

Sécurisation des groupes d'administration et des comptes Active Directory

Mis à jour le :

Sur cette page

- ↓ [Introduction](#)
- ↓ [Avant de commencer](#)
- ↓ [Création d'un nouveau compte utilisateur avec des droits Admins du domaine](#)
- ↓ [Protection du compte Administrateur](#)
- ↓ [Sécurisation du compte Invité](#)
- ↓ [Renforcement de la sécurité des comptes et des groupes d'administration de services](#)
- ↓ [Mise en place de meilleures pratiques d'utilisation des comptes et des groupes d'administration](#)
- ↓ [Informations complémentaires](#)

Introduction

Une partie importante de la sécurisation du réseau consiste à gérer les utilisateurs et les groupes qui ont un accès administratif au service d'annuaire Active Directory®. Les personnes mal intentionnées qui obtiennent les droits d'accès administratifs aux contrôleurs de domaine Active Directory peuvent ouvrir une brèche dans la sécurité de votre réseau. Ces personnes peuvent être des utilisateurs non autorisés ayant obtenu des mots de passe de type administrateur ou des administrateurs habilités, contraints de fournir des informations confidentielles. Qui plus est, notons toutefois que tous les problèmes ne sont pas forcément dus à un acte de malveillance. Un utilisateur disposant des droits d'accès de type administrateur peut très bien être à l'origine des problèmes occasionnés sans en être conscient s'il ne comprend pas exactement la ramification des changements de configuration. Pour ces raisons, il est important de gérer avec précaution les utilisateurs et les groupes disposant de droits d'accès de type administrateur sur les contrôleurs du domaine.

Les paramètres de sécurité par défaut de Microsoft® Windows Server suffisent à sécuriser les comptes Active Directory contre un grand nombre de menaces. Toutefois, certains paramètres par défaut relatifs aux comptes de type administrateur peuvent être renforcés pour relever le niveau de sécurité de votre réseau.

Ce guide contient une série d'instructions à suivre pas à pas pour la/le :

- Création d'un nouveau compte utilisateur avec des droits Admins du domaine
- Protection du compte Administrateur par défaut
- Sécurisation du compte Invité
- Renforcement de la sécurité des comptes et des groupes d'administration de services
- Mise en place de meilleures pratiques d'utilisation des comptes et des groupes d'administration

Utilisez les meilleures pratiques décrites dans ce guide de la même façon que vous gérez votre réseau. Elles vous aideront à réduire les risques induits par l'accès des utilisateurs non autorisés aux droits administratifs d'Active Directory. Elles vous aideront également à réduire les risques de malveillance ou d'accident dans votre organisation suite aux copies ou aux suppressions de données confidentielles, ou encore à la désactivation du réseau.

IMPORTANT : Toutes les procédures décrites dans ce document ont été développées à partir du menu Démarrer qui apparaît par défaut lors de l'installation du système d'exploitation. Si vous avez modifié ce

menu, les étapes peuvent légèrement varier.

[↑ Haut de la page](#)

Avant de commencer

Avant d'utiliser ce guide pour sécuriser vos groupes et vos comptes d'administration, effectuez tout d'abord les tâches contenues dans le chapitre « Sécurisation des contrôleurs de domaine Windows Server » du kit de sécurité.

De sorte à exécuter l'ensemble des procédures fournies dans ce guide, vous devez connaître le nom et le mot de passe du compte administrateur habilité, ou le nom et le mot de passe d'un compte membre du groupe administrateur sur vos contrôleurs de domaine. Déterminez le ou les serveurs sur votre réseau fonctionnant comme contrôleurs de domaine. Un contrôleur de domaine est un serveur fonctionnant sur Windows Server et sur lequel Active Directory est installé.

Avant de commencer, vous devez comprendre ce que sont exactement ces comptes et ces groupes d'administration, ainsi que la façon dont leur responsabilité est partagée par les administrateurs de services et de données. Pour visualiser et gérer des comptes et des groupes Active Directory, cliquez sur **Démarrer**, sélectionnez **Outils d'administration**, puis cliquez sur **Utilisateurs et ordinateurs Active Directory**.

Comprendre les comptes et les groupes d'administration

Les comptes d'administration dans un domaine Active Directory englobent :

- le compte Administrateur, créé à l'installation d'Active Directory, est installé sur le premier contrôleur du domaine. Il s'agit du compte le plus puissant du domaine. La personne qui installe Active Directory sur l'ordinateur crée le mot de passe de ce compte au moment de l'installation ;
- tous les comptes créés ultérieurement et placés dans un groupe possédant des privilèges administratifs ou auxquels sont directement attribués des privilèges administratifs ;

Les groupes d'administration dans un domaine Active Directory varient en fonction des services installés dans votre domaine. Ceux utilisés tout particulièrement pour gérer Active Directory sont les suivants :

- les groupes d'administration qui sont automatiquement créés dans le conteneur Builtin ;
- les groupes d'administration qui sont automatiquement créés dans le conteneur Utilisateurs ;
- tous les comptes créés ultérieurement et placés dans un autre groupe possédant des privilèges administratifs ou auxquels sont directement attribués des privilèges administratifs.

Comprendre les administrateurs de services et les administrateurs de données

Pour Active Directory dans Windows Server, il existe deux types de responsabilités administratives. Les administrateurs de services sont responsables de la maintenance et de la mise à disposition du service d'annuaire, y compris de la gestion des contrôleurs de domaine et de la configuration du service d'annuaire. Les administrateurs de données sont responsables de la gestion des données stockées dans le service d'annuaire, ainsi que sur les serveurs membres du domaine et sur les postes de travail.

Dans une petite structure, ces deux rôles peuvent incomber à la même personne, mais il est important de comprendre quels sont les administrateurs de services parmi les comptes et les groupes par défaut. Les comptes et les groupes d'administration de services ont le pouvoir le plus étendu sur votre environnement réseau et exigent une protection maximale. Ils sont responsables des paramètres au niveau des répertoires, de l'installation et de la maintenance des logiciels, de l'application des service packs pour le système d'exploitation et de la mise à jour des contrôleurs de domaine.

Le tableau suivant dresse la liste des groupes et des comptes par défaut utilisés dans le cadre de l'administration de services, leurs emplacements par défaut, ainsi qu'une brève description pour chacun d'entre eux. Les groupes du conteneur Builtin ne peuvent pas être déplacés sur un nouvel emplacement.

Groupes et comptes Administrateur de services par défaut

Nom du groupe ou du compte	Emplacement par défaut	Description

Administrateurs de l'entreprise	Conteneur Utilisateurs	Ce groupe est automatiquement ajouté aux groupes des Administrateurs dans chaque domaine de la forêt, en veillant à assurer un accès complet à la configuration de tous les contrôleurs du domaine.
Administrateurs du schéma	Conteneur Utilisateurs	Ce groupe possède des droits d'accès administratifs complets au schéma Active Directory.
Administrateurs	Conteneur Builtin	Ce groupe effectue un contrôle intégral sur tous les contrôleurs du domaine et sur le contenu des répertoires dans ce domaine. Il peut modifier l'appartenance des groupes d'administration dans le domaine. Il correspond au groupe d'administration des services le plus puissant.
Administrateurs du domaine	Conteneur Utilisateurs	Ce groupe est automatiquement ajouté au groupe des Administrateurs correspondant, dans chacun des domaines. Il exerce un contrôle absolu sur tous les contrôleurs du domaine et sur le contenu des répertoires dans ce domaine. Il peut également modifier l'appartenance des comptes d'administration à ce domaine.
Opérateurs de serveur	Conteneur Builtin	Par défaut, ce groupe intégré ne possède aucun membre. Il peut exécuter des tâches de maintenance, par exemple des sauvegardes et des restaurations sur les contrôleurs du domaine.
Opérateurs de comptes	Conteneur Builtin	Par défaut, ce groupe intégré ne possède aucun membre. Il peut créer et gérer des utilisateurs et des groupes dans le domaine, mais il ne peut gérer aucun compte d'administrateur de services. En règle générale, n'essayez pas d'ajouter des membres à ce groupe et ne l'utilisez pas pour des tâches d'administration déléguées.
Opérateurs de sauvegarde	Conteneur Builtin	Par défaut, ce groupe intégré ne possède aucun membre. Il peut exécuter des tâches de sauvegarde et de restauration sur les contrôleurs du domaine.
Administrateur du mode Restauration du service d'annuaire	Non stocké dans Active Directory	Ce compte spécial est créé au moment de l'installation d'Active Directory et n'est pas le même que le compte Administrateur de la base de données Active Directory. Ce compte est uniquement utilisé pour démarrer le contrôleur du domaine en mode Restauration du service d'annuaire. D'ailleurs, ce compte possède un accès intégral au système et à tous les fichiers du contrôleur de domaine.

Les comptes et les groupes répertoriés dans ce tableau et tous les membres appartenant aux groupes sont protégés par un processus à l'arrière-plan qui vérifie régulièrement et applique un descripteur de sécurité spécifique. Il s'agit d'une structure de données contenant des informations sur la sécurité et qui sont associées à un objet protégé. Ce processus veille à ce que toute tentative non autorisée qui parvient à modifier le descripteur de sécurité de l'un des comptes ou des groupes d'administration soit empêchée par les paramètres de protection.

