Centre **U**niversitaire d'**É**ducation et de **F**ormation des **A**dultes

Centre Régional de CNAM

WINDOWS NT 2000:
Prise en Charge - Administration

S4-Cours

Michel Cabaré

Juin 2003 ver 1.4

CUEFA - Département Formation Continue

BP 68

38402 ST MARTIN D'HÈRES

Objectif de ce support

La formation que vous suivez, à pour but de vous perfectionner avec le logiciel Microsoft Windows NT 2000 (version 5.0) sur environnement P.C.

Ce Support a pour but de vous fournir un certain nombre d'éléments concernant soit des manipulations de touches ou de souris, soit des notions théoriques concernant la gestion de réseaux locaux à l'aide de 2000

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

M i c h e l C a b a r é

TABLE DES MATIÈRES

ACTIVE DIRECTORY

Qu'est-ce un service d'annuaire ?:

Un service d'annuaire peut être comparé à un agenda téléphonique, celui-ci contient au départ des noms et des n° de téléphone, puis au fur et à mesure il peut s'enrichir d'autres éléments, comme des adresses postales ou Email...

On va définir un service d'annuaire tel que celui existant sous NT2000 et portant le nom d'**Active Directory** par ses fonctions :

- Un annuaire offre le moyen de **stocker des informations** sur les ressources du réseau afin de simplifier la recherche de ces informations. C'est un peu comme une base de registre globale à tout le réseau.
- Un annuaire offre le moyen de **gérer ces ressources** par l'intégration de tous les service nécessaires
- Un service d'annuaire agit comme un tableau de bords principal du système d'exploitation réseau, **il est distribué ou répliqué sur tous les ordinateurs** qui participent à la gestion du domaine de manière à en augmenter la fiabilité. Active directory n'utilise d'ailleurs que des contrôleurs de domaine homologues, les modifications effectuées par un administrateur sur un contrôleur sont immédiatement répercutées sur tous les autres contrôleurs
- Un annuaire étant amené à collecter/gérer des informations sur des machines différentes doit répondre à certaines normes. Les service **Actives Directory** utilisent le protocole **LDAP** (Lightweight Directory Acces protocol) normalisé . Active Directory localise les ressources grâce au protocole **DNS** (Domain Name System) et donc nécessite TCP/IP impérativement
- Active Directory est extensible, car on ne peut pas forcément tout prévoir dès le début !

Active Directory gère ses ressources de manière interne par un protocole particulier **X500** mais un peu "modifié" par Microsoft.

Ce qui fait que si AD est capable de trouver des ressources sur **tout système à la norme LDAP**, et si AD est interrogeable par tout **client LDAP**, on ne pourra **pas répliquer la structure AD de windows 2000 sur un autre système que Windows 2000**.

La structure Logique d'Active Directory dans un Domaine:

Domaine

Un **Domaine** est défini par une **limite de sécurité** unique dans le cadre d'un réseau informatique tournant sous Windows NT ou Windows 2000.

Sur un poste de travail isolé, le domaine est l'ordinateur lui-même.

Un domaine constitue une **Unité de duplication**, dans le cas ou plusieurs contrôleur de domaines sont présents. Dans ce cas, chaque contrôleur de domaine contient un réplica de l'annuaire Active Directory.

Dans un Domaine, tous les éléments qui en font partie ont une appelation commune, basée sur le **nom de Domaine**.

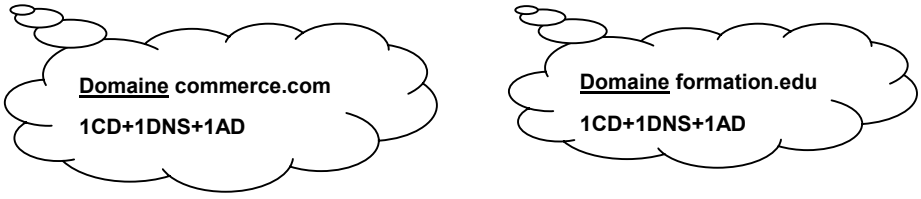
Annuaire & Espace de noms

Active Directory est essentiellement un espace de noms, comme c'est le cas de tout service d'annuaire. La **résolution de nom** consiste à passer d'un nom à l'objet ou l'information que ce nom représente. Un annuaire téléphonique constitue un espace de noms dans lequel les noms des abonnés peuvent être résolus en numéros de téléphone.

Active Directory constitue un **espace de noms** dans lequel le nom d'un objet de l'annuaire peut être résolu pour obtenir l'objet lui-même.

Active Directory & DNS

Puisqu'un annuaire c'est un espace de nom, Active Directory nécessite un serveur DNS par Domaine. Dans le cas ou on souhaite créer deux Domaines indépendant, il suffit d'avoir à disposition pour chaque domaine d'un serveur DNS gérant cet espace de nom...



N.B: Il ne faut pas confondre le problème de plusieurs domaines, avec la problématique de plusieurs Contrôleurs pour le même Domaine...

Contrôleur de schéma

Puisque Active directory est un annuaire, la structure de la base de donnée contenant cet annuaire doit être physiquement gérée en un endroit, portant le nom de **contrôleur de schéma**. Ce contrôleur est le seul à pouvoir modifier la structure de la base de AD, Il en faut un, toujours un mais rien qu'un (jamais deux...)

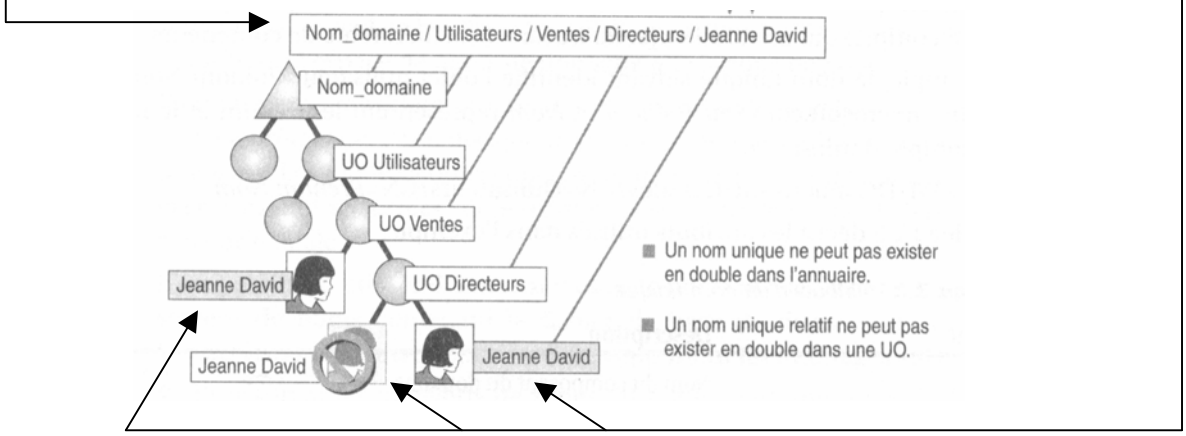
Nom

Chaque objet dans Active Directory est identifié par un nom correspondant à un chemin LDAP. Il y a deux sortes de noms différents.

Nom unique (**DN – Distinguished Name**). Le nom unique identifie le domaine qui contient l'objet, ainsi que le chemin d'accès complet permettant d'accéder à l'objet à travers la hiérarchie des conteneurs. Voici un exemple typique de nom unique :

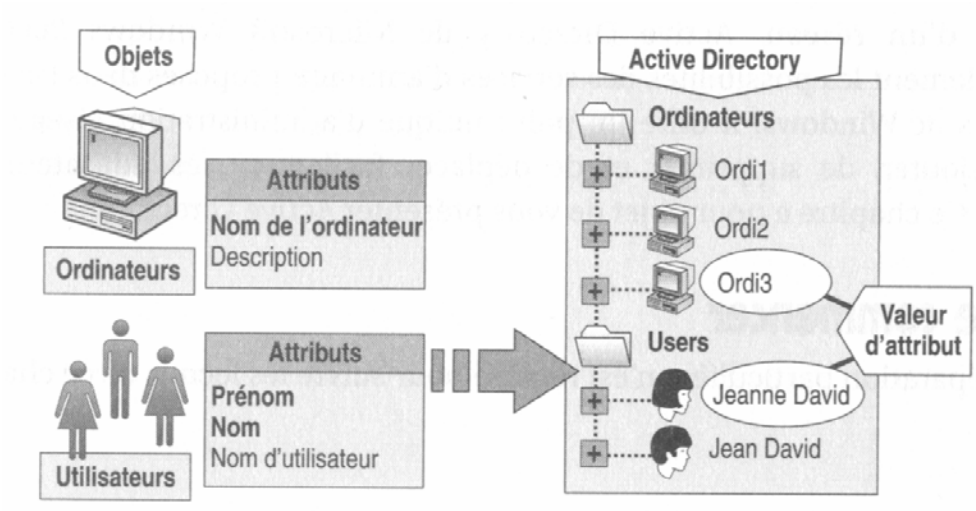
DC=Nom_Domaine//**OU**=Utilisateurs /**OU**=Ventes/**CN**=Jeanne David

Le nom relatif distinct (**RDN – Relative Distinguished Name**) d'un objet est la partie du nom qui constitue un attribut de l'objet à proprement parler. Dans l'exemple précédent, le nom relatif distinct de l'objet utilisateur est **CN**=Jeanne David. Le nom relatif distinct de l'objet parent est **OU**=Ventes.



Objet

Les **Objets** dans Active Directory peuvent être les données utilisateurs, les imprimantes, les serveurs, les bases de donnée, les groupes, les ordinateurs, les stratégies de sécurité. Un **Objet** est donc un ensemble d'attributs nommé et circonscrit qui représente un élément concret



Par rapport à la liste prévue initialement, il est possible de rajouter des objets supplémentaires. Certaines applications procèdent de cette manière lorsqu'elles s'installent…

Conteneur UO

certains objets, contenant d'autres objets, sont appelés **Conteneurs** ou **UO Unité Organisationelle** dans le langage Active Directory . Un conteneur est semblable à un objet dans la mesure où il possède des attributs et fait partie de l'espace de noms de Active Directory. Toutefois, contrairement à un objet, il ne représente rien de concret. Ce n'est qu'un réceptacle pour un ensemble d'objets et/ou pour d'autres conteneurs.

On pourra définir qui en est le responsable en octroyant des permissions supplémentaires par rapport à celles définies par défaut, c'et ce que l'on appelle de la **délégation de permission**

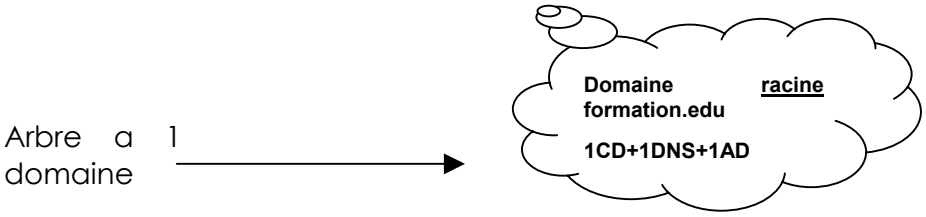
Une **OU** est une unité d'administration sur laquelle on notamment pourra appliquer des **stratégies de groupe**

La Structure Logique au sein de plusieurs Domaines:

Arbres-arborescence de domaines

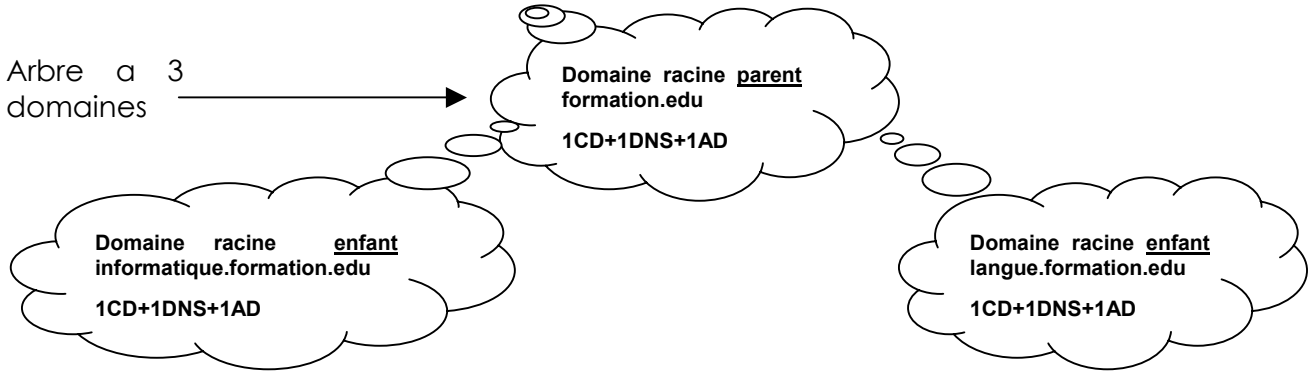
Un **domaine** seul, crée un **Arbre de domaine** (cet arbre est petit, sans branches, on peut dire que l'on a que la racine de l'arbre… mais …c'est un arbre quand même).

Autrement dit un domaine fait toujours partie d'un arbre, et si c'est le premier domaine que l'on crée, il sera défini comme le **domaine racine de la forêt**.



Un arbre, ou arborescence de domaine, c'est un ensemble de domaine hierarchisés.

Si on ajoute un domaine à un arbre, le nouveau domaine est un **domaine enfant**, il a une relation d'approbation transitive bidirectionelle avec son parent. Sont nom est hiérarchiquement lié au nom du domaine parent **enfant.parent.com** (le tronc se voit doté d'une branche…)

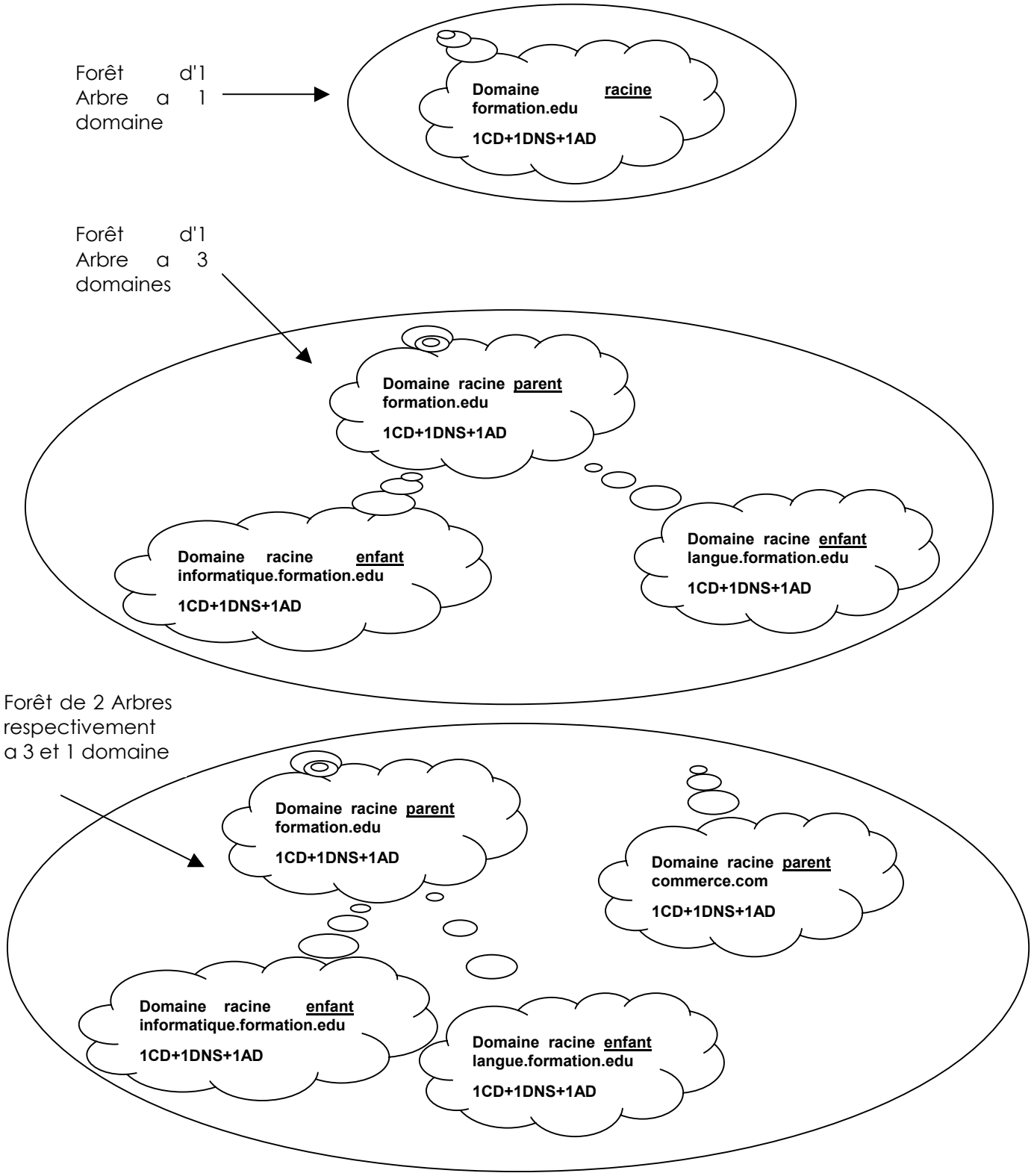


Une arborescence constitue un **espace de noms** hierarchisé et continu. Les serveurs DNS du (des) domaines enfants reprends le nom du serveur DNS de plus haut niveau (du parent)

Les relations d'approbation sont bidirectionelles et transitives. Dans un **arbre de domaine** ils partagent un même **schéma**, et un même **catalogue global**.

Forêts

Un **arbre** ne peut exister sans forêt, même s'il est seul. Donc un **arbre de domaine** seul crée une **forêt** (même s'il y a un seule arborescence …)



Une forêt permet d'établir des communications entre les arbres. Une forêt ne constitue pas un **espace de noms** hierarchisé et continu. Les serveurs DNS des arbres de la forêt sont indépendants

Les relations d'approbation sont bidirectionelles et transitives Lorsque plusieurs arbres de domaines sont interconnectés pour former une forêt. les

arbres de domaine de la forêt partagent un même **schéma**, et un même **catalogue global de AD**.

Catalogue Global

Le **catalogue global** c'est une liste de définition de tous les noms existant dans l'annuaire d'un domaine, afin d'éviter l'attribution d'un nom en "doublons". Le **Catalogue Global** permet de trouver tout objet dans Active Directory, et ce au travers du domaine, de l'arbre ou de la forêt… selon l'importance. Sans **Catalogue Global** une recherche s'effectuerait sur chaque domaine de la forêt

Le premier serveur devenant Contrôleur de Domaine devient serveur de catalogue global. Ce catalogue global peut etre répliqué sur tous les contrôleur de Domaine…. En théorie toutes les modifications sont possibles à n'importe quel moment depuis tout CD, le "dernier qui cause à raison". Dans la pratique, cette théorie du dernier qui cause est gérée par un n° **USN** (**update Sequence Number**) qui est incrémenté automatiquement par le CD au moment de la modification. Le n° le plus élevé remporte….

