Table des matières

1 Rappels historiques

1.1 Les premiers ordinateurs

En 1946, l'ENIAC (Electronic Numerical Integrator Analyser and Computer) est le premier ordinateur entièrement électronique programmable opérationnel. Il repose sur la technologie des tubes électroniques (« lampes »). Auparavant, les « ordinateurs » étaient électromécaniques. Il pèse 30 tonnes, mesure 1 x 2,5 x 30 mètres et consomme 150 kW ! La fréquence est de 0,5 MHz…

ENIAC, EDVAC, EDSAC, Mark I, MESM (МЭСМ).

L'invention du transistor en 1947 est une véritable révolution : même rôle qu'un « tube » mais beaucoup plus petit et résistant.

En 1956, IBM lance le premier disque dur : RAMAC 350. Il se compose de 50 plateaux de 24 pouces capables de stocker 5 Mo !

Les premiers ordinateurs de série sont commercialisés à la fin des années 50 avec notamment les Bull Gamma 60 (15 exemplaires) et IBM 1401 (10 000 exemplaires) illustré sur la photo.

Le premier « micro-ordinateur » abordable est signé DEC avec le PDP-1 : 120 000 $ dans 1 m^3…

Le circuit intégré qui a été inventé en 1958 commence à être utilisé en informatique au milieu des années 60. Il permet de réduire considérablement la taille des ordinateurs.

La micro-informatique débute dans les années 70 avec l'arrivée des premiers micro-processeurs comme le 8008 d'Intel.

Les premiers ordinateurs tels que nous les connaissons encore aujourd'hui sont arrivés en 1981 avec l'IBM PC. Cette micro-informatique évince partiellement le principe du serveur central avec des clients (mainframe).

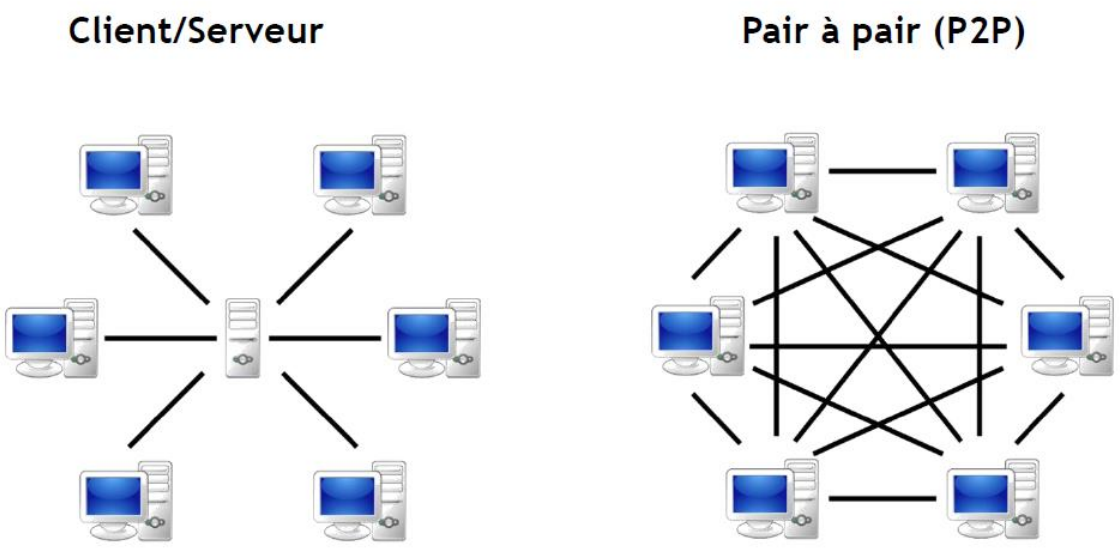
1.2 Réseaux

Les prémisses du réseau remontent au début des années 60 quand Norman Abramson de l'université d'Hawaii développe le système ALOHA (CSMA-CD). Le principe est utilisé par Xerox en 1973 pour concevoir l'Ethernet à 3 Mbps.

L'Ethernet n'est pas le meilleur protocole réseau, FDDI et Token-Ring sont nettement plus efficaces, mais il est bon marché. L'arrivée des switchs (commutateurs) rend l'Ethernet performant tout en préservant l'avantage de tarifs compétitifs. Depuis son lancement, la vitesse de l'Ethernet a évolué considérablement : 10 Mbps en 1980, 100 Mbps en 1995, 1 Gpbs en 1999, 10 Gbps en 2002 et 100 Gbps en 2012.

Au niveau des modèles, il existe deux grandes familles de réseaux :

- Client - Server : Tout passe par un serveur central. L'administration est centralisée avec comme avantages une sécurité accrue et des performances élevées. En contrepartie, il faut un serveur central spécifique et plus coûteux et plus de connaissances pour mettre le système en œuvre.
- Peer to Peer : Chaque machine est à la fois client et serveur. Un ordinateur peut par exemple partager une imprimante (serveur) tout en étant le client d'un autre ordinateur qui partage un dossier. Le système est simple à mettre en œuvre mais il faut administrer individuellement chaque machine du réseau, ce qui limite l'usage de ce modèle aux petits réseaux (jusqu'à une dizaine de postes).



1.3 Les servers

Quelle est la différence entre un client et un serveur ? Un serveur propose des… services. C'est le principe même d'un serveur ! Depuis la généralisation de la virtualisation, certains concepts ont cependant évolué.

Jusqu'au début de ce siècle, les serveurs étaient des machines physiques. De « belles grosses boites » avec un Windows Server sur lesquelles il fallait judicieusement équilibrer les rôles (ensemble de services) afin de ne pas surcharger un serveur au niveau du processeur, un autre au niveau des disques et un troisième au niveau de la mémoire…

Avec la montée en puissance des processeurs et grâce à la virtualisation, le serveur est toujours une « belle grosse boite » mais elle fait tourner un logiciel de virtualisation de premier niveau (ESXi ou Hyper-V). La machine physique devient un hôte (host) et les serveurs deviennent des machines virtuelles (« VM »). La tendance actuelle peut se résumer presque à : 1 rôle = 1 serveur. Les serveurs virtuels étant « gratuits », il est facile d'en créer un pour chaque besoin sans pour autant tomber dans l'excès.

Les rôles de serveurs les plus connus :

- Serveur de fichiers
- Serveur d'impression
- Serveur mail
- Server Web
- Server DB
- Server d'authentification
- Serveur de backup
- Serveur de certification

Windows Server est capable de remplir certains de ces rôles directement mais d'autres nécessitent des logiciels tiers.

