

# Active Directory et notions de groupes



# Les Groupes, Introduction

- Un groupe est un ensemble de comptes d'utilisateurs et d'ordinateurs, de contacts et d'autres groupes qui peut être géré comme une entité unique. Les utilisateurs et les ordinateurs qui appartiennent à un groupe sont les membres du groupe.
- L'utilisation de groupes peut simplifier l'administration en permettant d'assigner un même ensemble d'autorisations et de droits à plusieurs comptes à la fois, au lieu de les assigner à chaque compte individuellement.

# Les Groupes, Introduction

- Un groupe peut être basé sur l'annuaire ou être un groupe local d'un ordinateur particulier. Dans Active Directory, les groupes sont des objets d'annuaire qui résident dans des conteneurs de type domaine et unité d'organisation. Active Directory fournit, dès son installation, un ensemble de groupes par défaut et la possibilité de créer des groupes.

# Les Groupes, Introduction

- Les groupes définis dans Active Directory permettent d'effectuer les tâches suivantes :
  - Assigner des autorisations sur une ressource partagée à un groupe plutôt qu'à des utilisateurs individuels, ce qui simplifie l'administration. Tous les membres du groupe disposent du même accès à la ressource.
  - Déléguer des tâches d'administration en assignant des droits d'utilisateur une seule fois à un groupe via une stratégie de groupe, puis en ajoutant au groupe les membres auxquels vous souhaitez accorder les mêmes droits qu'au groupe.
  - Créer des listes de distribution de courrier électronique.

# Les Groupes, Introduction

- Les groupes se caractérisent par leur étendue et leur type. L'étendue détermine la limite d'application du groupe au sein d'un domaine ou d'une forêt. Le type d'un groupe détermine si ce groupe peut être utilisé pour assigner des autorisations à partir d'une ressource partagée (cas des groupes de sécurité) ou seulement pour des listes de distribution de courrier électronique (cas des groupes de distribution). Il existe également des groupes pour lesquels vous ne pouvez ni afficher, ni modifier les membres.

# Les Groupes, Introduction

- Ces groupes sont appelés des identités spéciales et servent à représenter différents utilisateurs à différents moments, en fonction des circonstances. Par exemple, le groupe Tout le monde représente tous les utilisateurs actuels du réseau, y compris les invités et les utilisateurs d'autres domaines.

# Étendue du Groupe

- Qu'il s'agisse d'un groupe de sécurité ou d'un groupe de distribution, tout groupe est caractérisé par une étendue qui délimite son application dans l'arborescence de domaine ou dans la forêt. Il existe trois étendues de groupe : universelle, globale et domaine local.

# Étendue du Groupe

- Les membres des groupes universels peuvent inclure d'autres groupes et comptes, provenant de n'importe quel domaine de l'arborescence de domaine ou de la forêt ; ils peuvent se voir assigner des autorisations dans n'importe quel domaine de cette arborescence ou de cette forêt.
- Les membres d'un groupe global peuvent comprendre d'autres groupes et comptes issus du seul domaine où ce groupe est défini ; ils peuvent se voir assigner des autorisations dans n'importe quel domaine de la forêt.

# Étendue du Groupe

- Les membres d'un groupe de domaine local peuvent comprendre d'autres groupes et comptes issus de domaines Windows Server 2003, Windows 2000 ou Windows NT ; ils peuvent se voir assigner des autorisations au sein de leur domaine uniquement.

# Récapitulatif des comportements des différentes étendues de groupe

- Étendue Universelle:
  - Lorsque le niveau de fonctionnalité du domaine est Windows 2000 en mode natif ou Windows Server 2003, les membres des groupes universels peuvent comprendre des comptes, des groupes globaux et des groupes universels provenant de n'importe quel domaine.
  - Lorsque le niveau de fonctionnalité du domaine est Windows 2000 en mode mixte, il n'est pas possible de créer des groupes de sécurité d'étendue universelle.

## Récapitulatif des comportements des différentes étendues de groupe

- Lorsque le niveau de fonctionnalité du domaine est Windows 2000 en mode natif ou Windows Server 2003, il est possible d'ajouter des groupes à d'autres groupes et de leur assigner des autorisations dans n'importe quel domaine.
- Il est possible de convertir les groupes en groupes de domaine local. Un groupe peut être converti en groupe de domaine local à condition de ne pas avoir pour membres d'autres groupes universels.