Relations d'approbation

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)

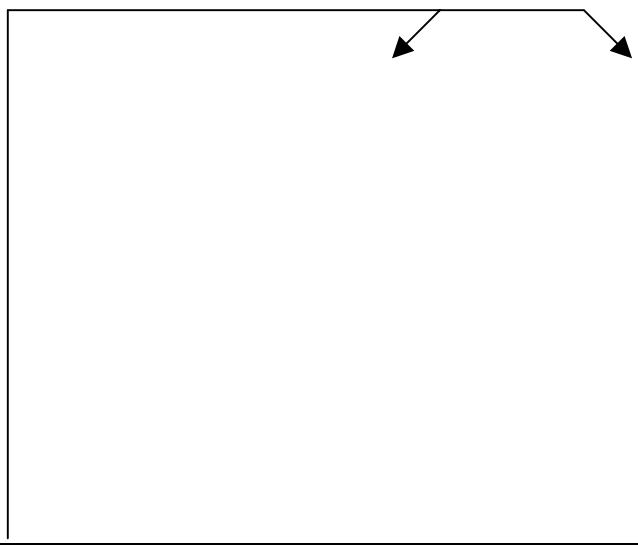
Elles peuvent être **bi-directionelles** , c'est à dire que 2 chemins d'approbation vont dans les 2 direction entre 2 domaines (Si A approuve B, alors B approuve A)

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…)

La structure Physique d'Active Directory:

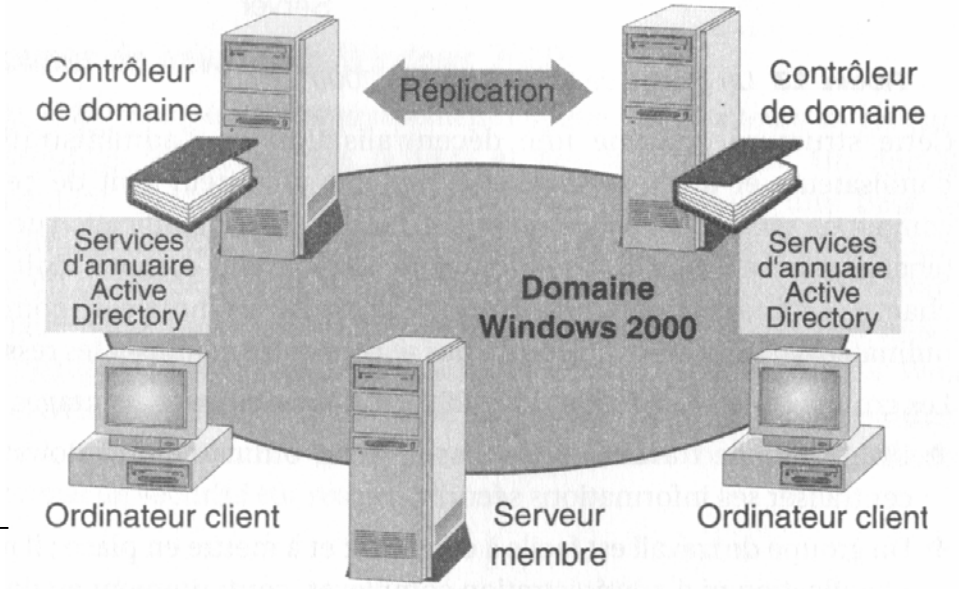
Contrôleur de Domaine

Dans un réseau avec domaine, c'est à dire constitué avec un ou plusieurs serveur NT2000 faisant office de contrôleur de domaine



On peut trouver toute sorte de machine, (y compris des postes NT4.0 et windows95-98 non représentés ici)

la sécurité est gérée sur le (les) contrôleurs du réseau uniquement



Avec Windows 2000, un **serveur** NT peut avoir l'un des trois rôles suivants vis-à-vis du domaine :

- **Les contrôleurs de domaine** contiennent les copies des comptes d'utilisateurs et d'autres données Active Directory pour un domaine donné : N.B : **Il en faut au moins 1 pour parler de Domaine NT 2000, il peut y en avoir plusieurs, ils sont alors tous homologues**
- Les **serveurs membres** appartiennent à un domaine, mais ne contiennent pas de copie des données Active Directory.
- Les **serveurs autonomes** appartiennent à un groupe de travail plutôt qu'à un domaine.

Sites

Un **site** est un emplacement d'un réseau qui contient des serveurs Active Directory. Un site est défini comme un ou plusieurs sous-réseaux TCP/IP "bien connectés". "(connectivité du réseau est extrêmement fiable et rapide vitesses de réseau local égales ou supérieures à 10 millions de bits par seconde).

Définir des sites permet de configurer l'accès à Active Directory et la manière dont la réplication va se faire entre les contrôleur de domaine.

Un site contient au minimum un contrôleur de Domaine.

Lorsqu'un utilisateur ouvre une session, le client Active Directory recherche les serveurs Active Directory qui font **partie du même site que l'utilisateur**. La détermination du site local à l'ouverture de session se fait facilement parce que le poste de travail de l'utilisateur sait déjà à quel sous-réseau TCP/IP il appartient et que les adresses de sous-réseaux se traduisent directement en adresses de sites Active Directory.

N.B: il est conseillé de penser son réseau en Domaine, et de gérer ensuite les problèmes de géographie physique par la notion de site, que de faire autant de domaines que de sites géographiques.

Lorsque l'on fait plusieurs domaines, c'est plutôt que les modèles d'administration et de sécurité diffèrent entre les domaines…

ASSISTANT ACTIVE DIRECTORY & DOMAINE

Promotion-Rétrogradation d'un serveur NT 2000:

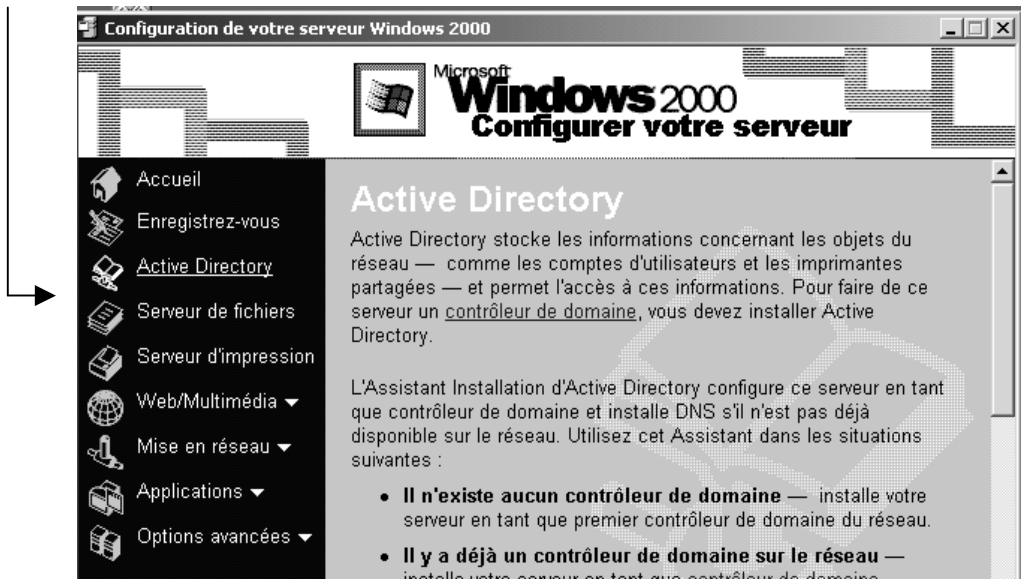
Pour créer un domaine, vous devez **promouvoir** un ou plusieurs ordinateurs exécutant **Windows 2000 Server** afin qu'ils deviennent un ou des contrôleurs de domaine.

L'Assistant Installation de **Active Directory** installe et configure les composants qui fournissent le service d'annuaire Active Directory aux utilisateurs et aux ordinateurs du réseau.

Pour "gérer" un serveur NT2000 au niveau de sa position en tant que contrôleur de domaine

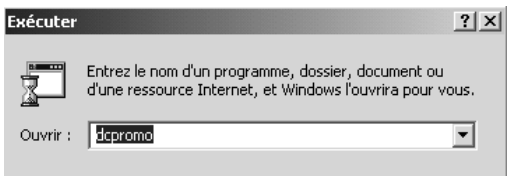
Démarrer/Programmes/Outils d'administration/Configurer votre serveur.

Cliquez sur **Active Directory**, puis lancez l'assistant



Ou bien

Démarrer/Exécuter et tapez ensuite **dcpromo**.



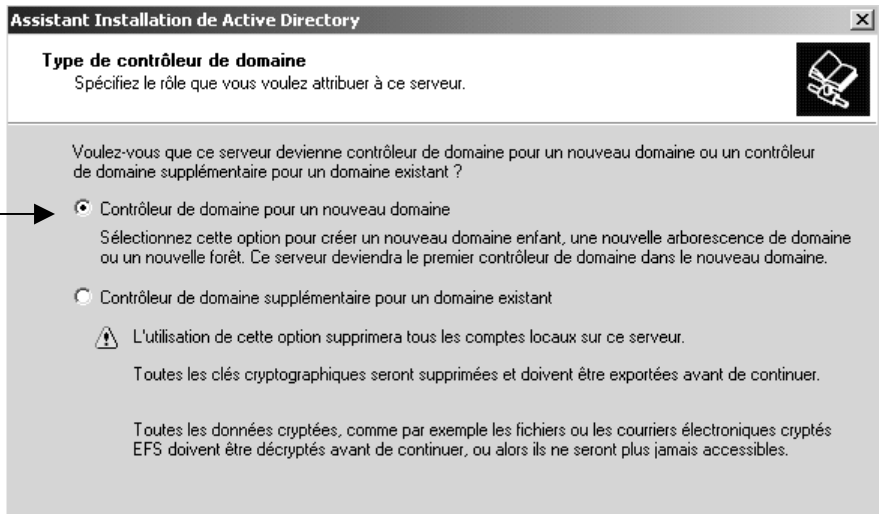
N.B: on doit disposer de privilèges d'administration suffisants pour créer- modifier un contrôleur de domaine.

N.B: Une connexion réseau active doit exister !

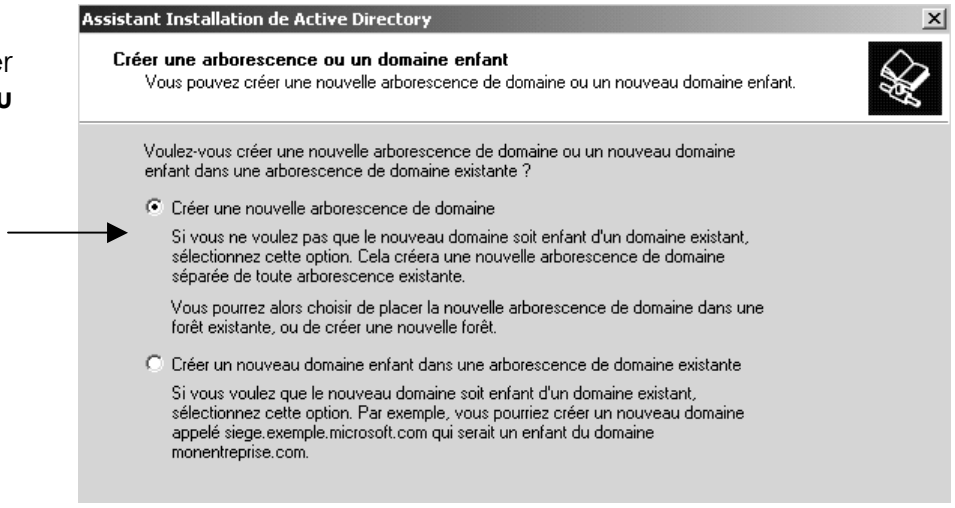
Assistant Active Directory (création d'un domaine) :

La création d'un domaine nécessite au minimum un Contrôleur de Domaine, celui doit être doté d'un espace disque NTFS pour pouvoir installer le service Active Directory dessus

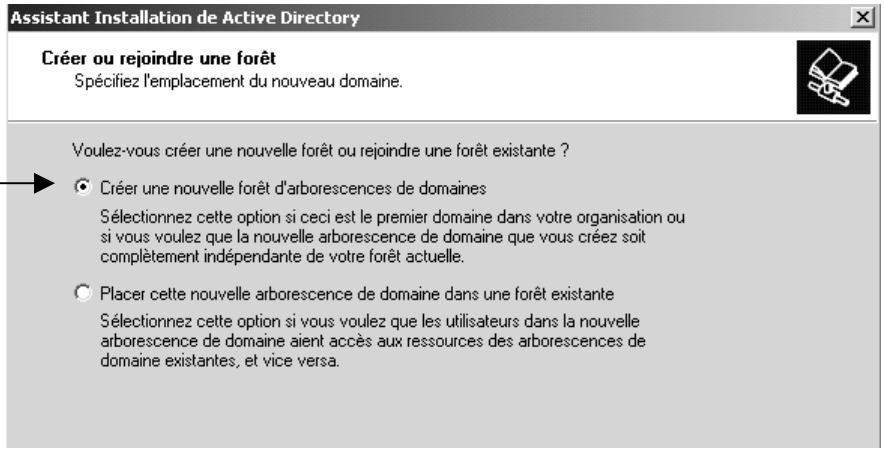
On crée ici donc le « **premier contrôleur de domaine du réseau** »



On veut créer « **un nouveau domaine indépendant** »



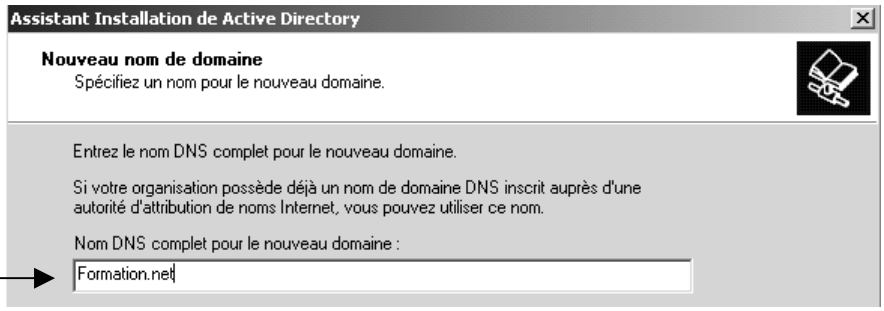
« **… de toute arborescence** »



Il faut donner le nom du domaine que l'on crée

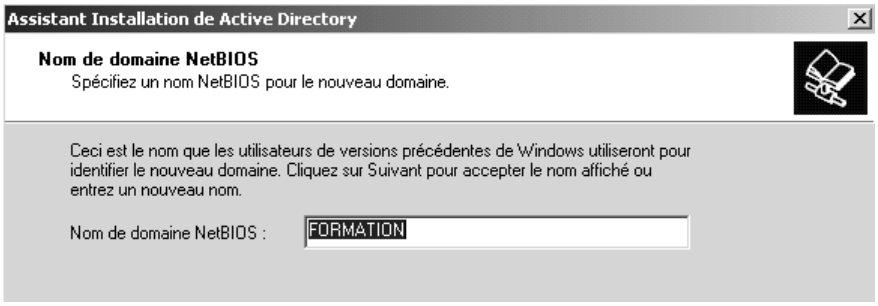
Par exemple

Formation.net



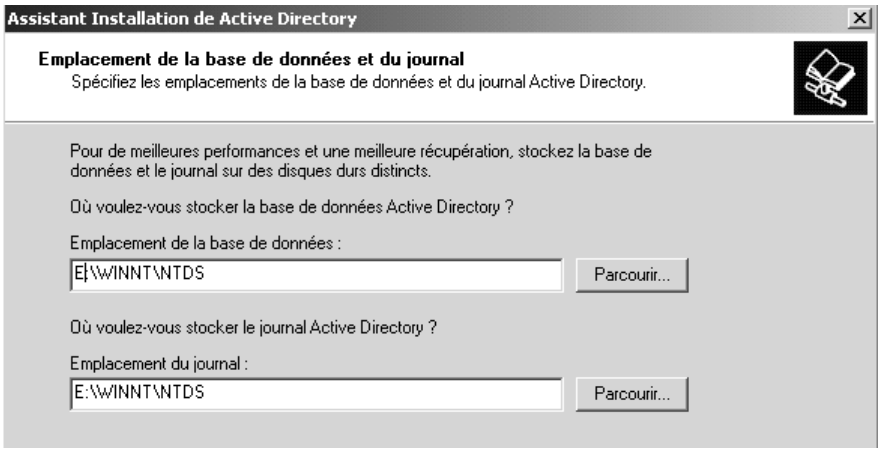
A partir duquel le nom **Netbios** sera automatiquement proposé

On accepte !

