Active Directory

- Gère un domaine windows
- Service d'annuaire
- Base d'annuaire distribuée des ressources réseau : comptes utilisateurs, groupes, ordinateurs, imprimantes, dossiers partagés, ...
- Administration centralisée
- Tolérance de panne
- Protocoles standard => interopérabilité (clients)
- Produit propriétaire => pas de serveur AD non microsoft

Un annuaire permet de localiser, rechercher, gérer des ressources représentées par des objets de l'annuaire. Il offre des mécanismes de sécurité pour protéger ses informations.
Active Directory est un annuaire permettant de gérer des ressources liées à la gestions du réseau (domaines, comptes utilisateurs, stratégies de sécurité, ...).
La base de données d'AD est distribuée ce qui lui améliore la tolérance de pannes. Son mode de fonctionnement multi-maître permet de conserver une gestions centralisée.
AD respecte le standard LDAP V3. Il est donc capable d'interagir avec des clients et des serveurs LDAP d'autres origines.
Les protocoles d'échange entre serveurs AD sont propriétaires et non publics. Un contrôleur de domaine ne pourra donc pas être une machine avec un annuaire d'un fournisseur tier.
Certaines produits microsoft sont intallées par défaut (ou fortement conseillés lors de l'installation): DNS, serveur WeB. D'autres bénéficient d'une forte intégration avec AD (serveur de courrier Exchange).
Quelques soient les qualités des produits concurrents (Serveur WeB Apache, annuaire open-ldap ou novell, serveur dns bind, ...) leur mise en place sera forcément moins naturelle que celles des produits microsoft.
Tout en étant un excellent produit, AD est l'un des maillons de la conquête du marché des serveurs par microsoft.
Le support par AD d'un certain nombre de procoles standard a pour but de fédérer l'ensemble des ressources réseau autour de serveurs microsoft.

Structure logique

- Forêts
- Arborescences
- Domaines
- Unités d'organisation

Il est important de planifier la structure avant de l'implanter. La structure logique: décomposition de l'entreprise en domaines, arborescences, unités d'organisation. Cette décomposition pourra être guidée par la structure de l'entreprise et, surtout, par les besoins d'administrations :

- Limites de sécurité (qui est responsable de quoi) : domaines
- Possibilité de délégation d'administration : unités d'organisation
- Autorisation d'accès aux ressources
- Contraintes ou configurations des comptes et des sessions des utilisateurs
- ...

Nous allons détailler les outils qui sont à la dispositions de l'architecte du réseau pour créer sa structure logique. Plus tard, nous parlerons de éléments qui l'inciteront à adopter une structure plutôt qu'une autre: délégation de tout ou partie de l'administration de tout ou partie d'un ensemble d'utilisateurs et, dans un autre chapitre, les stratégies de groupes (imposer des configurations aux utilisateurs et aux ordinateurs).

Domaine

- Limite de sécurité
- Unité d'administration
- Unité de réplication
- Mode d'un domaine: mixte ou natif (dépend de l'OS des contrôleurs de domaine)

Limite de sécurité: chaque domaine dispose de ses propres stratégies de sécurité.

Unité d'administration: L'administrateur du domaine gère l'ensemble de la sécurité sur son domaine. Il est le seul à pouvoir accorder des permissions sur les objets de son domaine. Sauf autorisation accordée explicitement, il ne gère rien en dehors de son domaine.

Unité de réplication: les données actives directory sont répliquées sur tous les contrôleurs de domaine toutes les 5 mn.

Mode d'un domaine: **mode mixte**: s'il reste des contrôleur de domaine NT4. Certaines fonctionnalités ne sont pas disponibles.
Mode natif: si tous les contrôleurs de domaine sont en W2K. L'OS des ordinateurs non contrôleur du domaine n'influe pas sur le mode.
Il est possible de passer du mode mixte au mode natif mais pas l'inverse.

Unités d'organisations

- Organisation logique à l'intérieur d'un domaine
- Contient des objet active directory
- Permet
  - De déléguer des pouvoirs
  - De simplifier la sécurité
  - D'appliquer une stratégie à des ordinateurs ou utilisateurs
- Rend obsolète la construction usuelle domaine de compte/domaine de ressources NT4

Une **unité d'organisation** (UO) est un « container » pouvant contenir des utilisateurs, des ordinateurs, des groupes, ... et d'autres unités d'organisation.
Une unité d'organisation doit être utilisée quand on souhaite déléguer des pouvoirs ou appliquer une stratégie particulière à un sous-ensembles des objets du domaine.
Il est possible de donner tout ou partie des droits d'administration sur les objets d'une UO à certains utilisateurs.
En créant une unité d'organisation regroupant les ordinateurs du domaine, on peut déléguer leur gestion à un utilisateur qui n'aura pas de droit sur les comptes utilisateurs. On évite de mettre en place deux domaines ressources/comptes comme sous NT4.
Sans UO, les utilisateurs sont dans le container *Users* (qui n'est pas une UO) et les ordinateurs dans un container *Computers* qui n'est pas une UO.

