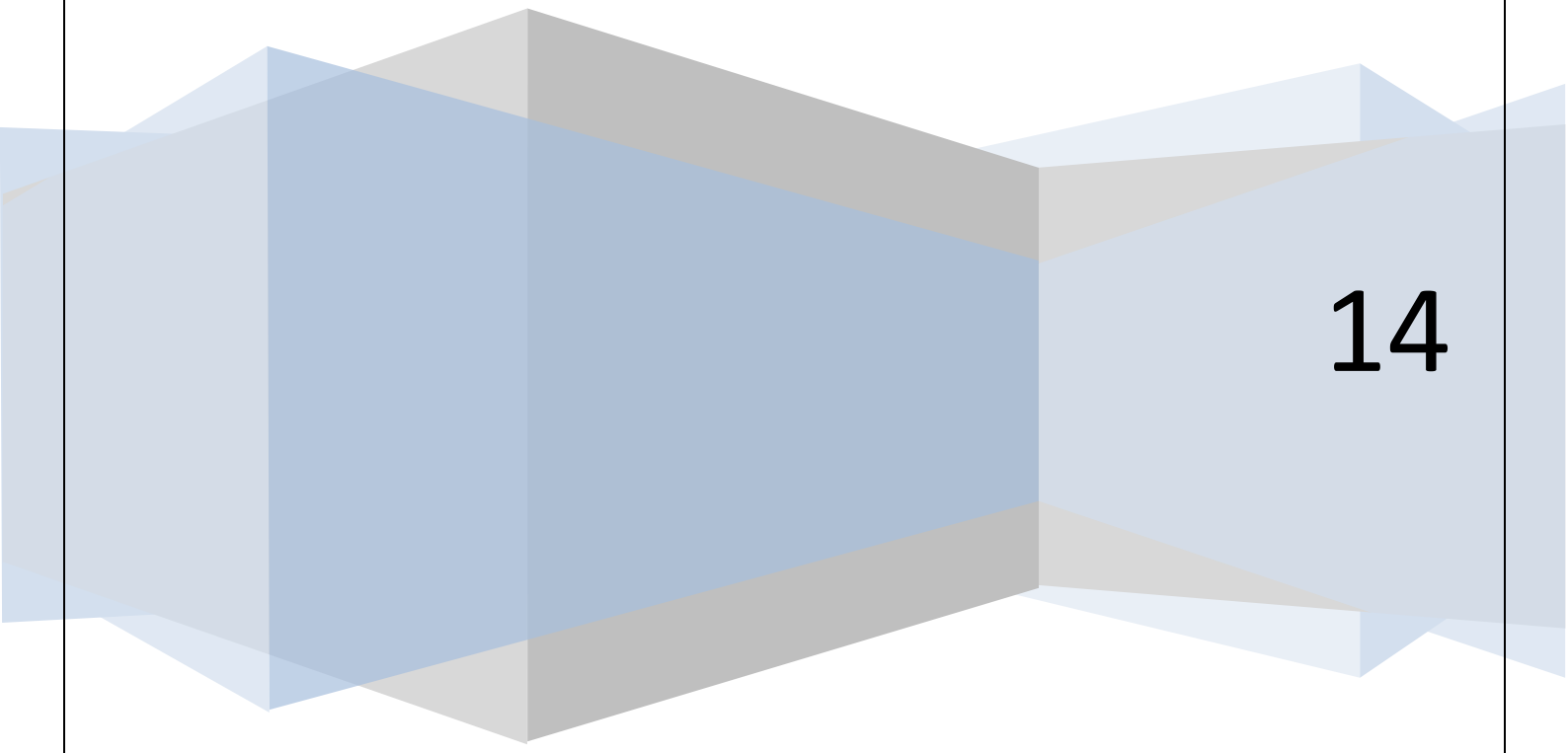
Techniques des Réseaux Informatiques

https://www.facebook.com/groups/2ATRI/

L'Administration d'un Réseau Informatiques sous Windows

2ATRI

Par : Khalid KATKOUT



14

Chapitre 1 : Service DHCP :

I- Généralités :

La saisie manuelle des paramètres de la carte réseau pose assez les problèmes :

- **Temps significatif pour la saisie.**
- **Charge administratif.**
- **Erreurs de la saisie qui posent les problèmes de la communication entre les différentes machines.**

II- Service DHCP :

DHCP (Dynamic Host Configuration Protocole) est un protocole qui permet d'attribuer dynamiquement la configuration des hôtes, il permet d'éviter les problèmes et des erreurs de saisie manuelle et réduit les charges administratives.

III- Installation du serveur DHCP sous Windows 2003 Server :

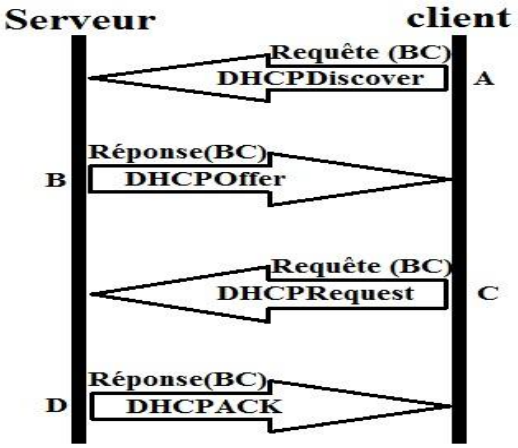
- **Pré-requis : configurer manuellement la carte réseau.**
- **Installer le service Active Directory, le serveur DHCP doit être un membre d'un domaine.**
- **Console « Gérer votre serveur », « Ajouter/Supprimer un rôle ».**
- **« Ajouter des composants Windows », « Mise en service réseau », « DHCP ».**

IV- Configuration du serveur DHCP :

- **Configuration d'une étendue : une étendue est caractérisée par son nom, plage des adresses IP, le masque, la durée de bail, plage des adresses IP à exclure, et autres options (passerelle, DNS…).**
- **Il faut activer le serveur DHCP, et l'étendue.**
- **Les options de DHCP :**
  - **Options étendue : attribuer à tous les clients d'étendue.**
  - **Options de réservation : attribuer aux machines où réserver les adresses IP à la base de leurs adresses MAC.**
  - **Options serveur : attribuer à tous les clients de serveur DHCP.**

V- Processus d'attribution des adresses IP à l'aide du protocole DHCP :

Pour attribuer des adresses IP, un serveur DHCP reçoit un ensemble d'adresses IP qu'il attribue ensuite sur demande à des clients pour une période de temps donnée. En DHCP on appelle bail le fait pour un hôte d'obtenir une adresse IP pour une période de temps définie par le serveur. Le protocole d'acquisition d'un bail comporte quatre messages principaux :



A- Le client DHCP émet en diffusion un premier message de demande de bail. Le type de ce message est baptisé DHCPDISCOVER.

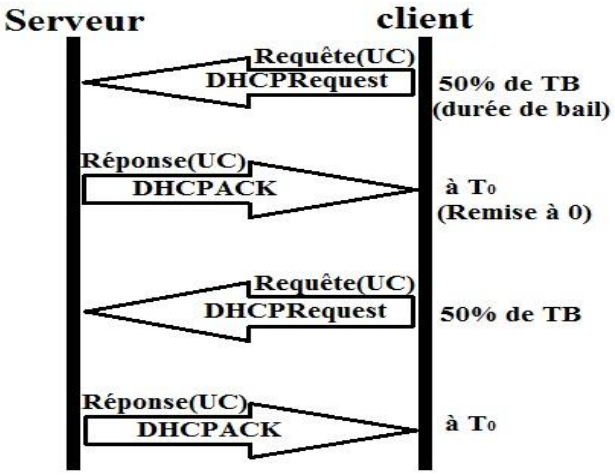
B- S'il existe plusieurs serveurs DHCP atteints par la diffusion et si ces serveurs disposent d'une adresse IP libre, ces serveurs DHCP proposent au client cette adresse IP associée à une durée

d'utilisation possible de l'adresse (une durée de bail). Ce message contient aussi l'adresse IP du serveur proposant l'offre. Le type de ce message de réponse est DHCPOFFER.