Ce descripteur de sécurité se trouve sur l'objet AdminSDHolder. Cela signifie que pour modifier les autorisations de l'un des groupes d'administrateurs de services ou de l'un des comptes membres, vous devez modifier le descripteur de sécurité de l'objet **AdminSDHolder** de sorte à ce qu'il soit appliqué de manière logique. Veillez à effectuer ces modifications car vous changez également les paramètres par défaut qui seront appliqués à tous les comptes d'administration protégés. Pour plus d'informations sur la modification des autorisations aux comptes d'administration de services, rendez-vous à l'adresse : « [Best Practice Guide for Securing Active Directory Installations](http://go.microsoft.com/fwlink/?LinkId=22342) » (Windows Server) du site Web de Microsoft <http://go.microsoft.com/fwlink/?LinkId=22342>.

Création d'un nouveau compte utilisateur avec des droits Admins du domaine

Si vous ne possédez pas de compte utilisateur qui soit membre du groupe Admins du domaine, autre qu'un compte Administrateur par défaut, créez-en un que vous utiliserez pour exécuter les tâches présentées dans ce guide. En tant qu'administrateur de votre réseau, vous utiliserez ce nouveau compte uniquement pour effectuer des tâches exigeant des droits d'accès de type Admins du domaine. Ne restez pas connecté sur ce compte après avoir réalisé les tâches demandées. Si l'ordinateur est frappé par un virus alors que vous êtes connecté en tant qu'administrateur du domaine, le virus se propagera dans le cadre de l'administration du domaine. Le virus pourra ainsi utiliser les droits de type administrateur pour se propager à la station de travail et au reste du réseau. Créez un autre compte utilisateur pour gérer vos données et pour une utilisation quotidienne de la gamme Office de Microsoft, de même que pour l'envoi et la réception de messages, mais n'ajoutez pas de compte utilisateur au groupe Admins du domaine. Sécurisez vos procédures de création et d'utilisation des comptes d'administration, tel que décrit par la suite dans ce document.

Configuration requise

- Droits : Admins du domaine (s'il s'agit du premier compte d'administration que vous créez, connectez-vous en utilisant le compte Administrateur par défaut)

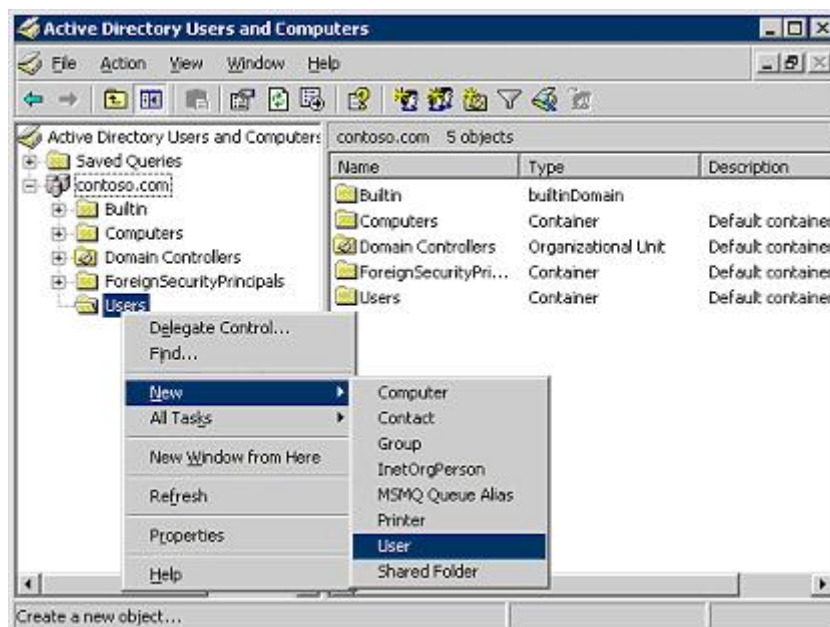
- Outils : Utilisateurs et ordinateurs Active Directory

- **Pour créer un nouveau compte utilisateur avec des droits Admins du domaine**

1. Ouvrez une session en tant que membre du groupe Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.

Remarque : Les copies d'écran de ce document reflètent un environnement de test et les informations peuvent différer de celles qui s'affichent sur votre écran.

2. Cliquez sur le conteneur **Utilisateurs** avec le bouton droit de la souris, cliquez sur **Nouveau**, puis sur **Utilisateur**.



3. Saisissez le **Prénom**, le **Nom** et le **nom d'ouverture de session de l'utilisateur**, puis cliquez sur **Suivant**. Tel que nous vous l'indiquons dans l'exemple ci-joint, vous devrez peut-être décider d'une convention d'appellation pour gérer les comptes d'administration. Par exemple, vous décidez d'ajouter "?ALT" au nom de l'administrateur pour générer le nom d'ouverture de session du compte d'administration.

New Object - User

Create in: contoso.com/Users

First name: Chris Initials:

Last name: Preston

Full name: Chris Preston

User logon name: cpreston-ALT @contoso.com

User logon name (pre-Windows 2000): CONTOSO\cpreston-ALT

< Back Next > Cancel

4. Saisissez et confirmez le mot de passe utilisateur, désactivez la case à cocher **L'utilisateur doit changer de mot de passe à la prochaine ouverture de session**, puis cliquez sur **Suivant**.

New Object - User

Create in: contoso.com/Users

Password:

Confirm password:

☒ User must change password at next logon

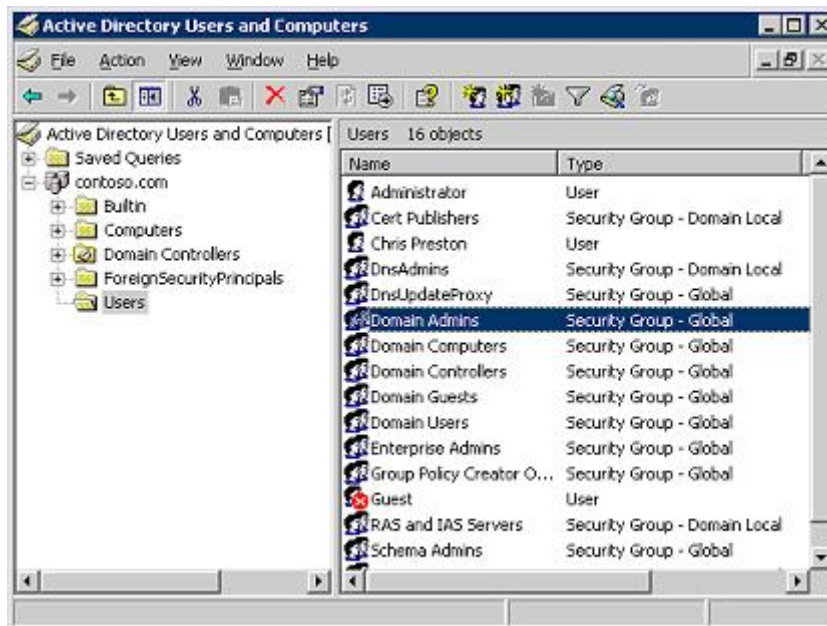
☐ User cannot change password

☐ Password never expires

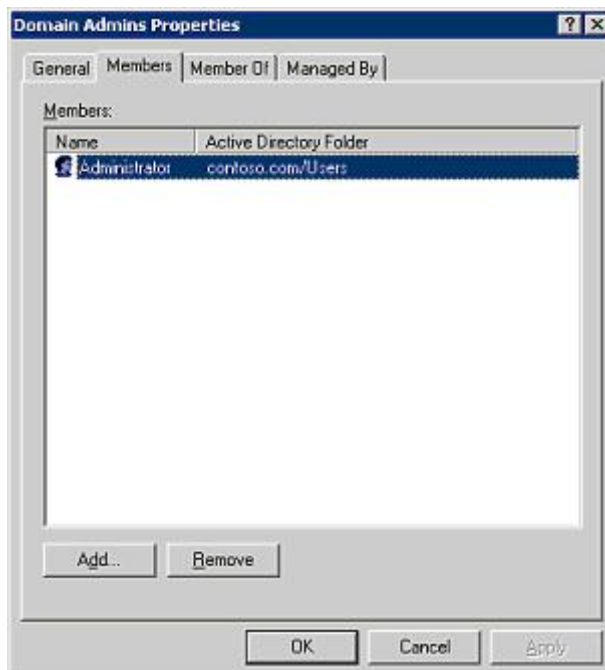
☐ Account is disabled

< Back Next > Cancel

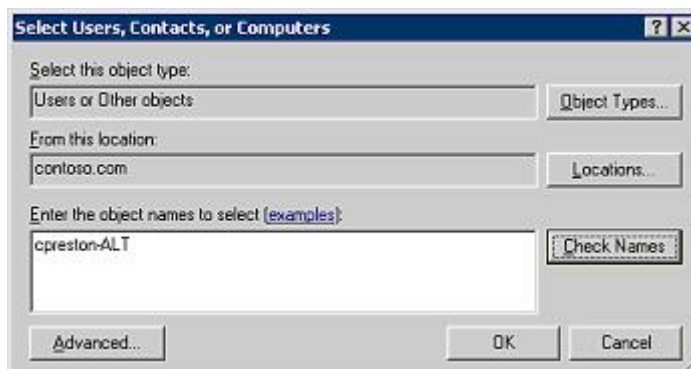
5. Revoyez les informations du compte, puis cliquez sur **Terminer**.
6. Une fois le conteneur **Utilisateurs** sélectionné, dans le volet d'informations (volet de droite), double-cliquez sur le groupe **Admins du domaine**.