2 Notion de partage, permissions et utilisateurs

Dans les anciennes versions de Windows (les « 9x »), le partage des ressources et la limitation d'accès se faisaient d'une façon simple. Partager une imprimante ou un dossier se résumait à un clic droit « partager ». Le contrôle d'accès à la ressource partagée était lié à un mot de passe. Il y avait donc un mot de passe pour chaque ressource partagée ! Pour sortir un document sur une imprimante partagée, il suffisait de taper le mot de passe de l'imprimante…

Ce système était d'une simplicité enfantine et convenait à un usage familial voire à celui d'une petite entreprise. Cependant, il ne dépendait que de la ressource : tout le monde ou, pire, n'importe qui, connaissant le mot de passe d'une ressource partagée pouvait accéder à cette ressource.

Les Windows Server (et tous les Windows depuis XP) reposent sur un autre mode de fonctionnement qui fait intervenir des utilisateurs appartenant à des groupes, des partages et des permissions.

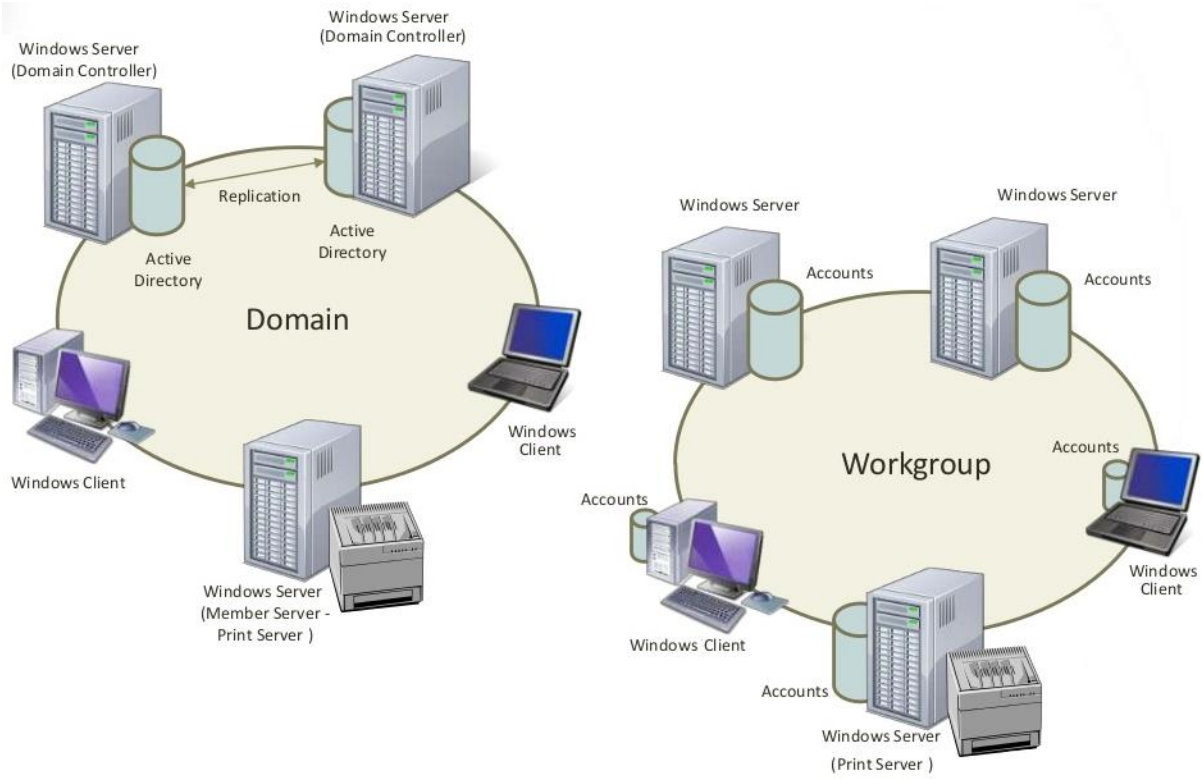
- Utilisateur : Chacun est un utilisateur, un « user » dans notre jargon, et au niveau de Windows les users sont systématiquement intégrés dans des groupes.

- Partage (lié au réseau) : Le partage est une ressource (imprimante, clés USB, disque dur, dossier) rendue accessible par le réseau. Le partage s'accompagne de permissions simples : read, modify et full control
- Permissions NTFS (lié au système de fichiers du disque) : 6 permissions standards formées sur base de 13 permissions avancées.

Ce mode de fonctionnement nettement plus avancé offre à la fois un haut niveau de sécurité et une excellente « granularité » (souplesse dans la configuration des permissions) : tout utilisateur fait partie d'un groupe, groupe pour lequel il existe des permissions et l'accès à chaque ressource est le résultat des permissions de partage et des permissions NTFS.

Note : ces points sont uniquement présentés sous forme de notions nécessaires à la présentation de l'Active Directory. Ils font l'objet d'un autre module de cours.

3 Groupe de travail et domaine



Dans un groupe de travail (workgroup), il existe une base de données des utilisateurs sur chaque ordinateur et chaque ordinateur utilise uniquement sa propre base de données. Le fichier SAM (Security Accounts Manager) stock les comptes (accounts est le terme anglophone usité) et les mots de passe. Pour autoriser un utilisateur à travailler sur plusieurs machines, il faut créer le compte sur chaque machine. Que ce soit la création d'un utilisateur ou le changement de mots de passe, chaque tâche administrative banale devient une corvée à faire sur tous les ordinateurs concernés !

Dans un domaine (domain), chaque ordinateur a sa propre base de données MAIS il existe une base de données centrale hébergée sur des machines spécifiques : les contrôleurs de domaines (domain

controller ou DC). Lorsque l'ordinateur se connecte dans le domaine, il utilise la base de données centrale. L'ordinateur peut également utiliser sa base de données locale (hors domaine).

Les Active Directory Domain Services ou AD DS représentent un ensemble de services destinés à gérer un domaine utilisant la base de données Active Directory. Ces services comprennent :

- Une base de données des utilisateurs, ordinateurs, imprimantes, domain controllers, etc.
- LDAP qui fait office d'intermédiaire dans les requêtes et les réponses.
- Kerberos pour assurer la sécurité.
- File réplication pour assurer la redondance.

Note : En développement, la redondance est à éviter car elle alourdit le programme. Dans le domaine qui nous concerne, la redondance est obligatoire afin d'éviter la perte d'informations ou l'incapacité à fournir un service.

L'Active Directory s'est d'abord appelé NT Directory Services (NTDS, soit « Services d'annuaire de NT » en français). On retrouve d'ailleurs encore cette nomenclature dans la littérature courante ainsi que dans le nom de certains utilitaires comme NTDSUTIL.EXE ou dans le nom du fichier de la base de données NTDS.DIT. L'Active Directory a été présenté pour la première fois en 1996, mais sa première utilisation remonte à Windows 2000 Server Edition en 1999. Le service d'annuaire Active Directory résulte de l'évolution de la base de compte plane SAM.