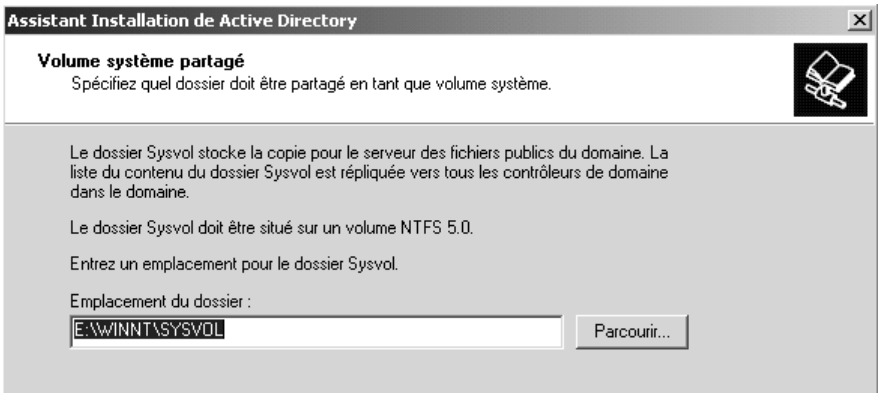


puis

Emplacement des fichiers stockant l'Active Directory ! (on peut les mettre ou l'on veut)

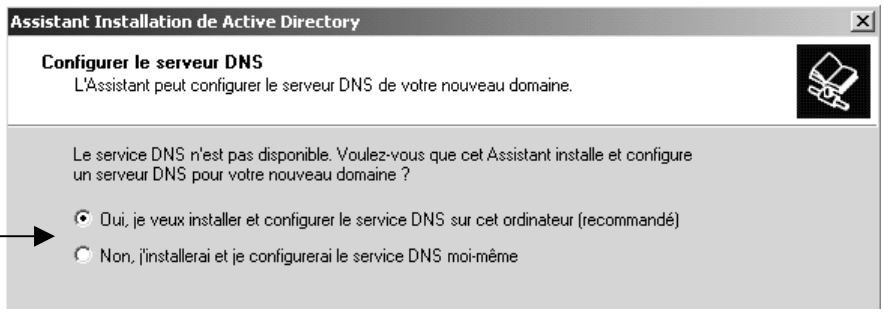


fichiers miroirs de l'Active Directory destinés à la lecture et réplication (on doit les mettre sur un volume NTFS)

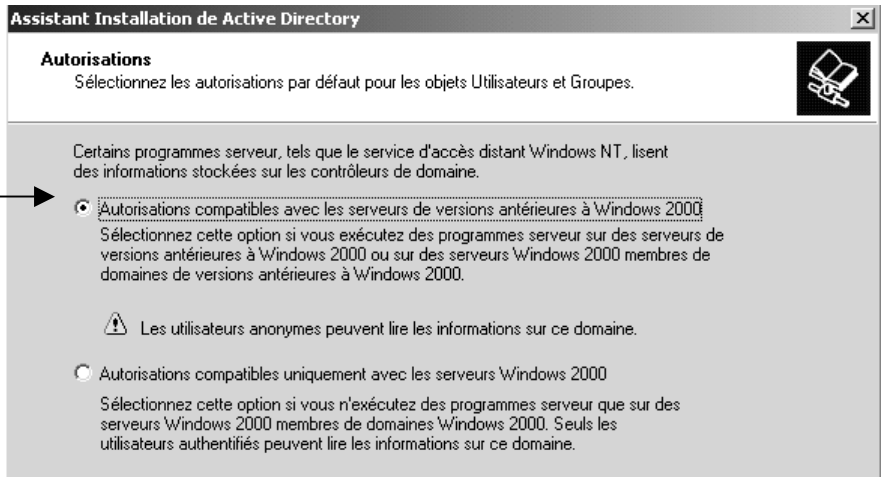


A la suite de quoi, NT2000 cherche un serveur DNS opérationnel pour faire fonctionner Active Directory

S'il ne le trouve pas, il va proposer d'en créer un



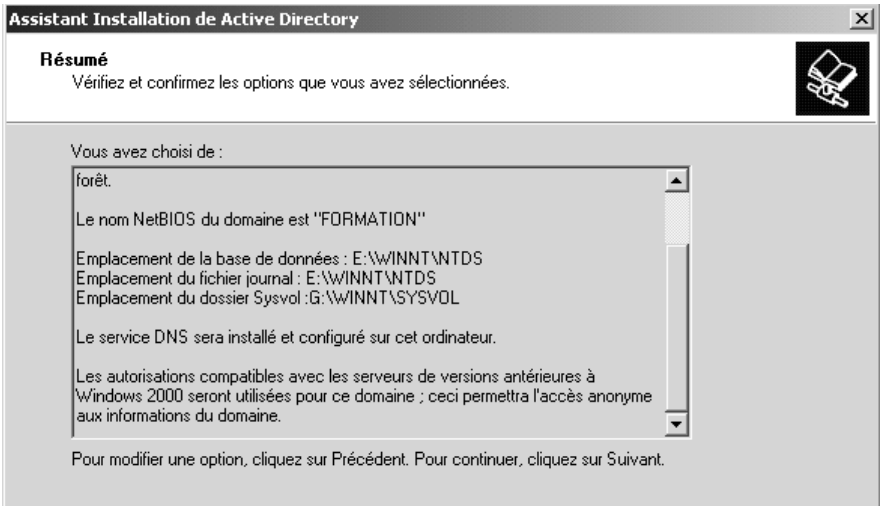
Ensuite le problème est de savoir si l'on se trouve dans un réseau uniquement composé de machines NT, ou non



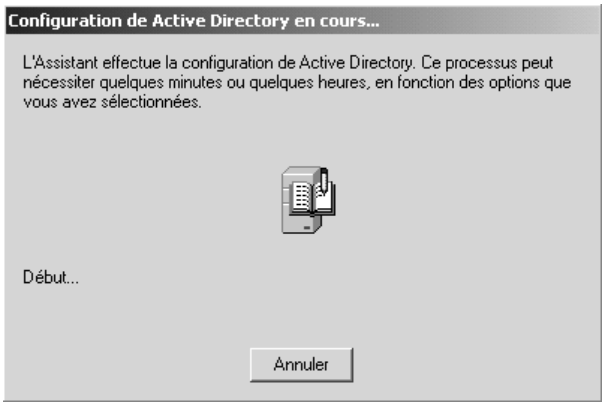
De manière générale il faut toujours prévoir des machine « non NT2000 »,

prévoir un mot de passe différent de celui d'ouverture de session

Après l'affichage d'un bref résumé



La transformation en contrôleur de Domaine peut alors commencer



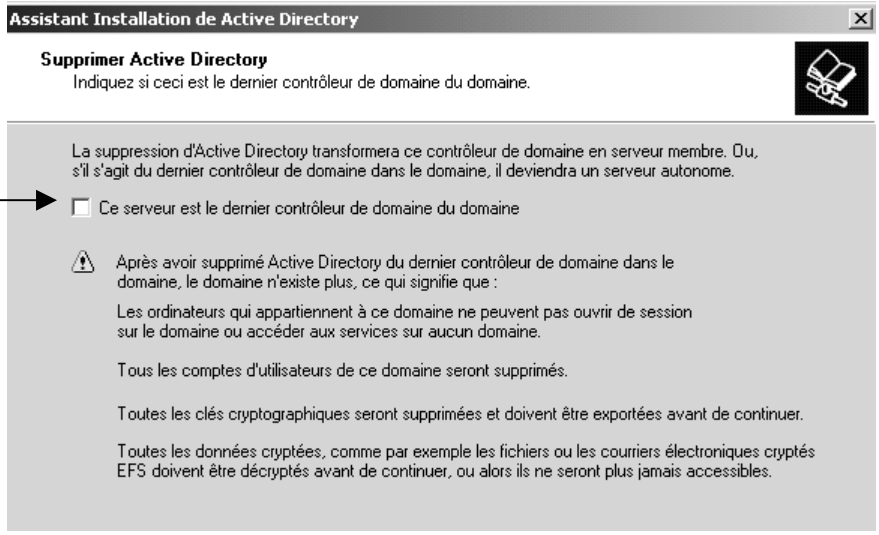
Le CD ROM NT server est nécessaire

et Il faut re-démarrer le nouveau contrôleur....

Assistant Active Directory (Rétrogradation d'un contrôleur) :

Si on souhaite enlever Active Directory d'un Contrôleur domaine. **Démarrer/Exécuter** et tapez ensuite **dcpromo**.

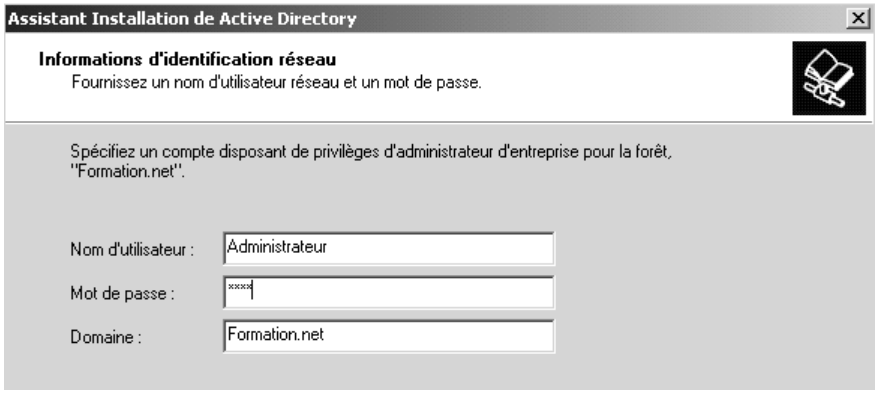
Une sérieuse mise en garde apparaît



Et on demande de « confirmer » que

Ce serveur est le dernier contrôleur de domaine

Il faut s'identifier



et recréer le mot de passe pour l'administrateur de ce qui va redevenir un serveur autome !

NB: Le mot de passe d'un serveur n'est pas forcément identique de celui du CD !

N.B: Noter au passage que lors de la "promotion" d'un serveur 2000 en CD le mot de passe de l'administrateur n'est pas changé....

puis un résumé s'affiche, et la rétrogradation s'opère…cela peut durer un certain temps. Enfin le re démarrage du poste est inévitable !

SERVICE DNS

Noms DNS:

Selon la définition de la RFC 952 le nom DNS d'un ordinateur est constitué de plusieurs parties séparées par des virgules, par exemple, **www.fnac.presse.fr.**

	NetBIOS	Full computer name
Type	Flat	Hierarchical
Character Restrictions	A-Z, a-z, 0-9, "espace", symbols: ! @ # $ % ^ & ') (. - _ { } ~ Unicode chars,	A-Z, a-z, 0-9, symbols: -_, Unicode chars. Le point '.' est le séparateur
Maximum Length	16 (dont 1 réservé) dont 15 en pratique	63 pour un nom de domaine 255 pour un FQDN
Name Service	NBNS (WINS and broadcast)	DNS

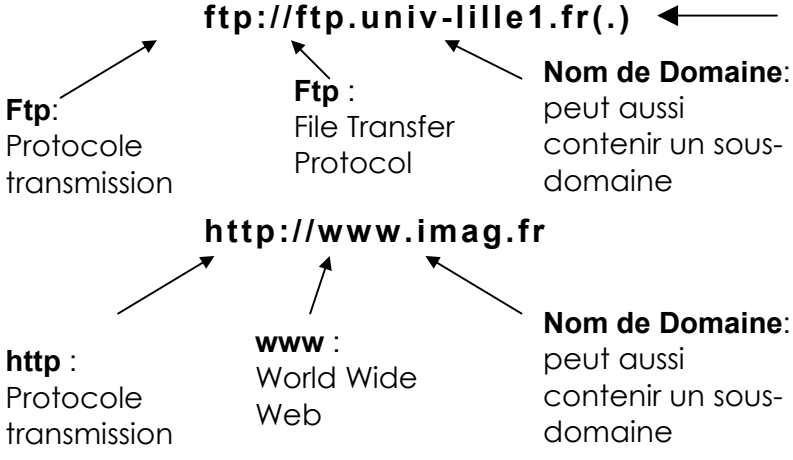
Windows 2000 utilise les noms DNS comportant des caractères soulignés, une fonction qui affectera votre choix de serveur DNS

Nom "Plat" Netbios

Les nom netbios sont crées-enregistrés lors du démarrage de chaque poste, et doivent être uniques sur tous le réseau. Ce simple constat pose les limites d'envergure des noms Netbios gérés par broadcast, d'ou l'apparition de serveur WINS sur les réseaux de taille moyenne-grande. Mais même ainsi, il parait impossible d'assurer l'unicité sur des réseau de grandes envergure...

Nom "Hierarchique" DNS

une URL se lit de droite à gauche

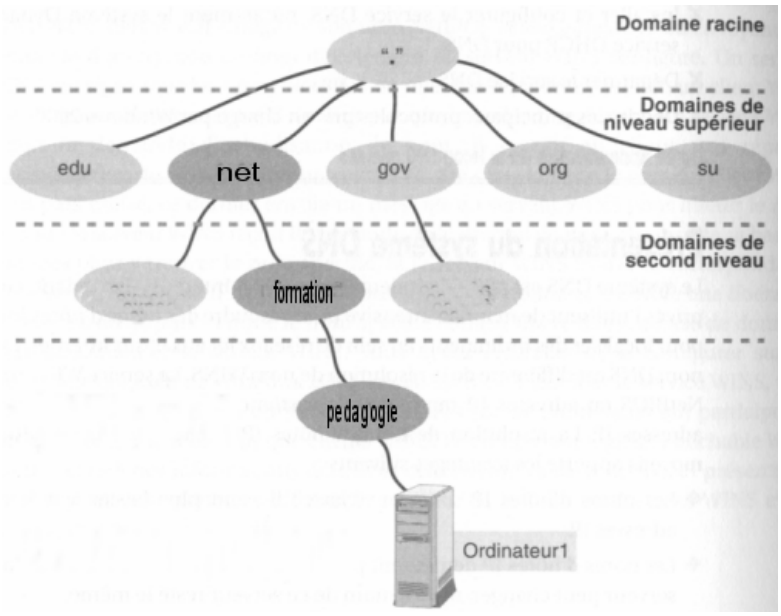


Un nom se termine par un point **.** qu'il n'est plus necessaire d'écrire, mais qui correspond au domaine "racine"

Un nom de domaine (imag.fr) se décompose en

- Un Top Level Domain (exemple : fr)
- Un nom d'organisation (appelé aussi nom de domaine) (ex : imag)

Structure des domaines



le **FQDN** (Fully Qualified Domain Name) de cet ordinateur est **Ordinateur1.pedagogie.formation.net**

Les Top Level Domain les plus courants sont:

Clé	Contenu
.com	Entreprise commerciale
.edu	éducation
.gov	organismes gouvernementaux
.mil	organisations militaires
.net	intervenant d'internet
.org	instance gouvernementale ou institution administrative

Cependant si ces domaines sont a priori internationaux, ils sont à forte dominante américaine. De plus chaque pays possède son nom de domaine (à l'exception des USA qui utilisent les 6 domaines précédents).

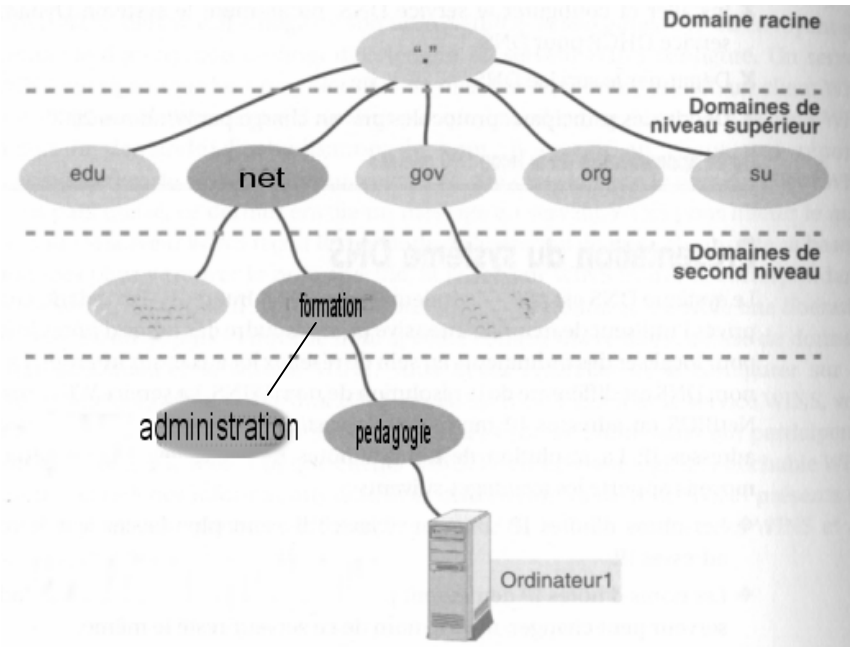
Clé	Contenu
.au	Australie
.ca	Canada
.fr	France
.uk	United Kingdom

L'internic se chargeant de l'attribution des adresses dans les domaines internationaux, c'est le NIC France qui se charge des attributions des noms de domaine en .fr

http://www.nic.fr

Zones DNS

Une **Zone** représente une partie de l'espace de nom de Domaine, a des fins de gestion.



Supposons que vous ayez deux régions, **administration** et **pedagogie**. Chaque région souhaite exploiter un serveur **DNS local**.

Pour répondre aux besoins des deux régions, vous pouvez ajouter un niveau comme par exemple :

administration.formation.net et

pedagogie.formation.net.

Chaque serveur DNS a une sous-section de domaine (une **zone** en jargon DNS).

Le serveur DNS central **formation.net** ne gère alors plus qu'un très petit nombre de noms de hosts. Il stocke en outre les noms et adresses IP des serveurs DNS de ces zones, à savoir **pedagogie.formation.net** et **administration.formation.net**.

Ainsi, si une machine **ordinateur1** se trouve dans la région **pedagogie**, elle se nommera.**ordinateur1**.**pedagogie**.**formation.net**

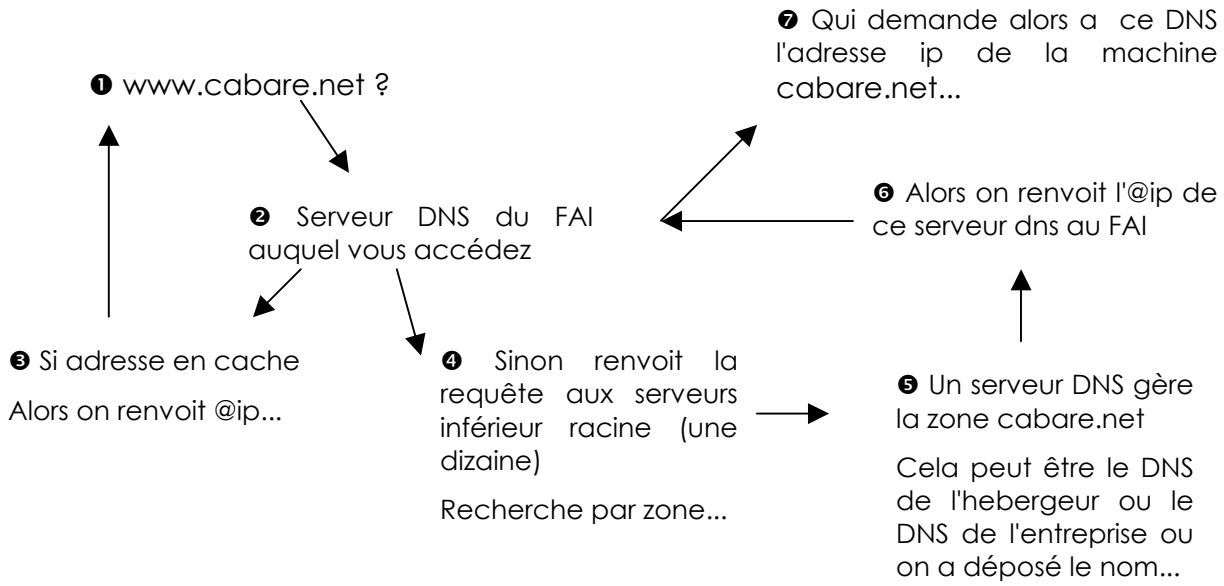
- Si cette machine **ordinateur1** essaye d'atteindre un autre poste du domaine pédagogie, sa requête sera traitée par le serveur DNS de **pedagogie.formation.net**
- Si cette machine **ordinateur1** essaye d'atteindre un poste du domaine administration, sa requête sera traitée par le serveur DNS de **pedagogie.formation.net,** et **redirigée** vers le serveur racine de niveau supérieur**,** à savoir **formation.net.** celui-ci connait le serveur qui gère la zone administration, c'est **administration.formation.net** il renvoit l'adresse de ce serveur DNS au serveur DNS **pedagogie.formation.net** qui peut alors refaire sa demande...

Réquêtes itératives ou récursives

Avec un raisonnement identique a celui précédant pour formation-administration décomposons la requête envoyée à un DNS pour un accès à un site sur Internet.

Vous êtes sur un poste et vous essayez d'atteindre l'URL **www.cabare.net.**

Vous pouvez vous permettre de demander en fait **www.cabare.net**, et cette demande est transmise au serveur DNS de votre FAI.



