Identity Console
Guide d’administration

Septembre 2022

Mentions légales

Pour plus d'informations sur les mentions légales, les marques, les exclusions de garantie, les garanties, les limitations en matière d'exportation et d'utilisation, les droits du gouvernement américain, la politique relative aux brevets et la compatibilité avec la norme FIPS, rendez-vous sur https://www.netiq.com/company/legal.

Table des matières

À propos de ce guide et de la bibliothèque

Le *guide d'administration* fournit des informations conceptuelles sur le produit NetIQ Identity Console (Identity Console). Il définit la terminologie utilisée et inclut des scénarios d'implémentation.

Pour obtenir la dernière version du *guide d'administration de NetIQ Identity Console*, consultez la version anglaise de la documentation sur le site de documentation en ligne de NetIQ Identity Console.

Public

Il est destiné aux administrateurs réseau.

Autres documents dans la bibliothèque

La bibliothèque propose les manuels suivants :

Guide d’installation

Décrit comment installer Identity Console. Ce manuel est destiné aux administrateurs réseau.

À propos de NetIQ Corporation

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

Notre point de vue

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

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

Services métiers critiques plus efficaces et plus rapidement opérationnels

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

Notre philosophie

Vendre des solutions intelligentes et pas simplement des logiciels

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

Vous aider à réussir, telle est notre passion

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

Nos solutions

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

- Gestion des systèmes et des applications
- Gestion des charges de travail
- Gestion des services

Contacter le support

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

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

Contacter le support technique

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

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

Contacter le support en charge de la documentation

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

Contacter la communauté d'utilisateurs en ligne

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

1 Présentation d'Identity Console

Identity Console est une console d'administration Web de pointe qui permet d'accéder de manière virtuelle, sécurisée et personnalisée aux utilitaires d'administration réseau par le biais d'Internet et d'un navigateur Web. Identity Console simplifie grandement la décentralisation des tâches d'administration.

Fonctionnalités d'Identity Console

Identity Console intègre les fonctionnalités suivantes :

- Administration des objets, des utilisateurs, des schémas, des partitions, des répliques, des droits eDirectory, etc.
- Gestion des pilotes et des ensembles de pilotes Identity Manager
- Gestion et affichage des statistiques de performances d'un pilote
- Inspection des objets, affichage du flux de données d'un pilote, gestion des droits et des bons de travail, etc.
- Gestion de l'état et des paramètres de synchronisation des mots de passe pour les pilotes
- Gestion des stratégies de mot de passe et des méthodes de connexion
- Gestion des certificats
- Administration des diverses ressources réseau
- Amélioration des mesures de sécurité pour protéger les données
- Amélioration de l'évolutivité pour gérer des objets eDirectory plus volumineux
- Connexion sécurisée au portail Identity Console au moyen de One SSO Provider (OSP)
- Exploitation de la dernière technologie d'interface utilisateur du secteur
- Facilité d'installation et de configuration au moyen de conteneurs Docker

2 Accès à Identity Console

Vous pouvez accéder à Identity Console et à toutes ses fonctionnalités à partir de n'importe quel navigateur Web pris en charge. Bien que vous puissiez accéder à Identity Console par le biais d'un autre navigateur Web que ceux mentionnés, nous ne garantissons pas une compatibilité intégrale avec un navigateur non compatible officiellement.

IMPORTANT : Pour plus d'informations sur les navigateurs Web pris en charge, reportez-vous au *guide d'installation d'Identity Console*.

Accès à Identity Console

Pour accéder à la version serveur d'Identity Console, procédez comme suit :

1. Saisissez l'URL suivante dans le champ d'adresse (URL) d'un navigateur Web pris en charge :

   Connexion sécurisée : `https://<adresse_ip_serveur/hostname>:<port>/identityconsole/`

   Dans cet exemple, *<adresse_IP_serveur>* correspond à une adresse IP au format IPv4. Le port à utiliser par défaut est 9000.
2. Connectez-vous à l'aide de votre DN d'utilisateur et de votre mot de passe.
3. Indiquez l'adresse IP ou DNS de l'arborescence eDirectory avec ou sans port sécurisé LDAP.

REMARQUE

- Le rafraîchissement d'un onglet dans Identity Console entraîne la déconnexion de l'utilisateur pour des raisons de sécurité.
- L'ouverture d'onglets Identity Console en double dans le navigateur entraîne la déconnexion de l'utilisateur pour des raisons de sécurité.
- Le DN doit être spécifié au format `cn=admin,ou=sa,o=system`.
- Lorsque eDirectory est configuré avec un port autre que celui par défaut, vous devez spécifier le numéro de port.

---

3 Navigation dans l'interface d'Identity Console

Cette section explique comment naviguer dans l'interface Web d'Identity Console.

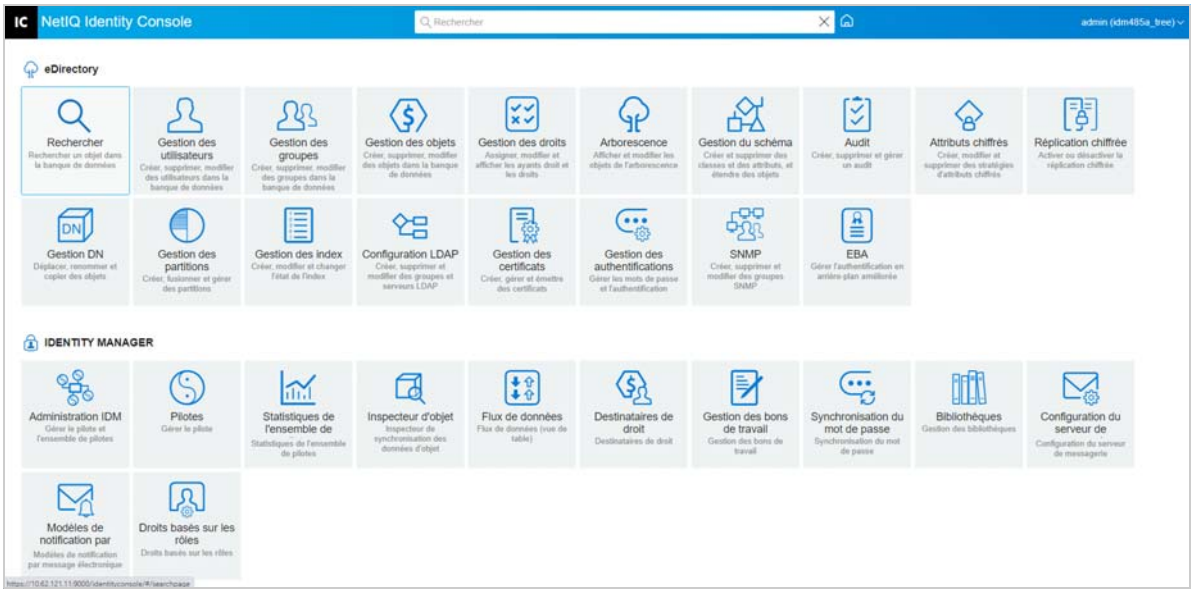
Recherche (version préliminaire)

La fonctionnalité **Recherche (version préliminaire)** fournit une présentation de cette fonction. Dans cette version préliminaire, vous pouvez spécifier des mots-clés, et le champ de recherche détermine la source d'informations pour la recherche et l'affichage des résultats correspondants. Grâce à cette option, vous pouvez rechercher une ressource et y accéder facilement sur n'importe quelle page de l'application Identity Console.

Interface d'Identity Console

L'interface d'Identity Console comprend les modules d'eDirectory et d'Identity Manager.

Figure 3-1 *Interface d'Identity Console*



IMPORTANT : Plusieurs animations GIF utilisées dans ce guide ne fonctionnent qu'avec la documentation en ligne. Si vous basculez vers la version PDF, seules les captures d'écran sont visibles.

Tableau 3-1 *Explication des différents modules du portail Web d'Identity Console*

Nom du module	Description
Rechercher	Rechercher un objet dans la banque de données. Pour plus d'informations, reportez-vous au Chapitre 4, « Exécution de recherches », page 23.
Gestion des utilisateurs	Créer, supprimer et modifier des utilisateurs dans la banque de données. Pour plus d'informations, reportez-vous au Chapitre 5, « Gestion des utilisateurs », page 27.
Gestion des groupes	Créer, supprimer et modifier des groupes dans la banque de données. Pour plus d'informations, reportez-vous au Chapitre 6, « Gestion des groupes », page 35.
Gestion des objets	Créer, supprimer et modifier des objets dans la banque de données. Pour plus d'informations, reportez-vous au Chapitre 7, « Gestion des objets », page 41.
Gestion des droits	Assigner, modifier et afficher les ayants droit et les droits. Pour plus d'informations, reportez-vous au Chapitre 8, « Gestion des droits », page 49.
Arborescence	Afficher et modifier les objets dans l'arborescence. Pour plus d'informations, reportez-vous au Chapitre 9, « Arborescence », page 53.
Gestion du schéma	Créer et supprimer des classes, des classes auxiliaires et des attributs, et étendre des objets. Pour plus d'informations, reportez-vous au Chapitre 10, « Gestion du schéma », page 57.
Audit	Activer, désactiver et gérer l'audit CEF. Pour plus d'informations, reportez-vous au Chapitre 11, « Gestion des événements d'audit », page 65.
Attributs chiffrés	Créer, modifier, supprimer et afficher la stratégie d'attributs chiffrés. Pour plus d'informations, reportez-vous au Chapitre 12, « Gestion des attributs chiffrés », page 71.
Réplication chiffrée	Activer, désactiver et afficher la réplication chiffrée. Pour plus d'informations, reportez-vous au Chapitre 13, « Gestion de la réplication chiffrée », page 75.
Gestion DN	Déplacer, renommer et copier des objets. Pour plus d'informations, reportez-vous au Chapitre 7, « Gestion des objets », page 41.
Gestion des partitions	Créer, fusionner et déplacer des partitions et des répliques. Pour plus d'informations, reportez-vous au Chapitre 14, « Gestion des partitions et des répliques », page 77.

Nom du module	Description
Gestion des index	Créer et modifier des index, et modifier leur état. Pour plus d'informations, reportez-vous au Chapitre 15, « Gestion des index », page 83.
Configuration LDAP	Créer, supprimer et modifier des objets LDAP. Pour plus d'informations, reportez-vous au Chapitre 16, « Configuration des objets LDAP », page 87.
Gestion des certificats	Créer et gérer des certificats de serveur et d'autorité de certification. Pour plus d'informations, reportez-vous à la section Chapitre 17, « Gestion des certificats », page 91.
Gestion des authentifications	Créer et gérer des méthodes et des séquences de connexion/post-connexion. Ce module vous permet également de gérer les stratégies de mot de passe et les ensembles de questions de vérification d'identité. Pour plus d'informations, reportez-vous au Chapitre 18, « Gestion du module Authentification », page 111.
SNMP	Créer, supprimer et modifier des groupes SNMP. Pour plus d'informations, reportez-vous à la section Chapitre 19, « Gestion des objets Groupe SNMP », page 127.
EBA	Gérer l'authentification en arrière-plan améliorée. Pour plus d'informations, reportez-vous au Chapitre 20, « Gestion de l'authentification en arrière-plan améliorée », page 131.
IDM Administration (Administration IDM)	Gérer les pilotes et les ensembles de pilotes Identity Manager. Pour plus d'informations, reportez-vous à la section Chapitre 21, « Gestion des pilotes et des ensembles de pilotes », page 135. Ce module permet également de gérer les propriétés des ensembles de pilotes. Pour plus d'informations, reportez-vous à la section Chapitre 22, « Gestion des propriétés des ensembles de pilotes », page 143.
Propriétés du pilote	Gérer les propriétés de différents pilotes. Pour plus d'informations, reportez-vous à la section Chapitre 23, « Gestion des propriétés des pilotes », page 157.
Statistiques de l'ensemble de pilotes	Gérer et afficher les statistiques d'un ensemble de pilotes. Pour plus d'informations, reportez-vous à Chapitre 24, « Gestion des statistiques des ensembles de pilotes », page 187.
Inspecteur d'objet	Gérer l'association d'objets et la synchronisation des données. Pour plus d'informations, reportez-vous à la section Chapitre 25, « Inspection des objets Identity Manager », page 189.

Nom du module	Description
Flux de données	Gérer et afficher le flux de données des pilotes. Pour plus d'informations, reportez-vous à la section Chapitre 26, « Gestion du flux de données », page 191.
Destinataires de droit	Gérer les destinataires de droit. Pour plus d'informations, reportez-vous à la section Chapitre 27, « Gestion des destinataires de droit », page 193.
Gestion des bons de travail	Gérer les bons de travail. Pour plus d'informations, reportez-vous à la Chapitre 28, « Gestion des bons de travail », page 195.
Synchronisation de mot de passe	Gérer la synchronisation et l'état des mots de passe. Pour plus d'informations, reportez-vous à la section Chapitre 29, « Gestion de l'état et de la synchronisation du mot de passe », page 199.
Gestion des bibliothèques	Gérer les bibliothèques. Pour plus d'informations, reportez-vous au Chapitre 30, « Gestion des bibliothèques », page 203.
Configuration du serveur de messagerie	Gérer les options du serveur de messagerie. Pour plus d'informations, reportez-vous au Chapitre 31, « Gestion des options du serveur de messagerie », page 205.
Modèles de notification par message électronique	Gérer les modèles de message électronique. Pour plus d'informations, reportez-vous au Chapitre 32, « Gestion des modèles de messages électroniques », page 207.

Gestion d'eDirectory à l'aide d'Identity Console

Cette section décrit les différentes tâches que vous pouvez effectuer pour gérer vos serveurs eDirectory à l'aide du portail Identity Console.

4 Exécution de recherches

La vignette Rechercher vous permet de spécifier une opération de recherche à effectuer sur l'arborescence Annuaire et d'afficher les résultats. Grâce à cette option, vous pouvez rechercher des objets, des utilisateurs, des groupes et d'autres éléments. Pour effectuer une opération de recherche sur différents objets de votre banque de données, procédez comme suit :

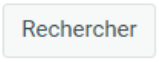
1. Indiquez le nom d'objet à rechercher. Utilisez un astérisque pour spécifier un nom partiel. Par exemple : `ldap*`, `*cert`, `*serveur*`, etc. Si vous utilisez uniquement un astérisque dans ce champ, Identity Console renvoie tous les résultats de la recherche correspondant au **type** et au **contexte** sélectionnés.

   REMARQUE : À l'aide du parcoureur de contexte, vous pouvez parcourir toute l'arborescence eDirectory en spécifiant un astérisque (*) dans le champ de recherche. Vous pouvez également filtrer les objets dans le parcoureur de contexte en utilisant la recherche par caractère joker. Par exemple, `admin*`. Ce comportement du parcoureur de contexte est pris en charge dans les différents modules d'Identity Console.

   ---

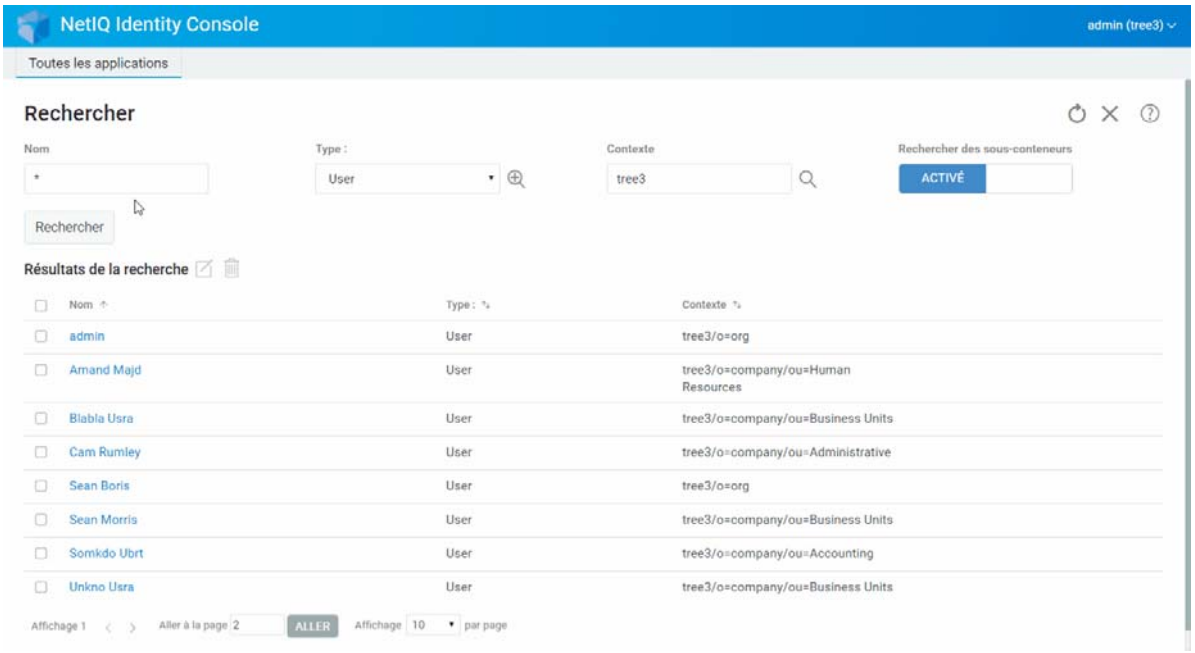
2. Sélectionnez le type d'objet de la recherche dans le champ **Type**. Identity Console affiche uniquement les objets du type spécifié. Le type **Utilisateur** est sélectionné par défaut dans ce champ.

   Cliquez sur l'icône  pour définir d'autres paramètres de recherche de niveau attribut. Pour plus d'informations, reportez-vous à la section « Configuration de la recherche avancée » page 24.

3. Indiquez le conteneur de début de l'opération de recherche dans le champ **Contexte**.
4. Si vous souhaitez que la recherche inclue des conteneurs subordonnés, **activez** l'option Rechercher des sous-conteneurs.
5. Cliquez sur le bouton 

.

Figure 4-1 *Exécution d'une opération de recherche*



Configuration de la recherche avancée

La recherche avancée permet d'optimiser la recherche d'objets souhaités dans l'annuaire.

Type d'objet : indique la classe de base recherchée. Par exemple : Utilisateur.

Classes auxiliaires : cliquez sur l'icône + pour indiquer une classe auxiliaire à inclure dans la recherche.

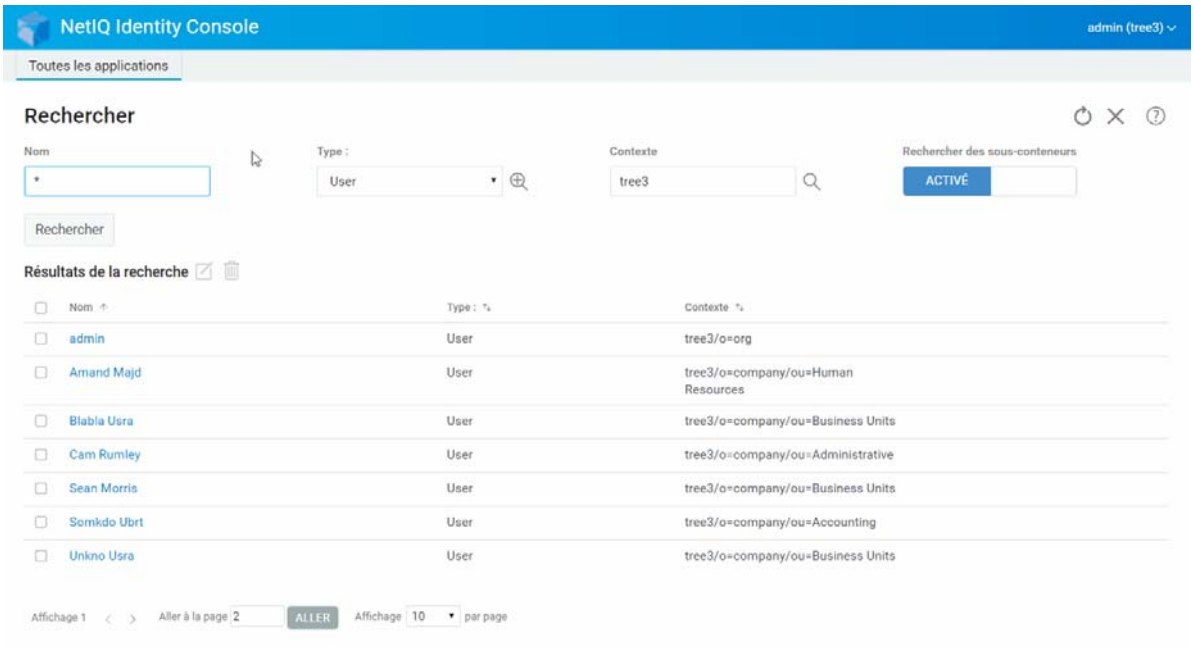
Attribut: spécifie un attribut (propriété) à utiliser en tant que partie du filtre.

Opérateur: spécifie l'opérateur logique à appliquer au filtre.

Valeur : spécifie la valeur d'attribut que vous utilisez en tant que filtre. Vous pouvez utiliser l'astérisque (*) en tant que caractère joker pour indiquer une partie de valeur. Par exemple : dup*, *ont et *upo*.

Par ailleurs, vous pouvez rassembler plusieurs filtres d'attribut dans un groupe de filtres en utilisant l'icône + Rule pour ajouter un second attribut à la liste. Si vous utilisez plusieurs filtres d'attribut, reliez-les à l'aide de l'opérateur logique ET ou OU.

Figure 4-2 *Configuration de la recherche avancée*



5 Gestion des utilisateurs

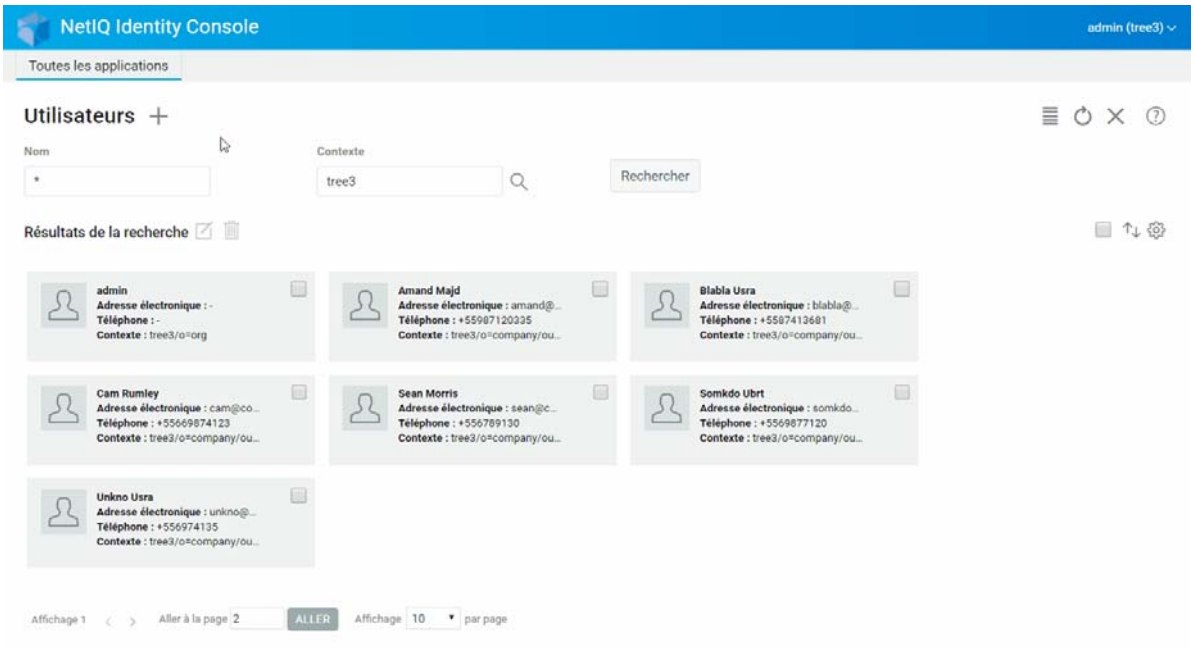
La gestion des utilisateurs et de leur accès au réseau constitue l'un des principaux objectifs de la banque de données. Grâce au portail Web d'Identity Console, vous pouvez effectuer les tâches suivantes concernant les utilisateurs :

Création d'un utilisateur

Pour créer un objet Utilisateur :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des utilisateurs**.
2. Cliquez sur l'icône +.
3. Sur la page Créer un utilisateur, fournissez au moins les informations requises concernant l'utilisateur, puis cliquez sur le bouton Créer.
   - **Nom d'utilisateur**
   - **Contexte**
   - **Nom**
   - **Mot de passe**
4. Un message de confirmation s'affiche pour signaler que l'objet Utilisateur a été créé.

Figure 5-1 *Création d'un utilisateur*

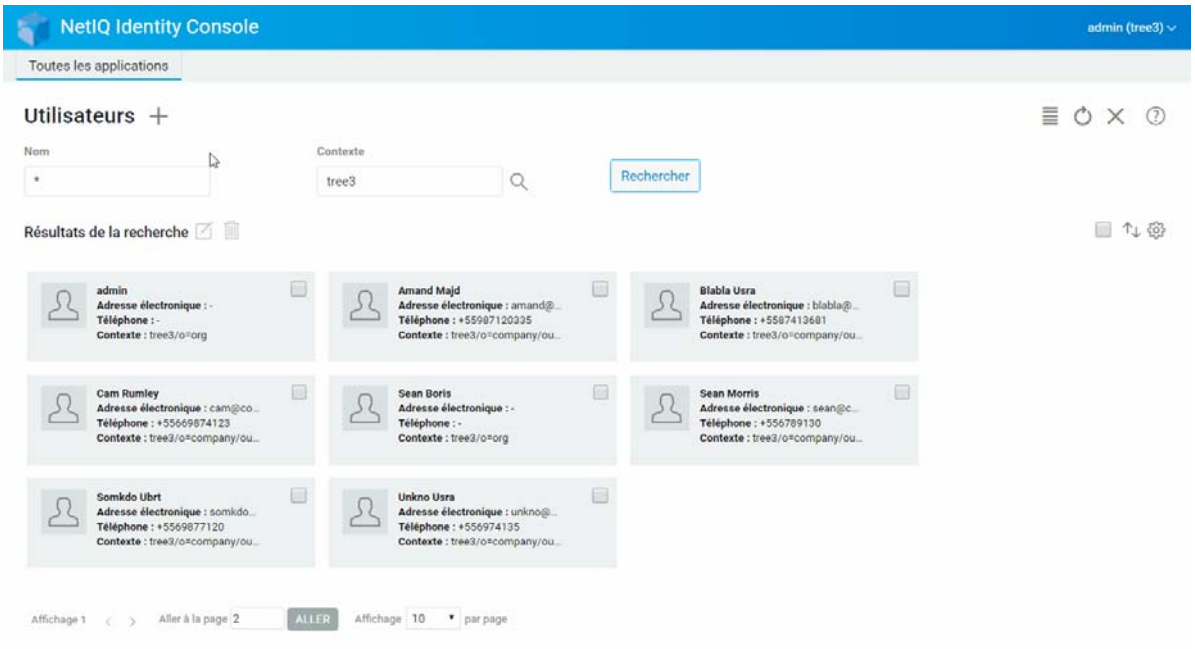


Suppression d'un utilisateur

Pour supprimer un objet Utilisateur :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des utilisateurs**.
2. Entrez le nom et le contexte de l'objet ou utilisez la fonction de recherche pour le localiser, puis cliquez sur le bouton Rechercher.
3. Sélectionnez l'objet Utilisateur souhaité dans la liste d'utilisateurs, puis cliquez sur l'icône 🗑.
4. Un message de confirmation s'affiche pour signaler que l'objet Utilisateur a été supprimé.

Figure 5-2 *Suppression d'un utilisateur*

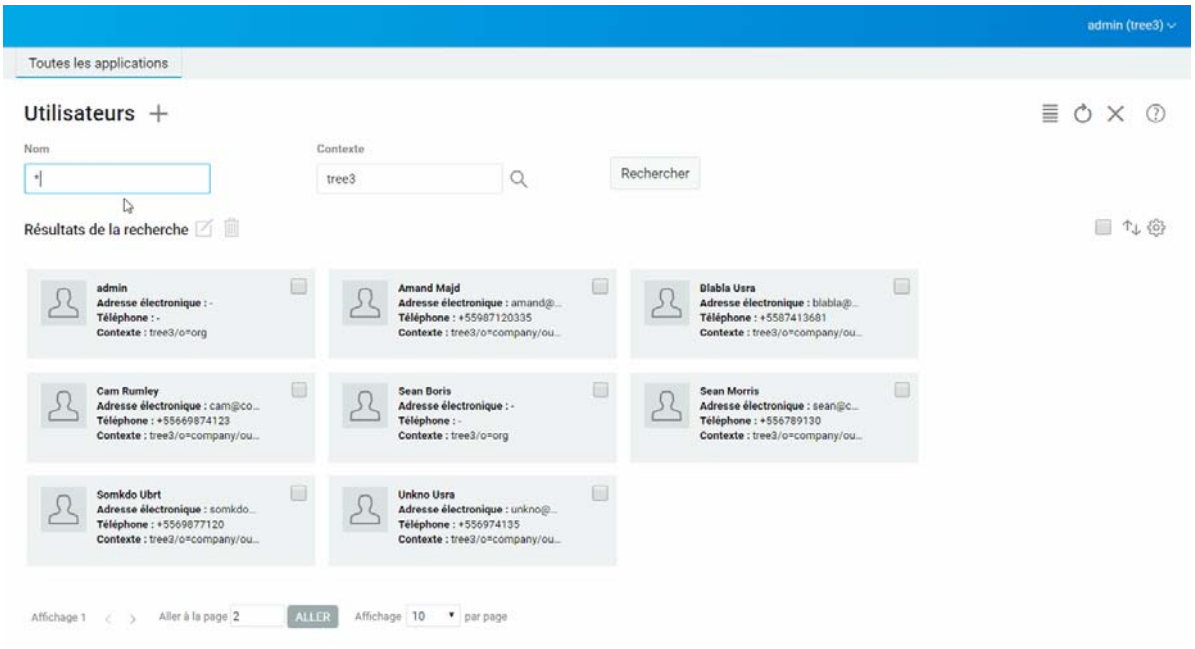


Modification d'un utilisateur

Pour modifier un objet Utilisateur :

1. Sur la page d'accueil d'Identity Console, cliquez sur l'option **Gestion des membres**.
2. Entrez le nom et le contexte de l'objet ou utilisez la fonction de recherche pour le localiser, puis cliquez sur le bouton Rechercher.
3. Sélectionnez l'objet Utilisateur souhaité dans la liste d'utilisateurs, puis cliquez sur l'icône .
4. Effectuez les modifications souhaitées, puis cliquez sur le bouton Enregistrer.
5. Un message de confirmation s'affiche pour signaler que l'objet Utilisateur a été modifié.

Figure 5-3 *Modification d'un utilisateur*

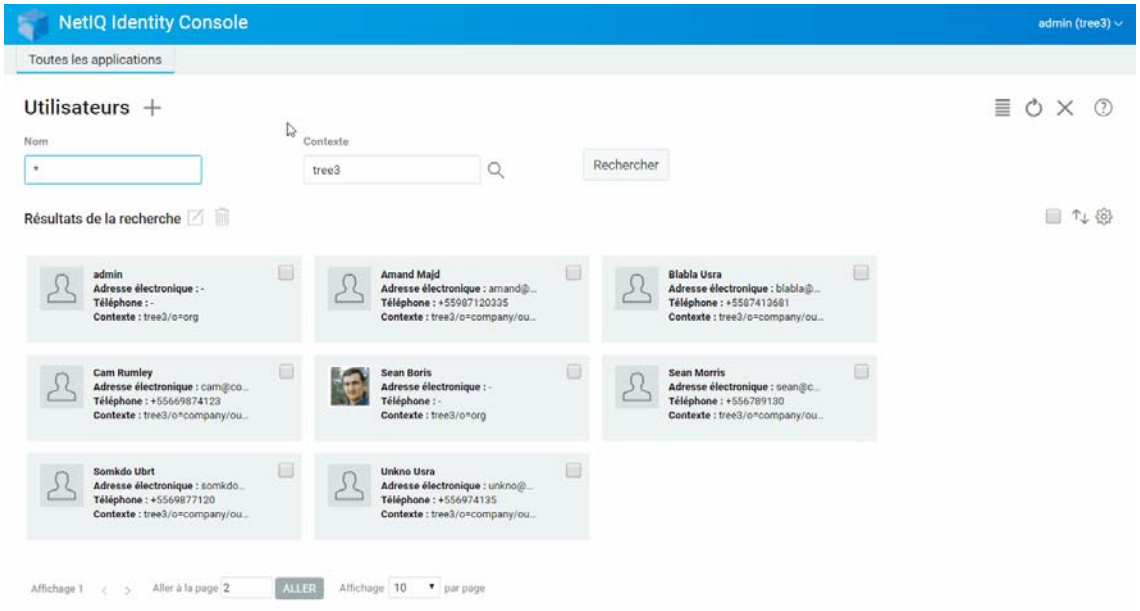


Recherche d'un utilisateur

Pour rechercher un objet Utilisateur :

1. Sur la page d'accueil d'Identity Console, cliquez sur l'option **Gestion des membres**.
2. Vous pouvez rechercher un utilisateur par nom ou par nom et contexte. Après avoir entré toutes les informations nécessaires, cliquez sur l'icône Rechercher.

Figure 5-4 *Recherche d'un utilisateur*

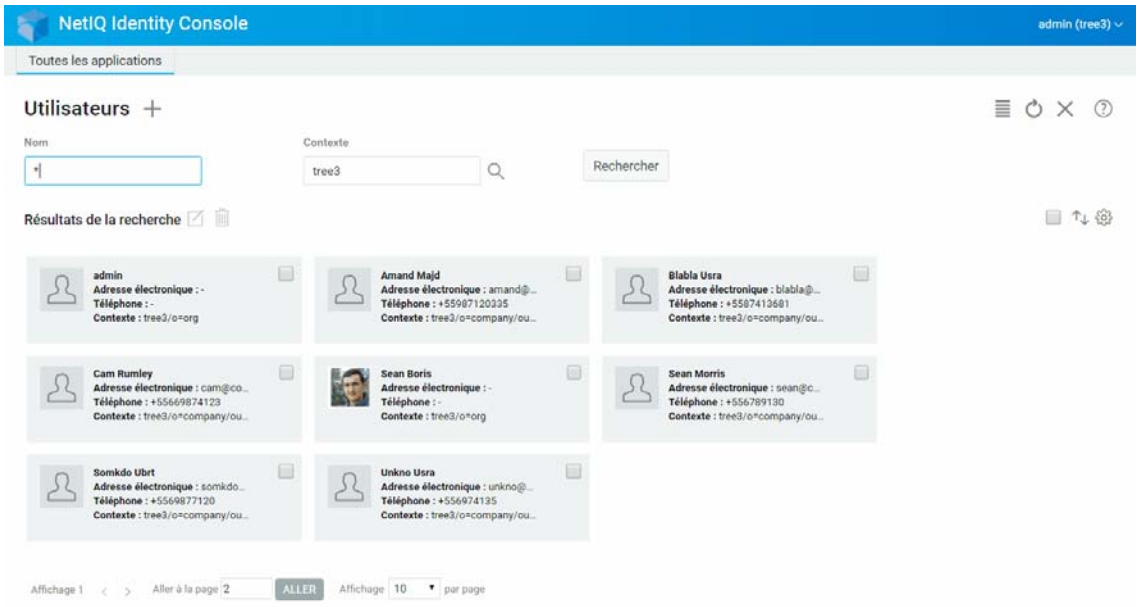


Définition de restrictions de mot de passe

Grâce aux restrictions de mot de passe, vous pouvez effectuer les opérations suivantes :

- Autoriser les utilisateurs à modifier leur mot de passe
- Appliquer un mot de passe pour la connexion
- Déterminer la robustesse des mots de passe
- Appliquer la modification périodique des mots de passe
- Déterminer la date d'expiration des mots de passe
- Appliquer la création de mots de passe uniques
- Déterminer la période de connexion gracieuse en cas d'expiration du mot de passe

Figure 5-5 *Restrictions de mot de passe*

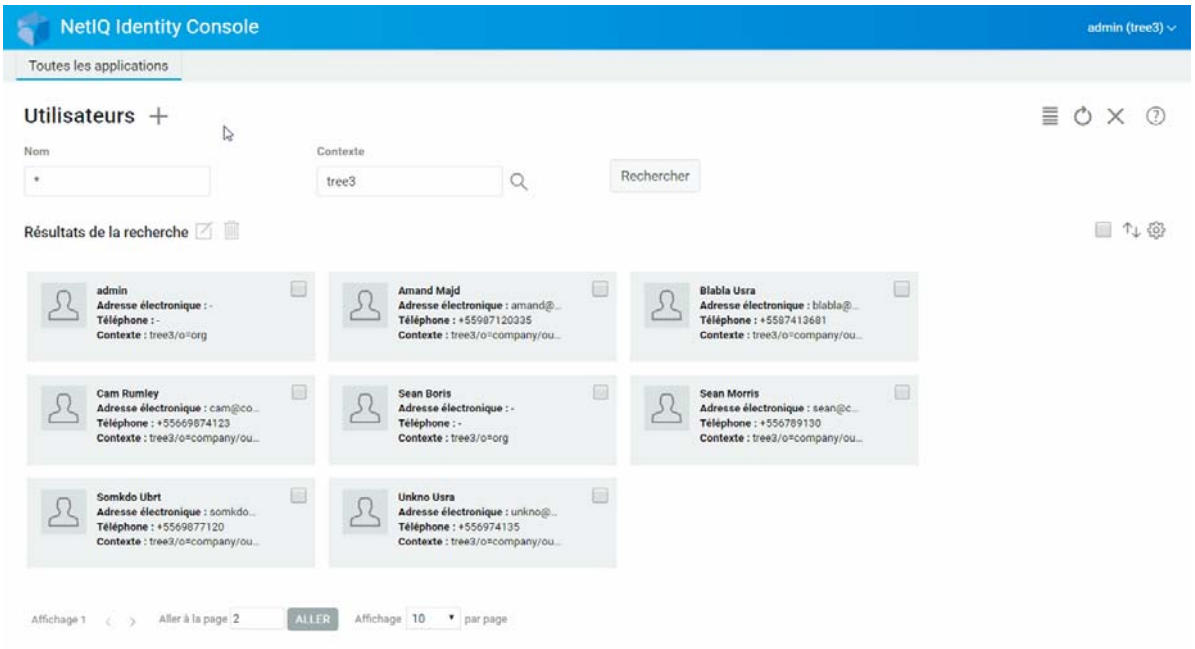


Désactivation et activation d'un compte utilisateur

Pour désactiver un compte utilisateur, procédez comme suit :

1. Sélectionnez l'utilisateur dont vous souhaitez désactiver le compte, puis cliquez sur l'icône .
2. Cliquez sur l'onglet **Restrictions** de la page **Modifier l'utilisateur**.
3. Développez l'onglet **Restrictions de connexion**, puis cochez la case **Compte désactivé**.
4. Cliquez sur l'icône Enregistrer.
5. Le compte utilisateur est à présent désactivé. Pour activer un compte utilisateur désactivé, décochez la case **Compte désactivé**.

Figure 5-6 *Désactivation et activation d'un compte utilisateur*

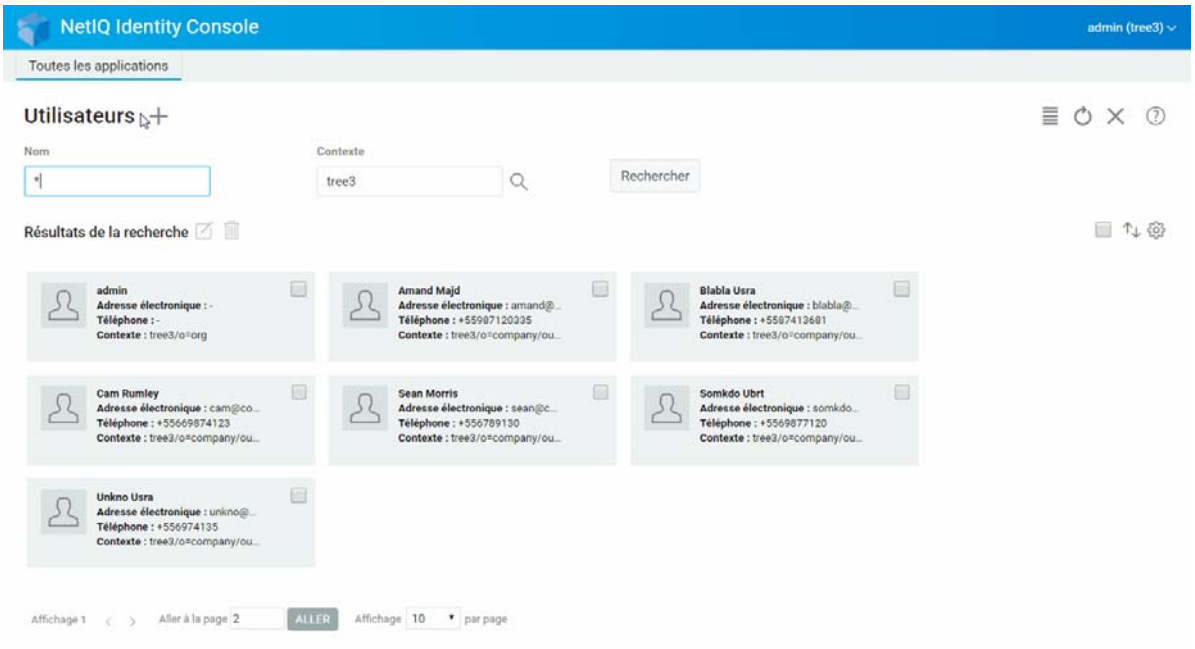


Définition de la date d'expiration d'un compte

Pour définir la date d'expiration d'un compte utilisateur, procédez comme suit :

1. Sélectionnez l'utilisateur pour lequel vous souhaitez définir une date d'expiration du compte, puis cliquez sur l'icône .
2. Cliquez sur l'onglet **Restrictions** de la page **Modifier l'utilisateur**.
3. Développez l'onglet **Restrictions de connexion**, cochez la case **Le compte a une date d'expiration**, puis indiquez une **date d'expiration**.
4. Cliquez sur l'icône Enregistrer.

Figure 5-7 *Définition de la date d'expiration d'un compte*

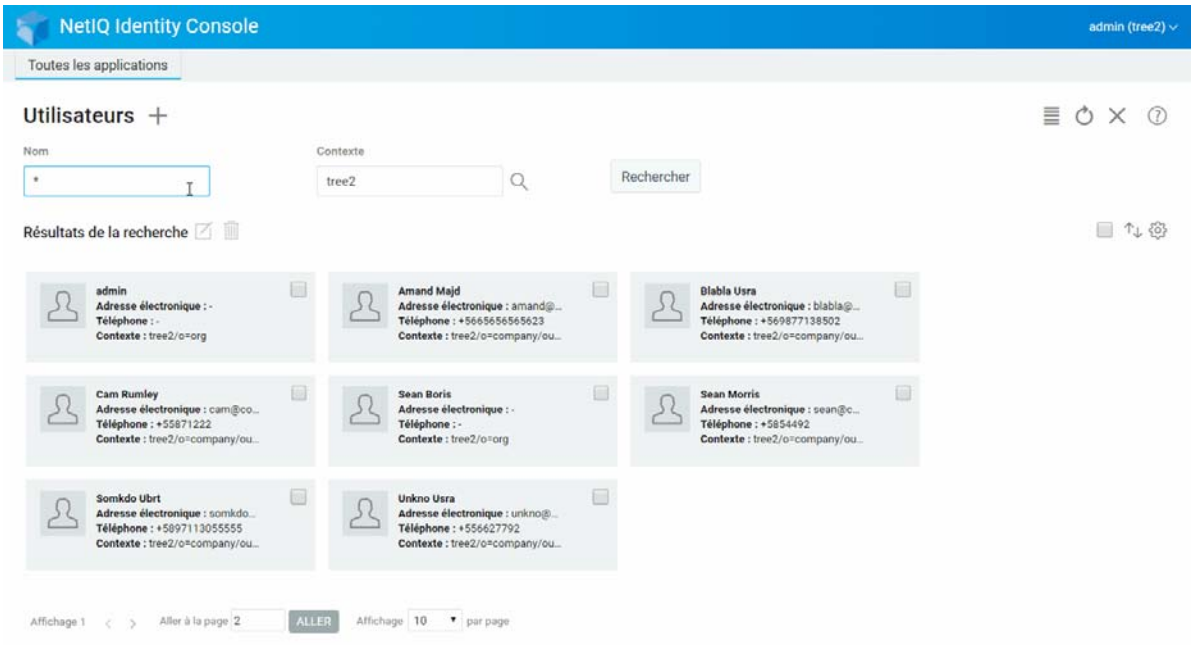


Vérification et suppression du verrouillage en cas d'intrusion

Vous pouvez consulter les détails du verrouillage en cas d'intrusion pour un compte utilisateur à l'aide du portail Web d'Identity Console. Pour afficher les détails d'un verrouillage en cas d'intrusion :

1. Sélectionnez l'utilisateur pour lequel vous souhaitez vérifier les informations de verrouillage en cas d'intrusion, puis cliquez sur l'icône .
2. Cliquez sur l'onglet **Restrictions** de la page **Modifier l'utilisateur**.
3. Développez l'onglet **Verrouillage en cas d'intrusion** et consultez les informations du verrouillage en cas d'intrusion.
4. Ensuite, sélectionnez l'onglet **Supprimer le verrouillage**, puis cliquez sur le bouton Supprimer le verrou.
5. Cliquez sur le bouton Enregistrer.

Figure 5-8 *Vérification et suppression du verrouillage en cas d'intrusion*



6 Gestion des groupes

Les groupes contiennent généralement un certain nombre de membres. Tout utilisateur qui crée un groupe en devient automatiquement le propriétaire. La fonctionnalité Gestion des groupes permet d'effectuer les opérations suivantes :

Pour plus d'informations sur l'utilisation et la configuration des objets Groupe, reportez-vous au *guide d'administration de NetIQ eDirectory 9.2* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

Création d'un groupe

Pour créer un groupe :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des groupes**.
2. Cliquez sur l'icône +.
3. Sur la page Créer un groupe, entrez les informations suivantes :
   - Indiquez le nom du groupe.
   - Indiquez le contexte.

   Sélectionnez **Groupe dynamique** pour faire du nouveau groupe un groupe dynamique de la classe `dynamicGroup`. Dans le cas contraire, le groupe est créé en tant que groupe statique.

   Sélectionnez **Groupe imbriqué** pour faire du nouveau groupe un groupe imbriqué afin qu'il soit créé avec la classe auxiliaire `nestedGroupAux`.

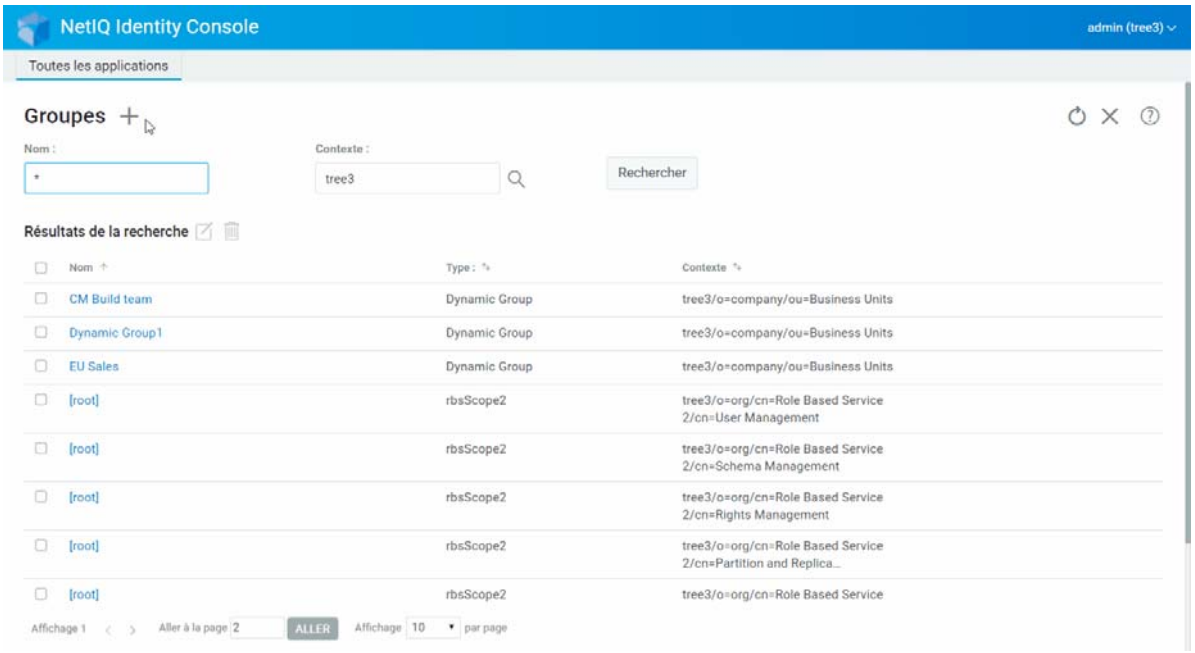
   REMARQUE : vous pouvez convertir un groupe statique en groupe dynamique ou en groupe imbriqué en suivant la procédure décrite dans la section Modification d'un objet. Cette conversion étend l'objet Groupe sélectionné pour qu'il appartienne à la classe `dynamicGroupAux` ou `nestedGroupAux`, respectivement.

   Un groupe peut être imbriqué ou dynamique. Vous ne pouvez pas créer de groupe combinant ces deux caractéristiques.

   ---

4. Après avoir entré toutes les informations nécessaires, cliquez sur le bouton Créer.
5. Un message de confirmation s'affiche pour signaler que le groupe a été créé.

Figure 6-1 *Création d'un groupe*

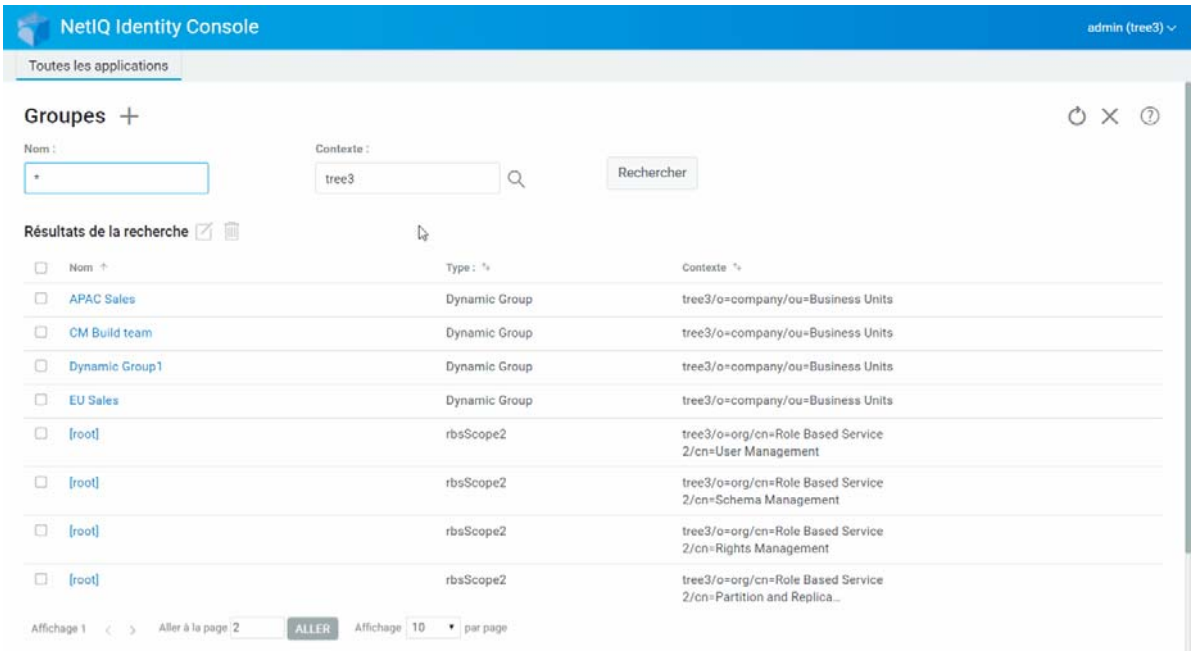


Suppression d'un groupe

Pour supprimer un groupe :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des groupes**.
2. Indiquez le nom et le contexte du groupe ou utilisez la fonction de recherche pour le localiser, puis cliquez sur le bouton Rechercher.
3. Sélectionnez le groupe à supprimer, puis cliquez sur l'icône .
4. Un message de confirmation s'affiche pour signaler que le groupe a été supprimé.

Figure 6-2 *Suppression d'un groupe*

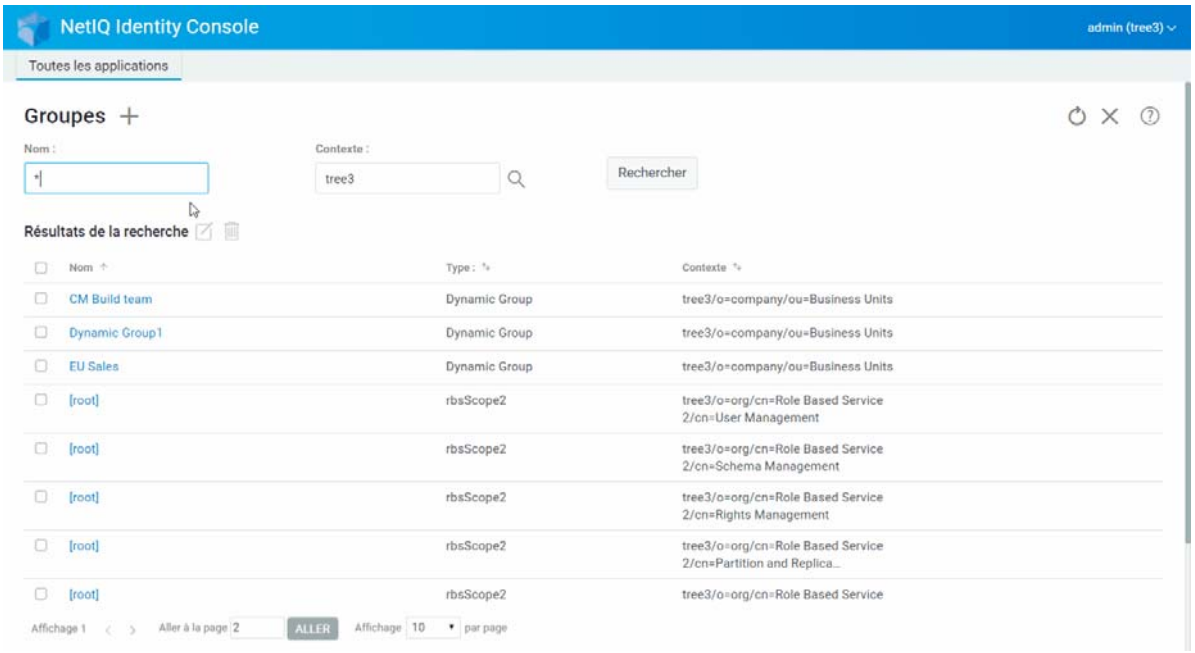


Modification d'un groupe

Pour modifier un groupe :

1. Sur la page d'accueil d'Identity Console, cliquez sur l'option **Gestion des groupes**.
2. Entrez le nom et le contexte du groupe, puis cliquez sur le bouton Rechercher.
3. Sélectionnez le groupe à modifier, puis cliquez sur l'icône .
4. Effectuez les modifications souhaitées, puis cliquez sur le bouton Enregistrer.
5. Un message de confirmation s'affiche pour signaler que le groupe a été modifié.

Figure 6-3 *Modification d'un groupe*

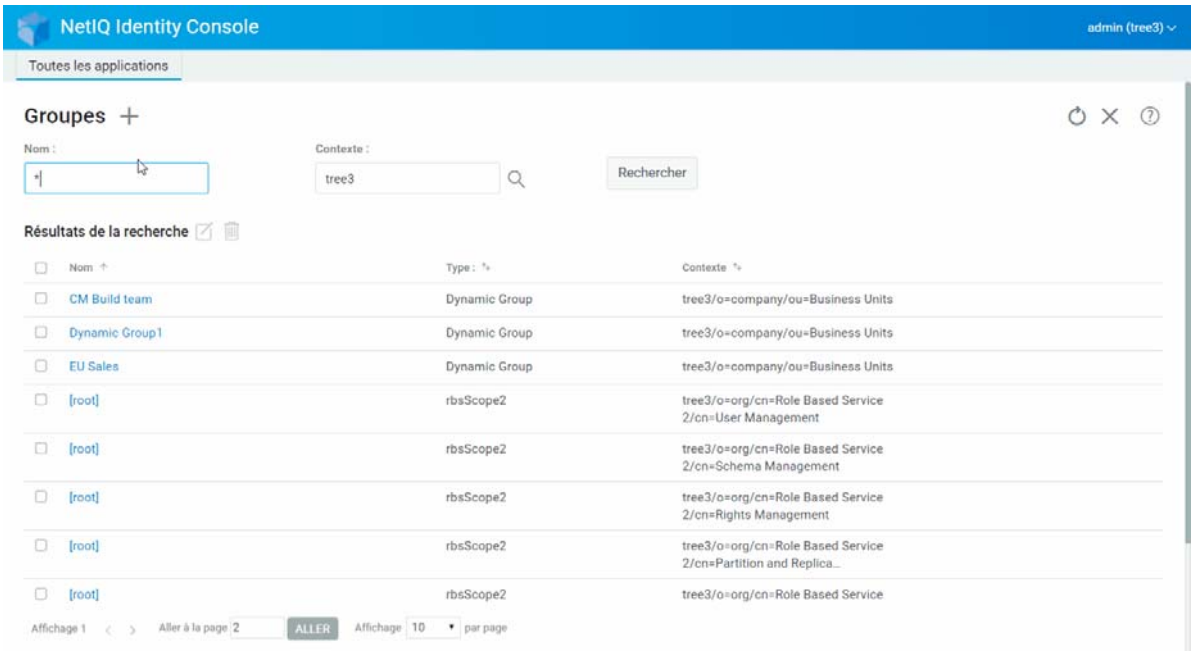


Ajout ou modification d'un membre d'un groupe

Pour ajouter ou modifier un membre d'un groupe :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des groupes**.
2. Entrez le nom et le contexte du groupe, puis cliquez sur le bouton Rechercher.
3. Sélectionnez le groupe souhaité, puis cliquez sur l'icône .
4. Sur la page **Modifier le groupe**, cliquez sur l'onglet **Membres**.
5. Utilisez l'icône pour ajouter un nouveau membre au groupe. Si vous souhaitez supprimer un membre du groupe, cliquez sur l'icône .
6. Après avoir effectué les modifications souhaitées, cliquez sur le bouton Enregistrer.
7. Un message de confirmation s'affiche pour signaler que le groupe a été modifié.

Figure 6-4 *Ajout ou modification d'un membre d'un groupe*

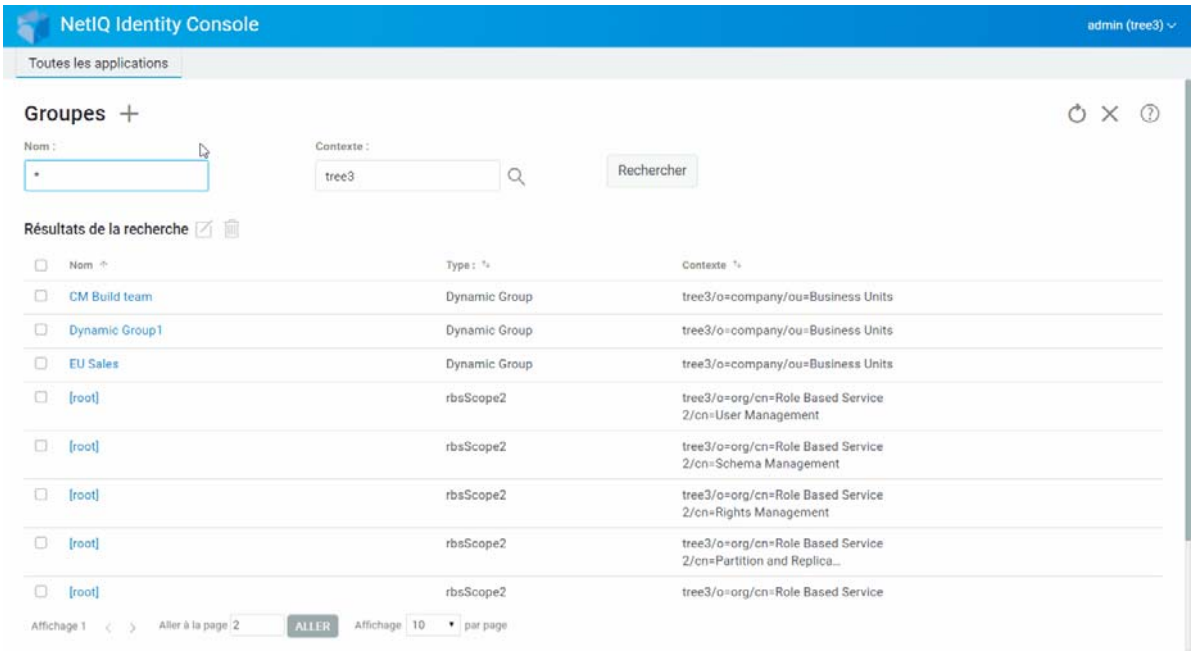


Recherche d'un groupe

Pour rechercher un groupe :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des groupes**.
2. Vous pouvez rechercher un groupe par nom ou par nom et contexte.
3. Après avoir entré toutes les informations nécessaires, cliquez sur l'icône Rechercher.

