Guide de démarrage rapide de NetIQ Identity Manager Standard Edition

Février 2015

Ce document fournit les instructions d'installation, de configuration et de mise à niveau d'Identity Manager 4.5 Standard Edition.

1 Présentation

Identity Manager 4.5 Standard Edition dispose des fonctions suivantes :

- Provisioning automatique basé sur les rôles
- Gestion des mots de passe (réinitialisation des mots de passe en self-service)
- Identity Reporting
- Structure de création de paquetages de contenu
- Single Sign-On (One SSO)
- Analyzer
- Designer

  Pour plus d'informations, reportez-vous au *Guide d'installation de NetIQ Identity Manager*.

IMPORTANT : les modules d'intégration pour Identity Manager Standard Edition et Advanced Edition restent les mêmes.

Pour plus d'informations sur les nouvelles fonctionnalités, les améliorations apportées et les fonctions qui ont été modifiées ou ne sont plus prises en charge dans cette version, reportez-vous aux Notes de version.

2 Composants

Identity Manager 4.5 Standard Edition comprend les composants suivants :

- Coffre-fort d'identité
- iManager
- Moteur Identity Manager
- Designer
- Analyzer
- Chargeur distant
- Service d'audit d'événements (EAS)
- Tomcat (serveur d'applications pris en charge)
- Single Sign-On (One SSO)
- Réinitialisation des mots de passe en self-service (SSPR, Self Service Password Reset)
- Identity Reporting

Pour plus d'informations sur l'interaction entre les composants d'Identity Manager, reportez-vous à la section « Introduction » du *Guide d'installation de NetIQ Identity Manager*.

3 Installation d'Identity Manager 4.5 Standard Edition

Téléchargez le logiciel sur le site Web du produit. Les fichiers `.iso` suivants contiennent l'image DVD pour l'installation des composants d'Identity Manager :

- `Identity_Manager_4.5_Linux_Standard.iso`
- `Identity_Manager_4.5_Windows_Standard.iso`

Les fichiers d'installation sont situés dans le répertoire `products` du paquetage d'installation d'Identity Manager. Pour plus d'informations sur les emplacements d'installation par défaut, reportez-vous à la section relative à la localisation des chemins d'installation dans les Notes de version.

NetIQ vous recommande de passer en revue les conditions préalables à l'installation dans les Notes de version, puis de suivre la liste de contrôle ci-dessous dans l'ordre indiqué. Chaque tâche fournit de brèves informations ainsi qu'une référence à l'emplacement où vous pourrez trouver des détails complets. Pour plus d'informations sur l'installation de chaque composant d'Identity Manager, reportez-vous au *Guide d'installation de NetIQ Identity Manager*.

Tâche	Remarques
1. Conditions préalables	◆ Passez en revue la configuration système requise pour chaque composant afin de veiller à ce que votre ordinateur ou les images virtuelles répondent aux conditions requises pour l'installation. Pour savoir quel composant spécifique peut être installé sur quel système d'exploitation, reportez-vous à la section Sélection d'une plate-forme de système d'exploitation pour Identity Manager dans le *Guide d'installation de NetIQ Identity Manager*. ◆ Pour plus d'informations sur les conditions préalables, la configuration système requise pour l'ordinateur, l'installation, la mise à niveau ou la migration, consultez la section Considérations et conditions préalables à l'installation du *Guide d'installation de NetIQ Identity Manager*.
2. Planification de votre installation	Reportez-vous à la section « Planification de l'installation d'Identity Manager » dans le *Guide d'installation de NetIQ Identity Manager*.
3. Ordre d'installation	Assurez-vous que vous installez les composants dans l'ordre suivant, car les programmes d'installation de certains composants ont besoin d'informations concernant des composants installés précédemment. 1. eDirectory 2. iManager 3. Moteur Identity Manager 4. Designer 5. Analyzer 6. Service d'audit d'événements (EAS) 7. Tomcat (serveur d'applications pris en charge) 8. Composants de gestion des mots de passe et Single Sign-On 9. Identity Reporting **IMPORTANT :** Les programmes d'installation installent les composants d'Identity Manager

Tâche	Remarques
4. Installation et configuration d'eDirectory	Installez le correctif eDirectory 8.8.8 Patch 3 ou une version ultérieure. Pour obtenir des instructions d'installation, reportez-vous à la section « Installation du coffre-fort d'identité » du *Guide d'installation de NetIQ Identity Manager*. ◆ Après l'installation et la configuration d'eDirectory, arrêtez les services eDirectory. ◆ Appliquez le correctif eDirectory le plus récent. ◆ Démarrez l'installation des services eDirectory.
5. Installation et configuration d'iManager	Installez le correctif iManager 2.7.7 Patch 2 ou une version ultérieure. Pour que l'audit fonctionne, installez le correctif iManager 2.7.7 Patch 3 ou une version ultérieure. Pour obtenir des instructions d'installation, reportez-vous à la section « Installation d'iManager » dans le *Guide d'installation de NetIQ Identity Manager*.
6. Installation du moteur Identity Manager, des pilotes et des plug-ins	Pour obtenir des instructions d'installation, reportez-vous à la section « Installation du moteur, des pilotes et des plug-ins Identity Manager » dans le *Guide d'installation de NetIQ Identity Manager*. **REMARQUE :** le programme d'installation ne crée pas l'objet DirMXL-PasswordPolicy dans le coffre-fort d'identité. Après l'installation du moteur Identity Manager, lancez Designer et créez l'ensemble de pilotes. Installez le paquetage des stratégies de mot de passe universel par défaut Identity Manager qui contient la stratégie `DirMXL-PasswordPolicy`. Ajoutez cette stratégie à l'ensemble de pilotes. Répétez cette procédure pour chaque ensemble de pilotes Identity Manager dans le coffre-fort d'identité.
7. Installation du service d'audit d'événements (EAS)	Pour obtenir des instructions d'installation, reportez-vous à la section « Installation du service d'audit d'événements (EAS) » du *Guide d'installation de NetIQ Identity Manager*.
8. Installation de Tomcat	Ne sélectionnez Tomcat que pour déployer Identity Reporting. Il n'est pas nécessaire d'installer une base de données PostgreSQL car vous n'installez pas RBPM. Pour obtenir des instructions d'installation, reportez-vous à la section « Installation de PostgreSQL et de Tomcat » du *Guide d'installation de NetIQ Identity Manager*. **REMARQUE :** Si vous installez Tomcat sur un ordinateur sur lequel iManager est installé, n'utilisez pas le port 8080 pour Tomcat. Si les autres ports sont déjà utilisés, modifiez-les au cours de l'installation.