Les objets Active Directory

- Instances d'une classe définie dans le Schéma :
  - Comptes utilisateurs,
  - ordinateurs,
  - imprimantes,
  - groupes,
  - dossiers partagés publiés
- Objets conteneur, objet feuille

Les objets Active Directory sont des instances des classes définies dans le Schema Active Directory. Ces objets sont un ensemble d'attributs obligatoires (doivent être renseignés pour que la création de l'objet aie lieu) ou facultatifs. Ainsi un utilisateur aura les attributs suivants nom, prénom, nom d'ouverture de session, numéro de téléphone, description, page WeB, ... Le nom est un attribut obligatoire. La description, le numéro de téléphone, sont des attributs facultatifs.
Un objet est appelé un **conteneur** s'il peut contenir d'autres objets (et d'autres conteneur). Les autres objets sont appelés des **objets feuille.**

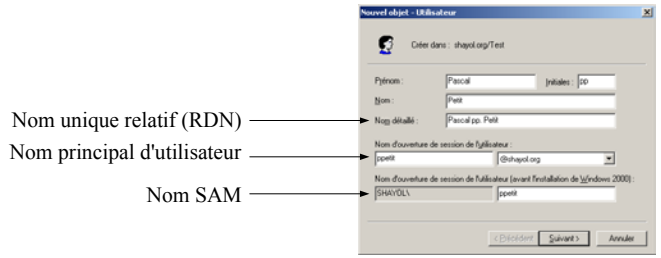
Nom des objets

CN= « Pascal PP Petit », OU=test, DC=shayol, DC=org

- Nom unique
- Nom unique relatif
- Identificateur global (GUID)
- Format des noms active directory
- Nom principal d'utilisateur
- Identifiant de sécurité :SID = RID + ID domaine

LDAP accepte plusieurs conventions de dénominations (cf RFC 2253: « Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names » et RFC 2247 : « Using Domains in LDAP/X.500 Distinguished Names »).
Le **nom unique relatif** (ou **RDN** Relatif Distinguished Name) est le nom identifiant l'objet dans le conteneur auquel il appartient. Le nom unique relatif est un attribut de l'objet. Deux objets appartenant au même conteneur ne peuvent avoir le même nom unique relatif. Deux objets situés dans des conteneurs différents peuvent avoir le même nom unique relatif. Notre utilisateur a « Pascal PP Petit » comme RDN. La taille maximale d'un RDN est de 255 caractères. A cette limite s'ajoute les contraintes sur le attributs définies dans le Schéma Active Directory. Ainsi, la taille d'un CN doit être inférieure à 64 caractères.
Le **nom unique** (ou **DN**, Distinguished Name) est constitué du nom unique relatif et du chemin d'accès complet à l'objet, nom de domaine inclus. Dans notre cas, c'est CN=Pascal PP Petit, OU=test, DC=Shayol, DC=Org. CN signifiant « Common Name », OU Organisation Unit et DC Domain composant. L'utilisateur « Pascal PP Petit » fait partie de l'unité d'organisation test du domaine shayol.org. La contrainte d'unicité sur le RDN fait que deux objets différents ne peuvent avoir le même nom unique.
Active Directory supporte plusieurs formats de noms d'objet : les noms uniques LDAP que nous venons de voir, les **URL LDAP** de l a forme :
LDAP://nom.du.Serveur/cn= "Pascal PP Petit",ou=test,dc=shayol,dc=org,
les **noms canoniques Active Directory** :
shayol.org/test/Pascal PP Petit

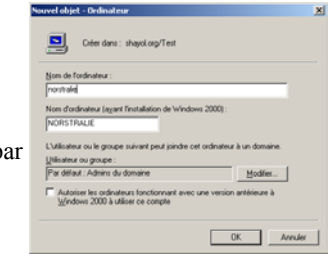
Nom des objets (2)



Active Directory identifie les objets par leur **Identifiant Global Unique (GUID** codé sur 128 bits**)**. Cet identifiant ne changera pas si l'objet est renommé ou déplacé. Si l'on a besoin de stocker une référence à l'objet dans une base de donnée, il faut utiliser le GUID car il ne changera pas.
Les noms de connexion : l'accès à un domaine ou à ses ressources se fait en fournissant un nom de connexion. Les principaux de sécurité d'utilisateurs ont deux nom de connexion possibles :
Nom principal d'utilisateur (ou UPN) : nom plus court que le nom unique. Il est de la forme nom@suffixe (petit@shayol.org dans notre cas).Le suffixe par défaut est le nom du domaine auquel appartient l'utilisateur. L'administrateur peut créer des suffixes nouveaux. Ainsi, il peut créer le suffixe société.com pour permettre à ses utilisateurs d'utiliser nom@societe.com plutôt que nom@sous-domaine.domaine.societe.com.
Nom de compte SAM: nom compatible NT4 de la forme **DOMAINE\utilisateur**. Dans notre cas, il s'agit de SHAYOL\petit. Ce nom est aussi appelé nom plat car il n'y a pas de hiérarchie de noms (pas d'UO, ...). Le nom doit être unique dans le domaine.
Tout principal de sécurité (donc tout utilisateur) ou tout groupe a un **identifiant de sécurité** (**SID** codé sur 128 bits). Cet identifiant fait partie du jeton d'accès de l'utilisateur (créé à l'ouverture de session). Il identifie l'utilisateur dans les ACL. Le SID est composé d'un partie locale (**RID**: **identifiant relatif**) et d'une partie identifiant le domaine de l'objet. Si l'objet est déplacé, le SID peut changer. Le SID est unique dans la forêt et un SID utilisé ne sera jamais réutilisé.

Compte d'ordinateur

- Nécessaire pour ordinateur WinNT ou W2K
- Création depuis l'ordinateur lors de l'inclusion dans le domaine
- Création à l'avance
  - Création du compte dans AD à l'avance
  - Inclusion de l'ordinateur par un utilisateur déclaré à la création du compte



Tout ordinateur windows 2000 ou NT membre d'un domaine a un compte d'ordinateur dans le domaine. Ce compte peut être crée lors de l'inclusion de l'ordinateur dans le domaine. Cette inclusion doit être réalisée depuis l'ordinateur à joindre sous un compte administrateur local en fournissant en plus lors de la procédure d'inclusion le nom et le mot de passe d'un utilisateur ayant le droit d'ajouter des ordinateurs dans le domaine.
Il est aussi possible de procéder en deux étapes :

- Création du compte sur le contrôleur de domaine par un utilisateur ayant ce droit. Lors de cette création (cf fenêtre ci-dessus), on peut déclarer le nom d'un utilisateur chargé de procéder à l'inclusion depuis l'ordinateur à inclure. Cet utilisateur n'a pas besoin d'avoir de droits particuliers. L'autorisation ne vaut que pour cet ordinateur.
- Depuis l'ordinateur à inclure: inclusion dans le domaine. On peut fournir le nom et le mot de passe de l'utilisateur déclaré lors de la création du compte.

