Concepts et planification

La gestion de la sécurité

Windows 2003: Système d'exploitation sécurisé.

Fonction de base du système d'exploitation: Contrôle discrétionnaire des activités des utilisateurs.

Action ou ressource refusée ou accordée en fonction de l'utilisateur.

Possibilités multiples de sécurisation:

- autorisation/interdiction d'utilisation d'une machine (obtention obligatoire d'un compte d'utilisateur de la part d'un utilisateur ayant le droit d'en fournir),
- autorisation/interdiction d'utiliser d'autres applications que celles dûment autorisées,
- autorisation/interdiction d'installer des applications,
- autorisation/interdiction d'installer des périphériques,
- autorisation/interdiction de modifier l'environnement de travail,
- restrictions d'accès aux ressources (fichiers, imprimantes, ...),
- audit des actions réalisées par les utilisateurs (ouvertures de sessions d'utilisateur, accès à des ressources,...),
- ...

Droit ou privilège: Autorisation d'exécuter une action système.

Exemples: Créer des comptes, installer un pilote d'imprimante, partager un répertoire, changer l'heure du système, arrêter le système, ...

Autorisation (ou permission): Autorisation d'accès à une ressource.

Exemples: Imprimer sur une imprimante partagée, lire un fichier, exécuter une application, ...

Tous les objets du système sont soumis à autorisations via des ACLs (Access Control Lists).

Exemples: Les fichiers, les répertoires, les imprimantes, les clefs du registre,...

RETOUR

Un utilisateur possède tous les droits : l'"Administrateur".
Il est nommé "Aministrator" dans les versions anglosaxones de Windows ("root" sous UNIX).

La gestion du réseau

NOS (Network Operating System): Système d'exploitation utilisable pour la connexion d'ordinateurs en réseau.

-> connexion et communication facile entre ces machines.

Nombre important de normes de câblage connectées aux machines via des cartes d'interface réseau (NIC, Network Interface Card):

- Ethernet épais, fin et double paires torsadées,
- Phonenet,
- Fibre optique,
- Infrarouge,
- Bluetooth,
- Wifi,
- Modem RTC et ADSL,
- ...

Nombre important de protocoles réseau reconnus (Pilotes conçus par Microsoft ou par des éditeurs tiers):

- NetBEUI,
- TCP/IP,
- IPX/SPX,
- DLC,
- Appletalk,
- ATM,
- TokenRing,
- FDDI,
- ...

Nombre important de services réseau tant du point de vue serveur que du point de vue client:

- SMB,
- Lan Manager,
- DNS,

- WWW,
- FTP,
- Telnet,
- SMTP,
- NNTP,
- NTP,
- Proxy,
- DHCP,
- WINS,
- ADS,
- ...

-> grande interopérabilité dans le cadre de réseaux hétérogènes à tout niveau.

Protocole natif de Windows NT: NetBEUI.

Protocole natif de Windows 2003 (et 2008): TCP/IP.

NetBEUI	
Avantages	Inconvénients
• Rapide • Peu gourmand en ressource système	• Pas de routage • Pas compatible avec Internet • Protocole potentiellement assez bavard sur le réseau

TCP/IP	
Avantages	Inconvénients
• Rapide • Peu gourmand en ressource système • Routage • Compatible avec Internet	• Possiblement complexe à paramétrer • Protocole des "hackers"

Windows 2003 inclut une interface NetBios qui permet d'utiliser TCP/IP avec les conventions de nom de NetBEUI sans même que

NetBEUI soit installé.
Cette interface existe car Windows étant historiquement associé à NetBEUI, il en intègre encore un nombre important de caractéristiques:

- dénomination des machines,
- explorateur réseau,
- ...

Elle permet de rester compatible avec des machines qui n'utiliseraient que ces conventions de nom.

Depuis Windows 2000 Microsoft encourage l'utilisation de TCP/IP même si la base de Windows NT et 9x reste NetBEUI.

Sécurité gérée au niveau du réseau.

Le partage de ressources

Utilisation d'une ressource partagée: Utilisation d'objets système offerts par une machine distante.

Ressources partageables:

- les répertoires et les fichiers qu'ils contiennent,
- les imprimantes,
- dans une certaine mesure, les applications (Exécution d'une application sur une machine distante avec écho d'exécution sur la machine locale) (possibilité d'utiliser le service Terminal Server pour configurer un serveur de terminaux Windows, équivalent fonctionnel à un serveur X pour des terminaux X).

