netwrix

Bonnes pratiques de gestion des groupes Active Directory

Table des matières

Le meilleur moyen de contrôler l'accès aux ressources et d'appliquer un modèle du moindre privilège consiste à utiliser les groupes Microsoft Active Directory. Ces groupes vous permettent également de recenser plus facilement les autorisations relatives à toutes vos ressources, qu'il s'agisse d'un serveur de fichiers indows ou d'une base de données SQL.

Étendues des groupes

Les objets que vous pouvez ajouter à un groupe AD dépendent de l'étendue de ce groupe.

Group scope	Members from the Same Domain	Members from Another Domain in the Same Forest	Members from a Trusted External Domain
Local	Users Computers Global groups Universal groups Domain local groups Local users defined on the same computer as the local group	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups
Domain Local	Users Computers Global groups Universal groups Domain local groups	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups
Universal	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups	N/A
Global	Users Computers Global groups	N/A	N/A

- **Les groupes locaux** sont vraiment locaux. Ils sont définis et disponibles uniquement pour l'ordinateur spécifique sur lequel ils ont été créés. Ne créez pas de nouveaux groupes locaux sur les postes de travail ; dans la plupart des cas, les seuls groupes locaux qu'il faut gérer sont les groupes d'utilisateurs et d'administrateurs.

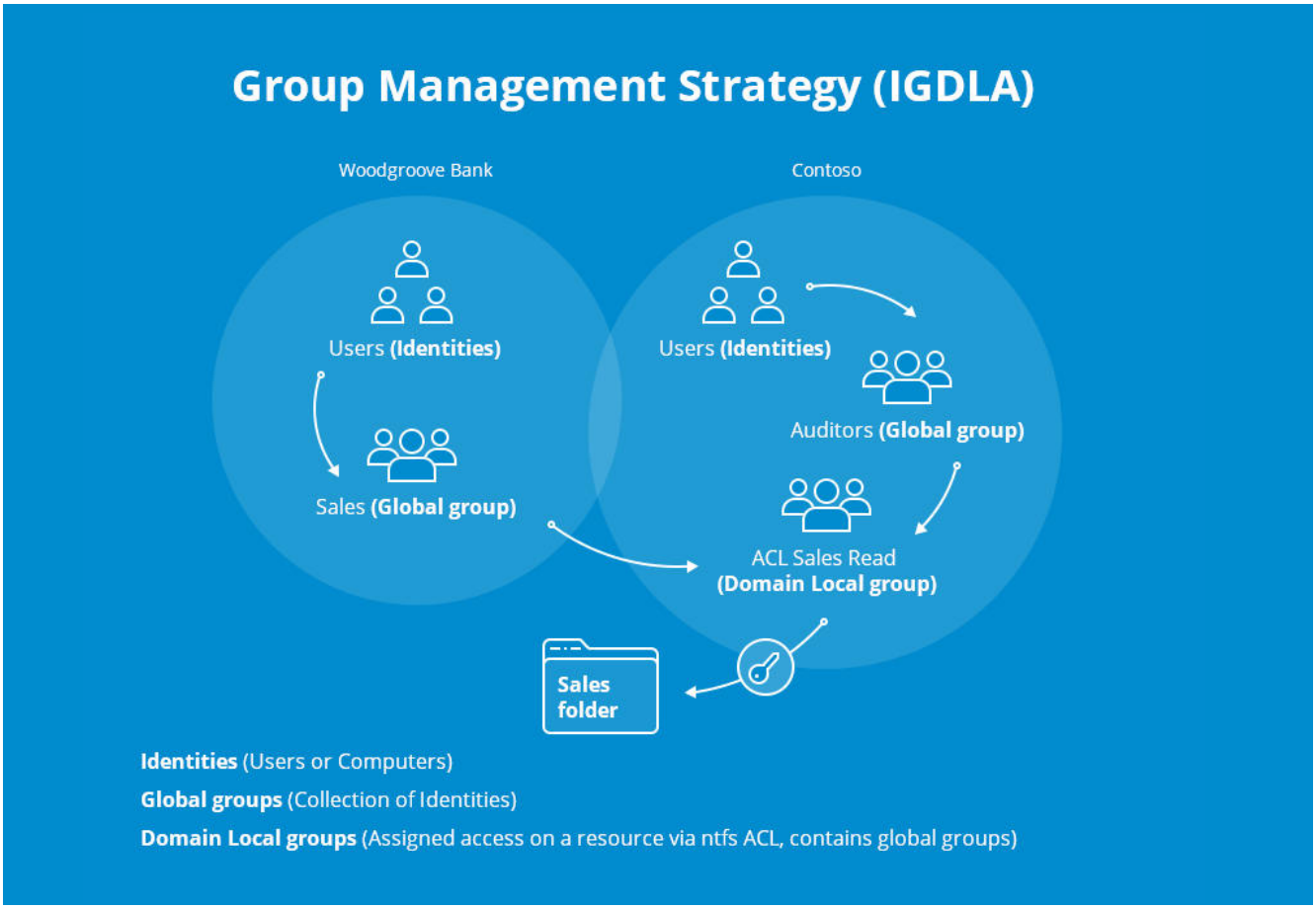
- **Les groupes locaux de domaine** permettent de gérer les autorisations des ressources, car ils peuvent être appliqués partout dans le domaine. Un groupe local de domaine peut inclure des membres du domaine de tout type et des membres issus de domaines de confiance. Supposons par exemple que vous deviez gérer l'accès à une collection de dossiers sur un ou plusieurs serveurs contenant des informations destinées aux responsables. Le groupe que vous créez dans ce but doit être un groupe local de domaine (par exemple, « DL_Managers_Modify »).