Cette procédure peut être utilisée pour permettre à l'utilisateur d'un ordinateur de joindre sa machine lui-même au domaine.
Lors de l'inclusion dans le domaine, le groupe des administrateurs du domaine est ajouté au groupe des administrateurs locaux de l'ordinateur, le groupe des utilisateurs du domaine est ajouté au groupe des utilisateurs de l'ordinateur (ce qui leur permettra d'ouvrir une session).
Un champ permettant de sélectionner l'entité (domaine ou ordinateur local) qui va valider le mot de passe est ajouté à la mire d'ouverture de session

Compte utilisateur

- Compte d'utilisateur local :
  - Stocké dans la base SAM de l'ordinateur
  - Donne accès aux ressources locales
  - Permet l'ouverture de session sur l'ordinateur
- Compte d'utilisateur du domaine :
  - Stocké au niveau du domaine dans Active Directory
  - Donne accès aux ressources réseau
  - Permet d'ouvrir des sessions sur les ordinateurs du domaine

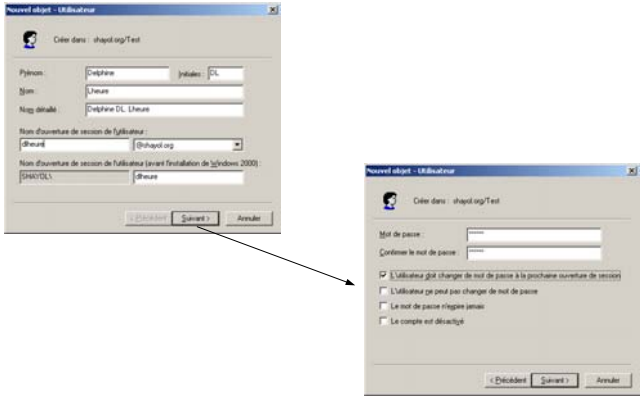
Un **compte d'utilisateur local** est un compte créé sur un ordinateur donné. Les informations du compte sont stockés dans la base de donnée de sécurité (base SAM) de l'ordinateur. Un tel compte permet d'ouvrir des sessions sur l'ordinateur et donne accès aux ressources locales à la machine. L'accès à des ressources réseau nécessite une nouvelle authentification (qui peut être transparente si login et mot de passe sont identiques). Les utilisateurs et groupes locaux se gèrent grâce à l'outil « utilisateurs et groupes locaux » accessibles notamment dans la mmc « gestion de l'ordinateur ».
Un **compte d'utilisateur du domaine** est créé sur un contrôleur de domaine et stocké dans Active Directory. Lorsqu'un utilisateur se connecte à un domaine, ses login et mot de passe sont envoyés à un contrôleur de domaine (et non pas par l'ordinateur local où il se connecte) pour validation. Si la validation réussit, l'utilisateur a accès à toutes les ressources du domaine auxquelles il est autorisé à accèder sans avoir besoin de s'authentifier à nouveau.
L'utilisation d'un domaine permet de centraliser la gestion des utilisateurs (cf « modèle domaine versus modèle groupe de travail » dans le chapitre sur l'installation de windows 2000).
Il n'y a pas de comptes d'utilisateurs locaux sur un ordinateur contrôleur de domaine. Les comptes existants sont importés dans Active Directory.
Les comptes d'utilisateurs de domaine se gère via la mmc « utilisateurs et ordinateurs active directory ».

Comptes prédéfinis dans un domaine

- Computers
- Users
- Comptes:
  - Administrateur
  - Invité
  - IUSR_NomOrdinateur et IWAM_NomOrdinateur

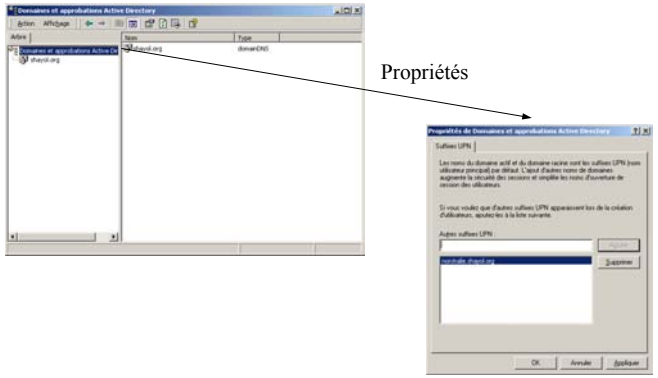
Par défaut, dans l'outil « Utilisateurs et ordinateurs Active Directory », les ordinateurs sont dans le conteneur **Computers** et les utilisateurs sont dans le conteneur **Users**. Cette situation initiale a vocation à évoluer. L'administration d'un domaine va conduire à créer des unités d'organisations qui auront vocations à accueillir ordinateurs ou utilisateurs ou les deux.
Le comptes **Administrateur** (différent du groupes des **Administrateurs**) est un compte ayant les droits les plus étendus sur l'ordinateur local. Il a pour vocation à gérer la configuration du système et notamment : la création des comptes utilisateurs, la sauvegarde, l'installation et la configuration des périphériques, des imprimantes, ...
Le compte administrateur ne peut pas être supprimé.
Dans un domaine, l'administrateur d'un contrôleur de domaine est administrateur du domaine. Il a des droits sur l'ensemble du domaine.
L'administrateur du premier contrôleur de domaine de la forêt est administrateur de l'entreprise. Il a des droits sur l'ensemble de la forêt.
Le compte invité est utilisé par les utilisateurs occasionnels. Ce compte est désactivé par défaut et n'a pas de mot de passe. L'activation de ce compte diminue la sécurité du système.
Les comptes IUSR_NomOrdinateur et IWAM_NomOrdinateur sont des comptes utilisés par IIS, le serveur WeB Microsoft.