Tâche	Remarques

9. Installation des composants de gestion des mots de passe et Single Sign-On	Pour obtenir des instructions d'installation, reportez-vous à la section « Installation des composants Single Sign-On et Gestion des mots de passe » du *Guide d'installation de NetIQ Identity Manager*.
	
	Après l'installation des composants Single Sign-On et Gestion des mots de passe, procédez comme suit :
	
	◆ **Étendez le schéma eDirectory.** Cette tâche permet d'étendre votre schéma eDirectory en ajoutant des définitions d'attributs et une classe d'objet
	
	1. Copiez le contenu suivant dans un fichier et enregistrez-le avec l'extension `.ldif`.
	
	`dn: o="Your Organization"`
	`changetype: modify`
	`add: ACL`
	`ACL: 7#subtree#[This]#pwmResponseSet`
	
	2. Dans iManager, accédez à **Rôles et tâches > Schéma > Étendre le schéma** > **Importer les données d'un fichier sur le disque**, puis cliquez sur **Suivant**.
	
	3. Cliquez sur **Fichier à importer** et recherchez le fichier `.ldif`. Vérifiez que ce fichier contient le nom de conteneur `Organization` en tant que `o="Votre organisation"` ; dans le cas contraire, ajoutez le nom de conteneur `Organization` existant et cliquez sur **Suivant**.
	
	4. Spécifiez des valeurs dans les champs suivants, cliquez sur **Suivant**, puis sur **Terminer**.
	
	◆ **Nom DNS/Adresse IP du serveur**
	◆ **Connexion d'authentification**
	◆ **DN utilisateur**
	◆ **Mot de passe**
	
	REMARQUE : Le serveur LDAP n'accepte pas de connexion non sécurisée par défaut. Vous pouvez utiliser une authentification SSL ou modifier les paramètres du serveur pour autoriser les connexions en texte clair.
	
	Une fois l'importation du fichier terminée, la fenêtre affiche un message indiquant la réussite de l'importation.
	
	◆ **Configurez l'audit SSL.** Si vous avez activé l'audit lors de l'installation de SSPR, vous devez fournir un certificat SSL pour auditer les événements. Pour obtenir des instructions sur l'importation du certificat SSL et l'audit des événements, reportez-vous à la section Setting Up SSL Auditing (https://www.netiq.com/documentation/sspr3/adminguide/data/b14knaes.html) (Configuration de l'audit SSL) du manuel *NetIQ Self Service Password Reset 3.2 Administration Guide* (Guide d'administration de NetIQ Self Service Password Reset 3.2)

Tâche	Remarques
10. Installation et configuration d'Identity Reporting	1. Pour plus d'informations sur les composants et la structure nécessaires pour Identity Reporting, reportez-vous à la section « Installation des composants du module Identity Reporting » du *Guide d'installation de NetIQ Identity Manager*. 2. Pour installer Identity Reporting à l'aide d'un assistant d'installation, au format interface graphique ou à partir de la console, reportez-vous à la section Section 3.1, « Installation d'Identity Reporting », page 5. 3. Pour effectuer une installation silencieuse, reportez-vous à la section Section 3.1.2, « Installation silencieuse d'Identity Reporting », page 10. 4. Pour configurer les pilotes, reportez-vous à la section « Configuration des pilotes pour Identity Reporting » du *Guide d'installation de NetIQ Identity Manager*. 5. Pour déployer les API REST pour Identity Reporting, reportez-vous à la section « Déploiement des API REST pour Identity Reporting » du *Guide d'installation de NetIQ Identity Manager*. **REMARQUE :** vous devez importer des définitions de rapport dans Identity Reporting. Pour les télécharger, utilisez la page de téléchargement au sein de l'application de génération de rapports.
11. Activation d'Identity Manager	Activez vos composants Identity Manager. Pour plus d'informations, reportez-vous à la section « Activation d'Identity Manager » du *Guide d'installation de NetIQ Identity Manager*.

3.1 Installation d'Identity Reporting

Le paquetage d'installation d'Identity Manager inclut les fichiers d'installation dans les répertoires `products/EAS` et `products/Reporting` au sein du fichier image `.iso`. Par défaut, le programme d'installation enregistre les composants aux emplacements suivants :

- **Linux** : `/opt/netiq/idm/apps/IDMReporting`
- **Windows** : `C:\netiq\idm\apps\IDMReporting`

3.1.1 Installation d'Identity Reporting avec l'assistant

La procédure suivante explique comment installer Identity Reporting avec l'assistant d'installation, au format interface graphique ou à partir de la console.

Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise répertoriée dans la section « Configuration système requise pour Identity Reporting » du *Guide d'installation de NetIQ Identity Manager* ainsi que les Notes de version.

1. Assurez-vous que la base de données SIEM est en cours d'exécution dans votre service d'audit d'événements.

   Le programme d'installation crée les tables dans la base de données et vérifie la connectivité. Le programme installe également un fichier JAR pour le pilote JDBC PostgreSQL et utilise automatiquement ce fichier pour établir la connectivité à la base de données.
2. Connectez-vous à l'ordinateur sur lequel vous voulez installer Identity Reporting.
3. Arrêtez le serveur d'applications. Dans ce cas, il s'agit de Tomcat.
4. (Conditionnel) Si vous disposez du fichier `.iso` pour le paquetage d'installation d'Identity Manager, accédez au répertoire contenant les fichiers d'installation d'Identity Reporting. Ceux-ci sont situés par défaut dans le répertoire `products/Reporting/`.

5 (Facultatif) Si vous avez téléchargé les fichiers d'installation d'Identity Reporting à partir du site Web de téléchargement NetIQ, procédez de la manière suivante :

5a Accédez au fichier `.tgz` pour localiser l'image téléchargée.

5b Lancez l'extraction du contenu du fichier dans un dossier sur l'ordinateur local.