# Récapitulatif des comportements des différentes étendues de groupe

- Étendue globale:
  - Lorsque le niveau de fonctionnalité du domaine est Windows 2000 en mode natif ou Windows Server 2003, les membres des groupes globaux peuvent comprendre des comptes et des groupes globaux du même domaine.
  - Lorsque le niveau de fonctionnalité du domaine est Windows 2000 en mode mixte, les membres des groupes globaux peuvent comprendre des comptes du même domaine.

## Récapitulatif des comportements des différentes étendues de groupe

- Il est possible d'ajouter des groupes à d'autres groupes de leur assigner des autorisations dans n'importe quel domaine.
- Un groupe peut être converti en groupe d'étendue universelle à condition de ne pas être membre d'un autre groupe d'étendue globale.

# Récapitulatif des comportements des différentes étendues de groupe

- Étendue de domaine local:
  - Lorsque le niveau de fonctionnalité du domaine est Windows 2000 en mode natif ou Windows Server 2003, les membres des groupes de domaine local peuvent comprendre des comptes, des groupes globaux et des groupes universels de n'importe quel domaine ainsi que des groupes de domaine local du même domaine.
  - Lorsque le niveau de fonctionnalité du domaine est Windows 2000 mixte, les membres des groupes de domaine local peuvent comprendre des comptes et des groupes globaux de n'importe quel domaine.

## Récapitulatif des comportements des différentes étendues de groupe

- Lorsque le niveau de fonctionnalité du domaine est Windows 2000 mixte, les membres des groupes de domaine local peuvent comprendre des comptes et des groupes globaux de n'importe quel domaine.
- Il est possible d'ajouter des groupes à d'autres groupes de domaine local et de leur assigner des autorisations dans ce domaine uniquement.
- Un groupe peut être converti en groupe d'étendue universelle à condition de ne pas avoir pour membre un autre groupe de domaine local.

# groupes avec une étendue de domaine local

- Les groupes avec une étendue de domaine local vous aident à définir et à gérer l'accès aux ressources à l'intérieur d'un domaine unique. Ces groupes peuvent avoir comme membres :
  - Des groupes avec une étendue globale
  - Des groupes avec une étendue universelle
  - Des comptes
  - D'autres groupes avec une étendue de domaine local
  - Un mélange des éléments mentionnés ci-dessus

## groupes avec une étendue de domaine local

- Par exemple, pour permettre à cinq utilisateurs d'accéder à une imprimante spécifique, vous pouvez ajouter les cinq comptes d'utilisateurs à la liste d'autorisations de l'imprimante. Cependant, si vous souhaitez ensuite autoriser les utilisateurs à accéder à une nouvelle imprimante, vous serez obligé de placer à nouveau les cinq comptes d'utilisateur dans la liste d'autorisations de la nouvelle imprimante.

## groupes avec une étendue de domaine local

- Avec un minimum de planification, vous pouvez simplifier cette tâche d'administration en créant un groupe avec une étendue de domaine local et l'autoriser à accéder à l'imprimante. Placez les cinq comptes d'utilisateurs dans un groupe ayant une étendue globale et ajoutez ce groupe à celui qui a une étendue de domaine local. Si vous souhaitez autoriser les cinq utilisateurs à accéder à la nouvelle imprimante, attribuez une autorisation d'accès au groupe qui a une étendue de domaine local. Tous les membres du groupe qui a une étendue globale accèdent automatiquement à la nouvelle imprimante.

## Récapitulatif des comportements des différentes étendues de groupe

- Étendue globale:
  - Utilisez des groupes avec une étendue globale pour gérer des objets annuaire qui nécessitent une maintenance quotidienne, tels que les comptes d'utilisateurs et d'ordinateurs. Comme les groupes qui ont une étendue globale ne sont pas répliqués à l'extérieur de leur propre domaine, les comptes situés dans un groupe qui a une étendue globale peuvent être modifiés régulièrement sans provoquer un trafic de réplication sur le catalogue global.

