SCiT
Service Conseil IT

41, rue André Ampère
ZAC de l'Aufresne
44150 ANCENIS
Tél. : 02 40 09 72 72
Fax : 02 40 83 43 74

Bonnes pratiques de la sécurité Windows (AD/Groupes/Partages)

TABLE DES MATIÈRES

1. Permission de partage 2
2. Permission NTFS 2
3. Bonnes pratiques 3
5. Mots de passe 6

41, rue André Ampère
ZAC de l'Aufresne
44150 ANCENIS
Tél. : 02 40 09 72 72
Fax : 02 40 83 43 74

Lorsque l'on créé un partage NTFS, deux niveaux de permissions sont à définir :

- ✓ Les permissions de partage
- ✓ Les permissions NTFS

Ces deux permissions sont indépendantes l'une de l'autre, c'est-à-dire qu'elles ne se modifient pas réciproquement. En revanche, le droit d'accès à la ressource finale résulte de la combinaison de ces deux permissions.

1.Permission de partage

Les permissions de partage s'appliquent uniquement pour les partages réseaux et ne s'appliquent donc pas aux utilisateurs ayant un accès local au dossier (accès à l'explorateur de fichiers sur le serveur de fichiers, par exemple lors d'un accès à un bureau à distance). On peut les définir sur trois niveaux :

- ✓ **Lecture :** voir les fichiers et les dossiers, ouvrir un fichier ou un dossier, exécuter un programme.
- ✓ **Modification :** en plus des droits de lecture, ce droit donne également la possibilité d'ajouter des fichiers, créer des dossiers, modifier les fichiers et de supprimer les fichiers et les dossiers.
- ✓ **Contrôle total :** les droits de modification et de lecture avec en plus la possibilité de modifier les permissions NTFS sur les dossiers et les fichiers.

Ce premier niveau de permission limite les droits de l'utilisateur, *même si ceux-ci sont plus ouverts avec les permissions NTFS*. Notez également que, par défaut, le groupe *administrateur* hérite du droit contrôle total et que le groupe *tout le monde* hérite du droit de lecture. Le droit de contrôle total ne devrait être donné qu'aux utilisateurs dont le rôle est d'administrer les droits NTFS, généralement celui des administrateurs systèmes. Le droit de modification devrait être donnée aux utilisateurs ayant pour objectifs d'alimenter le partage avec du contenu.

2.Permission NTFS

Les permissions NTFS définissent les droits de l'utilisateur sur l'objet lui-même, que celui-ci soit accédé par le réseau ou localement. On peut le définir sur l'objet (droit *explicite*) ou bien *par héritage* de l'objet parent (qui peut lui-même l'avoir hérité) et lui attribuer une *autorisation* ou une *interdiction*, l'interdiction prévalant toujours sur l'autorisation et le droit explicite prévalant toujours sur le droit hérité.
Par défaut, il existe six groupes de permission NTFS prédéfini. Ces groupes de permissions correspondent en réalité au groupement de droits spéciaux ; on les utilise pour les droits « classiques », mais il est tout à fait possible d'assigner directement les droits spéciaux sur un objet :

41, rue André Ampère
ZAC de l'Aufresne
44150 ANCENIS
Tél. : 02 40 09 72 72
Fax : 02 40 83 43 74

Droits	Contrôle total	Modifier	Lire et exécuter	Lister le contenu du dossier	Lecture	Écriture
Traverser le dossier Exécuter le fichier	☑	☑	☑	☑		
Lister les dossiers Lire les données	☑	☑	☑	☑	☑	
Attributs de lecture	☑	☑	☑	☑	☑	
Attributs de lecture étendus	☑	☑	☑	☑	☑	
Créer des fichiers Écrire des données	☑	☑				☑
Créer des dossiers Ajouter des données	☑	☑				☑
Attributs d'écriture	☑	☑				☑
Attributs d'écriture étendus	☑	☑				☑
Supprimer des sous-dossiers Supprimer des fichiers	☑					
Supprimer	☑	☑				
Lire les autorisations	☑	☑	☑	☑	☑	☑
Modifier les autorisations	☑					
Devenir propriétaire de l'objet	☑					
Synchroniser	☑	☑	☑	☑	☑	☑

Attention, bien que le droit « Lister le contenu du dossier » semble identique à « Lire et exécuter », celui-ci ne s'applique qu'au dossier là où son pendant s'applique aux deux. Vous pouvez ainsi donner un droit « lecture » tout en permettant aux utilisateurs de continuer à accéder aux sous-dossiers.

3.Bonnes pratiques

Lorsque les permissions se combinent, le droit de partage bornera le droit NTFS. Un utilisateur qui accède à un fichier sur lequel il possède le droit « contrôle total » mais dont le droit de partage ne lui accorde que le droit « lecture » ne pourra rien faire de plus que lire le fichier.