- Le processus ❶❷ puis ❸ est appellé requête récursive
- Le processus ❶❷puis ❹❺❻❼ est appellé requête itérative

Résolution de Noms et Résolution inverse

Chaque composant informatique d'Internet a une adresse IP unique sur 32 bit (par exemple **154.23.17.8**). Il est possible de nommer un élément en se référant à son adresse IP. Mais la plupart des utilisateurs préfèrent les noms plus faciles à retenir comme **http://toto.com**. Pour pouvoir utiliser ce type de noms, il faut une base de données capable de convertir les adresses IP en adresses mémorisables. On appelle cela la **résolution de noms**.

la **résolution de nom** (**forward lookup**) permet de trouver une adresse IP à partir d'un nom

la **résolution inverse** (**reverse lookup**) permet de trouver un nom à partir d'une adresse IP

Du fait du faible nombre de systèmes présents sur Internet à ses origines, les machines connectées à Internet prenaient en charge la résolution de noms via une simple table ASCII (**fichier HOSTS**) qui listait les adresses IP et les noms de machines correspondants. (Le code de TCP/IP permet toujours de placer un fichier HOSTS sur un système). Depuis 1984, les systèmes ont recours principalement à **DNS** pour la résolution de noms. Sinon il faudrait maintenir un fichier HOSTS qui contiendrait non seulement des centaines de millions d'ordinateurs, mais qui changerait quotidiennement !

L'implémentation la plus populaire de DNS est **BIND** (Berkeley Internet Name Domain) sous UNIX

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

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 2000

Installer le Service DNS sous NT 2000 :

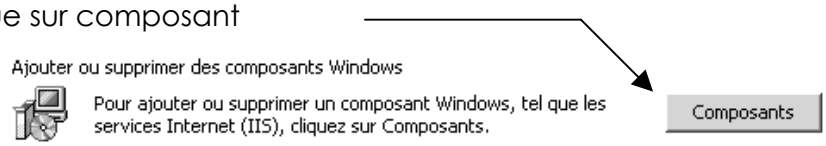
La résolution de nom via DNS ne peut se faire que sur une machine ayant une adresse IP fixe (cette adresse est ensuite rentrée sur chaque « client »)

Pour fonctionner avec Windows 2000, les serveurs DNS doivent

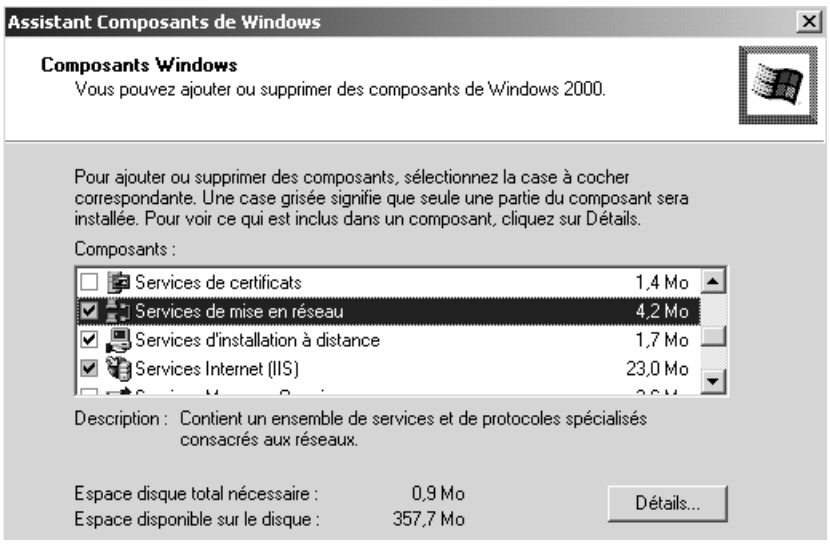
- supporter la RFC 2052 (et ses enregistrements SRV) et la RFC 2136 (DDNS). De nombreuses versions actuelles de DNS (notamment les dernières versions de BIND) les supportent. Le DNS NT4 non.
- accepter les noms de domaine incluant le caractère souligné. De nombreux enregistrements créés automatiquement 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)**

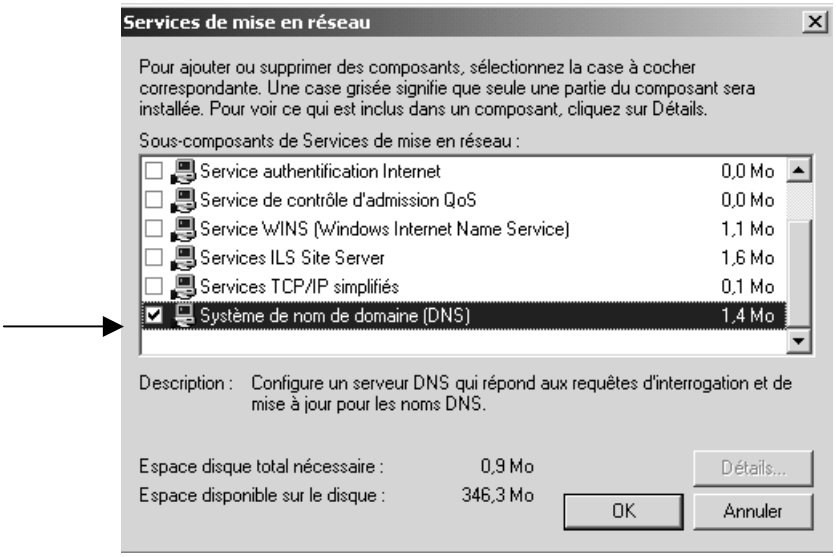
on clique sur composant



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



via Détails... on choisit alors **Système de nom de domaine (DNS)**

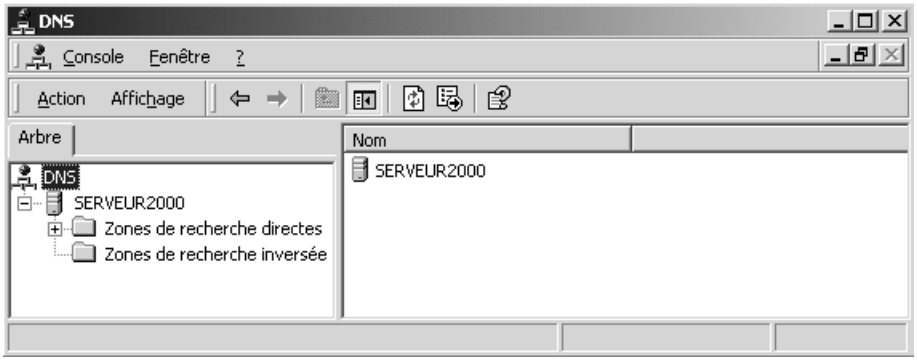


N.B : L'installation d'un serveur DNS est obligatoire dans le cadre d'un réseau NT 2000 et cette opération est requise pour installer Active Directory.

N.B : Le service DNS dans NT 2000 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

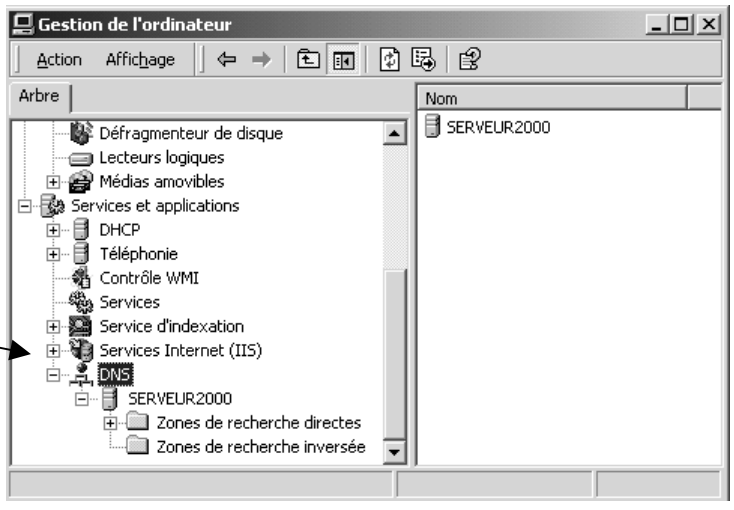
Démarrer / Programmes / Outils d'administration / DNS



ou via

Démarrer / Programmes / Gestion de l'ordinateur

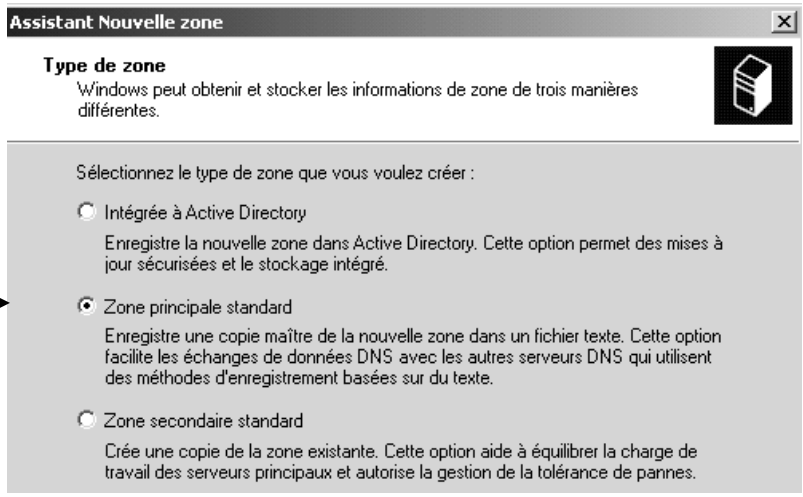
ou l'on retrouve dans **les services** le service DNS...



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...**

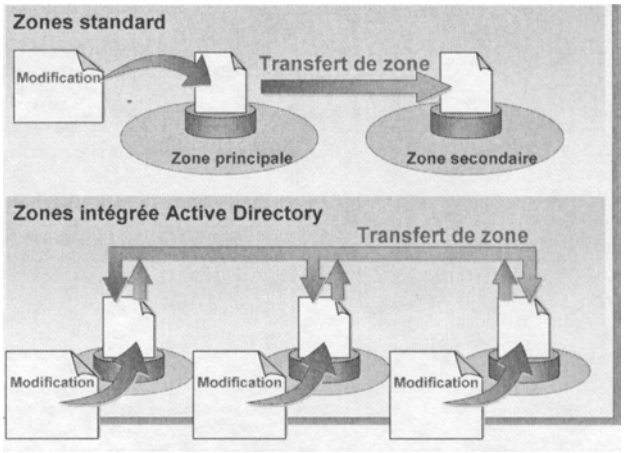
un assistant apparaît nous demandant quel type de zone on souhaite créer



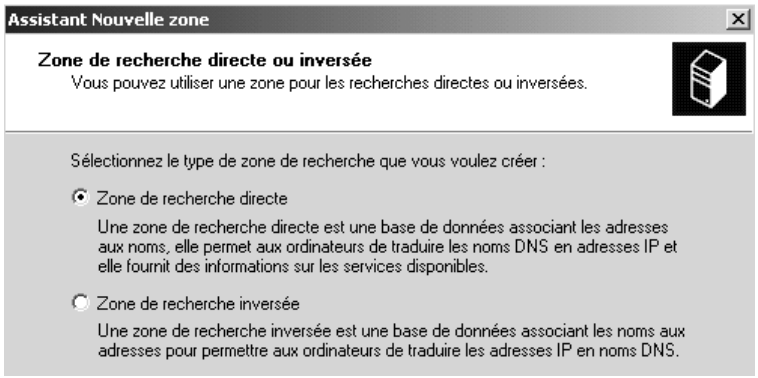
- **Intégrée à active directory** : c'est une solution propriétaire qui permet de stocker le fichier DNS non plus sous forme texte sur le serveur mais comme un objet au sein d'Active Directory, augmentant la sécurité, et remplaçant la duplication de ce fichier avec les "transfert de zone" par les mécanismes de réplication d'Active Directory., **à condition bien sûr de se placer au sein d'un réseau complètement NT 2000**.
- **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 :

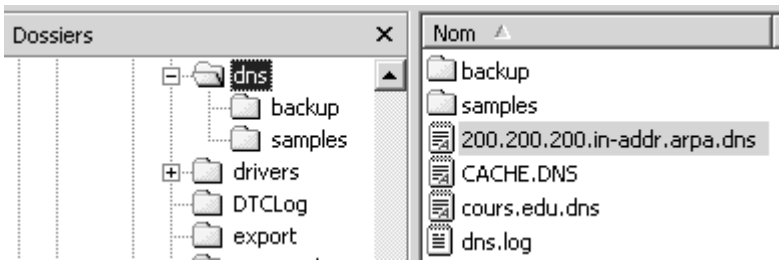


- **Zone de recherche directe** : **Forward Lookup Zone** : permet de retrouver l'adresse IP d'un appareil à partir de son nom (crée par défaut lors de l'installation de AD via DC promo). Crée un fichier avec le **nom de la zone** suivit du suffixe **.dns**
  ex: pour la zone formation.net crée le fichier 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 NT 2000 crée en général des fichiers situés dans un dossier nommé **..\WINNT\System32\dns**

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



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

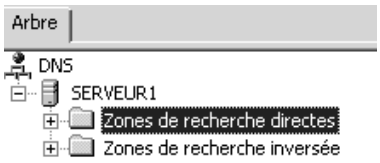
Le fichier **cache.dns** contient les enregistrement permettant la résolution de nom dans les domaines qui ne sont pas sous l'autorité du DNS visualisé.

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...

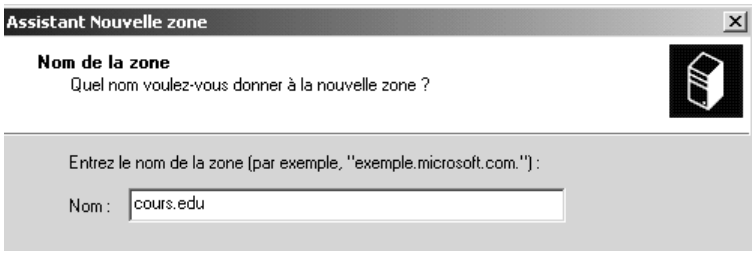
Zone de recherche directe

Il faut commencer par une zone de recherche directe :

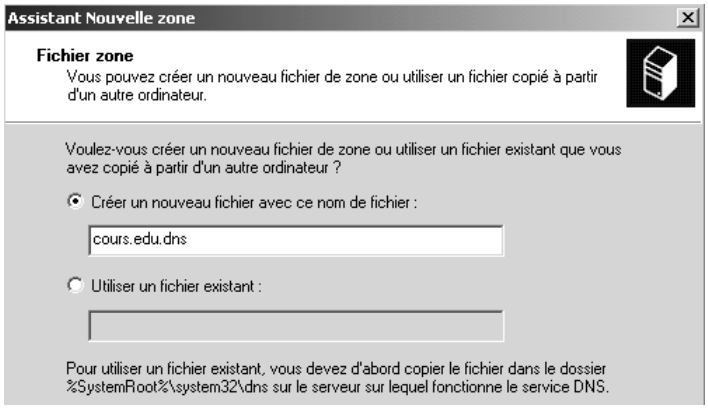
Il faut se placer sur



Puis demander une nouvelle zone via le menu contextuel



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

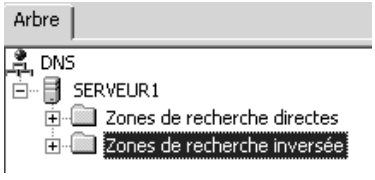


et donne un récapitulatif en fin d'opération…

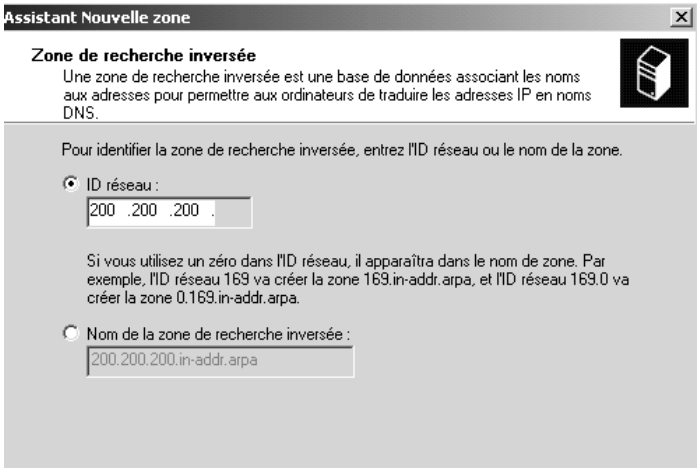
Zone de recherche inversée

On peut aussi donner une zone de recherche inversée :

Il faut se placer sur

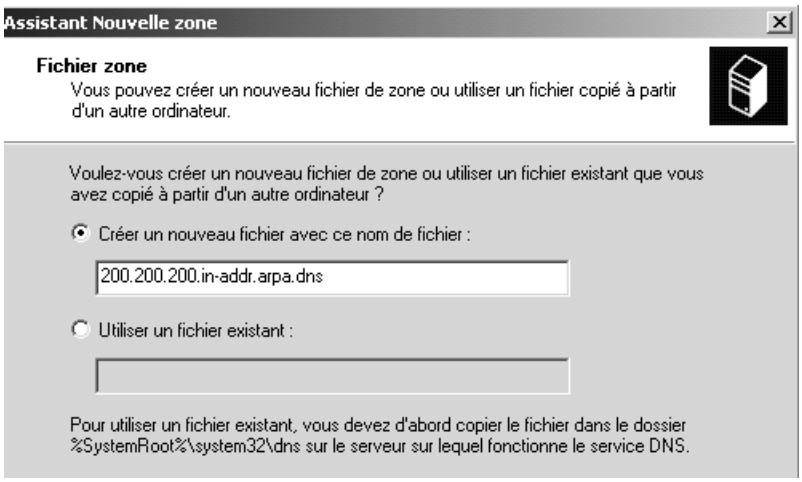


Puis demander une nouvelle zone via le menu contextuel



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

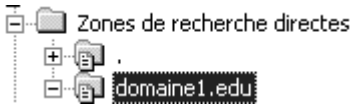
NT 2000 créera un fichier nommé *200.200.200*.**in-addr.arpa.dns**



et donne un récapitulatif en fin d'opération…

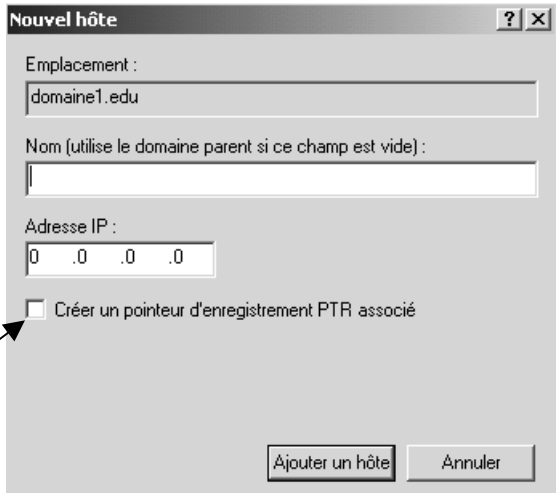
Définir un nouvel hôte :