## Récapitulatif des comportements des différentes étendues de groupe

- Même si l'attribution de droits et d'autorisations n'est valide qu'à l'intérieur du domaine où elle est effectuée, en appliquant des groupes avec une étendue globale de manière homogène sur les domaines appropriés, vous pouvez consolider les références aux comptes qui ont des objectifs similaires. Ceci permet de simplifier et de rationaliser la gestion des groupes à travers les domaines.

## Récapitulatif des comportements des différentes étendues de groupe

- Par exemple, dans un réseau qui comporte deux domaines, Europe et ÉtatsUnis, s'il existe un groupe avec une étendue globale nommé ComptabilitéGL dans le domaine ÉtatsUnis, il doit également exister un groupe appelé ComptabilitéGL dans le domaine Europe (sauf si la fonction comptabilité n'existe pas dans le domaine Europe).
- Il est fortement recommandé d'utiliser des groupes globaux ou universels au lieu de groupes de domaine local lorsque vous définissez des autorisations pour des objets d'annuaire du domaine répliqués sur le catalogue global.

# Récapitulatif des comportements des différentes étendues de groupe

- Étendue universelle:
  - Utilisez des groupes avec une étendue universelle pour consolider des groupes qui s'étendent sur plusieurs domaines. Pour y parvenir, ajoutez les comptes à des groupes qui ont une étendue globale et imbriquez ces groupes à l'intérieur de groupes qui ont une étendue universelle. Avec cette stratégie, aucune modification apportée à l'appartenance aux groupes d'étendue globale n'affectera les groupes qui ont une étendue universelle.

## Récapitulatif des comportements des différentes étendues de groupe

- Par exemple, dans un réseau qui comporte deux domaines, Europe et ÉtatsUnis, et un groupe d'étendue globale appelé ComptabilitéGL dans chaque domaine, créez un groupe avec une étendue universelle appelé ComptabilitéU, qui aura comme membres les deux groupes ComptabilitéGL, ÉtatsUnis\ComptabilitéGL et Europe\ComptabilitéGL. Le groupe ComptabilitéU peut ensuite être utilisé n'importe où dans l'entreprise. Les modifications apportées à l'appartenance aux groupes ComptabilitéGL individuels ne provoqueront pas la réplication du groupe ComptabilitéU.

## Récapitulatif des comportements des différentes étendues de groupe

- L'appartenance à un groupe d'étendue universelle ne doit pas être modifiée fréquemment. En effet, toute modification apportée à ces appartenances de groupe provoque la réplication de toute l'appartenance du groupe sur chaque catalogue global de la forêt.

## Modification de l'étendue d'un groupe

- Lors de la création d'un nouveau groupe, ce dernier est configuré par défaut en tant que groupe de sécurité d'étendue globale, quel que soit le niveau de fonctionnalité actuel du domaine. Il n'est pas possible de modifier l'étendue d'un groupe dans les domaines dont le niveau de fonctionnalité est Windows 2000 en mode mixte, mais les conversions suivantes sont autorisées dans les domaines dont le niveau de fonctionnalité est Windows 2000 en mode natif ou Windows Server 2003 :

## Modification de l'étendue d'un groupe

- **Global vers universel.** Cette conversion n'est autorisée que si le groupe n'est pas membre d'un autre groupe d'étendue globale.
- **Domaine local vers universel.** Cette conversion n'est autorisée que si le groupe n'a pas comme membre un autre groupe de domaine local.
- **Universel vers global.** Cette conversion n'est autorisée que si le groupe n'a pas comme membre un autre groupe d'étendue universelle.
- **Universel vers domaine local.** Cette opération n'est soumise à aucune restriction.

## Groupe sur ordinateur clients et serveurs autonome

- Certaines fonctionnalités de groupe, telles que les groupes universels, l'imbrication de groupes et la distinction entre groupes de sécurité et groupes de distribution ne sont disponibles que sur les contrôleurs de domaine et les serveurs membres Active Directory. Les comptes de groupe définis sur Windows 2000 Professionnel, Windows XP Professionnel, Windows 2000 Server et les serveurs autonomes exécutant Windows Server 2003 fonctionnent de la même façon que dans Windows NT 4.0 :

## Groupe sur ordinateur clients et serveurs autonome

- Seuls les groupes locaux peuvent être créés localement sur l'ordinateur. Un groupe local créé sur l'un de ces ordinateurs ne peut recevoir des autorisations que pour cet ordinateur.