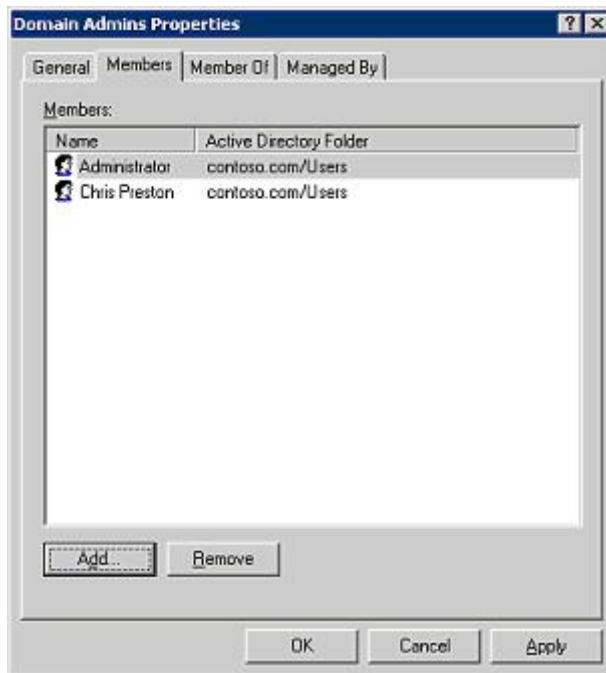
7. Cliquez dans l'onglet **Membres**.



8. Cliquez sur **Ajouter** puis, dans la boîte de dialogue **Sélectionnez les utilisateurs, les contacts ou les ordinateurs**, saisissez le nom d'ouverture de session du compte d'administration que vous venez de créer, puis cliquez sur **OK**.



9. Vérifiez que votre nouveau compte apparaît comme étant un membre du groupe **Admins du domaine**.



[↑ Haut de la page](#)

Protection du compte Administrateur

Toutes les installations d'Active Directory possèdent un compte appelé Administrateur dans chaque domaine. Ce compte ne peut pas être supprimé ni verrouillé. Sous Windows Server, le compte Administrateur peut être désactivé, mais il est automatiquement réactivé au démarrage de l'ordinateur en mode sans échec.

Un utilisateur malveillant qui tenterait de créer une brèche dans un système commencerait normalement par tenter d'obtenir le mot de passe du compte Administrateur tout puissant. Pour cette raison, renommez son mot de passe aussi souvent que possible et modifiez-en la **description** pour ne pas donner l'impression qu'il s'agit du compte Administrateur. En outre, créez un compte utilisateur appelé Administrateur que vous utiliserez comme leurre et qui ne posséderait en réalité aucune autorisation particulière ni aucun droit spécifique.

Attribuez toujours au compte Administrateur un mot de passe long et complexe. Utilisez des mots de passe différents pour les comptes Administrateur et Administrateur du mode Restauration du service d'annuaires. Pour plus d'informations sur la création de mots de passe complexes, reportez-vous au chapitre « Sélection de mots de passe sécurisés » du kit de sécurité.

Renommage du compte Administrateur par défaut

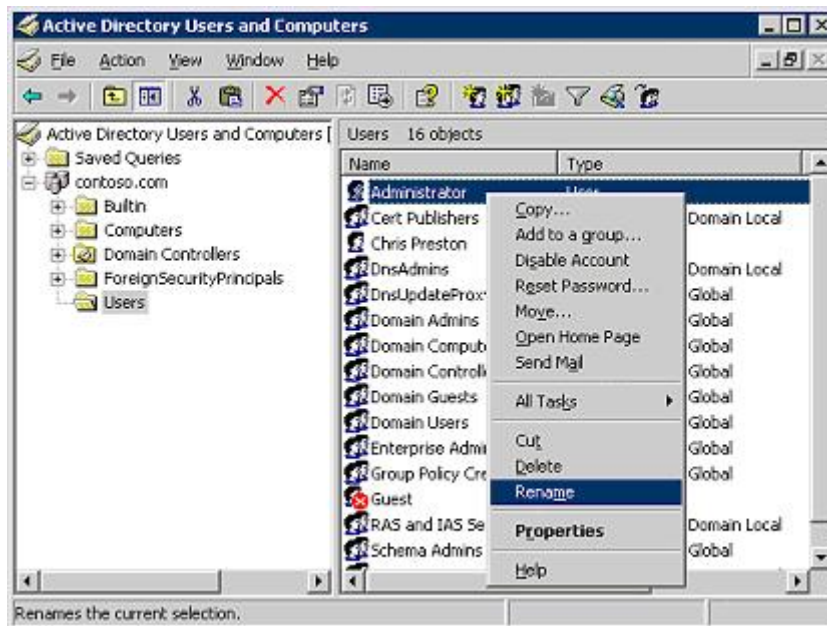
Cette procédure supprime toutes les informations jugées « évidentes » et qui pourraient attirer l'attention des pirates sur le fait que ce compte dispose de privilèges particuliers. Bien qu'un pirate qui découvrirait le compte Administrateur par défaut aurait encore besoin du mot de passe pour l'utiliser, le renommage du compte Administrateur par défaut rajoute un niveau de protection supplémentaire pour parer aux risques d'attaque. Utilisez un prénom et un nom fictifs, d'un format identique à celui des autres noms utilisateur. N'utilisez en aucun cas le nom fictif indiqué dans l'exemple ci-dessous.

Configuration requise

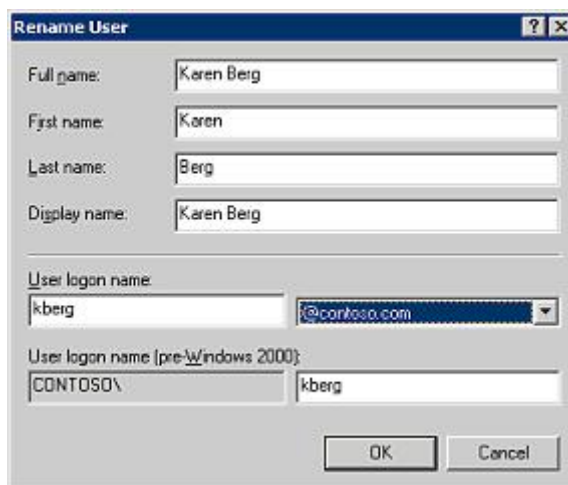
- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory
- **Pour renommer le compte Administrateur par défaut**
 1. Connectez-vous en tant que membre du groupe des Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
 2. Dans l'arborescence de la console (volet de gauche), cliquez sur **Utilisateurs**.

Dans le volet d'informations (volet de droite), cliquez avec le bouton droit de la souris sur

3. **Administrateur**, puis cliquez sur **Renommer**.



4. Saisissez le prénom et le nom fictifs, puis appuyez sur **ENTRÉE**.
5. Dans la boîte de dialogue Modification du nom de l'utilisateur, modifiez les valeurs relatives au **Nom complet**, au **Prénom**, au **Nom**, au **nom d'affichage**, au **nom d'ouverture de session de l'utilisateur** et au **nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)** pour les faire correspondre au nom de compte fictif, puis cliquez sur **OK**.



6. Dans le volet d'informations (volet de droite), cliquez avec le bouton droit de la souris sur le nouveau nom, puis cliquez sur **Propriétés**.
7. Dans l'onglet **Général**, supprimez la **Description** « Compte d'utilisateur d'administration » et saisissez une description qui ressemble à celle des autres comptes utilisateur (pour la plupart des entreprises, ce champ reste vide).

Karen Berg Properties

Member Of: Dial-in: Environment: Sessions:

Remote control: Terminal Services Profile: CDM+:

General Address Account Profile Telephones Organization

Karen Berg

First name: Karen Initials:

Last name: Berg

Display name: Karen Berg

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply

8. Dans l'onglet **Compte**, vérifiez que les noms d'ouverture de session sont corrects.

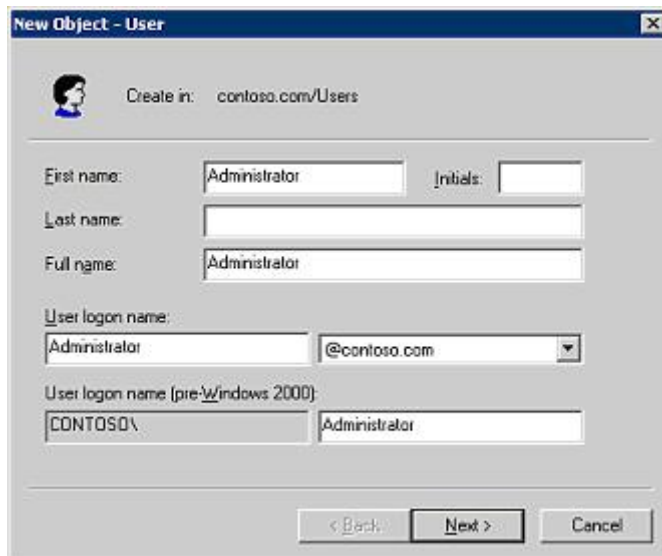
Remarque : Cette procédure modifie uniquement le nom d'ouverture de session du compte Administrateur par défaut, de même que les détails du compte, autant d'informations qu'une personne extérieure peut lire si elle réussit à obtenir une liste des comptes de votre système. Cette procédure n'affecte en rien la possibilité d'utiliser le compte Administrateur du mode de Restauration du service d'annuaire car il s'agit de deux comptes différents.