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



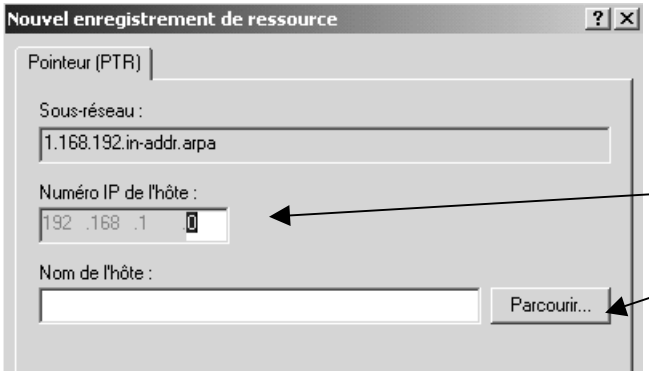
On donne le nom d'hôte et son adresse IP

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



Définir un pointeur d'enregistrement

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

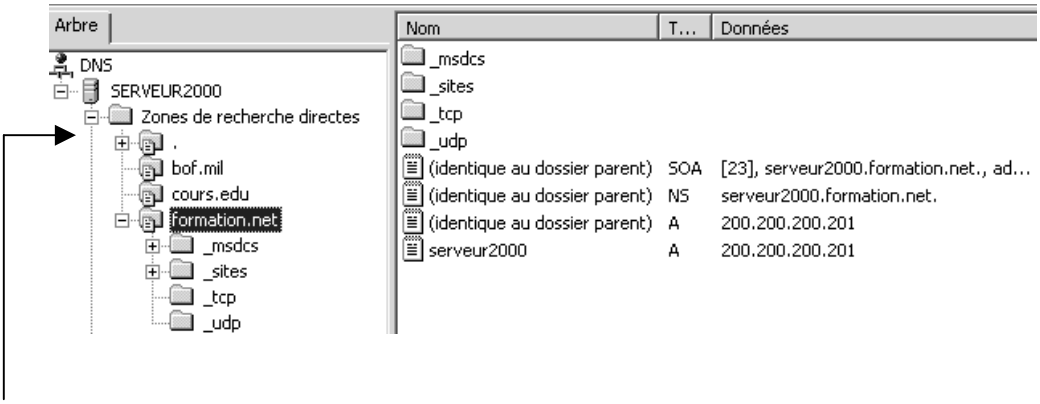


On donne uniquement le n° machine, et

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 gérés par le DNS (ceci est normé dans la RFC 1035). Pour mieux les visualiser, on peut demander **Affichage / Détaillé** dans la console DNS



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

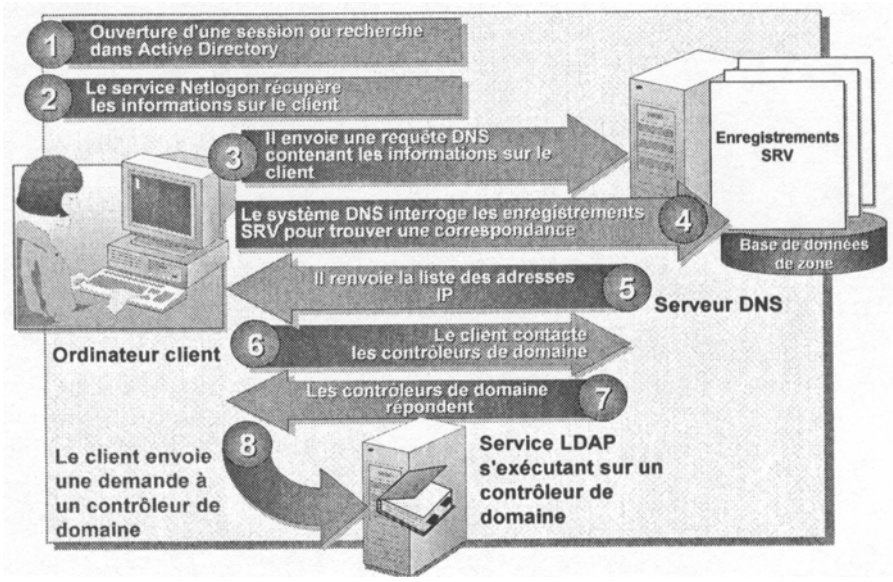
Les enregistrement de Ressource gérées par le DNS Windows NT 2000

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.



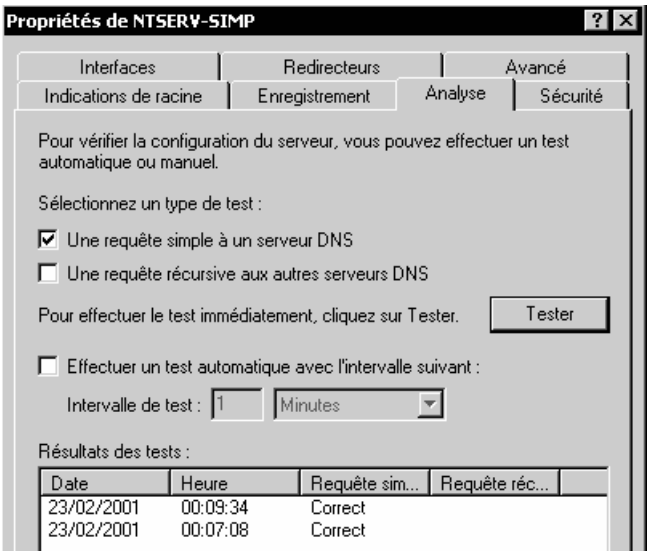
en effet pour ouvrir une session, ou parcourir AD, un client doit contacter un Contrôleur de Domaine. Tous les CD inscrivant a la fois des enregistrement de ressource A – hôte et des enregistrement de type SRV…(pour info on peut visualiser les enregistrement SRV crées par la déclaration d'un CD dans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

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
>
```

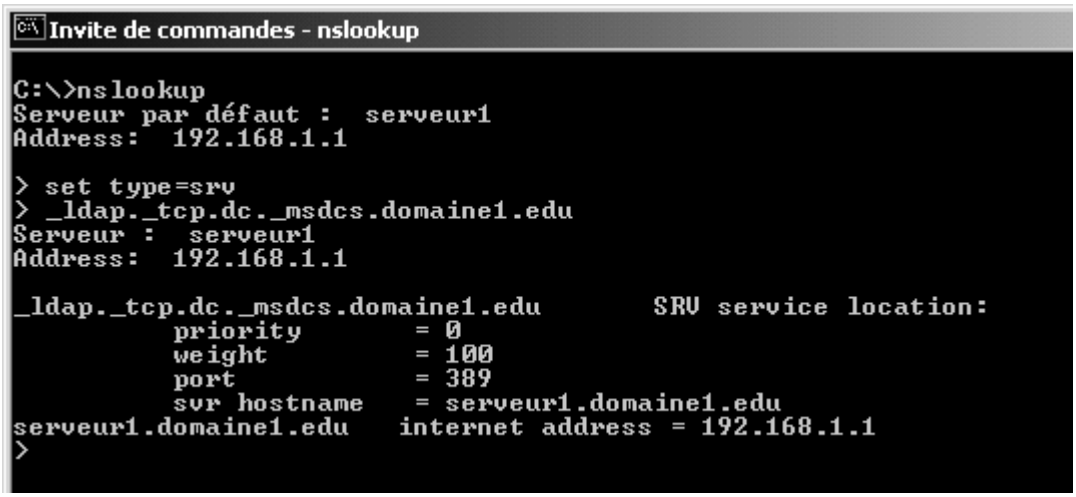
mode interactif 3°

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.

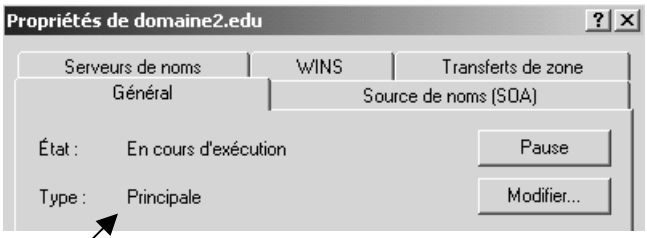
Dans l'exemple, si le nom de domaine DNS de votre domaine est **domaine1.edu**, tapez **_ldap._tcp.dc._msdcs.domaine1.edu**



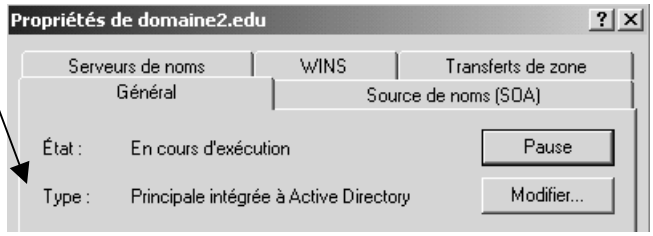
GESTION DNS WINDOWS 2000

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

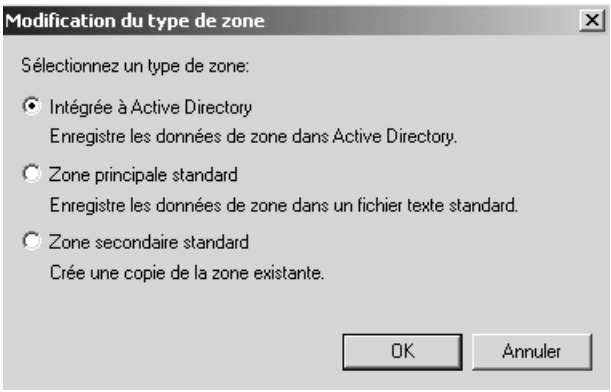
SI on a un doute pour savoir si notre zone principale est intégrée ou non dans Active Directory, il suffit de se place sur notre zone, puis demander propriété.



Type



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

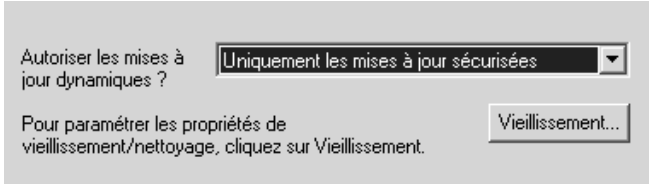


Il est préférable d'intégrer une zone dans AD !

(et la racine aussi si cela est necessaire)

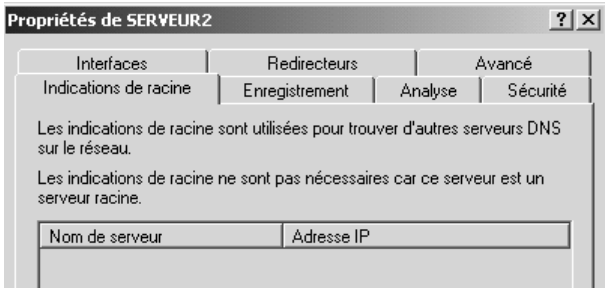
NB: on ne peut intégrer ou sortir que des zone principales

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

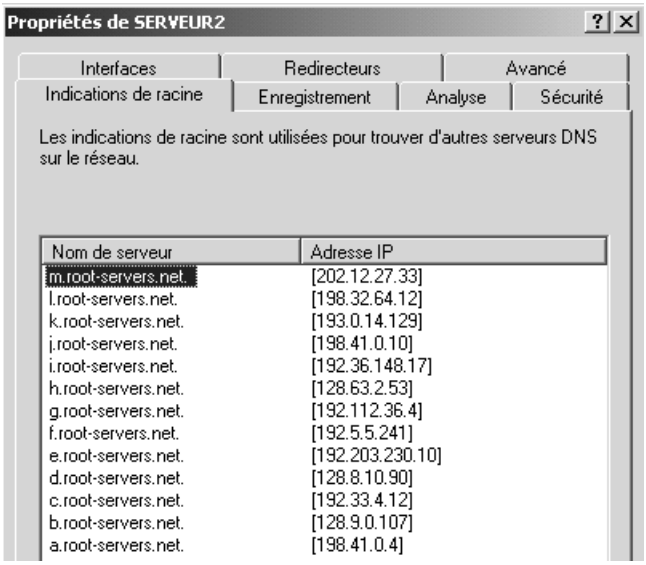


Si le serveur DNS "ne se prends pas pour un serveur racine", (n'a pas de zone racine) alors il utilise les indications de racine pour résoudre éventuellement les demandes qui lui parviennent.

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.

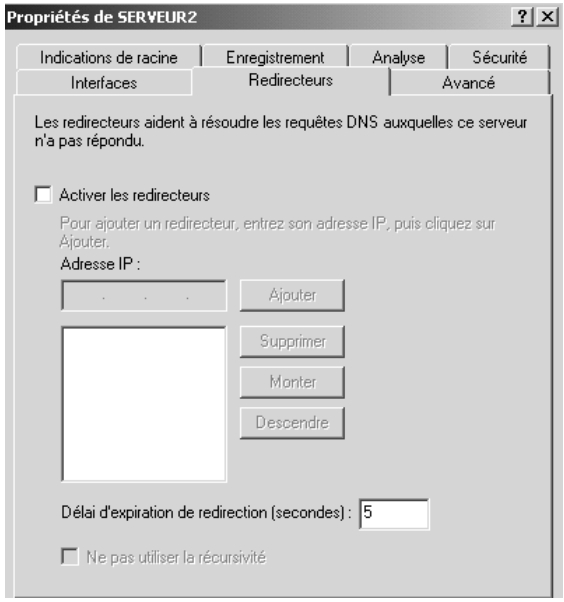
Redirecteurs

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

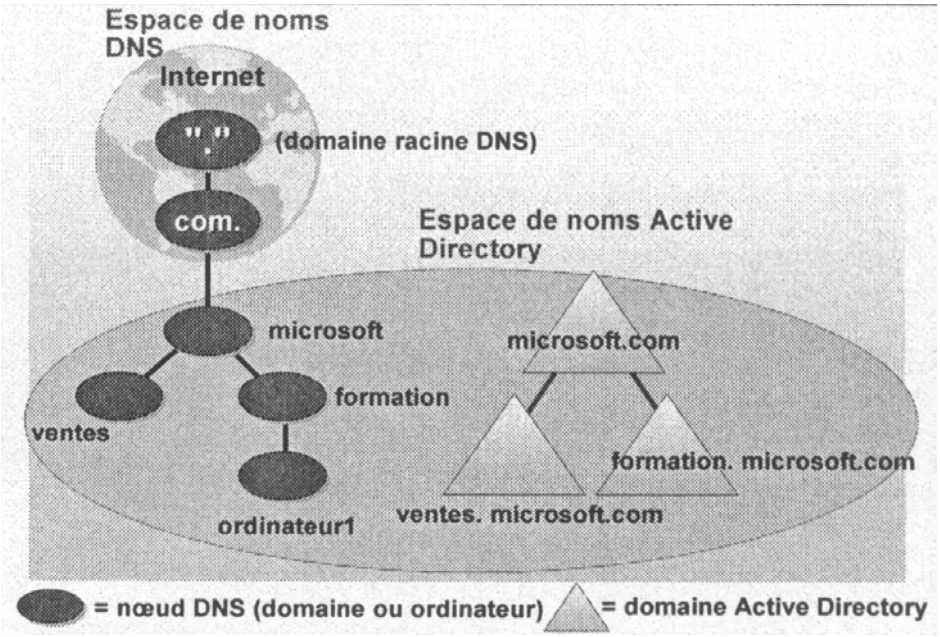
Un **redirecteur** à la priorité sur les indications de racine.

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 mecanismes AD suffiront.
- Si le serveur DNS est intégré à Active Directory, et ne possède pas un deuxième serveur DNS sur le domaine, un 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 reinstalle le serveur défaillant, une réplication de zone depuis le serveur de backup suffira à réinstaller la zone nouvellement reinstallée.
- 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...

RELATION DNS – WINS NOM NETBIOS

Protocole NetBeui :

Windows 9x et NT peuvent utiliser le protocole propriétaire Netbeui pour communiquer avec d'autre machine Windows.

D'ailleurs, pour les réseaux de petite taille, une vingtaine de postes, cette solution permet un partage simple des ressources. Cette solution permet aux **applications NETBIOS** d'accéder au réseau en s'appuyant sur le **protocole NETBEUI**.

Quelques définitions :

NetBIOS :

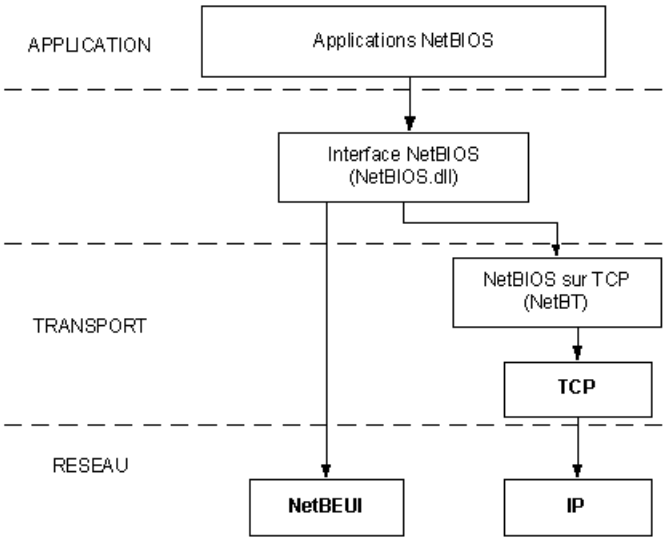
(Network Basic Input/output System) Interface de programmation qui permet aux applications d'accéder au réseau local. NetBIOS utilise un service de noms pour contrôler les échanges de point à point.

NetBEUI :

(NetBIOS Extended User Interface) est le protocole de transport des réseaux Windows. Il ne peut pas être routé et repose principalement sur les diffusions.

NetBT

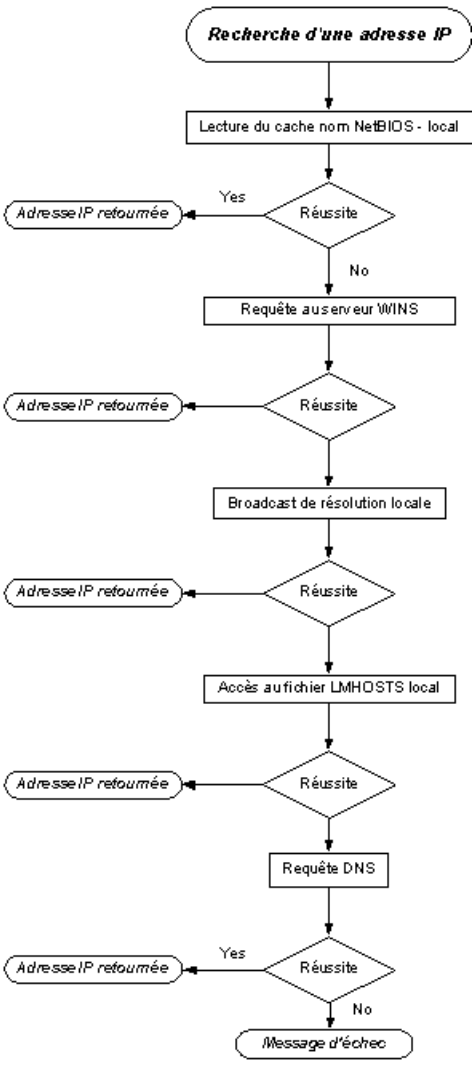
(NetBIOS sur TCP/IP) est le service de résolution de noms NetBIOS pour les réseaux Windows sous TCP/IP.



Résolution de nom NetBIOS

Windows NT peut utiliser différentes méthode pour effectuer la résolution de nom netbios :

- NetBIOS name cache (vérifiable via nbtstat –n)
- NetBIOS name server (WINS Il existe sous NT un serveur de nom NetBIOS connu sous l'appellation serveur WINS.)
- IP subnet broadcasts (limité au sous-réseau)
- Static Lmhosts file. (pour résoudre un nom netbios sur un autre réseau)
- Static Hosts file (**optionnel** pour un nom d'hôte)
- DNS servers (optionnel)



La manière dont NT va résoudre les nom Netbios, dépends du paramétrage du poste, et de la configuration du réseau existant. Les différents modes de résolution suivants sont possibles , on parle de type de noeud:

- **B-node (diffusion) :** utilise des broadcast pour l'enregistrement et la résolution des noms Netbios.
- **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. (donc utilise des boradcast) . Il continue à chercher une serveur WINS et repasse en p-node des qu'il en trouve un disponible
- **Microsoft-enhanced** : utilise les fichiers Lmhosts en plus des mode standard.

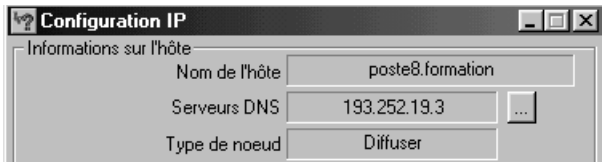
Par défaut, la plupart des clients sont paramétrés en B-nodes, c'est à dire émettent des broadcast...

il est bien sûr possible de voir le mode de résolution actuellement en cours sur une machine avec **IPCONFIG /ALL** dans la rubrique "**type de noeud**"

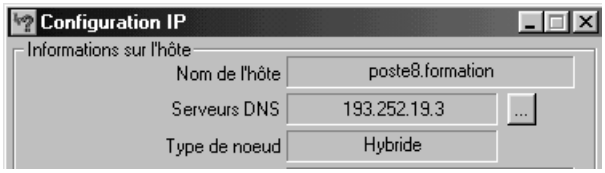
- on peut facilement demander de passer de **B-nodes** à **h-nodes**, et vice-versa.

Il suffit de renseigner ou non l'adresse d'un serveur Wins sur le client...

serveur Wins **non** renseigné



serveur Wins renseigné



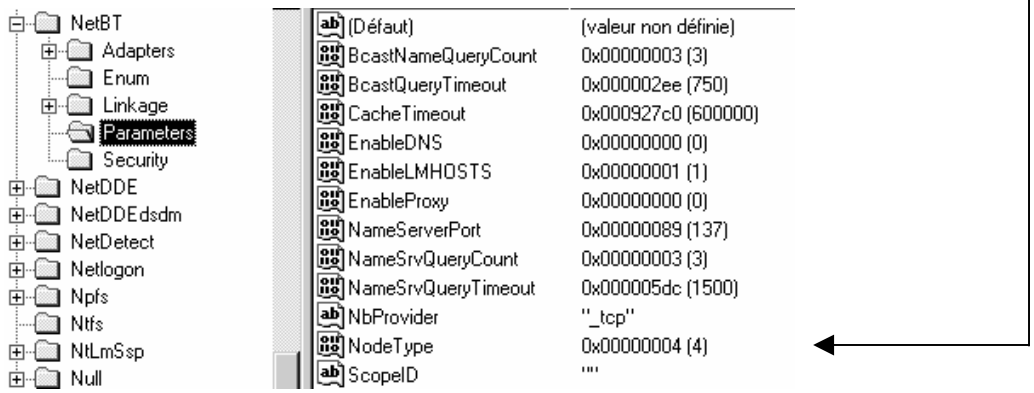
L'accès aux autres modes de résolution n'est possible que sur des machines NT ou 2000:

- Par exemple, l'activation des LmHosts se fait dans les propriétés avancées de TCP-IP, onglets Wins.
- Par exemple le passage en Type de noeud M-Nodes (4),