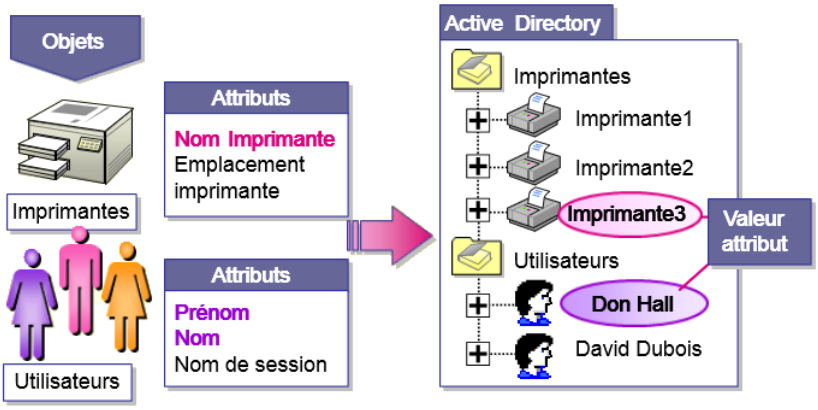
4 Cinq rôles Active Directory…

Avant de continuer plus avant, il est important de clarifier la situation ! Depuis Windows Server 2008, il n'existe pas moins de 5 rôles faisant référence à Active Directory.

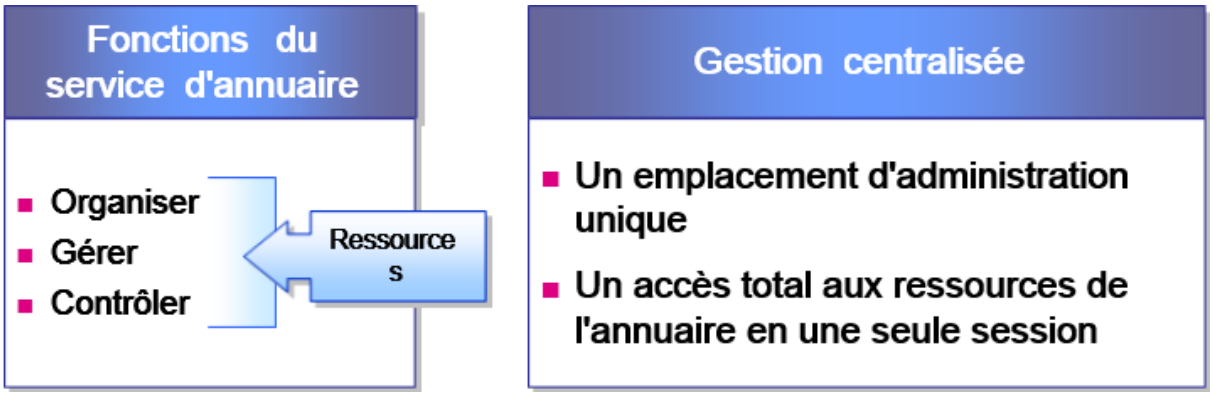
- AD DS : Le rôle Active Directory Domain Services comprend l'annuaire pour la gestion des utilisateurs, ordinateurs, groupes, etc., l'ouverture de session via des mécanismes d'authentification sécurisés et le contrôle d'accès aux ressources.
- AD CS : Le rôle Active Directory Certificate Services vise essentiellement la sécurité avec les certificats numériques et les clés.
- AD FS : Le rôle Active Directory Federation Services concerne tout ce qui est SSO (Single Sign-On), c'est-à-dire une authentification unique pour accéder à différents services. En étant par exemple identifié sur LinkedIn, Facebook ou Gmail, L'utilisateur est reconnu sur d'autres sites.
- AD RMS : Le rôle Active Directory Rights Management Services va beaucoup plus loin que les permissions dans la gestion des droits. Il permet par exemple d'autoriser la sauvegarde d'un document mais pas son impression ni son envoi par mail.
- AD LDS : Le rôle Active Directory Lightweight Directory Services (anciennement ADAM) est simple service d'annuaire.

5 Active Directory

L'Active Directory est un annuaire (répertoire, base de données) qui centralise les éléments d'un réseau tels que les comptes des utilisateurs, les postes de travail, les serveurs, les imprimantes, etc. Ces éléments sont les **objets uniques** associés à des attributs variables.



L'objectif principal d'Active Directory est de fournir des services centralisés d'administration pour organiser, gérer et contrôler les ressources.



La base de donnée de l'AD est très fortement indexée afin d'accélérer les recherches en lecture. L'AD utilise la même structure hiérarchique que DNS (voir le module DNS). Le protocole standard LDAP (Lightweight Directory Access Protocol) est utilisé pour l'interrogation et la mise à jour de la base de données AD.

L'Active Directory ne se présente bien entendu pas comme les bons vieux répertoires avec leurs fiches en papier du siècle dernier. Des analogies permettent de comprendre certaines notions de l'Active Directory.

Le domaine est un simple élément dans la composition d'ensemble plus complexe et hiérarchisé qui compte les éléments suivants :

- Forêt
- Arbre
- Domaine
- Site
- Organizational Unit

- Groupe
- Objets

Tous les points ne sont pas abordés dans ce module d'introduction à Active Directory.

6 Les fichiers de l'AD

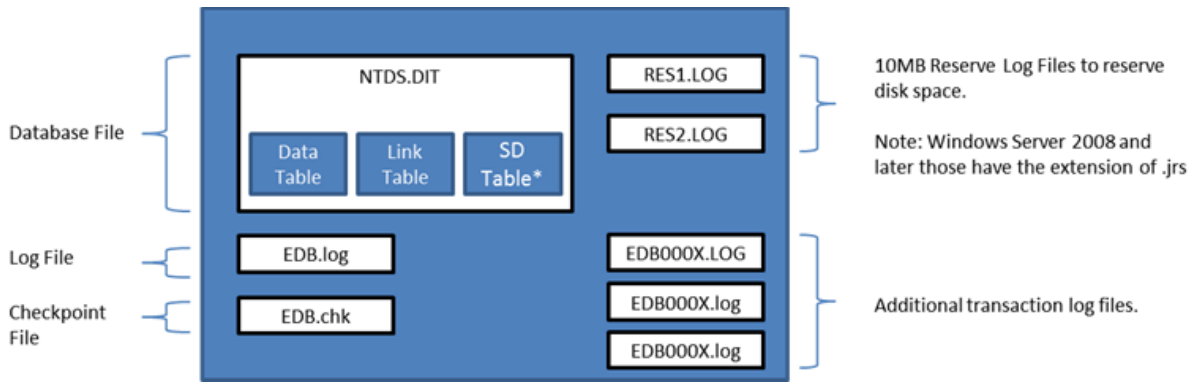
La base de données de l'AD est contenue dans le fichier : NTDS.DIT. Il est accompagné de plusieurs autres fichiers. Par défaut, NTDS.DIT se situe dans le répertoire *%systemroot%/NTDS*. Ce fichier est considéré, géré et répliqué comme s'il se composait de sections ou d'instances distinctes (les partitions). Les services de domaine Active Directory utilisent le moteur de base de données ESE (Extensible Storage Engine) introduit par Exchange Serveur pour modifier en toute sécurité le contenu du fichier NTDS.DIT. Comme de nombreux moteurs de base de données, l'ESE utilise des logs transactionnels.