Création d'un compte Administrateur leurre

Cette procédure ajoute un niveau de protection supplémentaire lorsque vous masquez le compte Administrateur par défaut. Un pirate qui prévoit de s'approprier le mot de passe du compte Administrateur est ainsi dupé puisqu'il attaque un compte ne possédant aucun privilège particulier.

Configuration requise

- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory
- **Pour créer un compte Administrateur leurre**
 1. Connectez-vous en tant que membre du groupe Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
 2. Cliquez sur le conteneur **Utilisateurs** avec le bouton droit de la souris, cliquez sur **Nouveau**, puis sur **Utilisateur**.
 3. Dans **Prénom** et **Nom d'ouverture de session de l'utilisateur**, saisissez **Administrateur**, puis cliquez sur **Suivant**.



New Object - User

Create in: contoso.com/Users

First name: Administrator Initials:

Last name:

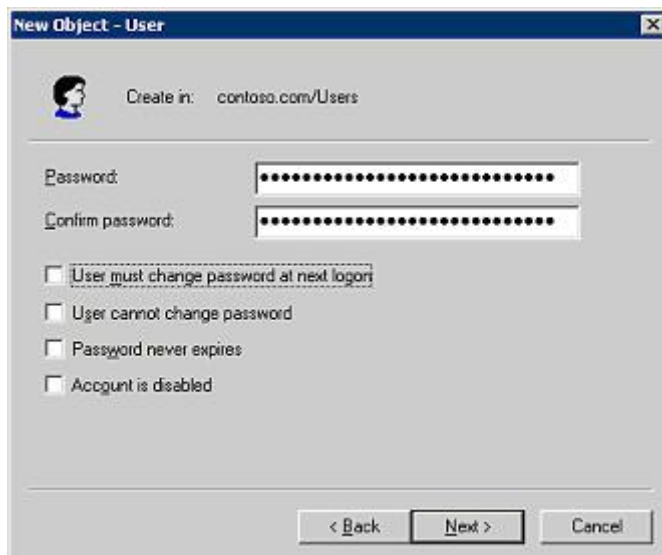
Full name: Administrator

User logon name: Administrator @contoso.com

User logon name (pre-Windows 2000): CONTOSO\ Administrator

< Back Next > Cancel

4. Saisissez, puis confirmez le mot de passe.
5. Désactivez la case à cocher **L'utilisateur doit changer de mot de passe à la prochaine ouverture de session.**



New Object - User

Create in: contoso.com/Users

Password:

Confirm password:

☐ User must change password at next logon

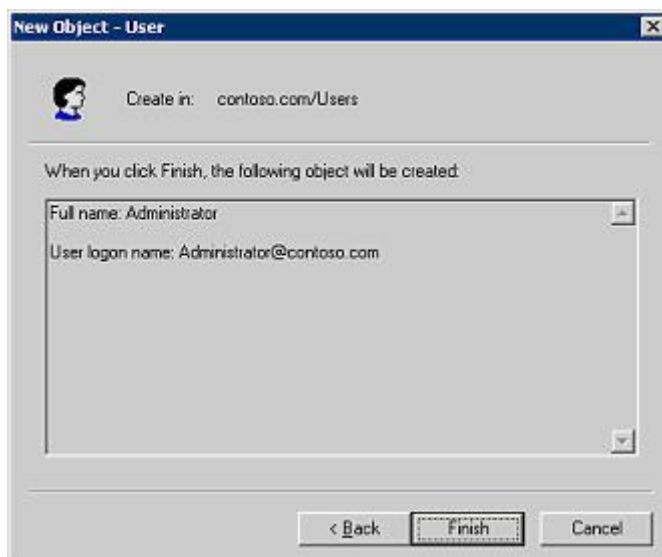
☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

6. Vérifiez que le compte leurre est créé, puis cliquez sur **Terminer**.



New Object - User

Create in: contoso.com/Users

When you click Finish, the following object will be created:

Full name: Administrator

User logon name: Administrator@contoso.com

< Back Finish Cancel

7. Dans le volet d'informations (volet de droite), cliquez avec le bouton droit de la souris sur

Administrateur, puis cliquez sur **Propriétés**.

8. Dans l'onglet **Général**, dans la zone **Description**, saisissez **Compte d'utilisateur d'administration**, puis cliquez sur **OK**.

[↑ Haut de la page](#)

Sécurisation du compte Invité

Le compte Invité permet aux utilisateurs ne possédant aucun compte dans votre domaine d'ouvrir une session sur ce domaine en tant qu'invité. Ce compte est désactivé par défaut et doit le rester, mais le fait de le masquer ajoute un niveau de protection supplémentaire contre les accès non autorisés. Utilisez un prénom et un nom fictifs au même format que celui des autres noms d'utilisateur.

Configuration requise

- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory
- **Pour renommer le compte Invité**
 1. Connectez-vous en tant que membre du groupe Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
 2. Dans l'arborescence de la console (volet de gauche), cliquez sur **Utilisateurs**.
 3. Dans le volet d'informations (volet de droite), cliquez avec le bouton droit de la souris sur **Invité**, puis cliquez sur **Renommer**.
 4. Saisissez le prénom et le nom fictifs, puis appuyez sur **ENTRÉE**.
 5. Cliquez avec le bouton droit de la souris sur le nouveau nom, puis cliquez sur **Propriétés**.
 6. Dans l'onglet **Général**, supprimez la **Description** « Compte d'utilisateur invité » et saisissez une description qui ressemble à celle des autres comptes utilisateur (pour la plupart des entreprises, ce champ reste vide).
 7. Dans les zones **Prénom** et **Nom**, saisissez les noms fictifs.
 8. Dans l'onglet **Compte**, saisissez un nouveau **Nom d'ouverture de session de l'utilisateur**, en utilisant le même format que celui des autres comptes d'utilisateur, par exemple l'initiale du prénom suivi du nom.
 9. Saisissez le même nom d'ouverture de session de l'utilisateur dans la zone **Nom d'ouverture de session de l'utilisateur (antérieure à Windows 2000)**, puis cliquez sur **OK**.
 10. Vérifiez que le compte est désactivé. L'icône doit apparaître avec un X rouge. Si elle est activée, cliquez sur le nouveau nom avec le bouton droit de la souris, puis cliquez sur **Désactiver le compte**.

[↑ Haut de la page](#)

Renforcement de la sécurité des comptes et des groupes d'administration de services

La création d'une sous-arborescence contrôlée d'une unité d'organisation (UO) dans Active Directory et sa configuration en fonction des paramètres de sécurité recommandés vous aident à sécuriser l'environnement de vos comptes et de vos stations de travail administrateurs de services.

Les UO sont des conteneurs de domaine pouvant regrouper d'autres unités, utilisateurs, groupes, ordinateurs et objets. Ces unités et sous-unités créent une structure hiérarchique au sein d'un domaine et sont principalement utilisées pour regrouper des objets et mieux les gérer.

En créant une sous-arborescence contenant tous les comptes administrateurs de services et les stations de travail d'administration, vous appliquez les paramètres relatifs à la sécurité et à la politique pour renforcer

leur protection.

Pour créer la sous-arborescence contrôlée, effectuez les tâches suivantes :

1. Créez la structure UO pour la sous-arborescence contrôlée.
2. Définissez les autorisations des UO de la sous-arborescence contrôlée.
3. Déplacez les groupes administrateurs de services vers la sous-arborescence contrôlée.
4. Déplacez les comptes utilisateur de type administrateur de services vers la sous-arborescence contrôlée.
5. Déplacez les comptes stations de travail de type administrateur de services vers la sous-arborescence contrôlée.
6. Activez les audits sur les UO de la sous-arborescence contrôlée.

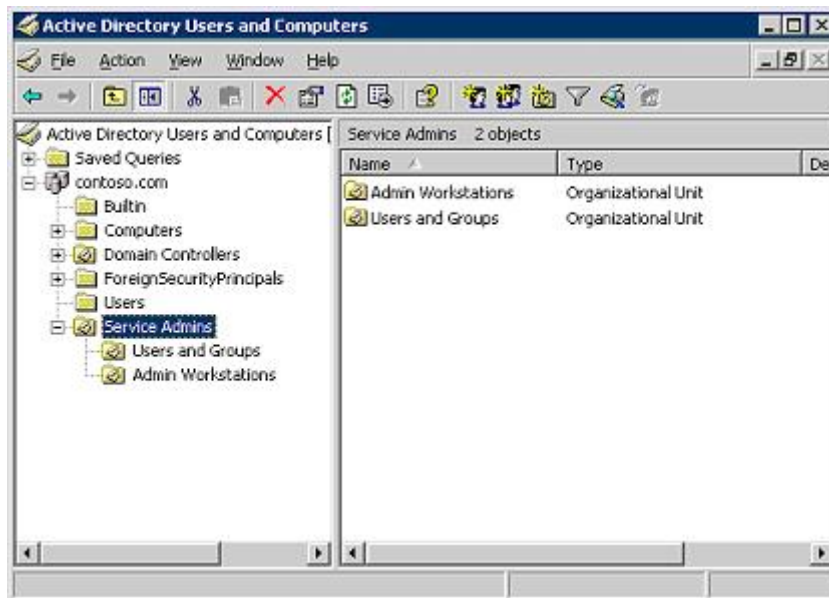
Créez la structure d'une UO pour la sous-arborescence contrôlée.

