

Gestion des utilisateurs sous Windows 2003 Serveur

Comptes locaux

Comptes Active Directory

SID et ACL

Les groupes

**Groupes de sécurité
Création et gestion des groupes**

Stratégie de groupe

**Généralités Ordre d'application
Filtrage de l'étendue des GPOs**

Comptes locaux :

Utilisation de l'outil « Gestion de l'ordinateur » : compmgmt.msc.

Données : SAM locale : \windows\system32\config\SAM

Stratégie de sécurité locale : SECEDIT

Comptes Active Directory :

Utilisation de l'outil : DSA.msc

Données : NTDS.DIT : \windows\NTDS

Paramétrage des comptes :

Horaire d'accès, ouverture de session restreinte aux machines clientes autorisées (si NetBIOS est activé sur le domaine), date d'expiration, répertoire personnel, (dossier de base : [\\servername%\%USERNAME%](#)), profil...)

Type de profil :

Profil local : spécifique à un utilisateur, local à la station de travail et stocké sur celle-ci.

Profil itinérant : créé par un administrateur, stocké sur un serveur et dupliqué sur le poste local après ouverture de session. Il « suit » l'utilisateur quelle que soit la station où il se connecte. (Créer sur le serveur (servername) un dossier partagé « profils ».

Dans l'onglet « profil » des propriétés de l'utilisateur, entrer : chemin du profil : [\\servername\profils\%username%](#)

Profil obligatoire : profil itinérant qui ne peut être modifié que par un administrateur. (Il faut renommer Ntuser.dat en Ntuser.man)

SID :

Les identificateurs de sécurité sont des valeurs numériques qui identifient un utilisateur ou un groupe.

Exemple : S1-5-21-D1-D2-D3-RID

Où RID (Relative Identifier) correspond à la partie spécifique à chaque ID. Tandis que les autres parties sont identiques sur un domaine.

Les ACL (Liste Contrôle d'accès) protègent les objets Active Directory : elles définissent qui peut faire quoi sur l'objet. Une ACL se compose d'entrées ACE (Access Control Entry). Chaque ACE contient un SID spécifiant l'utilisateur et précise le type d'accès accordé ou refusé.

Les groupes :

Groupes de sécurité :

Cf NT4.

Possèdent un SID.

Groupes locaux :

Ils sont créés sur des stations ou des serveurs autonomes.

Ils peuvent contenir n'importe lequel des trois autres groupes

Groupes locaux de domaine :

Ils ne peuvent être créés que sur un Contrôleur de Domaine.

Ils ne sont pas repris dans le catalogue global. Ils contiennent des membres qui proviennent de n'importe quel domaine mais n'ont des permissions que par rapport à des ressources de leur domaine.

Ils sont créés soit lorsqu'un serveur autonome devient Contrôleur de Domaine soit créés par après.

Il peut contenir :

- Groupes universels.
- Autres groupes locaux de domaine appartenant au même domaine.
- Groupes globaux de tous les domaines.
- Utilisateurs.

Groupes Globaux :

Ils ne peuvent être créés que sur un Contrôleur de Domaine.

Les permissions que peuvent avoir ce type de groupe sont relatives à des ressources situées dans tous les domaines. Attention, ce groupe ne peut contenir que des membres du même domaine que lui.

Il peut contenir :

- Autres groupes globaux du même domaine.
- Utilisateurs du même domaine.

Il peut être membre de :

- Groupe universel.
- Groupe local de n'importe quel domaine.
- Autres groupes globaux dans le même domaine.

Groupes Universels :

Ils ne peuvent être créés que sur un Contrôleur de Domaine. Ils sont repris dans le catalogue global en totalité et donc ils peuvent affecter les performances du réseau. Ils agissent au niveau de la forêt : ils peuvent contenir des membres de tous les domaines et se voir doter de permissions sur les ressources de tous les domaines

Ils peuvent contenir :

- Groupes globaux.

- Utilisateurs.
- Autres groupes Universels.

Ils peuvent être membre de :

- Groupe universel.
- Groupe local de n'importe quel domaine.

Création et gestion des groupes :

Via l'outil d'administration Utilisateurs et Ordinateurs Active Directory.

Stratégie de groupe :

Voir : Microsoft Knowledge Base Article - 816297

Les paramètres Stratégie de groupe définissent les différents composants relatifs à l'environnement de travail de l'utilisateur et qu'un administrateur système doit gérer, comme les programmes disponibles aux utilisateurs, les programmes apparaissant sur le Bureau de l'utilisateur et les options du menu **Démarrer**.
(ou encore : Attribuer des scripts, Rediriger des dossiers, Gérer des applications, Spécifier des options de sécurité).

C'est une amélioration par rapport aux stratégies système de NT4 qui consistaient en un fichier NTCONFIG.POL qui était placé dans le répertoire NETLOGON sur les PDC et BDCs. Les stratégies de groupes sont, elles, gérées par l'AD et en partie placées dans SYSVOL (le successeur de NETLOGON).

(Tatouage : sous Windows NT4, lorsqu'une stratégie de groupe était définie, elle persistait jusqu'à ce qu'elle soit supprimée. Les stratégies de groupes sont, elles, activées ou non).

Ils peuvent agir soit sur les utilisateurs soit sur les ordinateurs

.

Attention, malgré leur nom, les stratégies de groupe ne concernent pas les groupes mais bien des sites, des domaines ou des Ous (cette action est appelée « liaison »).

Les stratégies de groupes des utilisateurs sont appliquées lors de leur ouverture de session et les stratégies de groupe des ordinateurs sont appliquées au démarrage de la machine. Mais les postes clients consultent régulièrement l'Active Directory pour vérifier si il y a des changements dans les stratégies de groupes.

