Résumé du cours :

Administration de serveurs Microsoft Windows Server 2016

Michaël Margos

Table des matières

1. Module 1 – Les bases des Réseaux

1.1 Intranet / Extranet / DMZ

1.1.1 Les sous-réseaux et leurs classes

Le mot sous-réseau a deux significations. Sa signification ancienne mais plus générale est un réseau (Réseau informatique) physique faisant parti d'un réseau plus global (Internet). Au niveau d'IP, un sous-réseau est un sous-ensemble d'un réseau de classe.

L'utilisation de sous-réseau dans un réseau IP permet de diviser un gros réseau unitaire en ce qui apparaît comme plusieurs sous-réseaux. Cette notion a été introduite avant l'arrivée des classes de réseau dans IPv4, pour permettre à un seul site d'avoir un certain nombre de réseaux locaux. Même après l'introduction des classes de réseau, les sous-réseaux restent utiles pour réduire le nombre d'entrées dans la table de routage pour Internet en cachant des informations sur les sous-réseaux individuels d'un site. De plus, cela a permis de réduire la surcharge réseau, en divisant le nombre d'hôtes recevant des appels broadcast IP.

Le préfix réseau : Le groupe de Bits qui définit l'adresse d'un sous-réseau. Ce groupe est commun à tous les hôtes appartenant à ce sous-réseau.

L'identification de l'hôte : Le groupe de Bits restant, défini l'adresse de l'hôte. Ce groupe est distinct pour chaque hôte appartenant au même sous-réseau.

Le masque d'un sous-réseau : Le masque de sous-réseau est un masque indiquant le nombre de Bits utilisés pour identifier le sous-réseau, et le nombre de bits caractérisant les hôtes (ce qui indique aussi le nombre d'hôtes possibles dans ce sous-réseau).

Les classes des sous-réseaux :

Classe	Bits les plus significatifs	Début	Fin	Masque par défaut en notation décimale	Notation CIDR
A	0	1.0.0.0	127.0.0.0	255.0.0.0	/8
B	10	128.0.0.0	191.255.0.0	255.255.0.0	/16
C	110	192.0.0.0	223.255.255.0	255.255.255.0	/24
D	1110	224.0.0.0	239.255.255.0	255.255.255.0	
E	1111	240.0.0.0	255.255.255.0	255.255.255.0	

1.1.2 Réseau Local

Un réseau local, souvent désigné par l'acronyme anglais LAN de Local Area Network, est un réseau informatique à une échelle géographique relativement restreinte, par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d'entreprise.

Il permet de brancher, dans un rayon limité et sur un seul câble, tous types de terminaux (micro-ordinateur, téléphone, caisse enregistreuse, etc.). Historiquement, le pionnier dans ce domaine est le réseau Ethernet conçu par la société Rank Xerox, puis IBM a lancé son propre système, l'anneau à jeton ou Token Ring dans les années 1980.

C'est toutefois le réseau Ethernet qui s'est imposé, grâce à la simplicité de sa mise en œuvre et à l'augmentation progressive des débits de connexion, passés de 10 Mégabits/secondes, puis 100 Mégabits/s, pour atteindre aujourd'hui 1 Gigabits/s et même 10 Gigabits/s sur les réseaux les plus performants.

Adresses IP	Réseau/Masque	Nombre d'adresses
10.0.0.0 - 10.255.255.255	10.0.0.0/8	16,777,216 (2^{24})
172.16.0.0 - 172.31.255.255	172.16.0.0/12	1,048,576 (2^{20})
192.168.0.0 - 192.168.255.255	192.168.0.0/16	65,536 (2^{16})

Ces sous-réseaux:

- Peuvent utiliser le TCP/IP sans avoir de conflit avec les adresses de l' « extérieur »
- Peuvent attribuer des espaces d'adresses en fonction des besoins de l'entreprise de manière indépendante
- Son protégé de l' « extérieur » car ils ne sont pas connu par Internet
- Ne permettent pas aux hôtes de communiquer directement vers l' « extérieur » mais nécessitent l'utilisation d'un proxy ou d'un routeur
- Sont indépendant des fournisseurs d'accès

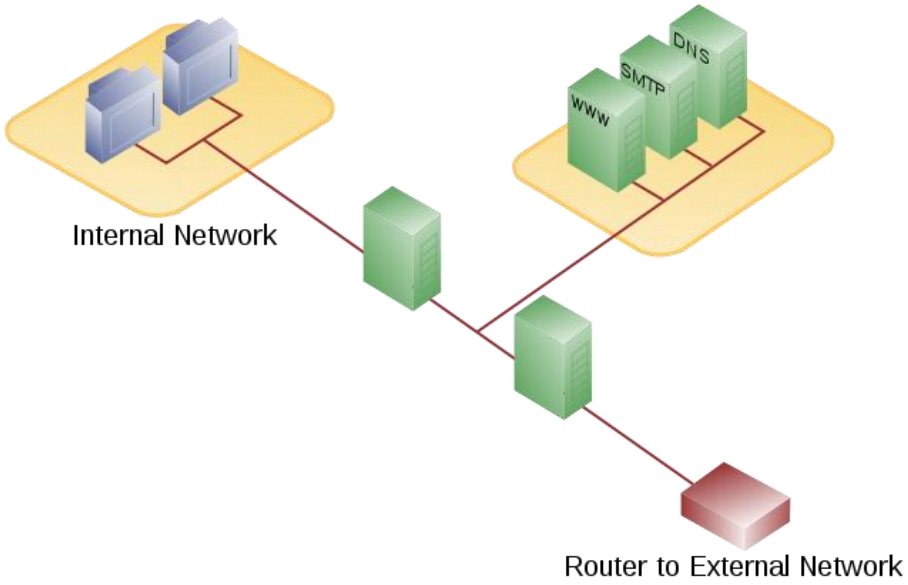
1.1.3 Réseau étendu

Un réseau étendu, souvent désigné par l'anglais Wide Area Network (WAN), est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Le plus grand WAN est le réseau Internet.

1.1.4 Zone démilitarisé

Une zone démilitarisée est un sous-réseau (DMZ) isolé par deux pare-feu (firewall). Ce sous-réseau contient des machines se situant entre un réseau interne (LAN - postes clients) et un réseau externe (typiquement, Internet).

La DMZ permet à ces machines d'accéder à Internet et/ou de publier des services sur Internet sous le contrôle du pare-feu externe. En cas de compromission d'une machine de la DMZ, l'accès vers le réseau local est encore contrôlé par le pare-feu interne.

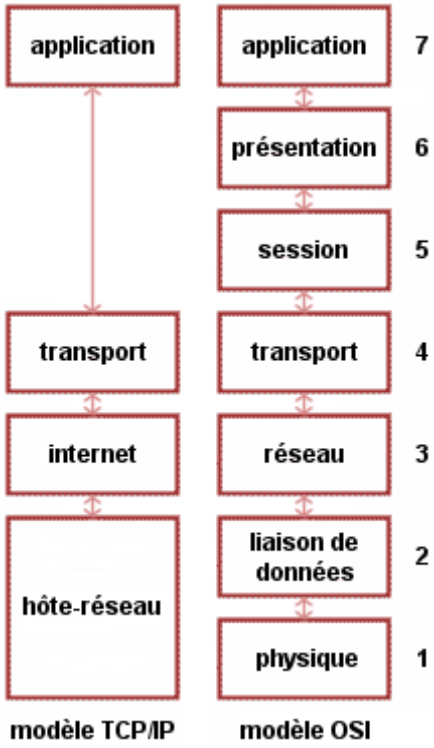


1.2 TCP/IP

1.2.1 Définition du protocole TCP/IP

Transmission Control Protocol/Internet Protocol. Protocole utilisé sur le réseau Internet pour transmettre des données entre deux postes de travail.
Le protocole de transport, TCP prend à sa charge l'ouverture et le contrôle de la liaison entre les deux stations de travail.
Le protocole d'adressage, IP assure le routage des paquets de données.
A voir comme un langage universel permettant à deux postes de travail de communiquer entre eux peu importe leur système d'exploitation.

1.2.2 Les couches du modèle TCP/IP



La couche hôte réseau

Cette couche est assez "étrange". En effet, elle semble "regrouper" les couches physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre à un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

La couche internet

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol).

