Administration Serveur Windows – sys 24 – cours -

Administration serveur windows 2000 - 2003

Michel Cabaré – Ver 1.0 – Sept 2006-

La formation que vous suivez, à pour but de vous initier avec le logiciel Microsoft Windows NT-2000-XP-2003 (version 4.0-5.x) sur environnement P.C.

Ce Support a pour but de vous fournir un certain nombre d'éléments concernant soit des manipulations, soit des notions théoriques concernant la gestion de réseaux locaux

Il ne peut en aucun cas se substituer à la participation à la formation, ni à tout ou partie de la documentation fournie avec le logiciel.

En effet, **et c'est là sa vocation première**, ce document doit **"servir de support à la prise de notes en formation, et sera donc avantageusement complété par vos soins"**. Son but est de permettre une présentation de vos notes plus structurée et donc plus facilement utilisable ensuite.

Bon Travail

Michel Cabaré

TABLE DES MATIÈRES

SERVICE DNS

Pré-requis des Serveurs DNS

L'implémentation la plus populaire de DNS est **BIND** (Berkeley Internet Name Domain) sous UNIX. En plus des concepts classiques de résolution de nom, pour travailler avec Windows 2000-2003, il faut situer les fonctionnalités suivantes :

DDNS

La méthode utilisée pour ajouter un nouvel enregistrement correspondant à un nouvel ordinateur - un nouveau host en terminologie DNS, dépend de votre logiciel serveur DNS. La plupart utilisent des fichiers ASCII.

Les solutions de serveur DNS les plus récentes n'exigent plus de mises à jour grâce au standard **DDNS** (**Dynamic DNS**) que décrit en détail la RFC 2136. Dans un réseau compatible DDNS, les ordinateurs font d'eux-mêmes les présentations sans qu'un administrateur ne doive intervenir sur le DNS

Enregistrements SRV

Les solutions de serveur DNS les plus récentes gèrent une autre sorte d'enregistrement DNS : les **enregistrements SRV** que décrit en détail la RFC 2052. Ces enregistrements permettent de demander à un serveur DNS si il connaît des machines jouant le rôle de serveur d'un type spécifique

Serveur principal – secondaire (optionnels)

Le serveur DNS peut remplir plusieurs fonctions par rapport à une zone, le serveur chargé de la gestion initiale de la zone est appelé **serveur principal** ou **primary**. mais les informations d'une zone peuvent être répliquées sur d'autres serveurs soit dans un objectif de fiabilité, soit pour un objectif de répartition de charge. Dans ce cas le serveur DNS qui recopie les information depuis le serveur DNS principal s'appelle un **serveur secondaire** ou **backup**. L'édition du fichier de la zone est faite sur le serveur principal qui envoie la version la plus récente du fichier au serveur DNS secondaire. Lorsqu'une machine envoie une requête au serveur secondaire, ce dernier y répond avec sa copie du fichier. Le fichier de zone du serveur secondaire a généralement une durée de vie (généralement de 24 heures). Si le serveur DNS primaire ne met pas à jour le fichier avant la période d'expiration, le serveur secondaire considère l'information comme dépassée. Si votre serveur DNS principal tombe en panne pendant quelques heures, vous n'aurez donc pas de problème. Les serveurs DNS secondaires peuvent être aussi nombreux que l'on le souhaite.

SERVICE DNS WINDOWS

Installer le Service DNS sous 2000-2003 :

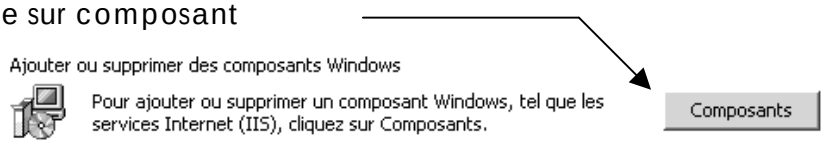
La résolution de nom via DNS ne peut se faire que sur une machine ayant une adresse IP fixe (cette adresse est ensuite rentrée sur chaque « client »)

Pour fonctionner avec Windows 2000-2003, les serveurs DNS doivent

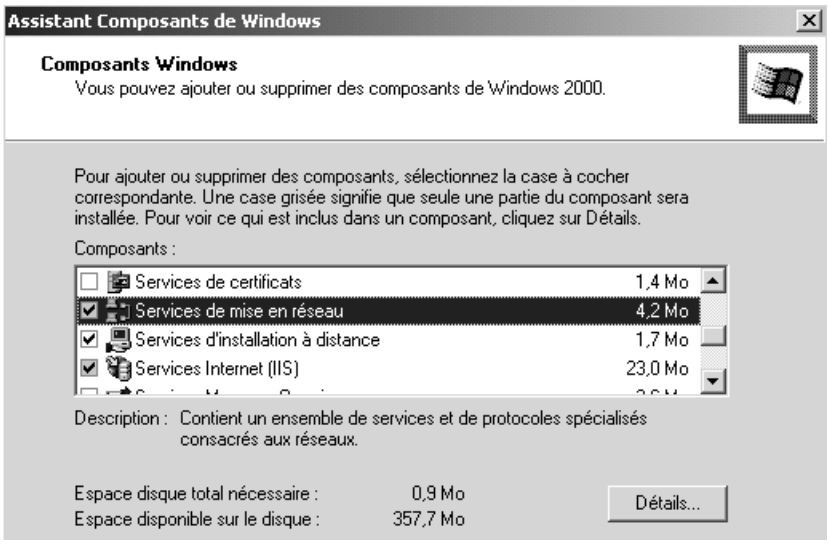
- supporter la RFC 2052 (et ses enregistrements SRV) et la RFC 2136 (DDNS). De nombreuses versions actuelles de DNS (notamment les dernières versions de BIND) les supportent. Le DNS NT4 non.
- accepter les noms de domaine incluant le caractère souligné. De nombreux enregistrements créés automatiquement par AD en comprennent. De nombreuses implémentations de DNS n'acceptent pas les enregistrements DDNS avec des noms comportant le caractère souligné. ! (On peut alors diviser votre domaine DNS existant en 2 zones, placer les serveurs Windows 2000 et NT dans une nouvelle zone avec un serveur DNS Windows 2000, et laisser vos autres machines dans l'ancienne zone.)

Dans le panneau de configuration, on demande **Ajout/Suppression de Programme** dans lequel on demande **Ajouter/Supprimer des composants Windows...(uniquement si on ne l'a pas fait lors du Dcpromo)**

on clique sur composant



dans liste composant Windows on va chercher **Services de mise en réseau**



Détails…

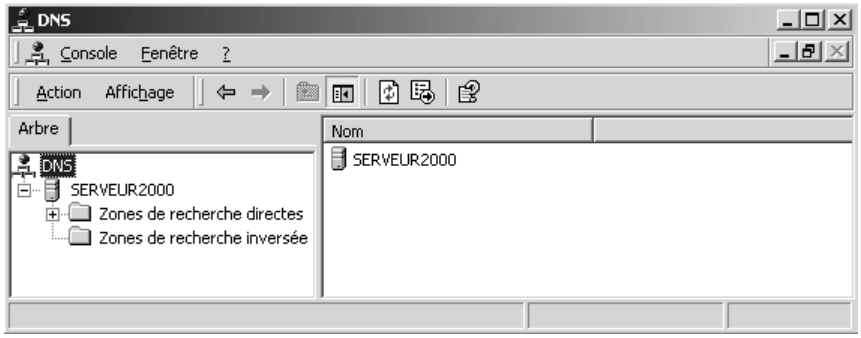
on choisit alors **Système de nom de domaine (DNS)**

N.B : L'installation d'un serveur DNS est obligatoire dans le cadre d'un réseau 2000-2003 et cette opération est requise pour installer Active Directory.

N.B : Le service DNS dans 2000-2003 est de type **Dynamic DNS** (**DDNS**) donc la mise à jour peut être effectuée soit par le client soit par le serveur DHCP qui aurait fournit l'adresse IP au client.

Pour administrer le service DNS on peut aller directement dans le menu

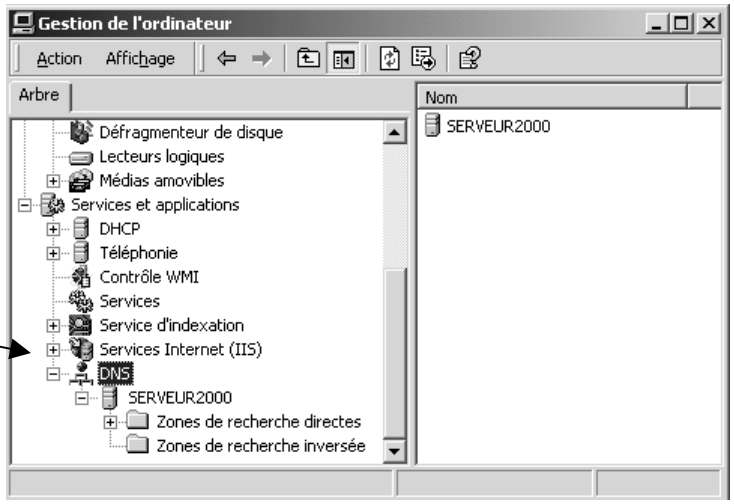
Démarrer / Programmes / Outils d'administration / DNS



ou via

Démarrer / Programmes / Gestion de l'ordinateur

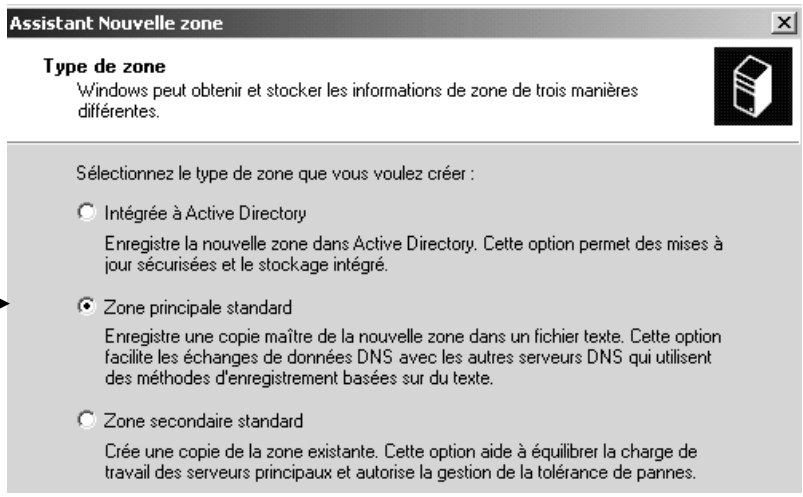
ou l'on retrouve dans **les services** le service DNS...



Définir une nouvelle Zone :

La première chose à faire étant de créer une zone, on fait un clic droit sur le serveur et on demande **nouvelle zone...**

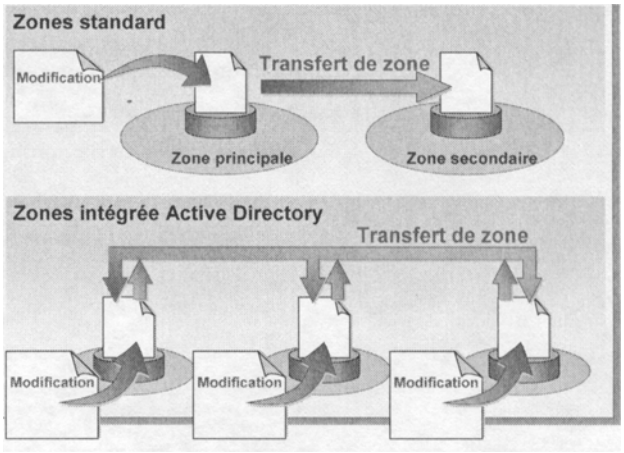
un assistant apparaît nous demandant quel type de zone on souhaite créer



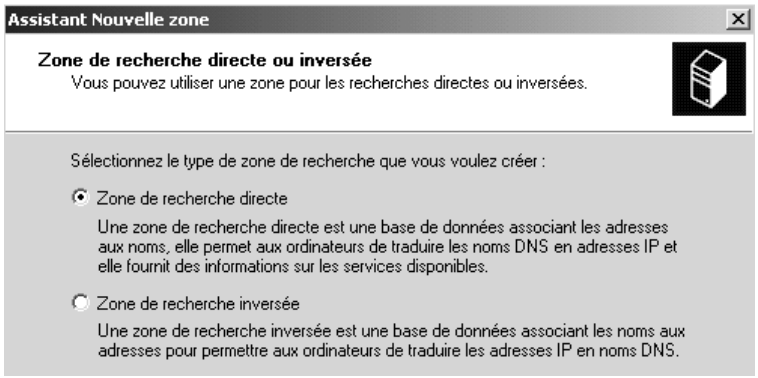
- **Intégrée à active directory** : c'est une solution propriétaire qui permet de stocker le fichier DNS non plus sous forme texte sur le serveur mais comme un objet au sein d'Active Directory, augmentant la sécurité, et remplaçant la duplication de ce fichier avec les "transfert de zone" par les mécanismes de réplication d'Active Directory., **à condition bien sûr de se placer au sein d'un réseau complètement 2000-2003**.
- **Zone principale standard** : par défaut, le 1° serveur du domaine doit contenir une zone principale standard. Les mises à jours se font directement sur cette zone.
- **Zone secondaire standard** : permet de mettre en place un serveur secondaire qui répliquera le contenu du serveur primaire par des mécanismes de "transfert de zone". Ne peut fonctionner bien sur que si un serveur DNS primaire existe déjà. Cette zone ne peut pas être directement modifiée mais est utilisée uniquement en lecture seule. Elle permet de la tolérance de panne et de la répartition de charge.

Si on se trouve dans un domaine 2000, et que l'on bénéficie d'une structure AD, il est vraiment intéressant d'intégrer le DNS dans AD, cela sécurise et facilite le mécanisme de **transfert de zone**

On utilisera en effet à la place les mécanismes de réplication d'Active Directory



Il faut choisir ensuite le type de la zone de recherche à créer :

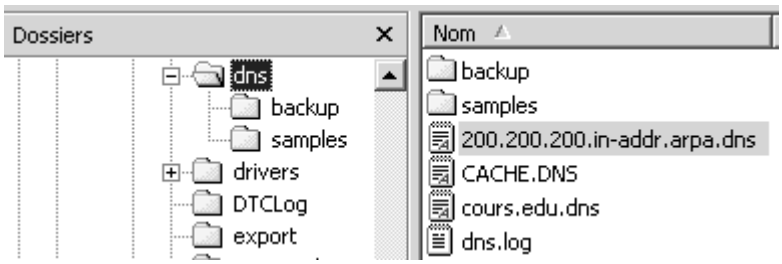


- **Zone de recherche directe** : **Forward Lookup Zone** : permet de retrouver l'adresse IP d'un appareil à partir de son nom (crée par défaut lors de l'installation de AD via DC promo). Crée un fichier avec le **nom de la zone** suivit du suffixe **.dns**
  ex: pour la zone formation.net crée le fichier formation.net.dns

- **Zone de recherche inversée** : **Reverse Lookup Zone** : permet de retrouver le nom d'un appareil à partir de son adresse IP (non crée par défaut). Crée un fichier avec **l'adresse ip reseau inversé** suivit du suffixe **.in-addr.arpa.dns**
  ex: 1 zone classe B 172.16.0.0 crée le fichier 16.172.in-addr.arpa.dns
  ex: 1 zone classe C 192.168.1.0 crée le fichier 1.168.192.in-addr.arpa.dns

L'installation du serveur DNS sous 2000-2003 crée des fichiers situés dans un dossier nommé **..\WINNT\System32\dns (sauf si intégration dans AD)**

Ces fichiers sont au format texte mais il vaut mieux les manipuler à travers l'interface prévus dans Windows



Ceux portant une extension **.dns** et **.arpa.dns** contiennent les résolution normales et inverses de noms,

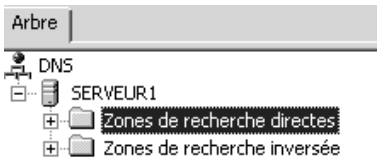
Le fichier **cache.dns** contient les enregistrement permettant la résolution de nom dans les domaines qui ne sont pas sous l'autorité du DNS visualisé.

N.B: Si on supprime une zone, le fichier correspondant n'est pas effacé automatiquement. Si on la recrée, le fichier correspondant est alors réutilisé ! Penser donc à effacer le fichier de la zone que l'on détruit...

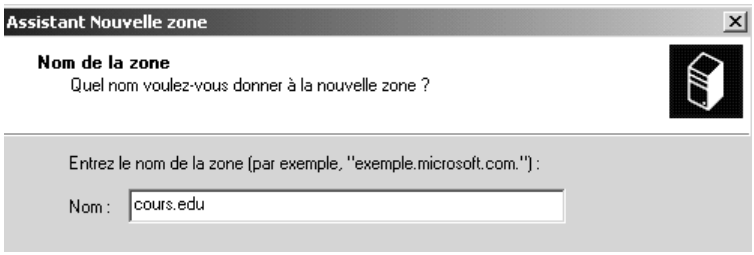
Zone de recherche directe

Il faut commencer par une zone de recherche directe :

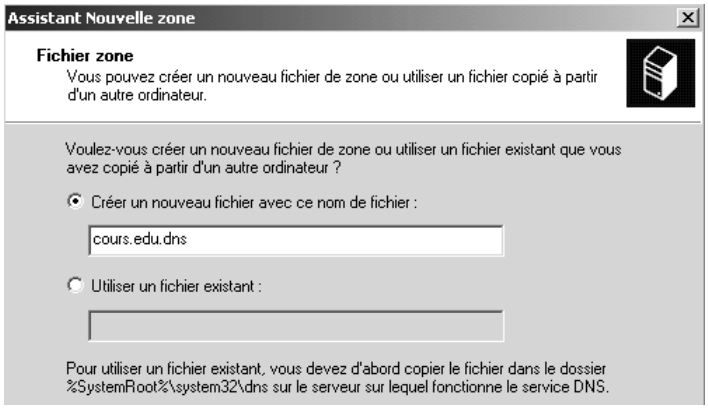
Il faut se placer sur



Puis demander une nouvelle zone via le menu contextuel



2000-2003 créera alors par défaut un fichier nommé *cours.edu***.dns**

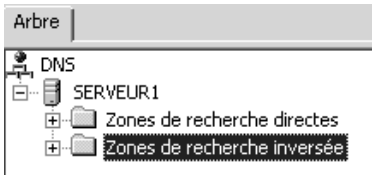


et donne un récapitulatif en fin d'opération…

Zone de recherche inversée

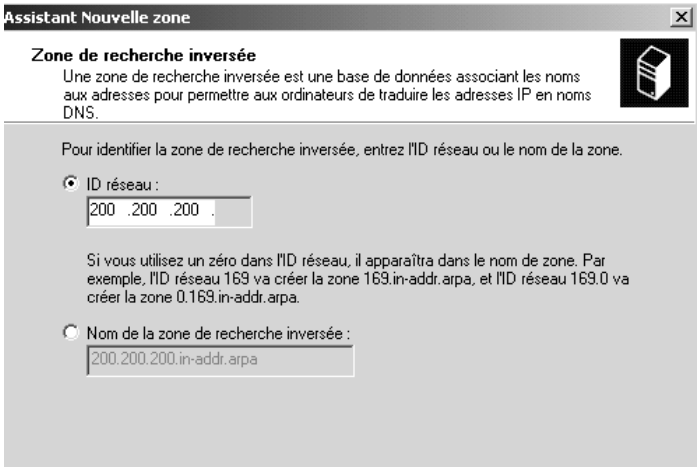
On peut aussi donner une zone de recherche inversée :

Il faut se placer sur

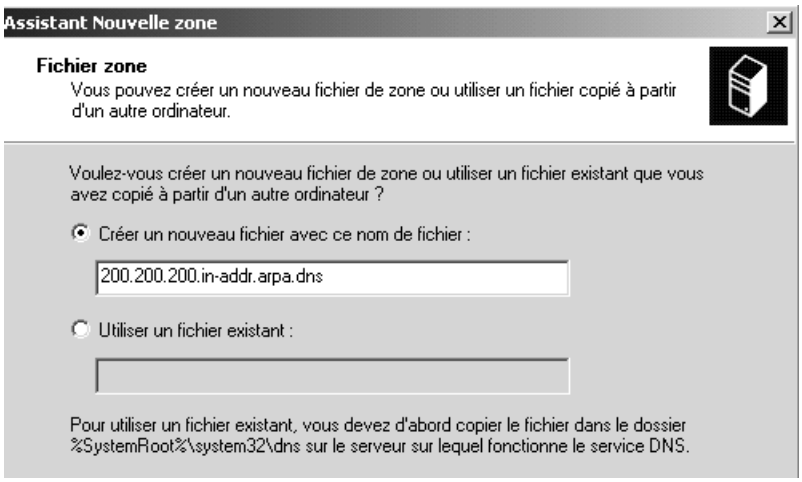


Puis demander une nouvelle zone via le menu contextuel

Dans laquelle il faut donner l'adresse IP de la zone inverse c.a.d l'adresse ip réseau



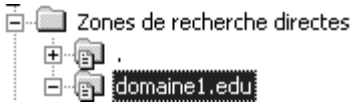
2000-2003 créera un fichier nommé *200.200.200.***in-addr.arpa.dns**



et donne un récapitulatif en fin d'opération...

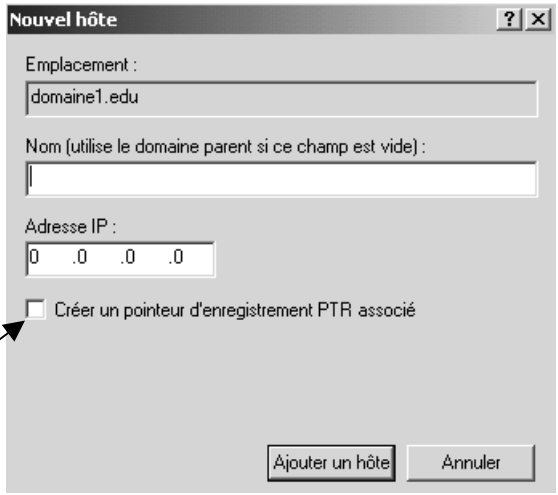
Définir un nouvel hôte :

Etant dans une zone de recherche directe, on peut créer un nouvel hôte via le menu contextuel...



On donne le nom d'hôte et son adresse IP

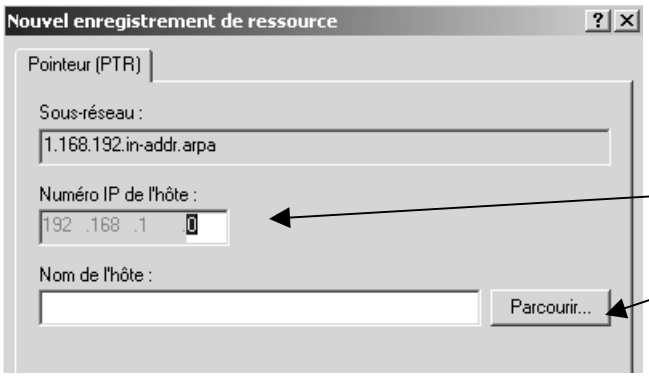
Si une zone inverse existe, on peut créer directement l'enregistrement correspondant...



N.B: si on défini un hôte sans qua la machine soit physiquement présente en ligne, nslookup sera ok alors que le ping restera impossible.

Définir un pointeur d'enregistrement

Etant dans une zone de recherche indirecte, on peut créer un nouveau pointeur via le menu contextuel...

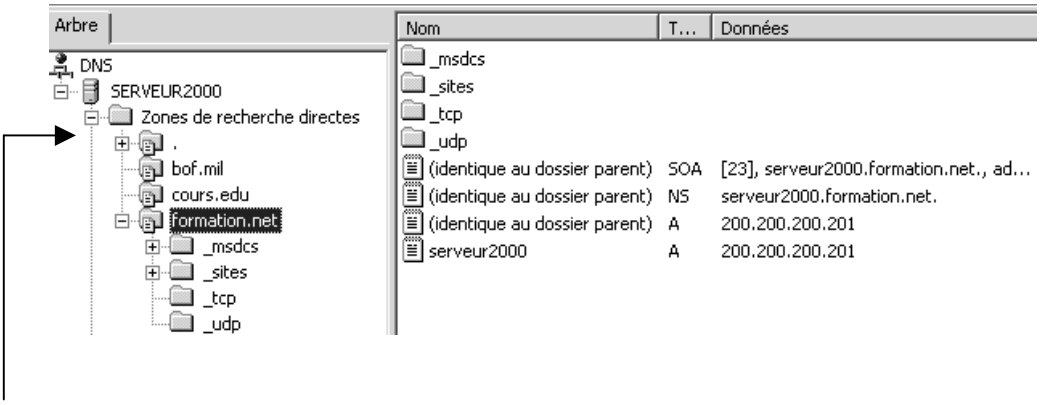


On donne uniquement le n° machine, et

on peut aller chercher le nom d'hôte correspondant

Structure du DNS :

Lorsque le service est installé et les zones définies, le DNS est géré à travers une base de donnée dans laquelle chaque enregistrement est prédéfini et correspond à un type de ressource (ceci est normé dans la RFC 1035). Pour mieux les visualiser, on peut demander **Affichage / Détaillé** .



N.B: Dans un DNS 2000 via DCpromo, la zone racine "." est crée

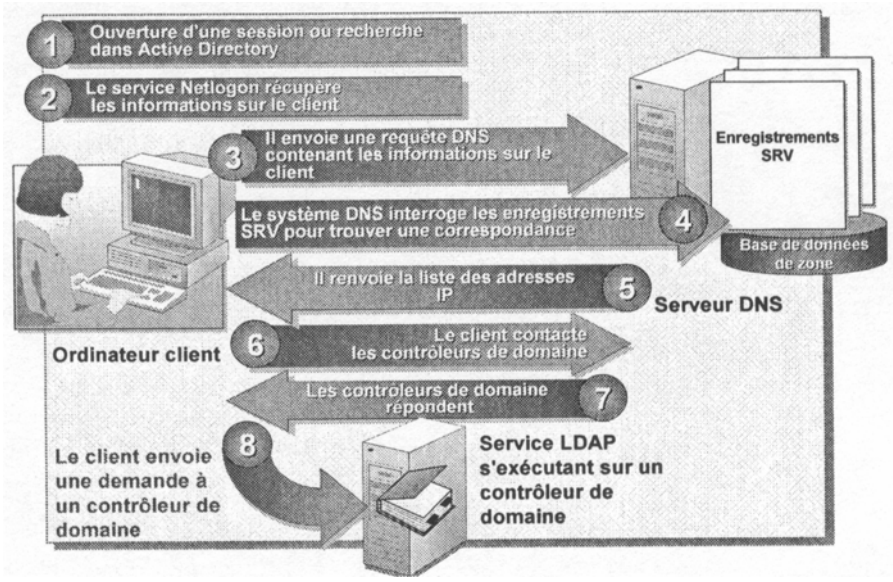
Les enregistrement de Ressource gérées par le DNS Windows NT 2000

Ce sont les types d'enregistrement communs a tout serveur DNS

Type	Nom de l'enregistrement	
SOA	Start of Authority (Source des noms)	C'est le premier enregistrement de donnée de la zone. En général il identifie le serveur de Nom ayant autorité sur le Domaine
NS	Name Server (Serveur de Nom)	C'est pour répertorier les différents serveurs de nom (secondaires) disponibles pour un domaine particulier
A	Alias (Hôte)	Dans une zone de recherche directe, un enregistrement de type hôte est utilisé pour retrouver des adresse IP à partir de noms
PTR	Pointer (Pointeur)	Dans une zone de recherche indirecte, un enregistrement de type pointeur est utilisé pour retrouver des noms à partir d'une adresse IP
SRV	Service (Service)	Cet enregistrement sert à localiser des machines sur lesquelles tournent des services particuliers pour le domaine (DHCP, Contrôleur ...)
CNAME	Alias (Alias)	Cet enregistrement permet de définir plusieurs noms pour une seule adresse IP
MX	Mail Exchanger (Serveur de Messagerie)	Cet enregistrement identifie un serveur de messagerie à contacter pour un domaine, et, s'il y en a plusieurs, dans quel ordre les contacter
HINFO	Host Information (Information sur l'hôte)	Cet enregistrement peut servir à connaître les ressources d'un équipement (UC, Système...)

Les enregistrement SRV gérées par le DNS Windows NT 2000

Ce sont de nouveaux types d'enregistrement permettant de repérer des typologies de serveur.



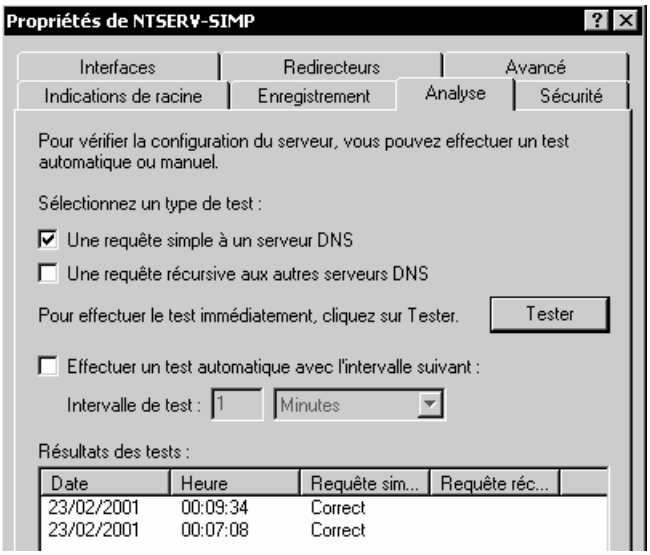
en effet pour ouvrir une session, ou parcourir AD, un client doit contacter un Contrôleur de Domaine. Tous les CD inscrivant a la fois des enregistrement de ressource A – hôte et des enregistrement de type SRV...(pour info on peut visualiser les enregistrement SRV crées par la déclaration d'un CD dans un fichier stocké en **WINNT\SYSTEM32\CONFIG** et nommé

Une fois ce mécanisme validé, le service netlogon mettra en cache les informations relatives au CD pour ne pas avoir a répéter ce processus à chaque fois !

Champs SRV	Description
_Service	Nom symbolique pour le service désiré défini dans la RFC 1700
_Protocole	type du protocole de transport. Généralement TCP ou UDP
Nom	Nom de domaine DNS auquel on fait référence
Ttl	Champs standard DNS
Classe	Champs standard DNS
Priorité	Définit la préférence pour un hôte spécifié dans le champ **cible**. Les clients DNS essaient de contacter le premier hôte accessible de la plus faible Priorité
Poids	Utilisé en même temps que **Priorité** pour offrir un mécanisme d'équilibrage entre plusieurs serveurs qui sont spécifiés dans le champ **cible** et qui correspondent tous au même niveau de préférence
Port	Port du serveur sur l'hôte **cible** qui offre le service indiqué dans le champ **service**
Cible	Spécifie le nom de domaine DNS de l'hôte (ordinateur) qui offre le type de service demandé

Test du DNS :

La bonne marche du serveur DNS peut se tester via les propriété du Serveur DNS dans la console MMC de gestion du DNS



Onglet **Analyse**

On peut s'assurer que tous les clients du réseau ait bien leur adresse résolue sur notre serveur DNS.

La bonne marche des enregistrement dans le DNS peut se tester via la commande **Nslookup**

Cet outil de diagnostic affiche des informations sur les serveurs de noms DNS (système de noms de domaine). **Nslookup** est disponible uniquement si le protocole TCP/IP est installé.

Nslookup en mode interactif

Nslookup propose deux modes : interactif et non interactif. On passe en mode inter-actif en tapant simplement **nslookup**, et on sort en tapant **exit**.

mode interactif 1°

- En premier argument, tapez le nom ou l'adresse IP de l'ordinateur pour lequel la recherche est effectuée.
- En deuxième argument, tapez le nom ou l'adresse IP d'un serveur de noms DNS. (Si omis, le serveur de noms DNS par défaut est utilisé)

Dans les exemples ci-dessous, un client correct se nomme "**client1r1"**, et le serveur DNS par défaut est le serveur "**serveur1"**

un client incorrect se nomme "**erreur"**

Ici on ne trouve pas de résolution pour le nom de ce client…"erreur"

```
> erreur serveur1
Serveur :  serveur1.domaine1.edu
Address:  192.168.1.1

*** serveur1 ne parvient pas à trouver erreur : Non-existent domain
```

Ici on ne trouve pas le serveur DNS …"erreur"

```
> client1r1 erreur
*** Impossible de trouver l'adresse pour le serveur erreurÿ: Non-existent domain
```

Ici on trouve le client "client1r1" sur le serveur DNS "serveur1"

```
> client1r1 serveur1
Serveur :  serveur1.domaine1.edu
Address:  192.168.1.1

Nom :    client1r1.domaine1.edu
Address:  192.168.1.2
```

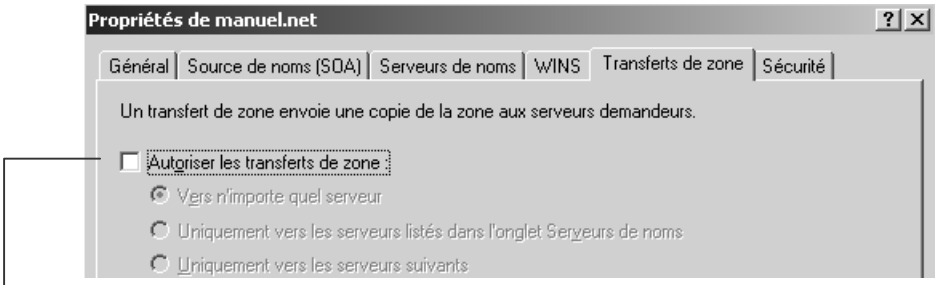
mode interactif 2°

nslookup accepte une autre commande en mode interactif, permettant de liste tous les enregistrement SRV présents dans le DNS.

avec **ls -t a** suivit de **nomdomaine** on obtient tous les enregistrement A Hôtes du Domaine

```
> ls -t a domaine1.edu
[serveur1]
 domaine1.edu.                  A      169.254.64.189
 domaine1.edu.                  A      192.168.1.1
 domaine1.edu.                  NS     server = serveur1.domaine1.edu
 gc._msdcs                      A      169.254.64.189
 gc._msdcs                      A      192.168.1.1
 client1r1                      A      192.168.1.2
 serveur1                       A      192.168.1.1
>
```

N.B : un certain type de requête peut être inhibée sir par défaut au niveau du paramétrage de la zone que l'on interroge on a demandé



Donnant

```
> ls -t a manuel.net
[localhost]
*** Impossible de fournir la liste du domaine manuel.net : Query refused
>
```

avec **set type=NS** suivit de **nomdomaine** on obtient tous les SRV correspondant a des NS name server

```
> set type=NS
> domaine1.edu
Serveur :  serveur1
Address:  192.168.1.1

domaine1.edu    nameserver = serveur1.domaine1.edu
serveur1.domaine1.edu   internet address = 192.168.1.1
>
```

avec **set type=SOA** suivit de nomdomaine on obtient tous les SRV correspondant a des SOA Start of Authority

```
> set type=SOA
> domaine1.edu
Serveur :  serveur1
Address:  192.168.1.1

domaine1.edu
        primary name server = serveur1.domaine1.edu
        responsible mail addr = admin
        serial  = 35
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
serveur1.domaine1.edu   internet address = 192.168.1.1
>
```

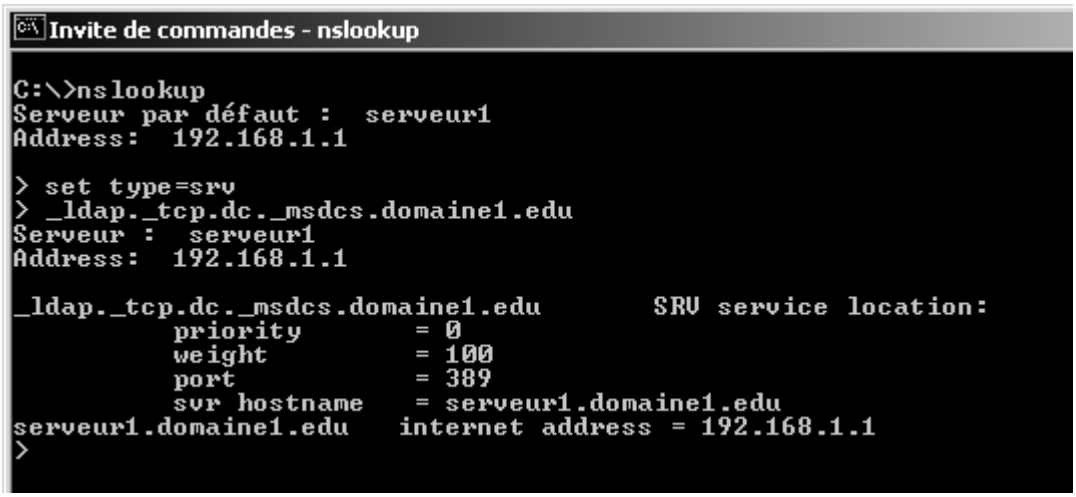
mode interactif 3°

Pour vérifier l'enregistrement DNS pour tous les contrôleurs de domaine à l'invite nslookup (">"), tapez :

set type=SRV suivit de **_ldap._tcp.dc._msdcs. nomdomaine**

où **nomdomaine** est le nom DNS configuré pour être utilisé avec votre domaine Active Directory et tout contrôleur de domaine qui lui est associé.

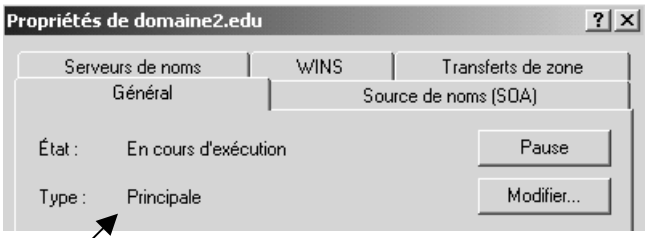
Dans l'exemple, si le nom de domaine DNS de votre domaine est **domaine1.edu**, tapez **_ldap._tcp.dc._msdcs.domaine1.edu**



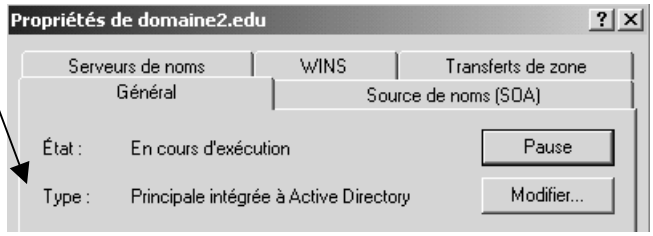
GESTION DNS WINDOWS 2000

Intégrer une zone DNS dans active directory (ou la sortir):

SI on a un doute pour savoir si notre zone principale est intégrée ou non dans Active Directory, il suffit de se place sur notre zone, puis demander propriété.



Type



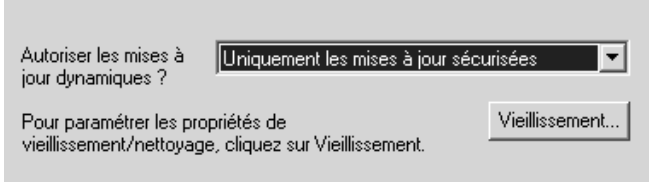
Pour modifier cet état de fait, il faut demander **Modifier...** et dans la boite de dialogue demander ce que l'on veut

Il est préférable d'intégrer une zone dans AD !

(et la racine aussi si cela est necessaire)

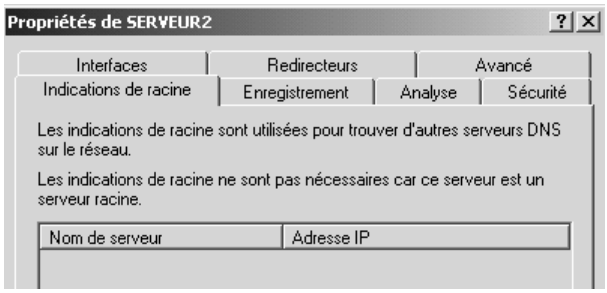
NB: on ne peut intégrer ou sortir que des zone principales

après confirmation, ilfaut penser éventuellement à autoriser les mises à jours dynamiques...(pour échanger avec les autres serveur DNS intégrés a AD)



Racine et indications de racine

La **racine** représentée par un point . est le plus haut niveau de l'espace de nom. Si on dispose d'un zone racine, le DNS se considère comme un DNS de niceau root et donc n'utilise pas les indications de racine

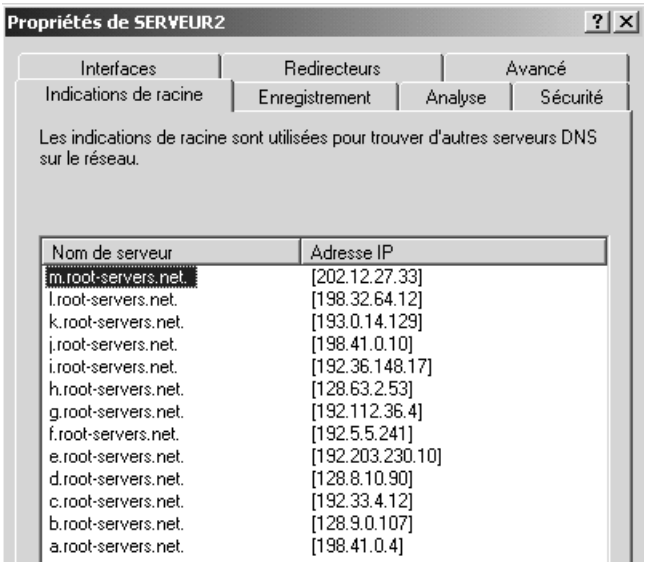


Si le serveur DNS "ne se prends pas pour un serveur racine", (n'a pas de zone racine) alors il utilise les indications de racine pour résoudre éventuellement les demandes qui lui parviennent.

A coté de ces serveurs standard de racine internet (dit root...)

On peut trouver le serveur DNS de Domaine...

Ou la machine serveur DNS de l'intranet...



Les enregistrements de ressources Indications de racine sont stockés soit dans Active Directory, soit dans des fichiers texte (fichiers %SystemRoot%\System32\DNS\Cache.dns). Windows utilise le serveur racine Internic standard. En outre, lorsqu'un serveur Windows 2000 interroge un serveur racine, il met automatiquement à jour sa liste de serveurs racine.

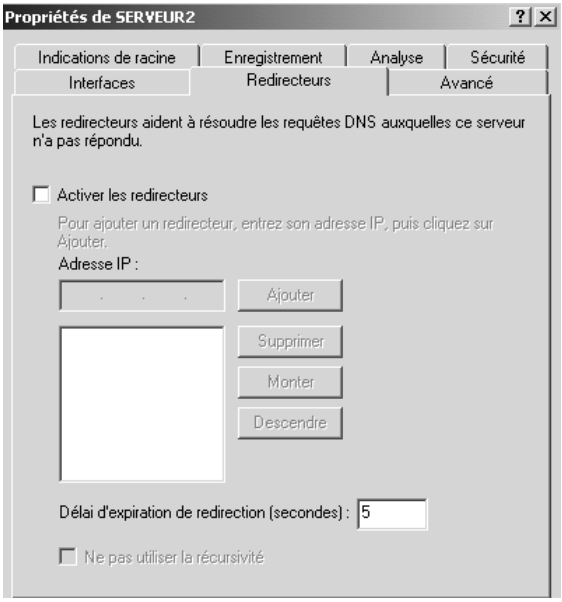
Redirecteurs

Un **redirecteur** sert à résoudre tout ce qui ne peut pas être résolu dans les zones du serveur DNS.

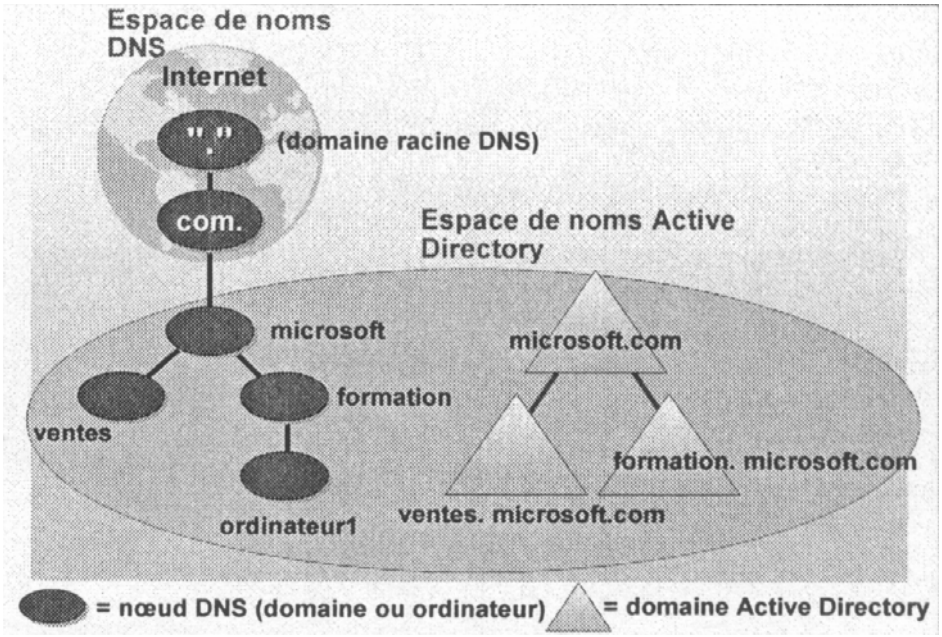
Un **redirecteur** à la priorité sur les indications de racine.

L'ordre de résolution étant :

1. Cache
2. Zone
3. Redirecteurs
4. Racine



NB: Si on se retrouve avec une zone racine dans le DNS, (et notamment si on a crée le DNS aves l'assistant lors du Dcpromo) il est possible que l'on ne puisse plus indiquer des redirecteurs, car ce serveur DNS se "trouve" comme étant un serveur Internet racine, donc au sommet de la pyramide. **Si on veut indiquer des redirecteurs, par exemple avec les DNS de votre FAI, il faudra supprimer cette zone racine**



Sauvegarde du serveur DNS:

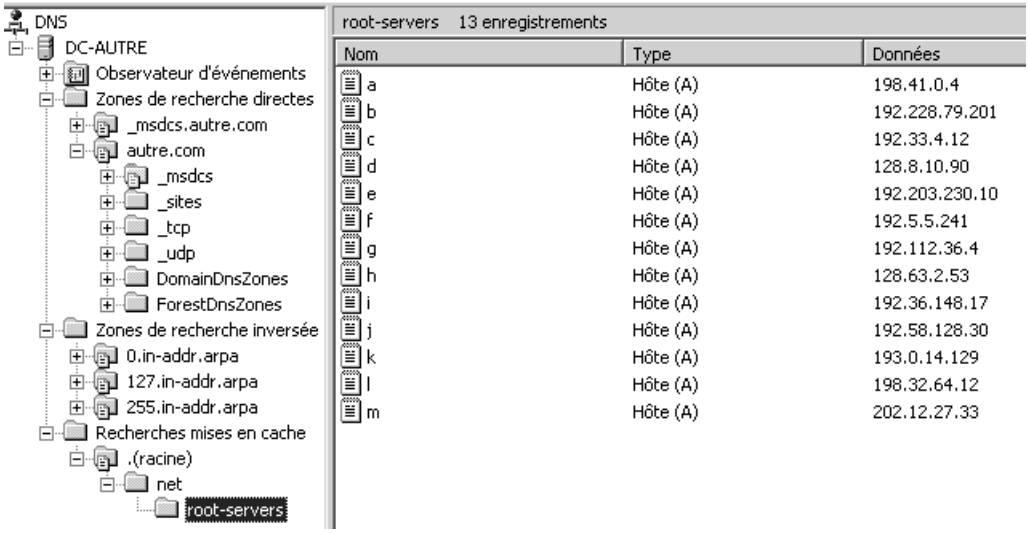
La sauvegarde des données de zone dans un serveur DNS sera radicalement différente, selon le type de serveur DNS.

- Si le serveur DNS est intégré à Active Directory, et possède un deuxième serveur DNS sur le domaine, une reinstallation éventuelle du serveur DNS défaillant suivit d'une réplication automatique via les mécanismes AD suffiront.
- Si le serveur DNS est intégré à Active Directory, et ne possède pas un deuxième serveur DNS sur le domaine, une restauration d'une sauvegarde initiale du système, remettra le serveur DNS en ordre de marche.
- Si le serveur est non intégré à Active Directory, s'il possède un serveur de backup, lorsque l'on réinstalle le serveur défaillant, une réplication de zone depuis le serveur de backup suffira à réinstaller la zone nouvellement réinstallée.
- Si le serveur est non intégré à Active Directory, s'il ne possède pas un serveur de backup, on sauvegarde le fichier crée dans le dossier **..\WINNT\System32\dns**. (le fichiers xxx.dns et xxx.arpa.dns contiennent les résolution normales et inverses).
  et on copie la clé **HKLM/SYSTEM/CCS/service/DNS...**

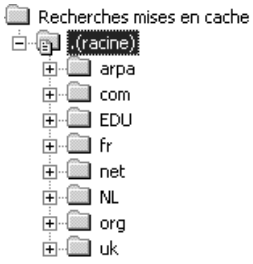
Le cache DNS sous 2003 Srv:

Sous 2003 server, par défaut on peut accéder à internet car les redirecteurs sont positionnés

Si on observe le contenu du cache d'un serveur DNS installé, on s'aperçoit que les serveurs racines de l'internet par défaut sont incorporés

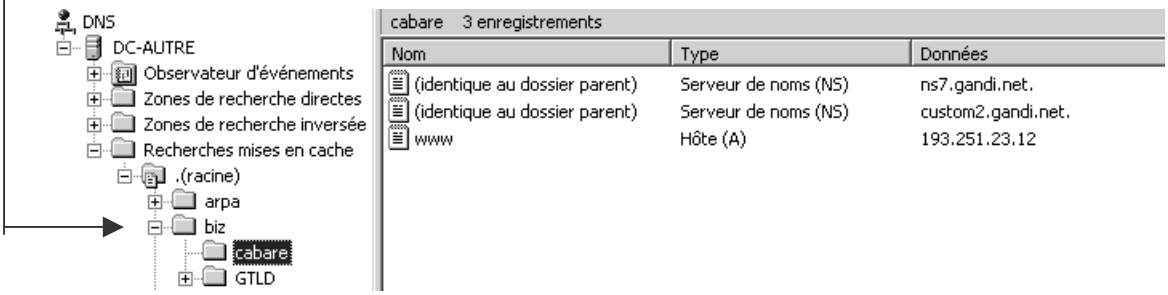


puis des les premières recherches sur le web le cache s'étoffe



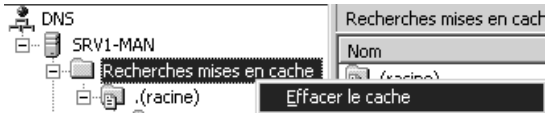
ainsi si on recherche un site très très connu, **http://www.cabare.biz**

on retrouvera dans le cache :



Effacer Le cache DNS 2003 Srv:

On peut le faire soit en se plaçant sur le serveur et en demandant



Soit en ligne de commande par **Dnscmd** est un outil de ligne de commande pour la gestion des serveurs DNS.