6 À partir du répertoire comprenant les fichiers d'installation, effectuez l'une des opérations suivantes :

- **Linux (console)** : Entrez `./rpt-install.bin -i console`
- **Linux (interface graphique)** : Entrez `./rpt-install.bin`
- **Windows** : Exécutez `rpt-install.exe`

7 Dans le programme d'installation, indiquez la langue que vous souhaitez utiliser pour l'installation, puis cliquez sur **OK**.

8 Lisez attentivement le texte d'introduction, puis cliquez sur **Suivant**.

9 Acceptez l'accord de licence, puis cliquez sur **Suivant**.

10 Pour terminer l'installation guidée, spécifiez des valeurs pour les paramètres suivants :

- **Dossier d'installation**

  Permet d'indiquer où sont stockés les fichiers d'installation.

- **Détails de la connexion au coffre-fort d'identité**

  Représente les paramètres de connexion pour le coffre-fort d'identité. Pour modifier ces paramètres une fois l'installation terminée, utilisez l'utilitaire de configuration de la création de rapports (`configupdate.sh`) situé dans le répertoire `/opt/netiq/idm/apps/IdentityReporting/bin/lib`.

  Serveur du coffre-fort d'identité

  Indique le nom DNS ou l'adresse IP du serveur du coffre-fort d'identité.

  Port LDAP sécurisé

  Spécifie le port LDAP qu'Identity Reporting doit utiliser pour communiquer avec le coffre-fort d'identité.

- **Plate-forme du serveur d'applications**

  Permet d'indiquer le serveur d'applications qui va exécuter le fichier core (`IDMRPT-Core.war`), le fichier de l'API REST EASREST (`easrestapi.war`), le fichier Webstart d'EAS (`easwebstart.war`) et le fichier WAR de référence de l'API REST Reporting (`rptdoc.war`). Pour Identity Reporting, NetIQ prend en charge uniquement Tomcat.

  REMARQUE : Ne modifiez pas les noms de ces fichiers WAR. Si vous modifiez les noms de fichier, le processus de déploiement échouera.

- **Détails du serveur d'applications**

  Permet d'indiquer le chemin d'accès au répertoire de déploiement ou des applications Web pour l'instance de Tomcat. Par exemple : `/opt/netiq/idm/apps/tomcat/webapps`.

- **Connexion au serveur d'applications**

  Représente les paramètres de l'URL permettant aux utilisateurs de se connecter à Identity Reporting sur le serveur d'applications. Par exemple, `https:myserver.mycompany.com:8080`.

  REMARQUE : Si OSP s'exécute sur une autre instance du serveur d'applications, vous devez également sélectionner l'option **Se connecter à un serveur d'authentification externe** et spécifier les valeurs du serveur OSP.

Protocole

Permet d'indiquer si vous voulez utiliser *http* ou *https*. Pour utiliser SSL pour les communications, entrez `https`.

Nom d'hôte

Permet d'indiquer le nom DNS ou l'adresse IP du serveur d'applications. N'utilisez pas `localhost`.

Port

Permet d'indiquer le port que le serveur d'applications doit utiliser pour communiquer avec Identity Manager.

Se connecter à un serveur d'authentification externe

Permet d'indiquer si une autre instance du serveur d'applications héberge le serveur d'authentification (OSP). Le serveur d'authentification dispose de la liste des utilisateurs qui peuvent se connecter à Identity Reporting.

Si vous sélectionnez cette option, indiquez également les valeurs correspondantes dans les champs **Protocole**, **Nom d'hôte** et **Port** pour le serveur d'authentification.

- **Détails du serveur d'authentification**

Permet d'indiquer le mot de passe que vous voulez créer pour que le service Identity Reporting puisse se connecter au client OSP sur le serveur d'authentification.

Pour modifier ce mot de passe après l'installation, utilisez l'utilitaire de configuration de la création de rapports.

- **Service d'audit d'événements**

Permet d'indiquer si vous voulez utiliser le service d'audit d'événements (Event Auditing Service, EAS) de NetIQ pour suivre les événements dans Identity Reporting.

Si vous sélectionnez cette option, indiquez également le nom DNS ou l'adresse IP du serveur qui héberge EAS.

- **Détails de la base de données**

Permet d'indiquer les paramètres SIEM de votre base de données.

Port de base de données

Permet d'indiquer le port de la base de données SIEM. La valeur par défaut est 15432.

Mot de passe du DBA

Permet d'indiquer le mot de passe du compte administrateur pour la base de données.

Si vous utilisez EAS, le programme d'installation crée ce mot de passe pour le compte `dbauser`.

Mot de passe de l'utilisateur idmrptsrv

Permet d'indiquer le mot de passe du propriétaire du schéma et des vues Identity Reporting dans la base de données.

Le programme d'installation crée ce mot de passe pour le compte `idmrptsrv`.

Mot de passe idmrptuser

Permet d'indiquer le mot de passe du compte permettant d'accéder à la base de données pour générer des rapports.

Le programme d'installation crée ce mot de passe pour le compte `idmrptuser`.

Tester la connexion à la base de données

Permet d'indiquer si vous souhaitez que le programme d'installation teste les valeurs spécifiées pour la base de données.

Le programme d'installation tente une connexion lorsque vous cliquez sur **Suivant** ou appuyez sur **Entrée**.

REMARQUE : Vous pouvez poursuivre l'installation même si la connexion à la base de données échoue. Toutefois, une fois l'installation terminée, vous devrez créer manuellement les tables et la connexion avec la base de données.

- **Détails de l'authentification**

  Il s'agit des paramètres relatifs au serveur d'authentification. Pour modifier ces paramètres une fois l'installation terminée, utilisez l'utilitaire de configuration de la création de rapports.

  Conteneur de base

  Permet d'indiquer le DN du conteneur qui répertorie les utilisateurs pouvant se connecter à Identity Reporting. Par exemple, `o=data`.

  REMARQUE : Dans le cas où le DN contient des caractères spéciaux, il se peut que vous ayez besoin de les faire précéder d'un caractère d'échappement. Pour plus d'informations, reportez-vous à la section 2.4 du document RFC 2253/4514.