La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable,

orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là une avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

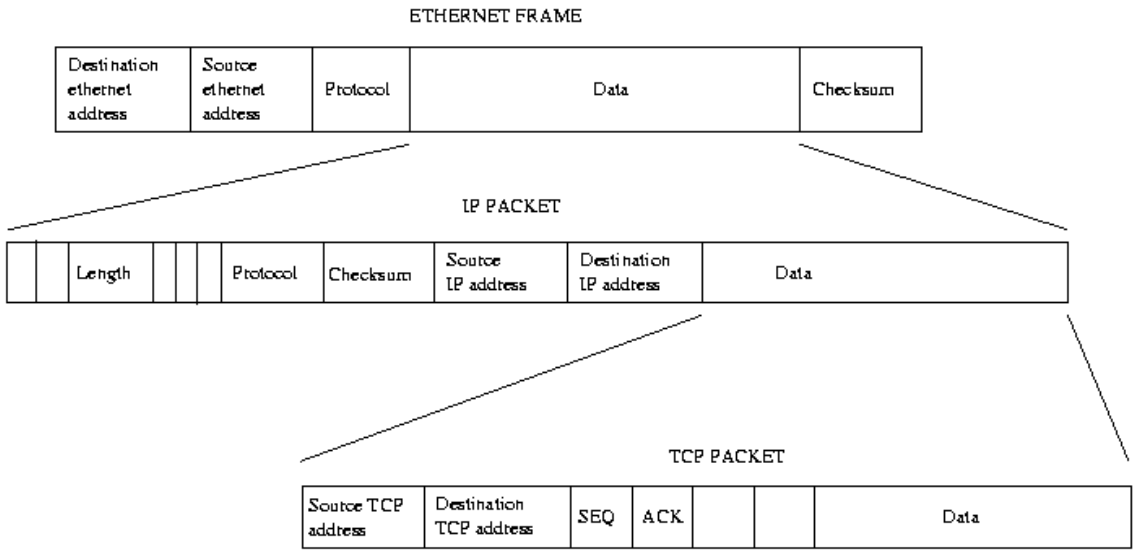
La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs.

1.2.3 La Trame TCP/IP

A titre informatif :



1.2.4 Les ports les plus communs

Les ports à connaitre:

- 22 SSH
- 25 SMTP
- 80 HTTP
- 443 HTTPS
- 3389 RDP

1.3 Domain Name System

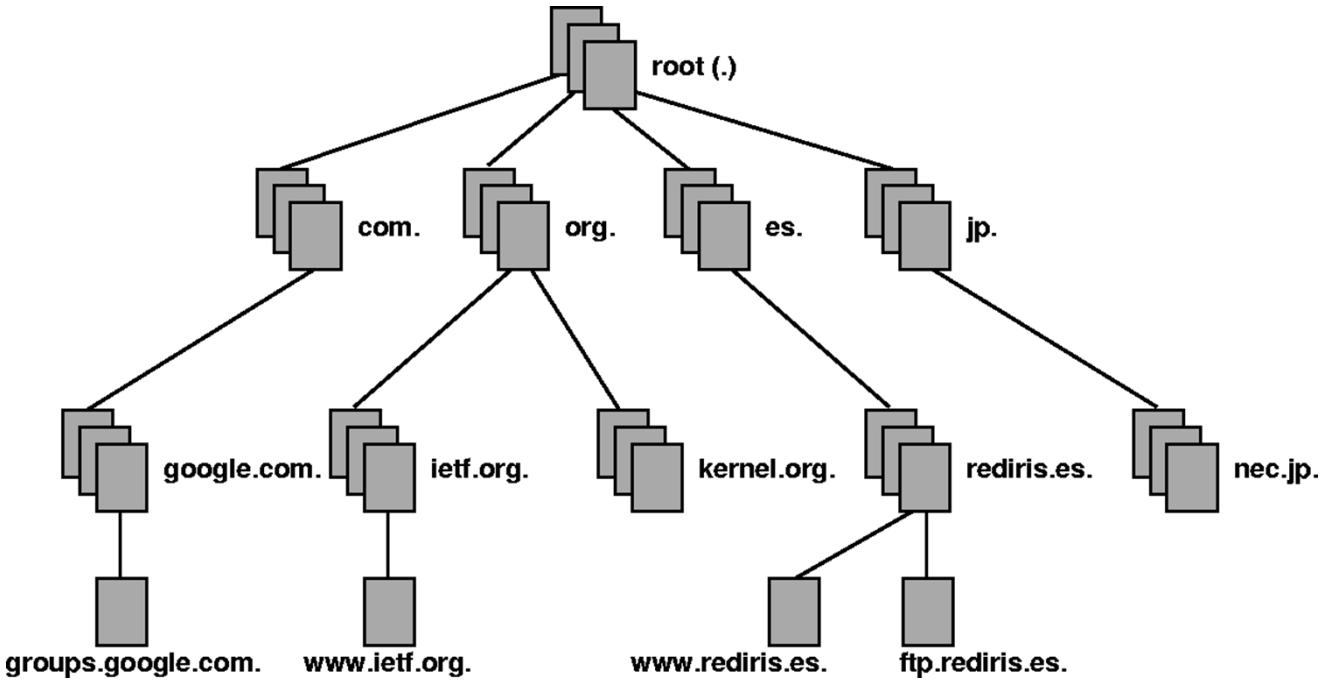
1.3.1 Définition du DNS

Le Domain Name System est un système de nomenclature de type hiérarchique pour les postes de travail, les services ou les ressources connecté à un réseau privé ou Internet.

Le serveur DNS permet d'associer des adresses IP à des noms d'hôtes, et inversement. Chaque domaine doit être défini dans un serveur DNS. Ces serveurs peuvent être interrogés pour associer un nom d'hôte à une adresse IP ou bien pour récupérer les adresses IP des serveurs de noms associés à un nom de domaine (entre autres requêtes possibles).

1.3.2 Comment le DNS fonctionne

Le fonctionnement du DNS ce base sur le Fully Qualified Domain Name (FQDN) qui permet au travers de la hiérarchie de définir la position de l'hôte dans l'arboresence.



1.3.3 Les types d'enregistrements DNS

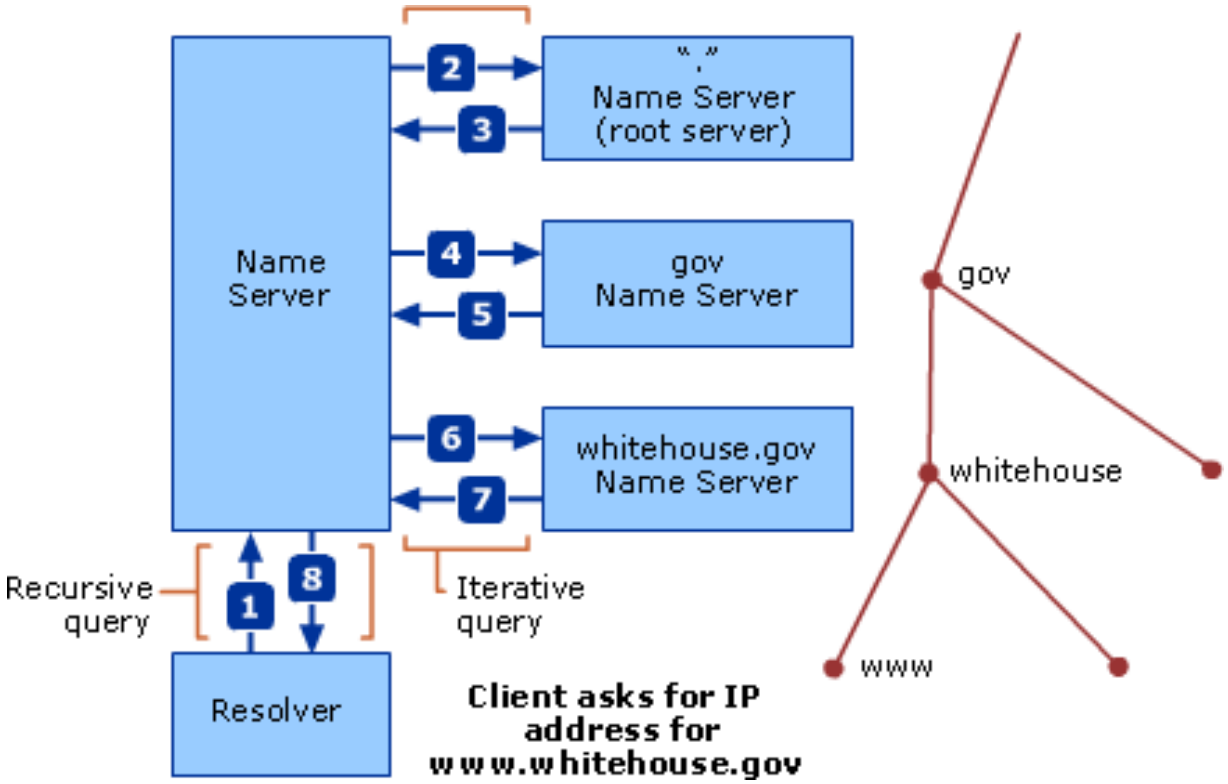
Description	Type	Data
Start of Authority	SOA	Owner Name Primary Name Server DNS Name, Serial Number Refresh Interval Retry Interval Expire Time Minimum TTL
Host	A	Owner Name (Host DNS Name) Host IP Address
Name Server	NS	Owner Name Name Server DNS Name
Mail Exchanger	MX	Owner Name Mail Exchange Server DNS Name, Preference Number
Canonical Name (an alias)	CNAME	Owner Name (Alias Name) Host DNS Name