Création des comptes sur un domaine



Sélectionn « users » ou l'unité d'organisation où doit être créé le compte utilisateur puis Action/Nouveau/utilisateur.
Les noms de l'utilisateurs ont été traités dans la section sur les noms des objets Active Directory.
Pour rappel :
le nom détaillé est le nom unique relatif (RDC). Le nom d'ouverture de session est le nom principal d'utilisateur. C'est kerberos qui est utilisé comme méthode d'authentification.
Le nom d'ouverture de session pré-windows 2000 est le nom plat d'ouverture de session de la forme *DOMAINE\NOM*. Il sera utilisé pour les connections avec la méthode d'authentification NTLM (windows NT). Il doit être inférieur à 20 caractères.
L'écran suivant traite du mot de passe de l'utilisateur :
•Mot de passe permet de fournir un mot de passe initial à l'utilisateur.
•L'utilisateur doit changer le mot de passer à la prochaine session impose l'utilisateur de changer son mot de passe lors de première ouverture de session.
•L'utilisateur ne peut pas changer son mot de passe: pour figer le mot de passe
•Le mot de passe n'expire jamais: pour éviter que le mot de passe doivent être changé au bout d'un certain temps.
•Le compte est désactivé: permet d'interdire l'utilisation d'un compte. On peut par la suite réactiver un compte désactivé.

Création d'un suffixe UPN



Il est possible de créer des suffixe de nom principal d'utilisateur. Cela peut être pratique pour simplifier le nom principal en remplaçant un nom de domaine complexe par un suffixe simple, en général de la forme societe.com.

Propriétés des comptes d'utilisateurs

- Options de mot de passe
- Délégation: interdire la délégation, autoriser la délégation des tâches à d'autres utilisateurs
- Chiffrement de mot de passe: réversible, pas de pré authentification kherberos, chiffrement DES
- Expiration de compte
- Restrictions horaires
- Restriction d'accès (se connecter à)

Profils utilisateurs, répertoire de base

- Profils locaux
- Profils itinérants
- Profils itinérant obligatoire
- Répertoire de base

Un **profil utilisateur** contient notamment l'ensemble des personnalisations de son environnement (couleurs, fond d'écran, menu démarrer, ...).
Par défaut, chaque utilisateur a un profil par ordinateur qui est stocké localement. S'il travaille sur un autre ordinateur, il utilise un nouveau profil qu'il lui faudra à nouveau personnaliser et il n'a pas accès aux fichiers sauvés sur le bureau.
Le profil est fichier nommé **ntuser.dat** situé dans un dossier portant le nom d'ouverture de session de l'utilisateur éventuellement suffixé par le nom du domaine. Ce dossier est situé sous le répertoire *« documents and settings »*.
profil itinérant: le profil est stocké sur un serveur et c'est le même profil qui sert sur tous les ordinateurs du domaine. Le profil et l'environnement sont chargés sur l'ordinateur local lors de l'ouverture de session (donc avoir sa collection de mp3 sur le bureau ralentit l'ouverture de la session le temps de la copie :-)).
On peut gérer les profiles utilisateurs grâce à l'onglet « profils des utilisateurs » de l'outil Système du panneau de configuration.
Profil itinérant obligatoire: on peut utiliser le même profil pour tous les utilisateurs en renommant le fichier ntuser.dat en ntuser.man (MANdatory) et en indiquant le même profil pour tous les utilisateurs.
Le **répertoire de base** d'un utilisateur est son dossier personnel. On peut spécifier un chemin réseau ce qui permettra à l'utilisateur d'y avoir accès depuis n'importe quel ordinateur. W2K remplace %username% par le nom d'ouverture de session de l'utilisateur. Les permissions sont automatiquement positionnées.

Création de masse

- Par copie d'un compte désactivé
- Via addusers, csvde, ldifde
- Net account
- Net users
- Net group
- Net localgroup

Une méthode classique pour créer facilement des comptes avec des propriétés complexes consiste à créer un compte type désactivé et à créer les autres comptes par copie de ce compte type. On créera un compte type par type d'utilisateur.
Lors d'une copie de compte, les informations suivantes sont conservées: les restrictions horaires, les 4 options liées au mot de passe, les restrictions d'accès, la date d'expiration, les options de profil et de dossier de base et l'appartenance aux groupes.
ADDUSERS est un exécutable du kit de ressources technique qui permet de lister dans un fichier, ajouter, modifier ou détruire des comptes utilisateurs à partir des données d'un fichier.
CSVDE est un outil qui per met d'importer un fichier CSV généré en général par un tableur ou par un script. CSVDE ne permet que de créer de nouvelle informations, pas de changer des informations existantes.
LDIFDE est un outil qui permet de créer, modifier ou supprimer des objets dans active directory à partir d'un fichier au format LDIF (LDAP Interchange Format)
net user ajoute, modifie ou liste des comptes utilisateurs (cf aide en ligne w2k)
net account permet d'obtenir et de modifier les paramètres d'ouverture de session et de mot de passe (cf aide en ligne de w2k)
net group, **net localgroup**: liste ou modifie des groupes globaux ou locaux (cf aide en ligne de w2k)

Gestion des comptes

- Réinitialiation du mot de passe
- Désactivation
- Suppression
- déverouillage
- déplacement

Groupes: présentation

- Un groupe est un ensemble d'utilisateurs
- Les membres d'un groupe bénéficient des droits attribués au groupe
- Un utilisateur peut être dans plusieurs groupes
- Les groupes peuvent contenir d'autres groupes
- Les groupes simplifient l'administration
- Jusqu'à 5000 membres
- Groupes de distribution et groupes de sécurité