Sécurité au niveau des ressources partagées.

Active Directory

Active Directory (AD) est un service d'annuaire destiné à contenir des "objets": utilisateurs, ordinateurs, applications, données partagées, ... et à être interrogé par d'autres machines via réseau.

AD est basé sur un système de gestion de base de données hiérarchique dérivé d'ACCESS.

Dans le cadre d'une utilisation "système", AD possède l'avantage d'intégrer nativement des fonctionnalités de distribution et de réplication de ses informations sur plusieurs serveurs Active Directory. Ainsi, il exonère le système d'intégrer ces caractéristiques essentielles à un fonctionnement pérenne.

Intérêt d'AD:

- Windows 2003 avec AD supporte des domaines de plusieurs millions de comptes d'utilisateurs alors que, dans la pratique, Windows NT 4.0 était limité à quelques dizaines de milliers.
- Windows 2003 avec AD supporte des domaines de plusieurs dizaines de milliers de machines alors que, dans la pratique, Windows NT était limité à quelques centaines.

Unité Organisationnelle

La caractéristique la plus fondamentale d'Active Directory (héritée de l'annuaire X.500) est l'Unité Organisationnelle (UO). Une UO est un objet conteneur de l'annuaire à même de contenir des feuilles ou d'autres objets conteneurs, créant ainsi une organisation arborescente de l'information.

L'extensibilité d'Active Directory

Un autre aspect d'AD est son extensibilité par la possibilité offerte de définir de nouveaux objets à partir d'un paradigme hiérarchique orienté objet qui permet la création de nouvelles classes d'objets par ajout d'attributs et héritage d'anciennes classes.

Kerberos

Kerberos V5.0 est le protocole d'authentification réseau de Windows 2003 pour les communications avec d'autres machines 2008, 2003, 2000, Vista ou XP.
Associé à Active Directory, il rend Windows 2003 très différent de Windows NT 4.0 du point de vue de la gestion de la sécurité où seul NTLM est utilisé.

Deux points importants sont à signaler:

- L'authentification mutuelle: Cette fonctionnalité permet aux

clients et serveurs, lors d'une communication d'informations, de vérifier l'authenticité de leurs identités respectives pour éviter les usurpations d'identité.

- L'approbation transitive: Si A fait confiance à B, et B fait confiance à C, alors A fait confiance à C.
  -> En particulier, cette loi est vérifiée pour les approbations entre "Domaines Windows 2003".

Kerberos succède à NTLM. Windows 2003 devra utiliser NTLM (dont il est pourvu) pour l'authentification avec des machines sous système d'exploitation de version antérieure ou des machines indépendantes (hors domaine, voir plus loin).

La notion de domaine Windows 2003

Domaine: Unité d'administration sous Windows 2003.

Domaine: Groupe de machines reliées en réseau et pouvant être administrées comme une machine unique du point de vue des comptes d'utilisateurs et de la politique de sécurité associée.

Active Directory permet une organisation différente de la classique et très rigide organisation de Windows NT 4.0 à base de domaines et d'approbation entre domaines.

Ce sont la souplesse de la gestion par base de données et les possibilités d'extension héritées de l'annuaire X.500 (à l'origine d'Active Directory) qui permettent ces nouvelles possibilités.

Les UO définies au sein des domaines permettent le contrôle de la délégation sous Windows 2003 alors que sous NT, ce sont les domaines.

La notion de domaine au sens Windows NT 4.0 disparaît donc avec Windows 2003 avec un emploi beaucoup plus souple.

Contrôleur de domaine (DC, Domain Controller): Machine chargée de l'administration du domaine (obligatoirement une machine sous Windows 2003 Server, 2000 Server ou 2008 Server).

La base de données des utilisateurs et des groupes d'utilisateurs (**SAM**, Security Account Manager, dans la terminologie NT 4.0) est

stockée sur les DCs du domaine au sein d'Active Directory et est répliquée automatiquement entre eux.

Autre définition d'un domaine: Ensemble d'ordinateurs partageant la même base de données d'utilisateurs et de groupes d'utilisateurs.