C- S'il a reçu plusieurs propositions, le client en choisit une et retourne une demande d'utilisation de cette adresse. Le type de ce troisième message est DHCPREQUEST. Ce message est également diffusé pour que les autres serveurs DHCP apprennent qu'ils n'ont pas été sélectionnés.

D- Le protocole se termine par la transmission d'un message DHCPACK par lequel le serveur DHCP sélectionné accuse réception de la demande et accorde l'adresse selon la durée de bail prévue. Les autres serveurs retirent définitivement leur offre.

VI- Processus de renouvellement :



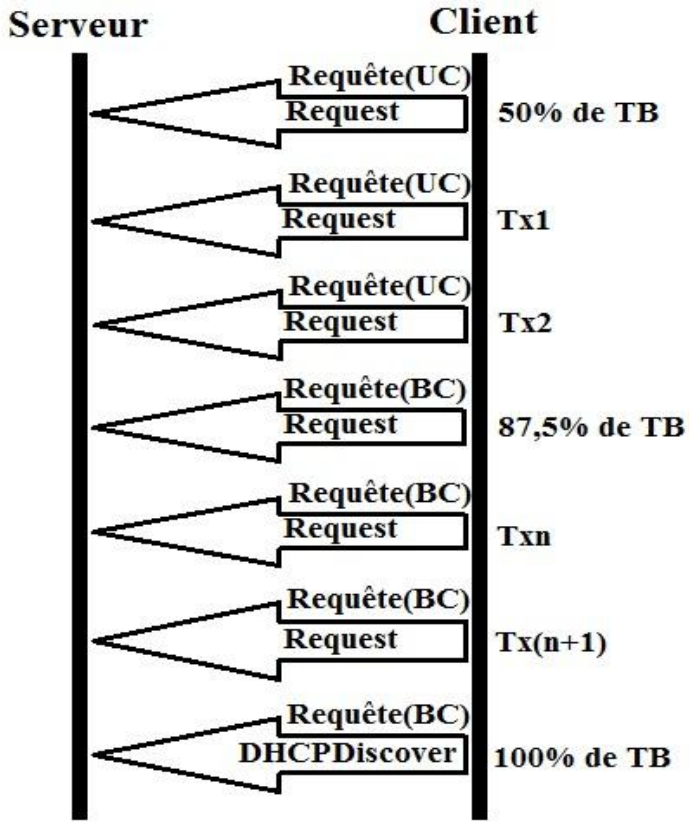
VII- Problèmes : Si une machine est paramétrée pour obtenir une adresse IP automatiquement et qu'elle n'arrive pas à contacter le serveur DHCP !!

Résolution : La machine utilise une adresse IP appartenant à la plage 169.254.0.0/16.

VIII- Problème de renouvellement :

Si la machine à obtenir une adresse IP d'un serveur DHCP, mais durant le processus de renouvellement le serveur DHCP ne répond plus !!

Résolution : La machine libère l'adresse IP et relance le processus demande d'autre adresse IP



Chapitre 2 : Résolution des noms NetBios :

I- Généralité :

Il est difficile pour un utilisateur de travailler avec des adresses IP. La résolution est le processus qui permet d'affecter automatiquement une traduction entre les noms alphanumériques et des adresses IP.

Tout les ordinateurs possèdent deux identificateurs :

- **Nom alphanumérique**
- **Adresse IP**

Dans les systèmes Windows on trouve deux types de noms :

- **Les noms NetBios**
- **Les noms d'hôtes**

Noms NetBios	Noms d'hôtes
Utiliser pour les services NetBios.	Utiliser pour les applications et les services qui utilisent le service DNS pour la résolution.
Taille maximale : 16 caractères (1 caractère pour désigne le service NetBios).	Taille maximale : 256 caractères
Peuvent présenter un ordinateur ou un groupe des ordinateurs.	Peuvent avoir un alias (poste00) ou un nom de domaine (poste00.tri.lan).

II- Noms NetBios :

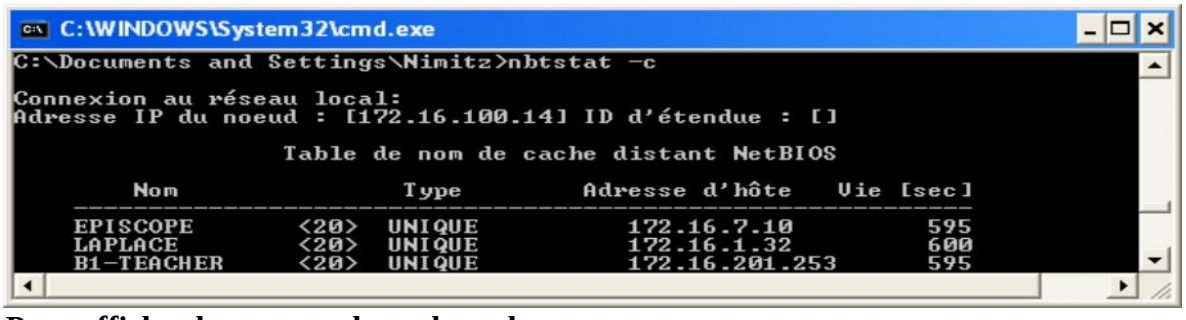
Un Nom NetBios est un nom qui permet d'identifier les services NetBios sur un ordinateur.
L'avantage de l'utilisation des noms NetBios, c'est que lors du processus de résolution, on demande l'adresse IP qui correspond au nom d'une machine qui exécute les services demandés.
Exemple : La requête de résolution demandera le nom NetBios : Poste00 <20>. Donc, on cherche au serveur de fichiers dans une machine nommée « Poste00 », nom seulement l'adresse IP de « Poste00 ».

III- Processus de résolution de noms NetBios :

1. **Lorsqu'une application a besoin de résoudre un nom NetBios, elle recherche dans la cache NetBios.**
2. **Si la cache NetBios ne résout pas la requête, le serveur WINS est alors interrogé.**
3. **Si le serveur WINS ne résout pas le nom NetBios en adresse IP, le client tente de la diffusion au sein du réseau local.**
4. **Si la diffusion n'aboutit à rien, le poste regarde dans le fichier Lmhosts.**
5. **Lorsque le noms NetBios est trouvé, l'adresse IP correspondant est renvoyé à l'application et on stocke l'information dans la cache des noms NetBios.**

IV- La cache de noms NetBios :

La cache est un espace mémoire où on stocke les noms NetBios récemment résolus pendant une durée bien déterminé.



- **Pour afficher le contenu du cache : nbtstat –c**
- **Pour affcicher les noms NetBios : nbtstat –n**
- **Pour vider le contenu de la cache : nbtstat –R**

V- Fichier Lmhosts :

Fichier Lmhosts est un fichier qui se situe dans « C:\Windows\System32\Drivers\etc\Lmhosts.sam », l'action doit le configurer pour mapper les ordinateurs et leurs adresses IP qui se situes on dehors du réseau local.