Pour créer la sous-arborescence, créez trois unités d'organisation :

- **Admins du service**, au niveau de la racine du domaine, pour conserver les deux sous-unités d'organisation suivantes ;
 - **Utilisateurs et groupes**, pour conserver les comptes utilisateur et groupe d'administration ;
 - **Stations de travail d'administration**, pour conserver les stations de travail d'administration.

Configuration requise

- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory
- **Pour créer la structure UO pour la sous-arborescence contrôlée**
 1. Connectez-vous en tant que membre du groupe Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
 2. Dans l'arborescence de l'arbre (volet de gauche), cliquez avec le bouton droit de la souris sur le nom du domaine, pointez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
 3. Dans la zone **Nom**, saisissez **Admins du service**, puis cliquez sur **OK**.
 4. Dans l'arborescence de la console (volet de gauche), cliquez avec le bouton droit de la souris sur **Admins du service**, pointez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
 5. Dans la zone **Nom**, saisissez **Utilisateurs et groupes**, puis cliquez sur **OK**.
 6. Dans l'arborescence de la console (volet de gauche), cliquez avec le bouton droit de la souris sur **Admins du service**, pointez sur **Nouveau**, puis cliquez sur **Unité d'organisation**.
 7. Dans la zone **Nom**, saisissez **Stations de travail d'administration**, puis cliquez sur **OK**.
 8. Vérifiez que la hiérarchie de l'unité d'organisation ressemble à la structure ci-après, que les administrateurs de services se situent au niveau du nom du domaine et que les Utilisateurs et groupes et les stations de travail d'administration sont situés sous les administrateurs de services.



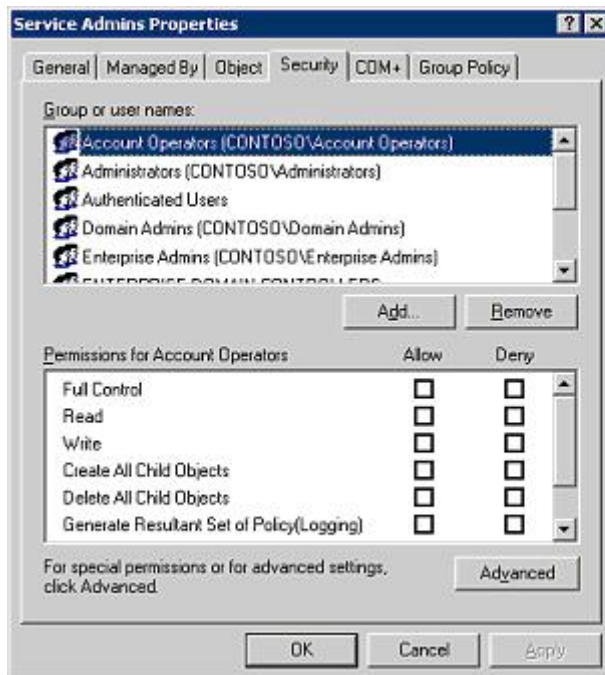
Définissez les autorisations sur les unités d'organisation de la sous-arborescence contrôlée.

En effectuant les opérations suivantes, vous pouvez limiter l'accès à la sous-arborescence contrôlée de sorte que les administrateurs du service puissent gérer l'appartenance aux groupes et aux stations de travail d'administration de services.

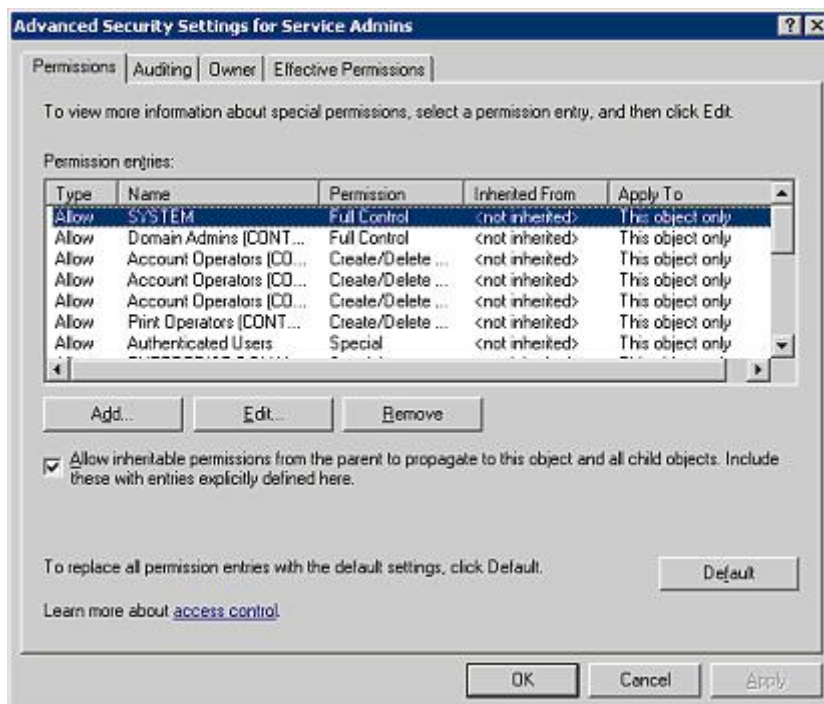
- Bloquez l'héritage des autorisations sur l'unité d'organisation des administrateurs de services de sorte que les modifications apportées aux autorisations héritées qui sont faites plus haut dans l'arborescence du domaine ne soient pas héritées, ce qui agit ainsi sur les paramètres de verrouillage.
- Définissez les autorisations sur l'unité d'organisation administrateurs de services.

Configuration requise

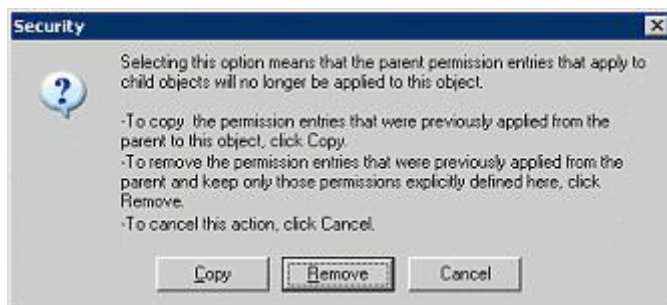
- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory
- **Pour définir les autorisations sur l'unité d'organisation administrateurs de services**
 1. Connectez-vous en tant que membre du groupe Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
 2. Dans le menu **Affichage**, sélectionnez **Fonctionnalités avancées**.
 3. À l'aide du bouton droit de la souris, cliquez sur l'unité d'organisation **Admins du service**, puis sur **Propriétés**.



4. Dans l'onglet **Sécurité**, cliquez sur **Avancée** pour visualiser toutes les entrées d'autorisation existant pour l'unité d'organisation concernée.



5. Désactivez la case à cocher **Permettre aux autorisations pouvant être héritées du parent d'être propagées à cet objet et tous les objets enfants**. Cela inclut les objets dont les entrées sont spécifiquement définies.
6. Dans la boîte de dialogue Sécurité, cliquez sur **Supprimer**. Cette action supprime les autorisations héritées du domaine.



7. Supprimez les autorisations restantes. Sélectionnez toutes les entrées d'autorisation restantes, puis cliquez sur **Supprimer**.
8. Pour chaque groupe énuméré dans la colonne Nom du tableau ci-dessous, ajoutez une entrée d'autorisation pour valider les colonnes **Accès** et **S'applique à** tel qu'indiqué. Pour ajouter une entrée, cliquez sur **Ajouter**, puis dans la boîte de dialogue **Sélectionner un utilisateur, un ordinateur ou un groupe**, cliquez sur **Avancé**. Dans la boîte de dialogue développée, cliquez sur **Rechercher maintenant**. Dans la zone des résultats de la recherche, cliquez deux fois sur **OK**. Cette action génère l'ouverture d'une boîte de dialogue Entrée d'autorisation, à partir de laquelle vous pouvez sélectionner les éléments Accès et S'applique à validés avec le tableau.

Paramètres des autorisations pour l'unité d'organisation administrateurs de services

Type	Nom	Accès	S'applique à
Autoriser	SYSTÈME	Contrôle total	Cet objet et tous les objets enfants
Autoriser	Administrateurs de l'entreprise	Contrôle total	Cet objet et tous les objets enfants
Autoriser	Admins du domaine	Contrôle total	Cet objet et tous les objets enfants
Autoriser	Administrateurs	Contrôle total	Cet objet et tous les objets enfants
Autoriser	Accès compatible avec les versions antérieures à Windows 2000	Lister le contenu Lire toutes les propriétés Autorisations de lecture	Objets utilisateur
Autoriser	Accès compatible avec les versions antérieures à Windows 2000	Lister le contenu Lire toutes les propriétés Autorisations de lecture	Objets InetOrgPerson
Autoriser	Contrôleurs de domaine d'entreprise	Lister le contenu Lire toutes les propriétés Autorisations de lecture	Cet objet et tous les objets enfants
Autoriser	Utilisateurs authentifiés	Lister le contenu Lire toutes les propriétés Autorisations de lecture	Cet objet et tous les objets enfants

Déplacement des groupes d'administrateurs de services dans l'unité organisationnelle Utilisateurs et groupes

Déplacez les groupes d'administrateurs de services suivants et faites-les passer de leur emplacement actuel dans le répertoire à l'unité d'organisation Utilisateurs et groupes de la sous-arborescence contrôlée.