1.3.4 Les zones DNS

Il existe par défaut trois zones DNS :

- Primaire
- Secondaire
- Stub

1.3.5 Les requêtes DNS



Il existe de types de requêtes DNS :

- Les requêtes Récursives
- Les requêtes Itératives

1.4 Dynamic Host Configuration Protocol

1.4.1 Définition du serveur DHCP

Dynamic Host Configuration Protocol (DHCP) est un terme anglais désignant un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres TCP/IP d'une station, notamment en lui assignant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et des serveurs de noms WINS.

1.4.2 Pourquoi utiliser le DHCP

La conception initiale d'IP supposait la préconfiguration de chaque hôte connecté au réseau avec les paramètres TCP/IP adéquats : c'est l'adressage statique. Sur des réseaux de grandes dimensions ou étendues, où des modifications interviennent souvent, l'adressage statique engendre une lourde charge de maintenance et des risques d'erreurs. En outre les adresses assignées ne peuvent être utilisées même si l'ordinateur qui la détient n'est pas en service.

DHCP apporte une solution à ces deux inconvénients :

- Seuls les ordinateurs en service utilisent une adresse de l'espace d'adressage;
- Toute modification des paramètres (adresse de la passerelle, des serveurs de noms) est répercutée sur les stations lors du redémarrage;

La modification de ces paramètres est centralisée sur les serveurs DHCP.

1.4.3 Les différents termes du DHCP

- Scope : est la plage d'adresses IP que le serveur DHCP va pouvoir attribuer
- Lease : est le temps durant lequel l'hôte va pouvoir utiliser l'IP qui lui a été assigné
- Reservation : est la réservation d'une adresse IP pour un hôte spécifique
- Exclusion : est le fait d'exclure une partie des adresses IP que le serveur peu attribuer
- DHCP relay agent : est un service de relais qui va permettre a des hôtes distant de communiquer avec le serveur DHCP
- Automatic Private IP Addressing (APIPA) : est le système d'attribution d'IP automatique dans le cas où le serveur DHCP est inexistant (169.254.x.x)

1.4.4 Comment le DHCP fonctionne

L'ordinateur équipé de TCP/IP, mais dépourvu d'adresse IP, envoie par diffusion un datagramme (DHCP DISCOVER) qui s'adresse au port 67 de n'importe quel serveur à l'écoute sur ce port. Ce datagramme comporte entre autres l'adresse physique(MAC) du client.

Tout serveur DHCP ayant reçu ce datagramme, s'il est en mesure de proposer une adresse (DHCP OFFER) sur le réseau auquel appartient le client, diffuse une offre DHCP à l'attention du client (sur son port 68), identifié par son adresse physique. Cette offre comporte l'adresse IP du serveur, ainsi que l'adresse IP et le masque de sous-réseau qu'il propose au client. Il se peut que plusieurs offres soient adressées au client.

Le client retient une des offres reçues (la première qui lui parvient), et diffuse sur le réseau un datagramme de requête DHCP (DHCP REQUEST). Ce datagramme comporte l'adresse IP du serveur et celle qui vient d'être proposée au client. Elle a pour effet de demander au serveur choisi l'assignation de cette adresse, l'envoi éventuel des valeurs des paramètres, et d'informer les autres serveurs qui ont fait une offre qu'elle n'a pas été retenue.

Le serveur DHCP choisi élabore un datagramme d'accusé de réception (DHCP ack) qui assigne au client l'adresse IP et son masque de sous-réseau, la durée du bail de cette adresse, deux valeurs T1 et T2 qui déterminent le comportement du client en fin de bail, et éventuellement d'autres paramètres :
adresse IP de la passerelle par défaut
adresses IP des serveurs DNS
adresses IP des serveurs WINS

2. Module 2 – Introduction à la gestion d'un environnement Microsoft Windows Server 2008

2.1 Les rôles d'un serveur

2.1.1 Les différentes éditions Windows Server 2008

Les différentes éditions à retenir:

- Windows Server 2008 Standard
- Windows Server 2008 Enterprise
- Windows Server 2008 Datacenter
- Windows Server 2008 Core

2.1.2 Définition des Rôles

Les rôles d'un serveur définissent sa fonction primaire et peuvent être de différents type tels que :

- Serveur d'Annuaire de Services
- Serveur DNS
- Serveur de Fichiers
- Serveur d'Impression
- Serveur Web
- …

2.1.3 Quels sont les rôles d'infrastructure

Les rôles dédiés à l'infrastructure sont :

- Active Directory Domain Services
- Active Directory Certificate Services
- Active Directory Rights Management Services
- DHCP Server
- DNS Server
- Fax Server
- File Services
- Hyper-V
- Network Policy and Access Services
- Print Services
- Terminal Services
- Windows Deployment Services

2.1.4 Quels sont les rôles applicatifs

Les rôles applicatifs sont :

- Serveur Applicatif
- Service UDDI
- Serveur Web Applicatif

2.1.5 Quels sont les rôles Active Directory

Les rôles de l'Annuaire de Services sont :

- Active Directory Domain Services
- Active Directory Lightweight Directory Services
- Active Directory Certificate Services
- Active Directory Rights Management Services
- Active Directory Federation Services

2.1.6 Intégration de l'AD DS avec les autres rôles Active Directory

Le rôles de l'Annuaire de Services du domaine (Active Directory Domain Services) peut englober les autres rôles de l'Annuaire. Dans la majorité des cas les autres rôles sont dépendant de ce premier.

2.1.7 Fonctionnalités d'un serveur Windows 2008 (Features)

Les Fonctionnalités (ou Features) d'un serveur vont permetre d'installer un service de type applicatif.

Quelques fonctionnalités d'un serveur Windows 2008 :

- .Net Framework
- BitLocker Drive Encryption
- Network Load Balancing
- Failover Clustering
- Windows PowerShell
- …

2.1.8 La version Windows Server 2008 Core

La version Windows server 2008 Core a les particularités suivantes :

- Nombre des rôles/fonctionnalités réduites
- Pas d'interface graphique
- Sécurité accrue

2.2 Aperçu d'un Active Directory

2.2.1 Définition d'un Annuaire de Services du domaine

L'Active Directory est un annuaire au sens informatique et technique chargé de répertorier tout ce qui touche au réseau comme le nom des utilisateurs, des imprimantes, des serveurs, des dossiers partagés, etc. L'utilisateur peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées.

Une arborescence *Active Directory* est composée de :

- La forêt : ensemble de tous les sous domaines *Active Directory*.
- L'arbre : domaine et toutes ramifications. Par exemple, dans l'arbre *domaine.tld*, *sous1.domaine.tld*,*sous2.domaine.tld* et *photo.sous1.domaine.tld* sont des sous-domaines de *domaine.tld*.
- Le domaine : constitue les feuilles de l'arborescence. *photo.sous1.domaine.tld* peut-être un domaine au même titre que *domaine.tld*.