Exemple :

1. Un objet de l'AD vient d'être modifié ; une transaction est lancée
2. Le moteur ESE écrit la modification en mémoire
3. Le moteur ESE écrit la transaction dans le fichier Edb.log
4. Le moteur ESE écrit dans la base de données NTDS.DIT
5. Le moteur ESE valide la transaction (Compare le fichier Log et les données dans la base NTDS.DIT)
6. Le moteur ESE met à jour le fichier de vérification de point de contrôle Edb.chk

Pour qu'une requête soit réussie, elle doit être totalement effectuée. Si pour une raison ou un autre la requête ne peut pas être complétée ou échoue, la base de données n'est pas modifiée.

Contenu du dossier *%systemroot%/NTDS* (sur un DC) :



Les fichiers :

1. NTDS.DIT : Le fichier physique qui contient toutes les données de l'AD. Il se compose de trois tables internes : data tables, link table et SD (Security Descriptor) table.
2. EDB.LOG : Le fichier de logs dans lequel les transactions sont écrites avant d'être transférées dans NTDS.DIT

3. EBD*.LOG : Les fichiers de logs additionnels si EBD.LOG n'a pas encore été transféré dans NTDS.DIT.
4. EDB.CHK : Ce fichier (pointeur) indique jusqu'à quel point les logs ont été transférés dans NTDS.DIT
5. RES1.LOG et RES2.LOG : Deux fichiers « soupapes » qui seront effacés si l'espace pour stocker les logs venait à manquer.

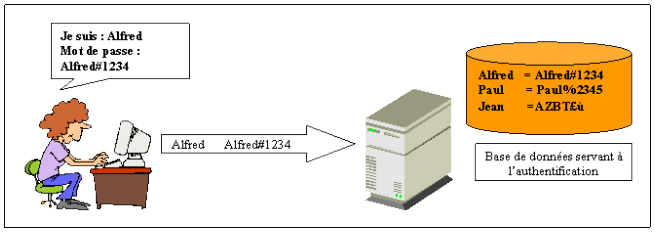
Conseil pratique : Placer une image ISO (quelques Go) dans le dossier NTDS afin d'avoir une vraie soupape de sécurité. Les 2 x 10 Mo ne constituent pas une sécurité suffisante.

7 Le domaine

Dans un environnement AD DS, le domaine est l'unité fondamentale de la structure logique. Un domaine est un ensemble d'objets qui partagent les mêmes ressources, le même espace de nom et qui ont la même frontière de sécurité. Un domaine constitue une limite administrative : les stratégies et les paramètres de sécurité ne peuvent s'étendre au-delà du domaine.

8 Les contrôleurs de domaine

8.1 DC



Un contrôleur de domaine est un serveur qui stocke et réplique les données de l'AD (NTDS.DIT, LOGS et SYSVOL), permet l'authentification des utilisateurs et appliquent les stratégies de groupes. Les DC gèrent les interactions entre l'utilisateur et le domaine, y compris les processus d'ouverture de session, l'authentification et les recherches dans l'annuaire (notamment via le Global Catalogue). La machine elle-même doit répondre à 4 critères :

- Exécuter un OS Windows Server
- Avoir un nom défini
- Avoir une adresse IP fixe
- « Une time zone configurée »

8.2 RODC

Le contrôleur de domaine en lecture seule (RODC) est un nouveau type de contrôleur de domaine introduit avec Windows Server 2008. Il permet de déployer facilement un contrôleur de domaine à des emplacements où la sécurité physique ne peut être garantie ou aux endroits avec une connexion lente. Il héberge des partitions en lecture seule de la base de l'AD.

Avantages :

- Sécurité renforcée

- Ouvertures de session plus rapides
- Accès plus efficace aux ressources du réseau

9 Les objets, les classes et les attributs

Les objets de l'AD sont regroupés en classes dont voici quelques exemples :

- Ordinateurs : les serveurs, les DC, les workstations, les laptops, les tablettes, etc.
- Imprimantes : les ressources de type « imprimante ».
- Utilisateurs : les comptes des utilisateurs pour l'authentification.
- Groupes : pour rassembler des objets pour leur attribuer des droits similaires.
- Unités organisationnelles : des containers pour agencer des objets de façon représentative.
- Contact : « utilisateur » sans authentification (exemple : un consultant externe).

Une classe d'objet se compose d'attributs.

Exemple : une société veut référencer ses camions et ses chauffeurs. Des informations utiles sont par exemple : nom, prénom, téléphone, permis, marque, modèle, immatriculation et poids.

Une classe d'objet se compose d'attributs, on peut la voir comme un modèle de fiche papier type pour un véhicule ou un chauffeur :

- Classe d'objet chauffeur : nom, prénom, téléphone, permis
- Classe d'objet véhicule : marque, modèle, permis, immatriculation, poids

Un objet est une fiche remplie :

- Nom : Thevenier, Prénom : Pascal, téléphone : +32 475 984 xxx, Permis : B
- Marque : Mercedes, Modèle : Actros, permis : C1E, immatriculation : 1-ABC-123, Poids : 8000 Kg.

Les objets de l'AD sont comparables aux fiches et les attributs sont les différents champs de la fiche : nom, prénom, adresse, etc. Un attribut peut servir à différentes classes d'objets.

Les objets de l'AD doivent être uniques ! Pour parvenir à cette unicité, chaque objet dispose d'identifiants uniques représentés par deux attributs : le DistinguishedName et le GUID.

9.1 Le DistinguishedName

Ce premier identifiant unique est aussi appelé DN et représente le chemin LDAP complet pour atteindre un objet de l'AD. Il n'est pas possible de créer deux objets avec le même nom.

Exemple :

- Domaine : abc.local
- OU de l'objet : informatique, administrateurs
- Nom de l'objet : Pascal

Le DN de l'objet Pascal : cn=pascal,ou=administrateurs,ou=informatique,dc=abd,dc=local

LDAP utilise le principe du DNS pour créer le chemin complet. DNS sera abordé en détail dans un autre module.

9.2 Le Globally Unique IDentifier

Le second identifiant unique est le Globally Unique Identifier ou GUID ; il correspond à l'attribut ObjectGUID. Lors de la création de l'objet, le GUID est généré par un algorithme sur base d'éléments dont le nom de l'objet et l'heure/date. Il est codé sur 128 bits et ne change jamais.