Cet outil permet d'écrire des scripts de fichiers de commandes en vue d'automatiser la gestion et la mise à jour des configurations existantes de serveur DNS

dnscmd *NomServeur* /clearcache

Ordre de Résolution DNS par le client 2000 XP:

Il peut être intéressant de se rappeler l'ordre de résolution du résolveur local pôur un nom d'höte.

RECHERCHE HOTE DNS

1. d'abords le cache DNS local en RAM est utilisé
2. Ensuite un fichier Host peut être utilisé
3. le serveur DNS est interrogé
4. on enchaîne sur une résolution NetBIOS si le nom est NON FQDN, c'est-à-dire du genre « poste1 » (si le nom est du genre « poste1.domaine.com » alors on n'enchaîne pas sur une recherche NetBios...)
    a. d'abords le cache local Netbios
    b. serveur WINS
    c. Diffusion Broadcast
    d. Consultation fichier LMHost

N.B : il est facile d'afficher le contenu du cache DNS local, par la commande **ipconfig /displaydns**

N.B : il est facile d'afficher le contenu du cache DNS local, par la commande **ipconfig /flushdns**

RELATION DNS – WINS NOM NETBIOS

Alors nom Netbios ou - hôte DNS ?

Sur les clients windows, un nom netbios est limité à **15 caractères maxi sans .**

Un nom d'hote DNS peut avoir **265 caractères maxi et 255 caractères maxi pour le FQDN avec un .**

Depuis une machine 95, 98 NT si on fait appel à une machine avec un "." on passera forcément par un DNS...

mais le voisinage réseau ne fera pas appel au DNS.

Ainsi dans un réseau avec un DNS en carafe, et une AD non fonctionnelle, les client 95-98 continueront à travailler entre eux...

- Depuis un poste 9x ou NT4, les contrôleur de Domaine sont localisés par NetBIOS. Par conséquent si des machines de ce genre restent présentes, un serveur WINS sera toujours le bienvenue.
- Depuis une machine 2000 ou XP, DNS est utilisé tout le temps, même pour construire le voisinage réseau, par exemple. Si le serveur DNS est en panne, il risque de ne pas pouvoir y avoir d'ouverture de session..., mais pour le voisinage réseau par exemple on se repliera sur des broadcast via netbios...

Qui peut le plus...

Cela peut donc apparaître complètement inutile de renseigner un serveur WINS sur un réseau ayant un serveur DNS fonctionnel et des clients uniquement 2000 ou XP, c'est redondant et cela n'apporte pas grand chose de plus. En effet, lors d'un DC promo, on inscrit automatiquement dans le DNS via des enregistrements de service, quelle machine est DC, de manière à ce que les client du serveur DNS sachent sur quelle machine ils doivent faire valider leur ouverture de session...

Mais un serveur Wins peut économiser de la bande passante pour toutes les applications qui utilisent encore la couche Netbios-Over Tcp-IP...

On peut alors dire que Le serveur Wins devient véritablement inutile lorsque :

1. on est dans un réseau composé uniquement de serveur 2000-2003 et de clients 2000 et XP
2. On a dévalidé la couche Netbios/Tcp-ip ...

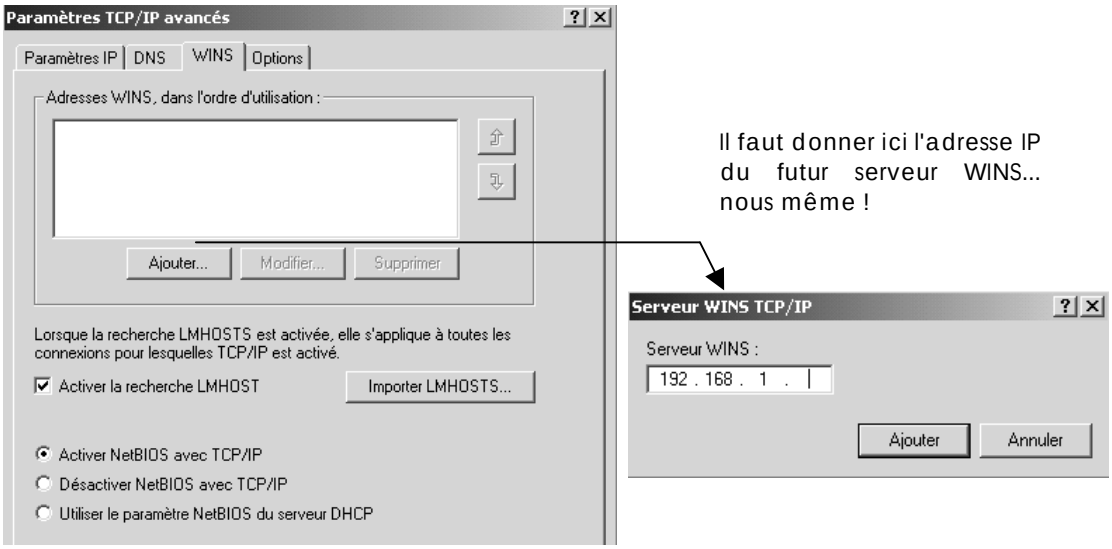
SERVICE WINS

Installer le Service WINS sous 2000 :

N.B : Ce serveur n'est pas forcément Contrôleur de Domaine !

La résolution de nom netbios via WINS ne peut se faire que sur une machine ayant une adresse IP fixe (cette adresse est ensuite rentrée sur chaque « client »)

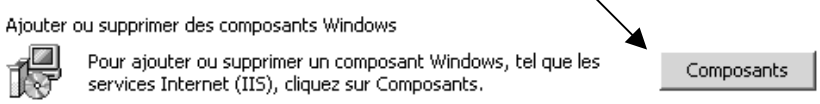
Il faut paramétrer le futur serveur WINS comme étant son propre client, c'est à dire dans les **propriétés avancées de TCP/IP**, on demande l'onglet **WINS** :



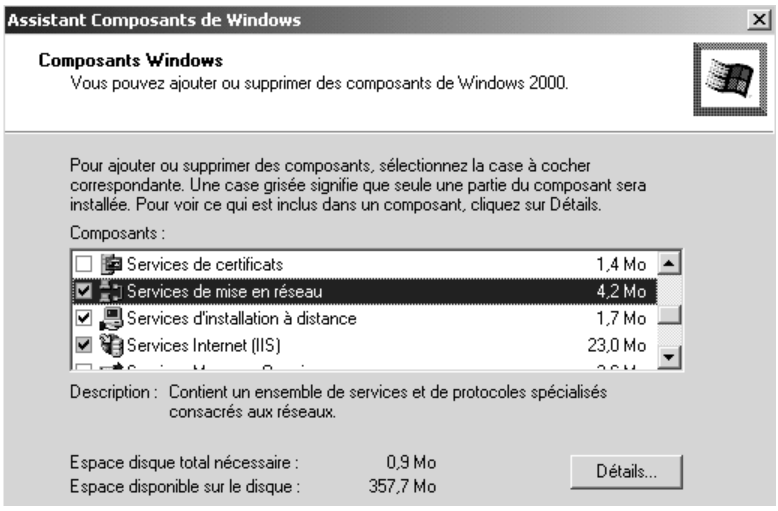
N.B: cette opération peut se faire aussi après installation du serveur WINS, mais le danger réside dans le fait que si cette adresse n'est pas renseignée, lors de son installation il inscrive ses propres enregistrements soit dans un autre serveur WINS déjà existant sur le réseau, soit nulle part...

Puis dans le panneau de configuration, on demande **Ajout/Suppression de Programme** dans lequel on demande **Ajouter/Supprimer des composants Windows...**

on clique sur composant

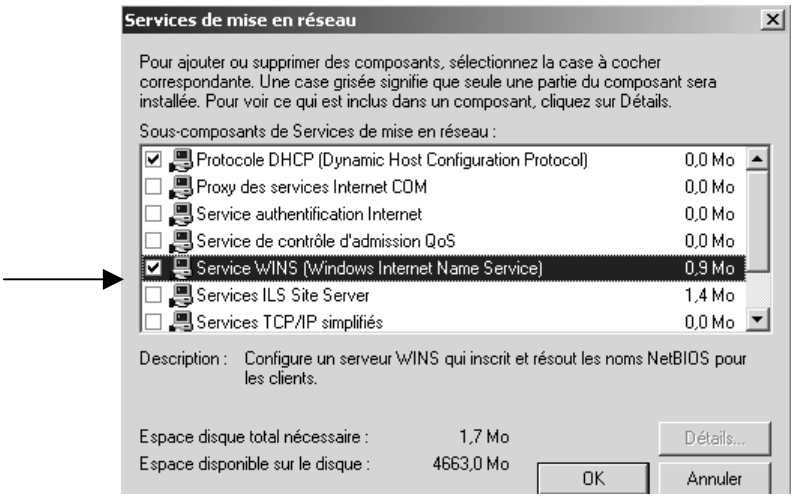


dans liste composant Windows on va chercher service de mise en réseau



via **Détails…**

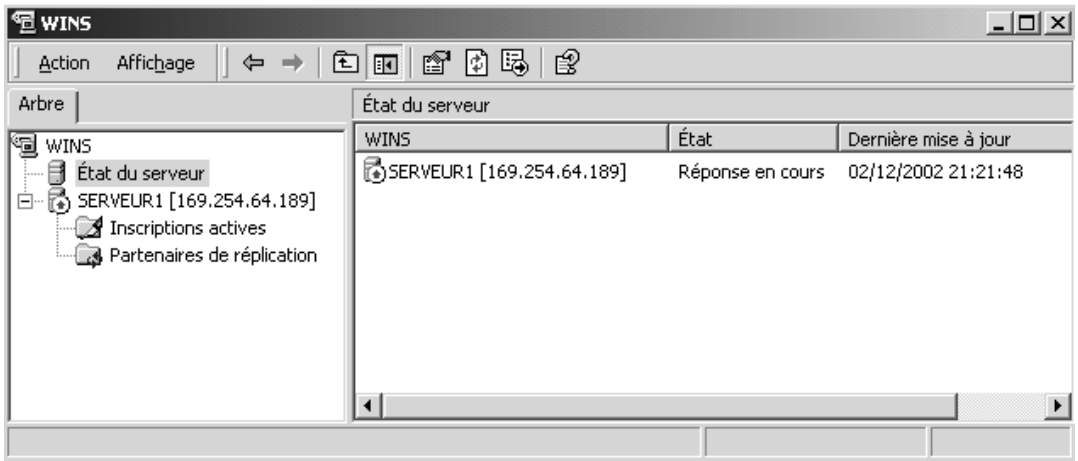
on choisit alors **Service Wins (Windows Internet Name Service)**



Pour administrer le service **WINS** on peut aller directement dans le menu

Démarrer / Programmes / Outils d'administration / WINS

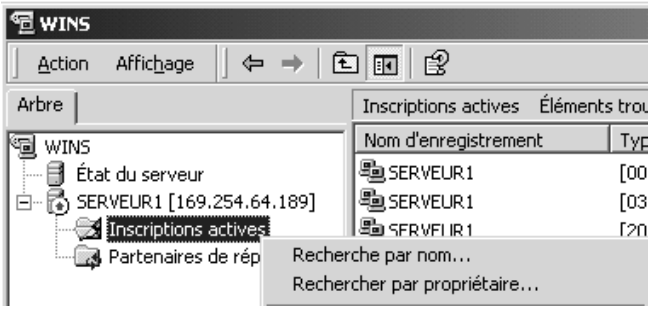
NB: ne pas prêter attention à l'adresse IP qui s'inscrit dans le cas d'une machine multi-résidente...
ce qui est d'ailleurs une configuration totalement déconseillée



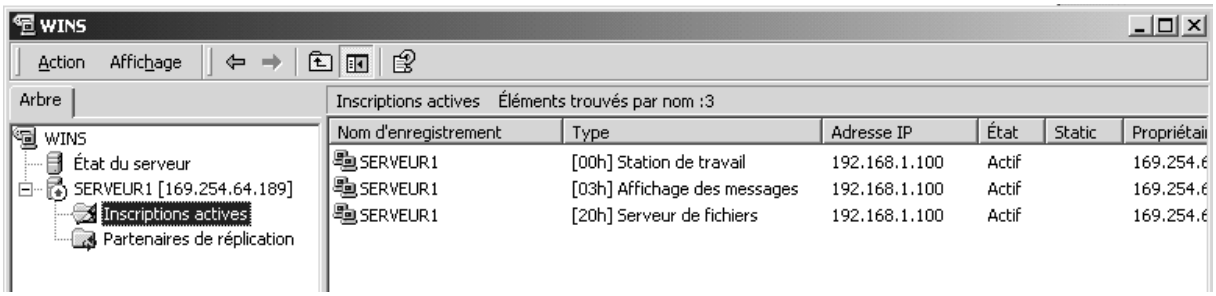
Ajouter un serveur, Visualiser une base :

Pour ajouter un serveur, il faut se placer sur Wins, et demander le menu **Action – ajouter un serveur....**

Pour visualiser les inscriptions dans la base, il suffit de se placer sur le serveur, puis de demander par un clic droit, une recherche par nom ou par propriétaire (voire tous les propriétaires)...



on obtiendra alors

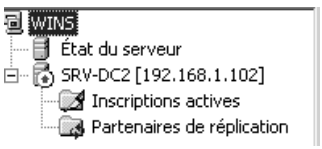


N.B : Comme les noms Netbios ne sont générés que au démarrage d'un poste, il peut être intéressant de renseigner Wins sur un client et de re-booter, on devrait alors voir l'inscription se ranger dans le serveur.

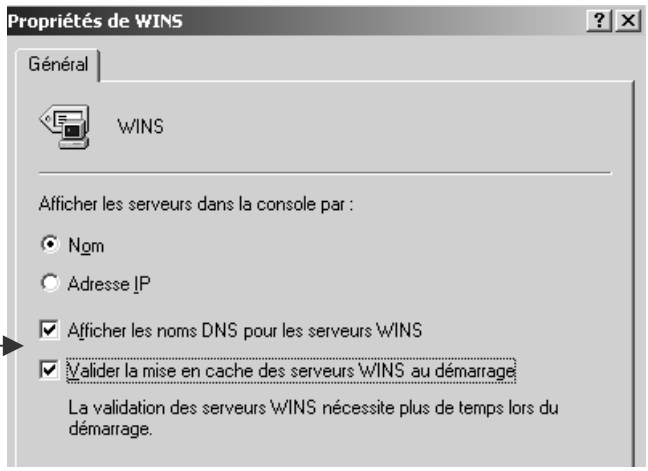
N.B : dans la même logique il faut re démarrer le serveur...

Paramétrage de base :

Pour les propriétés de **WINS** de manière générale on va demander

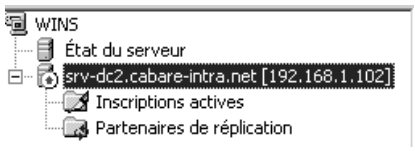


d'**Afficher les noms DNS** et de **Valider la mise en cache au démarrage**

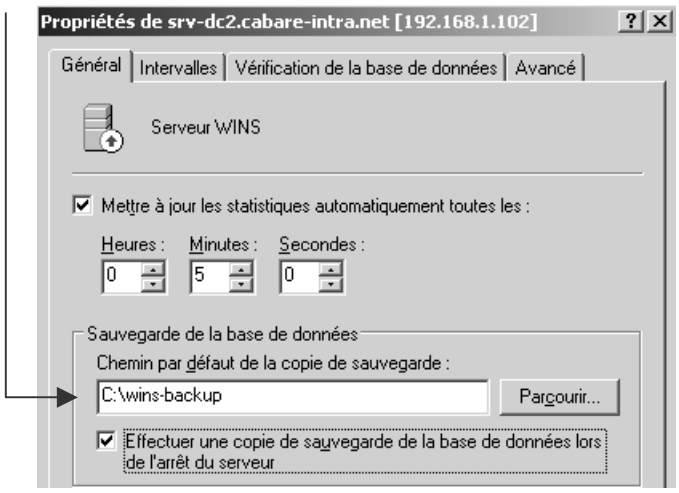


Pour les propriétés de **Serveur WINS**

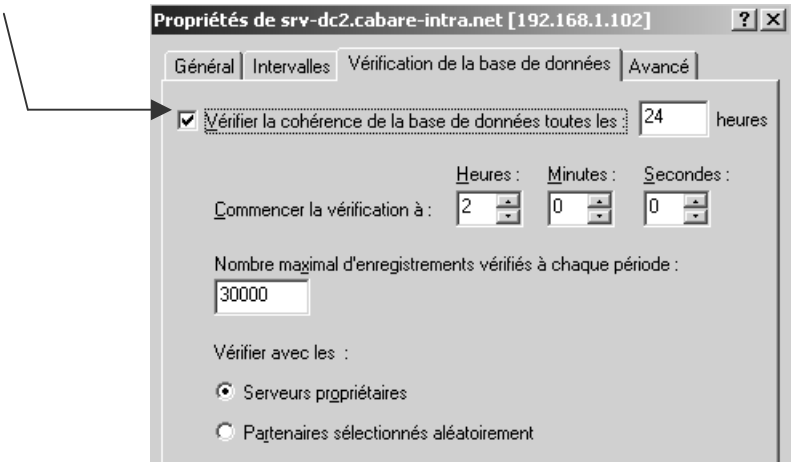
on va demander par rapport aux valeurs par défaut



De paramétrer un chemin de **Sauvegarde de la base de données**



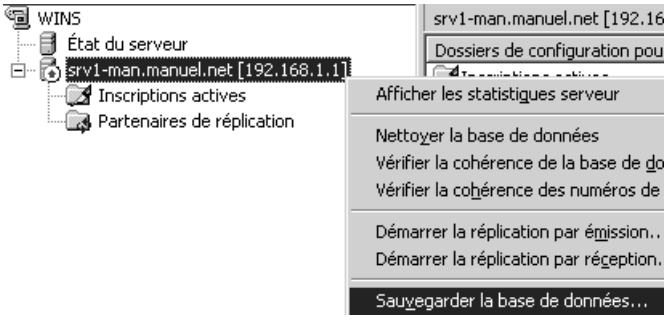
Et de **Vérifier la cohérence…**



Sauvegarder un serveur WINS:

Pour sauvegarder un serveur WINS, il faut:

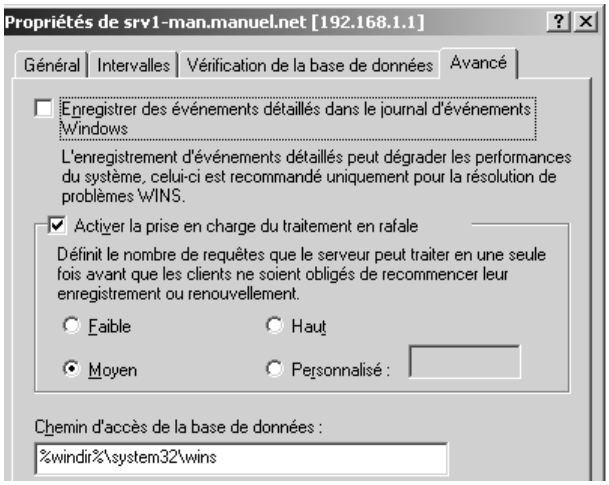
- Spécifier un dossier de sauvegarde : dans les **propriétés** du serveur Wins à configurer, onglet **général**, on indique le chemin par défaut...
- A partir de là, Wins y crée une copie de sauvegarde complète toutes les 3 heures.
- On peut aussi depuis l'icône du serveur demander un clic droit **Sauvegarder la base de donnée**
- On peut aussi passer une commande du genre **Nesth wins server @ip init backup**



Restaurer un serveur WINS:

Pour restaurer un serveur WINS il faut :

- Arrêter le service WINS
- Dans l'onglet **propriété** du serveur Wins à restaurer, demander l'onglet **avancé** et effacer tous les fichiers se trouvant dans le dossier qui est inscrit dans "**chemin d'accès de la base de donnée**"



- Dans la console WINS demander via clic droit pour le serveur WINS a restaurer **restaurer la base de donnée** en indiquant a ce moment le dossier dans lequel on a mis au préalable une copie de sauvegarde !

Compression base WINS

La base WINS se trouve dans le dossier **Winnt\system32\wins**

Lorsque la base WINS, c'est à dire le fichier **wins.mdb** est trop volumineuse, alors on peut la compresser, (environ une fois par mois par exemple ou autour des 30 Mega)

On utilise l'utilitaire en ligne de commande **jetpack.exe** avec la syntaxe suivante :

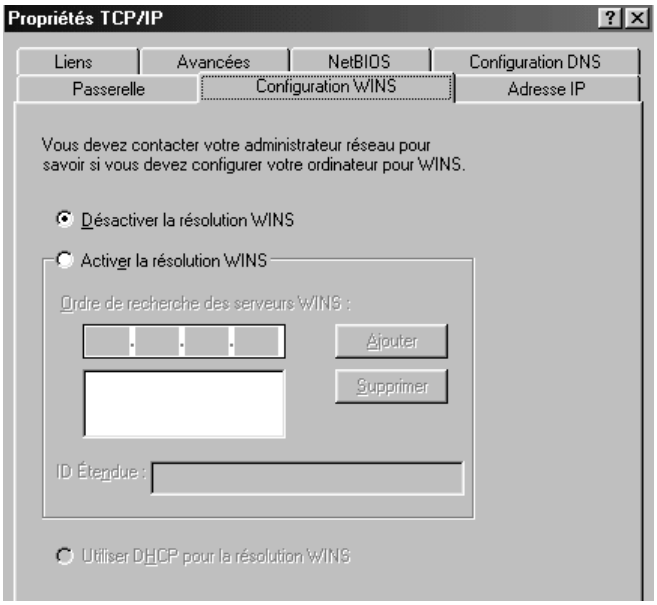
Jetpack wins.mdb

N.B: on prendra soin de faire cela sur un jeux de sauvegarde, puis de restaurer cette sauvegarde ensuite. Ne jamais compacter une base en cours d'utilisation...

Configurer manuellement un client WINS :

Cela se fait dans les propriétés de TCP/IP , avancées, onglet **Configuration WINS**, et on renseigne l'adresse IP du serveur WINS utilisé

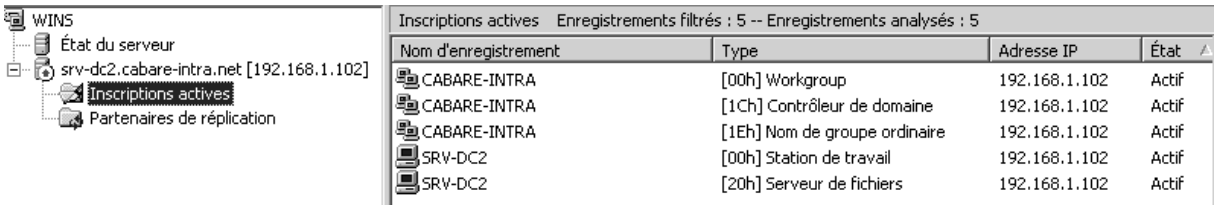
Exemple sous win98se...



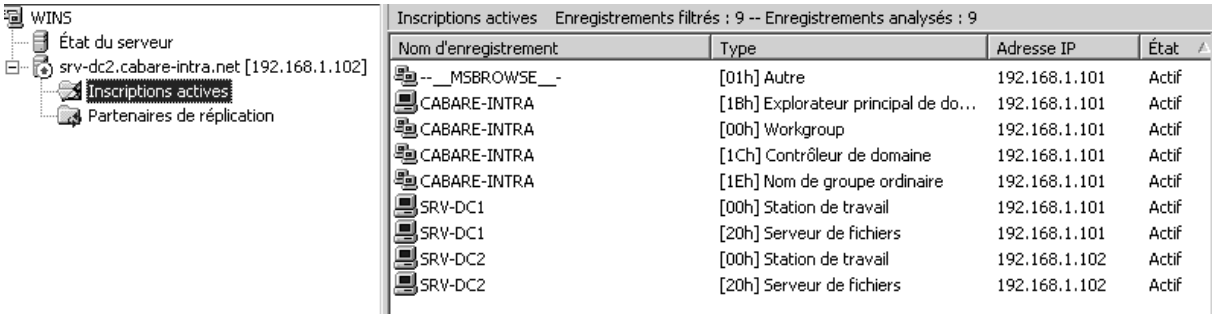
Inscriptions automatiques affichées dans WINS

Lorsque on demande de voir les inscriptions alors que par exemple l'on a

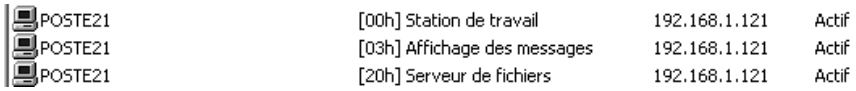
1 seul le serveur CD SRV-DC2 qui est inscrit dans le WINS (et il est le serveur WINS) on obtient quelque chose du genre :



Lorsque dans notre réseau, on paramètre notre premier DC avec les références de notre serveur WINS, les inscriptions se complètent – modifient de la manière suivante :



Si une machine POSTE21 démarre, alors les inscriptions suivantes se font...



Configurer un client WINS :

Cela se fait via DHCP. Il faut agir coté serveur, et coté client...

- Sur le **serveur DHCP**, en configurant des paramètres d'étendue

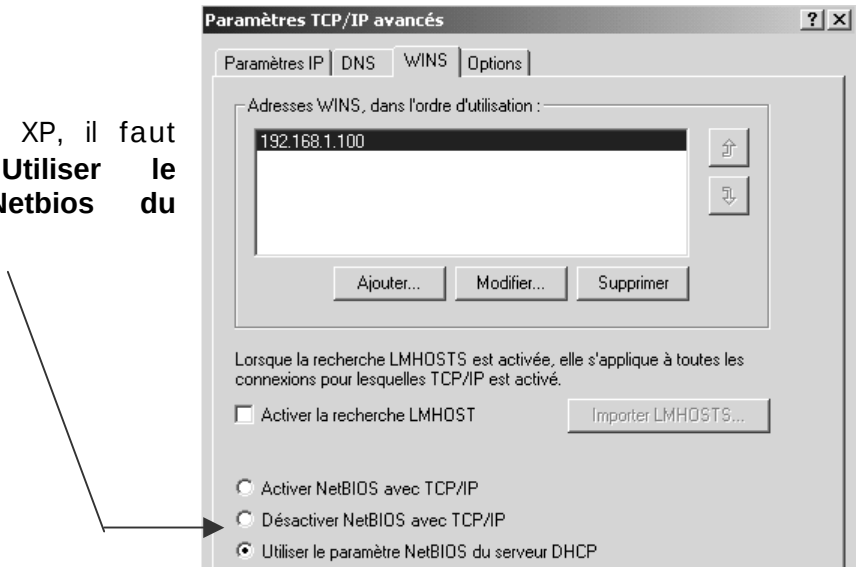
  044 Serveurs WINS/NBNS avec **l'adresse ip** du serveur principal

  046 Type de noeud WINS/NBT en configurant avec les valeurs possibles suivantes **en hexa 8 (Noeud H) 4 (Noeud M) 2 (Noeud P) 1 (Noeud B)**

- Sur le **client DHCP**, en configurant des paramètres **Configuration Wins**.

  Pour win 98, il faut demander **Utiliser DHCP pour la résolution Wins**

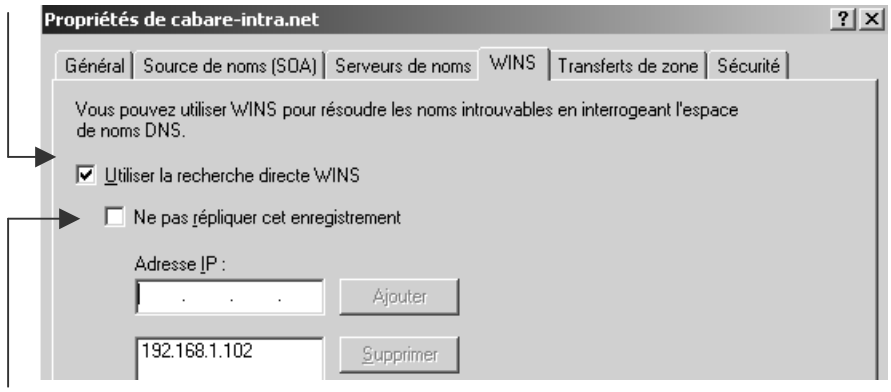
Pour 2000 et XP, il faut demander **Utiliser le paramètre Netbios du serveur DHCP**



Serveur DNS utilisant WINS pour la résolution :

Il pet être intéressant de porter à la connaissance de notre DNS les machines qui s'enregistrent de manière automatique dans notre serveur Wins... Le serveur DNS consultera le serveur WINS uniquement lorsqu'il ne trouvera pas d'enregistrement correspondant.Ce réglage se fait dans le serveur DNS.

Il faut agir sur les propriétés de la zone en demandant **Utiliser la recherche directe WINS**



N.B : il n'est pas forcément utile de répliquer cette fonction sur tous les serveurs DNS du Domaine... on peut ainsi avoir dans chaque segment du réseau un serveur DNS qui interroge un serveur Wins spécifique.

SERVICE DHCP

Objectif de DHCP :

Le protocole **DHCP** (Dynamic Host Configuration Protocol) centralise et gère l'attribution des informations de configuration TCP-IP en affectant automatiquement des adresses IP à des ordinateurs configurés pour utiliser DHCP. La mise en œuvre de DHCP élimine certains problèmes de configuration liés à la configuration manuelle de TCP-IP.

A chaque démarrage d'un client DHCP, ce dernier demande des informations d'adressage IP à un serveur DHCP. Un client ne choisit pas un serveur DHCP, il interrroge le réseau avec un broadcast DHCP pour repérer les serveurs DHCP pontentiel en vue de récupérer a terme notamment :

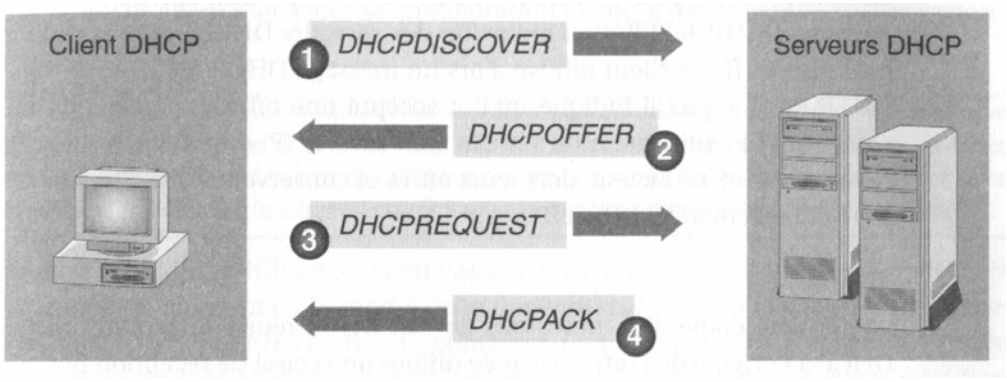
- Une adresse IP
- Un masque de sous-réseau.
- Des valeurs facultatives, comme une adresse de passerelle par défaut, une adresse DNS ou l'adresse du serveur WINS.

Lorsqu'un serveur DHCP reçoit une requête, il sélectionne des informations d'adressage IP dans une réserve d'adresses définie dans une base de données et les propose au client DHCP. Si le client les accepte, les informations d'adressage IP lui sont cédées sous la forme d'un bail d'une durée spécifique. Si aucune information d'adressage IP n'est disponible dans la réserve pour location au client, ce dernier ne peut pas initialiser TCP/IP. Il peut selon les cas se doter d'une adresse APIPA.(cf chap p).

Remarque : Le protocole DHCP est défini dans les RFC 1533, 1534, 1541 et 1542. et est dérivé du protocole BootP.

Fonctionnement de DHCP :

Pour configurer un client DHCP, le protocole DHCP travaille en 4 phases :



DHCPDISCOVER ou "Demande de bail IP" :

Le client ne disposant pas d'adresse IP et ne connaissant l'adresse IP d'aucun serveur, il utilise 0.0.0.0 comme adresse de source et 255.255.255.255 comme adresse de destination.

La demande de bail est envoyé au sein d'un message **DHCPDISCOVER**. Ce message contient également l'adresse matérielle et le nom d'ordinateur du client, afin que les serveurs DHCP puissent identifier l'émetteur de la requête. Tous les serveurs répondent s'ils le peuvent.

Le processus de bail IP est utilisé dans l'une des situations suivantes:

- TCP/IP est initialisé pour la première fois en tant que client DHCP.
- Le client demande une adresse IP spécifique qui lui est refusée. Il est possible que le serveur DHCP ait supprimé le bail.
- Le client disposait auparavant d'un bail d'adresse IP mais y a mis fin et en demande un nouveau.

DHCPOFFER ou "Offre de bail IP" :

Tous les serveurs DHCP qui ont reçu la demande et qui disposent d'une configuration valide vis-à-vis du client diffusent une proposition.

Le client ne disposant pas encore d'une adresse IP, l'envoi de la proposition s'effectue par diffusion sous forme de message **DHCPOFFER.**

Remarque : Lorsque aucun serveur DHCP n'est en ligne, le client DHCP attend une proposition pendant 1 seconde. S'il n'en reçoit aucune, il diffuse à nouveau la requête à trois reprises (selon des intervalles successifs de 9, 13 et 16 secondes). Si aucune proposition n'est reçue après quatre tentatives, le client essaie à nouveau toutes les 5 minutes.

DHCPREQUEST ou "Selection de bail IP" :

Après avoir reçu une proposition d'au moins un serveur DHCP, le client informe par diffusion tous les autres serveur DHCP de sa sélection, en acceptant la première proposition reçue.

La diffusion est envoyé dans un message **DHCPREQUEST** et comprend l'identificateur du serveur (AI) dont la proposition a été acceptée. Tous les autres serveurs DHCP retirent leur proposition afin que les adresses IP dont ils disposent restent disponibles pour la requête de bail IP suivante.

DHCPACK / NACK ou "Accusé de réception de bail IP" :

Le serveur DHCP dont la proposition est acceptée diffuse au client un accusé de réception stipulant la conclusion du bail, sous la forme d'un message **DHCPACK**. Ce message contient un bail valide pour une adresse IP et éventuellement d'autres informations de configurations.

Si un accusé de réception stipulant la non conclusion du bail (**DHCPNACK**) est diffusé (le client tente de souscrire le bail d'une adresse IP dont il disposait précédemment alors que cette adresse n'est plus disponible par exemple) le client retourne au processus de demande de bail IP.

"Renouvellement de bail IP" :

Tous le clients DHCP tentent de renouveler leur bail lorsqu'il atteint **50 %** de sa durée. Pour renouveler, un client DHCP envoie un message **DHCPREQUEST** directement au serveur DHCP avec qui il a conclu le bail en vigueur.

Si le serveur DHCP est disponible, il renouvelle le bail et envoie au client un accusé de réception stipulant la conclusion du renouvellement (**DHCPACK**) et la nouvelle durée, ainsi que les éventuelles mises à jour des paramètres de configuration.

Lorsque le client reçoit l'accusé de réception, il met à jour sa configuration. Si un client tente de renouveler son bail mais est dans l'impossibilité de contacter le serveur DHCP à l'origine de ce dernier, le client peut encore utiliser l'adresse, puisqu'il lui reste 50 % de la durée du bail.

Lorsqu'un client DHCP redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine. Pour ce faire, il diffuse un message **DHCPREQUEST** spécifiant la dernière adresse IP dont il avait le bail. Si la tentative se solde par un échec et qu'il lui reste encore du temps avant l'expiration du bail, le client DHCP continue à utiliser la même adresse IP.

Si un bail, lorsqu'il atteint **50 %** de sa durée, n'a pas pu être renouvelé par le serveur DHCP d'origine, le client tente de contacter les autres serveurs DHCP disponibles lorsque **87,5% du temps s'est écoulé**. Le client diffuse alors un message **DHCPREQUEST**. Tous les serveurs DHCP peuvent répondre par un message **DHCPACK(renouvellement du bail)** ou **DHPCNACK (obligeant le client DHCP à se réinitialiser** et à obtenir le bail d'une adresse IP différente).

Lorsque le bail expire ou qu'un message DHCPNACK est reçu, le client DHCP doit immédiatement cesser d'utiliser l'adresse IP. Il retourne alors au processus de souscription d'un nouveau bail d'adresse IP.

DHCPRELEASE ou libération des ressources:

Le client peut envoyer un message DHCPRELEASE lorsqu'il s'arrête. Ainsi le serveur DHCP peut de nouveau utiliser ces adresses pour un autre client...

N.B: Microsoft n'utilise pas cette commande. Lorsqu'une machine s'arrête, son Bail courre encore sur le serveur DHCP. Si le client se reconnecte au réseau avant la fin du bail, son bail sera réattribué par un demande DHCPREQUEST...

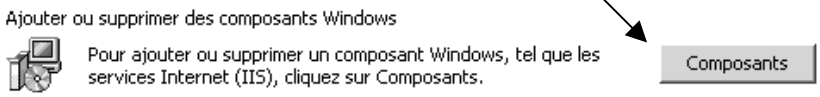
SERVEUR DHCP 2000-2003

Installer le Service DHCP :

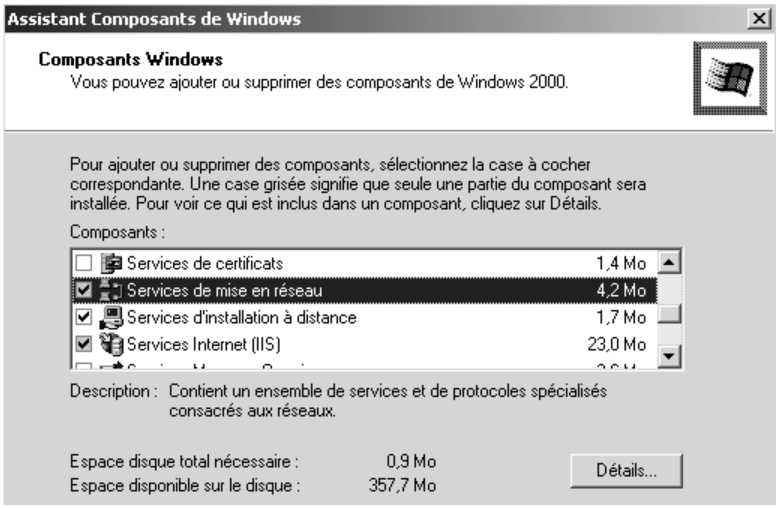
La gestion des adresses IP via DHCP ne peut se faire que sur une machine ayant une adresse IP fixe

Dans le panneau de configuration, on demande **Ajout/Suppression de Programme** dans lequel on demande **Ajouter/Supprimer des composants Windows...**

on clique sur composant

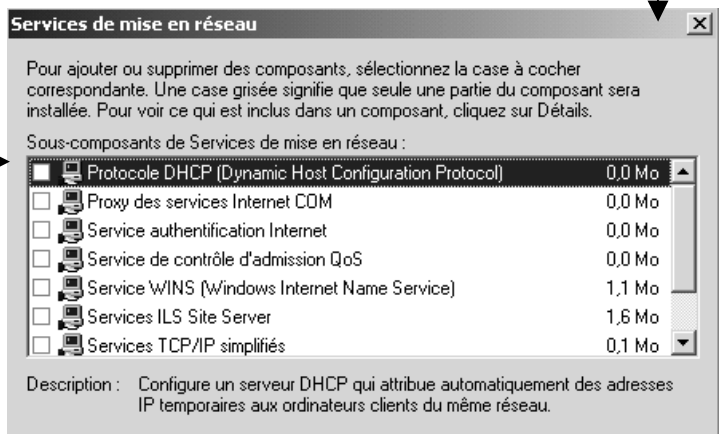


dans la liste composant Windows on va chercher service de mise en réseau



Détails...

on choisit alors **Protocole DHCP**



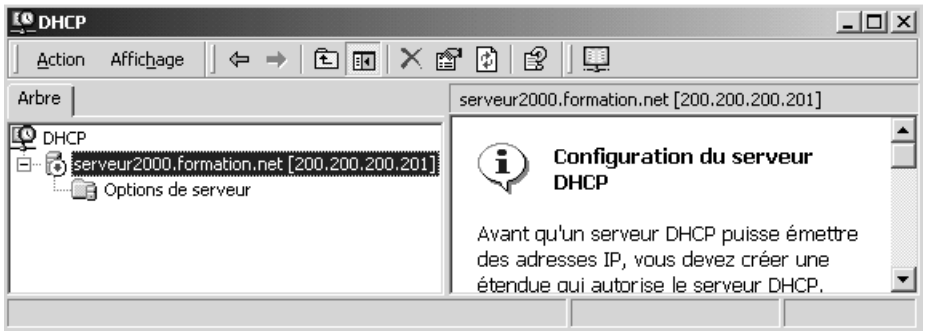
on revient et on fait suivant pour terminer l'assistant

Gestion Service DHCP :

Le service **DHCP** démarre automatiquement. Pour l'administrer on peut aller directement dans le menu

Démarrer / Programmes / Outils d'administration / DHCP

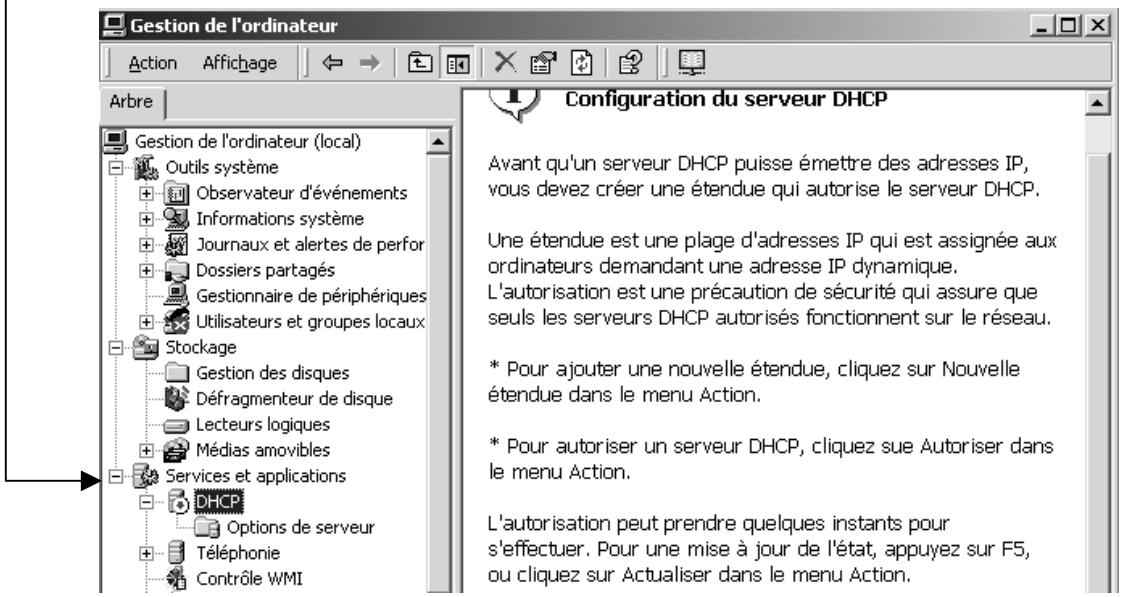
(et on a DHCP uniquement)



ou via

Démarrer / Programmes / Gestion de l'ordinateur

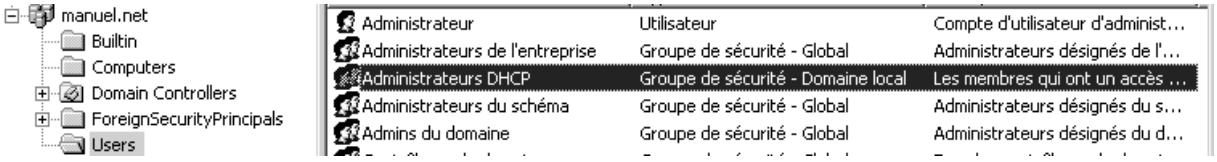
ou l'on retrouve dans **les services** le service DHCP...



A partir du moment ou le serveur DHCP est installé, deux nouveaux groupes Locaux sont crées sur le serveur 2003

Administrateurs DHCP

Utilisateurs DHCP



On peut donc donner à un utilisateur l'appartenance au groupe **Opérateur de Serveur + Administrateur DHCP**.

Il pourra administrer le serveur DHCP mais pas créer de nouveau administrateur, gérer les disques Durs ou bricoler l'adresse IP du serveur...

N.B : Cela ne veut pas dire que seul les membres de ce groupe **Administrateurs DHCP** peuvent administrer DHCP, mais simplement que l'on peut prévoir un niveau d'accès autour du serveur DHCP uniquement (les admins de domaine administrent aussi le serveur DHCP…)

DHCP de Domaine, ou DHCP Autonome:

Un serveur DHCP n'a aucunement besoin d'être dans un domaine, et encore moins d'être installé sur le CD pour assurer pleinement son rôle. Simplement cela peut éviter des soucis ultérieurs en cas de présence d'autres serveurs DHCP windows « indésirables ».

En effet lorsque un serveur DHCP sur un serveur autonome démarre, (il n'a pas à être autorisé… car il n'est pas dans un domaine) il envoit en requête d'information de présence en diffusion (broadcast). Si un autre serveur DCHP réponds, en lui indiquant qu'il est serveur de domaine, alors le serveur DHCP, tout autonome qu'il soit, stoppe son service. Par contre, s'il ne reçoit aucun acquittement, alors il démarre son service.

Un serveur DCHP autonome ne répondra jamais avec des informations de domaine (et pour cause…)

On comprends alors qu'il peut être intéressant que le 1° serveur DHCP soit dans le Domaine, car dans le cas ou un autre serveur de DHCP est installé :

- Soit il fait aussi partie du Domaine, (et là on sait ce que l'on fait…)
- Soit il est autonome, et lorsqu'il démarrera il recevra un acquittement de la part du serveur DHCP de Domaine, qui le fera arrêter sons service.

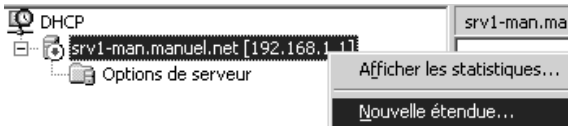
N.B : Ces échanges de trâmes concernent les serveurs DCHP montés sur un Windows Server 2000-2003 (le serveur DHCP NT4 ne gère pas ces échanges, et encore moins les autres serveurs DHCP existants …)

Création et Activation d'étendue :

La première chose à faire étant de créer une étendue (d'adresses IP) que DHCP doit administrer. Chaque serveur nécessite au moins une étendue présentant une réserve d'adresses IP disponibles pour la cession par bail à des clients. Plusieurs étendues sont créées dans les cas suivants :

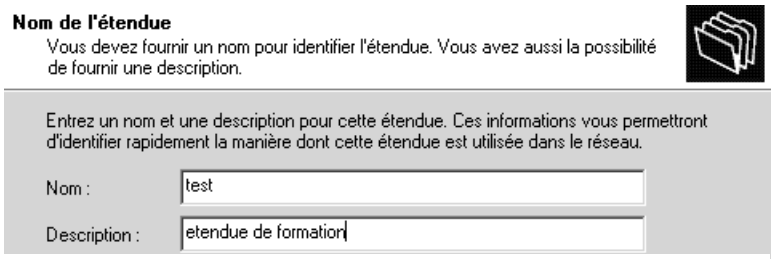
- Partage de la charge entre plusieurs serveurs DHCP.
- Attribution d'adresses IP spécifiques à un sous-réseau. (Une seule étendue peut être affectée à un sous-réseau spécifique.)