2.2.2 Les avantages de l'Active Directory

Les avantages d'utiliser un Annuaire de Services sont :

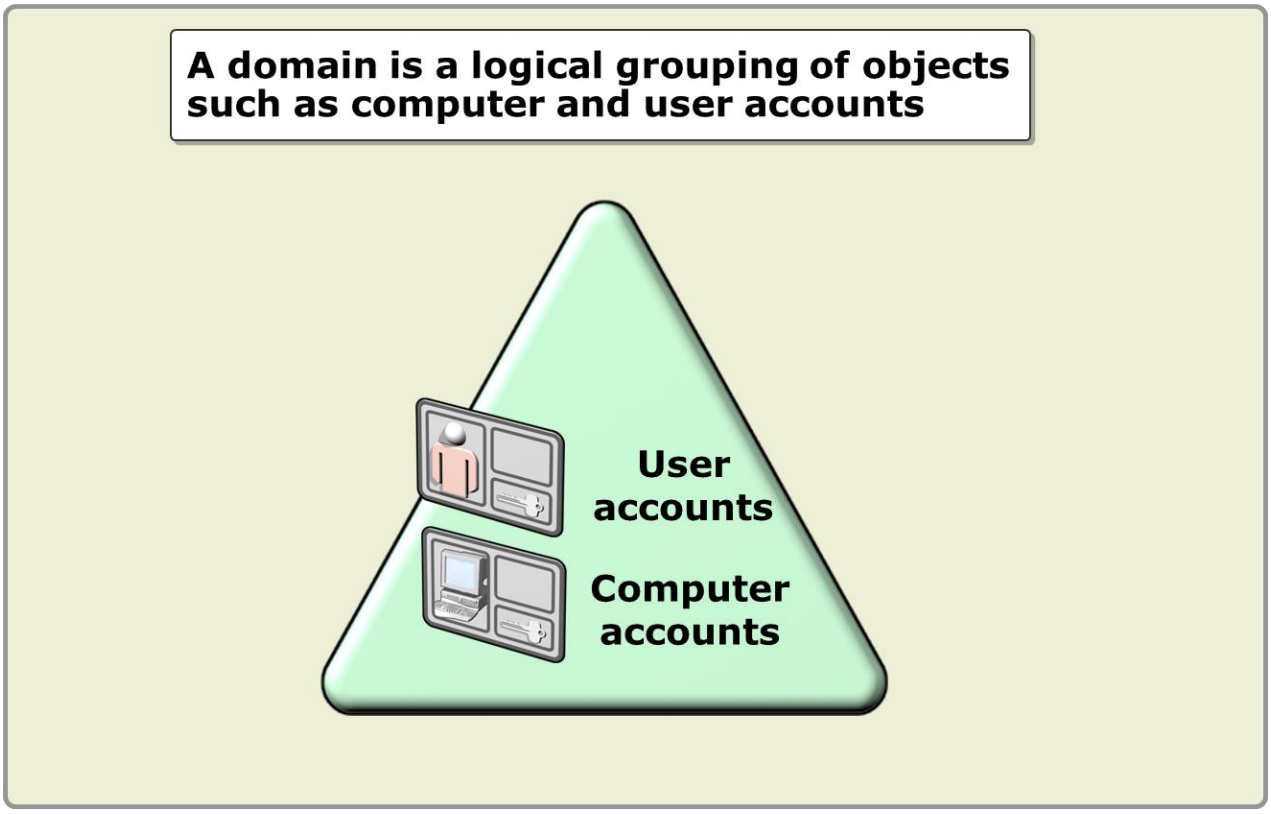
- Simplification de la gestion de la sécurité
- Stockage récurent des informations
- Utilisation des Stratégies de Groupes
- Extensibilité
- Délégation de l'administration

2.2.3 Définition d'un Domaine

Chez Microsoft, un domaine est une entité logique vue comme une enveloppe étiquetée. Il reflète le plus souvent une organisation hiérarchique dans une entreprise. Par exemple, le domaine "COMPTA" désigne l'ensemble des machines réseau (stations, imprimantes, ...) du service Comptabilité, et les comptes utilisateurs qui sont autorisés à s'y connecter.

Le domaine permet à l'administrateur réseau de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données.

Cette base de donnée est stockée sur des serveurs particuliers (Windows Server NT4, 2000, 2003, 2008, 2008R2), appelés Contrôleurs de Domaine (Domain Controller, en anglais).



2.2.4 Définition d'une unité organisationnelle (Organizational Unit OU)

Une Unité organisationnelle (Organizational Units ; OU ; UO) est un objet conteneur qui permet de hiérarchiser l'Active Directory. L'Active Directory permet une hiérarchisation des domaines. À l'intérieur de ces domaines, il existe maintenant des possibilités de structuration et de hiérarchisation des utilisateurs.

Les OU sont le meilleur moyen de créer ces structures hiérarchiques dans Active Directory. Outre la structuration d'informations, qui offre une clarté accrue dans les annuaires complexes notamment, les OU présentent un avantage important : elles tiennent lieu de frontière pour la délégation d'autorisations administratives. Il est donc possible de personnaliser les droits des différents utilisateurs/groupes de façon ciblée (gestion des mots de passe ; droits d'accès : autorisations concernant les installations...).

2.2.5 Définition d'une Foret

Quand vous créez le premier contrôleur de domaine de votre organisation, vous créez le premier domaine (ou domaine racine de la forêt) et la première forêt de celle-ci.

Le conteneur Active Directory situé au niveau supérieur est appelé une « forêt ». Une forêt se compose d'un ou de plusieurs domaines ayant en commun un schéma et un catalogue global.

Une forêt est une limite de sécurité et d'administration pour tous les objets qu'elle contient. Un domaine est une limite d'administration destinée à faciliter la gestion d'objets tels qu'utilisateurs, groupes et ordinateurs. De plus, chaque domaine applique ses propres stratégies de sécurité et relations d'approbation avec les autres domaines.

Plusieurs arborescences de domaine d'une même forêt ne constituent pas un espace de noms contigu : leurs noms de domaine DNS ne sont pas contigus. Si les arborescences d'une forêt ne partagent pas le même espace de noms, en revanche, chaque forêt comporte un seul et unique domaine racine, appelé « domaine racine de forêt ». Celui-ci est, par définition, le premier domaine créé dans la forêt. Les groupes Administrateurs de l'entreprise et Administrateurs du

schéma sont situés dans ce domaine. Par défaut, les informations d'identification d'administration de leurs membres sont à l'échelle de la forêt.

2.2.6 Définition d'un Contrôleur de Domaine

Le Contrôleur de Domaine (Domain Controller) est l'entité physique qui va héberger et gérer l'Annuaire de Services du Domaine (Active Directory Domaine Service) sous forme d'une base de données..

2.2.7 Définition d'un Contrôleur de Domaine en Lecture Seul (Read Only Domain Controller RODC)

Un contrôleur de domaine en lecture seule (RODC) est un nouveau type de contrôleur de domaine du système d'exploitation Windows Server® 2008. Il permet aux organisations de déployer facilement un contrôleur de domaine à des emplacements où la sécurité physique ne peut être garantie. Il héberge des partitions en lecture seule de la base de données des services de domaine Active Directory® (AD DS).

2.2.8 Les Fonctionnalités d'un Contrôleur de Domaine en Lecture Seul

Les contrôleurs de domaine en lecture seule résolvent certains des problèmes qui sont fréquemment rencontrés dans les succursales. Ces emplacements peuvent être dépourvus de contrôleur de domaine. Sinon, ils peuvent avoir un contrôleur de domaine accessible en écriture, mais sans la sécurité physique, la bande passante réseau ou les compétences locales nécessaires à sa prise en charge. Les fonctionnalités suivantes des contrôleurs de domaine en lecture seule atténuent ces problèmes :

- Base de données AD DS en lecture seule
- Réplication unidirectionnelle
- Mise en cache des informations d'identification
- Séparation des rôles d'administrateur
- Serveur DNS (Domain Name System) en lecture seule

3. Création des objets de l'Annuaire de Services

3.1 Gestion des comptes utilisateurs

3.1.1 Définition d'un compte utilisateur

Un compte utilisateur de domaine est un objet utilisateur défini au niveau de l'Annuaire de Service. C'est un compte classique appartenant au domaine et non pas uniquement à la base d'authentification locale du poste de travail. Il permet l'authentification et l'accès a des ressources locales et réseaux.

Les avantages de ce type de comptes :

- Centralisation des comptes pour l'administration
- Permet de dissocier l'utilisateur de son poste de travail
- L'utilisateur peut utiliser le même compte sur plusieurs postes de travail différents

3.1.2 Les noms associés avec les comptes utilisateur de l'Annuaire

Afin de s'authentifier a l'Annuaire de services il existe plusieurs façons de proceder :

- User Logon Name : NomUtilisateur (ex. Gregory)
- User Logon Name (pre-Windows 2000) : NomdeDomaine\NomUtilisateur (ex. WS2K8LAB\Gregory)
- User Principal Name (UPN) : NomUtilisateur@NomduDomaineFQDN (ex. gregory@ws2k8lab.priv)

3.2 Création des comptes des stations de travail

3.2.1 Définition d'un compte de station de travail

Un compte ordinateur de domaine est un objet ordinateur défini au niveau de l'Annuaire de Service. Il va permettre l'authentification des postes de manière centralisé. Il va également donner la possibilité d'utiliser des stratégies de groupes sur ces mêmes postes.