```
Configuration IP de Windows NT
        Nom d'hôte . . . . . . . . . . . . : wksnt4
        Serveurs DNS . . . . . . . . . . . :
        Type de noeud. . . . . . . . . . . : Mixte
        Id d'étendue NetBIOS . . . . . . . :
        Routage IP activé. . . . . . . . . : Non
        WINS Proxy activé. . . . . . . . . : Non
        Résolution NetBIOS utilisant DNS . : Non
```

ne peut se faire via modification de la base de registre par ajout d'une clé de type Dword dans l'entrée

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBt\Parameters



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

Fichier LMhosts et fichiers Hosts:

Un fichier **HOSTS** permet d'établir un mappage entre une adresse IP et un nom de machine (nom d'hôte), c'est un fichier issu du monde unix. L'alternative au fichier hosts est un serveur DNS.

A utiliser lorsque : on souhaite effectuer des transactions IP (ping, ftp…) lorsque la machine à atteindre n'a pas eut son nom résolu par DNS

Permet donc d'être sûr de trouver un poste, indépendamment du fonctionnel d'un serveur DNS.

Un fichier **LMHOSTS** permet également d'établir un mappage entre une adresse IP et un nom de machine (nom d'ordinateur ou nom netbios). L'alternative au fichier LMHOSTS est le service WINS. Le fichier LMHOSTS (Lan Manager HOSTS) concerne essentiellement les réseau Microsoft.

A utiliser lorsque : on souhaite effectuer des transactions réseau microsoft, (Lan Manager commande net…, mecanisme de voisinage réseau…) lorsque la machine à atteindre ne fait pas partie du même sous-réseau, et qu'il n'y a pas de serveurs WINS opérationnel

Permet donc d'être sûr de trouver un poste, indépendamment du fonctionnel d'un serveur WINS.

A noter qu'un nom d'hôte et un nom d'ordinateur (nom netbios) sont deux choses différentes. En toute rigueur, ils se définissent ainsi :

Nom netbios sous 98-nt4 :

Propriétés Voisinage réseau

Onglet identification

Nom d'ordinateur

Nom d'hôte sous 98-nt4:

Propriété TCP/IP

onglet DNS

Hôte

Nom netbios = **Nom d'hôte** sous 2000:

Propriétés Poste de Travail

Onglet identification réseau

Nom d'ordinateur

Par défaut, dans un réseau microsoft, le nom d'hôte et le nom d'ordinateur sont les mêmes.

Un nom d'hôte pourra donc prendre la forme soit d'un nom d'ordinateur (nom Netbios) soit d'un nom du type ordinateur.masociété.com (FQDN: Fully Qualified Domain Name).

Pour les routeurs, un nom d'hôte semble plus adapté car un routeur n'est généralement pas une machine Windows (bien que Windows NT puisse faire office de routeur) mais un boitier électronique contenant la plupart du temps un micro noyau de type UNIX.

Fichiers lmhosts (nom netbios)

Situé pour les postes NT – 2000 en **WINNT\SYSTEM32\DRIVERS\ETC**

Ou pour les postes windows 98 en **WINDOWS**

Un exemple est fournit sur les machines avec le fichier **lmhosts.sam** avec une extension .sam pour sample qu'il faut évidemment enlever pour rendre actif le fichier **lmhosts**. Il permet de solutionner un nom netbios sur un autre sous-réseau.

```
# Ce fichier est compatible avec les fichiers lmhosts de
Microsoft LAN
# Manager 2.x TCP/IP et les extensions offertes sont les
suivantes:
#
#       #PRE
#       #DOM:<domaine>
#       #INCLUDE <nom_de_fichier>
#       #BEGIN_ALTERNATE
#       #END_ALTERNATE
#       \0xnn (caractère non imprimable)
```

Donc un fichier lmhost peut contenir une ligne du genre

192.168.1.1 NOMPOSTE #PRE

avec 192.168.1.1 l'adresse ip du POSTE

avec NOMPOSTE le nom NETBIOS du POSTE

Après modification du fichier **lmhosts** il faut impérativement redémarrer le poste, ou faire une commande en ligne

Nbtstat –R (avec le R majuscule...)

Pui vérifier la prise ne compte avec un

Nbtstat –c (avec le c minuscule...)

Fichiers hosts (nom d'hôte)

Un exemple est fournit au même emplacement sur les machines avec le fichier **hosts.sam** avec une extension .sam pour sample qu'il faut 2videmment enlever pour rendre actif le fichier **hosts**. Il permet de solutionner un nom d'hôte. Un fichier hosts peut contenir une ligne du genre

```
# Copyright (c) 1998 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP stack for
Windows98
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

Attention, le fichier contient toujours une ligne blanche vide à la fin !

Nom NetBios :

N.B: On peut utiliser l'utilitaire **nbtstat** pour voir les noms NetBIOS avec la syntaxe suivante :

nbtstat –n

ou nbtstat –a nommachine

Les **15 premiers caractères** d'un nom peuvent être spécifiés par un utilisateur. En revanche, le **16e caractère** du nom (hexadécimal 00-FF) indique toujours un type de ressource:

Name	Nb (hexa)	Type	Usage
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
-- MSBrowse --	01	G	Domain Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Microsoft Exchange Connector
<computername	23	U	Microsoft Exchange Store
<computername>	24	U	Microsoft Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Clients Remote Control
<computername>	44	U	SMS Admin Remote Control Tool
<computername>	45	U	SMS Clients Remote Chat
<computername>	46	U	SMS Clients Remote Transfer
<computername>	4C	U	DEC TCPIP service on NT
<computername>	42	U	mccaffee anti-virus
<computername>	52	U	DEC TCPIP service on NT
<computername>	87	U	Microsoft Exchange MTA
<computername>	6A	U	Microsoft Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Application
<username>	03	U	Messenger Service

<domain>	0	G	Domain Name
<domain>	1B	U	Domain
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	IIS
<IS~computer name>	00	U	IIS
<computername>	[2B]	U	Lotus Notes Server Service

Unique (U): Utilisé pour associer l'ordinateur désigné par son nom dans Nom d'ordinateur à une adresse IP unique dans l'adresse IP de cette entrée mappée statique. Lorsque vous sélectionnez ce type de nom, trois types d'enregistrements sont ajoutés statiquement à la base de données WINS pour le nom d'ordinateur spécifié. Les types [00h]**WorkStation**, [03h]**Messenger** et [20h] **Serveur de fichiers**.

Noms uniques NetBIOS

Format	Description
nom_ordinateur [00h]	Inscrit par le service Station de travail sur le client WINS. En général, ce nom est appelé *nom d'ordinateur NetBIOS*.
nom_ordinateur [03h]	Inscrit par le service Affichage des messages sur le client WINS. Ce service est utilisé par le client pour envoyer et recevoir des messages. Ce nom est généralement ajouté au nom d'ordinateur NetBIOS du client WINS et au nom de l'utilisateur actuellement connecté à ce client pour envoyer des messages sur le réseau.
nom_ordinateur [06h]	Inscrit sur le client WINS par le service de routage et d'accès distant (lorsque ce service est démarré).
nom_domaine [1Bh]	Inscrit par chaque contrôleur de domaine Windows NT Server qui s'exécute en tant qu'explorateur principal de domaine. Cet enregistrement de nom est utilisé pour permettre l'exploration à distance des domaines. Lorsque ce nom est demandé à un serveur WINS, ce dernier renvoie l'adresse IP de l'ordinateur qui a inscrit ce nom.
nom_ordinateur [1Fh]	Inscrit par les services NetDDE (Network Dynamic Data Exchange). Ne s'affiche que si les services NetDDE sont démarrés sur l'ordinateur.
nom_ordinateur [20h]	Inscrit par le service Serveur sur le client WINS. Ce service est utilisé pour fournir des points de service au client WINS, qui lui permettent de partager ses fichiers sur le réseau.
nom_ordinateur [21h]	Inscrit sur le client WINS par le service Client RAS (lorsque ce service est démarré).
nom_ordinateur [BEh]	Inscrit par l'Agent de surveillance du réseau et n'apparaissant que si ce service est démarré sur le client WINS. Si le nom d'ordinateur compte moins de 15 caractères, les espaces restants sont remplis par des signes plus (+).
nom_ordinateur [BFh]	Inscrit par l'utilitaire de surveillance du réseau (livré avec Microsoft Systems Management Server). Si le nom d'ordinateur compte moins de 15 caractères, les espaces restants sont remplis par des signes plus (+).
nom_utilisateur [03h]	Les noms des utilisateurs actuellement connectés sont inscrits dans la base de données WINS. Chaque nom d'utilisateur est inscrit par le service Serveur de sorte que les utilisateurs peuvent recevoir toutes les commandes **net send** envoyées au nom d'utilisateur. Si plusieurs utilisateurs se connectent sous le même nom, seul le premier ordinateur connecté avec ce nom enregistre le nom.

Group (G): Appelé aussi groupe ordinaire. Ce type est utilisé pour ajouter une entrée statique pour l'ordinateur, spécifié par un nom dans un mappage statique, dans un groupe de travail utilisé sur votre réseau. Si vous utilisez le type, l'adresse IP de l'ordinateur n'est pas stockée dans WINS, mais résolue par le biais des diffusions du sous-réseau local.

Noms de groupes NetBIOS

Format	Description
nom_domaine [00h]	Inscrit par le service Station de travail de sorte qu'il puisse recevoir les diffusions d'exploration provenant d'ordinateurs LAN Manager.
nom_domaine [1Ch]	Inscrit à l'usage du contrôleur de domaine dans le cadre du domaine. Peut contenir jusqu'à 25 adresses IP.
nom_domaine [1Dh]	Inscrit à l'usage des explorateurs principaux (un seul explorateur principal par sous-réseau). Les explorateurs de sauvegarde utilisent ce nom pour communiquer avec l'explorateur principal, en extrayant la liste des serveurs disponibles de l'explorateur principal. Les serveurs WINS renvoient toujours une réponse positive d'inscription pour *nom_domaine*[1D], même si le serveur WINS n'*inscrit* pas ce nom dans sa base de données. En conséquence, lorsque le *domain_name*[1D] est demandé à un serveur WINS, ce dernier renvoie une réponse négative, ce qui force le client à lancer une diffusion de résolution de noms.
nom_groupe [1Eh]	Un nom de groupe ordinaire. Tout ordinateur configuré en tant qu'explorateur de réseau peut diffuser vers ce nom, et écouter les diffusions vers ce nom, pour choisir un explorateur principal. Un nom de groupe mappé statiquement utilise ce nom pour s'inscrire sur le réseau. Lorsqu'un serveur WINS reçoit une demande de nom se terminant par [1E], il renvoie toujours l'adresse de diffusion du réseau local du client qui a émis la demande. Le client peut ensuite utiliser cette adresse pour diffuser aux membres du groupe. Ces diffusions sont destinées au sous-réseau local et ne doivent pas traverser de routeurs
nom_groupe [20h]	Un nom de groupe spécial appelé *groupe Internet* est inscrit sur les serveurs WINS pour identifier des groupes d'ordinateurs pour des besoins administratifs. Par exemple, "printersg" peut être un nom de groupe inscrit utilisé pour identifier un groupe administratif de serveurs d'impression.
-- __MSBROWSE__ [01h]	Inscrit par l'explorateur principal pour chaque sous-réseau. Lorsqu'un serveur WINS reçoit une demande concernant ce nom, il renvoie toujours l'adresse de diffusion du réseau local du client qui a émis la demande.

enfin, moins important

Multihomed (M): Utilisé pour inscrire un nom unique pour un ordinateur ayant plusieurs adresses IP (plusieurs cartes utilisant chacune une adresse unique ou une seule carte réseau configurée avec plusieurs adresses IP).

Internet **Group (I):** Utilisés pour des groupes administratifs spéciaux définis par l'utilisateur. Vous pouvez utiliser ce type pour regrouper des ressources. Par exemple, vous pouvez indiquer un groupe de fichiers ou de serveurs d'impression pour organiser les ressources partagées visibles lorsque vous parcourez les favoris réseau. Chaque groupe Internet est représenté par un *nom de groupe* partagé de type [20h] dans la base de données WINS

Domain Name (D): Indique une entrée mappée de *nom de domaine* [1C] pour la localisation des contrôleurs de domaine Windows NT

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 **255 caractères maxi 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 une machine 2000, DNS est utilisé tout le temps, même pour construire le voisinage réseau, par exemple. Si le serveur DNS est en carafe, 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…

Il est complètement inutile de renseigner un serveur WINS sur un réseau ayant un serveur DNS fonctionnel et des clients 2000, 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 enregistrement 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…

Wins peut simplement accéllerer les ouverture de session pour les client non 2000 afin qu'ils trouvent plus rapidement une machine donnée (en l'occurence le serveur)

MECANISME DU VOISINAGE RESEAU

Principe de fonctionnement :

Lorsque l'on clique sur voisinage réseau, on a souvent une réponse lors du démarrage de la machine comme quoi le "parcours du réseau est impossible", or **il suffit d'attendre et tout rentre dans l'ordre**...

Mais la signification du message est la suivante : actuellement un **Explorateur Principal** n'est pas encore identifié...

Environ toutes les 12 minutes, les serveurs annoncent leur présence avec des trâmes spéciales au format NetBios. Une élection d' Explorateur Principal peut arriver lorsque

- un ordinateur n'arrive pas à trouver un Explorateur Principal
- Lorsque un Explorateur Principal arrive sur le réseau, ou s'arrête.
- Lorsque un Contrôleur de Domaine démarre:

Lorsque une élection est lancée, un algorithme compliqué basé sur plusieurs variables se déroule (type de OS, version d'OS, configuration, adressage IP, nombre de machines présentes etc) et un seul Explorateur Principal sera déclaré !

A chaque fois qu'un PC démarre, il est configuré par défaut pour tenter de savoir s'il doit devenir Explorateur...