# Types de groupes

- Les groupes sont utilisés pour regrouper des comptes d'utilisateurs, des comptes d'ordinateur et d'autres comptes de groupes en unités faciles à gérer. Le fait de travailler avec des groupes plutôt qu'avec des utilisateurs individuels simplifie considérablement la maintenance et l'administration du réseau.
- Active Directory met en œuvre 2 types de groupes : groupes de distribution et groupes de sécurité. Vous pouvez utiliser les groupes de distribution pour créer des listes de distribution de courrier électronique et les groupes de sécurité pour affecter des autorisations à des ressources partagées.

# Types de groupes

- Groupes de distributions:
  - Les groupes de distribution peuvent être utilisés uniquement avec des applications de courrier électronique (par exemple Microsoft Exchange) pour envoyer du courrier à un ensemble d'utilisateurs. Les groupes de distribution ne sont pas activés pour la sécurité, ce qui signifie qu'ils ne peuvent pas être répertoriés dans des listes de contrôle d'accès discrétionnaire (DACL, Discretionary Access Control List). Si vous avez besoin d'un groupe pour contrôler l'accès à des ressources partagées, créez un groupe de sécurité.

# Types de groupes

- Groupes de sécurité:
  - Utilisés avec soin, les groupes de sécurité constituent une méthode efficace pour assigner l'accès aux ressources de votre réseau. Les groupes de sécurité vous permettent d'effectuer les tâches suivantes :
    - *Assigner des droits d'utilisateur à des groupes de sécurité dans Active Directory*
    - *Assigner aux groupes de sécurité des autorisations sur les ressources*

# Types de groupes

- Comme les groupes de distribution, les groupes de sécurité peuvent également être utilisés comme une entité de courrier électronique. Lorsque vous envoyez un message de courrier électronique à un groupe, ce message est envoyé à tous les membres du groupe.

## Conversion d'un groupe de sécurité en groupe de distribution et vice-versa

- Vous pouvez convertir à tout moment un groupe de sécurité en groupe de distribution et vice-versa, mais à condition que le niveau fonctionnel du domaine soit Windows 2000 en mode natif ou supérieur. Il est impossible de convertir des groupes lorsque le niveau fonctionnel du domaine est Windows 2000 en mode mixte.

# Groupes locaux par défaut

- Le dossier Groupes situé dans Utilisateurs et groupes locaux de la console MMC (Microsoft Management Console) affiche les groupes locaux par défaut ainsi que les groupes locaux que vous avez créés. Les groupes locaux par défaut sont créés automatiquement lorsque vous installez un serveur autonome ou un serveur membre exécutant Windows Server 2003. L'appartenance à un groupe local fait bénéficier l'utilisateur de certains droits et autorisations pour effectuer diverses tâches sur l'ordinateur local.

# Groupes locaux par défaut

- Vous pouvez ajouter aux groupes locaux des comptes d'utilisateurs, des comptes d'utilisateurs de domaine, des comptes d'ordinateurs et des comptes de groupe locaux. Toutefois, vous ne pouvez pas ajouter des comptes d'utilisateurs locaux et des comptes de groupes locaux aux comptes de groupes du domaine.

# Descriptions des groupes par défaut

- Le Groupe Administrateurs:

- Descriptions:

→ Les membres de ce groupe possèdent le contrôle total du serveur et peuvent affecter des droits d'utilisateur et des autorisations de contrôles d'accès aux utilisateurs en fonction des besoins. Le compte Administrateur est également un membre par défaut. Lorsque ce serveur est joint à un domaine, le groupe Admins du domaine est automatiquement ajouté à ce groupe. Ce groupe disposant du contrôle total du serveur, il est conseillé d'y ajouter des utilisateurs avec précaution. Pour plus d'informations, voir Groupes locaux par défaut et Groupes par défaut.

## Descriptions des groupes par défaut

- Droits d'utilisateurs par défaut:
  - Accéder à cet ordinateur à partir du réseau ; ajuster les quotas mémoire pour un processus ; permettre l'ouverture d'une session locale ; autoriser l'ouverture de session par les services Terminal Server ; sauvegarder des fichiers et des répertoires ; ignorer le contrôle de parcours ; modifier l'heure du système ; déboguer des programmes créer un fichier d'échange; forcer l'arrêt à partir d'un système distant ; augmenter la priorité de planification ; charger et décharger des pilotes de périphérique ; gérer le journal d'audit et de sécurité ;

## Descriptions des groupes par défaut

modifier les variables d'environnement de microprogrammation ; effectuer des tâches de maintenance sur les volumes ; optimiser un processus ; optimiser les performances système ; retirer un ordinateur d'une station d'accueil ; restaurer des fichiers et des répertoires ; arrêter le système ; s'approprier des fichiers ou d'autres objets.