4. Module 4 – Création des Groupes et Unités Organisationnelles

4.1 Introduction aux Groupes

4.1.1 Définition des Groupes

Les groupes sont une collection d'objets, de l'annuaire, similaires de types :

- Utilisateur
- Ordinateur
- Autre groupe

Il existe deux types de groupe:

Groupe de distribution :
Il s'agit d'une implémentation pour les serveurs de mail (par exemple : Microsoft Exchange Server) pour pouvoir envoyer des mails à un groupe d'utilisateur. Il est limité à cette tâche et ne permettent aucune autre action.

Groupe de sécurité :
Les groupes de sécurité permettent deux types de droits qui doivent se corréler entre eux.
Assigner des droits utilisateurs et assigner des autorisations sur des ressources.
Il permet aussi l'envoie de mail au groupe (comme les groupes de distribution).

Qu'il s'agisse d'un groupe de sécurité ou d'un groupe de distribution, tout groupe est caractérisé par une étendue qui délimite son application dans l'arborescence de domaine ou dans la forêt. La limite d'une étendue de groupe est également déterminée par le paramètre de niveau fonctionnel du domaine qui lui est associé. Il existe trois étendues de groupe : universelle, globale et domaine local.

4.1.2 Les niveaux fonctionnels d'un Domaine

- Windows serveur 2000 Mixte
- Windows serveur 2000 Natif
- Windows serveur 2003 Intérim
- Windows serveur 2003 Natif
- Windows serveur 2008
- Windows serveur 2008 R2

4.1.3 Etendue des Groupes Globaux (Global Groups GG)

Étendue du groupe	Le groupe peut inclure comme membres…	Le groupe peut recevoir des autorisations dans…	L'étendue du groupe peut être convertie en…
Globale	Comptes du même domaine en tant que groupe global parent	Les autorisations des membres peuvent être attribuées dans tout domaine	Universelle (s'il ne s'agit pas d'un membre de tout autre groupe global)
	Groupes globaux du même domaine en tant que groupe global parent		

4.1.4 Etendue des Groupes Universelles (Universal Groups UG)

Étendue du groupe	Le groupe peut inclure comme membres…	Le groupe peut recevoir des autorisations dans…	L'étendue du groupe peut être convertie en…
Universelle	Comptes de tout domaine de la forêt où réside ce groupe universel	Tout domaine ou forêt	Domaine local
	Groupes globaux de tout domaine de la forêt où réside le groupe universel		Global (si aucun autre groupe universel n'existe en tant que membres)
	Groupes universels de tout domaine de la forêt où le réside le groupe universel		

4.1.5 Etendue des Groupes Domaine Locaux (Domain Local Groups DL)

Étendue du groupe	Le groupe peut inclure comme membres…	Le groupe peut recevoir des autorisations dans…	L'étendue du groupe peut être convertie en…
Domaine local	Comptes de tout domaine	Les autorisations des membres peuvent être attribuées dans le même domaine que le groupe local parent	Universelle (si aucun autre groupe local n'existe en tant que membre)
	Groupes globaux de tout domaine		
	Groupes universels de tout domaine		
	Groupes locaux du même domaine que le groupe local parent		

4.1.6 L’usage des Groupes

Quand utiliser des groupes avec une étendue de domaine local ?

Les groupes avec une étendue de domaine local vous aident à définir et à gérer l'accès aux ressources à l'intérieur d'un domaine unique. Par exemple, pour permettre à cinq utilisateurs d'accéder à une imprimante spécifique, vous pouvez ajouter les cinq comptes d'utilisateur à la liste d'autorisations de l'imprimante. Cependant, si vous souhaitez ensuite autoriser les utilisateurs à accéder à une nouvelle imprimante, vous êtes obligé de placer à nouveau les cinq comptes d'utilisateur dans la liste d'autorisations de la nouvelle imprimante.

Avec un minimum de planification, vous pouvez simplifier cette tâche d'administration en créant un groupe avec une étendue de domaine local et l'autoriser à accéder à l'imprimante. Placez les cinq comptes d'utilisateur dans un groupe ayant une étendue globale et ajoutez ce groupe à celui qui a une étendue de domaine local. Si vous souhaitez autoriser les cinq utilisateurs à accéder à la nouvelle imprimante, attribuez une autorisation d'accès au groupe qui a une étendue de domaine local. Tous les membres du groupe qui a une étendue globale accèdent automatiquement à la nouvelle imprimante.

Quand utiliser des groupes avec une étendue globale ?

Utilisez des groupes avec une étendue globale pour gérer des objets annuaire qui nécessitent une maintenance quotidienne, tels que les comptes d'utilisateurs et d'ordinateurs. Comme les groupes qui ont une étendue globale ne sont pas répliqués à l'extérieur de leur propre domaine, les comptes situés dans un groupe qui a une étendue globale peuvent être modifiés régulièrement sans provoquer un trafic de réplication sur le catalogue global. Pour plus d'informations sur les groupes et la réplication, voir Mode de fonctionnement de la réplication.

Même si l'attribution de droits et d'autorisations n'est valide qu'à l'intérieur du domaine où elle est effectuée, en appliquant des groupes avec une étendue globale de manière homogène sur les domaines appropriés, vous pouvez consolider les références aux comptes qui ont des objectifs similaires. Ceci permet de simplifier et de rationaliser la gestion des groupes à travers les domaines. Par exemple, dans un réseau qui comporte deux domaines, Europe et Etats-Unis, s'il existe un groupe avec une étendue globale nommé ComptabilitéGL dans le domaine Etats-Unis, il doit également exister un groupe appelé ComptabilitéGL dans le domaine Europe (sauf si la fonction comptabilité n'existe pas dans le domaine Europe).

Il est fortement recommandé d'utiliser des groupes globaux ou universels au lieu de groupes de domaine local lorsque vous définissez des autorisations pour des objets d'annuaire du domaine répliqués sur le catalogue global. Pour plus d'informations, voir Réplication du catalogue global.

Quand utiliser des groupes avec une étendue universelle ?

Utilisez des groupes avec une étendue universelle pour consolider des groupes qui s'étendent sur plusieurs domaines. Pour y parvenir, ajoutez les comptes à des groupes qui ont une étendue globale et imbriquez ces groupes à l'intérieur de groupes qui ont une étendue universelle. Si vous avez recours à cette stratégie, aucune modification apportée à l'appartenance aux groupes d'étendue globale n'affecte les groupes d'étendue universelle.

Par exemple, dans un réseau qui comporte deux domaines, Europe et Etats-Unis, et un groupe d'étendue globale appelé ComptabilitéGL dans chaque domaine, créez un groupe avec une étendue universelle appelé ComptabilitéU, qui aura comme membres les deux groupes ComptabilitéGL, ÉtatsUnis\ComptabilitéGL et Europe\ComptabilitéGL. Le groupe ComptabilitéU peut ensuite être utilisé n'importe où dans l'entreprise. Les modifications apportées à l'appartenance aux groupes ComptabilitéGL individuels ne provoqueront pas la réplication du groupe ComptabilitéU.

L'appartenance à un groupe d'étendue universelle ne doit pas être modifiée fréquemment. En effet, toute modification apportée à ces appartenances de groupe provoque la réplication de toute l'appartenance du groupe sur chaque catalogue global de la forêt. Pour plus d'informations sur la réplication et les groupes universels, voir Sites et catalogues globaux.

4.1.7 L'imbrication de Groupes (Group Nesting)

L'imbrication vous permet d'ajouter un groupe en tant que membre d'un autre groupe. Vous imbriquez des groupes pour consolider les comptes membres et réduire le trafic de réplication.

4.1.8 Stratégies d'imbrication de Groupes Group Nesting Strategie)

Pour une bonne gestion des autorisations sur des objets **Active Directory**, il faut utiliser à bon escient les groupes. Ceci dans le but de dissocier et de prévenir tous problèmes futures, il faut acquérir l'habitude suivante: un objet ou entité d'objet dans un domaine doit posséder un groupe local pour attribuer les autorisations sur cet objet ou entité.