- **Les groupes universels** d'Active Directory sont utiles dans les forêts multi-domaines. Ils vous permettent de définir des rôles ou de gérer des ressources couvrant plusieurs domaines. Chaque groupe universel est stocké dans le domaine dans lequel il a été créé, mais son appartenance aux groupes est stockée dans le catalogue global et répercutée à l'ensemble de la forêt. N'utilisez pas les groupes universels si vous n'avez qu'un seul domaine.

- **Les groupes globaux** servent principalement à définir des collections d'objets de domaine (utilisateurs, autres groupes globaux et ordinateurs) en fonction des rôles métier, ce qui signifie qu'ils servent principalement de groupes de rôles. Les groupes d'utilisateurs basés sur des rôles (par exemple, « RH » ou « Marketing ») et les groupes d'ordinateurs basés sur des rôles (par exemple, « Postes de travail marketing ») sont généralement des groupes globaux.

Bonnes pratiques de gestion des groupes imbriqués d'Active Directory

Comme l'illustre le tableau ci-dessus, un groupe peut être membre d'un autre groupe ; ce processus s'appelle l'imbrication. L'imbrication vous permet de mieux gérer et administrer votre environnement en fonction des rôles métier, des fonctions et des règles de gestion.



- Les comptes d'utilisateur et d'ordinateur doivent être membres de groupes globaux qui correspondent à des rôles métier, par exemple « Ventes » ou « RH ». Ces groupes globaux doivent être membres de groupes locaux de domaine qui appliquent les règles de gestion – en déterminant qui a accès à quoi, par exemple. Ces groupes locaux de domaine reçoivent des autorisations d'accès aux ressources. Dans le cas d'un dossier partagé, l'accès est accordé en ajoutant le groupe local de domaine à la liste de contrôle d'accès (ACL) du dossier avec des autorisations offrant le niveau d'accès approprié.

- Autrement dit :
  - Ajoutez des comptes d'utilisateur et d'ordinateur à un groupe global.
  - Ajoutez le groupe global à un groupe universel.
  - Appliquez à une ressource les autorisations du groupe de sécurité Active Directory pour le groupe
  - local de domaine.
  - Les comptes du groupe global initial auront accès à la ressource selon les autorisations appliquées au groupe local de domaine.

Différences entre groupes de sécurité et groupes de distribution

Les groupes de sécurité et les groupes de distribution d'Active Directory sont deux choses différentes. Par exemple, vous pouvez utiliser les groupes de sécurité pour attribuer des autorisations aux ressources partagées, et les groupes de distribution pour créer des listes de diffusion de courrier électronique dans un environnement Exchange. Grâce à cette technologie, lorsqu'un utilisateur « se connecte » à un ordinateur, la machine crée son « jeton d'accès ». Un jeton d'accès contient tous les SID (identificateurs de sécurité) des groupes de sécurité dont l'utilisateur est membre. Les SID des groupes de distribution ne sont pas inclus. Pour faire simple, vous ne pouvez pas attribuer d'autorisations aux groupes de distribution, et même si vous le faisiez, cela n'aurait aucun effet.