Contrairement au modèle NT 4.0 où existe un et un seul contrôleur de domaine "principal" auquel il peut être adjoint 0, 1 ou plusieurs contrôleurs de domaine "secondaires", un domaine Windows 2003 contient 1 ou plusieurs contrôleurs de domaine placés au même niveau hiérarchique.
Le problème de la "solution" NT 4.0 est que l'indisponibilité du contrôleur primaire entraîne l'arrêt de toute possibilité d'administration du domaine: comptes d'utilisateur et machines. Dans le modèle Windows 2003, ce n'est plus le cas car toutes les tâches d'administration peuvent être poursuivies.

Définition possible de plusieurs domaines sur le même réseau.

ATTENTION: Ne pas confondre les notions de domaine Windows 2003 et domaine TCP/IP. Les domaines 2003 portent fréquemment des noms mappés sur leurs équivalents TCP/IP et permettent l'administration centralisée de leurs machines. En revanche, les domaines TCP/IP n'incluent pas cette notion d'administration système centralisée.

ATTENTION: Existence d'opérations à "maître de domaine unique" qui ne sont en charge que d'un seul contrôleur de domaine. Ces maîtres d'opération peuvent être changés mais ils doivent exister sinon les domaines sont disfonctionnels.

Les étendues NIS ou NYS sont ce qui ressemble le plus dans le monde UNIX aux domaines Windows 2003 pour l'administration des comptes d'utilisateurs et des groupes d'utilisateurs.

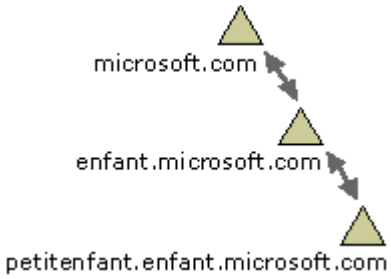
Approbation

Il est possible d'établir des relations d'approbation entre domaines permettant (s'ils y sont autorisés) aux utilisateurs d'un domaine d'utiliser les ressources disponibles au sein d'un autre domaine.

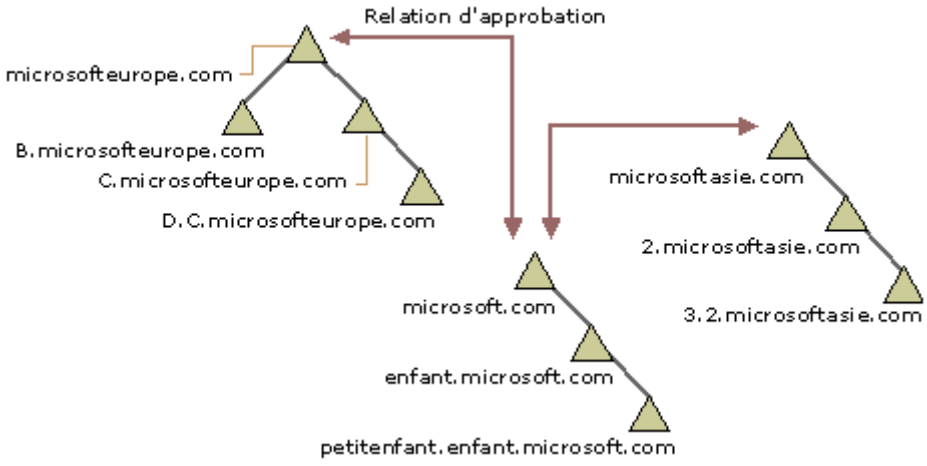
Elles pourront être créées:

- implicitement (voir plus loin) auquel cas elles sont bidirectionnelles et créées automatiquement,
- explicitement auquel cas elles sont unidirectionnelles et créées explicitement par les administrateurs des domaines concernés.

Arborescence de domaines: Structure de domaines hiérarchisée sur un mode arborescent par des relations d'approbation implicites. La base est constituée du domaine racine, qui possède un ou plusieurs domaines enfants, qui peuvent eux-mêmes posséder des domaines enfants. Les noms de ces domaines respectent les mêmes conventions que les noms TCP/IP -> espace de noms contigu pour tous les domaines fils d'un domaine racine.



Forêt: Ensemble d'arborescences de domaines sans racine commune. La racine de la forêt est la première arborescence à avoir joint la forêt lors de sa création. Tous les domaines racines des arborescences de la forêt possèdent implicitement une relation d'approbation bidirectionnelle avec la racine de la forêt.