Groupes de distribution: les groupes peuvent être utilisés par des applications pour traiter les utilisateurs par lot. Exemple: courrier électronique. Un groupe de distribution n'a rien à voir avec la sécurité W2K;
Groupes de sécurité: un groupe de sécurité peut être utilisé pour gérer les permissions et les droits. Un groupe de sécurité peut être utilisé comme groupe de distribution (l'inverse est faux).
Les groupes simplifient l'administration car on peut appliquer une fois au groupe des droits et permissions complexes dont ses membres bénéficieront. C'est plus simple et rapide que de l'appliquer individuellement à chaque membre. Si un nouvel utilisateur doit avoir ces droits, on l'ajoute au groupe.
Les groupes simplifient l'administration car ils permettent de la centraliser et de contrôler les droits et permissions directement au niveau du domaine (cf plus loin) par l'imbrication des groupes globaux dans les groupes locaux (cf « planification » plus loin).
Un groupe peut contenir jusqu'à 5000 membres qui peuvent eux-même être des groupes. Ainsi, si vous souhaitez avoir un groupe désignant tous les étudiants de l'université, il vous faudra créer des groupes intermédiaires (par filière par exemple) et inclure ces groupes dans le groupe global. Ce groupe contiendra moins de 5000 membres (ses membres seront les groupes de filières) mais il représentera tous les membres de ses groupes membres soit bien plus que 5000 étudiants.

Groupes: étendue de groupes

- Groupes locaux sur un ordinateur autonome
- Groupes locaux de domaine
- Groupes globaux
- Groupes universels
- Restriction dans un domaine en mode mixte

Groupes locaux (ordinateur non contrôleur de domaine) : groupe propre à l'ordinateur local permettant de donner des droits sur les ressources locales de la machine. Ils se gèrent avec la mmc « utilisateurs et groupes locaux » ou avec « gestion de l'ordinateur ». Exemple: le groupe administrateurs.
Groupes locaux de domaine:ce sont des groupes utilisables uniquement dans le domaine pour donner accès à des ressources du domaine.
Groupes globaux: les groupes globaux peuvent être utilisés dans tous les domaines de la forêt mais on ne peut les utiliser pour donner des permissions ou des droits. Pour cela, on inclut les groupes globaux dans des groupes locaux.
Groupes universels: ils peuvent être utilisés dans tous les domaines de la forêt et peuvent contenir des membres appartenant à tous les domaines de la forêt. C'est le seul type de groupe dont la liste des membres est stockée dans le serveur de catalogue global. **Tout ajout ou suppression de membre a donc un impact sur la réplication et sur le trafic réseau**. C'est la raison pour laquelle on conseille de ne mettre que d'autres groupes dans les groupes universels de façon à avoir des groupes universels dont la liste des membres ne change pas.
Dans un domaine en mode mixe:

- Il n'y a pas de groupes universels
- Les groupes locaux de domaine ne sont visibles que depuis les contrôleurs de domaine
- Pas de groupes emboîtés

Groupes locaux de domaine (LD)

- Peut contenir
  - des utilisateurs, des groupes globaux et des groupes universels de tous les domaines de la forêt;
  - des groupes de domaine locaux de son domaine
- Utilisable seulement dans son domaine;
- Peut être membre de DL de son domaine;
- On peut l'utiliser pour affecter droits et permissions
- Membres non copiés dans le catalogue global.

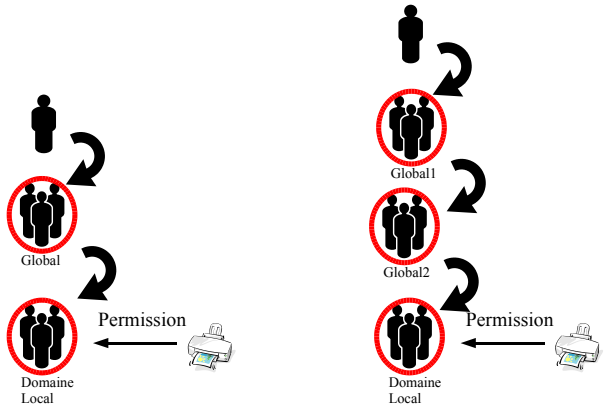
Groupes globaux

- Peut contenir des utilisateurs, des groupes globaux du **même** domaine;
- Peut être membre de groupes (DL, G, U) de tout domaine de la forêt
- On **ne** peut **pas** l'utiliser pour affecter droits et permissions
- Membres non copiés dans le catalogue global.

Groupes universels

- Peut contenir des utilisateurs, des groupes globaux et des groupes universels de **tous** les domaines de la forêt;
- Peut être membre de DL de tout domaine et de groupes universels
- On peut l'utiliser pour affecter droits et permissions
- Ses membres copiés dans le catalogue global.

Planification des groupes

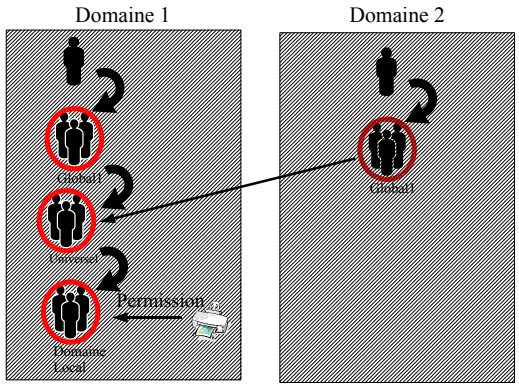


Si vous n'avez qu'un seul domaine, contrairement à NT, W2K vous permet de tout gérer avec des groupes locaux de domaine.
Microsoft conseille néanmoins d'utiliser une stratégie d'utilisation incluant des groupes globaux :

- On met les permissions/Droits sur les groupes locaux
- Les groupes locaux contiennent des groupes globaux
- Les utilisateurs sont dans les groupes globaux

Les groupes globaux sont gérés au niveau du domaine. Attribuer les permissions aux groupes locaux est ainsi la seule tâches à réaliser sur l'ordinateur hébergeant la ressource. Tout le reste se gère au niveau du domaine.
Si on a beaucoup d'utilisateurs, on peut utiliser l'imbrication des groupes globaux comme sur l'exemple 2.

