'OpenText eDirectory sur AWS

Ce guide recommande l'instance AWS EC2 et le volume EBS les mieux adaptés au déploiement d'OpenText eDirectory sur AWS VPC. Pour vous aider à estimer vos besoins en matière de taille, nous avons fourni les facteurs d'estimation les plus utiles ainsi que divers scénarios de performances, qui sont testés dans un environnement de test contrôlé avec des paramètres de configuration spécifiques.


- « Commencer avec la sélection d'instance AWS EC2 » page 141
- « Détails des environnements de test des performances » page 142
- « Détermination des exigences de taille » page 144


## Commencer avec la sélection d'instance AWS EC2

Avant de déployer OpenText eDirectory sur AWS, vous devez déterminer les types d'instance EC2 et de volume EBS pour obtenir des performances optimales sur votre serveur OpenText eDirectory. Les performances d'OpenText eDirectory dépendent de plusieurs ressources relatives à la manière dont une entreprise envisage de l'utiliser. Voici quelques-unes des ressources à prendre en compte pour votre estimation :

- **Catégorie d'instance AWS EC2 :** vous devez sélectionner la catégorie d'instance appropriée à votre environnement. Nous avons pris en compte les catégories d'instance suivantes pour les différents scénarios de performances de notre environnement de test :
  - Postes de travail génériques
  - Optimisé pour la mémoire
  - Optimisé pour le calcul

  Il est également recommandé d'utiliser des instances EC2 optimisées pour EBS afin de déployer OpenText eDirectory, en vue de bénéficier d'une bande passante dédiée entre l'instance EC2 et le volume EBS associé. Cela permet également une utilisation efficace de l'IOPS prévu sur un volume EBS. Dans certains cas, l'optimisation EBS n'est pas activée par défaut. Dans ce cas, vous devez l'activer manuellement.

- **Type d'instance AWS EC2 :** après avoir sélectionné la catégorie d'instance appropriée pour votre environnement, un type d'instance doit être sélectionné en fonction des besoins commerciaux ou de la charge attendue. AWS propose une large sélection de types d'instance EC2 sous chaque catégorie d'instance. Il existe des sous-catégories sous chaque catégorie en fonction de divers paramètres, tels que le type de processeur ou le débit réseau. Le nombre de coeurs de processeur, le volume de RAM, la capacité réseau et le coût dépendent du type d'instance sélectionné. Pour plus d'informations sur les types d'instance, voir Types d'instance Amazon EC2.

- **Types de volume AWS EBS** : étant donné que le volume racine ou le stockage local dans l'instance EC2 est périssable, vous devez attacher un volume EBS (Elastic Block Storage) AWS à votre instance EC2 pour stocker la DIB OpenText eDirectory et d'autres fichiers serveur qui doivent être conservés. Les volumes EBS vous permettent de conserver les données stockées même après la fin de l'instance AWS EC2, ce qui facilite les scénarios de récupération de données. Les données stockées dans le volume EBS sont répliquées par défaut dans la même zone de disponibilité. Pour plus d'informations, voir Types de volume EBS.

OpenText eDirectory étant un service d'annuaire à lecture intensive, la sélection du type de volume EBS dépendra des E/S disque élevées. Pour cette raison, il est recommandé d'utiliser les types de volume SSD plutôt que les types de volume HDD, car les types de volume SSD gèrent les E/S disque petites ou aléatoires plus efficacement que les types de volume HDD, qui sont essentiellement utilisés pour la lecture en continu des E/S disque.

Le type de volume SSD IOPS prévu (io1 et io2) vous permet de spécifier un taux d'IOPS cohérent lors de la création des types de volume par rapport au type de volume SSD générique (gp2) où les performances peuvent être instables. En outre, le SSD générique reliera la configuration d'IOPS à la taille du disque, ce qui n'existe pas avec les types de volume SSD IOPS prévus.

# Détails des environnements de test des performances

Dans cette section, nous présentons les différents paramètres de configuration, catégories d'instance et types utilisés dans notre environnement de test contrôlé.

## Types d'instance EC2 :

Les types d'instance suivants ont été utilisés lors des tests des performances :

***Tableau 6-3*** *Type d'instance 4xLarge*

| Catégorie | Type | UC | Mémoire | Optimisé pour EBS | Bande passante EBS |
|---|---|---|---|---|---|
| Otimisé pour le calcul | c5a.4xlarge | 16 processeurs, 3,3 GHz | 32 Go | Oui | 3 170 Mbit/s |

***Tableau 6-4*** *Type d'instance 2xLarge*

| Catégorie | Type | UC | Mémoire | Optimisé pour EBS | Bande passante EBS |
|---|---|---|---|---|---|
| Postes de travail génériques | m5a.2xlarge | 8 processeurs, 2,5 GHz | 32 Go | Oui | 2 880 Mbit/s |
| Optimisé pour la mémoire | r5a.2xlarge | 8 processeurs, 2,5 GHz | 64 Go | Oui | 2 880 Mbit/s |
| Otimisé pour le calcul | c5a.2xlarge | 8 processeurs, 3,3 GHz | 16 Go | Oui | 3 170 Mbit/s |

***Tableau 6-5*** *Type d'instance xLarge*

| Catégorie | Type | UC | Mémoire | Optimisé pour EBS | Bande passante EBS |
|---|---|---|---|---|---|
| Postes de travail génériques | m5a.xlarge | 4 processeurs, 2,5 GHz | 16 Go | Oui | 2 880 Mbit/s |
| Optimisé pour la mémoire | r5a.xlarge | 4 processeurs, 2,5 GHz | 64 Go | Oui | 2 880 Mbit/s |
| Otimisé pour le calcul | c5a.xlarge | 4 processeurs, 3,3 GHz | 8 Go | Oui | 3 170 Mbit/s |

## Paramètres courants

***Tableau 6-6*** *Explication des paramètres courants*

| Paramètre | Description |
|---|---|
| Détails du VPC AWS | Un sous-réseau public et un sous-réseau privé. Client et OpenText eDirectory sont tous deux dans le sous-réseau privé VPC. |
| Détails de l'instance EC2 OpenText eDirectory | ◆ **Système d'exploitation**: serveur SUSE Enterprise Linux 15 SP2 (HVM), type de volume SSD<br>◆ **Build OpenText eDirectory** : OpenText eDirectory 9.2<br>◆ **Elastic Block Storage** : SSD IOPS prévu io2, 100 Go, IOPS – 1 000<br>◆ **Dib** : 3 Go, plus de 2 millions d'utilisateurs |
| Opérations | ◆ **Opération** : opérations de recherche et de modification LDAPS (636)<br>◆ **Pourcentage :**80 % d'opérations en lecture et 20 % en écriture.<br>◆ **Étendue de la recherche** : recherche dans la sous-arborescence<br>◆ **Base de recherche** : ou=users,o=novell<br>◆ **Filtre de recherche**: utilisateur aléatoire sous Base de recherche<br>◆ **Attributs**: sn;title |
| Optimisation d'OpenText eDirectory | **Paramètre OpenText eDirectory Flaim DB :**<br>preallocatecache=true<br>cache=4000000000cpinterval=360 |

| Paramètre | Description |
| --- | --- |
| Instance EC2 client LDAP | ◆ **Système d'exploitation** : RHEL8.0<br>◆ **Outil client LDAP** : JMeter 5.1<br>◆ **Type d'instance EC2** : m5d.4xlarge, 16 processeurs, 64 Go de RAM<br>◆ **Plage de ports TCP** : 1024-65534 |

# Détermination des exigences de taille

Dans cette section, nous présentons nos recommandations sur la base des données de performances pour les scénarios couramment utilisés. Ces données vous aideront à déterminer l'instance AWS EC2 optimale pour votre environnement. Avant de commencer avec l'estimation de taille appropriée pour votre déploiement OpenText eDirectory, vous devez identifier la catégorie d'instance la mieux adaptée à votre déploiement.

## Scénario n° 1 : identification de la catégorie d'instance AWS EC2

Dans ce scénario de performances, nous déterminerons la catégorie d'instance AWS EC2 appropriée pour le déploiement et les opérations d'OpenText eDirectory.

Les graphiques ci-dessous représentent respectivement le temps de réponse moyen (en millisecondes) et des opérations par seconde par rapport au nombre de threads. La mesure a été calculée à partir de trois catégories d'instances : Utilisation générique, Optimisé pour la mémoire et Optimisé pour le calcul, qui appartiennent au type d'instance 2xlarge.

***Figure 6-2*** *Modification du temps de réponse moyen en fonction du nombre de threads exécutés simultanément pour m5a par rapport à r5a et à c5a*