VI- Noms d'hôtes :

Dans les noms d'hôtes, il y a :

- **Nom : Identificateur du poste dans le réseau.**
- **Nom d'hôtes : Nom DNS d'un périphérique réseau.**

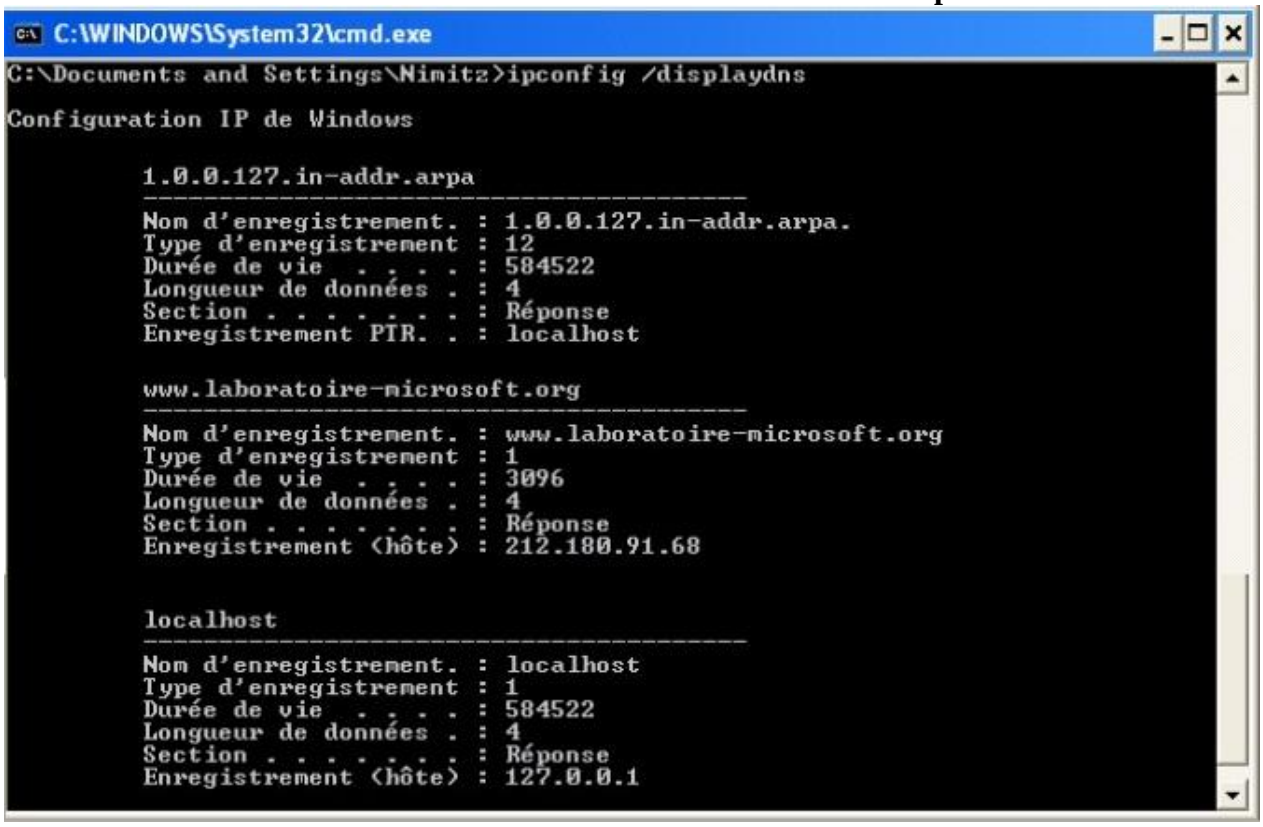
Un nom de domaine pleinement qualifié (*FQDN*) est nom DNS. C'est la forme lisible et hiérarchique du nom complet d'un ordinateur. Le *FQDN* (Fully Qualified Domain Name) définit un nom d'hôte complet (exemple : www.labo-microsoft.com). Il inclut la partie domaine où suffixe (labo-microsoft.com) et la partie hôte (www), ce qui permet la résolution des noms d'hôtes sur Internet. Les noms d'hôtes sont utilisés pour trouver un périphérique réseau sur un réseau.

VII- Processus de résolution de noms d'hôtes :

1. **Si une application ou service veut résoudre un nom d'hôte (navigateur web), elle recherche dans la cache des noms d'hôtes (créé à partir de fichier Hosts et les dernières recherches).**
2. **Si l'entrée n'existe pas dans la cache, le poste client envoi un requête vers le serveur DNS.**
3. **Si ces méthodes de résolution ont échoué et que le nom ne dépasse pas 15 caractères, le poste client passe à la méthode de résolution des noms NetBios.**
4. **Lorsque le nom d'hôte est trouvé, il est renvoyé à l'application et on le stocke dans la cache des noms d'hôtes.**

VIII- Cache de résolution client :

Stocke le contenu du fichier Hosts et les noms d'hôtes résolus récemment pendent une durée TTL.



- **Pour Afficher le contenu de la cache : ipconfig /displaydns**
- **Pour vider la cache : ipconfig /flushdns**

IX- Fichier Hosts :

Fichier Hosts est un fichier texte statique, il sert à stocker des entrées statiques (127.0.0.1 localhost). Toutes les entrées dans ce fichier seront présentées dans la cache sous une durée de vie.

X- TTL (Time To Live) :

Définir le temps de blocages des réponses attribués à partir de la zone dans les caches des machines ayant interrogé la zone.

Chapitre 3 : Serveur WINS:

I- Définition :

Le serveur WINS (Windows Internet Name Server) a été créé pour le but de limiter le trafic de diffusion et de paramétrer la résolution des noms NetBios sur plusieurs segments de réseaux.

II- Composants du service WINS :

- Serveur WINS : Ordinateur qui traite les requêtes d'inscription de noms provenant des clients WINS, inscrit les noms et les adresses IP du client.

- Base de donnée WINS : Stocke et réplique les mappages des noms NetBios aux adresses IP du réseau.

- Client WINS : Ordinateur configurer pour utiliser directement un serveur WINS.

- Agent Proxy WINS : Ordinateur qui contrôle la diffusion des requêtes de noms et réponds au requêtes clients, lorsque les noms n'existent pas dans le réseau, le Proxy communique avec un serveur WINS pour résoudre ces noms.

III- Type de nœud NetBios :

0x1	**B**	**Broadcost**	**Utilise la diffusion pour l'enregistrement et la résolution des noms.**
0x2	**P**	**Peer to Peer**	**Utilise un serveur de noms (WINS) pour la résolution.**
0x4	**M**	**Mixed**	**Utilise la méthode B puis P.**
0x8	**H**	**Hybrid**	**Utilise la méthode P puis B.**

IV- Comment le serveur WINS résout les noms NetBios ?:

1- Le client WINS contacte le premier serveur WINS pour résoudre les noms.

2- Si le premier serveur WINS ne répond pas, le client contacte d'autres serveurs WINS disponibles jusqu'au obtienne une réponse.

3- Si le serveur WINS résout le nom NetBios, l'adresse IP est renvoyée au client.

4- Si aucun serveur WINS ne peut résoudre le nom NetBios, le client avec le type de nœud H tente une diffusion. Si la diffusion a échoué, le client parcourt son fichier Lmhosts local.