Planification des groupes (2)



Les groupes universels sont utiles pour partager des ressources entre domaines d'une même forêt car un groupe universel peut contenir des groupes de tout domaine de la forêt.
On évitera d'inclure des utilisateur dans des groupes universels car la liste de leurs membres sont dans le catalogue global (répliqué sur tous les serveurs de catalogues globaux). Toute modification de la liste des membres d'un groupe universel entraîne donc une modification et une réplication du catalogue global.
Une bonne politique consiste à n'inclure que des groupes globaux dans les groupes universels.

Modèle de contrôle d'accès W2K

- Autorisations basées sur l'utilisateur
- Accès discrétionnaire aux objets sécurisables
- Héritage des permissions
- Privilèges administratifs
- Audit des événements du système.

Quelques notions qui seront développées par la suite :
Autorisations basées sur l'utilisateur: un programme a les droits de l'utilisateur qui l'exécute.
Accès discrétionnaire aux objets sécurisables:Le propriétaire d'un objet peut contrôler qui peut l'utiliser et avec quel genre d'accès. Windows 2000 permet de plus de gérer l'accès à des propriétés précises de l'objet ou à l'objet entier.
Héritage des permissions: Les permissions placées sur un conteneur (répertoire par exemple) sont héritées par les nouveaux objets (comme sous NT) mais aussi par les objets existants (nouveauté W2K).
Privilèges administratifs: Il est possible de gérer l'accès d'utilisateurs ou de groupe à certaines fonctions d'administration. Les stratégies de groupe W2K permettent une gestion centralisée des privilèges administratifs sur tous les ordinateurs du domaine.
Audit: il est possible de détecter les échecs ou les réussites de toute action ayant trait à la sécurité (de l'ouverture de session à l'utilisation de privilèges en passant par les accès aux fichiers ou répertoires)

Limiter les accès

- Principal de sécurité : utilisateur, groupe, ordinateur ou service :
  - Ont des comptes
  - Sont identifiés par Identifiant de sécurité (SID) créé lors de la création du compte
  - Jeton d'accès :
    - Créé lors de l'ouverture de session ou de la connexion d'un principal
    - Fournit un contexte de sécurité

Les autorisations W2K sont basées sur l'utilisateur : toute application démarre dans le **contexte de sécurité** de l'utilisateur et ne peut faire que ce que l'utilisateur a le droit de faire. Cette notion est valable pour les **principaux de sécurité** (utilisateurs, groupes, ordinateurs ou service) qui sont les entités qui doivent avoir des comptes.

Le **compte utilisateur** : Toute personne faisant partie d'un domaine doit avoir un compte utilisateur

Le compte contient les informations sur l'utilisateur, ses appartenances aux groupes et les informations concernant la politique de sécurité.

Un **SID** (**identifiant de sécurité**) est attribué automatiquement par W2K au nouveau compte lors de sa création ou lors de son déplacement.

Jeton d'accès : Il est créé à l'ouverture de session de l'utilisateur.

Il comprend un ID de sécurité pour l'utilisateur, un pour les groupes auxquels il appartient et des informations nom de l'utilisateur etc..

Chaque processus possédera une copie du jeton d'accès, de même W2K se référera aux ID de sécurité en cas de tentative d'accès à un objet.

Il sont comparés à la liste de permission de l'objet pour validation des droits d'accès à celui-ci.

Sujet

- Sujet : processus s'exécutant dans le contexte de sécurité d'un principal authentifié
- Prise d'identité: possibilité pour un processus de s'exécuter dans un contexte de sécurité différent de celui de son processus père. Utile pour les pour les applications client/serveur.

Le programme exécuté par un utilisateur ne doit pas avoir plus de droits d'accès aux objets que ceux que possède l'utilisateur.

SUJET :

Il est la combinaison du jeton d'accès de l'utilisateur et du programme exécuté.

Il est employé par W2K pour suivre et gérer les droits des programmes.

Le programme s'exécute donc dans le contexte de sécurité de l'utilisateur.

Le contexte de sécurité contrôle les droits d'accès aux objets que possède le sujet .

Emprunt d'identité: Un processus peut utiliser les attributs de sécurité d'un autre. Ainsi, un processus serveur emprunte l'identité d'un processus client pour compléter une tâche impliquant des objets auxquels il n'a normalement pas droit.

Objets

- Objets sécurisables, informations de sécurité (Permissions)
- Listes de contrôle d'accès (ACL)
  - DACl: liste de contrôle d'accès discrétionnaire: permissions
  - SACL: liste de contrôle d'accès Système (Audit)

Les informations de sécurité des objets

Un objet pouvant contenir d'autres objets est appelé un **conteneur**. Un dossier est un exemple de conteneur. Les objets contenus dans un conteneur sont appelés les **enfants** du conteneur tandis que le conteneur est le **parent** de ces objets.

Tous les objets nommés et certains anonymes peuvent être sécurisés.

Le **descripteur de sécurité** détaille les attributs de sécurité d'un objet.

Il comporte 4 parties :

ID de sécurité du propriétaire

Indique l'utilisateur ou le groupe processeur de l'objet.

Il peut changer les permissions d'accès à l'objet.

ID de sécurité du groupe

Employé uniquement par POSIX

Liste de contrôle discrétionnaire (DACL)

Identifie les droits d'accès des utilisateurs et des groupes, les ACL sont contrôlés par le propriétaire.

ACL système (SACL)

Contrôle les messages d'audits générés par le système, ils sont contrôlés par les administrateurs de sécurité.

Contrôle d'accès

- Principe de base :

Les sujets agissent sur les objets

- Comparaison du jeton d'accès du principal associé au sujet et du descripteur de sécurité de l'objet.