Pour créer une étendue Il faut se placer sur le serveur DHCP sur la gauche, et demander le menu **Action/Nouvelle Etendue...**

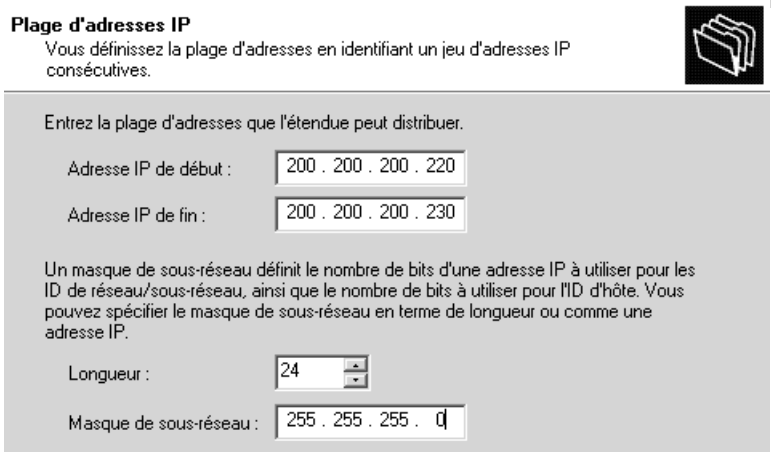


ceci déclenche un assistant qui va nous demander :

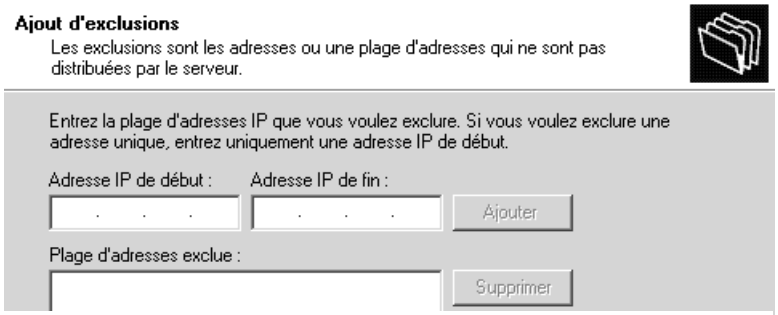
le nom de l'étendue



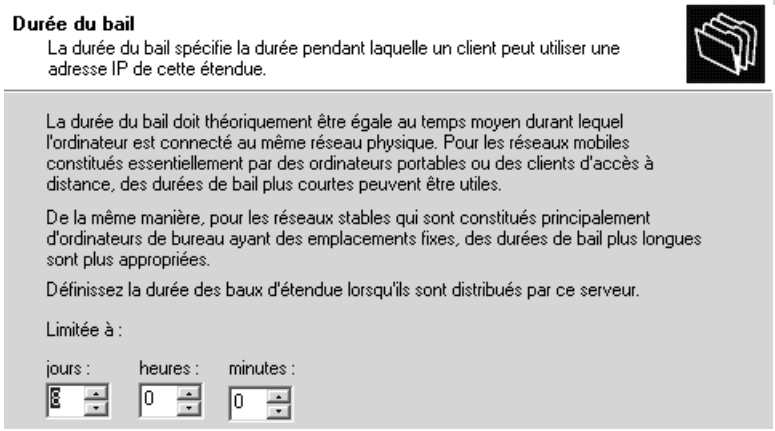
les plages d'adresses à attribuer



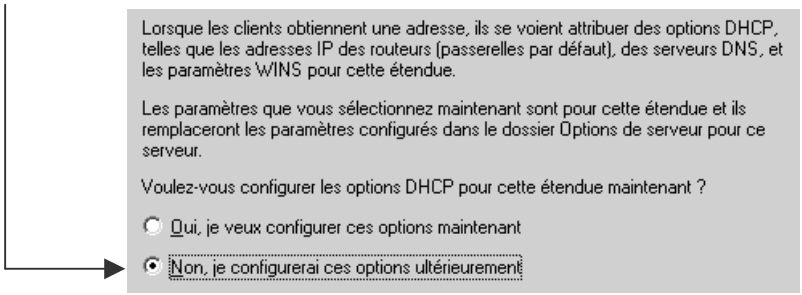
les éventuelles exclusions



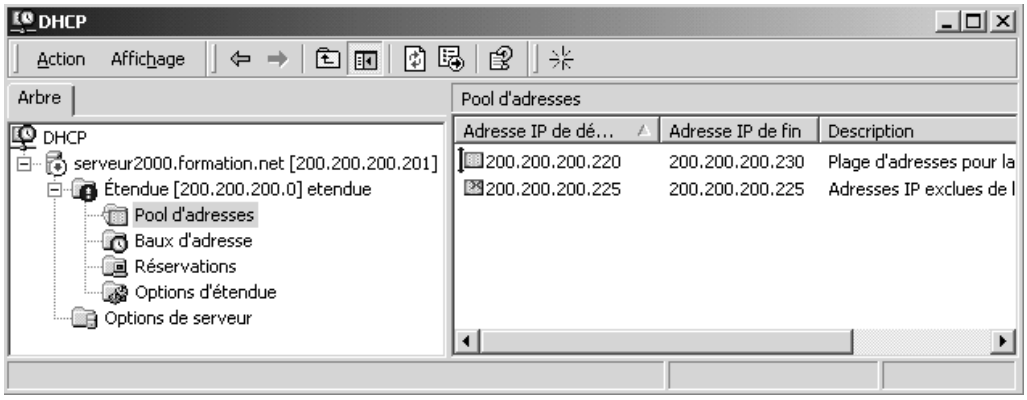
la durée du bail



Et si on veut indiquer un **Routeur**, un **serveur DNS** et un **serveur WINS (NON !)**



on obtient enfin

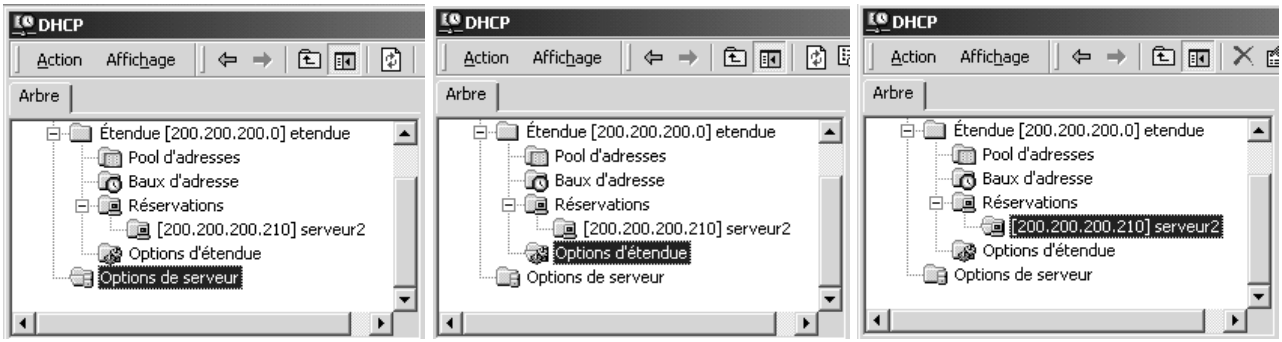


Configuration des options d'étendue DHCP:

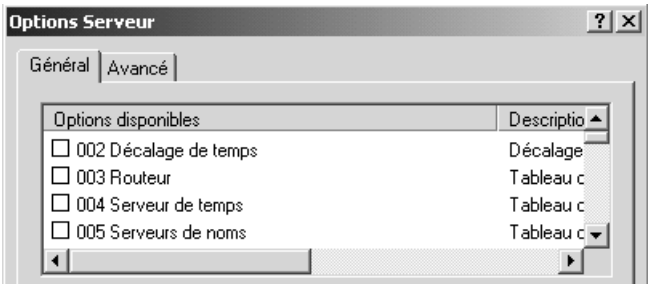
Une fois l'étendue DHCP créée, vous pouvez configurer des options pour les clients DHCP.

Il existe trois niveaux d'options, même si nous nous limiterons à **Serveur**.

- **Serveur - Globales**: Les options de serveur sont disponibles pour tous les clients DHCP. Elles ont utilisés lorsque tous les clients de tous les sous-réseaux requièrent les mêmes informations de configuration. Par exemple, lorsque tous les clients utilisent le même serveur DNS.
- **Etendue** : Les options limitées à l'étendue ne sont disponibles qu'aux clients dont l'adresse IP cédée par bail est issue de l'étendue. Par exemple, lorsque vous disposez d'une étendue distincte par sous-réseau, vous pouvez définir une adresse de passerelle par défaut pour chaque sous-réseau.
- **Reservation :** Les options limitées au client sont créées pour un client spécifique utilisant un bail d'adresse DHCP réservé.



N.B: Priorité des options : Les options globales sont toujours utilisées, sauf si les options limitées à l'étendue s'appliquent. De même Les options limitées à l'étendue s'appliquent toujours sauf su des options limitées au client existent.



Options DHCP standard :

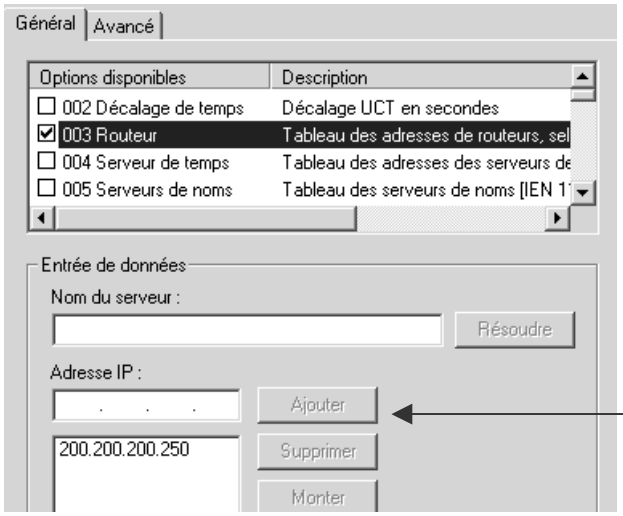
Pour configurer les option d'étendue DHCP :aller dans le menu

Options DHCP, cliquez sur **Serveur** - **Global**

Option	Description
003 Router	Spécifie l'adresse IP d'un routeur, telle que la passerelle par défaut.
006 DNS Servers	Spécifie l'adresse IP d'un ou plusieurs DNS.
015 Domain Name	Spécifie le nom de domaine DNS par défaut.
044 WINS/NBNS Servers	Spécifie l'adresse IP d'un serveur WINS accessible aux clients. Lorsque l'adresse d'un serveur WINS est configurées manuellement sur un client, cette configuration prévaut sur les valeurs configurées pour la présente option.
046 Type noeud	Type de diffusion pour la résolution de nom Netbios

Cochez l'option DHCP à configurer,:

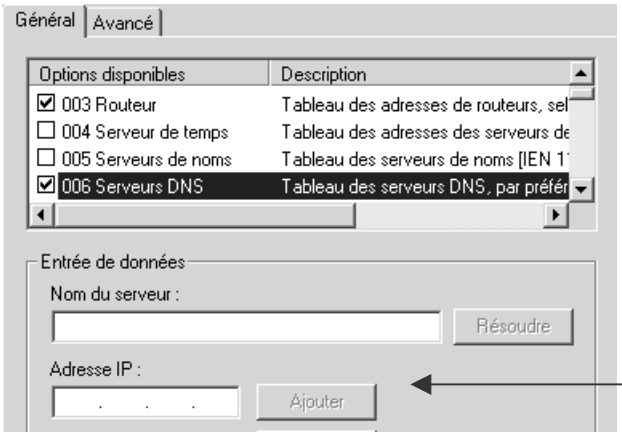
003 Routeur :



Si besoin bien sûr…

Et on indique l'adresse ip de la passerelle par défaut

006 Serveur DNS :

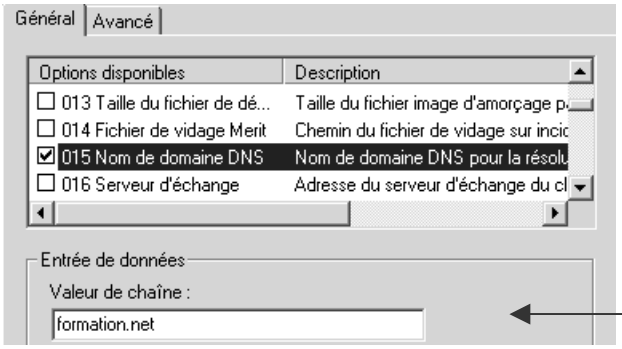


Obligatoire si utilisation du **DDNS**

Et on indique l'adresse ip du serveur DNS par défaut

N.B : en général on y associe également l'entrée permettant de spécifier le nom de domaine d'appartenance **15 Nom de domaine DNS (obligatoire si on utilise DDNS)**

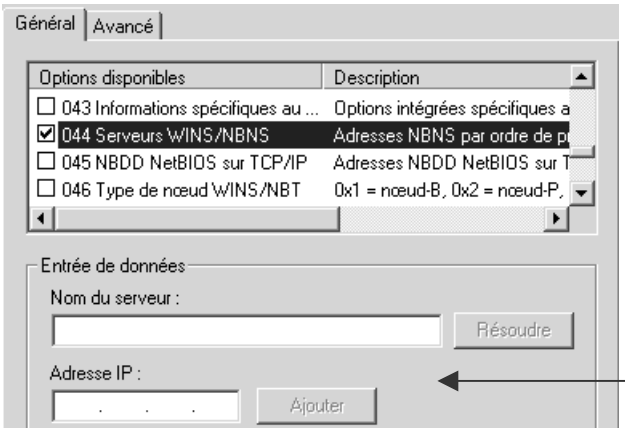
15 Nom de domaine DNS :



Obligatoire si utilisation du **DDNS**

Et on indique le nom de domaine

44 Serveur WINS :

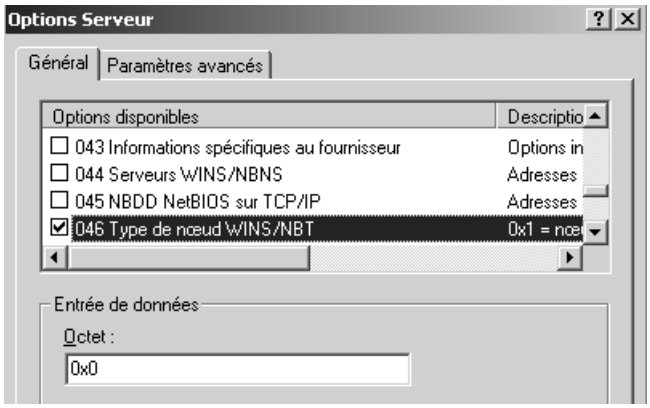


Si besoin bien sûr... et en général associé à

046 type de nœud

Et on indique l'adresse ip du serveur WINS par défaut

46 type de nœud WINS :



Si besoin bien sûr... toujours associé à

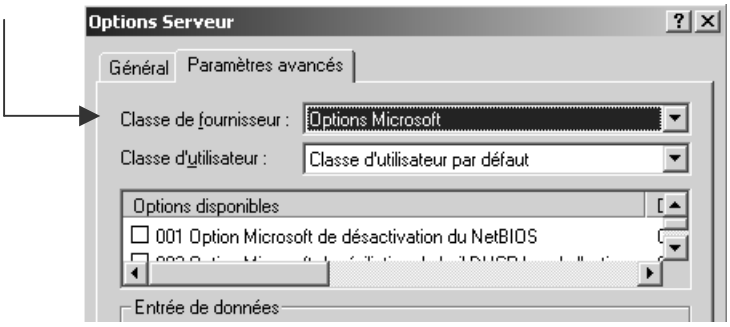
44 Serveur Wins

Les valeurs possibles étant :	**1**	**b-node**	**diffuser**
	2	**p-node**	**homologues**
	4	**m-node**	**mélangé - mixte**
	8	**h-node**	**hybride**

- **B-node (diffusion) :** utilise des broadcast pour la résolution des noms.
- **P-node** : utilise un serveur de nom NetBios (Wins) pour l'enregistrement et la résolution des noms Netbios.
- **M-node** : utilise des broadcast pour l'enregistrement. Pour la résolution, utilise d'abords des Broadcast, puis en l'absence de réponse passe ne mode P-node (donc utilise un serveur WINS)
- **H-node (hybride)** : utilise un serveur de nom NetBios (Wins) pour l'enregistrement et la résolution des noms Netbios . Si un serveur ne peut pas être trouvé, il passe en b-node. Continue à chercher une serveur WINS et repasse en p-node des qu'il en trouve un disponible

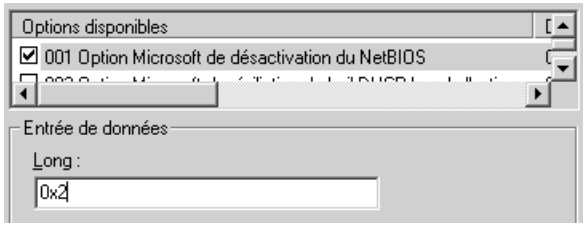
Options DHCP Microsoft :

Il faut dans les options demander l'onglet **Paramètres avancés** et indiquer **Options Microsoft**



Essentiellement deux options sont intéressantes :

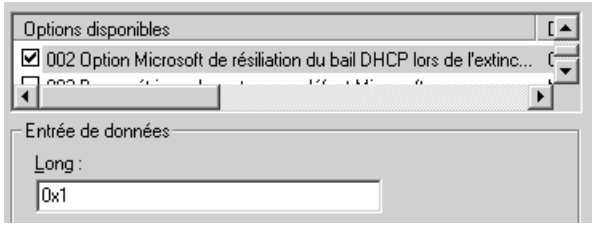
Options désactivation du netBIOS



2 désactive

Que à partir des clients windows 2000

Options libérer le bail DHCP à la fermeture



0 ne libère pas

1 libère

N.B : si on veut que les postes windows 98 libèrent également le bail lors de l'extinction du poste, il faut alors modifier 2 clés de la base de registre

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\DHCP

Valeur ReleaseLeaseOnShutdown

Type DWORD valeur 0x00000001

Et

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Shutdown

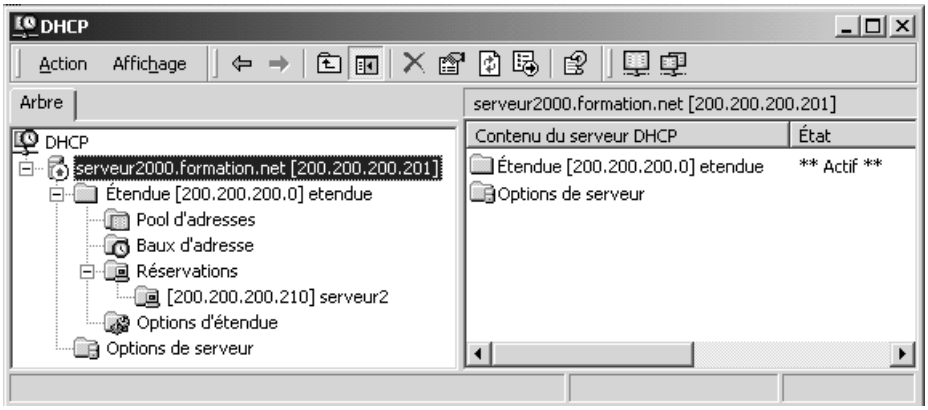
Valeur FastReboot

Type STRING valeur 0

Autoriser / Interdire un serveur DHCP:

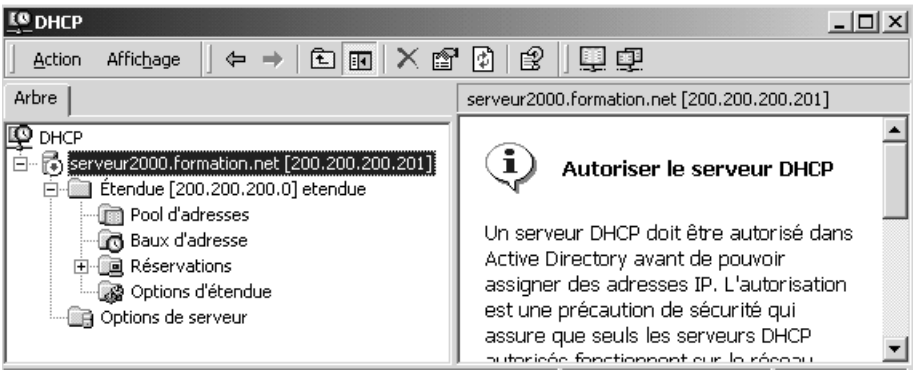
Une fois positionné sur le serveur, en haut à gauche, on demande le menu

Action / Autoriser



Un délais peut être nécessaire avant que l'autorisation ne devienne effective, et un rafraîchissement de l'écran sera utile.

Action / Interdire



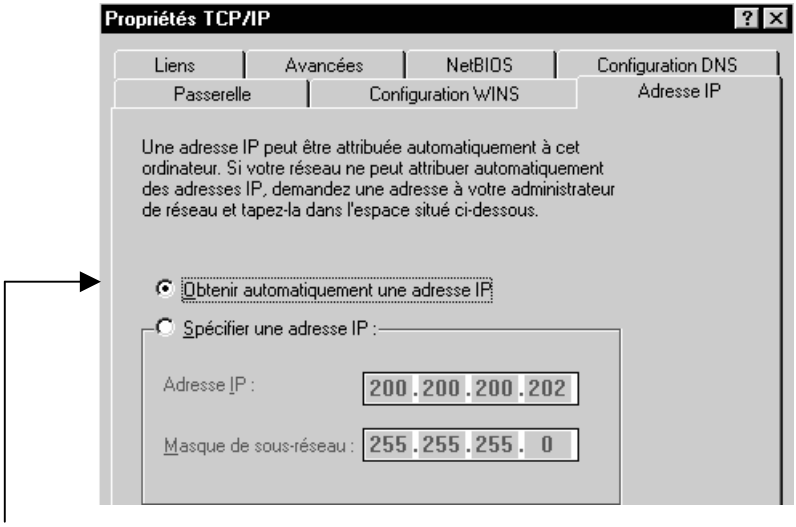
CLIENT DHCP

Un Client Windows 95-98

soit par **propriétés** de **voisinage réseau**,(sur le bureau)

soit par **démarrer / paramètres / panneau de configuration / réseau**

puis propriétés de TCP/IP

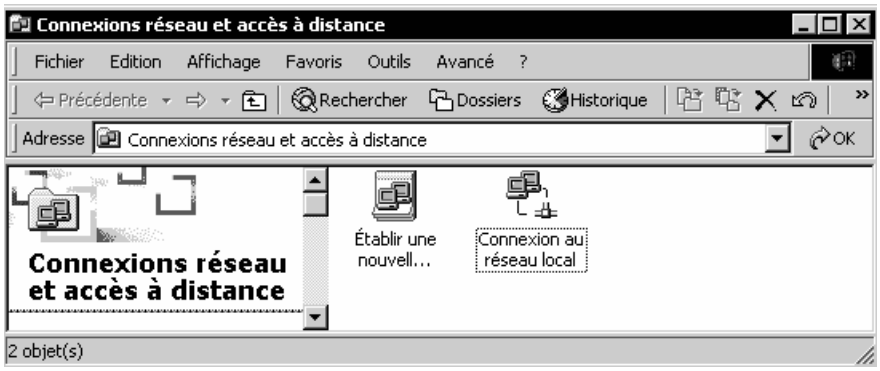


Lorsque on demande une adresse automatique, tout le reste du paramétrage IP devient "inactif"

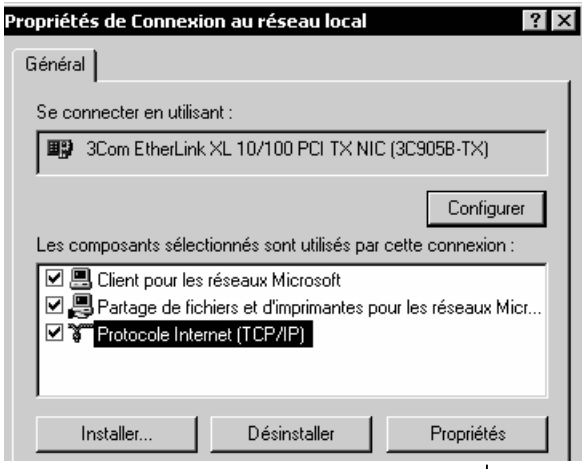
Client DHCP NT 2000:

Un poste devient client DHCP simplement en demandant dans le paramétrage de TCP/IP « **Obtenir automatiquement une adresse IP** »

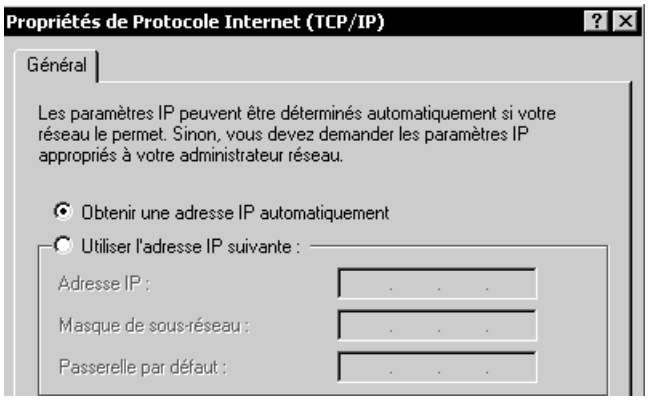
- soit par **propriétés** de **favoris réseau**,(sur le bureau)
- soit par **démarrer / paramètres / connexion réseau** et accès à distance
- soit par **démarrer / paramètres / panneau de configuration / connexion réseau et accès à distance**



puis **propriétés de connexion au réseau local**



puis **Propriétés** de TCP/IP



Lorsque on demande une adresse automatique, tout le reste du paramétrage IP devient "inactif"

Gestion des adresse dynamiques :

- Sous Windows98, a travers l'utilitaire **winipcfg** on peut demander de libérer – renouveller une adresse reçue dynamiquement...

- Sous 2000, A travers l'utilitaire **ipconfig** on peut demander de libérer – renouveller une adresse reçue dynamiquement...par les options

  Ipconfig /release

  et

  Ipconfig /renew ...

Remarques

N.B: si aucun serveur DHCP n'est présent, un mécanisme dit "adresses APIPA" se met en oeuvre, (voir "adresses automatiques APIPA") uniquement pour des postes **Windows 98** et **Windows NT 2000** les postes **Windows 95** et **Windows NT 4.0** ne gèrent pas les adresses APIPA

GESTION SERVEUR DHCP

Adresse fixes avec DHCP :

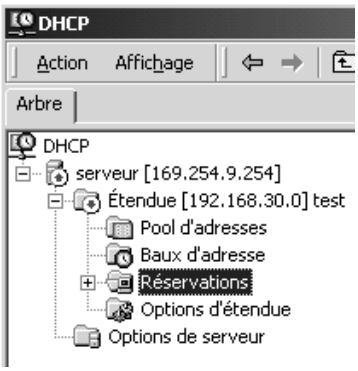
La fonctionnalité la plus importante, est celle de pouvoir connaître l'adresse Ip qui a été affectée à telle ou telle machine...

Pour palier a ce manque d'information (association adresse ip et nom machine) on peut travailler de deux manière différentes :

- On affecte une adresse fixe à un poste, par le biais d'un mecanisme de réservation à base d'adresse mac
- On fait agir le serveur DHCP avec le serveur DNS (ou WINS le cas échéant), on parlera alors de DDNS.

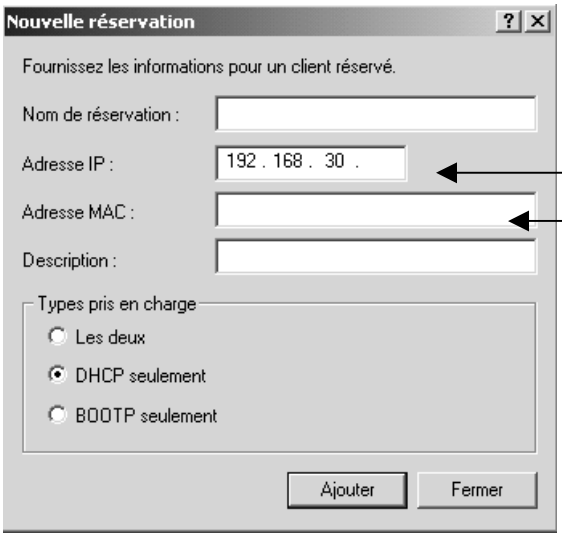
Réservation d'adresse :

Pour réserver une adresse, il est nécessaire de se placer sur le dossier des réservations dans l'onglet de l'étendue,



Et demander par un clic droit **Réservation**

On obtient alors



Il faut indiquer ici au minimum :

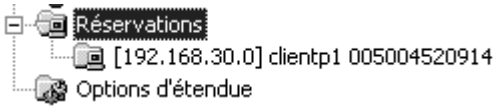
L'adresse ip

L'adresse mac-(ethernet-réseau) de la carte réseau du poste visé

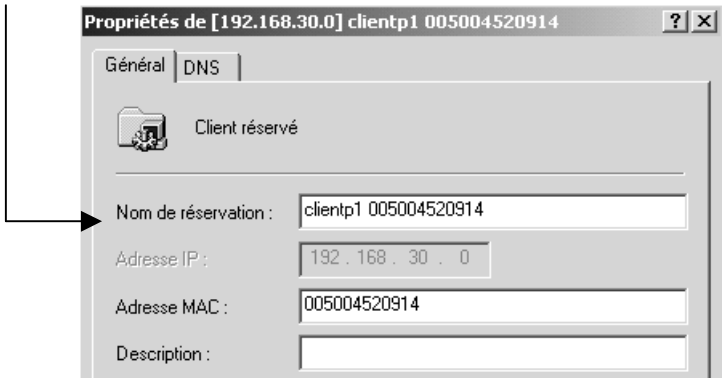
La réservation est faite. Désormais lorsque le poste ayant l'adresse physique xxxxxxxxxx fera sa demande d'adresse ip, il obtiendra toujours celle-là

Dans la pratique on souhaiterait visualiser rapidement des adresses mac utilisées, en correspondance avec les adresses IP....

Pour obtenir un affichage des réservation assez parlant, comme celui-ci



il faut remplir aussi le champs **Nom de réservation** avec l'adresse mac.



Sauvegarde automatique serveur DHCP :

Par défaut, Windows sauvegarde la base DHCP toutes les heures....cela consiste en fait à dupliquer le contenu du dossier DHCP a l'intérieur de system32.

la sauvegarde s'effectue dans un dossier nommé **backup/jet**

Dossier DHCP en **system32\dhcp**

Dossier Sauvegarde en **\backup\jet**

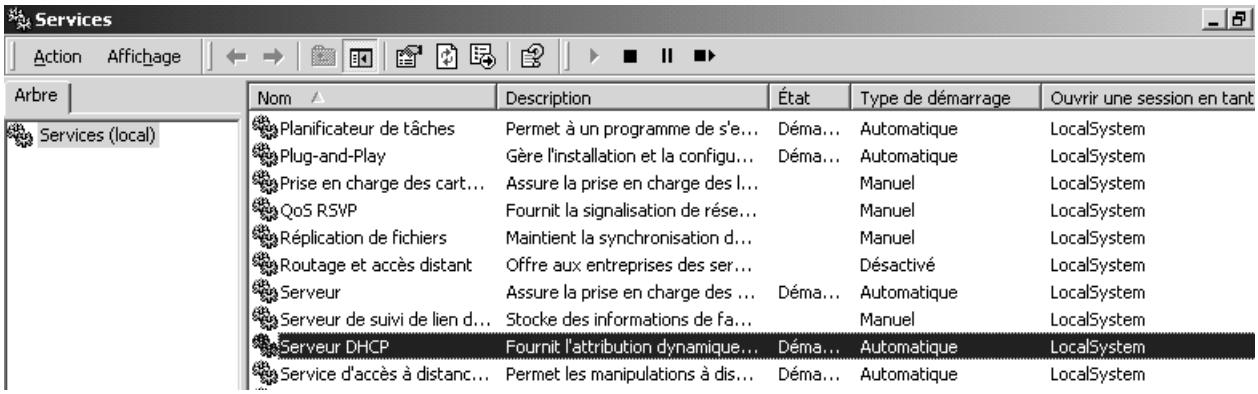
en cas de problème détecté, win2000 peut essayer d'utiliser automatiquement cette sauvegarde.

Sauvegarde manuelle serveur DHCP :

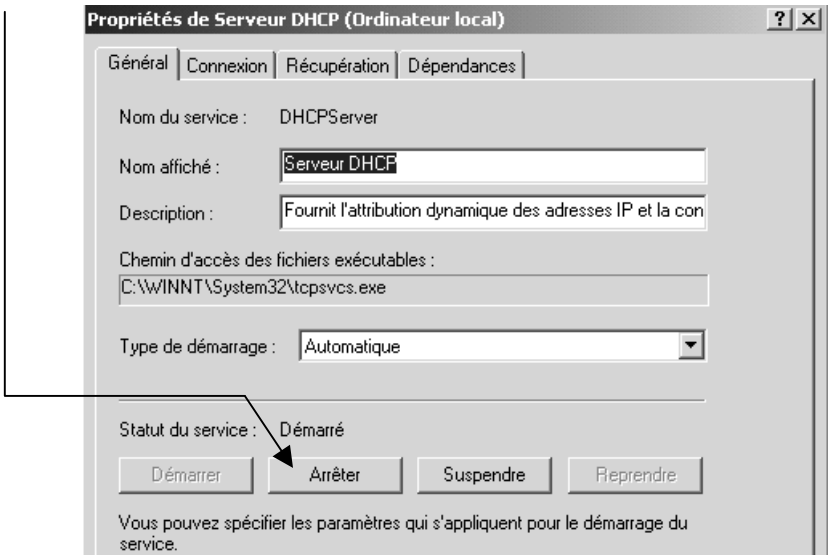
Il est possible de forcer une sauvegarde manuellement. Il va falloir arrêter le service DHCP, copier les fichiers de sauvegarde a leur emplacement d'origine, puis re-démarrer le serveur DHCP.

Pour stopper le service dhcp on demande

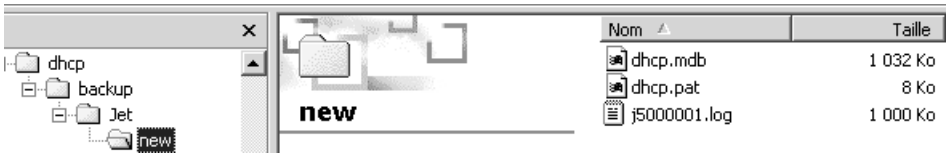
Programme / outils d'administration / services /



Dans les propriétés du service DHCP on arrête le service

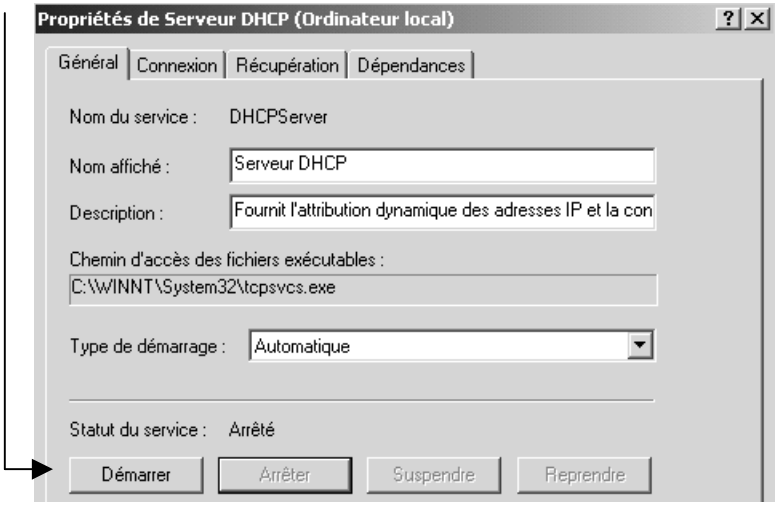


On copie le contenu du dossier **Winnt\system32\dhcp\backup\jet\new**



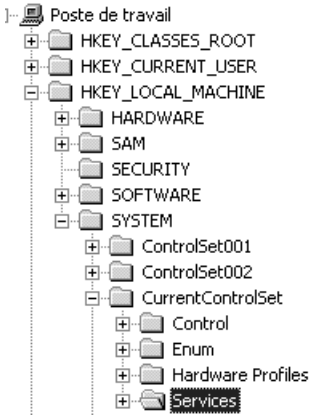
dans le dossier **Winnt\system32\dhcp**

puis on re-démarre le service



Paramétrage sauvegarde automatique :

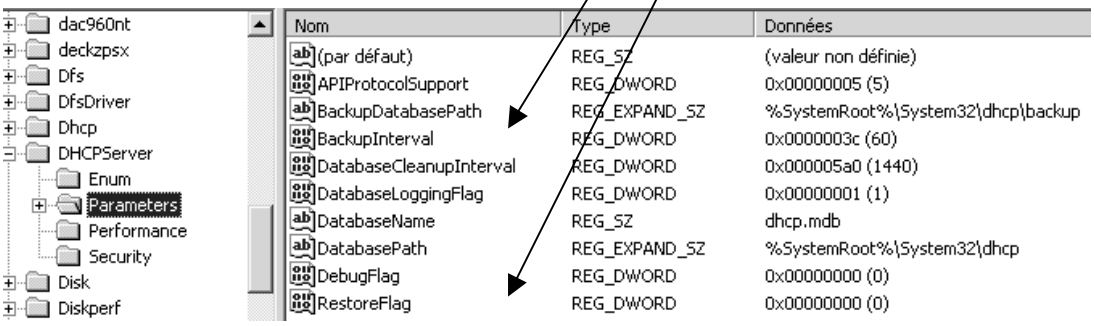
Le paramétrage de la sauvegarde se trouve dans la base de registre .



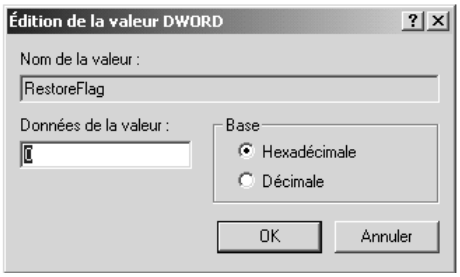
Dans la section **Parameters** se trouvent les 2 clés qui nous interessent

BackupInterval

Restore flag



Par défaut vaut 0, si un indique qu'une restauration doit être effectuée. Lorsque cette restauration sera faite, la valeur sera repositionnée à 0



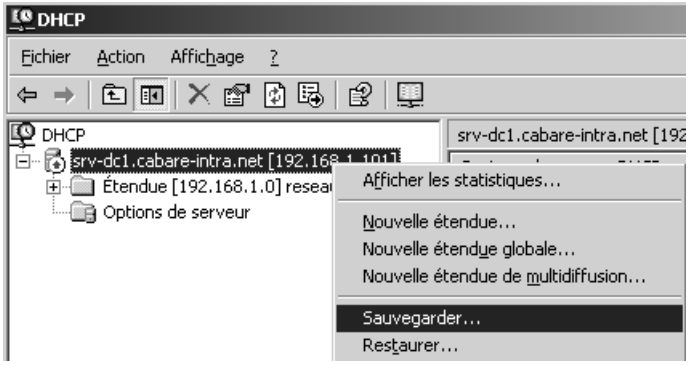
Par défaut vaut 60 mn soit 3c en hexa. Indique tous les « combien » la restauration doit être effectuée.

Ici a été modifié à 10 mn...

Sauvegarde sous 2003 srv :

Les choses se sont bien simplifiées, puisqu'il suffit maintenant de demander depuis l'interface d'administration

Clic droit sur serveur / **Sauvegarder…**



Compression base DHCP :

Lorsque la base Dhcp, c'est à dire le fichier **dhcp.mdp** est trop volumineux, alors on peut le compresser, (environ une fois par mois par exemple)

On utilise l'utilitaire en ligne de commande **jetpack.exe** avec la syntaxe suivante :

Jetpack dhcp.mdb

N.B: on prendra soin de faire cela sur un jeux de sauvegarde, puis de restaurer cette sauvegarde ensuite. Ne jamais compacter une base en cours d'utilisation...

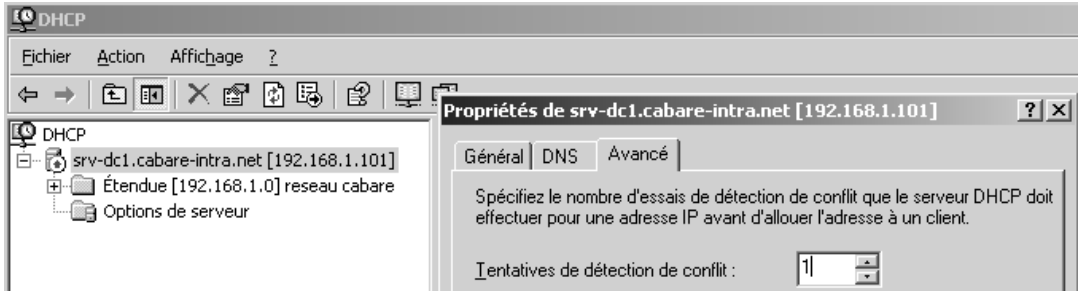
Serveurs DHCP Redondants :

Comme tout serveur important, on peut avoir besoin de fiabiliser notre serveur DHCP. Plusieurs techniques sont possible, en voici plusieurs très simples, basées sur des approchent différentes :

- On distribue 2 plages d'adresses différentes sur chaque serveur. Les deux serveurs DHCP sont totalement indépendants...
  - En cas de panne, la reprise est automatique par le 2° serveur
  - Il faut avoir une bonne quantitée d'adresses IP : le double !

- On distribue la même plage, avec vérification préalable avant tout octroit d'adresse.
  - En cas de panne, la reprise est automatique par le 2° serveur
  - Cela accroît légèrement le trafic réseau

  Cette vérification doit être faite par chaque serveur en demandant les **propriétés** du serveur, onglet **Avancée**, et en positionnant **Tentatives de détection de conflit** à **1**



N.B: cette technique génère un léger surcroît de trafic, car le serveur DHCP va effectuer un ping avant d'attribuer une adresse.

- On Crée deux fois la même plage sur chaque serveur, mais en plus on effectue des exclusions de 50% des adresses dans chacune des plages, et opposées (croisées) sur chaque serveur
  - En cas de panne, la reprise est manuelle sur le 2° serveur, il suffit de lever l'exclusion sur la plage

ADRESSES APIPA - ALTERNATIVES

Principe des adresses APIPA:

Dans les réseaux locaux simples, on peut mettre en place un nouveau système d'attribution automatique des adresses IP, donc sans ni attribuer une adresse IP fixe à chaque poste, ni avoir recours à un serveur DHCP...

Le fonctionnement est le suivant :

1. Une machine installée avec un protocole TCP/IP tente de contacter un serveur DHCP pour recevoir une adresse IP de manière dynamique (elle doit être configurée pour...)
2. Si aucun serveur DHCP ne réponds, la fonction APIPA génère une adresse IP au format 169.254.xxx.xxx avec un masque de sous-réseau 255.255.0.0. Si cette adresse est déjà utilisée la fonction APIPA en sélectionne une autre pour un maximum de 10 coups.
3. Une fois une adresse prise, l'ordinateur la diffuse et l'utilise jusqu'à ce qu'un serveur DHCP n'apparaisse opérationnel sur le réseau !

quelques remarques :

- l'IANA (Internet Assigned Number Authority) à réservé les adresses de **169.254.0.0** à **169.254.255.255** à la fonction APIPA, ces adresse n'étant pas routables !
- Par conséquent les machines utilisant des adresse APIPA ne peuvent communiquer qu'avec des machines faisant partie du même sous-réseau, et dotée d'un adresse au format 169.254.xxx.xxx

APIPA et Windows NT 2000:

Pour que NT 2000 gère les adresse APIPA, il est nécessaire d'utiliser TCP/IP comme protocole et de demander le bouton Option "Obtenir une adresse IP automatiquement" dans Propriétés de Protocole Internet (TCP/IP)

Par défaut les adresses APIPA sont actives, il est possible de les inhiber en allant dans la base de registre et en demandant

HKEY_LOCALMACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID_carte_réseau et en lui ajoutant l'entrée

IPAutoconfigurationEnabled avec une valeur de 0

(si cette entrée n'existe pas ou que sa valeur est fixée à 1 APIPA est activée)

N.B: Windows 98 **gère** également APIPA

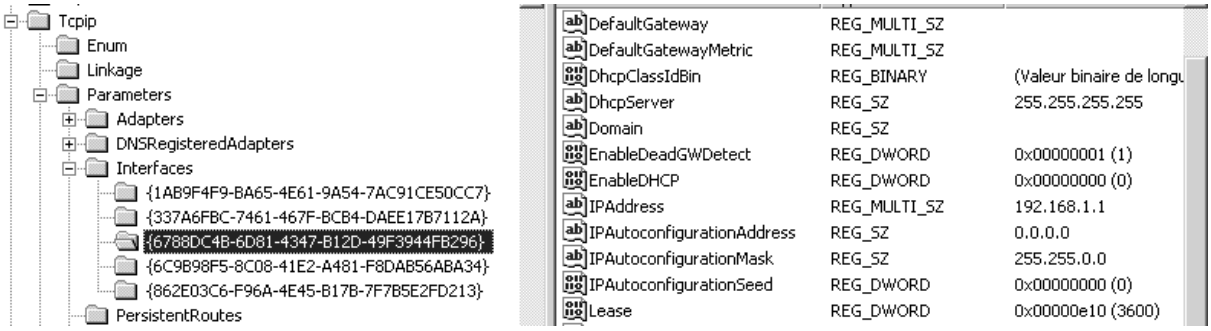
N.B: Windows NT 4.0 **ne gère pas** les adresses APIPA

Désactivation adresse APIPA:

Par défaut les adresses APIPA sont actives, il est possible de les inhiber en allant dans la base de registre et en demandant

Pour chaque carte réseau sélectivement :

HKEY_LOCALMACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID_carte_réseau et en lui ajoutant l'entrée

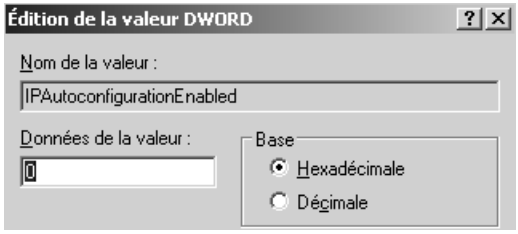


IPAutoconfigurationEnabled avec une valeur de 0

(si cette entrée n'existe pas ou que sa valeur est fixée à 1 APIPA est activée)

On peut aussi invalider les adresse APIPA globalement pour toutes les cartes en ajoutant la même clé

IPAutoconfigurationEnabled avec une valeur de 0



Directement au niveau de l'entrée

...CurrentControlSet\Services\Tcpip\Parameters

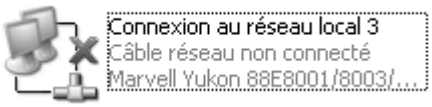
Désactivation Media Sense:

Windows dispose de la fonction de « Détection de support ». **Media Sense**

Un « état de la liaison » est défini comme étant le support physique connecté ou inséré sur le réseau.

Chaque fois que Windows détecte un état « inactif »  sur le support, il supprime les protocoles liés de cette carte jusqu'à ce que l'état détecté soit de nouveau « actif ».

Pour que votre carte réseau ne détecte plus cet état,



il faut modifier le registre

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Ajoutez la valeur de Registre suivante :

Nom de la valeur : **DisableDHCPMediaSense**

Type de données : **REG_DWORD - Booléenne**

Plage de données de la valeur : 0, 1 (False, True) Par défaut : 0 (False)

Adresse IP alternative:

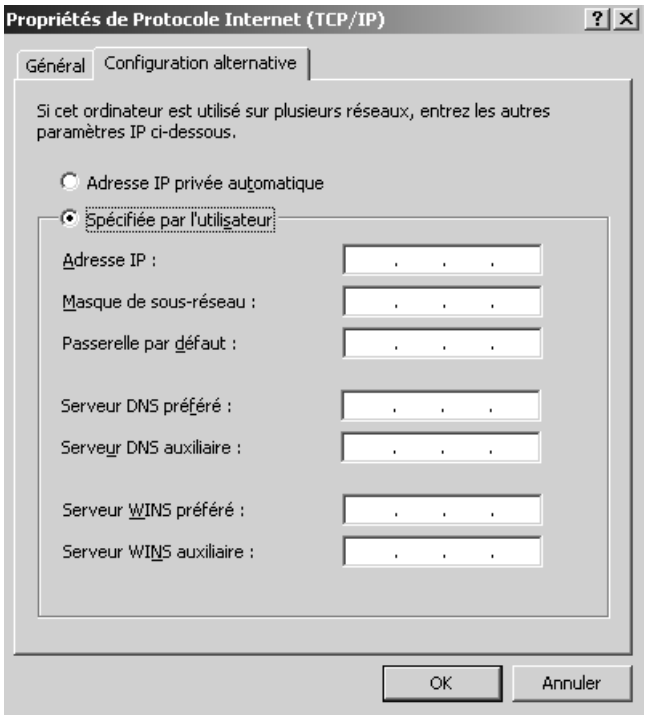
Si un client DHCP ne trouve pas de serveur DHCP, il peut donc prendre une adresse APIPA.

Mais il est possible de lui spécifier une adresse alternative, qui lui sera attribuée dans le cas ou un serveur DHCP est manquant. Et donc prenant la place du mécanisme APIPA.

Cela peut permettre ainsi de pouvoir avoir sur un portable, une configuration « Bureau » en tant que client DHCP, et une configuration « maison » avec une adresse privées classique.

N.B : seuls les **Admins** ou **Opérateurs de configuration Réseau** peuvent modifier ce paramétrage.

Lorsque sur une carte on est en client DHCP, alors un onglet supplémentaire est activé : l'onglet **Configuration alternative**



Il est possible ici d'indiquer une configuration complète...

N.B : si on utilise ce mécanisme de **Configuration Alternative**, il ne faut pas alors dévalider les adresses APIPA avec la modification de la base de registre du chapitre précedent.

Toute présence de clé **IPAutoconfigurationEnabled** annulera ce mécanisme

DYNAMIC DNS WINDOWS 2000

Principe du DDNS :

Les systèmes à partir de Windows 2000 exploitent une autre fonction DNS : le **DDNS**.

- Lorsqu'un client Windows 2000 ou XP démarre, il demande à son serveur DNS local d'ajouter son nom dans la base de données.
- Pour les clients de versions antérieures à Windows 2000 qui ne savent pas demander au serveur DNS de les ajouter à la base de données de la zone, le serveur DHCP de Windows 2000 remplira cette tâche pour eux. Ainsi, même les anciens PC peuvent être ajoutés dynamiquement au fichier de zone

Pour utiliser cette fonction il faut travailler

1. coté serveurs DHCP
2. coté Serveur DNS,
3. mais aussi coté client, 2000 - XP ou « autres ».