# Descriptions des groupes par défaut



# Imbrication de groupes

- L'imbrication vous permet d'ajouter un groupe en tant que membre d'un autre groupe. Vous imbriquez des groupes pour consolider les comptes membres et réduire le trafic de réplication.
- Les options d'imbrication sont variables selon que le niveau de fonctionnalité de votre domaine Windows Server 2003 est Windows 2000 en mode natif ou Windows 2000 en mode mixte.

# Imbrication de groupes

- Les groupes définis dans les domaines dont le niveau fonctionnel est Windows 2000 en mode natif et les groupes de distribution définis dans les domaines dont le niveau fonctionnel est Windows 2000 en mode mixte peuvent avoir les membres suivants :
  - Les groupes avec une étendue universelle peuvent avoir comme membres : des comptes, des comptes d'ordinateurs, d'autres groupes avec une étendue universelle et des groupes avec une étendue globale de n'importe quel domaine.
  - Les groupes avec une étendue globale peuvent avoir comme membres : des comptes du même domaine et d'autres groupes avec une étendue globale du même domaine.

# Imbrication de groupes

- Les groupes avec une étendue globale peuvent avoir comme membres : des comptes du même domaine et d'autres groupes avec une étendue globale du même domaine.
- Les groupes avec une étendue de domaine local peuvent avoir comme membres : des comptes, des groupes avec une étendue universelle et des groupes avec une étendue globale, tous de n'importe quel domaine. Ces types de groupes peuvent également avoir comme membres d'autres groupes à étendue locale du même domaine.

# Imbrication de groupes

- Les groupes de sécurité définis dans des domaines de niveau fonctionnel Windows 2000 en mode mixte sont limités aux types de membres suivants :
  - Les groupes avec une étendue globale ne peuvent avoir comme membres que des comptes.
  - Les groupes avec une étendue de domaine local peuvent avoir comme membres d'autres groupes avec une étendue globale et des comptes.

# Imbrication de groupes

- Il n'est pas possible de créer des groupes de sécurité avec une étendue universelle dans des domaines dont le niveau fonctionnel est Windows 2000 en mode mixte dans la mesure où l'étendue universelle n'est prise en charge que dans les domaines de niveau fonctionnel Windows 2000 en mode natif ou Windows Server 2003.

# Identité spéciales

- En plus des groupes contenus dans les conteneurs Utilisateurs et Builtin, les serveurs exécutant Windows Server 2003 comprennent plusieurs identités spéciales. Par commodité, ces identités sont souvent appelées groupes. Ces groupes spéciaux n'ont pas une appartenance au groupe spécifique qui peut être modifiée, mais ils peuvent représenter des utilisateurs divers à des moments différents, selon les circonstances. Les groupes spéciaux sont les suivants :

# Identité spéciales

## - Ouverture de session anonyme:

Représente les utilisateurs et les services qui accèdent à un ordinateur et ses ressources sans utiliser un nom de compte, un mot de passe ou un nom de domaine. Sur les ordinateurs exécutant Windows NT ou version antérieure, le groupe Anonymous Logon est un membre par défaut du groupe Tout le monde. Sur les ordinateurs exécutant un membre de la famille Windows Server 2003, le groupe Anonymous Logon n'est pas un membre par défaut du groupe Tout le monde.

# Identité spéciales

- Tout le monde:

Représente tous les utilisateurs du réseau actuels, y compris les invités et les utilisateurs d'autres domaines. Chaque fois qu'un utilisateur ouvre une session sur le réseau, il est ajouté automatiquement au groupe Tout le monde.

# Identité spéciales

## - Réseau:

Représente les utilisateurs qui accèdent actuellement à une ressource spécifique sur le réseau (par opposition aux utilisateurs qui accèdent à une ressource en ouvrant une session locale sur l'ordinateur qui contient cette ressource). Chaque fois qu'un utilisateur accède à une ressource spécifique sur le réseau, il est ajouté automatiquement au groupe Réseau.