Un programme est un processus comportant des des threads d'exécution. Lors que l'utilisateur tente d'accéder à un objet, il le fait grâce à un thread d'un programme. Pour accèder à un objet, un thread doit s'identifier auprès du sous-système de sécurité. N'ayant pas d'identifiant de sécurité, le thread va devoir en emprunter un à un principal de sécurité : l'utilisateur qui a lancé le programme dans notre cas. Le thread a une copie du jeton d'accès de l'utilisateur qui l'exécute qui lui permettra de s'identifier comme appartenant à l'utilisateur qui l'a lancé.
Le jeton d'accès contient des informations permettant d'identifier l'utilisateur et tous les groupes auxquels il appartient.
Ce jeton va être comparé avec la DACL du descripteur de sécurité de l'objet. Si le sous-système de sécurité ne peut conclure lors de cette comparaison, il refuse l'accès à l'objet.

Héritage

- Conteneur, parents, enfants
- Héritage des permissions

Un objet pouvant contenir d'autres objets est appelé un **conteneur**. Un dossier est un exemple de conteneur. Les objets peuvent hériter des permissions de leur parent.

Quand on annule l'héritage, on se voit proposer deux choix pour les permissions héritées :

- supprimer les permissions correspondantes des ACL

- laisser les choses en l'état en recopiant les permissions correspondantes comme si elles avaient été définies localement .

Les second choix rend ce permissions indépendantes de celle du parent (ce qui peut être une bonne ou une mauvaise chose suivant le contexte) et permet de les modifier localement.

L'héritage est un mécanisme puissant qui permet de changer finement les permissions sur toute une arborescence en modifiant simplement celles de sommet de l'arborescence.

Droits

- Droit du propriétaire
- Propriétaire initial
- Changement de propriétaire
- Permissions
- Droits utilisateurs
  - Droits de procédure de connexion
  - Privilèges

Un **droit** est l'autorisation d'effectuer une opération. Le seul droit inhérent est celui qu'à le **propriétaire** d'un objet de contrôler l'accès à cet objet. Le propriétaire a donc ce droit même s'il n'apparaît pas dans la DACL.Les autres droits doivent être explicitement attribués. Le **propriétaire initial** d'un objet est son créateur. Un autre utilisateur peut **s'approprier un objet** si le propriétaire l'y a autorisé. Les administrateurs peuvent s'approprier un objet sans l'accord de son propriétaire.
On distingue deux types de droits :
• Les **permissions** : autorisation d'accès à un objet précis
•Les **droits utilisateurs**: autorisation d'effectuer une opération qui affecte tout l'ordinateur plutôt qu'un objet précis. On en distingue deux sortes:

- Les **droits de procédures de connexion** : contrôle de l'accès à un ordinateur
- Les **privilèges**.: contrôle de la manipulation des ressources système.

Les droits d'utilisateurs sont affectés à travers la stratégie de sécurité (locale, du contrôleur de domaine, du domaine, ...). Nous développerons cela quand nous parlerons de stratégies de groupes.
En cas de conflit entre permission et privilège, le privilège l'emporte (exemple: accès aux fichiers et opérateur de sauvegarde qui aura le droit d'accéder au fichiers pour réaliser des sauvegardes mais pas pour l'ouvrir dans d'autres programmes si l'accès lui est interdit).

Délégation de tâche

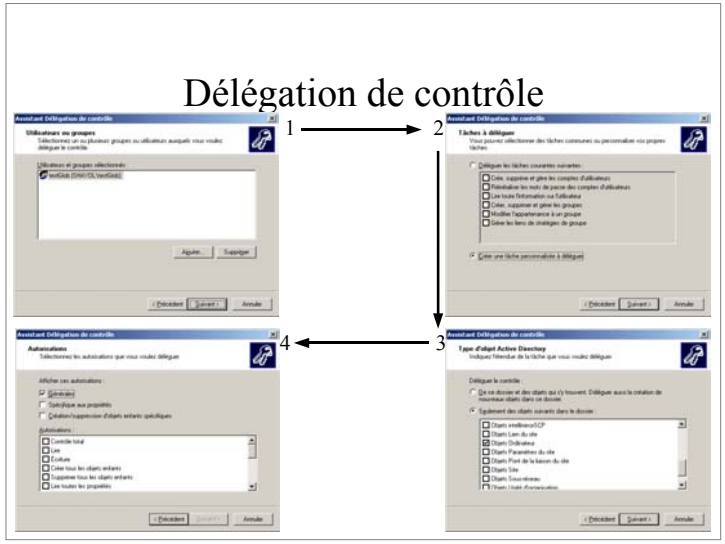
- Délégation de contrôle sur le domaine ou sur une unité d'organisation
- Création de console MMC personnalisées,
- Administration à distance

Déléguer le contrôle de tâches revient à accorder tout ou partie des droits sur des objets Active Directory à des utilisateurs ou à des groupes utilisateurs. La délégation porte sur les objets d'un certain type d'une unité d'organisation ou du domaine.
Les tâches à déléguer peuvent être choisies dans une liste de tâches courantes. Il est aussi possible de créer des tâches personnalisées en précisant finement les types d'objets concernés et pour ces types d'objet les autorisations accordées.
Les **console de gestion microsotf (ou MMC)** sont des outils de gestion modulaires et personnalisables. Les outils d'administrations que vous avez déjà eu l'occasion d'utiliser sont des consoles MMC. Vous pouvez ajouter ou retirer des composants à une console MMC (par exemple, ajouter « Utilisateurs et ordinateurs Active Directory » à la console « Gestion de l'ordinateur »), faire qu'une console démarre sur une unité d'organisation précise plutôt que sur le domaine, ...
Une console MMC peut gérer un ordinateur distant. Elle peut être installée facilement sur un poste windows 2000 pro. Pour cela, il faut installer adminpak.msi (cd rom windows 2000 server) sur le poste W2K pro.