V- Comment un client WINS inscrit et libère des noms NetBios ?:

- Au démarrage de l'ordinateur, le service NetBios sur le protocole TCP/IP va envoyer une demande d'enregistrement des noms NetBios à un serveur WINS.

- Un nom NetBios est inscrit de façon temporaire sur le serveur WINS. Le serveur WINS envoi un message au client lors de son inscription pour l'informer de la durée de l'enregistrement TTL. Ce Dernier sera renouveler son enregistrement à la fin du TTL.

- Si le processus de renouvellement n'est pas effectué dans le temps imparti, l'inscription sur le serveur va être supprimée. Le renouvellement est donc nécessaire pour ce type d'enregistrement contrairement aux enregistrements statiques qui n'utilisent pas le TTL.

La durée TTL est par défaut 6 jours.

Chapitre 4 : Serveur DNS :

I- Introduction :

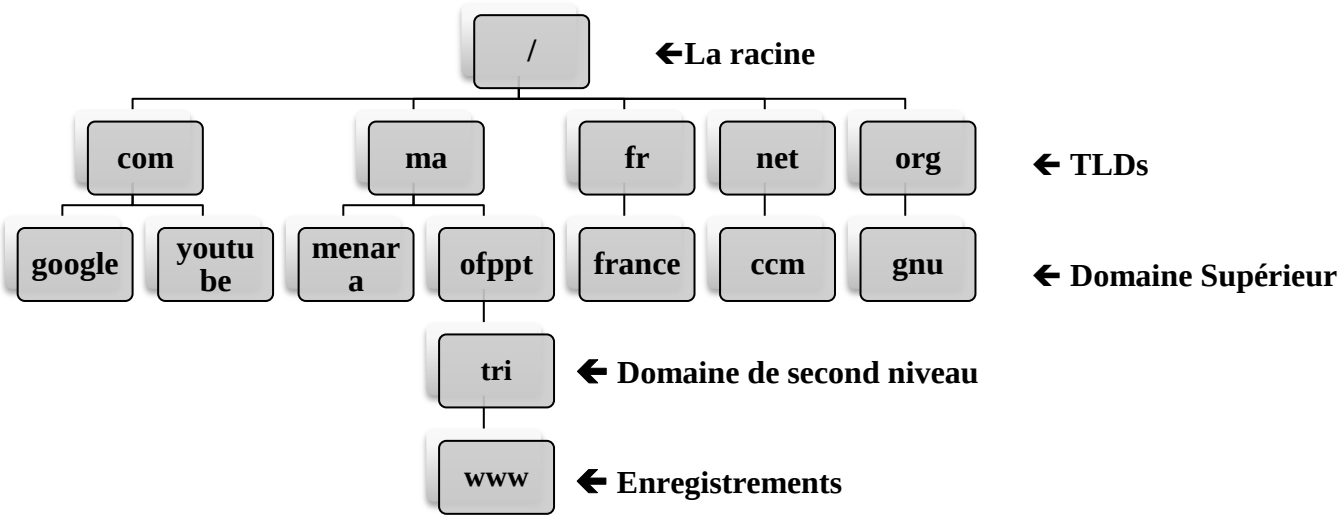
DNS (Domain Name System) est une base de données hiérarchisée distribuée, utilisée sur les réseaux IP pour résoudre et transposer les noms des ordinateurs en des adresses IP. C'est la principale méthode de la résolution des noms d'hôtes.

Le système de noms DNS est une structure hiérarchique et logique appelée espace de nom de domaine.

II- Qu'est ce qu'un espace de nom de domaine DNS ?

La structure hiérarchique de l'espace de noms de domaines est telle que :

- **Domaine Racine : qui se trouve en haut de la structure du noms de domaine, représente par point.**
- **Domaine de niveau supérieur : représente les TLDs (on a 224 TLD comme : com, fr, net …)**
- **Domaine de niveau second : est un nom unique de logueur variable, il est enregistré directement auprès des entreprises.**
- **Sous-domaines : permet à une organisation de subdiviser son nom de domainepar département ou service (exemple : microsoft.supinfo.com).**



Le nom de domaine pleinement qualifié FQDN décrit la relation exacte entre un hôte et son domaine.

III- Types de TLD :

- **gTLD : Generic TLD, caractère générique (com, org, …)**
- **ccTLD : Code Country TLD : représente les pays du monde (fr, ma, …)**
- **iTLD : Infrastructure TLD : c'est l'arpa, utilisé dans les résolutions inverses.**
- **sTLD : Sponsored TLD, sponsorisé par des entreprises, des communautés, … (gov : gouvernement de USA)**

IV- Les propriétés du serveur DNS :

1- Les composants de serveur DNS :

- **Serveur DNS : Ordinateur exécute le serveur DNS**
  Héberge une partie de l'espace de noms
  Fait autorité pour un espace de noms
  Traite les demandes de résolution des noms soumises par les clients.
- **Client DNS : Ordinateur exécute le service client DNS**
- **Enregistrement de ressources DNS : entrée de base de données DNS qui mappe les noms d'hôtes à des ressources.**

2- Les requêtes DNS :

Une requête est une demande de résolution des noms envoyée à un serveur DNS. Il existe 2 types de requête : récursive et itérative.

La requête peut être lancé par client ou par serveur.

- Requête récursive : est un requête envoyée à un serveur DNS dans laquelle le client DNS demande au serveur DNS de fournir une réponse complète.

- Requête itérative : est un requête envoyée à un serveur DNS dans laquelle le client DNS demande au serveur DNS de fournir une meilleure réponse.

3- Les indications de racine :

Les indications de racine sont des enregistrements de ressource DNS stocké sur un serveur DNS qui répertorient les adresse IP des serveurs racines du système DNS.

Ils sont trouvés dans 'cache.dsn' qui se trouve dans le dossier '%systemroot%\system32\dns\'.

4- Les redirecteurs :

Un redirecteur est un serveur DNS que d'autres serveurs DNS internes désignent comme responsable du transfert des requêtes pour la résolution des noms de domaines externes ou hors sites.

5- La mise en cache de serveur DNS :

La mise en cache est le processus qui consiste à stocker temporairement (durant le TTC de la réponse) dans un sous système de mémoire spéciale des informations ayant fait l'objet d'un accès récent pour y accéder plus rapidement ensuite.

V- Les enregistrements et les zones DNS :

1- Les enregistrements des ressources :

Un enregistrement de ressource est une structure de base de données DNS standard qui contient des informations utilisées pour traiter les requêtes DNS.

Il existe plusieurs types des enregistrements de ressources :

- A (Host) : résous un nom d'hôte en adresse IP.

- PTR (Pointeur) : résous un adresse IP en nom d'hôte.

- SOA (Start Of Autority : Début de la description d'une zone) : Premier enregistrement dans tout les fichiers de la zone.

- SRV (Service) : Résoud les noms des serveurs qui fournissent des services.

- NS (Name Server : Serveur de noms) : Identifie le serveur DNS associé à chaque zone.

- MX (Mail eXchange : Chemin pour messagerie) : Identifie le serveur de messagerie à chaque zone.

- CNAME (Canonical NAME : Nom officiel) : Un nom d'hôte qui fait la référence d'un autre nom d'hôte.

2- Les types des zones :

Une zone est un ensemble des mappages de noms d'hôtes à adresses IP.

Il existe différents types de la zone :

- Zone Principale Standard : (Lecture/Ecriture) : Doit toujours être crée en premier pour une nouvelle zone.