Coté serveur DHCP :

Il faut effecteur une configuration sur les 2 serveurs conjointement :

- Sur le **serveur DHCP** l'adresse du ou des **serveurs DNS à utiliser** pour cette opération, ainsi que le nom de domaine par défaut

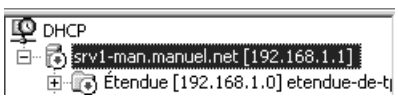
  006 Serveur DNS :

  15 Nom de domaine DNS :

  voir « configuration d 'étendues » d'un serveur DHCP

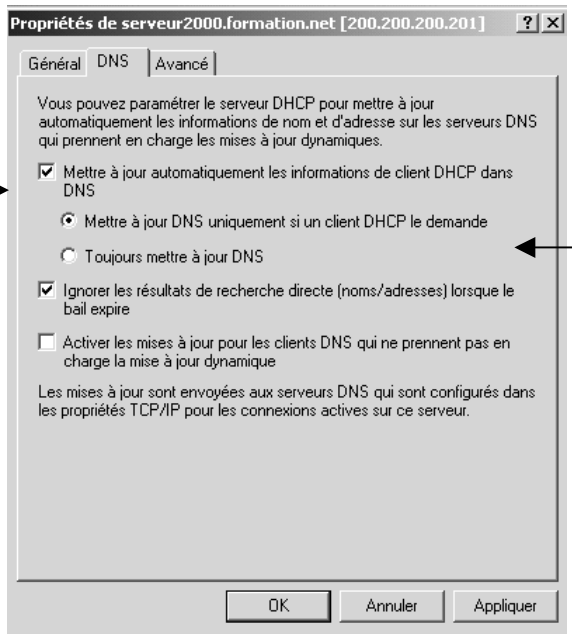
- Un **serveur DHCP 2000-2003** est capable de demander la mise à jour dynamique de son enregistrement auprès du **serveur DNS**. Son paramétrage par défaut le lui autorise

Dans **propriétés** du **serveur DHCP**



onglet **DNS**

Cochée par défaut

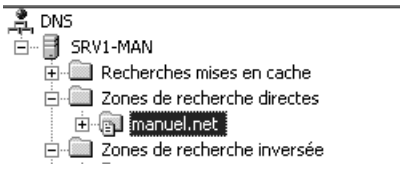


Donc, Par défaut un **serveur DHCP** NT2000 ***enregistre auprès du serveur DNS*** les **client DHCP** NT2000 qui en font la demande…

N.B : Si un client DHCP 2000 XP avait sa case «**demande d'enregistrement**» non coché, on pourrait dans le serveur DHCP demander de « **Toujours mettre à jour le DNS** »

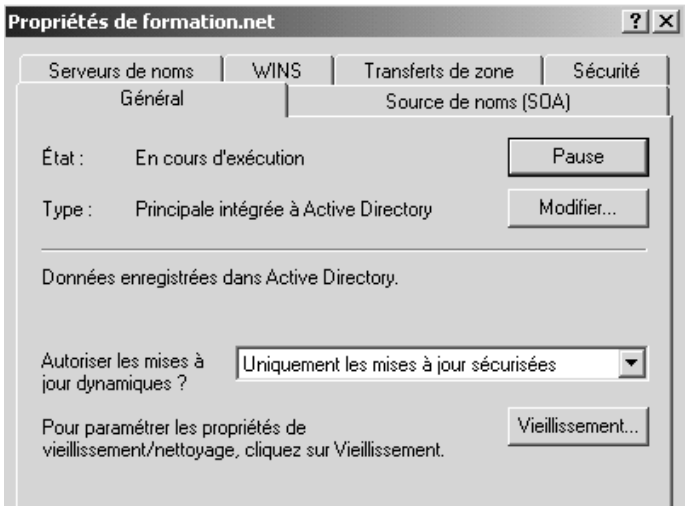
Coté serveur DNS :

Sur de la zone du **serveur DNS**



On demande **Propriétés** onglet **Général**

- Sur le serveur DNS d'Autoriser les **mises à jour dynamiques**

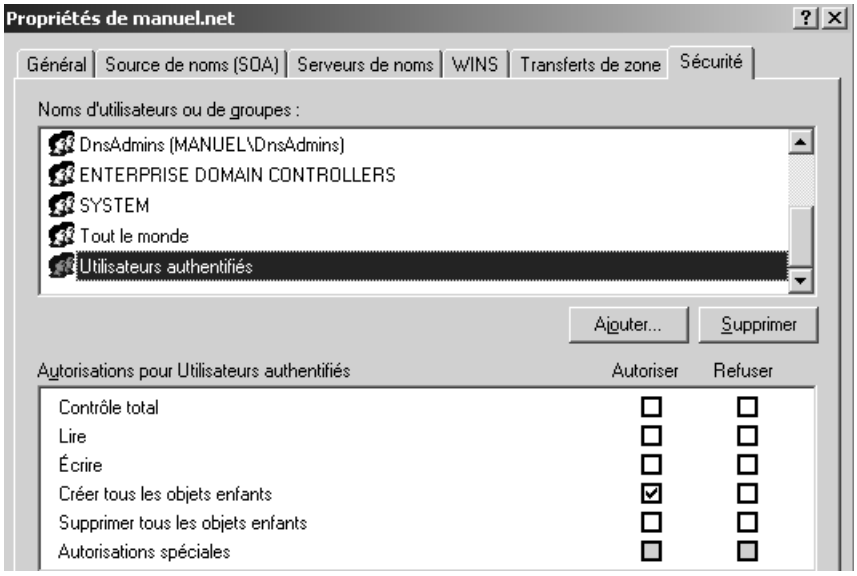


Il faut autoriser les mises à jours dynamiques en

- "Oui" si on n'a pas intégré DNS à "Active directory"
- "Uniquement les mises à jour sécurisées" si le DNS est intégré à Active directory

Les membres du Groupe **Utilisateurs Authentifiés** ont le droit de s'inscrire dans le DNS de manière automatique (donc tous les utilisateurs et ordinateurs ayant un compte dans AD)

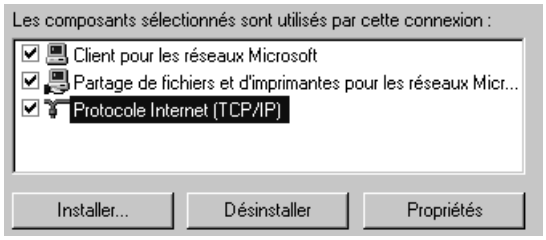
Si on demande de voir les permissions de sécurité de notre zone dans le DNS on obtient



Coté Clients:

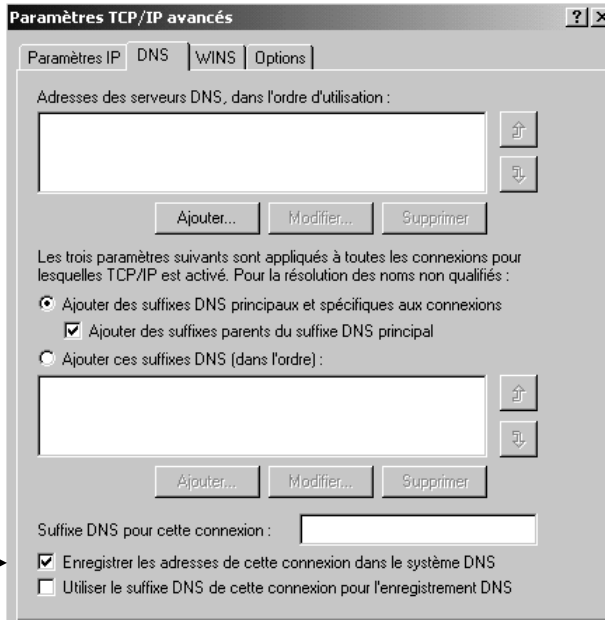
Fonctionnement standard depuis des machines NT2000 :

- Un **client DHCP NT 2000** est capable de demander la mise à jour dynamique de son enregistrement auprès du serveur DHCP. Son paramétrage par défaut le lui autorise



Dans les propriétés Avancées TCPIP

Onglet **DNS**



Cochée par défaut

- Sous 2000, A travers l'utilitaire **ipconfig** on peut demander de libérer – renouveller une adresse reçue dynamiquement...par les options ***/release /renew*** ...

- Mais on peut aussi utiliser des options permettant de de recréer l'inscription de l'hôte dans le DNS A travers l'utilitaire **ipconfig** par les options **/flushdns** et **/registerdns** ...

  ipconfig /flushdns et **ipconfig /registerdns**

```
/flushdns    Vide le cache de la résolution DNS.
/registerdns Actualise tous les baux DHCP et réinscrit les noms DNS.
```

  Ce qui fait que un séquence complète de libération adresse IP, purge cache DNS, Reprise d'adresse Ip et Réinscription dans le DNS serait

  ipconfig /flushdns

  ipconfig /release

  ipconfig /renew

  ipconfig /registerdns

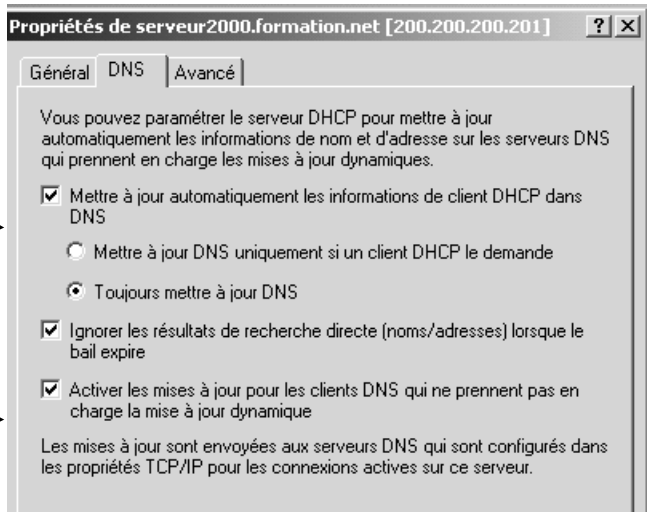
Fonctionnement depuis des machines « avant » NT2000 :

Il faut bien comprendre que pour les clients DHCP de type windows 95-98, et même NT4.0, ceux-ci ne sont pas capables d'effectuer une demande d'inscription auprès du DNS

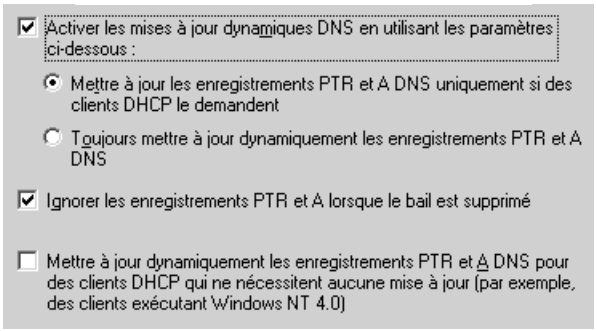
Mais le serveur DHCP NT2000 peut le faire à leur place à la double condition de demander dans son paramétrage DNS :

1. Activer les mises à jour pour les clients DNS qui ne prennent pas en charge la mise à jour dynamique
2. Mettre à jour automatiquement les informations de client DHCP dans DNS + Toujours mettre à jour DNS

Donc dans **propriétés** du **serveur DHCP** onglet **DNS**



Libéllés sous 2003 SRV

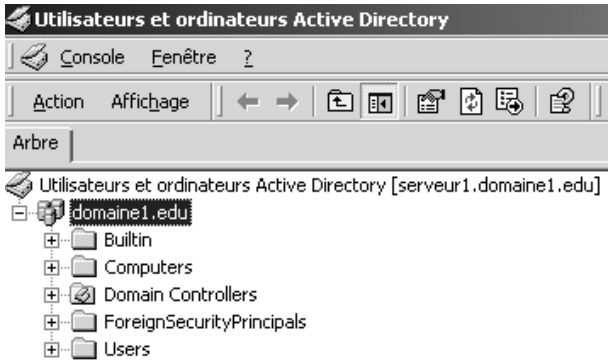


N.B: il est fondamental de distribuer par le DHCP deux paramètres qui sont le "*code 006 serveur DNS*" et le "*code 15 nom de domaine*". (cf chapitre DHCP)

STRUCTURE PAR DEFAUT D'ACTIVE DIRECTORY

Repérer la structure d'AD :

Il faut lancer la console **Utilisateur et ordinateur Active Directory** et l'on obtient alors



La visualisation complète est possible en demandant le menu contextuel **fonctionnalités avancées**

Il existe des **conteneur**

et des **Unités Organisationelles**

Builtin (conteneur, pas de GPO)

Contient les groupes de sécurité intégrés par défaut

Computers (conteneur, pas de GPO)

Emplacement par défaut des comptes d'ordinateur

Domain Controllers (Unité Organisationelle, GPO possible)

Emplacement par défaut des contrôleur de domaine

ForeignSecurityprincipals (conteneur, pas de GPO)

Contient les SID des domaines externes approuvés

Users (conteneur, pas de GPO)

Emplacement par défaut des comptes d'utilisateur et des groupes

LostAndFound (conteneur, pas de GPO)

Contient les objets orphelins, dont les conteneur ont été supprimés

System (conteneur, pas de GPO)

Contient les paramètres systèmes de AD

Notions sur la structure d'AD :

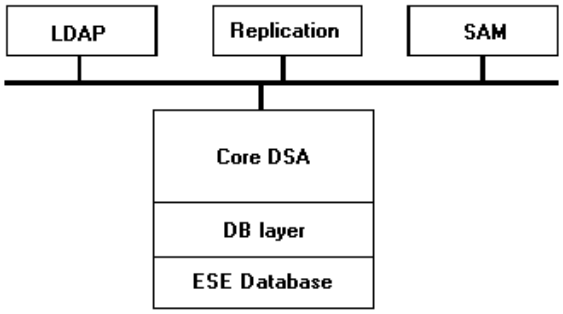
Le service Active Directory de Windows 2000 s'intègre dans le processus d'autorité de sécurité locale (**LSASS.EXE**) et peut ainsi gérer des informations confidentielles, telles que des mots de passe de comptes

trois composants assurent la communication avec d'autres services internes ou externes :

L'interface LDAP (conforme à RFC 2222) donne accès à des clients LDAP, tels que des stations de travail Windows 2000 ou Windows 9*x* avec le package client Active Directory.

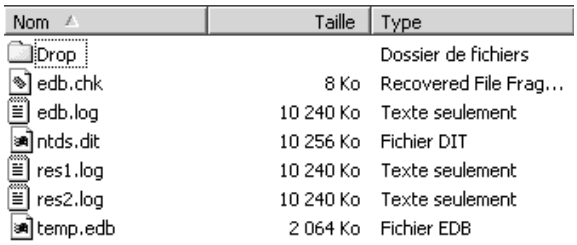
L'interface de Réplication assure la réplication d'annuaires avec d'autres contrôleurs de domaine Active Directory.

L'interface SAM met en œuvre des services de sécurité



Le service Active Directory est mis en œuvre en trois couches : l'agent du service d'annuaire (DSA, *Directory Service Agent*) principal, la couche de base de données (DB) et le moteur d'enregistrement extensible (ESE, *Extensible Storage Engine*).

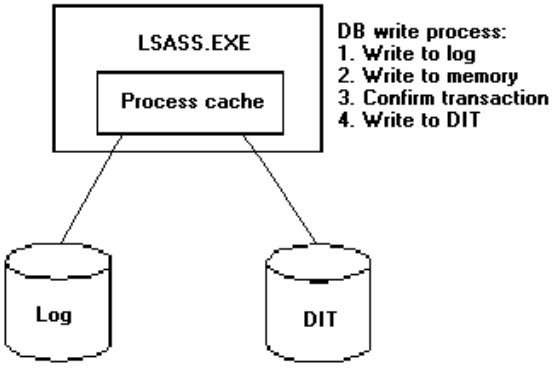
La base de données Active Directory est stockée dans le fichier **Ntds.dit** et des journaux de transactions sont stockés dans les fichiers **.log**



Nom	Taille	Type
Drop		Dossier de fichiers
edb.chk	8 Ko	Recovered File Frag...
edb.log	10 240 Ko	Texte seulement
ntds.dit	10 256 Ko	Fichier DIT
res1.log	10 240 Ko	Texte seulement
res2.log	10 240 Ko	Texte seulement
temp.edb	2 064 Ko	Fichier EDB

Si le contrôleur de domaine ne peut pas s'arrêter normalement (coupure de courant...), la base de données n'est plus à jour. Les journaux des transactions sont alors employés pour récupérer la base de données. L'image disque est toujours maintenue à jour selon le mécanisme suivant:

1. Lsass.exe écrit la modification dans le fichier journal.
2. Lsass.exe écrit la modification dans une page de base de données dans la mémoire tampon.
3. Lsass.exe confirme la transaction.
4. La modification est écrite sur disque (lors de l'arrêt ou pendant les périodes d'inactivité).



Pour améliorer les performances des contrôleurs de domaine devant traiter des débits élevés de demandes,

- placez le système d'exploitation Windows 2000 sur un premier disque dur,
- le fichier de base de données Active Directory sur un deuxième
- les fichiers journaux sur un troisième.

Utilisez toujours des lecteurs mis en miroir sur les contrôleurs de domaine pour éviter la perte de données résultant d'un incident de disque dur

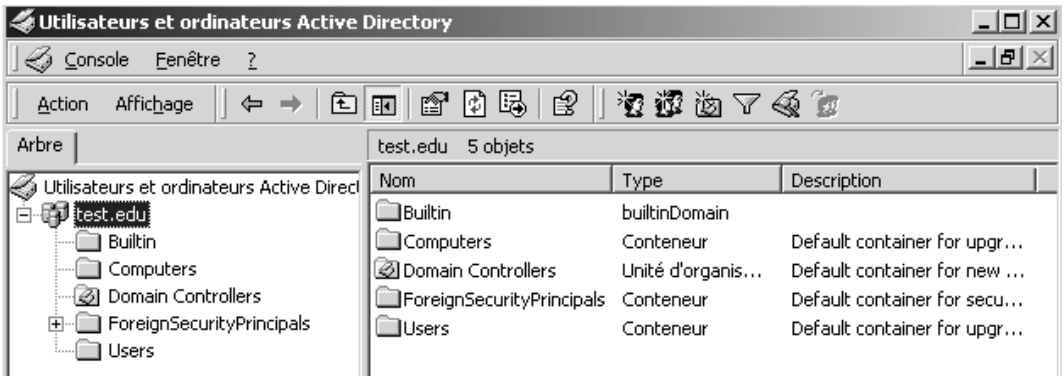
Les paramètres de stockage de la base de données Active Directory sont relativement prévisibles. De nombreuses sociétés n'atteindront peut-être jamais un annuaire de 100 000 utilisateurs et il convient donc de noter que (du point de vue de l'utilisation de l'espace disque) les besoins en matériel du contrôleur de domaine ne sont pas énormes (dans la plupart des cas, **la base de données d'annuaire reste de loin inférieure à 1 Go**).

Cf livre blanc "Dimensionnement de la base de données Active Directory" microsoft

PUBLICATION DANS ACTIVE DIRECTORY

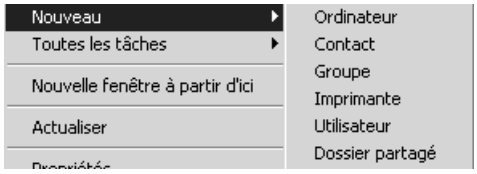
Publication d'un dossier partagé :

Il faut lancer la console **Utilisateur et ordinateur Active Directory**



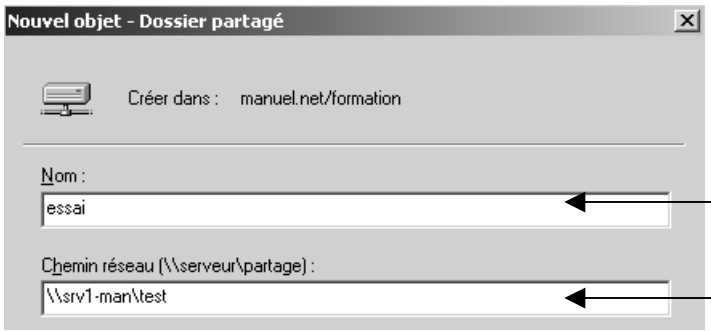
se placer dans l'arborescence là où l'on veut créer notre objet (ou créer une UO **formation** pour l'occasion)

puis dans cette **Unité Organisationnelle**



ici par exemple un **Dossier partagé**

ce qui amène la boite suivante

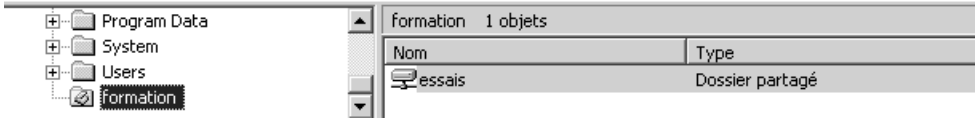


On indique le nom de l'objet que l'on publie

Ici **essai**

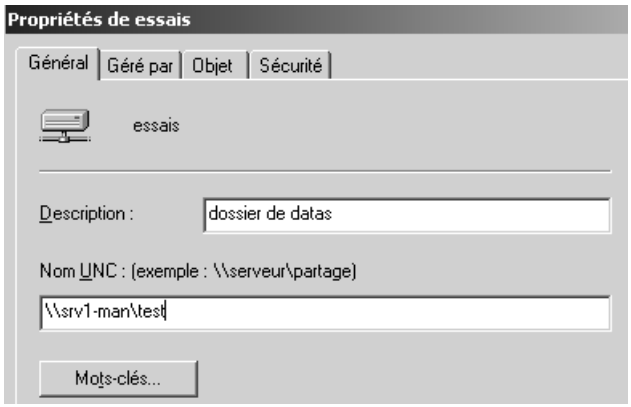
Et bien sûr on donne son chemin réseau....(une machine 2000-XP ou NT4.0, ou 98)

mon dossier partagé est "publié" désormais dans Active Directory

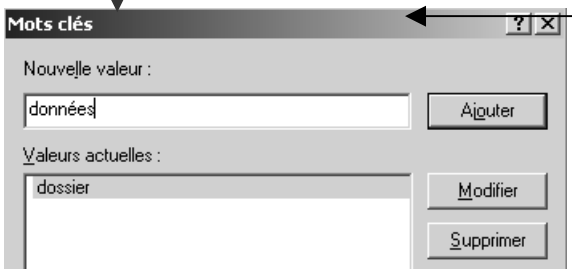


Propriétés d'un dossier publié :

un double clic dessus, ou **propriétés** me permet de le paramétrer :



avec des **Mots clés...**



Recherche d'un dossier méthode classique :

la recherche dans une méthode "classique" (via le voisinage réseau)

demande de passer dans "réseau microsoft windows" et de se rappeler le chemin a parcourir pour arriver à ma ressource,

à savoir par exemple :

dans quel workgroup, / domaine cela se trouve

sur quelle machine

sous quel nom...

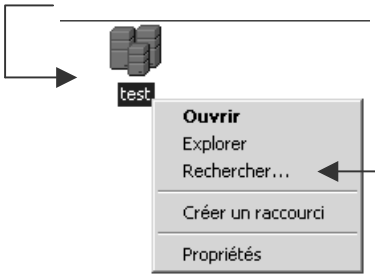
Recherche d'un dossier publié dans AD:

Le plus difficile est de trouver l'icône Active Directory

- Depuis un Client 2000 dans les **Favoris Réseau**, / parcours de **Tout le Réseau** et on demande d'afficher le **contenu entier du réseau**, on obtient alors

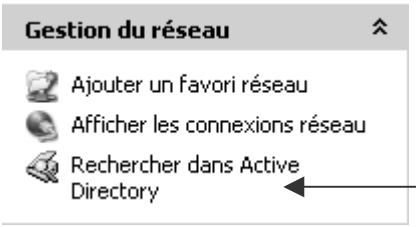
double clic dans dans **Active directory**

Pour obtenir une icône représentant le domaine.



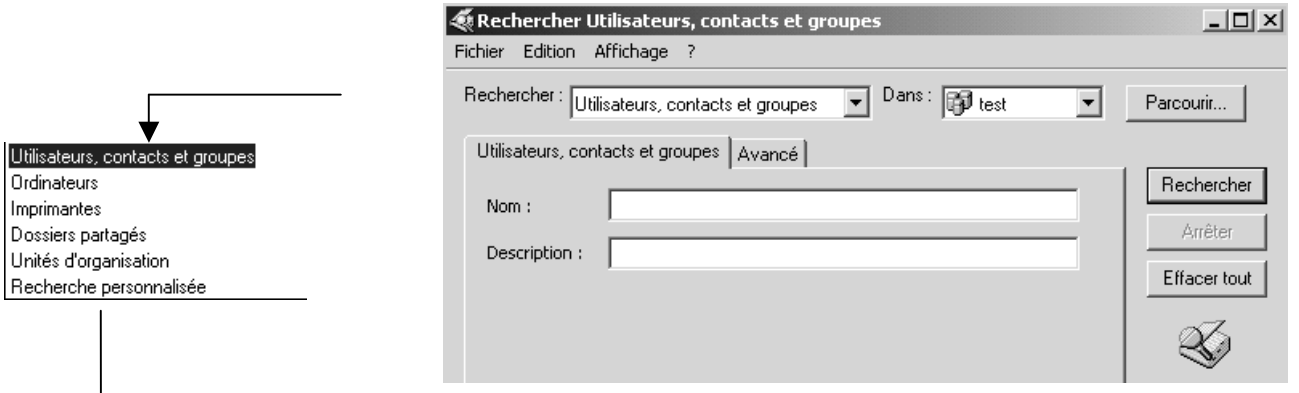
On peut alors faire un clic bouton droit sur mon domaine, **Rechercher...**

- Depuis un Client XP dans les **Favoris Réseau**, on affiche sur la gauche une section Gestion du réseau, dans laquelle on trouve

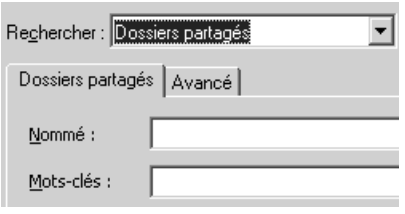


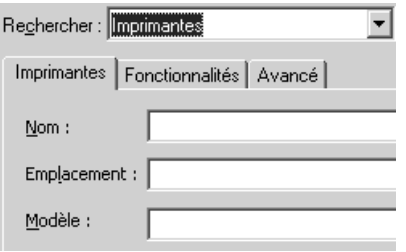
Rechercher dans Active Directory...

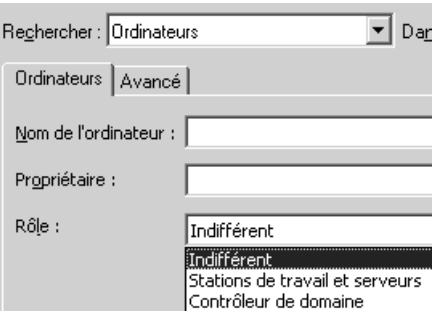
On obtient alors la boite de recherche **Rechercher Utilisateurs, ...**



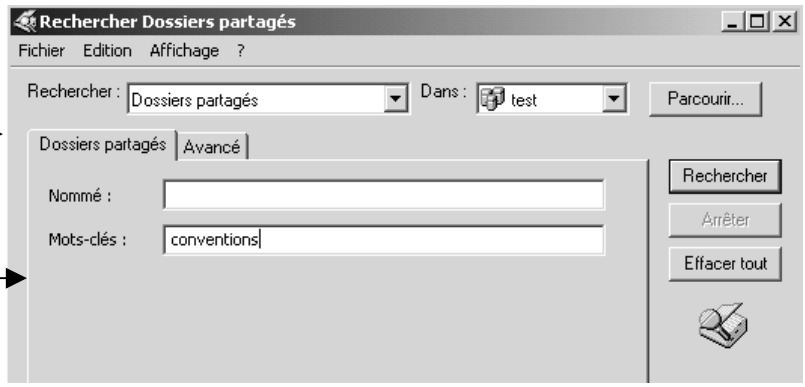
Selon ce que l'on cherche





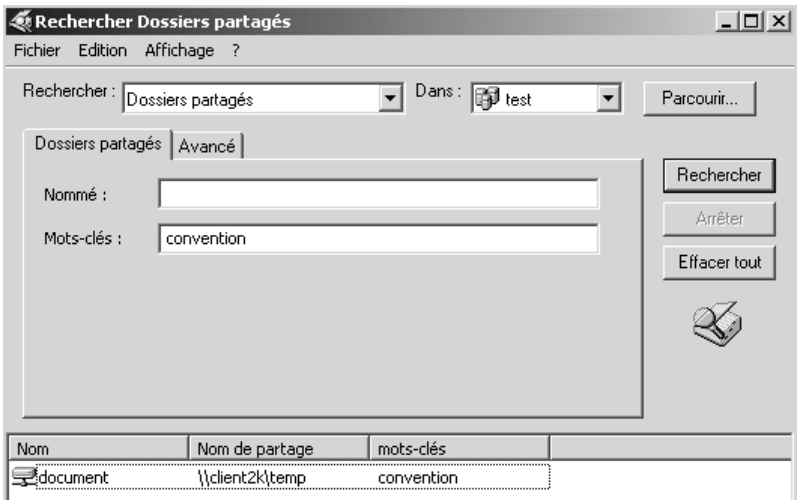


Je donne mon mot clé…



Et avec **Rechercher…**

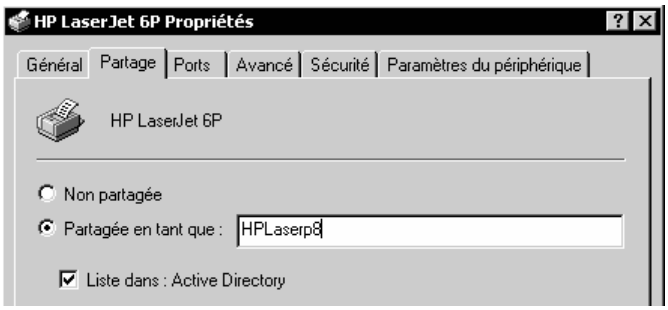
On obtient



Publication d'une imprimante partagée sous 2000-XP:

Sur un poste 2000 ou XP, ayant une imprimante installée localement,

lorsque l'on partage cette imprimante, celle-ci peut être automatiquement publiée dans AD



pour lui rentrer des paramètres il suffit d'aller sur son onglet **Général…**

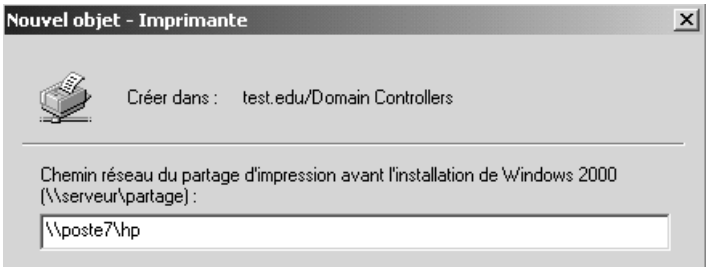
Publication d'une imprimante partagée sous windows NT4.0 et 95:

Sur un poste windows NT 4.0 ou 95-98, ayant une imprimante locale,

lorsque l'on partage cette imprimante, celle-ci pour être publiée dans l'AD doit l'être manuellement :

dans la mmc **utilisateurs et ordinateurs active directory,** On se place sur l'UO que l'on veut, et on demande par le menu contextuel nouveau / Imprimante

on obtient alors

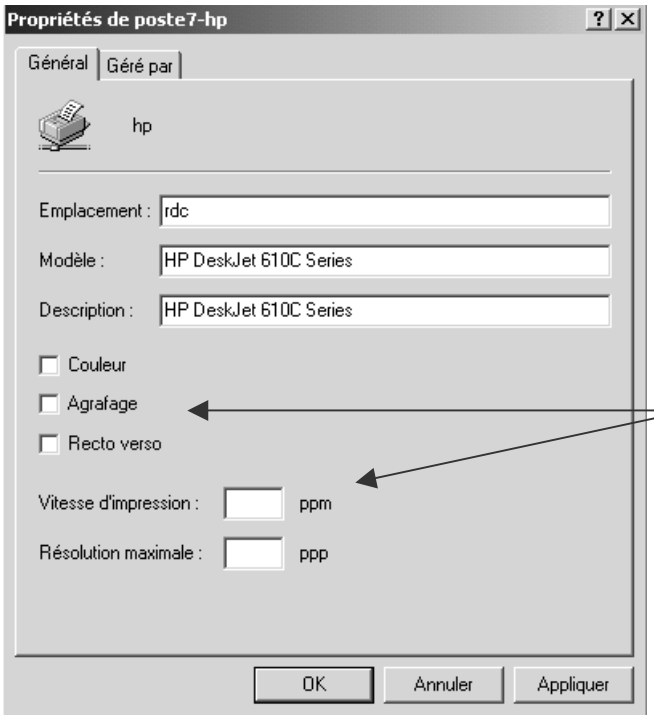


on indique le chemin →

l'imprimante est "publiée"

Propriété d'une imprimante publiée:

une fois publiée dans AD, on peut lui modifier ses **Propriétés...**



Ces propriétés permettront une recherche plus efficace des imprimantes

Recherche d'une imprimante publiée dans AD :

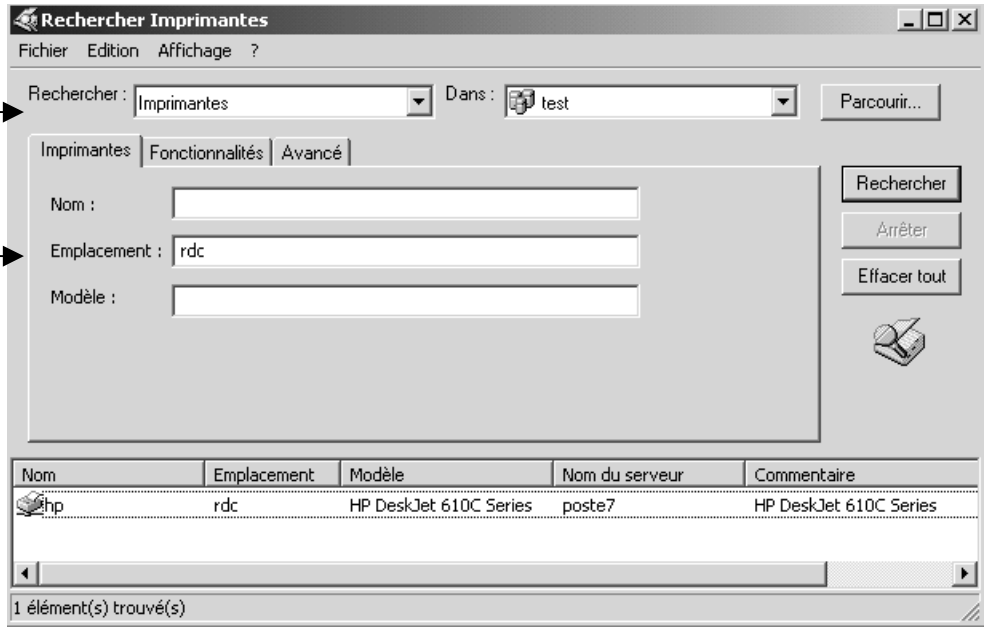
la recherche dans une méthode "classique" (via voisinage réseau) demande de passer dans "réseau microsoft windows" et de se rappeler le chemin a parcourir pour arriver à ma ressource, soit le nom du workgroup + nom machine + nom de partage de mon imprimante (système analogue a celui de la recherche d'un dossier partagé)

La recherche dans Active Directory se veut différente:

Et avec **Rechercher... Imprimante**

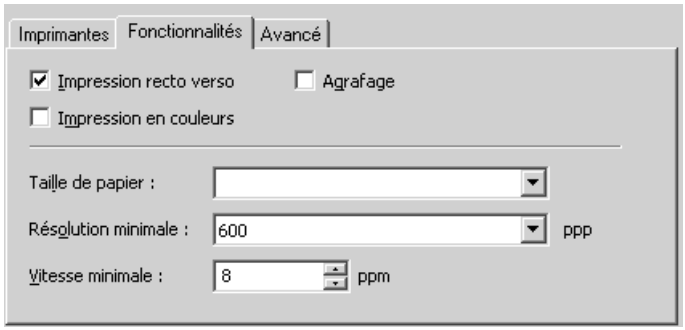
Et un mot clé

On obtient



Il faut bien penser que si lors de la publication on à renseigné les champs d'information, alors une recherche plus complète est possible

Onglet **Fonctionnalités**



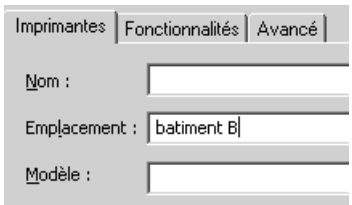
Il devient possible de chercher les imprimantes

effectuant du Recto-verso

avec une resolution minimale de 600 ppp

à la vitesse de 8 ppm

Onglet **Imprimantes**

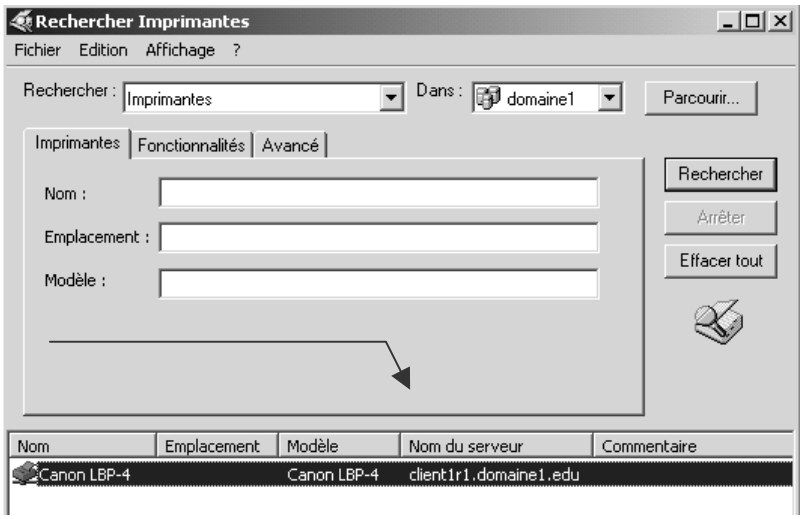


dans le batiment B

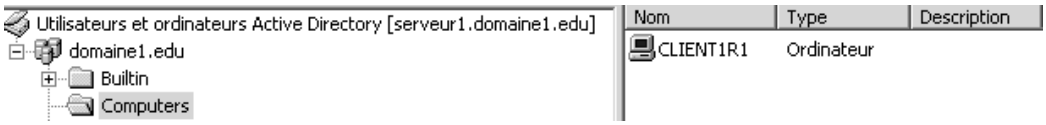
N.B : le bon usage de ces fonctions suppose une correcte utilisation des mot clés et des valeurs possible (lorsque les champs sont ouvert...)

Placement d'une imprimante publiée dans AD :

Par défaut, lorsqu'une imprimante est publiée dans AD, elle est placée dans l'objet ordinateur du serveur d'impression qui la publie, ici par exemple **clientr1**...



mais on ne voit pas cette imprimante dans Active Directory



Pour cela il faut demander le menu

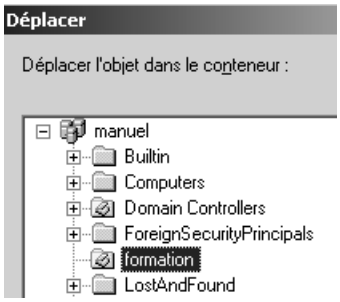
Affichage / Utilisateurs, Groupes et Ordinateurs en tant que conteneur qui amène

Déplacement d'un objet publié dans AD :

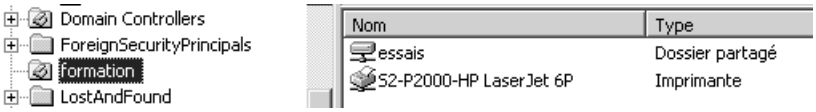
On peut alors si cette imprimante est visualisée, décider de la placer dans une UO plus convenable.

On se place sur l'imprimante et on demande clic droit **Déplacer…**

Et puis on demande la nouvelle UO de stockage (ici formation)



pour obtenir



Qui peut publier - utiliser dans AD ? :

La Publication

D'une manière générale on peut dire que par défaut pour publier :

- Seul l'Administrateur par défaut publie depuis le serveur de Domaine
- Tous les clients 2000-XP nativement peuvent publier s'ils ont installé les outils d'administration 2000 ou 2003 (voir chap admin à distance)
- Les client Windows 95-98, NT 4.0 ne publient jamais (mais ils peuvent partager des ressources, publiées par d'autres...)

L' Utilisation

D'une manière générale on peut dire que par défaut pour utiliser les fonctionnalités d' AD il faut être « client LDAP », ce qui correspond à :

- Tous les postes 2000 utilisent AD
- Tous les clients windows 95-98 et NT4.0 peuvent effectuer des recherches plus sommaires s'ils ont installé les outils client AD (voir chap client-98-NT & AD)

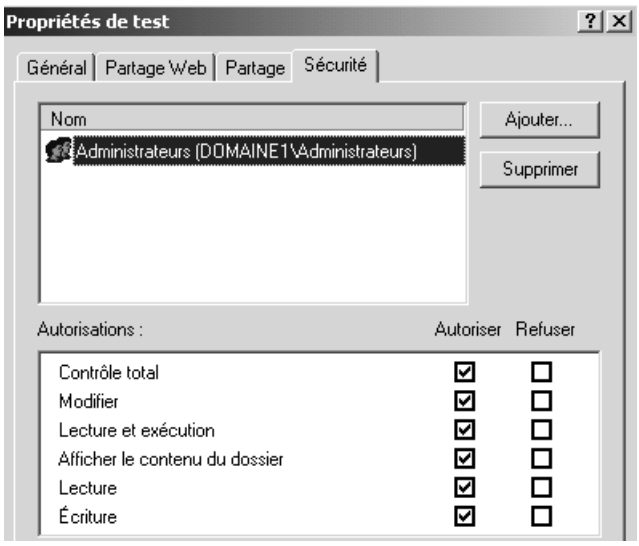
Permissions objets publiés & ressources partagées :

Mais qui peut voir quoi dans AD ?

Cela dépends de la liste des permissions existantes sur les objets publiés, en effet de manière claire **l'objet publié est complètement distinct de la ressource partagée qu'il représente**.

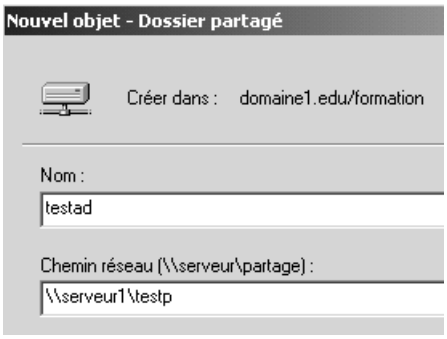
Permissions des Ressource partagée :

Si on prends le cas d'un dossier nommé **test** et partagé sous le nom **testp** avec des permissions NTFS pour l'administrateur en contrôle total,

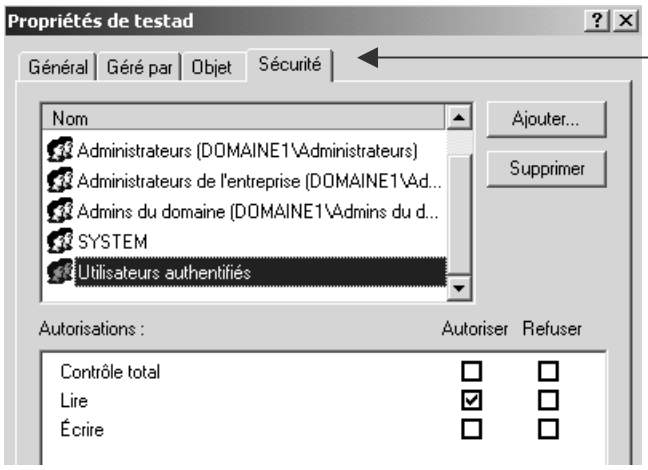


Permissions des Objets Publiés :

Lors de sa publication dans AD, nommée **testad**, les permissions d'accès à ce dossier sont accessibles via les **propriétés** de cet objet



Ici par exemple tous les utilisateurs authentifiés peuvent « voir » cet objet



Pour que l'onglet **Sécurité** soit présent lorsque l'on demande les propriétés d'un objet dans AD il faut d'abords sur les propriétés de cet objet demander **affichage/fonctionnalités avancées**

N.B : voir un objet dans AD ne veut pas dire pouvoir s'en servir…pour que des objets soient visible dans AD il suffit de donner une permissions **lire**

N.B : pour les objets publiés par défaut, ils seront toujours accessibles à travers la recherche dans AD. Par contre pour les objets publiés manuellement (pas par l'installation par défaut) si la permission lire n'est pas donnée, ces objets n'apparaîtront pas lors d'une recherche

Exemple :

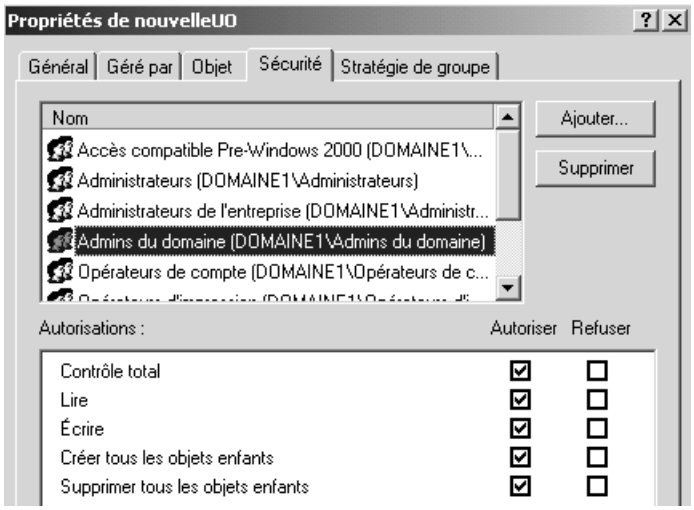
Pour un dossier publié j'enlève la permission lire au groupe utilisateurs authentifiés.

- si je suis logué en tant qu'utilisateur, une recherche de tous les dossiers publiés ne donne rien,
- alors que si je suis logué en tant qu'administrateur, le même recherche aboutira…

GESTION D'ACTIVE DIRECTORY

Permissions et propriétés des objets dans AD :

L'idée c'est de dire que tout objet dans AD dispose de sécurités, que l'on visualise classiquement une fois positionné sur l'objet de AD, par l'onglet **Propriétés/Sécurité**

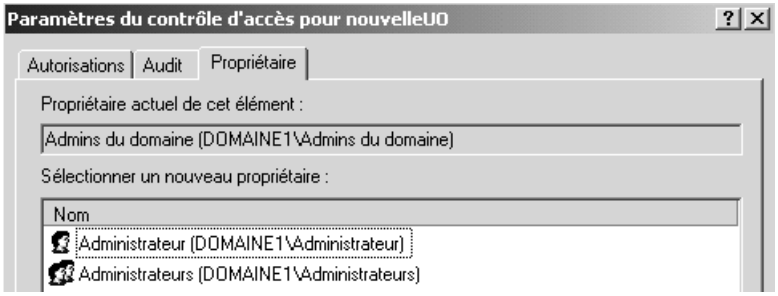


NB : la gestion des permissions se fait de manière identique a celle des permissions NTFS...

Cela peut se faire sur chaque objet...

N.B : attention à la notion d'héritage...

et de propriétaire, via le bouton **avancées**



NB : si membre du groupe administrateur prends possession d'un objet, le propriétaire par défaut est le groupe.

Délégation de compétences-contrôle :

Il s'agit ici d'attribuer le responsabilité de gestion d'un objet AD à un autre utilisateur (ou groupe). Il est fortement conseillé de passer par l'assistant, en se plaçant au départ dans 2 cas de figure différents :

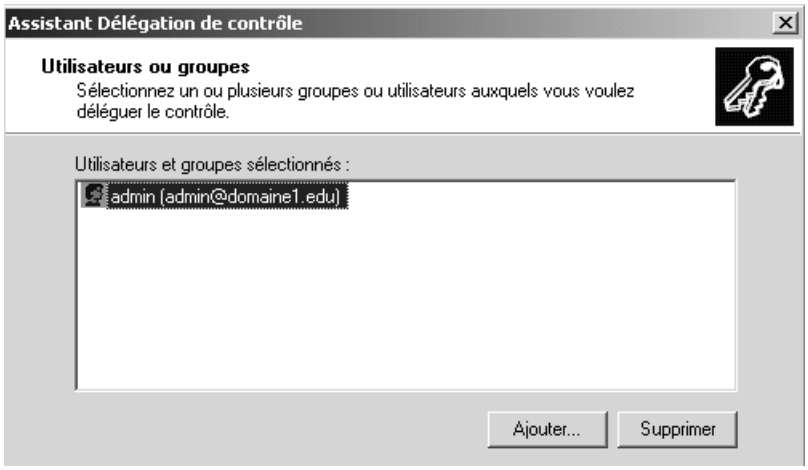
- Délégation de compétences au niveau d'une OU via l'assistant (conseillé)
- Attribution d'autorisations spécifiques sur des OU ou des objets (déconseillé)

N.B : On ne traitera ici que de la **délégation de compétenc**e au niveau de l'**OU** via l'Assistant

Il suffit de se placer sur l'OU souhaitée, puis clic contextuel et on demande le menu **Délégation de contrôle**

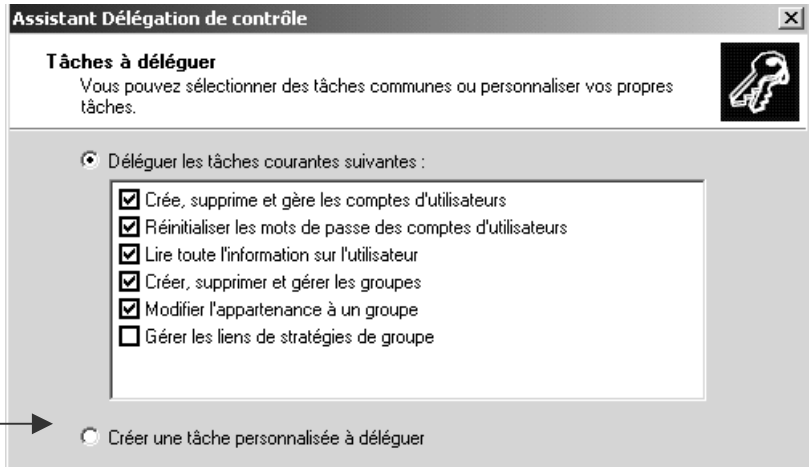
L'assistant se déclenche alors et nous demande successivement :

Pour qui on souhaite effectuer la délégation



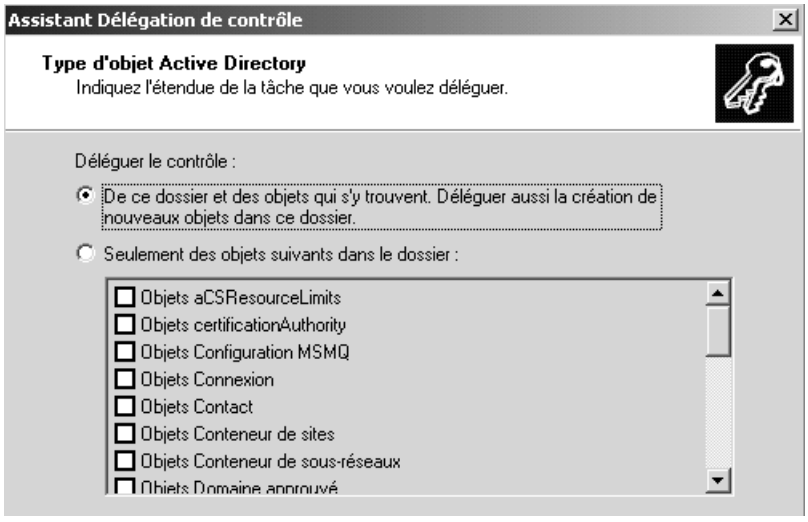
Si on veut accepter une tâche pré-définie, il suffit de choisir...

Sinon il faut cocher



Dans ce cas

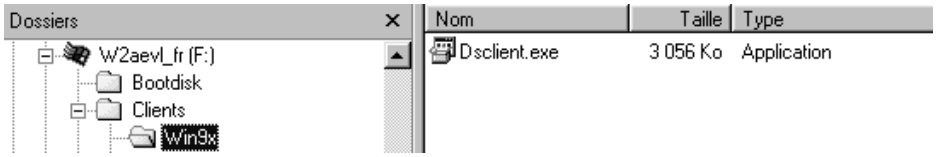
Le plus simple est de déléguer un **contrôle total...**



CLIENTS 95-98-NT & ACTIVE DIRECTORY

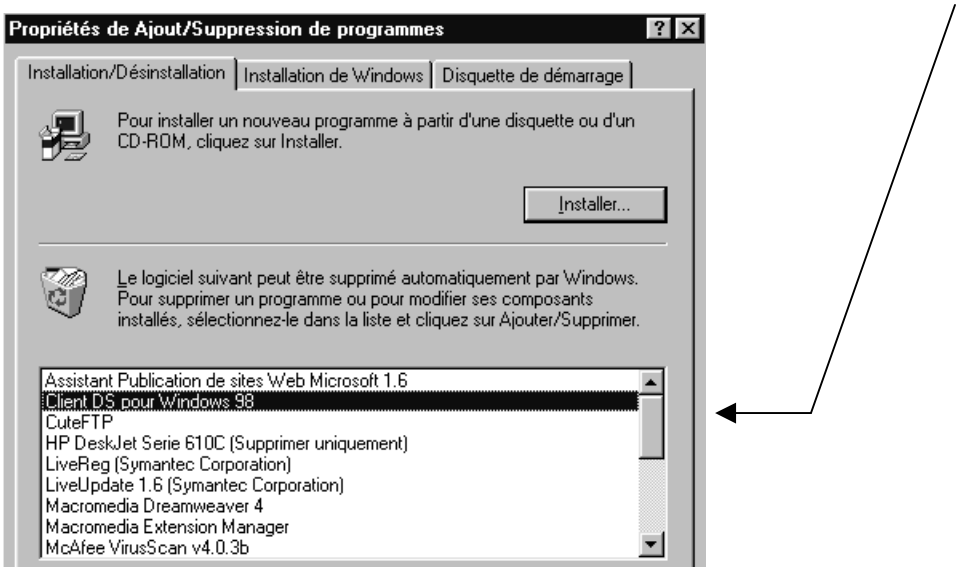
Extensions Client 95-98 Active directory :

Il faut lancer sur chaque client windows 95-98 un petit programme (fournit sur le Cd de Windows 2000 Server)



dont l'installation est basique...