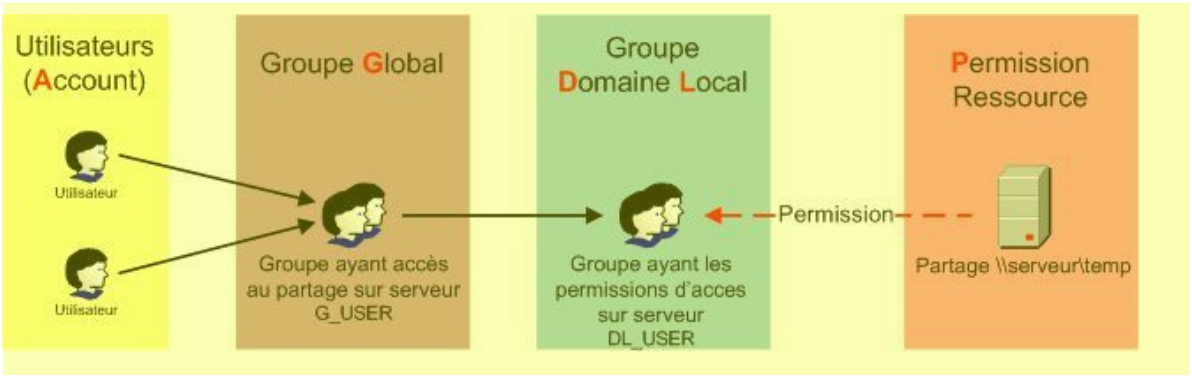
Par exemple: je possède une imprimante qui se nomme '*printercouloir*' et je veux associer un nombre d'utilisateur restreint et spécifique à cette imprimante. Il faut alors créer un groupe '*dl_printercouloir*' (groupe de sécurité avec une étendue locale). Ajouter les membres à celle-ci et attribuer les autorisations pour l'imprimante au nouveau groupe ainsi créé.

Appliquer cette stratégie peut être fastidieux au début mais le gain en maintenance sera conséquent. Par exemple, un an plus tard, une nouvelle imprimante '*printercouloir2*' est ajoutée et vous souhaitez que seuls les utilisateurs qui avaient déjà accès à l'imprimante '*printercouloir*' y aient accès. Très simplement, vous n'aurez à donner que des autorisations au groupe '*dl_printercouloir*'. Si vous aviez donné des autorisations nominativement auparavant, il aurait fallu reprendre chaque membre un par un et donnez des autorisations à chacun.

Ci-dessus a été explicité une partie de la stratégie **A G DL P** (**A**ccount, **G**lobal group, **D**omain Local group, **P**ermission) et **A G U DL P** (**A**ccount, **G**lobal group, **U**niversal group, **D**omain Local group,**P**ermission).

AGDLP

Ce type de stratégie est très efficace seulement dans un domaine restreint (pas de notion de forêt).

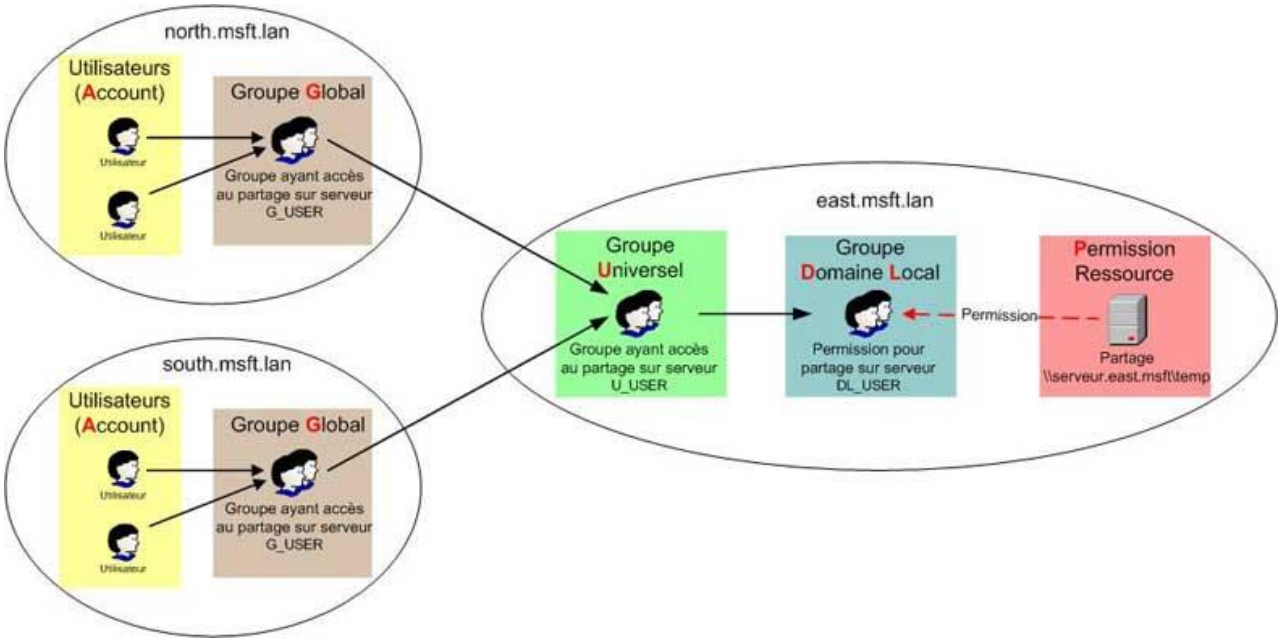


Les tâches à suivre:

1. Ajoutez les utilisateurs dans des groupes de sécurité avec une étendue globale.
2. Ajoutez les groupes globaux à un groupe de sécurité avec une étendue locale qui sera réservée aux permissions de l'objet ou d'une entitée d'objet.
3. Ajoutez les autorisations pour le ou les objets au groupe domaine local précédemment créé.

AGUDLP

Voici la méthode à retenir si vous possédez une forêt Active Directory:



Les tâches à suivre:

1. Ajoutez les utilisateurs dans des groupes de sécurité avec une étendue globale dans chaque domaine où se situe l'utilisateur.
2. Ajoutez les groupes globaux à un groupe de sécurité avec une étendue universelle (ceci pour limiter le traffic lors de la réplication de la forêt **Active Directory** si vous effectuez des modifications de permission)
3. Ajoutez le ou les groupes universels à un groupe de sécurité avec une étendue locale qui sera réservée aux permissions de l'objet ou d'une entitée d'objet.
4. Ajoutez les permissions pour le ou les objets au groupe local précédemment créé.

4.1.9 Groupes Membre et Membre de

Afin d'identifier l'appartenance d'un group il existe deux onglets dans les propriétés du group :

- Membre qui définit les membres (objets) appartenant à ce group
- Membre de qui définir a quels autres il appartient

4.2 Création des Unités Organisationnelles

4.2.1 Définition de la Hiérarchie d'une Unité Organisationnelle

Les Unités Organisationnelles (OU) ont la particularité de pouvoir être crée de manière hiérarchique afin de facilité l'administration de celles-ci.

4.2.2 Exemples d'hiérarchies

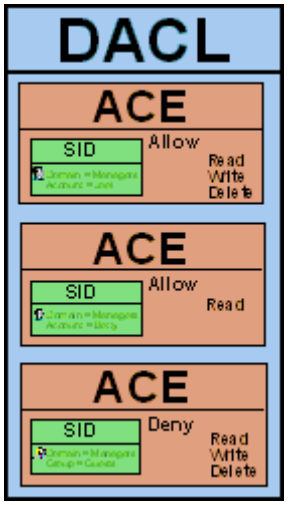
Example	Benefit
Geographic OUs	• Can be administered at the location level
Departmental OUs	• Delegation by job function
Resource OUs	• Designed to manage resource (nonuser) objects
By management	• Build OUs around the administration of the business

4.2.3 Résumé des UO et des Groups

OU	Groupe
Vous pouvez appliquer directement une GPO sur une OU	Vous ne pouvez pas appliquer directement une GPO sur un groupe
Un utilisateur ne peut appartenir que a une seule OU à la fois	Un utilisateur peut appartenir à plusieurs groupes simultanément
Vous ne pouvez pas utiliser une OU pour attribuer ou refuser des permissions a des ressources	Les groupes sont utilisés pour autoriser ou refuser les permission aux ressources
Vous ne pouvez pas utiliser une OU pour distribuer du courrier e-mail	Vous pouvez utiliser les groupes afin d'envoyer du courrier e-mail

5. Module 5 - Gestion des Accès aux ressources dans l'Annuaire

5.1 Les contrôles d'accès



SID (Security IDentifier) : chaque objet entité de sécurité (utilisateur, groupe et ordinateur) aura un identificateur de sécurité qui sera unique dans une forêt Active Directory. Cet identificateur est automatiquement créé lors de la création de l'entité de sécurité. Ce numéro unique est composé du SID du domaine + d'un RID défini par la maître RID du domaine.