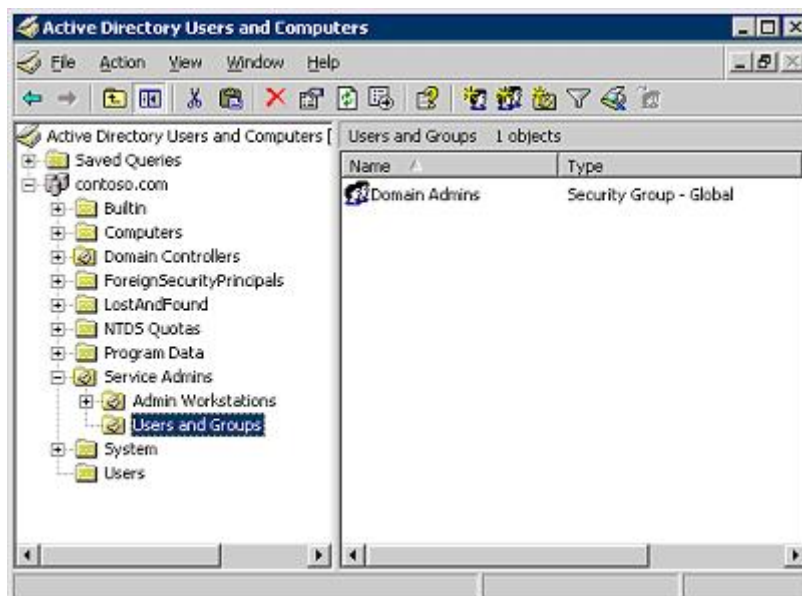
- Admins du domaine et sous-groupes imbriqués.
- Administrateurs de l'entreprise et sous-groupes imbriqués.
- Administrateurs du schéma et sous-groupes imbriqués.
- Tous les groupes imbriqués dans les groupes administrateurs du domaine, opérateurs du serveur, opérateurs de sauvegarde ou opérateurs du compte.
- Tous les groupes disposant de droits délégués et qui accordent efficacement aux utilisateurs ses droits administrateurs de services.

Les groupes intégrés (administrateurs, opérateurs du serveur, opérateurs du compte et opérateurs de sauvegarde) ne peuvent pas être déplacés de leur conteneur par défaut vers la sous-arborescence contrôlée. Toutefois, ces groupes sont protégés par défaut par AdminSDHolder dans Windows Server.

Si votre organisation n'a créé aucun sous-groupe imbriqué ni accordé aucun droit d'administration de services délégué à un groupe quel qu'il soit, vous devez déplacer uniquement les administrateurs du domaine, les administrateurs de l'entreprise et les administrateurs du schéma.

Configuration requise

- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory
- **Pour déplacer les groupes de type administrateur des services dans l'unité d'organisation Utilisateurs et groupes**
 1. Connectez-vous en tant que membre du groupe Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
 2. Dans l'arborescence de la console (volet de gauche), cliquez sur **Utilisateurs**.
 3. Dans le volet d'informations (volet de droite), cliquez avec le bouton droit de la souris sur **Admins du domaine**, puis cliquez sur **Déplacer**.
 4. Dans la zone **Déplacer**, double-cliquez sur **Administrateurs de services**, cliquez sur **Utilisateurs et groupes**, puis sur **OK**.
 5. Vérifiez que le groupes Admins du domaine se trouve maintenant dans l'unité d'organisation **Utilisateurs et groupes**.



6. Renouvelez la procédure pour tous les groupes de type administrateur de services énumérés ci-dessus. Vous remarquerez que si vous avez imbriqué des groupes dans des groupes Builtin, du

type Administrateur, ou des groupes précédemment créés et auxquels ont été affectés des droits administratifs, il se peut que leur emplacement d'origine ne soit pas celui du conteneur **Utilisateurs**.

Déplacement des comptes utilisateur du type administrateur de services dans l'unité d'organisation Utilisateurs et groupes

Déplacez les comptes utilisateur suivants et faites-les passer des emplacements actuels dans le répertoire à l'unité d'organisation Utilisateurs et groupes de la sous-arborescence contrôlée :

- Tous les comptes utilisateur administratifs sont membres de l'un des groupes de type administrateur de services énumérés dans le tableau des groupes et des comptes de type administrateur de services par défaut. Ce tableau intègre également le compte Administrateur de domaine (précédemment renommé).
- Le compte administrateur leurre que vous avez créé précédemment dans ce guide.

Nous vous avons conseillé de créer deux comptes pour chaque administrateur de services : un pour les tâches d'administration de services et l'autre pour l'administration des données et l'accès utilisateur type. Positionnez les comptes utilisateur d'administration dans l'unité d'organisation Utilisateurs et groupes de la sous-arborescence contrôlée. Si ces comptes existent déjà dans le répertoire, déplacez-les à présent dans la sous-arborescence. Les comptes utilisateur normaux pour ces administrateurs ne doivent pas être positionnés dans la sous-arborescence contrôlée. Les comptes utilisateur normaux resteront à leur emplacement d'origine dans le conteneur Utilisateurs ou dans une unité d'organisation utilisée par votre entreprise pour stocker les comptes utilisateur.

Configuration requise

- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory
- **Pour déplacer les comptes de type administrateur de services dans l'unité d'organisation Utilisateurs et groupes**
 1. Connectez-vous en tant que membre du groupe Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
 2. Dans l'arborescence de la console (volet de gauche), cliquez sur **Utilisateurs**.
 3. Dans le volet d'informations (volet de droite), cliquez sur le nom du compte administrateur renommé avec le bouton droit de la souris, puis cliquez sur **Déplacer**.
 4. Dans la zone **Déplacer**, double-cliquez sur **Administrateurs du service**, cliquez sur **Utilisateurs et groupes**, puis sur **OK**.
 5. Vérifiez que le compte se trouve maintenant dans l'unité d'organisation **Utilisateurs et groupes**.
 6. Renouvelez la procédure pour tous les comptes de type administrateur de services énumérés ci-dessus. Vous remarquerez que si vous avez créé auparavant des comptes d'administration ou d'autres unités d'organisation, leur emplacement d'origine peut très bien se situer en dehors du conteneur **Utilisateurs**.

Déplacement des comptes stations de travail d'administration dans l'unité d'organisation stations de travail d'administration

Déplacez les comptes stations de travail utilisés par les administrateurs dans l'unité d'organisation stations de travail d'administration de votre sous-arborescence contrôlée.

IMPORTANT : Ne déplacez en aucun cas les comptes du contrôleur de domaine en dehors de l'unité d'organisation contrôleurs de domaine, même si certains administrateurs les utilisent pour effectuer des tâches administratives. En déplaçant ces comptes, vous désorganisez l'application logique des politiques de contrôle de domaine sur l'ensemble des domaines et cette action n'est pas prise en charge.

Configuration requise

- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory

- **Pour déplacer des comptes stations de travail d'administration dans l'unité d'organisation stations de travail d'administration**

1. Ouvrez une session en tant que membre du groupe de type administrateur du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
2. Dans l'arborescence de la console (volet de gauche), cliquez sur **Ordinateurs**.
3. Dans le volet d'informations (volet de droite), cliquez sur le nom d'une station de travail utilisée par un administrateur avec le bouton droit de la souris, puis cliquez sur **Déplacer**.
4. Dans la zone **Déplacer**, double-cliquez sur **Administrateurs du service**, cliquez sur **Stations de travail d'administration**, puis sur **OK**.
5. Vérifiez que le compte de l'ordinateur se trouve désormais dans l'unité d'organisation **Stations de travail d'administration**.
6. Renouvelez la procédure pour toutes les stations de travail d'administration.

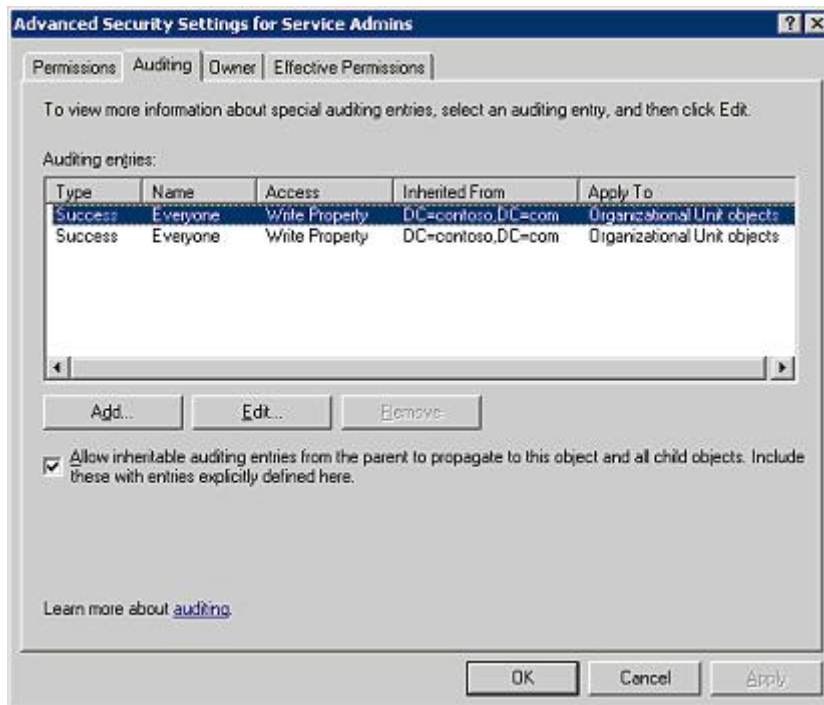
Activation de l'audit sur la sous-arborescence contrôlée

Les audits et le suivi des ajouts, des suppressions et des modifications apportées aux comptes, aux stations de travail et aux politiques de type administrateur de services aident dans certains cas à identifier les modifications incorrectes ou non autorisées qui révèlent la plupart du temps des actions ou des tentatives d'accès non autorisées à votre système. En partant du principe que vous avez autorisé les audits sur vos contrôleurs de domaine en accord avec les recommandations effectuées dans le chapitre « Sécurisation des contrôleurs de domaine Windows Server » du kit de sécurité, le fait d'autoriser les audits sur les unités d'organisation de type administrateurs de services crée un journal d'audit de sécurité qui suit les modifications apportées. La surveillance de ce journal à la recherche des changements effectués sur la sous-arborescence contrôlée et la vérification de la légitimité de ces changements aident à identifier les utilisations frauduleuses. Pour accéder au journal de l'audit de sécurité, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, cliquez sur **Observateur d'événements**, puis sur **Sécurité**.