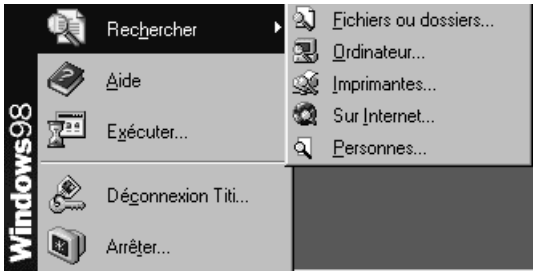
On peut vérifier dans la panneau de configuration que l'installation est faite



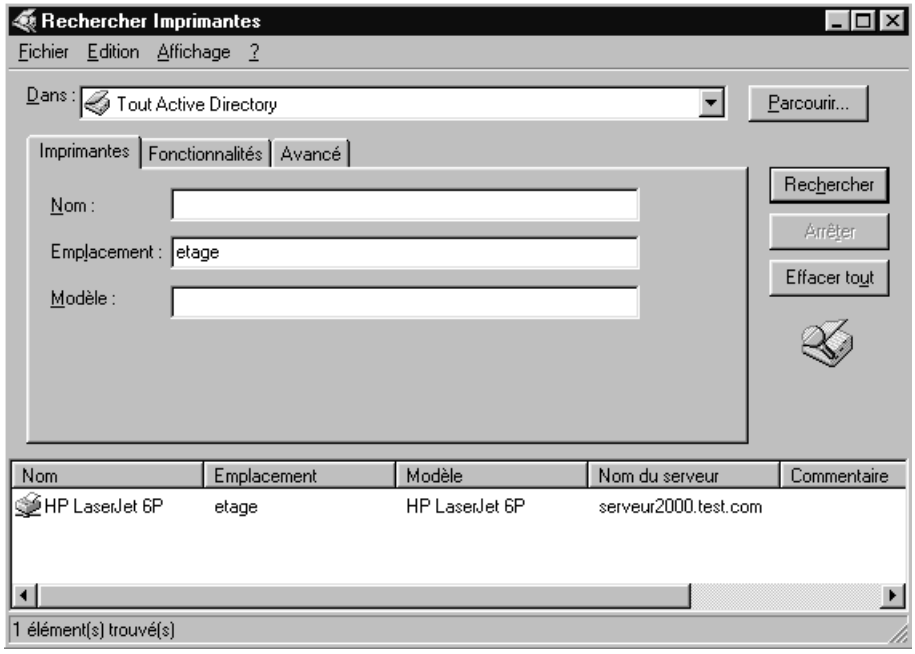
N.B: Ne pas oublier de faire que le client soit bien déclaré dans le DNS du domaine, (sur le serveur) et que son paramétrage IP indique le DNS du domaine...

Utiliser Active Directory depuis 95-98 :

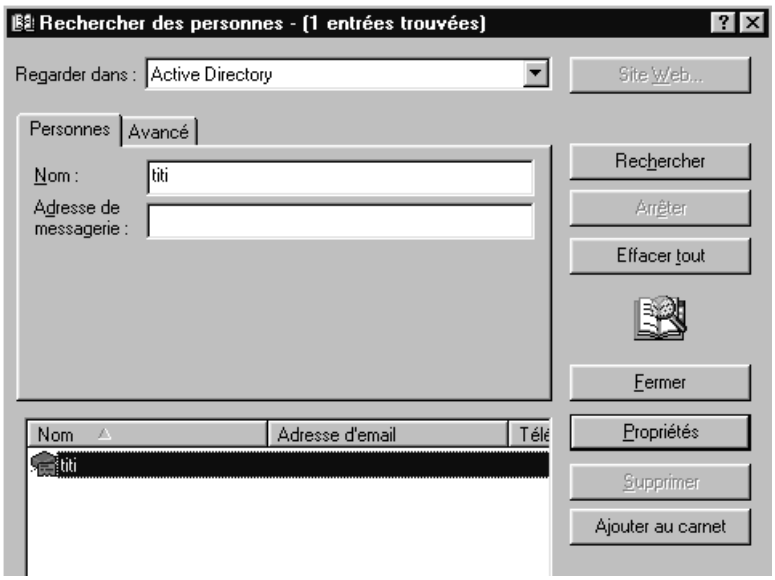
L'interface n'est pas aussi complète que celle disponible depuis les clients 2000, mais elle permet quand même d'enrichir remarquablement le menu **Démarrer/ Rechercher** disponible dans Windows 98



Si les recherches de fichier et d'ordinateurs n'évoluent pas véritablement, par contre on voit une nouvelle entrée permettant de rechercher des imprimantes

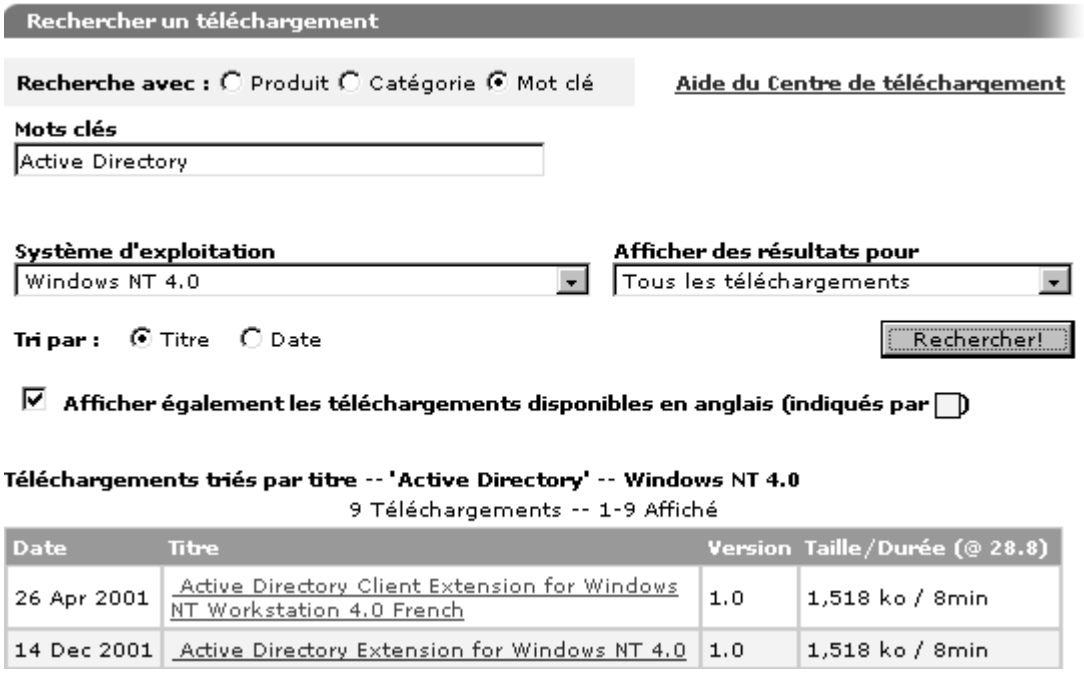


et la recherche des personnes s'étoffe quelque peu...



Extensions Client WKS NT4.0 Active directory :

Il faut lancer sur chaque client Workstation 4.0 un petit programme qu'il faut récupérer sur le site de microsoft



(le nom est homonyme de celui portant les extensions AD pour les clients windows, mais ce n'est pas le même fichier ...)

dont l'installation est basique, à condition que le système NT4 soit au minimum dans la configuration suivante :

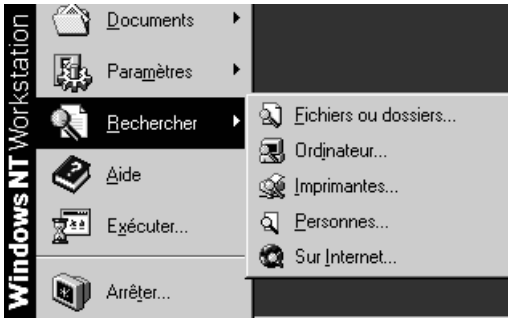
- le sp6 doit être installé
- IE ver 4.0 minimum doit être installé

Puis on installe le fichier **DSclient.exe**

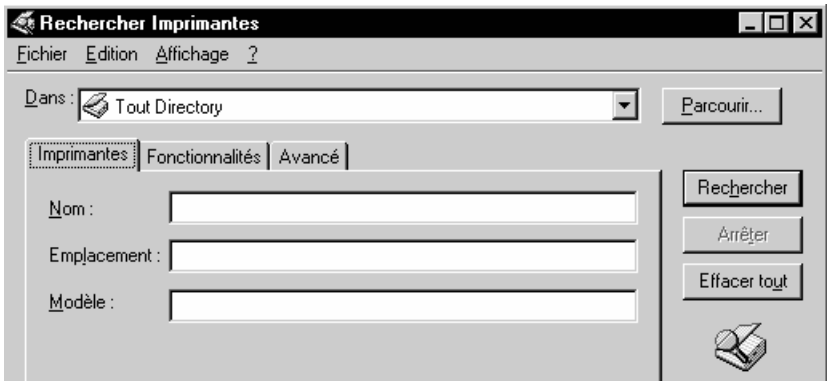
qui amène à ...

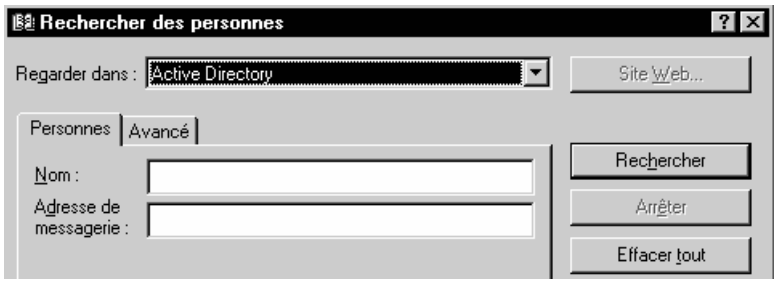
Utiliser Active Directory depuis NT4.0 Wks :

L'interface n'est pas aussi complète que celle disponible depuis les clients 2000 ou XP, mais elle permet quand même d'enrichir remarquablement le menu **Démarrer/ Rechercher** disponible dans Windows NT WKS



avec comme pour les client windows





Encore faut il que cette station NT soit rattachée au domaine Windows sur lequel on effectue une recherche avec Active Directory...!

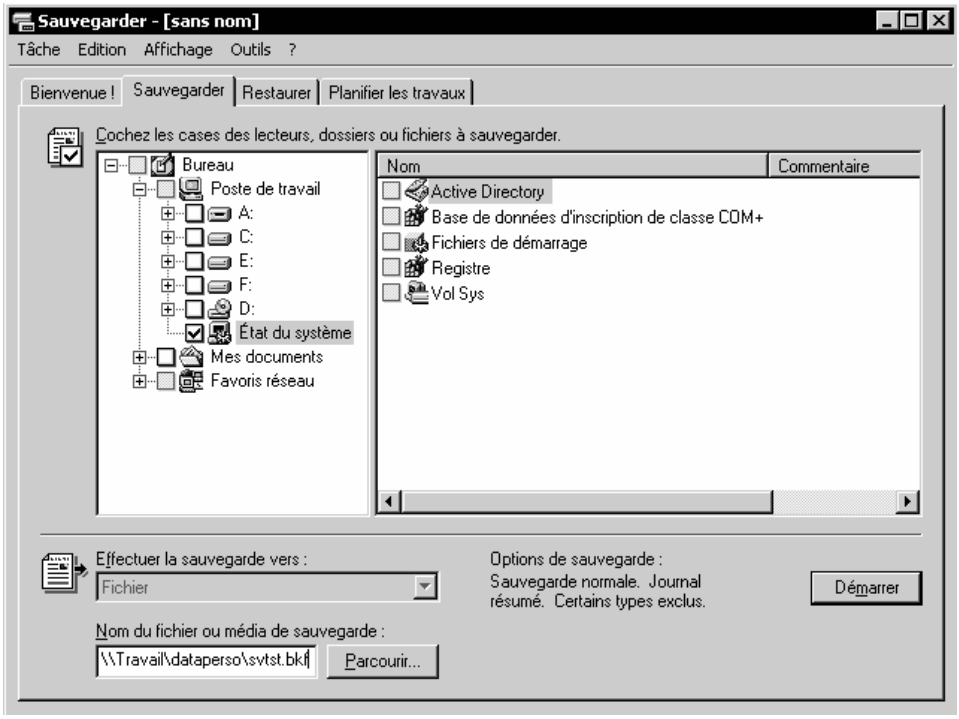
SAUVEGARDE-RESTAURATION DE A.D.

Sauvegarder Active Directory:

L'intérêt de sauvegarder Active Directory, est surtout présent dans le cas ou l'on dispose d'un seul contrôleur de Domaine... en effet si on dispose de 2 CD, il existe toujours une méthode imparable de sauvegarder une AD qui se serait crashée sur une machine, c'est réinstaller le contrôleur de Domaine et attendre la réplication de la copie qui se trouve sur le serveur resté opérationnel...

Par conséquent nous ne traiterons dans ce chapitre que de la méthode de restauration d'une copie sauvegardée de AD sur un Contrôleur de Domaine. (la technique de duplication entre deux CD sera étudiée ultérieurement)

Si on souhaite sauvegarder Active Directory, on parle de sauvegarde de l'**état du système**...



NB : on peut indiquer un chemin valable sur le réseau →

et dans le menu **outils / options** dans l'onglet **général** il vaut mieux demander de **Vérifier les données**

N.B: cette sauvegarde ne doit pas être plus ancienne que 60 jours... car le CD ne garde des traces sur les objets supprimés que pendant cette durée !

N.B: cette sauvegarde ne peut se faire que depuis le serveur (et non a distance) et sans applications en cours de fonctionnement !

Contenu Sauvegarde état du système:

Lorsque l'on fait une sauveagarde de l'état du système avec un serveur 2003 Contrôleur de domaine, voici ce qui est sauvegardé

- Active Directory :
  des que le serveur est contrôleur de Domaine, son AD est suvegardée
- Volume partagé SYSVOL :
  contenant les modèles des stratégies de groupe, les stratégies, les scripts...
- Le Registre :
  tout la base de registre du système et donc des applications installées
- Fichiers de démarrage du système :
  les fichie ntdetect, NTLDR, boot.ini ...

Mais rien ne vous empêche de sauvegarder plus...

Ceci dit, le problême des applications métiers reste entier, elles doivent et peuvent faire l'objet de procédures de sauvegarde propres !

Restaurer Active Directory:

Lorsque l'on souhaite restaurer Active Directory, deux méthodes permettent de le faire :

- Méthode de restauration non forcée (via l'outils de sauvegarde)
- Méthode de restauration forcée (via le mode de restauration des services d'annuaire)

Si on utilise la méthode non forcée, après restauration, et s'il y a d'autres CD alors la réplication va rentrer en jeu, et les différences entre la restauration effectuées de AD et les copies de AD présentent sur les autres CD vont modifier a terme l'état de la restauration....

↳ On **risque de ne pas avoir exactement** après re-synchronisation, **une restauration de AD** comportant exactement ce qu'il y avait dans la sauvegarde. Mais une résultante des données les plus récentes !

Si on utilise la méthode forcée, après restauration, et s'il y a d'autres CD alors la réplication va rentrer en jeu **Mais** les objet de la copie de AD que vous venez de restaure vont avoir un n° de version plus élevé que tous ceux présent dans les autres copies de AD.

↳ On **a exactement** après re-synchronisation, **une restauration de AD** comportant exactement ce qu'il y avait dans la sauvegarde.

Exécuter une restauration non forcée:

Si on a un seul CD de domaine, c'est l'opération à faire...

Il faut suivre le mode opératoire suivant :

1. redémarrer l'ordinateur, **F8** et sélectionner l'option de démarrage **Mode restauration des services d'annuaire**
2. il faut s'identifier en utilisant le compte local de la SAM identifié comme **administrateur restauration service d'annuaire**
   Ce compte est différent de celui de l'administrateur de Domaine, il a été saisie lors du DCPROMO qui a créer le serveur CD...
3. dans l'utilitaire de sauvegarde demander obligatoirement de **Restaurer l'état du système**
4. Redémarrer le serveur

Exécuter une restauration forcée:

Si on a un plusieurs CD de domaine, c'est l'opération à faire pour être sur du contenu de AD après la sauvegarde.

N.B: La restauration forcée ne fonctionne pas pour les modifications qui aurait été faites sur le schéma d'annuaire. On ne peut donc pas annuler des modification sur le schéma par cette technique.

Il faut suivre le mode opératoire suivant :

1. redémarrer l'ordinateur, **F8** et sélectionner l'option de démarrage **Mode restauration des services d'annuaire**
2. il faut s'identifier en utilisant le compte local de la SAM identifié comme **administrateur restauration service d'annuaire**
3. dans l'utilitaire de sauvegarde demander obligatoirement de **Restaurer l'état du système**
   A partir de maintenant, on a effectué une restauration de AD. Si on veut marquer des objets (incrémenter leur n° de +100000) pour qu'il ne soient pas modifiés par la réplication entre AD, alors il faut utiliser Ntdsutil !
4. ne pas redémarrer le serveur et exécuter la commande en ligne **Ntdsutil.exe**

   Cet utilitaire est un utilitaire en mode interactif, à niveau (genre netsh ou nslookup). On sort d'un niveau (ou de l'utilitaire) via la commande **quit**.

   Il se lance par la commande **ntdsutil**

```
C:\>ntdsutil
ntdsutil: quit

C:\>_
```

Le niveau qui nous intéresse ici est celui accessible par la commande **Authoritative restore**

```
ntdsutil: Authoritative restore
```

5. maintenant il faut décider si on veut rendre "autoritaire" toute notre AD, ou seulement une OU (par exemple OU *test* dans *formation.net*)

Toute AD	Seulement une OU
Restore database	**Restore subtree** **OU=***test***,DC=***formation***,DC=***net*

Tapez " **restore subtree ou=**<*Nom UO*>**,dc=**<*nom du domaine*>**,dc=**<*xxx*> " (sans les guillemets), puis valider

- <*Nom UO*> représente le nom de l'unité organisationnelle que vous souhaitez restaurer
- <*nom du domaine*> représente le nom du domaine dans lequel l'unité organisationnelle réside
- <*xxx*> représente le nom du domaine du niveau supérieur du contrôleur de domaine, par exemple com, org ou net.

6. sortir de la commande par **quit**...
7. Redémarrer le serveur

INSTALLER UN C.D. SUPPLEMENTAIRE

Le Principe de Sécurité :

On l'a déjà dit, le principe étant de dupliquer AD sur une deuxième serveur, de manière à se mettre dans une situation de tolérance aux pannes, et de répartir la charge des ouvertures de session…

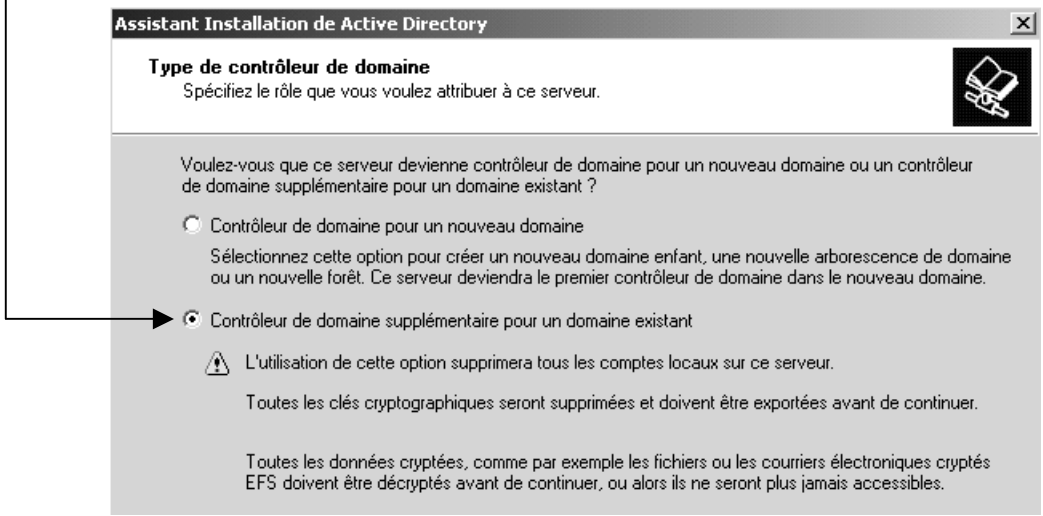
Lorsque l'on va exécuter **DCPROMO**, on va convertir l'ordinateur en Contrôleur de Domaine, et l'on va y dupliquer Active Directory

Dans l'assistant, il faudra bien sûr s'identifier sur un compte de domaine habilité à ajouter un contrôleur, en général l'administrateur.... Mais il faut pour autant être capable de **joindre** le Contrôleur de Domaine opérationnel, ce qui suppose que :

- Soit **notre serveur est déjà membre du domaine** (et là il n'y a pas de problème, car on peut s'identifier sur le CD…)
- Soit **notre serveur est autonome**, c'est à dire fait parti d'un workgroup. Alors là il faut au moins que dans les paramètres tcp/IP **on renseigne le serveur DNS** comme le serveur DNS du domaine que l'on souhaite rejoindre….

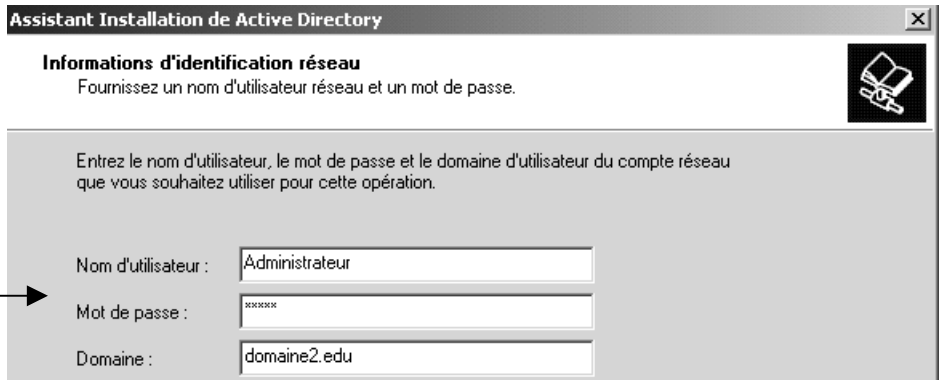
N.B: si on veut mettre toutes les chances, soyons progressif, rentrons le serveur autonome sur le domaine, puis exécutons un **Dcpromo**…

A part les premières boites de dialogue, l'assistant **Dcpromo** est déjà connu On va demander de se joindre à un Domaine existant

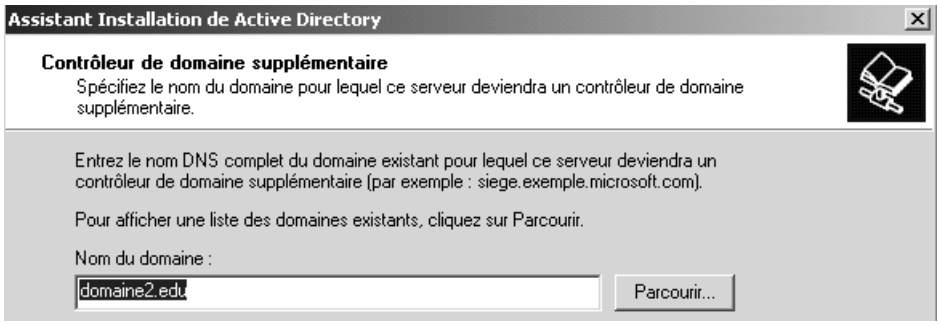


et pour pouvoir faire cela il faut s'identifier avec un compte autorisé à joindre un CD supplémentaire, c'est-à-dire un **Admins du Domaine**…

Identification sur le domaine...

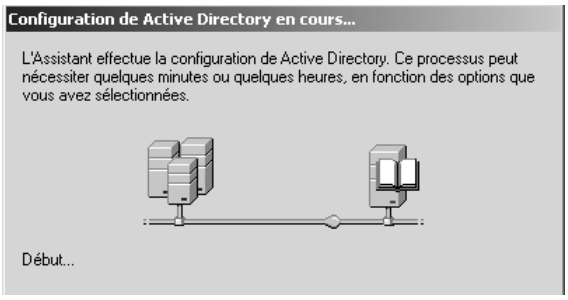


et spécifier à quel Domaine notre contrôleur de domaine veut participer



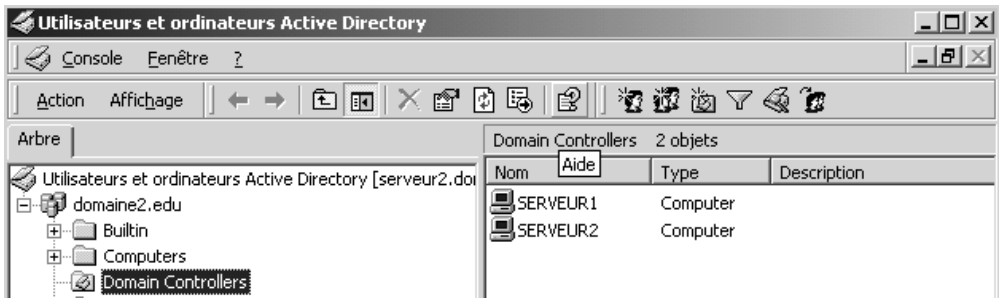
Le reste de l'assistant est identique à celui qui se déroule lors d'un **Dcpromo** de création de domaine...

Le temps nécessaire est le temps normal de création d'une structure AD plus la recopie du contenu existant sur le CD sur notre serveur....



Et cela se termine par le message traditionnel...

On se retrouve avec 2 contrôleurs de Domaines. Ceux-ci apparaissent automatiquement dans l'UO d'Active Directory **Domain Controllers**...



N.B: penser à dupliquer le **catalogue global** si on veut créer plus rapidement des comptes pendant une panne du CD d'origine

AJOUTER UN 2° DNS DANS A.D.

Ajouter un serveur DNS sur Contrôleur de Domaine :

Lorsque l'on à rajouté notre 2° **CD** pour notre Domaine, celui-ci s'est contenté d'utiliser le serveur DNS présent sur le premier Contrôleur de Domaine. Si le 1° serveur s'arrête, notre 2° serveur est opérationnel, mais comme on ne disposera plus de serveur DNS sur le réseau, cela risque de poser de sérieux problèmes...

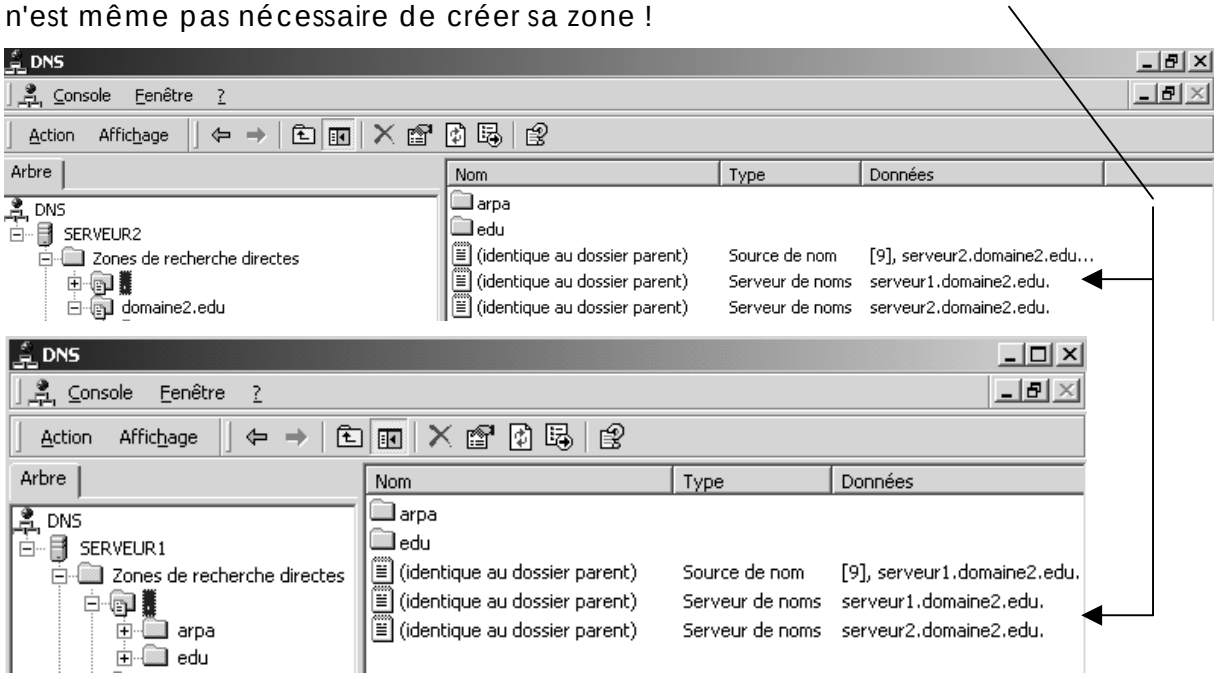
Il faut donc **installer un serveur DNS** sur notre 2° C.D.

Normalement il faudrait le paramétrer en **serveur secondaire pour une zone existante, il est beaucoup plus facile d'intégrer ce 2° serveur à AD...**

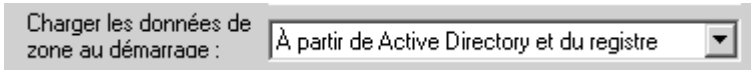
On installe classiquement notre serveur DNS sur notre 2° serveur C.D. (Ajout/Supression... de services de mise en réseau, système de nom de domaine...)

Réplication des Serveur DNS intégré à AD :

L'intégration de la zone du serveur DNS à AD, permet d'avoir une réplication serveur maître serveur secondaire automatique, via la réplication de AD. Il n'est même pas nécessaire de créer sa zone !



Il faut juste vérifier que le serveur initialise sa zone au démarrage via AD (dans les **propriétés** / **avancées** du serveur DNS...)

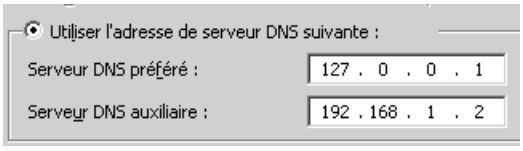


on peut aussi demander à un serveur DNS de recharger sa zone...

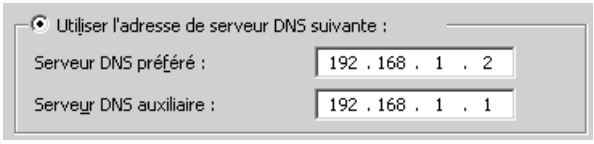
Reglages Adresses IP et redirecteurs:

Chaque serveur DNS doit indiquer

- qu'il dépends de lui-même, (1° serveur DNS)
- et du serveur dont il est le réplica (2° serveur DNS)



et aussi



Si la notion de re-directeur est utilisée sur le 1° serveur DNS, il faut les re-paramétrer sur le 2° serveur DNS

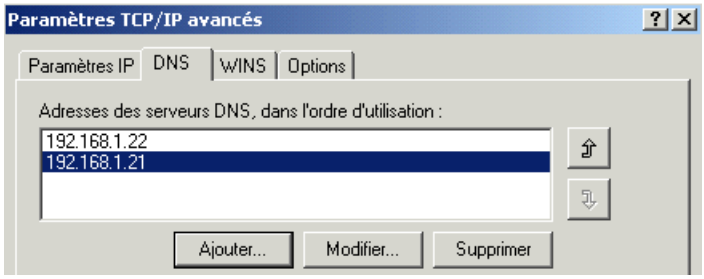
En effet ces réglages sont indiqués "hors zone" et donc non répliqués via AD, ils doivent donc être reconstruits sur chaque serveur DNS...)

Paramétrage des clients :

Il est juste nécessaire de spécifier pour les clients que le serveur DNS auxilliaire se trouve à telle adresse IP (l'adresse de notre 2° CD avec son Serveur DNS...

Il suffit d'indiquer dans les paramètres TCP/IP l'adresse de nos deux serveurs DNS,

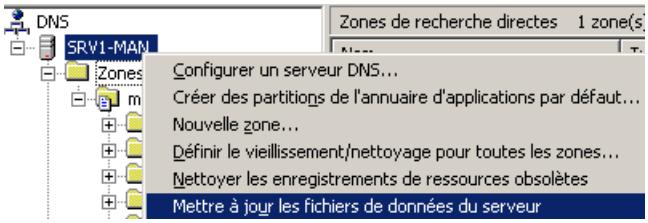
Ou s'il y en a plusieurs on peut demande **avancé**



Sur quel serveur modifier les enregistrement ? :

Même si l'intégration de la zone du serveur DNS à AD, permet d'avoir une réplication serveur maître serveur automatique, on peut, après avoir modifié des enregistrements, demander

Mettre à jours les fichiers de données du serveur



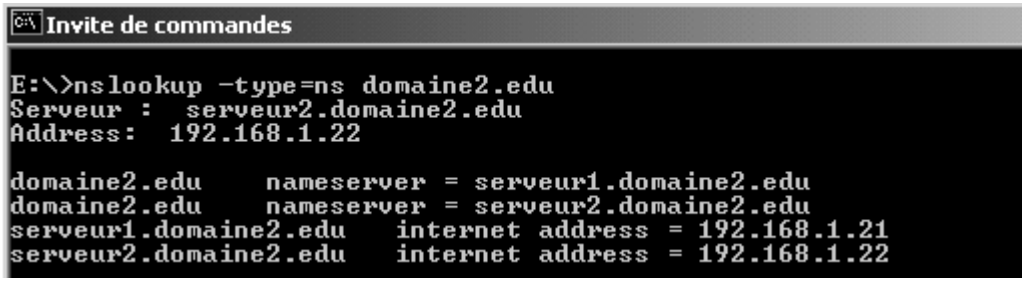
Cela incrémente le n° de série du serveur sur lequel la modification vient d'être faite et permet aux autres serveurs de savoir qu'ils doivent se répliquer

Liste de tous les serveurs DNS disponibles sur le domaine :

La commande en ligne **nslookup** est toujours d'actualité avec la syntaxe suivante :

Nslookup –type=ns domaine

Elle permet de lister tous les serveurs de nom d'un domaine (pour nous ici 2) enregistrés comme tels



AJOUTER UN 2° DNS HORS A.D.

Ajouter un serveur DNS sur Contrôleur de Domaine :

Lorsque l'on à rajouté notre 2° **CD** pour notre Domaine, celui-ci s'est contenté d'utiliser le serveur DNS présent sur le premier Contrôleur de Domaine. Si le 1° serveur s'arrête, notre 2° serveur est opérationnel, mais comme on ne disposera plus de serveur DNS sur le réseau, cela risque de poser de sérieux problèmes...

Il faut donc **installer un serveur DNS** sur notre 2° C.D.

On peut, comme on l'a vu dans le chapitre précédant, intégrer ce serveur à AD, mais plus "classiquement" il faudrait le paramétrer en **serveur secondaire pour une zone existante ...**

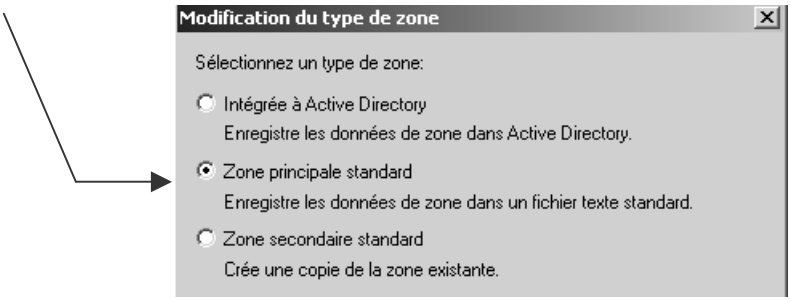
On installe classiquement notre serveur DNS sur notre 2° serveur C.D. (Ajout/Suppression de services de mise en réseau, système de nom de domaine...)

Création de serveurs DNS en "backup" réciproques :

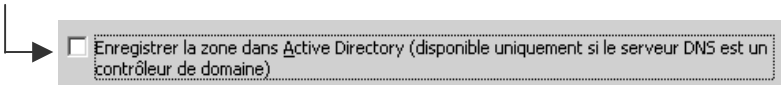
La non intégration de la zone du serveur DNS à AD, permet de mettre en œuvre une technique courante sur internet dans laquelle chaque serveur DNS possède une zone secondaire, stockant une "copie" de la zone principale du serveur qu'il est censé dupliquer.

Pour effectuer cela il faut effectivement que la zone soit stockée dans un fichier, et non intégrée dans AD...

- Sur le CD "principal", il faut vérifier que le type de zone soit bien "**zone principale standard**...



Sous 2003 il faut décocher la case



valider la manipulation avec

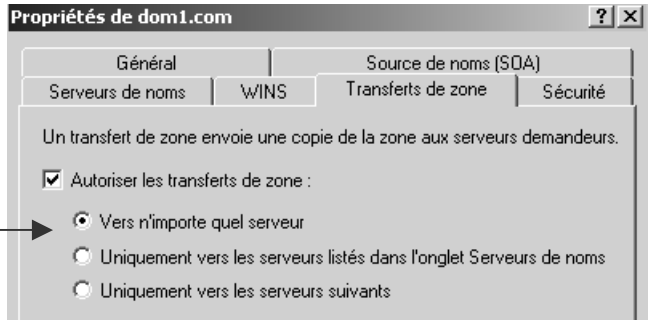
ipconfig /flushdns puis

ipconfig /registerdns,

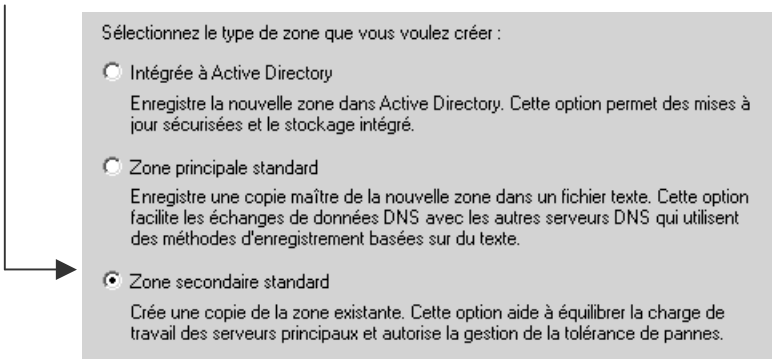
oire un vidage du cache ou un restart....

- Toujours sur le CD "principal", sélectionner la zone et demander menu contextuel **propriétés**...onglet **Transferts de zone**

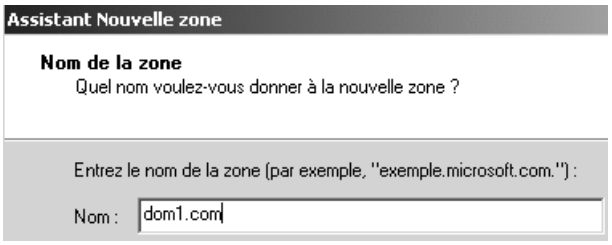
Dans un 1° temps autoriser les transferts vers tous les serveurs



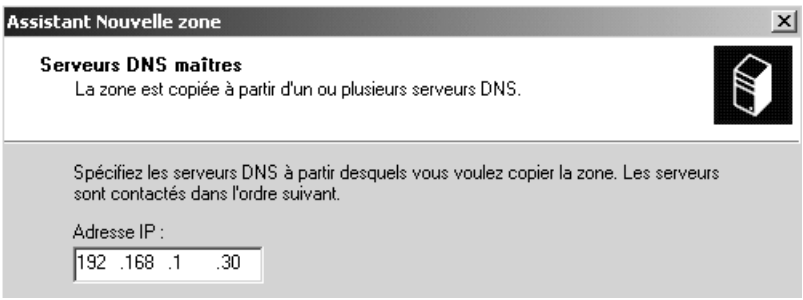
- Sur l'autre CD "backup", il faut créer une zone de type **Zone secondaire standard**. Cela se fait via l'assistant création de zone



Puis on donne le nom complet de la zone que l'on souhaite dupliquer



et l'adresse IP du serveur DNS qui héberge la zone principale homonyme...

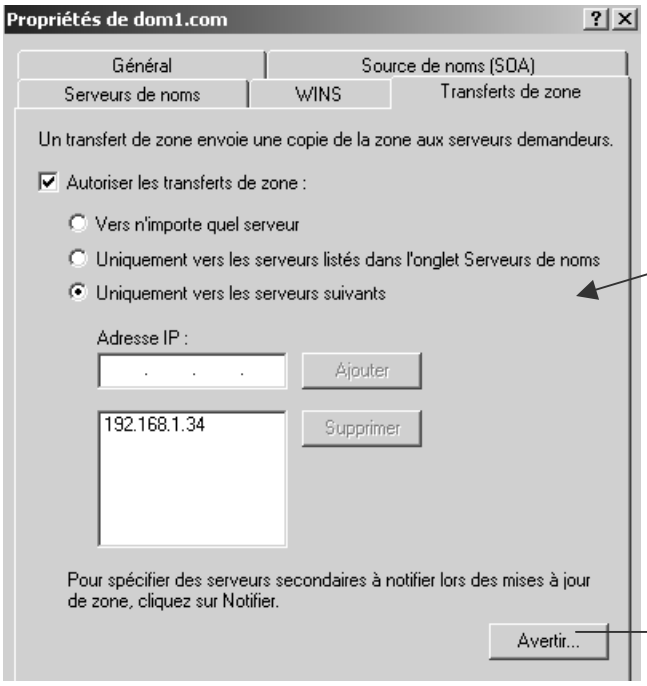


L'assistant terminé, on devrait voir remonter une copie de la zone....

Affinage de la duplication :

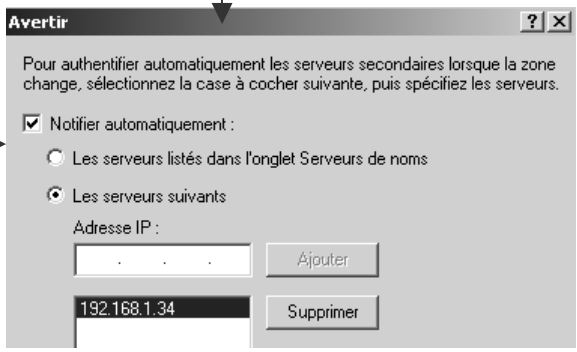
une fois les réplications de base vérifiées, on peut optimiser et sécuriser un peut...

Toujours sur le CD "principal", sélectionner la zone et demander menu contextuel **propriétés**...onglet **Transferts de zone**



Il faut autoriser les transferts de zone uniquement vers les serveurs que l'on a repéré...

Et indiquer aussi les serveur que l'on doit informer des changements...



DUPLICATION AD INTRA-SITE

Duplication d'AD entre CD :

A partir du moment ou l'on crée un **Domaine**, on crée un **Site** dans lequel notre **CD** se place. Lorsque l'on rajoute un 2° **CD** pour notre Domaine, il fait partie automatiquement du même **Site.**

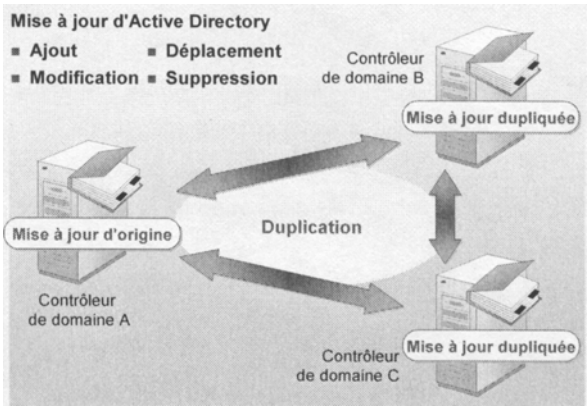
La **duplication** des informations stockées dans les AD de chaque contrôleur de Domaine, prends alors le nom de **Duplication intrasite**

Le principe de mise à jour des modifications entre les copies des AD stockées sur les Contrôleur de Domaine est celui dit de «**duplication multi-maître** », dans lequel chaque CD possède une copie identique à l'autre, et à l'initiative de la demande de duplication. Il se peut que 2 CD fassent une demande de duplication au même moment, mais ce genre de conflit est résolu automatiquement dans la structure de réplication intra-site de AD.

N.B : il existe là une différence fondamentale avec ce qui existait sous NT.40 lors des échanges de SAM entre le CPD et les CDS, échangent qui se faisaient selon un schéma dit de duplication « **maître-esclave** », car tout se faisait à l'initiative du CPD qui restait unique et détenait « l'original » à dupliquer sur les CSD...(d' ou les manipulation de promotion d'un CSD enCPD, etc...)

La **duplication** des informations stockées dans AD se fait *suite à une. Modification de AD .*

Une modification de AD cela peut être ajout d'un objet, modification des valeurs stockées dans un objet, modification du nom d'un objet ou suppression d'un objet.



N.B: ce délai est un **délai de 5 min et est non paramétrable !**

N.B: par sécurité, si aucune modification n'est effectuée pendant toutes une période données, (par défaut 1 heure), une duplication des informations est effectuée également.

N.B: Il existe des modifications urgentes, qui sont notifiées immédiatement, sans l'attente du délai de 5 mn, ce sont par exemple les verrouillage de compte, et de manière générale les paramètres critiques au niveau sécurité.

Résolution de conflits de Duplication d'AD:

Le principe de mise à jour des modifications entre les copies des AD étant dit de «**duplication multi-maître** », 2 CD peuvent effectuer une demande de duplication au même moment, avec des AD ayant des objets différents…

Le principe étant toujours celui de base « le dernier qui modifie à raison… ». Pour mettre en œuvre ce principe, AD travaille avec un système de cachet contenant un ensemble de 3 éléments :

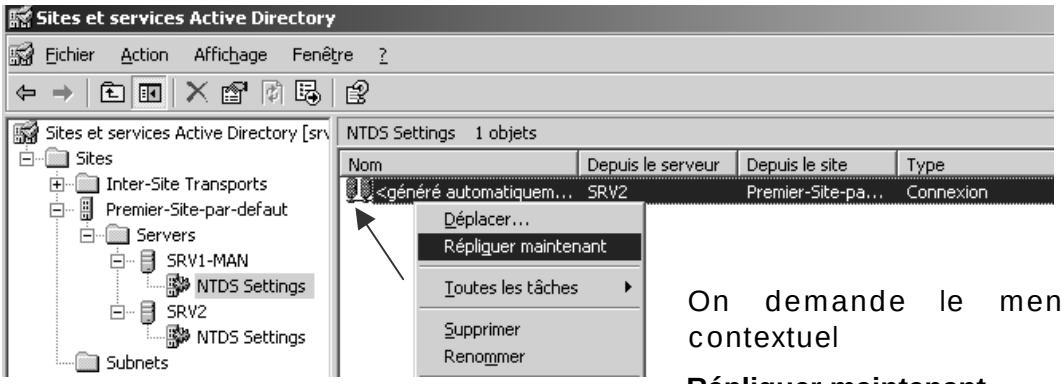
- Le n° **GUID** (**Globaly Unique identifier**) du serveur sur lequel la modification de l'AD à été faite,
- Le N° de Version **USN** (**Update Sequence number**) définit pour chaque objet et pour chaque attribut d'objet, incrémenté automatiquement à chaque mise à jour d'origine
- La date prise sur le CD sur lequel la modification à été faite…

Forcer la duplication :

Si on forcer la réplication intra, on se met dans

Sites et services Active Directory,

On sélectionne le serveur dont on souhaite activer la réplication,



On demande le menu contextuel

Répliquer maintenant

DUPLICATION AD INTER-SITE

Utilité d'un Site :

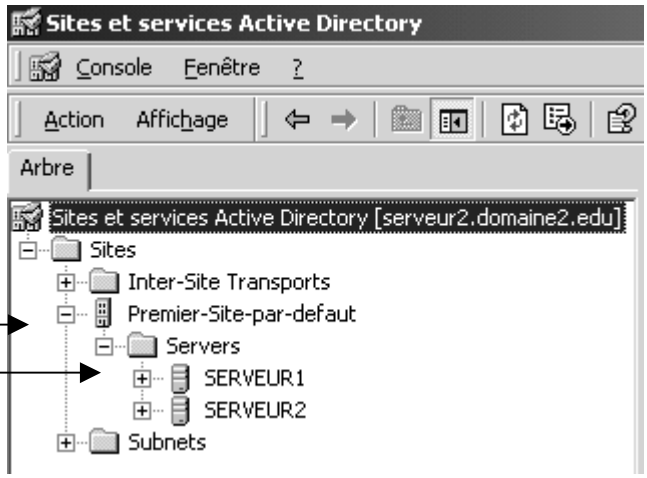
Si on ne spécifie rien lors de l'installation des DC, par défaut on se retrouve systématiquement dans un site par défaut, nommé **Premier-Site-par-défaut**, et contenant tous mes serveurs CD.

La mmc permettant de visualiser les sites AD se lance depuis le menu **programmes / outils d'administration/ Sites et services Active Directory**

On retrouve le site crée par défaut

« **Premier-Site-par-defaut** »

et tous nos **C.D.**



par défaut toujours, la **duplication** des informations stockées dans les AD de chaque contrôleur de Domaine, prends alors le nom de **Duplication intrasite**

Mais un site peut être utilisé pour gérer la structure physique d'un domaine, c'est à dire notamment l'éloignement physique de deux « parties » d'un même domaine.

La création de 2 sites différents permet notamment :

1. de contrôler le **trafic de duplication** des AD (ce qui, comme on l'a vu, n'est pas possible dans un site)
2. Et lorsque un utilisateur ouvre une session, un contrôleur de domaine est cherché dans le même site que celui de la station

Par conséquent on pense à créer notre domaine, puis on gère les situations « physiques » par la notion de site.