Figure 6-5 *Recherche d'un groupe*



7 Gestion des objets

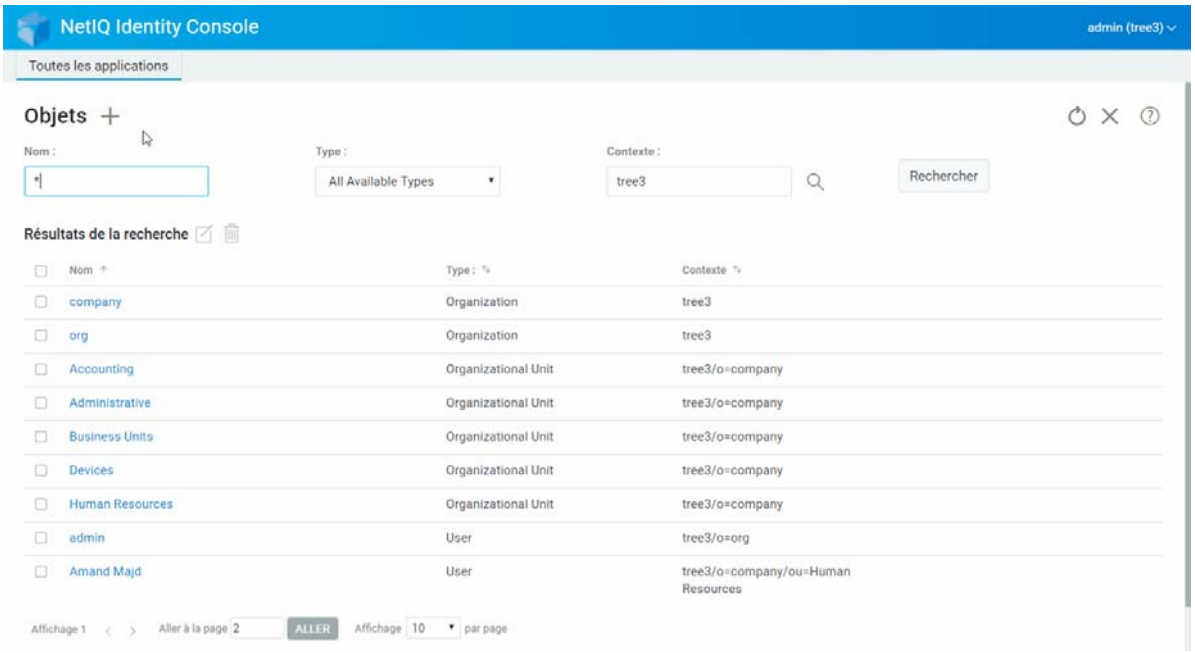
Identity Console vous permet de gérer différents objets dans votre banque de données. Grâce à ce module, vous pouvez créer, modifier, supprimer et rechercher des objets.

Création d'un objet

Pour créer un objet :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des objets**.
2. Cliquez sur l'icône +.
3. Sur la page Créer un objet, entrez les informations suivantes :
   - Indiquez le nom de l'objet.
   - Indiquez le type.
   - Indiquez le contexte.
4. Après avoir entré toutes les informations nécessaires, cliquez sur **Suivant** > **Créer**.
5. Un message de confirmation s'affiche pour signaler que l'objet a été créé.

Figure 7-1 *Création d'un objet*

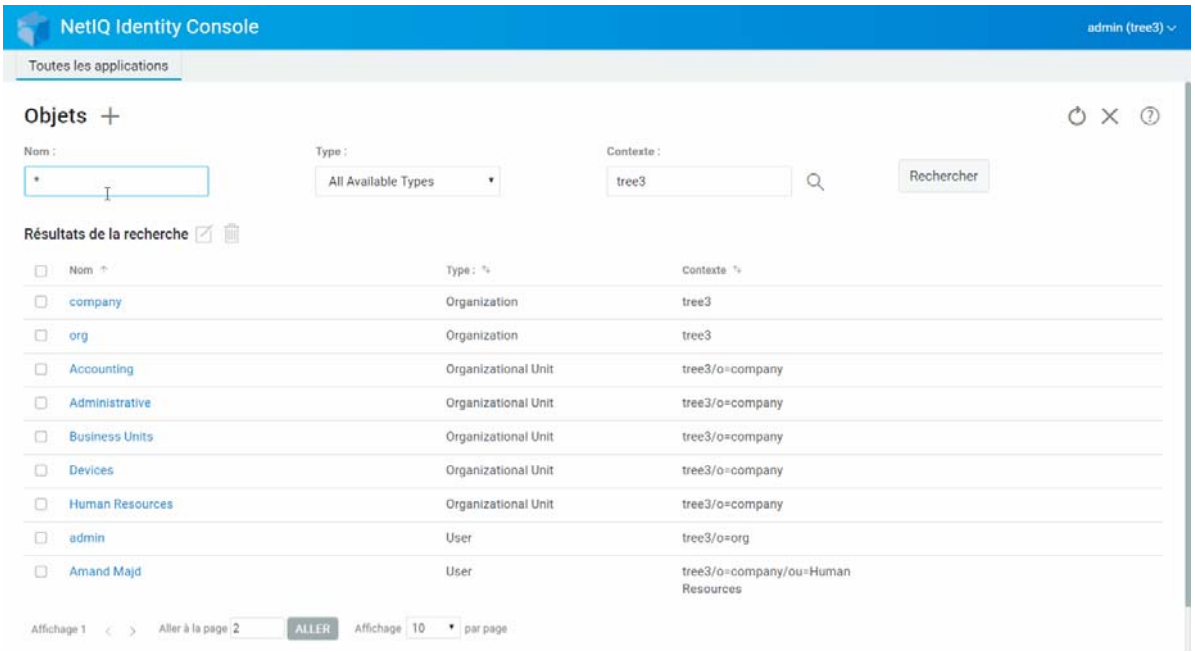


Suppression d'un objet

Pour supprimer un objet :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des objets**.
2. Indiquez le nom, le type et le contexte de l'objet ou utilisez la fonction de recherche pour le localiser, puis cliquez sur le bouton Rechercher.
3. Sélectionnez l'objet souhaité dans la liste de recherche, puis cliquez sur l'icône 🗑.
4. Un message de confirmation s'affiche pour signaler que l'objet a été supprimé.

Figure 7-2 *Suppression d'un objet*

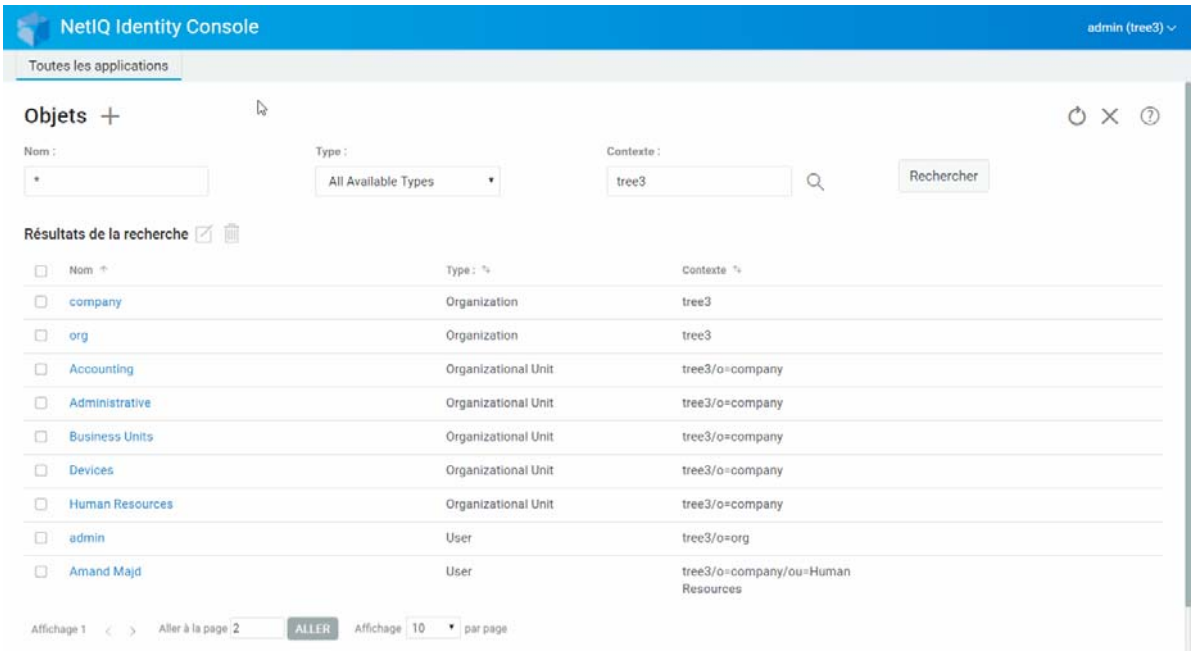


Modification d'un objet

Pour modifier un objet :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des objets**.
2. Entrez le nom, le type et le contexte de l'objet, puis cliquez sur le bouton Rechercher.
3. Sélectionnez l'objet souhaité dans la liste de recherche, puis cliquez sur l'icône .
4. Effectuez les modifications souhaitées, puis cliquez sur le bouton Enregistrer.
5. Un message de confirmation s'affiche pour signaler que l'objet a été modifié.

Figure 7-3 *Modification d'un objet*

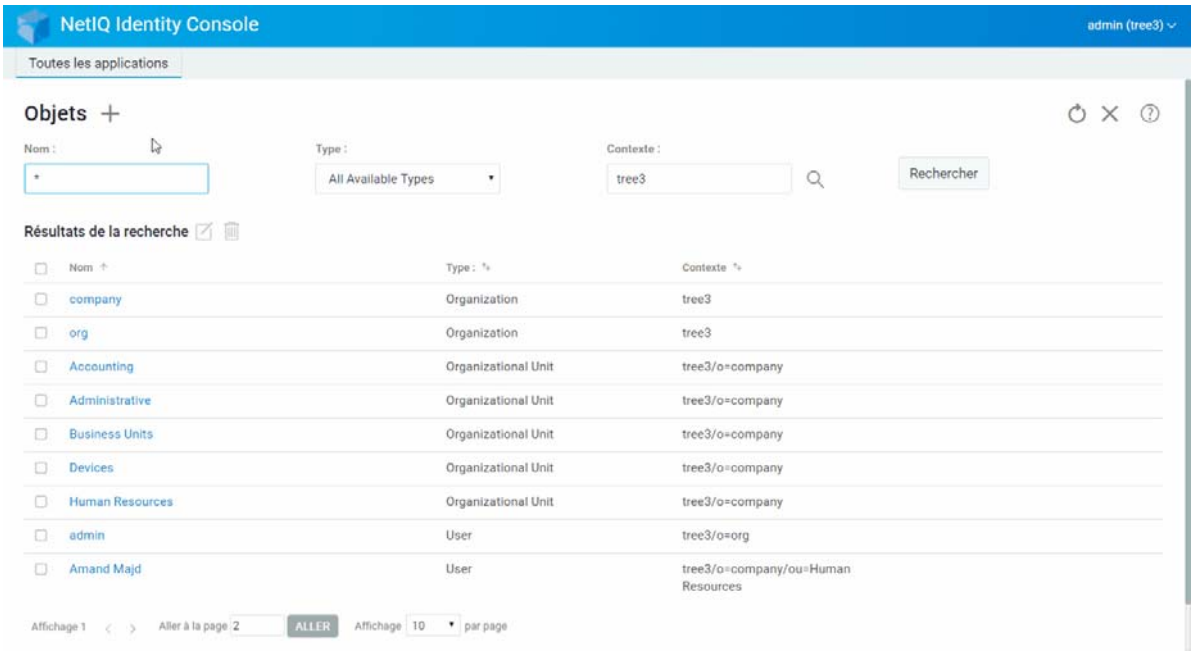


Recherche d'un objet

Pour rechercher un objet :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des objets**.
2. Vous pouvez rechercher un objet par nom ou par nom, type et contexte.
3. Après avoir entré toutes les informations nécessaires, cliquez sur le bouton Rechercher.

Figure 7-4 *Recherche d'un objet*



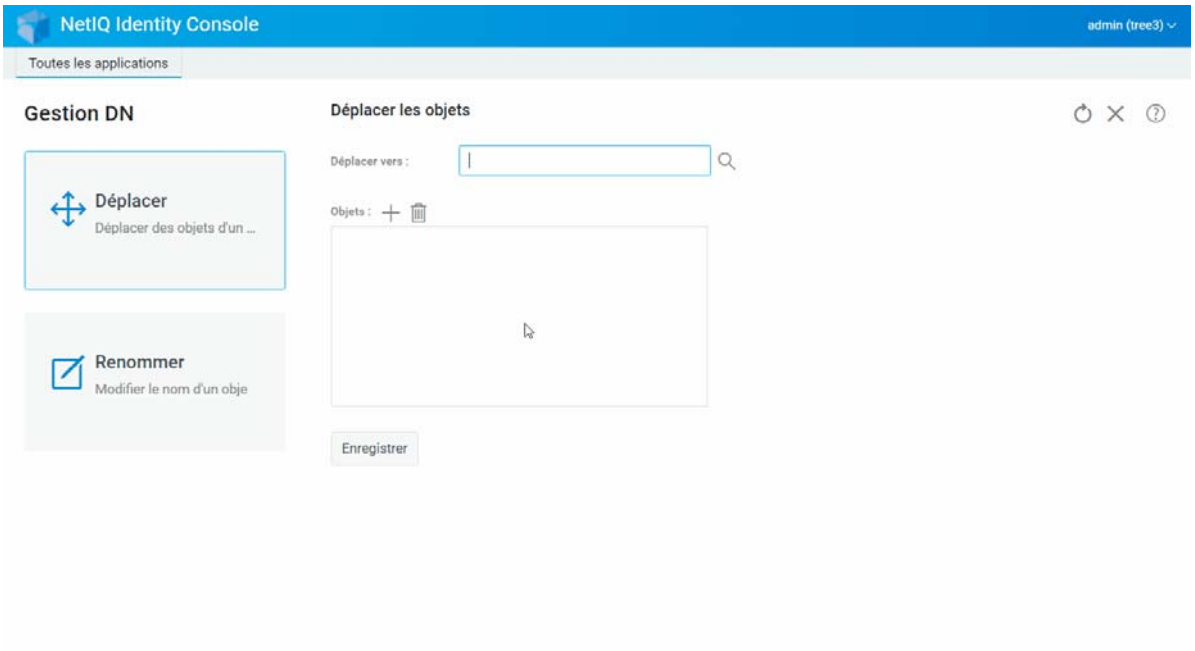
Déplacement d'un objet

Pour déplacer un objet :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion DN**.
2. L'option **Déplacer un objet** est sélectionnée par défaut.
3. Dans le champ **Déplacer vers**, sélectionnez le conteneur vers lequel vous souhaitez déplacer l'objet.
4. Cliquez sur l'icône + pour ajouter l'objet à déplacer vers un autre conteneur.

   Si vous souhaitez supprimer un objet sélectionné, cliquez sur l'icône 🗑.
5. Cliquez sur le bouton Enregistrer.
6. Un message de confirmation s'affiche pour signaler que l'opération de déplacement de l'objet a réussi.

Figure 7-5 *Déplacement d'un objet*

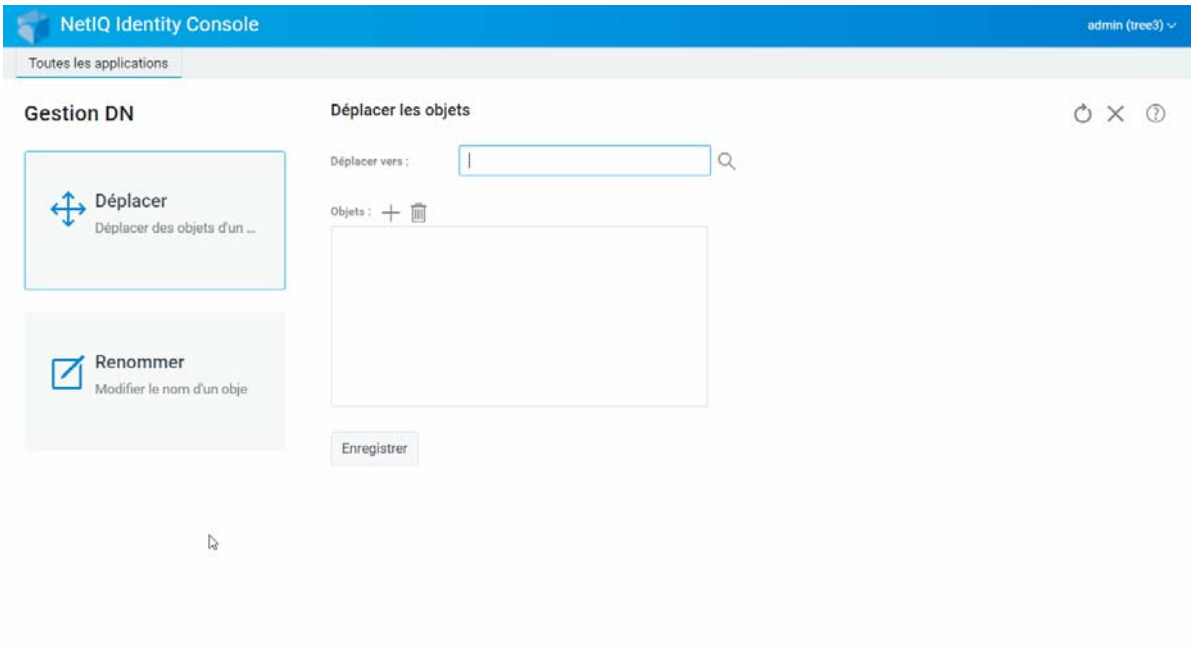


Changement du nom d'un objet

Pour renommer un objet :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion DN**.
2. Sélectionnez l'option **Renommer un objet**.
3. Utilisez la fonction de recherche pour rechercher l'objet à renommer dans le champ **Nom de l'objet**.
4. Indiquez uniquement le nouveau nom de l'objet dans le champ **Nouveau nom**. Ne spécifiez pas le contexte.
5. Si vous le souhaitez, enregistrez l'ancien nom.
6. Cliquez sur le bouton Enregistrer.
7. Un message de confirmation s'affiche pour signaler que l'opération de changement de nom de l'objet a réussi.

Figure 7-6 *Changement du nom d'un objet*



8 Gestion des droits

Les droits couvrent les droits des ayants droit et les ayants droit eDirectory. Lorsque vous créez une arborescence, les assignations de droits par défaut généralisent les conditions d'accès et de sécurité sur votre réseau. Identity Console vous permet d'effectuer les tâches suivantes concernant les droits :

- « Modification du filtre des droits hérités » page 49
- « Modification des droits d'un ayant droit » page 50
- « Affichage des droits effectifs » page 51

Pour plus d'informations sur les droits eDirectory, reportez-vous au *guide d'administration de NetIQ eDirectory 9.2* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

Modification du filtre des droits hérités

eDirectory intègre un mécanisme de filtre des droits hérités (IRF) qui permet de bloquer l'héritage des droits sur chaque élément subordonné.

Pour plus d'informations sur les filtres de droits hérités, reportez-vous au *guide d'administration de NetIQ eDirectory 9.2* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des droits**.
2. Sélectionnez **Filtre des droits hérités**.

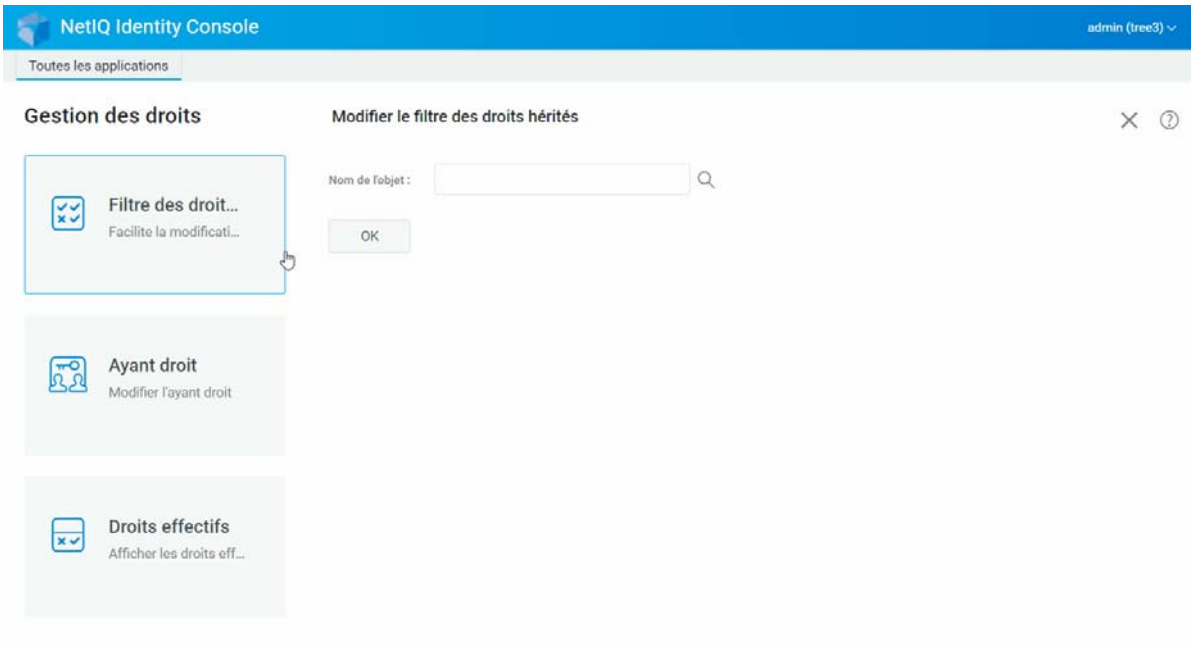
   REMARQUE : l'option Filtre des droits hérités est sélectionnée par défaut.

3. Indiquez le nom complet de l'objet dont vous souhaitez modifier le filtre de droits hérités ou utilisez l'icône du sélecteur d'objet pour le localiser, puis cliquez sur **OK**.

   Cette opération affiche la liste de filtres de droits hérités qui ont déjà été définis sur l'objet.
4. Sous **Propriétés**, éditez la liste des filtres de droits hérités si nécessaire, puis cliquez sur **Appliquer**.

   Pour éditer la liste de filtres, vous devez disposer du droit Superviseur ou Contrôle d'accès sur la propriété ACL de l'objet. Vous pouvez définir des filtres qui annulent les droits hérités sur l'objet dans son entier, sur toutes les propriétés de l'objet et sur des propriétés en particulier.

Figure 8-1 *Modification du filtre des droits hérités*



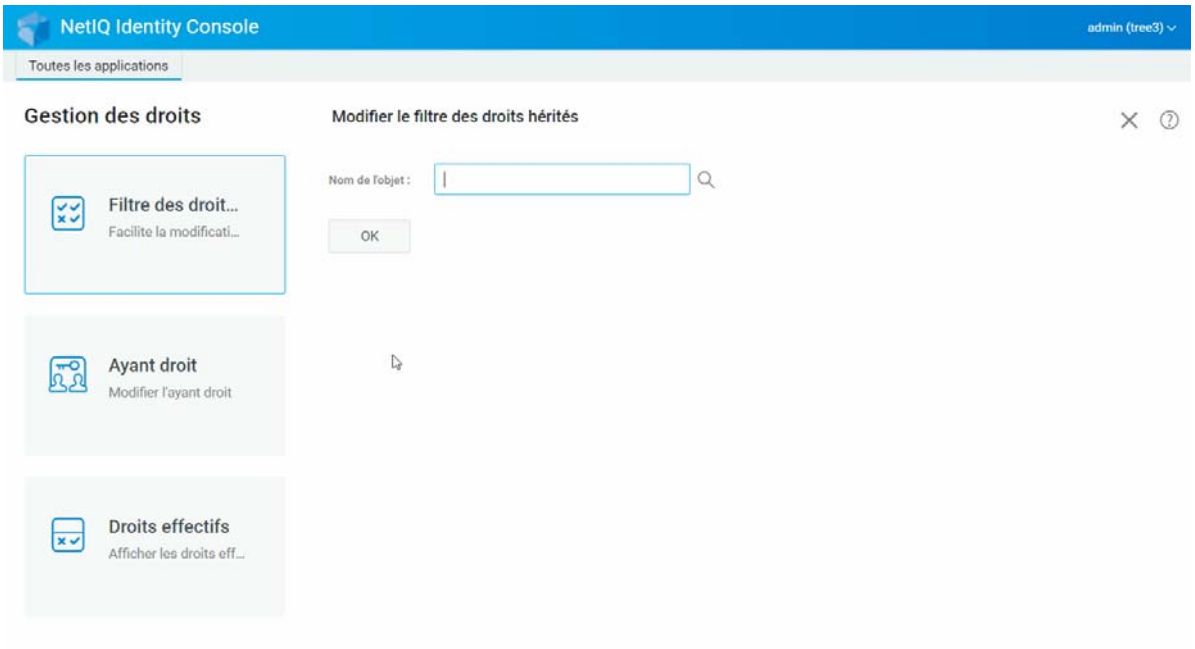
Modification des droits d'un ayant droit

Un ayant droit est un objet qui s'est vu accorder des droits explicites sur un autre objet de votre arborescence Annuaire. Pour modifier la liste des ayants droit d'un objet donné :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des droits**.
2. Sélectionnez **Ayant droit**.
3. Indiquez le nom de l'objet pour lequel vous souhaitez afficher la liste d'ayants droit ou utilisez l'icône du sélecteur d'objet pour le localiser, puis cliquez sur **OK**.

   Cette opération ouvre une liste des ayants droit actuellement assignés à l'objet.
4. Modifiez la liste d'ayants droit selon vos besoins, puis cliquez sur **OK**.
   - Pour ajouter un ayant droit, cliquez sur l'icône .
   - Pour supprimer un ayant droit, cochez la case correspondante, puis cliquez sur l'icône .
   - Pour modifier l'assignation de droits d'un ayant droit, cliquez sur le lien **Droits assignés** de cet ayant droit.

Figure 8-2 *Modification des droits d'un ayant droit*



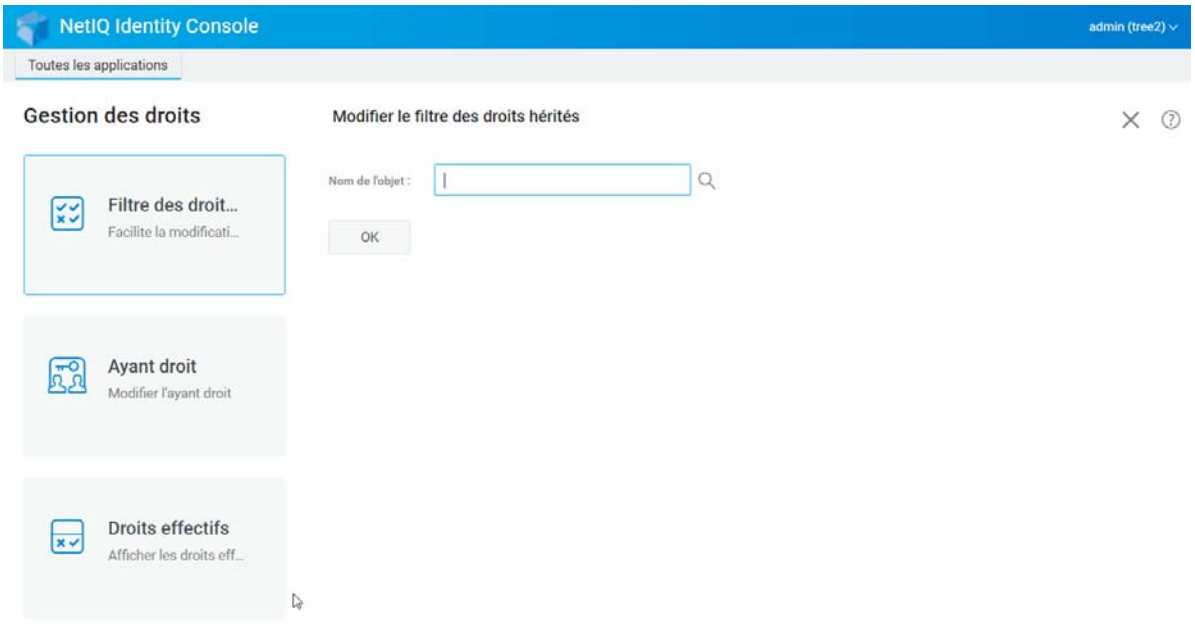
Affichage des droits effectifs

Les droits effectifs sont une combinaison de droits explicites et hérités qu'un objet possède dans l'arborescence Annuaire. Pour afficher les droits effectifs d'un objet sur un autre :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des droits**.
2. Sélectionnez **Droits effectifs**.
3. Indiquez le nom de l'ayant droit pour lequel vous souhaitez afficher les droits ou utilisez l'icône du sélecteur d'objet pour le localiser, puis cliquez sur **OK**.
4. Dans le champ Nom de l'objet, spécifiez le nom de l'objet pour lequel vous souhaitez afficher les droits effectifs de l'ayant droit.

   eDirectory calcule les droits effectifs et les affiche dans le champ **Droits effectifs**.

Figure 8-3 *Affichage des droits effectifs*



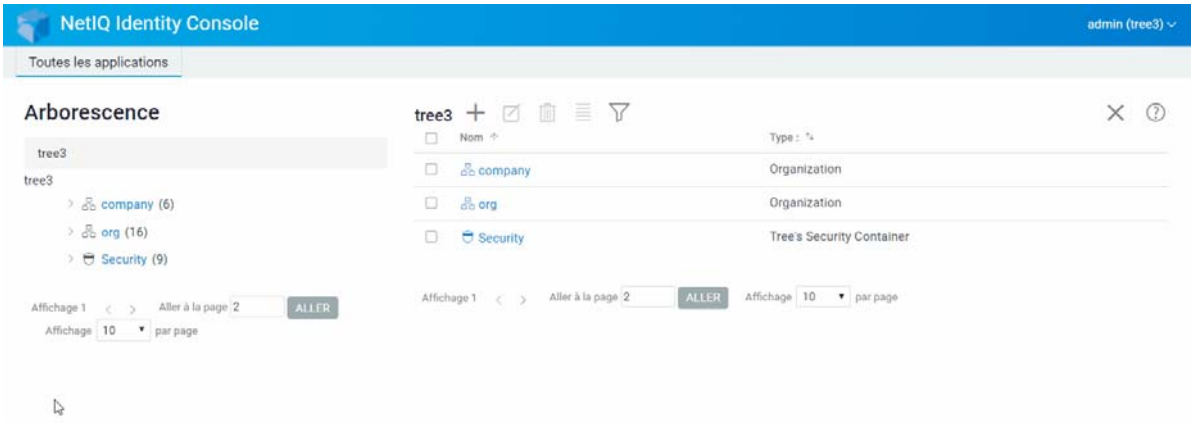
9 Arborescence

Grâce à l'arborescence, vous pouvez parcourir une arborescence Annuaire et créer, supprimer et modifier divers objets de cette arborescence. L'arborescence comporte un cadre de navigation et un cadre de contenu.

Cadre de navigation de l'arborescence

Dans l'arborescence, le cadre de navigation affiche la structure de l'annuaire. Il affiche les conteneurs qui comprennent un volume (système de fichiers), les objets, etc. Vous pouvez cliquer sur toutes les options affichées sous le cadre de navigation pour parcourir la structure de l'annuaire. Par défaut, le cadre de navigation affiche jusqu'à 10 objets subordonnés par conteneur, mais vous pouvez modifier ce paramètre sous le tableau de bord du cadre de navigation dans l'arborescence.

Figure 9-1 *Cadre de navigation de l'arborescence*



Cadre de contenu de l'arborescence

Si vous sélectionnez l'un des objets Conteneur dans le cadre de navigation, le cadre de contenu affiche tous les objets de ce conteneur. Le cadre de contenu est celui dans lequel vous affichez et modifiez les objets Annuaire. Il comporte un en-tête qui propose plusieurs opérations possibles :

Barre de titre : la barre de titre du cadre de contenu affiche le nom de l'objet Conteneur actuellement sélectionné.

En-tête de liste d'objets : l'en-tête de liste d'objets permet d'accéder aux éléments suivants.

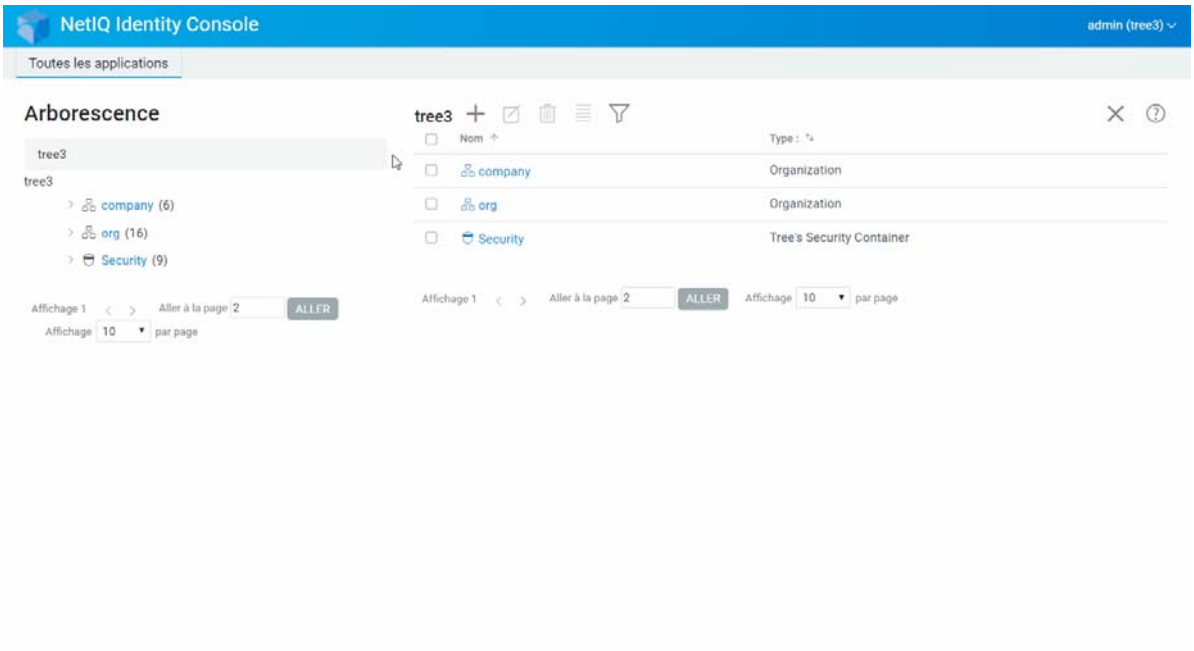
- **Ajouter** : cliquez sur l'icône  pour ajouter un nouvel objet.
- **Modifier** : sélectionnez un objet, puis cliquez sur l'icône  pour le modifier. Vous accédez alors aux propriétés de l'objet sélectionné, qui vous permettent de modifier ses attributs. Il n'est pas possible de modifier plusieurs objets en même temps.
- **Supprimer** : sélectionnez un objet, puis cliquez sur l'icône  pour supprimer l'objet sélectionné. Il est possible de supprimer plusieurs objets à la fois. Les objets non-feuilles ne peuvent pas être supprimés.
- **Opérations** : sélectionnez un objet, puis cliquez sur l'icône  pour ouvrir un menu déroulant contenant les tâches prises en charge pour l'objet sélectionné. Pour effectuer une tâche, sélectionnez-la dans le menu déroulant et indiquez les informations requises.
- **Nombre d'objets** : l'arborescence affiche dans la partie inférieure de la page le nombre d'objets dans la page actuelle. Par défaut, le cadre de contenu affiche jusqu'à 20 objets subordonnés par conteneur, mais vous pouvez modifier ce paramètre.
- **Tout sélectionner** : la case à cocher de l'en-tête permet de sélectionner tous les objets de la page actuelle.
- **Trier** : les colonnes **Nom** et **Type** peuvent être triées. Cliquez sur l'une de ces colonnes pour faire basculer le tri des objets entre l'ordre alphabétique croissant et décroissant.
- **Filtre de recherche** : cliquez sur l'icône  pour ouvrir la fenêtre contextuelle de filtre. Cette option vous permet de créer un filtre qui limite les objets affichés dans la liste. Selon vos besoins, vous pouvez filtrer sur un type et un nom d'objet.

  Sélectionnez l'option  pour ouvrir la boîte de dialogue de filtre avancé qui vous permet de créer un filtre à l'aide de presque tous les attributs d'objet. Pour plus d'informations, reportez-vous à la section « Configuration de la recherche avancée » page 24.

Pour effectuer une opération sur un objet, cochez sa case, puis sélectionnez l'icône d'opération  dans l'en-tête Liste d'objets. Sélectionnez l'objet (niveau actuel) sur lequel effectuer une opération dans le conteneur que vous parcourez actuellement. Vous pouvez effectuer les opérations suivantes à l'aide de cette option :

- « Modification du filtre des droits hérités » page 49
- « Modification des droits d'un ayant droit » page 50
- « Extension d'un objet » page 62
- « Changement du nom d'un objet » page 46
- Définir un mot de passe
- « Affichage des droits effectifs » page 51

Figure 9-2 *Cadre de contenu de l'arborescence*



10 Gestion du schéma

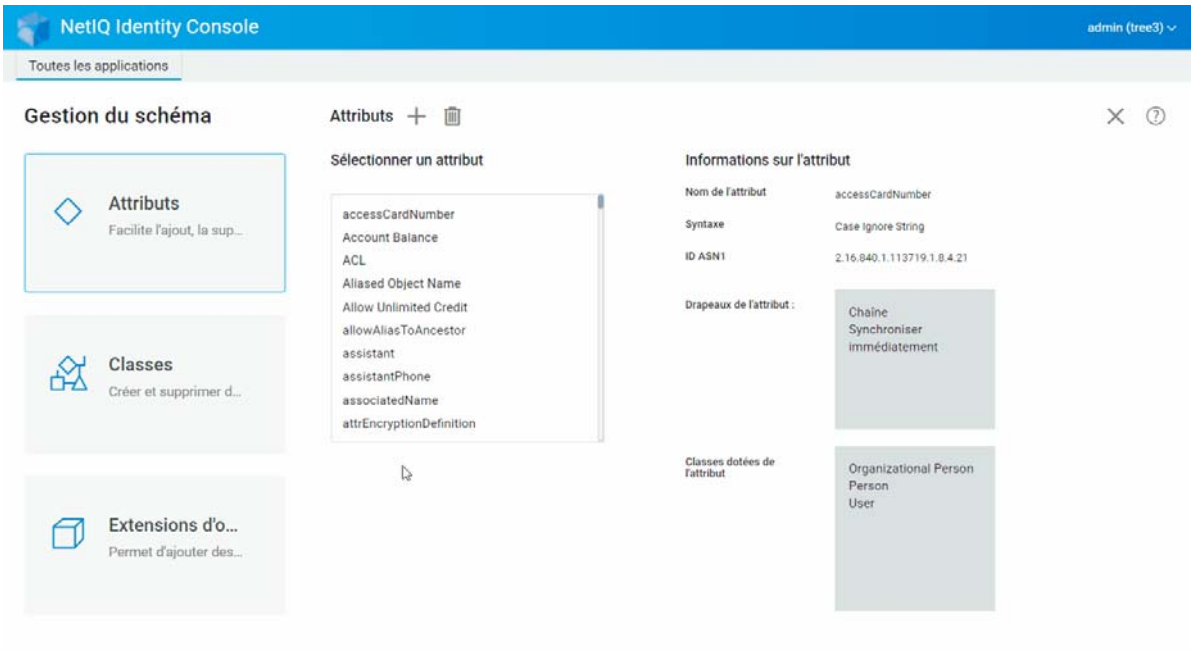
Le schéma de l'annuaire définit les types d'objets qui peuvent être créés dans l'arborescence (par exemple, utilisateurs, imprimantes, groupes, etc.), ainsi que les informations obligatoires ou facultatives lors de la création d'un objet. Identity Console propose les tâches suivantes liées au schéma :

Création d'un attribut

Vous pouvez définir des types d'attribut personnalisés et les ajouter en tant qu'attributs facultatifs aux classes d'objet existantes. Toutefois, vous ne pouvez pas ajouter d'attributs obligatoires à des classes existantes. Pour créer un attribut:

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion du schéma**.
2. Cliquez sur l'icône +.
3. Sur la page Créer un attribut, entrez les informations suivantes :
   - Nom de l'attribut
   - ID ASN1 (facultatif)
   - Syntaxe
   - Drapeaux de l'attribut
4. Après avoir entré toutes les informations nécessaires, cliquez sur le bouton Créer.
5. Un message de confirmation s'affiche pour signaler que l'attribut a été créé.

Figure 10-1 *Création d'un attribut*



Création d'une classe

L'option **Gestion des schémas** permet de définir des classes personnalisées. Vous pouvez ensuite étendre des objets distincts à l'aide des propriétés définies dans ces classes. Pour créer une classe :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion du schéma**, puis sélectionnez **Classes**.
2. Cliquez sur l'icône +.
3. Sur la page Créer un attribut, entrez les informations suivantes :
   - Nom de classe
   - ID ASN1 (facultatif)
   - Drapeaux de la classe : sélectionnez l'un des drapeaux de classe suivants :
     - **Classe effective :** activez ce drapeau pour créer une classe effective pouvant être utilisée pour créer des objets.
     - **Classe non effective :** Elle est utilisée comme marque de réservation pour un groupe d'attributs. Une classe non effective ne peut pas être utilisée pour la création d'objets, mais elle peut être spécifiée comme classe dont les attributs peuvent être transmis (par héritage) aux autres classes. La classe Personne, par exemple, est une classe non effective dont la classe Utilisateur a hérité des attributs.
     - **Classe auxiliaire :** ensemble d'attributs qui ne peuvent être associés qu'à des objets individuels et non à des classes entières.
     - **Classe du conteneur :** activez ce drapeau pour faire de cette classe une classe Conteneur. Lorsque cette classe est ensuite utilisée pour créer des objets, ces objets deviennent des objets Conteneur (OU, par exemple). Ne définissez cet indicateur que pour une classe d'objet Feuille.

REMARQUE : si vous sélectionnez des classes effectives et non effectives, vous devez également indiquer des valeurs de superclasse. Si vous choisissez la classe auxiliaire, la superclasse est facultative.

4 Après avoir entré toutes les informations nécessaires, cliquez sur **Suivant**.

5 Dans l'écran suivant, sélectionnez les attributs facultatifs, obligatoires et d'assignation de nom, puis cliquez sur **OK**.

6 Un message de confirmation s'affiche pour signaler que la classe a été créée.

Assignation d'attributs à une classe

Vous pouvez ajouter des attributs facultatifs à des classes existantes à chaque modification des besoins de votre organisation ou lorsque vous vous préparez à fusionner des arborescences. Pour ajouter un attribut à une classe existante:

REMARQUE : les attributs obligatoires ne peuvent être définis qu'au moment de la création d'une classe. Un attribut obligatoire doit être fourni au moment de la création d'un objet.

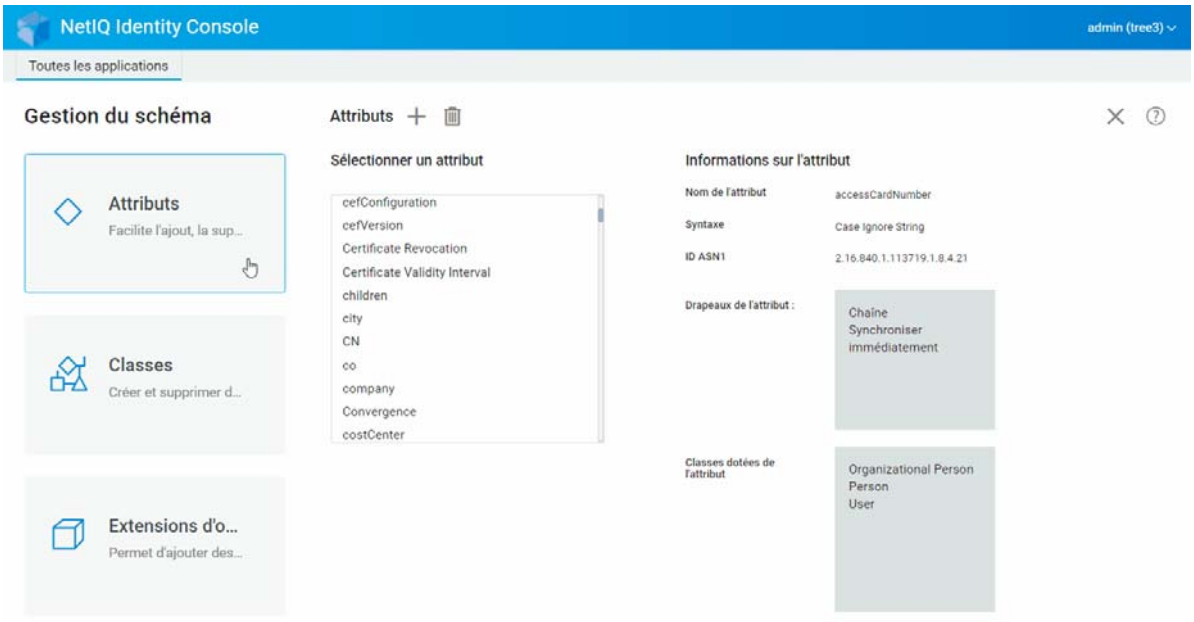
1 Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion du schéma**, puis sélectionnez **Classes**.

2 Cliquez sur une classe dans la liste **Sélectionner une classe**.

3 Les informations de la classe correspondante s'affichent dans la partie droite de l'écran.

4 Cliquez sur le bouton + situé en regard de l'option **Attributs**, sélectionnez les attributs à ajouter, puis cliquez sur **Ajouter** > **Enregistrer**.

Figure 10-2 *Assignation d'attributs à une classe*

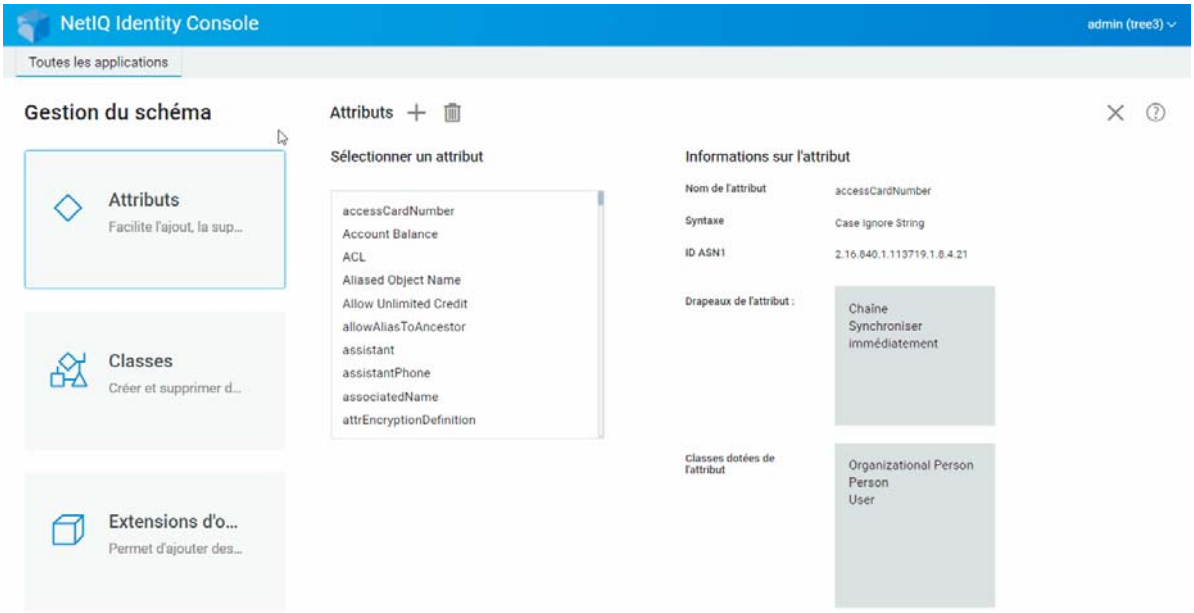


Affichage des informations sur l'attribut

Vous pouvez afficher les détails sur la structure d'un attribut tels que la syntaxe, les drapeaux et les classes qui utilisent l'attribut. Pour afficher les informations concernant un attribut :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion du schéma**, puis sélectionnez **Attributs**.
2. Cliquez sur un attribut dans la liste **Sélectionner un attribut**.
3. Les informations de l'attribut correspondant s'affichent dans la partie droite de l'écran.

Figure 10-3 *Affichage des informations sur un attribut*



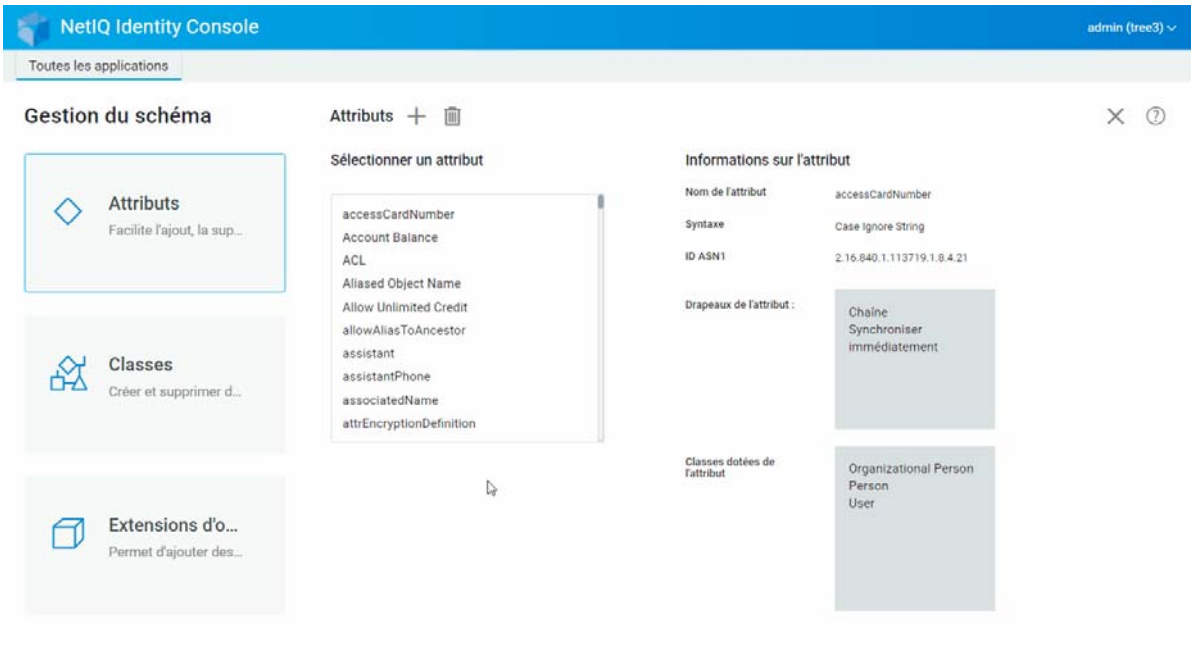
Suppression d'un attribut

Vous pouvez supprimer les attributs inutilisés qui ne font pas partie du schéma de base de votre arborescence eDirectory. Cette opération peut être utile après la fusion de deux arborescences Annuaire ou si un attribut est devenu obsolète. Pour supprimer un attribut :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion du schéma**, puis sélectionnez **Attributs**.
2. Dans la liste **Sélectionner un attribut**, sélectionnez l'attribut à supprimer, puis cliquez sur l'icône .

   REMARQUE : l'icône n'est activée que si vous sélectionnez un attribut qui peut être supprimé.
3. Cliquez sur **OK** pour confirmer la suppression.

Figure 10-4 *Suppression d'un attribut*



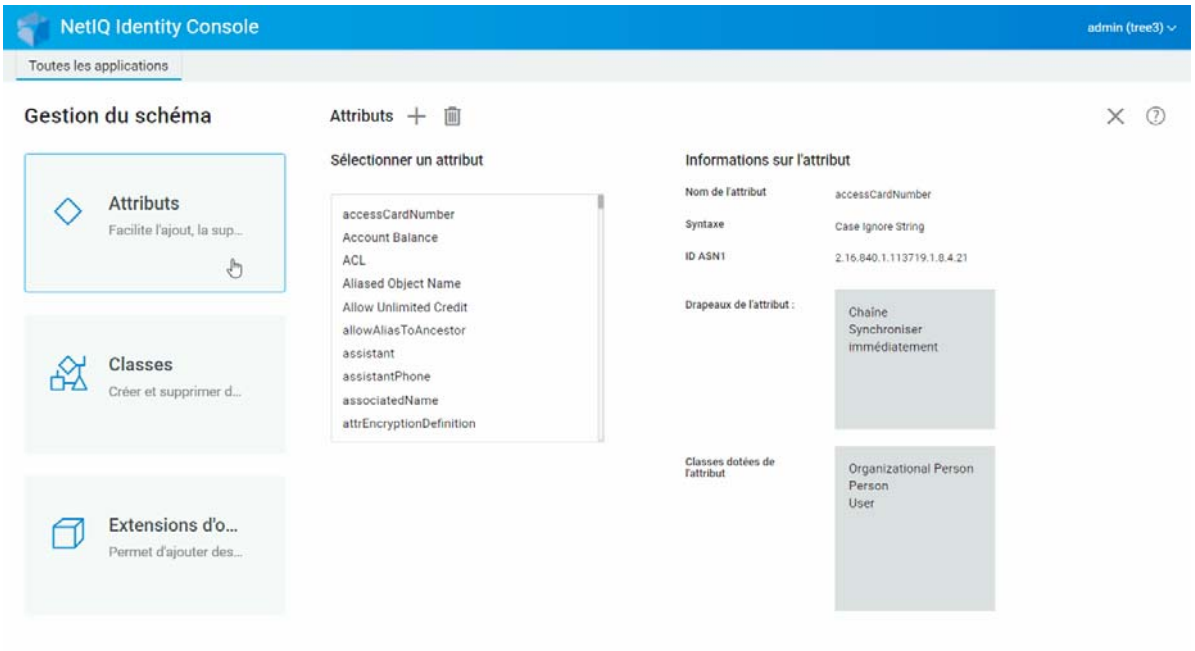
Suppression d'une classe

Vous pouvez supprimer les classes inutilisées qui ne font pas partie du schéma de base de votre arborescence eDirectory. Identity Console vous empêche de supprimer des classes qui sont actuellement utilisées dans des partitions répliquées localement. Pour supprimer une classe :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion du schéma**, puis sélectionnez **Classes**.
2. Dans la liste **Sélectionner une classe**, sélectionnez la classe à supprimer, puis cliquez sur l'icône .

   REMARQUE : l'icône n'est activée que si vous sélectionnez une classe qui peut être supprimée.
3. Cliquez sur **OK** pour confirmer la suppression.

Figure 10-5 *Suppression d'une classe*



Extension d'un objet

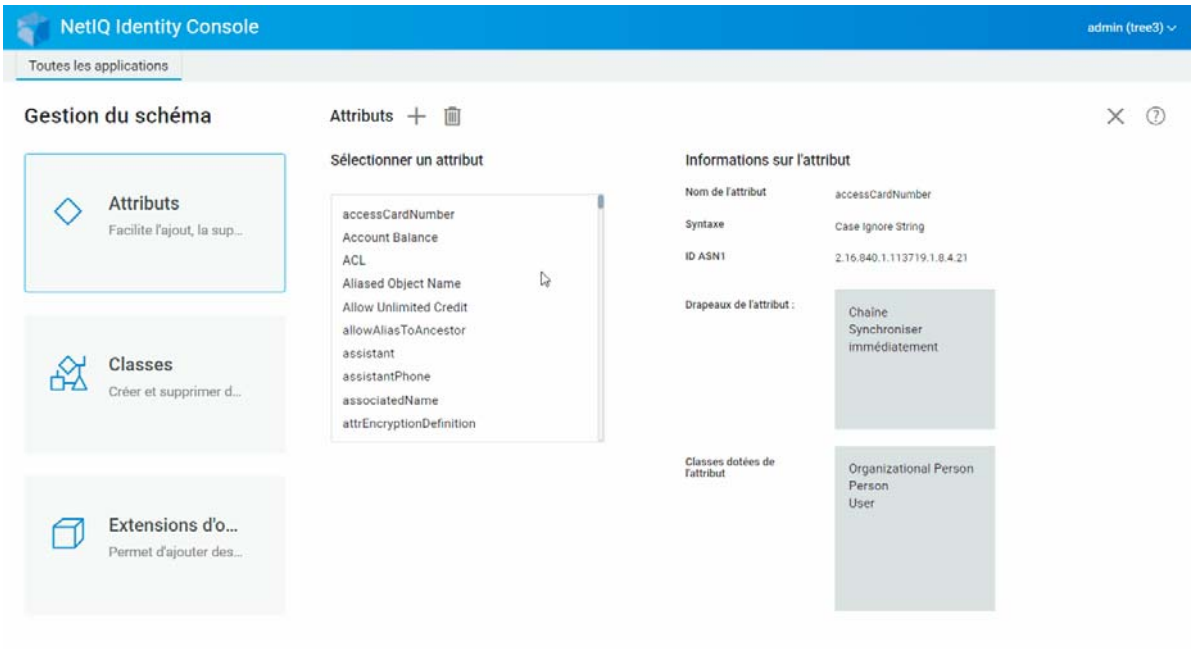
Pour étendre un objet, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion du schéma**, puis sélectionnez **Extension d'objet**.
2. Indiquez le nom de l'objet ou utilisez le sélecteur d'objet pour sélectionner l'objet à étendre, puis cliquez sur l'icône .
3. Cliquez sur l'icône , sélectionnez une classe auxiliaire, puis cliquez sur **OK**.

   REMARQUE : si un attribut obligatoire est attaché à la classe auxiliaire sélectionnée, vous devez entrer les valeurs requises dans la fenêtre contextuelle **Attributs obligatoires**.

   ---
4. Un message de confirmation s'affiche pour signaler que la classe auxiliaire a été ajoutée à l'objet.
5. Pour supprimer une classe auxiliaire de l'objet, sélectionnez la classe correspondante, puis cliquez sur l'icône .

Figure 10-6 *Extension d'un objet*



11 Gestion des événements d'audit

Ce chapitre explique comment gérer les différents événements d'audit à l'aide d'Identity Console. Grâce à cette fonctionnalité, vous pouvez activer ou désactiver les événements d'audit pour le serveur NCP.

Configuration des événements d'audit CEF

1. Connectez-vous à Identity Console à l'aide de votre nom d'utilisateur et de votre mot de passe.
2. Sélectionnez **Audit**.
3. Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.

   REMARQUE : lorsque vous activez les événements CEF pour un serveur NCP pour la première fois, peu d'événements sont sélectionnés par défaut.

   ---

4. Configurez les événements d'audit CEF :
   - **Configuration d'événements :** activez ou désactivez les événements suivants en fonction de l'audit requis pour votre environnement :

REMARQUE : par défaut, chaque catégorie d'événements figurant dans la section Configuration d'événements est réduite. Vous pouvez développer chacune de ces catégories pour sélectionner des événements individuels.

Options	Description
Événements de sécurité	Sélectionnez les événements de sécurité pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour ajouter ou supprimer un membre, pour détecter un intrus, pour changer de mot de passe, pour authentifier des utilisateurs, etc.
Événements d'objets	Sélectionnez les événements d'objets pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour créer, supprimer, renommer, déplacer et rechercher des objets.
Événements d'attributs	Sélectionnez les événements d'attributs pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour lire et supprimer des attributs et pour ajouter, supprimer et comparer des valeurs d'attributs.
Événements LDAP	Sélectionnez les événements LDAP pour lesquels vous souhaitez consigner des événements.

- **Paramètres avancés :** grâce aux paramètres avancés, vous pouvez effectuer les opérations suivantes :
  - **Global :** vous pouvez sélectionner ou désélectionner les paramètres globaux pour les entrées en double.
    - **Ne pas envoyer d'événement répliqué :** sélectionnez cette option pour ne plus recevoir les événements en double en raison de la réplication à partir d'autres serveurs.
  - **Consigner les valeurs de l'événement :** les événements sont consignés dans un fichier texte. Les valeurs d'événements de plus de 768 octets sont considérées comme de « grandes valeurs ». Vous pouvez consigner des événements de n'importe quelle taille.
    - **Consigner de grandes valeurs :** sélectionnez cette option pour consigner les événements dont la taille est supérieure à 768 octets.
    - **Consigner les valeurs d'attribut :** sélectionnez cette option pour afficher les valeurs d'attribut. Cette option s'applique uniquement aux événements **Ajouter une valeur** et **Supprimer la valeur**.
    - **Consigner les valeurs d'attributs chiffrés :** sélectionnez cette option pour afficher les valeurs d'attributs chiffrés. Cette option s'applique uniquement aux événements **Ajouter une valeur** et **Supprimer la valeur**.

    REMARQUE : si la taille de l'événement est supérieure à 768 octets, sa valeur est tronquée et enregistrée dans le fichier journal.