Eléments interconnectables au sein un domaine

(1) Avec ouverture de session de travail

- Un ou plusieurs contrôleurs de domaine (sous Windows 2003 ou 2000 Server et Active Directory) sans hiérarchie particulière.
- Des machines clientes simples sous Windows 2003 ou 2000

Server (mais sans Active Directory), Vista, XP ou 2000 Professionnel. Pour un poste Windows 2003 ou 2000 Server, on parle alors de "Serveur membre".
- Des machines clientes simples sous Windows NT 4.0 ou 3.51, Server ou Workstation.

Toutes ces machines réfèrent à la même base de données des utilisateurs dupliquée au sein d'AD sur chacun des DC.

Les ouvertures de session sont authentifiées par le premier contrôleur disponible trouvé sur le réseau.

(2) Sans ouverture de session sur l'un des DCs

Etablissement possible de connexions "simples" avec d'autres machines sous Windows 2003, 2000, NT 4.0 ou 3.51, Windows Vista, XP, 98, 95 et 3.11 ou tout autre système d'exploitation reconnaissant l'un des protocoles installés sur la machine serveur et assurant les services de connexion des serveurs du domaine.

Fourniture d'un login et d'un mot de passe.

Accès limité aux ressources partagées accessibles à l'utilisateur authentifié.

Conventions UNC (Uniform Naming Convention) pour la désignation des utilisateurs et des ressources:

- **domaine\utilisateur** pour un nom d'utilisateur,
- **\\serveur\ressource** pour l'accès à une ressource partagée.

(3) Autres possibilités

Toute machine en accès via un service sans authentification explicite (WWW, FTP anonymous, ...) ou gérant son propre système d'authentification (SQL Server, Oracle, ...).

Types de machine

Les contrôleurs de domaine

Gestion centralisée de la base de données des utilisateurs et des groupes d'utilisateurs ainsi que de la politique de sécurité associée.

Authentification des ouvertures de session et des accès aux

ressources partagées qu'ils proposent.

Administration des utilisateurs.

Redondance des bases de données d'utilisateurs et de groupes d'utilisateurs.

Déploiement des politiques de sécurité.

Maintenance du domaine.

Les machines Windows Vista, XP ou 2000 Professionnel

Machines clientes simple du domaine.

Pas de stockage d'une copie de la base de données des utilisateurs.

Soumission des ouvertures de session à un DC.

Pas de rôle d'administration.

Les machines Windows Server en serveurs simples

Machines gérées comme des machines Windows Vista, XP ou 2000 Professionnel du point de vue de la base de données des utilisateurs (pas d'Active Directory) mais possédant les capacités de Windows Server du point de vue des services réseau autres que ceux de gestion des domaines.

Exemples:

- Partage de ressources sur une machine qu'on ne souhaite pas être contrôleur de domaine.
- Fonctionnement d'un logiciel qui nécessite Windows Server sur une machine qu'on ne souhaite pas être contrôleur de domaine.

Les autres systèmes

Toute machine quel que soit son système d'exploitation.

Conditions nécessaires pour l'établissement d'une connexion:

- Reconnaître l'un des protocoles du serveur de domaine.
- Être capable d'émettre un nom de login ainsi que le mot de passe

associé (Protocole d'authentification reconnu par les contrôleurs du domaine).
- Être capable de gérer la partie cliente du service auquel l'accès est réalisé.

-> Privilèges pour l'accès aux ressources partagées accédées accordés au compte de connexion sans avoir pour autant ouvert de session.

DDNS, WINS et DHCP

Une implantation Windows 2003 nécessitera fréquemment le déploiement des services DDNS (Dynamic Domain Name Service), WINS (Windows Internet Name Service) et DHCP (Dynamic Host Configuration Protocol).

Seul DDNS est réellement nécessaire car les domaines Windows 2003 l'utilisent obligatoirement.
L'implantation de DDNS permet la constitution du serveur de nom du domaine Windows 2003 construit (généralement équivalent à un domaine TCP/IP).
Par rapport à un serveur DNS classique, DDNS autorise l'enregistrement automatique et dynamique des clients.
S'il est installé sur une machine contrôleur de domaine, cet enregistrement peut être réalisé au sein d'Active Directory. La distribution automatique de cette base vers tous les contrôleurs eux-mêmes munis de DDNS permet de créer des serveur DNS synchronisés et donc de pérériser le fonctionnement du système de résolution de noms..