# Identité spéciales

- Interactif:

Représente tous les utilisateurs connectés actuellement à un ordinateur spécifique et qui accèdent à une ressource donnée sur cet ordinateur (par opposition aux utilisateurs qui accèdent à la ressource sur le réseau). Chaque fois qu'un utilisateur accède à une ressource spécifique sur l'ordinateur auquel il est actuellement connecté, il est ajouté automatiquement au groupe Interactif.

# Identité spéciales

- Même si les identités spéciales peuvent recevoir des droits et des autorisations pour les ressources, ces appartenances au groupe ne peuvent pas être modifiées ou affichées. Les étendues de groupe ne s'appliquent pas aux identités spéciales. Les utilisateurs sont affectés automatiquement à ces identités spéciales chaque fois qu'ils ouvrent une session sur une ressource spécifique ou qu'ils y accèdent.

# Où les groupes peuvent-ils être créés ?

- Dans Active Directory, les groupes sont créés à l'intérieur de domaines. Vous créez les groupes à l'aide de Utilisateurs et ordinateurs Active Directory. Avec les autorisations nécessaires, des groupes peuvent être créés dans le domaine racine de la forêt, dans tout autre domaine de la forêt ou dans une unité d'organisation.

# Où les groupes peuvent-ils être créés ?

- En plus du domaine dans lequel il est créé, un groupe se caractérise également par son étendue. L'étendue d'un groupe détermine :
  - Le domaine à partir duquel les membres peuvent être ajoutés
  - Le domaine dans lequel les droits et autorisations attribués au groupe sont valides

# Où les groupes peuvent-ils être créés ?

- Choisissez le domaine ou l'unité d'organisation où vous créez un groupe en fonction de l'administration requise pour le groupe. Par exemple, si votre annuaire comporte plusieurs unités d'organisation, chacune avec un administrateur différent, vous pouvez créer des groupes avec une étendue globale à l'intérieur de ces unités d'organisation. Ceci permettra aux administrateurs de gérer l'appartenance au groupe des utilisateurs dans l'unité d'organisation respective.

## Où les groupes peuvent-ils être créés ?

- Si les groupes sont requis pour le contrôle d'accès à l'extérieur de l'unité d'organisation, vous pouvez imbriquer les groupes situés à l'intérieur de l'unité d'organisation dans des groupes ayant une étendue universelle (ou d'autres groupes ayant une étendue globale) et pouvant être utilisés ailleurs dans la forêt.

# Où les groupes peuvent-ils être créés ?

- Si le niveau fonctionnel de domaine est paramétré pour Windows 2000 mode natif ou version ultérieure, le domaine contient une hiérarchie d'unités d'organisation et l'administration est déléguée à des administrateurs situés sur chaque unité d'organisation, il est donc plus efficace d'imbriquer des groupes avec une étendue globale. Par exemple, si l'unité d'organisation UO1 contient les unités d'organisation UO2 et UO3, un groupe avec une étendue globale situé sur l'UO1 peut avoir comme membres des groupes avec une étendue globale situés sur l'UO2 et l'UO3.

# Où les groupes peuvent-ils être créés ?

- Dans l'UO1, l'administrateur peut ajouter ou supprimer des membres de groupe. Dans l'UO2 et l'UO3, les administrateurs peuvent ajouter ou supprimer des membres de groupe pour les comptes à partir de leurs propres unités d'organisation et sans avoir des droits d'administration pour le groupe qui a l'étendue globale dans l'UO1.

# Où les groupes peuvent-ils être créés ?

- Remarque:
  - Les groupes peuvent être déplacés à l'intérieur d'un domaine. Toutefois, seuls les groupes qui ont une étendue universelle peuvent être déplacés d'un domaine à l'autre. Les droits et autorisations attribués à un groupe ayant une étendue universelle sont perdus lorsque le groupe est déplacé vers un autre domaine. De nouveaux droits et autorisations doivent être attribués.

# Sources

- [www.microsoft.com](http://www.microsoft.com)
- [www.laboratoire-microsoft.org](http://www.laboratoire-microsoft.org)
- Bouquin Windows 2003 serveur (édition Microsoft press)