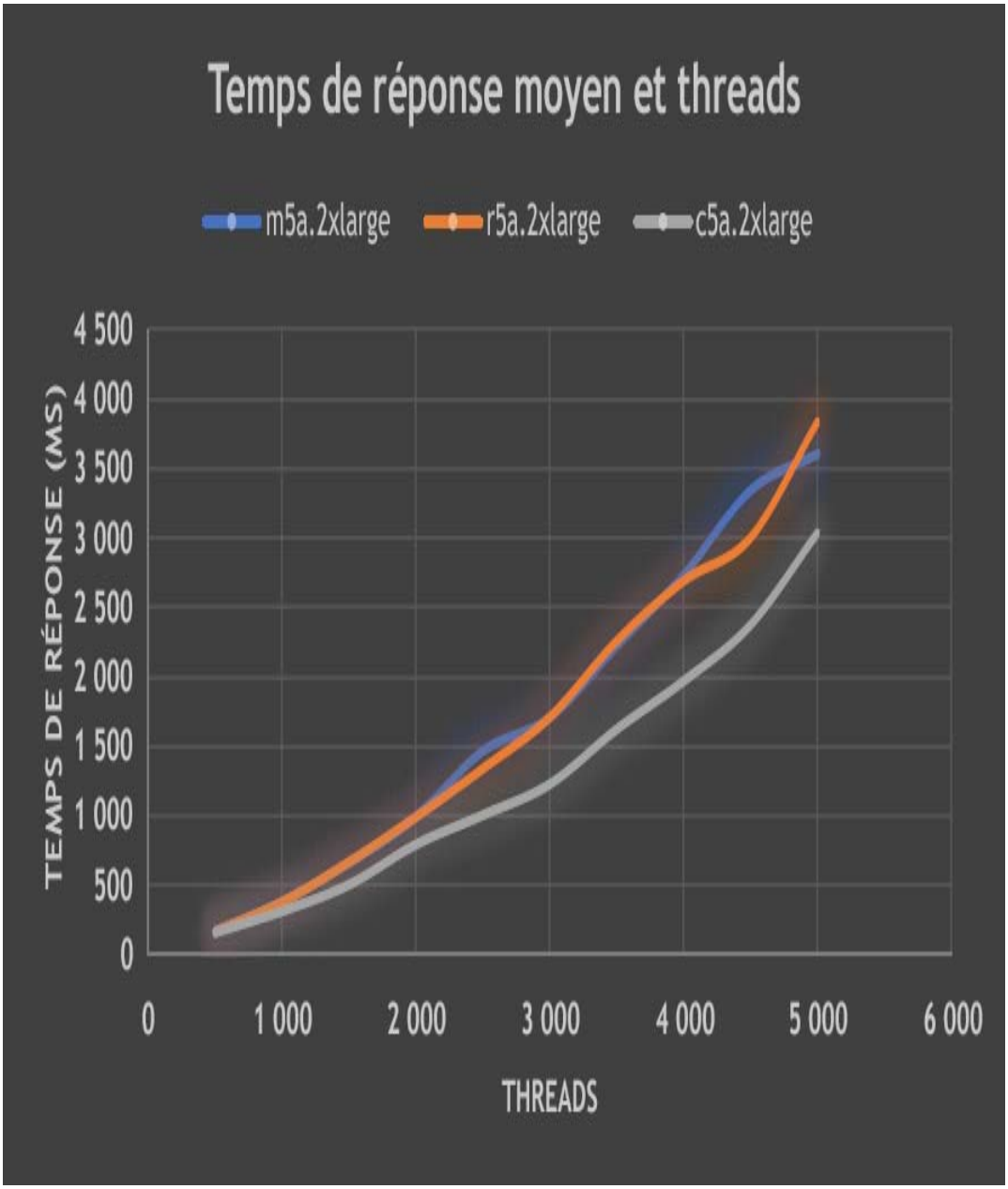
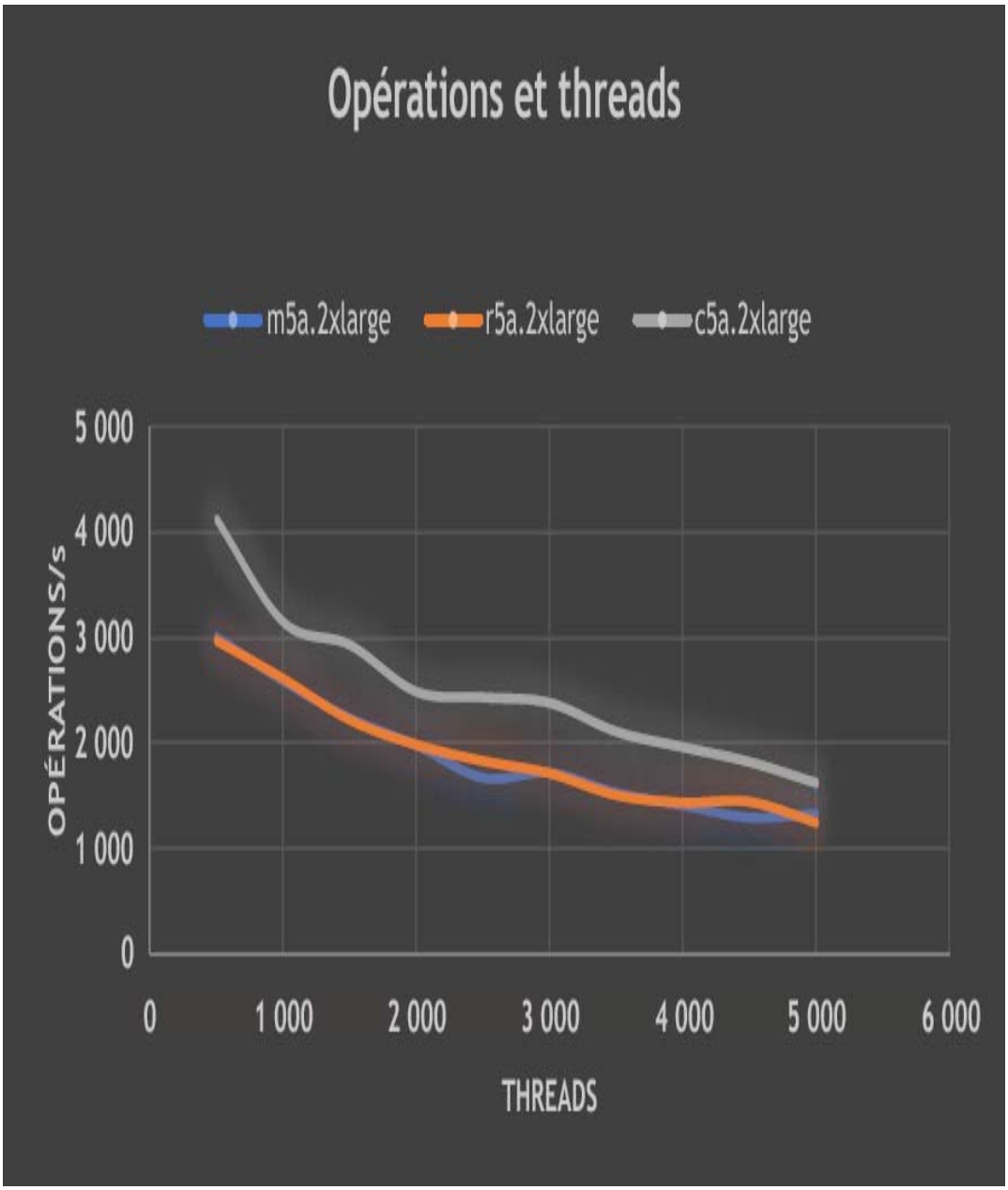


***Figure 6-3*** *Modification du nombre d'opérations exécutées simultanément en fonction du nombre de threads*




Les graphiques ci-dessous représentent respectivement le temps de réponse moyen (en millisecondes) et des opérations par seconde par rapport au nombre de threads. La mesure a été calculée à partir de trois catégories d'instances : Utilisation générique, Optimisé pour la mémoire et Optimisé pour le calcul, qui appartiennent au type xlarge.

***Figure 6-4*** *Modification du temps de réponse moyen en fonction du nombre de threads exécutés simultanément pour m5a par rapport à r5a et à c5a*

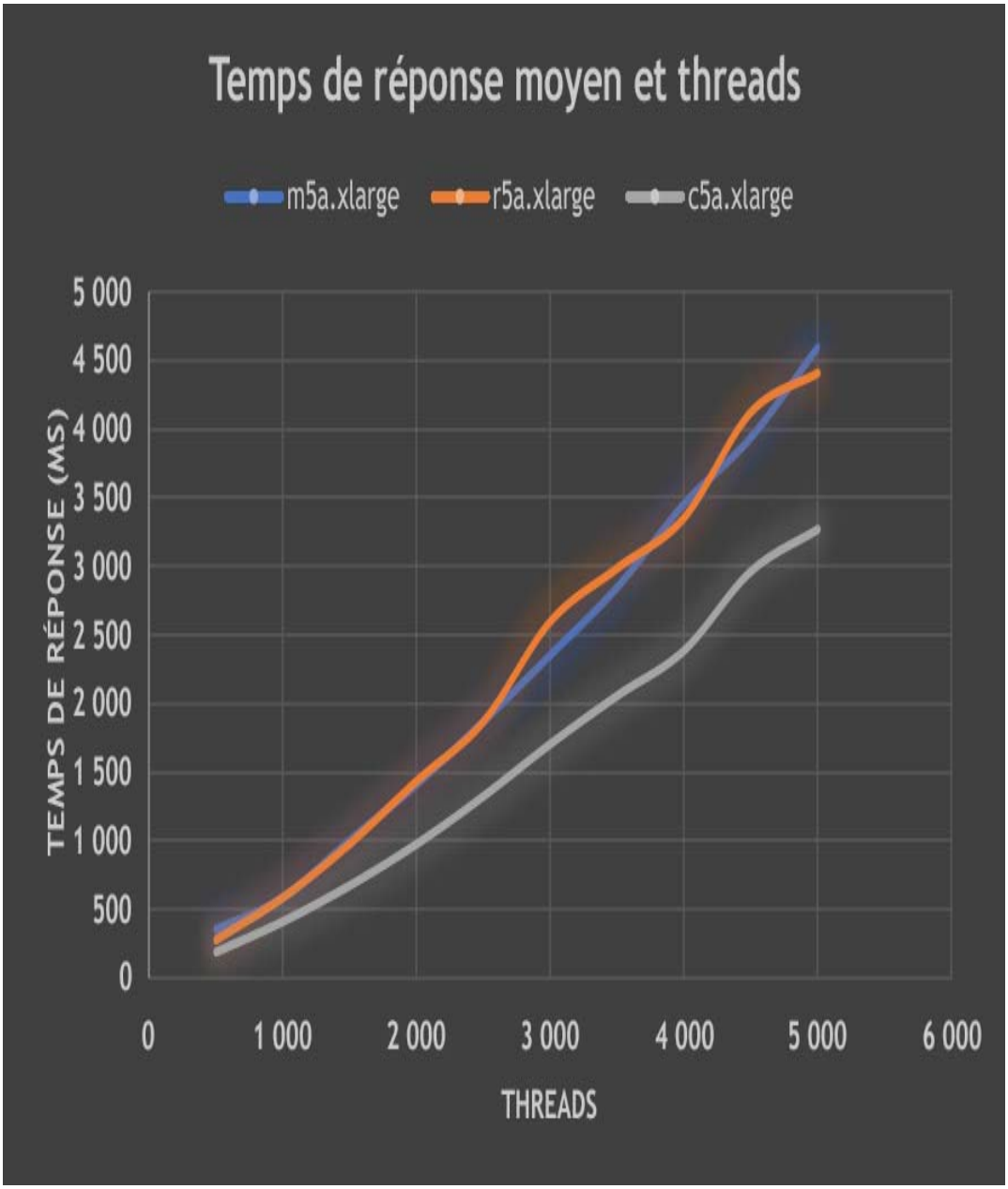
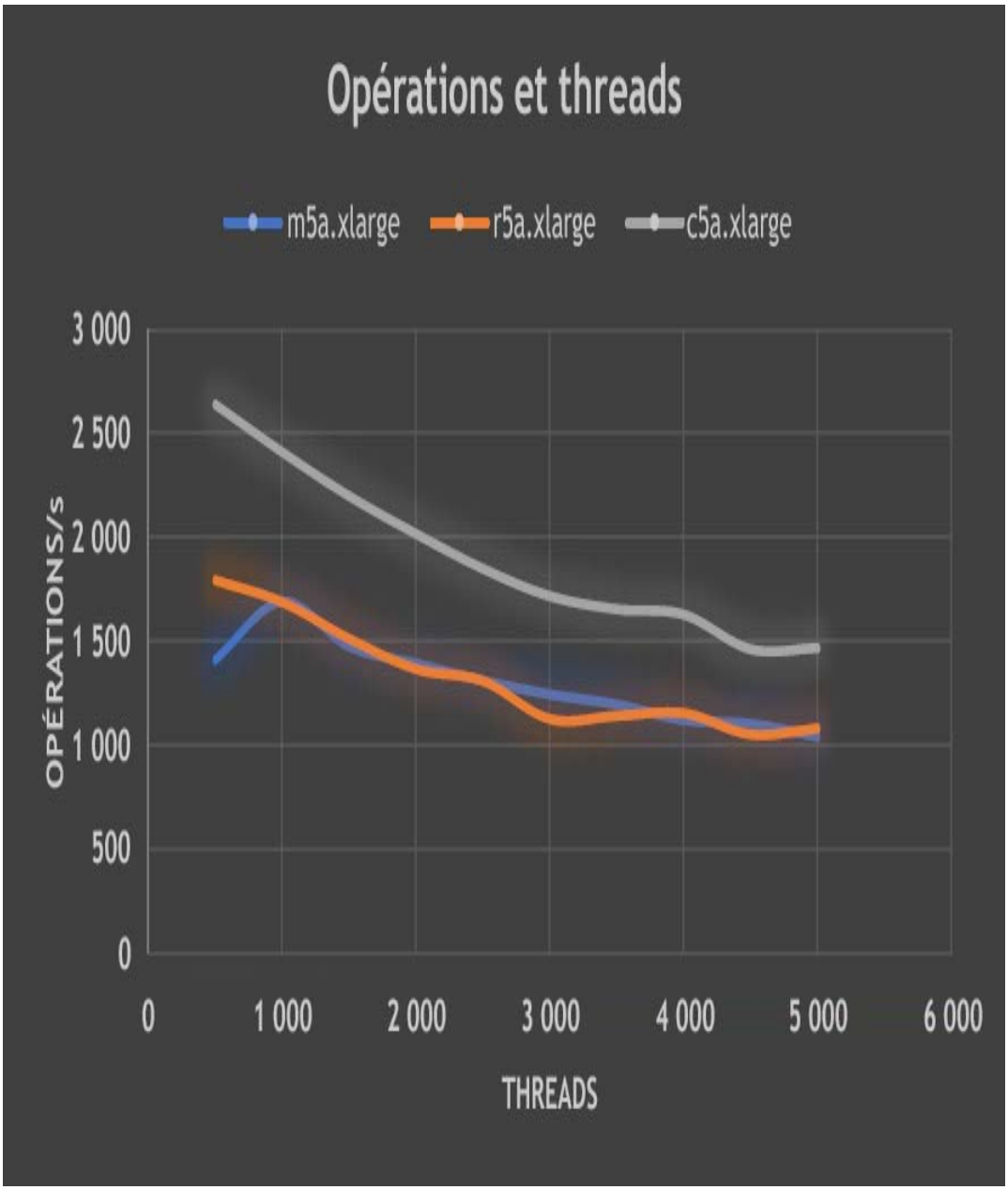