L'utilisation de WINS n'est réellement intéressante que lorsque plusieurs sous-réseaux TCP/IP différents doivent communiquer entre eux via routage et donc constituer un seul et même domaine de nom et que, de plus, la convention de nom simplifiée de NetBEUI doit pouvoir être utilisée (volonté de simplification pour les utilisateurs, présence de machines anciennes, utilisation souhaitée du voisinage réseau, ...) qui n'autorise pas le routage. La connexion entre ces sous-réseaux est établie physiquement et logiquement au moyen de routeurs dédiés au protocole TCP/IP.
Le problème se pose alors de faire "se trouver" respectivement les machines lorsque qu'un ordinateur situé sur un sous-réseau doit

"parler" avec une machine d'un autre sous-réseau. Sans sortir des différents sous-réseaux, le problème ne se pose pas car il est géré nativement par l'interface NetBEUI. Pour les communications entre sous-réseaux, l'information transitera et sera routée au sein de "paquets" TCP/IP. WINS apporte un service de nom permettant d'associer automatiquement bijectivement les noms TCP/IP et les nom NetBIEU.
Les machines seront configurées pour interroger un serveur WINS si elles ont besoin d'une résolution de nom. Au démarrage, toute machine configurée pour utiliser éventuellement un serveur WINS s'enregistre dans sa base de manière à la renseigner.
Sous Windows 2003, tout comme avec DDNS, une base de données WINS est stockée au sein d'Active Directory si le serveur WINS est contrôleur de domaine et est donc distribuée sur les contrôleurs. Il est possible de configurer un ensemble de serveurs WINS indépendants pour qu'ils échangent leurs bases de données.

L'utilisation de DHCP, même si elle n'est pas obligatoire, permet de centraliser la gestion des paramètres TCP/IP des machines d'un domaine.

Les utilisateurs et les groupes d'utilisateurs

Les utilisateurs

Obligation d'être référencé en tant qu'utilisateur autorisé pour pouvoir utiliser une machine Windows 2003 ou accéder à une ressource partagée par une machine Windows 2003.

Stockage dans la base de données des utilisateurs et des groupes d'utilisateurs au sein d'Active Directory d'un certain nombre d'informations concernant chaque utilisateur:

- nom d'utilisateur complet,
- nom d'utilisateur principal (UPN, User Principal Name),
- nom d'utilisateur raccourci (équivalent NT 4.0, convention UNC),
- mot de passe,
- les restrictions apportées aux actions qui lui sont autorisées,
- ...

Exemple de nom: John Smith comme nom complet, john.smith@w2k3.univ-fcomte.fr comme nom principal (ATTENTION,

le nom principal est formaté comme une adresse électronique), w2k3 \smith comme nom équivalent NT en convention UNC et smith comme nom raccourci.

Les groupes

Regroupement des utilisateurs en groupes d'utilisateurs possédant un même jeu de droits et d'autorisations.

Un utilisateur peut appartenir à plusieurs groupes. Un groupe peut appartenir à un groupe.

-> Possibilité de gestion hiérarchisée des comptes des utilisateurs.

-> Facilité de gestion.

Deux types de groupe:

- Groupes de sécurité: Leurs membres sont susceptibles de se voir attribuer des autorisations ou des droits via le groupe. Ils peuvent aussi servir de listes de distribution.
- Groupes de distribution: Ils peuvent servir de listes de distribution mais pas à l'attribution d'autorisations ou de droits.

Trois étendues de groupe sur une machine Windows 2003 Server contrôleur de domaine:

- Groupe à étendue universelle: Ils peuvent avoir comme membres des groupes et des comptes de n'importe quel domaine Windows 2003 dans l'arborescence de domaine ou dans la forêt et peuvent recevoir des autorisations dans n'importe quel domaine de l'arborescence de domaine ou de la forêt.

- Groupe à étendue globale: Ils peuvent avoir comme membres des groupes et des comptes du domaine dans lequel le groupe est défini et peuvent recevoir des autorisations dans n'importe quel domaine de la forêt.

- Groupe à étendue de domaine local: Ils peuvent avoir comme membres des groupes et des comptes du domaine Windows 2003 et peuvent être utilisés pour octroyer des autorisations à l'intérieur d'un domaine uniquement et seulement vers des machines Serveur contrôleur ou membre.