Présentation des types d'événements CEF

Vous pouvez configurer CEF pour consigner les événements dans les catégories suivantes :

- Sécurité
- Objets
- Attributs
- LDAP

Vous pouvez auditer les ensembles de types d'événement par défaut suivants :

Catégorie	Type d'événement
Sécurité	◆ ACL modifiée ◆ Ajout d'un membre ◆ Suppression d'un membre ◆ Intrusion détectée ◆ Connexion désactivée ◆ Connexion activée ◆ Connexion ◆ Modification des équivalents de sécurité ◆ Configuration de l'audit ◆ Modification du mot de passe ◆ Déverrouillage du compte ◆ Déconnexion ◆ Connexion ◆ Emprunt d'identité ◆ Authentification ◆ Vérification du mot de passe ◆ Modification de la configuration de la connexion ◆ Informations d'identification de la requête
Objets	◆ Créer un objet ◆ Supprimer l'objet ◆ Renommer l'objet ◆ Déplacer l'objet ◆ DSU lu ◆ Rechercher
Attributs	◆ Lire l'attribut ◆ Supprimer l'attribut ◆ Ajouter une valeur ◆ Supprimer la valeur ◆ Comparer la valeur de l'attribut

Catégorie	Type d'événement
LDAP	◆ Liaison LDAP ◆ Réponse de la liaison LDAP ◆ Annulation de la liaison LDAP ◆ Connexion LDAP ◆ Recherche LDAP ◆ Réponse de la recherche LDAP ◆ Réponse de l'entrée de recherche LDAP ◆ Ajout LDAP ◆ Réponse de l'ajout LDAP ◆ Comparaison LDAP ◆ Réponse de la comparaison LDAP ◆ Modification LDAP ◆ Réponse de la modification LDAP ◆ Suppression LDAP ◆ Suppression de réponse LDAP ◆ Modification de DN LDAP ◆ Réponse de la modification du DN LDAP ◆ Abandon LDAP ◆ Opération étendue LDAP ◆ Opération étendue du système LDAP ◆ Réponse de l'opération étendue LDAP ◆ Modification de la configuration du serveur LDAP ◆ Opération LDAP inconnue ◆ Modification de mot de passe LDAP

Configuration du filtrage d'audit CEF

À l'aide de filtres et de notifications d'événement, CEF est capable de signaler la survenue ou la non-survenue d'un type d'événement spécifique. Vous pouvez également filtrer les événements pour un(e) ou plusieurs classes ou attributs d'objet spécifiques, selon le type d'événement. CEF évalue tous les événements générés en fonction des filtres configurés sur le serveur eDirectory et ne consigne que les événements qui correspondent à ces filtres.

Cette section fournit les informations nécessaires pour configurer les filtres et les notifications du système.

- « Filtrage des événements eDirectory à l'aide du filtre d'exclusion » page 69
- « Filtrage des événements d'objet CEF » page 69
- « Filtrage des événements d'attribut CEF » page 70

Filtrage des événements eDirectory à l'aide du filtre d'exclusion

Cliquez sur le lien **Filtre d'exclusion** afin de configurer le filtrage des classes d'objet et des attributs pour lesquels vous ne souhaitez pas générer d'événement. Vous pouvez sélectionner des classes d'objet et des attributs.

Pour configurer le filtrage des événements eDirectory indésirables :

1. Dans Identity Console, sélectionnez **Audit** sur la page d'accueil.
2. Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.
3. Accédez à **Paramètres avancés**, puis cliquez sur **Filtre d'exclusion** sous **Filtres**.

   La fenêtre Filtrage des exclusions CEF s'affiche.
4. Dans la liste **Classes d'objets disponibles**, sélectionnez les classes d'objets pour lesquelles vous ne souhaitez pas collecter d'événements, puis cliquez sur la flèche droite pour les déplacer dans la liste **Classes d'objets sélectionnées**.
5. Dans la liste **Attributs disponibles**, sélectionnez le nombre souhaité d'attributs. Sélectionnez l'attribut, puis cliquez sur la flèche droite pour l'ajouter à la liste des attributs sélectionnés.
6. Cliquez sur **OK**.

À l'aide du filtre configuré, le module d'audit CEF arrête de générer des événements pour toutes les classes d'objets et les attributs sélectionnés.

Filtrage des événements d'objet CEF

Vous pouvez configurer le filtrage des objets de manière à ne rechercher qu'un seul événement ou un type d'événements spécifique. Par exemple, si vous souhaitez être averti lorsqu'une personne crée un compte utilisateur dans eDirectory, vous pouvez créer un filtre de sélection de la classe d'objet Utilisateur pour consigner les événements dans le cadre de la création d'un nouvel objet Utilisateur.

Pour configurer le filtrage des comptes, cliquez sur le lien Événements d'objets, sélectionnez la classe, puis cliquez sur **OK** pour quitter l'application.

Pour configurer des filtres pour les événements de gestion des comptes :

1. Dans Identity Console, sélectionnez **Audit** sur la page d'accueil.
2. Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.
3. Accédez à **Paramètres avancés**, puis cliquez sur **Événements d'objet** sous **Filtres**.

   La fenêtre Filtrage de la configuration des objets CEF s'affiche.
4. Dans la liste **Classes d'objets disponibles**, sélectionnez une classe d'objet, cliquez sur la flèche droite pour déplacer la classe d'objet vers la liste **Classes d'objets sélectionnées**, puis cliquez sur **OK**.

À l'aide du filtre configuré, le module d'audit CEF vérifie tous les événements générés pour les classes d'objets sélectionnées et consigne ces événements.

Filtrage des événements d'attribut CEF

Cliquez sur le lien **Événements d'attributs** pour configurer le filtrage des événements d'attributs. Par exemple, si vous souhaitez être averti lorsqu'une personne ajoute une nouvelle valeur d'attribut dans eDirectory, vous pouvez créer un filtre pour consigner des événements en cas d'ajout d'une nouvelle valeur.

Pour configurer le filtrage des événements d'attribut :

1. Dans Identity Console, sélectionnez **Audit** sur la page d'accueil.
2. Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.
3. Accédez à **Paramètres avancés**, puis cliquez sur **Événements d'attribut** sous **Filtres**.

   La fenêtre **Filtrage de la configuration des attributs** s'affiche.
4. Dans la liste **Classes d'objets disponibles**, sélectionnez les classes d'objets pour lesquelles vous souhaitez collecter les événements, puis cliquez sur la flèche droite pour les déplacer dans la liste **Classes d'objets sélectionnées**.
5. Dans la liste **Attributs disponibles**, sélectionnez le nombre souhaité d'attributs pour les classes d'objet sélectionnées. Sélectionnez l'attribut, puis cliquez sur la flèche droite pour l'ajouter à la liste des attributs sélectionnés.

   REMARQUE : si vous sélectionnez une classe d'objet, tous les événements d'attributs pour tous les attributs de cette classe d'objet sont sélectionnés. Dans ce cas, vous obtiendrez tous les événements d'attributs pour l'ensemble des attributs sélectionnés dans les classes d'objet sélectionnées.

   ---
6. Cliquez sur **OK**.

Lorsque le filtre est configuré, le module d'audit CEF contrôle tous les événements générés pour les classes d'objet et les attributs sélectionnés et consigne ces événements.

12 Gestion des attributs chiffrés

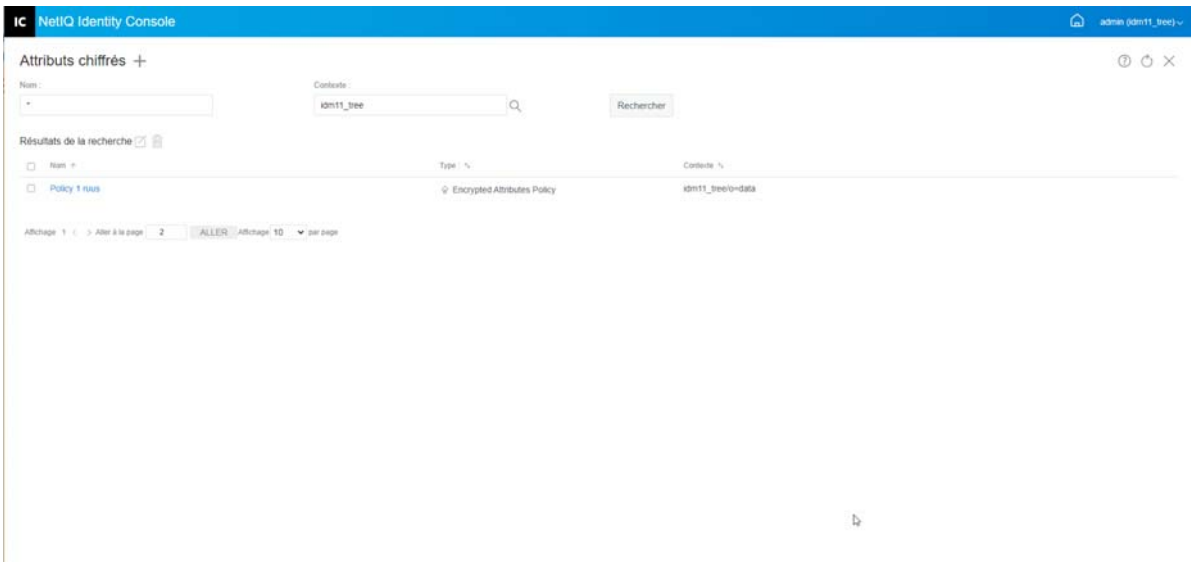
Identity Console permet de lire les attributs chiffrés en toute sécurité à partir du serveur eDirectory. Grâce à Identity Console, vous pouvez créer, modifier ou supprimer plusieurs stratégies pour ces attributs chiffrés.

Création d'une stratégie d'attributs chiffrés

Pour créer une stratégie d'attributs :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Attributs chiffrés**.
2. Cliquez sur l'icône +.
3. Sur la page Créer une stratégie des attributs chiffrés, entrez les informations suivantes :
   - Indiquez le nom de la stratégie.
   - Entrez ou sélectionnez le contexte.
   - Sélectionnez le serveur NCP.
   - Sélectionnez des attributs.
4. Après avoir entré toutes les informations nécessaires, cliquez sur **Terminer**.
5. Un message de confirmation s'affiche pour signaler que la stratégie a été créée.

Figure 12-1 *Création d'une stratégie d'attributs chiffrés*

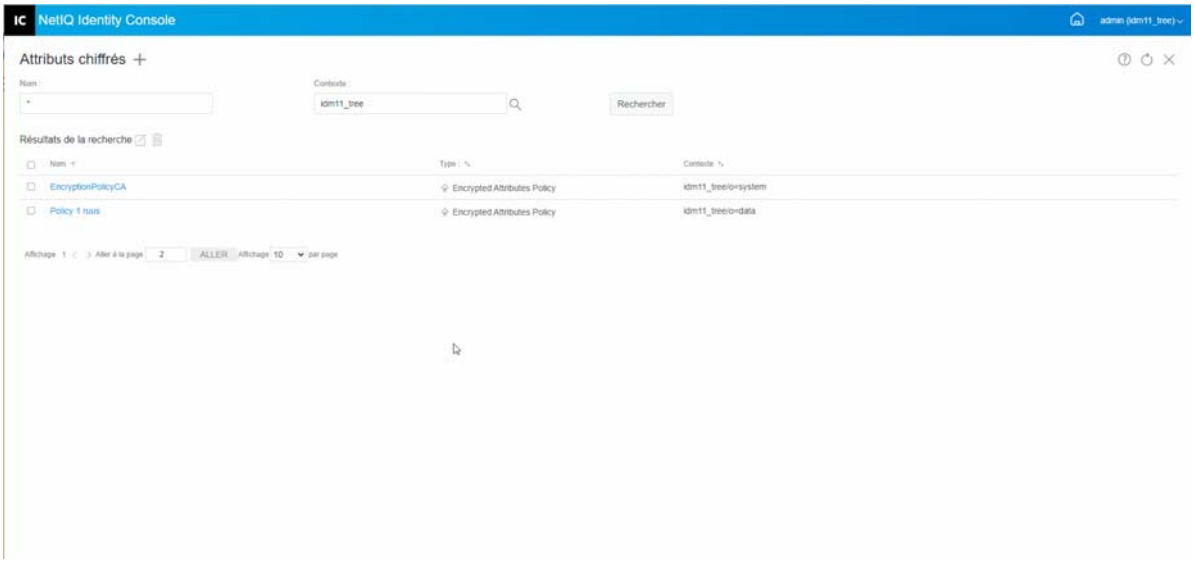


Suppression d'une stratégie d'attributs chiffrés

Pour supprimer une stratégie d'attributs chiffrés :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Attributs chiffrés**.
2. Indiquez le nom et le contexte de l'attribut ou utilisez la fonction de recherche pour le trouver, puis cliquez sur le bouton Rechercher.
3. Sélectionnez le ou les attributs de la liste, puis cliquez sur l'icône 🗑.
4. Un message de confirmation s'affiche pour signaler que la stratégie a été supprimée.

Figure 12-2 *Suppression d'une stratégie d'attributs chiffrés*

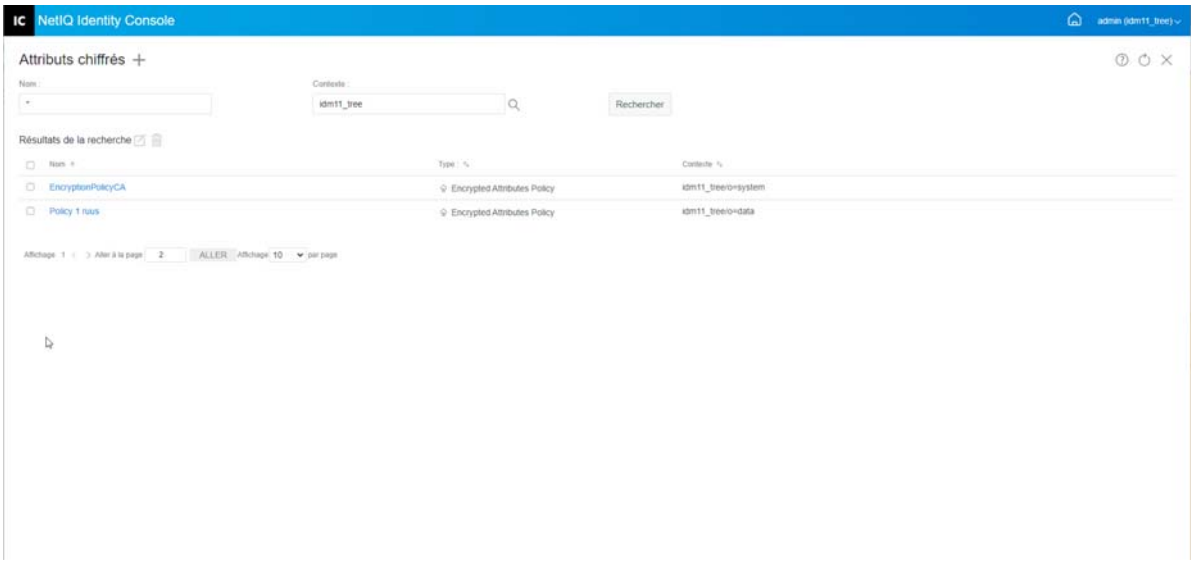


Modification d'une stratégie d'attributs chiffrés

Pour modifier une stratégie d'attributs chiffrés :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Attributs chiffrés**.
2. Entrez le nom et le contexte de l'objet, puis cliquez sur le bouton Rechercher.
3. Sélectionnez l'attribut souhaité dans la liste d'objets, puis cliquez sur l'icône ✎.
4. Effectuez les modifications souhaitées, puis cliquez sur le bouton Enregistrer.
5. Un message de confirmation s'affiche pour signaler que la stratégie a été modifiée.

Figure 12-3 *Modification d'une stratégie d'attributs chiffrés*



13 Gestion de la réplication chiffrée

Pour activer la réplication chiffrée, vous devez configurer une partition correspondante. Les paramètres de configuration sont stockés dans l'objet Racine de la partition. Vous ne pouvez activer la réplication chiffrée qu'au niveau d'une partition. Lorsque vous activez la réplication chiffrée au niveau d'une partition, la réplication entre toutes les répliques qui hébergent la partition est chiffrée. Imaginons, par exemple, que la partition P1 comporte les répliques R1, R2, R3 et R4. Vous pouvez chiffrer la réplication entre toutes les répliques.

- « Activation de la réplication chiffrée pour une partition » page 75

Activation de la réplication chiffrée pour une partition

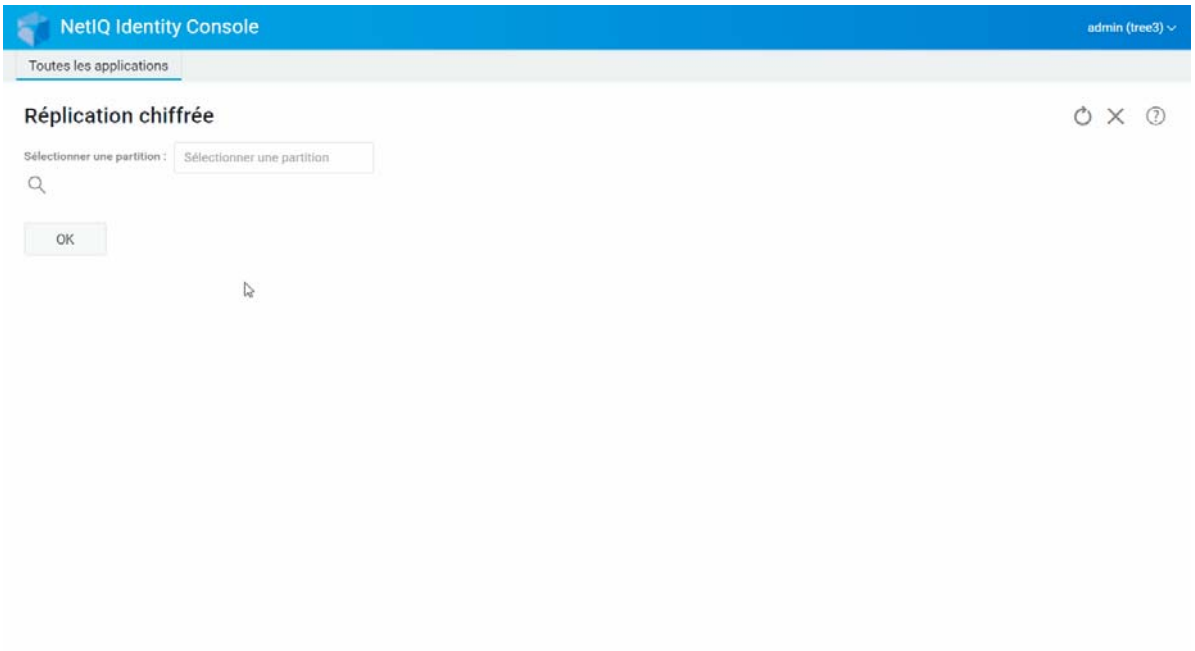
Pour activer la réplication chiffrée pour une partition :

REMARQUE : pour activer une partition pour la réplication chiffrée, tous les serveurs hébergeant cette partition doivent exécuter eDirectory 9.2 ou une version ultérieure.

---

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Réplication chiffrée**.
2. Indiquez ou recherchez la partition pour laquelle vous voulez activer la réplication chiffrée.
3. Veillez à sélectionner l'option **Activer la réplication chiffrée**. Si vous souhaitez désactiver la réplication chiffrée pour une partition, désélectionnez cette option.
4. Cliquez sur **Terminer**.
5. Un message de confirmation s'affiche pour signaler que la réplication chiffrée a été activée.

Figure 13-1 *Activation de la réplication chiffrée pour une partition*



14 Gestion des partitions et des répliques

Les opérations sur les partitions et les répliques vous permettent de gérer la présentation et la distribution d'eDirectory sur vos serveurs Annuaire.

Les partitions créent des divisions logiques de l'arborescence eDirectory. Par exemple, si vous choisissez une unité organisationnelle et la créez en tant que nouvelle partition, vous séparez l'unité organisationnelle et tous ses objets subordonnés de sa partition parent. L'objet Unité organisationnelle choisi devient la racine de la nouvelle partition. Les répliques de la nouvelle partition se trouvent sur les mêmes serveurs que celles de la partition parent, et les objets de cette nouvelle partition sont placés dans l'objet Racine de la partition.

Les tâches suivantes peuvent être effectuées à l'aide du module Partition :

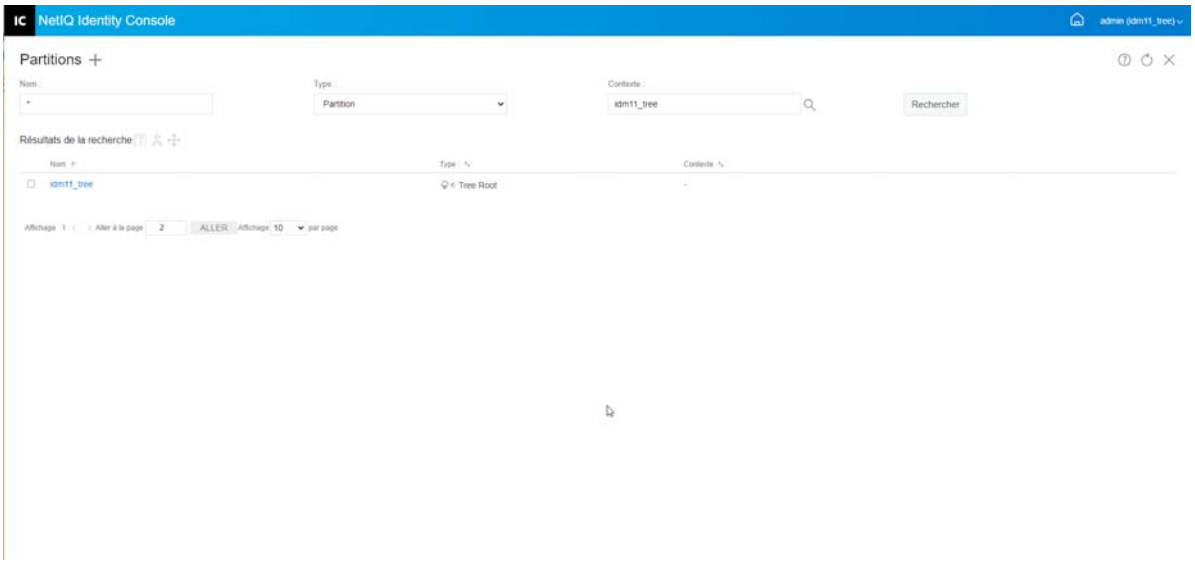
- « Création d'une partition » page 77
- « Fusionner une partition » page 78
- « Modification d'une partition » page 79
- « Déplacement d'une partition » page 80

Création d'une partition

Pour créer une partition, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des partitions**.
2. Cliquez sur l'icône  .
3. Sur la page Créer une partition, spécifiez le conteneur à utiliser en tant que racine de la nouvelle partition ou utilisez l'icône du sélecteur d'objet  pour le localiser, puis cliquez sur **Créer**.
4. Un message de confirmation s'affiche pour signaler que la partition a été créée.

Figure 14-1 *Création d'une partition*

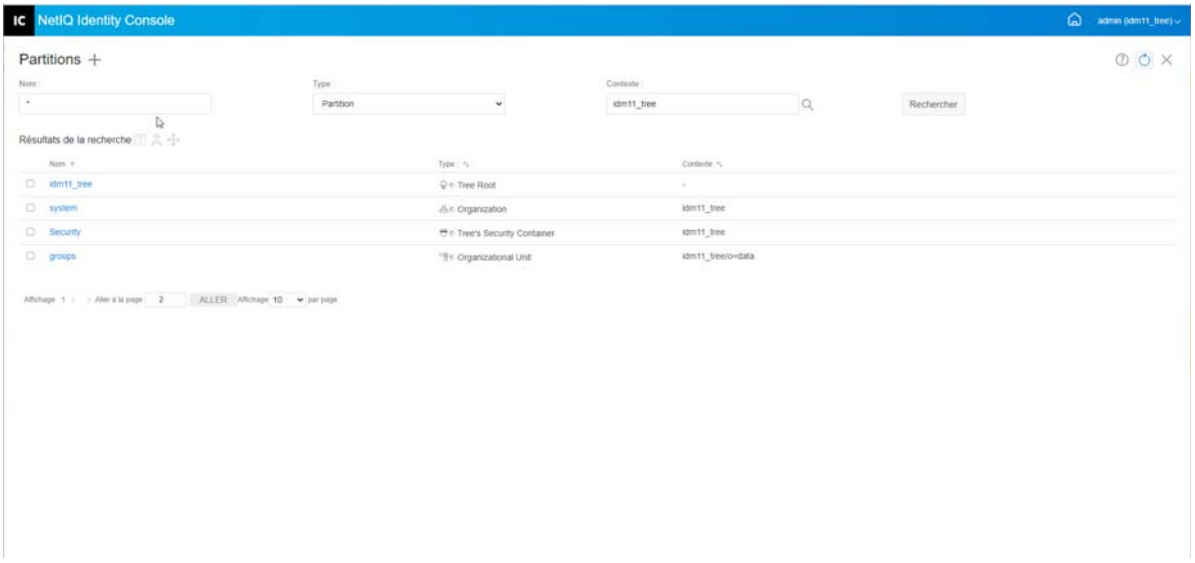


Fusionner une partition

Pour fusionner une partition avec la partition parent correspondante, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des partitions**.
2. Indiquez le nom, le type et le contexte de la partition concernée ou utilisez la fonction de recherche pour la localiser, puis cliquez sur le bouton Rechercher.
3. Sélectionnez la partition souhaitée dans la liste de recherche, cliquez sur l'icône  , puis cliquez sur **OK**.
4. Un message de confirmation s'affiche pour signaler que la partition a été fusionnée.

Figure 14-2 *Fusion d'une partition*



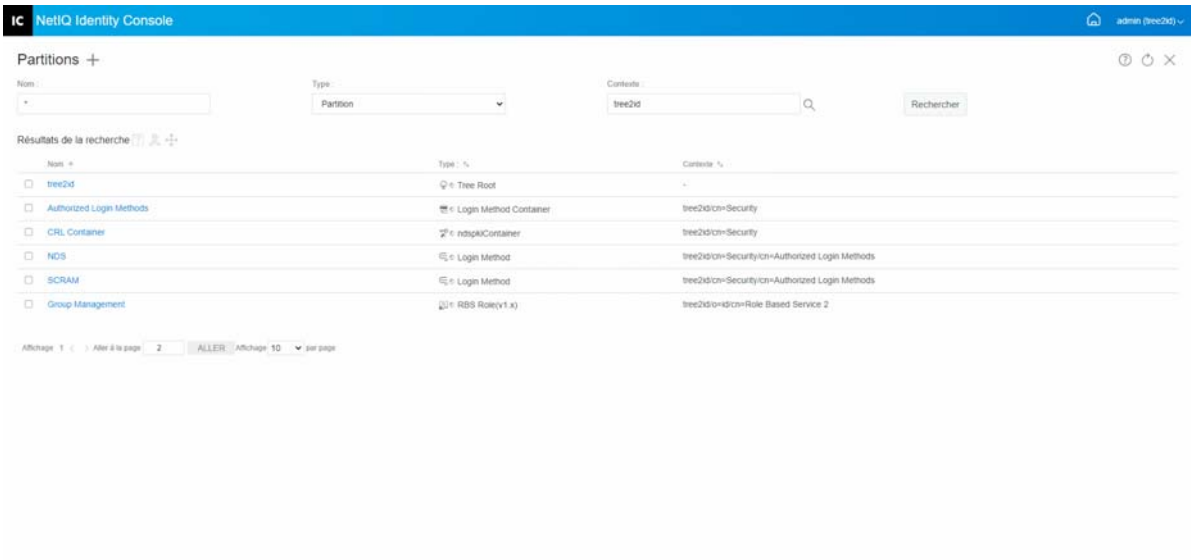
Modification d'une partition

Pour modifier une partition, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des partitions**.
2. Entrez le nom, le type et le contexte de la partition concernée, puis cliquez sur le bouton Rechercher.
3. Sélectionnez la partition souhaitée dans la liste de recherche, puis cliquez sur l'icône .
4. Cliquez sur l'option **Éditer** sous **Filtre** pour modifier les filtres de répliques et les classes et attributs correspondants, puis cliquez sur **OK**.

   Si vous avez sélectionné **Serveur** dans le champ **Type**, la liste de tous les serveurs s'affiche. Cliquez sur chaque serveur pour afficher la liste de toutes les partitions correspondantes.
5. Un message de confirmation s'affiche pour signaler que la partition a été modifiée.

Figure 14-3 *Modification d'une partition*



Déplacement d'une partition

Si vous déplacez une partition, la sous-arborescence correspondante est déplacée dans l'arborescence Annuaire. Cette opération est également une opération de nettoyage et greffage. Vous ne pouvez pas déplacer les partitions qui n'ont pas de subordonnées. Si des partitions subordonnées existent, vous devez d'abord les fusionner avant d'effectuer l'opération de déplacement.

Lorsque vous déplacez une partition, eDirectory modifie toutes les références à l'objet racine de cette partition. Le nom commun de l'objet reste inchangé ; cependant, le nom complet du conteneur (et de tous les objets qui lui sont subordonnés) est modifié.

REMARQUE : Lorsque vous déplacez une partition, vous devez respecter les règles d'endiguement d'eDirectory. Par exemple, vous ne pouvez pas déplacer un objet Unité organisationnelle qui se trouve directement sous la racine de l'arborescence Annuaire, car les règles d'endiguement de la racine n'autorisent que le déplacement des objets Lieu, Pays ou Organisation.

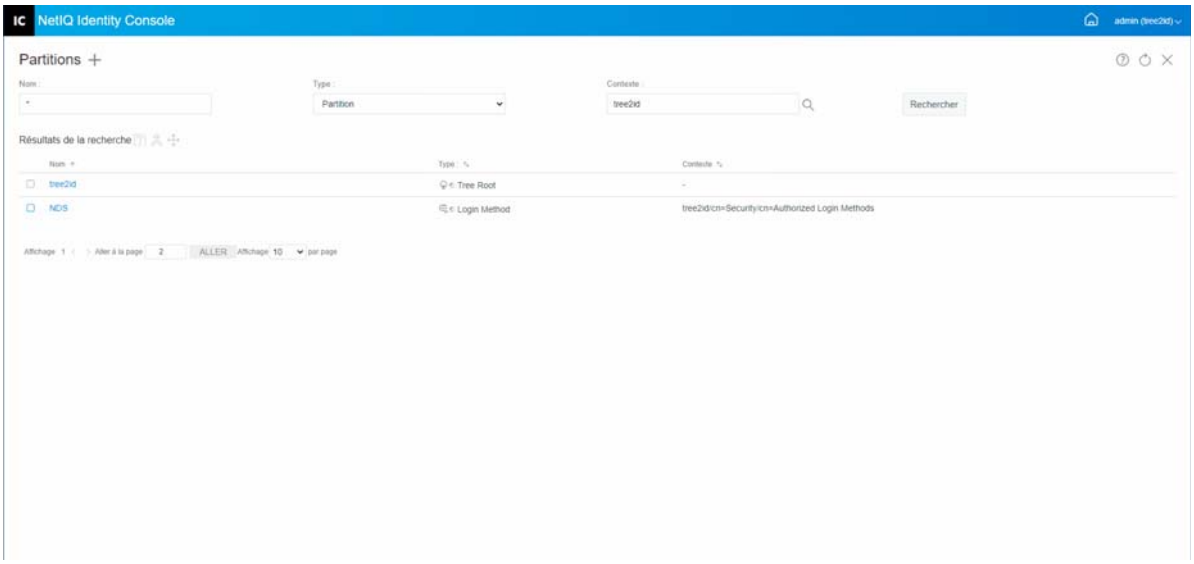
Pour déplacer une partition, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des partitions**.
2. Entrez le nom, le type et le contexte de la partition concernée, puis cliquez sur le bouton Rechercher.
3. Sélectionnez la partition souhaitée dans la liste de recherche, puis cliquez sur l'icône .
4. Sélectionnez l'objet Conteneur vers lequel vous souhaitez déplacer la partition spécifiée, puis cliquez sur **OK**.

REMARQUE : l'option **Créer un alias au lieu de la partition déplacée** renvoie, par le biais d'un pointeur, au nouvel emplacement de la partition. Si vous créez un alias, les opérations qui sont tributaires de l'ancien emplacement se poursuivent sans interruption jusqu'à ce que vous puissiez les mettre à jour pour qu'elles reflètent le nouvel emplacement. Les utilisateurs pourront continuer à se connecter au réseau et retrouver les objets à leur emplacement d'origine dans l'Annuaire.

5 Un message de confirmation s'affiche pour signaler que l'opération de déplacement de la partition a réussi.

Figure 14-4 *Déplacement d'une partition*



15 Gestion des index

Le gestionnaire d'index est un attribut de l'objet Serveur qui vous permet de gérer les index des bases de données. Ces index sont utilisés par eDirectory pour optimiser les performances des requêtes.

NetIQ eDirectory est livré avec un ensemble d'index offrant des fonctionnalités de recherche élémentaire. Ces index par défaut s'appliquent aux attributs ci-dessous.

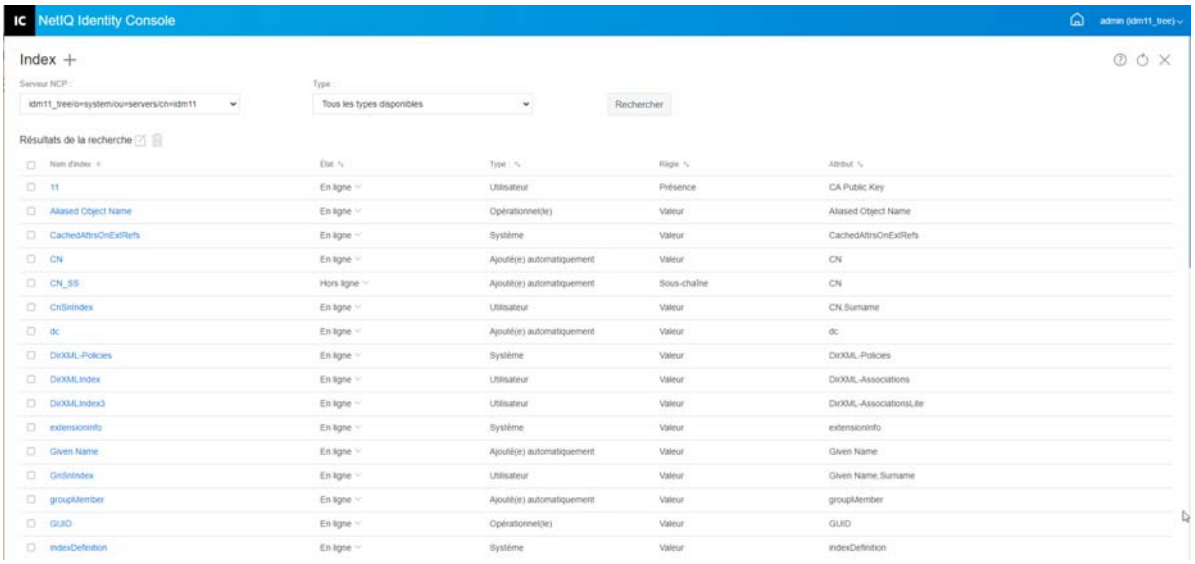
Le module Index permet d'effectuer les tâches suivantes :

Création d'un index

Pour créer un index, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des index**.
2. Cliquez sur l'icône +.
3. Entrez le nom de l'index.
4. Sélectionnez le ou les serveurs souhaités dans la liste des serveurs NCP disponibles.
5. Sélectionnez le ou les attributs requis.
6. Sélectionnez la règle d'index:
   - 6a **Sous-chaîne:** cette règle recherche un sous-ensemble de la chaîne de valeur d'un attribut. Par exemple, une requête visant à rechercher les entrées dont l'attribut « LastName » (nom de famille) comporte « der » renverrait aussi bien « Derington », que « Anderson » et « Lauder ». Un index de sous-chaînes est le type d'index dont la création et la gestion exigent le plus de ressources système.
   - 6b **Présence:** cette règle requiert uniquement la présence d'un attribut au lieu de valeurs spécifiques de l'attribut. Une requête visant à rechercher toutes les entrées comportant un attribut Script de connexion utiliserait un index de présence.
   - 6c **Valeur :** cette règle recherche la valeur complète ou la première partie de la valeur d'un attribut. Par exemple, la concordance de valeur peut être utilisée pour rechercher les entrées dont l'attribut « LastName » (nom de famille) est « Jensen » et celles dont l'attribut « LastName » commence par « Jen ».
7. Cliquez sur le bouton Créer.
8. Un message de confirmation s'affiche pour signaler que l'index a été créé.

Figure 15-1 *Création d'un index*

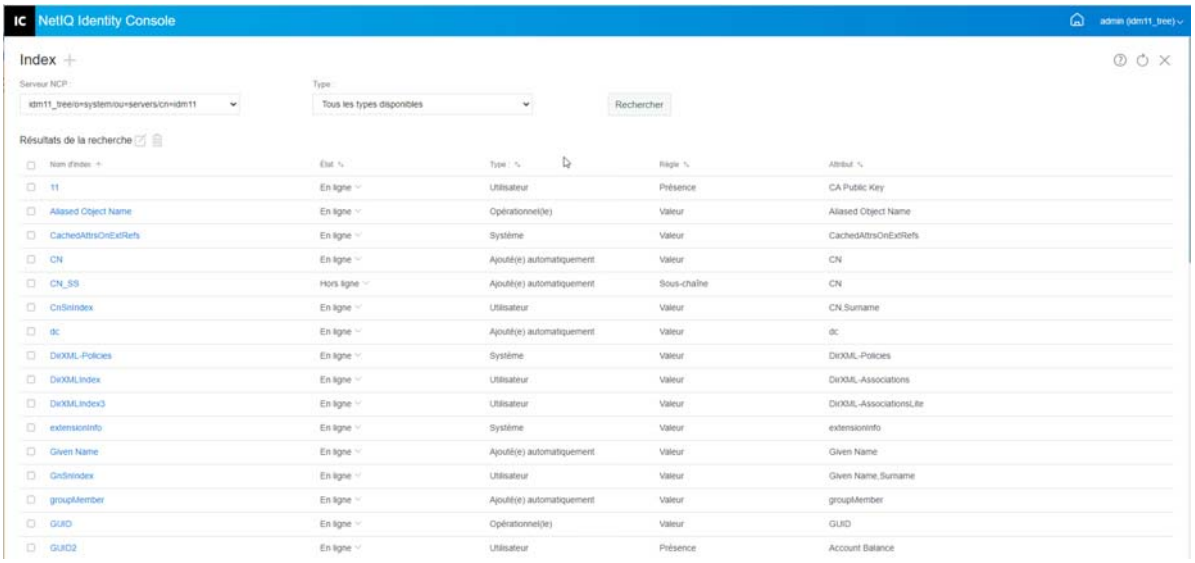


Suppression d'un index

Pour supprimer un index, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des index**.
2. Sélectionnez le serveur NCP et le type d'index souhaités, puis cliquez sur le bouton Rechercher.
3. Sélectionnez l'index souhaité dans la liste de recherche, puis cliquez sur l'icône 🗑.
4. Un message de confirmation s'affiche pour signaler que l'index a été supprimé.

Figure 15-2 *Suppression d'un index*



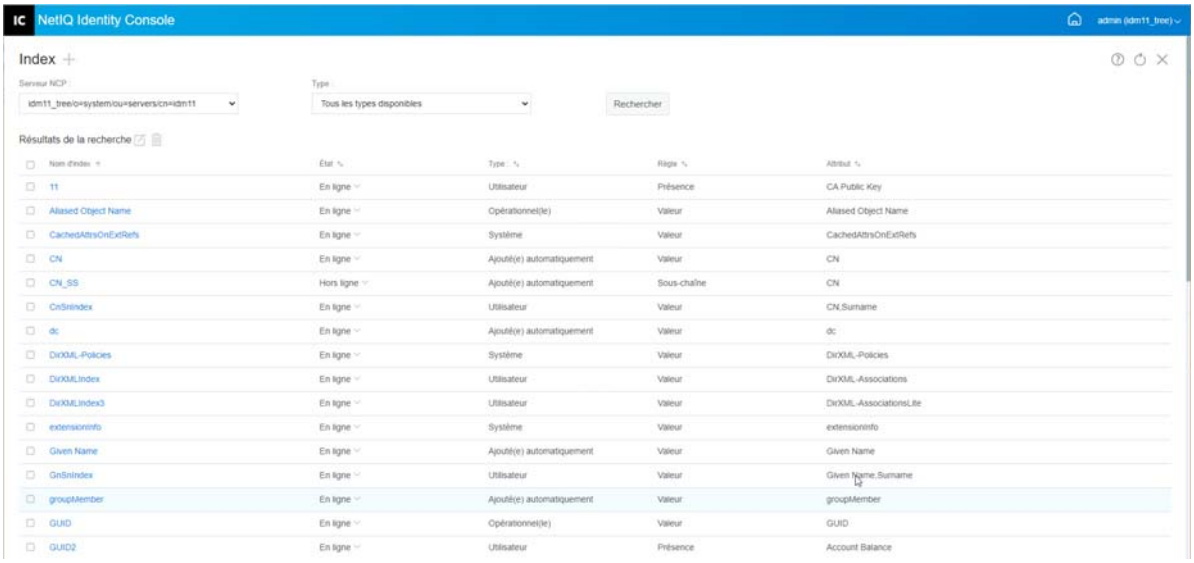
Copie d'un index

Si vous pensez qu'un index utilisé sur un serveur peut être utile sur un autre serveur, vous pouvez copier la définition de cet index d'un serveur vers un autre. En examinant les données de prédicat, vous pourriez également constater le cas de figure inverse : un index qui répondait à un besoin sur plusieurs serveurs n'est plus utile sur l'un de ces serveurs. Dans ce cas, vous pouvez supprimer l'index inutile de ce serveur.

Pour copier un index, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des index**.
2. Sélectionnez le serveur NCP et le type d'index souhaités, puis cliquez sur le bouton Rechercher.
3. Sélectionnez l'index souhaité dans la liste de recherche, puis cliquez sur l'icône .
4. Sélectionnez le ou les serveurs NCP vers lesquels vous souhaitez copier l'index, puis cliquez sur le bouton Enregistrer.
5. Un message de confirmation s'affiche pour signaler que l'index a été copié.

Figure 15-3 *Copie d'un index*



Modification de l'état d'un index

Pendant les périodes d'activité intensive, vous pouvez optimiser les performances en mettant temporairement hors ligne certains index. Par exemple, pour accélérer les opérations de chargement par lot, il est possible que vous souhaitiez suspendre tous les index définis par l'utilisateur. Dans la mesure où l'ajout et la modification d'objets impliquent la mise à jour des index

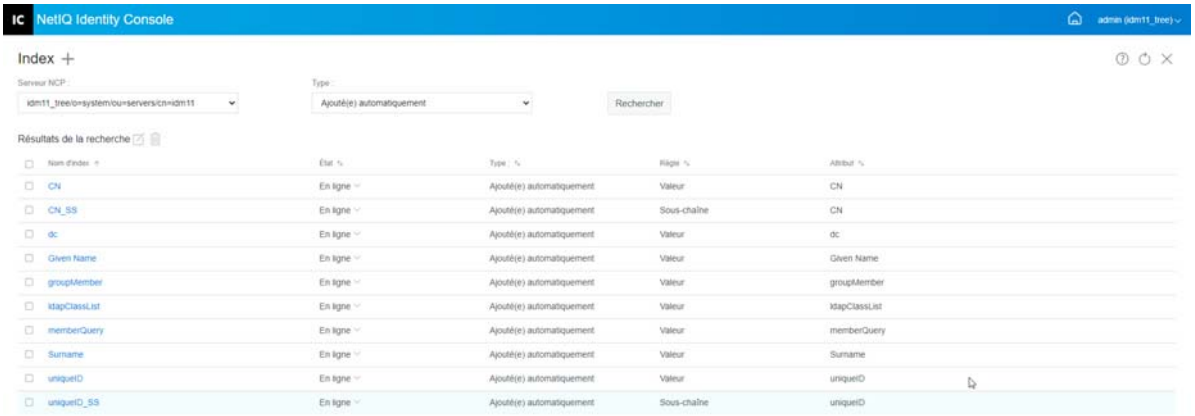
définis, l'activation simultanée de tous les index peut ralentir considérablement les opérations de chargement par lot des données. Une fois les opérations de chargement par lot terminées, vous pouvez remettre en ligne les index.

Pour mettre un index hors ligne, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Gestion des index**.
2. Sélectionnez le serveur NCP et le type d'index souhaités, puis cliquez sur le bouton Rechercher.
3. Cliquez sur la liste déroulante **État** dans la liste des index. Un index peut avoir l'un des deux états suivants :
   - **En ligne:** en cours d'exécution
   - **Hors ligne :** mis en attente. L'index peut être redémarré.

REMARQUE : il est impossible de modifier l'état des types d'index Système et Opérationnel. Ces index ne peuvent pas non plus être supprimés.

Figure 15-4 *Mise hors ligne d'un index*



16 Configuration des objets LDAP

Une installation eDirectory crée un objet Serveur LDAP et un objet Groupe LDAP. La configuration par défaut des services LDAP est consignée dans ces deux objets. Vous pouvez modifier la configuration par défaut à l'aide de la tâche de gestion LDAP dans Identity Console.

L'objet Serveur LDAP représente des données de configuration propres au serveur. L'objet Groupe LDAP contient toutefois des informations de configuration qui peuvent être partagées par plusieurs serveurs LDAP. Cet objet fournit des données de configuration communes et représente un groupe de serveurs LDAP. Les serveurs ont des données communes.

Vous pouvez associer plusieurs objets Serveur LDAP à un objet Groupe LDAP. Tous les serveurs LDAP associés obtiennent alors leur configuration de serveur de l'objet Serveur LDAP mais reçoivent les informations communes ou partagées de l'objet Groupe LDAP.

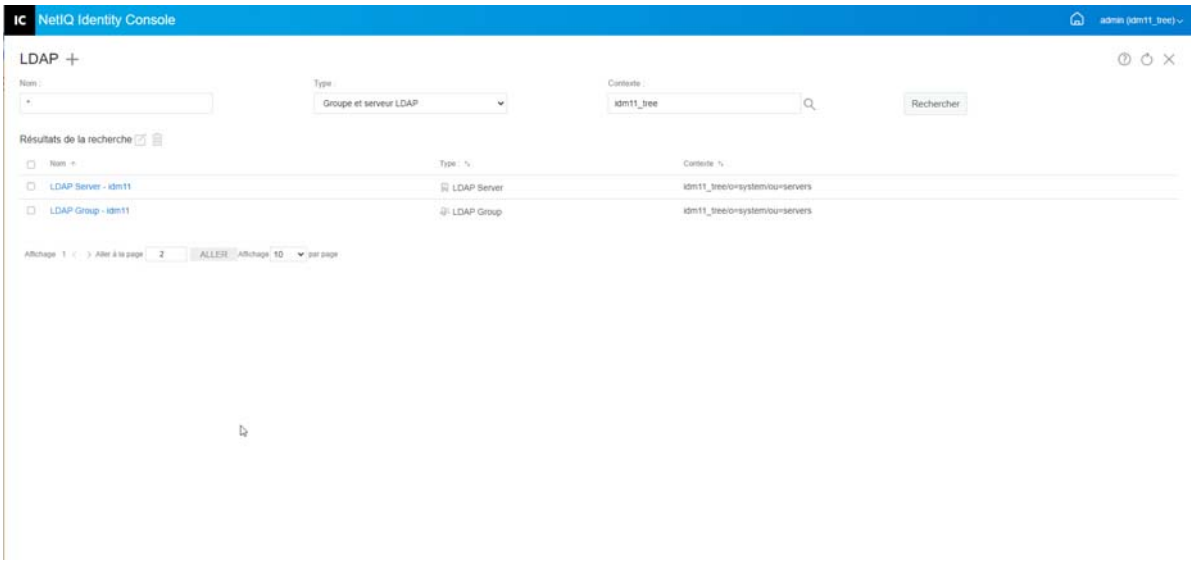
Le module LDAP permet d'effectuer les tâches suivantes :

Création d'un objet LDAP

Pour créer un objet LDAP, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Configuration LDAP**.
2. Cliquez sur l'icône  .
3. Sur la page Créer un objet LDAP, spécifiez le nom, le type et le contexte de l'objet souhaité, ou utilisez l'icône Rechercher un contexte  pour le localiser, puis cliquez sur **Créer**.
4. Un message de confirmation s'affiche pour signaler que l'objet LDAP a été créé.

Figure 16-1 *Création d'un objet LDAP*

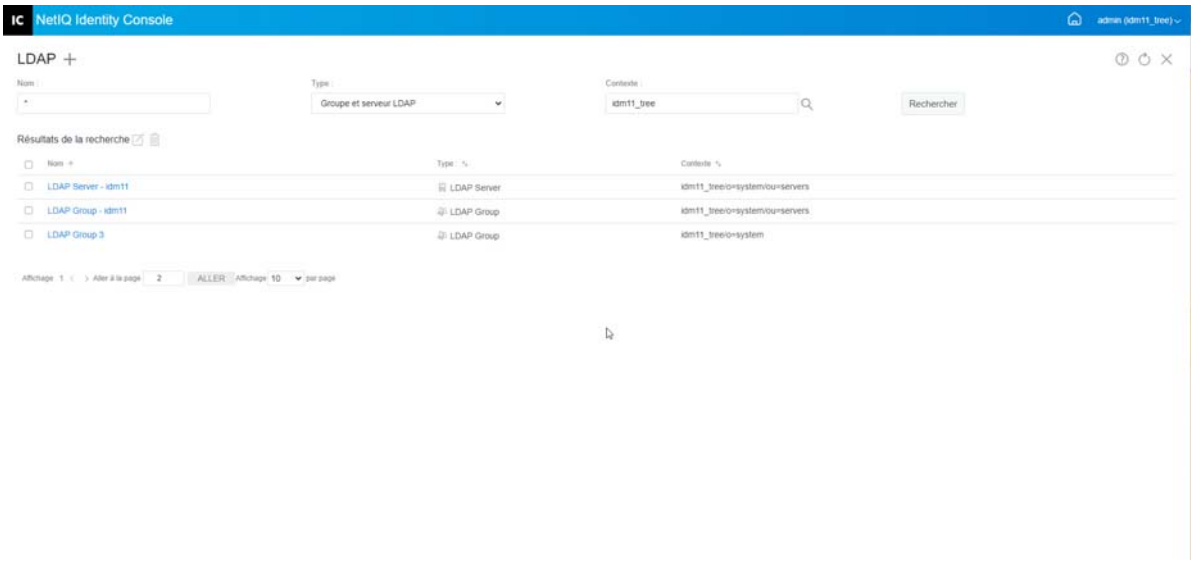


Suppression d'un objet LDAP

Pour supprimer un objet LDAP, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Configuration LDAP**.
2. Spécifiez le nom, le type et le contexte de l'objet LDAP souhaité, puis cliquez sur le bouton Rechercher.
3. Sélectionnez le ou les objets LDAP souhaités dans la liste de recherche, puis cliquez sur l'icône .
4. Un message de confirmation s'affiche pour signaler que le ou les objets LDAP ont été supprimés.

Figure 16-2 *Suppression d'un objet LDAP*

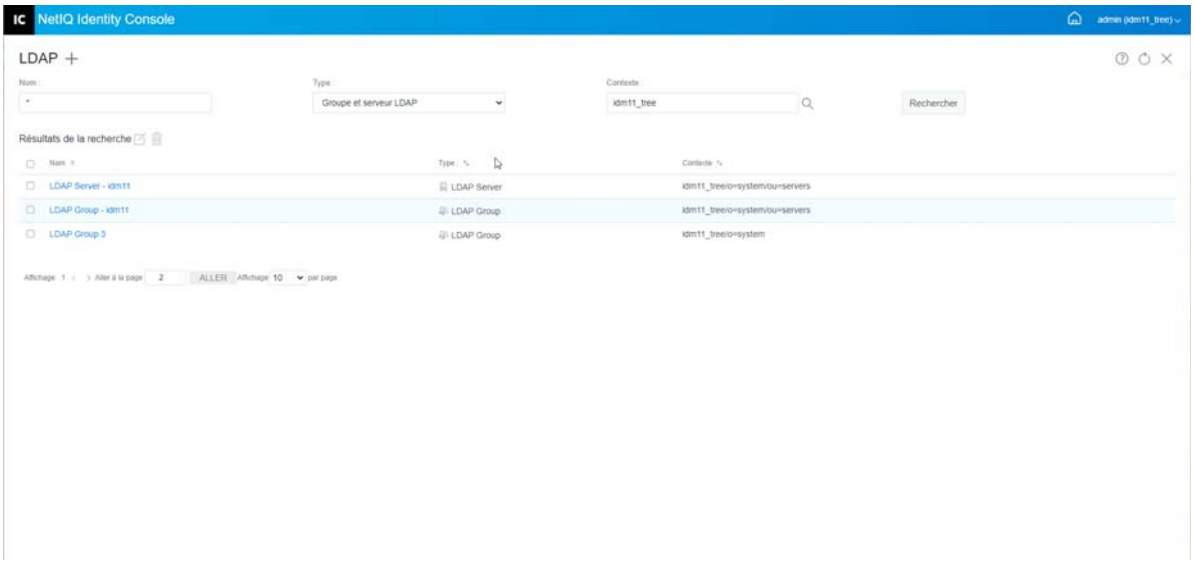


Modification d'un objet LDAP

Pour modifier un objet LDAP, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Configuration LDAP**.
2. Entrez le nom, le type et le contexte de l'objet LDAP souhaité, puis cliquez sur le bouton Rechercher.
3. Sélectionnez l'objet LDAP souhaité dans la liste de recherche, puis cliquez sur l'icône .
4. Modifiez les attributs et les informations de l'objet LDAP, puis cliquez sur le bouton Enregistrer. Pour plus d'informations sur les attributs des objets LDAP, reportez-vous à la section Configuration des objets Serveur LDAP et Groupe LDAP sous Linux dans le *guide d'administration de NetIQ eDirectory*.
5. Un message de confirmation s'affiche pour signaler que l'objet LDAP a été modifié.

Figure 16-3 *Modification d'un objet LDAP*



17 Gestion des certificats

NetIQ Certificate Server est automatiquement installé lors de l'installation d'eDirectory. Il propose des services de cryptographie à clé publique intégrés dans eDirectory, qui permettent de créer, d'émettre et de gérer des certificats utilisateur et de serveur. Ces services permettent de protéger les transmissions de données confidentielles sur des canaux de communication publics tels qu'Internet.

REMARQUE : Si vous souhaitez utiliser le module Gestion des certificats avec Identity Console, vous devez effectuer une mise à niveau de votre serveur eDirectory vers la version 9.2.4 HF2.

Identity Console propose les tâches suivantes liées à la gestion des certificats :

- « Gestion de l'autorité de certification » page 91
- « Gestion des certificats de serveur » page 95
- « Gestion des certificats utilisateur » page 98
- « Gestion des racines approuvées et des conteneurs » page 100
- « Création d'objets Certificat de serveur par défaut » page 103
- « Émission d'un certificat de clé publique » page 104
- « Gestion de l'objet SAS Service » page 108

Gestion de l'autorité de certification

Par défaut, la procédure d'installation de NetIQ Certificate Server crée l'autorité de certification organisationnelle (CA) pour vous. Vous êtes invité à spécifier le nom d'une autorité de certification organisationnelle. Lorsque vous cliquez sur Terminer, l'autorité de certification organisationnelle est créée avec les paramètres par défaut et placée dans le conteneur de sécurité. Si vous souhaitez mieux contrôler la création de l'autorité de certification organisationnelle, vous pouvez la créer manuellement à l'aide du portail Identity Console. En outre, si vous supprimez l'autorité de certification organisationnelle, vous devrez la recréer.

Grâce au module Autorité de certification, vous pouvez effectuer les tâches suivantes :

- « Création d'un objet Autorité de certification organisationnelle » page 92
- « Sauvegarde des certificats de l'autorité de certification organisationnelle » page 92
- « Restauration d'une autorité de certification organisationnelle » page 93
- « Validation des certificats de l'autorité de certification organisationnelle » page 94
- « Remplacement d'un certificat de l'autorité de certification organisationnelle » page 94
- « Révocation d'un certificat de l'autorité de certification organisationnelle » page 94

Création d'un objet Autorité de certification organisationnelle

Pour créer un objet Autorité de certification organisationnelle, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion de l'autorité de certification**.
2. S'il n'existe aucun objet Autorité de certification organisationnelle, la boîte de dialogue de création d'un objet Autorité de certification organisationnelle s'ouvre, de même que l'assistant correspondant qui crée l'objet. Suivez les instructions à l'écran pour créer l'objet.

   REMARQUE : assurez-vous que le chemin d'accès au fichier CRL spécifié ici correspond au chemin d'installation d'eDirectory.

   ---
3. Une fois l'autorité de certification créée, il est recommandé d'effectuer une sauvegarde de la paire de clés publique/privée de l'autorité de certification et de la conserver en lieu sûr. Pour plus d'informations, reportez-vous à la section « Sauvegarde des certificats de l'autorité de certification organisationnelle » page 92.

Sauvegarde des certificats de l'autorité de certification organisationnelle

Il est recommandé de sauvegarder la clé privée et les certificats de votre autorité de certification organisationnelle en cas d'échec irrécupérable du serveur hôte de l'autorité de certification organisationnelle. Dans ce cas, le fichier de sauvegarde vous permettra de restaurer votre autorité de certification organisationnelle sur n'importe quel serveur de l'arborescence.

REMARQUE : la sauvegarde d'une autorité de certification organisationnelle n'est possible que pour les autorités de certification organisationnelle créées avec la version 9.0 (ou version ultérieure) de NetIQ Certificate Server. Dans les versions précédentes de NetIQ Certificate Server, la clé privée de l'autorité de certification organisationnelle était créée de manière à rendre toute exportation impossible.

Le fichier de sauvegarde contient la clé privée de l'autorité de certification, un certificat auto-signé, un certificat de clé publique et plusieurs autres certificats nécessaires à son fonctionnement. Ces informations sont stockées au format PKCS#12 (également appelé PFX).

L'autorité de certification organisationnelle doit être sauvegardée lorsqu'elle fonctionne correctement.

Pour sauvegarder l'autorité de certification organisationnelle, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion de l'autorité de certification**.
2. Cliquez sur l'onglet **Certificats**.
3. Sélectionnez l'option **Self Signed Certificate** (Certificat auto-signé) ou **Public Key Certificate** (Certificat de clé publique). Les deux certificats sont inscrits dans le fichier lors de l'opération de sauvegarde. Il est recommandé de sélectionner le certificat auto-signé pour les certificats RSA et ECDSA séparément.
4. Cliquez sur l'icône  .

5 Choisissez d'exporter la clé privée, spécifiez un mot de passe comportant 6 caractères alphanumériques ou plus à utiliser pour chiffrer le fichier PFX, sélectionnez le format d'exportation PKCS12, puis cliquez sur **OK**.

6 Le fichier de sauvegarde chiffré est inscrit à l'emplacement spécifié. Il peut à présent être stocké à un emplacement sécurisé pour pouvoir être utilisé en cas d'urgence.

Restauration d'une autorité de certification organisationnelle

Si l'objet Autorité de certification organisationnelle a été supprimé ou altéré, ou si le serveur hôte de l'autorité de certification organisationnelle a connu un échec irrérupérable, le bon fonctionnement de l'autorité de certification organisationnelle peut être restauré à l'aide d'un fichier de sauvegarde créé conformément aux indications de la section « Sauvegarde des certificats de l'autorité de certification organisationnelle » page 92.

Pour restaurer l'autorité de certification organisationnelle, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion de l'autorité de certification**.

2 Dans la partie supérieure de l'écran (en regard de **Gestion des autorités de certification**), cliquez sur ↑↓ pour supprimer l'autorité de certification organisationnelle existante.

3 Vous êtes à présent invité à configurer une nouvelle autorité de certification organisationnelle. La boîte de dialogue de création d'un objet Autorité de certification organisationnelle et l'Assistant qui crée cet objet apparaissent.

4 Dans la boîte de dialogue de création, spécifiez le serveur qui doit héberger l'autorité de certification organisationnelle et le nom de l'objet Autorité de certification organisationnelle.

5 Sélectionnez **Importer**.

6 Sélectionnez les certificats RSA et ECDSA. NetIQ Certificate Server exige que les deux certificats portent le même nom d'objet. Novell Certificate Server ne prend cependant pas en charge l'importation de certificats d'autorité de certification auto-signés externes. Toutefois, il vous permet d'importer les certificats d'autorité de certification subordonnée.

7 Dans les écrans suivants, recherchez et sélectionnez le nom du fichier RSA et ECDSA.

8 Entrez le mot de passe qui a servi à chiffrer le fichier lors de la sauvegarde, puis cliquez sur **OK**.

9 La clé privée et les certificats de l'autorité de certification organisationnelle ont à présent été restaurés et l'autorité de certification est totalement opérationnelle. Le fichier peut maintenant être enregistré à nouveau pour une utilisation ultérieure.

Validation des certificats de l'autorité de certification organisationnelle

Si vous suspectez la présence d'un problème lié à un certificat ou que vous pensez qu'il n'est peut-être plus valide, vous pouvez facilement le valider à l'aide d'Identity Console. Tous les certificats de l'arborescence eDirectory peuvent être validés, y compris ceux émis par des autorités de certification externes.

Le processus de validation des certificats comprend plusieurs vérifications des données contenues dans le certificat, ainsi que des données de la chaîne de certificats. Une chaîne de certificats est constituée d'un certificat d'autorité de certification racine et, éventuellement, de certificats d'une ou plusieurs autorités de certification intermédiaires.

Pour valider un certificat :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion de l'autorité de certification**.
2. Cliquez sur l'onglet **Certificats**.
3. Sélectionnez l'option **Self Signed Certificate** (Certificat auto-signé) ou **Public Key Certificate** (Certificat de clé publique).
4. Cliquez sur pour valider le certificat sélectionné de l'autorité de certification.