  Attribut de connexion

  Permet de spécifier l'attribut que vous voulez utiliser pour lancer une recherche dans la sous-arborescence du conteneur des utilisateurs. Par exemple, `cn`

  Paramètres régionaux cible

  Permet d'indiquer la langue à utiliser pour Identity Reporting. L'application utilise les paramètres régionaux spécifiés pour traiter les recherches.

- **Références du coffre-fort d'identité**

  Représente les références du coffre-fort d'identité pour le serveur de ce dernier.

  Administrateur du coffre-fort d'identité

  Indique le DN de l'administrateur autorisé à accorder et révoquer des rôles pour d'autres utilisateurs.

  Mot de passe de l'administrateur du coffre-fort d'identité

  Spécifie le mot de passe de l'administrateur.

  Chemin du fichier Keystore

  Indique le chemin d'un fichier Keystore qui contient les certificats à approuver dans les connexions SSL. Par défaut, il s'agit du même chemin que celui créé par le programme d'installation OSP SSPR.

  Mot de passe Keystore

  Spécifie le mot de passe pour l'ouverture du fichier Keystore. Le mot de passe par défaut est *changeit*.

  DN du conteneur du rôle d'administrateur de création de rapports

  Indique le DN du conteneur dans lequel le programme d'installation crée le rôle reportAdmin.

  DN de l'administrateur de création de rapports

  Indique le DN de l'utilisateur auquel le programme d'installation assigne le rôle reportAdmin.

  REMARQUE : Assurez-vous que le conteneur dans lequel réside le rôle reportAdmin n'inclut aucun objet portant le même nom.

- **Chemin du dossier de la base JRE**

  Représente l'emplacement du JRE utilisé par le serveur d'applications.

  Dossier de la base JRE Java

  Spécifie le chemin du JRE utilisé par le serveur d'applications. Par exemple : `/opt/netiq/idm/apps/jre`

- **Envoi de messages électroniques**

  Il s'agit des paramètres relatifs au serveur SMTP qui envoie les notifications de rapport. Pour modifier ces paramètres une fois l'installation terminée, utilisez l'utilitaire de configuration de la création de rapports.

  Adresse électronique par défaut

  Spécifie l'adresse électronique qu'Identity Reporting doit utiliser pour envoyer des notifications par message électronique.

  Serveur SMTP

  Permet d'indiquer le nom DNS ou l'adresse IP de l'hôte de messagerie électronique SMTP utilisé par Identity Reporting pour les notifications. N'utilisez pas `localhost`.

  Port du serveur SMTP

  Permet d'indiquer le numéro de port du serveur SMTP. La valeur par défaut est 465.

  Utiliser SSL pour SMTP

  Permet d'indiquer si vous voulez utiliser le protocole SSL pour les communications avec le serveur SMTP.

  Exiger l'authentification du serveur

  Permet d'indiquer si vous voulez demander une authentification pour les communications avec le serveur SMTP.

  Si vous sélectionnez cette option, indiquez également les informations d'identification du serveur de messagerie électronique.

- **Détails du rapport**

  Il s'agit des paramètres de gestion des rapports finalisés.

  Conserver les rapports terminés pendant

  Permet d'indiquer pendant combien de temps les rapports sont conservés dans Identity Reporting avant d'être supprimés. Par exemple, pour six mois, tapez `6` puis sélectionnez **Mois**.

  Emplacement des définitions de rapport

  Permet d'indiquer où vous voulez stocker les définitions de rapport. Par exemple, `/opt/netiq/IdentityReporting`.

- **Novell Identity Audit**

  Il s'agit des paramètres relatifs à l'audit d'Identity Reporting.

  Activer l'audit d'Identity Reporting

  Permet d'indiquer si vous voulez envoyer les événements consignés dans les journaux vers un serveur d'audit.

  Si vous sélectionnez cette option, indiquez également l'emplacement du cache des journaux d'audit.

  Dossier de mise en cache des journaux d'audit

  Applicable uniquement lorsque vous activez la fonction d'audit pour Identity Reporting.

  Permet d'indiquer l'emplacement du dossier de mise en cache à utiliser à des fins d'audit. Par exemple, `/opt/novell/Identity Reporting`.

REMARQUE : si vous activez la fonction d'audit, assurez-vous que le fichier `logevent` contient des chemins valides pour le répertoire du cache et le fichier nauditpa.jar. Si ces paramètres ne sont pas définis correctement, Identity Reporting ne démarre pas.

- **Certificats NAudit**

  Applicable uniquement lorsque vous activez la fonction d'audit pour Identity Reporting.

  Il s'agit des paramètres relatifs au service NAudit, lequel transmet les événements depuis Identity Reporting vers EAS.

  Préciser un certificat existant / Générer un certificat

  Indique si vous souhaitez utiliser un certificat existant pour le serveur NAudit ou en créer un nouveau.

  Entrez une clé publique

  Applicable uniquement si vous voulez utiliser un certificat existant.

  Permet de répertorier les certificats de clé publique personnalisés utilisables par le service NAudit pour authentifier les messages d'audit envoyés à EAS.

  Entrez une clé RSA

  Applicable uniquement si vous voulez utiliser un certificat existant.

  Permet d'indiquer le chemin d'accès au fichier de clé privée personnalisé utilisable par le service NAudit pour authentifier les messages d'audit envoyés à EAS.

11 Vérifiez les informations affichées dans la fenêtre Résumé avant installation, puis cliquez sur **Installer**.

3.1.2 Installation silencieuse d'Identity Reporting

Une installation silencieuse (non interactive) n'affiche aucune interface utilisateur et ne soumet aucune question à l'utilisateur. Au lieu de cela, le système utilise les informations contenues dans un fichier `.properties`. Vous pouvez exécuter l'installation silencieuse avec le fichier par défaut ou modifier le fichier pour personnaliser le processus d'installation.

Pour préparer l'installation, passez en revue les conditions préalables et la configuration système requise répertoriée dans la section « Configuration système requise pour Identity Reporting » du *Guide d'installation de NetIQ Identity Manager*. Reportez-vous également aux notes de version relatives à votre édition.

1 (Facultatif) Pour ne pas avoir à spécifier dans le fichier `.properties` les mots de passe des comptes administrateur en vue d'une installation silencieuse, utilisez la commande `set` ou `export`. Exemples :

- **Linux** : `export NOVL_ADMIN_PWD=`*`myPassWord`*
- **Windows** : `set NOVL_ADMIN_PWD=`*`myPassWord`*

La procédure d'installation silencieuse lit les mots de passe à partir de l'environnement (au lieu du fichier `.properties`).