Exemple :

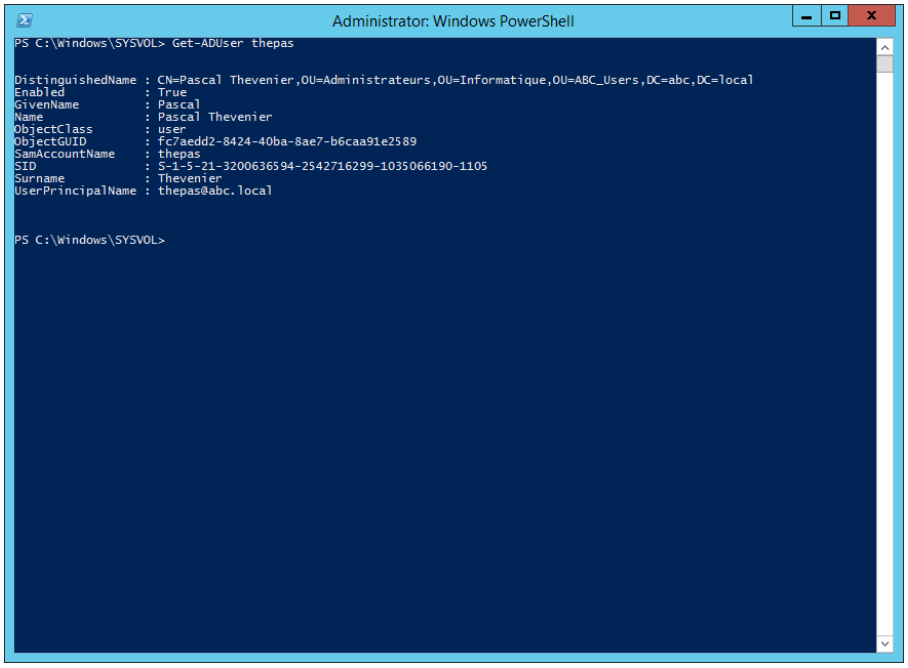
- Création d'un user : Pascal
- Son GUID est : a947c767-94df-4638-ac78-062c35702397
- Suppression de Pascal
- Création d'un nouvel user : Pascal
- Son GUID est : fc7aedd2-8424-40ba-8ae7-b6caa91e2589

Les GUID sont sans surprise totalement différents et ils le seront toujours même si le DN est resté le même.

9.3 Quelques attributs courants

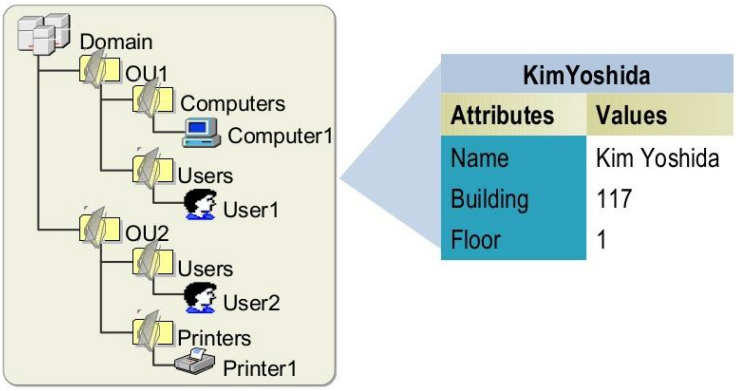
GivenName	Prénom
Surname	Nom
Name	Prénom Nom
SamAccountName	identifiant d'ouverture de session
UserPrincipalName	identifiant d'ouverture de session avec *@nomdomaine*
Mail	adresse mail
AdminCount	1 pour admin, 0 pour les autres
Description	Description de l'objet
AccountExpires	Date d'expiration du compte
PwdLastSet	Date de dernière modification du mot de passe
UserAccountControl	Etat du compte

La commande PowerShell : `Get-ADUser <SamAccountName>` permet de voir quelques-uns des attributs utilisés pour la classe user.



10 Les unités organisationnelles (OU)

Les unités organisationnelles sont des objets de l'Active Directory mais ce sont surtout des conteneurs dans lesquels prennent place les objets de l'AD comme des utilisateurs, des groupes, des ordinateurs et d'autres OU. Les OU servent notamment à agencer de manière représentative la structure hiérarchique et/ou logique d'une entreprise.



L'OU est la plus petite entité à laquelle il est possible d'attribuer des paramètres de stratégie de groupe ou déléguer une autorité administrative. Ces usages seront vus plus tard dans d'autres modules.

Le domaine étant une limite administrative, une OU ne peut pas contenir des objets d'autres domaines.

Les OU sont un peu comparables aux dossiers qui permettent d'organiser les fichiers sur le disque dur.

11 Les groupes

S'il est possible de gérer une dizaine d'utilisateurs au cas par cas, le travail deviendrait rapidement conséquent et fastidieux avec une vingtaine d'utilisateurs. De plus, dans la très grande majorité des cas, des nombreux utilisateurs doivent avoir accès aux mêmes ressources avec les mêmes droits.

Un groupe est un ensemble de comptes utilisateurs auxquels sont assignés droits et permissions.

- Un groupe peut contenir d'autres groupes (et donc être contenu dans un autre groupe).
- Un utilisateur peut faire partie de plusieurs groupes.

Un droit concerne les actions systèmes qu'une personne est autorisée à effectuer sur un ordinateur par exemple : arrêter le système, modifier l'heure, partager un répertoire, etc.

Les permissions autorisent l'accès à des ressources partagées comme des dossiers, des imprimantes, des applications, etc.

11.1 Sécurité et distribution

Il existe deux types de groupes (selon leur rôle) :

- Les groupes de sécurité servent à assigner les permissions d'accès aux ressources. Sécurité oblige, un groupe de sécurité possède un SID.
- Les groupes de distribution sont utilisés pour créer des listes de diffusion et servent essentiellement à des applications de messagerie comme Exchange. Pas de SID.