Remplacement d'un certificat de l'autorité de certification organisationnelle

Si un certificat est endommagé ou non valide pour quelque raison que ce soit ou si vous souhaitez simplement remplacer le certificat existant, suivez la procédure ci-dessous :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion de l'autorité de certification**.
2. Cliquez sur l'onglet **Certificats**.
3. Sélectionnez l'option **Self Signed Certificate** (Certificat auto-signé) ou **Public Key Certificate** (Certificat de clé publique).
4. Cliquez sur pour remplacer le certificat sélectionné de l'autorité de certification.
5. Importez un certificat de l'autorité de certification au format `.pfx` ou `.p12` et spécifiez un mot de passe pour chiffrer la clé privée.
6. Cliquez sur **OK**.

Révocation d'un certificat de l'autorité de certification organisationnelle

Pour révoquer un certificat, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion de l'autorité de certification**.
2. Cliquez sur l'onglet **Certificats**.

3 Sélectionnez l'option **Self Signed Certificate** (Certificat auto-signé) ou **Public Key Certificate** (Certificat de clé publique).

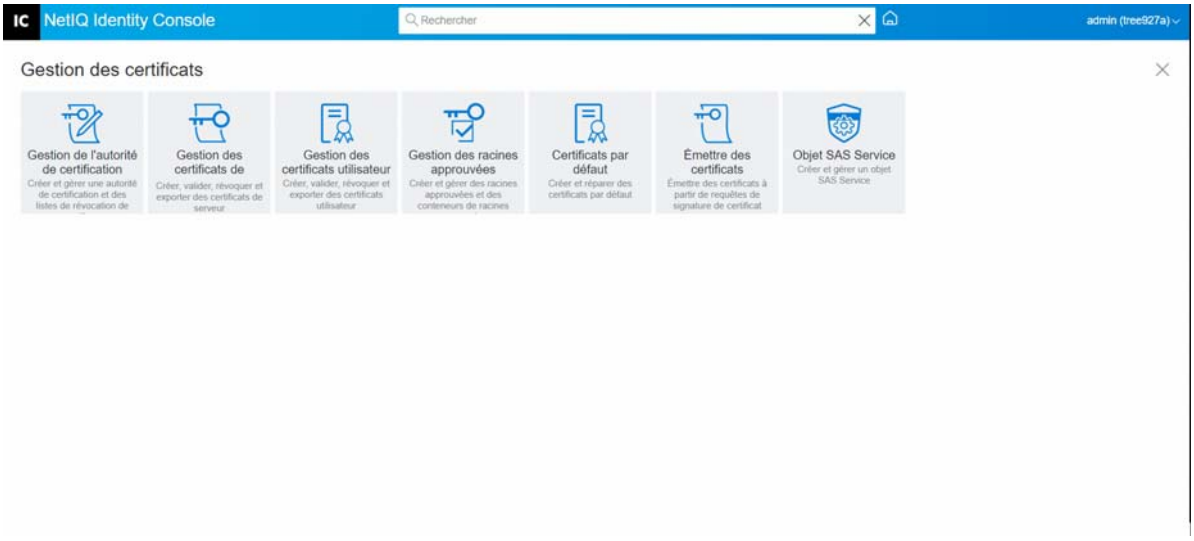
4 Cliquez sur l'icône ⊘.

5 Prenez connaissance des risques associés à la révocation des certificats de serveur.

6 Sélectionnez un motif de révocation valide dans la liste déroulante, sélectionnez la date de fin de validité, puis indiquez tout autre commentaire.

7 Cliquez sur **OK** pour terminer la révocation.

Figure 17-1 *Gestion de l'autorité de certification*



Gestion des certificats de serveur

Grâce au module Gestion des certificats de serveur, l'administrateur peut effectuer les tâches suivantes :

- « Création d'objets Certificat de serveur » page 95
- « Exportation d'un objet Certificat de serveur » page 96
- « Validation d'un objet Certificat de serveur » page 96
- « Remplacement d'un objet Certificat de serveur » page 96
- « Révocation d'un objet Certificat de serveur » page 97
- « Suppression d'un objet Certificat de serveur » page 97

Création d'objets Certificat de serveur

Pour créer un objet Certificat de serveur, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats de serveur**.

2 Cliquez sur l'icône +.

3 Sur la page **Créer un certificat de serveur**, indiquez un **surnom** et un serveur, puis sélectionnez l'une des options suivantes :

- **Standard (paramètres par défaut) :** cette option permet de créer un objet Certificat de serveur par défaut de type RSA ou ECDSA.
- **Personnalisé (l'utilisateur spécifie les paramètres) :** cette option permet de spécifier les paramètres personnalisés de l'objet Certificat de serveur.
- **Import (Allows to Import a PKCS12 File) (Importer (permet d'importer un fichier PKCS12)) :** cette option permet d'importer un fichier PKCS12 au format `.pfx` ou `.p12`.

4 Après avoir spécifié les paramètres souhaités, cliquez sur **Suivant** pour consulter le résumé du certificat.

5 Dans l'écran **Résumé**, cliquez sur **OK** pour créer un objet Certificat de serveur.

Exportation d'un objet Certificat de serveur

Pour exporter un objet Certificat de serveur, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats de serveur**.

2 Sélectionnez le serveur approprié dans la liste déroulante.

3 Sélectionnez le certificat de serveur approprié dans la liste, puis cliquez sur l'icône  .

4 Dans l'écran suivant, cochez la case **Exporter la clé privée**, puis indiquez un mot de passe pour protéger la clé privée. Confirmez le mot de passe et sélectionnez le format d'exportation.

REMARQUE : les certificats de serveur ne peuvent être exportés qu'au format PKCS12.

---

5 Cliquez sur **OK** pour exporter l'objet Certificat de serveur.

Validation d'un objet Certificat de serveur

Pour valider un objet Certificat de serveur, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats de serveur**.

2 Sélectionnez le serveur approprié dans la liste déroulante.

3 Sélectionnez le certificat de serveur approprié dans la liste, puis cliquez sur l'icône  .

4 Un message de confirmation s'affiche pour signaler que l'objet Certificat de serveur a été validé.

Remplacement d'un objet Certificat de serveur

Si un certificat de serveur est endommagé ou non valide pour quelque raison que ce soit ou si vous souhaitez simplement remplacer le certificat par défaut existant, suivez la procédure ci-dessous :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats de serveur**.

2 Sélectionnez le serveur approprié dans la liste déroulante.

3. Sélectionnez le certificat de serveur approprié dans la liste, puis cliquez sur l'icône ↑↓.
4. Prenez connaissance des risques associés au remplacement des certificats de serveur, puis cliquez sur **OK**.
5. Dans l'écran suivant, recherchez et sélectionnez le nouveau certificat de serveur au format `.pfx` ou `.p12`, puis spécifiez un mot de passe.
6. Cliquez sur **OK** pour remplacer le certificat de serveur.

Révocation d'un objet Certificat de serveur

Pour révoquer un objet Certificat de serveur, procédez comme suit :

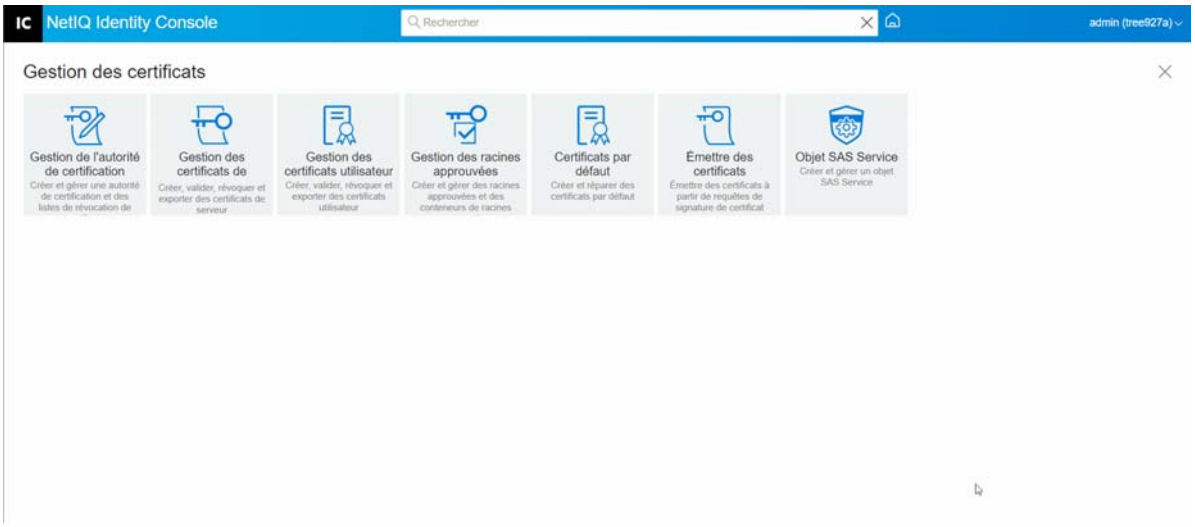
1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats de serveur**.
2. Sélectionnez le serveur approprié dans la liste déroulante.
3. Sélectionnez le certificat de serveur approprié dans la liste, puis cliquez sur l'icône ⊘.
4. Prenez connaissance des risques associés à la révocation des certificats de serveur, puis cliquez sur **OK**.
5. Dans l'écran suivant, sélectionnez un motif de révocation valide dans la liste déroulante, sélectionnez la date de fin de validité, puis indiquez tout autre commentaire.
6. Cliquez sur **OK** pour terminer la révocation.

Suppression d'un objet Certificat de serveur

Pour supprimer un objet Certificat de serveur, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats de serveur**.
2. Sélectionnez le serveur approprié dans la liste déroulante.
3. Sélectionnez le certificat de serveur approprié dans la liste, puis cliquez sur l'icône 🗑.
4. Dans l'écran suivant, cliquez sur **OK**.
5. Un message de confirmation s'affiche pour signaler que l'objet Certificat de serveur a été supprimé.

Figure 17-2 *Gestion des certificats de serveur*



Gestion des certificats utilisateur

Grâce au module Gestion des certificats utilisateur, vous pouvez effectuer la tâche suivante :

- « Création d'un objet Certificat utilisateur » page 98
- « Exportation d'un objet Certificat utilisateur » page 99
- « Validation d'un objet Certificat utilisateur » page 99
- « Révocation d'un objet Certificat utilisateur » page 99
- « Suppression d'un objet Certificat utilisateur » page 99

Création d'un objet Certificat utilisateur

Pour créer un objet Certificat utilisateur, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats utilisateur**.
2. Cliquez sur l'icône +.
3. Sur la page **Créer un certificat utilisateur**, indiquez un **surnom** et un serveur, puis sélectionnez l'une des options suivantes :
   - **Standard (paramètres par défaut) :** cette option permet de créer un objet Certificat utilisateur par défaut de type RSA ou ECDSA.
   - **Personnalisé (l'utilisateur spécifie les paramètres) :** cette option permet de spécifier les paramètres personnalisés de l'objet Certificat utilisateur.
   - **Importer :** cette option permet d'importer un fichier de certificat au format CERT ou PKCS12.
4. Après avoir spécifié les paramètres souhaités, cliquez sur **Suivant** pour consulter le résumé du certificat.
5. Dans l'écran **Résumé**, cliquez sur **OK** pour créer un objet Certificat utilisateur.

Exportation d'un objet Certificat utilisateur

Pour exporter un objet Certificat utilisateur, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats utilisateur**.
2. Sélectionnez le serveur approprié dans la liste déroulante.
3. Sélectionnez le certificat utilisateur approprié dans la liste, puis cliquez sur l'icône .
4. Dans l'écran suivant, cochez la case **Exporter la clé privée**, puis indiquez un mot de passe pour protéger la clé privée. Confirmez le mot de passe et sélectionnez le format d'exportation.

   REMARQUE : les certificats utilisateur ne peuvent être exportés qu'au format PKCS12.
5. Cliquez sur **OK** pour exporter l'objet Certificat utilisateur.

Validation d'un objet Certificat utilisateur

Pour valider un objet Certificat utilisateur, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats utilisateur**.
2. Sélectionnez le serveur approprié dans la liste déroulante.
3. Sélectionnez le certificat utilisateur approprié dans la liste, puis cliquez sur l'icône .
4. Un message de confirmation s'affiche pour signaler que l'objet Certificat utilisateur a été validé.

Révocation d'un objet Certificat utilisateur

Pour révoquer un objet Certificat utilisateur, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats utilisateur**.
2. Sélectionnez le serveur approprié dans la liste déroulante.
3. Sélectionnez le certificat utilisateur approprié dans la liste, puis cliquez sur l'icône .
4. Prenez connaissance des risques associés à la révocation des certificats utilisateur.
5. Sélectionnez un motif de révocation valide dans la liste déroulante, sélectionnez la date de fin de validité, puis indiquez tout autre commentaire.
6. Cliquez sur **OK** pour terminer la révocation.

Suppression d'un objet Certificat utilisateur

Pour supprimer un objet Certificat utilisateur, procédez comme suit :

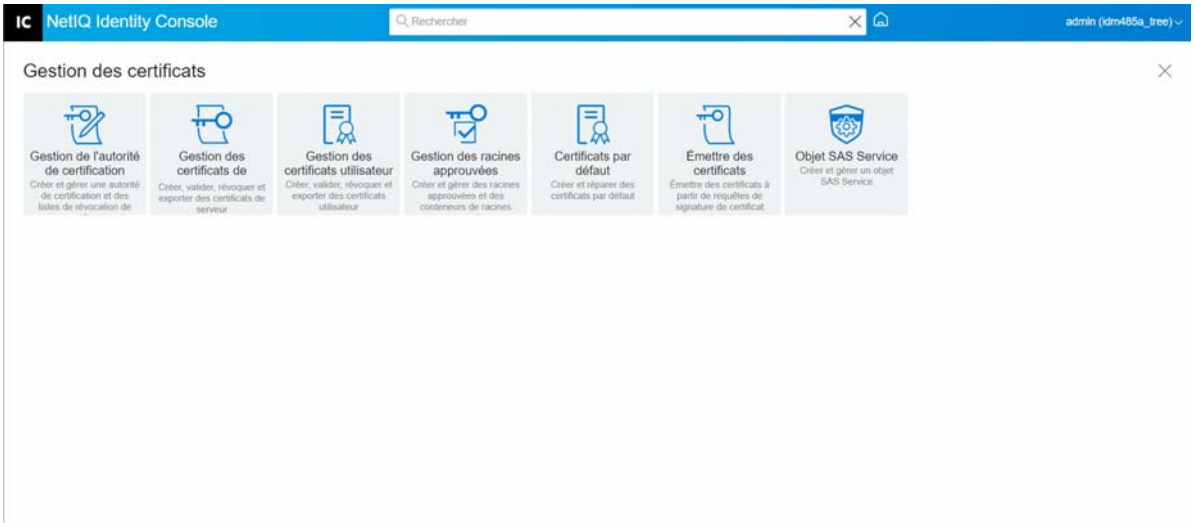
1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des certificats utilisateur**.
2. Sélectionnez le serveur approprié dans la liste déroulante.

3 Sélectionnez le certificat utilisateur approprié dans la liste, puis cliquez sur l'icône .

4 Dans l'écran suivant, cliquez sur **OK**.

5 Un message de confirmation s'affiche pour signaler que l'objet Certificat utilisateur a été supprimé.

Figure 17-3 *Gestion des certificats utilisateur*



Gestion des racines approuvées et des conteneurs

Les racines approuvées constituent la base de l'approbation dans le cadre de la cryptographie à clé publique. Elles sont utilisées pour valider les certificats signés par d'autres autorités de certification, et permettent d'établir des connexions SSL sécurisées, de sécuriser le courrier électronique et de procéder à l'authentification par certificat.

Grâce au module Gestion des racines approuvées, vous pouvez effectuer les tâches suivantes :

- « Création d'un conteneur de racines approuvées » page 100
- « Création d'un objet Certificat de racine approuvée » page 101
- « Exportation d'un objet Certificat de racine approuvée » page 101
- « Validation d'un objet Certificat de racine approuvée » page 102
- « Suppression d'un objet Certificat de racine approuvée » page 102
- « Suppression d'un conteneur de racines approuvées » page 102

Création d'un conteneur de racines approuvées

Pour créer un conteneur de racines approuvées, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des racines approuvées**. La case à cocher **Conteneur de racines approuvées** est activée par défaut.

2 Cliquez sur l'icône pour créer un conteneur de racines approuvées.

3 Spécifiez un nom pour le conteneur de racines approuvées.

4 Utilisez le sélecteur d'objet pour rechercher le conteneur approprié.

5 Cliquez sur le bouton **OK**.

6 Un message de confirmation s'affiche pour signaler que le conteneur de racines approuvées a été créé.

Création d'un objet Certificat de racine approuvée

Pour créer un objet Racine approuvée, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des racines approuvées**. La case à cocher **Conteneur de racines approuvées** est activée par défaut. Cochez la case **Racine approuvée**.

2 Cliquez sur l'icône + pour créer un objet Racine approuvée.

3 Spécifiez un nom pour l'objet Racine approuvée.

4 Sélectionnez le conteneur de racines approuvées approprié dans la liste déroulante.

5 Recherchez et sélectionnez le fichier de certificat approprié au format `.der` ou `.b64`.

REMARQUE : Un objet Racine approuvée peut stocker tout type de certificat (certificats d'autorités de certification, certificats d'autorités de certification intermédiaires ou certificats utilisateur).

---

6 Cliquez sur le bouton **OK**.

7 Un message de confirmation s'affiche pour signaler que l'objet Racine approuvée a été créé.

Exportation d'un objet Certificat de racine approuvée

Pour exporter un objet Certificat de racine approuvée, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des racines approuvées**. La case à cocher **Conteneur de racines approuvées** est activée par défaut. Cochez la case **Racine approuvée**.

2 Sélectionnez le certificat racine approuvé approprié dans la liste, puis cliquez sur l'icône .

3 Dans l'écran suivant, cochez la case **Exporter la clé privée**, puis indiquez un mot de passe pour protéger la clé privée. Confirmez le mot de passe et sélectionnez le format d'exportation.

REMARQUE : les certificats de racine approuvée ne peuvent être exportés qu'au format DER ou BASE64.

---

4 Cliquez sur **OK** pour exporter l'objet Certificat de racine approuvée.

Validation d'un objet Certificat de racine approuvée

Pour valider un objet Certificat de racine approuvée, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des racines approuvées**. La case à cocher **Conteneur de racines approuvées** est activée par défaut. Cochez la case **Racine approuvée**.
2. Sélectionnez le certificat racine approuvé approprié dans la liste, puis cliquez sur l'icône .
3. Un message de confirmation s'affiche pour signaler que l'objet Certificat de racine approuvée a été validé.

Suppression d'un objet Certificat de racine approuvée

Pour supprimer un objet Certificat de racine approuvée, procédez comme suit :

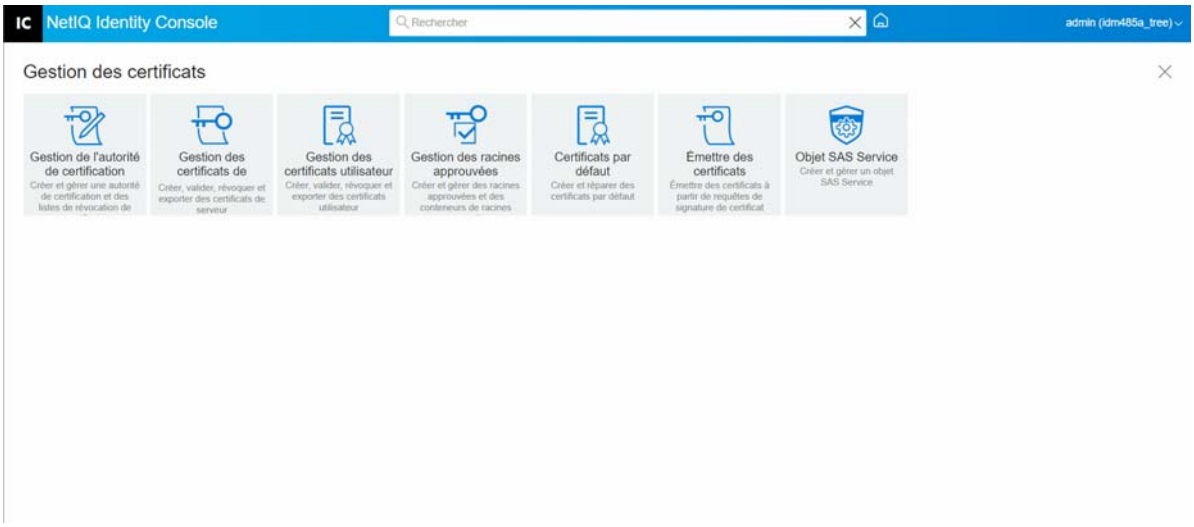
1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des racines approuvées**. La case à cocher **Conteneur de racines approuvées** est activée par défaut. Cochez la case **Racine approuvée**.
2. Sélectionnez le certificat racine approuvé approprié dans la liste, puis cliquez sur l'icône .
3. Dans l'écran d'avertissement, cliquez sur **OK**.
4. Un message de confirmation s'affiche pour signaler que l'objet Certificat de racine approuvée a été supprimé.

Suppression d'un conteneur de racines approuvées

Pour supprimer un conteneur de racines approuvées, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Gestion des racines approuvées**. La case à cocher **Conteneur de racines approuvées** est activée par défaut.
2. Sélectionnez le conteneur de racines approuvées approprié dans la liste, puis cliquez sur l'icône .
3. Dans l'écran d'avertissement, cliquez sur **OK**.
4. Un message de confirmation s'affiche pour signaler que le conteneur de racines approuvées a été supprimé.

Figure 17-4 *Gestion des conteneurs de racines approuvées*



Création d'objets Certificat de serveur par défaut

Le programme d'installation de Certificate Server crée des objets Certificat de serveur par défaut.

- SSL CertificateDNS - *nom_serveur*
- Un certificat pour chaque adresse IP configurée sur le serveur (IPAG *xxx.xxx.xxx.xxx* - *nom_serveur*)
- Un certificat pour chaque nom DNS configuré sur le serveur (DNSAG*www.exemple.com* - *nom_serveur*)

REMARQUE : eDirectory ne crée pas automatiquement le certificat SSL CertificateIP. Le nom DNS du certificat SSL contient toutes les adresses IP répertoriées dans le champ Subject Alternative Name (Autre nom de l'objet). Lorsque vous tentez de créer ou de réparer des certificats par défaut à l'aide d'Identity Console, le certificat SSL CertificateIP n'est pas créé ni réparé par défaut. Toutefois, l'interface de plug-in propose une case à cocher que vous pouvez sélectionner afin de remplacer le comportement par défaut et forcer la création/réparation du certificat SSL CertificateIP.

À partir de la version 9.0 d'eDirectory, les certificats ECDSA sont créés automatiquement si l'autorité de certification organisationnelle dispose d'un certificat ECDSA.

Si ces certificats sont altérés ou non valides pour une raison quelconque, ou si vous souhaitez simplement remplacer les certificats par défaut existants, vous pouvez utiliser l'assistant de création de certificats de serveur par défaut, comme indiqué dans la procédure suivante :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Certificats par défaut**.
2. Sélectionnez le ou les serveurs pour lesquels vous souhaitez créer des certificats par défaut, puis cliquez sur **Suivant**.
3. Sélectionnez Oui si vous souhaitez écraser les certificats de serveur par défaut existants ou choisissez Non pour les écraser uniquement s'ils ne sont pas valides.

4 (Single Server only) (Un seul serveur uniquement) Si vous souhaitez utiliser l'adresse DNS existante, sélectionnez cette option. Si vous souhaitez utiliser une autre adresse DNS, sélectionnez cette option et spécifiez la nouvelle adresse DNS.

5 (Single Server only) (Un seul serveur uniquement) Si vous souhaitez utiliser l'adresse IP par défaut existante, sélectionnez cette option. Si vous souhaitez utiliser une autre adresse IP, sélectionnez cette option et spécifiez la nouvelle adresse IP.

6 Cliquez sur **Suivant**.

7 Passez en revue la page de résumé, puis cliquez sur **Finish** (Terminer).

Si vous souhaitez mieux contrôler la création de l'objet Certificat de serveur, vous pouvez le créer manuellement. Pour plus d'informations, reportez-vous à la section « Création d'objets Certificat de serveur » page 95.

Figure 17-5 *Création d'objets Certificat de serveur par défaut*

Émission d'un certificat de clé publique

Votre autorité de certification organisationnelle fonctionne de la même manière qu'une autorité de certification externe. Autrement dit, elle est capable d'émettre des certificats à partir de requêtes de signature de certificat (CSR). Vous pouvez émettre des certificats à l'aide de votre autorité de certification organisationnelle lorsqu'un utilisateur envoie une requête vous invitant à signer le certificat. L'utilisateur qui demande le certificat peut se servir du certificat émis et l'importer directement dans l'application qui prend en charge la cryptographie.

Cette tâche vous permet de générer des certificats destinés aux applications codées qui ne reconnaissent pas les objets Certificat de serveur.

Pour émettre un certificat, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Émettre des certificats**.

2 Recherchez et sélectionnez un fichier CSR.

3 Sélectionnez le type de clé approprié et l'utilisation de la clé correspondante sous Spécifications d'utilisation de la clé. Ces options vous permettent de sélectionner un type de clé. Des valeurs d'utilisation de clé sont prédéfinies pour chacun des types de clé:

- 3a **Non spécifié :** il s'agit de l'option par défaut ; elle n'active pas d'utilisation de la clé dans le certificat.
- 3b **Autorité de certification :** cette option active les utilisations de clé Signature de certificat et Signature CRL.
- 3c **Chiffrement :** Cette option active l'utilisation de la clé Key Encipherment (Codage de la clé).
- 3d **Signature :** Cette option active l'utilisation de la clé Signature digitale.
- 3e **SSL ou TSL :** Cette option permet de configurer la clé de telle sorte qu'elle puisse être utilisée dans les transactions SSL (Secure Socket Layer) ou TLS.
- 3f **Personnalisé :** cette option permet de sélectionner manuellement une ou toutes les options d'utilisation de la clé.
- 3g **Définir l'extension d'utilisation de la clé sur Critique:** Vous pouvez définir l'extension d'utilisation de la clé sur Critique pour tous les types de clé, à l'exception de « Non spécifié ». Toute extension critique doit être comprise par le logiciel destinataire avant que le certificat puisse être utilisé dans un but quelconque. Dès lors, il peut être risqué de définir une extension comme critique, car toutes les applications ne pourront pas utiliser le certificat. Le risque est toutefois minime pour des extensions bien connues, telles que l'utilisation de la clé. En général, si l'utilisation de la clé est indiquée, l'extension est désignée comme critique.

4 Vous pouvez décider de coder une extension d'**utilisation de clés étendues** dans le certificat. Pour activer cette fonction, sélectionnez **Activer l'utilisation de clés étendues** :

- 4a **Serveur :** cette option active l'utilisation de clés étendues Authentification du serveur.
- 4b **Utilisateur :** cette option active les utilisations de clés étendues Authentification de l'utilisateur et Protection des messages électroniques.
- 4c **Personnalisé :** cette option permet de sélectionner une ou toutes les utilisations de clés étendues.
- 4d **N'importe laquelle :** Permet d'utiliser la clé pour n'importe quelle utilisation de clé étendue.
- 4e **Définir l'extension de l'utilisation de clés étendues sur Critique :** Toute extension critique doit être comprise par le logiciel destinataire avant que le certificat puisse être utilisé dans un but quelconque. Dès lors, il peut être risqué de définir une extension comme critique, car toutes les applications ne pourront pas utiliser le certificat. De nombreuses applications ne comprenant pas l'extension d'utilisation de clé étendue, si vous définissez cette extension comme critique, le certificat risque de ne pas être accepté par une application spécifique. Ne paramétrez donc cette extension sur Critique que si cela est vraiment nécessaire.

5 Sélectionnez les **contraintes de base** appropriées :

5a Type de certificat :

5a1 Non spécifié : Sélectionnez cette option si vous ne souhaitez pas ajouter d'extension de contraintes de base au certificat.

5a2 Autorité de certification : Sélectionnez cette option pour ajouter une extension de contraintes de base Autorité de certification au certificat. Si le certificat est destiné à une autorité de certification, vous devez sélectionnez cette option.

5a3 Entité Fin : Sélectionnez cette option pour ajouter une extension de contraintes de base au certificat spécifiant qu'il s'agit d'un certificat Entité Fin (et non d'une autorité de certification). Remarque : s'il s'agit d'un certificat de type Entité Fin, la longueur du chemin doit être définie sur Non spécifié.

5b Longueur du chemin :

5b1 Non spécifié : Sélectionnez cette option si vous ne souhaitez pas spécifier le nombre de niveaux d'autorités de certification subordonnées qui peuvent être créés sous cette autorité de certification.

REMARQUE : s'il s'agit d'un certificat de type Entité Fin, la longueur du chemin doit être définie sur Non spécifié.

5b2 Spécifié : Sélectionnez cette option si vous souhaitez spécifier le nombre de niveaux d'autorités de certification subordonnées qui peuvent être créés sous cette autorité de certification. Cliquez sur les flèches haut et bas pour indiquer la longueur du chemin.

REMARQUE : si le certificat en cours de création est une autorité de certification subordonnée, la longueur du chemin doit être cohérente avec celle de l'autorité de certification supérieure. Par exemple, si la longueur du chemin de l'autorité de certification supérieure est de 3, celle de la subordonnée doit être inférieure ou égale à 2. Si la longueur du chemin de l'autorité de certification supérieure est non spécifiée, celle de la subordonnée peut également être non spécifiée ou présenter n'importe quelle valeur spécifique.

5c Définir l'extension des restrictions de base sur critique: En général, l'extension des contraintes de base doit être définie sur critique pour les certificats Autorité de certification. Toute extension critique doit être comprise par le logiciel destinataire avant que le certificat puisse être utilisé dans un but quelconque. Dès lors, il peut être risqué de définir une extension comme critique, car toutes les applications ne pourront pas utiliser le certificat. Le risque est toutefois minime pour des extensions bien connues, telles que des contraintes de base.

6 Spécifiez les paramètres de certificat suivants :

6a Nom du sujet: affiche le nom complet avec type de votre arborescence eDirectory.

6b Nom du sujet: affiche le nom complet avec type de votre arborescence eDirectory.

6c Période de validité: Utilisez la liste déroulante pour spécifier une période de validité pour le certificat. Elle peut varier de 6 mois au maximum, soit l'année 2036 (limite temporelle basée sur une valeur temporelle de 32 bits). Si vous sélectionnez l'option Indiquer les

dates, vous pouvez modifier les champs Date d'entrée en vigueur et Date d'expiration pour créer une période de validité personnalisée. La date maximale choisie doit être comprise dans la période de validité de l'autorité de certification.

6c1 **Date d'entrée en vigueur :** Permet d'afficher ou de modifier la date et l'heure de début de validité du certificat.

6c2 **Date d'expiration :** Permet d'afficher ou de modifier la date et l'heure de fin de validité du certificat.

6d **Extensions personnalisées:** Permet au serveur de certificats de prendre en charge toutes les extensions standard ou personnalisées que vous souhaitez inclure lors de la création d'un certificat. Les extensions doivent être préalablement créées et stockées dans un fichier (une extension par fichier). Elles doivent toutes être codées en ASN.1 comme défini dans l'IETF RFC 2459/3280 section 4.2.

Si vous souhaitez inclure une ou plusieurs extensions personnalisées dans le certificat que vous créez, cliquez sur Nouveau, puis recherchez un fichier contenant l'extension personnalisée et ajoutez-la au certificat. Pour ajouter d'autres extensions, répétez la procédure.

Pour supprimer un fichier d'extensions personnalisées, sélectionnez-le, puis cliquez sur l'icône  .

7 Sélectionnez le format de certificat approprié parmi les options suivantes :

7a **Fichier au format DER binaire :** cette option permet d'enregistrer ou d'exporter un certificat vers le fichier indiqué dans le champ Nom du fichier. Par défaut, le fichier de certificat est exporté avec l'extension .DER à la racine du disque C: d'un poste de travail Identity Console Windows et dans le répertoire privé d'un poste de travail Identity Console Linux.

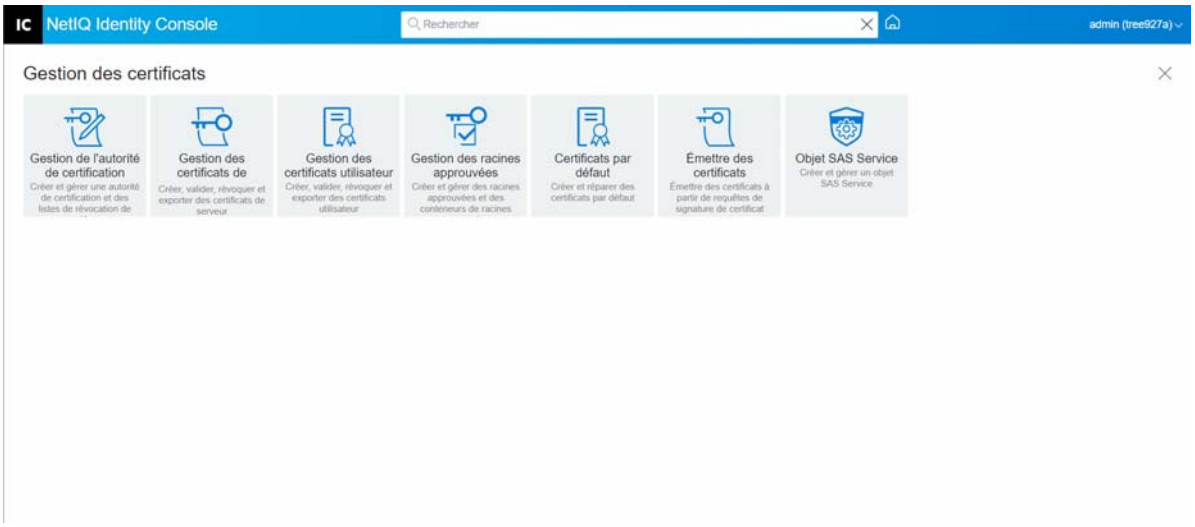
7b **Fichier au format Base64 :** cette option permet d'enregistrer une requête de signature de certificat (CSR) ou d'exporter un certificat vers le fichier indiqué dans le champ Nom du fichier. Par défaut, les fichiers de certificat et de CSR sont exportés avec l'extension .B64 à la racine du disque C: d'un poste de travail Identity Console Windows et dans le répertoire privé d'un poste de travail Identity Console Linux.

7c **Fichier au format CER :** cette option permet d'enregistrer une requête de signature de certificat (CSR) ou d'exporter un certificat vers le fichier indiqué dans le champ Nom du fichier. Par défaut, les fichiers de certificat et de CSR sont exportés avec l'extension .CER à la racine du disque C: d'un poste de travail Identity Console Windows et dans le répertoire privé d'un poste de travail Identity Console Linux.

8 Consultez le résumé du certificat dans l'écran suivant, puis cliquez sur **OK**.

9 Un message de confirmation s'affiche pour signaler que le certificat a été émis.

Figure 17-6 *Émission d'un certificat de clé publique*



Gestion de l'objet SAS Service

L'objet SAS Service facilite la communication entre un serveur et ses certificats. Si vous supprimez un serveur d'une arborescence eDirectory, vous devez également supprimer l'objet SAS Service qui lui est associé. Si vous souhaitez restaurer le serveur dans l'arborescence, vous devez créer l'objet SAS Service qui l'accompagne. À défaut, vous ne pouvez pas créer de nouveaux certificats de serveur.

L'objet SAS Service est automatiquement créé dans le cadre de la vérification de l'état de santé du serveur. Il n'est pas nécessaire de le créer manuellement.

Vous ne pouvez créer un nouvel objet SAS Service que si le conteneur de l'objet Serveur ne contient pas encore d'objet Service avec un nom approprié. Par exemple, pour un serveur nommé WAKE, l'objet SAS Service est appelé SAS Service - WAKE. L'utilitaire ajoute les pointeurs DS de l'objet Serveur vers l'objet SAS, et de l'objet SAS vers l'objet Serveur. Il configure également les entrées ACL correctes sur l'objet SAS Service.

Si un objet SAS Service avec un nom approprié existe déjà, vous ne pouvez pas en créer un nouveau. Les pointeurs DS de l'ancien objet SAS Service peuvent être erronés ou manquants ou les ACL peuvent se révéler incorrectes. Dans ce cas, vous pouvez supprimer l'objet SAS Service endommagé et utiliser Identity Console pour en créer un nouveau.

Création ou suppression d'un objet SAS Service

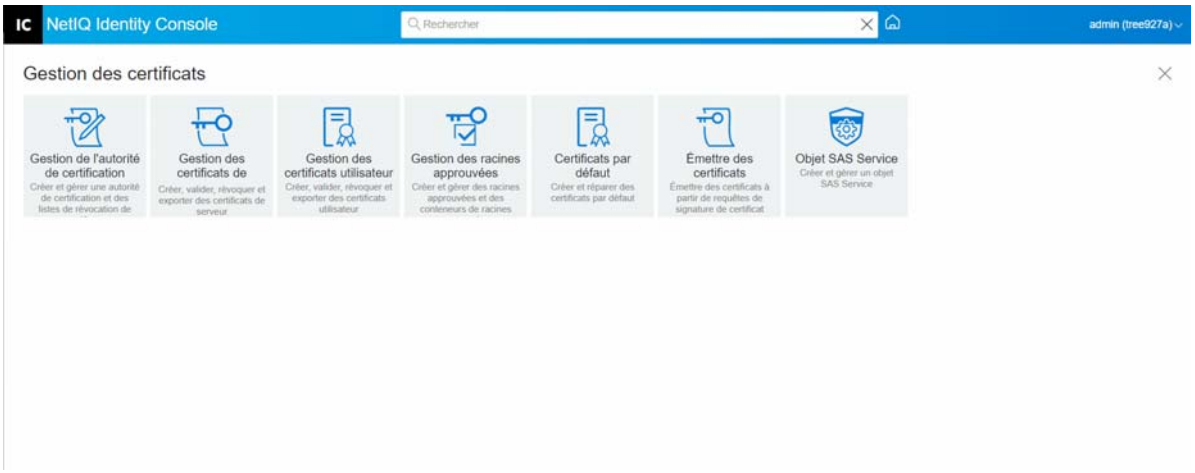
Pour créer ou supprimer un objet SAS Service, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des certificats** > **Objet SAS Service**.
2. Si aucun objet SAS Service n'a été créé pour un serveur existant, cliquez sur l'icône + pour en créer un.
3. Un message de confirmation s'affiche pour signaler que l'objet SAS Service a été créé.

4 Pour supprimer un objet SAS Service, cliquez sur l'icône .

5 Cliquez sur **OK** dans l'écran de confirmation pour supprimer l'objet SAS Service.

Figure 17-7 *Gestion d'un objet SAS Service*



18 Gestion du module Authentification

Grâce au module Authentification, vous pouvez effectuer les tâches suivantes :

Gestion des méthodes et des séquences de connexion et de post-connexion

NMAS prend en charge un certain nombre de méthodes de connexion et de post-connexion développées par NetIQ et d'autres fournisseurs de solutions d'authentification. Certaines méthodes requièrent du matériel et des logiciels supplémentaires. Assurez-vous que vous disposez du matériel et de tous les logiciels nécessaires pour les méthodes que vous comptez utiliser.

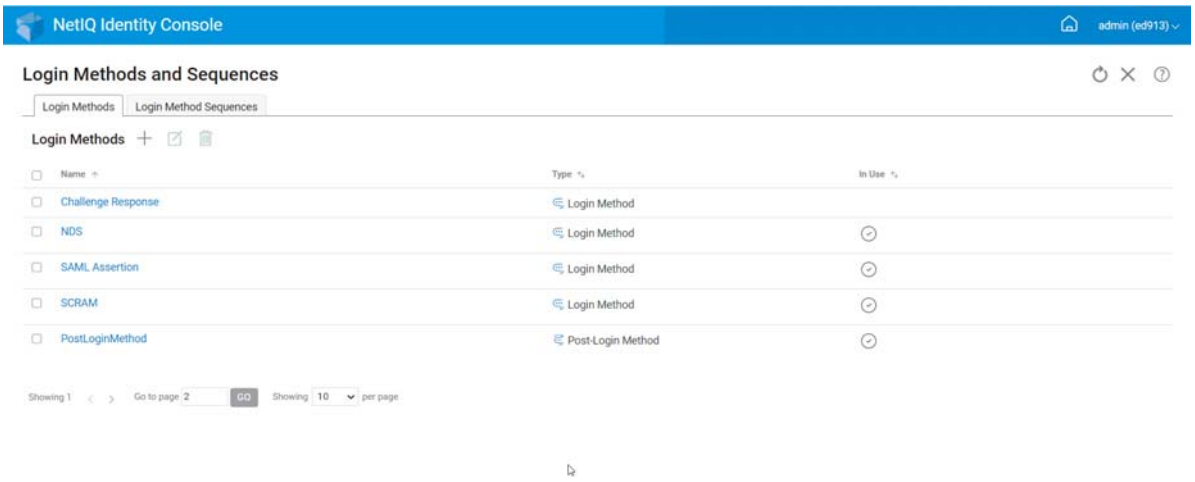
Cette section explique comment installer et configurer des méthodes et des séquences de connexion et de post-connexion pour NMAS.

Installation d'une méthode de connexion ou de post-connexion

Pour installer une méthode de connexion, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Séquences et méthodes de connexion**.
2. Cliquez sur l'icône + pour installer une nouvelle méthode de connexion.
3. Recherchez et sélectionnez le fichier (.zip) de la méthode de connexion à installer, puis cliquez sur **Suivant**.
4. Suivez l'assistant d'installation pour effectuer le processus d'installation de la méthode de connexion.

Figure 18-1 *Installation d'une nouvelle méthode de connexion*

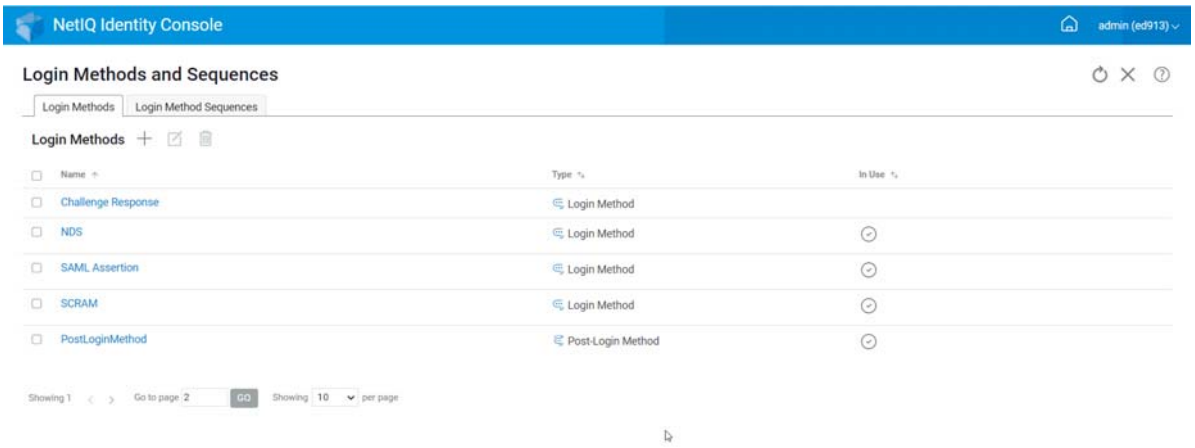


Mise à jour d'une méthode de connexion ou de post-connexion existante

Pour mettre à jour une méthode de connexion existante, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Séquences et méthodes de connexion**.
2. Sélectionnez la méthode de connexion à mettre à jour dans la liste, puis cliquez sur l'icône .
3. Recherchez et sélectionnez le fichier (.zip) de la méthode de connexion à mettre à jour, puis cliquez sur **Suivant**.
4. Suivez l'assistant de mise à jour pour effectuer la mise à jour de la méthode de connexion.

Figure 18-2 *Mise à jour d'une méthode de connexion existante*

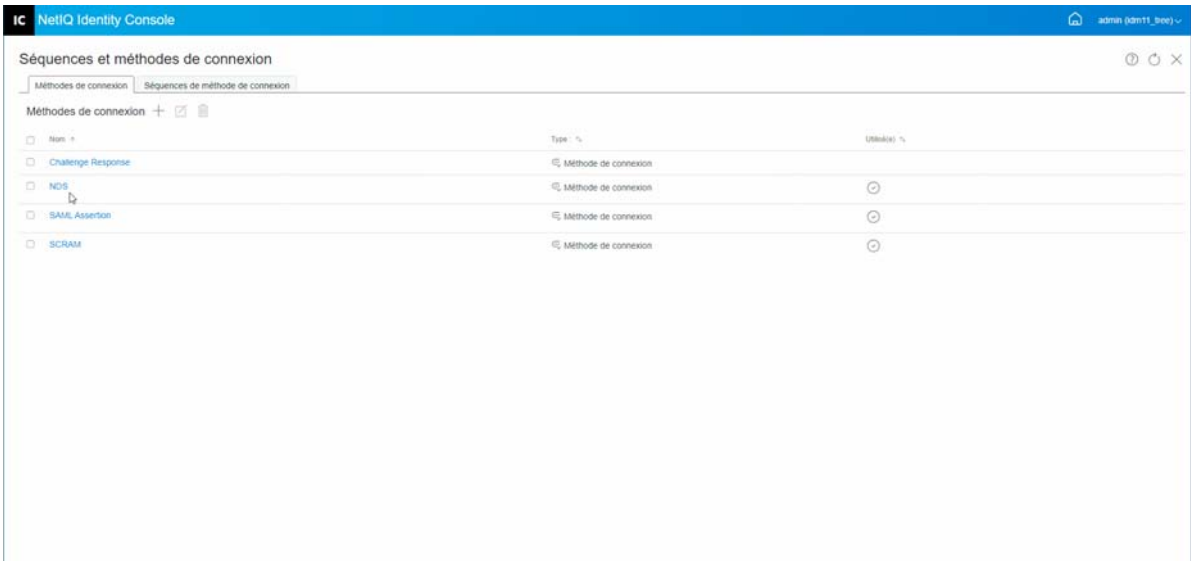


Désinstallation de méthodes de connexion ou de post-connexion

Pour désinstaller une ou plusieurs méthodes de connexion ou de post-connexion, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Séquences et méthodes de connexion**.
2. Sélectionnez la ou les méthodes de connexion à désinstaller dans la liste, puis cliquez sur l'icône 🗑.
3. Dans l'écran suivant, cliquez sur **OK**.
4. Un message de confirmation s'affiche pour signaler que la ou les méthodes de connexion ont été désinstallées.

Figure 18-3 *Désinstallation d'une méthode de connexion*



Création d'une séquence de méthode de connexion

Lorsque plusieurs méthodes de connexion sont créées pour votre environnement, vous pouvez choisir l'ordre d'utilisation de ces méthodes. Pour créer une méthode de connexion, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Séquences et méthodes de connexion**.
2. Sélectionnez l'onglet **Séquences de méthode de connexion**.
3. Cliquez sur l'icône + pour créer une séquence de méthode de connexion.
4. Spécifiez un **nom**, puis sélectionnez le **type de séquence** approprié.
5. Sélectionnez les méthodes de connexion et de post-connexion requises dans la liste des méthodes de connexion et de post-connexion disponibles.

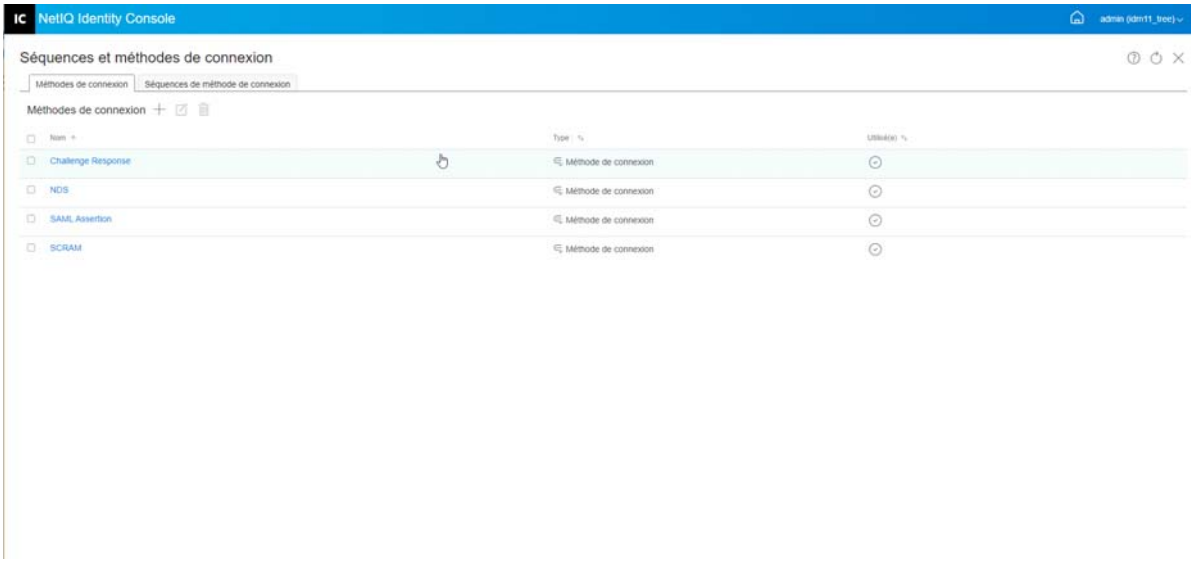
REMARQUE : pour déterminer l'ordre des méthodes de connexion, cliquez sur les flèches vers le haut et vers le bas visibles sur les objets Méthode de connexion.

---

6 Cliquez sur le bouton **Créer**.

7 Un message de confirmation s'affiche pour signaler qu'une séquence de méthode de connexion a été créée.

Figure 18-4 *Création d'une séquence de méthode de connexion*



Modification d'une séquence de méthode de connexion

Pour modifier une séquence de méthode de connexion existante, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Séquences et méthodes de connexion**.

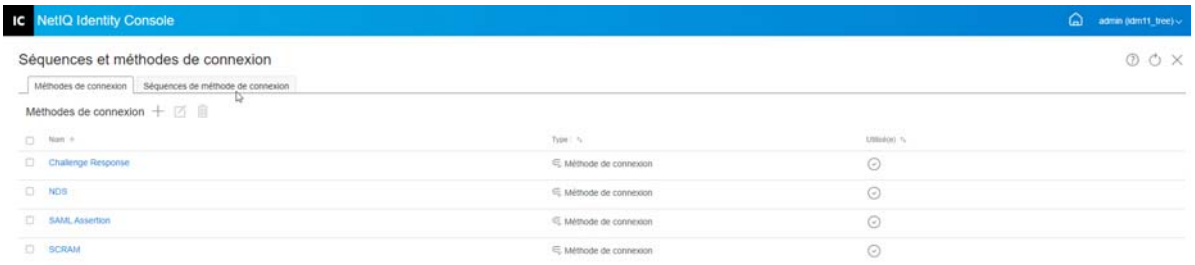
2 Sélectionnez l'onglet **Séquences de méthode de connexion**.

3 Cliquez sur l'icône ☑ pour modifier une séquence de méthode de connexion existante.

4 Apportez les modifications nécessaires sur la page **Modifier la séquence de méthode de connexion**, puis cliquez sur **Enregistrer**.

5 Un message de confirmation s'affiche pour signaler que la séquence de méthode de connexion a été modifiée.

Figure 18-5 *Modification d'une séquence de méthode de connexion*

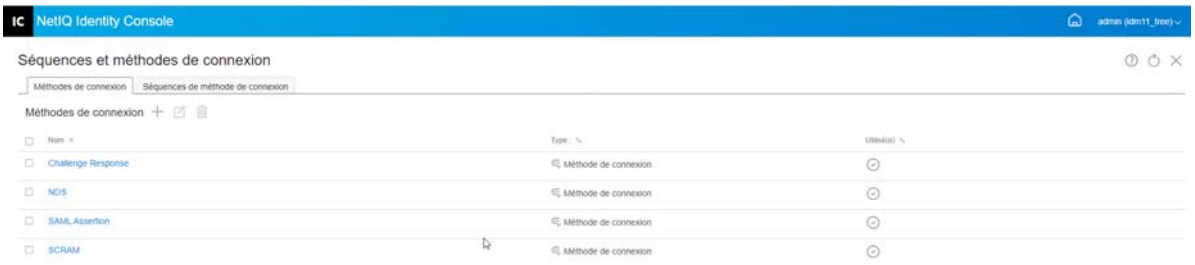


Autorisation ou annulation de l'autorisation d'une séquence de méthode de connexion

Une séquence de méthode de connexion doit être autorisée et définie par défaut pour pouvoir être associée à des utilisateurs, des conteneurs et des partitions. Pour autoriser une séquence de méthode de connexion, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Séquences et méthodes de connexion**.
2. Sélectionnez l'onglet **Séquences de méthode de connexion**.
3. Sélectionnez la séquence de méthode de connexion appropriée dans la liste, puis cliquez sur l'icône ⊘.
4. Pour annuler l'autorisation d'une séquence de méthode de connexion, sélectionnez-la, puis cliquez sur l'icône ⊗.
5. Vous pouvez également autoriser ou annuler l'autorisation d'une séquence de méthode de connexion à l'aide de la liste déroulante située dans la colonne **Autorisé(e)** de la liste des séquences de méthode de connexion.

Figure 18-6 *Autorisation ou annulation de l'autorisation d'une séquence de méthode de connexion*

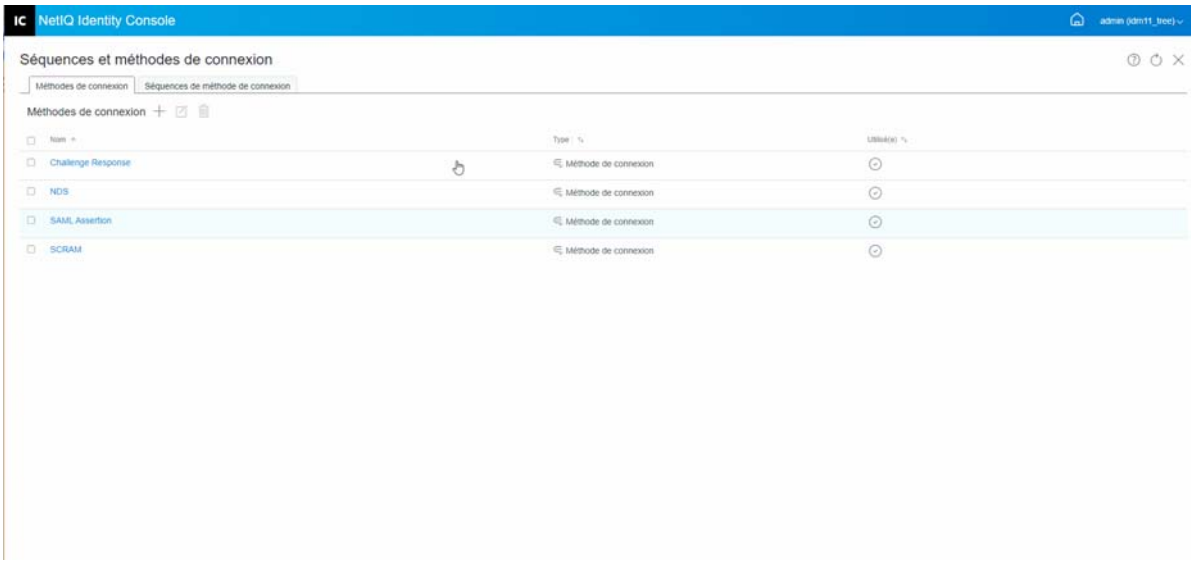


Définition d'une séquence de méthode de connexion par défaut

Pour définir une séquence de connexion par défaut afin que les utilisateurs ne doivent pas spécifier de séquence de connexion lorsqu'ils se connectent, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Séquences et méthodes de connexion**.
2. Sélectionnez l'onglet **Séquences de méthode de connexion**.
3. Activez l'icône pour définir une séquence de méthode de connexion autorisée par défaut.

Figure 18-7 *Définition d'une séquence de méthode de connexion par défaut*

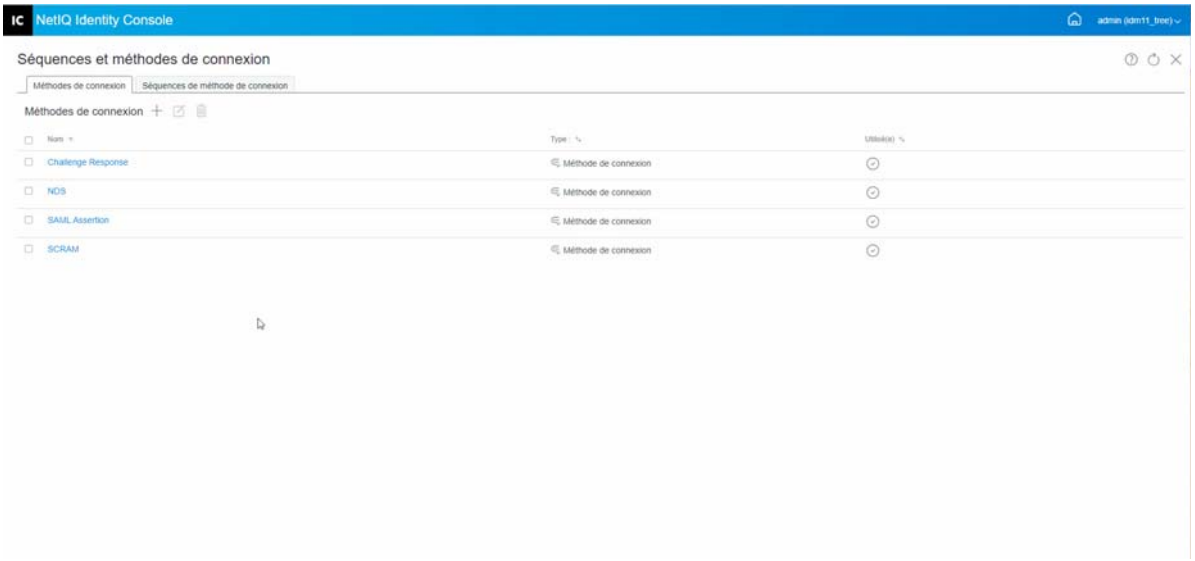


Suppression d'une séquence de méthode de connexion

Pour supprimer une séquence de méthode de connexion, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Séquences et méthodes de connexion**.
2. Sélectionnez l'onglet **Séquences de méthode de connexion**.
3. Sélectionnez la séquence de méthode de connexion appropriée dans la liste, puis cliquez sur l'icône .
4. Dans l'écran de confirmation suivant, cliquez sur **OK**.

Figure 18-8 *Suppression d'une séquence de méthode de connexion*



Gestion des stratégies de mot de passe

Une règle de mot de passe est un ensemble de principes définis par l'administrateur et régissant les critères de création et de remplacement des mots de passe par les utilisateurs finals. NMAS vous permet d'appliquer des stratégies de mot de passe que vous assignez aux utilisateurs dans eDirectory. Les stratégies de mot de passe peuvent également inclure des fonctions de mot de passe oublié en self-service afin de réduire les appels au service d'assistance concernant les mots de passe oubliés. Une autre fonctionnalité est le self-service de réinitialisation de mot de passe qui permet aux utilisateurs de modifier leur mot de passe pendant qu'ils affichent les règles que l'administrateur a définies dans la stratégie de mot de passe. Les utilisateurs accèdent à ces fonctions via l'application utilisateur Identity Manager ou Identity Console.

Grâce au module Stratégies de mot de passe, vous pouvez effectuer les tâches suivantes :

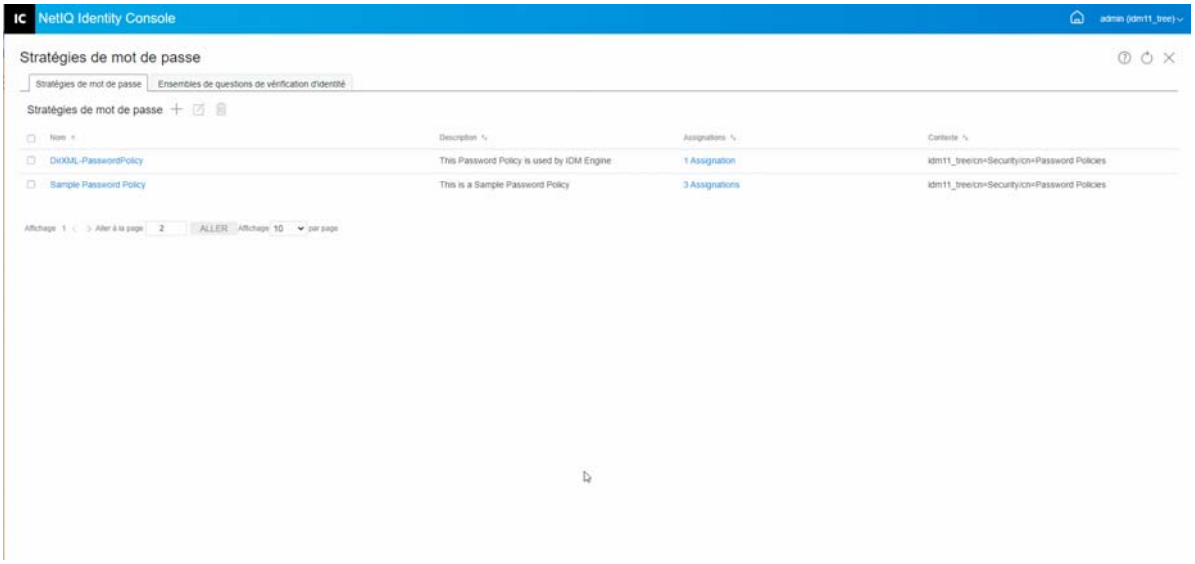
- « Création d'une stratégie de mot de passe avec les paramètres par défaut » page 118
- « Création d'une stratégie de mot de passe avec des paramètres personnalisés » page 118
- « Modification d'une stratégie de mot de passe » page 122
- « Suppression de stratégies de mot de passe » page 122

Création d'une stratégie de mot de passe avec les paramètres par défaut

Pour créer une stratégie de mot de passe, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Stratégies de mot de passe**.
2. Cliquez sur l'icône + pour créer une stratégie de mot de passe.
3. Dans l'écran suivant, indiquez un nom, un contexte, une description et un message de changement de mot de passe.
4. Si vous souhaitez créer une stratégie de mot de passe avec les paramètres par défaut, cochez la case **Créer une stratégie de mot de passe basée sur les paramètres par défaut**, puis cliquez sur **Suivant** pour afficher la page **Résumé**.
5. Vérifiez les informations de la page **Résumé**, puis cliquez sur **Créer**.
6. Un message de confirmation s'affiche pour signaler que la stratégie de mot de passe a été créée.