Indiquez les mots de passe suivants :

NETIQ_DB_RPT_USER_PASSWORD

Permet d'indiquer le mot de passe de l'administrateur de la base de données SIEM.

NETIQ_IDM_SRV_PWD

Permet de spécifier le mot de passe du propriétaire des objets et schémas de la base de données pour la création de rapports.

NETIQ_IDM_USER_PWD

Permet d'indiquer le mot de passe de l'utilisateur idmrptuser, lequel dispose d'un accès en lecture seule aux données des rapports.

NETIQ_EAS_SYSTEM_PASSWORD

Permet d'indiquer le mot de passe pour le serveur EAS.

Vous pouvez copier le mot de passe système à partir de la propriété système indiquée dans le fichier `activemqusers.properties` figurant sur l'ordinateur sur lequel EAS est installé.

NETIQ_ADMIN_PWD

(Facultatif) Pour autoriser les recherches sur le sous-conteneur lors de la connexion, vous devez indiquer le mot de passe du compte administrateur LDAP.

NETIQ_SMTP_PASSWORD

(Facultatif) Pour utiliser l'authentification pour les communications électroniques, vous indiquez le mot de passe de l'utilisateur SMTP par défaut.

2 Pour spécifier les paramètres d'installation, procédez comme suit :

2a Vérifiez que le fichier `.properties` figure dans le même répertoire que le fichier d'exécution de l'installation.

Par commodité, NetIQ fournit deux fichiers `.properties`. Par défaut, ils figurent dans le répertoire `products/Reporting` de l'image `.iso` :

- Le fichier `rpt_installonly.properties` vous permet d'utiliser les paramètres d'installation par défaut.
- Vous utilisez le fichier `rpt_configonly.properties` pour personnaliser les paramètres d'installation.

2b Dans un éditeur de texte, ouvrez le fichier `.properties`.

2c Spécifiez les valeurs des différents paramètres. Pour obtenir une description de ces paramètres, reportez-vous à l'Étape 10 page 6.

2d Enregistrez et fermez le fichier.

3 Pour lancer la procédure d'installation, saisissez l'une des commandes suivantes :

- **Linux** : `./rpt-install.bin -i silent -f` *`path_to_properties_file`*
- **Windows** : `./rpt-install.exe -i silent -f` *`path_to_properties_file`*

REMARQUE : Si le fichier `.properties` se trouve dans un autre répertoire que celui du script d'installation, vous devez en indiquer le chemin complet. Le script décompresse les fichiers requis dans un répertoire temporaire et lance l'installation en mode silencieux.

3.1.3 Tâches de post-installation

- Pour modifier les propriétés après l'installation, exécutez l'utilitaire de mise à jour de configuration en fonction de votre plate-forme.
  - **Linux :** Exécutez `configupdate.sh` à partir de `/opt/netiq/idm/apps/IdentityReporting/bin/lib`.
  - **Windows :** Exécutez `configupdate.bat` à partir de `C:\netiq\idm\apps\IdentityReporting\bin\lib`.

Si vous utilisez l'outil de configuration pour modifier un paramètre d'Identity Reporting, vous devez redémarrer le serveur d'applications pour que les modifications soient prises en compte. Toutefois, vous n'avez pas à redémarrer le serveur après avoir effectué des modifications dans l'interface utilisateur Web pour Identity Reporting.

- Accédez à l'URL de création de rapports en tant qu'administrateur de rapports. L'URL se présente selon le modèle suivant : `http://server:port/IDMRPT/`. Assurez-vous que l'authentification et l'autorisation ont réussi. NetIQ recommande de ne pas essayer de vous connecter avec des droits administratifs insuffisants.

  IMPORTANT : Si vous vous êtes connecté à l'application de création de rapports sous l'identité d'un utilisateur ne disposant pas des droits appropriés, l'option de déconnexion et le lien Accueil ne s'affichent pas.

4 Mise à niveau d'Identity Manager

Pour Identity Manager 4.0.2 Standard Edition, NetIQ prend en charge les chemins de mise à niveau suivants :

- Identity Manager 4.0.2 Standard Edition vers Identity Manager 4.5 Standard Edition
- Identity Manager 4.5 Standard Edition vers Identity Manager 4.5 Advanced Edition

Vous ne pouvez pas effectuer une mise à niveau directe d'Identity Manager 4.0.2 Standard Edition vers Identity Manager 4.5 Advanced Edition. Cependant, vous pouvez choisir l'une des approches suivantes pour effectuer la mise à niveau :

- Mise à niveau d'Identity Manager 4.0.2 Standard Edition vers Identity Manager 4.5 Standard Edition, suivie d'une mise à niveau vers Identity Manager 4.5 Advanced Edition.
- Mise à niveau d'Identity Manager 4.0.2 Standard Edition vers Identity Manager 4.0.2 Advanced Edition, suivie d'une mise à niveau vers Identity Manager 4.5 Advanced Edition.

4.1 Mise à niveau d'Identity Manager 4.0.2 Standard Edition vers Identity Manager 4.5 Advanced Edition

Pour effectuer la mise à niveau, NetIQ vous recommande de consulter les Conditions préalables à la mise à niveau dans les Notes de version, puis d'exécuter les tâches suivantes dans le même ordre :

Tâche	Remarques
1. Vérification des différences entre une mise à niveau et une migration	Pour plus d'informations, reportez-vous à la section « Notions de mise à niveau et de migration » du *Guide d'installation de NetIQ Identity Manager*.
2. Mise à niveau vers Identity Manager 4.0. 2	Une mise à niveau ou une migration directe vers Identity Manager 4.5 à partir d'une version antérieure à 4.0.2 n'est pas possible. Pour plus d'informations, reportez-vous au *Guide d'installation de NetIQ Identity Manager 4.0.2*.
3. Obtention des fichiers nécessaires pour la mise à niveau/ migration	Assurez-vous que vous disposez de la dernière version du kit d'installation pour la mise à niveau/migration d'Identity Manager vers la version 4.5 Standard Edition.
4. Interaction entre les composants d'Identity Manager	Pour plus d'informations, reportez-vous à l'« Introduction » du *Guide d'installation de NetIQ Identity Manager*.