***Figure 6-5*** *Modification du nombre d'opérations exécutées simultanément en fonction du nombre de threads*




## Recommandation

Comme dans le scénario de test ci-dessus, vous devez utiliser les instances optimisées pour le calcul avec le volume EBS pour obtenir les meilleures performances OpenText eDirectory lors d'un déploiement dans un environnement AWS. Le type d'instance doit être choisi initialement en fonction de la charge attendue. Vous pouvez toujours redimensionner le type d'instance s'il ne répond pas aux exigences de ressources. Vous devez également attacher le volume SSD IOPS prévu à l'instance EC2 pour optimiser l'E/S et les performances de débit.

## Scénario n° 2 : identification de l'exigence de taille AWS EC2

Dans le scénario de performances précédent, nous avons déterminé que la catégorie d'instance AWS EC2 appropriée pour le déploiement et les opérations d'OpenText eDirectory était Optimisé pour le calcul.

Dans ce scénario de test des performances, les données ont été collectées à partir de trois types d'instances Optimisé pour le calcul différents, à savoir xlarge, 2xlarge et 4xlarge pour vous aider à trouver le guide de taille le mieux adapté.

Les graphiques ci-dessous représentent respectivement le temps de réponse moyen (en millisecondes) et des opérations par seconde par rapport au nombre de threads. Pour ce test, 500 millisecondes ont été considérées comme le temps de réponse moyen maximum acceptable.

***Figure 6-6*** *Modification du temps de réponse moyen en fonction du nombre de threads exécutés simultanément pour xlarge par rapport à 2xlarge et à 4xlarge*

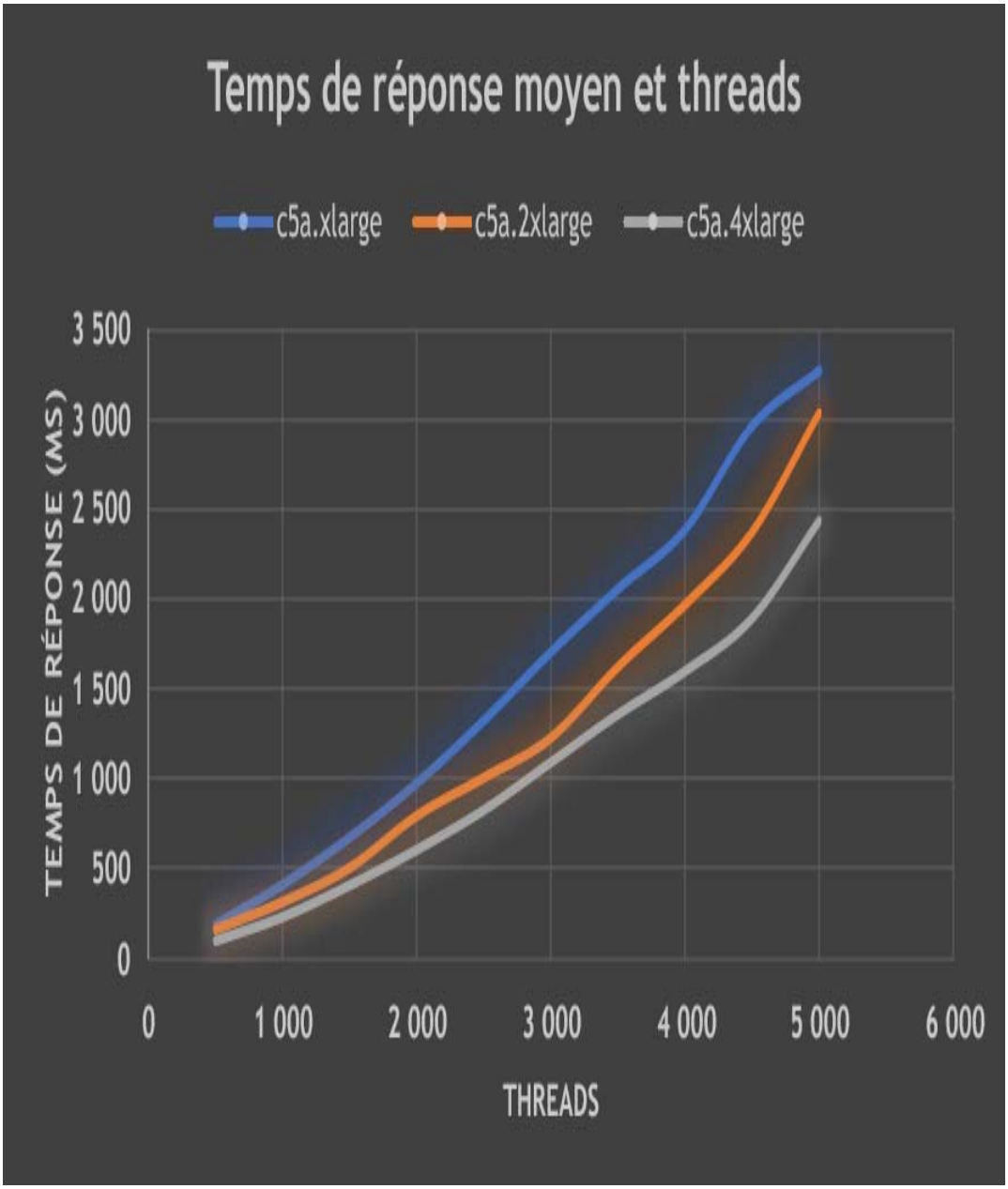
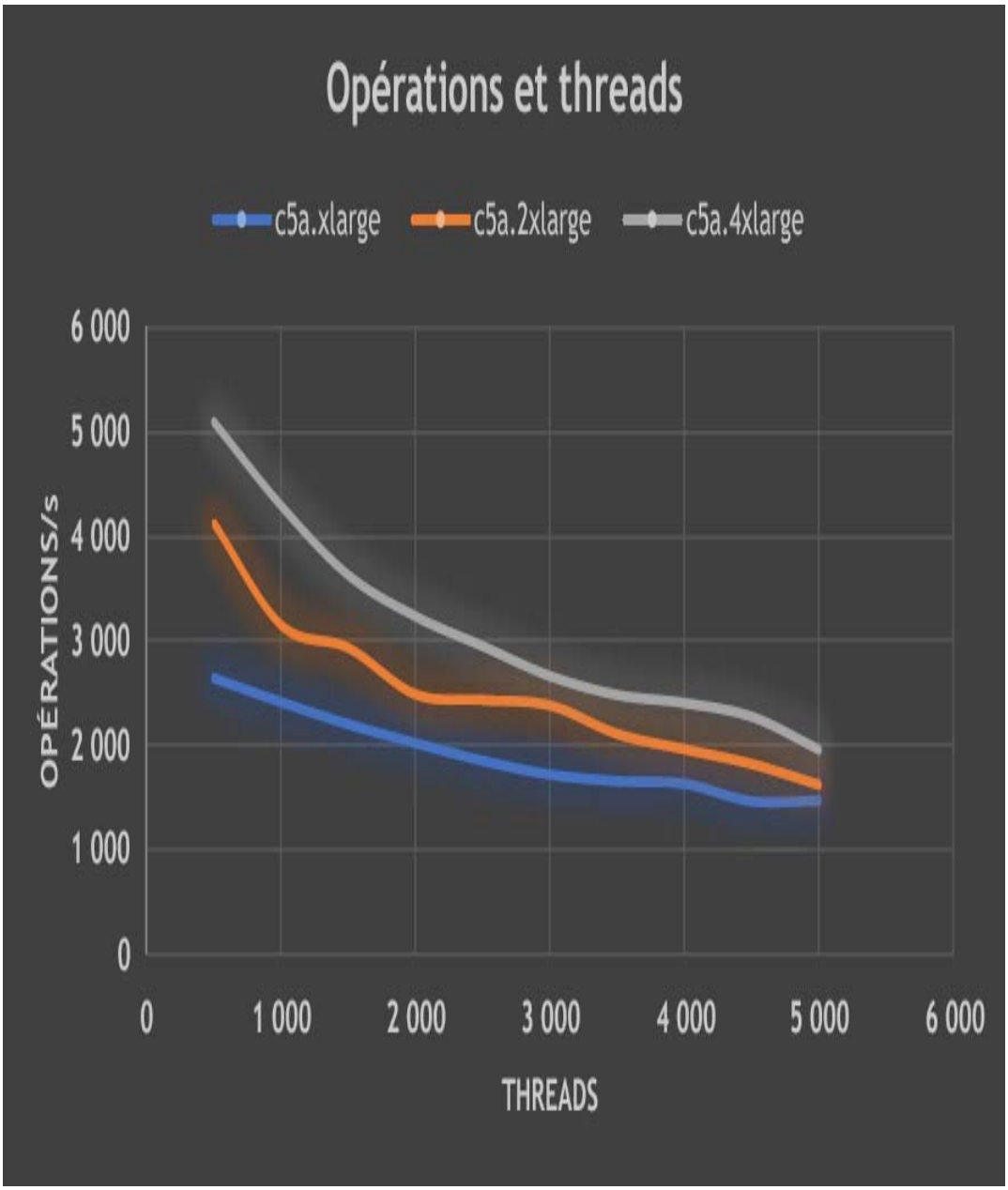


***Figure 6-7*** *Modification du nombre d'opérations exécutées simultanément en fonction du nombre de threads*




## Recommandation

Le tableau suivant indique le nombre maximal de threads mesuré et les opérations correspondantes par seconde possibles, afin de conserver le temps de réponse moyen dans la limite acceptable de 500 millisecondes pour chaque instance EC2 spécifiée.

| Type d'instance | Threads | Opérations par seconde |
|---|---|---|
| c5a.xlarge | 1200 | 2 300 |
| c5a.2xlarge | 1 500 | 2 900 |
| c5a.4xlarge | 1 750 | 3 500 |

Vous pouvez sélectionner la taille d'instance de calcul la mieux adaptée en fonction des valeurs de thread et de débit attendues, comme expliqué ci-dessus.