Figure 18-9 *Création d'une stratégie de mot de passe avec les paramètres par défaut*



Création d'une stratégie de mot de passe avec des paramètres personnalisés

Pour créer une stratégie de mot de passe avec des paramètres personnalisés, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Stratégies de mot de passe**.
2. Cliquez sur l'icône + pour créer une stratégie de mot de passe.
3. Dans l'écran suivant, indiquez un nom, un contexte, une description et un message de changement de mot de passe.

4 Si vous souhaitez créer une stratégie de mot de passe avec des paramètres personnalisés, cliquez sur **Suivant**.

5 Sur la page **Configuration**, effectuez les opérations suivantes :

5a **Activer le mot de passe universel:** L'activation du mot de passe universel pour une stratégie permet d'utiliser les options de la fonction des stratégies de mot de passe. Toutefois, avant de pouvoir activer le mot de passe universel pour une règle, vous devez satisfaire aux conditions préalables pour le mot de passe universel dans votre environnement.

5b **Activer les règles de mots de passe avancées:** Cette option active les règles de mot de passe sous Règles de mot de passe avancées. Ces règles vous aident à sécuriser votre environnement en vous permettant de contrôler des critères, tels que la durée de vie d'un mot de passe et le contenu d'un mot de passe (par exemple, combinaison de lettres, de chiffres, de majuscules, de minuscules et de caractères spéciaux). Vous pouvez exclure les mots de passe que vous estimez peu sûrs, tels que le nom de votre société.

5c **Synchronisation de mot de passe:** Ces options déterminent la manière dont le mot de passe universel est synchronisé dans eDirectory avec d'autres types de mots de passe du coffre-fort d'identité. La synchronisation du mot de passe contient les options suivantes :

5c1 **Supprimer le mot de passe NDS lors de la définition du mot de passe :** si vous sélectionnez cette option, le mot de passe NDS est désactivé lorsque le mot de passe universel est défini. Les utilisateurs ne pourront pas utiliser les anciennes méthodes ou les anciens utilitaires qui se connectent directement avec le mot de passe NDS au lieu de communiquer avec NMAS. Si vous définissez cette option, l'option suivante **Synchroniser le mot de passe NDS lors de la définition du mot de passe** est désactivée par défaut.

5c2 **Synchroniser le mot de passe NDS lors de la définition du mot de passe :** si vous sélectionnez cette option, la définition d'un mot de passe universel dans des applications telles qu'Identity Console modifie également le mot de passe NDS.

5c3 **Synchroniser le mot de passe simple lors de la définition du mot de passe :** cette option garantit la compatibilité avec NetIQ et les clients tiers à l'aide d'un mot de passe simple et du provisioning de l'utilisateur.

5c4 **Synchroniser le mot de passe de distribution lors de la définition du mot de passe :**

cette option détermine si le moteur méta-annuaire peut récupérer ou définir le mot de passe universel d'un utilisateur dans eDirectory.

5d **Récupération du mot de passe universel:** Les options suivantes sont disponibles :

5d1 **Autoriser l'utilisateur à récupérer le mot de passe:** cette option permet à l'agent utilisateur de récupérer le mot de passe. Cette option détermine si la fonction de mot de passe oublié en libre-service peut récupérer un mot de passe pour le compte d'un utilisateur afin de le lui envoyer dans un message électronique. Si vous ne sélectionnez pas cette option, la fonction correspondante apparaît en grisé sous l'onglet Mot de passe oublié de la stratégie de mot de passe.

5d2 **Autoriser l'administrateur à récupérer les mots de passe :** Cochez cette case si l'un de vos services le nécessite. Identity Manager ne nécessite pas que les administrateurs récupèrent les mots de passe. Toutefois, certains services tiers peuvent tirer parti de cette option.

5d3 **Autoriser les personnes suivantes à récupérer les mots de passe :** cliquez sur l'icône + pour sélectionner l'utilisateur approprié qui est censé récupérer le mot de passe.

5e Authentification:

5e1 Vérifier si les mots de passe existants respectent la stratégie de mot de passe (la vérification a lieu lors de la connexion) : Cette option est utile si vous déployez une nouvelle stratégie de mot de passe ou si vous modifiez les règles de mot de passe avancées pour une stratégie existante et si vous souhaitez garantir que les mots de passe existants respectent les règles de mot de passe nouvelles ou modifiées.

Si vous sélectionnez cette option, lorsque les utilisateurs se connecteront, leurs mots de passe seront analysés pour vérifier qu'ils sont bien conformes aux règles de mot de passe avancées définies dans la stratégie de mot de passe nouvelle ou modifiée. Si un mot de passe existant n'est pas conforme, l'utilisateur est invité à le changer.

Lorsque vous avez terminé, cliquez sur **Suivant**.

6 Les **règles de mot de passe avancées** vous permettent de sécuriser votre environnement en déterminant les informations sur les mots de passe, comme la durée de vie du mot de passe, la fréquence de changement du mot de passe et le contenu d'un mot de passe.

Les caractères spéciaux ne sont ni les chiffres (0-9) ni les caractères alphabétiques.

Sur la page Règles de mot de passe avancées, effectuez les opérations suivantes :

6a Vous pouvez gérer les paramètres de syntaxe du mot de passe à l'aide de la stratégie de complexité Microsoft (antérieure à Microsoft Windows Server 2008), de la stratégie de mot de passe Microsoft Server 2008 ou de la syntaxe Novell.

6b Spécifiez les valeurs requises pour les options Éditer le mot de passe, Durée de vie du mot de passe, Longueur et composition du mot de passe et Exclusions de mot de passe dans l'assistant, puis cliquez sur **Suivant**.

7 Pour réduire les coûts liés au service d'assistance, activez les fonctions **Mot de passe oublié** en self-service destinées aux utilisateurs qui ont oublié leur mot de passe. Ces fonctions en self-service sont mises à disposition des utilisateurs via le portail Identity Console. Sur la page Mot de passe oublié, effectuez les opérations suivantes :

REMARQUE : si vous activez l'option Mot de passe oublié, vous devez également indiquer si un ensemble de questions de vérification d'identité est requis pour aider l'utilisateur à se connecter.

7a Ensembles de stimulations : si vous utilisez des ensembles de questions de vérification d'identité, l'utilisateur ne peut utiliser la fonction de mot de passe oublié en self-service qu'après avoir répondu aux questions de l'ensemble de questions de vérification d'identité. Pour vous assurer que l'utilisateur est invité à saisir ces informations via le portail Identity Console, sélectionnez l'option **Exiger l'ensemble de questions de vérification d'identité**.

7b Opération : les options disponibles sous cet onglet permettent à l'utilisateur de réinitialiser le mot de passe à l'aide des ensembles de questions de vérification d'identité et du mot de passe universel, d'activer l'envoi du mot de passe actuel ou de l'indice de mot de passe par message électronique et d'afficher l'option d'indice de mot de passe.

7c Authentification: cochez la case **Forcer l'utilisateur à configurer des questions de vérification d'identité et/ou une astuce lors de l'authentification** pour vous assurer que l'utilisateur est invité à spécifier les ensembles de questions de vérification d'identité ou l'indice de mot de passe.

Lorsque vous avez terminé, cliquez sur **Suivant**.

8 Une stratégie ne prend effet qu'une fois assignée à un ou plusieurs objets. Nous vous recommandons d'assigner les stratégies le plus près possible de la racine de l'arborescence pour simplifier l'administration. Vous pouvez assigner une stratégie de mot de passe aux objets suivants :

8a **Objet Stratégie de connexion:** il est recommandé de créer une stratégie de mot de passe par défaut pour tous les utilisateurs de l'arborescence et de l'assigner à l'objet Stratégie de connexion situé dans le conteneur de sécurité.

8b **Conteneur constituant la racine d'une partition:** si vous assignez une stratégie à un conteneur qui constitue la racine d'une partition, tous les utilisateurs de la partition, y compris ceux placés dans les sous-conteneurs, héritent de l'assignation de la stratégie.

8c **Conteneur ne constituant pas la racine d'une partition:** Si vous assignez une stratégie à un conteneur qui ne constitue pas la racine d'une partition, seuls les utilisateurs de ce conteneur particulier héritent de l'assignation de la stratégie. Les utilisateurs des sous-conteneurs n'héritent pas de la stratégie.

Pour appliquer la stratégie à tous les utilisateurs d'un conteneur qui n'est pas la racine, assignez-la individuellement à chaque sous-conteneur.

8d **Un utilisateur:** Il est possible d'assigner une stratégie à un ou plusieurs utilisateurs.

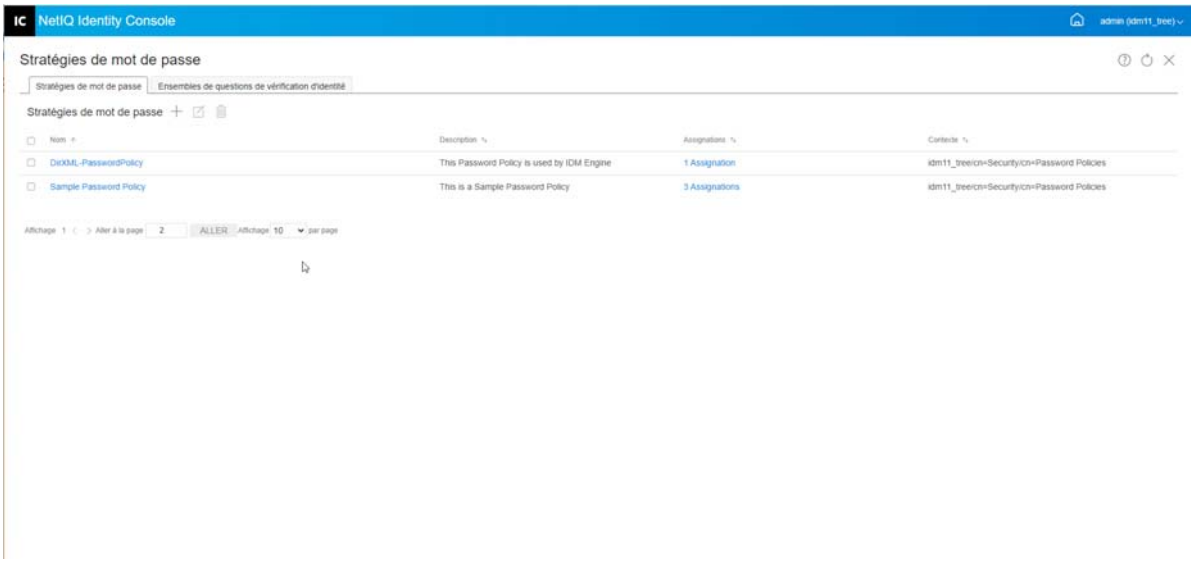
Pour assigner une stratégie, cliquez sur l'icône +. Ensuite, recherchez et sélectionnez l'objet approprié pour assigner une stratégie de mot de passe.

Si vous souhaitez supprimer une association de stratégie, sélectionnez la stratégie appropriée dans la liste, puis cliquez sur l'icône 🗑.

9 Vérifiez les informations de la page **Résumé**, puis cliquez sur **Créer**.

10 Un message de confirmation s'affiche pour signaler que la stratégie de mot de passe a été créée.

Figure 18-10 *Création d'une stratégie de mot de passe avec des paramètres personnalisés*

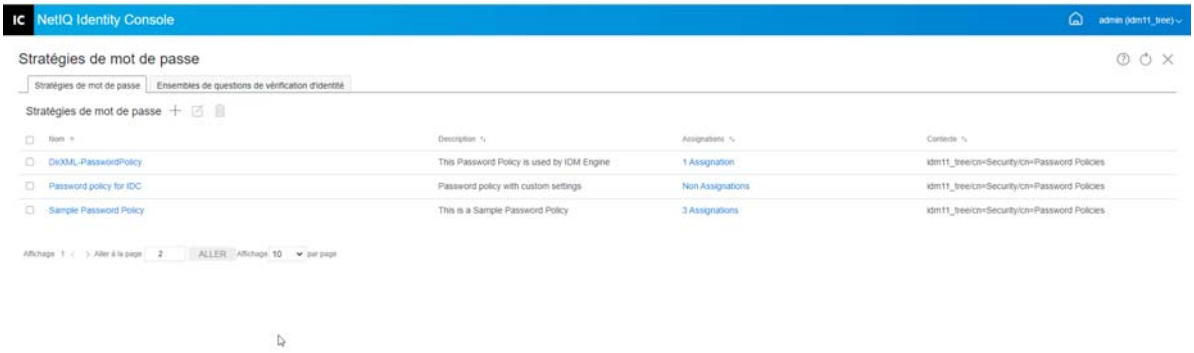


Modification d'une stratégie de mot de passe

Pour modifier une stratégie de mot de passe existante, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Stratégies de mot de passe**.
2. Sélectionnez la stratégie de mot de passe appropriée dans la liste, puis cliquez sur l'icône .
3. Apportez les modifications nécessaires sur la page **Modifier la stratégie de mot de passe**, puis cliquez sur **Enregistrer**.

Figure 18-11 *Modification d'une stratégie de mot de passe*

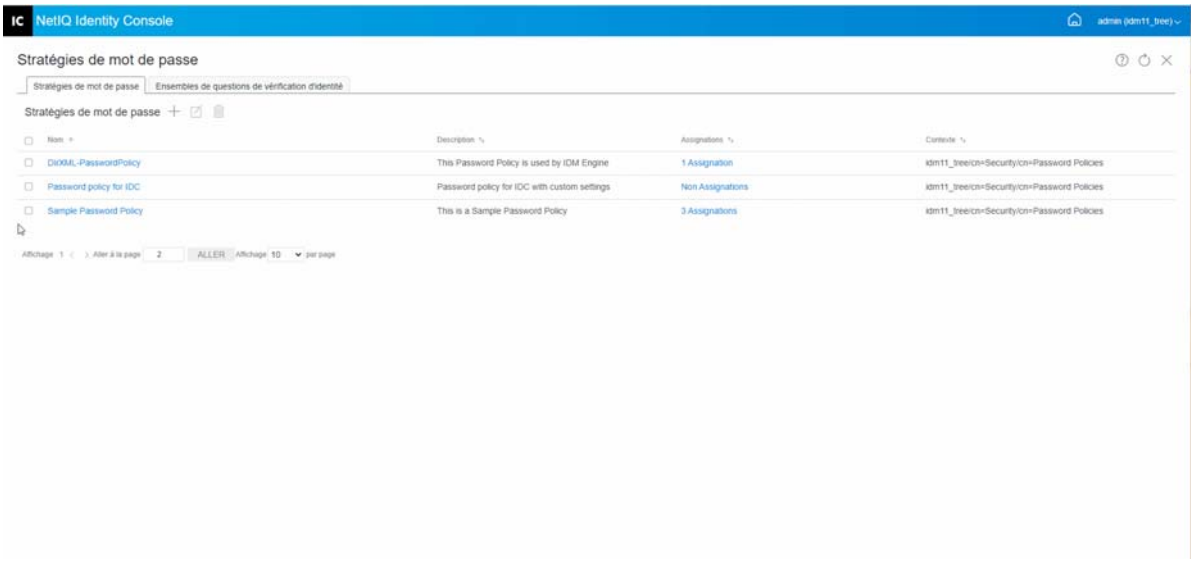


Suppression de stratégies de mot de passe

Pour supprimer des stratégies de mot de passe, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Stratégies de mot de passe**.
2. Sélectionnez les stratégies de mot de passe appropriées dans la liste, puis cliquez sur l'icône .
3. Dans l'écran d'avertissement suivant, cliquez sur **OK**.
4. Un message de confirmation s'affiche pour signaler que les stratégies de mot de passe ont été supprimées.

Figure 18-12 *Suppression d'une stratégie de mot de passe*



Gestion des ensembles de questions de vérification d'identité

Un ensemble de questions de vérification d'identité est constitué d'une ou de plusieurs questions auxquelles un utilisateur doit répondre pour établir son identité. Un ensemble de questions de vérification d'identité appartient à la fonction de mot de passe en libre-service.

Lorsqu'un utilisateur a du mal à de souvenir de son mot de passe ou à l'utiliser, il peut utiliser la fonction de mot de passe en libre-service au lieu d'appeler le support technique. Un ensemble de questions de vérification d'identité permet à un utilisateur de valider son identité et de recevoir ensuite un indice ou un mot de passe dans un message électronique, ou de réinitialiser un mot de passe en utilisant un navigateur Web.

Vous pouvez permettre aux utilisateurs de créer leurs propres questions ou exiger qu'ils répondent aux questions que vous créez.

La page Ensemble de questions de vérification d'identité permet de rechercher des ensembles de questions de vérification d'identité, d'en créer des nouveaux et d'en modifier des existants.

- « Création d'un ensemble de questions de vérification d'identité » page 123
- « Modification d'un ensemble de questions de vérification d'identité » page 124
- « Suppression d'un ensemble de questions de vérification d'identité » page 125

Création d'un ensemble de questions de vérification d'identité

Pour créer un ensemble de questions de vérification d'identité, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Stratégies de mot de passe** > **Ensembles de questions de vérification d'identité**.
2. Cliquez sur l'icône + pour créer un ensemble de questions de vérification d'identité.

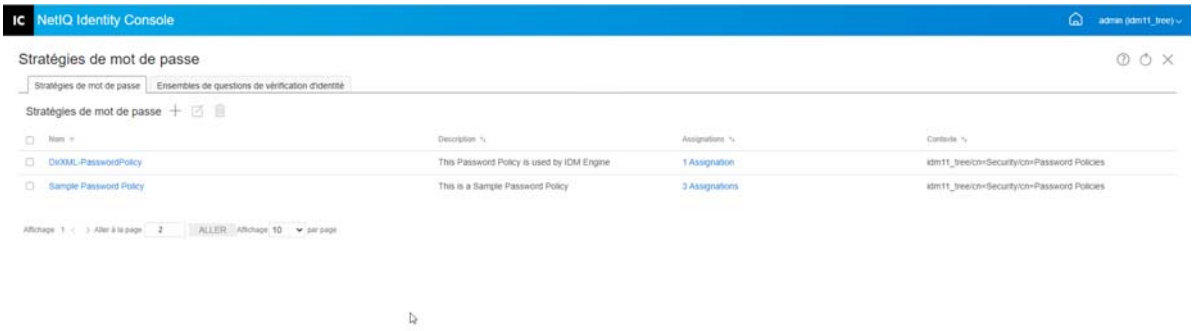
3 Indiquez le nom de l'objet Ensemble de questions de vérification d'identité, puis sélectionnez le conteneur ou le sous-conteneur dans lequel l'ensemble de questions de vérification d'identité doit être créé.

4 Créez un ensemble de questions à poser pour récupérer le mot de passe de l'utilisateur. Vous pouvez également sélectionner l'un des ensembles de questions aléatoires existants.

5 Définissez le nombre de questions à poser, puis cliquez sur **Créer**.

6 Un message de confirmation s'affiche pour signaler que l'ensemble de questions de vérification d'identité a été créé.

Figure 18-13 *Création d'un ensemble de stimulations*



Modification d'un ensemble de questions de vérification d'identité

Pour modifier un ensemble de questions de vérification d'identité existant, procédez comme suit :

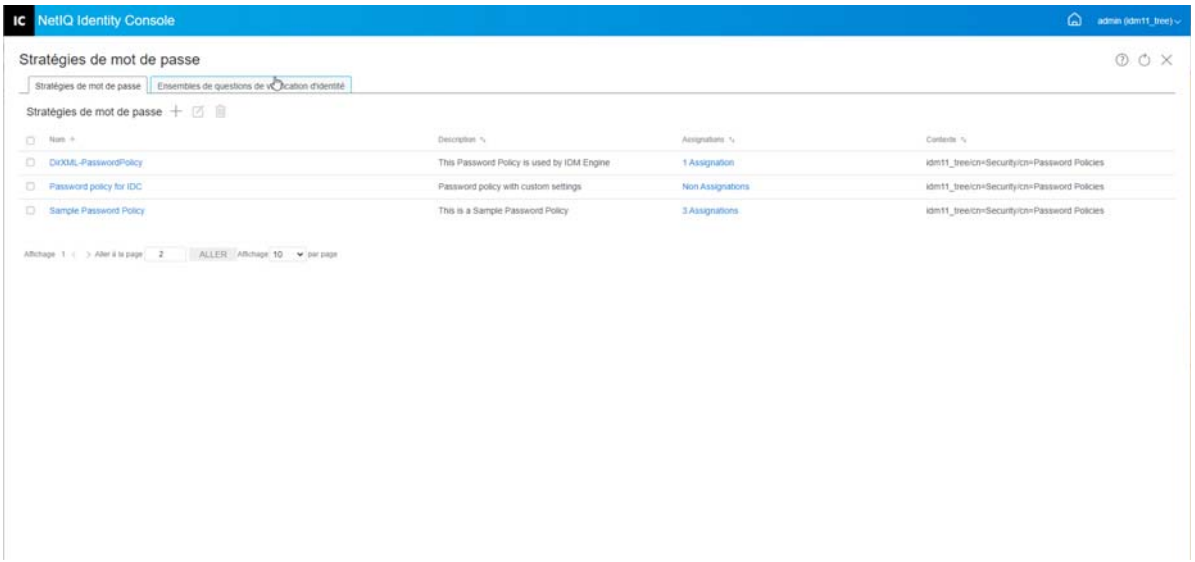
1 Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Stratégies de mot de passe** > **Ensembles de questions de vérification d'identité**.

2 Sélectionnez l'ensemble de questions de vérification d'identité approprié dans la liste, puis cliquez sur l'icône ☑.

3 Apportez les modifications nécessaires sur la page Modifier l'ensemble de questions de vérification d'identité, puis cliquez sur **Enregistrer**.

4 Un message de confirmation s'affiche pour signaler que l'ensemble de questions de vérification d'identité a été modifié.

Figure 18-14 *Modification d'un ensemble de questions de vérification d'identité*

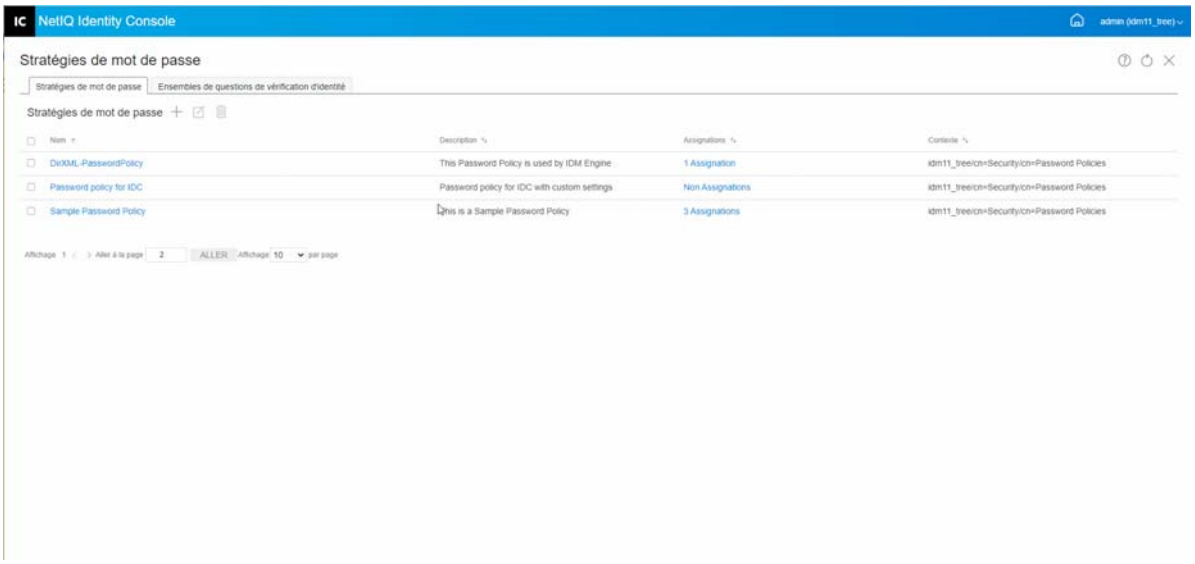


Suppression d'un ensemble de questions de vérification d'identité

Pour supprimer un ensemble de questions de vérification d'identité, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur **Gestion des authentifications** > **Stratégies de mot de passe** > **Ensembles de questions de vérification d'identité**.
2. Sélectionnez l'ensemble de questions de vérification d'identité approprié dans la liste, puis cliquez sur l'icône .
3. Dans l'écran de confirmation, cliquez sur **OK**.
4. Un message de confirmation s'affiche pour signaler que l'ensemble de questions de vérification d'identité a été supprimé.

Figure 18-15 *Suppression d'un ensemble de questions de vérification d'identité*



19 Gestion des objets Groupe SNMP

Le protocole SNMP (Simple Network Management Protocol) correspond au protocole Internet standard d'exploitation et de maintenance. Il permet l'échange de données de gestion entre les applications de console de gestion et les périphériques qu'elles gèrent.

Grâce au module SNMP, vous pouvez effectuer les tâches suivantes :

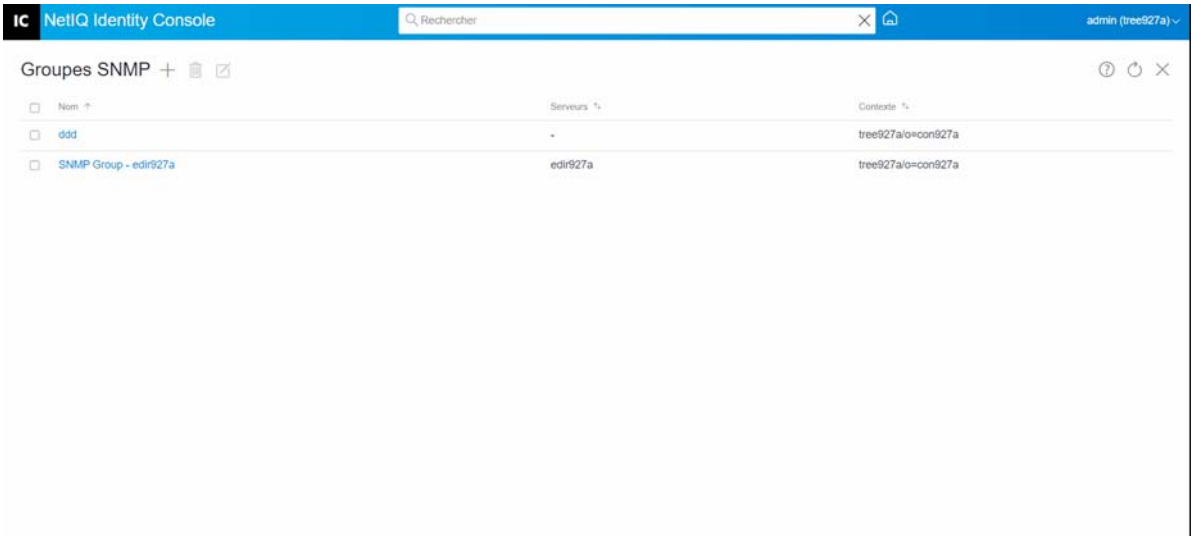
- « Création d'un objet Groupe SNMP » page 127
- « Modification d'un objet Groupe SNMP » page 128
- « Suppression d'un objet Groupe SNMP » page 128

Création d'un objet Groupe SNMP

Pour créer un objet Groupe SNMP, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur le module **SNMP**.
2. Cliquez sur l'icône + pour créer un objet Groupe SNMP.
3. Indiquez un nom et sélectionnez le contexte du nouvel objet Groupe SNMP.
4. Cliquez sur le bouton **Créer**.
5. Un message s'affiche à l'écran pour confirmer que l'objet Groupe SNMP a été créé.

Figure 19-1 *Création d'un objet Groupe SNMP*

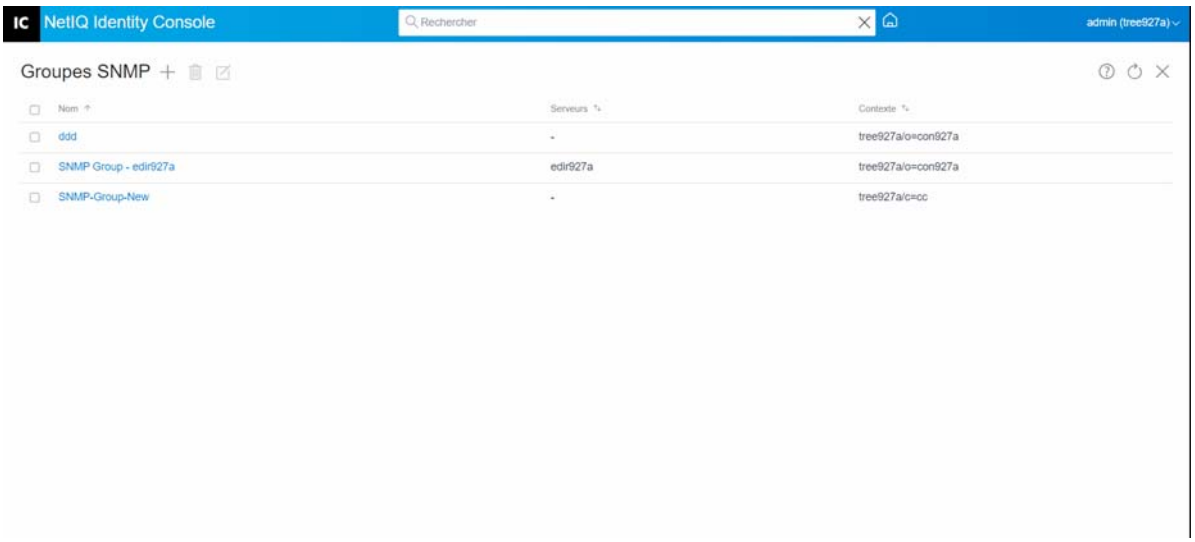


Modification d'un objet Groupe SNMP

Pour modifier un objet Groupe SNMP, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur le module **SNMP**.
2. Sélectionnez l'objet Groupe SNMP à modifier, puis cliquez sur l'icône .
3. Modifiez les paramètres configurables sur la page **Général**/**Trappes**.
4. Lorsque vous avez terminé, cliquez sur le bouton **Enregistrer**.
5. Un message s'affiche à l'écran pour confirmer que l'objet Groupe SNMP a été modifié.

Figure 19-2 *Modification d'un objet Groupe SNMP*

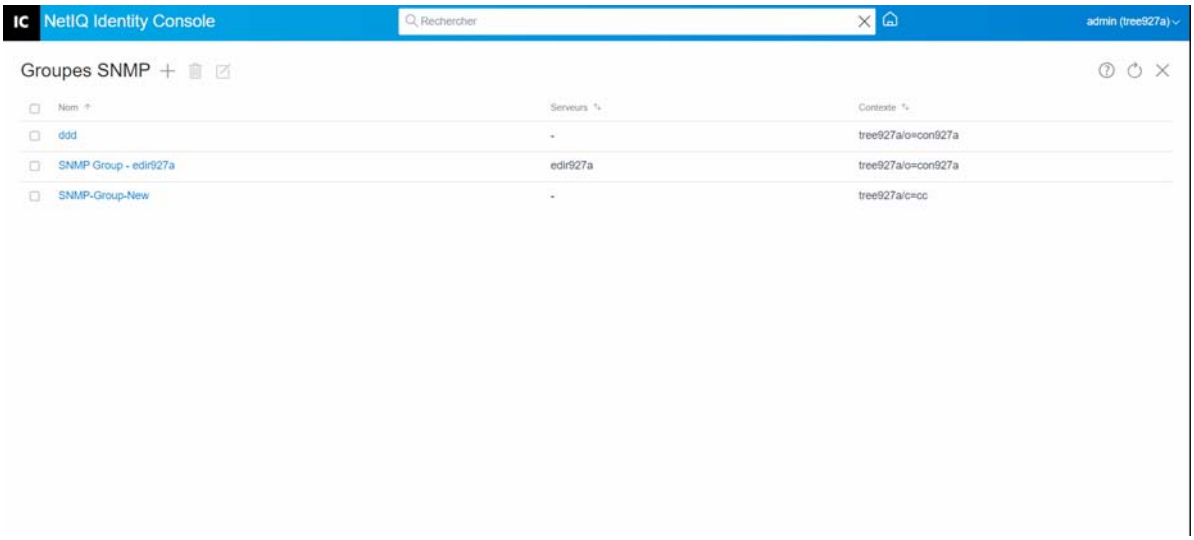


Suppression d'un objet Groupe SNMP

Pour supprimer un objet Groupe SNMP, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur le module **SNMP**.
2. Sélectionnez l'objet Groupe SNMP à modifier, puis cliquez sur l'icône .
3. Dans l'écran suivant, cliquez sur **OK**.
4. Un message s'affiche à l'écran pour confirmer que l'objet Groupe SNMP a été supprimé.

Figure 19-3 *Suppression d'un objet Groupe SNMP*



20 Gestion de l'authentification en arrière-plan améliorée

Pour que vous puissiez accéder à eDirectory à partir du plug-in EBA d'Identity Console, votre arborescence doit comporter un serveur EBA ayant un fichier eba.p12 valide. Pour plus d'informations sur l'activation d'EBA dans votre arborescence eDirectory, reportez-vous à la section Activation de l'authentification EBA sur une arborescence eDirectory dans le *Guide d'administration de NetIQ eDirectory*.

REMARQUE : Si vous souhaitez utiliser le module EBA avec Identity Console, vous devez effectuer une mise à niveau de votre serveur eDirectory vers la version 9.2.4 HF2.

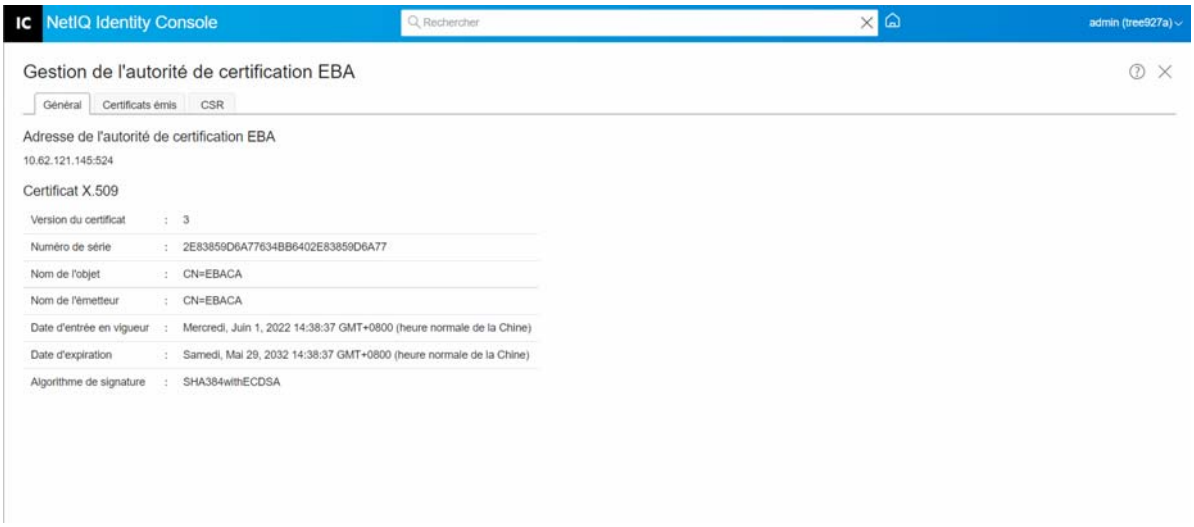
Pour ouvrir la page Gestion de l'autorité de certification EBA, connectez-vous au portail Identity Console, puis cliquez sur le module **EBA**.

La page de gestion de l'autorité de certification EBA comprend les onglets ci-dessous, lesquels permettent de gérer les différents aspects de l'autorité de certification EBA :

- **Général :** Affiche l'adresse IP de l'autorité de certification EBA et son certificat.
- **Certificats émis:** Affiche les certificats de l'autorité de certification NCP, accompagnés de leur adresse IP et de leur port.

  Pour révoquer un certificat, sélectionnez-le, puis cliquez sur ⊘. N'utilisez cette option que dans les cas extrêmes, car le serveur possédant le certificat d'autorité de certification NCP cessera de fonctionner si vous révoquez son certificat. En règle générale, un certificat doit être révoqué lorsqu'un serveur est endommagé.
- **Requête de signature de certificat (CSR) :** affiche la liste des requêtes de signature de certificat en attente d'approbation par l'administrateur. Pour approuver une requête de signature de certificat, sélectionnez le certificat dans la liste, puis cliquez sur **Approuver**.

Figure 20-1 *Gestion de l'authentification en arrière-plan améliorée*



II Gestion d'Identity Manager à l'aide d'Identity Console

Cette section décrit les différentes tâches que vous pouvez effectuer pour gérer vos serveurs Identity Manager à l'aide du portail Identity Console.

21 Gestion des pilotes et des ensembles de pilotes

Un ensemble de pilotes est un conteneur qui regroupe des pilotes Identity Manager. Vous ne pouvez activer qu'un seul ensemble de pilotes à la fois sur un serveur. Par conséquent, tous les pilotes actifs doivent être regroupés au sein du même ensemble de pilotes. Vous pouvez créer un ensemble de pilotes à l'aide de l'outil Designer. Pour plus d'informations, reportez-vous à la section Configuring Driver Sets (Configuration d'ensembles de pilotes) du manuel *NetIQ Designer for Identity Manager Administration Guide* (Guide d'administration de NetIQ Designer pour Identity Manager).

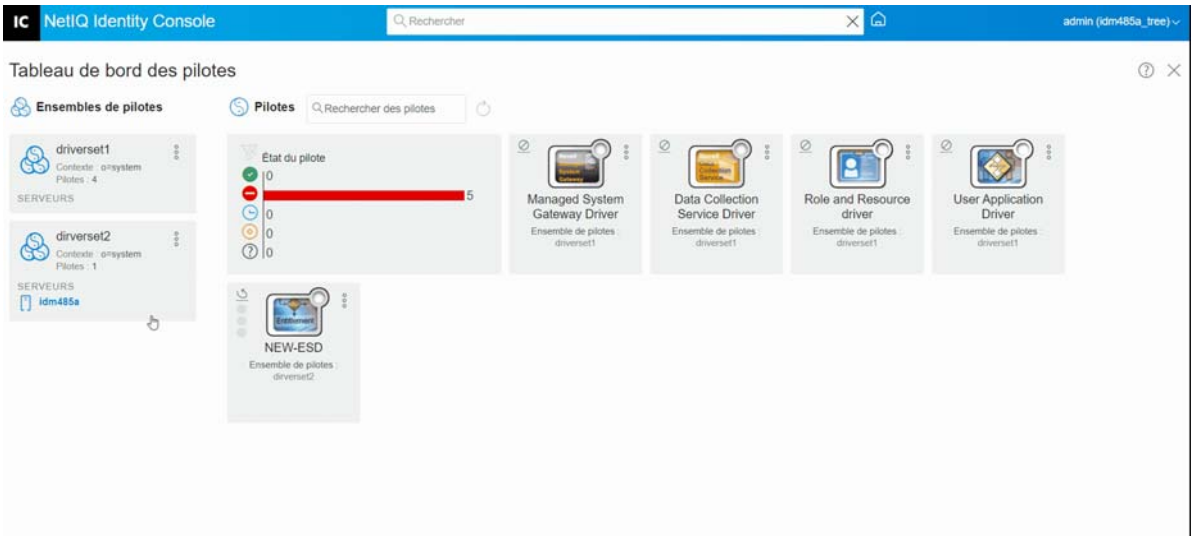
Ajout ou suppression d'un serveur

Un ensemble de pilotes peut être associé à un ou plusieurs serveurs à la fois. Toutefois, selon vos besoins, vous pouvez associer un autre objet Ensemble de pilotes au serveur disponible.

Pour ajouter un nouveau serveur, cliquez sur l'icône sur l'objet Ensemble de pilotes spécifique > sélectionnez **Ajouter des serveurs**, puis choisissez le serveur approprié dans le parcoureur de contexte.

Pour supprimer un serveur existant, sélectionnez l'option **Supprimer le serveur**.

Figure 21-1 *Ajout d'un serveur à un ensemble de pilotes*



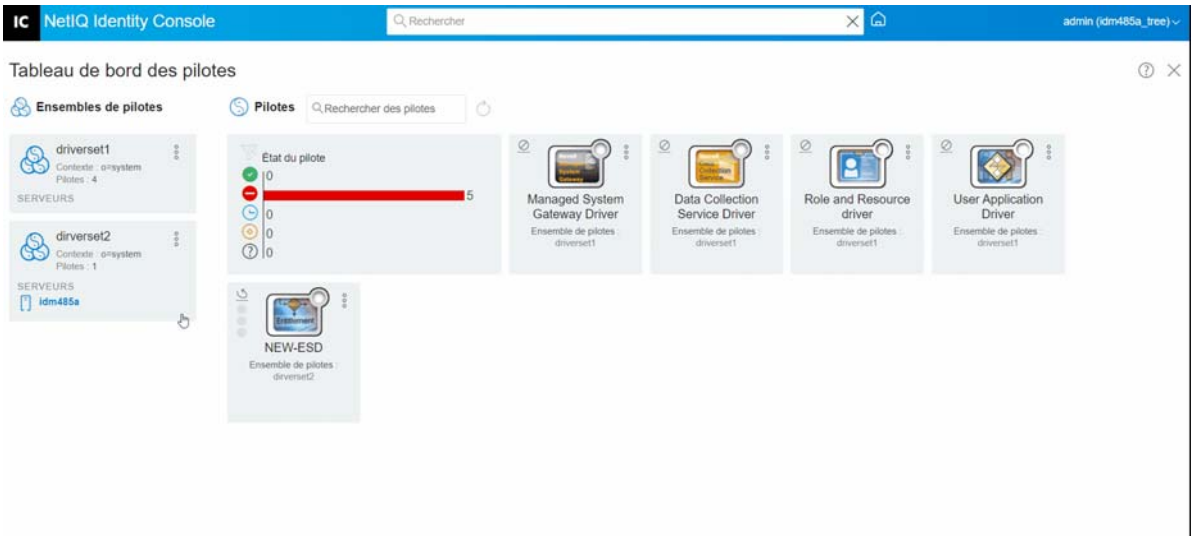
Activation d'un ensemble de pilotes à l'aide d'une clé d'activation du produit

Avant d'utiliser un ensemble de pilotes et les pilotes qu'il contient, vous devez l'activer à l'aide du code d'activation que vous avez reçu dans votre ID d'adresse électronique. Après avoir acheté une licence, vous recevrez votre clé d'activation de la part de NetIQ. Pour activer l'ensemble de pilotes à l'aide de votre clé d'activation, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'onglet **Administration IDM**.
2. Cliquez sur l'icône Opérations correspondant à la zone de l'ensemble de pilotes à activer, puis cliquez sur **Installation de l'activation**.

   Lors de l'application de l'activation, chaque onglet d'ensemble de pilotes dans la vignette Administration IDM affiche les informations d'activation de tous les serveurs associés à cet ensemble de pilotes. Ces informations permettent d'identifier le moment d'expiration de l'activation.
3. Si vous avez téléchargé le fichier d'activation sur votre ordinateur, cochez la case **Sélectionner un fichier contenant des informations d'identification**.
4. Recherchez et sélectionnez le fichier d'activation, puis cliquez sur **Soumettre**.
5. Vous pouvez également activer l'ensemble de pilotes en utilisant le contenu du fichier d'activation. Cochez la case **Entrer les informations d'identification**.
   - **5a** Ouvrez le fichier de référence d'activation du produit, puis copiez son contenu dans le Presse-papiers.
   - **5b** Si vous avez choisi de copier le contenu, n'incluez pas d'espaces ni de lignes supplémentaires. Vous devez commencer la copie à partir du premier tiret (-) des informations d'identification (----DÉBUT DES INFORMATIONS D'IDENTIFICATION D'ACTIVATION DU PRODUIT) jusqu'au dernier tiret (-) (FIN DES INFORMATIONS D'IDENTIFICATION D'ACTIVATION DU PRODUIT. Cliquez ensuite sur **Terminer**.
6. Un message de confirmation s'affiche pour signaler que l'ensemble de pilotes a été activé.

Figure 21-2 *Activation d'un ensemble de pilotes*

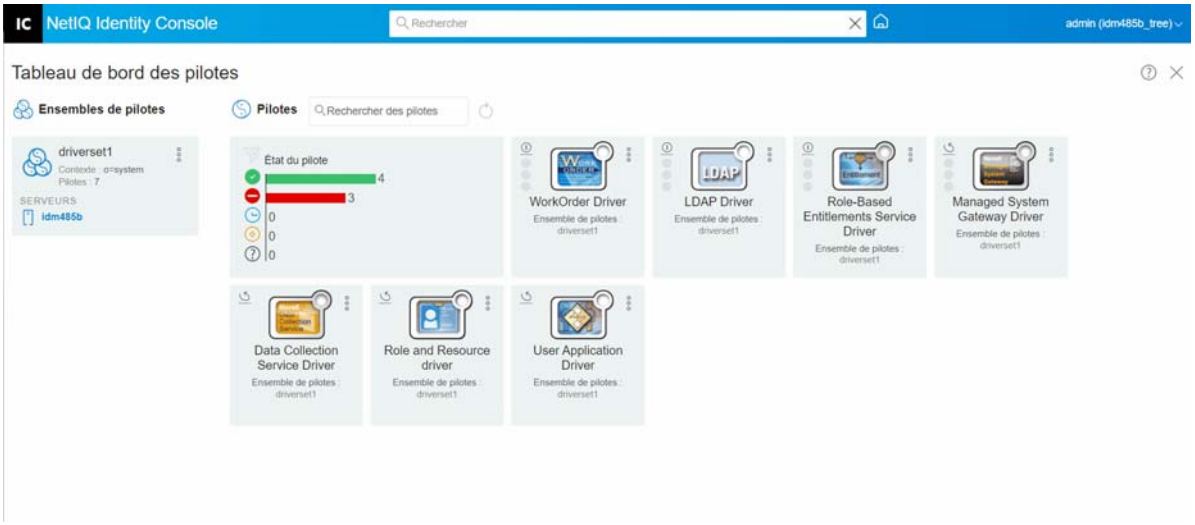


Affichage des informations d'activation d'un ensemble de pilotes

Après avoir activé un ensemble de pilotes, vous devez vérifier qu'il a bien été activé. Pour ce faire, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'onglet **Administration IDM**.
2. Cliquez sur l'icône Opérations ⋮ correspondant à l'objet Ensemble de pilotes dont vous souhaitez vérifier les informations d'activation, puis cliquez sur **Infos d'activation**.
3. La fenêtre des informations relatives à l'activation s'affiche sur votre ordinateur. Cette page vous permet de vérifier les informations d'activation de l'ensemble de pilotes donné.

Figure 21-3 *Affichage des informations d'activation d'un ensemble de pilotes*

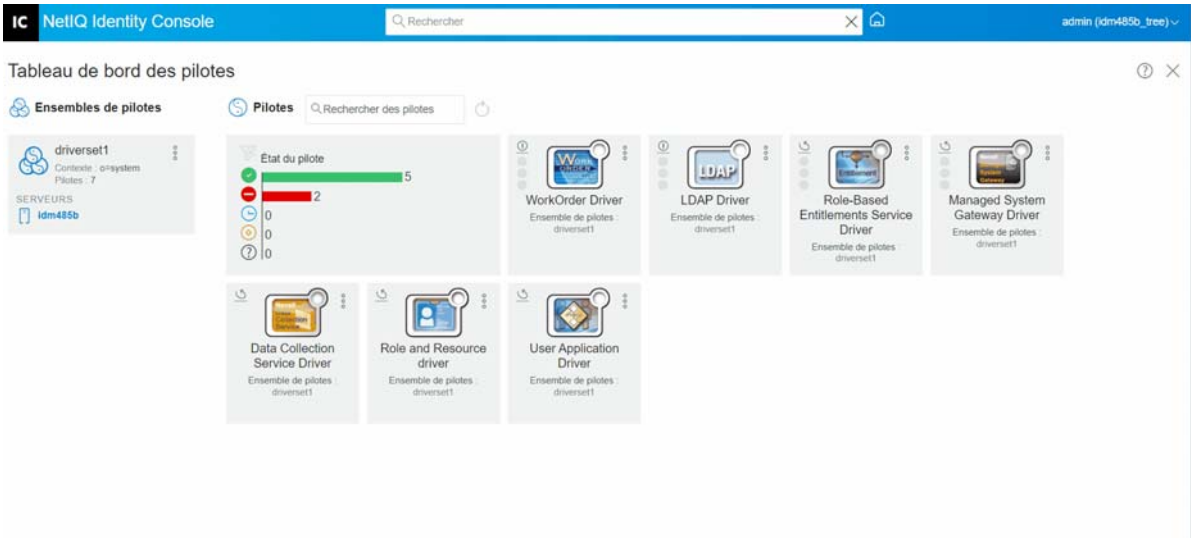


Démarrage et arrêt d'un pilote

Lorsqu'un pilote est créé, il est arrêté par défaut. Pour que le pilote soit opérationnel, vous devez le démarrer. Identity Manager est un système piloté par les événements. Ainsi, une fois le pilote démarré, il reste inactif jusqu'à ce qu'un événement se produise. Pour démarrer/arrêter un pilote, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'onglet **Administration IDM**.
2. Cliquez sur l'objet Ensemble de pilotes approprié à droite de l'écran de votre ordinateur pour afficher tous les pilotes qui y sont associés.
3. Cliquez sur l'icône Opérations correspondant au pilote concerné, puis sélectionnez **Démarrer le pilote**.
4. Pour arrêter un objet Pilote, cliquez sur l'icône Opérations correspondant au pilote concerné, puis sélectionnez **Arrêter le pilote**.
5. (Facultatif) Vous pouvez également démarrer ou arrêter simultanément tous les pilotes situés dans le même objet Ensemble de pilotes. Pour ce faire, cliquez sur l'icône Opérations correspondant à l'objet Ensemble de pilotes concerné, puis sélectionnez **Démarrer tous les pilotes** ou **Arrêter tous les pilotes**.

Figure 21-4 *Démarrage et arrêt d'un pilote*



Recherche d'un pilote

Identity Console permet de rechercher un pilote spécifique sur votre serveur. Pour rechercher un pilote, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'onglet **Administration IDM**.
2. Indiquez le nom du pilote dans la zone de **recherche**. L'objet Pilote correspondant s'affiche alors sur l'écran de votre ordinateur. Vous pouvez également rafraîchir la liste des pilotes en cliquant sur l'icône .

Figure 21-5 *Recherche d'un pilote*

Filtrage des pilotes et des ensembles de pilotes

Les pilotes peuvent être filtrés en fonction de leur état à partir de la page **IDM Administration** (Administration IDM). Pour filtrer les pilotes, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'onglet **Administration IDM**.
2. Cliquez sur les icônes suivantes dans la vignette d'**état des pilotes** pour filtrer les pilotes en fonction de leur état :
   - Cliquez sur l'icône pour filtrer tous les pilotes en cours d'exécution sur votre serveur.
   - Cliquez sur l'icône pour filtrer tous les pilotes arrêtés sur votre serveur.
   - Cliquez sur l'icône pour filtrer tous les pilotes en cours de démarrage.
   - Cliquez sur l'icône pour filtrer tous les pilotes en cours d'arrêt.
   - Cliquez sur l'icône pour filtrer les pilotes auxquels aucun état n'est associé. Lorsqu'aucun serveur n'est associé à un ensemble de pilotes, les pilotes qu'il contient présentent l'état **Inconnu(e)**.

Pour désactiver le filtre appliqué aux pilotes, cliquez sur l'icône affichée dans la vignette d'**état des pilotes**.

3 Vous pouvez également filtrer les ensembles de pilotes à l'aide du portail Identity Console. Par défaut, le portail Identity Console affiche tous les pilotes associés à tous les ensembles de pilotes de votre serveur. Si vous souhaitez afficher les pilotes dans un ensemble de pilotes spécifique, vous devez sélectionner cet ensemble dans la liste des ensembles de pilotes située à gauche du portail Identity Console. Pour désactiver la sélection de l'ensemble de pilotes, cliquez de nouveau sur l'ensemble de pilotes sélectionné.

Figure 21-6 *Filtrage des pilotes et des ensembles de pilotes*

Suppression d'un ensemble de pilotes

Pour supprimer un ensemble de pilotes, procédez comme suit :

1 Sur la page de renvoi d'Identity Console, cliquez sur l'onglet **Administration IDM**.

2 Cliquez sur le bouton Opérations dans l'ensemble de pilotes à supprimer.

3 Sélectionnez **Supprimer**.

Opérations de pilote

Les opérations suivantes sont disponibles à l'aide de l'icône Opérations dans la vignette d'un pilote :

- **Démarrer le pilote** : permet de démarrer le pilote.
- **Arrêter le pilote** : permet d'arrêter le pilote.
- **Redémarrer le pilote** : permet de redémarrer un pilote arrêté.

- **Supprimer le pilote** : permet de supprimer le pilote.
- **Statistiques** : permet d'afficher les statistiques de performances du pilote.
- **Copier les données** : permet de copier les données du pilote d'un serveur à un autre. Cette option n'est disponible que pour un environnement multiserveur.

22 Gestion des propriétés des ensembles de pilotes

Cette section fournit des informations sur les propriétés communes à tous les ensembles de pilotes. Elle aborde toutes les propriétés (Mot de passe nommé, Niveau de consignation, Inspecteur d'ensemble de pilotes, etc.).

Cette section présente les tâches suivantes :

Configuration d'un ensemble de pilotes

Pour modifier la configuration d'un ensemble de pilotes, procédez comme suit :

1. Cliquez sur **IDM Administration** (Administration IDM) > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Driver Set Properties** (Propriétés de l'ensemble de pilotes).
2. Par défaut, la page **Configuration de l'ensemble de pilotes** s'affiche. Les options de configuration de l'ensemble de pilotes sont les suivantes :

Mot de passe nommé

Identity Manager vous permet de stocker en toute sécurité plusieurs mots de passe pour un ensemble de pilotes. Cette fonction est appelée « mots de passe nommés ». Chaque mot de passe est accessible par l'intermédiaire d'une clé ou d'un nom.

Vous pouvez ajouter des mots de passe nommés à un ensemble de pilotes ou à un pilote spécifique. Les mots de passe nommés d'un ensemble de pilotes sont disponibles pour tous les pilotes de l'ensemble.

Pour utiliser un mot de passe nommé dans une règle de pilote, désignez-le par le nom du mot de passe au lieu d'utiliser le mot de passe réel. Le moteur Identity Manager envoie alors le mot de passe au pilote. Vous pouvez utiliser la méthode décrite dans cette section pour la mémorisation et la récupération des mots de passe nommés, avec n'importe quel pilote, sans apporter de modification au module d'interface pilote.

Pour accéder au mot de passe nommé, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Mot de passe nommé** sous **Configuration de l'ensemble de pilotes**.

Pour ajouter un nouveau mot de passe nommé, cliquez sur l'icône . Pour supprimer un mot de passe nommé existant, sélectionnez le mot de passe approprié, puis cliquez sur l'icône .

Global Configuration Values (Valeurs de configuration globales)

Cette option affiche une liste ordonnée des objets Configuration globale. Les objets contiennent les définitions de valeurs de configuration globale (VCG) d'extension pour le pilote qu'Identity Manager charge au démarrage du pilote. Vous pouvez ajouter ou supprimer des objets Configuration globale et modifier l'ordre d'exécution de ces objets. Cliquez sur l'icône pour enregistrer les VCG. Pour rafraîchir la liste de VCG, cliquez sur l'icône .

Configuration des paramètres d'environnement Java

Pour configurer les paramètres d'environnement Java, procédez comme suit :

1. Dans Identity Console, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes**.
2. Cliquez sur **Paramètres d'environnement Java** sous **Configuration de l'ensemble de pilotes** pour afficher la page de propriétés qui contient les paramètres d'environnement Java.
3. Modifiez les paramètres suivants selon vos besoins :

   Ajouts au chemin de classe: indiquez des chemins supplémentaires dans lesquels la machine virtuelle Java (JVM) peut rechercher des fichiers de paquetage (`.jar`) et de classe (`.class`). Ce paramètre équivaut à la commande `java -classpath`. Si vous saisissez plusieurs chemins de classe, séparez-les par un point-virgule (;) pour une JVM Windows et par un deux-points (:) pour une JVM UNIX ou Linux.

   Options JVM: indiquez des options supplémentaires à utiliser avec la JVM. Reportez-vous à votre documentation JVM pour connaître les options valides.

   `DHOST_JVM_OPTIONS` est la variable d'environnement correspondante. Elle spécifie les arguments pour JVM 1.2. Par exemple :

   ```
   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
   ```

   Les chaînes d'option sont séparées par un espace. Si une chaîne d'option contient un espace, elle doit être placée entre guillemets.

   L'option d'attribut de l'ensemble de pilotes est prioritaire sur la variable d'environnement `DHOST_JVM_OPTIONS`. Cette variable d'environnement est ajoutée au bas de la liste des pilotes.

Taille du tas initiale: indiquez la taille de segment initiale (minimale) disponible pour la JVM. L'augmentation de la taille du tas initiale peut améliorer le temps de démarrage et le débit. Utilisez une valeur numérique suivie de G, M ou K. Si aucune lettre n'est spécifiée, la taille par défaut est exprimée en octets. Ce paramètre équivaut à la commande `java -Xms`.

`DHOST_JVM_INITIAL_HEAP` est la variable d'environnement correspondante. Elle indique la taille de segment initiale de la JVM selon un nombre d'octets au format décimal. Elle est prioritaire par rapport à l'option d'attribut de l'ensemble de pilotes.

Reportez-vous à votre documentation JVM pour plus d'informations sur la taille du tas initiale par défaut pour JVM.

Taille de segment maximale : indiquez la taille de segment maximale disponible pour la JVM. Utilisez une valeur numérique suivie de G, M ou K. Si aucune lettre n'est spécifiée, la taille par défaut est exprimée en octets. Ce paramètre équivaut à la commande `java -Xmx`.

`DHOST_JVM_MAX_HEAP` est la variable d'environnement correspondante. Elle indique la taille de segment maximale de la JVM selon un nombre d'octets au format décimal. Elle est prioritaire par rapport à l'option d'attribut de l'ensemble de pilotes.

Reportez-vous à votre documentation JVM pour plus d'informations sur la taille du tas maximum par défaut pour JVM.

4 Cliquez sur pour enregistrer les modifications.

5 Redémarrez le coffre-fort d'identité pour appliquer les modifications apportées.

Gestion de la liste des attributs avec valeur

Pour ajouter des attributs à la liste des attributs avec valeur pour un ensemble de pilotes spécifique, procédez comme suit :

1 Dans Identity Console, sélectionnez le module **Gestion des objets**.

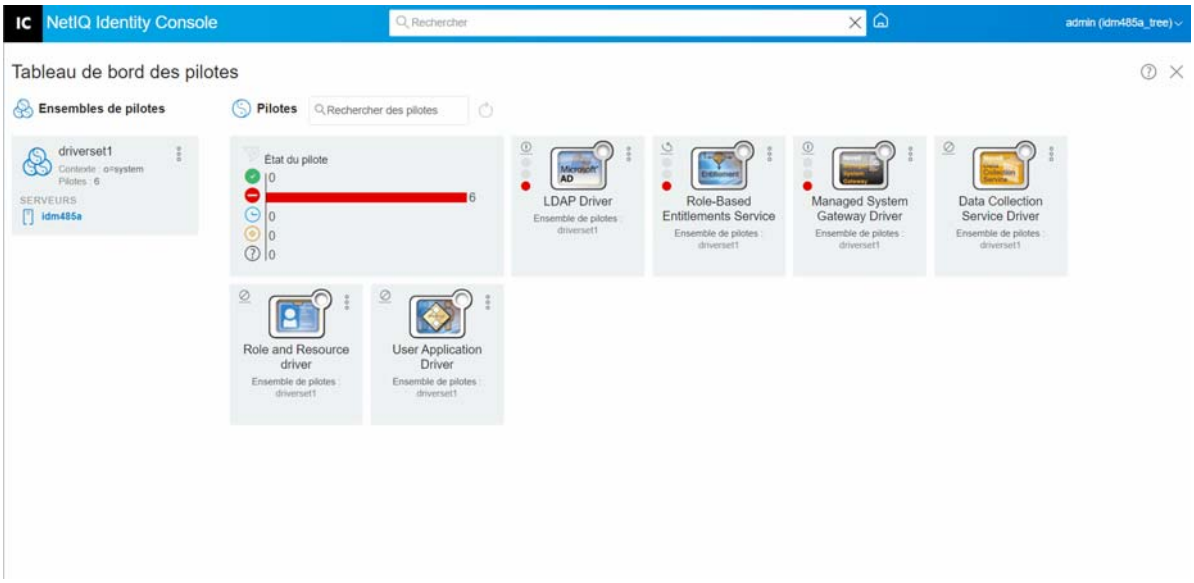
2 Sélectionnez le type **DirXML-DriverSet** dans la liste déroulante, puis cliquez sur le bouton Rechercher.