Sauf cas particulier, ces groupes sont déployés et accessibles sur toutes les machines du domaine de définition et des domaines approuvant le domaine de définition.

Un seul type de groupe peut être défini sur une machine Windows Vista, XP ou 2000 Professionnal ou 2000, 2003 ou 2008 Server en serveur simple:

- les groupes locaux.

Sur ces machines, quand elles appartiennent à un domaine, réception des groupes globaux et universels du domaine d'un des contrôleurs de domaine.

Après l'installation initiale de Windows

Deux comptes d'utilisateur locaux:

- un compte "invité" (Attention!!! pas de mot de passe), actif sur Windows Vista, 2000 ou XP Professionnal, désactivé sous Windows 2000 ou 2003 Serveur
- un compte "administrateur" d'administration local

Différents groupes intégrés locaux:

- Administrateurs
- Invités
- Utilisateurs
- Utilisateurs avec pouvoirs (utilisateurs possédant certains privilèges d'administration non relatifs aux domaines)
- Opérateurs de sauvegarde
- Réplicateurs

Différents groupes spéciaux (ne possédant pas de membre):

- Créateur/propriétaire (propriétaires des objets)
- Système (activités liées au système d'exploitation)
- Réseau (activités d'utilisateurs provenant du réseau)
- Anonymous logon (utilisateur non authentifié)
- Utilisateur authentifié (utilisateur authentifié)
- Batch (processus batch)
- Dialup (utilisateur via un accès dial-up)
- Tout le monde (tout utilisateur authentifié référant au domaine

natif ou à un domaine approuvé)
- Interactif (utilisateur qui accède à une ressource en se connectant localement à l'ordinateur proposant cette ressource)
- Service (un service)

Après l'installation de Windows 2000 ou 2003 Serveur en contrôleur de domaine

Deux comptes d'utilisateur associés au domaine:

- un compte "invité" du domaine
- un compte "administrateur" d'administration du domaine

Groupes intégrés créés au sein d'Active Directory:

- Administrateurs (domaine local)
- Invités (domaine local)
- Utilisateurs (domaine local)
- Opérateurs de compte (domaine local) (gestion des comptes et des groupes d'utilisateurs sauf pour ceux qui possèdent des privilèges d'administration)
- Opérateurs de serveur (domaine local) (gestion du bon fonctionnement des serveurs du réseau)
- Opérateurs d'impression (domaine local) (gestion du bon fonctionnement des activités liées aux imprimantes)
- Duplicateurs (domaine local) (gestion des activités de réplication de répertoires)
- Admins du domaine (global)
- Invités du domaine (global)
- Utilisa. du domaine (global)
- Ordinateurs du domaine (global)
- Contrôleurs du domaine (global)
- Éditeurs de certificats (global)
- Administrateurs de l'entreprise (universel ou global)
- Administrateurs de stratégie de groupe (universel ou global)
- Administrateurs du schéma (universel ou global)

Sur les Windows membres simples d'un domaine

Groupes et utilisateurs issus du domaine:

- les comptes
  - "invité" du domaine

    - "administrateur" d'administration du domaine
- les groupes
    - Admins du domaine (global)
    - Invités du domaine (global)
    - Utilisa. du domaine (global)
    - ...

Sur ces machines, existence préservée et utilisation possible des comptes et groupes locaux. Sur les contrôleurs de domaine, existence préservée mais utilisation impossible des comptes et groupes locaux.

Création des utilisateurs et de nouveaux groupes locaux, globaux ou universels par l'administrateur système ou toute personne possédant les privilèges administrateur, admins du domaine ou opérateur de comptes.

Contenu précis d'un compte d'utilisateur d'un domaine

Informations pouvant être renseignées lors de la création ou bien à tout autre moment après la création:

- Nom d'utilisateur complet
- Nom d'utilisateur principal (UPN, User Principal Name)
- Nom d'utilisateur raccourci (équivalent NT 4.0, convention UNC)
- Mot de passe
- Adresse électronique
- Numéros de téléphone
- Horaires d'accès
- Stations de travail autorisées pour l'accès
- Adresse postale
- Date d'expiration (date au delà de laquelle le compte est désactivé, les fichiers personnels ne sont pas détruits s'il y en a)
- Répertoire de base (généralement, le répertoire personnel) (répertoire local ou réseau)
- Script d'ouverture de session (fichier de commandes lancé à l'ouverture de session, mais pas lors du simple accès à une ressource partagée)
- Profil (localisation des fichiers de configuration de l'utilisateur)
- Place de l'utilisateur dans son organisation
- Groupes auxquels appartient l'utilisateur
- Informations de configuration Remote Access Service
- Informations de configuration de l'utilisateur pour les services

Terminal Server

SID (Security Identifier): Identificateur unique utilisé pour désigner un utilisateur ou un groupe d'utilisateurs au sein d'un domaine Windows 2003.