Délégation de contrôle

La méthode la plus simple consiste à **déléguer des tâches prédéfinies**.
Pour cela :
•Sélectionner l'unité d'organisation concernée
•Puis Action/délégation de contrôle
•Choisir les utilisateurs ou groupes concernés. Il est évidemment conseillé de déléguer à un groupe dans lequel on insérera les utilisateurs concernés.
•Choisir les tâches courantes concernées (réinitialiser les mots de passe, créer les comptes utilisateurs, ...)
•Valider le récapitulatif.

Délégation de contrôle



Si l'on souhaite déléguer une tâche personnalisée, c'est plus délicat.
L'étape 2 (choix des tâches) est remplacée par :

•Spécification de l'étendue de la délégation en sélectionnant les types d'objets concernés par la délégation

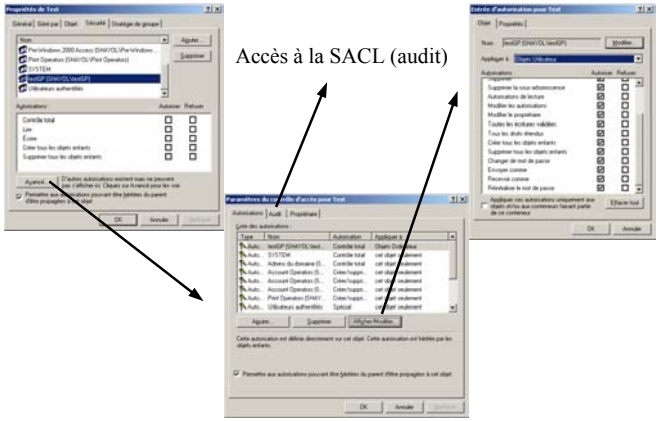
•Définir les autorisations que l'on accorde sur ces objets:

- Générales: autorisations courantes
- Spécifiques aux propriétés: autorisations que l'on peut affecter aux attributs de l'objet
- création/suppression d'objet enfants: pour afficher les autorisations permettant de créer et supprimer des objets enfants

•Sélectionner les autorisations dans la liste

•Valider le récapitulatif

Modification de délégation, Audit



La modification ou la suppression des taches déléguées est accessible via le bouton avancé de l'onglet sécurité des propriétés de l'unité d'organisation (ou du domaine).

L'onglet **audit** de la fenêtre obtenue permet de modifier les SACL de l'objet et donc de surveiller les actions des utilisateurs auxquels on a délégué le contrôle.

Création d'une console personnalisée

- L'administration W2K: des consoles MMC pré-créées;
- En standard, un jeu plus riche sur un contrôleur de domaine mais installable sur tout ordinateur W2K (adminpak)
- Administration à distance
- Possibilité de créer des consoles personnalisées

Windows 2000 propose des outils d'administration qui sont des **MMC** (**Microsoft Management console**). Un jeu de consoles standard est livré avec tout ordinateur windows 2000. Le jeu de console est plus riche sur un contrôleur de domaine que sur un ordinateur windows 2000 pro.
L'installation des consoles manquantes sur un ordinateur W2K pro ou server non contrôleur de domaine est possible.
Les consoles MMC permettent d'effectuer la majeure partie des tâches d'administration à distance.
Il est possible de modifier les consoles livrées. On peut ainsi ajouter le composant enfichable « utilisateur et ordinateurs Active Directory » à la MMC « gestion de l'ordinateur ».
On peut aussi créer des consoles personnalisées :

- Limitée à un seul outil;
- Limitée aux objets que leurs utilisateurs devront gérer;
- Restreintes à une seule fenêtre;
- Proposant une liste de tâches d'administration pour faciliter le travail de leur utilisateur.

C'est particulièrement pratique dans le cas d'une délégation de l'administration de certains objets.

Création d'une console personnalisée

- Utilisation de mmc.exe
- Ajout de composants enfichables, extensions
- Mode auteurs, mode utilisateur

L'outil mmc.exe permet de créer des consoles personnalisées et de modifier des consoles existantes.
Une console est constituée d'un ou plusieurs composants logiciels enfichables. Un composant logiciel enfichable peut être composé d'extensions. Certains composants peuvent être utilisés à la fois comme composants logiciels enfichable et comme des extensions.
Exemple: « gestion de l'ordinateur » est une console composée de nombreuses extensions (Observateur d'événements, utilisateurs et groupes locaux, ...).
Les consoles personnalisées peuvent être fournies à des utilisateurs ayant des droits d'administration limités. Il est possible de limiter les consoles ainsi livrées pour les rendre non modifiables. Pour cela, on définit le mode d'une console:

- **Mode auteur** (**mode par défaut**) : autorise la modification de la console (ajout/suppression de composants, création de fenêtres, ...)
- **Mode utilisateur accès total**: l 'utilisateur peut se déplacer parmi les objets gérés par la console, créer des nouvelles fenêtres, ... mais ne peut enregistrer ces modifications ni ajouter/supprimer des composants enfichables
- **Mode utilisateur accès limité, fenêtre multiples**: idem mais pas de déplacement possible
- **Mode utilisateur, accès limité, fenêtre unique**: idem mais une seul fenêtre.

Bibliographie

- Structure logique AD: reskit tome 6 chap. 1
- Maîtres d'opération, catalogue global : reskit tome 6, chapitre 1, chapitre 7
- Les RFC concernant LDAP : cf http://www.rfc-editor.org/ pour le texte des RFCs et l'annexe B du tome 6 du reskit pour la liste des RFCs concernées.

Bibliographie (2)

- Sécurité: reskit tome 6 chap. 12
- Sécurité: "Modèle de sécurité windows », Joel Marchand (hsc), MISC No 2.
  http://www.hsc.fr/ressources/articles/mod_sec_win/index.html.fr