Les stratégies de groupe locales (c'est-à-dire, hors AD) sont gérées à partir de l'outil SECEDIT.exe

Stratégie de groupe au niveau de l'AD :

Les paramètres de la stratégie de groupe sont stockées dans un objet stratégie de groupe (GPO). Ces objets (GPO) stockent leurs informations dans deux endroits :

GPT : une structure de dossier nommée **Modèle de stratégie de groupe**, dans le dossier SYSVOL de tous les contrôleurs de domaine. Le nom du dossier qui contient le GPT est le GUID (Globally Unique Identifier) de l'objet stratégie de groupe. Il contient des informations

sur la stratégie logicielle, le déploiement d'applications, les scripts et les paramètres de sécurité.

GPC : un **conteneur de stratégie** de groupe de Active Directory. Il contient des sous-conteneurs pour les informations de version, d'état.

Ils sont gérés par L'Editeur d'objets de stratégie de groupe (GPEDIT.MSC) ou par la console « Utilisateurs et ordinateurs Active Directory » ou par la console « Sites et Service Active Directory ».

Ordre d'application :

Les stratégies sont appliquées dans l'ordre ci-dessous :

1. L'objet Stratégie de groupe local unique.
2. Objets Stratégie de groupe du site, dans un ordre spécifié par l'administration.
3. Objets Stratégie de groupe du domaine, dans un ordre spécifié par l'administration.
4. Objets Stratégie de groupe de l'unité d'organisation, de la plus grande à la plus petite (de l'unité parent vers l'unité enfant), dans un ordre spécifié par l'administration au niveau de chaque unité d'organisation.

Les paramètres de stratégie de groupe sont cumulatifs et hérités des conteneurs parents.

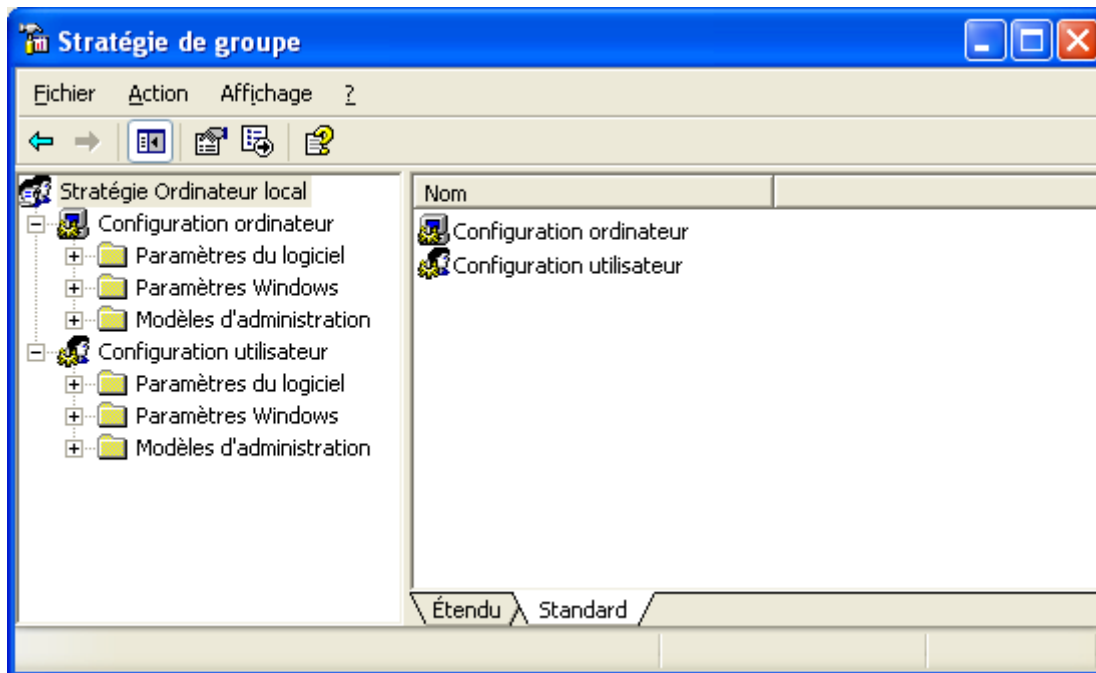
Par défaut, les stratégies des enfants ont priorité sur les stratégies des parents en cas d'incohérence. Si les paramètres sont cohérents, les deux stratégies, la plus ancienne et la plus récente, collaborent à la stratégie effective.

Des stratégies peuvent être bloquées au niveau du site, du domaine ou de l'unité d'organisation pour ne pas hériter d'un niveau supérieur. Inversement on peut imposer une stratégie aux enfants avec l'option « Ne pas passer outre ».

Filtrage de l'étendue des GPOs :

Un objet stratégie de groupe s'applique à tous les utilisateurs et les ordinateurs du conteneur avec lequel il est associé. L'utilisation de groupe de sécurité, avec les permissions « Lire » et « appliquer la stratégie » permet de filtrer.

Exemples :



1. Attribuer des scripts :

Configuration Ordinateur / Configuration Utilisateur : Paramètres Windows : Scripts.
(Vérifiez la différence entre les deux.)

« Ajouter » un script

Le recopier dans un des quatre dossiers de SYSVOL suivant :

SYSVOL\Sysvol\mondomaine\Policies\{GUID}\User\Scripts\Logon

SYSVOL\Sysvol\mondomaine\Policies\{GUID}\User\Scripts\Logoff

SYSVOL\Sysvol\mondomaine\Policies\{GUID}\Machine\Scripts\Startup

SYSVOL\Sysvol\mondomaine\Policies\{GUID}\Machine\Scripts\Shutdown

Le GUID est pour l'objet stratégie de groupe.