# 7 Déploiement d'OpenText eDirectory à l'aide d'un conteneur Docker

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


- « Présentation de Docker » page 153
- « Planification du déploiement d'OpenText eDirectory à l'aide d'un conteneur Docker » page 153
- « Déploiement d'un conteneur OpenText eDirectory » page 154
- « Tâches de post-configuration » page 161
- « Gestion du stockage des données OpenText eDirectory » page 164
- « Mise à niveau d'OpenText eDirectory à l'aide d'un conteneur Docker » page 165


## Présentation de Docker

Docker est la technologie de conteneurisation d'applications la plus courante. Il s'agit d'une plate-forme conçue pour créer, déployer et exécuter 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'OpenText 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'OpenText 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'OpenText 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 OpenText 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 OpenText 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.
- ❒ openSUSE Leap 15.4 fonctionne efficacement avec Docker Community Edition version 20.10.9-ce ou similaire.

### 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 d'image Docker pour OpenText eDirectory doit être téléchargé à partir du portail Licence de logiciel et téléchargement.
- ❒ 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 OpenText eDirectory

L'image de base du système d'exploitation de l'image Docker pour OpenText eDirectory est openSUSE Leap 15.4. Le fichier d'archive de l'image OpenText eDirectory doit être téléchargé sur la machine hôte Docker. Après avoir téléchargé le fichier d'archive, il doit être extrait, puis l'image doit être chargée dans le registre Docker local à l'aide des commandes suivantes :

```
tar -xvf eDirectory_93x_Container.tar.gz
docker load --input eDirectory_93x/eDirectory_93x.tar.gz
```

La commande ci-dessus charge une image Docker nommée `edirectory:9.3.x`.

Le conteneur Docker pour OpenText 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 OpenText eDirectory » page 54.

---

**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 OpenText 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 OpenText eDirectory. Pour plus d'informations, reportez-vous à la section « Gestion du stockage des données OpenText eDirectory » page 164.

---

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

Avant de déployer OpenText 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 du conteneur sur `on-failure` avec 5 comme nombre de tentatives à l'aide du drapeau `--restart` sur la commande docker run. Les conteneurs doivent être redémarrés manuellement si le daemon Docker sur la machine hôte est redémarré.
- Vous ne devez utiliser le conteneur OpenText 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 --filter status="running"
  ```

- 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 OpenText 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 (https://docs.docker.com/engine/containers/run/#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).
- Vous devez définir l'option `--stop-timeout` dans la commande Docker run avec une valeur de 180. Cela permet de s'assurer que le service nds reçoit suffisamment de temps pour s'arrêter normalement.

---

**REMARQUE :** Si vous utilisez une version autonome antérieure d'OpenText eDirectory, vous ne pouvez pas migrer la configuration vers l'environnement Docker à l'aide d'un conteneur Docker pour OpenText eDirectory 9.3.

---

Le conteneur Docker pour OpenText 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 OpenText eDirectory dans un réseau hôte » page 157
- « Déploiement d'un conteneur OpenText eDirectory dans un réseau superposé défini par l'utilisateur » page 159

# Déploiement d'un conteneur OpenText eDirectory dans un réseau hôte

Les conteneurs OpenText 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 OpenText eDirectory dans une même arborescence. Un réseau hybride permet d'introduire des conteneurs Docker pour OpenText eDirectory en toute transparence dans un environnement de production existant qui héberge déjà un déploiement OpenText 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 OpenText eDirectory conteneurisé apparaît en tant que serveur OpenText 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 OpenText eDirectory :

```
docker run -it --name eDir-container-1 --stop-timeout 180 --restart on-
failure:5 --memory="700M" --cpuset-cpus="1" --pids-limit="300" --volume
eDir-volume1:/config --network=host edirectory:9.3.0 new -t docker-tree1 -
n novell -S m1 -B 164.99.1.1@524 -o 1028 -O 1030 -L 389 -l 636 --configure-
eba-now yes
```

L'exemple suivant indique comment ajouter un serveur de répliques d'un conteneur OpenText eDirectory à une arborescence existante :

```
docker run -it --name eDir-container-2 --stop-timeout 180 --restart on-
failure:5 --memory="700M" --cpuset-cpus="1" --pids-limit="300" --volume
eDir-volume2:/config --network=host edirectory:9.3.0 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
```

Pour plus d'informations sur EBA, reportez-vous à la section Affichage des informations relatives à l'authentification EBA dans le Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3).

La liste ci-dessous décrit les paramètres d'ajout d'un serveur de répliques de conteneur OpenText eDirectory à une arborescence existante.

***Tableau 7-1*** *Description des paramètres de configuration*

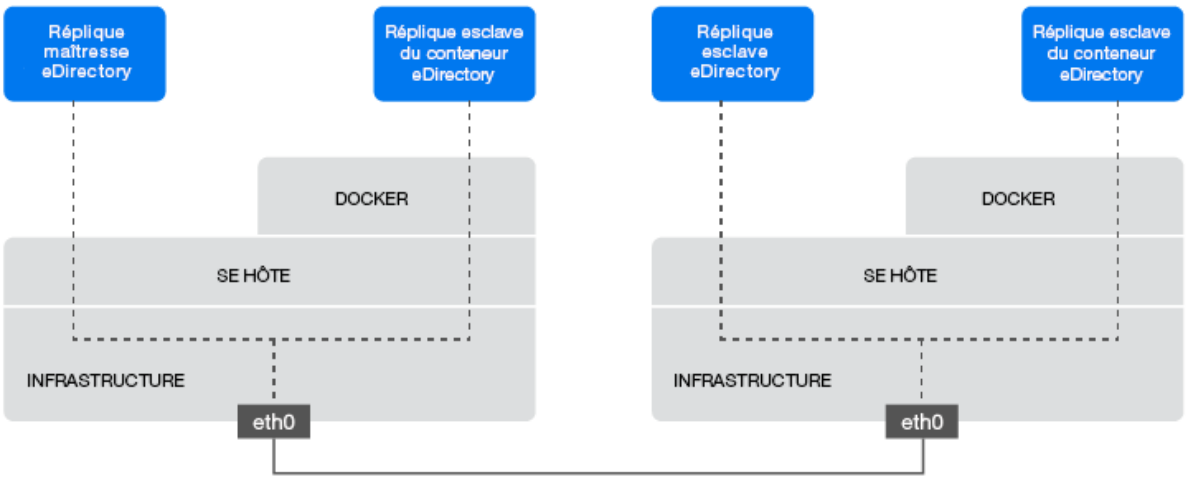
| Paramètre de configuration | Description |
|---|---|
| --name eDir-container-1 | Nom du conteneur Docker |
| --volume eDir-volume1 | Nom du volume Docker utilisé pour stocker les données OpenText eDirectory |

| Paramètre de configuration | Description |
|---|---|
| edirectory:9.3.0 | Image Docker que vous avez téléchargée et chargée. Notez le numéro de version : aucun avertissement ne vous avertit qu'il ne s'agit probablement pas de la version que vous avez téléchargée. |
| -t docker-tree1 | Nom de l'arborescence OpenText eDirectory |
| -n novel | Conteneur OpenText eDirectory dans lequel l'objet Serveur sera placé |
| -S m1 | Nom de l'objet Serveur qui sera créé dans OpenText eDirectory |
| -B164.99.1.1 | Adresse IP de l'hôte Docker |
| -o 1028 | Port HTTP OpenText eDirectory |
| -O1030 | Port HTTPS OpenText eDirectory |
| -L 389OpenText | Port LDAP eDirectory |
| -l 636 | Port LDAPS OpenText eDirectory |
| --configure-eba-now Yes | Yes – install EBA now |

**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 OpenText 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 7-1*** *Déploiement d'un conteneur OpenText eDirectory dans un réseau hôte*



# Déploiement d'un conteneur OpenText 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 OpenText eDirectory qui s'exécutent sur plusieurs hôtes de daemon Docker. Un conteneur OpenText 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 OpenText 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 OpenText eDirectory. De plus, la migration des conteneurs OpenText 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 OpenText eDirectory dans un réseau superposé défini par l'utilisateur, vous devez tenir compte des recommandations suivantes :

- Le serveur de répliques maîtresses du conteneur OpenText eDirectory et ses répliques R/W doivent être déployés au sein d'un même réseau superposé. Les communications avec d'autres serveurs OpenText 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 Identity Console dans le même réseau superposé défini par l'utilisateur à des fins d'administration d'OpenText eDirectory. Pour plus d'informations sur le déploiement des conteneurs Docker pour Identity Console, reportez-vous à la section Installation d'OpenText Identity Console en tant que 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 OpenText eDirectory :

```
docker run -it --name eDir-container-1 --stop-timeout 180 --restart on-
failure:5 --memory="700M" --cpuset-cpus="1" --pids-limit="300" --volume
eDir-volume1:/config --network=myOverlay --ip=10.0.0.5 edirectory:9.3.0
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 OpenText 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 OpenText 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 --stop-timeout 180 --restart on-
failure:5 --memory="700M" --cpuset-cpus="1" --pids-limit="300" --volume
eDir-volume2:/config --network=myOverlay --ip=10.0.0.6 edirectory:9.3.0
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>
```

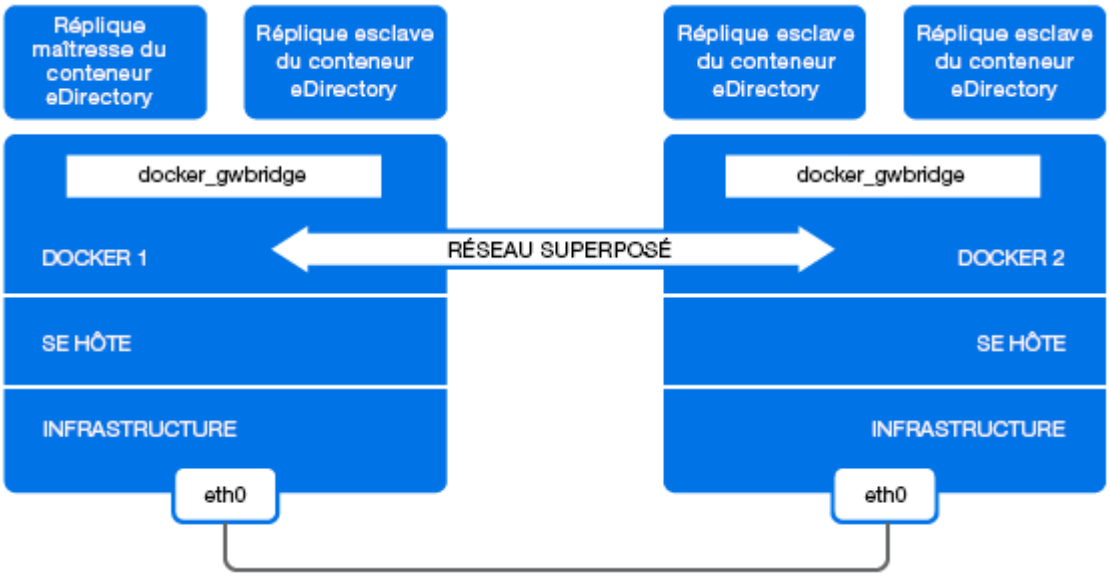
---

**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`.
- L'option `-B @524` permet aux services NCP, http et https de se relier à toutes les interfaces disponibles.

---

***Figure 7-2*** *Déploiement d'un conteneur OpenText eDirectory dans un réseau superposé défini par l'utilisateur*




# Tâches de post-configuration

Vous devez effectuer les tâches suivantes après avoir déployé les conteneurs OpenText eDirectory.

- « Exécution de commandes sur un conteneur OpenText eDirectory en cours d'exécution » page 161
- « Configuration d'OpenSLP pour le conteneur Docker pour OpenText eDirectory » page 162
- « Installation des méthodes NMAS dans un conteneur Docker pour OpenText eDirectory » page 163
- « Installation de nouveaux paquetages dans un conteneur Docker pour OpenText eDirectory » page 163
- « Configuration du fichier de propriétés CEF dans un conteneur Docker pour OpenText eDirectory » page 164

---

**REMARQUE :** L'image de base du système d'exploitation de l'image Docker pour OpenText eDirectory est openSUSE Leap avec SysVinit comme système init. vous devez ajouter toutes les variables d'environnement requises pour le service OpenText eDirectory dans le fichier `pre_ndsd_start`.

---

## Exécution de commandes sur un conteneur OpenText eDirectory en cours d'exécution

Exécutez la commande suivante sur la machine hôte Docker pour obtenir un shell bash dans le conteneur Docker pour OpenText eDirectory :