Tâche	Remarques
5. Exigences système	Assurez-vous que votre ordinateur dispose des prérequis logiciels et matériels pour une version plus récente d'Identity Manager. Pour plus d'informations, consultez la section « Considérations et conditions préalables à l'installation » du *Guide d'installation de NetIQ Identity Manager* et les Notes de parution qui l'accompagnent.
6. Sauvegarde du projet, de la configuration de pilote et des bases de données actuels	Pour plus d'informations, reportez-vous à la section « Sauvegarde de la configuration actuelle » du *Guide d'installation de NetIQ Identity Manager*.
7. Mise à niveau d'Analyzer	Effectuez la mise à niveau vers la version la plus récente de Designer. Pour plus d'informations, reportez-vous à la section « Mise à niveau d'Analyzer » du *Guide d'installation de NetIQ Identity Manager*.
8. Mise à niveau de Designer	Effectuez la mise à niveau vers la version la plus récente de Designer. Pour plus d'informations, reportez-vous à la section « Mise à niveau de Designer » du *Guide d'installation de NetIQ Identity Manager*.
9. Mettre à niveau eDirectory	Sur le serveur exécutant Identity Manager, mettez à niveau edirectory vers la version la plus récente et installez les derniers correctifs. Pour plus d'informations, reportez-vous au manuel *NetIQ eDirectory 8.8 Installation Guide* (Guide d'installation de NetIQ eDirectory 8.8) et aux notes de version d'Identity Manager.
10. Mise à niveau d'iManager	Mettez à niveau iManager vers la version et le correctif les plus récents. Pour obtenir les instructions de mise à niveau, reportez-vous à la section « Mise à niveau d'iManager » du *Guide d'installation de NetIQ Identity Manager*.
11. Arrêtez les pilotes	Arrêtez les pilotes associés au serveur sur lequel vous avez installé le moteur Identity Manager (méta-annuaire). Pour plus d'informations, reportez-vous à la section « Arrêt des pilotes » du *Guide d'installation de NetIQ Identity Manager*.
12. Mettez à niveau le moteur Identity Manager	Pour plus d'informations, reportez-vous à la section « Mise à niveau d'Identity Manager » du *Guide d'installation de NetIQ Identity Manager*. **REMARQUE :** si vous migrez le moteur Identity Manager vers un nouveau serveur, vous pouvez utiliser les mêmes répliques eDirectory que celles figurant sur le serveur Identity Manager actuel. Pour plus d'informations, reportez-vous à la section « Migration d'Identity Manager vers un nouveau serveur » du *Guide d'installation de NetIQ Identity Manager*
13. (Conditionnel) Mise à niveau du chargeur distant	Si l'un des pilotes de l'ensemble de pilotes du moteur Identity Manager est un pilote de chargeur distant, mettez à niveau les serveurs de chargeur distant pour chaque pilote. Pour plus d'informations, reportez-vous à la section « Mise à niveau du chargeur distant » du *Guide d'installation de NetIQ Identity Manager*.
14. (Conditionnel) Mise à niveau des paquetages	Si vous utilisez des paquetages plutôt que des fichiers de configuration de pilote, mettez à niveau les paquetages sur les pilotes existants afin d'obtenir de nouvelles stratégies. Pour plus d'informations, reportez-vous à la section « Mise à niveau des pilotes Identity Manager » du *Guide d'installation de NetIQ Identity Manager*. Cette action n'est requise que si une version plus récente d'un paquetage est disponible et qu'une nouvelle fonction est incluse dans les stratégies d'un pilote que vous souhaitez ajouter à votre ensemble de pilotes existant.

Tâche	Remarques
15. Application de la clé d'activation d'Identity Manager 4.5 Standard Edition	Veillez à bien activer Identity Manager 4.5 Standard Edition dans iManager. Si vous n'appliquez pas l'activation, le moteur Identity Manager et les pilotes s'exécutent en mode d'évaluation.
16. Suppression de fichiers et dossiers RBPM et Identity Reporting	Supprimez des fichiers et dossiers RBPM et Identity Reporting de votre serveur d'applications actuel. Pour ce faire, vous devez effectuer les opérations suivantes : 1. (Conditionnel) Désinstallez les fichiers WAR RBPM et Identity Reporting de votre serveur d'applications. À cette fin, suivez les instructions de la documentation propre à votre serveur d'applications. 2. Arrêtez le serveur d'applications sur lequel RBPM et Identity Reporting sont installés. 3. Exécutez le programme de désinstallation d'Identity Reporting afin de supprimer les fichiers et dossiers d'installation. Pour plus d'informations, reportez-vous à la section « Désinstallation d'Identity Reporting » du *Guide d'installation de NetIQ Identity Manager*. 4. Exécutez le programme de désinstallation de RBPM pour supprimer les fichiers et dossiers d'installation. Pour plus d'informations, reportez-vous à la section « Désinstallation du module de provisioning basé sur les rôles » du *Guide d'installation de NetIQ Identity Manager*.
17. Suppression des pilotes de l'application utilisateur et du service de rôles et de ressources	Supprimez les pilotes de l'application utilisateur et du service de rôles et de ressources de l'ensemble de pilotes de l'installation mise à niveau ainsi que du projet Designer. Pour plus d'informations, reportez-vous à la section « Suppression des pilotes pour le module de provisioning basé sur les rôles » du *Guide d'installation de NetIQ Identity Manager*.