3 Cliquez sur l'ensemble de pilotes approprié dans la liste de recherche.

4 Pour ajouter des attributs sans valeur à la liste des attributs avec valeur, cliquez sur l'icône + située en regard des **attributs avec valeur**, puis sélectionnez les attributs sans valeur appropriés dans la liste.

5 Lorsque vous avez terminé, cliquez sur **OK**.

Figure 22-1 *Gestion des paramètres de configuration d'un ensemble de pilotes*



Gestion des travaux pour les ensembles de pilotes

Identity Console permet de planifier les événements à l'aide de l'option Travaux pour tous les pilotes contenus dans l'ensemble de pilotes correspondant.

La page Job Scheduler (Planificateur du travail) contient le nom et la description du travail, et indique si le travail est activé ou désactivé, ainsi que le moment de son exécution planifiée. Cliquez sur le nom du travail pour ouvrir la page Travaux. Cliquez sur l'icône activer/désactiver sous la colonne Activé pour activer ou désactiver le travail. Cliquez sur la description du travail pour afficher sa description complète.

Pour accéder à la page Travaux, sur la page principale d'Identity Console, sélectionnez **IDM Administration** (Administration IDM) > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Driver Set Properties** (Propriétés de l'ensemble de pilotes) > **Avancé(e)**. L'onglet Tâches contient une table affichant les objets Tâche existants du pilote sélectionné, répertoriés avec leur nom distinctif complet dans l'entrée Pilote.

Grâce à la page Job Scheduler (Planificateur du travail), vous pouvez effectuer les tâches suivantes :

- **Créer un travail** : cliquez sur l'icône + pour créer un travail.

  Dans la fenêtre contextuelle **Nouveau travail**, procédez comme suit pour créer un travail :

  1. Indiquez le nom du travail.
  2. Sélectionnez le type de travail souhaité.
  3. Cliquez sur l'icône ⌄, puis sélectionnez le serveur sur lequel vous souhaitez exécuter le travail dans la liste des serveurs disponibles. Sinon, indiquez un nom de serveur, puis sélectionnez le serveur souhaité.
  4. Cliquez sur le bouton **Créer**.

- **Démarrer un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône .
- **Arrêter un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône .
- **Activer un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône .
- **Désactiver un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône .
- **Obtenir l'état** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône .
- **Supprimer un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône .

Cliquez sur un travail pour accéder à la page des **propriétés du travail**. Vous pouvez y définir la manière dont le travail doit s'exécuter.

Général : affiche le nom de la classe Java du travail. À partir de cette page, vous pouvez activer ou désactiver le travail, le supprimer après son exécution, sélectionner les serveurs sur lesquels il doit s'exécuter, spécifier le serveur de messagerie et lui donner un nom et une description.

Planifier : permet de définir le moment d'exécution du travail. Spécifiez l'heure de démarrage du travail et indiquez si vous souhaitez l'exécuter tous les jours, toutes les semaines, tous les mois ou tous les ans. Vous pouvez également personnaliser le moment d'exécution du travail ou l'exécuter manuellement.

Étendue : permet de définir les objets auxquels ce travail s'applique. Un objet peut être un conteneur, un groupe dynamique, un groupe ou une feuille. Cliquez sur Ajouter pour sélectionner l'objet auquel vous voulez appliquer la tâche. Vous pouvez cliquer sur le bouton Parcourir pour sélectionner un objet, puis sur OK. Pour supprimer un objet de la liste d'étendue, cochez la case à gauche d'un objet DN pour sélectionner un objet d'étendue, puis cliquez sur Supprimer.

Une fois l'objet ajouté, sélectionnez-le pour afficher d'autres options. Si vous sélectionnez un groupe, vous pouvez appliquer la tâche aux membres du groupe ou au groupe uniquement. Si vous sélectionnez un objet Conteneur, vous pouvez appliquer le travail à tous les descendants du conteneur, à tous les enfants du conteneur ou au conteneur uniquement.

Paramètres : permet d'ajouter des paramètres au travail et de visualiser leur configuration actuelle. Ces paramètres changent en fonction du type de travail sélectionné.

Résultats : permet de définir ce que vous voulez faire des résultats du travail. La page de résultats est divisée en deux : les résultats intermédiaires et les résultats définitifs. Les résultats suivants sont possibles : Réussite, Avertissement, Erreur et Abandon. À droite de la colonne des résultats se trouve la colonne Opération. Cette colonne permet de sélectionner la façon dont vous souhaitez être notifié de chaque résultat. Parmi les opérations possibles figurent l'envoi d'un résultat d'audit ou d'un e-mail avec les résultats. Si vous ne sélectionnez aucune option, aucune opération n'est réalisée.

Dans l'onglet **Trace**, vous pouvez configurer la trace pour un pilote spécifique. Pour plus d'informations, reportez-vous à la section « Configuration du niveau de trace » page 176.

Gestion des bibliothèques pour un ensemble de pilotes spécifique

Les objets Bibliothèque stockent plusieurs stratégies et d'autres ressources partagées par un ou plusieurs pilotes. Vous pouvez créer un objet Bibliothèque dans un objet Ensemble de pilotes ou dans n'importe quel conteneur eDirectory. Une arborescence eDirectory peut contenir plusieurs bibliothèques. Un pilote peut faire référence à n'importe quelle bibliothèque de l'arborescence tant que le serveur qui exécute le pilote contient une réplique en lecture/écriture ou maîtresse de l'objet Bibliothèque.

Les feuilles de style, les stratégies, les règles et les autres objets Ressource peuvent être stockés dans une bibliothèque et être référencés par un ou plusieurs pilotes.

Grâce au module Library Management (Gestion des bibliothèques), vous pouvez effectuer les tâches suivantes :

- « Affichage et suppression d'une bibliothèque existante » page 148
- « Affichage et suppression d'un objet de la bibliothèque » page 148

Affichage et suppression d'une bibliothèque existante

Pour afficher et supprimer une bibliothèque existante, procédez comme suit :

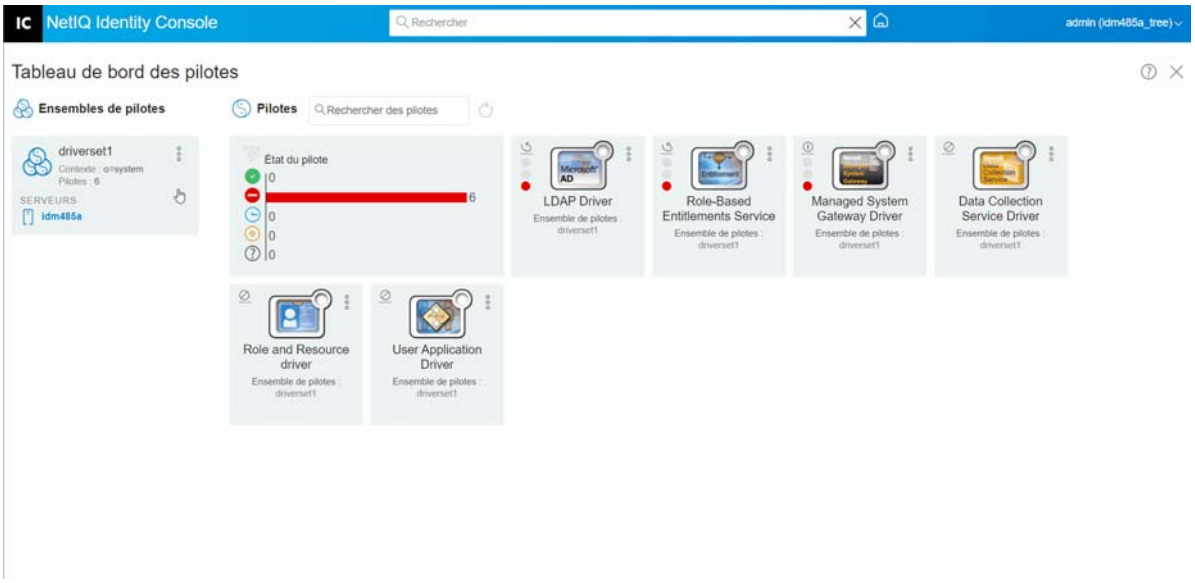
1. Dans Identity Console, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Avancé(e)** > **Bibliothèques**.
2. Sélectionnez la bibliothèque appropriée dans la liste.
3. Cliquez sur l'icône . Cliquez sur **OK** pour confirmer l'opération.

Affichage et suppression d'un objet de la bibliothèque

Vous pouvez afficher et supprimer des stratégies et des tables d'assignation à partir des objets Bibliothèque. Pour supprimer un objet, procédez comme suit :

1. Dans Identity Console, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Avancé(e)** > **Bibliothèques**.
2. Cliquez sur la bibliothèque appropriée dans la liste.
3. Pour supprimer une stratégie, sélectionnez l'onglet **Stratégies**.
4. Sélectionnez la stratégie appropriée dans la liste, puis cliquez sur l'icône .
5. Pour supprimer une table d'assignation, sélectionnez l'onglet **Tables d'assignation**.
6. Sélectionnez la table d'assignation appropriée dans la liste, puis cliquez sur l'icône .
7. Cliquez sur **OK** pour confirmer l'opération.

Figure 22-2 *Gestion des travaux et des bibliothèques pour un ensemble de pilotes*



Configuration des niveaux de consignation et de trace d'un ensemble de pilotes

Pour configurer la consignation et le suivi d'un ensemble de pilotes, sur la page principale d'Identity Console, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Configuration de la consignation et du suivi**. Cette section présente les tâches suivantes :

- « Configuration du niveau de consignation » page 149
- « Configuration du niveau de trace » page 150
- « Trace du script DirXML » page 151

Configuration du niveau de consignation

Chaque ensemble de pilotes possède un champ Niveau de consignation qui permet de définir le niveau d'erreurs à suivre. Le niveau que vous indiquez ici détermine quels messages sont disponibles pour les journaux. Par défaut, le niveau de consignation est défini pour le suivi des messages d'erreur (cela inclut également les messages d'erreur irrécupérable). Pour assurer le suivi d'autres types de messages, modifiez le niveau de consignation. Pour configurer le niveau de consignation, dans Identity Console, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Configuration de la consignation et du suivi** > **Niveau de consignation**. Le tableau ci-dessous décrit les paramètres de niveau de consignation :

Option	Description
Désactiver la consignation dans les journaux DriverSet, Subscriber et Publisher	Désactive la consignation pour tous les pilotes de l'objet Ensemble de pilotes, du canal Abonné et du canal Éditeur.

Option	Description
Nombre maximal d'entrées du journal (50-500)	Nombre d'entrées du journal. La valeur par défaut est 50.
Niveaux de consignation	Vous avez le choix parmi les niveaux de consignation suivants : ◆ **Consigner les erreurs** : consigne les erreurs uniquement. ◆ Consigner les erreurs et les avertissements : consigne les erreurs et les avertissements. ◆ **Consigner des événements spécifiques** : consigne les événements sélectionnés. Si vous sélectionnez cette option, la liste d'événements suivante est activée : ◆ **Événements du moteur méta-annuaire** ◆ **Événements d'état** ◆ **Événements de l'opération** ◆ **Événements de transformation** ◆ **Événements de provisioning de référence** ◆ **Mettre à jour l'heure de la dernière consignation uniquement** : met à jour l'heure de la dernière consignation. ◆ **Consignation désactivée** : désactive la consignation pour le pilote.

Configuration du niveau de trace

Vous pouvez configurer la trace pour un ensemble de pilotes spécifique. Selon le niveau de trace spécifié pour un ensemble de pilotes, la fonction de trace affiche les événements liés au pilote lorsque le moteur traite les événements. Le niveau de trace d'un pilote ne concerne que le pilote ou l'ensemble de pilotes dans lequel la trace est définie. Si vous utilisez le chargeur distant, le fichier de trace du chargeur distant est directement défini en conséquence et ne contient que la trace du module d'interface pilote.

Pour configurer la trace pour un ensemble de pilotes, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Configuration de la consignation et du suivi** > onglet **Trace**. Le tableau ci-dessous décrit les paramètres de trace :

Paramètre	Pilote
Niveau de trace	Plus le niveau de trace du pilote augmente, plus la quantité d'informations affichées dans Trace est importante. Le niveau de trace Un affiche les erreurs, mais pas leur cause. Pour afficher les informations de synchronisation du mot de passe, définissez le niveau de trace sur cinq. Si vous sélectionnez l'option **Utiliser le paramètre de l'ensemble de pilotes**, la valeur associée à l'ensemble de pilotes est utilisée.

Paramètre	Pilote
Niveau de trace XSL	Trace affiche les événements XLS. Ne définissez ce niveau de trace que lorsque vous corrigez les feuilles de style XSL. Si vous ne souhaitez pas afficher les informations XSL, définissez le niveau sur zéro.
Port de débogage Java	Permet aux développeurs de joindre un débogueur Java. Redémarrez le coffre-fort d'identité après avoir joint le débogueur Java.
Fichier de trace	Spécifiez le nom et l'emplacement du fichier dans lequel les informations Identity Manager sont écrites pour le pilote sélectionné. Si vous sélectionnez l'option **Utiliser le paramètre de l'ensemble de pilotes**, la valeur associée à l'ensemble de pilotes est utilisée.
Codage du fichier de trace	Le fichier de trace utilise le codage par défaut du système. Vous pouvez si vous le souhaitez spécifier un autre codage. Si vous sélectionnez l'option **Utiliser le paramètre de l'ensemble de pilotes**, la valeur associée à l'ensemble de pilotes est utilisée.
Taille maximum du fichier de trace	Permet de définir une limite pour le fichier de trace Java. Si vous définissez la limite de fichier sur Illimitée, la taille du fichier augmente jusqu'à ce qu'il n'y ait plus de place sur le disque. **REMARQUE :** si la limite de taille du fichier est spécifiée, le fichier de trace est créé dans plusieurs fichiers. Identity Manager divise automatiquement la taille de fichier maximale par dix et crée dix fichiers distincts. La taille combinée de ces fichiers est égale à la taille maximale du fichier de trace. Si vous sélectionnez l'option **Utiliser le paramètre de l'ensemble de pilotes**, la valeur associée à l'ensemble de pilotes est utilisée.

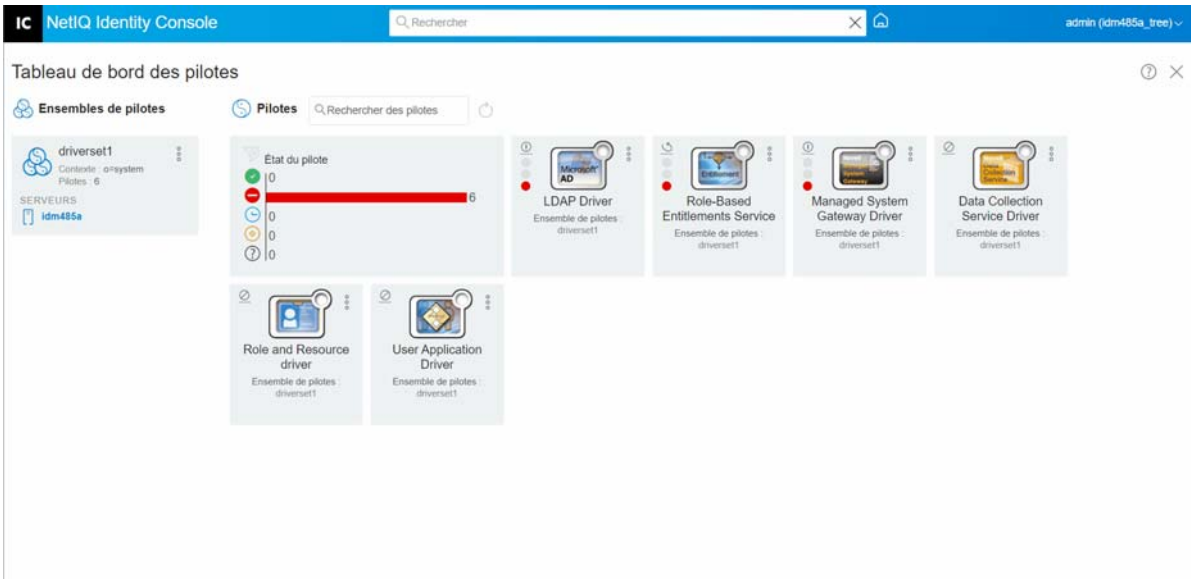
Trace du script DirXML

L'option de suivi du script DirXML permet de sélectionner un niveau de trace pour un ensemble de pilotes. La valeur sélectionnée est appliquée à toutes les stratégies de l'ensemble de pilotes. Vous avez le choix parmi les options de trace de script DirXML suivantes :

- Suivi du script DirXML activé
- Suivi du script DirXML désactivé
- Suivi de la règle de script DirXML activé
- Suivi de la règle de script DirXML désactivé

Cliquez sur  pour enregistrer les modifications.

Figure 22-3 *Gestion des niveaux de consignation et de trace d'un ensemble de pilotes*



Gestion de l'inspecteur et des statistiques des ensembles de pilotes

Vous pouvez utiliser l'inspecteur d'ensemble de pilotes pour afficher des informations détaillées sur les objets associés à un ensemble de pilotes. Cette section présente les tâches suivantes :

- « Affichage des statistiques d'un ensemble de pilotes » page 152
- « Affichage des informations sur la version » page 153
- « Affichage des statistiques d'association » page 154

Affichage des statistiques d'un ensemble de pilotes

Vous pouvez utiliser le portail Identity Console pour afficher diverses statistiques relatives à un seul pilote ou à un ensemble de pilotes. Il s'agit notamment de la taille du fichier de cache, de la taille des transactions non traitées dans le fichier de cache, des transactions les plus anciennes et les plus récentes, ainsi que du nombre total de transactions non traitées par catégorie (ajout, suppression, modification, etc.). Pour afficher les statistiques d'un ensemble de pilotes, procédez comme suit :

1. Dans Identity Console, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Inspecteur et statistiques** > **Statistiques**.
2. Sélectionnez le serveur approprié dans la liste déroulante.

   La page qui s'affiche vous permet de consulter les statistiques de tous les pilotes contenus dans l'ensemble de pilotes.

   - Pour rafraîchir les statistiques, cliquez sur l'icône .
   - Pour fermer les statistiques d'un pilote, cliquez sur le bouton situé dans le coin supérieur droit de la fenêtre des statistiques du pilote.

- Pour ouvrir les statistiques de tous les pilotes, cliquez sur **Opérations** > **Tout afficher**.
- Pour réduire la liste des transactions non traitées pour un pilote, cliquez sur le bouton situé au-dessus de la liste. Pour réduire la liste des transactions non traitées pour tous les pilotes, cliquez sur **Opérations** > **Réduire toutes les transactions**.
- Pour développer la liste des transactions, cliquez sur le bouton . Pour développer la liste des transactions non traitées pour tous les pilotes, cliquez sur **Opérations** > **Développer toutes les transactions**.
- Pour fermer le tableau de bord des statistiques pour les pilotes désactivés, cliquez sur **Opérations**, puis sélectionnez **Close Disabled Drivers** (Fermer les pilotes désactivés).

Affichage des informations sur la version

Le moteur Identity Manager, les modules d'interface pilote et les fichiers de configuration de pilote contiennent chacun un numéro de version distinct. L'option Identification de la version d'Identity Console vous permet de connaître les versions du moteur Identity Manager et des modules d'interface pilote. Les fichiers de configuration de pilote contiennent leur propre convention de dénomination. Pour afficher les informations de version, procédez comme suit :

1. Dans Identity Console, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Inspecteur et statistiques** > **Identification de la version**.
2. Affichez une vue de niveau supérieur des informations de version :
   - L'arborescence eDirectory pour laquelle vous êtes authentifié.

     REMARQUE : eDirectory est appelé le « coffre-fort d'identité » lorsqu'il est utilisé dans l'environnement Identity Manager.
   - L'ensemble de pilotes que vous avez sélectionné.
   - Les serveurs associés à l'ensemble de pilotes.

     Si l'ensemble de pilotes est associé à plusieurs serveurs, vous pouvez afficher les informations Identity Manager sur chaque serveur.
   - Pilotes
3. Cliquez sur l'icône **Afficher** pour afficher une représentation textuelle des informations contenues dans la vue de niveau supérieur.
4. Cliquez sur le bouton Exporter pour exporter et enregistrer le texte dans un fichier situé sur votre unité locale ou réseau.

Affichage des statistiques d'association

La fonction Statistiques d'association d'Identity Manager permet de consulter les détails d'association des identités gérées par Identity Manager. Identity Manager utilise ces statistiques pour obtenir le nombre d'associations pour les pilotes Identity Manager.

Pour obtenir les objets actifs, inactifs et gérés par le système pour un pilote, exécutez le travail de statistiques d'association. Vous pouvez planifier le travail de statistiques d'association pour une exécution quotidienne, hebdomadaire, mensuelle ou annuelle. Par défaut, il est planifié pour s'exécuter chaque semaine.

Le tableau de bord Statistiques d'association affiche les détails d'association. Vous pouvez également afficher ces détails en exportant les associations dans un fichier.

REMARQUE

- Le nombre d'associations pour les pilotes est déterminé pour chaque serveur. Si un objet est associé à plusieurs pilotes, le nombre d'associations est calculé de manière unique pour chaque pilote.
- Si vous avez plus de 200 000 associations, il est recommandé de définir la taille de segment maximale du pilote sur une valeur supérieure ou égale à 2 Go. Pour plus d'informations sur la définition de la taille de segment, reportez-vous à la section « Configuration des paramètres d'environnement Java » page 144.

Pour afficher les statistiques d'association, procédez comme suit :

1. Dans Identity Console, sélectionnez **Administration IDM** > **cliquez sur le menu contextuel (trois points) de l'ensemble de pilotes concerné** > **Propriétés de l'ensemble de pilotes** > **Inspecteur et statistiques** > **Statistiques d'association**.
2. Sélectionnez le serveur pour lequel vous souhaitez exécuter les statistiques d'association.
3. Le nombre d'associations affiche le résultat calculé précédent.

   Identity Console affiche le nombre d'associations pour les objets actifs, inactifs et gérés par le système pour tous les pilotes associés à l'ensemble de pilotes.

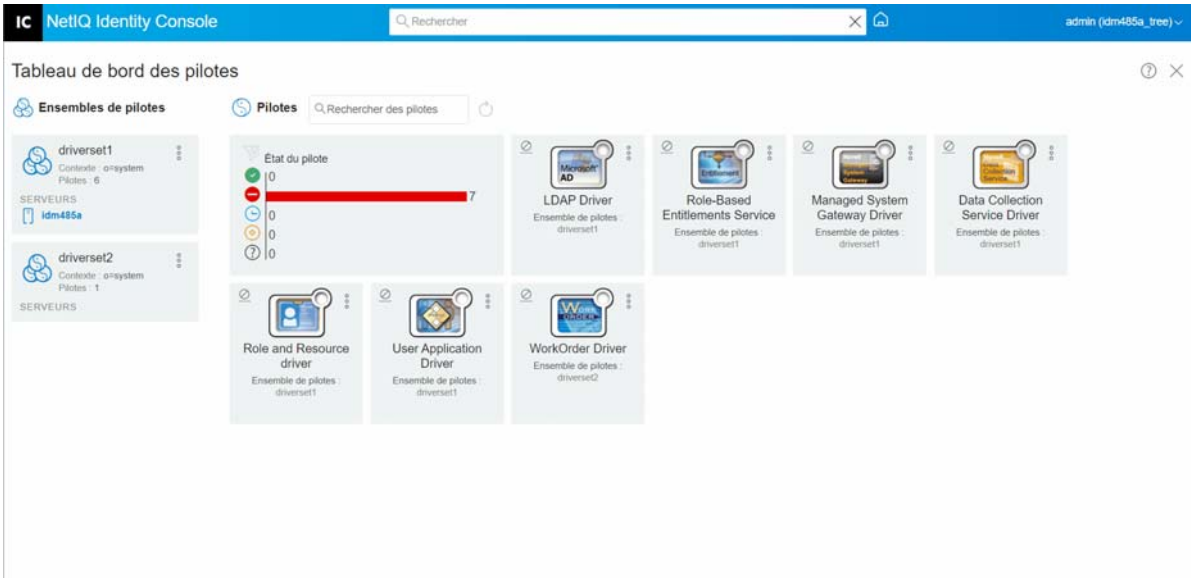
   Identity Console assimile les groupes et les unités d'organisation à des objets gérés par le système. Identity Console considère qu'un objet est inactif si son attribut `Connexion désactivée` a la valeur true (vrai) et que l'objet n'a pas été modifié au cours des 120 derniers jours. Tous les objets restants sont considérés comme des objets gérés actifs.
4. Cliquez sur l'icône pour obtenir les résultats mis à jour.

   Lorsqu'un pilote est désactivé sur le serveur, Identity Console ne l'affiche pas dans le tableau de bord.
5. Cliquez sur l'icône pour exporter les informations sur le système et sur le nombre d'associations pour les pilotes associés au serveur.
6. Pour exporter les objets associés à un pilote spécifique, cliquez sur en regard des objets requis, puis enregistrez le fichier.

REMARQUE : dans le cas de pilotes Fan-out, seuls les objets uniques sont exportés. Si un objet est associé à plusieurs instances d'un pilote Fan-out, Identity Console affiche tous les nombres d'associations dans le tableau de bord. Toutefois, si vous choisissez d'exporter les objets dans un fichier, Identity Console exporte uniquement les objets uniques.

7 Cliquez sur **Opérations**, puis sélectionnez l'option souhaitée pour organiser le tableau de bord du nombre d'associations.

Figure 22-4 *Gestion des statistiques d'un ensemble de pilotes*



23 Gestion des propriétés des pilotes

Cette section fournit des informations sur les propriétés communes à tous les pilotes. Elle aborde toutes les propriétés (Mot de passe nommé, Valeurs de contrôle du moteur, Niveau de consignation, etc.).

Les informations d'activation d'un pilote s'affichent et vous rappellent d'activer l'expiration du pilote.

Pour modifier la configuration d'un pilote, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'onglet **Pilotes**.
2. Cliquez sur la vignette du pilote concerné pour afficher la page de configuration correspondante.

   Par défaut, la page **Paramètres de connexion** s'affiche. Les options de configuration du pilote sont les suivantes :

Paramètres de connexion

Les paramètres de connexion déterminent si le pilote doit être exécuté en local ou à distance.

- **Java :** cette option permet de spécifier le nom de la classe Java instanciée pour le composant de module d'interface du pilote. Cette classe peut se trouver dans le répertoire classes sous la forme d'un fichier de classe ou dans le répertoire `lib` sous la forme d'un fichier `.jar`. Sélectionnez cette option pour exécuter le pilote en local. Vous devez également spécifier le mot de passe de l'objet Pilote et la limite de cache du pilote. Pour définir un nouveau mot de passe, cliquez sur le lien **Définir un mot de passe**.

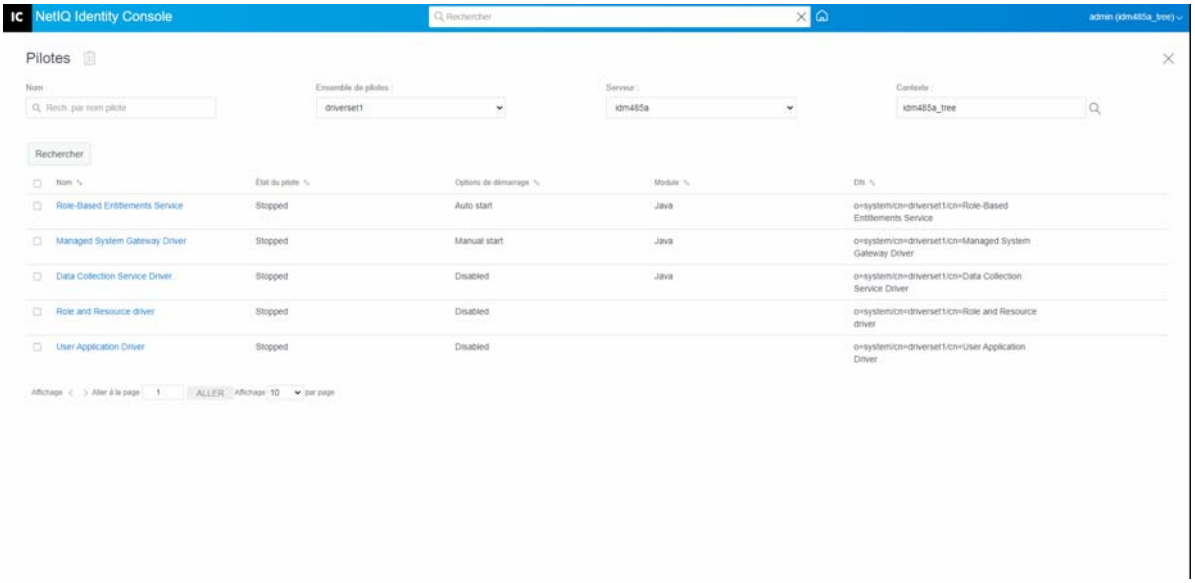
  Par exemple : `com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim`.
- **Natif :** cette option permet de spécifier le nom du fichier `.dll` développé dans un langage natif (tel que C++) pour le pilote. Vous devez également spécifier le mot de passe de l'objet Pilote et la limite de cache du pilote. Pour définir un nouveau mot de passe, cliquez sur le lien **Définir un mot de passe**.

  Par exemple : `addriver.dll`.

- **Se connecter au chargeur distant :** cette option est utilisée lorsque le pilote se connecte à distance au système connecté. Si vous sélectionnez cette option, vous devez spécifier les sous-options suivantes :
  - **Paramètres de connexion au chargeur distant** : indiquez les informations détaillées sur l'environnement du chargeur distant, comme le nom d'hôte et le port de connexion.
  - **Mot de passe du chargeur distant** : indiquez le mot de passe du chargeur distant.
  - **Mot de passe de l'objet Pilote** : indiquez le mot de passe de l'objet Pilote. Si vous utilisez le chargeur distant, vous devez entrer un mot de passe sur cette page. Le chargeur distant se sert de ce mot de passe pour s'authentifier auprès du module d'interface pilote distant.
- **Authentification** : les paramètres d'authentification sont utilisés pour authentifier le moteur Identity Manager et les serveurs du chargeur distant. spécifiez les paramètres suivants.
  - **ID d'authentification** : indiquez un ID d'application utilisateur. Cet ID permet de transmettre les informations d'abonnement du coffre-fort d'identité à l'application.
  - **Contexte d'authentification** : indiquez l'adresse IP ou le nom du serveur avec lequel le module d'interface d'application doit communiquer.
  - **Mot de passe de l'application** : définissez le mot de passe d'authentification de l'application.

Lorsque vous avez terminé, cliquez sur l'icône pour enregistrer la configuration.

Figure 23-1 *Gestion des paramètres de connexion*



Configuration de pilote

La section de configuration du pilote permet de configurer les paramètres spécifiques du pilote, les valeurs de contrôle du moteur, les valeurs de configuration globale, etc. Lorsque vous modifiez les paramètres d'un pilote, vous adaptez le comportement de celui-ci à votre environnement réseau. Cette section présente les tâches suivantes :

Paramètres de pilote

Les paramètres d'un pilote sont divisés en paramètres du pilote, paramètres d'abonné et paramètres de l'éditeur. Ces paramètres sont remplis en fonction de la configuration de votre pilote. Pour plus d'informations sur les paramètres des pilotes, reportez-vous au guide consacré au pilote spécifique dans la documentation relative aux pilotes Identity Manager.

Lorsque vous avez terminé, cliquez sur le lien pour enregistrer les paramètres. Si vous souhaitez définir les paramètres sur leur valeur par défaut, cliquez sur l'icône . Pour modifier la configuration du pilote à l'aide du fichier XML, cliquez sur l'icône .

Global Configuration Values (Valeurs de configuration globales)

Cette option affiche une liste ordonnée des objets Configuration globale. Les objets contiennent les définitions de valeurs de configuration globale (VCG) d'extension pour le pilote qu'Identity Manager charge au démarrage du pilote. Vous pouvez afficher ou modifier les objets sous l'onglet **Valeurs de configuration globale** à l'aide de l'éditeur XML. Cliquez sur l'icône pour enregistrer les VCG. Pour rafraîchir la liste de VCG, cliquez sur l'icône . Pour supprimer une VCG, sélectionnez l'objet GCV approprié, puis cliquez sur l'icône .

Valeurs de contrôle du moteur

Les valeurs de contrôle du moteur permettent de modifier certains comportements par défaut du moteur Identity Manager. Ces valeurs ne sont accessibles que si un serveur est associé à l'objet Ensemble de pilotes.

Option	Description
Subscriber channel retry interval in seconds (Intervalle de réessai du canal Abonné (en secondes))	L'intervalle de réessai du canal Abonné détermine la fréquence à laquelle le moteur Identity Manager effectue un nouveau traitement d'une transaction mise en cache après que l'objet Abonné du module d'interface d'application renvoie un état de réessai.
Qualified form for DN-syntax attribute values (Format complet des valeurs de l'attribut DN-syntax)	La spécification complète des valeurs de l'attribut DN-syntax détermine si ces valeurs sont présentées selon un format complet ou non complet avec barre oblique. Le paramètre « True » (Vrai) signifie que les valeurs sont présentées au format complet.
Qualified form from rename events (Format complet des événements de changement de nom)	Le format complet des événements de changement de nom détermine si la partie de nouveau nom des événements de changement de nom provenant du coffre-fort d'identité est présentée au canal Abonné avec des qualificatifs de type. Exemple : CN=. Le paramètre « True » (Vrai) signifie que les noms sont présentés au format complet.
Maximum eDirectory replication wait time in seconds (Temps d'attente maximal de réplication d'eDirectory (en secondes))	Ce contrôle détermine le temps maximal pendant lequel le moteur Identity Manager attend qu'une modification particulière soit répliquée entre la réplique locale et une réplique distante. Cela ne concerne que les opérations pour lesquelles le moteur Identity Manager doit contacter un serveur eDirectory distant dans la même arborescence et peut devoir attendre la réplication d'une modification vers ou à partir du serveur distant pour que l'opération puisse être effectuée (par exemple, déplacement d'un objet lorsque le serveur Identity Manager ne contient pas la réplique maîtresse de l'objet déplacé ou opérations de droits sur le système de fichiers pour les utilisateurs créés à partir d'un modèle).
Use non-compliant backwards-compatible mode for XSLT (Utiliser un mode non conforme de compatibilité avec les versions précédentes pour XSLT)	Ce contrôle met le processeur XSLT utilisé par le moteur Identity Manager en mode de compatibilité avec les versions précédentes. Dans ce mode, le processeur XSLT utilise un ou plusieurs comportements non conformes aux normes XPath 1.0 et XSLT 1.0. Ce contrôle est prévu à des fins de compatibilité avec les versions précédentes pour les feuilles de style DirXML existantes qui dépendent des comportements non standard. Par exemple, le comportement de l'opérateur XPath « != » lorsqu'un opérande est un ensemble de nœuds et que l'autre n'est pas un ensemble de nœuds est incorrect dans les versions DirXML jusqu'à Identity Manager 2.0 y compris. Ce comportement a été corrigé, mais il est toutefois désactivé par défaut grâce à ce contrôle en faveur de la compatibilité avec les versions précédentes pour les feuilles de style DirXML existantes.
Maximum application objects to migrate at once (Nombre maximal d'objets Application à migrer simultanément)	Ce contrôle sert à limiter le nombre d'objets Application que le moteur Identity Manager demande à partir d'une application au cours d'une requête unique effectuée dans le cadre d'une opération de migration d'objets à partir de l'application. Si des erreurs java.lang.OutOfMemoryError se produisent au cours d'une opération de migration à partir de l'application, ce nombre doit être défini sur une valeur inférieure à celle par défaut. La valeur par défaut est 50. **REMARQUE :** ce contrôle ne limite pas le nombre d'objets Application pouvant être migrés ; il limite simplement la taille du lot.

Option	Description
Set creatorsName on objects created in Identity Vault (Définir creatorsName sur les objets créés dans le coffre-fort d'identité)	Ce contrôle est utilisé par le moteur Identity Manager pour déterminer si l'attribut creatorsName doit être défini sur le DN de ce pilote sur tous les objets créés par ce pilote dans le coffre-fort d'identité. La définition de l'attribut creatorsName permet d'identifier facilement les objets créés par ce pilote, mais avec une perte de performances. S'il n'est pas défini, l'attribut creatorsName prend par défaut la valeur du DN de l'objet Serveur NCP qui héberge le pilote.
Write pending associations (Écrire les associations en attente)	Ce contrôle détermine si le moteur Identity Manager écrit une association en attente sur un objet lors du traitement du canal Abonné. L'écriture d'une association en attente n'apporte que peu d'avantages, voire aucun, mais elle entraîne une perte de performances. Néanmoins, il est possible de l'activer à des fins de compatibilité avec les versions précédentes.
Use password event values (Utiliser les valeurs d'événement lié au mot de passe)	Ce contrôle détermine la source de la valeur indiquée pour l'attribut nspmDistributionPassword pour les événements d'ajout et de modification du canal Abonné. Le paramètre False (Faux) signifie que la valeur actuelle de nspmDistributionPassword est obtenue et indiquée comme étant la valeur de l'événement de l'attribut. En d'autres termes, seule la valeur du mot de passe actuel est disponible. Cette représente l'opération par défaut. Le paramètre True (Vrai) signifie que la valeur indiquée avec l'événement eDirectory est déchiffrée et indiquée comme étant la valeur de l'événement de l'attribut. En d'autres termes, l'ancienne valeur de mot de passe (le cas échéant) et la valeur du mot de passe de rechange au moment de l'événement sont disponibles. Ainsi, vous pouvez synchroniser les mots de passe dans certaines applications qui requièrent l'ancien mot de passe pour permettre la configuration d'un nouveau mot de passe.
Retry Out of Band events (Réessayer les événements hors limite)	Ce contrôle détermine si les événements de synchronisation hors limite doivent être réessayés ou non si l'état **retry** (réessayer) est reçu pour l'événement de synchronisation hors limite. Si le contrôle a la valeur False (Faux), la synchronisation hors limite n'est pas réessayée. S'il a la valeur True (Vrai), la synchronisation hors limite est réessayée jusqu'à ce qu'elle réussisse.
Use Rhino ECMAScript engine (Utiliser le moteur ECMAScript Rhino)	Détermine si le moteur Identity Manager utilise le moteur ECMAScript Rhino. Le moteur utilise Rhino comme moteur ECMAScript par défaut. La valeur par défaut de ce contrôle est **true** (vrai). Si vous lui assignez la valeur **false** (faux), le moteur utilise le script Nashorm.
Enable Subscriber Service Channel (Activer le canal du service Abonné)	Détermine si le moteur Identity Manager traite les requêtes hors limite sur le canal du service Abonné du pilote. Voici quelques exemples courants de ces requêtes : rafraîchissement d'une carte de code, collecte de données et requêtes déclenchées à partir de dxcmd. Lorsque ce contrôle a la valeur true (vrai), le canal traite séparément ces requêtes sans interrompre le traitement normal des événements. Ce contrôle n'est actuellement disponible qu'avec le pilote Fan-out JDBC (activé par défaut).

Option	Description
Enable password synchronization status reporting (Activer la création de rapports d'état de synchronisation des mots de passe)	Ce contrôle détermine si le moteur Identity Manager signale l'état des événements de changement de mot de passe du canal Abonné. La création de rapports de l'état des événements de changement de mot de passe du canal Abonné permet à des applications telles que l'application utilisateur Identity Manager de surveiller l'avancement de la synchronisation d'un changement de mot de passe à synchroniser avec l'application connectée.
Combine values from template object with those from add operation (Combiner les valeurs d'un objet Modèle à celles d'une opération d'ajout)	Ce contrôle détermine si le moteur Identity Manager combine les valeurs similaires d'un modèle de création et d'une opération d'ajout lors de l'opération d'ajout. La définition de la valeur sur Vrai provoque l'utilisation des valeurs d'attribut à plusieurs valeurs du modèle en plus des valeurs du même attribut spécifiées dans l'opération d'ajout. La définition de la valeur False (Faux) ignore les valeurs du modèle si des valeurs du même attribut sont spécifiées dans l'opération d'ajout.
Allow event loopback from publisher to subscriber channel (Autoriser le bouclage d'événements du canal Éditeur vers le canal Abonné)	Ce contrôle détermine si le moteur Identity Manager autorise le bouclage d'un événement du canal Éditeur du pilote vers le canal Abonné. Si la valeur est False (Faux), le moteur Identity Manager n'autorise pas le bouclage des événements. Si la valeur est True (Vrai), le moteur Identity Manager autorise le bouclage des événements du canal Éditeur vers le canal Abonné.
Revert to calculated membership value behavior (Rétablir le comportement des valeurs d'adhésion calculées)	Ce contrôle détermine la méthode utilisée par le moteur Identity Manager lors des opérations de lecture et de recherche liées à l'adhésion à un groupe. Si la valeur est False (Faux, par défaut), le moteur Identity Manager, lors de la lecture ou de la recherche des attributs Membre et Adhésion à un groupe dans les objets du coffre-fort d'identité, ne renvoie que les valeurs « statiques ». Les valeurs statiques sont des objets ayant reçu une adhésion au groupe par assignation directe au groupe plutôt que par héritage via un groupe imbriqué. Si la valeur est True (Vrai), le moteur Identity Manager rétablit la méthode utilisée avant Identity Manager 3.6. Dans ce cas, les recherches du moteur Identity Manager sur les attributs Membre et Adhésion à un groupe renvoyaient toutes les valeurs « calculées ». Les valeurs calculées comprennent des objets qui 1) reçoivent une adhésion de manière statique ou 2) reçoivent l'adhésion de manière dynamique en vertu des calculs de hiérarchie de groupe imbriqué utilisés par eDirectory. La recherche d'un attribut Membre d'un groupe renvoie alors tous les objets directement assignés au groupe ou dont l'appartenance a été assignée via un groupe imbriqué.
Maximum time to wait for driver shutdown in seconds (Temps d'attente maximal de l'arrêt du pilote (en secondes))	Ce contrôle détermine le temps maximal pendant lequel le moteur Identity Manager attend l'arrêt du canal Éditeur du pilote. Si le pilote ne s'arrête pas dans le délai spécifié, le moteur Identity Manager y met fin.

Option	Description
Regular Expression escape meta-characters (Méta-caractères d'échappement d'expression régulière)	Ce contrôle détermine les méta-caractères qui sont échappés lors de l'extension de la variable locale en cas d'utilisation dans un contexte d'expression régulière. Tous les caractères à échapper doivent être ajoutés sous la forme d'une liste séparée par des virgules pour cette valeur de contrôle. Si un méta-caractère n'est pas présent dans la valeur de contrôle, il n'est pas échappé lors de l'extension de la variable locale qui contient une expression régulière. Lorsque vous utilisez ce contrôle, veillez à respecter les points suivants : ◆ La valeur n'est pas vide. Le caractère par défaut est ***$***. Ce caractère est requis pour l'extension de la variable locale. ◆ La valeur doit être une liste valide séparée par des virgules (,), faute de quoi des erreurs se produiront lors de l'évaluation de la stratégie. ◆ Pour échapper tous les méta-caractères, spécifiez la valeur « \,$,^,.,?,*,+,[,],(,),| ». ◆ Si un méta-caractère ne doit pas être échappé, supprimez-le de la valeur. ◆ Pour échapper un méta-caractère, faites-le suivre d'une barre oblique (\).
Ignore Entitlement Changes of other drivers (Ignorer les modifications de droit des autres pilotes)	Ce contrôle détermine si le moteur Identity Manager ignore ou traite les modifications de droit des autres pilotes. La valeur par défaut est True. Le pilote ignore alors automatiquement les modifications de droit des autres pilotes. Si ce contrôle a la valeur False (Faux), les modifications de droit des autres pilotes sont mises en cache et traitées par ce pilote.
Allow Entitlement event loopback from cprs to subscriber channel (Autoriser le bouclage d'événements de droit de cprs vers le canal Abonné)	Ce contrôle détermine si le moteur Identity Manager autorise le bouclage d'un événement de droit généré par une assignation CPRS vers le canal Abonné du pilote. La valeur par défaut est False. L'événement n'est alors pas bouclé vers le canal Abonné. Si ce contrôle a la valeur True (Vrai), l'événement est transmis au canal Abonné du pilote.

Options de démarrage

Les options de démarrage permettent de définir l'état d'un pilote au démarrage du serveur Identity Manager.

- **Démarrage automatique** : le pilote démarre à chaque démarrage du serveur Identity Manager.
- **Manuel(le)** : le pilote ne démarre pas au démarrage du serveur Identity Manager. Vous devez le démarrer à l'aide du portail Identity Console.
- **Désactivé(e)** : le pilote dispose d'un fichier de cache qui stocke tous les événements. Lorsque vous sélectionnez l'option Désactivé(e) pour le pilote, ce fichier est supprimé et aucun nouvel événement n'est stocké dans le fichier tant que l'état du pilote n'est pas remplacé par Manuel(le) ou Démarrage automatique.

Après avoir choisi l'option de démarrage souhaitée, cliquez sur l'icône pour l'enregistrer. Pour réinitialiser l'option de démarrage, cliquez sur l'icône .

Mot de passe nommé

Identity Manager vous permet de stocker en toute sécurité plusieurs mots de passe pour un pilote. Cette fonction est appelée « mots de passe nommés ». Chaque mot de passe est accessible par l'intermédiaire d'une clé ou d'un nom.

Vous pouvez ajouter des mots de passe nommés à un ensemble de pilotes ou à un pilote spécifique. Les mots de passe nommés d'un ensemble de pilotes sont disponibles pour tous les pilotes de l'ensemble, tandis que ceux d'un pilote ne sont disponibles que pour ce pilote.

Pour utiliser un mot de passe nommé dans une règle de pilote, désignez-le par le nom du mot de passe au lieu d'utiliser le mot de passe réel. Le moteur Identity Manager envoie alors le mot de passe au pilote. Vous pouvez utiliser la méthode décrite dans cette section pour la mémorisation et la récupération des mots de passe nommés, avec n'importe quel pilote, sans apporter de modification au module d'interface pilote.

Pour ajouter un nouveau mot de passe nommé, cliquez sur l'icône . Pour supprimer un mot de passe nommé existant, cliquez sur l'icône . Pour enregistrer la liste, cliquez sur l'icône .

Équivalents de sécurité

La page Équivalents de sécurité vous permet d'afficher ou de modifier la liste des objets avec lesquels le pilote dispose d'une équivalence de sécurité explicite. Cet objet dispose en effet de tous les droits des objets indiqués.

Pour ajouter un nouvel objet à la liste d'équivalents de sécurité, cliquez sur l'icône . Si vous ajoutez ou supprimez un objet dans la liste, le système l'ajoute ou le supprime automatiquement dans la propriété « Sécurité égale à moi » de cet objet. Il n'est pas nécessaire d'ajouter l'ayant droit [Public] ni les conteneurs parent de cet objet à la liste, car cet objet dispose déjà implicitement d'une équivalence de sécurité.

Pour supprimer un objet existant de cette liste, cliquez sur l'icône . Pour enregistrer la liste, cliquez sur l'icône .

Objets exclus

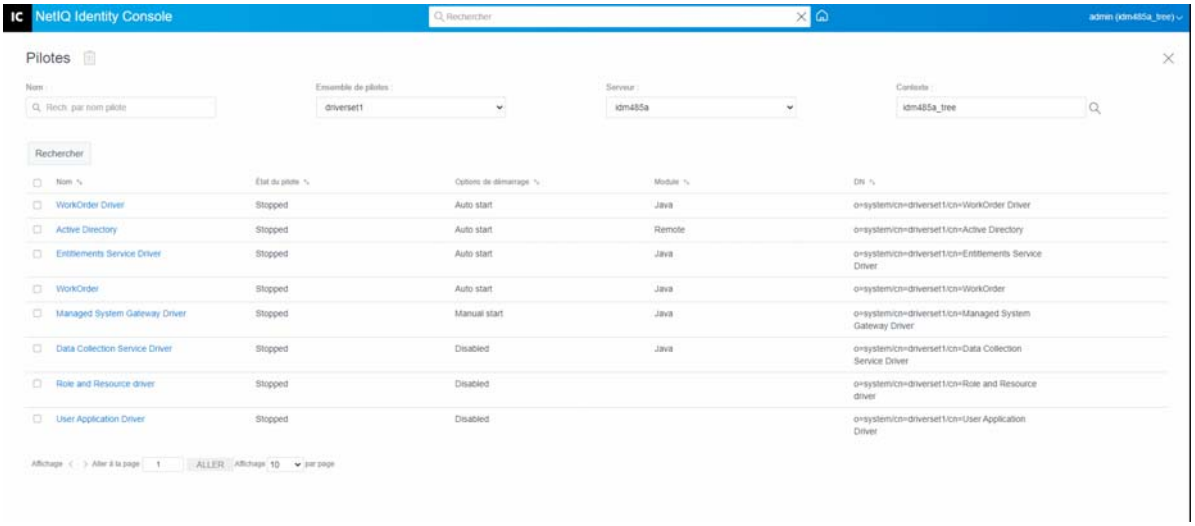
Cette option permet de créer une liste d'objets qui ne seront pas répliqués dans l'application. Nous vous recommandons d'ajouter dans cette liste tous les objets qui représentent un rôle administratif (par exemple, l'objet Admin). Pour ajouter un objet à cette liste, cliquez sur l'icône . Pour supprimer un objet existant de cette liste, cliquez sur l'icône . Pour enregistrer la liste, cliquez sur l'icône .

Gestion de la liste des attributs avec valeur

Pour ajouter des attributs à la liste des attributs avec valeur pour un pilote spécifique, procédez comme suit :

1. Dans Identity Console, sélectionnez le module **Gestion des objets**.
2. Sélectionnez le type **Dir-XML-Driver** dans la liste déroulante, puis cliquez sur le bouton Rechercher.
3. Cliquez sur le pilote approprié dans la liste de recherche.
4. Pour ajouter des attributs sans valeur à la liste des attributs avec valeur, cliquez sur l'icône + située en regard des **attributs avec valeur**, puis sélectionnez les attributs sans valeur appropriés dans la liste.
5. Lorsque vous avez terminé, cliquez sur **OK**.

Figure 23-2 *Gestion de la configuration des pilotes*



Transformation et synchronisation des données

Cette section présente les tâches suivantes :

- « Vue de synchronisation des données » page 165
- « Filtres d'attributs de classe » page 168
- « Script ECMA » page 169
- « Assignation d'attributs réciproque » page 169

Vue de synchronisation des données

La page de présentation du pilote contient les fonctions suivantes :

- « Filtre » page 166
- « Toutes les stratégies » page 166

- « Migrer les données vers le coffre-fort d'identité » page 166
- « Migration des données à partir du coffre-fort d'identité » page 167
- « Synchroniser les objets » page 167
- « Trace du script DirXML » page 167

Filtre

Les filtres présents sur le pilote permettent d'indiquer les classes et attributs qu'une application peut échanger avec le coffre-fort d'identité. Pour qu'une classe spécifique soit traitée par le moteur méta-annuaire, ajoutez-la au filtre du canal approprié. Vous pouvez également filtrer les objets en fonction d'une valeur d'attribut que vous définissez.

Pour ajouter des classes et des attributs à inclure pour la synchronisation et modifier le filtre de pilotes, cliquez sur **Filtre** sur le canal Éditeur ou Abonné.

REMARQUE : la représentation graphique de la présentation montre deux objets distincts pour le filtre du pilote sur les canaux Éditeur et Abonné. Bien que deux objets soient affichés, le même filtre est utilisé pour les deux canaux.

Toutes les stratégies

Par défaut, la page Toutes les stratégies est affichée. Pour importer une stratégie existante dans le conteneur, cliquez sur l'icône  . Vous pouvez également supprimer une stratégie qui n'est plus utile. Pour sélectionner un niveau de trace pour votre pilote, cliquez sur l'icône  . Pour déplacer les stratégies vers le haut ou vers le bas dans la liste, utilisez les icônes  et  .

REMARQUE : L'ajout et le déploiement de nouvelles stratégies pour les pilotes ne sont pas pris en charge dans Identity Console. Il est recommandé d'utiliser iManager et Identity Designer pour ajouter et déployer de nouvelles stratégies.

Migrer les données vers le coffre-fort d'identité

Grâce à cette tâche, vous pouvez définir les critères qu'Identity Manager utilise pour migrer les objets d'une application vers le coffre-fort d'identité. Lorsque vous migrez un objet, le moteur Metadirectory applique à l'objet toutes les stratégies de concordance, de placement et de création, ainsi que le filtre Éditeur. Les objets sont migrés vers le coffre-fort d'identité selon l'ordre indiqué dans la liste des classes. Vous pouvez effectuer les tâches suivantes :

1. **Ajouter une classe et des attributs** : pour ajouter ou supprimer des classes et des attributs à migrer, cliquez sur l'icône  . Sélectionnez ensuite la classe et les attributs correspondants à ajouter. Après avoir sélectionné la classe et les attributs souhaités, cliquez sur **Ajouter** pour enregistrer les modifications apportées.
2. **Éditer la valeur d'un attribut** : pour modifier la valeur d'un attribut de migration définie lors de l'édition de la liste, cliquez sur l'icône  Éditer l'attribut.

3 **Réorganiser la liste des classes** : utilisez les boutons ↑ et ↓ pour modifier l'ordre des classes de la liste. Les objets sont migrés vers le coffre-fort d'identité selon l'ordre indiqué dans la liste des classes.

4 **Rafraîchir** : cliquez sur l'icône ⟳ pour rafraîchir la liste.

Migration des données à partir du coffre-fort d'identité

L'onglet **Exporter** permet de sélectionner les conteneurs ou les objets à migrer du coffre-fort d'identité vers une application. Lorsque vous migrez un objet, le moteur méta-annuaire applique à l'objet toutes les stratégies de concordance, de création et de placement, ainsi que le filtre Abonné.

Pour migrer des objets ou des conteneurs du coffre-fort d'identité vers une autre application, cliquez sur l'icône +. Recherchez et sélectionnez l'objet à migrer, puis cliquez sur **OK** pour l'ajouter à la liste de migration. Pour supprimer un objet de la liste de migration, cliquez sur l'icône 🗑.

Une fois les objets à migrer sélectionnés, cliquez sur ▷ pour démarrer la migration. L'avancement de la migration s'affiche à l'écran. Si vous souhaitez arrêter la migration, cliquez sur le bouton ⊡.

Synchroniser les objets

L'opération de synchronisation recherche les objets modifiés et les synchronise. Sélectionnez **Examiner tous les objets** pour lancer immédiatement la synchronisation. Vous pouvez également définir les date/heure de démarrage de la synchronisation.

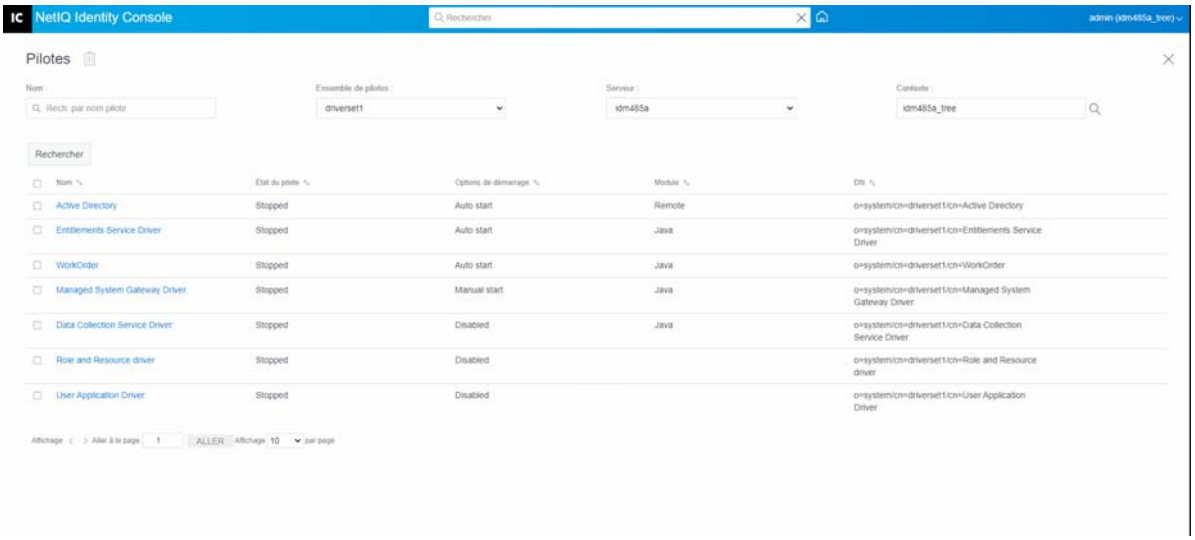
Trace du script DirXML

L'option de suivi du script DirXML permet de sélectionner un niveau de trace pour un pilote. Elle applique également les paramètres de trace à tous les canaux Éditeur et Abonné. Vous avez le choix parmi les options de trace de script DirXML suivantes :

- Suivi du script DirXML activé
- Suivi du script DirXML désactivé
- Suivi de la règle de script DirXML activé
- Suivi de la règle de script DirXML désactivé

Cliquez sur 💾 pour enregistrer les modifications.

Figure 23-3 *Gestion de la synchronisation des données des pilotes*



Filtres d'attributs de classe

Les filtres d'attributs de classe permettent de spécifier les classes et les attributs qu'une application peut échanger avec le coffre-fort d'identité. Pour qu'une classe spécifique soit traitée par le moteur méta-annuaire, ajoutez-la au filtre du canal approprié. Vous pouvez également filtrer les objets en fonction d'une valeur d'attribut que vous définissez. Vous pouvez effectuer les opérations suivantes :

- **Définir un modèle** : cette option permet de définir les options par défaut de tous les attributs ajoutés au filtre. Cliquez sur l'icône située en regard du libellé Filtres d'attributs de classe.
- **Ajouter une classe** : cliquez sur l'icône pour ajouter une nouvelle classe.
- **Ajouter un attribut** : cliquez sur l'icône pour ajouter un nouvel attribut.
- **Copier le filtre depuis** : cette option permet de copier un filtre à partir d'un autre pilote. Cliquez sur l'icône pour copier le filtre.
- **Éditer le fichier XML** : cette option permet d'éditer les paramètres de filtre de classes et d'attributs. Pour cela, cliquez sur l'icône Éditer le fichier XML .
- **Supprimer une classe ou un attribut** : pour supprimer une classe ou un attribut, cliquez sur l'icône située en regard de la classe ou de l'attribut correspondant.

Vous pouvez définir les options suivantes pour une valeur de classe et d'attribut sur les canaux Éditeur et Abonné :

- Synchroniser
- Ignorer
- Notifier
- Réinitialiser

Autorité de fusion

Si aucun attribut n'est en cours de synchronisation dans l'un ou l'autre des canaux, aucune fusion ne se produit.

Si un attribut est en cours de synchronisation dans l'un des canaux mais pas dans l'autre, toutes les valeurs existantes de la destination de ce canal sont supprimées et remplacées par celles de la source du canal en question. Si la source a plusieurs valeurs et si la destination ne peut en avoir qu'une, une seule des valeurs est utilisée du côté de la destination.

Si un attribut est synchronisé dans les deux canaux et si les deux côtés ne peuvent accueillir qu'une valeur, l'application connectée acquiert les valeurs stockées dans le coffre-fort d'identité, sauf s'il n'en contient pas. Dans ce scénario, le coffre-fort d'identité acquiert les valeurs à partir de l'application connectée.

Si un attribut est en cours de synchronisation dans les deux canaux et si un seul côté peut avoir plusieurs valeurs, la valeur du canal à une seule valeur est ajoutée au canal à plusieurs valeurs si elle ne s'y trouve pas déjà. Si aucune valeur ne se trouve du côté ne pouvant en avoir qu'une seule, vous pouvez choisir celle que vous voulez ajouter. Vous pouvez définir les options suivantes pour la fusion de l'autorité :

- Par défaut
- Coffre-fort d'identité
- Application
- Aucun

Cliquez sur  pour enregistrer les modifications.

Script ECMA

Affiche une liste ordonnée des fichiers de ressources ECMAScript. Ces fichiers contiennent les fonctions d'extension pour le pilote qu'Identity Manager charge au démarrage du pilote. Vous pouvez importer des fichiers supplémentaires en cliquant sur , supprimer des fichiers existants en cliquant sur  ou modifier l'ordre d'exécution des fichiers. Vous pouvez également déplacer les scripts vers le haut ou vers le bas dans la liste. Pour enregistrer la liste de scripts ECMA, cliquez sur l'icône  .

Assignation d'attributs réciproque

Les assignations d'attributs réciproques permettent de créer et de gérer les liens en amont, ou références, entre les objets. Par exemple, l'objet Groupe inclut un attribut Membres qui fait référence tous les objets Utilisateur qui appartiennent à ce groupe. De même, chaque objet Utilisateur inclut un attribut Adhésion à un groupe qui fait référence aux objets Groupe dont cet utilisateur est membre. Afin que le moteur méta-annuaire synchronise l'attribut Membres de l'objet

Groupe avec l'attribut Adhésion à un groupe de l'objet Utilisateur pour tous les objets Groupe et Utilisateur du coffre-fort d'identité, ces attributs doivent être liés. Les liens entre les attributs Objet sont appelés assignations d'attributs réciproques.

Grâce à ce module, vous pouvez effectuer les opérations suivantes :

Création d'assignations personnalisées d'attributs réciproques

Cette section ne s'applique que si la page Assignation d'attributs réciproques affiche l'invite **Le pilote ne contient pas d'assignations personnalisées d'attributs réciproques. Cliquez sur l'icône « + » ci-dessus pour créer des assignations de base d'attributs réciproques**.