Le droit de partage est un limiteur d'accès : en aucun cas ce droit ne viendra se substituer à un droit NTFS. Vous pouvez avoir un droit de partage « contrôle total », si le fichier que vous accédez est en lecture seul au niveau des permissions NTFS il ne vous sera pas possible de le modifier ou de le supprimer. Ci-après un résumé des bonnes pratiques à adopter lorsque vous gérez un serveur de fichiers.

- ✓ **Assigner les permissions à des groupes**

41, rue André Ampère
ZAC de l'Aufresne
44150 ANCENIS
Tél. : 02 40 09 72 72
Fax : 02 40 83 43 74

De cette manière, les droits sont définis une fois pour toute et il n'est plus nécessaire de les modifier sur la ressource. L'administration est faite en ajoutant ou supprimant les utilisateurs du groupe. Pour interdire complétement l'accès de manière temporaire, configurer la permission « contrôle total » sur « refuser ».

- ✓ **Assigner le minimum de droit requis**

Cette stratégie vous évitera des accès non souhaité. Par exemple, si un utilisateur n'a pas besoin de modifier les fichiers, limitez son accès à la lecture.

- ✓ **NTFS et Partage**

Pour limiter les droits, privilégiez les permissions NTFS lorsque l'utilisateur à un accès local à la ressource (connexion sur le serveur par exemple). Limiter les droits avec les permissions de partage n'est efficace que pour une connexion réseau.

- ✓ **Organiser les ressources**

Créer une arborescence permettant de regrouper les privilèges à attribuer. Si trois dossiers à partager ont un accès commun en lecture seule, par exemple, il est plus pertinent de ne créer qu'un dossier partagé commun à la racine sur lequel on donne le droit de lecture. Ce type de partage permet ensuite de limiter les accès en utilisant les permissions NTFS.

- ✓ **Groupe « Tout le monde »**

Ne jamais définir une permission NTFS sur « refuser » pour le groupe « Tout le monde » : ce groupe contient les comptes ayant accès à la ressource et un droit refusé préemptant une approbation, cela provoquerait automatiquement un accès refusé à tous les utilisateurs.

- ✓ **Éviter de refuser explicitement un accès à une ressource**

Il vaut mieux gérer directement l'accès à la ressource en retirant le droit de l'utilisateur, plutôt que le lui interdisant explicitement. Par défaut, une absence de droit est une interdiction.

- ✓ **Administration**

Le groupe « Administrateurs » devrait toujours avoir le contrôle total sur la ressource. Le groupe local du serveur de fichier est suffisant.

- ✓ **Privilégier les noms courts**

En utilisant des noms courts, vous simplifiez le partage de l'information avec des ressources hétérogène et permettez aux utilisateurs d'identifier rapidement les ressources.

4. Utiliser les groupes de sécurité Active Directory

Les groupes de sécurité Active directory ont pour objectif de simplifier les tâches d'administration quotidienne et d'assurer un haut niveau de sécurité sur les accès. Ils sont particulièrement adaptés

41, rue André Ampère
ZAC de l'Aufresne
44150 ANCENIS
Tél. : 02 40 09 72 72
Fax : 02 40 83 43 74

aux partages de fichiers. Chaque groupe peut être défini avec un scope différent : cela définit la portée du groupe au sein d'une forêt ou d'une arborescence de domaines. En fonction de son scope, le groupe peut accepter différents types d'objets comme membre :

Scope	Membres…	Permissions sur…	Conversion vers…
Universel	• Compte de n'importe quel domaine appartenant à la même forêt. • Groupe Global de n'importe quel domaine appartenant à la même forêt. • Groupe universel de n'importe quel domaine appartenant à la même forêt.	N'importe quel domaine ou forêt.	Groupe Local Groupe Global (à condition qu'aucun groupe universel n'en soit membre)
Global	• Compte du même domaine • Groupe global du même domaine	N'importe quel domaine	Groupe universel (à condition qu'aucun autre groupe global n'en soit membre)
Local	• Compte de n'importe quel domaine ou forêt • Groupe Global de n'importe quel domaine ou forêt • Groupe Universel de n'importe quel domaine ou forêt • Groupe Local du même domaine	Uniquement le domaine d'appartenance.	Groupe Universel (à condition qu'aucun autre groupe local n'en soit membre)

- ✓ **Utilisation d'un groupe local :**

Ce groupe est à utiliser pour les accès aux ressources d'un domaine. Il devrait avoir pour membre des groupes globaux contenant les utilisateurs.