- Zone Secondaire Standard : (Lecture seule) : Contient toutes les modifications effectuées sur le fichier de la zone principale. On utilise la zone secondaire pour avoir une tolérance en panne et pour réduire les charges pour la zone principale.

- Zone de Stub : contient uniquement les enregistrements de ressources nécessaires à l'identification du serveur DNS faisant l'autorité pour la zone.

3- La zone de recherche directe et la zone de recherche inversée :

- Zone de recherche directe : c'est une zone utilisée pour résoudre les noms d'hôtes en adresses IP.

- Zone de recherche inversée : c'est une zone utilisée pour résoudre les adresses IP en noms d'hôtes.

Chapitre 5 : Active Directory :

Stocke des informations sur les ressources de tout le réseau et permet aux utilisateurs de localiser, gérer et utiliser ces ressources.
Utilise le protocole LDAP (Lightweight Directory Acces Protocole)

I- Fonctionnalités

- **Organise l'annuaire en section**
- **Espace de stockage central**
- **Sécurité intégrée**

1- Avantages :

- **Réduction du T.C.O.**
- **Administration souple**
- **Évolutivité**
- **Administration simplifiée**

2- Le chemin LDAP comprend :

- **Les noms uniques :**

Identifie le domaine dans lequel est situé l'objet, ainsi que le chemin complet
CN= katkout khalid,OU=Phone Groupe ,DC=Maroc,DC=Casablanca

- **Les noms uniques relatifs :**

Est la partie du nom unique qui permet d'identifier l'objet dans le conteneur.

3- Accès au réseau :

- **Session sur le domaine :**

Le mon de l'utilisateur peut être écris : nom@domaine + password
Le compte utilisateur Є au domaine (est stocké sur le serveur et sur le poste client)

- **Session locale :**

Compte utilisateur = nom d'authentification + password
Le compte utilisateur Є a un groupe
Session locale uniquement (est stocké sur le poste client sur la S.A.M.)

II- Création de compte utilisateur

Pour importer en bloc des comptes utilisateurs utiliser

- **Csvde crée plusieurs comptes utilisateurs. Commande csvde –i –f <*fichier*>**
- **Ldifde crée, modifie et supprime plusieurs comptes utilisateurs**

Attention ne pas mettre de mot de passe sur le fichier d'exportation : il est en clair

- **Format du fichier :**

Cn=katkout khalid, ou=Phone Groupe, dc=Maroc, dc=Casablanca, c=com, user=katkout, katkout@khalid.com, KATKOUT Khalid 512.

- **Attribut valeur**
- **Dn (nom unique) Cn=katkout khalid, ou=Phone Group, dc=Maroc, dc=Casablanca, dc=com.**
- **ObjectClassUser : SAM AccountName katkout**
- **UserPrincipalName katkout@khalid.com**
- **DisplayName katkout Khalid**
- **UserAccountControl la valeur 512 active le compte la valeur 514 désactive le compte**

III- Structure d'Active Directory

1- Domaine :

Est une limite de sécurité : lorsque l'administrateur ne peut administrer que son domaine, à moins qu';il ne soit habilité à intervenir sur les autres domaines.
Est une unité de duplication : les domaines constituent également des unités de duplication. Dans un domaine, les ordinateurs appelés contrôleurs de domaine contiennent un réplica de l'annuaire d'Active Directory. Chaque contrôleur d'un domaine donné est en mesure de recevoir des modifications et de les dupliques vers l'ensemble de ses homologue au sein du domaine.

2- Unité d'organisation : Est un objet conteneur utilisé pour organiser les objets d'un domaine. Une OU peut contenir des comptes d'utilisateur, des ordinateurs, des imprimantes, ainsi que d'autres OU.

- **Hiérarchisation des unités d'organisation :**

- **Par type d'objet**
- **Par type organisationnel**

3- Arborescences : Est une organisation hiérarchique de domaines. Windows 2000 partageant un espace de noms contigus.
Le nouveau domaine est un domaine enfant d'un domaine parent. Chaque domaine enfant à une relation bidirectionnelle transitive avec son domaine parent.
4- Forêts : Comprend une ou plusieurs arborescences. Les forêts ne forment pas un espace de nom contigu. En revanche les forêts partagent un schéma et un catalogue global commun
5- Catalogue global : Est un référentiel d'information qui contient un sous-ensemble d'attributs relatifs à tous les objets d'Active Directory
- Le catalogue global permet de :

- **Trouver des informations Active Directory dans toute la forêt.**
- **Utiliser des informations d'appartenance à des groupes universels pour ouvrir des sessions sur le réseau.**

Un serveur de catalogue global est un contrôleur de domaine qui conserve une copie du catalogue global et qui traite les requêtes qui lui sont destinées. Le premier contrôleur de domaine que vous créez dans Active Directory devient automatiquement le serveur de catalogue global, par la suite on peut rajouter d'autres contrôleurs de catalogue global.
- Activer / désactiver un catalogue global :
Dans la console Site et service Active Directory, dans l'arborescence console, développer le contrôleur de domaine qui va héberger ou héberge le catalogue global.
Clic droit sur NTDS Settings puis Propriété. Activer ou désactiver la case à cocher catalogue global
6- Structure physique d'Active Directory : Dans Active Directory la structure logique est séparée de la structure physique. La structure logique organise les ressources réseau, tandis que la structure physique sert à configurer et à gérer le trafic réseau. Ce sont les contrôleurs de domaine et de sites qui forment la structure physique d'Active Directory.
7- Contrôleur de domaine : Est un contrôleur du domaine exécutant Windows 2000 Server qui stocke un réplica de l'annuaire, gère les modifications et les duplique vers les autres contrôleurs du même domaine. Ils gèrent les ouvertures de session, d'authentification, et de recherche dans l'annuaire.
Les domaines mappent la structure logique de l'organisation.
8- Sites : Est une combinaison d'un ou plusieurs sous-réseaux IP connecté par une liaison haut débit.
Les sites mappent la structure physique du réseau.
9- Gestion de la duplication Active Directory : Implique le transfert et le maintien des données Active Directory entre les contrôleurs de domaine du réseau. AD utilise la duplication multi-maîtresse
Fonctionnement de la duplication : La duplication intervient du fait des changements apportés à AD

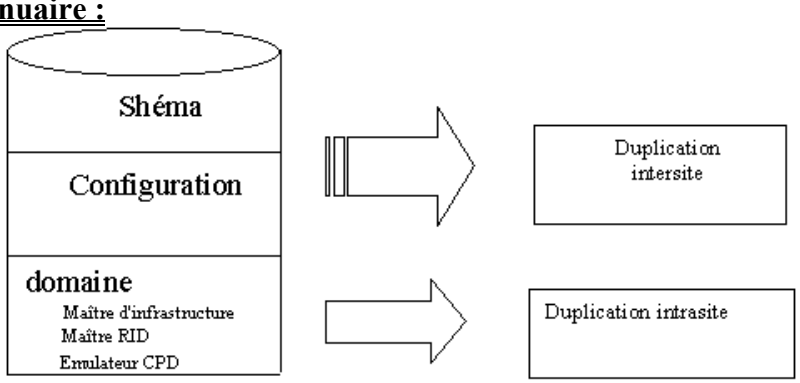
- **nouveaux comptes utilisateurs**
- **changement d'attributs d'objet**
- **suppression d'objet**

la latence de duplication :