1. Cliquez sur l'icône + pour créer une liste d'assignations personnalisées d'attributs réciproques.
2. Les assignations d'attributs par défaut du pilote s'affichent. À présent, vous pouvez ajouter, supprimer ou modifier des assignations.

Ajout d'une assignation d'attributs réciproques

Lorsque vous créez une assignation d'attributs réciproques, vous devez commencer par ajouter l'un des attributs à la liste d'assignations réciproques.

1. Cliquez sur l'icône + située en regard du menu déroulant Opérations.
2. Dans la nouvelle entrée d'attribut, sélectionnez l'attribut souhaité dans la liste déroulante.
3. Spécifiez les détails de l'assignation réciproque :
   - 3a **Classe source** : indiquez le nom de la classe à laquelle l'attribut de la liste d'assignations est associé. Par exemple, si vous avez placé l'attribut Adhésion au groupe dans la liste des assignations réciproques, la classe source associée est Utilisateur.
   - 3b **Classe de destination** : indiquez le nom de la classe associée à l'attribut pour lequel vous souhaitez créer une assignation réciproque. Par exemple, si vous avez placé l'attribut Adhésion au groupe dans la liste des assignations réciproques, la classe de destination associée est Groupe.
   - 3c **Attribut réciproque** : indiquez le nom de l'attribut pour lequel vous souhaitez créer une assignation réciproque.

4 Pour assigner l'attribut à un autre attribut réciproque, cliquez sur l'icône  située à droite du nom de l'attribut.

Une nouvelle section correspondant à l'attribut est ajoutée à la fin de la liste des attributs. Sélectionnez la classe source, la classe cible et l'attribut réciproque.

Suppression d'une assignation d'attributs réciproques

Pour supprimer une assignation d'attributs réciproques, procédez comme suit :

1 Cochez la case correspondant à l'attribut réciproque à supprimer en regard de la **classe source**.

2 Cliquez sur l'icône  située en regard de la liste déroulante des attributs.

Suppression d'un attribut de la liste de correspondances réciproques

Pour supprimer un attribut de la liste de correspondances réciproques, procédez comme suit :

1 Cochez la case en regard de l'attribut à supprimer.

2 Cliquez sur l'icône  en regard de la liste déroulante **Opérations**.

Réorganisation des attributs assignés

Les assignations d'attributs sont résolues dans l'ordre de la liste, de haut en bas. Vous pouvez déplacer les attributs assignés dans la liste pour vous assurer qu'ils seront résolus dans l'ordre approprié. De manière générale, vous devez d'abord répertorier les assignations particulières, puis les assignations plus générales. Par exemple, une assignation de l'attribut Membre d'un objet Groupe doit être répertoriée avant une assignation de l'attribut Membre de n'importe quel objet (option <N'importe quelle classe>).

Cochez la case située en face de l'attribut assigné à déplacer, puis cliquez sur  pour le déplacer vers le haut ou sur  pour le déplacer vers le bas.

Suppression d'une assignation personnalisée d'attributs réciproques

Vous pouvez supprimer les assignations d'attributs personnalisées que vous avez créées. Le moteur méta-annuaire doit alors utiliser les assignations d'attributs par défaut du pilote.

Pour supprimer une assignation personnalisée d'attributs réciproques, cliquez sur l'icône  située en haut de l'écran.

Édition du fichier XML d'un attribut réciproque

Si vous le souhaitez, vous pouvez éditer directement le fichier XML d'un attribut réciproque. Pour ce faire, sur la page Assignation personnalisée d'attributs réciproques, cliquez sur l'icône Éditer le fichier XML  . Un éditeur XML de base s'ouvre et vous permet de modifier le fichier XML. Lorsque vous avez terminé, cliquez sur OK ou sur Annuler pour fermer l'éditeur XML.

Configuration avancée

Les paramètres avancés concernent les tâches suivantes :

- « Gestion des droits » page 172
- « Gestion des tables d'assignation d'objets » page 172
- « Gestion des travaux pour les pilotes » page 173

Gestion des droits

La page Droits contient un tableau qui présente tous les droits actuellement définis au sein du pilote sélectionné (avec le nom distinctif complet correspondant). Cette page permet d'effectuer les opérations suivantes :

- **Éditer dans un fichier XML** : pour éditer un droit dans un fichier XML, sélectionnez le droit souhaité dans la liste, puis cliquez sur l'icône . Activez ensuite la case à cocher **Enable XML Editing** (Activer l'édition XML).
- **Supprimer** : pour supprimer un droit, cochez la case située à gauche de son nom, puis cliquez sur l'icône . Un message s'affiche pour indiquer que l'opération ne peut pas être annulée et qui vous demande si vous êtes sûr de vouloir supprimer le droit sélectionné. Cliquez sur **OK** pour supprimer le droit ou sur **Annuler** pour arrêter l'opération. Vous pouvez cocher plusieurs cases pour supprimer plusieurs droits, ou cliquer sur la case située dans la partie supérieure gauche pour supprimer tous les droits.

Gestion des tables d'assignation d'objets

Les stratégies Identity Manager utilisent des tables d'assignation pour assigner un ensemble de valeurs à un autre ensemble de valeurs. Lorsque vous installez le paquetage de droits, les stratégies de ce paquetage sont ajoutées à l'ensemble de stratégies de démarrage du pilote. Le pilote n'exécute ces stratégies qu'une seule fois, lors de son démarrage. Pour plus d'informations, reportez-vous à la section Mapping Table Objects (Objets de la table d'assignation) du manuel *NetIQ Identity Manager Driver Administration Guide* (Guide d'administration des pilotes de NetIQ Identity Manager).

Grâce à la table d'assignation d'objets, vous pouvez effectuer les opérations suivantes :

- **Modifier une assignation existante** : pour modifier une table d'assignation d'objets existante, cliquez sur l'assignation souhaitée dans la liste, puis effectuez les opérations ci-dessous dans l'écran suivant :
  - Ajoutez une colonne.

    Indiquez une valeur pour la colonne, puis indiquez si la valeur est sensible à la casse, non sensible à la casse ou numérique.
  - Ajoutez une ligne et spécifiez une valeur pour cette ligne.
  - Cliquez sur l'icône .

- **Supprimer une assignation** : pour supprimer une assignation de la liste, sélectionnez l'assignation souhaitée dans la liste, puis cliquez sur l'icône  .
- **Éditer dans un fichier XML** : pour éditer une assignation dans un fichier XML, sélectionnez l'assignation souhaitée dans la liste, puis cliquez sur l'icône  . Activez ensuite la case à cocher **Enable XML Editing** (Activer l'édition XML).

Gestion des travaux pour les pilotes

Identity Console permet de planifier les événements à l'aide de l'option Travaux pour chaque pilote.

La page Job Scheduler (Planificateur du travail) contient le nom et la description du travail, et indique si le travail est activé ou désactivé, ainsi que le moment de son exécution planifiée. Cliquez sur le nom du travail pour ouvrir la page Travail. Cliquez sur l'icône activer/désactiver sous la colonne Activé pour activer ou désactiver le travail. Cliquez sur la description du travail pour afficher sa description complète.

L'onglet Travaux contient une table affichant les objets Travail existants pour le pilote sélectionné, répertoriés avec leur nom distinctif complet dans l'entrée du pilote.

Grâce à la page Job Scheduler (Planificateur du travail), vous pouvez effectuer les tâches suivantes :

- **Créer un travail** : cliquez sur l'icône  pour créer un travail.

  Dans la fenêtre contextuelle **Nouveau travail**, procédez comme suit pour créer un travail :

  1. Indiquez le nom du travail.
  2. Sélectionnez le type de travail souhaité.
  3. Cliquez sur l'icône  , puis sélectionnez le serveur sur lequel vous souhaitez exécuter le travail dans la liste des serveurs disponibles. Sinon, indiquez un nom de serveur, puis sélectionnez le serveur souhaité.
  4. Cliquez sur le bouton **Créer**.
- **Démarrer un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône  .
- **Arrêter un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône  .
- **Activer un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône  .
- **Désactiver un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône  .
- **Obtenir l'état** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône  .
- **Supprimer un travail** : sélectionnez un travail en cliquant sur la case située à gauche de son nom, puis cliquez sur l'icône  .

Cliquez sur un travail pour accéder à la page des **propriétés du travail**. Vous pouvez y définir la manière dont le travail doit s'exécuter.

Général : affiche le nom de la classe Java du travail. À partir de cette page, vous pouvez activer ou désactiver le travail, le supprimer après son exécution, sélectionner les serveurs sur lesquels il doit s'exécuter, spécifier le serveur de messagerie et lui donner un nom et une description.

Planifier : permet de définir le moment d'exécution du travail. Spécifiez l'heure de démarrage du travail et indiquez si vous souhaitez l'exécuter tous les jours, toutes les semaines, tous les mois ou tous les ans. Vous pouvez également personnaliser le moment d'exécution du travail ou l'exécuter manuellement.

Étendue : permet de définir les objets auxquels ce travail s'applique. Un objet peut être un conteneur, un groupe dynamique, un groupe ou une feuille. Cliquez sur Ajouter pour sélectionner l'objet auquel vous voulez appliquer la tâche. Vous pouvez cliquer sur le bouton Parcourir pour sélectionner un objet, puis sur OK. Pour supprimer un objet de la liste d'étendue, cochez la case à gauche d'un objet DN pour sélectionner un objet d'étendue, puis cliquez sur Supprimer.

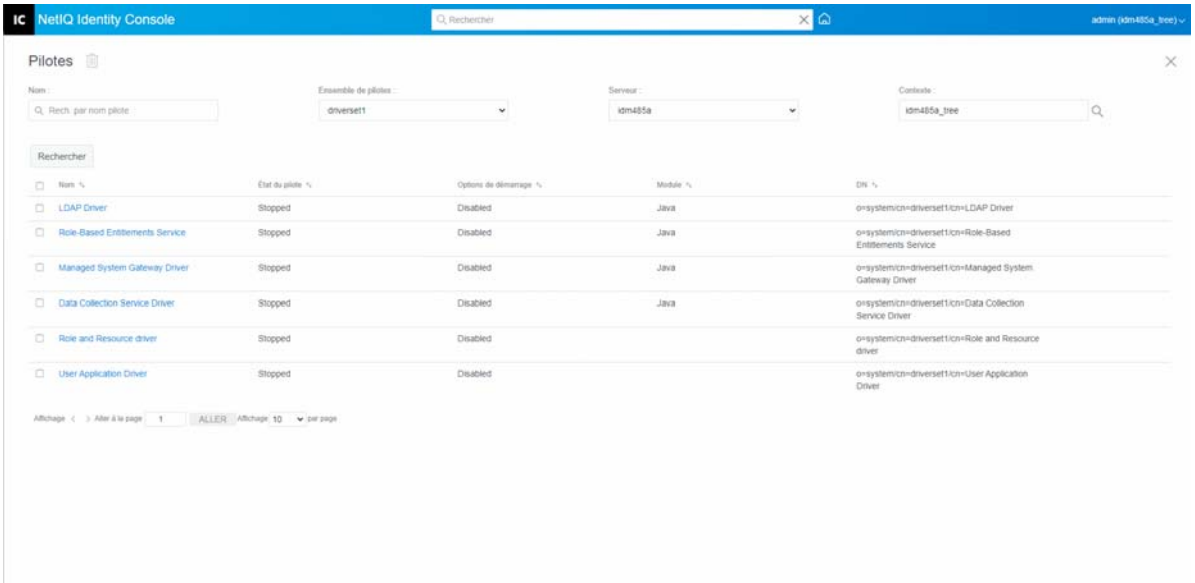
Une fois l'objet ajouté, sélectionnez-le pour afficher d'autres options. Si vous sélectionnez un groupe, vous pouvez appliquer la tâche aux membres du groupe ou au groupe uniquement. Si vous sélectionnez un objet Conteneur, vous pouvez appliquer le travail à tous les descendants du conteneur, à tous les enfants du conteneur ou au conteneur uniquement.

Paramètres : permet d'ajouter des paramètres au travail et de visualiser leur configuration actuelle. Ces paramètres changent en fonction du type de travail sélectionné.

Résultats : permet de définir ce que vous voulez faire des résultats du travail. La page de résultats est divisée en deux : les résultats intermédiaires et les résultats définitifs. Les résultats suivants sont possibles : Réussite, Avertissement, Erreur et Abandon. À droite de la colonne des résultats se trouve la colonne Opération. Cette colonne permet de sélectionner la façon dont vous souhaitez être notifié de chaque résultat. Parmi les opérations possibles figurent l'envoi d'un résultat d'audit ou d'un e-mail avec les résultats. Si vous ne sélectionnez aucune option, aucune opération n'est réalisée.

Dans l'onglet **Trace**, vous pouvez configurer la trace pour un pilote spécifique. Pour plus d'informations, reportez-vous à la section « Configuration du niveau de trace » page 176.

Figure 23-4 *Gestion des paramètres avancés*



Configuration des niveaux de consignation et de trace des pilotes

Pour configurer la consignation et le suivi d'un pilote, sur la page principale d'Identity Console, sélectionnez l'onglet **Pilotes** > **Configuration de la consignation et du suivi**. Cette section présente les tâches suivantes :

- « Configuration du niveau de consignation » page 175
- « Configuration du niveau de trace » page 176

Configuration du niveau de consignation

Chaque pilote possède un champ Niveau de consignation qui permet de définir le niveau d'erreurs à suivre. Le niveau que vous indiquez ici détermine quels messages sont disponibles pour les journaux. Par défaut, le niveau de consignation est défini pour le suivi des messages d'erreur (cela inclut également les messages d'erreur irrécupérable). Pour assurer le suivi d'autres types de messages, modifiez le niveau de consignation. Pour configurer le niveau de consignation, sélectionnez l'onglet **Configuration de la consignation et du suivi** > **Niveau de consignation**. Le tableau ci-dessous décrit les paramètres de niveau de consignation :

Option	Description
Utiliser les paramètres de consignation de l'ensemble de pilotes	Si vous sélectionnez cette option, le pilote consigne les événements en fonction des paramètres de consignation de l'objet Ensemble de pilotes.
Désactiver la consignation dans les journaux d'ensemble de pilotes, d'abonné et d'éditeur	Cette option désactive la consignation pour ce pilote dans l'objet Ensemble de pilotes, le canal Abonné et le canal Éditeur.
Nombre maximal d'entrées du journal (50-500)	Nombre d'entrées du journal. La valeur par défaut est 50.

Option	Description
Niveaux de consignation	Vous avez le choix parmi les niveaux de consignation suivants : ◆ **Consigner les erreurs** : consigne les erreurs uniquement. ◆ Consigner les erreurs et les avertissements : consigne les erreurs et les avertissements. ◆ **Consigner des événements spécifiques** : consigne les événements sélectionnés. Si vous sélectionnez cette option, la liste d'événements suivante est activée : ◆ **Événements du moteur méta-annuaire** ◆ **Événements d'état** ◆ **Événements de l'opération** ◆ **Événements de transformation** ◆ **Événements de provisioning de référence** ◆ **Mettre à jour l'heure de la dernière consignation uniquement** : met à jour l'heure de la dernière consignation. ◆ **Consignation désactivée** : désactive la consignation pour le pilote.

Configuration du niveau de trace

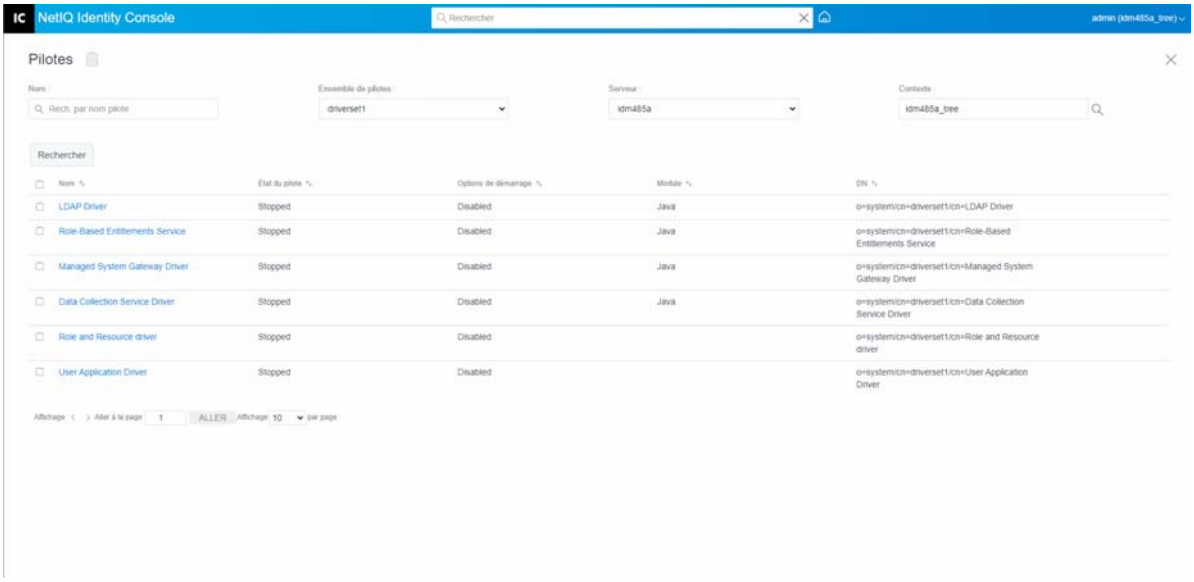
Vous pouvez configurer la trace pour un pilote spécifique. Selon le niveau de trace spécifié pour un pilote, la fonction de trace affiche les événements liés au pilote lorsque le moteur traite les événements. Le niveau de trace d'un pilote ne concerne que le pilote ou l'ensemble de pilotes dans lequel la trace est définie. Si vous utilisez le chargeur distant, le fichier de trace du chargeur distant est directement défini en conséquence et ne contient que la trace du module d'interface pilote.

Pour configurer la trace pour un pilote, sélectionnez l'onglet **Configuration de la consignation et du suivi** > **Trace**. Le tableau ci-dessous décrit les paramètres de trace :

Paramètre	Pilote
Niveau de trace	Plus le niveau de trace du pilote augmente, plus la quantité d'informations affichées dans Trace est importante. Le niveau de trace Un affiche les erreurs, mais pas leur cause. Pour afficher les informations de synchronisation du mot de passe, définissez le niveau de trace sur cinq. Si vous sélectionnez l'option **Utiliser le paramètre de l'ensemble de pilotes**, la valeur associée à l'ensemble de pilotes est utilisée.
Fichier de trace	Spécifiez le nom et l'emplacement du fichier dans lequel les informations Identity Manager sont écrites pour le pilote sélectionné. Si vous sélectionnez l'option **Utiliser le paramètre de l'ensemble de pilotes**, la valeur associée à l'ensemble de pilotes est utilisée.

Paramètre	Pilote
Nom de la trace	Les messages de trace du pilote commencent par la valeur saisie en lieu et place du nom du pilote. Utilisez ce paramètre si le nom du pilote est particulièrement long.
Codage du fichier de trace	Le fichier de trace utilise le codage par défaut du système. Vous pouvez si vous le souhaitez spécifier un autre codage.
Taille maximum du fichier de trace	Permet de définir une limite pour le fichier de trace Java. Si vous définissez la limite de fichier sur Illimitée, la taille du fichier augmente jusqu'à ce qu'il n'y ait plus de place sur le disque. **REMARQUE :** si la limite de taille du fichier est spécifiée, le fichier de trace est créé dans plusieurs fichiers. Identity Manager divise automatiquement la taille de fichier maximale par dix et crée dix fichiers distincts. La taille combinée de ces fichiers est égale à la taille maximale du fichier de trace. Si vous sélectionnez l'option **Utiliser le paramètre de l'ensemble de pilotes**, la valeur associée à l'ensemble de pilotes est utilisée.

Figure 23-5 *Gestion des niveaux de consignation et de trace des pilotes*



Inspection des pilotes

Vous pouvez utiliser l'inspecteur de pilote pour afficher des informations détaillées sur les objets associés à un pilote. Cette section présente les tâches suivantes :

- « Inspecteur de pilote » page 178
- « Inspecteur de cache du pilote » page 179
- « Inspecteur de cache de synchronisation hors limite » page 180

- « Manifeste du pilote » page 180
- « Surveillance de l'état de santé du pilote » page 181

Inspecteur de pilote

Pour afficher les objets associés à un pilote, procédez comme suit :

1. Dans Identity Console, sélectionnez **Pilotes** > **Inspecteur** > onglet **Inspecteur de pilote**.
2. Dans le champ **Pilote**, indiquez le nom distinctif complet du pilote à inspecter ou cliquez sur l'icône Parcourir pour rechercher et sélectionner le pilote souhaité.
3. Après avoir sélectionné le pilote à inspecter, cliquez sur **OK** pour afficher la page Inspecteur de pilote.

   Cette page affiche des informations sur les objets associés au pilote sélectionné. Vous pouvez effectuer les opérations suivantes :

   - **Supprimer :** supprime l'association entre le pilote et un objet. Cochez la case située en regard de l'objet que vous ne souhaitez plus associer au pilote, cliquez sur l'icône  , puis sur **OK** pour confirmer la suppression.
   - **Rafraîchir :** sélectionnez l'icône Rafraîchir pour relire tous les objets associés au pilote et rafraîchir les informations.
   - **Afficher:** sélectionnez le nombre d'associations à afficher par page. Vous pouvez sélectionner un nombre prédéfini (25, 50 ou 100) ou préciser le nombre de votre choix. 10 associations par page correspond à la valeur par défaut. Si le nombre d'associations est supérieur au nombre affiché, cliquez sur les flèches pour afficher les pages suivantes et précédentes des associations.
   - **Opérations :** effectuez des opérations sur les objets associés au pilote. Cliquez sur **Opérations**, puis sélectionnez l'une des options suivantes :
     - **Afficher toutes les associations :** affiche tous les objets associés au pilote.
     - **Filtrer les associations « Désactivé(e) » :** affiche tous les objets associés au pilote dont l'état est Désactivé(e).
     - **Filtrer les associations « Manuel(le) » :** affiche tous les objets associés au pilote dont l'état est Manuel(le).
     - **Filtrer les associations « Migrer » :** affiche tous les objets associés au pilote dont l'état est Migrer.
     - **Filtrer les associations « En attente » :** affiche tous les objets associés au pilote dont l'état est En attente.
     - **Filtrer les associations « Traité(e) » :** affiche tous les objets associés au pilote dont l'état est Traité(e).
     - **Filtrer les associations « Non défini(e) » :** affiche tous les objets associés au pilote dont l'état est Non défini(e).
     - **Résumé des associations :** affiche l'état de tous les objets associés au pilote.
   - **DN de l'objet:** affiche le DN des objets associés.
   - **État :** affiche l'état de l'association de l'objet.
   - **ID de l'objet:** affiche la valeur de l'association.

Inspecteur de cache du pilote

Vous pouvez afficher les transactions dans le fichier de cache d'un pilote à l'aide d'Identity Console. L'**inspecteur de cache du pilote** affiche des informations sur le fichier de cache, y compris la liste des événements que le pilote doit traiter.

1. Dans Identity Console, sélectionnez **Pilotes** > **Inspecteur** > onglet **Inspecteur de cache du pilote**.
2. Dans le champ **Pilote**, indiquez le nom distinctif complet du pilote dont vous souhaitez inspecter le cache ou cliquez sur l'icône Parcourir pour rechercher et sélectionner le pilote souhaité. Cliquez ensuite sur **OK** pour afficher la page Inspecteur de cache du pilote.

   Le fichier de cache d'un pilote ne peut être lu que lorsque le pilote n'est pas en cours d'exécution. Si le pilote est arrêté, la page Inspecteur de cache du pilote affiche le cache. Si le pilote est en cours d'exécution, la page affiche le message « `Le pilote n'est pas arrêté. Impossible de lire le cache` » en lieu et place des entrées du cache. Pour arrêter le pilote, cliquez sur le bouton  . Le cache est alors lu et affiché.

   - **Cache du pilote sur le serveur :** affiche le serveur qui contient cette instance du fichier de cache. Si le pilote est exécuté sur plusieurs serveurs, vous pouvez choisir un autre serveur de la liste pour afficher le fichier de cache du pilote correspondant à ce serveur.
   - **Icônes Démarrer/Arrêter le pilote :** affichent l'état actuel du pilote et permettent de démarrer ou d'arrêter le pilote. Le cache ne peut être lu que lorsque le pilote est arrêté.
   - **Supprimer :** sélectionnez des entrées du cache, puis cliquez sur l'icône  pour les supprimer du fichier de cache.
   - **Opérations :** permet d'effectuer des opérations sur les entrées du fichier de cache. Cliquez sur **Opérations** pour développer le menu, puis sélectionnez l'une des options suivantes :
     - **Effacer tous les événements en cache :** permet d'effacer tous les événements mis en cache.
     - **Résumé du cache :** affiche le résumé de tous les événements stockés dans le fichier de cache.

Affichage des détails du système connecté pour les pilotes

Pour afficher les détails du système connecté pour un pilote spécifique, procédez comme suit :

1. Dans Identity Console, cliquez sur le module **Inspecteur d'objet**.
2. Recherchez et sélectionnez l'objet Pilote spécifique dont vous souhaitez afficher les systèmes connectés.
3. Tous les détails du système connecté correspondant à l'objet Pilote sélectionné s'affichent sur votre ordinateur.

Inspecteur de cache de synchronisation hors limite

Pour afficher les événements du cache de synchronisation hors limite, procédez comme suit :

1. Dans Identity Console, sélectionnez **Pilotes** > **Inspecteur** > onglet **Inspecteur de cache de synchronisation hors limite**.
2. Dans le champ **Pilote**, indiquez le nom distinctif complet du pilote dont vous souhaitez inspecter le cache ou cliquez sur l'icône Parcourir pour rechercher et sélectionner le pilote souhaité. Cliquez ensuite sur **OK**.

   Le fichier de cache d'un pilote ne peut être lu que lorsque le pilote n'est pas en cours d'exécution. Si le pilote est arrêté, la page Inspecteur de cache du pilote affiche le cache. Si le pilote est en cours d'exécution, la page affiche le message « `Le pilote n'est pas arrêté. Impossible de lire le cache` » en lieu et place des entrées du cache. Pour arrêter le pilote, cliquez sur le bouton  . Le cache est alors lu et affiché.

   - **Nom du fichier de cache :** affiche le nom de fichier du cache.
   - **Cache du pilote sur le serveur :** affiche le serveur qui contient cette instance du fichier de cache. Si le pilote est exécuté sur plusieurs serveurs, vous pouvez choisir un autre serveur de la liste pour afficher le fichier de cache du pilote correspondant à ce serveur.
   - **Icônes Démarrer/Arrêter le pilote :** affichent l'état actuel du pilote et permettent de démarrer ou d'arrêter le pilote. Le cache ne peut être lu que lorsque le pilote est arrêté.
   - **Supprimer :** sélectionnez des entrées du cache, puis cliquez sur l'icône  pour les supprimer du fichier de cache.
   - **Opérations :** permet d'effectuer des opérations sur les entrées du fichier de cache. Cliquez sur **Opérations** pour développer le menu, puis sélectionnez l'une des options suivantes :
     - **Résumé du cache :** affiche le résumé de tous les événements stockés dans le fichier de cache.
     - **Effacer tous les événements en cache :** permet d'effacer tous les événements mis en cache.

Manifeste du pilote

Le manifeste du pilote est en quelque sorte un CV du pilote. Il indique les éléments pris en charge par le pilote et comprend quelques paramètres de configuration. Le manifeste doit être fourni par le développeur du pilote. Un administrateur réseau n'a généralement pas besoin de modifier le manifeste du pilote. Si l'administrateur souhaite éditer le manifeste du pilote, sélectionnez **Pilotes** > **Inspecteur** > **Manifeste du pilote** > option **Enable XML Editing** (Activer l'édition XML).

Surveillance de l'état de santé du pilote

La surveillance de l'état de santé du pilote vous permet d'afficher l'état de santé actuel d'un pilote (vert, jaune ou rouge), ainsi que de définir les opérations à effectuer en réponse à chacun de ces états.

Vous créez les conditions (critères) qui déterminent chacun des états de santé et définissez les opérations à exécuter lors de chacun de leurs changements. Par exemple, si l'état de santé du pilote passe de l'état vert à l'état jaune, vous pouvez exécuter des opérations telles que le redémarrage ou l'arrêt du pilote, ainsi que l'envoi d'un message électronique à la personne chargée de résoudre les problèmes du pilote.

Grâce à ce module, vous pouvez effectuer les tâches suivantes :

- « Modification des conditions d'état de santé d'un pilote » page 181
- « Modification des opérations selon l'état de santé d'un pilote » page 184
- « Création d'un état personnalisé » page 185
- « Modification d'un état personnalisé » page 186

Modification des conditions d'état de santé d'un pilote

Vous devez contrôler les conditions déterminant chaque état de santé. L'état vert représente un pilote sain, tandis qu'un état rouge représente un pilote non sain.

Les conditions de l'état vert sont évaluées les premières. Si le pilote ne remplit pas les conditions de l'état vert, ce sont celles de l'état jaune qui sont alors évaluées. S'il ne remplit pas non plus les conditions de l'état jaune, son état de santé est automatiquement défini sur rouge.

Pour modifier les conditions d'un état, procédez comme suit :

1. Dans Identity Console, ouvrez la page Configuration de l'état de santé du pilote correspondant au pilote dont vous souhaitez modifier les conditions :
   - **1a** Ouvrez la page d'accueil d'Identity Console.
   - **1b** Sélectionnez **Pilotes** > **cliquez sur le pilote approprié dans la liste** > **Inspecteur** > **Configuration de l'état de santé du pilote**.
2. Cliquez sur l'onglet correspondant à l'état (vert ou jaune) à modifier.

   Cet onglet affiche les conditions actuelles de l'état de santé. Celles-ci sont organisées en groupes. Les opérateurs logiques AND et OR permettent de combiner les conditions et les groupes. L'exemple suivant illustre une condition où l'état est vert :

   ```
   GROUP1
   Condition1 and
   Condition2
   Or
   GROUP2
   Condition1 and
   Condition2 and
   Condition3
   ```

Dans cet exemple, un état vert est affecté au pilote si les conditions du GROUPE1 ou celles du GROUPE2 sont vraies. Si aucun groupe de conditions n'est vrai, alors les conditions de l'état jaune sont évaluées.

Les conditions pouvant être évaluées sont les suivantes :

- **État du pilote :** en cours d'exécution, arrêté, démarrage, pas en cours d'exécution ou en cours d'arrêt. Par exemple, l'une des conditions par défaut de l'état de santé vert est que le pilote est en cours d'exécution.
- **Pilote en dépassement de la capacité du cache :** état du cache utilisé pour conserver les transactions du pilote. Un dépassement de la capacité du cache dans le pilote signifie que tout le cache disponible a été utilisé. Par exemple, la condition par défaut de l'état de santé vert est que la condition Pilote en dépassement de la capacité du cache est fausse et que celle de l'état de santé jaune est que la condition Pilote en dépassement de la capacité du cache est vraie.
- **Le plus récent:** âge de la transaction la plus récente dans le cache.
- **Le plus ancien:** âge de la transaction la plus ancienne dans le cache.
- **Taille totale:** taille du cache.
- **Taille non traitée :** taille de toutes les transactions non traitées dans le cache.
- **Transactions non traitées :** nombre des transactions non traitées contenues dans le cache. Vous pouvez indiquer tous les types de transaction ou juste certains types (ajouts, suppressions, changements de nom, etc.).
- **Historique des transactions :** nombre de transactions traitées à différents points du canal Abonné ou Éditeur sur une période donnée. Cette condition utilise plusieurs éléments et suit le format suivant :

  <*type de transaction*> <*emplacement et durée de la transaction*> <*opérateur relationnel*> <*nombre de transactions*>.

  - <*type de transaction*> : précise le type de la transaction en cours d'évaluation. Il peut s'agir de toutes les transactions, des ajouts, des suppressions, des changements de nom, etc.
  - <*emplacement et durée de la transaction*> : précise l'emplacement dans le canal Abonné ou Éditeur, ainsi que la période d'évaluation. Vous pouvez, par exemple, évaluer le nombre total des transactions traitées comme événements signalés de l'éditeur au cours des dernières 48 heures. Par défaut, les données de l'historique des transactions sont conservées pendant deux semaines. En d'autres termes, vous ne pouvez indiquer de durée supérieure à deux semaines que si vous modifiez le paramètre par défaut de durée des données des transactions.
  - <*opérateur relationnel*> : précise que les transactions identifiées doivent être égales, différentes, inférieures, inférieures ou égales, supérieures ou supérieures ou égales au <nombre de transactions>.
  - <*nombre de transactions*> : précise le nombre de transactions en cours d'utilisation dans l'évaluation.

  L'exemple ci-après illustre la condition Historique des transactions :

  ```
  <nombre d'ajouts> <en tant que commandes d'éditeur> <au cours des
  dernières 10 minutes> <est inférieur à> <1 000>
  ```

- **Historique disponible :** quantité des données de l'historique des transactions disponible pour l'évaluation. Cette condition garantit qu'aucune condition Historique des transactions ne provoque l'échec de l'état actuel en raison d'une insuffisance des données collectées pour l'historique des transactions.

  Supposons, par exemple, que vous souhaitez utiliser la condition Historique des transactions afin d'évaluer le nombre d'ajouts en tant que commandes d'éditeur au cours des dernières 48 heures (exemple affiché plus haut, dans la section Historique des transactions). Cependant, vous ne souhaitez pas que la condition échoue si les données sont récoltées depuis moins de 48 heures, ce qui peut être le cas après la configuration initiale de l'état de santé du pilote ou si le serveur du pilote redémarre (car les données de l'historique des transactions sont conservées en mémoire). Vous pouvez donc créer des groupes de conditions, comme l'illustre l'exemple suivant :

  ```
  Group1 Historique disponible <est inférieur à> <48 heures> ou Group2
  Historique disponible <est supérieur ou égal à> <48 heures> et
  Historique des transactions <nombre d'ajouts> <en tant que commandes
  d'éditeur> <au cours des dernières 48 heures> <est inférieur à>
  <1 000>
  ```

  L'état est évalué sur vrai si l'un des groupes de conditions est évalué sur vrai, ce qui signifie a) qu'il y a moins de 48 heures de données ou b) qu'il y a au moins 48 heures de données et que le nombre d'ajouts en tant que commandes d'éditeur au cours des dernières 48 heures est inférieur à 1 000.

  L'état est évalué sur faux si les deux conditions sont évaluées sur faux, ce qui signifie a) qu'il y a au moins 48 heures de données et que b) le nombre d'ajouts comme commandes d'éditeur au cours des dernières 48 heures est supérieur à 1 000.

3. Modifiez les critères selon vos besoins.

   - Pour ajouter un nouveau groupe, cliquez sur l'icône + en regard de **Groupes de conditions**.
   - Pour ajouter une condition, cliquez sur l'icône + en regard des opérateurs logiques (ET/OU). Vous pouvez également cliquer sur le lien **Ajouter une condition**.
   - Pour réorganiser les groupes de conditions ou les conditions, cochez la case située en regard du groupe ou de la condition à déplacer, puis cliquez sur les flèches pour le déplacer vers le haut ou vers le bas. Les flèches permettent également de déplacer une condition d'un groupe à un autre.

4. Lorsque vous avez terminé, enregistrez les modifications apportées en cliquant sur le bouton **Enregistrer**.
5. Si vous souhaitez modifier les opérations associées aux conditions définies, passez à la section « Modification des opérations selon l'état de santé d'un pilote » page 184.

Modification des opérations selon l'état de santé d'un pilote

Vous avez la possibilité de définir les opérations à exécuter lors des changements d'état de santé du pilote. Si l'état passe de vert à jaune, par exemple, vous pouvez arrêter ou redémarrer le pilote, générer un événement ou démarrer un workflow. De même, si l'état passe du jaune au vert, toutes les opérations associées à l'état vert sont exécutées.

Les opérations d'un état de santé ne sont exécutées qu'une seule fois lorsque les conditions sont remplies ; tant que l'état reste vrai, elles ne sont pas répétées. Si l'état change parce que ses conditions ne sont plus remplies, les opérations seront exécutées lorsque les conditions le seront de nouveau.

1. Dans Identity Console, ouvrez la page Configuration de l'état de santé du pilote correspondant au pilote dont vous souhaitez modifier les opérations :
   - **1a** Ouvrez la page d'accueil d'Identity Console.
   - **1b** Sélectionnez **Pilotes** > **cliquez sur le pilote approprié dans la liste** > **Inspecteur** > **Configuration de l'état de santé du pilote**.
2. Cliquez sur l'onglet **Vert**, **Jaune** ou **Rouge** correspondant à l'état dont vous souhaitez modifier les opérations.
3. Cliquez sur l'icône plus (+) située en regard de l'en-tête **Opérations** afin d'ajouter une opération, puis sélectionnez le type d'opération souhaité :
   - **Démarrer le pilote:** Démarre le pilote.
   - **Arrêter le pilote:** Arrête le pilote.
   - **Redémarrer le pilote :** arrête puis démarre le pilote.
   - **Effacer le cache du pilote :** supprime toutes les transactions du cache, y compris les transactions non traitées.
   - **Envoyer un message électronique:** envoie un message électronique à un ou plusieurs destinataires. Le modèle que vous souhaitez utiliser dans le corps du message électronique doit déjà exister. Pour inclure les informations de nom de pilote, de nom de serveur et d'état de santé actuel dans le message électronique, ajoutez les jetons `$Driver$`, `$Server$` et `$HealthState$` au modèle de message électronique, puis incluez-les dans le texte du message. Exemple :

     ```
     The current health state of the $Driver$ driver running on $Server$ is $HealthState$.
     ```

     IMPORTANT : pour envoyer un message électronique à plusieurs utilisateurs, séparez les différentes adresses électroniques par une virgule (,). N'utilisez pas de point-virgule.
   - **Écrire le message de trace :** écrit un message dans le fichier journal du travail d'état de santé du pilote ou dans celui de l'ensemble de pilotes si le fichier de trace n'est pas configuré dans le travail d'état de santé du pilote.
   - **Générer un événement:** génère un événement exploitable par Audit et Sentinel.
   - **Exécuter ECMAScript :** exécute un script ECMA existant.

     Pour plus d'informations sur la construction des scripts ECMA, reportez-vous à la section Using ECMAScript in Policies (Utilisation de ECMAScript dans les stratégies) dans le document *NetIQ Identity Manager - Using Designer to Create Policies* (NetIQ Identity Manager - Utilisation de Designer pour créer des stratégies).

- **Démarrer le workflow:** démarre un workflow de provisioning.
- **Sur erreur :** si une opération échoue, indique comment procéder avec les opérations restantes, l'état de santé en cours et le travail d'état de santé du pilote.
  - **Affecter les opérations par :** vous pouvez poursuivre ou arrêter l'exécution des opérations restantes ou définir le paramètre actuel sur la valeur par défaut. Le paramètre actuel n'a d'effet que si vous disposez de plusieurs opérations Avec erreur et avez défini l'option Affecter les opérations par dans l'une des opérations Avec erreur précédentes.
  - **Affecter l'état par :** vous pouvez enregistrer l'état actuel, le rejeter ou définir le paramètre actuel sur la valeur par défaut. Si vous enregistrez l'état, ses conditions continuent à être évaluées sur vrai. Si vous le refusez, ses conditions sont évaluées sur faux. Le paramètre actuel n'a d'effet que si vous disposez de plusieurs opérations Avec erreur et avez défini l'option Affecter l'état par dans l'une des opérations Avec erreur précédentes.
  - **Affecter le travail d'état de santé du pilote par :** vous pouvez poursuivre l'exécution du travail, abandonner et désactiver le travail ou définir le paramètre actuel sur la valeur par défaut. Si vous poursuivez l'exécution du travail, celui-ci termine l'évaluation des conditions en vue de déterminer l'état de santé du pilote et d'effectuer des opérations associées à l'état. L'abandon et la désactivation du travail arrêtent l'activité en cours du travail et le travail ; le travail n'est pas réexécuté tant que vous ne l'activez pas. Le paramètre actuel n'a d'effet que si vous disposez de plusieurs opérations Avec erreur et avez défini le paramètre Affecter le travail sur l'état de santé du pilote par dans l'une des opérations Avec erreur précédentes.

4 Lorsque vous avez terminé, enregistrez les modifications apportées en cliquant sur le bouton **Enregistrer**.

Création d'un état personnalisé

Vous pouvez créer un ou plusieurs états personnalisés pour exécuter des opérations indépendamment de l'état de santé actuel du pilote (vert, jaune ou rouge). Si les conditions d'un état personnalisé sont remplies, ses opérations sont exécutées quel que soit l'état de santé actuel.

À l'instar des états de santé vert, jaune et rouge, les opérations d'un état personnalisé ne sont exécutées qu'une seule fois lorsque les conditions sont remplies ; tant que l'état reste vrai, elles ne sont pas répétées. Si l'état change parce que ses conditions ne sont plus remplies, les opérations seront exécutées lorsque les conditions le seront de nouveau.

1 Dans Identity Console, ouvrez la page Configuration de l'état de santé du pilote correspondant au pilote dont vous souhaitez créer un état personnalisé :

   1a Ouvrez la page d'accueil d'Identity Console.

   1b Sélectionnez **Pilotes** > **cliquez sur le pilote approprié dans la liste** > **Inspecteur** > **Configuration de l'état de santé du pilote**.

2 Cliquez sur l'icône + située en regard des icônes d'état de santé du pilote (vert, jaune et rouge).

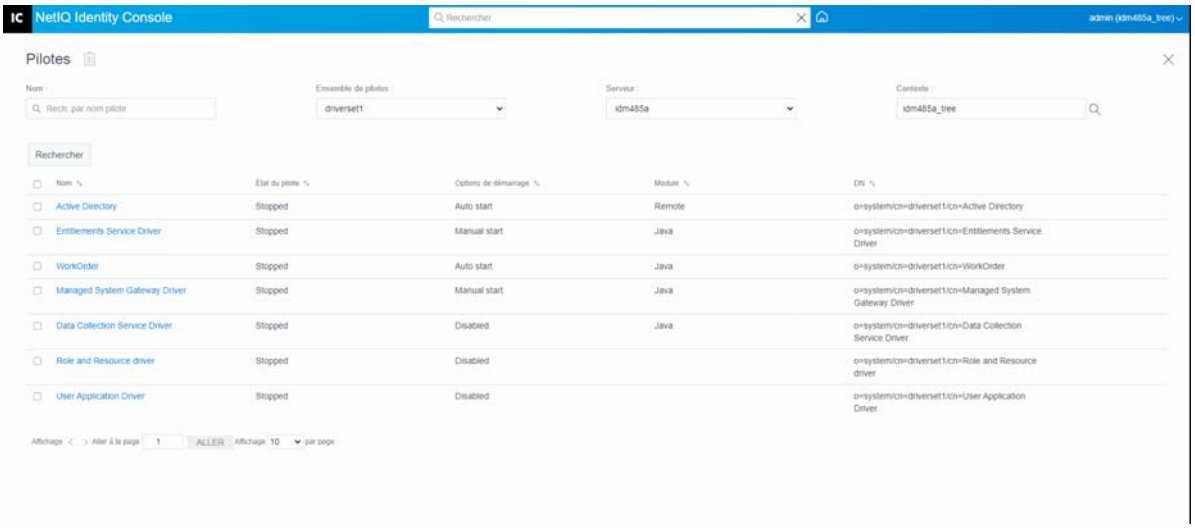
3 Suivez les instructions des sections « Modification des conditions d'état de santé d'un pilote » page 181 et « Modification des opérations selon l'état de santé d'un pilote » page 184 pour définir les conditions et les opérations de l'état personnalisé.

Modification d'un état personnalisé

Pour modifier un état personnalisé, procédez comme suit :

1. Dans Identity Console, ouvrez la page Configuration de l'état de santé du pilote correspondant au pilote dont vous souhaitez créer un état personnalisé :
   - **1a** Ouvrez la page d'accueil d'Identity Console.
   - **1b** Sélectionnez **Pilotes** > **cliquez sur le pilote approprié dans la liste** > **Inspecteur** > **Configuration de l'état de santé du pilote**.
2. Cliquez sur l'icône  située en regard des icônes d'état de santé du pilote (vert, jaune et rouge).
3. Suivez les instructions des sections « Modification des conditions d'état de santé d'un pilote » page 181 et « Modification des opérations selon l'état de santé d'un pilote » page 184 pour définir les conditions et les opérations de l'état personnalisé.

Figure 23-6 *Gestion de l'inspecteur de pilote*



24 Gestion des statistiques des ensembles de pilotes

Vous pouvez utiliser le portail Identity Console pour afficher diverses statistiques relatives à un seul pilote ou à un ensemble de pilotes. Il s'agit notamment de la taille du fichier de cache, de la taille des transactions non traitées dans le fichier de cache, des transactions les plus anciennes et les plus récentes, ainsi que du nombre total de transactions non traitées par catégorie (ajout, suppression, modification, etc.). Pour afficher les statistiques d'un ensemble de pilotes, procédez comme suit :

1. Dans Identity Console, ouvrez la page **Statistiques de l'ensemble de pilotes**.
2. Sélectionnez le serveur approprié dans la liste déroulante.

   La page qui s'affiche vous permet de consulter les statistiques de tous les pilotes contenus dans l'ensemble de pilotes.

   - Pour rafraîchir les statistiques, cliquez sur l'icône .
   - Pour fermer les statistiques d'un pilote, cliquez sur le bouton situé dans le coin supérieur droit de la fenêtre des statistiques du pilote.
   - Pour ouvrir les statistiques de tous les pilotes, cliquez sur **Opérations** > **Tout afficher**.
   - Pour réduire la liste des transactions non traitées pour un pilote, cliquez sur le bouton situé au-dessus de la liste. Pour réduire la liste des transactions non traitées pour tous les pilotes, cliquez sur **Opérations** > **Réduire toutes les transactions**.
   - Pour développer la liste des transactions, cliquez sur le bouton . Pour développer la liste des transactions non traitées pour tous les pilotes, cliquez sur **Opérations** > **Développer toutes les transactions**.
   - Pour fermer le tableau de bord des statistiques pour les pilotes désactivés, cliquez sur **Opérations**, puis sélectionnez **Close Disabled Drivers** (Fermer les pilotes désactivés).

Figure 24-1 *Gestion des statistiques d'un ensemble de pilotes*

25 Inspection des objets Identity Manager

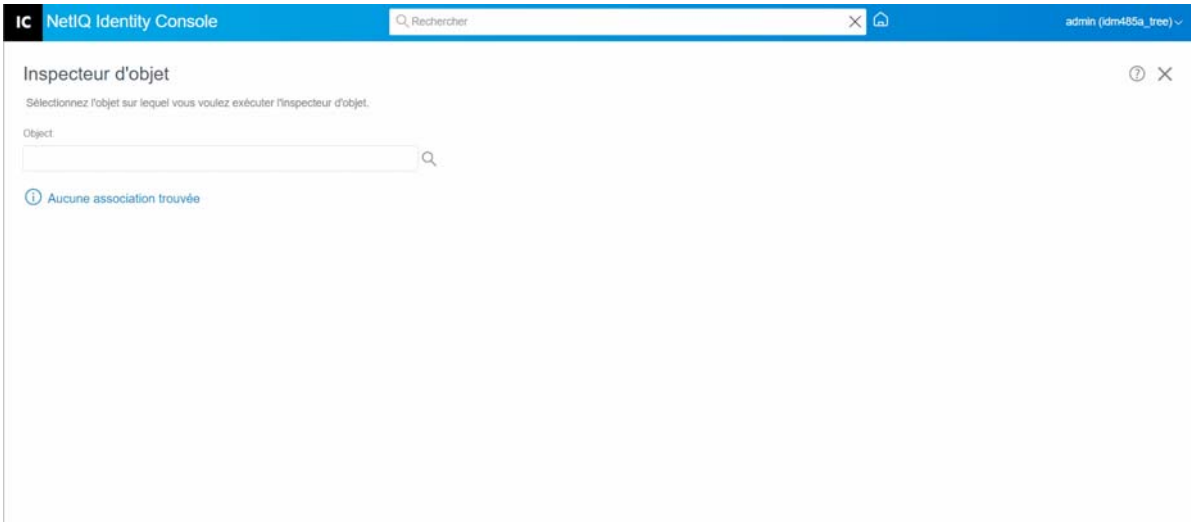
Vous pouvez utiliser l'inspecteur d'objet pour afficher des informations détaillées sur la manière dont un objet participe aux relations Identity Manager. Ces relations incluent les systèmes connectés qui sont associés à l'objet, le mode de circulation des données entre le coffre-fort d'identité et les systèmes connectés, les valeurs d'attribut actuellement stockées dans le coffre-fort d'identité et sur les systèmes connectés, la configuration des pilotes des systèmes connectés, etc.

Pour inspecter un objet Identity Manager, cliquez sur l'option **Inspecteur d'objet** sur la page principale d'Identity Console. Indiquez le nom distinctif complet de l'objet à inspecter ou cliquez sur l'icône Parcourir pour rechercher et sélectionner l'objet souhaité.

La section Systèmes connectés répertorie tous les systèmes connectés auxquels l'objet est associé. Grâce à la page **Inspecteur d'objet**, vous pouvez effectuer les opérations suivantes :

- **Ajout d'une association** : pour ajouter une nouvelle association à un système connecté, cliquez sur l'icône +. Recherchez et sélectionnez l'**objet Pilote d'intégration**, puis spécifiez l'**ID d'objet associé**.
- **Supprimer une association** : pour supprimer une association avec un système connecté, cochez la case située à gauche de l'association concernée, puis cliquez sur l'icône. Pour supprimer toutes les associations, cochez la case située sous la colonne Supprimer, puis cliquez sur l'icône.

Figure 25-1 *Inspection des objets Identity Manager*



26 Gestion du flux de données

Le flux de données illustre les canaux Éditeur et Abonné de plusieurs pilotes au sein d'une même vue. Cette option permet d'afficher et de mettre à jour la propriété des données de tous les pilotes.

Pour accéder à la vue de table du flux de données, cliquez sur le module **Flux de données (vue de table)** sur la page principale d'Identity Console. Ensuite, recherchez et sélectionnez le conteneur approprié pour afficher la liste des pilotes.

Pour gérer la propriété des données d'un pilote, procédez comme suit :

1 Chaque pilote comporte deux boutons permettant de gérer le flux de données sur les canaux Éditeur et Abonné. Le bouton à gauche gère le flux de données sur le canal Éditeur, tandis que le bouton à droite gère le flux de données sur le canal Abonné.

   1a **Synchroniser** : sélectionnez cette option pour synchroniser l'attribut spécifique. L'icône se change alors en ↑ sur le canal Éditeur et en ↓ sur le canal Abonné.

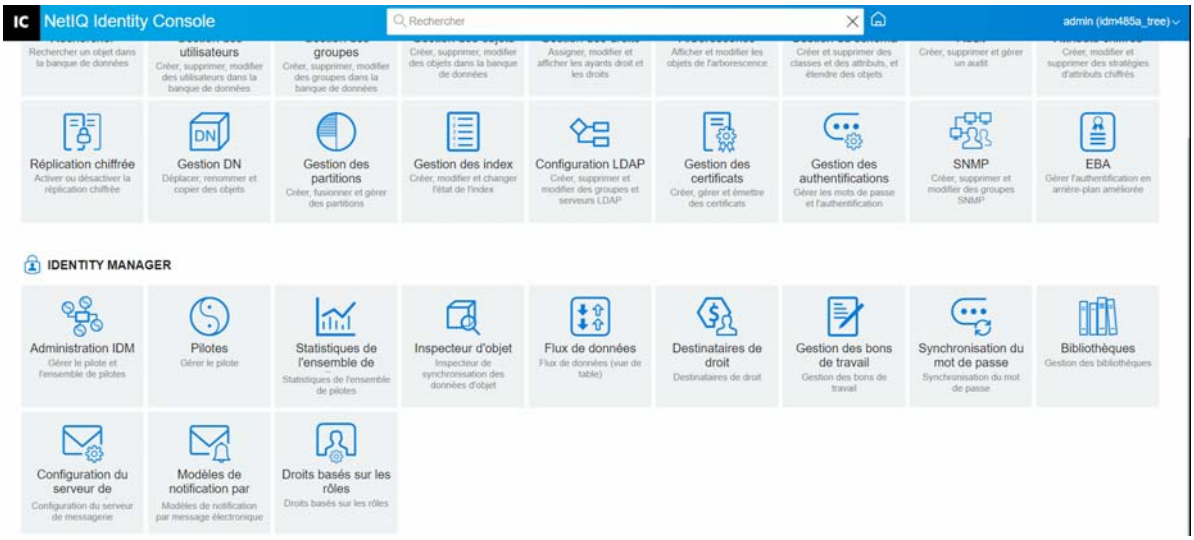
   1b **Ignorer** : sélectionnez cette option pour arrêter la synchronisation de l'attribut spécifique. L'icône se change alors en ⊘.

   1c **Notifier** : sélectionnez cette option pour être averti des modifications apportées à un attribut spécifique. Les modifications ne sont toutefois pas synchronisées automatiquement. L'icône se change alors en 🔔.

   1d **Réinitialiser** : sélectionnez cette option pour rétablir la valeur de l'attribut sur la valeur spécifiée par l'autre canal. L'icône se change alors en ↻.

   REMARQUE : vous ne pouvez définir cette valeur que sur un seul des canaux Éditeur ou Abonné, pas sur ces deux canaux simultanément.

Figure 26-1 *Gestion du flux de données*



27 Gestion des destinataires de droit

Les résultats et les références de droit sont gérés dans les objets pour lesquels un droit a été accordé ou révoqué. Les références et résultats de droit contiennent des informations sur l'état accordé ou révoqué du droit pour cet objet. Les destinataires du droit sont les objets contenant des références à un droit.

Références de droit

Pour afficher les références et les résultats de droit, cliquez sur l'option **Destinataires de droit** sur la page principale d'Identity Console, puis sélectionnez Références de droit. Indiquez ensuite le nom distinctif complet de l'objet correspondant à `DirXML-EntitlementRecipient`. Vous pouvez cliquer sur le bouton Sélecteur d'objet  pour sélectionner l'objet.

Résultats de droit

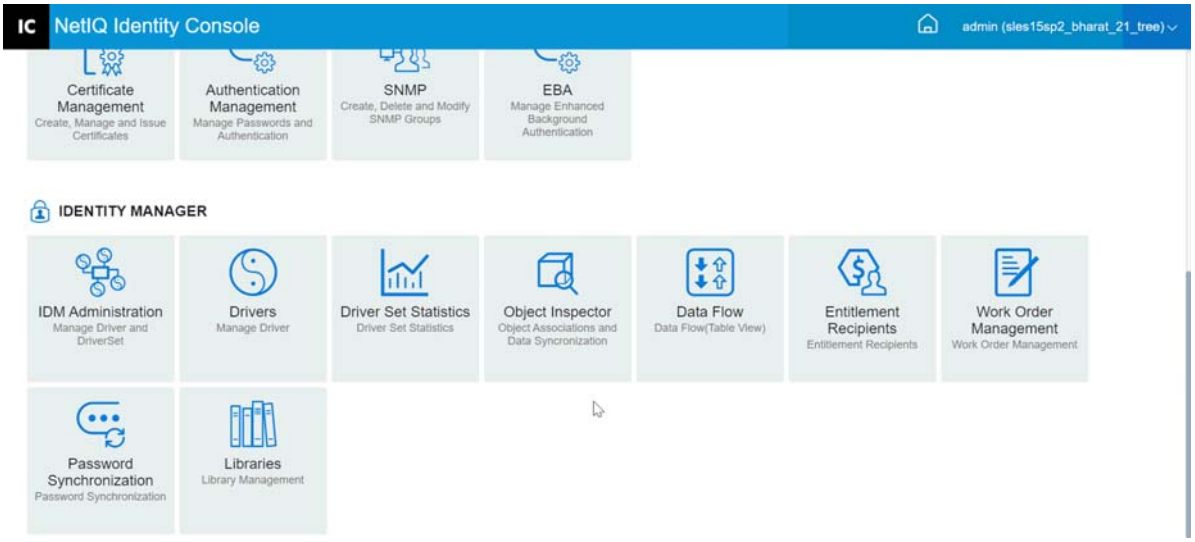
Le tableau des résultats de droit d'Identity Console affiche les résultats de droit associés à l'objet sélectionné. Pour afficher le droit associé, sélectionnez le DN du droit. Pour afficher les résultats du droit au format XML, sélectionnez l'ID du résultat correspondant.

- **En-têtes des colonnes des résultats de droit** : les en-têtes des colonnes contiennent le nom distinctif complet du droit, indiquent son état actuel (accordé ou révoqué), l'origine des résultats (source), l'état du résultat, les éventuels messages qui accompagnent le résultat, le tampon horaire du résultat, ainsi que l'identification du résultat.
  - **DN de droit** : cliquez sur le nom distinctif complet du droit de l'objet pour ouvrir la page Modifier l'objet. Cette page permet de voir comment les attributs d'eDirectory ont été assignés à l'objet. Vous pouvez également utiliser cette page pour modifier les attributs de l'objet. Le nombre de catégories affichées dans la page Modifier l'objet dépend de l'objet sélectionné.
  - **État** : indique si le droit a été accordé ou révoqué. Si le plug-in trouve une autre valeur dans le flux XML, il l'affiche directement.
  - **Message** : affiche les messages que le module d'interface DirXML a associés à l'état des résultats. Les informations stockées dans la partie <msg></msg> du fichier de résultats XML. Cliquez sur l'entrée ID de résultat pour afficher les détails complets du résultat dans une page Visionneuse XML.

- **Tampon horaire** : heure à laquelle le moteur du droit a traité et écrit le résultat. Cliquez sur l'entrée ID de résultat pour afficher les détails complets du résultat dans une page Visionneuse XML.
- **ID de résultat** : cliquez sur l'entrée d'ID de résultat pour afficher les détails complets du résultat dans une page Visionneuse XML. Lorsque vous avez terminé de consulter les résultats, cliquez sur Fermer.

Pour supprimer une entrée de résultats de droit, cochez la case située à gauche de l'entrée de résultats de droit, puis sélectionnez **Supprimer**.

Figure 27-1 *Gestion des destinataires de droit*



28 Gestion des bons de travail

Les pilotes Identity Manager peuvent créer des bons de travail à la suite des événements qu'ils traitent. Par exemple, si vous utilisez un pilote de ressources humaines (SAP HR, PeopleSoft, etc.), vous pouvez configurer le pilote pour qu'il génère un bon de travail chaque fois qu'un nouvel utilisateur est ajouté.

Vous pouvez utiliser Identity Console pour créer et gérer des bons de travail pour différents pilotes qui prennent en charge cette fonctionnalité.

Création d'un bon de travail

Pour créer un bon de travail, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Bon de travail**.
2. Cliquez sur l'icône + pour créer un bon de travail.
3. Indiquez le nom du bon de travail, puis cliquez sur **OK**.

   Le nom est utilisé pour désigner l'objet Bon de travail dans le coffre-fort d'identité.
4. Renseignez les champs suivants :

   État : l'état d'un nouveau bon de travail peut être **En attente** ou **En suspens**. Normalement, l'état d'un bon de travail est **En attente**. Vous pouvez arrêter un bon de travail en sélectionnant **En suspens**. Lorsqu'un bon de travail a été traité, l'état résultant apparaît dans ce champ.

   Échéance : Vous pouvez demander au pilote de faire le bon de travail immédiatement ou programmer celui-ci. Pour planifier une date d'échéance, cliquez sur l'icône de calendrier. Utilisez le calendrier pour choisir la date souhaitée. Utilisez les flèches pour sélectionner le mois, l'année et l'heure.

   Répéter un bon de travail: sélectionnez cette option pour que le bon de travail soit traité plusieurs fois. Indiquez l'intervalle de temps en choisissant le nombre de semaines, de jours, d'heures ou de minutes avant que le bon de travail ne se répète. Le bon de travail cesse de se répéter à la date de suppression, sauf s'il est manuellement supprimé ou édité ou si le pilote renvoie un message d'erreur.

   Date de suppression: Utilisez la commande du calendrier pour sélectionner une date pour supprimer les bons de travail configurés. Les bons de travail comportant un état d'erreur ne sont pas supprimés, sauf si vous sélectionnez l'option **Supprimer le bon de travail même s'il comporte une erreur**.

Bons de travail dépendants: lorsque vous créez un bon de travail, vous pouvez le rendre dépendant d'un ou de plusieurs bons de travail. Cliquez sur pour rechercher et sélectionner les bons de travail dépendants. Pour supprimer un bon de travail de la liste, sélectionnez-le, puis cliquez sur .

Type : utilisez ce champ pour spécifier un type de bon de travail. Le pilote ne modifie pas cet attribut. L'attribut est transmis à l'objet WorkToDo lors du traitement du bon de travail.

Numéro de bon de travail: indiquez le numéro unique du bon de travail. Cette valeur peut être assignée par un système de bons de travail d'entreprise différent de NetIQ eDirectory (par exemple, une base de données de bons de travail).

Coordonnées: Coordonnées de la personne responsable du bon de travail.

Journal de traitement du bon de travail: lorsqu'un bon de travail a été traité, le pilote consigne les résultats du bon de travail avec son état dans ce champ. Ainsi, vous pouvez vérifier l'état actuel du bon de travail et identifier d'éventuels problèmes rencontrés par le pilote lors de la tentative de configuration du bon de travail.

L'attribut d'état du bon de travail reste en attente jusqu'à son traitement. Le bon de travail est traité à l'expiration de la date d'échéance. Le pilote signale les résultats de traitement en définissant l'attribut de statut sur Configuré, Avertissement, ou Erreur. Si le bon de travail est en suspens, il est ignoré.