ACE (Access Control Entrie) : un ACE est un couple : un SID et une permission

DACL (Discretionary Access Control List) : c'est une liste d'ACE pour un objet. Tout objet dans Active Directory possède une DACL. C'est grâce à celle-ci qu'on autorise ou non une entité de sécurité. Toute entité de sécurité non listé dans cette DACL aura de suite un accès refusé.

SACL (System Access Control Lists): cette liste d'ACE est particulière et très peu utilisé. Elle permet d'auditer un certain nombre d'événements (sécurité, réseau) sur l'objet d'une ou plusieurs entités. On pourra ainsi déterminer les violations d'accès ainsi que son étendu qu'on souhaite auditer.

5.1.1 Définition des Jetons d'accès (Access Tokens)

Un jeton d'accès ou jeton de sécurité identifie le contexte de sécurité d'un processus ou plus précisément d'un thread.

Pendant l'ouverture de session interactive/non-interactive, un jeton de sécurité est créé pour représenter l'utilisateur qui se connecte.

Tous les programmes qu'exécute l'utilisateur héritent d'une copie de ce jeton initial.

5.2 Gestion des permissions de fichiers et répertoires NTFS

5.2.1 Définition des permissions NTFS

Vous pouvez contrôler l'accès aux répertoires et fichiers en définissant les autorisations d'accès NTFS. Ces autorisations permettent de définir le niveau d'accès que vous souhaitez accorder à des utilisateurs ou groupes d'utilisateurs spécifiques. Pour empêcher tout accès non autorisé à vos ressources, il est fondamental de configurer correctement les autorisations relatives aux fichiers et répertoires.

Permissions des Fichiers	**Permissions des Répertoires**
Read	Read
Write	Write
Read & Execute	List Folder Contents
Modify	Read & Execute
Full Control	Modify
	Full Control

5.2.2 Définition de l'héritage des permissions

L'héritage des permissions est utilisé afin de facilité les tâches administratives et d'éviter de devoir attribuer des permissions à chaque objet indépendamment. La relation de l'héritage est de type parent/enfant.

5.2.3 Altération des permissions NTFS l'hors d'une copie ou d'un déplacement

Moving within a partition	Does not create a new file - simply updates location in directory. File keeps its original permissions.
Moving across a partition	Creates a new file and deletes the old one. Inherits the target folders permissions.
Copying within a partition	Creates a new file which inherits permissions of target folder.

5.3 Attribuer des permissions aux ressources partagées

5.3.1 Définition d'un répertoire partagé

Un répertoire partagé est un répertoire qui permet l'accès a son contenu au travers du réseau de l'entreprise.

Les fichiers ne peuvent pas être partagés directement mais doivent faire partie d'un répertoire partagé afin de pouvoir y accéder au travers du réseau de l'entreprise.

5.3.2 Définition des répertoires partagés Administratifs

Les répertoires partagés Administratifs sont des répertoires partagés caché. Ils facilitent l'administration ainsi que l'intégration avec l'Annuaire de services.

5.3.3 Les permissions des répertoires partagés

Permission Level	Access
Read	• Allows for viewing of data in files • Allows for subfolder browsing • Programs in the shared folder can be executed • By default, applied to the Everyone group
Change	• All the permissions in the Read category • New files and subfolders can be created • Data in existing files can be modified or removed • Files and subfolders can be deleted
Full Control	• Full permissions included in the Read and Change categories plus permission to change security settings

5.3.4 Les moyens de connexion à un répertoire partagé

Il existe plusieurs manieres de ce connecter a un repertoire partagé.
Les deux plus utilisé sont :

- L'accès direct au travers du réseau (\\nomduserveur\nomdupartage)
- L'accès au travers d'un « mapped » drive, ce qui veux dire que l'on va attribuer une lettre de partition à un partage réseaux. Ce mapped drive sera accessible tels que n'importe quel autre partition du système.

5.4 Détermination des permissions effectives

5.4.1 Définition des permissions effectives

- Les permissions NTFS sont cumulatives (La permission Write englobe la permission Read etc.)
- La permission Deny l'emporte sur les autres permissions
- Les permissions peuvent être appliquées à des utilisateurs ou à des groupes
- Les permissions sur les fichiers passent outre les permissions des répertoires
- Le créateur des fichiers/répertoires et le propriétaire de ces fichiers/répertoires

5.4.2 Les effets de la combinaison des permissions NTFS et des permissions des répertoires partagés

Quand l'on combine les permission NFTS et de partage c'est les permission les plus restrictives qui l'emporte.

Il faut impérativement correctement définir les deux types de permissions afin de donner à l'utilisateur les droits désirés. Dans le cas contraire l'utilisateur ce verra refuser l'accès à ces ressources.

6. Création et Configuration des Stratégies Groupes

6.1 Introduction aux Stratégies de Groupes (Group Policy Object GPO)

6.1.1 Définition de la Gestion de Configuration

La gestion de la configuration est un principe qui consiste à centraliser l'approche administrative de la gestion d'un environnement. Nous allons regrouper les utilisateurs et les ordinateurs afin de leurs appliquer des modifications de manière centralisé et globale sans devoir traiter chaque objet indépendamment.

- Setting : est le paramètre d'une GPO qui va définir une configuration
- Scope : est l'étendue (champ d'action sur les groupes et ordinateurs) d'une GPO
- Application : est le mécanisme d'application de la GPO aux utilisateurs/ordinateurs
- Group Policy : est le conteneur des trois définitions citées ci-dessus

6.1.2 Définition d'une Stratégie de Groupe (Group Policy Object GPO)

Le terme *Stratégie* désigne la configuration logicielle du système par rapport aux utilisateurs.

Les stratégies de groupe ou GPO (Group Policies Object) permettent de configurer des restrictions d'utilisation de Windows où des paramètres à appliquer soit sur un ordinateur donné soit sur un compte utilisateur donné. Il est ainsi possible d'agir sur :

- La définition d'un environnement adapté : Il est possible par exemple de rediriger certains répertoires leurs contenus
- Le déploiement de logiciels : Une automatisation complète de l'installation des programmes sur les postes clients est possible en fonction du profil de l'utilisateur
- L'application des paramètres de sécurité : Le contexte de sécurité de l'environnement utilisateur peut être modifié

Voici un exemple de stratégie de groupe :

- Menu Démarrer et Barre des tâches

1. Suppression du menu Documents dans le menu Démarrer
2. Suppression des Connexions réseau et accès distant du menu Démarrer
3. Suppression du menu Exécuter dans le menu Démarrer
4. Désactivation de la fermeture de session dans le menu Démarrer
5. Désactivation de la commande Arrêter

- Panneau de configuration

1. Désactivation du Panneau de configuration
2. Masque de certaines applications du Panneau de configuration

- Système

1. Activation des quotas de disque
2. Désactivation des outils de modifications du Registre

3. Désactivation de l'invite de commandes

- Internet Explorer

1. Désactivation de la modification des paramètres de la page de démarrage

Une stratégie de groupe et composée d'un objet Active Directory et d'un dossier dont le nom est le SID de la GPO et que l'on trouve dans le répertoire SYSVOL disponible sur chaque contrôleur de domaine. Les GPO ne peuvent être appliquées qu'à des conteneurs : site, domaine ou encore unité d'organisation mais elles peuvent être assignées plusieurs fois à des conteneurs différents. Le contenu d'une GPO sera donc appliqué sur les comptes utilisateurs et ordinateurs contenus dans le conteneur et plusieurs GPO peuvent être liée à un même conteneur.