```
docker exec -it eDir-container-1 /bin/bash
```

La commande ci-dessus permet de définir le chemin d'accès binaire OpenText 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

Tree Name: EDR93E
Server Name: .CN=Master.O=server.T=EDR93E.
Binary Version: 40301.00
Root Most Entry Depth: 0
Product Version: OpenText eDirectory for Linux x86_64 v9.3 [DS]
```

Vous pouvez exécuter la commande ci-dessus directement à partir de la machine hôte. Voici un exemple :

```
docker exec -it eDir-container-1 /opt/novell/eDirectory/bin/ndsstat

Tree Name: EDR93E
Server Name: .CN=Master.O=server.T=EDR93E.
Binary Version: 40301.00
Root Most Entry Depth: 0
Product Version: OpenText eDirectory for Linux x86_64 v9.3 [DS]
```

## Configuration d'OpenSLP pour le conteneur Docker pour OpenText eDirectory

Procédez comme suit pour démarrer le serveur SLP dans un conteneur OpenText 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 OpenText 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.
- Si vous ne configurez pas OpenSLP, il se peut que le message d'erreur `-626` s'affiche.

---

## Installation des méthodes NMAS dans un conteneur Docker pour OpenText eDirectory

Effectuez les tâches suivantes pour installer les méthodes NMAS dans un conteneur OpenText eDirectory :

---

**REMARQUE :** par défaut, les méthodes NMAS sont disponibles dans `/home/nds/eDirectory/nmas`.

---

1. Connectez-vous au conteneur OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

   ---

3. Quittez la console du conteneur :

   ```
   exit
   ```

4. Redémarrez le conteneur OpenText eDirectory :

   ```
   docker restart eDir-container-1
   ```

## Installation de nouveaux paquetages dans un conteneur Docker pour OpenText eDirectory

Le système d'exploitation de base inclus dans l'image OpenText eDirectory contient toutes les dépendances pour le fonctionnement normal de l'application OpenText eDirectory dans un environnement de conteneur. Si un nouvel utilitaire ou outil de débogage doit être introduit et s'il n'est pas inclus par défaut dans l'image, il doit être introduit séparément dans le conteneur en cours d'exécution.

Exécutez la commande suivante pour installer un nouveau paquetage dans un conteneur OpenText eDirectory en cours d'exécution à l'aide de `zypper`:

```
docker exec --user root -it eDir-container-1 zypper in <package>
```

Vous pouvez également installer de nouveaux paquetages après les avoir copiés directement dans le conteneur à partir de la machine hôte Docker à l'aide de la commande `docker cp`. Pour plus d'informations, reportez-vous à la section docker cp.

## Configuration du fichier de propriétés CEF dans un conteneur Docker pour OpenText eDirectory

Vous devez effectuer les modifications suivantes dans le fichier de propriétés CEF pour activer la consignation des fichiers de mise en cache et de déploiement. Le fichier de propriétés CEF (`auditlogconfig.properties`) se trouve dans le dossier `/config/eDirectory/inst/conf`.

```
# Cache location directory
# Directory should be available for creating cache files
log4j.appender.S.CacheDir=/config/eDirectory/inst/data

# Log file for appender R.
log4j.appender.R.File=/config/eDirectory/inst/data/log/cef-events.log
```

Pour plus d'informations, consultez Configuration du fichier de propriétés CEF dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

---

**REMARQUE :** Pour configurer la mise en cache du système d'événements, définissez les variables d'environnement comme indiqué ci-dessous dans le fichier `pre_ndsd_start` situé dans le dossier `/opt/novell/eDirectory/sbin` du conteneur OpenText eDirectory :

```
export NDSD_EVENT_DISK_CACHE=1
export NDSD_EVENT_DISK_CACHE_DIR=/config/eDirectory/inst/data/data
```

---

# Gestion du stockage des données OpenText eDirectory

Docker Volume est le mécanisme de stockage persistant privilégié pour les données et la configuration d'OpenText 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 OpenText 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 OpenText 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 OpenText eDirectory. Pour plus d'informations sur la mise à niveau d'un conteneur eDirectory, reportez-vous à la section « Mise à niveau d'OpenText eDirectory à l'aide d'un conteneur Docker » page 165.

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 OpenText 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 edir930: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 OpenText eDirectory.

# Mise à niveau d'OpenText eDirectory à l'aide d'un conteneur Docker

Quand une nouvelle version de l'image OpenText eDirectory est disponible, l'administrateur peut effectuer une mise à niveau pour déployer le conteneur à l'aide de la dernière version d'OpenText 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'OpenText 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 OpenText eDirectory et des données d'application de l'ancien conteneur stockées dans le volume Docker :

   L'exemple ci-dessous indique comment démarrer un conteneur OpenText eDirectory avec un volume monté à des fins de stockage :

   ```
   docker run -it --name eDir1-Host --stop-timeout 180 --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 OpenText eDirectory créé à l'étape 2 :

   ```
   docker run -it --name eDir1-Host --stop-timeout 180 --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 OpenText eDirectory.

---

**REMARQUE**

- Le conteneur OpenText 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 OpenText eDirectory

Si un conteneur OpenText 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 OpenText eDirectory et le volume Docker du conteneur concerné. Procédez comme suit pour récupérer un conteneur OpenText eDirectory :

1. Arrêtez et supprimez le conteneur concerné.
2. Démarrez un nouveau conteneur avec la même image OpenText eDirectory et le volume du conteneur concerné. L'exemple suivant montre comment récupérer un conteneur concerné :

   ```
   docker run -it --name eDir1-Host --stop-timeout 180 --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 OpenText eDirectory concerné.

# 8 Installation d'OpenText eDirectory sous Linux et Windows avec des adresses IPv6

OpenText eDirectory 932 prend en charge les adresses IPv4 et IPv6. Vous pouvez activer les adresses IPv6 au cours du processus d'installation d'OpenText eDirectory. Lors de la mise à niveau à partir d'une version antérieure, vous devez activer manuellement la prise en charge des adresses IPv6.

OpenText eDirectory 9.3 prend en charge les méthodes de transition Dual IP stack, Tunneling et Pure IPv6. Seules les adresses IP globales sont prises en charge. Par exemple,

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

La fonctionnalité OpenText 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 OpenText 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
```

OpenText eDirectory 9.3 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 OpenText eDirectory 9.3 sur Linux et Windows où les adresses IPv6 sont déjà configurées :


- « Configuration d'OpenText eDirectory sur Linux avec IPv6 » page 168
- « Installation ou mise à niveau d’OpenText eDirectory sous Windows avec IPv6 » page 169

Pour plus d'informations sur les différences entre les plates-formes Linux et Windows pour IPv6, voir « Dépannage des problèmes IPV6 ».

# Configuration d'OpenText eDirectory sur Linux avec IPv6

Cette section fournit des informations sur la configuration d'OpenText eDirectory sur un ordinateur Linux prenant déjà en charge les adresses IPv6 :

## Création d'une nouvelle arborescence OpenText eDirectory

Vous pouvez configurer une nouvelle arborescence OpenText 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 d'OpenText 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 d'Identity Console après la configuration initiale. Pour plus d'informations, reportez-vous à la section « Ajout d'URL LDAP pour IPV6 sur l'objet Serveur LDAP » page 169.

## Ajout d’un serveur à une arborescence OpenText 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 d'OpenText 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 d'Identity Console après la configuration initiale. Pour plus d'informations, reportez-vous à la section « Ajout d'URL LDAP pour IPV6 sur l'objet Serveur LDAP » page 169.

## Activation d’adresses IPv6 sur des serveurs OpenText 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:abcd:bcde:cdef:aaaa]@524

http.server.interfaces=164.99.90.148@8028,[2015::4]@8028,[2015:1234:23
45:3456:abcd:bcde:cdef:aaaa]@8028

https.server.interfaces=164.99.90.148@8030,[2015::4]@8030,[2015:1234:2
345:3456: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'OpenText eDirectory, vous pouvez utiliser la commande `ldapconfig` ou Identity Console 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 Identity Console :

1. Connectez-vous à OpenText Identity Console, puis cliquez sur **Configuration LDAP**.
2. Dans le menu **Résultats de la recherche** > sélectionnez le serveur LDAP - <server name/CN>.
3. Cliquez sur **Modifier le serveur LDAP** > **Informations >** Interface LDAP .
4. Dans la fenêtre **Ajouter un élément** > ajoutez des URL LDAP dans le champ Interfaces LDAP.
5. Cliquez sur **Ajouter**, puis sur **Enregistrer**.

   Le message Serveur LDAP modifié avec succès !, cliquez sur **OK**.

# Installation ou mise à niveau d’OpenText eDirectory sous Windows avec IPv6

Cette section fournit des informations sur la configuration d'OpenText 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 d'OpenText eDirectory

Si vous souhaitez utiliser des adresses IPv6, veillez à cocher la case **Activer IPv6** dans **Préférence IPv6** lors de l'installation d'OpenText 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 OpenText 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 OpenText iMonitor

Vous pouvez accéder à OpenText iMonitor sur les adresses IPv6 à l'aide du lien suivant :

```
http://[2015::3]:8028/nds
```

# 9 Fonctionnement d'OpenText eDirectory en mode FIPS

OpenText eDirectory 9.3 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'OpenText eDirectory en mode FIPS.

Vous pouvez exécuter OpenText eDirectory en mode FIPS 140-2 pris en charge par les modules NICI et OpenSSL.


- « Configuration d'OpenText eDirectory en mode FIPS » page 171


## Configuration d'OpenText eDirectory en mode FIPS

À partir d'OpenText eDirectory 9.3, le mode FIPS par défaut est désactivé sur NICI et OpenSSL sur toutes les plates-formes. OpenText eDirectory fournit des paramètres pour configurer le mode FIPS en fonction de vos besoins. Lorsque le mode FIPS est activé pour le serveur OpenText eDirectory, toutes les applications et tous les modules qui s'exécutent dans OpenText eDirectory, y compris OpenSSL, sont en mode FIPS. Par exemple, les opérations LDAP, HTTP ainsi que toutes les opérations de chiffrement utilisent l'authentification EBA. Le fonctionnement d'OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

Vous ne devez définir qu'un seul drapeau pour activer le mode FIPS pour OpenText eDirectory. Cela active à la fois NICI et OpenSSL.