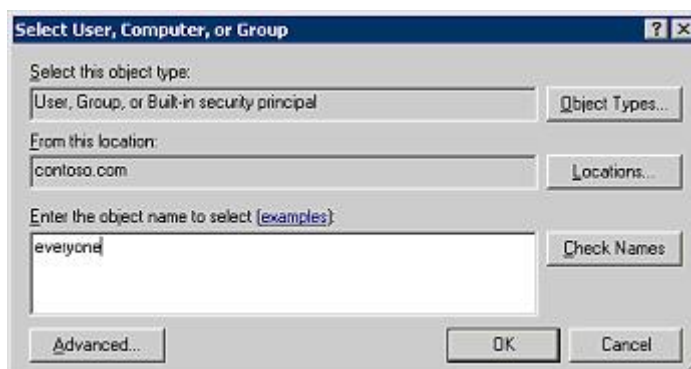
Configuration requise

- Droits : Admins du domaine
- Outils : Utilisateurs et ordinateurs Active Directory
- **Pour activer les audits sur la sous-arborescence contrôlée**

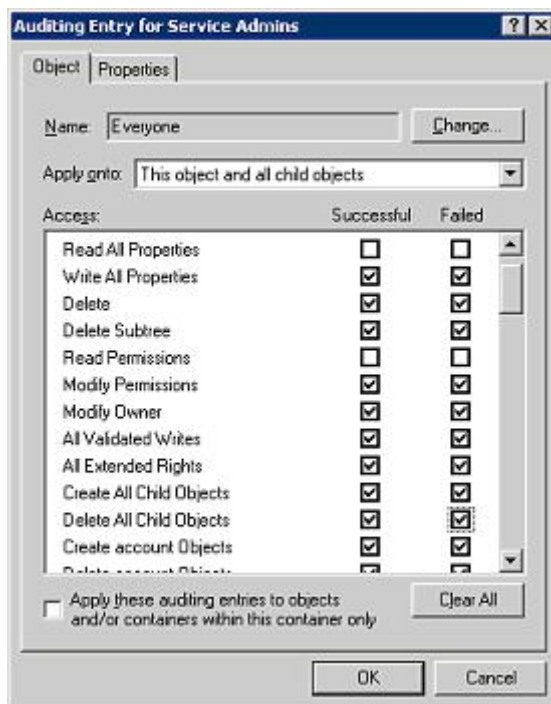
1. Ouvrez une session en tant que membre du groupe Admins du domaine, puis ouvrez Utilisateurs et ordinateurs Active Directory.
2. Dans le menu **Affichage**, sélectionnez **Fonctionnalités avancées**.
3. À l'aide du bouton droit de la souris, cliquez sur l'unité d'organisation **Administrateurs du service**, puis sur **Propriétés**.
4. Dans l'onglet **Sécurité**, cliquez sur **Avancée**, puis sélectionnez l'onglet **Audit** pour afficher les paramètres d'audit existants pour l'unité d'organisation. Notez que dans cet exemple, les paramètres courants sont hérités du domaine.



5. Cliquez sur **Ajouter** pour créer une entrée d'audit qui s'appliquera à l'unité d'organisation des **Administrateurs du service** et aux unités enfants.
6. Dans la zone **Entrer le nom de l'objet à sélectionner**, saisissez **Tout le monde**, puis cliquez sur **OK**.



7. Dans la zone **Accès**, sélectionnez **Succès** et **Échec** pour les éléments d'accès présentés dans le tableau ci-dessous, puis cliquez sur **OK**. Notez qu'en activant certaines cases à cocher, d'autres éléments d'accès sont automatiquement sélectionnés. Il n'est pas possible d'intervenir à ce niveau.



Paramètres d'audit sur l'unité d'organisation de type administrateur de services

Type	Nom	Accès	S'applique à
Toutes	Tout le monde	Écrire toutes les propriétés	Cet objet et tous les objets enfants
Toutes	Tout le monde	Supprimer	Cet objet et tous les objets enfants
Toutes	Tout le monde	Supprimer la sous-arborescence	Cet objet et tous les objets enfants
Toutes	Tout le monde	Modifier les autorisations	Cet objet et tous les objets enfants
Toutes	Tout le monde	Modifier le propriétaire	Cet objet et tous les objets enfants
Toutes	Tout le monde	Toutes les écritures validées	Cet objet et tous les objets enfants
Toutes	Tout le monde	Tous les droits étendus	Cet objet et tous les objets enfants
Toutes	Tout le monde	Créer tous les objets enfants	Cet objet et tous les objets enfants
Toutes	Tout le monde	Supprimer tous les objets enfants	Cet objet et tous les objets enfants

[↑ Haut de la page](#)

Mise en place de meilleures pratiques d'utilisation des comptes et des groupes d'administration

La mise en place des meilleures pratiques suivantes pour l'utilisation des comptes et des groupes d'administration aide à réduire la possibilité que vos ordinateurs ou votre réseau soient en contact avec des utilisateurs non autorisés qui accèdent à un compte possédant des droits élevés ou avec des utilisateurs habilités qui perturbent votre réseau de manière non intentionnelle, par leur utilisation non conforme des droits qu'ils possèdent :

- Limitez le nombre des comptes d'administration de services.
- Séparez les comptes d'administration et d'utilisation pour les utilisateurs administratifs.
- Faites appel à des personnes dignes de confiance.
- Limitez les droits administrateur aux droits strictement nécessaires.
- Contrôlez le processus d'ouverture de session d'administration.

- Sécurisez les stations de travail de type administrateur de services.
- Comprenez la façon dont les données sont déléguées dans votre entreprise.

Limitez le nombre des comptes de type administrateur de services.

En attribuant avec parcimonie les comptes de type administrateur de services et en faisant que leur nombre soit aussi limité que possible sans pour autant gêner l'organisation de votre entreprise, vous limitez ainsi les accès non autorisés. Pour les petites entreprises, deux comptes Admins du domaine suffisent. En limitant le nombre des membres, vous réduisez ainsi le nombre de comptes d'administration susceptibles d'être compromis par des utilisateurs malveillants. Les tâches effectuées par les administrateurs de services seront limitées à la modification de la configuration du service Active Directory et à la reconfiguration des contrôleurs du domaine.

N'utilisez pas les comptes administrateurs de services pour des tâches administratives quotidiennes, par exemple la gestion des comptes et des serveurs membres ; utilisez plutôt pour cela un compte utilisateur classique.

Pour utiliser votre compte utilisateur normal et effectuer sur le serveur une gestion des comptes et des membres, placez les objets à gérer dans une unité d'organisation séparée, puis faites de votre compte utilisateur l'un des membres du groupe avec les autorisations vous permettant de gérer l'unité d'organisation concernée.

Des droits d'accès Admins du domaine sont nécessaires pour pouvoir mener à bien les étapes suivantes :

1. Créez une unité d'organisation à la racine du domaine appelée **Données**. Utilisez cette unité pour stocker tous les objets à gérer par les administrateurs de données, par exemple les utilisateurs réguliers, leurs stations de travail et les serveurs membres.

Remarque : Vous pouvez également créer deux unités d'organisation au moins dans l'unité **Données**, l'une appelée **Utilisateurs** et l'autre **Ordinateurs**, puis déplacez tous les comptes utilisateur et ordinateur des conteneurs Utilisateurs et ordinateurs dans les unités d'organisation respectives. En déplaçant les objets vers les unités d'organisation, vous appliquez la politique en vigueur au niveau du groupe. Vous pouvez également créer votre propre modèle d'unité d'organisation pour répondre aux exigences de votre délégation et de la politique du groupe.