11.2 Portée

Les groupes portent sur des étendues différentes :

- Domain Local : uniquement dans le domaine d'appartenance
- Global : dans n'importe quel domaine (trusted domains, pour plus tard)
- Universal : dans n'importe quel domaine d'une forêt ou d'une trusted forest (pour plus tard)

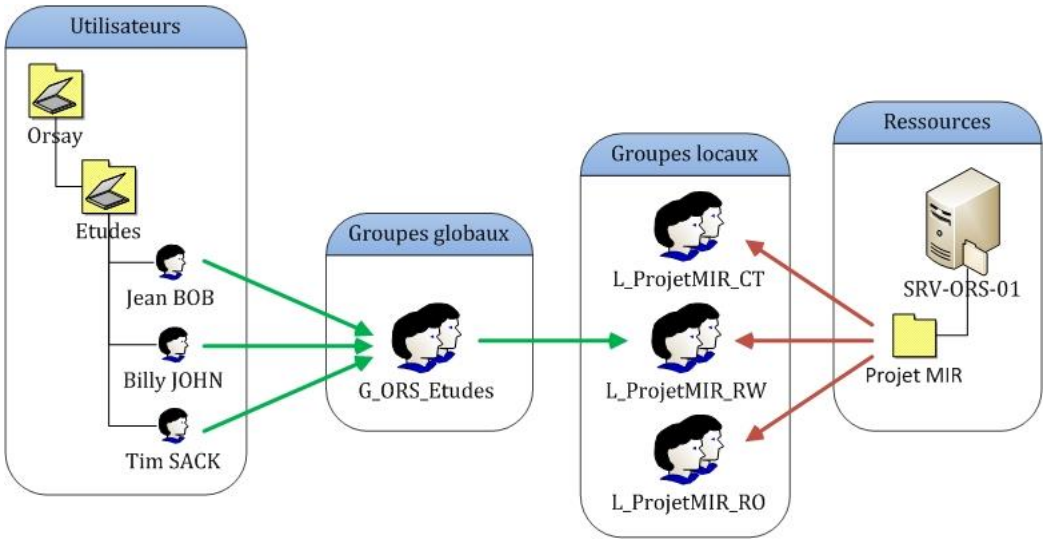
11.3 Usage

- Le Groupe Local est à utiliser pour les accès aux ressources d'un domaine. Il devrait avoir pour membre des groupes globaux contenant les utilisateurs.
- Le Groupe Global 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).
- Le Groupe Universal est à utiliser pour regroupe des groupes ayants une portée multi-domaines. Ce type groupe ne sera répliqué vers les catalogues globaux que lorsqu'une modification sera réalisée dans sa liste de membres. La modification des membres d'un groupe global lui appartenant, celle-ci n'affecte pas le groupe universel (optimisation réseau).

11.4 Exemple

Il est vivement conseillé d'être explicite et méthodique dans l'appellation des groupes :

- Local Group : L_NomRessources_Permission
- Global Group : G_NomDuGroupe

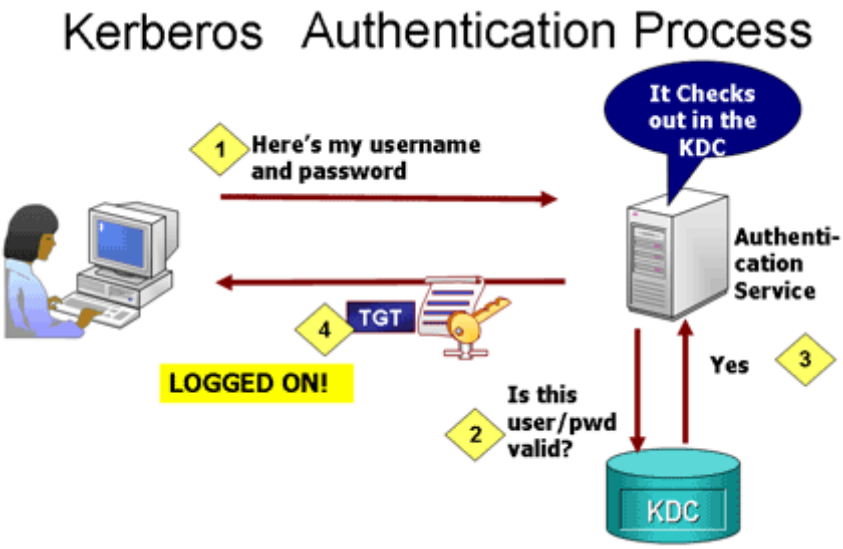


Cet exemple montre l'usage de bonnes pratiques :

- L_ProjetMIR_CT : **L** pour groupe **L**ocal, ProjetMIR pour la ressource et CT pour Contrôle Total.
- G_ORS_Etudes : **G** pour groupe **G**lobal, ORS pour Orsay et Etudes (ensemble d'étudiants).

12 Authentification et ouverture de session

L'authentification via un serveur Kerberos n'est pas propre à l'environnement Windows. De manière globale on parle d'une identification auprès d'un KDC (Key Distribution Center). Dans le cas de l'AD, le KDC est un DC.



L'utilisateur entre des informations d'identification (en anglais ses credentials) sur un ordinateur du domaine pour ouvrir une session.

Les credentials sont envoyées au DC qui va les crypter et les comparer avec les données présentes dans l'AD. Le processus ne continue que si la concordance est avérée.

Le DC génère un Ticket Granting Ticket (TGT) et un Privilege Attribute Certificate (PAC) contenant des informations sur l'utilisateur avec notamment les SID des groupes auxquels appartient l'utilisateur qu'il envoie.

Quand l'ordinateur client a reçu le TGT, l'utilisateur est authentifié. Le Local Security Authority (LSA) combine le PAC avec les éléments de sécurité locale de la machine pour former un token. L'ouverture de session débute et l'utilisateur peut de charger sont profil et d'accéder aux ressources.

L'examen de ce processus d'authentification et d'ouverture de session permet de comprendre pourquoi il est nécessaire de quitter sa session et ouvrir une nouvelle session afin de bénéficier d'éventuels changements dans droits et permissions.

https://msdn.microsoft.com/en-us/library/windows/desktop/aa446597(v=vs.85).aspx

https://technet.microsoft.com/en-us/library/cc782880(v=ws.10).aspx

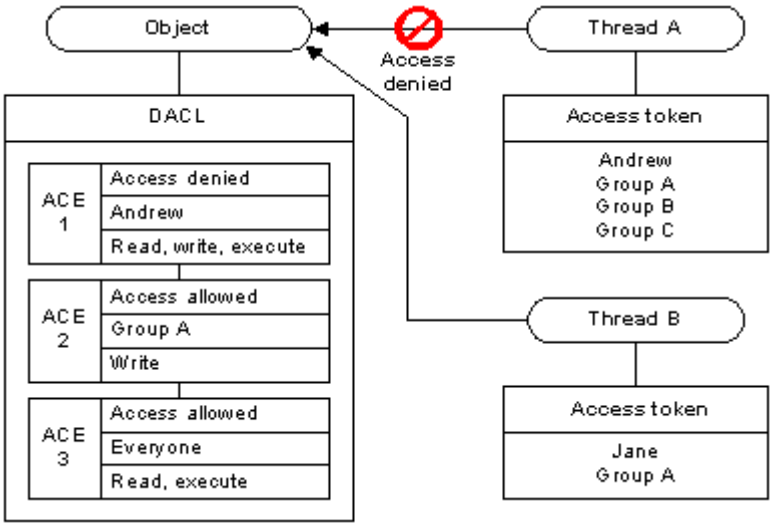
http://serverfault.com/questions/786079/does-active-directory-send-a-users-access-token-across-the-network/786225