Tâche	Remarques
18. Installation des composants d'Identity Reporting	Installez les composants d'Identity Reporting. Pour ce faire, vous devez effectuer les opérations suivantes : 1. Créez une sauvegarde des données EAS. Pour plus d'informations, reportez-vous à la section « Sauvegarde du schéma pour les pilotes » du *Guide d'installation de NetIQ Identity Manager*. 2. Mettez à niveau le service d'audit d'événements (EAS). Pour mettre à niveau EAS, installez la nouvelle version sur l'ancienne. Pour plus d'informations, reportez-vous à la section « Mise à niveau du service d'audit d'événements »du *Guide d'installation de NetIQ Identity Manager*. 3. Le programme d'installation propose des options pour installer Tomcat et PostgreSQL. Choisissez d'installer Tomcat uniquement. Pour plus d'informations, reportez-vous à la section « Installation de PostgreSQL et de Tomcat pour Identity Manager » du *Guide d'installation de NetIQ Identity Manager*. 4. Installez et configurez NetIQ One SSO Provider (OSP) et la réinitialisation de mot de passe en self-service (SSPR, Self Service Password Reset). Pour plus d'informations, reportez-vous à la section « Installation des composants Single Sign-On et Gestion des mots de passe » du *Guide d'installation de NetIQ Identity Manager*. 5. Installez Identity Reporting. Durant l'installation, spécifiez le nom DNS ou l'adresse IP du serveur qui héberge le service EAS mis à niveau. Pour plus d'informations, reportez-vous à la section « Installation d'Identity Reporting » du *Guide d'installation de NetIQ Identity Manager*. 6. (Conditionnel) Mettez à jour la configuration du pilote du service de collecte de données pour votre nouveau serveur d'applications (Tomcat). 7. Supprimez les références à `reportRunner` de la base de données PostgreSQL avant de démarrer le serveur d'applications après l'installation d'Identity Reporting. a. (Conditionnel) Arrêtez Tomcat. b. Dans le dossier racine d'Identity Reporting, renommez le dossier `reportContent`. Exemple : `/opt/netiq/idm/apps/IdentityReporting` c. Dans le dossier racine de Tomcat, nettoyez les répertoires `temp` et `work`. d. Dans EAS, connectez-vous à la base de données PostgreSQL et générez les instructions suivantes pour supprimer les références à `reportRunner` : ◆ `DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE rpt_def_id='com.novell.content.reportRunner';` ◆ `DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE def_id='com.novell.content.reportRunner';` e. Démarrez Tomcat.
19. Démarrez les pilotes	Démarrez les pilotes associés à Identity Reporting et au moteur Identity Manager. Pour plus d'informations, reportez-vous à la section « Lancement des pilotes » du *Guide d'installation de NetIQ Identity Manager*.

Tâche	Remarques
20. (Conditionnel) Restauration de vos paramètres personnalisés	(Conditionnel) Si vous disposez de stratégies et de règles personnalisées, restaurez vos paramètres personnalisés. Pour plus d'informations, reportez-vous à la section « Restauration de stratégies et de règles personnalisées sur le pilote » du *Guide d'installation de NetIQ Identity Manager*.
21. (Conditionnel) Mise à niveau de Sentinel	(Conditionnel) Si vous utilisez NetIQ Sentinel, veillez à exécuter le dernier Service Pack. Pour plus d'informations sur la mise à niveau de Sentinel, reportez-vous au manuel *NetIQ Sentinel Installation and Configuration Guide* (Guide d'installation et de configuration de NetIQ Sentinel).

4.2 Mise à niveau d'Identity Manager 4.5 Standard Edition vers Identity Manager 4.5 Advanced Edition

La mise à niveau d'Identity Manager 4.5 Standard Edition vers Identity Manager 4.5 Advanced Edition implique des changements de configuration des composants d'Identity Manager. Vous n'avez pas besoin d'exécuter le programme d'installation d'Identity Manager pour effectuer cette mise à niveau.

Identity Manager 4.5 Advanced Edition comprend toutes les fonctions incluses dans l'édition Standard ainsi que des fonctions supplémentaires telles que des applications d'identité. La section Nouvelles fonctionnalités d'Identity Manager dans les Notes de version d'Identity Manager 4.5 Advanced Edition décrit brièvement les nouvelles fonctions du produit. Vous souhaiterez peut-être prendre quelques minutes pour consulter cette section.

Pour effectuer la mise à niveau, NetIQ recommande de suivre les étapes de la liste de contrôle ci-dessous dans l'ordre indiqué :

Tâche	Description
1. Vérification des différences entre une mise à niveau et une migration	Passez en revue les différences entre une mise à niveau et une migration. Pour plus d'informations, reportez-vous à la section « Notions de mise à niveau et de migration » du *Guide d'installation de NetIQ Identity Manager*.
2. Mise à niveau vers Identity Manager 4.5 Standard Edition	Une mise à niveau ou une migration directe vers Identity Manager 4.5 à partir d'une version antérieure à 4.0.2 n'est pas possible. Pour plus d'informations, reportez-vous au Guide d'installation de NetIQ Identity Manager 4.0.2.
3. Obtention des fichiers nécessaires pour la mise à niveau/migration	Assurez-vous que vous disposez de la dernière version du kit d'installation pour la mise à niveau d'Identity Manager vers la version 4.5 Advanced Edition.
4. Renseignez-vous sur les interactions entre les différents composants Identity Manager	Pour plus d'informations, reportez-vous à l'« Introduction » du *Guide d'installation de NetIQ Identity Manager*.
5. Exigences système	Assurez-vous que votre ordinateur dispose des prérequis logiciels et matériels pour une version plus récente d'Identity Manager. Pour plus d'informations, reportez-vous à la section « Considérations et conditions préalables à l'installation » du *Guide d'installation de NetIQ Identity Manager* et aux Notes de version correspondant à la version vers laquelle vous souhaitez effectuer la mise à niveau.