Il peut exister jusqu'à 5 types de machines dans un réseau Windows

Non-Browser / Non Explorateur

Un **non-browser** ou **non Explorateur** est un ordinateur qui a été configuré pour ne pas maintenir une liste des ordinateurs devant apparaître dans le voisinage réseau

Potential Browser / Explorateur Potentiel

Un **Potential-Browser** ou **Explorateur Potentiel** est un ordinateur capable de maintenir une liste des ordinateurs devant apparaître dans le voisinage réseau , et pouvant être promu comme Explorateur principal. Un **Explorateur Potentiel** est aussi capable de jouer le rôle d'un **Explorateur de Secours**, s'il est piloté par un **Explorateur Principal**

Backup Browser / Explorateur de Secours

Un **Backup-Browser** ou **Explorateur de Secours** reçoit une copie des ordinateurs devant apparaître dans le voisinage réseau depuis un **Explorateur Principal** et fournis cette liste à la demande des autres ordinateurs du domaine ou du groupe de travail

N.B: Lorsqu'un poste démarre, c'est l' **Explorateur Principal** qui lui indique s'il doit devenir un **Explorateur de Secours** ou non

Master Browser / Explorateur Principal

Un **Master-Browser** ou **Explorateur Principal** est responsable de la collecte des informations nécessaires à la création et à mise à jour de la liste des ordinateurs figurant dans le voisinage réseau. Cette liste inclus tous les serveurs du domaine de l' **Explorateur Principal** et la liste de tous les domaines sur le réseau. Les machines windows annoncent leur présence à l' **Explorateur Principal** par un datagrame appelé "server annoucement", et celui-ci les ajoute

- Si un Domaine s'étends sur plus d'un sous-réseau, l' **Explorateur Principal** travaille de la manière suivante :
  - ✓ Il gère la liste pour le sous-réseau dont il fait partie
  - ✓ fournit cette liste à chaque Explorateur de Secours de chaque sous-réseau
- Si un sous-réseau comprends plusieurs Domaines, chaque Domaine à son **Explorateur Principal** et éventuellement ses **Explorateurs de Secours**

Domain Master Browser / Explorateur Principal de Domaine

Un **Domain Master-Browser** ou **Explorateur Principal de Domaine** est responsable de la collecte des informations pour la création et la mise à jour de la liste pour tout le domaine, collecte les informations des **Explorateur Principaux** des autres sous-réseaux et fournit les informations aux **Explorateur Principaux** des autres sous-réseaux.

Un **Explorateur Principal de Domaine** est toujours le Contrôleur Principal de Domaine

N.B: Un poste peu jouer plusieurs rôles, par exemple l' **Explorateur Principal** peut aussi être un **Explorateur Principal de Domaine**

Rafraîchissement Tests et vérifications :

Quelles sont les vitesses de rafraîchissement ?

de quelques secondes, à plusieurs minutes, jusqu'à 12 minute pour la prise en compte d'un serveur dans un Domaine, ce qui par rebonds peut aller à 24 minutes entre 2 Domaines...

Pour la suppression d'une machine c'est pire, Microsoft annonçant jusqu'à 45 minutes pour la mise à jour d'une liste "rayant" une machine qui ne se serait pas correctement déconnectée du réseau (arrêt système brutal...)

Peut on éviter l'élections d'un Explorateur ? :

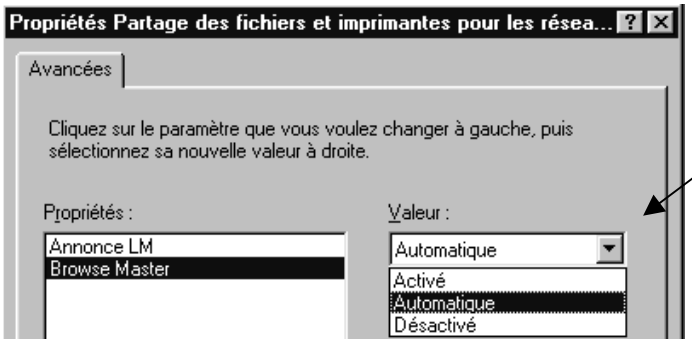
la réponse est non; il doit y en avoir toujours un, mais on peut a la limite accélérer un peut les choses

En implémentant un serveur WINS qui diminuera le trafic réseau pour les résolution de nom Netbios,

En implémentant un serveur DNS qui diminuera le trafic réseau pour les résolution de nom

En modifiant le status d'une machine : si on modifie dans propriété de partage des fichiers et imprimantes le fait qu'une machine soit éligible ou non (on peut éviter les élections et diminuer les trames émises...)

Sous Windows 95-98



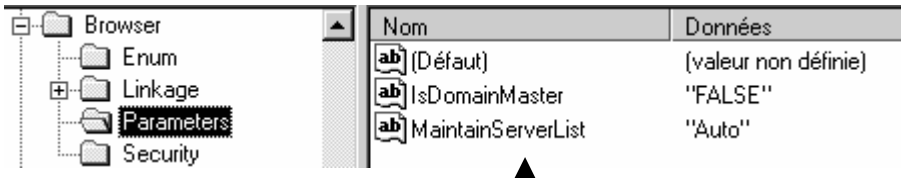
définir qui peut être Browse Master

N.B: Il doit y en avoir toujours 1 seul !

- Si on est sur que sur le sous réseau il existe toujours un Maître explorateur, on peut alors demander **Désactivé**

Sous Windows NT ou 2000

Il faut modifier la base de registre NT "ce qui reste délicat"



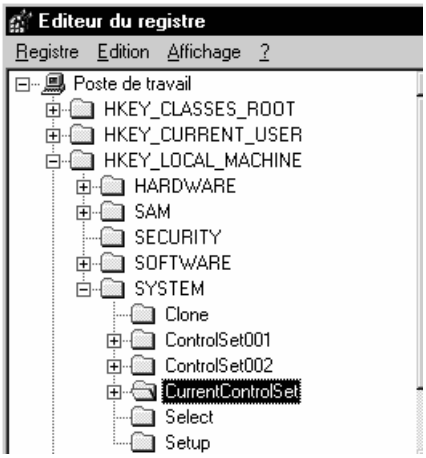
Il faut se positionner sur la clé

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\ Parameters

et y modifier la clé de type DWORD-value nommée **MaintainServer List**
les valeurs possibles sont **"Auto" "No" et "Yes"**

- Si on est sur que sur le sous réseau il existe toujours un Maître explorateur, on peut alors demander **No**

En accélérant la vitesse de rafraîchissement...Il faut modifier la base de registre NT "ce qui reste délicat"



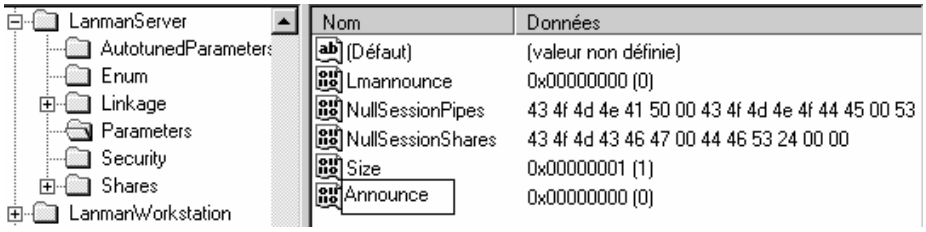
Il faut se positionner sur la clé **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\LanmanServer\ Parameters**

et y créer une clé de type DWORD-value

en allant dans le menu

Edition / nouveau / valeur Dword

et y entrer la clé **Announce**



cette valeur Announce il faut ensuite la modifier via le menu

Edition / modifier

une valeur de 60 secondes (3c hexa) semble un bon compromis entre vitesse et nombre de trâmes...

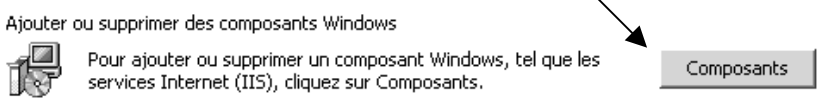
SERVICE WINS

Installer le Service WINS sous NT 2000 :

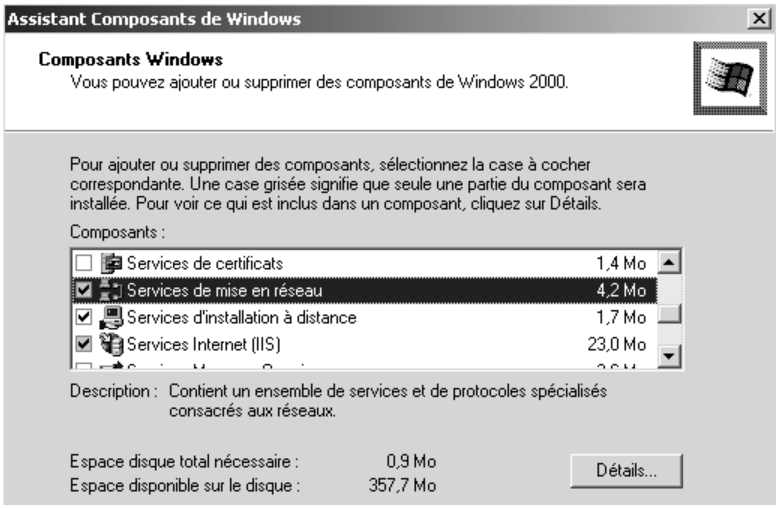
La résolution de nom netbios via WINS ne peut se faire que sur une machine ayant une adresse IP fixe (cette adresse est ensuite rentrée sur chaque « client »)

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

on clique sur composant

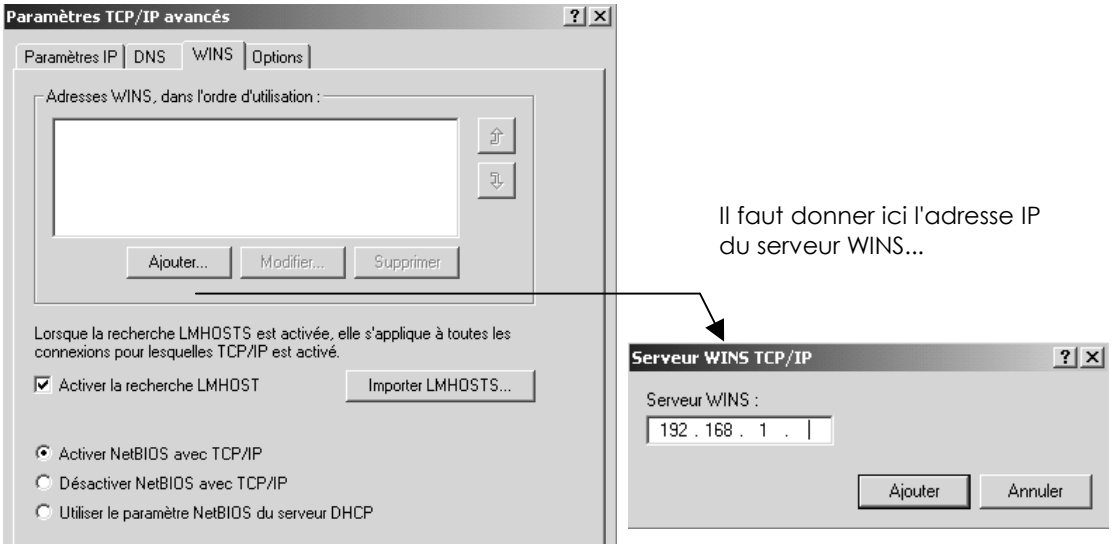


dans liste composant Windows on va chercher service de mise en réseau



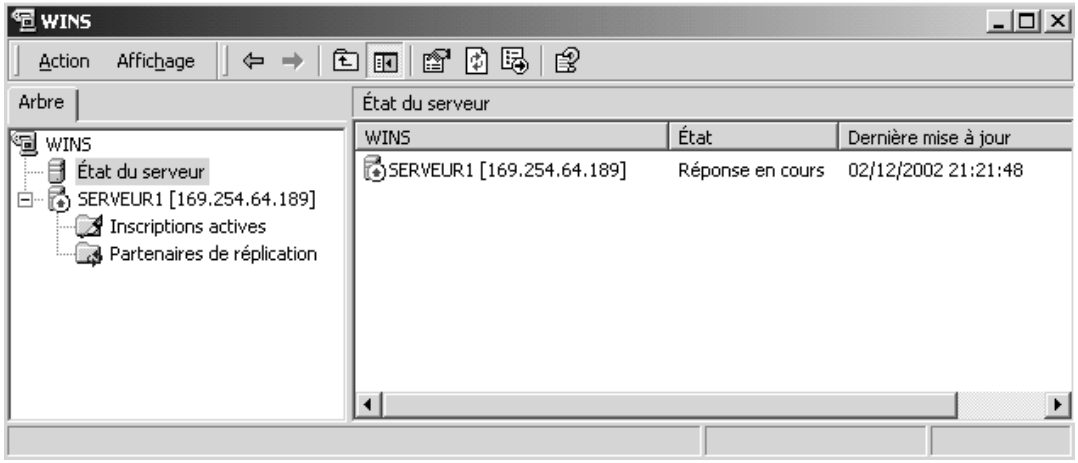
via Détails... on choisit alors **Service Wins (Windows Internet Name Service)**

Une fois installé, il faut paramétrer le serveur WINS comme étant son propre client, c'est à dire que dans les **propriétés avancées de TCP/IP**, il faut demander l'onglet **WINS** :



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

Démarrer / Programmes / Outils d'administration / WINS

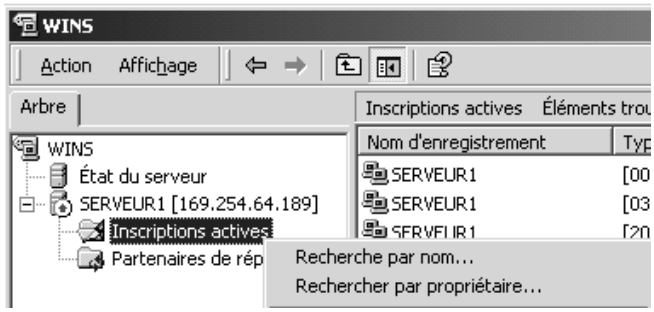


NB: ne pas préter attention à l'adresse IP qui s'inscrit dans le cas d'une machine multi-résidente...

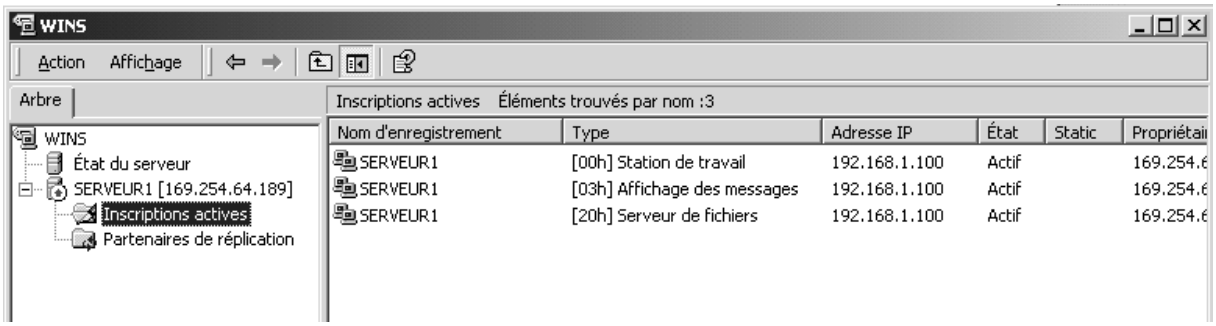
Ajouter un serveur, Visualiser une base :

Pour ajouter un serveur, il faut se placer sur Wins, et demander le me nu 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



Sauvegarder un serveur WINS:

Pour sauvegarder un serveur WINS, il faut spécifier un dossier de sauvegarde, et/ou faire une sauvegarde manuelle.

- Spécifier un dossier de sauvegarde : dans les **propriétés** du serveur Wins à configurer, onglet **général**, on indique le chemin par défaut de la sauvegarde...
- A partir de là, Wins y crée une copie de sauvegarde complète toutes les 3 heures.

Pour restaurer un serveur WINS il faut :

- Arrêter le service WINS
- Dans l'onglet propriété su 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)

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

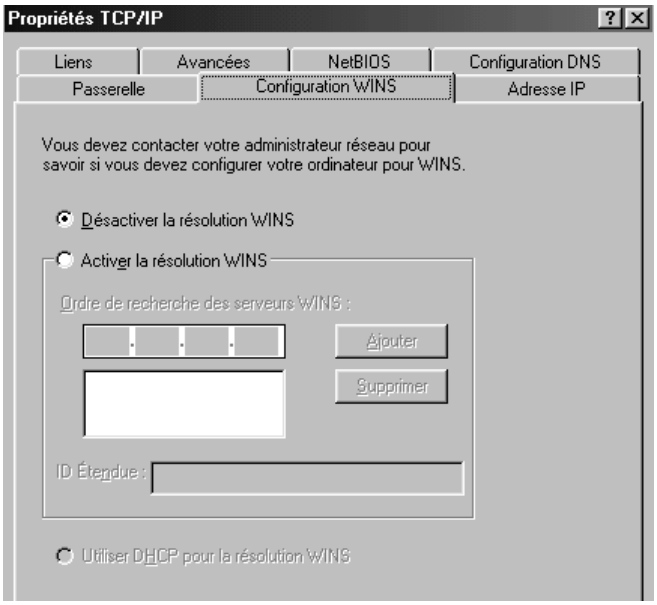
Jetpack wins.mdb

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...



Configurer automatiquement 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

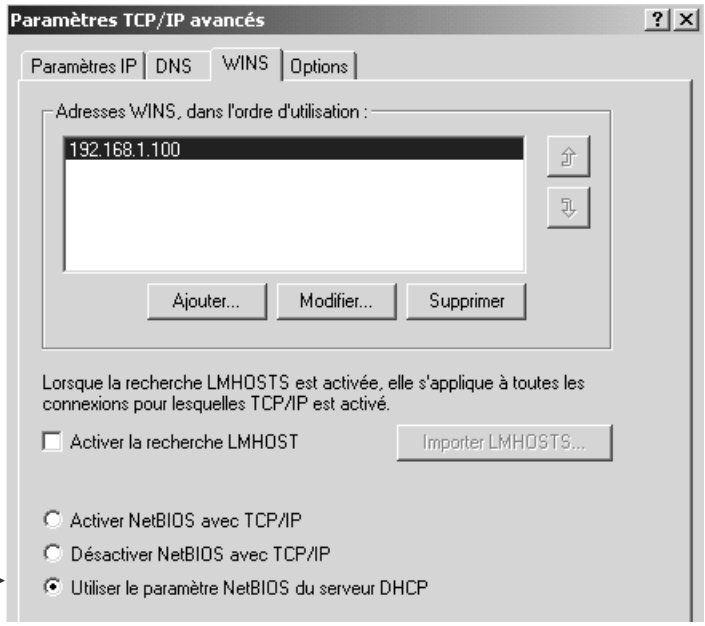
044 Serveurs WINS/NBNS avec **l'adresse ip** du serveur principal

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, il faut demander **Utiliser le paramètre Netbios du serveur DHCP**



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, telles qu'une adresse de passerelle par défaut, une adresse DNS (Domain Name Server) et l'adresse du serveur de nom NetBios.

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.

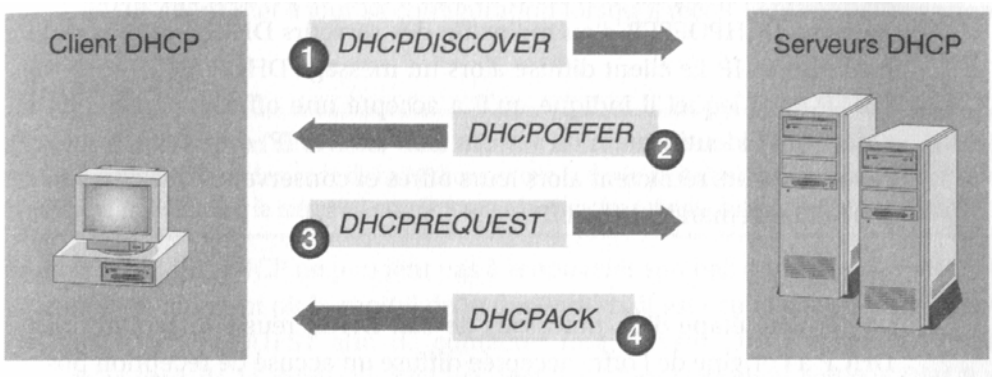
Si le client les accepte, les informations d'adressage IP lui sont cédées sous la forme d'un bail d'une durée spécifique.