- ✓ **Utilisation d'un groupe global :**

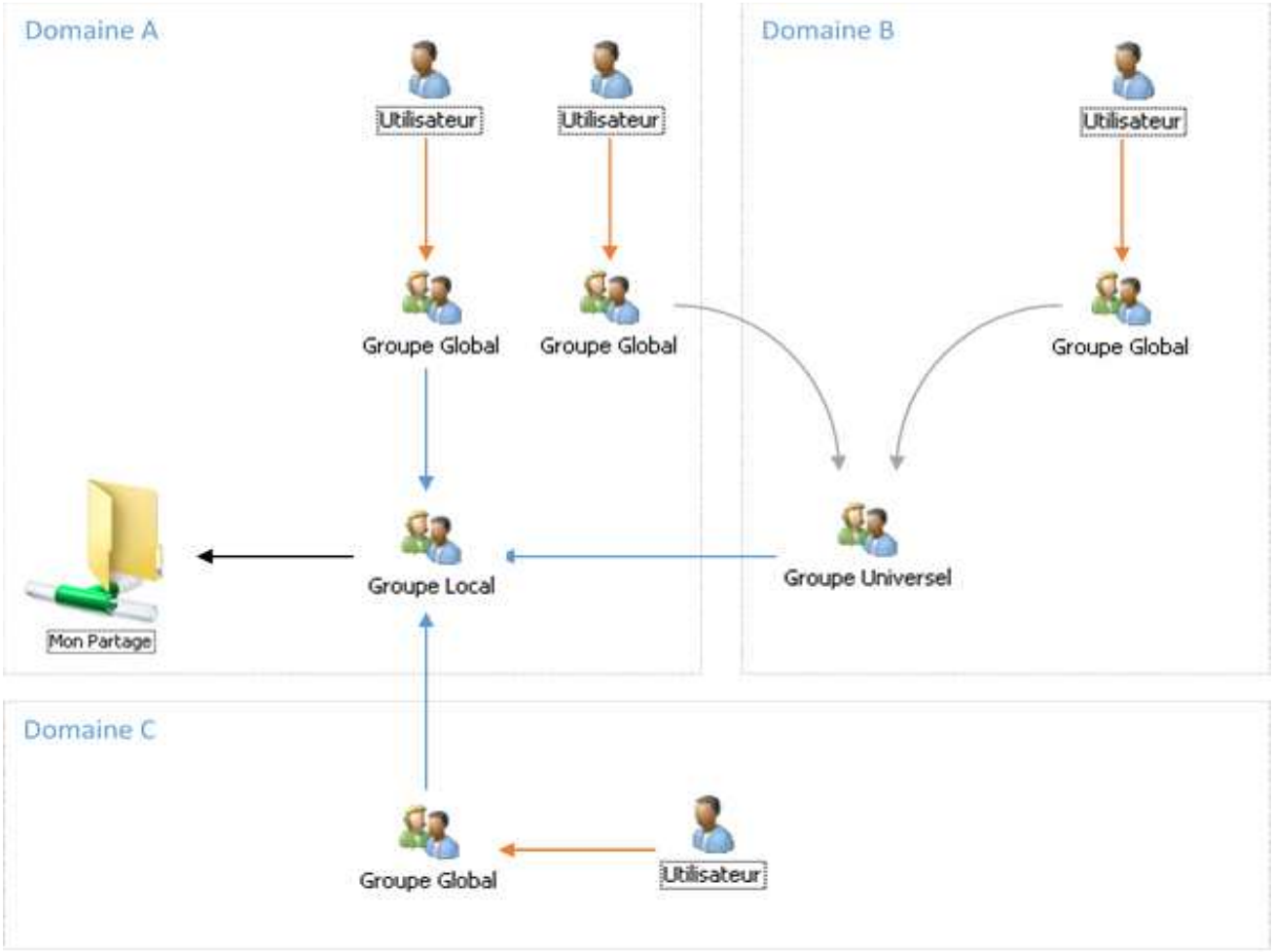
Ce groupe est à utiliser pour gérer les objets réclamant une maintenance quotidienne comme les comptes utilisateurs et ordinateurs. Ce type de groupe n'est pas répliqué en dehors de son propre domaine : les modifications à répétition qui seront faites ne provoqueront pas de réplications vers les catalogues Globaux (optimisation réseau).

- ✓ **Utilisation d'un groupe universel :**

Ce groupe est à utiliser pour regroupe des groupes ayants une portée multi-domaine : ce groupe ne sera répliqué vers les catalogues globaux que lorsque une modification sera réalisée dans sa

41, rue André Ampère
ZAC de l'Aufresne
44150 ANCENIS
Tél. : 02 40 09 72 72
Fax : 02 40 83 43 74

liste de membre. La modification des membres d'un groupe global lui appartenant n'affecte pas le groupe universel (optimisation réseau).



En respectant l'utilisation et la portée des différents types de groupes, vous éviterez de multiplier le nombre total d'objets de votre annuaire, simplifiant ainsi vos tâches d'administration.

5. Mots de passe

Il est primordial de créer des mots de passe avec une syntaxe forte (majuscules, chiffres etc …) pour éviter les piratages de compte soit par des mots de passe identique au nom d'utilisateur, soit par une attaque de type dictionnaire. Il peut s'y adjoindre une politique de changement de mot de passe à intervalles régulières pour renforcer la sécurité. Cette politique est à valider en fonction du niveau de sécurité nécessaire.