Exécutez les conditions préalables suivantes avant d'activer la FIPS NICI pour que la connexion NDS fonctionne :

1. Créer - Stratégie de mot de passe PBKDF2 (Fonction de dérivation de clé basée sur un mot de passe 2). Pour plus d'informations, voir Compréhension du stockage des mots de passe non réversibles. Assignez ensuite la stratégie de mot de passe PBKDF2 à tous les utilisateurs.
2. Définissez SCRAM comme séquence de connexion par défaut. Pour plus d'informations, voir Authentification par mot de passe.
3. Une fois la stratégie PBKDF2 assignée, il est recommandé à tous les utilisateurs de modifier leur mot de passe avant d'activer FIPS dans NICI.
4. Activez FIPS NICI une fois que le mot de passe de tous les utilisateurs a été modifié. Pour activer NICI en mode FIPS, voir Utilisation de NICI pour configurer le mode FIPS au niveau du système.
5. TLS et FIPS dans NICI sont activés en fonction de la configuration de `nici.cfg`.

Pour activer le mode FIPS dans OpenText eDirectory pour NICI et OpenSSL :

- **Windows :** La fonction FIPS peut être activée sous Windows, ce qui permet de définir le drapeau Niveau de restriction NICI sur 1 dans le registre Windows. Pour plus d'informations, voir Utilisation de NICI pour configurer le mode FIPS au niveau du système (https://www.netiq.com/documentation/edirectory-93/nici_admin_guide/data/agbdek3.html#b1habb0n).
- **Linux :** FIPS dans NICI est activé en fonction de la configuration de `nici.cfg`. Pour plus d'informations, voir Utilisation de NICI pour configurer le mode FIPS au niveau du système (https://www.netiq.com/documentation/edirectory-93/nici_admin_guide/data/agbdek3.html#b1habb0n).

---

**REMARQUE :** Il n'est pas recommandé de désactiver FIPS une fois qu'il est activé.

---

# 10 Déplacement de la DIB

Après avoir installé et configuré OpenText 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 OpenText 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 OpenText™ 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 d'OpenText eDirectory.

# 11 Conditions requises pour la mise à niveau d'OpenText eDirectory 9.3

L'une des fonctionnalités uniques d'OpenText 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 OpenText 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 d'OpenText 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 d'OpenText 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 OpenText eDirectory 9.3.


- « Changements de référence dans 8.8 SP1 ou versions ultérieures » page 175
- « Procédure de mise à niveau dans la version 9.3 » page 176


## Changements de référence dans 8.8 SP1 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.

---

**REMARQUE :** Il est recommandé de ne pas mettre directement à niveau OpenText eDirectory de la version 8.8SP1 vers la version 9.3. Vous devez passer par la version 9.2, puis par la version 9.3. La mise à niveau d'OpenText eDirectory à partir d'une version antérieure de 8.8 SP1 vers la version 9.2 a

une incidence sur les performances de votre serveur OpenText eDirectory. Cela se produit, car tous les index sont recréés automatiquement. Si vous êtes en cours de mise à niveau à partir de la version 8.8 SP1 et des versions ultérieures, ce problème ne se produira pas.

---

La nouvelle façon de maintenir les références nécessite néanmoins de mettre à niveau la base de données si l'instance d'OpenText eDirectory existante est mise à niveau vers la version 8.8 SP1 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 9.3

La commande `ndsconfig upgrade` permet de mettre à niveau la configuration nécessaire des composants tels que HTTP, LDAP, SNMP, SAS et NMAS.

### Utilisation de l'option Force pour mettre à niveau OpenText eDirectory à partir de versions antérieures sur Linux

OpenText eDirectory 9.3 ne prend en charge que les mises à niveau à partir de la version 9.2 ou ultérieure sur Linux.

Pour effectuer une mise à niveau depuis la version 8.8.8 d'OpenText eDirectory, effectuez une mise à niveau vers OpenText eDirectory 9.2, puis vers eDirectory 9.3. Après la mise à niveau vers eDirectory 9.2, exécutez le certificat de réparation dans Identity Console, puis vers OpenText eDirectory 9.3. Pour plus d'informations sur la réparation du certificat par défaut, consultez

---

**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'OpenText 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`.

---

# 12 Configuration d'OpenText eDirectory sous Linux

OpenText eDirectory contient des utilitaires qui simplifient la configuration de différents composants d'OpenText eDirectory sous Linux. Les sections suivantes traitent des fonctionnalités et de l'utilisation des composants de configuration d'OpenText eDirectory :


- « Utilitaires de configuration » page 177
- « Paramètre de configuration » page 180
- « Considérations relatives à la sécurité » page 186


## Utilitaires de configuration

Cette section traite de l'utilisation des utilitaires de configuration OpenText eDirectory suivants :


- « Utilitaire ndsconfig » page 177
- « Utilisation des outils LDAP pour configurer les objets Serveur LDAP et Groupe LDAP » page 178
- « Utilisation de l'utilitaire nmasinst pour configurer le service NMAS (NetIQ Modular Authentication Service) » page 178
- « Personnalisation d'OpenText eDirectory » page 178


### Utilitaire ndsconfig

L'utilitaire ndsconfig permet de configurer OpenText eDirectory. Vous pouvez également l'utiliser pour ajouter le serveur de répliques OpenText eDirectory à une arborescence existante ou pour créer une arborescence. Pour plus d'informations, reportez-vous à la section « Exécution de l'utilitaire ndsconfig pour ajouter ou supprimer le serveur de répliques OpenText eDirectory » page 54.

---

**REMARQUE**

- vérifiez que le nom du serveur NCP est unique au sein du réseau.

---

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 « Paramètre de configuration » page 180.

**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 OpenText 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 « Utilisation d'outils LDAP sur Linux » dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.

## Utilisation de l'utilitaire nmasinst pour configurer le service NMAS (NetIQ Modular Authentication Service)

Pour OpenText eDirectory 9.3, 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 section « Exécution de l'utilitaire nmasinst pour configurer NMAS » page 69.

## Personnalisation d'OpenText eDirectory


- « Utilisation du script d'initialisation de ndsd » page 178
- « Utilisation d'OpenText eDirectory sur les plates-formes SLES 15 et RHEL 8 » page 179


### 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` n'est actuellement pris en charge que par les plates-formes SLES 15, RHEL 8, RHEL 9 et ultérieures. Pour plus d'informations, reportez-vous à la section « Utilisation d'OpenText eDirectory sur les plates-formes SLES 15 et RHEL 8 » page 179.

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 OpenText eDirectory, employez l'utilitaire ndsmanage.

**REMARQUE :** exécutez les commandes suivantes pour démarrer et arrêter OpenText eDirectory sous SLES 15 et RHEL 8 ou version ultérieure.

- Pour démarrer ndsd, exécutez `systemctl start ndsd*`
- Pour arrêter ndsd, exécutez `systemctl stop ndsd*`

La configuration d'OpenText 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 OpenText 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 OpenText eDirectory. Pour plus d'informations sur les variables d'environnement, consultez le document TID 7018431.

## Utilisation d'OpenText eDirectory sur les plates-formes SLES 15 et RHEL 8

OpenText 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 OpenText SLP.

Pour démarrer ou arrêter OpenText eDirectory, employez l'utilitaire `ndsmanage`.

La configuration d'OpenText 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'OpenText 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`.

# Paramètre de configuration

Les paramètres de configuration d'OpenText 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 OpenText 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. |

| Paramètre | Description |
| --- | --- |
| n4u.base.dclient.use-udp | DClient peut utiliser UDP en plus de TCP pour communiquer avec les serveurs OpenText 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 OpenText SLP et non par OpenSLP. |
| n4u.nds.advertise-life-time | OpenText 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 |
| n4u.nds.dir | Base de données des informations de l'annuaire OpenText 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 OpenText eDirectory.<br><br>Valeur par défaut = aucune valeur |
| n4u.nds.server-name | Nom du serveur OpenText eDirectory.<br><br>Valeur par défaut = aucune valeur |

| Paramètre | Description |
| --- | --- |
| `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 OpenText 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 OpenText 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 d'OpenText 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) d'OpenText eDirectory.<br><br>Valeur par défaut = 2<br><br>Plage = 1 à 10080 |
| `n4u.nds.backlink-interval` | Intervalle (en minutes) au terme duquel est exécuté le contrôle de cohérence des liens en amont d'OpenText 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 d'OpenText eDirectory.<br><br>Valeur par défaut = 780<br><br>Plage = 2 à 10080 |

| Paramètre | Description |
| --- | --- |
| 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 OpenText 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 d'OpenText eDirectory sont stockés ici.<br><br>Valeur par défaut = /etc |
| n4u.server.vardir | Les fichiers journaux d'OpenText eDirectory et des utilitaires sont stockés ici.<br><br>Emplacement par défaut = /var/opt/novell/eDirectory/log |
| 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. |

| Paramètre | Description |
| --- | --- |
| `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 OpenText 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 : `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 OpenText 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 OpenText 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 OpenText eDirectory. Il s'agit du nombre d'opérations simultanées susceptibles d'être exécutées au niveau du serveur OpenText eDirectory.<br><br>Valeur par défaut = 64<br><br>Plage = 32 à 512<br><br>Consultez le *dépannage* pour définir une valeur optimale. |
| `n4u.server.idle-threads` | Nombre maximal de threads inactifs autorisés dans le serveur OpenText 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 |
| `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. |

| Paramètre | Description |
| --- | --- |
| 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 OpenText 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 OpenText Directory est exécuté en mode FIPS.<br><br>Valeur par défaut = 1. Cela signifie qu'OpenText 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 d'OpenText 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.

# 13 Déploiement d'OpenText eDirectory sur les grappes haute disponibilité

Configurer plusieurs serveurs via la synchronisation représente la méthode principale grâce à laquelle OpenText 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 OpenText 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 d'OpenText 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 d'OpenText eDirectory doit être située sur le stockage partagé de la grappe. L'instance root OpenText eDirectory sur chaque nœud de grappe doit être configurée pour utiliser la DIB sur le stockage partagé.

Outre la DIB, il faut partager les données NICI 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 OpenText eDirectory doivent également résider sur le stockage partagé.

OpenText eDirectory 9.3 inclut un utilitaire destiné aux serveurs Linux et Windows qui configure automatiquement OpenText 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 OpenText eDirectory sur les nœuds 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 d'OpenText 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 qu'OpenText eDirectory ne prend pas en charge l'équilibrage de la charge en utilisant plusieurs nœuds de grappe.

---

Cette section comprend les rubriques suivantes :


- « Mise en grappe des services OpenText eDirectory sur Linux » page 188
- « Mise en grappe des services OpenText eDirectory sur Windows » page 191

- « Dépannage des environnements en grappe » page 194
- « Options de l'utilitaire de configuration » page 195

# Mise en grappe des services OpenText eDirectory sur Linux

Cette section explique comment configurer OpenText eDirectory 9.3 en utilisant la mise en grappe haute disponibilité sur Linux.

- « Conditions préalables » page 188
- « Installation et configuration d'OpenText eDirectory » page 188
- « Configuration du serveur SNMP dans des environnements Linux en grappe » page 191

## 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 d'OpenText eDirectory et NICI
- Adresse IP virtuelle
- OpenText eDirectory 9.1 ou version ultérieure

---

**REMARQUE :** L'utilitaire nds-cluster-config prend uniquement en charge la configuration de l'instance OpenText eDirectory root. OpenText eDirectory ne prend pas en charge la configuration de plusieurs instances et les installations non root d'OpenText eDirectory dans un environnement de grappe.