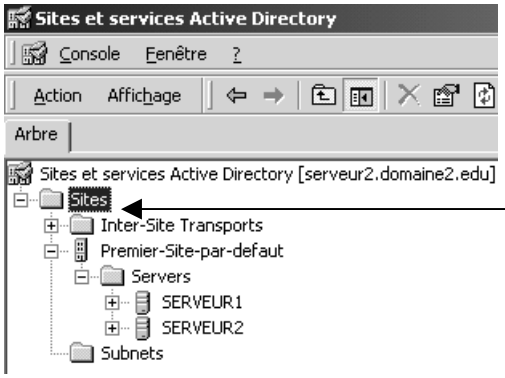
Un site est défini par une plage d'adresses TCP-IP suivant les règles .

- Si toutes les machines d'un domaine ont les mêmes plages d'adresse IP (ID réseau+masque) on ne peut avoir qu'un seul site.
- Dans un site on peut avoir des plages d'adresses IP différentes, il suffira de poser des masques et de faire du routage interne…
- Mais si **on veut avoir 2 sites**, il est impératif d'avoir pour **chacun de ces sites des plages d'adresses IP différentes** ou **poser des masques et de faire du routage** …

Création de Site :

Lorsque l'on veut créer un site, il va falloir créer aussi un sous réseau et l'associer au site.

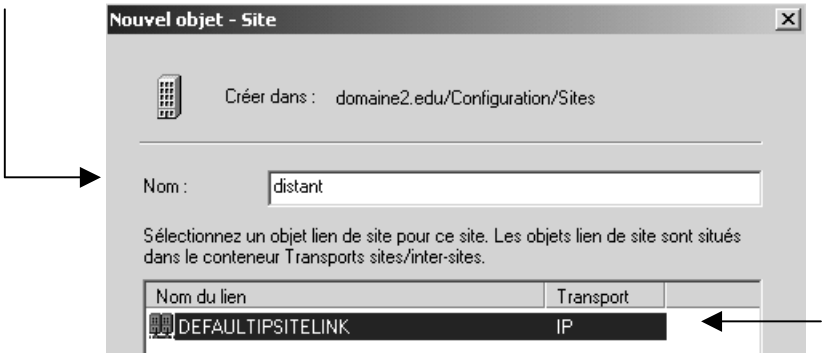
Pour créer un nouveau site, il faut se mettre sur le dossier **Sites**



Et demander clic droit

Nouveau site

Il faut donner ensuite un nom au site que l'on crée (ici « **distant** »)



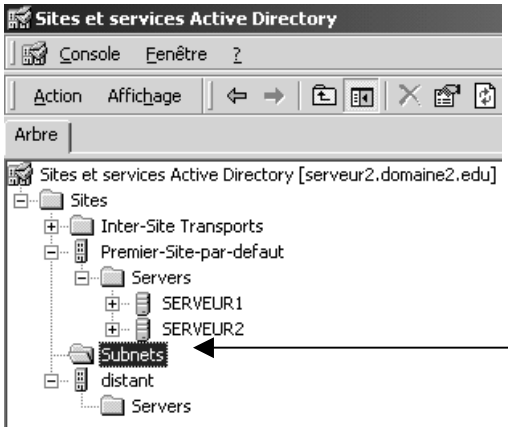
Et sélectionner le lien par défaut

Un message de mise en garde nous rappelles les actions qui restent à faire :

- Définir un sous réseau
- L'associer à notre site
- Vérifier que notre site est bien lié aux autres sites du domaine
- Mettre dans le site au moins un Contrôleur de Domaine

Définir un sous -réseau :

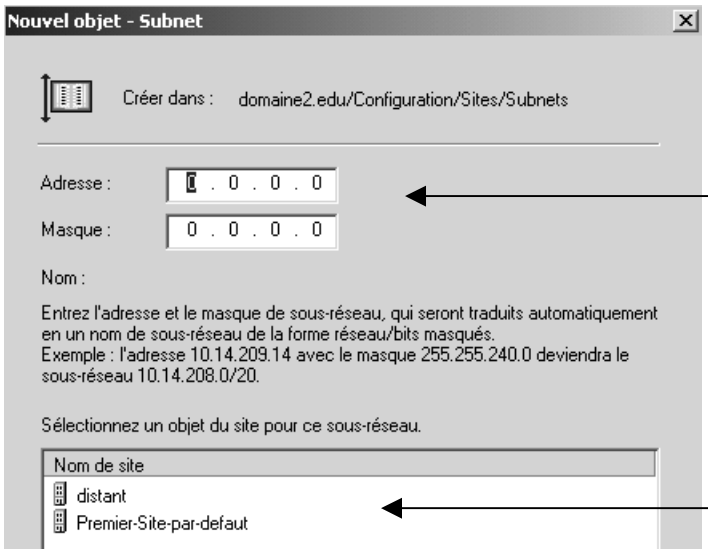
Pour créer un sous-réseau, il faut se mettre sur le dossier **Subnets**



Et demander clic droit

Nouveau Subnet

on obtient



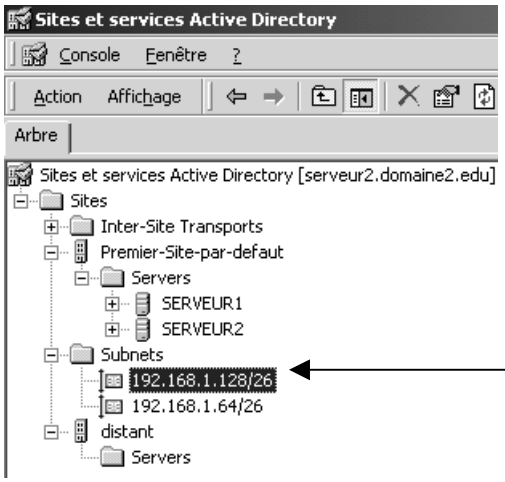
Il faut rentrer là les adresses et les masques de sous-réseau correspondant aux sites que l'on doit gérer...

Soit pour nous par exemple une **adresse privée réseau de classe** C **192.168.1.xx**, si on veut créer des sous réseau dans cette adresse, il va falloir poser un masque de sous réseau autre que 255.255.255.0

Voir chapitre « annexe TCP/IP » pour les calcul de sous réseau TCP/IP.

Associer un sous -réseau à un site:

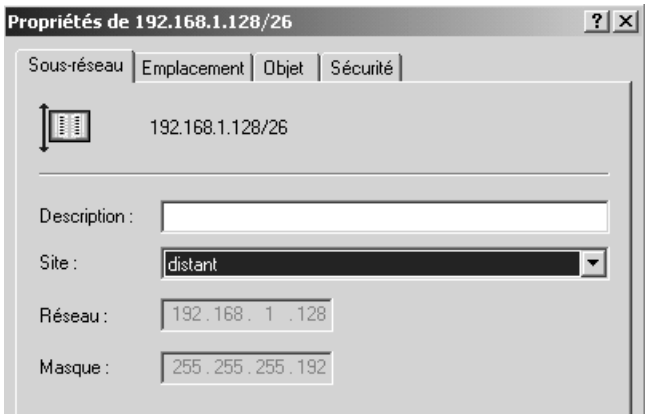
Pour associer une plage d'adresse à une notion de site, , il faut se mettre sur chaque sous réseau à associer, et demander **Propriétés**



Et demander clic droit

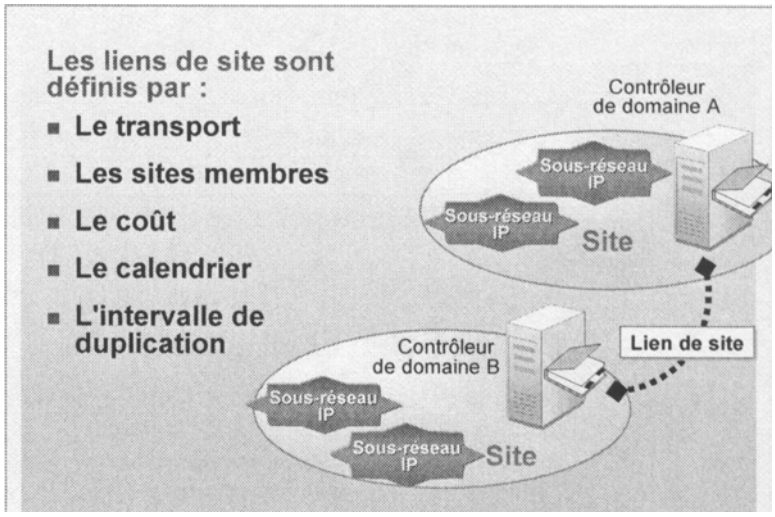
Propriétés

Vérifier que ce sous réseau soit bien associé à un site



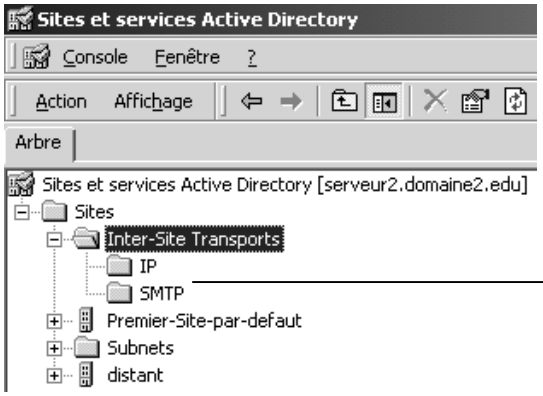
Création des liens de site:

Avoirs des sites c'est bien, il faut encore définir de quelle manière les liaisons vont pouvoir se faire entre sites : c'est d'ailleurs la tout l'objectif, pour pouvoir paramétrer les échanges inter-sites !



Si on part du principe que les liaisons entre sites sont des liaisons non permanentes, on va pouvoir définir un certain nombre de paramètres

Pour créer une liaison entre site, , il faut se mettre sur **Inter-Site transports**



2 types de transports sont disponibles :

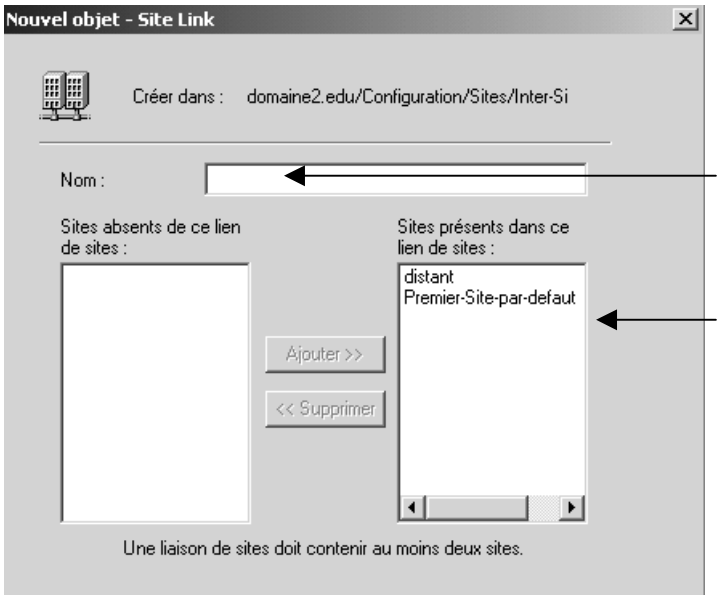
- **IP (RPC)** protocole **Remote Procedure Call** par défaut
- **SMTP** protocole **Simple MAIL Transfer Protocol** moins utilisé en l'espèce.

on choisit le type de transport (toujours **RPC**)

Et demander clic droit

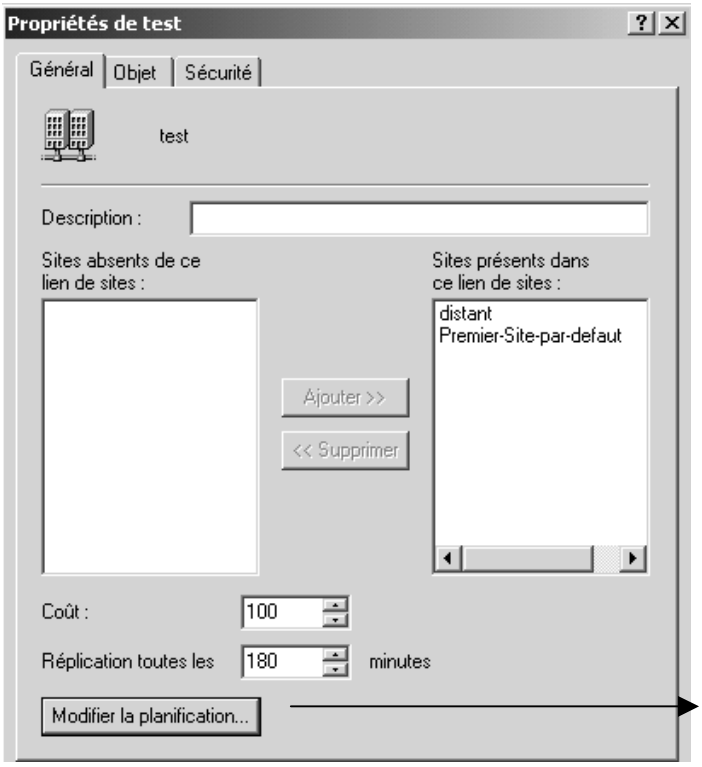
Lien vers un nouveau site

On va créer un nouvel objet Lien

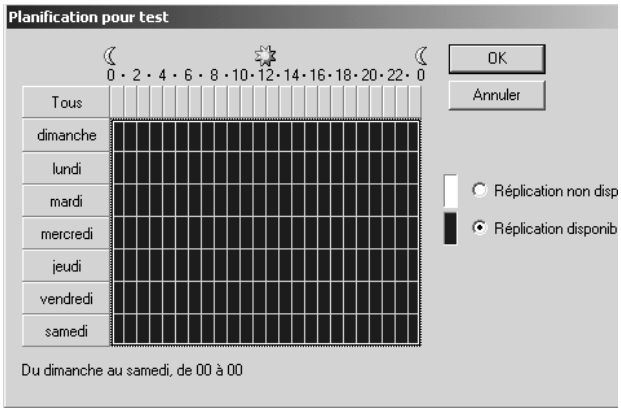


Que l'on doit nommer

Et dans lequel if faut inclure au moins 2 sites

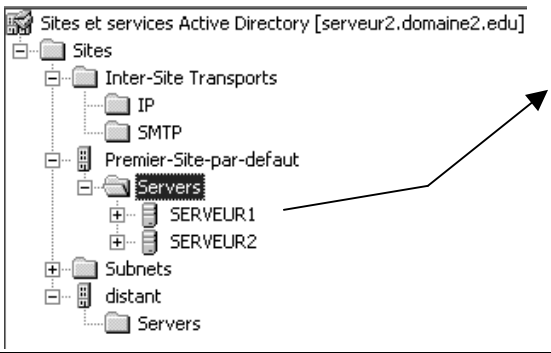


et pour lequel ensuite les propriétés vont permettre de configurer un certains nombre de choses...

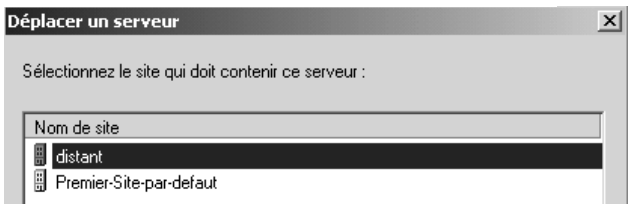


Mettre un **CD** dans chaque site:

Il faut avoir un Contrôleur de Domaine minimum par site, ce qui se fait soit par l'installation d'un nouveau contrôleur, soit par le déplacement d'un contrôleur existant



Sur le serveur à déplacer, on demande clic droit **déplacer**

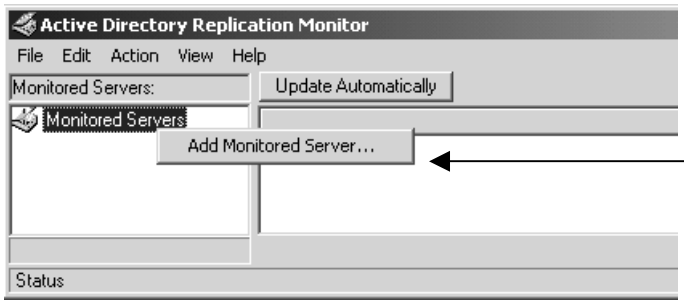


Visualiser le schéma de la duplication :

Si on veut visualiser le trafic entre 2 CD dans un schéma de réplication intra-site il faut installer un outils fournit sur le CD 2000 et stocké dans le dossier **SUPPORT\TOOLS\SETUP**

On installe ces outils avec les options par défaut...

On lance ensuite depuis le menu **Windows 2000 support Tools/Tools/Active Directory Replication Monitor**

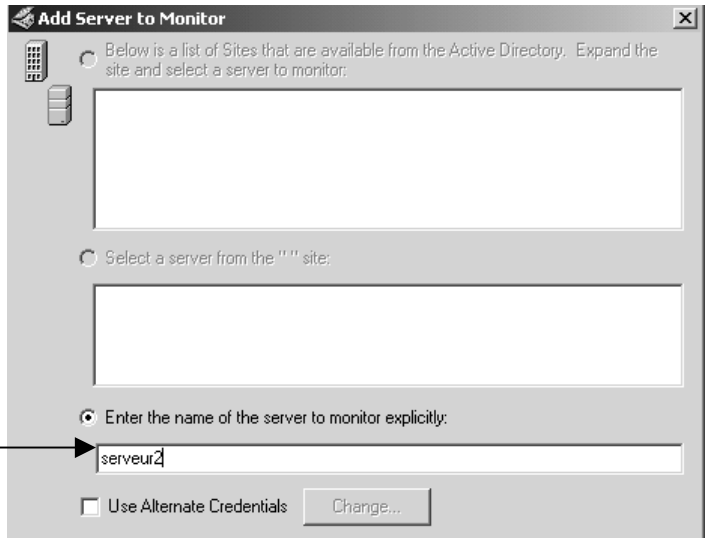


On demande un clic droit sur **monitored served** et on demande d'ajouter notre serveur...

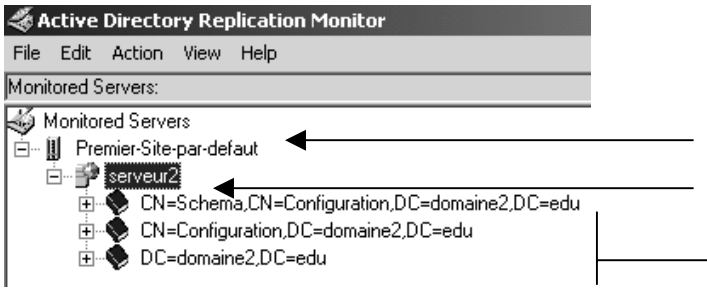
on obtient alors

On garde **add the server explicitly by name** ...

et on y ajoute notre machine



on à alors une vision de la réplication de AD :



Notre site par défaut

Notre serveur

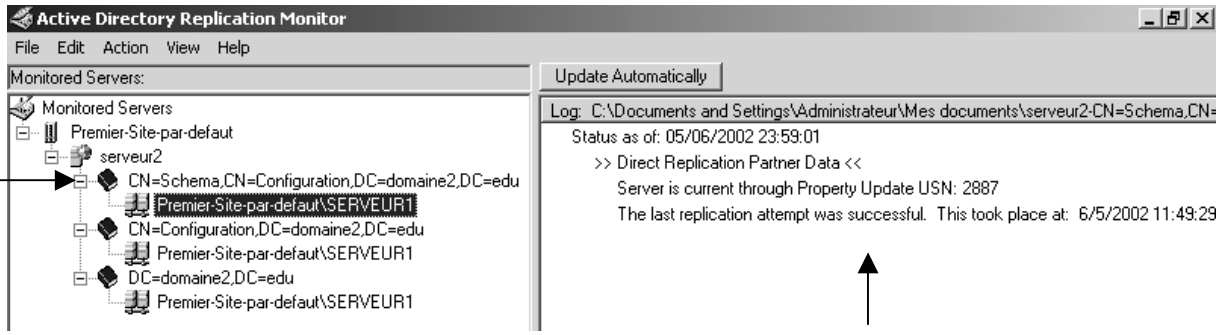
Les 3 composants de Active directory :**Schéma – Configuration - Domaine**

Le schéma : définition des règles de construction de AD, c'est la structure de AD, qui est unique dans tout le domaine, la forêt (éventuellement répliquée entre tous les DC de la forêt). *Unique !*

Configuration : structure de cette AD, quels domaines et quels sites en font partie, quels contrôleurs de domaine existent pour chacun d'eux... *Unique !*

Domaine : Contient les définitions des objets propres au domaine crée dans cette AD. Dupliquée sur tous les CD du domaine. *Il peut y en avoir de multiple dans une forêt...(mais une par domaine)*

Si on se place sur une partie de l'AD, et que l'on demande de voir le détail,



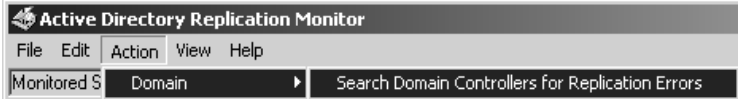
on à l'information "en clair"

N.B: un clic droit + **synchronize with this replication partner** force la duplication !

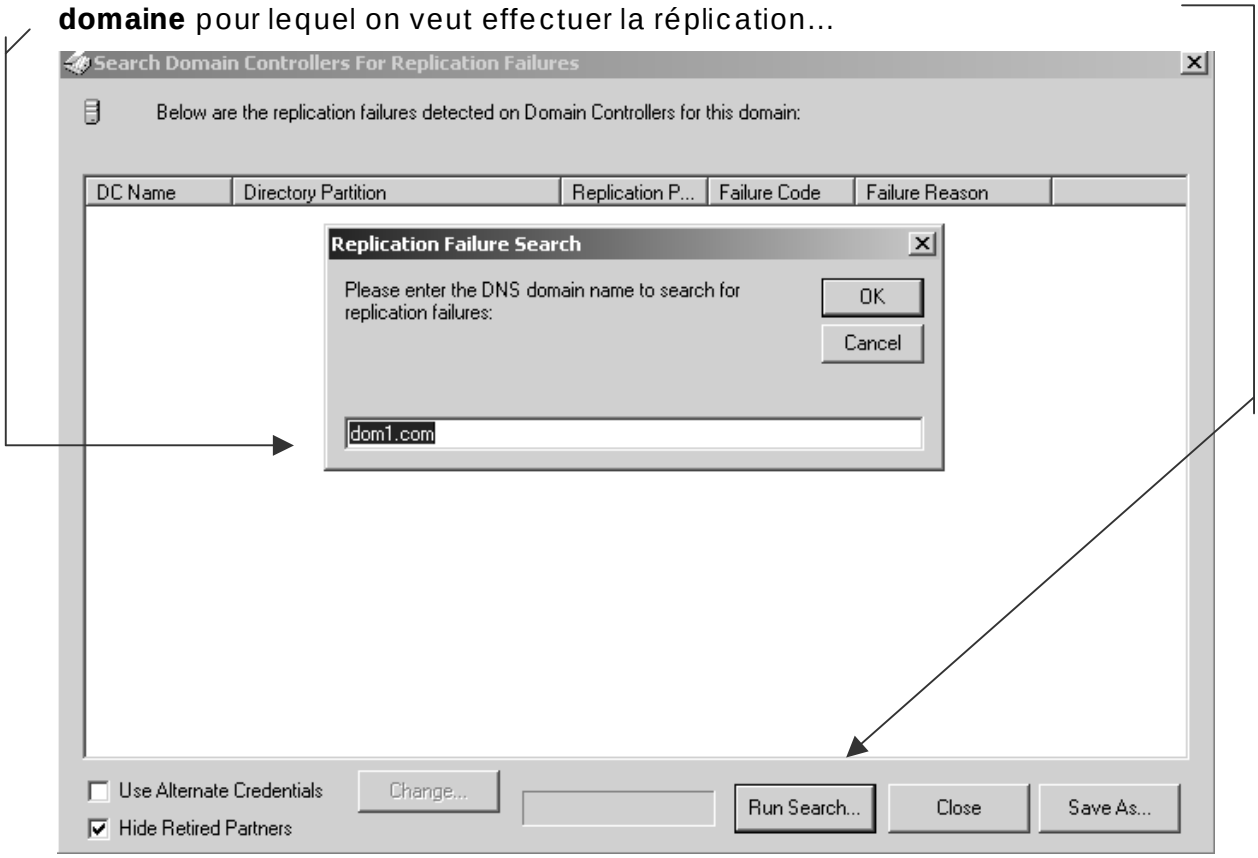
Vérification Recréer le schéma de la duplication :

Si on veut vérifier le trafic entre 2 CD dans un schéma de réplication intra-site il faut installer un outils fournit sur le CD 2000 et stocké dans le dossier **SUPPORT\TOOLS\SETUP**

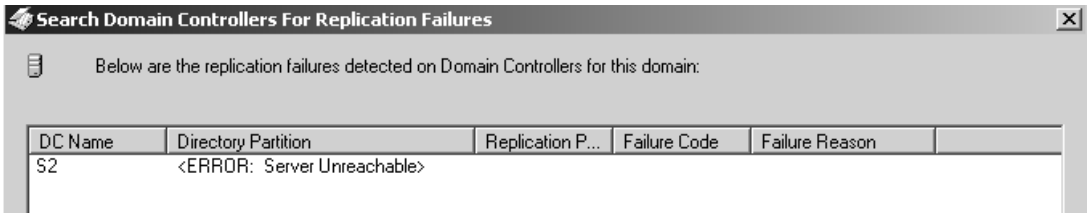
On installe ces outils avec les options par défaut...puis et on ajoute les serveurs dans notre visualisation. Puis on demande



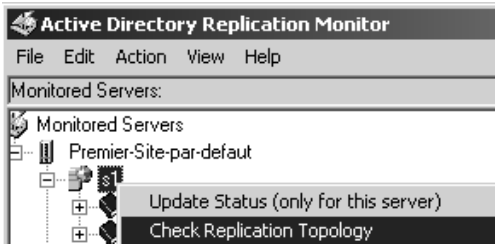
Dans la boite de dialogue, on demande alors **Run Search** et on indique le **domaine** pour lequel on veut effectuer la réplication...



le résultat s'affiche...



on peut vérifier (et éventuellement recréer la topologie de réplication) via un clic contextuel sur un serveur et **check replication Topology**



LES ROLES FSMO

Notion de Rôles de maître d'opérations:

Dans un Domaine 2000-2003 on répète tout le temps que les contrôleur sont tous homologues, que l'on est dans un schéma de réplication de AD de maître à maître….

Malheureusement, dans AD il existe des rôles précis que l'on appelle des **rôles de maître d'opération**. dits **rôles FSMO (Flexible Single Master Opération)**

Ces rôles sont au nombre de 5

1. Contrôleur de schéma
2. Maître d'attribution de nom de domaine
3. Emulateur CPD (NT 4.0)
4. Maître identificateur Relatif RID
5. Maître d'infrastructure

1 & 2 sont **uniques pour la forêt**

3 – 4 – 5 **sont uniques pour un Domaine**

Heureusement ces rôles peuvent être déplacés sur n'importe quel CD

Par défaut, les 5 rôles sont stockés de la manière suivante :

- Le premier DC d'un nouveau domaine dans une nouvelle forêt renferme les 5 rôles de maître d'opération (1-2-de For1 + 3-4-5 Dom1)
- Le premier DC d'un nouveau domaine qui rejoint une forêt existante renferme les 3 rôles de maître d'opération du nouveau domaine (3-4-5 de Dom2)
- Le DC suivant d'un domaine utilise les 3 rôles de maître d'opération du Domaine qu'il rejoint

- **donc <u>dans une forêt à 1 domaine</u> il existe 5 rôles dont 2 rôles stockés sur le 1° CD de forêt et dont 3 sont crées sur le 1° CD du domaine (cela peut être le même CD...)**

- **donc <u>dans une forêt à X domaine</u> il existe 2 rôles stockés sur le 1° CD de forêt, et 3 rôles de domaine crées sur les 1° DC des X domaine**

Signification des 5 Rôles de maître d'opérations:

Voyons brièvement les 5 rôles de maître d'opération

Le Contrôleur de Schéma

Il contient la définition de la construction de AD, c'est le seul pouvant modifier la « structure » de AD (modifier ou rajouter un champs dans la BD…)

Si absent : on ne peut pas modifier la structure AD. Pour nous c'est peut gênant au quotidien, mais certaines applications, comme Exchange par exemple, modifie l' AD …

Le premier CD qui s'installe, est **Contrôleur de schéma**

Maître d'attribution de nom de Domaine + (serveur Catalogue Global)

Il contrôle l'ajout ou la suppression de Domaines dans la forêt. (Et tient aussi un catalogue global de tous les objets définis dans l'AD pour éviter les doublons…. Ces deux rôles doivent toujours être associés.)

Si absent : on ne peut pas ajouter ou supprimer de domaine enfants

Le premier CD qui s'installe, est **Maître d'attribution de nom de Domaine**

Emulateur CPD (NT4.0)

Il joue le rôle de CPD pour continuer a faire travailler les CSD (en mode mixte), et gère les changement de mot de passe depuis les clients NT ou windows98.

Si absent : plus de synchro des éventuel CSD, plus de modifications de mot de passe depuis des poste non 2000

Maître RID

Il attribue des **bloc RID (Relative Identifier)** qui sont unique pour chaque CD.

Lorsque l'on crée un objet, le SID objet =identificateur RID + identificateur SID du domaine.

Si absent : lorsque l'on a épuisé le stock de paquets RID sur un CD, si on ne peut plus en faire la demande au serveur maître, alors on ne peut plus créer d'objets : tout simplement.

Maître d'infrastructure (désactivé si 1 Domaine dans 1 forêt)

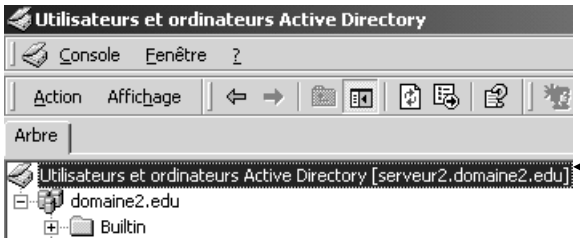
Met à jours les références d'objets d'un domaine aux autres domaines.

Des que cela est possible (2 domaines ayant chacun 2 DC), le maître d'infrastructure de doit pas être sur le même DC que le Catalogue Global.

Si absent : cela ne pose problème que si l'on est en présence d'une forêt à plusieurs Domaines.
Dans le cas d'une Forêt à un Domaine, ce rôle ne fonctionne pas…

Localiser les 5 maîtres d'opérations:

Avec la console **Utilisateur et ordinateur Active Directory** on peut trouver les 3 maîtres de domaine :

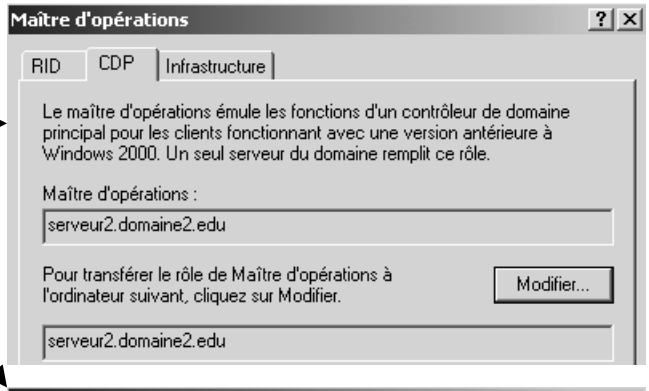


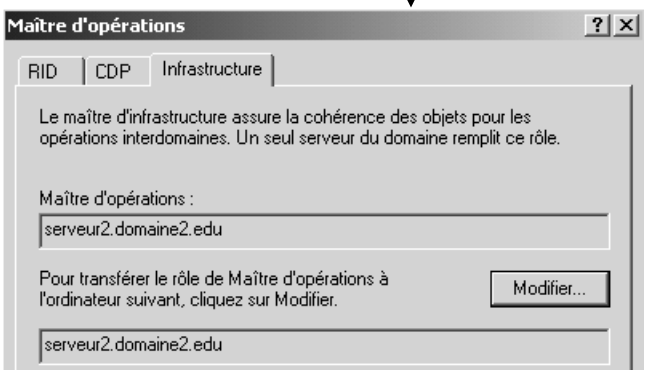
En se plaçant sur **Utilisateur et ordinateurs Active Directory** on demande clic droit **Maîtres d'opérations…**

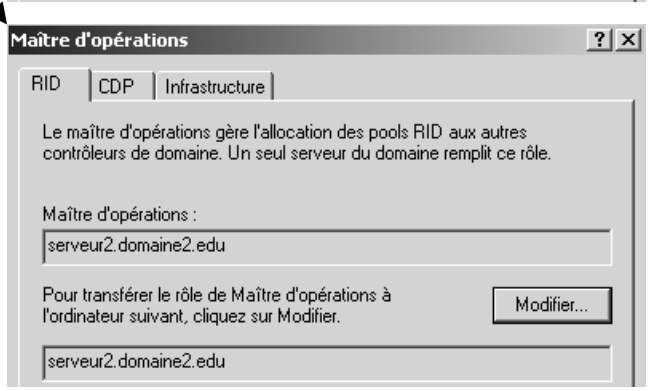
pour obtenir un boîte à 3 onglets

Les 3 rôles de domaine

- Emulateur CPD (NT 4.0)
- Maître identificateur Relatif RID
- Maître d'infrastructure

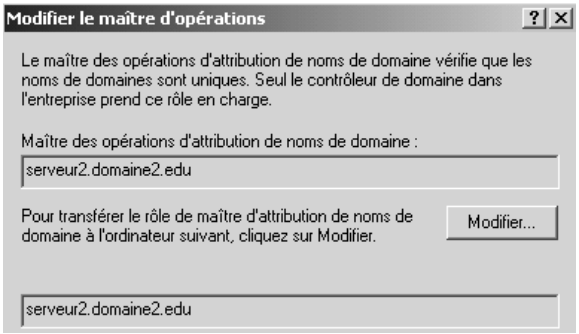






Avec la console **Domaine et approbation Active Directory** on peut trouver qui est maître d'attribution de Domaine

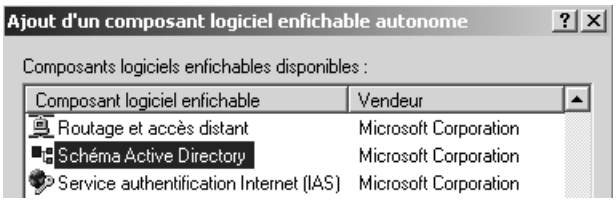
En se plaçant sur **Domaines et approbations Active Directory** on demande clic droit **Maîtres d'opérations…**



Pour localiser le maître de schéma, c'est le plus difficile. Il d'abords créer l'exécutable qui pourra ouvrir la console mmc

Via la commande **regsvr32.exe %systemroot%\system32\schmmgmt.dll**

Puis on peut alors créer une console,



Et en lançant cette console **Schéma active Directory**

En se plaçant sur **Schéma Active Directory** on demande clic droit **Propriétés / Maîtres d'opérations…**

Transférer un maître d'opération:

Bien sûr, le transfert ne peut se faire qu'entre 2 Contrôleurs de Domaine fonctionnels et en relation. On utilise pour cela les mêmes consoles que celles vues dans le chapitre précédent.

Qui peut transférer des rôles de maître d'opération ?

- **Contrôleur de schéma** : GG Administrateurs du schéma
- **Maître d'attribution de nom de domaine** : GG Administrateurs de l'entreprise
- **Emulateur CPD (NT 4.0)** : GG Administrateurs du domaine
- **Maître identificateur Relatif RID** : GG Administrateurs du domaine
- **Maître d'infrastructure** : GG Administrateurs du domaine

N.B : Si on est sur le serveur maître d'opération, il faut alors d'abords se connecter sur le serveur sur lequel on veut effectuer le transfert. On peut aussi ouvrir la console directement sur le serveur sur lequel on veut transférer le rôle.

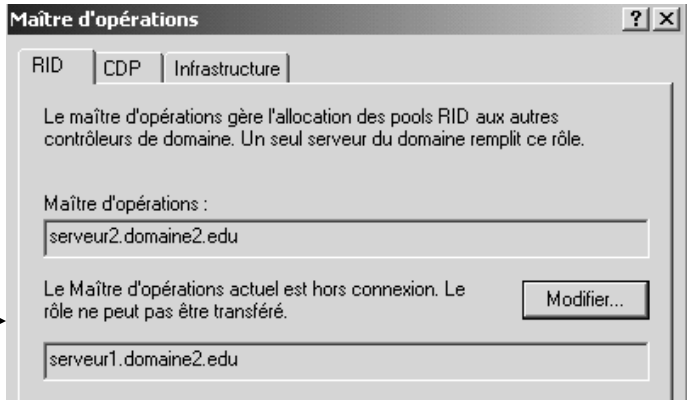
N.B : Mais lorsque l'on travaille avec le Contrôleur de schéma, on est toujours logué logiquement par défaut sur le serveur maître d'opération ! Il faut bien penser à se connecter sur le serveur sur lequel on veut effectuer le transfert…

Prendre le rôle d'un maître d'opération:

Et si la machine tombe en panne ? Evidemment on n'a pas transféré au préalable les rôles nécessaires.

Si on pense pouvoir attendre la réparation, **le mieux est de ne rien faire**, selon l'importance des la gêne, et la durée de la panne…

Sinon on peut envisager de « **prendre le rôle** », ce qui est délicat car parfois source de perte d'information. LE MODE OPERATOIRE EST IDENTIQUE, il faut juste passer outre les messages de mise ne garde !



L'utilitaire NTDSUTIL:

Cet utilitaire est un utilitaire en mode interactif, a niveau (genre netsh ou nslookup). On sort d'un niveau (ou de l'utilitaire) via la commande **quit**.

Il se lance par la commande **ntdsutil**

```
C:\>ntdsutil
ntdsutil: quit

C:\>_
```

Le niveau qui nous intéresse ici est celui accessible par la commande **roles**

```
ntdsutil: roles
fsmo maintenance:
```

il faut ensuite taper la commande **connections**

```
fsmo maintenance: connections
server connections: _
```

puis le nom du serveur sur lequel on désire effectuer une connection à travers la commande **connect to server xxxxx**

```
server connections: connect to server s1
Liaison à s1...
Connecté à s1 en utilisant les informations d'identification d'un utilisateur co
nnecté localement
server connections: _
```

une fois la connection effectuée, on remonte au niveau précédant avec la commande **quit**,

```
server connections: quit
fsmo maintenance:
```

et la on peut taper **seize** suivit du rôle que l'on veut prendre…. Ou on peut taper **transfert** suivit du rôle que l'on veut transférer….

CATALOGUE GLOBAL

Notion de Catalogue Global :

Le catalogue global est un résumé de tout ce que contient la forêt. On va y retrouver tous tes objets mais avec des propriétés simplifiées.

par exemple pour un utilisateur on aura son nom son prénom mais pas forcement le numéro de tel ou l'adresse ... mais on saura par contre à quel domaine il appartient et quel contrôleur de domaine contacter pour avoir les information restantes.

L'idée générale de cet outil est de localiser plus rapidement tous les objets d'une foret.

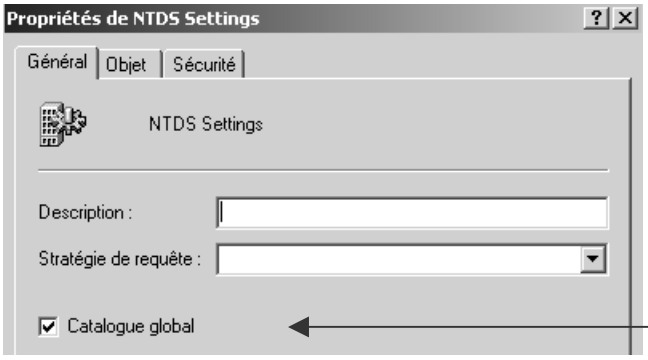
Il sert aussi sur des domaines en mode natif pour vérifier l'appartenance aux groupes universels. Si d'ailleurs il n'est pas disponible les utilisateurs non administrateur ne peuvent plus ouvrir de session. (ce n'est plus vrai avec Windows 2003)

Localisation du Catalogue Global :

A part le **premier DC du premier domaine de la forêt**, Un DC n'est PAS par défaut serveur de Catalogue Global

On peut vérifier si un DC est serveur de catalogue global via la mmc **site et service Active Directory**

dans laquelle on demande les propriétés de **NTDS Settings** de notre serveur



On sait ici que notre serveur est Serveur de Catalogue Global

Il est stocké dans un fichier **NTDS.DIT** stocké dans le dossier **WINNT\NTDS**

Son nom vient de NT directory Service . Directory Information Tree !

Serveurs supplémentaires de Catalogue Global :

N.B: tout autre CD par défaut n'est pas GC, pour qu'il le devienne, il faut cocher la case précédente **Catalogue Global** manuellement

Il faut toutefois respecter quelques règles essentielles

Combien de serveur de CG faut il avoir ? :

- Il est préférable d'avoir au moins deux GC dans la forêt. En mettre de trop peut être gênant car cela induit un trafic de réplication supplémentaire (réplication du catalogue)
- Si une structure de site existe, il est préférable avoir un serveur de CG dans chaque site physique.

Sur quels rôles de serveur FSMO dois-je installer un serveur de GC? :

- Si plusieurs domaines existent dans la forêt, les serveurs ayant le rôle de Maitres d'infrastructure ne doivent pas être serveur de GC. Car ils travaillent sur les mêmes types d'objets. Si cette règle n'est pas observée, le transfert d'un objet entre 2 domaines risque de poser pb…
- Le maître d'attribution de nom de domaine de la foret lui doit toujours être serveur de catalogue global car il l'utilise pour rechercher si le nom de domaine que l'on cherche à installer n'est pas déjà présent dans la foret.

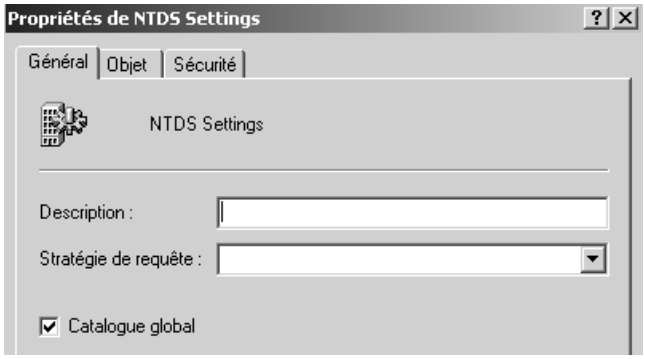
Ni Duplicata, Ni transfert :

A la différence des rôle de maître d'opération, que l'on attribue a un serveur et que l'on peut transférer, le serveur de catalogue global peut s'installer sur n'importe quel CD (en respectant les règles énoncées précédemment), et suite à une réplication de AD, il contiendra une copie complète de catalogue global.

Donc pour installer un serveur de Catalogue Global sur un CD, il suffit via la mmc **site et service Active Directory**

Demander les **Propriétés de NTDS Settings** du serveur sur lequel on veut installer un nouveau catalogue global !

on coche la case Catalogue global



Une attente de 15mn (réplication de AD) voire un reboot de la nouvelle machine DC/GC peut être nécessaire . Le journal des applications devrait consigner l'opération

Pour désinstaller un serveur, on décoche la case…

N.B: On ne transfère pas un serveur de Catalogue Global, mais on procède de la manière suivante :

1. on en active un 2°,
2. on attend une réplication,
3. puis on désactive le 1° (en faisant attention a ce qu'il ne s'agisse pas du CD qui a le rôle de maître d'attribution de nom de domaine de la foret) Si cela est nécessaire, on transfère également ces rôles...

---

exemple de distribution de roles fsmo et serveur de CG:

1 domaine dans une forêt avec 1 CD

serveur CD1

- Contrôleur de schéma
- Maître d'attribution de nom de domaine + Serveur de Catalogue Global

1 & 2 sont **uniques pour la forêt**

- Emulateur CPD (NT 4.0)
- Maître identificateur Relatif RID
- Maître d'infrastructure (désactivé)

3 – 4 – 5 **sont uniques pour un Domaine**

2 domaines dans une forêt avec 2 CD domaine 1 et un Cd domaine2

Domaine 1 serveur CD1

- Contrôleur de schéma
- Maître d'attribution de nom de domaine + Serveur de Catalogue Global

1 & 2 sont **uniques pour la forêt**

- Emulateur CPD (NT 4.0)
- Maître identificateur Relatif RID

3 – 4 – 5 **sont uniques pour un Domaine**

Domaine 1 serveur CD2

- Maître d'infrastructure

Domaine 2 serveur CD1

- Emulateur CPD (NT 4.0)
- Maître identificateur Relatif RID
- Maître d'infrastructure

Domaine 2 serveur CD2 (inutile a ce niveau là)

- -

NB: dans cet exemple, si on n'avait qu'un seul CD pour le domaine 1, on aurait désactivation du maître d'infrastructure, et non fonctionnalité du transfert d'objet d'un domaine à l'autre (...)

SUPPRESSION DU C.D. D'ORIGINE

Dcpromo pour "dépromoter":

Normalement lors d'un **Dcpromo** un autre DC pour transférer les rôles est cherché.... c'est fiable, mais il vaut mieux vérifier manuellement que les transferts se soient bien effectués...

Maintenant, en toute connaissance de cause, un changement de CD pourrait se faire simplement par :

- Installation du nouveau serveur
- Ajout des serveurs installés nécessaires : DNS (création de la zone), éventuellement DHCP (récuperation d'un backup)...
- Attente de la réplication de AD (ou forcer via replmon.exe)
- Vérification du Transfert de rôles de maître (si besoin car normalement lors d'un Dcpromo un autre DC pour transférer les rôles est cherché....)
- Duplicata du catalogue global
- Arrêt de l'ancien contrôleur
- Vérification paramétrage nouveau DC
- Allumage et Retrait de l'ancien contrôleur

Bien sûr, le transfert ne peut se faire qu'entre 2 Contrôleurs de Domaine fonctionnels et en relation. On utilise pour cela les mêmes consoles que celles vues dans le chapitre précédent.

N.B : Si on est sur le serveur maître d'opération, il faut alors d'abords se connecter sur le serveur sur lequel on veut effectuer le transfert

RELATIONS D'APPROBATIONS

Approbations implicites:

Dans un modèle de domaine unique ou dans un environnement où il n'existe pas de relation d'approbation "explicite" entre deux domaines quelconques, la relation d'approbation "implicite" est active et nécessaire du point de vue opérationnel.

Cette approbation implicite existe entre tous les ordinateurs Windows NT membres d'un domaine et un contrôleur de domaine de leur domaine

Les relations d'approbation implicites sont établies en rendant un ordinateur membre d'un domaine...

Approbations explicites :

Lorsque le terme **Approbation** est utilisé dans le contexte de Windows NT, il décrit souvent une relation entre deux domaines Windows NT. Chaque domaine impliqué tient soit le rôle du **domaine approbateur**, soit celui du **domaine approuvé**. Pour toute relation d'approbation donnée, il existe un canal unique de communications discrètes entre chaque contrôleur de domaine du domaine approbateur et un contrôleur de domaine du domaine approuvé

Les relations d'approbations explicites peuvent être de différentes natures :

- Elles peuvent être **uni-directionelles**, c'est à dire que ce n'est pas parce que un domaine approuve un autre domaine, que la réciproque est vrai. (Si A approuve B, alors B n'approuve pas A)
- Elles peuvent être **bi-directionelles** , c'est à dire que 2 chemins d'approbation vont dans les 2 direction entre 2 domaines (Si A approuve B, alors B approuve A)
- Elles peuvent être **transitives** , c'est à dire que 2 chemins d'approbations permettent d'en définir un troisième (Si A approuve B, et B approuve C alors A approuve C...)

Approbation Unidirectionelle non transitive :

Il peut être nécessaire de créer des relations d'approbation explicites entre des domaines.

Lorsque vous établissez une relation d'approbation entre deux domaines, les utilisateurs d'un domaine peuvent obtenir l'accès à des ressources qui se trouvent dans un autre domaine approuvé

1. dans le cas d'une approbation entre un domaine Microsoft Windows NT 4.0 et un domaine Windows 2000. (NT 4.0 ne peut pas entretenir des relations d'approbation transitive avec des domaines Windows 2000)
2. lorsque des domaines Windows 2000 appartenant à des forêts disparates souhaitent partager une relation d'approbation

   exemple : Une approbation unidirectionnelle d'un domaine "pare-feu" vers un domaine "production" permet aux comptes du domaine interne d'être approuvés par le domaine externe, sans permettre l'inverse.

N.B: La création d'une relation d'approbation entre un domaine Windows 2000 et un domaine Windows NT 4.0 est similaire à l'établissement d'une relation d'approbation entre deux domaines Windows NT 4.0.. la résolution de nom NETBIOS doit être activée

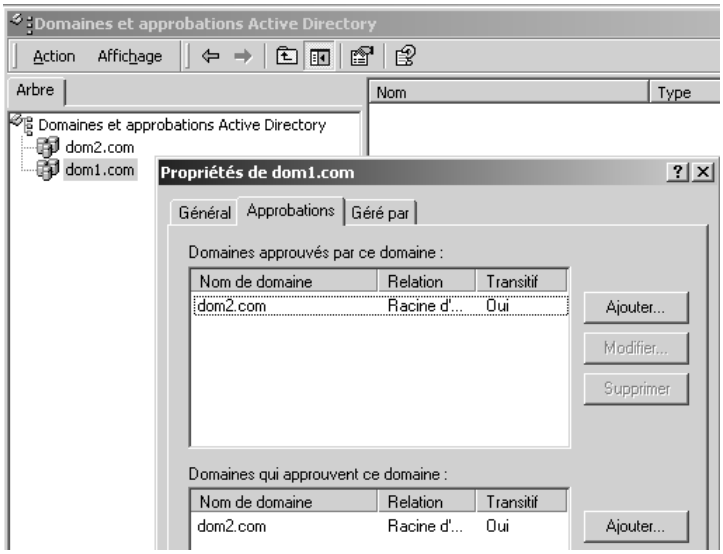
Mise en oeuvre

Soit un domaine ayant le rôle du **domaine approbateur (ex: AUTRE.COM)**, soit celui du **domaine approuvé (ex: DOM1.COM)**. On veut donc que les utilisateurs du domaine DOM1 puissent avoir accès (soient approuvés...) à des ressources qui se trouvent dans le domaine AUTRE. Mais pas le contraire !

la résolution de nom DNS doit être opérationnelle entre les 2 domaines...

Sur le domaine approuvé (dom1.com)

1. Sur un CD du domaine approuvé (DOM1) il faut lancer **Domaines et approbations Active Directory**...sur la partie gauche on se place sur notre domaine, puis on demande **propriétés**, onglet **Approbations**



Ici, notre domaine dom1.com, approuve déjà un domaine dom2.com...