Tâche	Description
6. Arrêt du serveur d'applications sur lequel Identity Reporting est installé	Dans ce cas, le serveur d'applications est Tomcat.
7. Désinstallation d'Identity Reporting	Désinstallez les fichiers WAR Identity Reporting de votre serveur d'applications. À cette fin, suivez les instructions de la documentation propre à votre serveur d'applications. Pour plus d'informations, reportez-vous à la section « Désinstallation d'Identity Reporting » du *Guide d'installation de NetIQ Identity Manager*.
8. Application de la clé d'activation d'Identity Manager 4.5 Advanced Edition	Veillez à bien appliquer la clé d'activation d'Identity Manager 4.5 Advanced Edition dans iManager, car sans cela, le moteur Identity Manager ne se met pas à niveau. **IMPORTANT :** Pour qu'Identity Manager affiche correctement la version et le nom de la marque après la mise à niveau, appliquez le correctif 2 d'Identity Manager 4.5 disponible sur le site Web de téléchargement de NetIQ (http://download.novell.com/Download?buildid=vNsTfMo9g-4~). Pour plus d'informations sur le téléchargement et l'application du correctif, reportez-vous à la section « Application du correctif Identity Manager 4.5 » du *Guide d'installation de NetIQ Identity Manager*.
9. Création et déploiement des pilotes de l'application utilisateur, du service de rôles et de ressources et de la passerelle système gérée	Pour plus d'informations, reportez-vous à la section « Création et déploiement des pilotes pour les applications d'identité » du *Guide d'installation de NetIQ Identity Manager*.
10. (Conditionnel) Installation du serveur d'applications	Installez WebSphere ou JBoss comme serveur d'applications. Si vous préférez Tomcat, vous pouvez réutiliser l'instance existante de Tomcat.
11. Installation et configuration des applications d'identité	**REMARQUE :** le processus de mise à niveau ne supprime pas les rôles existants assignés aux utilisateurs dans eDirectory. Si le rôle d'utilisateur Administrateur de rapports persiste dans le logiciel mis à niveau, assurez-vous que vous supprimez ce rôle pour des raisons de sécurité. Le programme d'installation installe les composants suivants : ◆ Administrateur de catalogue ◆ Home and Provisioning Dashboard ◆ Module de provisioning basé sur les rôles (RBPM) Pour plus d'informations, reportez-vous à la section « Installation des applications d'identité » du *Guide d'installation de NetIQ Identity Manager*.
12. Démarrez le serveur d'applications	Si votre serveur d'applications n'est pas Tomcat, démarrez votre serveur d'applications (WebSphere ou JBoss) et Tomcat. Vous devez exécuter ce dernier car NetIQ prend en charge l'installation d'OSP uniquement sur Tomcat.

Tâche	Description
13. Mise à jour de la configuration du pilote du service de collecte de données	(Conditionnel) Mettez à jour la configuration du pilote du service de collecte de données pour votre nouveau serveur d'applications. Mettez à jour la configuration du pilote de service de collecte de données pour enregistrer le pilote de passerelle système gérée. Pour plus d'informations, reportez-vous à la Section 4.3, « Mise à jour des informations de configuration du pilote du service de collecte de données », page 19.
14. Installation et configuration d'Identity Reporting	Indiquez les détails du serveur EAS existant au cours de l'installation. Pour plus d'informations, reportez-vous à la section relative à l'« installation du module de création de rapports » du *Guide d'installation de NetIQ Identity Manager*. Pour consigner les événements Identity Reporting sur le serveur EAS, effectuez les opérations suivantes : 1. Arrêtez le serveur d'applications. Par exemple, `/etc/init.d/idmapps_tomcat_init stop` 2. Arrêtez le thread d'audit en exécutant la commande suivante : `ps -eaf | grep naudit` 3. Autorisez la création de rapports à utiliser la fonction d'audit. a. (Facultatif) Mettez à jour l'utilitaire ConfigUpdate pour qu'il s'exécute en mode GUI. b. Lancez l'utilitaire ConfigUpdate et sélectionnez l'onglet **Création de rapports**. c. Sélectionnez la case **Activer l'audit pour EAS**. Si elle est déjà activée, désélectionnez-la, puis cliquez sur **OK**. d. Lancez à nouveau l'utilitaire ConfigUpdate et sélectionnez l'onglet **Création de rapports**. e. Sélectionnez la case à cocher **Activer l'audit pour EAS**, puis cliquez sur **OK**. 4. Démarrez le serveur d'applications. Par exemple, `/etc/init.d/idmapps_tomcat_init start`
15. Démarrez les pilotes	Démarrez les pilotes associés à Identity Reporting et au moteur Identity Manager. Pour plus d'informations, reportez-vous à la section « Lancement des pilotes » du *Guide d'installation de NetIQ Identity Manager*.
16. (Conditionnel) Restauration de vos paramètres personnalisés	(Conditionnel) Si vous disposez de stratégies et de règles personnalisées, restaurez vos paramètres personnalisés. Pour plus d'informations, reportez-vous à la section « Restauration de stratégies et de règles personnalisées sur le pilote » du *Guide d'installation de NetIQ Identity Manager*.
17. (Conditionnel) Mise à niveau de Sentinel	(Conditionnel) Si vous utilisez NetIQ Sentinel, veillez à exécuter le dernier Service Pack. Pour plus d'informations sur la mise à niveau de Sentinel, reportez-vous au manuel *NetIQ Sentinel Installation and Configuration Guide* (Guide d'installation et de configuration de NetIQ Sentinel).

4.3 Mise à jour des informations de configuration du pilote du service de collecte de données

1. Lancez Designer, puis sélectionnez **DCS Driver Configuration (Configuration du pilote DCS) > Driver Parameters (Paramètres du pilote) > Driver Options (Options du pilote)**.
2. Dans la section Enregistrement de la passerelle système gérée, changez les paramètres comme indiqué ci-dessous :
   - Définissez l'option **Register Manage System Gateway** (Enregistrer la passerelle système gérée) sur **Yes** (Oui).
   - Changez le DN du pilote MSGW. Par exemple : `CN=Pilote de passerelle système gérée,cn=driverset1,o=system`.
   - Changez le DN utilisateur. Par exemple : `cn=admin,ou=sa,o=system`.
   - Spécifiez le mot de passe du DN utilisateur.

     Pour plus d'informations sur la configuration du pilote, reportez-vous à la section « Configuration du pilote pour le service de collecte de données (DCS, Data Collection Service) » du *Guide d'installation de NetIQ Identity Manager*.
3. Sauvegardez les paramètres, puis déployer le pilote DCS.
4. Redémarrez le pilote DSC.

   La mise à niveau du Identity Reporting peut ne pas rendre compte immédiatement de la version Advanced Edition. La version change lorsque le lot suivant d'événements est traité.

5 Désinstallation d'Identity Manager 4.5 Standard Edition

Certains composants d'Identity Manager présentent des conditions préalables pour la désinstallation. Veillez à lire la section complète pour chaque composant avant de commencer le processus de désinstallation. Pour plus d'informations, reportez-vous à la section « Désinstallation des composants d'Identity Manager » du *Guide d'installation de NetIQ Identity Manager*.

6 Mentions légales