---

## Installation et configuration d'OpenText eDirectory

1 Installez et configurez OpenText 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 OpenText eDirectory » page 45.

---

**REMARQUE**

- Pendant la configuration d'OpenText eDirectory, le nom de serveur NCP par défaut est le nom de serveur hôte de l'ordinateur sur lequel vous avez installé OpenText eDirectory. Comme OpenText 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 OpenText eDirectory sur le nœud de grappe primaire.
- Pendant le processus de configuration, assurez-vous de définir l'adresse IP virtuelle de votre installation d'OpenText eDirectory. Dans un environnement en grappe, OpenText 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 d'OpenText eDirectory en utilisant la commande `ndsstat`.

OpenText 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 OpenText 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 nœud en grappe primaire, ouvrez un terminal et exécutez la commande suivante pour arrêter le service OpenText 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 OpenText 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 OpenText eDirectory en exécutant la commande suivante :

```
ndsmanage startall
```

12 Vérifiez l'état d'OpenText eDirectory en utilisant ndsstat. Les services d'OpenText eDirectory doivent être fonctionnels et en cours d'exécution.

13 Arrêtez les services OpenText 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 d'OpenText eDirectory sur le nœud de grappe secondaire que celle installée sur le noeud de grappe primaire, mais ne configurez pas OpenText 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 d'OpenText eDirectory situées sur le système de fichiers en grappe.

19 Démarrez les services OpenText eDirectory en exécutant la commande suivante :

```
ndsmanage startall
```

Vérifiez l'état de eDirectory en utilisant la commande ndsstat.

20 Arrêtez les services d'OpenText eDirectory sur le noeud secondaire en exécutant la commande ndsmanage stopall.

21 Après avoir configuré avec succès OpenText eDirectory sur les deux nœuds de la grappe, vous devez aussi modifier le mode de démarrage du service ndsd sur chaque nœud en utilisant la commande suivante :

```
chkconfig -d ndsd
```

22 Une fois que l'utilitaire de configuration a terminé de configurer le nœud secondaire, vous pouvez utiliser le gestionnaire de grappes pour ajouter les services d'OpenText 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 « Installation et configuration des services SNMP pour OpenText eDirectory » dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.
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 qu'OpenText 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 OpenText eDirectory sur Windows

Cette section explique comment configurer OpenText eDirectory 9.3 en utilisant la mise en grappe haute disponibilité sur Windows.


- « Conditions préalables » page 191
- « Installation et configuration d'OpenText eDirectory » page 192
- « Configuration du serveur SNMP dans des environnements Windows en grappe » page 194


## 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
- OpenText eDirectory 9.3

## Installation et configuration d'OpenText eDirectory

1. Installez et configurez OpenText 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'OpenText eDirectory 9.3 sur un serveur Windows » page 78.
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 OpenText 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 d'OpenText 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 pas spécifier un nom de lecteur uniquement. 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`

    En plus de déplacer les données eDirectory vers le système de fichiers partagé, l'utilitaire copie la clé de registre des services OpenText 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 OpenText 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 d'OpenText eDirectory pour réaliser une installation sans surveillance d'OpenText eDirectory sur le nœud 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 OpenText 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 d'OpenText 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 OpenText eDirectory, vérifiez OpenText eDirectory, puis cliquez sur **Arrêter**.

24 Cliquez sur **Oui** pour confirmer.

25 Pour configurer OpenText eDirectory dans le groupe Ressource de grappe, créez une nouvelle ressource dans le groupe Ressource à utiliser pour OpenText 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 « Installation et configuration des services SNMP pour OpenText eDirectory » dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*.
2. Enregistrez le mot de passe OpenText 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 d'OpenText 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 nœuds 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 OpenText 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 OpenText 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 d'OpenText eDirectory

Ce chapitre développe les informations suivantes :


- « Désinstallation d'OpenText OpenText eDirectory sous Windows » page 197
- « Désinstallation d'OpenText eDirectory sous Linux » page 202
- « Désinstallation sans surveillance d'OpenText eDirectory sous Linux » page 203
- « Avertissements concernant la désinstallation d'OpenText eDirectory » page 204


## Désinstallation d'OpenText OpenText eDirectory sous Windows

Pour supprimer OpenText eDirectory, ConsoleOne, l'agent Annuaire SLP et NICI sur des serveurs Windows, utilisez le Panneau de configuration de Windows.

---

**IMPORTANT :** La suppression d'OpenText 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 OpenText eDirectory sur le serveur, vous devez les copier dans un autre emplacement avant de supprimer OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

---


- « Désinstallation d'OpenText eDirectory, ConsoleOne et de l'agent Annuaire SLP » page 197
- « Désinstallation sans surveillance d'OpenText eDirectory » page 198
- « Désinstallation de NICI » page 201
- « Désinstallation des bibliothèques d'exécution Microsoft Visual C++ 2005 et Visual C++ 2012 » page 202


---

**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 d'OpenText eDirectory, ConsoleOne et de l'agent Annuaire SLP

1. Sur le serveur Windows où est installé OpenText eDirectory, cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **Ajout/Suppression de programmes**.
2. Sélectionnez **OpenText 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 d'OpenText eDirectory

Sur Windows, la désinstallation sans surveillance d'OpenText eDirectory utilise des fichiers texte prédéfinis qui facilitent ledit processus. Vous pouvez effectuer les actions suivantes en utilisant le mode de désinstallation sans surveillance d'OpenText eDirectory :

- Déconfiguration du OpenText eDirectory installé.
- Désinstallation autonome d'OpenText eDirectory.
- Désinstallation et déconfiguration de eDirectory.

Les sections suivantes abordent les diverses fonctionnalités de la désinstallation sans surveillance d'OpenText eDirectory :


- « Fichiers de réponse » page 198
- « Sections et clés du fichier remove.rsp » page 198
- « Ajouter des fonctionnalités à la désinstallation automatisée » page 199
- « Supprimer les modifications du fichier de configuration » page 200
- « Désinstallation sans surveillance d'OpenText eDirectory à l'aide du fichier de réponses » page 201


## Fichiers de réponse

La désinstallation d'OpenText 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 d'OpenText 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 d'OpenText 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 d'OpenText 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 d'OpenText 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 d'OpenText 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 OpenText 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 d'OpenText eDirectory dans le système local sur lequel les bibliothèques et binaires sont copiés. Par défaut, OpenText eDirectory est installé dans `C:\Novell\NDS` sauf si cela est modifié dans le fichier réponses.

**DataDir :** Jusqu'à la version 9.2 d'OpenText 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 OpenText eDirectory. Les trois types de configuration sont :

- deconfigure : effectue la déconfiguration d'OpenText eDirectory.
- uninstall : effectue la désinstallation d'OpenText eDirectory.
- full : effectue la désinstallation et la déconfiguration d'OpenText 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 d'OpenText 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 d'OpenText 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 d'OpenText 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 d'OpenText eDirectory ou la configuration combinée, supprimez les dossiers suivants :

- `C:\Novell\NDS` (emplacement par défaut, ou un autre depuis le répertoire installé d'OpenText eDirectory)
- `C:\Novell\NDS\Files` (emplacement par défaut, ou un autre depuis l'emplacement de la DIB d'OpenText 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 OpenText 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 qu'OpenText 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 d'OpenText eDirectory sous Linux

Utilisez l'utilitaire `nds-uninstall` pour désinstaller les composants d'OpenText eDirectory installés sur les ordinateurs Linux. Cet utilitaire désinstalle eDirectory de l'hôte local. Vous devez déconfigurer le serveur OpenText 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 d'OpenText 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 copier les journaux de transactions individuelles dans un autre emplacement avant de supprimer OpenText 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 d'OpenText™ eDirectory CE 24.4 (v9.3)*.

---

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 d'OpenText 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>◆ OpenText eDirectory installé à un emplacement personnalisé<br>◆ OpenText eDirectory installé par un utilisateur non-root |
| `NOVLsubag` | Il se peut que `NOVLsubag` soit utilisé par :<br>◆ OpenText eDirectory installé à un emplacement personnalisé<br>◆ OpenText eDirectory installé par un utilisateur non-root |

# Désinstallation sans surveillance d'OpenText eDirectory sous Linux

1. Supprimez les instances d'OpenText eDirectory :

   ```
   ndsconfig rm -a <user name> -w passwd -c
   ```

2. Utilisez l'un des scripts automatisés suivants pour déconfigurer OpenText 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 OpenText eDirectory, exécutez le script nds-uninstall pour supprimer les paquetages OpenText eDirectory :

```
nds-uninstall -u
```

# Avertissements concernant la désinstallation d'OpenText eDirectory

Quand vous désinstallez OpenText eDirectory et le réinstallez, le serveur OpenText 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 OpenText 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 d'OpenText eDirectory et d'installer une version précédente, car :

- cela ne rétablit pas les mises à niveau associées au schéma ;
- OpenText 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 d'OpenText 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 OpenText eDirectory est réinstallé ;
- cela ne rétablit pas les mises à niveau associées au schéma ;

# A Paquetages Linux pour OpenText eDirectory

OpenText 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 d'OpenText eDirectory. Ces paquetages contiennent des fichiers makefile qui décrivent les paramètres à prendre en compte pour installer un composant défini d'OpenText 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 OpenText 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 d'OpenText eDirectory |
| NDScommon | Contient les pages du manuel du fichier de configuration et des utilitaires d'installation et de désinstallation d'OpenText 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 OpenText eDirectory Server. Il contient également les utilitaires de gestion d'OpenText 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>◆ 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 OpenText 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 d'OpenText eDirectory et l'utilitaire de fusion des arborescences OpenText 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 OpenText 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 OpenText eDirectory. Ce paquetage dépend du paquetage NDSbase. |
| NLDAPbase | Contient les bibliothèques LDAP, leurs extensions et les outils LDAP suivants :<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 OpenText des bibliothèques d'exécution LDAP et de sécurité (Client NICI). |
| NOVLsubag | Contient les utilitaires et bibliothèques d'exécution du sous-agent SNMP d'OpenText eDirectory. Ce paquetage dépend des paquetages NICI, NDSbase et NLDAPbase. |
| NOVLpkit | Fournit des services PKI indépendants d'OpenText eDirectory. Ce paquetage dépend des paquetages NICI et NLDAPsdk. |

| Paquetage | Description |
|---|---|
| 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. |
| NDSdexvnt | Contient la bibliothèque qui gère les événements générés dans OpenText 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 pour OpenText Language Management. |
| NOVLxis | Contient les bibliothèques d'exécution pour NetIQ XIS. |
| NOVLsas | Contient les bibliothèques SAS d'OpenText. |
| NOVLntls | Contient la bibliothèque TLS d'OpenText.<br>Ce paquetage est identifié sous le nom ntls sous Linux. |
| NOVLldif2 | Contient l'utilitaire OpenText Offline Bulkload et dépend des paquetages NDSbase, NDSserv, NOVLntls, NOVLlmgnt et NICI. |
| NOVLncp | Contient les services NCP chiffrés d'OpenText 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 d'OpenText eDirectory

OpenText eDirectory 9.3 intègre un outil de diagnostic qui permet de déterminer si l'état de santé d'OpenText 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 d'OpenText 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 d'OpenText 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 OpenText 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 d'OpenText 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 209
- « Avec un utilitaire autonome » page 210


### Avec la mise à niveau

Les vérifications de l'état de santé sont exécutées par défaut à chaque mise à niveau d'OpenText 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 d'OpenText 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 d'OpenText 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`<br>`ndscheck [--version \| -v] Display version`<br>`information ndscheck [-h <hostname port]>] [-a`<br>`<admin FDN>] [-F <log file>] [-D] [-q] [--config-`<br>`file <file name>]` |
| Windows | `ndscheck`<br><br>Syntaxe :<br><br>`ndscheck [--help \| -?] Display command usage`<br>`ndscheck [--version \| -v] Display version`<br>`information ndscheck [-h <hostname port]>] [-a`<br>`<admin FDN>] [-F <log file>] [-D] [-q] [--config-`<br>`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 212.