NB: distinguer les 2 volets

Domaine approuvés

et

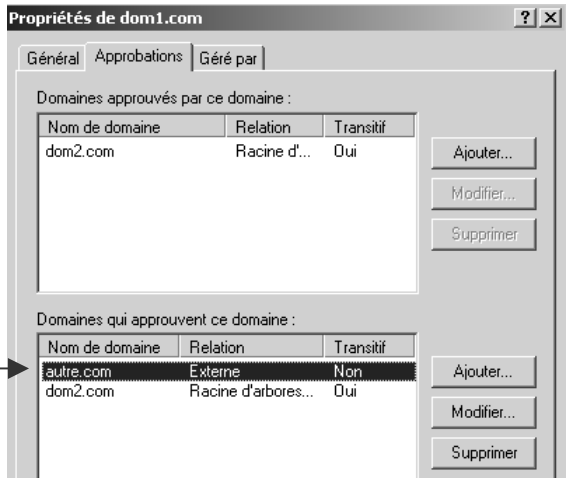
Domaines qui approuvent

2. Dans le volet "**Domaines qui approuvent ce domaine**" demander **ajouter** et saisir le nom AUTRE.COM et un mot de passe (pour cette relation)

N.B: le mot de passe demandé ici est lié à la relation d'approbation uniquement

3. Une fois validé par Ok, on ne pas vérifier l'approbation, (il faudrait pour cela s'identifier avec un compte autorisé a modifier les relations d'approbation, sur le domaine autorisé à approuver...(c'est à dire le domaine approbateur autre.com) CAR SUR L'AUTRE DOMAINE LA RELATION N'EST PAS ENCORE FAITE !

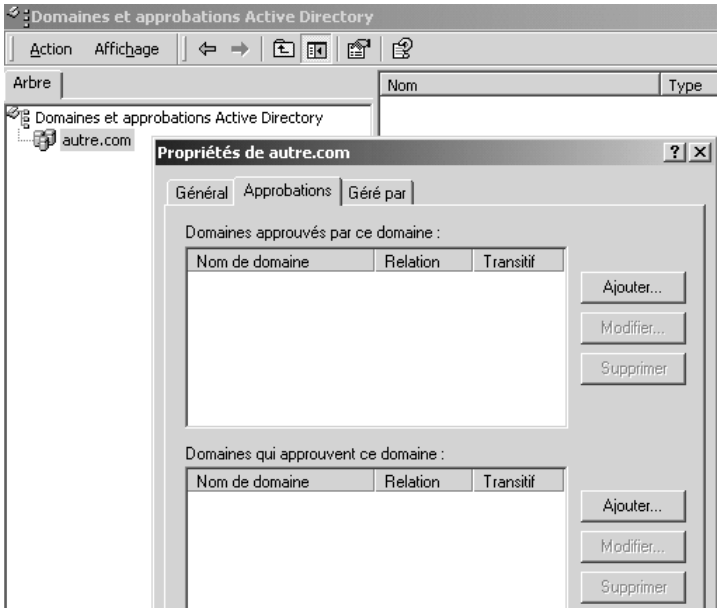
Voici donc notre nouvelle relation d'approbation avec le domaine AUTRE.COM



4. Quitter

Sur le domaine approbateur (autre.com)

1. Sur un CD du domaine autorisé à approuver (autre.com) il faut lancer **Domaines et approbations Active Directory**...Cliquer avec le bouton droit sur notre domaine, **Propriétés** onglet **Approbations**



2. Dans la zone "**Domaines approuvés par ce domaine**" demander **ajouter** et saisir le nom DOM1.COM et le mot de passe (pour cette relation)

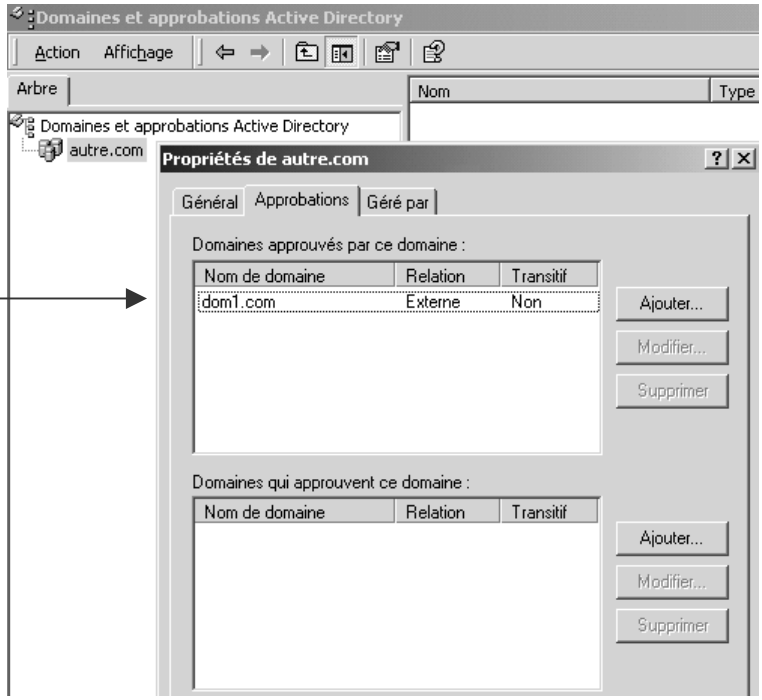
N.B: le mot de passe demandé ici est lié à la relation d'approbation uniquement

CELA DOIT ETRE LE MEME QUE CELUI DONNE POUR L'AUTRE MOITIE...

3. ok et on doit obtenir un message de confirmation

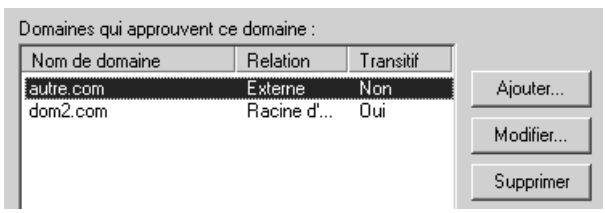
et notre relation doit apparaître ainsi :

Voici donc notre nouvelle relation d'approbation avec le domaine DOM1.COM



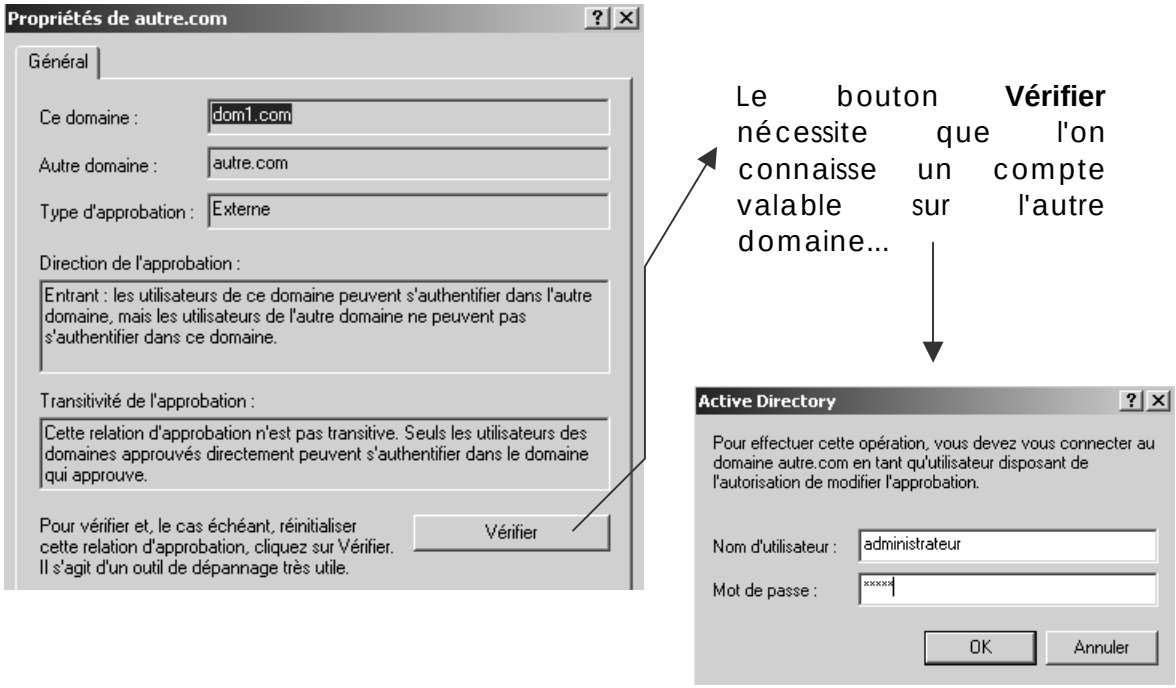
Tester la relation

La relation peut se tester de n'importe quel coté, soit du coté approuvant, soit du coté approuvé.



Pour tester la relation il faut demander, une fois la relation à tester sélectionnée, **Modifier**...

on obtient alors



N.B: il existe aussi un utilitaire en ligne de commande nommé **nltest.exe**...

Approbations Bidirectionelles non transitives :

Par rapport au cas présenté ci-dessus, il s'agit uniquement de construire la relation "réciproque"...

1. dans le cas d'une approbation entre un **domaine Microsoft Windows NT 4.0 et un domaine Windows 2000**
2. Entre domaines Windows 2000 **appartenant à des forêts disparates**

Approbations Bidirectionelles transitives :

Par rapport au cas présenté ci-dessus, ces relations sont celles qui se construisent automatiquement lorsque l'on crée des domaines du type suivant :

- **Enfant** (relation bidirectionelle avec le parent, transitive avec le grand-parent ou le petit-enfant...)
- **Nouvelle arborescence à l'intérieur d'une même forêt** (relation bidirectionelle avec toutes les arborescence de la forêt, transitive avec le grand-parent ou le petit-enfant éventuels...)

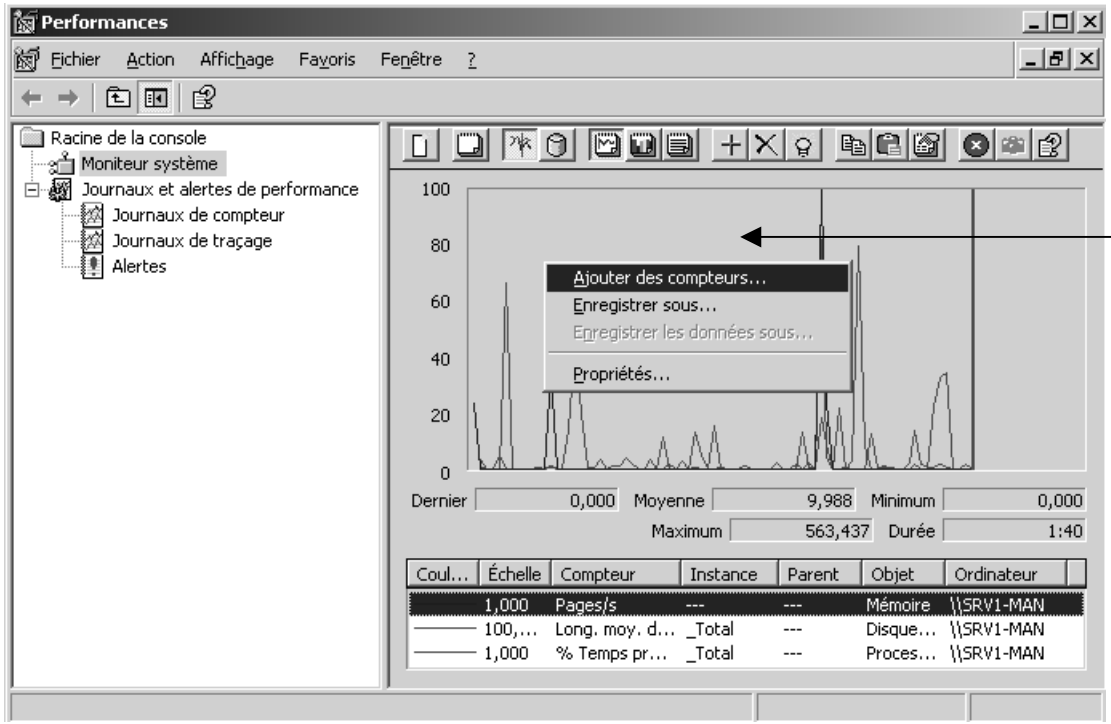
MONITEUR SYSTEME

L'analyseur de performance :

Il se lance depuis le menu

Outils d'Administration / Analyseur de performance (sous 2000) ou

Outils d'Administration / Performances (sous 2003)

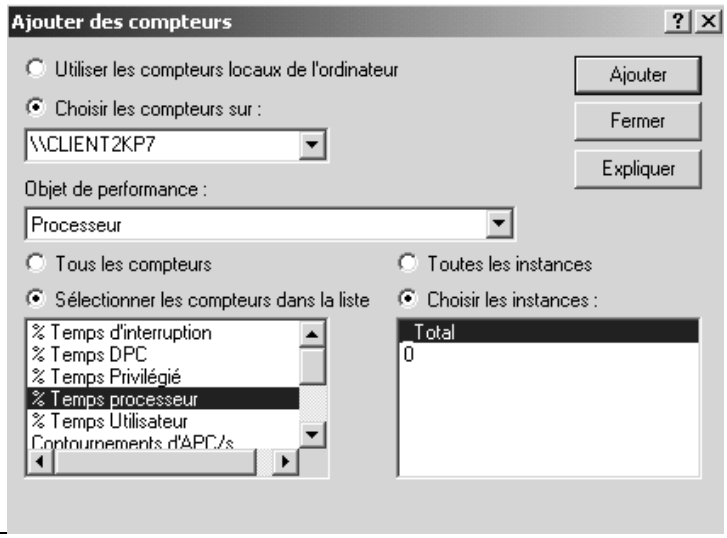


On ajoute des compteurs en demandant un menu contextuel à droite ...

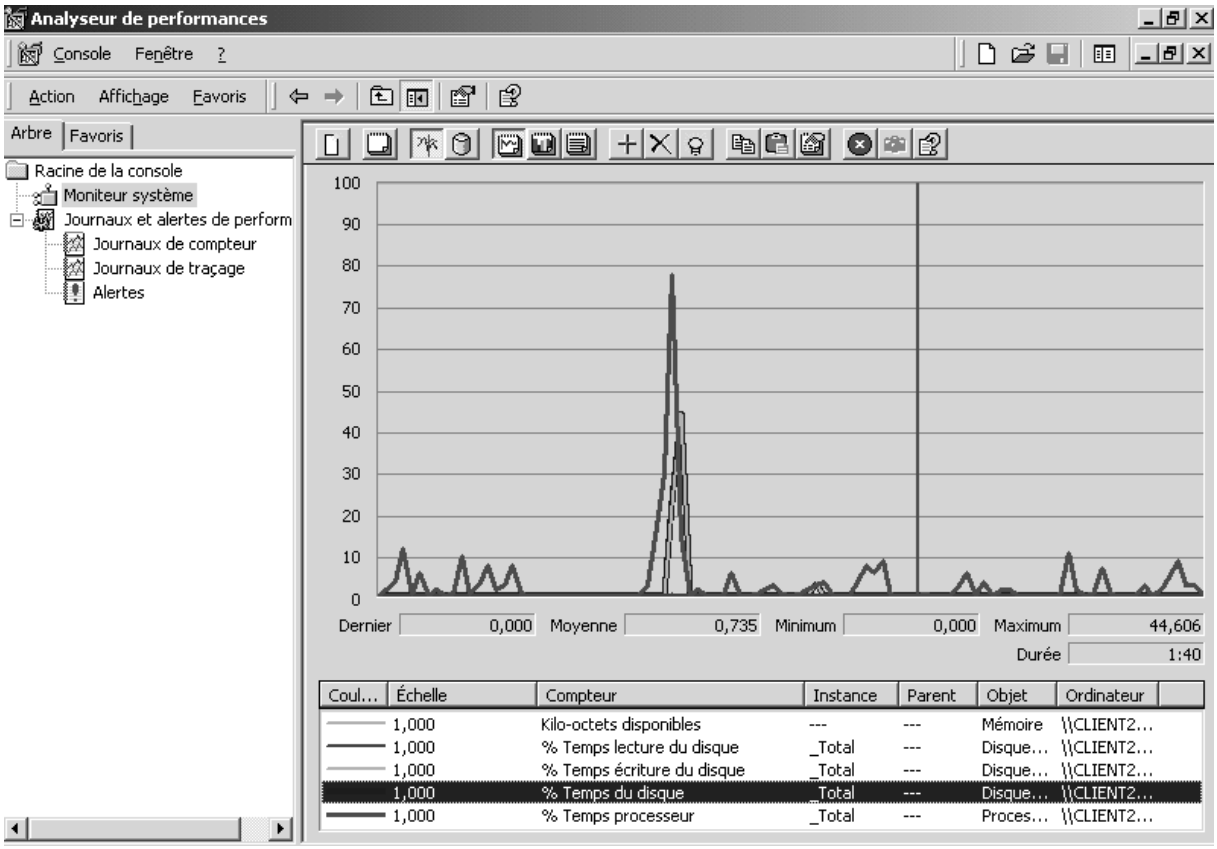
Et on peut créer des compteurs sur toute machine sur laquelle on peut accéder

Par exemple classiquement :

- **% temps processeur**
- **% ko dispo Mémoire**
- **Disque physique % temps ecriture**
- **Disque physique % temps lecture**



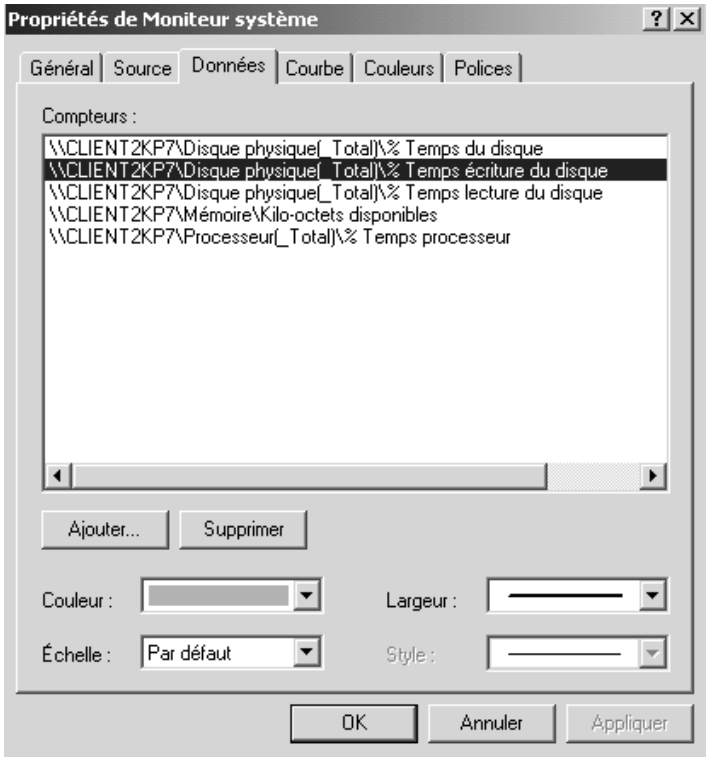
Créons un moniteur système surveillant ces points sur notre machine



La mise en forme est évidemment possible

Il suffit de choisir par le menu contextuel **Propriétés**,

puis de sélectionner l'onglet et le compteur voulu...

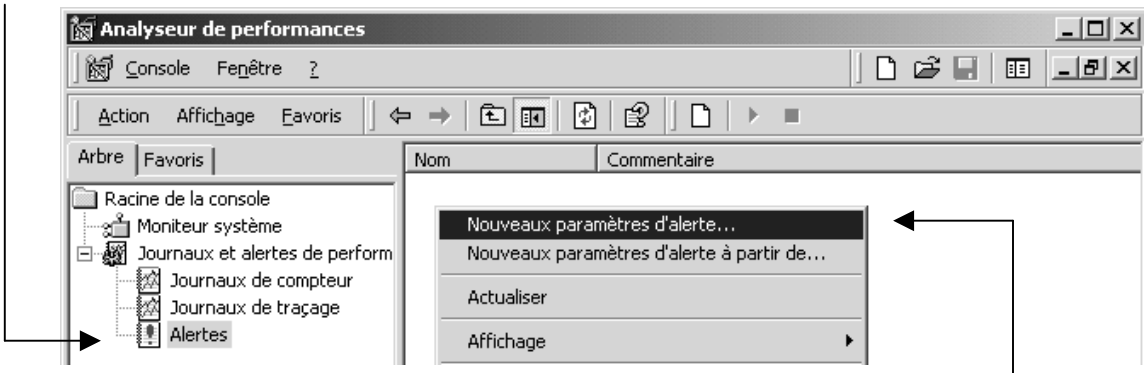


NB: Ajouter visuellement des compteurs, ne charge pas le processeur, car les compteurs sont renseigné automatiquement par le système, il s'agit ici simplement de décider de les afficher visuellement, ou non...

Gestion des alertes :

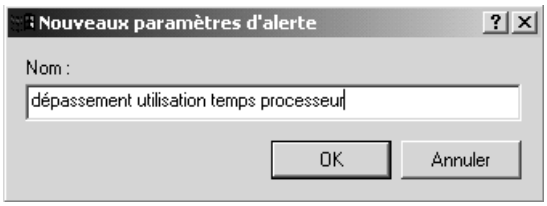
Ce qui est très intéressant, dans l'analyseur de performance, c'est la possibilité de configurer des alertes...permettant d'avoir une information comme quoi tel ou tel seuil est atteint ou dépassé !

Il faut se placer sur les **Alertes**, à gauche

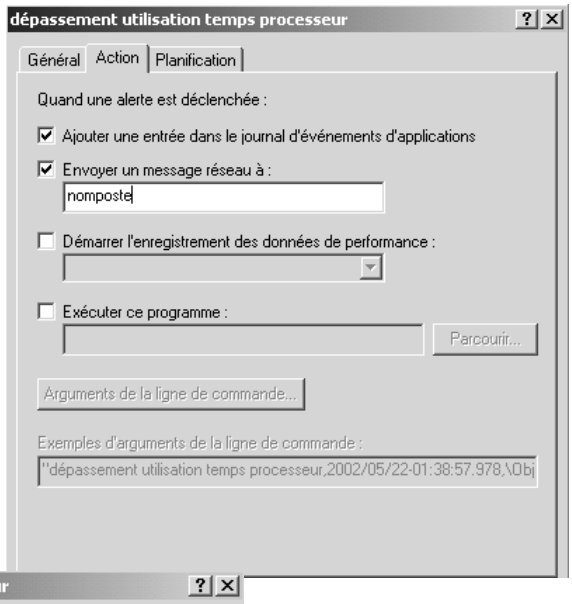


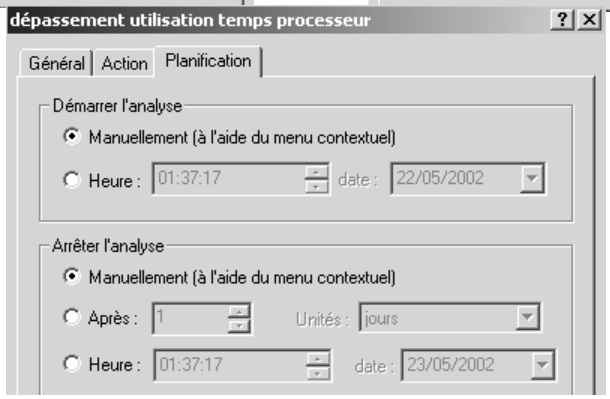
et demander à droite via le menu contextuel, **Nouveau paramètres d'alerte**

il faut donner un nom a notre détection d'alerte

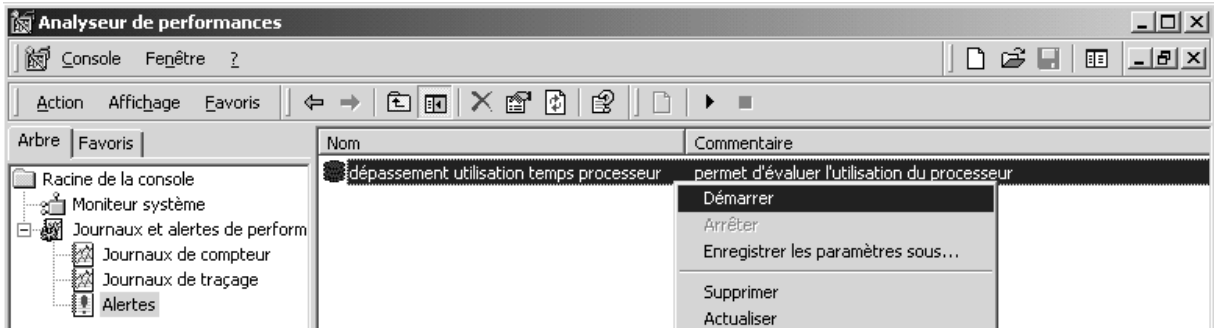


puis la paramétrer avec les 3 onglets **Général**, **Action** et **Planification**





Enfin il faut la démarrer avec le menu contextuel

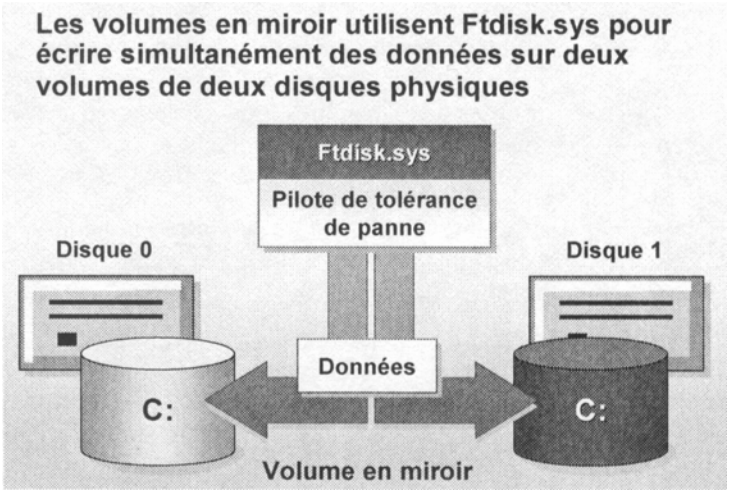


N.B: les alertes se placent sur le s clients et "réfèrent" sur les serveurs... jamais le contraire.

VOLUMES EN MIROIR

Principe du Raid1 :

L'idée est de recopier systématiquement un disque sur un autre...



N.B: Le 2° disque doit être de taille >= au premier disque...

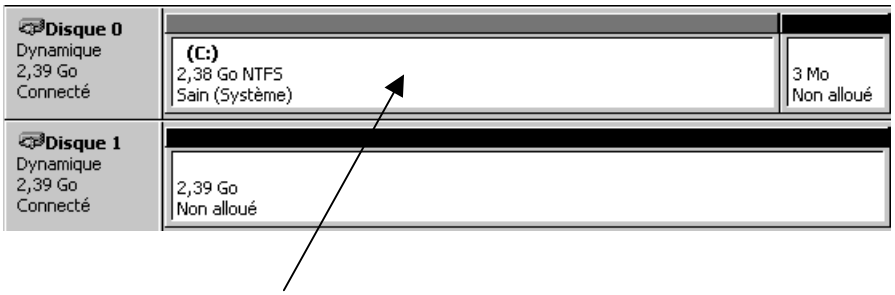
Ce système est préconisé pour les partitions système, et supporte les système de fichier FAT et NTFS

Le RAID1 est de bonne performances en lecture, et un peu moins bon en écriture...., ce qui le prédispose pour la sécurisation du système d'exploitation

Le RAID1 consomme 50% de la place disque, donc est relativement cher en prix du Mo sécurisé...

Création d'un miroir (de volume existant) :

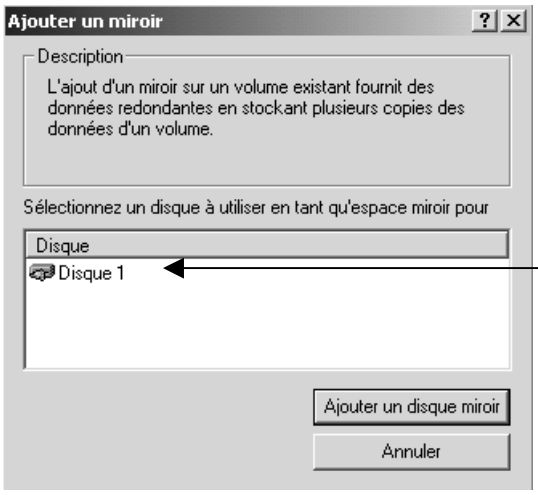
cela ne peut se faire que sur des disques dynamiques, en FAT ou NTFS, et le 2° disque doit être de capacité **>=** au premier...



il faut se placer sur le volume que l'on veut mettre en miroir, et demander via un clic droit de la souris →

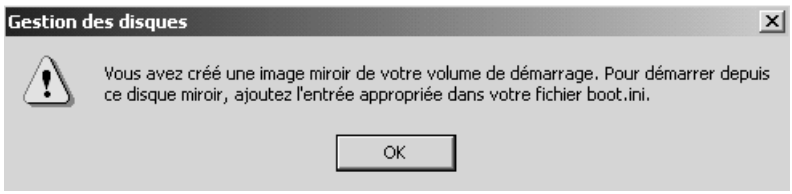
Ajouter un disque miroir

On obtient alors

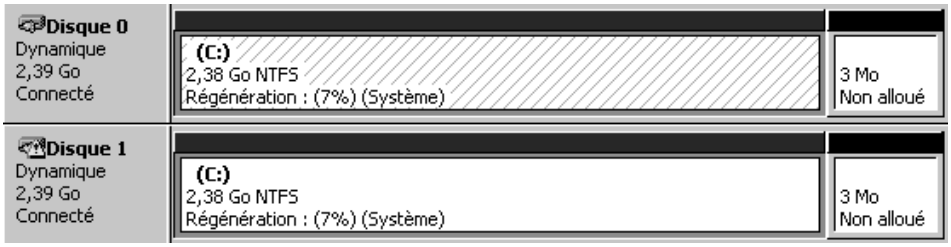


Dans laquelle il faut choisir le disque à utiliser pour construire le mirroir

N.B: ce message de mise en garde n'apparaît que si on met en miroir le disque système...(cf chapitre suivant création "miroir disque système")

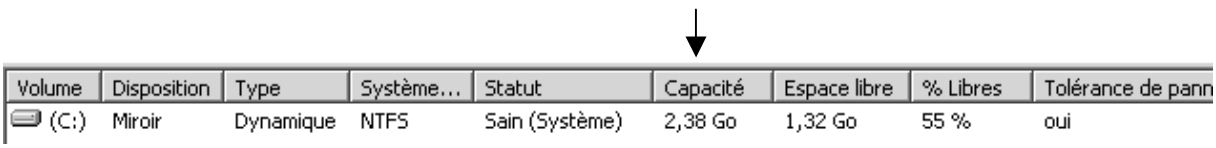


puis la construction du miroir commence



pour se finir avec

on peut remarque que dans le gestionnaire de disque, la capacité totale du miroir est de 50% de la somme des tailles des 2 disques (1 disque sur deux...)



Volume	Disposition	Type	Système...	Statut	Capacité	Espace libre	% Libres	Tolérance de pann
(C:)	Miroir	Dynamique	NTFS	Sain (Système)	2,38 Go	1,32 Go	55 %	oui

Création d'un miroir de disque système :

Pourquoi doit on modifier le boot.ini en cas de mirroring système ?

Rappels : la commande gérant le multiboot sous NT est une commande permettant d'indiquer sur quel disque on doit aller chercher les fichiers de NT. Sur un système de base, avec sur la carte mère 1 les deux contrôlleurs IDE pilotant chacun un disque IDE configuré en maître on peut alors dire que

le disque1 est atteint par **multi(0)disk(0)rdisk(0)partition(...)**

le disque2 est atteint par **multi(0)disk(0)rdisk(1)partition(...)**

NT étant installé (par exemple) sur le premier disque, on aura alors la commande suivante dans le fichier boot.ini

multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Server" /fastdetect

Si on installe un système de mirroring entre ces deux disques, on aura alors pour les deux un boot.ini identique, ce qui est normal !

1° cas de défaillance : disque2 ko

c'est le cas le plus simple, il suffit de remplacer le 2° disque, puis de reconstruire le miroir... pendant tout le temps, le disque restant reste opérationnel et utilisable (c'est bien un disque que l'on va chercher avec **multi(0)disk(0)rdisk(0**)... dans boot.ini, que le 2° disque soit présent, ou absent !)

2° cas de défaillance : disque1 ko

ce cas nécessite un détail de la situation, en effet le disque "miroir restant" est opérationnel mais avec un boot.ini renseigné comme devant aller chercher le 1° disque.

Si le disque 1 est physiquement absent, on bootera sans pb

si le disque 1 est physiquement présent, on ne bootera plus tant que on ne modifiera pas le fichier boot.ini pour inscrire **rdisk(1**) à la place de **rdisk(0)**. Une fois cela fait,(avec une disquette système par exemple)on remet un disque 1 ok est on peut reconstruire le miroir...

Création d'un miroir (de volumes non alloués) :

Il suffit de faire un clic droit, et demander de créer un volume en miroir dans l'assistant. Il faut alors indiquer quels disques veut on mettre dans le miroir parmi les disques disponibles

Suppression d'un miroir :

La suppression d'un miroir est une opération qui de perds pas les données du miroir, mais qui "désolidarise" les deux disques.

A partir de la on peut faire ce que l'on veut des volumes récupérés !

PANNES VOLUMES EN MIROIR

Panne sur disque classiques :

L'idée est de briser le miroir, puis de le reconstruire

Panne sur disque système :

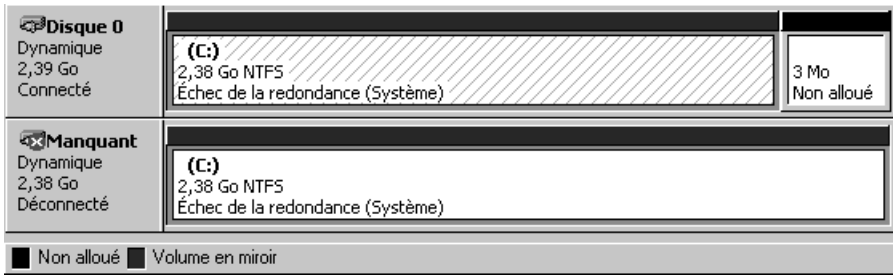
lorsque un panne arrive, la solution dépends du disque sur lequel la panne arrive.... Sur un système de base, avec sur la carte mère 1 les deux contrôlleurs IDE pilotant chacun un disque IDE configuré en maître on peut alors dire que NT étant installé (par exemple) sur le premier disque.

le disque1 est atteint par **multi(0)disk(0)rdisk(0)partition(...)**

le disque2 est atteint par **multi(0)disk(0)rdisk(1)partition(...)**

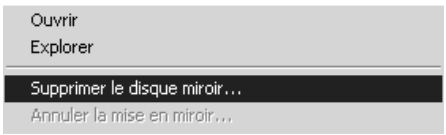
1° cas : panne du disque 2 "miroir"

il est certain que si le disque est juste déconnecté, ou absent, on pourra tenter des commandes du type réactiver le disque....

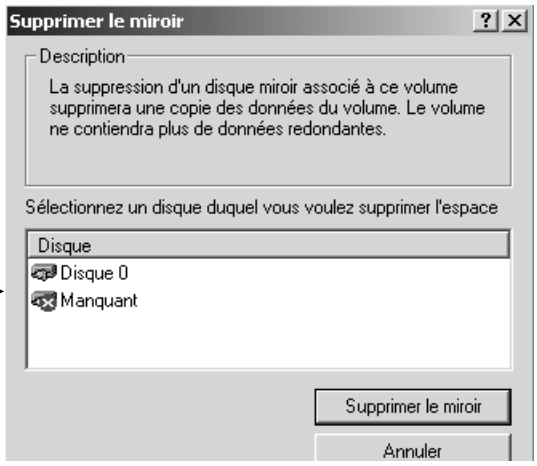


mais partons du principe que le 2° disque est irrémédiablement endommagé. Il va falloir briser le miroir, puis le reconstruire lorsque l'on aura introduit un nouveau 2°disque en état de marche.

pour briser le miroir, on sélectionne l'un des 2 membre du miroir et on demande

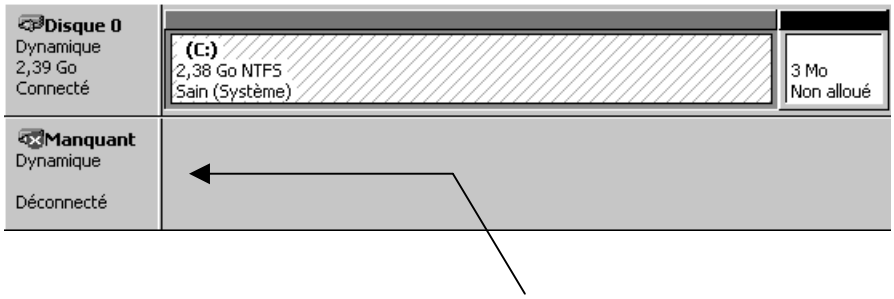


il faut choisir le disque sur lequel on veut supprimer le miroir



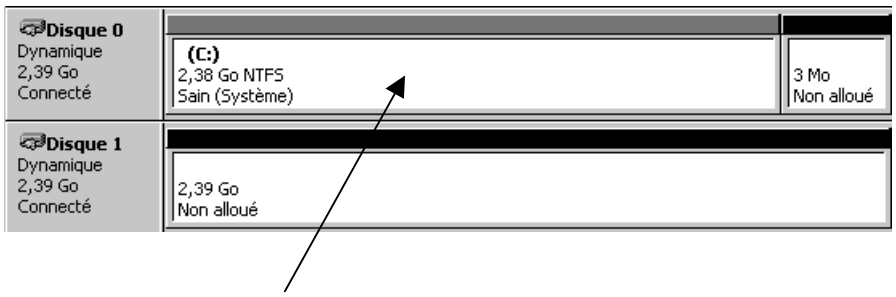
et confirmer

on obtient alors



N.B: il faut ensuite "supprimer" le disque manquant via clic droit de la souris

Après réintroduction d'un disque en état de marche....(import...) on se retrouve dans la situation initiale, de création d'un volume miroir.



il faut se placer sur le volume que l'on veut mettre en miroir, et demander via un clic droit de la souris

Ajouter un disque miroir

Le reste est classique !!!!

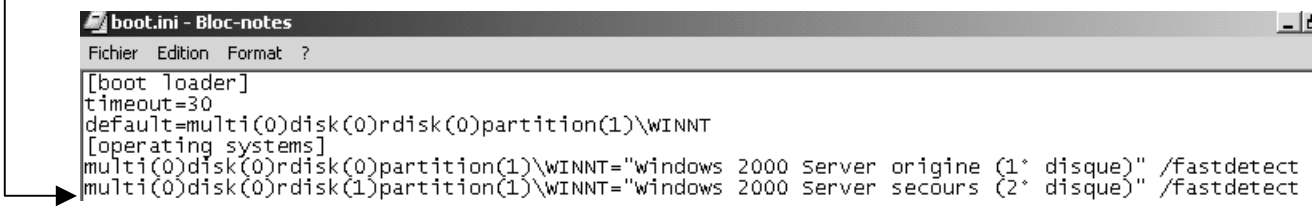
2° cas : panne du disque 1 "boot"

cette fois-ci il faut se prémunir contre une défaillance du 1° disque, et donc se préparer à booter sur le 2° disque restant du miroir....

on va se créer une **disquette de démarrage** permettant de booter soit depuis NT installé sur le 1° disque, soit depuis NT installé sur le 2° disque...

pour créer la disquette de démarrage, il faut :

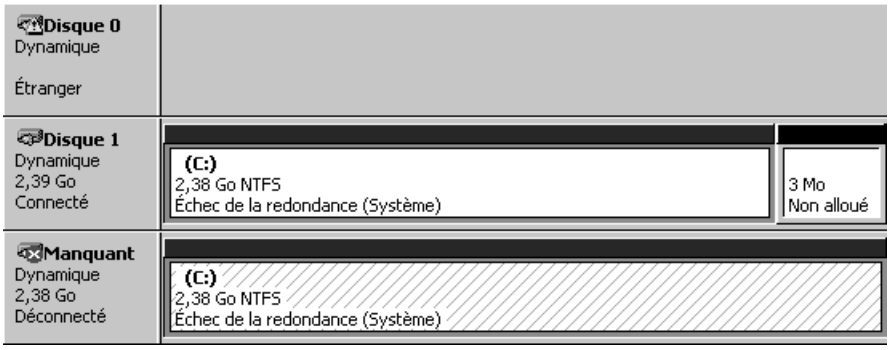
- formater la disquette **depuis NT** (pour que celle-ci cherche automatiquement un ntldr...)
- copier dessus les 3 fichiers minimum que sont **ntdetect.com**, **ntldr** et **boot.ini**
- modifier le fichier boot.ini en y rajoutant l'entrée permettant de booter sur un 2° disque, soit



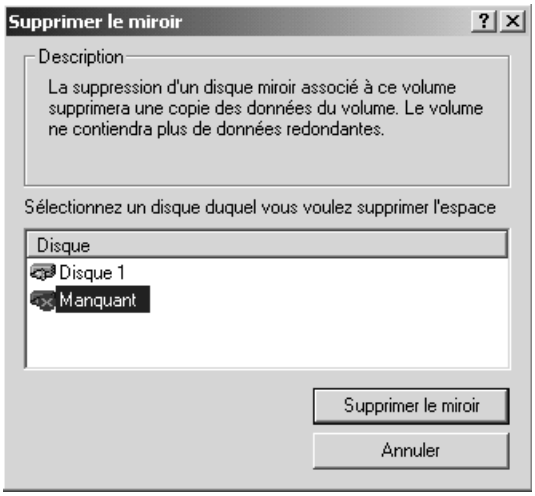
lorsque le 1° disque tombe en défaillance, il faut booter sur la disquette, et demander de démarrer sur Windows de secours.... (ou alors enlever physiquement le disque défaillant....) et le tour est joué !

pour réparer, on introduit un disque correct en 1° disque, il faut booter sur la disquette, et demander de démarrer sur Windows de secours....

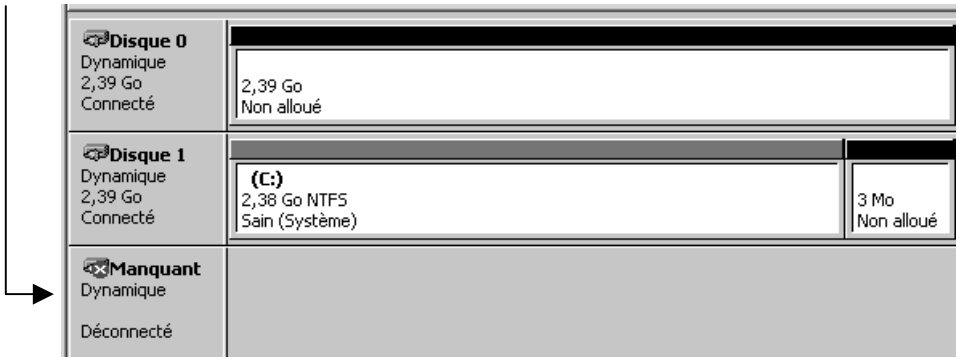
on prends alors la main, et dans le gestionnaire de disque on peut voir



Il faut alors importer le disque étranger.... briser le miroir,



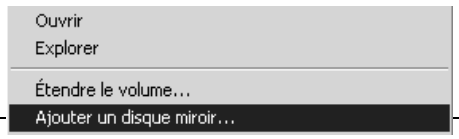
puis supprimer le disque manquant,



pour retrouver

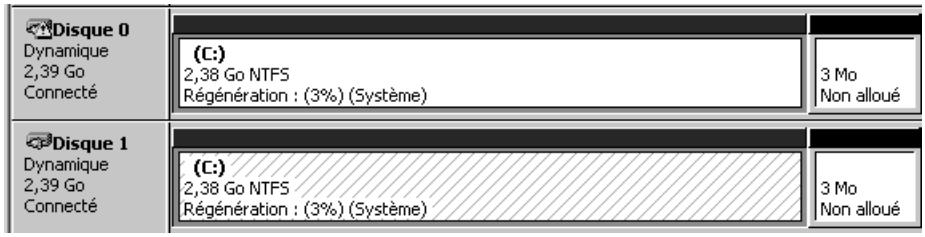
Il ne reste plus qu'à recréer le miroir classiquement!!!

il faut se placer sur le volume que l'on veut mettre en miroir, et demander via un clic droit de la souris →



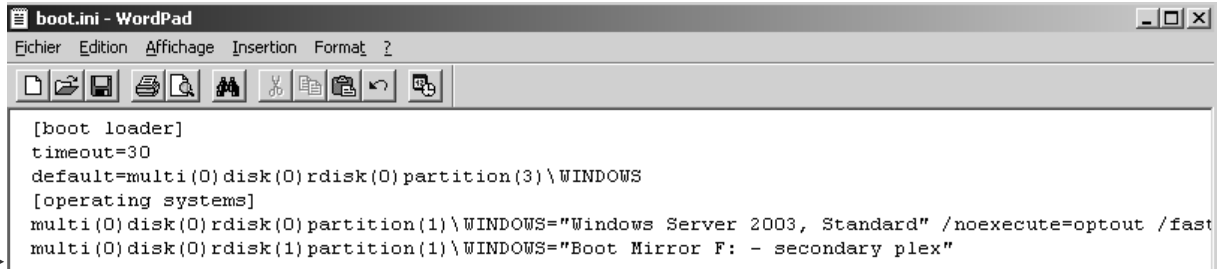
Ajouter un disque miroir

Le reste est classique !!!!



Boot ini Raid1 et 2003 Serveur :

Pour nous aider un peu, lors de la création du miroir, 2003 modifie lui-même le fichier Boot.ini pour nous donner le chemin du disque miroir.

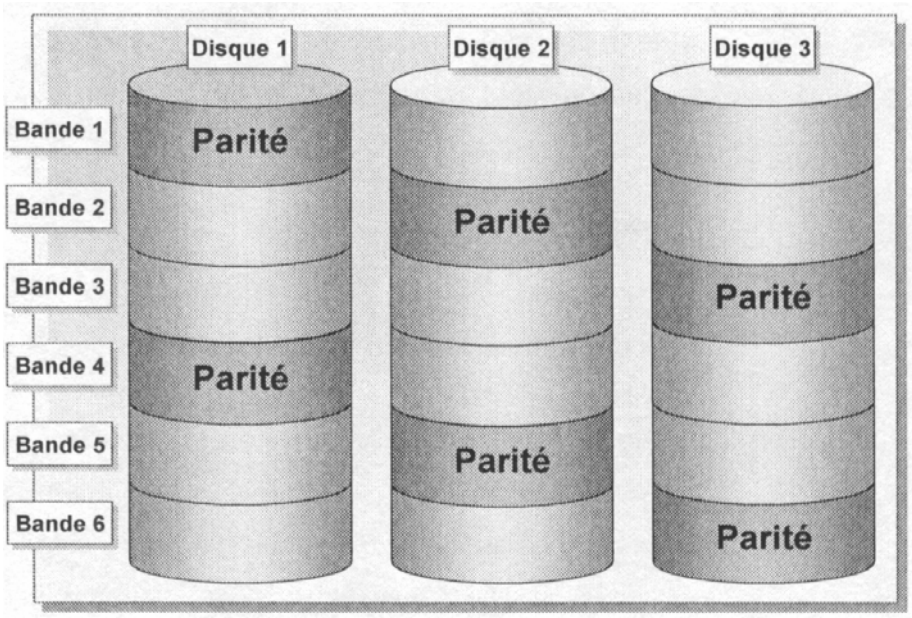


Il faudra donc impérativement faire une disquette d'amorçage après construction du miroir par Windows 2003 !

VOLUMES EN RAID5

Principe du Raid5 :

L'idée est de pouvoir recalculer un disque à partir des autres disques du système Raid5 ...



N.B: Les 3° disques doivent être de taille = ...

Ce système est préconisé pour les partitions de données, et supporte les système de fichier FAT et NTFS

Le RAID5 est de bonne performances en lecture, et un peu moins bon en écriture...., néanmoins il est plus rapide en écriture que le miroring... ce qui le prédispose au stockage des données...

Le RAID1 consomme de la place disque en fonction du nombre de disque qui le compose , donc est relativement moins cher en prix du Mo sécurisé que le miroring...

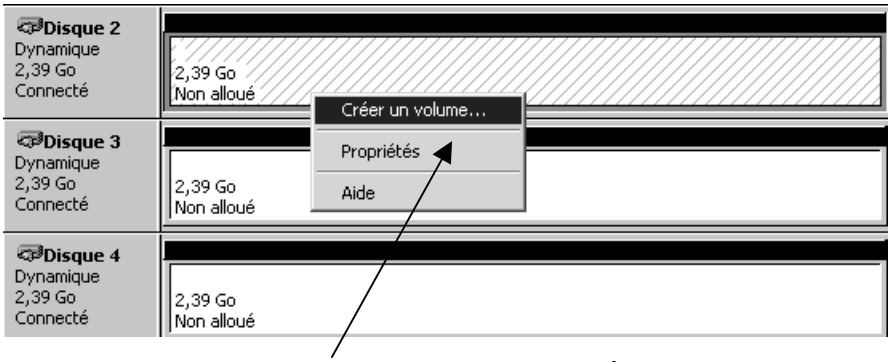
Le calcul de la place consommée et de 1 disque par système RAID5 mis en place.... L'ajout de disques supplémentaire ne modifie pas la sécurité, mais augmente la place disque de stockage et la vitesse d'accès au données.

Exemple avec des disques de 2 Giga :

Nombre de disques	Espace disque utilisé	Espace disque disponible	Redondance
3	6 Go	4 Go	33%
4	8 Go	6 Go	25%
5	10 Go	8 Go	20%

Création d'un volume Raid5 :

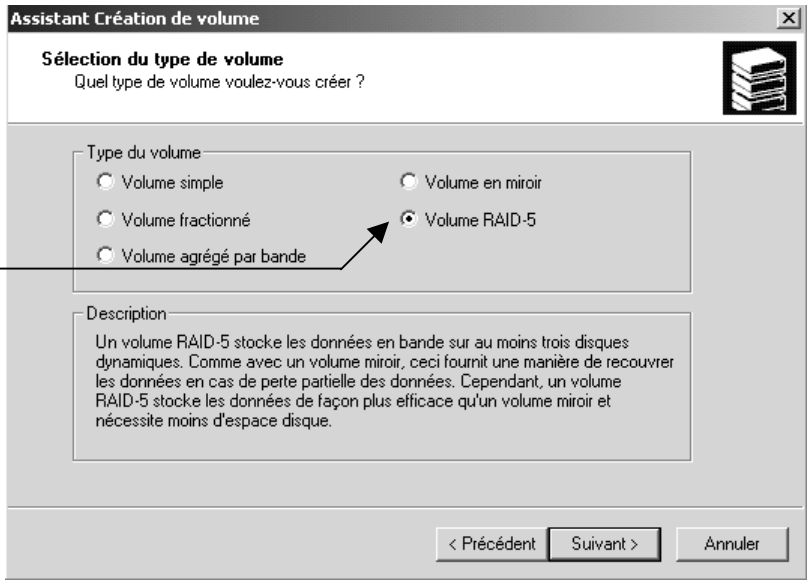
cela ne peut se faire que sur des disques dynamiques, en FAT ou NTFS, et les 3° disques (minimum)doivent être de capacité **équivalente**...