13 ACE et DACL

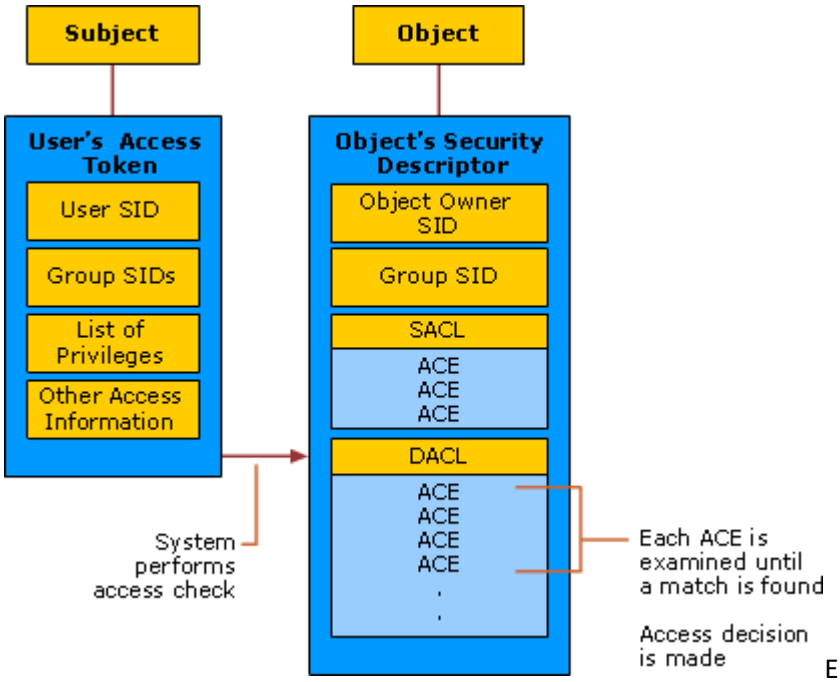
Un des points essentiels de la sécurité est de garantir les accès aux objets uniquement aux utilisateurs autorisés. Pour y parvenir Windows utilise les DACL ou ACL. Il s'agit des (Discretionary) Access Control List qui autorisent ou non l'accès à un objet.

En l'absence de DACL sur un objet, tout le monde dispose du full access sur cet objet.

Si un DACL est présent mais qu'il ne contient aucun ACE (Access Control Entries) qui sert à explicitement autoriser des accès, personne ne peut accéder à l'objet.



Si un DACL est présent et qu'il est accompagné d'ACE, l'accès se fait en fonction des ACE. Les ACE sont des couples : utilisateur (ou groupe) et permission (ou interdiction). Les ACE servent donner essentiellement à autoriser l'accès (allow). L'interdiction (deny) est utilisée par exemple pour retirer l'accès à un ou deux membres d'un groupe.



Enfin, les SACL (system access control list) servent à contrôler les tentatives d'accès aux objets. Elles ont donc un rôle d'audit, de surveillance.

14 Partage et Permissions NTFS de base

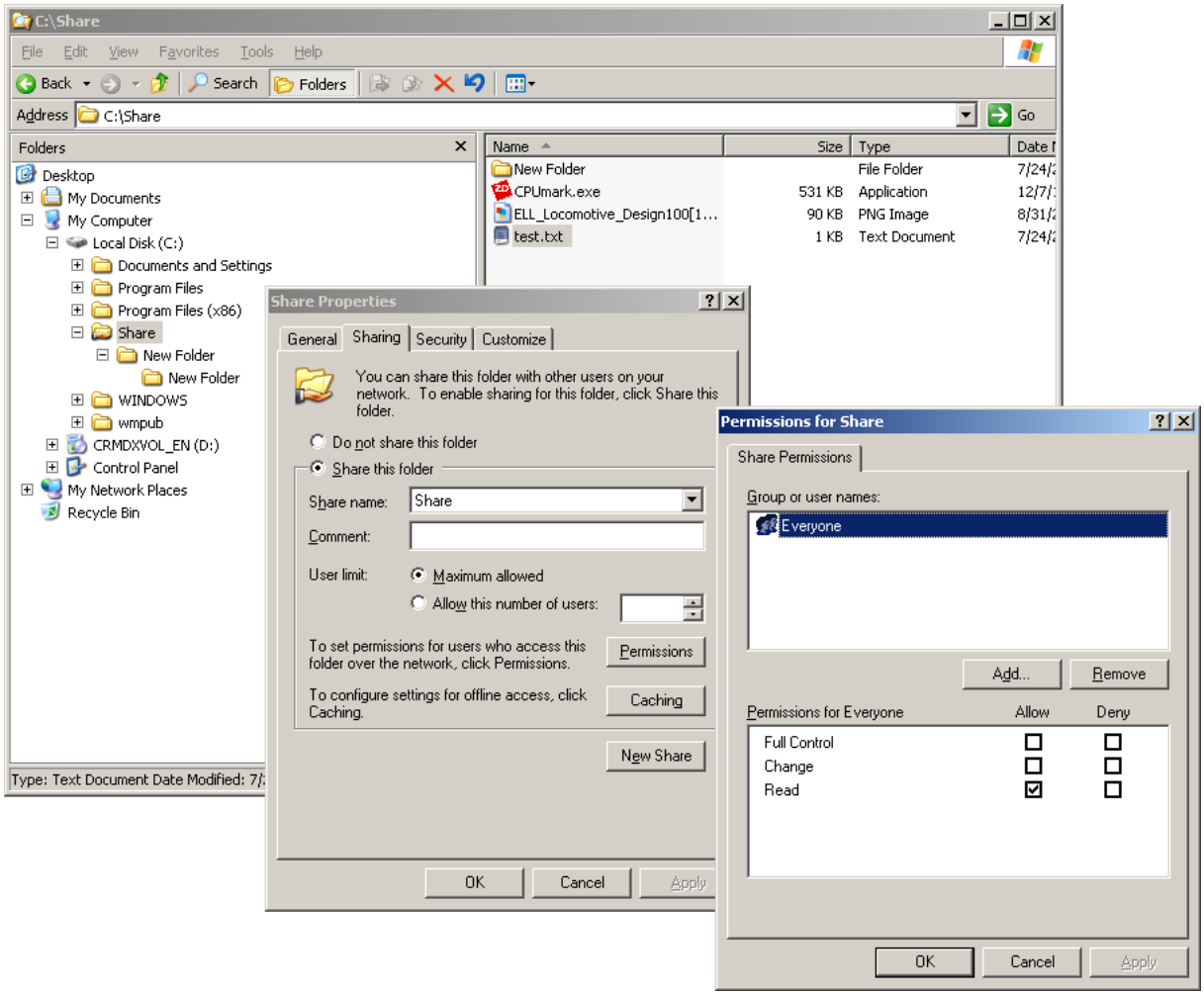
14.1 Partage (share)