- **toute les 5 mn par défaut lors d'une modification**
- **toute les heures en absence de modification**
- **notification immédiate lors de duplication urgente (tout ce qui touche à la sécurité (ex verrouillage de comptes))**

résolution des conflits : la duplication dans AD est conçue sur un modèle à plusieurs maîtres, ainsi tous les ordinateur proposant un mise à jour à plusieurs maîtres doivent gérer les conflits
Pour réduire les conflits, les contrôleur de domaine enregistrent et dupliquent les changements apportés aux objets au niveau des attributs plutôt qu'au niveau des objets. Ainsi les modifications portées à deux attributs différents d'un objet, tels que le mot de passe de l'utilisateur et le code postal, n'entraîneront pas de conflit même s'ils ont été modifié en même temps.
Cachet unique globaux
Il est défini par 3 composants :
a – numéro de version : augmente à chaque mise à jour ; le N° le plus petit est écrasé
b – dateur : date heure système
c – serveur GUID : il identifie le contrôleur du domaine à l'origine de la modification

10- Partition de l'annuaire :



Partition de schéma : Contient la définition de tous les objets et attributs qui peuvent être crées dans l'annuaire, ainsi que les règles de création et de gestion de ces objets et attributs. Elle est dupliquée sur tous les contrôleurs de domaine de la forêt. Il ne peut y avoir qu'un seul schéma dans la forêt.
Partition de configuration : Contient les informations portant sur la structure d'AD , y compris quels domaines et quels sites existent, quel contrôleur de domaine existent dans chacun d'eux et quels services sont disponibles. Elle est dupliquée sur tous les contrôleurs de domaine de la forêt. Il ne peut y avoir qu'une seule partition de configuration dans la forêt
Partition de domaine : Contient des informations concernant tous les objets spécifique au domaine crées dans AD, y compris les utilisateurs, les groupes, les ordinateurs, les OU. Elle est dupliquée au sein de son domaine. Il peut y avoir plusieurs partitions de domaine par forêt
Le serveur de catalogue global : C'est un contrôleur de domaine qui stocke les partitions d'annuaire actualisables ainsi qu'un réplica partiel de partition d'annuaire qui contient un copie en lecture seule des parties d'informations stockées dans cette partition.

- Le vérificateur de KCC : C'est un processus intégré sur chaque contrôleur de domaine qui génère automatiquement la topologie de duplication dans la forêt. Il calcule automatiquement la meilleure connexion possible entre chaque contrôleur de domaine et établi de nouveaux liens en cas de panne. Le KCC ne peut faire que 3 bonds donc il gènère une topologie de duplication automatique pour que le KCC n'ait pas plus de 3 sauts pour que tout les contrôleurs de domaine suivants soient à jour.

- Réplication immédiate : Dans site et service Active Directory, développer Sites, premier site par défaut puis sur serveurs sélectionner le contrôleur de domaine sur lequel à mise à jour à été entreprise cliquer sur NTDS Settings cliquer droit sur l'objet de connexion du partenaire de réplication puis cliquer sur répliquer maintenant ensuite <OK>

- Duplication intersites

On peut planifier manuellement la duplication intersite. Pour optimiser la bande passante on peut on peur compresser le trafic de duplication ce qui augmente le temps processeur du contrôleur de domaine.

- Protocole de duplication

RPC Ø duplication intersites et intrasite
SMTP Ø duplication intersites (préférez RPC)

- Surveillance de duplication

- **Réplication monitor : outils graphique ne peut être exécuté que sur tout contrôleur de domaine, serveur membre ou tout ordinateur exécutant W2K Advanced serveur. Se trouve dans support Tools.**
- **Repadmin : outils en ligne de commande**

Le maître d'opération : est un contrôleur de domaine qui joue le rôle de contrôleur de modification. Il a 5 rôles

- **contrôleur de schéma : Contrôle toute mise à jour apportée au schéma. Le schéma contient la liste des classes d'objets et d'attributs, liste qui sert à créer tout les objets d'Active Directory tels que les ordinateurs les utilisateurs les imprimantes**

Rôle à l'échelle de la forêt. Un seul contrôleur de schéma par forêt

- **maître d'attribution de non de domaine : Contrôle l'ajout ou la suppression de domaine dans la forêt. Le Contrôleur de domaine est aussi serveur de catalogue global. Uu seul maître d'attribution de nom de domaine par forêt.**
- **émulateur CPD : Prend en charge les contrôleurs secondaires de domaines (CSD) exécutant Windows NT en mode mixte. Il est le premier contrôleur de domaine crée dans un nouveau domaine. Met à jour les modifications des mots de passe pour le client antérieur à W2K.**

Réduit les délais de duplication en cas de modification des mots de passe pour les ordinateurs clients W2K. Gère la synchronisation horaire. Elimine les risque d'écrasement des objets GPO.

- **maître d'identificateur relatif (RID) : Attribue des blocs d'identificateurs RID à chaque contrôleur de son domaine. Empêche la duplication d'objets s'ils se déplacent d'un contrôleur de domaine à un autre. Pour afficher l'allocation du pool RID utiliser dcdiag.**
- **Maître d'infrastructure : Mise à jour, dans son domaine, des références à des objets situés dans un autre domaine. La référence à l'objet contient le GUID et éventuellement le SID. Le maître d'infrastructure ne doit pas être sur le même contrôleur de domaine que celui qui héberge le catalogue global. Dans une forêt à un seul domaine il n'y a pas de maître d'infrastructure.**

Le maître d'infrastructure d'un domaine étudie régulièrement le réplica des données de l'annuaire, les références aux objets qui ne se trouvent pas sur ce contrôleur de domaine. Il demande au serveur de catalogue global des informations courantes sur le nom unique et l'identificateur de sécurité de chaque objet référencés.

Gestion des rôles de maître d'opérations :

Lorsqu'on crée un domaine Windows 2000, le système d'exploitation configure automatiquement tous les rôles du maître d'opérations. Il peut être nécessaire de réattribuer un rôle de maître d'opérations un autre contrôleur de domaine dans la forêt ou dans le domaine. Il faut exécuter la procédure ci-desous

- Identifier le conteneur du rôle de maître d'opération : Selon de maître d'opération à déterminer il faut utiliser l'une des console Active Directory

- **Utilisateur et ordinateur Active Directory**
- **Domaine et approbation Active Directory**
- **Schéma Active Directory**

- Identification du maître RID, de l'émulateur CPD et du maître d'infrastructure :

Ouvrir la console Utilisateur et ordinateur AD :

- **Clic droit sur Utilisateurs et ordinateurs AD puis clic sur Maître d'opérations**
- **Clic sur onglet RID , PDC ou infrastructure**

Le nom du maître d'opération actuel s'affiche dans la zone Maître d'opération

- Identification du maître d'attribution de nom de domaine :

- **Ouvrir la console Domaine et approbation AD**
- **Clic droit sur Domaine s et approbations AD puis clic sur Maître d'opérations**

Le nom du maître d'attribution de nom de domaine actuel s 'affiche dans la boite de dialogue Modifier le maître d'opérations.

- Identification du contrôleur de schéma :

- **Enregistrer une MMC Schéma AD en exécutant la commande**

Regsrv32.exe %systemroot%\system32\schmmgmt.dll

- **Cliquer <OK> pour fermer le message indiquant la réussite de l'enregistrement.**
- **Créer un MMC personnalisée**
- **Ajouter le composant logiciel enfichable Schéma AD à cette console**
- **Dans l'arborescence de la console, clic droit sur Schéma AD , puis sur Maître d'opérations**

Le nom du contrôleur de schéma actuel s'affiche dans la boite de dialogue Modifier le maître d'opérations.