Exemple:
S-1-5-21-3292650235-2243138800-104724495-1005

Tout SID ayant été utilisé ne le sera jamais plus.

Les stratégies de groupes

Via l'utilisation des stratégies de groupes (stratégies de sécurité), il est possible de gérer de manière centralisée un grand nombre de paramètres relatifs aux utilisateurs et aux ordinateurs d'un domaine.

Les possibilités offertes par les stratégies de groupes sont très larges:

- gestion de l'interface graphique,
- gestion des applications utilisables par les utilisateurs,
- installation d'applications,
- gestion des mises à jour,
- droits des utilisateurs,
- configuration automatique des applications,
- ...

Les profils

Profil: Ensemble d'informations visibles ou masquées (exemple: clefs et valeurs du registre pour le paramètrage des applications) définissant l'environnement de travail d'un utilisateur.

Par exemple, pour chaque utilisateur:

- son menu démarrer,
- son bureau,
- son dossier "Mes documents",
- son registre (fichier NTUser.dat):
  - ses connexions réseaux, ses montages d'imprimante réseau,
  - ses variables d'environnement (path, set, ...),

    - ses définitions de couleurs, de police de caractères,...
    - ses paramétrages logiciels,
    - ...
- ...

Stockage local des profils dans des ensembles de fichiers et de répertoires stockés dans le répertoire "Documents and Settings", généralement dans un répertoire portant le nom de l'utilisateur.

"Default User": Profil par défaut géré par le système et attribué par copie à chaque utilisateur (faute d'une configuration contraire) lors de sa première connexion sur une machine. Le profil par défaut doit être configuré sur chaque poste client.

"All Users": Profil commun à tous les utilisateurs. On y trouve en particulier les entrées communes du Menu démarrer, le bureau commun et la partie du registre commune à tous les utilisateurs de cette machine. Ce profil n'est généralement modifiable que par l'administrateur.

Attribution possible d'un profil personnel à tout utilisateur modifiable uniquement par lui.

Dans le cadre d'un domaine, centralisation possible de la gestion de manière que tout utilisateur retrouve son profil quel que soit l'ordinateur sur lequel il se connecte.

-> Profils sauvegardés dans un répertoire partagé d'un serveur de fichiers du domaine (accessible à toutes les machines du domaine).

- Lors de la connexion, téléchargement automatique du profil sur le poste client dans le répertoire "Documents and settings".
- Utilisation du profil (avec ou sans modification) sur le poste client.
- Lors de la déconnexion, déchargement automatique du profil du poste client vers le serveur.
- Conservation éventuelle du profil local en cache sur le poste client. Sinon, effacement.

La sécurité: Les privilèges (droits)

Privilège (droit): Autorisation attribuée aux utilisateurs et aux

groupes d'utilisateurs leur permettant d'exécuter une action système.

Privilège attribué à un groupe automatiquement attribué à l'ensemble de ses membres.

A l'installation du système d'exploitation, attribution par le programme d'installation de privilèges par défaut aux groupes d'utilisateurs et utilisateurs intégrés.

Via les stratégies de groupes, les administrateurs pourront changer les privilèges des groupes et utilisateurs intégrés et attribuer des privilèges aux groupes qu'ils créent.

Existence d'un "groupe par défaut" dans lequel tout utilisateur est automatiquement placé.

La sécurité: les autorisations

Autorisation: Autorisation d'accès à une ressource accordée par un administrateur à un utilisateur ou un groupe d'utilisateurs.

- Accès sécurisé pour les fichiers et répertoires créés dans une partition NTFS.
- Accès sécurisé pour les imprimantes.
- Accès sécurisé aux ressources réseau (répertoires, imprimantes, ...).
- Accés sécurisé à tous les objets du système d'exploitation soumis à l'attribution d'ACLs..