Un partage est une ressource rendue disponible via le réseau comme une imprimante, une unité optique, un disque, un dossier, etc. L'accès à une ressource partagée se fait via le chemin UNC (Universal Naming Convention). Exemple \\serveur1\partage

- *serveur1* est l'ordinateur proposant le partage
- *partage* est le dossier partagé

Par défaut, Windows propose d'utiliser le nom du dossier pour le partage. En ajoutant un $ à la fin du nom de partage, Share$, le dossier ne fera pas visible par défaut. Il faudra donner le chemin d'accès \\server\share$ pour y accéder. Ce type de partage s'appelle un partage administratif, il est utilisé pour partager des dossiers que les utilisateurs n'ont pas besoin de voir.

Le point de partage est une porte d'entrée avec seulement trois permissions : Read, Change et Full control. Par défaut, Windows propose de faire le partage pour Everyone, c'est-à-dire « tout le monde ». Il existe un héritage automatique des permissions du parent aux enfants.



Read : consulter et utiliser

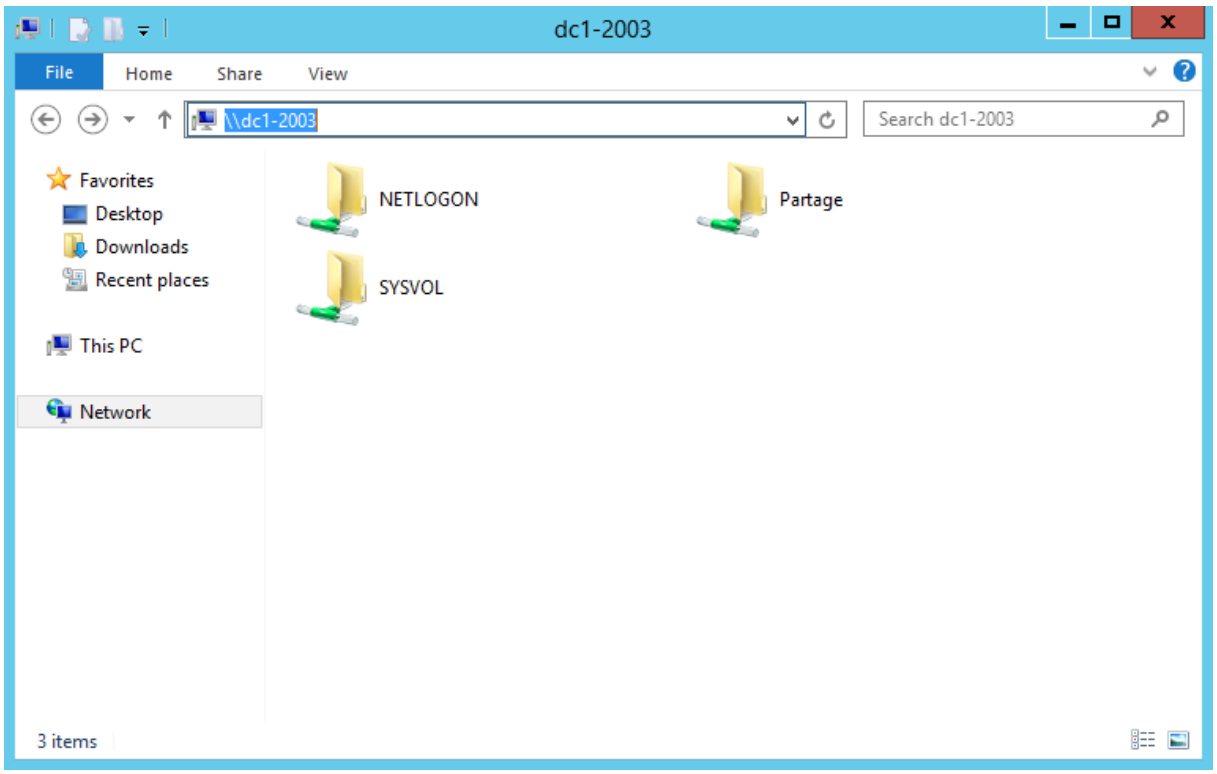
- Permet de : lire le contenu de fichier, exécuter un programme, aller dans un (sous) dossier.
- Ne permet pas : de renommer un fichier/dossier, d'effacer un fichier, de changer le contenu d'un fichier/dossier, de créer un nouveau fichier/dossier, de changer les permissions

Change : Read (consulter et utiliser) + créer, modifier et effacer

- Permet en plus de : créer des fichiers/dossiers, renommer des fichiers/dossiers, changer le contenu de fichier, effacer des fichiers/dossiers.
- Ne permet pas : de changer les permissions.

Full Control : tout faire, y compris changer les permissions

Taper le nom d'un ordinateur ayant des ressources partagées affiche directement ces ressources sauf les partages administratifs. Depuis DC2-2012, taper \\DC1-2003 montre directement Partage (partagé en tant que Partage) mais pas Share (partagé en tant que Share$). NETLOGON et SYSVOL sont des fichiers systèmes partagés. Selon les versions de Windows (Server) l'affichage des partages affiché par \\serveur varie.



14.2 Permissions NTFS de base

Les permissions NTFS s'appliquent… aux disques formatés en NTFS ! Il existe six permissions NTFS de base avec un comportement légèrement différent en fonction de leur application sur un dossier ou un fichier :

Autorisation	Dossier	Fichier
Read	Affiche dossier et sous dossiers	Lire contenu : image, texte, etc.
Write	Créer dossiers	Créer des fichiers
List folder content	Liste et traverse les dossiers	-
Read & Execute	Liste et traverse les dossiers	Voir le contenu et exécuter
Modifiy	Supprimer/renommer dossiers	Supprimer/renommer fichiers
Full Control	Tout + modifier les permissions	Tout + modifier les permissions

Plusieurs principes de base sont à bien conserver à l'esprit lors qu'il est question de permissions !

- Les permissions sont cumulatives (++++)
- Les interdictions ont priorité sur les autorisations (deny > allow)
- Les permissions des fichiers l'emportent sur les permissions des répertoires (file > folder)
- Pas de permission = pas d'accès
- Les permissions qui s’appliquent à un dossier sont héritées dans les sous dossiers.
- L’héritage peut être coupé
- Attention aux permissions nativement attribuée au disque dur !

14.3 Permissions effectives

Les permissions effectives résultent du cumul des différentes permissions attribuées via le partage, les groupes et les éventuelles permissions attribuées directement à l’utilisateur.