6.1.3 Les Stratégies de Groupes par défaut

L'hors de la création d'un domaine il y a deux GPO qui sont créés par défaut :

- Domain Group Policy Objet : celle-ci s'applique à l'entièreté des utilisateurs/ordinateurs du domaine
- Domain Controller Group Policy Objet : celle-ci s'applique uniquement aux contrôleurs de domaine

6.1.4 Le champ d'application d'une GPO

Le champ d'application d'une GPO est dépendant de plusieurs paramètres :

- Scope : est la définition des objets contenu dans l'OU sur laquelle la GPO est appliqué
- GPO link : est le lien qui ce crée entre la GPO et l'OU. Tant que ce lien n'existe pas la GPO ne sera pas appliquée à l'OU
- Security group filtering : Nous permet de définir l'application de la GPO de manière plus granulaire au niveau des groupes et utilisateurs (autoriser ou pas l'application d'une GPO sur un utilisateur/ordinateur appartenant à une OU)

6.1.5 Rafraichissement des GPO

Un ordinateur vérifie qu'il utilise la dernière version des GPO toutes les 90 minutes environ (plus ou moins 30 minutes déterminées de façon aléatoire) afin d'éviter que plusieurs ordinateurs fassent des requêtes au contrôleur de domaine en même temps.

En ce qui concerne les contrôleurs de domaines, ils sont réactualisés toutes les 5 minutes. Ce paramètre est configurable dans la GPO elle-même. Vous pouvez forcer le rafraîchissement sur chaque ordinateur en utilisant la commandes suivante :

- gpudate /force

6.1.6 Le résultat d'une GPO (RSoP)

Le Resultant Set of Policy (RSoP) est le résultat final de l'application des différentes GPO sur un utilisateur/ordinateur.

Etant donné que dans une OU nous pouvons appliquer plusieurs GPO il est important de savoir quels sont les paramètres finaux qui serons appliqué.

Il existe pour ce faire plusieurs outils afin de déterminer le paramètre final effectif de la GPO.

6.2 Implémentation des GPO

6.2.1 Les GPO Locales

Les GPO locales sont appliqué avant les GPO du domaine ce qui implique que les GPO du domaine écrasent les paramètres de la GPO locale.

Dans les versions Windows 2000/XP/2003 il n'existe qu'une seule GPO locale.

Dans les versions Vista/7/2008/2008R2 il existe quatre GPO locales :

- Local GPO
- Administrators GPO
- Non-Administrators GPO
- Per-user GPO

6.2.2 Les GPO du Domaine

Les GPO du domaine sont créés au niveau de l'Annuaire de Service et sont stocké sur le contrôleur de domaine sous le répertoire SYSVOL.

Il existe par défaut deux GPO de domaine :

- Domain GPO
- Domain Controller GPO

6.2.3 Création, liaison et édition des GPO

Les manipulations de base d'un GPO sont :

- Création : L'hors de la création de la GPO un nouvel objet va être créé dans l'annuaire de services et va être stocké dans le répertoire SYSVOL du système et ce sur tous les contrôleurs du domaine.
- Liaison : Consiste à lier une GPO a un domaine ou une OU afin que celle-ci y soit appliqué.
- Edition : Consiste à configurer les différents paramètres que nous voulons appliquer au travers de cette GPO.

6.2.4 L'héritage des GPO et leur précédence

L'ordre dans lequel les objets GPO sont appliqués dépend du conteneur active directory auquel sont liés les objets. Ils sont hérités et appliqués dans l'ordre suivant :local, au site, au domaine puis à l'unité d'organisation (Local -> Site -> Domain -> OU -> OU etc.).

Chaque paramètre d'une GPO peut être configuré ou non, s'il n'est pas configuré, un paramètre ne provoque pas de conflit. Cependant si des paramètres configurés entrent en conflit, l'échelle de priorité précédente détermine le paramètre à appliquer. Lorsque plusieurs GPO sont appliqués sur une OU, la GPO la plus élevée (la première) est la plus prioritaire et la dernière, la moins prioritaire.

En cas de conflit dans la configuration des GPO de différents niveaux, par défaut, on appliquera le paramètre de la GPO la plus proche de l'objet. Voici les règles applicables par défaut :

- Dans le cas d'un domaine, les GPO appliquées celui-ci sont héritées de domaine père en domaines fils.
- Dans le cas d'une Unité d'organisation, les GPO appliquées à celle-ci sont héritées d'une unité d'organisation mère en unités d'organisations filles.

Il existe néanmoins des exceptions dans la mesure où pour chaque conteneur (OU ou domaine) les deux options suivantes sont configurables :

- Bloquer l'héritage : Lorsque cette case est cochée, aucune GPO supérieure ne sera héritée par le conteneur en question.
- Ne pas passer outre : Cette exception va empêcher qu'une GPO plus proche de l'objet utilisateur ou ordinateur ne prime sur une GPO plus éloigné.

Dans la mesure où ils sont définis une seule fois pour tout le domaine dans la première GPO, certains paramètres font exception à l'ordre d'application et aux possibilités d'héritage : c'est le cas des paramètres de mots de passe et ceux de verrouillage de compte. Si ces derniers sont définis à un autre emplacement, ils n'auront aucun effet.

6.2.5 Systèmes déconnecté

Dans le cas où un ordinateur du domaine a été déconnecté il appliquera la dernière GPO gardé en mémoire. Aussitôt qu'il ce reconnectera il recevra la mise à jour des GPO du domaine.

6.2.6 Compréhension de l'application effective d'un paramètre

L'application effective d'un paramètre peut prendre effet dès lors ou :

- Une réplication des GPO ce fait entre l'ordinateur et le domaine
- Lors d'un logon/logoff d'un utilisateur
- Lors d'un redémarrage de l'ordinateur
- Lors d'une mise à jour manuelle

7. Les Commandes de Microsoft Windows Server 2008 Core

7.1 Les commandes réseau

7.1.1 Changer le nom de l'ordinateur

La commande utilisée pour changer le nom de l'hôte est :

Netdom renamecomputer NomActuel /newname :NouveauNom

Ex. netdom renamecomputer TOTO /newname :TATA

7.1.2 Changer l'adresse IP

La commande utilisée pour définir une adresse IP est :

Netsh interface ipv4 set address Nomdelinterface static AddresseIP Masque Passerelle

Ex. netsh interface ipv4 set address ''Connexion au réseau locale'' static 192.168.152.50 255.255.255.0 192.168.152.2

7.1.3 Changer le serveur DNS

La commande utilisée pour définir un serveur DNS est :

Netsh interface ipv4 add dnsserver name=Nomdelinterface address=AdresseIpduserveurDNS

Ex. netsh interface ipv4 add dnsserver name="Connexion au réseau locale'' address=192.168.152.10

7.1.4 Rejoindre un domaine

La commande utilisée pour rejoindre un domaine est :

Netdom join NomdelOrdinateur /domain:NomduDomaine /userD:UtilisateurduDomaine /passwordD :MotdePasseUtilisateur

Ex. netdom join TATA /domain:WS2K8LAB.PRIV /userD:Administrator /passwordD:P@ssw0rd

7.1.5 Activer/Désactiver le pare-feu

La commande utilisée pour activer/désactiver le parefeu est :

Netsh advfirewall set NomduProfile state ON|OFF

Ex. netsh advfirewall set all state off

7.1.6 Activer le bureau a distance

La commande utilisée pour activer le bureau a distance est :

Cscript c:\windows\system32\scregedit.wsf /ar 0

7.2 La commande DCPROMO

La commande DCPROMO est utilisée afin de promouvoir un serveur au rang de contrôleur de domaine. Cela implique qu'il obtiendra une copie de l'Annuaire de services dans ca base locale.

Sur une version Windows Core il est possible d'utiliser cette commande de deux manières différentes :

- Via un fichier qui contiendra les paramètres de la commande (dcpromo /unattend :nomduficher)
- Directement spécifier les paramètres via la ligne de commande

Voici un exemple d'un fichier DCPROMO :

```
[DCINSTALL]
UserName=administrator
UserDomain=WS2KLAB.PRIV
Password=P@ssw0rd1
CreateorJoin=Join
DomainNetbiosName=WS2K8LAB
SiteName=Default-First-Site-Name
ReplicaOrNewDomain=replica
ReplicaDomainDNSName=WS2K8LAB.PRIV
DatabasePath="%systemroot%'NTDS"
LogPath="%systemroot%'NTDS"
SYSVOLPath="%systemroot%'SYSVOL"
InstallDNS=yes
ConfirmGC=yes
SafeModeAdminPassword=P@ssw0rd1
RebootOnCompletion=no
```

Voici un exemple de la commande DCPROMO avec les paramètres directement défini dans la ligne de commande :

```
dcpromo /unattend /InstallDns:yes /confirmGC:yes /replicaOrNewDomain:replica /databasePath:"e:\ntds" /logPath:"e:\ntdslogs" /sysvolpath:"g:\sysvol" /safeModeAdminPassword:FH#3573.cK /rebootOnCompletion:yes
```