- **Pending (En attente) :** le pilote attend la date d'échéance pour terminer le bon de travail.
- **Configuré:** le bon de travail a été traité avec succès.
- **Error (Erreur) :** le pilote n'a pas pu effectuer le bon de travail.
- **Avertissement :** il existe un avertissement concernant le bon de travail. Par exemple, si le bon de travail a un bon de travail dépendant avec une date d'échéance ultérieure, le pilote envoie un avertissement.

Description : La description du bon de travail.

Contenu du bon de travail : les données de ce champ sont utilisées par les règles du pilote pour traiter le bon de travail. Par exemple, il peut s'agir du code XML que la transformation de la commande utilise pour traiter le bon de travail.

Suppression d'un ordre de travail existant

Pour supprimer un ordre de travail existant, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Bon de travail**.
2. Sélectionnez le bon de travail à supprimer.
3. Cliquez sur l'icône .

Filtrage de la liste des bons de travail

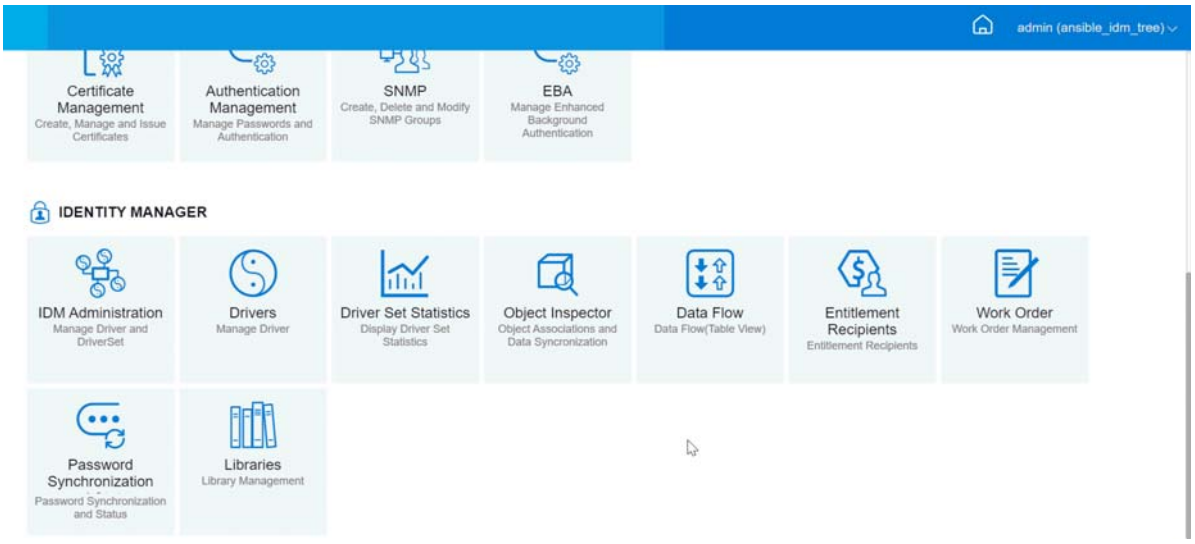
Pour filtrer la liste des bons de travail, procédez comme suit :

1. Sur la page de renvoi d'Identity Console, cliquez sur l'option **Bon de travail**.
2. Sous Gestion des bons de travail, cliquez sur **Opérations**.

3 Dans le menu déroulant, sélectionnez le type de filtre :

- **Tout afficher :** tous les bons de travail associés au pilote sont répertoriés.
- **Configuré:** seuls les bons de travail configurés associés au pilote sont répertoriés.
- **Error (Erreur) :** seuls les bons de travail comportant un état d'erreur sont répertoriés.
- **En suspens:** les bons de travail placés manuellement en suspens sont répertoriés.
- **Pending (En attente) :** les bons de travail qui ne sont pas encore à échéance sont répertoriés.

Figure 28-1 *Gestion des bons de travail*



29 Gestion de l'état et de la synchronisation du mot de passe

Vous pouvez vérifier la synchronisation et l'état du mot de passe de chaque pilote à l'aide du portail Identity Console. Pour cela, sur la page principale d'Identity Console, sélectionnez le module **Synchronisation du mot de passe**.

Grâce à ce module, vous pouvez effectuer les opérations suivantes :

- « Vérification de l'état de synchronisation du mot de passe » page 199
- « Vérification des paramètres de synchronisation du mot de passe » page 200

Vérification de l'état de synchronisation du mot de passe

Vous pouvez déterminer si le mot de passe de distribution d'un utilisateur donné est identique au mot de passe du système connecté. Pour vérifier l'état de synchronisation du mot de passe, procédez comme suit :

1. Dans Identity Console, sélectionnez **Synchronisation du mot de passe** > **État du mot de passe**.
2. Recherchez et sélectionnez l'utilisateur dont vous souhaitez consulter l'état du mot de passe.
3. Les différents états de mot de passe sont les suivants :
   - Les mots de passe sont synchronisés.
   - Les mots de passe NE sont PAS synchronisés.
   - L'état du mot de passe est inconnu car il est impossible de contacter le système connecté pour demander une vérification du mot de passe.
   - Une erreur s'est produite.

REMARQUE : Pour afficher plus de détails sur chacun des états ci-dessus, passez le pointeur de la souris sur l'état concerné dans la colonne **État du mot de passe**.

La tâche État du mot de passe amène le pilote à procéder à une vérification du mot de passe de l'objet. Tous les pilotes ne prennent pas en charge la vérification du mot de passe. Ceux qui le font doivent contenir une fonction de vérification de mot de passe dans le manifeste du pilote. Identity Console n'autorise pas l'envoi d'opérations de vérification du mot de passe aux pilotes dont le manifeste ne contient pas cette fonctionnalité.

L'opération Vérifier le mot de passe de l'objet traite le mot de passe de distribution. Si le mot de passe de distribution n'est pas mis à jour, la vérification du mot de passe de l'objet pourrait signaler que les mots de passe ne sont pas synchronisés.

Le mot de passe de distribution n'est pas mis à jour dans les cas suivants :

- Vous utilisez la méthode de synchronisation à l'aide du mot de passe NDS ou du mot de passe universel. Pour plus d'informations, reportez-vous à la section « Création d'une stratégie de mot de passe avec des paramètres personnalisés » page 118.

REMARQUE : l'opération État du mot de passe vérifie le mot de passe NDS au lieu du mot de passe universel pour le coffre-fort d'identité. Autrement dit, si la stratégie de mot de passe de l'utilisateur ne spécifie pas que le mot de passe NDS doit être synchronisé avec le mot de passe universel, les mots de passe sont toujours signalés comme n'étant pas synchronisés. En fait, le mot de passe de distribution et le mot de passe sur le système connecté pourraient être synchronisés, mais la vérification de l'état des mots de passe ne sera pas exacte, à moins que le mot de passe NDS et le mot de passe de distribution ne soient synchronisés avec le mot de passe universel.

Vérification des paramètres de synchronisation du mot de passe

Grâce à la synchronisation des mots de passe, vous pouvez synchroniser les mots de passe entre systèmes connectés à l'aide d'Identity Manager. Pour afficher les paramètres de synchronisation du mot de passe des systèmes connectés, sélectionnez l'ensemble de pilotes approprié dans la liste déroulante.

La synchronisation des mots de passe permet de configurer des systèmes connectés pour effectuer les opérations suivantes :

- Publier des mots de passe vers Identity Manager.
- S'abonner aux mots de passe émis par Identity Manager ou d'autres systèmes connectés.
- Appliquer les stratégies de mot de passe aux systèmes connectés.
- Envoyer des messages de notification.

Pour vérifier les paramètres de synchronisation du mot de passe, procédez comme suit :

1. Sur la page principale d'Identity Console, sélectionnez **Synchronisation du mot de passe** > **Synchronisation du mot de passe**.
2. Recherchez l'ensemble de pilotes qui contient le pilote dont vous souhaitez vérifier les paramètres.
3. Cliquez sur le nom du pilote souhaité dans la liste.

   REMARQUE : les paramètres activés et désactivés varient en fonction du pilote. Seuls les paramètres des fonctions prises en charge par le pilote sont disponibles.

   ---

4. Vérifiez que les paramètres sont configurés correctement.

   Identity Manager accepte les mots de passe (canal Éditeur): si cette option est activée, Identity Manager autorise la circulation des mots de passe du système connecté vers le coffre-fort d'identité. Si vous désactivez cette option, aucun élément <password> (mot de passe) ne peut circuler vers Identity Manager. Ils sont supprimés de XML par une stratégie de synchronisation de mot de passe sur le canal Éditeur.

Ce paramètre s'applique aux mots de passe utilisateur fournis par le système connecté et aux valeurs de mot de passe créées par une stratégie sur le canal Éditeur.

Si cette option est activée mais que l'option Mot de passe de distribution ci-dessous est désactivée, une valeur <password> (mot de passe) provenant du système connecté est écrite directement dans le mot de passe universel dans le coffre-fort d'identité. Si la stratégie de mot de passe de l'utilisateur n'autorise pas le mot de passe universel, le mot de passe est écrit dans le mot de passe NDS.

Utiliser le mot de passe de distribution pour la synchronisation de mot de passe: ce paramètre est disponible uniquement si le paramètre **Identity Manager accepte les mots de passe (canal Éditeur)** est activé.

Si cette option est activée, une valeur de mot de passe issue du système connecté est écrite dans le mot de passe de distribution. Le mot de passe de distribution est réversible, c'est-à-dire qu'il est possible de l'extraire de la banque de données du coffre-fort d'identité en vue de la synchronisation du mot de passe. Il est utilisé par Identity Manager pour la synchronisation bidirectionnelle du mot de passe avec les systèmes connectés. Cette option doit être activée pour qu'Identity Manager puisse distribuer les mots de passe de ce système aux autres systèmes.

Accepter le mot de passe uniquement s'il respecte la stratégie de mot de passe de l'utilisateur : ce paramètre n'est disponible que si le paramètre **Utiliser le mot de passe de distribution pour la synchronisation du mot de passe** est activé.

Si vous sélectionnez cette option, Identity Manager n'écrit pas le mot de passe depuis ce système connecté vers le mot de passe de distribution du coffre-fort d'identité et ne le publie pas sur les systèmes connectés si le mot de passe ne respecte pas la stratégie de mot de passe de l'utilisateur.

Si un mot de passe n'est pas conforme, activez le paramètre **Reset the user's password to the Distribution Password)** (Réinitialiser le mot de passe de l'utilisateur sur le mot de passe de distribution) pour réinitialiser le mot de passe de l'utilisateur sur le système connecté. Vous pouvez ainsi appliquer la stratégie de mot de passe sur le système connecté ainsi que dans le coffre-fort d'identité. Si vous ne sélectionnez pas cette option, les mots de passe utilisateur peuvent ne plus être synchronisés sur les systèmes connectés. Toutefois, vous devez tenir compte des stratégies de mot de passe du système connecté lorsque vous décidez d'utiliser ou non cette option. Certains systèmes connectés peuvent ne pas autoriser la réinitialisation car ils ne permettent pas la répétition des mots de passe.

Si vous utilisez le paramètre **Notifier à l'utilisateur l'échec de la synchronisation du mot de passe par courrier électronique**, vous pouvez informer les utilisateurs de l'échec de définition ou de réinitialisation d'un mot de passe. La notification est particulièrement utile pour cette option. Si l'utilisateur change de mot de passe en adoptant un mot de passe accepté par le système connecté mais refusé par Identity Manager car non conforme à la stratégie de mot de passe, il ne sera informé de la réinitialisation de son mot de passe que lorsqu'il recevra une notification ou qu'il tentera de se connecter avec son ancien mot de passe au système connecté.

Toujours accepter les mots de passe ; ignorer les stratégies de mot de passe: ce paramètre n'est disponible que si le paramètre **Utiliser le mot de passe de distribution pour la synchronisation du mot de passe** est activé.

Si vous sélectionnez cette option, Identity Manager n'applique pas la stratégie de mot de passe de l'utilisateur pour ce système connecté. Identity Manager écrit le mot de passe de ce système connecté dans le mot de passe de distribution du coffre-fort d'identité et le distribue aux autres systèmes connectés, indépendamment du respect de la stratégie de mot de passe.

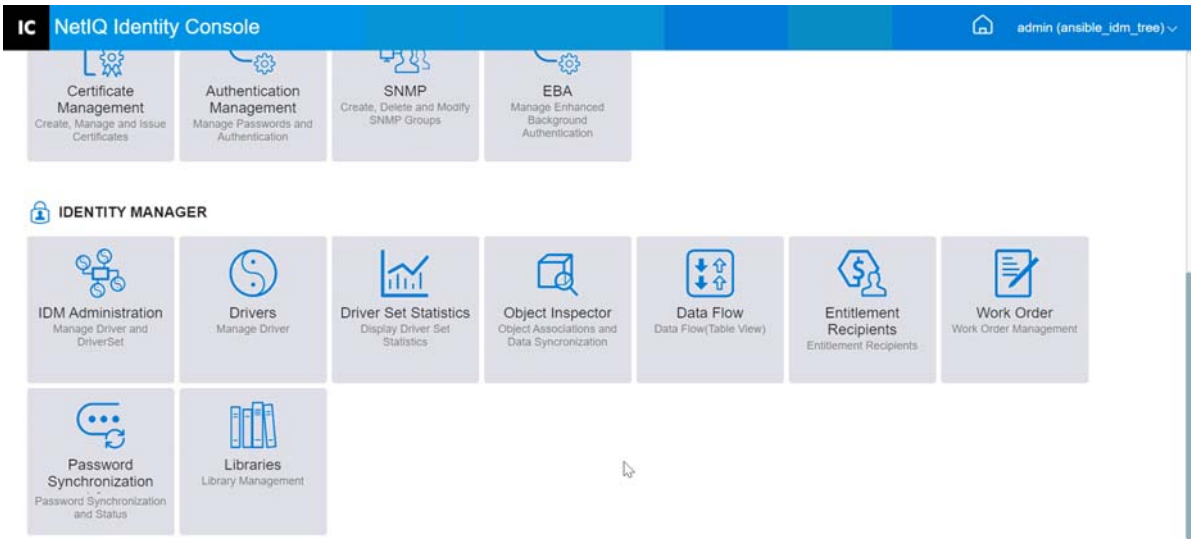
L'application accepte les mots de passe (canal Abonné): si vous sélectionnez cette option, le pilote envoie les mots de passe du coffre-fort d'identité vers ce système connecté. Ainsi, si un utilisateur modifie le mot de passe sur un autre système connecté qui publie les mots de passe vers le mot de passe de distribution du coffre-fort d'identité, le mot de passe est modifié sur ce système connecté.

Par défaut, le mot de passe de distribution est identique au mot de passe universel du coffre-fort d'identité, ce qui permet d'envoyer au système connecté les modifications du mot de passe universel réalisées dans le coffre-fort d'identité.

Informer l'utilisateur de l'échec de la synchronisation des mots de passe par message électronique: si vous sélectionnez cette option, un message électronique est envoyé à l'utilisateur si un mot de passe n'est pas synchronisé, défini ou réinitialisé. Le message envoyé à l'utilisateur repose sur un modèle de message électronique. Ce modèle est fourni par l'application de synchronisation de mot de passe. Toutefois, pour que le modèle fonctionne, vous devez le personnaliser et spécifier un serveur de messagerie pour l'envoi des messages de notification. Pour obtenir les instructions correspondantes, reportez-vous à la section Configuring E-Mail Notification (Configuration de la notification par courrier électronique) dans le manuel *NetIQ Identity Manager Password Management Guide* (Guide de gestion des mots de passe dans NetIQ Identity Manager).

5 Lorsque vous avez terminé, cliquez sur **Enregistrer** pour enregistrer les modifications apportées. Les paramètres sont enregistrés en tant que valeurs de configuration globale.

Figure 29-1 *Gestion de la synchronisation des mots de passe*



30 Gestion des bibliothèques

Les objets Bibliothèque stockent plusieurs stratégies et d'autres ressources partagées par un ou plusieurs pilotes. Vous pouvez créer un objet Bibliothèque dans un objet Ensemble de pilotes ou dans n'importe quel conteneur eDirectory. Une arborescence eDirectory peut contenir plusieurs bibliothèques. Un pilote peut faire référence à n'importe quelle bibliothèque de l'arborescence tant que le serveur qui exécute le pilote contient une réplique en lecture/écriture ou maîtresse de l'objet Bibliothèque.

Les feuilles de style, les stratégies, les règles et les autres objets Ressource peuvent être stockés dans une bibliothèque et être référencés par un ou plusieurs pilotes.

Grâce au module Library Management (Gestion des bibliothèques), vous pouvez effectuer les tâches suivantes :

- « Affichage et suppression d'une bibliothèque existante » page 203
- « Affichage et suppression d'un objet de la bibliothèque » page 203

Affichage et suppression d'une bibliothèque existante

Pour afficher et supprimer une bibliothèque existante, procédez comme suit :

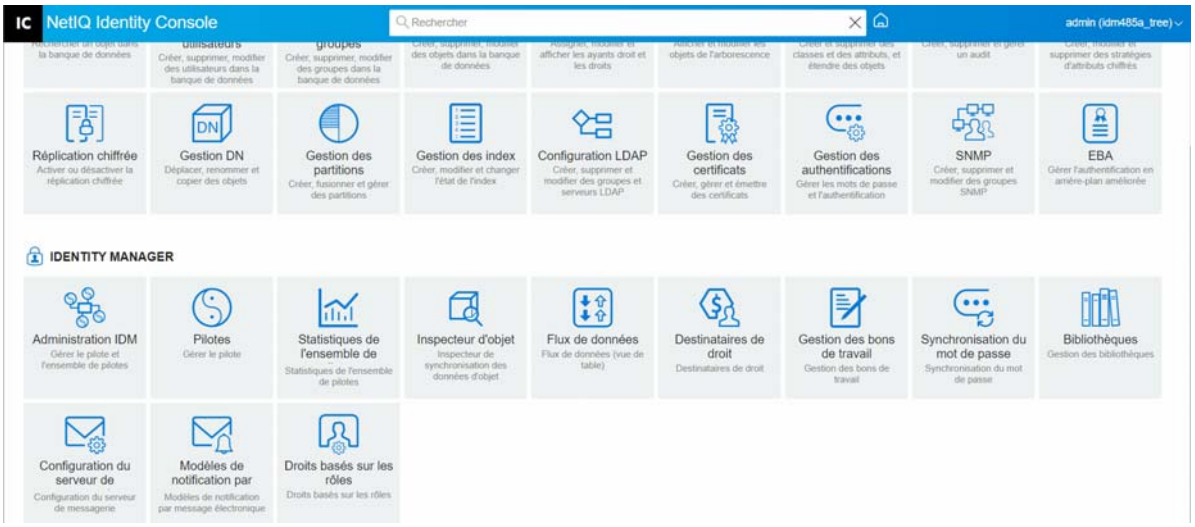
1. Sur la page d'accueil d'Identity Console, sélectionnez le module **Libraries** (Bibliothèques).
2. Sélectionnez la bibliothèque appropriée dans la liste.
3. Cliquez sur l'icône . Cliquez sur **OK** pour confirmer l'opération.

Affichage et suppression d'un objet de la bibliothèque

Vous pouvez afficher et supprimer des stratégies et des tables d'assignation à partir des objets Bibliothèque. Pour supprimer un objet, procédez comme suit :

1. Sur la page d'accueil d'Identity Console, sélectionnez le module **Libraries** (Bibliothèques).
2. Cliquez sur la bibliothèque appropriée dans la liste.
3. Pour supprimer une stratégie, sélectionnez l'onglet **Stratégies**.
4. Sélectionnez la stratégie appropriée dans la liste, puis cliquez sur l'icône .
5. Pour supprimer une table d'assignation, sélectionnez l'onglet **Tables d'assignation**.
6. Sélectionnez la table d'assignation appropriée dans la liste, puis cliquez sur l'icône .
7. Cliquez sur **OK** pour confirmer l'opération.

Figure 30-1 *Gestion des bibliothèques*



31 Gestion des options du serveur de messagerie

Vous pouvez utiliser les options du serveur de messagerie pour spécifier les paramètres du serveur de messagerie SMTP.

Nom d'hôte

Nom de l'hôte de votre serveur de messagerie SMTP. Il peut également s'agir d'une adresse IP. Vous pouvez également spécifier un port personnalisé suivi du nom ou de l'adresse IP de l'hôte.

IMPORTANT : utilisez les deux-points (:) comme séparateur entre le nom ou l'adresse IP de l'hôte et le port.

De

Vous pouvez spécifier une adresse électronique valide qui s'affiche en tant que champ De de l'en-tête d'un message électronique.

Valeur de timeout

L'option de timeout permet de définir le délai (en secondes) d'envoi des messages électroniques de notification.

Voulez-vous activer SSL ?

Vous pouvez activer l'option SSL, si nécessaire.

Authentification auprès du serveur avec les références

Cette option renforce la sécurité du serveur SMTP. Si votre serveur demande une authentification avant d'envoyer un message électronique, spécifiez le nom d'utilisateur et le mot de passe ici.

Bien que les informations d'authentification soient spécifiées ici, vous pouvez aussi être amené à les spécifier de manière séparée pour l'application qui envoie les messages de notification.

Par exemple, vous pouvez utiliser les informations d'authentification que vous indiquez ici pour envoyer des messages de notification Mot de passe oublié. Cependant, le module de synchronisation de mots de passe d'Identity Manager utilise la stratégie du pilote pour envoyer des messages de notification. Il se peut que vous deviez également fournir les informations d'authentification de cette stratégie du pilote.

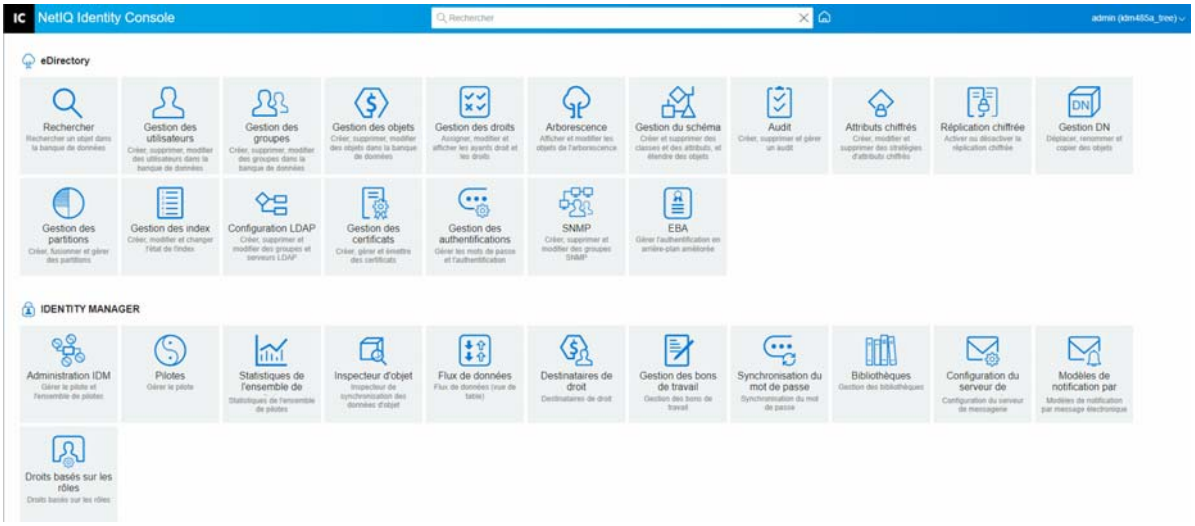
Pour authentifier le serveur, procédez comme suit :

1. Sélectionnez l'option **Authentification sur le serveur avec des informations d'identification**.
2. Indiquez un **nom d'utilisateur** et un **mot de passe**.
3. Cliquez sur **Tester la connexion au serveur** pour vérifier la connectivité.

4. Cliquez sur **Enregistrer**.

REMARQUE : après que vous avez enregistré les informations d'identification, l'option **Tester la connexion au serveur** est désactivée.

Figure 31-1 *Configuration du serveur de messagerie*



32 Gestion des modèles de messages électroniques

Cette liste affiche les modèles de notification disponibles. Ces modèles servent à envoyer un message électronique aux utilisateurs de cette arborescence. Vous pouvez personnaliser ces modèles avec le texte de votre choix.

Certaines applications fournissent leurs propres modèles. Ces objets Modèle sont placés dans le conteneur de sécurité, généralement situé à la racine de l'arborescence.

Vous pouvez trier la liste par nom, par date ou par objet.

Objet

Le texte que voit un utilisateur dans le titre de l'objet du message électronique. Pour modifier un modèle, cliquez sur le titre de l'objet de ce modèle. Grâce à l'interface Éditer le modèle de notification par message électronique, vous pouvez modifier le modèle et ses détails.

Nom du modèle

Le nom de chaque modèle est unique. L'application qui envoie le message électronique fait référence à ce nom.

Dernière modification

La date et l'heure de la dernière modification du modèle.

Nouveau

Permet de créer un modèle de message électronique.

1. Cliquez sur l'icône +.
2. Indiquez le nom du nouveau modèle (par exemple, Approbation), puis cliquez sur **OK**.

Si vous avez désactivé les fenêtres contextuelles, vous revenez à la fenêtre contextuelle Éditer le modèle de notification par message électronique. Le nom du nouveau modèle apparaît dans la colonne Nom, mais [Sans objet] apparaît dans la colonne de titre de l'objet. Dans ce cas, cliquez sur [Sans objet] afin de pouvoir fournir des détails dans le nouveau modèle.

Éditer le modèle de notification par message électronique

La page Éditer le modèle de notification par message électronique permet de modifier le modèle de message électronique. Vous pouvez personnaliser le modèle avec le texte de votre choix.

Nom du modèle

Affiche le nom du modèle.

Objet

Le texte que voit un utilisateur dans le titre de l'objet du message électronique. Vous pouvez modifier le texte de la ligne Objet. Le nom réel du modèle ne change pas.

Envoyer en tant que

Format utilisé par le serveur SMTP pour envoyer le message électronique : texte ou HTML.

Jetons ou balises de remplacement

Les balises de remplacement permettent de personnaliser le message en fonction de l'utilisateur. Vous pouvez copier des balises de remplacement dans la liste des balises disponibles et les coller dans le message.

Chaque modèle comprend des jetons ou balises de remplacement par défaut. Ces variables sont nécessaires pour personnaliser le message électronique en fonction de l'utilisateur. Par exemple, le modèle de message Mot de passe oublié qui envoie un mot de passe à l'utilisateur contient le jeton ou la balise de remplacement par défaut « CurrentPassword ».

Ajouter : vous pouvez définir d'autres jetons ou balises de remplacement à utiliser dans le corps du message.

Pour ajouter un jeton ou une balise de remplacement, procédez comme suit :

1. Cliquez sur l'icône  .
2. Indiquez le **nom** et la **description** souhaités dans la fenêtre **Add Replacement Tag** (Ajouter une balise de remplacement).
3. Cliquez sur **OK**.
4. Le nouveau jeton ou la nouvelle balise de remplacement s'affiche dans la colonne Balises de remplacement.

Copier la balise : cliquez sur  pour copier la balise sélectionnée dans le tampon système, puis cliquez pour la coller et l'utiliser dans la ligne d'objet ou le corps du message.

Supprimer : sélectionnez un jeton ou une balise de remplacement dans la liste, puis cliquez sur  pour supprimer la balise de la liste. Veillez à ne pas supprimer de balises nécessaires pour le corps du message.

Corps du message

Texte du message électronique.

Cliquez sur **Mettre à jour** après avoir apporté toutes les modifications au modèle de notification par message électronique.

Supprimer

Supprime (du coffre-fort d'identité) les modèles que vous avez créés. Vous ne pouvez pas supprimer les modèles par défaut fournis avec les applications telles qu'Identity Manager.

1. Sélectionnez le modèle à supprimer.

Si vous cliquez sur la ligne d'objet du modèle, Identity Console ouvre la boîte de dialogue Edit Email Templates (Éditer les modèles de message électronique).

2. Cliquez sur l'icône Supprimer.
3. Cliquez sur **OK**.

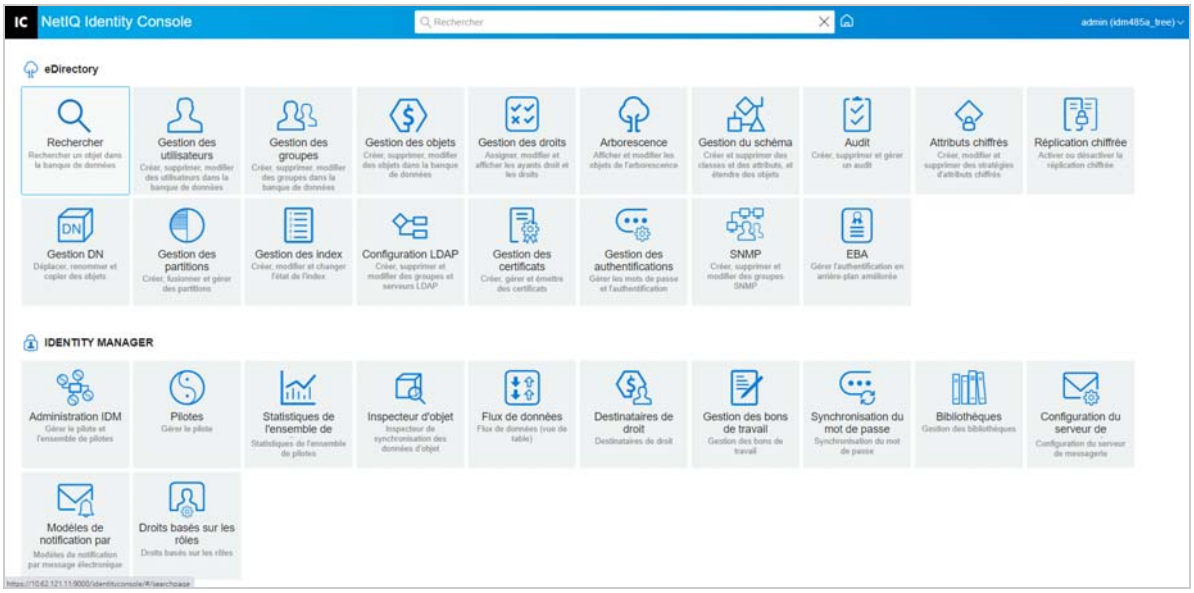
Filtrer les modèles

Permet de filtrer les modèles de message électronique à afficher. Seuls les modèles sélectionnés s'affichent. L'option de filtrage de tous les modèles de message électronique affiche l'ensemble des modèles.

Rafraîchir les modèles

Cliquez sur l'icône pour rafraîchir et supprimer les modèles de filtre appliqués.

Figure 32-1 *Modèles de notification par message électronique*



33 Gestion des droits basés sur les rôles

Grâce aux droits RBE, vous pouvez octroyer des droits sur les systèmes connectés à un groupe d'utilisateurs de NetIQ® Identity Console. Les stratégies RBE permettent de rationaliser la gestion des stratégies d'entreprise et de limiter la configuration des pilotes Identity Manager.

Le module Droits basés sur les rôles comprend les fonctionnalités suivantes :

Droits basés sur les rôles

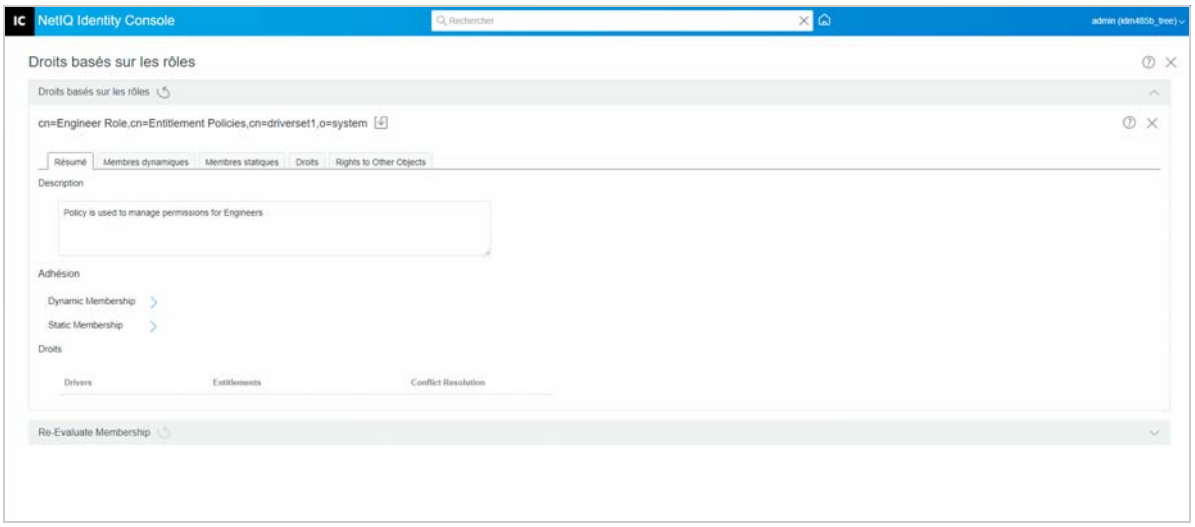
Une stratégie RBE est un objet Groupe dynamique d'Identity Console doté de fonctions supplémentaires qui permettent d'octroyer des droits RBE sur les systèmes connectés. Lorsque vous créez une stratégie RBE, vous devez définir les membres de la stratégie et les droits à leur accorder. Chaque stratégie RBE est associée à un seul objet Ensemble de pilotes assigné à un serveur donné. À l'instar d'un pilote Identity Manager, chaque stratégie de droits ne peut gérer que les objets d'une réplique maître ou lecture/écriture sur le serveur auquel elle est assignée.

Les sections ci-après expliquent en détail les droits basés sur les rôles :

Résumé

Cette page affiche une vue de haut niveau des critères d'adhésion et des droits pour la stratégie de droits.

Figure 33-1 *Page de résumé*



Adhésion :

Les critères spécifiés pour les membres dynamiques sont affichés avec la syntaxe d'un filtre LDAP. Le champ Rechercher une identité indique l'objet dont les droits sont utilisés pour la requête de membres dynamiques, et les champs DN de base et Étendue indiquent la portion de l'arborescence sur laquelle porte la requête.

Vous pouvez afficher les inclusions et exclusions de membres statiques en cochant la case.

La liste globale des membres n'est pas affichée sur la page Résumé car elle risquerait d'être trop longue. Pour voir une liste combinée de tous les membres de la stratégie de droit, qu'ils soient dynamiques ou statiques, utilisez l'onglet Membre > Afficher les membres.

Droits :

Droits sur les systèmes connectés accordés aux membres de la stratégie de droit. N'oubliez pas que les droits basés sur les rôles ne sont pas étroitement liés aux systèmes connectés. Autrement dit, l'état d'un droit sur un système connecté ne s'affiche pas dans l'interface stratégie de droit. Si vous accordez un droit à une stratégie de droit et si, par la suite, ce droit n'est plus disponible sur le système connecté, il continue de figurer dans la stratégie de droit jusqu'à ce que vous le supprimiez manuellement.

Résolution des conflits :

Pour les droits RBE associés à des valeurs, les méthodes de résolution des conflits permettent de déterminer les valeurs attribuées à un utilisateur si plusieurs stratégies RBE lui accordent des valeurs différentes. L'appartenance à une liste de distribution de courrier électronique est un exemple de droit associé à des valeurs (ici, le nom des listes de distribution).

La méthode de résolution des conflits est définie séparément pour chaque droit sur chaque objet Pilote. Si un droit est utilisé dans plusieurs stratégies RBE, la méthode utilisée est la même pour toutes les stratégies RBE. Pour changer la méthode de résolution des conflits associée à un droit, modifiez le paramètre correspondant à ce droit dans le manifeste du pilote.

- **Non reconnu :** la stratégie RBE n'a pas été terminée dans l'assistant, ou le paramètre a été entré de façon incorrecte dans le manifeste du pilote.

- **Fusionner :** le paramètre par défaut est Fusionner (`union` dans le manifeste du pilote). L'utilisateur obtient, pour le droit concerné, toutes les valeurs découlant de toutes les stratégies RBE dont il est membre.

  Lorsque ce paramètre par défaut est utilisé, l'ordre de priorité des stratégies n'a pas d'importance pour le droit concerné.

  Par exemple, un utilisateur peut se voir accorder le droit d'être membre de listes de distribution de courrier électronique pour le pilote GroupWise® A par deux stratégies RBE différentes, la stratégie Gestionnaires et la stratégie Membres de l'équipe. Avec la première stratégie, l'utilisateur devient membre de la liste de distribution de courrier électronique Gestionnaires ; avec la seconde, il devient membre de la liste de distribution Membres de l'équipe. Si le paramètre est défini sur Fusionner, l'utilisateur devient membre des deux listes de distribution de courrier électronique.

- **Priorité :** ce paramètre indique que, si plusieurs stratégies RBE accordent à un utilisateur des valeurs différentes pour le même droit à partir du même objet Pilote, l'utilisateur ne se voit accorder que les valeurs spécifiées dans la stratégie RBE la plus élevée de la liste.

  Lorsque le paramètre Priorité est utilisé, l'ordre de priorité des stratégies est important pour le droit concerné.

  Par exemple, un utilisateur peut se voir accorder le droit d'être membre de listes de distribution de courrier électronique pour le pilote GroupWise A par deux stratégies RBE différentes, la stratégie Gestionnaires et la stratégie Membres de l'équipe. Avec la stratégie Gestionnaires, l'utilisateur devient membre de la liste de distribution de courrier électronique Gestionnaires ; avec la stratégie Membres de l'équipe, il devient membre de la liste de distribution Membres de l'équipe. La stratégie Gestionnaires apparaît dans la liste de stratégies avant la stratégie Membres de l'équipe. Si le paramètre est défini sur Fusionner, l'utilisateur devient membre de la liste de distribution de courrier électronique Gestionnaires uniquement.

  Le paramètre de résolution des conflits Priorité peut s'avérer utile si, par exemple, un attribut autorise seulement une valeur sur le système connecté. Si deux stratégies RBE différentes accordent chacune une valeur à l'utilisateur, celui-ci obtiendra la valeur accordée par la stratégie RBE qui figure en premier dans la liste.

REMARQUE : aucun paramètre de résolution des conflits n'est fourni pour les droits qui ne sont pas associés à des valeurs, par exemple les comptes. Les droits de ce type sont toujours accordés aux membres de la stratégie RBE, quelle que soit la priorité des stratégies dans la liste.

Membres dynamiques

Les critères spécifiés pour les membres dynamiques sont affichés avec la syntaxe d'un filtre LDAP. Le champ Rechercher une identité indique l'objet dont les droits sont utilisés pour la requête de membres dynamiques, et les champs DN de base et Étendue indiquent la portion de l'arborescence sur laquelle porte la requête.

Filtre d'adhésion

Vous pouvez définir les critères d'adhésion, comme l'emplacement dans l'arborescence et les attributs de l'objet correspondant. Par exemple, l'adhésion à la stratégie peut dépendre de la présence de l'utilisateur dans le conteneur actif ou de la présence dans l'intitulé de la fonction du

mot Responsable. Les utilisateurs qui répondent aux critères définis deviennent automatiquement membres de la stratégie RBE. Vous n'avez pas à les ajouter un par un. L'adhésion dynamique revient à définir un objet Groupe dynamique.

Si un objet est modifié et ne répond plus aux critères, les droits de l'utilisateur sont automatiquement révoqués lorsque ce dernier est réévalué.

Définir les paramètres de recherche

Indiquez l'emplacement des utilisateurs que la stratégie de droit doit gérer. Choisissez le conteneur où se trouvent les utilisateurs (DN de base) et indiquez sur quel niveau la recherche doit porter (Étendue de la recherche). Pour que la stratégie de droit puisse gérer les utilisateurs du conteneur spécifié, les utilisateurs doivent se trouver dans une réplique en lecture/écriture ou une réplique maîtresse sur le serveur.

Les options d'étendue de la recherche sont les suivantes :

- Ce conteneur et les sous-conteneurs : les utilisateurs qui se trouvent sous ce conteneur dans l'arborescence sont des membres de la stratégie de droits s'ils respectent les critères spécifiés pour l'adhésion dynamique. Les utilisateurs présents dans les sous-conteneurs peuvent également être membres s'ils répondent aux critères.
- Uniquement ce conteneur : les utilisateurs qui appartiennent à ce conteneur ne sont membres de la stratégie de droits que s'ils respectent les critères spécifiés pour l'adhésion dynamique. Les utilisateurs présents dans les sous-conteneurs de ce conteneur ne peuvent pas être membres, même s'ils répondent à ces critères.

Définir les critères de filtrage

Indiquez les caractéristiques qui déterminent quels utilisateurs sont membres de la stratégie de droit.

Dans la page Résumé d'une stratégie de droit, les critères applicables aux membres dynamiques apparaissent avec la syntaxe d'un filtre LDAP.

Par défaut, la définition dynamique des membres inclut dans l'étendue de la recherche tous les objets de la classe Utilisateur (ainsi que les objets des classes dérivées) comme membres de la stratégie de droit.

REMARQUE : si vous créez une classe d'objet dérivée de Utilisateur, une stratégie de droits existante n'a connaissance de cette classe que si vous modifiez cette stratégie. Cela évite que des droits ne soient accordés par mégarde aux utilisateurs d'une nouvelle classe. Lorsqu'une modification est apportée à la stratégie de droit, la liste des classes dérivées de la classe Utilisateur pour cette stratégie est mise à jour.

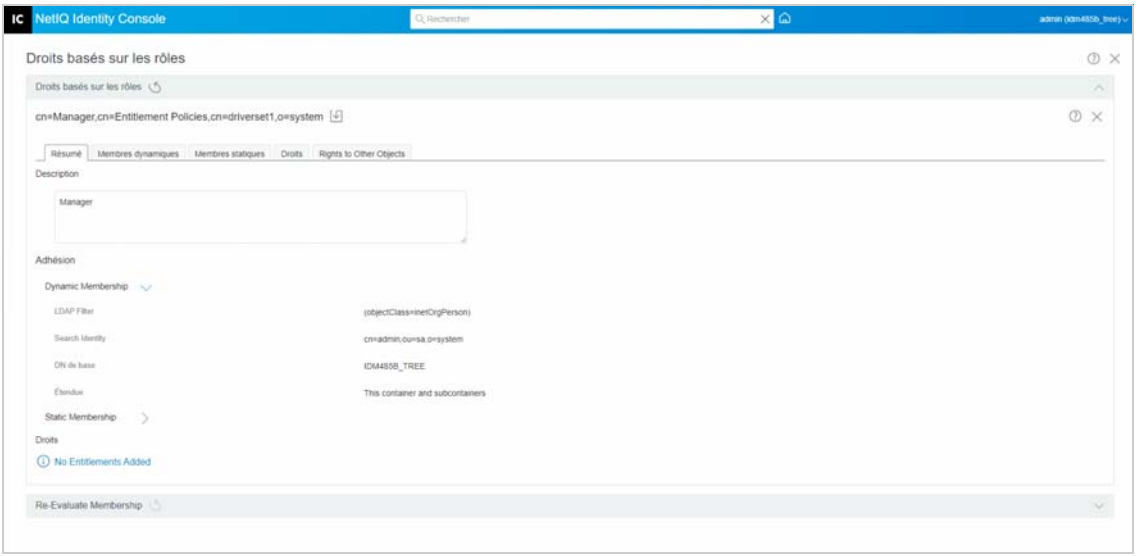
Création d'une adhésion dynamique

Sous l'onglet Membres dynamiques, procédez comme suit :

1. Cliquez sur l'onglet **Membres dynamiques**.
2. Utilisez les filtres **Identité de recherche**, **Commencer la recherche à** et **Étendue de la recherche** selon vos besoins.

3 Cliquez sur l'option **Créer un groupe** correspondante pour créer une condition ou une ligne, puis fournissez les critères de recherche ou les conditions requis.

Figure 33-2 *Membres dynamiques*



Étendue de la recherche : l'étendue de la recherche indique l'ensemble d'entrées au niveau ou au-dessous du DN de base de recherche qui peuvent être considérés comme des correspondances potentielles pour une opération de recherche.

Critères de recherche : vous pouvez limiter une recherche pour vous aider à localiser un enregistrement ou un groupe d'enregistrements spécifiques parmi un nombre important d'enregistrements.

DN de base : un DN de base est le point à partir duquel un serveur recherche des utilisateurs.

Groupe LDAP : organisation hiérarchique d'utilisateurs, de groupes et d'unités organisationnelles qui sont des conteneurs pour les utilisateurs et les groupes.

REMARQUE : l'utilisateur peut créer un ou plusieurs groupes avec des conditions. Les conditions sont constituées d'attributs, d'opérateurs et de valeurs. Par défaut, la condition **Classe d'objet** > **est égal** > **Utilisateur** est spécifiée.

Membres statiques

Les membres statiques sont une classe de membres déclarés à l'aide de mots-clés statiques. Un membre statique dispose de certains accès limités.

Sous l'onglet Membres statiques, vous pouvez effectuer les opérations suivantes :

Inclure des membres :

Ajoutez de manière statique les membres qui ne sont pas inclus par le filtre d'adhésion dynamique.

Exclure des membres :

Excluez les membres qui satisfont aux critères du filtre mais qui ne doivent pas être inclus dans la stratégie de droits.

Droits

Grâce aux droits RBE, vous pouvez octroyer des droits sur les systèmes connectés et des droits dans Identity Manager. Il peut s'agir de l'un des droits suivants :

- Comptes sur les systèmes connectés.
- Appartenance aux listes de distribution de courrier électronique sur les systèmes connectés.
- Appartenance à un groupe sur les systèmes connectés.
- Attributs des objets correspondants sur les systèmes connectés, selon les valeurs que vous spécifiez.

REMARQUE : la fonctionnalité Droits faisant partie d'Identity Manager, vous devez installer et configurer les pilotes Identity Manager pour qu'ils prennent en charge cette fonctionnalité avant de pouvoir accorder des droits sur les systèmes connectés.

Créer un droit

Sous l'onglet Droits, procédez comme suit :

1. Cliquez sur l'onglet **Droit**.
2. Cliquez sur + pour **ajouter des pilotes** et fournir des droits sur les systèmes connectés.

   L'écran **Add Driver** (Ajouter un pilote) s'affiche.
3. Sélectionnez le pilote de votre choix dans le menu déroulant.
4. Cliquez sur **Ajouter**.

   L'écran **Add Entitlements** (Ajouter des droits) s'affiche.
5. Dans le menu déroulant, sélectionnez le **groupe de droits** à ajouter.
6. Sélectionnez le **type de requête** :
   - **Cached (En cache) :** lorsque les requêtes ont déjà été exécutées.
   - **External Query (Requête externe) :** lorsque les requêtes sont nouvelles.

   L'écran **Add Group Entitlement** (Ajouter un droit de groupe) s'affiche.
7. Sélectionnez un droit de groupe dans le menu déroulant, puis cliquez sur **Sélectionner**.

Droits sur d'autres objets

Utilisez cette page pour donner à l'ayant droit d'une stratégie des droits sur un objet eDirectory. Chaque membre de la stratégie de droit devient alors un ayant droit de l'objet.

Vous pouvez assigner des droits à tous les attributs, mais également cliquer sur Ajouter une propriété pour assigner des droits à des propriétés spécifiques.

La case à cocher Hériter détermine si les droits sont répercutés aux niveaux inférieurs de l'arborescence. Si, par exemple, vous attribuez des droits à un objet Conteneur, et si vous souhaitez que la stratégie de droits attribue les mêmes droits aux objets et aux sous-conteneurs de ce conteneur, cochez cette case.

Les droits sur les objets eDirectory sont accordés aux membres de la stratégie de droit une fois que toutes les modifications ont été apportées sur cette page. En revanche, les droits dans les systèmes connectés sont accordés à chaque membre de la stratégie lorsqu'un attribut utilisé pour l'appartenance dynamique est modifié pour un utilisateur ou que l'utilisateur est déplacé ou renommé. La même chose s'applique lorsque des droits sont révoqués. La tâche de réévaluation de l'appartenance permet d'imposer une mise à jour.

Créer des droits sur d'autres objets

Pour créer des droits, procédez comme suit :

1 Cliquez sur l'onglet **Rights to Other Objects** (Droits sur d'autres objets).

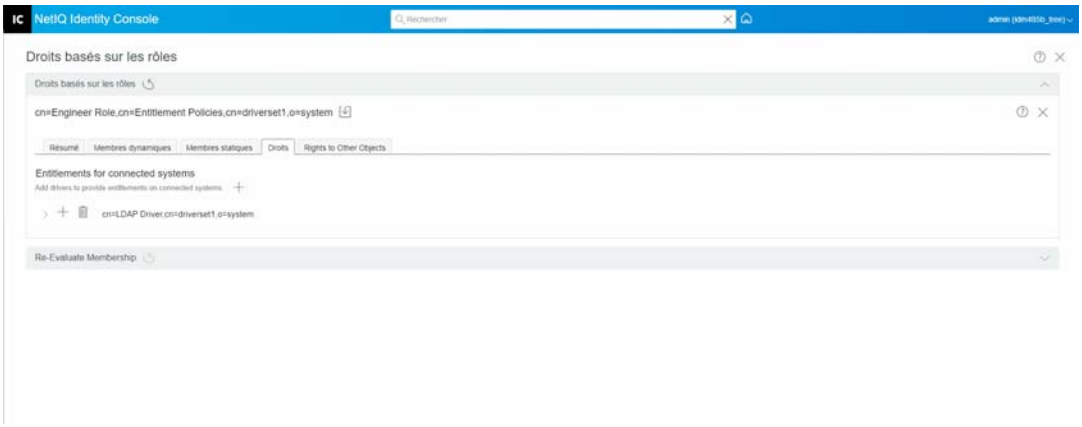
Vous pouvez ajouter un nouvel objet et rechercher les objets dont cette stratégie de droits doit être un ayant droit.

1a Pour ajouter un objet, cliquez sur le bouton +.

La page **PARCOUREUR DE CONTEXTE** s'affiche. Elle se compose d'`objets`.

1b Développez les `objets`, sélectionnez des groupes ou des utilisateurs selon vos besoins, puis assignez-leur des droits.

Figure 33-3 *Droits sur d'autres objets*

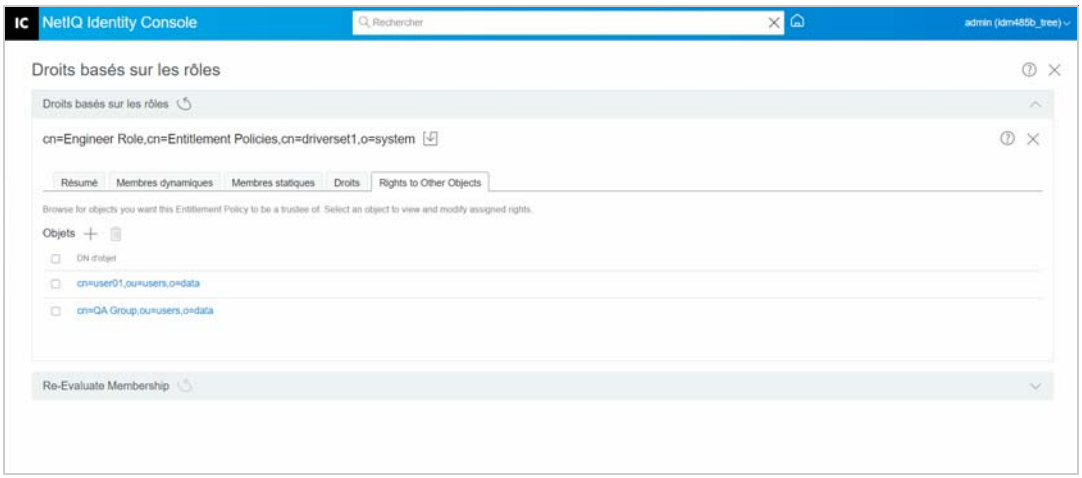


1c Pour ajouter d'autres propriétés, cliquez sur +.

La page **SÉLECTIONNER UNE PROPRIÉTÉ** s'affiche. Elle contient la liste des propriétés qu'un objet peut comporter.

1d Cliquez sur **Terminé**.

Figure 33-4 *Sélectionner des propriétés*



2 (Facultatif) Définissez la priorité des stratégies RBE à l'aide des flèches **haut** et **bas** .

La définition de la priorité des stratégies consiste à résoudre les conflits de droits entre plusieurs stratégies. La stratégie la plus élevée a la priorité la plus élevée. Pour plus d'informations, reportez-vous à la section « Définir la priorité des stratégies RBE » page 218.

Définir la priorité des stratégies RBE

Lorsque vous créez des stratégies RBE, il est possible que les stratégies concernant un utilisateur particulier soient en conflit.

Les stratégies RBE figurent dans la liste selon l'ordre de priorité. Vous pouvez changer l'ordre de la liste en utilisant les boutons fléchés vers le haut et vers le bas.

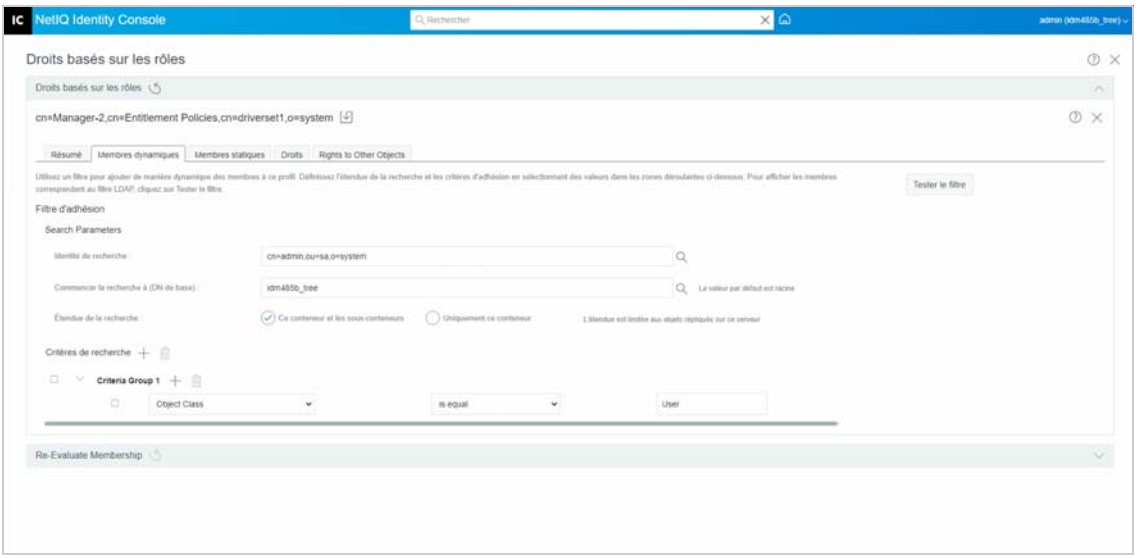
- Ce paramètre peut s'avérer utile si, par exemple, un attribut sur le système connecté n'autorise qu'une seule valeur. Si deux stratégies RBE différentes accordent chacune une valeur pour cet attribut au même utilisateur, celui-ci reçoit·la valeur de stratégie RBE qui figure en premier dans la liste. Supposons également que vous ayez configuré votre environnement pour qu'il utilise les droits pour placer les utilisateurs dans une hiérarchie sur un autre système. Vous voulez que chaque utilisateur soit placé à un endroit et pas à deux endroits à la fois.
- N'oubliez pas que ce paramètre peut être différent pour chaque droit offert par chaque pilote.
- En règle générale, vous devez placer les stratégies de gestionnaire ou d'administrateur plus haut dans la liste que les stratégies d'utilisateurs finals ou de simples collaborateurs. Placez les groupes les plus étroits avant les groupes les plus larges.

Pour définir la priorité des stratégies RBE :

1 Sélectionnez la stratégie de droits à mettre à niveau ou à passer à une version antérieure.

2 Définissez la priorité des stratégies RBE à l'aide des flèches **haut** et **bas** .

Figure 33-5 *Définition de la priorité des stratégies*

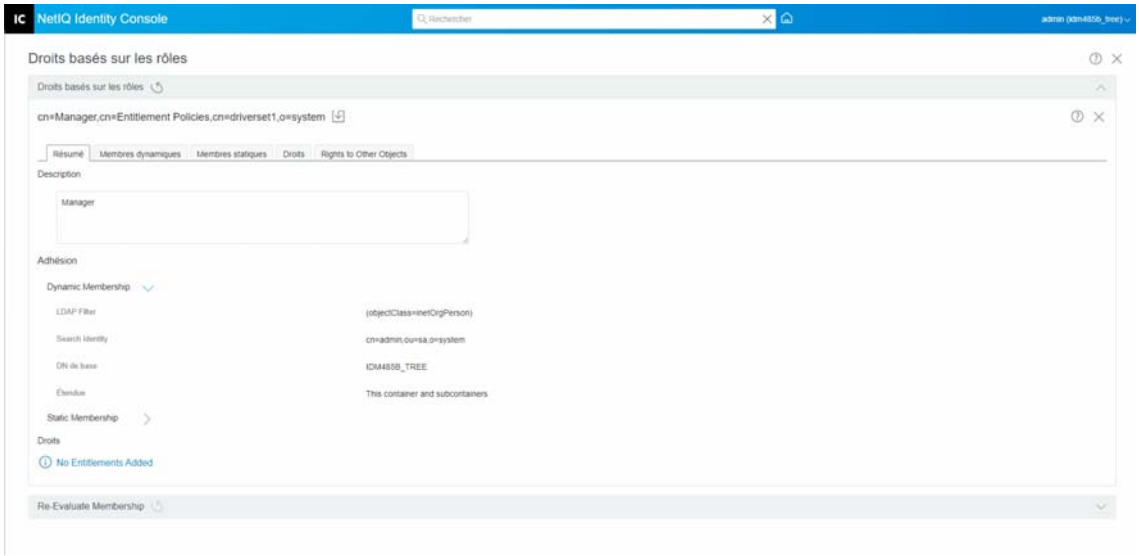


3 Cliquez sur le bouton Enregistrer .

Le résumé des détails de l'adhésion à la stratégie s'affiche dans l'onglet **Résumé**.

4 Redémarrez le pilote.

Figure 33-6 *Fermer et redémarrer*



REMARQUE : vous devez redémarrer le pilote pour que les modifications prennent effet.

Réévaluer l'adhésion

Grâce à la fonction **Droits basés sur les rôles**, vous pouvez octroyer des droits sur les systèmes connectés à un groupe d'utilisateurs.

Lorsque vous créez ou modifiez une stratégie RBE, l'adhésion de chaque utilisateur doit être réévaluée pour vérifier si les droits sur les systèmes connectés doivent être accordés, modifiés ou révoqués. Par défaut, la réévaluation se fait pour un utilisateur à la fois, lorsqu'un attribut de définition des membres est modifié ou qu'un utilisateur est déplacé ou renommé. Ce comportement par défaut permet de réduire l'utilisation des ressources système, mais peut entraîner un délai important entre le moment où la stratégie RBE est modifiée et celui où les droits sont accordés, modifiés ou révoqués pour l'utilisateur concerné.

Vous pouvez vérifier que les droits d'un utilisateur sont tous mis à jour en même temps à l'aide de la tâche « Réévaluer les stratégies RBE » page 220 pour spécifier les utilisateurs qui doivent être réévalués immédiatement. Il est recommandé de le faire chaque fois que vous créez ou que vous modifiez une stratégie RBE.

Avant Identity Manager 3.6, la réévaluation de l'adhésion était effectuée pour toutes les stratégies RBE d'un ensemble de pilotes et non pour une stratégie de droits individuelle. Depuis Identity Manager 3.6, il est toutefois possible d'**évaluer** une stratégie RBE et d'**ajouter** ses membres à la **liste d'objets** sélectionnée. Si vous avez défini une stratégie de droits et créé une liste d'adhésion, le titre Évaluez une stratégie de droits pour **ajouter** ses membres à la liste s'affiche en regard de

l'entrée Objets sélectionnée. Sélectionnez la stratégie souhaitée, puis cliquez sur l'icône + pour ajouter les membres de la stratégie à la **liste d'objets** sélectionnée. Vous pouvez ajouter ou supprimer des membres ou des objets de la **liste d'objets** sélectionnée.

Pour utiliser au mieux les ressources système, apportez toutes les modifications souhaitées aux stratégies RBE d'un ensemble de pilotes particulier avant d'utiliser la tâche « Réévaluer les stratégies RBE » page 220.

REMARQUE : la réévaluation des droits est nécessaire uniquement pour les droits sur des systèmes connectés. Lorsque des droits Identity Console sont modifiés pour une stratégie RBE, les modifications apportées sont immédiatement appliquées à chaque utilisateur. Le pilote du services de droits doit être en cours d'exécution pour que les réévaluations d'adhésion puissent être effectuées.

Réévaluer les stratégies RBE

Pour réévaluer l'adhésion :

1. Cliquez sur **Réévaluer l'adhésion** > **Sélectionner un ensemble de pilotes**.

   La liste des stratégies créées s'affiche.

2. Sélectionnez la stratégie à évaluer, puis cliquez sur **Evaluate** (Évaluer).

   L'onglet **Objets** affiche les utilisateurs qui font partie du groupe.

3. (Facultatif) Pour ajouter un utilisateur spécifique, cliquez sur +.

Vous ne pouvez utiliser la fonction **Ajouter** que lorsque des utilisateurs sont manquants dans la liste et que vous souhaitez ajouter des utilisateurs spécifiques.

4 (Facultatif) Pour supprimer un utilisateur donné, cliquez sur .

Vous ne pouvez utiliser la fonction **Supprimer** que si vous souhaitez supprimer des utilisateurs spécifiques de la liste.

5 Cliquez sur le bouton Réévaluer l'adhésion .

Figure 33-7 *Réévaluer l'adhésion*