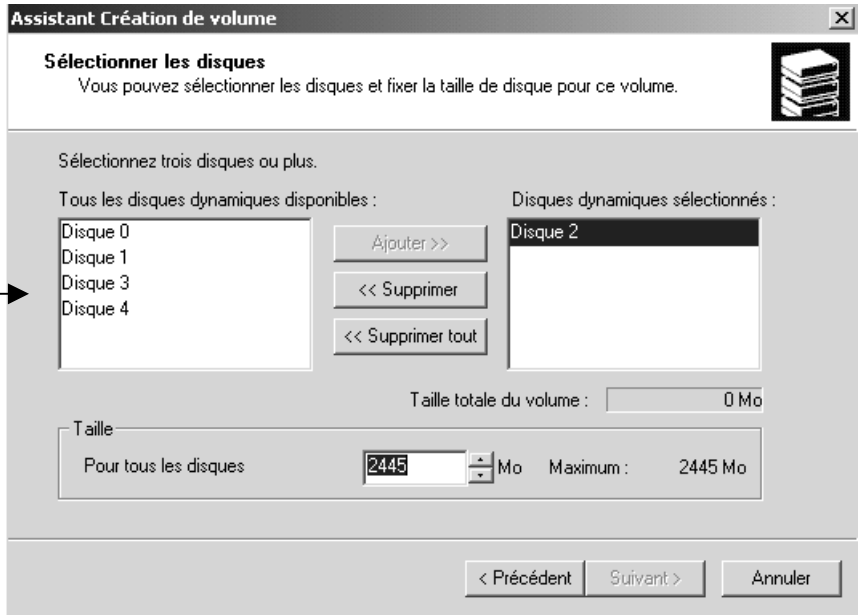
il faut se placer sur le volume que l'on veut créer, et demander via un clic droit de la souris

Créer un volume

de type **RAID-5**

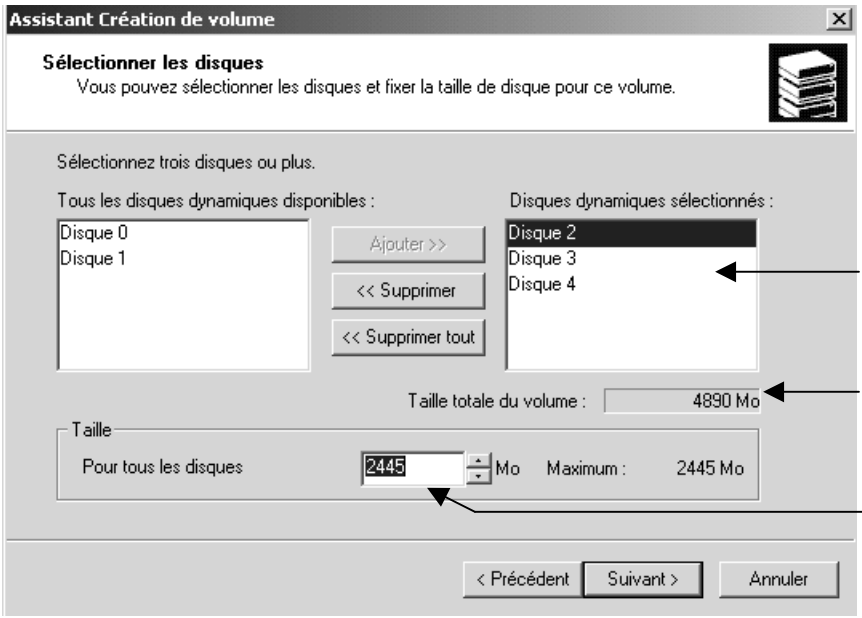


Puis dans l'étape suivante de l'assistant



Choisir les disques ayant un volume non alloué identique entre eux, pour créer le volume RAID5

Une fois ce choix fait, on a alors

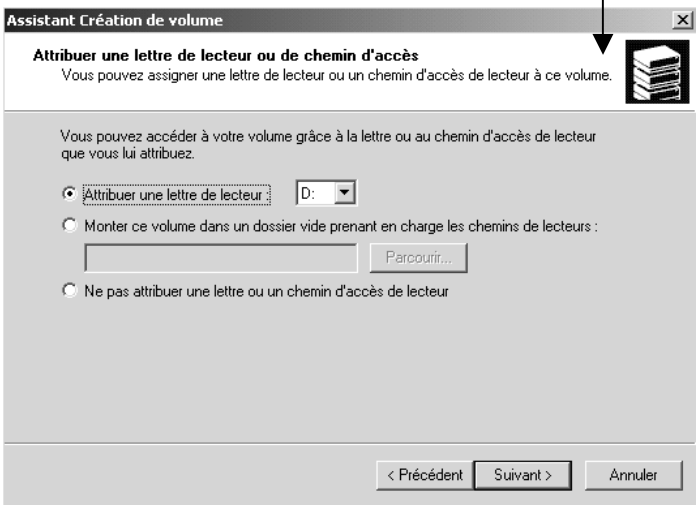


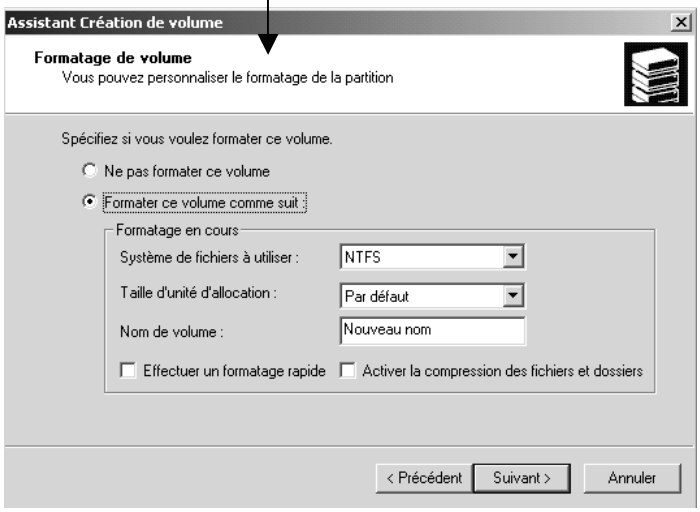
Liste des disques participant au RAID5

Volume global du RAID 5

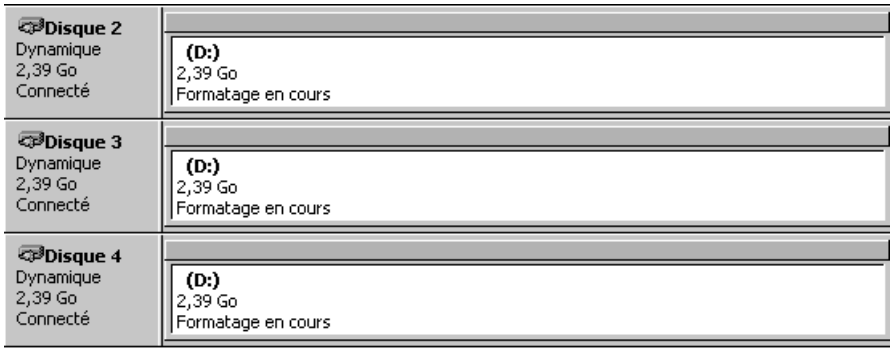
Volume pris sur chaque disque

ensuite il faut indiquer le lecteur , et le type de formatage





et la construction du volume RAID s'effectue

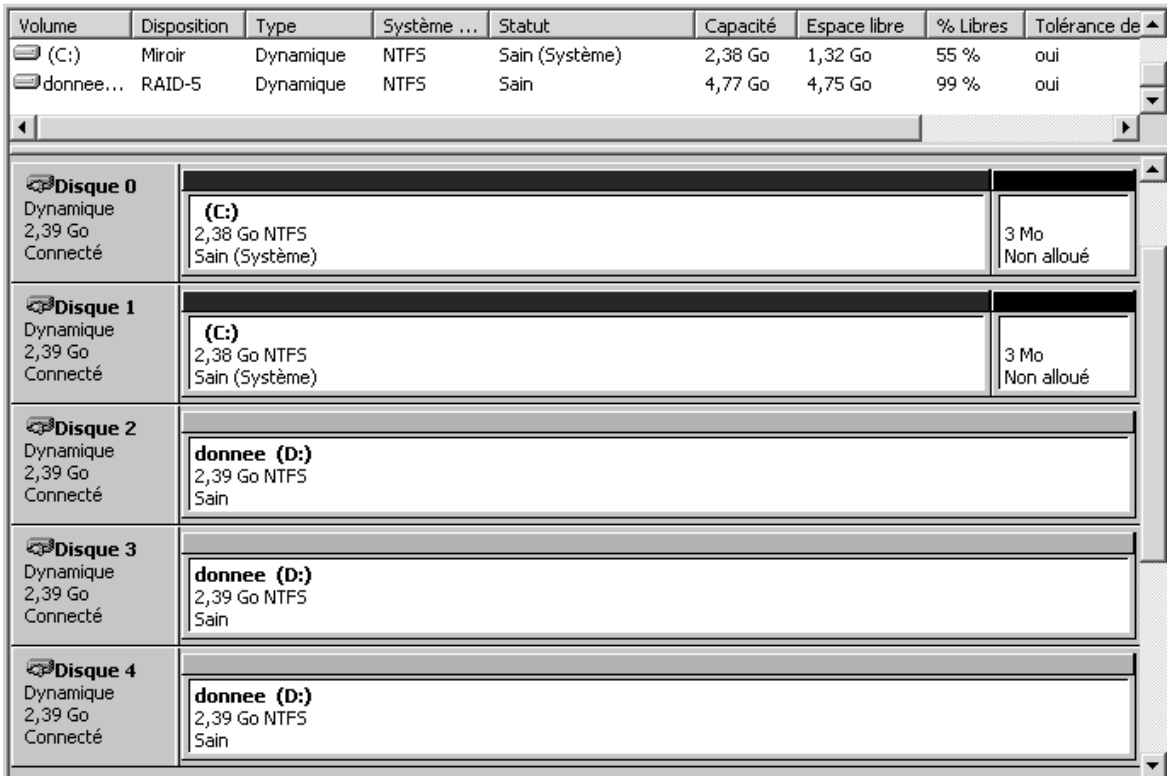


pour obtenir finalement dans le gestionnaire de disque

Volume	Disposition	Type	Système ...	Statut	Capacité	Espace libre	% Libres	Tolérance de
(C:)	Miroir	Dynamique	NTFS	Sain (Système)	2,38 Go	1,32 Go	55 %	oui
donnee...	RAID-5	Dynamique	NTFS	Sain	4,77 Go	4,75 Go	99 %	oui

EXEMPLE :

Aspect d'un système disque ayant 5 disques, 2 en RAID1 (système) et 3 en RAID5 (données)



Suppression d'un RAID5 :

La suppression d'un volume en RAID5 est une opération qui perds les données du volume !

Il est donc nécessaire de copier ailleurs les données que l'on veut garder !

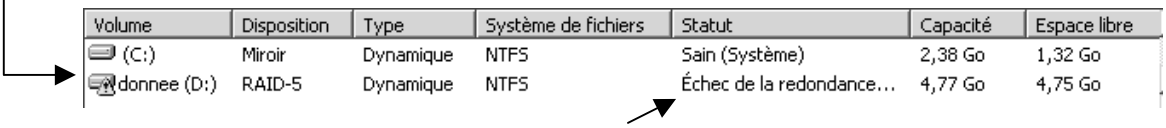
A partir de la on peut faire ce que l'on veut des volumes récupérés !

PANNES VOLUMES EN RAID5

Panne d'un disque :

Soit une solution en RAID5 du type suivant

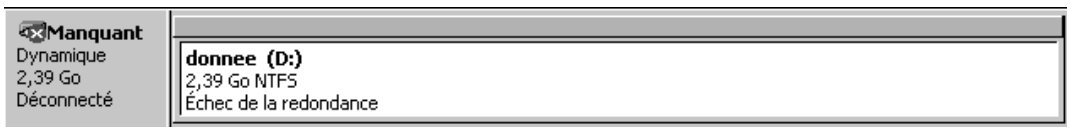
Si un problème survient sur un des disques du RAID5, le système reste utilisable mais affiche un message



Cela signifie que le système n'est plus à tolérance de panne....

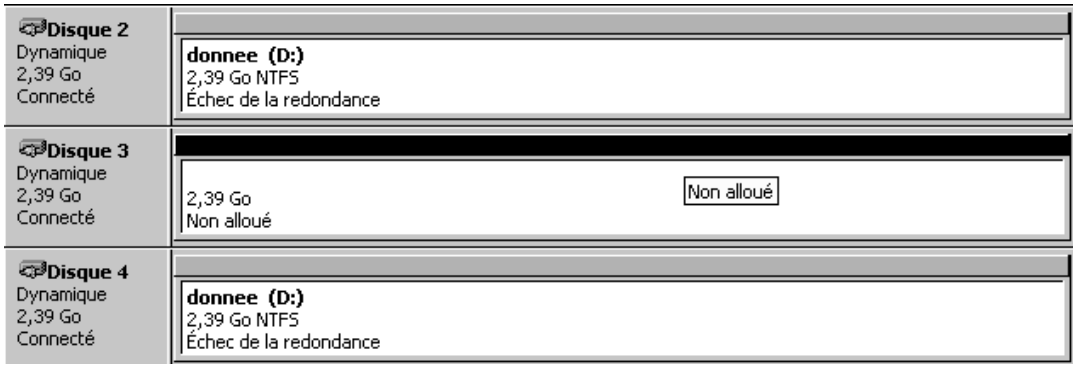
le disque posant problème est celui affichant

Ancien disque détecté comme défaillant ...

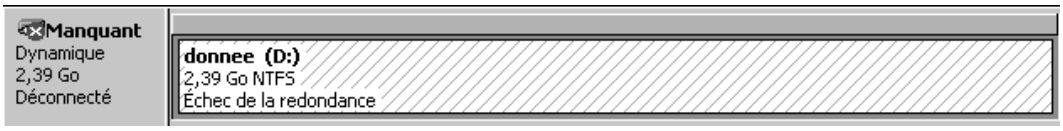


après remplacement physique du disque (ou vérification du disque et demande de reconnexion ayant échouée), on se retrouve avec

N.B: nouveau disque pour remplacer le disque défaillant ...



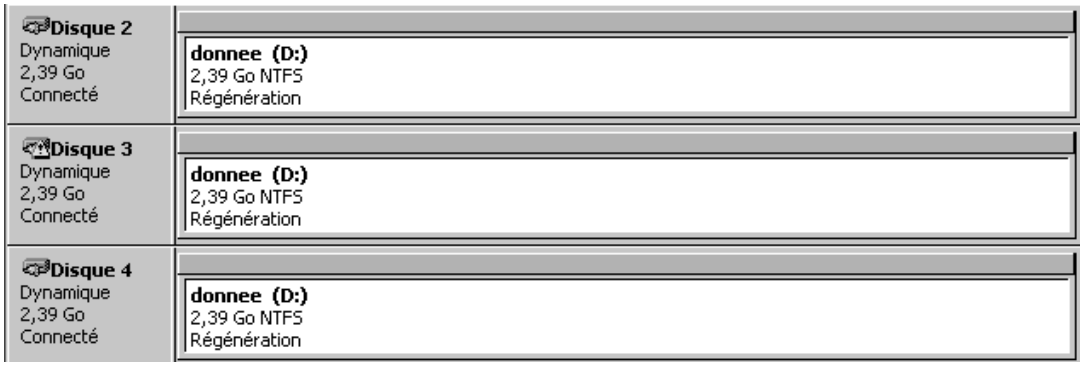
on se place sur le disque posant problème



et on demande clic droit

on choisit le nouveau disque disponible

et automatiquement alors



Panne de plusieurs disques :

Le système n'est plus opérationnel, il faut avoir recours a des sauvegardes...

SYSTEME DFS

DFS ou Systèmes de Fichiers Distribués :

Le service **DFS** donne un point de référence unique et une arborescence logique des ressources disques, et ce quelque soit leur emplacement physique dans le réseau...

Ainsi un utilisateur qui navigue dans une arborescence DFS, n'a pas besoin de connaître les noms des serveurs qui stockent physiquement ces ressources.

Une racine DFS est le niveau le plus élevé de la structure DFS, car elle est le point de départ de la structure arborescente partagée...

Chaque serveur 2000 ne peut héberger qu'une seule racine DFS, mais dans un domaine on peut avoir autant de racine DFS que l'on souhaite...

Il existe des racine **DFS autonomes**, c'est à dire hébergées sur un seul ordinateur, la topologie étant stockée sur cet ordinateur. **DANS CE CAS UN DOMAINE N'EST PAS RECQUIS !**

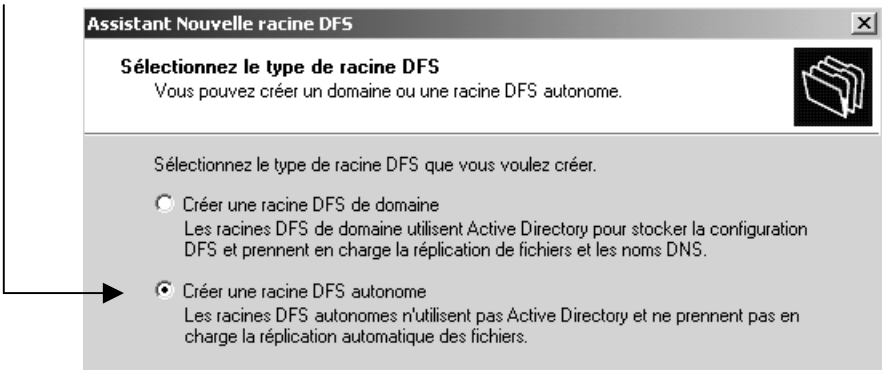
Il existe des racines **DFS de Domaine**, c'est à dire hébergées sur plusieurs serveurs du domaine, la topologie étant stockée dans Active Directory

Création d'une racine DFS autonome :

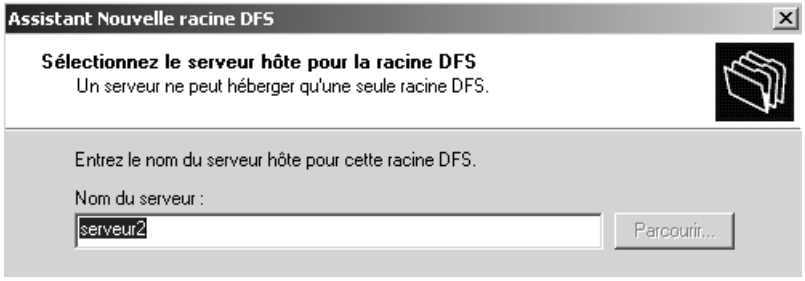
Il faut lancer dans les outils d'administration **Système de fichiers distribués**

Puis on demande avec le menu contextuel, **Nouvelle racine DFS**, ce qui déclenche un assistant...

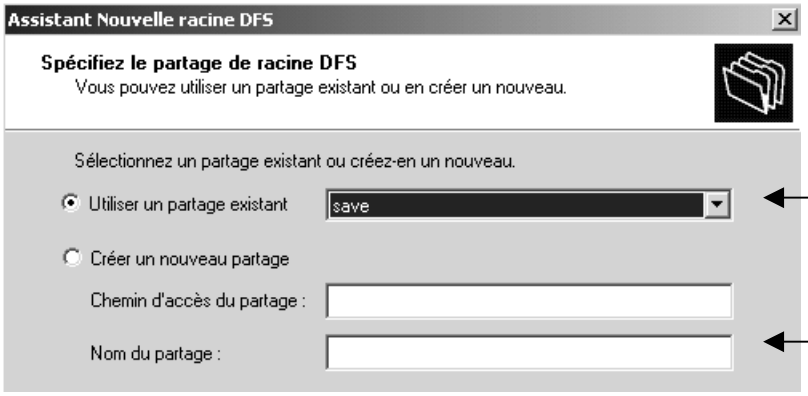
Dans lequel on va demande de créer une racine autonome



Puis il faut indiquer le nom du serveur 2000 sur lequel on veut installer la racine DFS



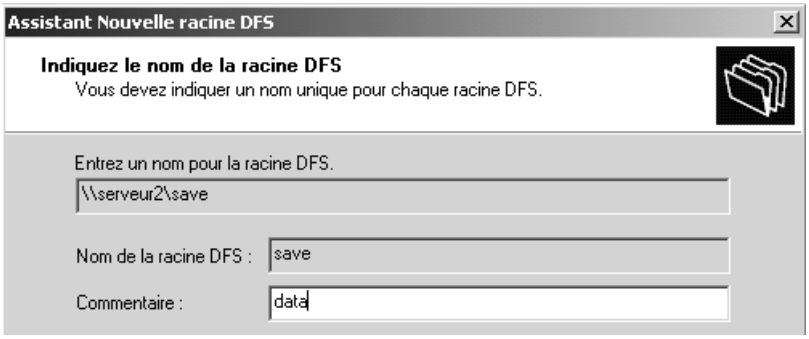
Et indiquer le partage que l'on veut rendre racine DFS



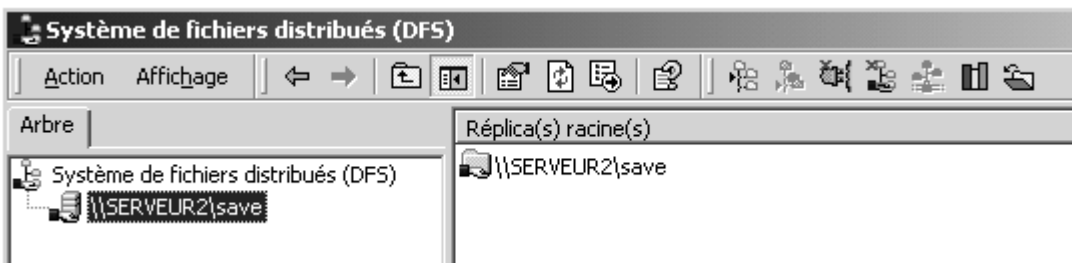
Ici apparaît une liste de tous les partages existants sur ce serveur...

Mais on peut s'en créer un à la volée

Il faut ensuite confirmer le nom de la racine DFS



pour obtenir enfin notre structure :



Ajout d'un lien dans une arborescence DFS autonome :

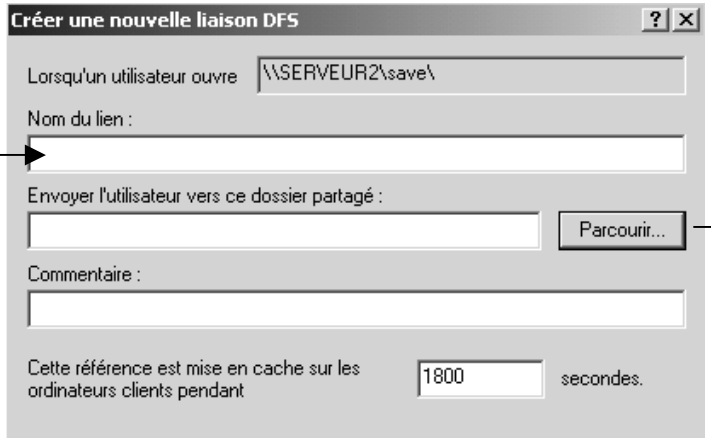
toujours dans les outils d'administration **Système de fichiers distribués**

On se place sur notre racine...

Et on demande par un clic contextuel une **Nouvelle liaison DFS**

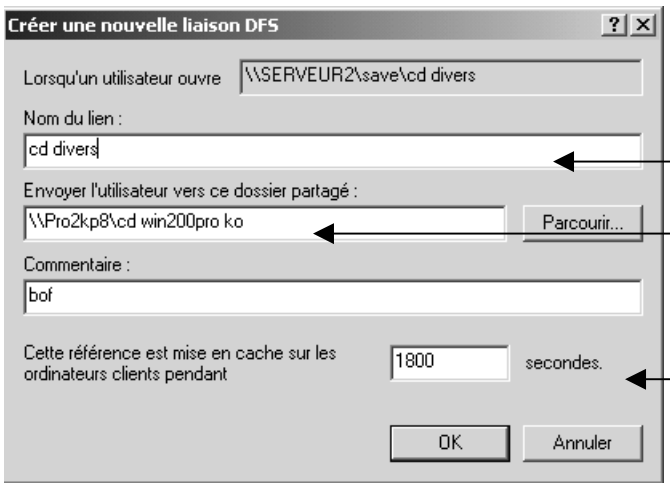
Dans la boite de dialogue qui apparaît

Il va falloir rentrer le **Nom du lien**



Et définir quel dossier partagé correspond

Pour obtenir par exemple

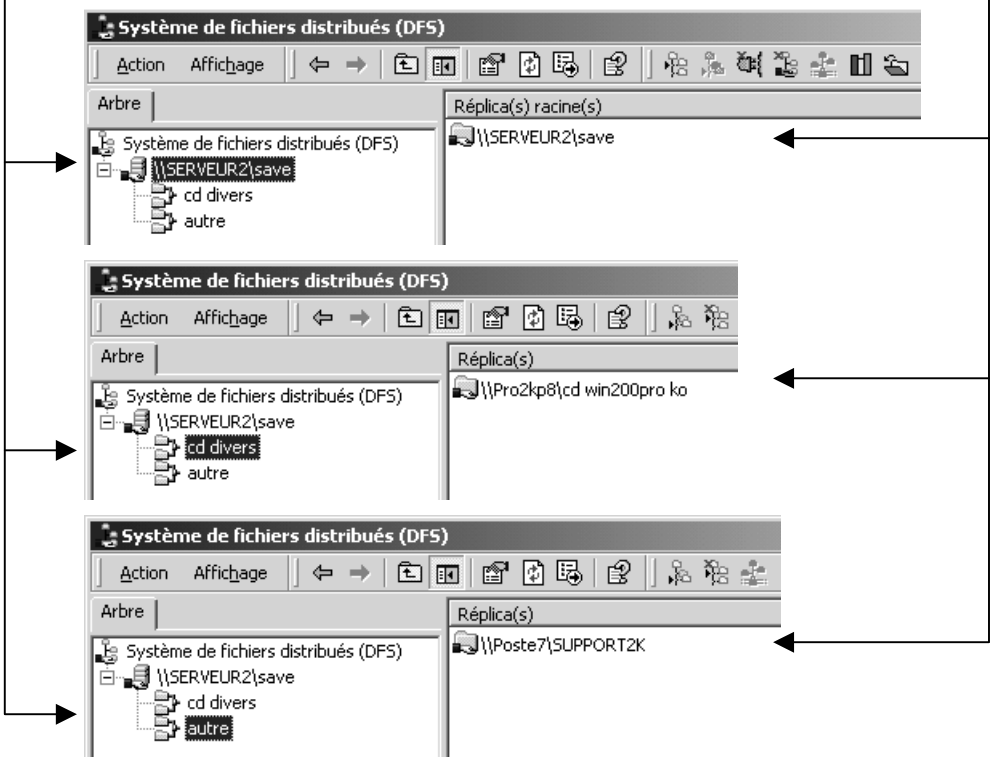


A un **Nom de lien DFS**

Correspond un **dossier partagé** sur n'importe quelle machine du réseau !

Toutes les xx s le client met à jour sa référence

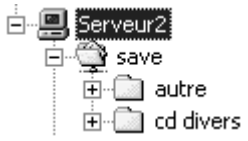
On peut ainsi construire une arborescence logique correspondant a différents emplacement éparpillés absolument dans tout le réseau...



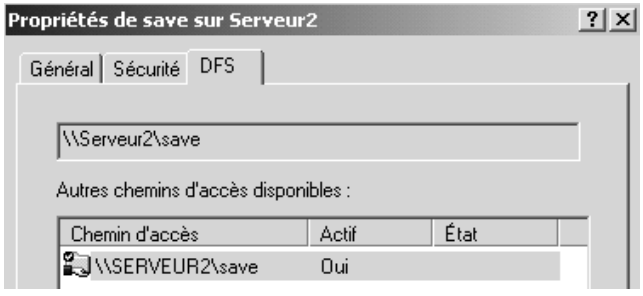
Utilisation d'une arborescence DFS autonome :

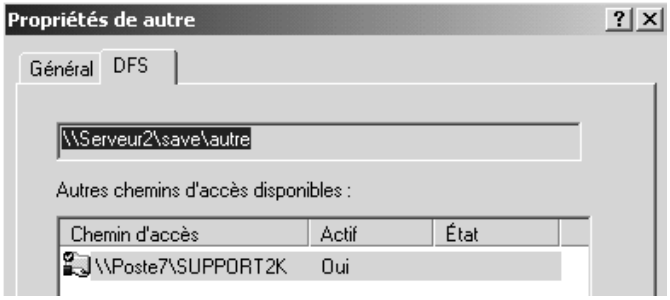
La seule chose que l'utilisateur doivent savoir, c'est où se trouve la racine de l'arborescence DFS, (c'est à dire son nom de partage sur le serveur...)

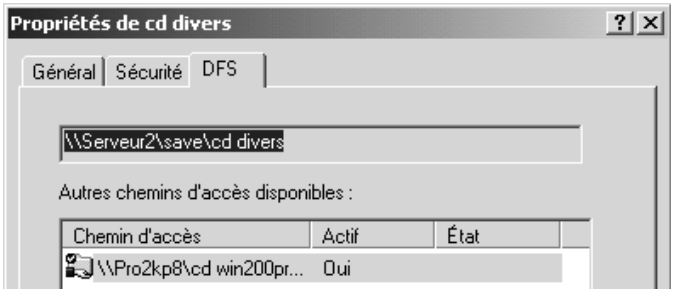
Depuis une machine quelconque 2000 on visualise une arborescence...



par propriété que alors on voit l'emplacement



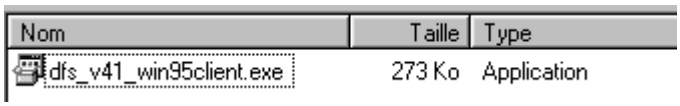




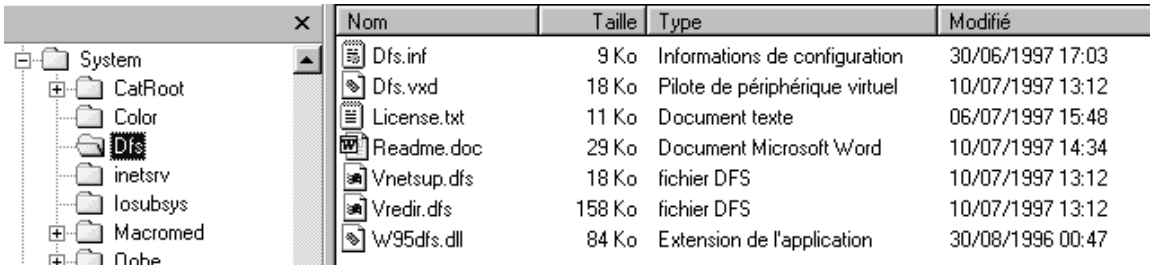
Utilisation de DFS depuis un poste Win95 :

Si les clients DFS sont prévus en standard pour les postes **2000**, Windows **NT4.0** et **Windows98** , il n'en est pas de même pour les clients **windows95**

Il est nécessaire pour ceux-ci d'installer un client DFS spécifique que l'on aura préalablement téléchargé sur le site de microsoft..



ce client s'installe dans un dossier DFS du dossier système de windows95...



Création d'une racine DFS de Domaine :

Cela suppose que l'on ait au minimum la configuration suivante :

- Le serveur racine DFS fasse partie d'un Domaine
- Il ait été installé un **SP2** minimum
- Un patch correctif **Q265365** ait été installé

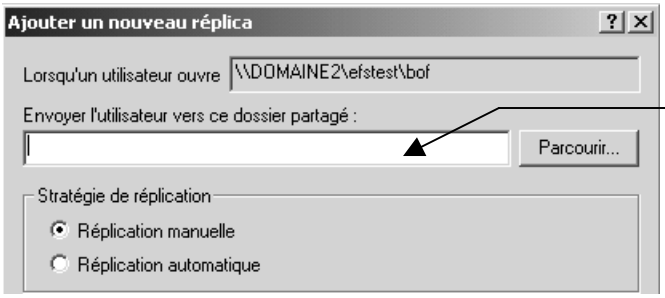
Création de réplica:

Cela suppose que l'on ait au minimum la configuration suivante :

- Il ait été installé un **SP1** minimum

Cela permet de créer une autre instance d'un lien DFS, et pas conséquent cela améliore la notion de DFS en ce qui concerne 2 points : la tolérance de panne et la répartition de charge.

Pour créer un replica on se pose sur le lien DFS et on demande par le clic droit souris **Nouveau réplica**...



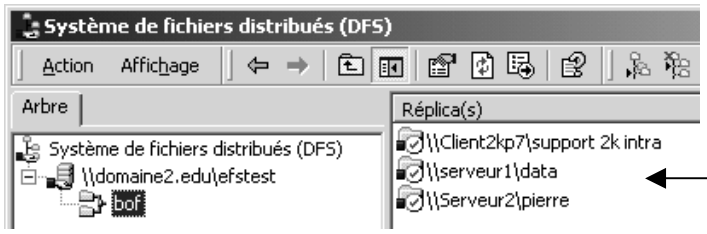
On indique ici le partage sur un autre poste...

Chaque lien DFS peut avoir 32 réplicas...

Il est important que les données soient équivalentes sur tous les réplicas...

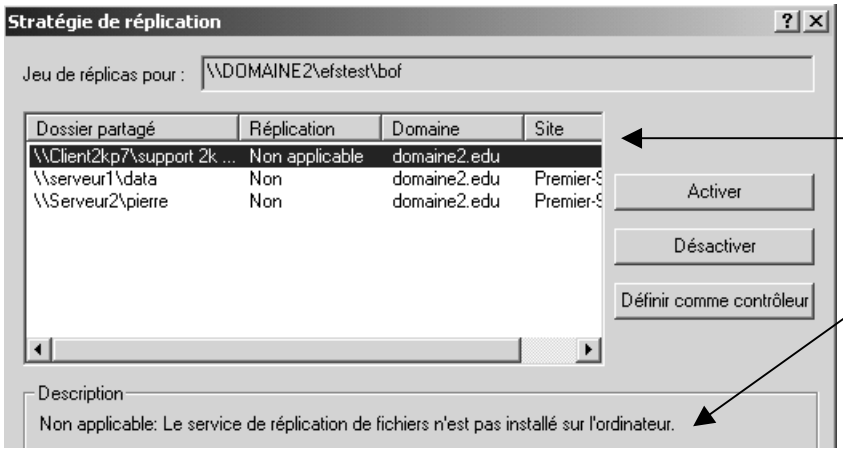
Il existe un mécanisme de réplication que l'on peut mettre en œuvre, mais uniquement si les réplicas sont sur des **serveurs 2000** et dans **1 domaine**.

Soit un lien DFS ici avec 3 réplicas



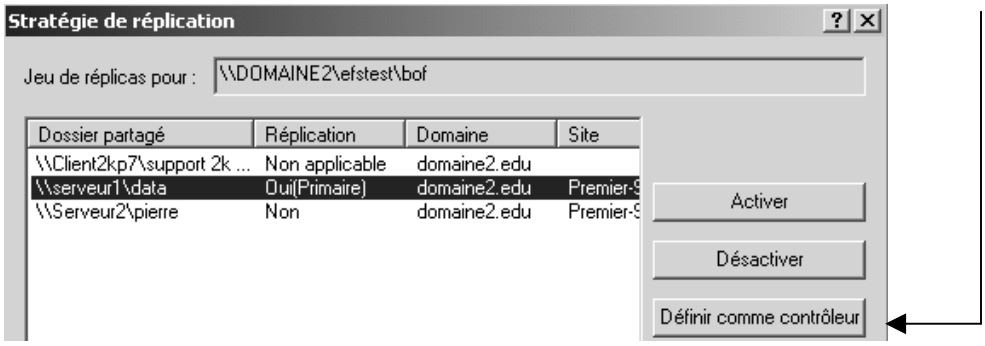
2 réplicas sur serveur et 1 réplica sur un client 2000

en se plaçant sur le lien DFS, on demande par le clic droit **Stratégies de réplication**

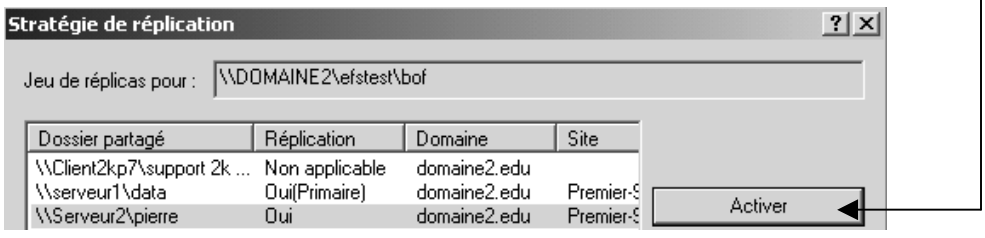


On ne peut pas faire de stratégie de réplication si le poste n'est pas un serveur 2000

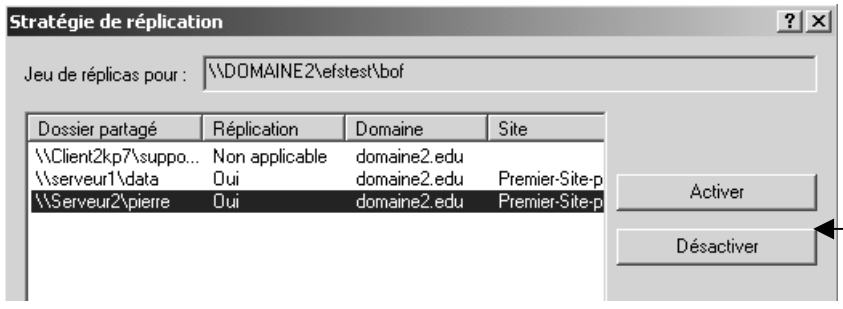
Il va falloir décider qui est contrôleur de la duplication (pour le 1° échange)



puis qui participe à la duplication



pour obtenir enfin



Il n'y a plus de notion de **contrôleur**., toute modification est reportée sur les 2 réplicas

ADMINISTRATION A DISTANCE

Principe de base :

Normalement, sous 2000 2003 Serveur, l'administration du serveur ne peut se faire que depuis une session locale sur le serveur.

On peut cependant administrer à distance un serveur depuis n'importe quel client 2000 (pour Serveur 2000) et uniquement depuis un XP SP2 pour un serveur 2003, et ce de deux manière principales :

- on a installé les outils d'administration sur le client 2000-XP
- on ouvre une session avec terminal service sur le serveur depuis n'importe quel client 2000

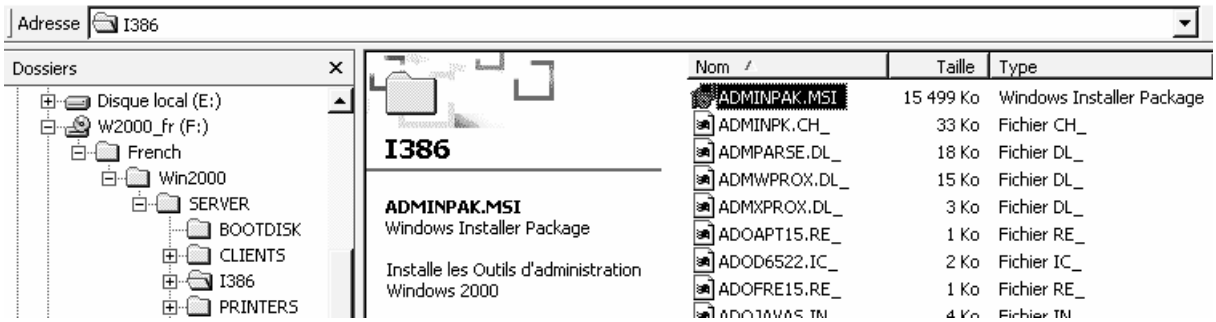
La première méthode n'offre pas la totalité de l'administration du serveur, mais elle permet de cibler les machines utilisables.

La deuxième méthode ouvre la totalité de l'administration du serveur (puisque l'on ouvre une session a distance **sur le serveur**...) mais elle est plus délicate a mettre en œuvre !

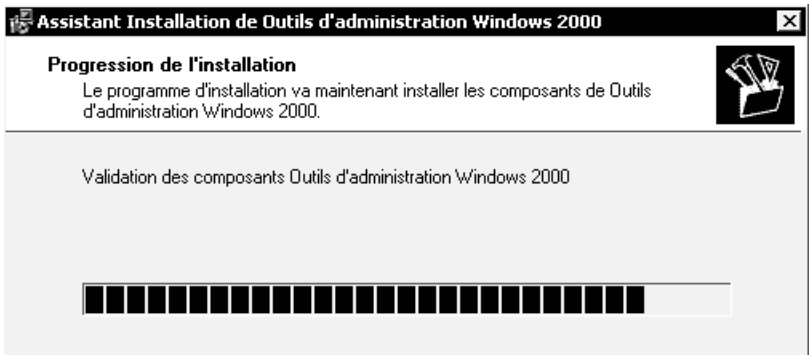
Installer les outils depuis le CD serveur 2000 :

le fichier permettant l'installation des outils d'Administration, est stocké dans le CD de distribution 2000 serveur, dans le dossier i386...

c'est le fichier **Adminpak.msi**



l'exécution de ce fichier déclenche un assistant



une nouvelle entrée apparaît dans le menu programme...

dans laquelle il sera facile de retrouver ce que l'on cherche....

Installer les outils depuis le serveur :

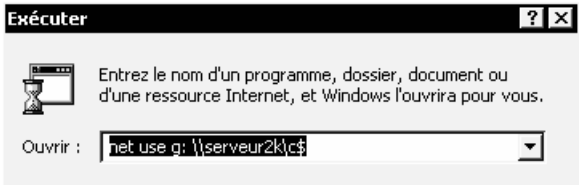
Si on n'a pas un CD 2000 server sous la main, il faut savoir que dans le dossier système du serveur c'est à dire en standard dans **Winnt/system32** le fichier **Adminpak.msi** est également stocké...

le problème c'est que en général, on ne partage pas la racine du disque de NT....

mais si on se rappelle que tous les disques sont partagés de manière administrative en C$ ou en D$, il suffit alors de faire une petite commande du type :

net use x: \\serveur2k\c$

dans exécuter par exemple :



pour se créer un lecteur x: pointant vers le disque système de notre serveur...

dans lequel on accède physiquement au disque du serveur

il suffit ensuite d'aller dans le dossier **Winnt\system32**

Installer le Package AdminPAck pour serveur 2003 :

le fichier permettant l'installation des outils d'Administration sur un poste XP SP2, est assez volumineux.

L'installation se passe sans commentaires

Mais si on a bien du coup les outils d'administration de notre serveur sur le poste XP

, il y a parfois quelques petits soucis...

Il faut consulter l'article **KB304718** de la bas Microsoft si on a des soucis avec l'administration a distance.

MISE A NIVEAU D'UN DOMAINE NT4 EN NT2000

Planification de l'ordre dans lequel les serveurs sont mis à niveau

Lors de la planification de l'ordre dans lequel les serveurs d'un domaine doivent être mis à niveau, vous avez le choix entre deux approches différentes :

- commencer par mettre à niveau les contrôleurs de domaine
- commencer par mettre à niveau les serveurs membres.

Vous pouvez mélanger ces deux approches. Toutefois, lorsque vous commencez la mise à niveau des contrôleurs de domaine, vous devez effectuer celle du contrôleur principal de domaine en premier.

Si vous commencez par la mise à niveau des serveurs membres (sans mettre à niveau les contrôleurs de domaine), un certain nombre de fonctionnalités qui ne nécessitent pas Active Directory deviennent disponibles. Les fonctionnalités Active Directory deviennent disponibles que si vous commencez la mise à niveau des contrôleurs de domaine.

Ordre de mise à niveau des serveurs	Avantages	Inconvénients
Contrôleurs de domaine d'abord (vous devez commencer par le contrôleur principal de domaine	Fournit toutes les fonctionnalités Active Directory, ainsi que les autres fonctionnalités de Windows 2000 Server (voir la liste ci-dessous)	Nécessite l'organisation des structures Active Directory au moment de la mise à niveau. Dans un domaine de petite taille (de 2 à 5 serveurs), cette organisation ne demande pas beaucoup de temps
Serveurs membres d'abord	Fournit une prise en charge des protocoles et d'autres fonctionnalités (voir la liste plus loin dans cette section) que vous ayez effectué ou non la mise à niveau des contrôleurs de domaine et l'organisation des structures Active Directory	Ne fournit pas les fonctionnalités Active Directory.

Rappel des mises à niveau possibles :

Lors de la planification de l'ordre dans lequel les serveurs d'un domaine doivent être mis à niveau, vous avez le choix entre deux approches différentes :

Windows 9x	➔	Windows 2000 Professionnel
Windows NT4/3.51 Workstation	➔	Windows 2000 Professionnel ou Windows 2000 Server
Windows NT4/3.51 Server	➔	Windows 2000 Server ou Windows 2000 Advanced Server
Windows NT4 Entreprise Edition	➔	Windows 2000 Advanced Server

La mise à jour depuis Windows 3.x, Windows NT Workstation 3.5 et Back Office Small Business Server 4.5 n'est pas supportée.

Fonctionnalités avec la mise à niveau des contrôleurs de domaine

Lorsque les contrôleurs de domaine sont mis à niveau et commencent à communiquer sur un réseau, toutes les fonctionnalités de Windows 2000 Server deviennent disponibles par l'intermédiaire de ces serveurs.

- Stratégie de groupe, que vous pouvez utiliser pour définir des stratégies qui s'appliquent à un site, un domaine ou une unité organisationnelle donnés dans Active Directory.
- Utilisation des normes Internet, dont l'accès via le protocole LDAP et un espace de noms basé sur le service DNS (Domain Name System).
- Interfaces du service Active Directory (ADSI, Active Directory Service Interfaces), puissant environnement de développement.

Fonctionnalités avec la mise à niveau d'un serveur quelconque

- Outils de gestion : Console MMC (Microsoft Management Console) Plug-and-Play Gestionnaire de périphériques Assistant Ajout/Suppression de matériel (dans le Panneau de configuration)
- Prise en charge des systèmes de fichiers : La dernière version du système de fichiers NTFS assure la prise en charge des quotas de disque, de la défragmentation des structures d'annuaire et des E/S réseau compressées.
- Services d'applications : Modèle de pilote Win32, DirectX 5.0 et Windows Script Host.
- Sécurité : Système de fichiers de cryptage

Sauvegardes et autres préparations

Il est conseillé de sauvegarder chaque serveur avant de le mettre à niveau.

En outre, pour préserver l'intégrité de votre réseau existant, vous pouvez supprimer temporairement un contrôleur secondaire de domaine de votre réseau. Pour cela, sur votre réseau Windows NT existant, choisissez un contrôleur secondaire de domaine, assurez-vous qu'il contient une copie à jour de la base de données de comptes d'utilisateurs et sauvegardez-le. Ensuite, déconnectez son câble réseau. Après avoir mis à niveau votre contrôleur principal de domaine vers Windows 2000 (vous devez mettre à niveau le contrôleur principal de domaine en premier), ce système déconnecté peut devenir contrôleur principal de domaine Windows NT, si nécessaire.

N.B : Si la mise à niveau se déroule normalement, vous ne pouvez pas transformer le contrôleur secondaire de domaine Windows NT en contrôleur principal de domaine. Dans ce cas, vous terminez le processus de mise à niveau, puis vous reconnectez le serveur déconnecté pour le mettre à niveau à son tour.

Mise à niveau du CPD

Lors de la migration du PDC vers Windows 2000, l'Active Directory va être rempli avec le contenu de l'ancienne base SAM de Windows NT. Le serveur est alors en mode mixte (il supporte des BDC NT4

Une fois le contrôleur principal de domaine transformé en contrôleur de domaine Windows 2000, celui-ci est entièrement compatible avec les versions antérieures. Il **émule un contrôleur principal de domaine Windows NT 4.0** pour les autres serveurs et clients.). Ainsi la réplication a encore lieu. L'ajout de BDC (NT4) est toujours possible. Si le serveur Windows 2000 tombe, la promotion d'un BDC est aussi possible. Enfin les SIDs sont conservés.

Nouveau serveur CD 2000 remplaçant l'ancien CPD NT4

On ne peut plus migrer notre serveur NT, donc il faut effectuer la manipulation suivante :

1. Installer le nouveau serveur en CSD NT4
2. Le promouvoir CPD de Domaine
3. Le migrer en CD 2000

Mise à niveau des CSD

Deux options sont possibles : en faire des **DC** ou des **serveurs membres**. On peut, sous 2000, changer le rôle d'un serveur sans réinstallation. Avec l'utilitaire **dcpromo** il est possible de faire d'un DC un serveur membre et d'un serveur membre un DC du même domaine ou d'un nouveau domaine de la forêt.

N.B : On ne peut pas, par contre, transformer un DC d'un domaine en un DC d'un autre domaine, il faut passer par l'étape serveur membre.

Pour installer Windows 2000 sur un CSD si le CPD ne peut pas être migré : le débrancher du réseau, le promouvoir en CPD, le migrer vers Windows 2000 en DC puis exécuter dcpromo pour le rétrograder en serveur membre. Après avoir mis à niveau votre contrôleur principal de domaine et vous être assuré qu'il fonctionne comme vous le souhaitez, mettez à niveau vos contrôleurs secondaires de domaine un par un.

Mose mixte ou Natif

Après avoir mis à niveau tous les contrôleurs de domaine vers Windows 2000, vous pouvez passer votre domaine du mode mixte (avec lequel le domaine peut comporter des contrôleurs de domaine Windows NT) au mode natif (avec lequel le domaine ne peut comporter que des contrôleurs de domaine Windows 2000). Cette décision est importante **car vous ne pouvez pas revenir en mode mixte après être passé en mode natif**.

Les raisons de rester en mode mixte

Si certains des BDCs sont encore sous Windows NT4, si certaines des applications installées sur un PDC ou un BDC ne supportent pas Windows 2000 ou si l'on souhaite pouvoir revenir à l'état antérieur, il faut rester en mode mixte. Le passage en mode natif est irréversible.

Le basculement en mode natif

Une fois cette manipulation effectuée, deux nouveaux types de groupe sont disponibles : les groupes universels et les groupes locaux à un domaine. La limite de taille de la base SAM est supprimée (le nombre de compte est alors théoriquement illimité). L'imbrication de groupes devient possible. La réplication est désormais de type multi maître entre les DC (domain contrôlers) de l'AD.

Cela se demande depuis la mmc **Domaines et approbations Active Directory** dans les propriétés du domaine