2. Créez une autre unité d'organisation à la racine du domaine appelée **Admins des données**.
3. Dans l'unité d'organisation **Admins des données**, créez un groupe local de sécurité du domaine appelé **nom_domaine Admins de données**, par exemple Admins de données Contoso. Les membres de ce groupe sont responsables de la gestion des données dans l'unité d'organisation **Données**.
4. Modifiez les autorisations existantes dans l'unité d'organisation **Données** et ce, de la façon suivante :

- Supprimez toutes les autorisations accordées aux opérateurs de compte et d'impression.
- Ajoutez l'entrée ci-jointe :

Type	Nom	Accès	S'applique à
Autoriser	Admins de données	Contrôle total	Cet objet et tous les objets enfants

5. Déplacez le compte utilisateur normal créé pour votre administrateur de domaine sur l'unité d'organisation **Données**.
6. Ajoutez le compte au groupe de sécurité **Admins de données** de **nom_domaine**.
7. Si par la suite vous souhaitez déléguer la gestion des données à d'autres administrateurs, créez leurs comptes utilisateur dans l'unité d'organisation **Admins de données** et ajoutez leurs compte au groupe de sécurité **Admins de données** de **nom_domaine**.

Séparation des comptes d'administration et d'utilisation pour les utilisateurs

administratifs

Pour chaque utilisateur jouant un rôle du type administrateur de services, créez deux comptes : un compte utilisateur classique à utiliser pour les tâches normales et l'administration des données, et un compte de type administrateur de services à utiliser uniquement pour les tâches d'administration de services. Pour ce dernier compte, nous vous conseillons de n'activer aucune messagerie ni d'utiliser aucune application courante, comme par exemple Microsoft Office ou les outils de navigation sur Internet. Affectez toujours des mots de passe différents à ces deux comptes. En prenant de telles précautions, vous réduisez les possibilités d'accès aux comptes, de même que les temps de connexion au système de ces comptes d'administration.

Affectation de personnes dignes de confiance

Les administrateurs de services contrôlent la configuration et le fonctionnement du service d'annuaire. Ainsi, cette responsabilité doit-elle être attribuée uniquement aux utilisateurs fiables et dignes de confiance, qui ont démontré un comportement responsable et qui sont en mesure de comprendre entièrement les opérations effectuées. Ces utilisateurs devront être familiarisés avec les politiques en vigueur dans votre entreprise au sujet de la sécurité et des opérations, et ils devront prouver leur volonté de renforcement de ces politiques.

Limitation des droits administrateur aux droits strictement nécessaires

Active Directory contient un groupe intégré d'opérateurs de sauvegarde. Les membres de ce groupe sont considérés comme étant des administrateurs de services car ils ont la possibilité d'ouvrir une session en local et de restaurer des fichiers sur les contrôleurs du domaine, notamment les fichiers du système d'exploitation. L'appartenance au groupe des opérateurs de sauvegarde dans Active Directory doit être limitée aux seuls individus qui sauvegardent et restaurent les contrôleurs du domaine.

Tous les serveurs membres contiennent également un groupe intégré d'opérateurs de sauvegarde, en local, sur chaque serveur. Les individus responsables de la sauvegarde des applications sur un serveur membre (par exemple, Microsoft SQL Server) doivent être membres du groupe des opérateurs de sauvegarde en local sur ce serveur. Par contre, ces utilisateurs ne devraient pas être membres du groupe des opérateurs de sauvegarde dans Active Directory.

Sur un serveur réservé au contrôleur du domaine, vous pouvez réduire le nombre des membres du groupe des opérateurs de sauvegarde. Si possible, les contrôleurs du domaine doivent être dédiés, mais dans de petites entreprises, un contrôleur de domaine est souvent utilisé pour exécuter d'autres applications. Dans ce cas, les utilisateurs responsables de la sauvegarde des applications sur le contrôleur du domaine doivent également avoir des fonctions d'administrateur de services car ils possèdent des privilèges leur permettant de restaurer des fichiers, y compris les fichiers système, sur les contrôleurs de domaine.

Évitez d'utiliser le groupe des opérateurs de compte pour déléguer une tâche d'administration de données uniquement, par exemple une gestion du compte. Les autorisations de répertoire par défaut confère au groupe la possibilité de modifier les comptes ordinateur des contrôleurs du domaine, notamment leur suppression. Par défaut, le groupe des opérateurs du compte ne contient et ne doit contenir aucun membre.

Contrôle du processus d'ouverture d'une session d'administration

Les membres des groupes Administrateurs, Administrateurs de l'entreprise et Admins du domaine constituent les groupes les plus puissants sur votre domaine. Pour réduire les risques inhérents à la sécurité, il vous faudra peut-être mettre en place des étapes supplémentaires pour renforcer les droits administratifs, par exemple des cartes à puce pour les demandes d'ouverture de session d'administration ou deux formulaires d'identification, chacun de ces formulaires étant détenu par un administrateur différent. Ces précautions supplémentaires sont abordés dans le « [Best Practice Guide for Securing Active Directory Installations](http://go.microsoft.com/fwlink/?LinkId=22342) » (Windows Server) sur le site Web de Microsoft <http://go.microsoft.com/fwlink/?LinkId=22342>.

Sécurisation des stations de travail de type administrateur de services

Outre la limitation des accès aux ressources stockées sur les contrôleurs de domaine et des accès aux informations stockées dans le répertoire, vous pouvez également renforcer la sécurité en contrôlant les stations de travail utilisées par les administrateurs de services pour des fonctions purement administratives. Les administrateurs de services doivent uniquement ouvrir une session sur des ordinateurs bien gérés, c'est-à-dire des ordinateurs pour lesquels toutes les mises à jour de sécurité et des antivirus sont installées. Si vous utilisez des droits d'accès du type administrateur de services sur un ordinateur qui n'est pas bien

géré, vous courrez le risque de compromettre vos droits d'accès dans l'éventualité où cet ordinateur serait la cible d'un utilisateur malveillant.

Pour plus d'informations sur la façon de limiter les administrateurs à l'utilisation de certaines stations de travail et de mettre en place des précautions supplémentaires, consultez le « [Best Practice Guide for Securing Active Directory Installations](http://go.microsoft.com/fwlink/?LinkId=22342) » (Windows Server) sur le site Web de Microsoft <http://go.microsoft.com/fwlink/?LinkId=22342>.

Compréhension de la délégation de données

Dans une petite entreprise, il est fort probable qu'il n'y ait qu'un ou deux administrateurs et que la délégation des données ne soit pas nécessaire. Toutefois, en fonction de la croissance de votre entreprise, il vous faudra désigner des administrateurs de données et leur déléguer une partie de l'administration des données. Les administrateurs de données sont responsables de la gestion des données stockées dans l'annuaire et sur les ordinateurs membres du domaine. Les administrateurs des données n'ont aucun contrôle sur la configuration et la distribution du service d'annuaire lui-même ; ils contrôlent les sous-ensembles des objets dans cet annuaire. L'utilisation des autorisations sur ces objets sont stockées dans l'annuaire et il est possible de limiter le contrôle effectué par un compte administrateur à des zones très spécifiques de l'annuaire. Les administrateurs de données gèrent également les ordinateurs (autres que les contrôleurs du domaine) membres de leur domaine. Ils gèrent les ressources locales, comme par exemple les impressions et le partage de fichiers sur les serveurs locaux, ainsi que les comptes des groupes et des utilisateurs pour la partie de l'organisation dont ils ont la charge. Les administrateurs de données peuvent faire valoir l'ensemble de leurs droits sur les stations de travail de gestion et ils n'ont besoin d'aucun accès physique aux contrôleurs du domaine.

La délégation de l'administration des données s'effectue en créant des groupes et en leur accordant des droits et des autorisations utilisateur appropriés, ainsi qu'en appliquant aux membres de ces groupes les paramètres en vigueur au niveau de la politique du groupe. Une fois ces étapes effectuées, il s'agit d'ajouter des comptes utilisateur aux groupes créés. La partie stratégique de cette opération consiste à accorder un accès propre et à appliquer les politiques correspondantes, en partant du principe que vous devez mettre en place un nombre d'autorisations aussi limité que possible, une sécurité optimale, tout en permettant néanmoins aux administrateurs d'effectuer leurs fonctions de délégation.

Pour plus d'informations sur la délégation de l'administration des données, consultez le « [Best Practices for Delegating Active Directory Administration](http://go.microsoft.com/fwlink/?LinkId=22707) » sur le site Web de Microsoft <http://go.microsoft.com/fwlink/?LinkId=22707>.

[↑ Haut de la page](#)

Informations complémentaires

- Pour plus d'informations sur la sécurisation d'Active Directory, consultez :
- « Sécurisation des contrôleurs de domaine Windows Server » dans le kit de sécurité.
- « [Best Practice Guide for Securing Active Directory Installations](http://go.microsoft.com/fwlink/?linkid=22342) » (Windows Server) sur le site Web de Microsoft à l'adresse <http://go.microsoft.com/fwlink/?linkid=22342>.
- « [Best Practices for Delegating Active Directory Administration](http://go.microsoft.com/fwlink/?linkid=22707) » sur le site Web de Microsoft à l'adresse <http://go.microsoft.com/fwlink/?linkid=22707>.

Pour plus d'informations générales sur les comptes Builtin et la migration de Microsoft® Windows NT® 4.0 à Active Directory, consultez :

- « [Default Groups](http://go.microsoft.com/fwlink/?linkid=22706) » sur le site Web TechNet à l'adresse <http://go.microsoft.com/fwlink/?linkid=22706>.
- « [Migrating from Windows NT Server 4.0 to Windows Server](http://go.microsoft.com/fwlink/?linkid=22709) » sur le site Web de Microsoft à l'adresse <http://go.microsoft.com/fwlink/?linkid=22709>.

[↑ Haut de la page](#)

[Gérez votre profil](#)