Propriétaire: Utilisateur qui a créé ou qui s'est approprié un fichier ou un répertoire (il possède généralement tous les droits sur cet objet).

Contrôle d'accès organisé par l'administrateur (effectué au niveau utilisateur ou plus globalement au niveau groupe d'utilisateurs).

Autorisations pouvant être attribuées par l'administrateur (simplifié)

Pour les répertoires (on fixe les permissions pour le répertoire lui-même et pour les fichiers qu'il contient ou qu'il contiendra lors de leur création):

- Contrôle total
- Modification
- Lecture et exécution
- Affichage du contenu du dossier
- Lecture
- Ecriture
- Autorisations spéciales ...

Pour les fichiers

- Contrôle total
- Modification
- Lecture et exécution
- Lecture
- Ecriture
- Autorisations spéciales ...

Autorisations spéciales:

- Contrôle total
- Parcours du dossier/exécuter le fichier
- Liste du dossier/lecture de données
- Attributs de lecture
- Lecture des attributs étendus
- Création de fichier/écriture de données
- Création de dossier/ajout de données
- Attributs d'écriture
- Ecriture d'attributs étendus
- Suppression
- Autorisations de lecture
- Modification des autorisations
- Appropriation

Contrôle total: toutes les permissions précédentes sont attribuées.

Pour un dossier, action de configuration des autorisations réalisable sur:

- ce dossier seulement
- ce dossier, les sous-dossiers et les fichiers
- ce dossier et les sous-dossiers
- ce dossier et les fichiers
- les sous-dossiers et les fichiers seulement

- les sous-dossiers seulement
- les fichiers seulement

NTFS 5 autorise l'héritage des autorisations pour un sous-répertoire depuis son répertoire parent. Il permet d'ajouter des autorisations spécifiques à ces autorisations héritées.
NTFS 5 permet aussi à un répertoire de laisser ou non ses sous-répertoires hériter de ses propres autorisations.

A l'installation du système, permissions par défaut attribuées aux fichiers et répertoires du système d'exploitation aux groupes et utilisateurs intégrés -> sécurité minimale.

Droit de l'administrateur: Prendre possession et changer les permissions de l'intégralité des objets.

Lors de la création d'un fichier ou d'un répertoire, attribution à cet objet des autorisations du répertoire dans lequel il est placé (le créateur en est le propriétaire).

Lors du déplacement d'un fichier ou d'un répertoire, conservation des informations de sécurité.

La sécurité: L'audit

Audit: Conservation d'une trace des événements détectés sur une machine.

A chaque événement, enregistrement d'une ligne de description dans l'un des journaux d'événements.

Evénements pouvant être audités:

- Système (audit des activités du système d'exploitation)
- Sécurité (audit de l'activité des utilisateurs et de l'utilisation des ressources)
- Application (audit des applications et des services)
- Active Directory (spécifique aux DC)
- DNS (spécifique aux serveurs DNS)
- Réplication de fichiers (spécifique aux machines réplicatrices)

-> autant de journaux différents.

Journaux Système et Application: Audit du fonctionnement de la machine pour détecter les dysfonctionnements éventuels soit hardware, soit software.

Journal sécurité: Audit des activités des utilisateurs.

Événements pouvant être audités dans le journal sécurité:

- Les ouvertures et fermeture de session
- Les accès aux fichiers et objets
- L'utilisation de ses droits par un utilisateur
- La gestion des utilisateurs et des groupes
- Les modifications de la stratégie de sécurité
- Les démarrages et arrêts du système
- Le suivi de processus

Par défaut, audit activé seulement pour les événements liés aux journaux Système, Application, Active Directory, DNS et Réplication de fichiers.

La gestion des partitions et des systèmes de fichiers

Introduction du système de fichiers NTFS avec Windows NT 4.0.

Nécessaire à la gestion de la sécurité d'accès aux fichiers, à l'implantation de la compression à la volée et à l'encryptage des données.

Nouvelle évolution avec Windows 2000 vers NTFS 5 qui permet de rendre les disques "dynamiques" et apporte les fonctionnalités plus élaborées de gestion logicielle des disques en RAID (agrégats par bandes, disques en miroir, agrégats par bandes avec parité -> disques RAID).

Gestion du système de fichiers FAT32 (Windows 98).

Gestion du système de fichiers FAT16.

Gestion des noms longs.