Conseils pour la gestion des groupes

- Avant de se lancer dans des tâches de gestion de groupes, configurez les capacités d'audit d'Active Directory de manière à enregistrer les ajouts, les suppressions et les modifications d'appartenance aux groupes. Ceci peut se faire avec des outils natifs ou avec des outils tiers comme Netwrix Auditor for Active Directory.
- Créez un groupe global pour chaque rôle ou service (ventes, marketing, direction, comptables, etc.).
- Mettez en place des conventions d'appellation standard dans toute votre organisation afin de faciliter l'identification des informations essentielles relatives à un groupe. Les noms de groupe peuvent inclure des détails critiques sur le groupe, par exemple le niveau d'accès, le type de ressource, le niveau de sécurité, l'étendue du groupe, les capacités de messagerie, etc. Par exemple, le nom de groupe « DL_Managers_Modify » signifie que pour le dossier sélectionné, les responsables ne doivent avoir que des autorisations de modification.
- Organisez les groupes d'une manière facile à comprendre, par exemple en fonction de la situation géographique ou de la hiérarchie dans l'entreprise. Utilisez les descriptions de groupe pour décrire de manière détaillée l'objectif du groupe.
- Les services informatiques sont souvent réticents à déléguer les responsabilités de gestion des groupes AD, pourtant ils sont vraiment les derniers à devoir les assumer. Les groupes doivent être gérés par les employés propriétaires des contenus régis par les groupes, et non par des informaticiens disposant d'une visibilité limitée sur l'objectif du groupe. En refusant de déléguer le contrôle, le service informatique paralyse les ressources informatiques et enlève du pouvoir aux personnes qui devraient posséder et gérer leurs groupes.
- Les employés devraient être habilités à s'ajouter aux groupes appropriés sans avoir à passer par le service informatique pour être ajoutés manuellement. Choisissez une solution logicielle de gestion des groupes en libre-service dotée d'un workflow d'appartenance : les utilisateurs demandent à être membres des groupes qui leur sont utiles, les propriétaires des groupes reçoivent des notifications et peuvent approuver ou refuser la demande en cliquant sur un bouton.
- Dans la plupart des cas, l'appartenance à un groupe doit être définie de manière dynamique dans votre système informatique RH ou vos bases de données de projets par des informations telles que des règles, des attributs AD, des données sur les employés et les sous-traitants. Vous pouvez utiliser ces sources de données pour créer des groupes dynamiques constamment actualisés. Par exemple, si un employé est retiré du système RH, son compte sera automatiquement supprimé des groupes dynamiques dont l'appartenance dépend de ce système.

About Netwrix

Netwrix est un éditeur de logiciels qui permet aux professionnels de la sécurité et de la gouvernance de l'information de reprendre le contrôle des données sensibles, réglementées et stratégiques, quel que soit leur emplacement. Plus de 10 000 organisations du monde entier s'appuient sur les solutions Netwrix pour sécuriser leurs données sensibles, tirer pleinement parti des contenus d'entreprise, réussir les audits de conformité en déployant moins d'efforts et en dépensant moins et améliorer la productivité de leurs équipes informatiques et de leurs travailleurs du savoir.

Fondée en 2006, Netwrix a obtenu plus de 150 distinctions sectorielles et a été sélectionnée dans les listes Inc. 5000 et Deloitte Technology Fast 500, qui recensent les entreprises à la croissance la plus rapide aux États-Unis.

Pour en savoir plus, visitez www.netwrix.fr.

Siège social :
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Tél : +33 9 75 18 11 19 **Gratuit :** 888-638-9749 **EMEA:** +44 (0) 203-588-3023
netwrix.com/social

Gardez un œil sur vos groupes Active Directory

avec Netwrix Auditor

- Enquêtez sur l'état courant de vos groupes AD incluant leurs autorisations et leurs membres
- Détectez toutes les modifications apportées à chaque groupe et fournissez les détails essentiels : qui a modifié quoi, quand et où, ainsi que les valeurs avant et après
- Soyez averti de toutes les modifications importantes apportées à vos groupes AD
- Annulez des modifications sans aucun temps d'arrêt ni restauration à partir d'une sauvegarde

Télécharger un essai de 20 jours