Transfert de rôle de maître d'opérations :

Maître d'opération	Groupe autorisé
Contrôleur de schéma	Administrateurs du schéma
Maître d'attribution de nom de domaine	Administrateurs de l'entreprise
Emulateur CPD	Admins du domaine
Maître RID	Admins du domaine

Maître d'infrastructure	Admins du domaine

- Transfert des rôles de maître RID, émulateur CPD et maître d'infrastructure :

- **Ouvrir la console Utilisateur et Ordinateur AD**
- **Dans l'arborescence de la console, clic droit sur Utilisateur et ordinateurs AD , puis clic sur se connecter au domaine**
- **Dans la liste des contrôleurs de domaine disponibles, clic sur le contrôleur de domaine qui devient le nouveau maître d'opérations puis <OK>**
- **Dans l'arborescence de la console, clic droit sur le contrôleur de domaine qui devient le nouveau maître d'opération, puis clic sur Maître d'opérations**
- **Clic sur l'onglet correspondant au rôle de maître d'opération à transférer, par exemple CPD, puis clic sur Modifier.**

Attention : Vérifier que vous ne transférez pas le rôle de maître d'infrastructure dans un contrôleur de domaine qui héberge déjà un catalogue global.

- Transfert du rôle de maître d'attribution de nom de domaine :

- **Ouvrir la console Domaine et approbation AD**
- **Dans l'arborescence de la console, clic droit sur Domaine et approbations AD , puis clic sur Se connecter au domaine**
- **Dans la liste des contrôleurs de domaine disponibles, clic sur le contrôleur de domaine qui devient le nouveau maître d'attribution de nom de domaine puis <OK>**
- **Dans l'arborescence de la console, clic droit sur Domaines et approbations AD, puis clic sur Maître d'opérations**
- **Le nom du contrôleur de domaine que vous avez spécifié s'affiche**
- **Clic sur Modifier.**

Attention : Vérifier que le contrôleur de domaine qui contient le rôle de maître d'attribution de nom de domaine héberge également le catalogue global.

- Transfert du rôle de contrôleur de schéma :

- **Ouvrir la console Schéma AD**
- **Dans l'arborescence de la console, clic droit sur Schéma AD, puis clic sur Modifier le contrôleur de domaine**
- **Clic sur Spécifier un nom, taper le nom du contrôleur de domaine dans lequel transférer le rôle de contrôleur de schéma, puis <OK>**
- **Dans l'arborescence de la console, clic droit sur schéma AD, puis sur Maître d'opérations**
- **Le mon du contrôleur de domaine que vous avez spécifié s'affiche**
- **Clic sur Modifier**

Attention : Vous devez enregistrer la MMC d'administration de schéma, schmgmt.dll avant d'ouvrir AD

Prise du rôle de maître d'opérations :

Le transfert d'un maître d'opération défaillant vers un nouveau contrôleur de domaine doit obligatoirement précédé de la déconnexion physique définitive du maître d'opération en panne
Utiliser la console AD ou la commande ntdsutil pour transférer le rôle.
Prise des rôle émulateur CPD et maître d'infrastructure

- **Ouvrir la console Utilisateurs et ordinateurs AD**
- **Dans l'arborescence de la console, clic droit sur Utilisateurs et ordinateurs AD , puis clic sur Maître d'opérations**
- **Dans la boite de dialogue Maître d'opérations, clic sur onglet du rôle de maître d'opérations à prendre**
- **Clic sur Modifier, puis lorsqu'un message indique qu'un transfert n'est pas envisageable, clic sur <OUI>**
- **Clic sur <OK> dans la page d'avertissement, puis à nouveau <OK> pour effectuer un transfert forcé**
- **Clic sur <OK> pour fermer la boite de dialogue Maître d'opérations**
- **Vérifier que le rôle de maître d'opérations est bien réattribué**

Prise des autres rôles de maître d'opérations

La perte temporaire du contrôleur de schéma, du maître de nom de domaine ou du maître RID n'est pas perceptible par l'utilisateur final et n'a généralement aucune incidence sur votre mission d'administrateur. En cas de panne définitive déconnecter physiquement l'ordinateur0 Et utiliser la commande ntdsutil

- Utilisation de la commande ntdsutil

- **A l'invite de commande taper ntdsutil**
- **A l'invite de ntdsutil taper roles**
- **A l'invite fsmo maintenance, taper connections**
- **A l'invite server connections taper quit**
- **A l'invite fsmo maintenance, taper l'une des commande suivantes approprié**
- **Seize RID master**
- **Seize PDC**
- **Seize infrastructures master**
- **Seize domain naminf master**
- **Seize schéma master**
- **A l'invite fsmo maintenance, taper quit**
- **A l'invite ntdsutil, taper quit**
- **Vérifier que le rôle de maître d'opérations a bien été réattribué**

Défaillance de l'émulateur CPD : A de grave conséquence sur le fonctionnement du réseau

- **perte des modifications des mots de passe pour les ordinateurs antérieur à W2K**
- **perte de la diminution de latence pour la mise à jour des mots de passe**
- **perte de la synchronisation horaire entre contrôleurs**

Défaillance du maître d'infrastructure : N'est pas grave tant qu'elle ne dure pas longtemps

Défaillance des autres maîtres d'opérations

- **ne doit être envisagée qu'en dernier recours**
- **déconnecter l'ordinateur défaillant**
- **utiliser ntdssutil**

IV- Défragmentation de la base de données :

La défragmentation s'effectue automatiquement lors du processus de nettoyage de la mémoire. La défragmentation hors connexion doit être effectuée manuellement. Elle est nécessaire pour créer une version compressée du fichier de base de données d'origine (ntds.dit).

Procédure

a- sauvegarder AD par précaution
b- redémarrer le contrôleur en mode menu d'option avancée de Windows 2000 touche F8 au démarrage
c- sélectionner Mode restauration des services d'annuaire puis <Entrée>
d- ouvrir une session en Administrateur
e- à l'invite taper ntdsutil puis <Entrée>
f- taper files puis <Entrée> ; l'invite revoie Files pour gérer les fichiers de données
g- définir un emplacement ayant un espace disque suffisant pour stocker la base de données compressée : taper compact to <lecteur>:\<répertoire>
h- taper quit (2 fois pour sortir du processus)
i- copier le nouveau fichier ntds.dit sur l'ancien fichier ntds.dit dans le chemin actuel de la base de données d'AD que vous avez noté à l'étape 6
j- redémarrer le contrôleur.

1- Préparation de l'installation d'Active Directory

Configuration requise :

- **Ordinateur exécutant Windows 2000 Server ou +**
- **Espace disque de 200 Mo pour Active Directory et 50 Mo pour les fichiers journaux (création du dossier SYSVOL)**
- **Partition NTFS**
- **Protocole TCP/IP installé et configuré pour utiliser DNS**
- **Privilèges administratifs nécessaires**
- **Création d'un premier domaine (Sous le nom de Premier-Site-par-défaut)**

Lancer l'assistant d'installation :

dcpromo.exe

Choisir le contrôleur de domaine et le type de domaine

Indiquer le nom de domaine, nom DNS, nom NetBIOS

L'emplacement du volume de base, du journal et du volume système partagé.

Autorisations

Mot de passe à utiliser en mode restauration des services d'annuaire

2- Ajout d'un contrôleur de domaine réplica :

La tolérance de panne exige au moins deux contrôleurs de domaine par domaine.

Plusieurs contrôleurs de domaines permettent d'éviter de surcharger le contrôleur de domaine.