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 211.

## 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 OpenText 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 OpenText eDirectory :

- Normal (page 211)
- Avertissement (page 211)
- Critique (page 212)

Le résultat des vérifications de l'état de santé est consigné dans un fichier journal. Pour plus d'informations, reportez-vous à la section « Fichiers journaux » page 212.

## 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 d'OpenText eDirectory.

Si l'état de santé est vérifié dans le cadre de la mise à niveau d'OpenText 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 d'OpenText 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 OpenText eDirectory

Destinée aux administrateurs, cette annexe contient des informations sur la configuration des installations OpenSLP pour OpenText eDirectory sans Novell Client.


- « Protocole SLP » page 215
- « Concepts fondamentaux de SLP » page 215
- « Paramètres de configuration » page 218


## 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 OpenText

La version OpenText 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 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 d'OpenText 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 d'OpenText 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 qu'OpenText eDirectory n'indique jamais d'étendue dans ses enregistrements. Cela ne signifie pas pour autant que l'étendue utilisée avec OpenText 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 217).

# 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 OpenText 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 OpenText 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'OpenText 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 OpenText.

| Problèmes connus | Actions suggérées |
|---|---|
| L'installation dure longtemps.<br><br>Lorsque vous installez OpenText 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 d'OpenText eDirectory échoue pour les administrateurs de conteneurs<br><br>Le programme d'installation d'OpenText 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 OpenText 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 OpenText 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 OpenText 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 OpenText eDirectory sera installé pour CHACUNE des plates-formes. Par exemple, si le premier serveur sur lequel OpenText eDirectory 9.0 doit être installé fonctionne sous Linux et qu'OpenText 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 *OpenText eDirectory 8.7.x Readme Addendum (Addendum au fichier Lisezmoi de Novell eDirectory 8.7.x)*. |

| Problèmes connus | Actions suggérées |
| --- | --- |
| Modules d'écoute par défaut pour la nouvelle interface réseau | Sous Windows, OpenText eDirectory écoute sur toutes les interfaces configurées sur l'ordinateur pour les protocoles NCP, HTTP, HTTPS, LDAP et LDAPS par défaut. Ajoutez une nouvelle adresse d'interface réseau sur l'ordinateur et redémarrez OpenText eDirectory. Ce dernier commencera à écouter automatiquement sur cette adresse et ajoutera les renvois correspondants.<br><br>**REMARQUE :** sous Linux, des interfaces doivent être ajoutées manuellement au paramètre `n4u.server.interfaces`. |
| Problèmes de réplication après la mise à niveau<br><br>Lorsque vous effectuez une mise à niveau de vers OpenText 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 OpenText Identity Console, sélectionnez **Gestion des objets**.<br>2. Dans la fenêtre **Objets>** cliquez sur l'onglet de la liste déroulante **Types** > sélectionnez Serveur NCP > et cliquez sur **Rechercher**.<br>3. Sous **Résultats de la recherche** > sélectionnez le serveur NCP.<br>4. Sous l'onglet Général, sélectionnez **Autre**.<br>5. Dans l'onglet **Modifier les objets** > cliquez sur **Attributs de valeur** .<br>6. Dans l'écran SÉLECTIONNER LES ATTRIBUTS, **sélectionnez NCPKeyMaterialName** > cliquez sur **OK**.<br><br>Par exemple, **SSLCertificateDNS**.<br>7. Exécutez le contrôleur de connectivité (limber) sur le serveur où l'attribut est modifié (étape 6). Pour plus d'informations sur l'utilisation du contrôleur de connectivité (limber), consultez le Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3). |

| Problèmes connus | Actions suggérées |
| --- | --- |
| Erreur 1603 rencontrée lors de l'application de correctifs à OpenText eDirectory<br><br>Après l'exécution de `sysprep.exe` sous Windows, l'installation ou la mise à jour d'eDirectory vers un répertoire exigeant des privilèges de groupe d'utilisateurs authentifiés peut entraîner une erreur 1603.<br><br>L'utilisateur **Administrateur** fait partie du groupe **Utilisateurs authentifiés** (tous les utilisateurs connectés) et du groupe **Administrateurs**. Selon les instructions de dépannage de Microsoft, cette adhésion à deux groupes peut provoquer des conflits avec le système UAC (contrôle d'accès utilisateur), ce qui peut bloquer les privilèges d'installation de l'administrateur. La modification des privilèges du groupe **Utilisateurs authentifiés** a résolu le problème et la mise à niveau peut s'effectuer correctement. | Pour résoudre les échecs d'installation/de mise à jour d'OpenText eDirectory sur les systèmes Windows après l'exécution de `sysprep.exe`, l'administrateur doit modifier les autorisations sur le répertoire OpenText eDirectory installé. En particulier, supprimez le groupe **Utilisateurs authentifiés** des autorisations du répertoire. Pour ce faire, accédez à l'option **Propriétés** du répertoire et à l'onglet **Sécurité**, où le groupe **Utilisateurs authentifiés** peut être supprimé de la liste des privilèges accordés. |

# 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 OpenText.

| Problèmes connus | Actions suggérées |
| --- | --- |
| Le serveur Annuaire retourne des renvois de boucle | Lorsqu'OpenText 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. |

| Problèmes connus | Actions suggérées |
| --- | --- |
| Échec de recherche de nom d'arborescence : erreur -632 lors de la configuration d'OpenText eDirectory 9.0 sous Linux | Lors de la configuration d'OpenText 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>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` |
| 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>Après avoir installé OpenText eDirectory, vous devez configurer votre environnement pour exclure le répertoire DIB stocké sur votre serveur OpenText 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 d'OpenText eDirectory pour sauvegarder votre répertoire DIB. Pour plus d'informations sur la sauvegarde d'OpenText eDirectory, voir Sauvegarde et suppression des journaux de transactions individuelles dans le *Guide d'administration d'OpenText™ eDirectory CE 24.4 (v9.3)*. |
| 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 OpenText 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 OpenText 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>Lorsque vous configurez la deuxième instance d'OpenText eDirectory sur votre hôte, vous êtes invité à utiliser le chemin par défaut. | Sélectionnez un chemin différent et poursuivez. |

| Problèmes connus | Actions suggérées |
| --- | --- |
| L'utilitaire ndsconfig affiche une erreur lors de la configuration d'eDirectory en tant qu'utilisateur non-root.<br>◆ `Échec de la définition du groupe edirAdmin`<br>◆ `AVERTISSEMENT : impossible de définir l'autorisation sur le répertoire`<br>◆ `Vérifier si le serveur est prêt à répondre aux requêtes`<br>Un utilisateur peut rencontrer ces erreurs lors de l'installation ou de la mise à niveau d'OpenText eDirectory 9.2.5 ou version ultérieure, si l'une des conditions suivantes est vraie :<br>◆ Si le groupe d'utilisateurs edirAdmin est manquant dans OpenText eDirectory.<br>◆ L'utilisateur n'est pas membre du groupe d'utilisateurs edirAdmin. | Pour résoudre ce problème, l'administrateur doit d'abord créer le groupe d'utilisateurs edirAdmin manuellement, puis ajouter l'utilisateur à ce groupe.<br>Sur le serveur sur lequel OpenText eDirectory est installé, ouvrez un terminal et exécutez les commandes suivantes :<br>◆ Pour ajouter le groupe edirAdmin, exécutez `groupadd edirAdmin`<br>◆ Pour ajouter un utilisateur au groupe edirAdmin, exécutez usermod -a -G edirAdmin <username><br>où `username` est le nom de l'utilisateur. Par exemple, pour ajouter l'utilisateur John au groupe edirAdmin, vous devez exécuter la commande :<br>`$ usermod -a -G edirAdmin john`<br>**REMARQUE :** Avant d'ajouter l'utilisateur au groupe d'utilisateurs edirAdmin, l'administrateur doit s'assurer qu'il n'est connecté à aucune session de terminal. Une fois ajouté, l'utilisateur peut se connecter et configurer OpenText eDirectory à l'aide de l'utilitaire ndsconfig. |

# Résolution des problèmes liés à plusieurs instances d'OpenText 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 OpenText.

| Problèmes connus | Actions suggérées |
| --- | --- |
| Si la première instance est inactive, HTTP ne fonctionne pas<br>Sous Linux, si OpenText 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>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 OpenText eDirectory. |

| Problèmes connus | Actions suggérées |
| --- | --- |
| 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 d'OpenText 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 OpenText.

| 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><br>`source /opt/novell/eDirectory/bin/ndspath`<br><br>Après avoir exporté la commande, entrez `ndsconfig` pour exécuter l'utilitaire ndsconfig au lieu de `./ndsconfig`. |

| Problèmes connus | Actions suggérées |
| --- | --- |
| 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><br>Pour éviter ce problème, saisissez le nom du paramètre à obtenir comme suit :<br><br>`ndsconfig get <paramètre_à_afficher>`<br><br>Pour une liste des paramètres, consultez la page du manuel `nds.conf`. |
| La variable d'environnement `NDSD_NLDAP_IGNORE_CRITICALITY = True` est manquante dans le fichier `/etc/opt/novell/eDirectory/conf/env` lors de la mise à niveau d'OpenText eDirectory sous OES 2018SP2. | Pour résoudre ce problème, vous devez exécuter manuellement la commande de mise à niveau ndsconfig pour ajouter la variable d'environnement `NDSD_NLDAP_IGNORE_CRITICALITY = True` dans le fichier `/etc/opt/novell/eDirectory/conf/env`. |

# 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 OpenText 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 OpenText Certificate Server sur un serveur non répertorié en saisissant 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 Identity Console pour créer une autorité de certification organisationnelle et des certificats de serveur et exporter la racine approuvée.

### 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 OpenText 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 OpenText 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'OpenText 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 Identity Console pour modifier manuellement l'association par défaut. La procédure suivante vous explique comment effectuer la modification :

1. Connectez-vous à Identity Console > **Gestion des objets** > dans le menu déroulant **Type** > sélectionnez l'objet Serveur http > cliquez sur **Rechercher**.
2. Dans le menu **Résultats de la recherche** > sélectionnez le serveur http - <server name/CN>.
3. Dans l'onglet **Modifier les objets** > cliquez sur **Attributs de valeur** .

4 Dans l'écran **SÉLECTIONNER LES ATTRIBUTS** > recherchez l'attribut httpKeyMaterialObjects > cliquez sur **Éditer** .

5 Modifiez l'association de l'objet Serveur HTTP à DNS de certificat SSL > cliquez sur **OK**.

# Résolution des problèmes d'installation

Si le correctif de pont n'est pas appliqué dans un environnement OpenText eDirectory 9.2.8 avec EBA activé, l'ajout d'une réplique OpenText eDirectory 9.3 envoie les messages d'erreur suivants :

- **Linux** : le correctif de pont n'est pas appliqué sur un ou plusieurs serveurs EBA de l'anneau.
- **Windows** : les informations d'identification sont incorrectes. Vérifiez et réessayez.

**Solution de contournement :** Appliquez le correctif de pont à tous les serveurs.