Lancer dcpromo.exe et suivre l'assistant

Utilisation d'un script d'installation sans assistance : Un fichier réponse contenant les paramètres requis pour une session d'installation sans assistance. Contient uniquement la section [DCInstall]

Ligne de commande dcpromo /answer : <fichier_réponse>

3- Configuration du service d'annuaire :

- **Opération commune à toutes les installations**
- **Création des entrées de Registre nécessaires**
- **Paramétrage des compteurs de performances pour Active Directory**
- **Configuration du serveur pour enrôler automatiquement un certificat de contrôleur de domaine X509.**
- **Démarrage du protocole d'authentification Kerberos version 5**
- **Paramétrage de la stratégie d'autorité de sécurité locale**
- **Installation de raccourcis vers les outils d'administration dans Active Directory**
- **Configuration des partitions de l'annuaire**
- **Création de la partition d'annuaire de schéma**

Contient le conteneur Schéma, qui stocke les définitions de classe et d'attribut de tous les objets d'Active Directory.

Elle est dupliquée dans tous les contrôleurs de domaine de la forêt

- **Création de la partition de configuration d'annuaire.**

Contient le conteneur configuration qui stocke les objets configuration de l'ensemble de la forêt. Les objets configuration stockent des informations sur les sites, les services, et les partitions d'annuaire.

Elle est dupliquée dans tous les contrôleurs de domaine la forêt.

- **Création de la partition d'annuaire de domaine**

Contient un conteneur de domaine, tel que le conteneur consoto.msft, qui stocke les utilisateurs, les ordinateurs, les groupes et autres objets d'un domaine Windows 2000.

Elle est dupliquée dans tous les contrôleurs de domaine d'un même domaine.

4- Configuration du service d'annuaire :

Démarrage automatique des services :

• Localisateur RPC : Permet aux applications distribuées d'utiliser le service de noms RPC (Remote Procédure Call)

• Ouverture de session réseau : Exécute le service de localisateur de contrôleur de domaine. Crée un canal fiable pour l'enregistrement des ressources SRV dans DNS entre l'ordinateur client et le contrôleur de domaine.

• Centre de distribution des clés : KDC (Key Distribution Center) : gère une base de données avec des informations sur les comptes pour toutes les entités de sécurité dans son domaine.

• Messagerie intersites : ISM (InterSite Messaging) utilisé pour la duplication du courrier intersites Serveur Suivi de liaisons distribuées. Sert à résoudre les raccourcis et les liens OLE vers les fichiers résidents NTFS dont le nom et/ou le chemin ont changé.

• Service de temps Windows : Synchronise les horloges des ordinateurs clients et des serveurs exécutant W2K.

Paramétrage de la sécurité :

Active la sécurité sur le service d'annuaire et les dossiers de duplication des fichiers

Configure des listes DACL sur les fichiers et les objets d'Active Directory

5- Autres opérations d'installation d'Active Directory

• Règle le nom de domaine racine DNS de l'ordinateur
• Détermine si le serveur est déjà membre du domaine
• Crée un compte d'ordinateur dans l'unité d'organisation Domain Controllers
• Applique le mot de passe fourni par l'utilisateur pour le compte administrateur
• Crée un objet de référence croisé dans le conteneur Configuration
• Ajoute des raccourcis
• Crée le dossier partagé SYSVOL (qui contient les stratégies de groupe) et NETLOGON (qui contient les scripts d'ouverture de session des ordinateurs)
• Crée le conteneur Schéma et Configuration
• Attribue des rôles spécifiques au contrôleur de domaine.

6- Vérification après installation

- **Vérification des enregistrements SRV : Utiliser la commande nslookup puis taper : ls –t SRV *domaine,* Ou utiliser l'outils d'administration DNS double cliquer sur le serveur puis sur Zone de recherche directe : si les enregistrements SRV sont inscrits. On trouve les dossiers : _msdcs ; _sites ; _tcp ; _udp**
- **Vérification du dossier SYSVOL et NETLOGON**

Utiliser la commande net share, dans la liste des dossiers partagés on devrait voir NETLOGON racine_système\SYSVOL\domaine\SCRIPTS, SYSVOL racine_système\SYSVOL

- **Vérification de la base de données d'annuaire et des fichiers journaux**

Menu <Démarrer> puis <Exécuter> taper %systemroot%\ntds
L'explorateur de Windows s'ouvre et affiche le contenue du dossier Ntds qui doit comporter les fichiers suivants :
Ntds.dit : il s'agit du fichier de base de données d'annuaire
Edb.* : il s'agit des journaux de transaction et des fichiers de points de vérification
Res*.log : il s'agit des fichiers journaux réservés

- **Vérification des résultats de l'installation par le biais des journaux d'événements**

7- Implémentation de zone de recherche intégrée dans Active Directory
Après l'installation d'Active Directory, intégrer une zone DNS à Active Directory afin que DNS puisse utiliser AD pour stocker et dupliquer les bases de données de zone DNS.
Utiliser DNS pour intégrer une zone DNS à Active Directory :

- **Implémenter une zone de recherche directe : <outils d'administration> <DNS> <zone de recherche directe> puis clic droit sur <Propriétés>**
- **Implémenter une zone de recherche inversée : Idem pour zone de recherche inversée**

8- Publication dans Active Directory
C'est l'action de créer ou rechercher des objets dans AD. Tout objet exécutant W2K est automatiquement publié dans AD. C'est le serveur d'impression qui publie les imprimantes sur AD.
Pour afficher les objets imprimante : Menu Affichage cliquer sur Utilisateurs, Groupes et Ordinateurs en tant que conteneurs.
Pour mettre à jour des imprimantes orphelines utiliser le nettoyeur de disque : Démarrer Programmes Outils systèmes Nettoyeur de disque.
Publication d'une imprimante n'exécutant pas W2K
Avec la console Utilisateurs et ordinateurs Active Directory en faisant : Nouveau puis cliquer sur imprimante taper le chemin UNC (\\serveur\partage\) de l'imprimante ou le script Pubprn.vbs. Taper CSRIPT %systemroot%\system32\pubprn.vbs <*paramètre*s>
Exemple : pour publier une imprimante sur un serveur dans l'OU Sales et le domaine consoto.msft : taper à l'invite
Pubprn.vbs *serveur* « ldap://OU=Sales DC=Consoto, DC=msft »
Définition de l'emplacement des imprimantes
Active Directory repère les imprimantes du sous réseau. En conséquence il faut segmenter le réseau de façon logique pour pouvoir distribuer correctement les imprimantes dans un réseau.
Le nom de l'imprimante est limité à 32 caractères et le nom complet à 260 caractères.
Le nom détaillé peut aider les utilisateurs à repérer géographiquement les imprimantes. On peut ainsi donner dans ce champ des renseignements utiles
Configuration et administration d'un dossier partagé

Publication d'un dossier

Dans la console utilisateurs et ordinateurs Active Directory cliquer droit sur l'OU dans la laquelle vous souhaitez faire le partage, choisir Nouveau puis dossier partagé dans la zone nom taper le chemin UNC du dossier (\\serveur\partage)

9- Délégation du contrôle de l'administration :

Dans la console <Utilisateurs et ordinateurs Active Directory> dans l'OU ou la délégation doit avoir lieu cliquer sur <Action> puis <Déléguer le contrôle> pour ouvrir l'assistant.

10- Suppression d'Active Directory :

L'assistant d'installation permet de supprimer Active Directory.

Lancer : dcpromo.exe