Si aucune informations 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 adresse APIPA).

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 utilise un processus en quatre 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 lorsqu'une des situations suivantes se produit :

- 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 exemle) 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 nouveua utliser 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...

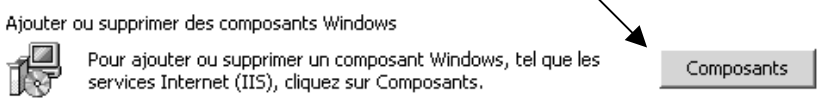
SERVEUR DHCP N.T.2000

Installer le Service DHCP :

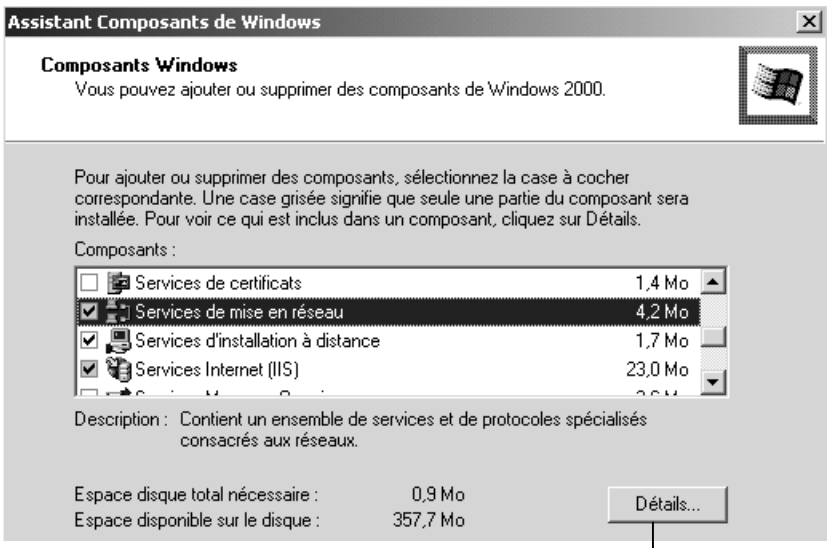
La gestion des adresses IP via DHCP ne peut se faire que sur une machine ayant une adresse IP fixe

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

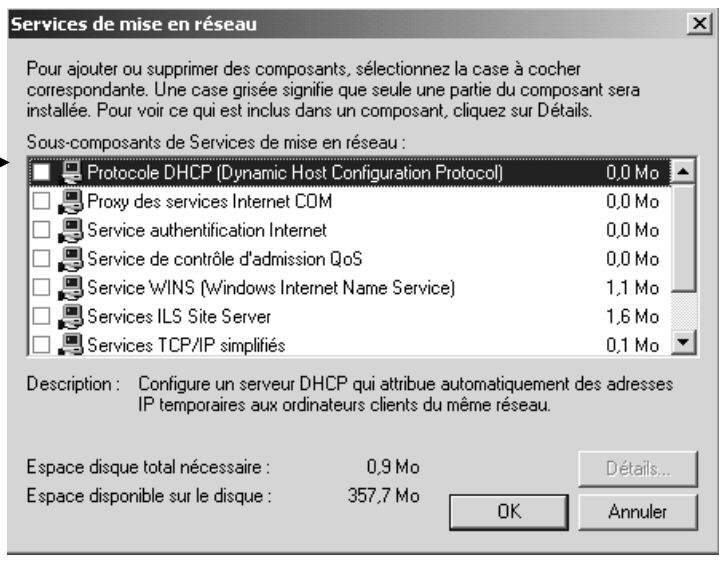
on clique sur composant



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



via Détails... on choisit alors **Protocole DHCP**

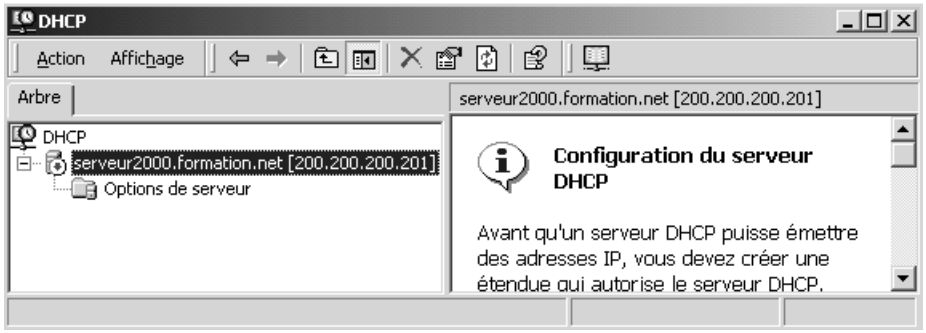


on revient et on fait suivant pour terminer l'assistant

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

Démarrer / Programmes / Outils d'administration / DHCP

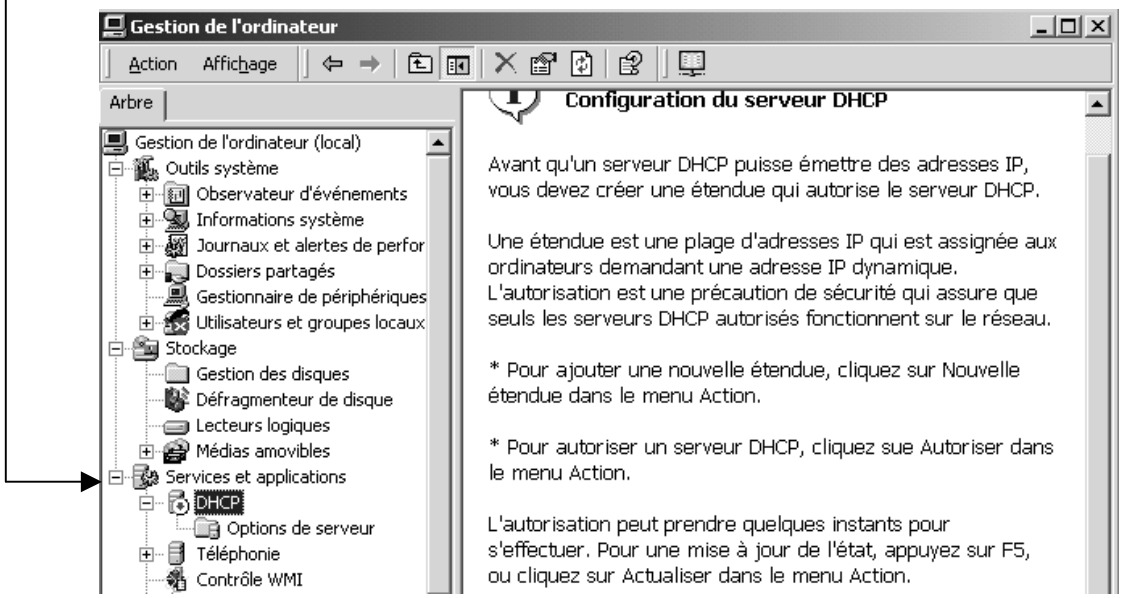
(et on a DHCP uniquement)



ou via

Démarrer / Programmes / Gestion de l'ordinateur

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



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 :

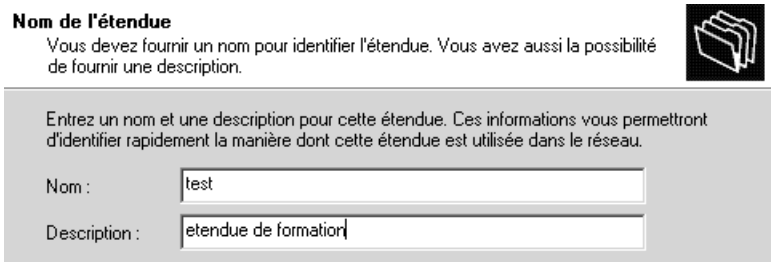
- Partage de la charge entre plusieurs serveurs DHCP.
- Attribution d'adresses IP spécifiques à un sous-réseau.

N.B : Une seule étendue peut être affectée à un sous-réseau spécifique.

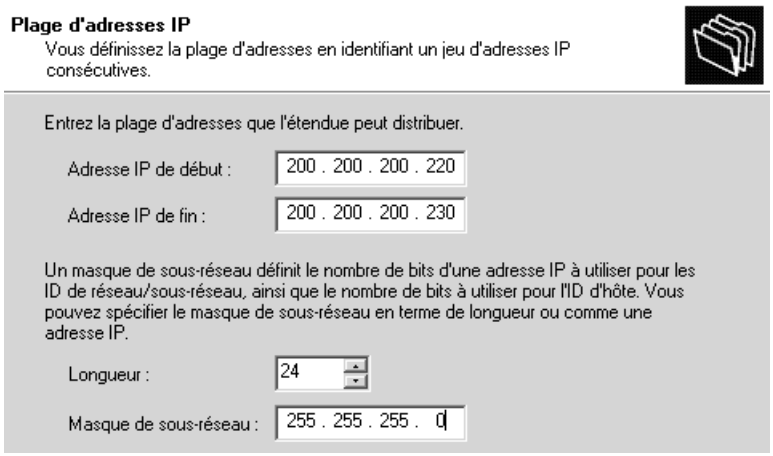
Pour créer une étendue Il faut se placer sur le serveur DHCP sur la gauche, et demander le menu **Action/Nouvelle Etendue...**

ceci déclenche un assistant qui va nous demander :

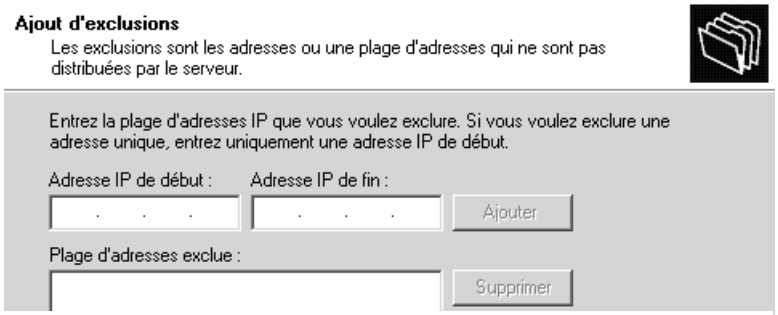
le nom de l'étendue



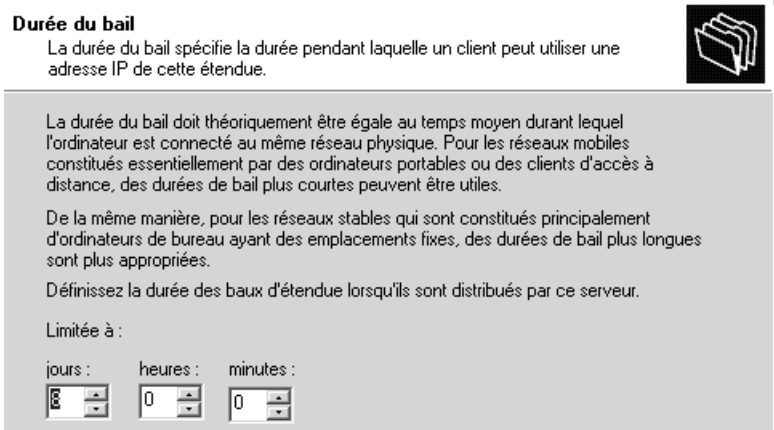
les plages d'adresses à attribuer



les éventuelles exclusions

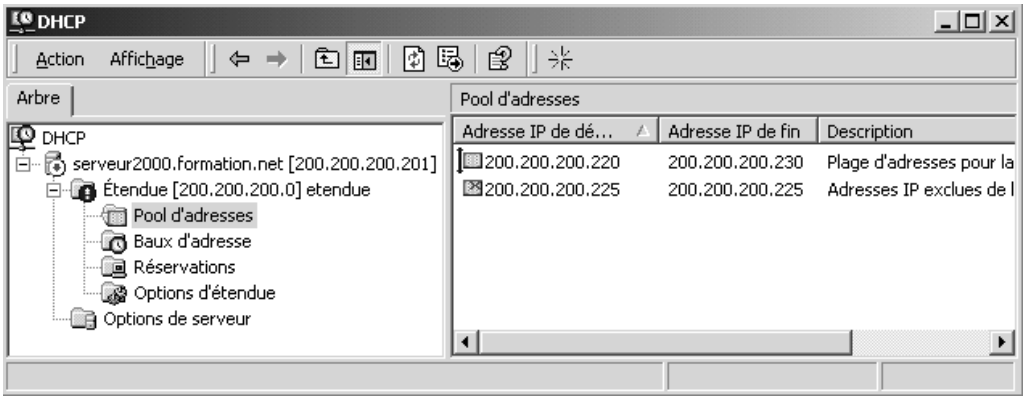


la durée du bail



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

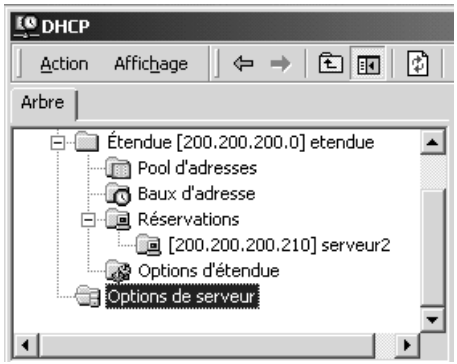
on obtient enfin

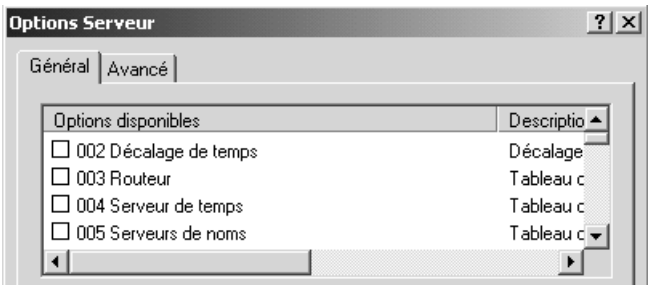


Configuration des options d'étendue DHCP:

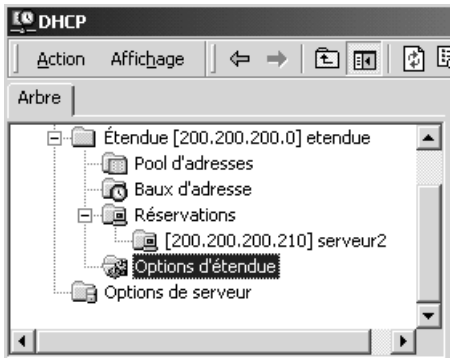
Une fois l'étendue DHCP créée, vous pouvez configurer des options pour les clients DHCP. Il existe trois niveaux d'options, nous nous limiterons à **Serveur**.

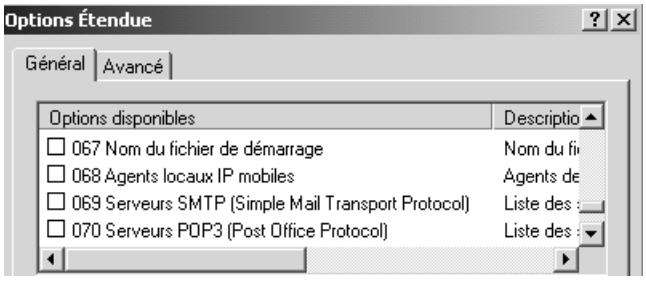
- **Serveur - Globales**: Les options de serveur sont disponibles pour tous les clients DHCP. Elles ont utilisés lorsque tous les clients de tous les sous-réseaux requièrent les mêmes informations de configuration. Par exemple, lorsque tous les clients utilisent le même serveur DNS.



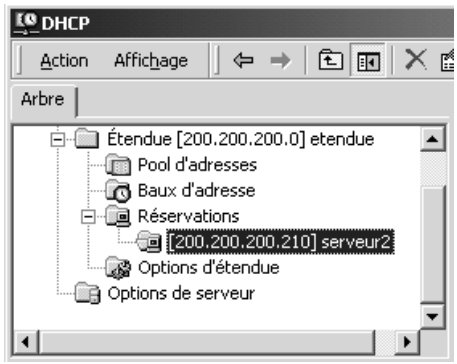


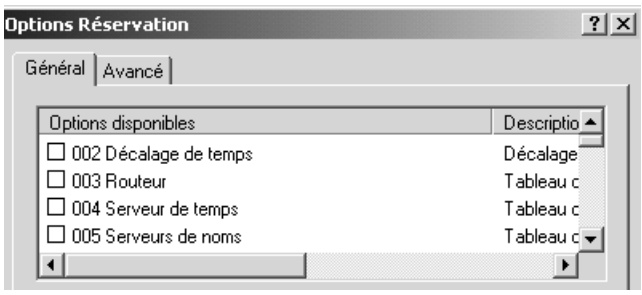
- **Etendue** : Les options limitées à l'étendue ne sont disponibles qu'aux clients dont l'adresse IP cédée par bail est issue de l'étendue. Par exemple, lorsque vous disposez d'une étendue distincte par sous-réseau, vous pouvez définir une adresse de passerelle par défaut pour chaque sous-réseau.





- **Reservation :** Les options limitées au client sont créées pour un client spécifique utilisant un bail d'adresse DHCP réservé.





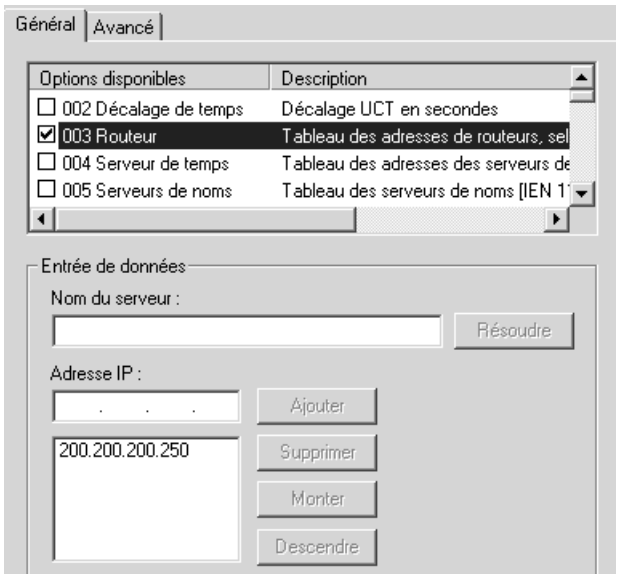
N.B: Priorité des options : Les options globales sont toujours utilisées, sauf si les options limitées à l'étendue s'appliquent. De même Les options limitées à l'étendue s'appliquent toujours sauf su des options limitées au client existent.

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

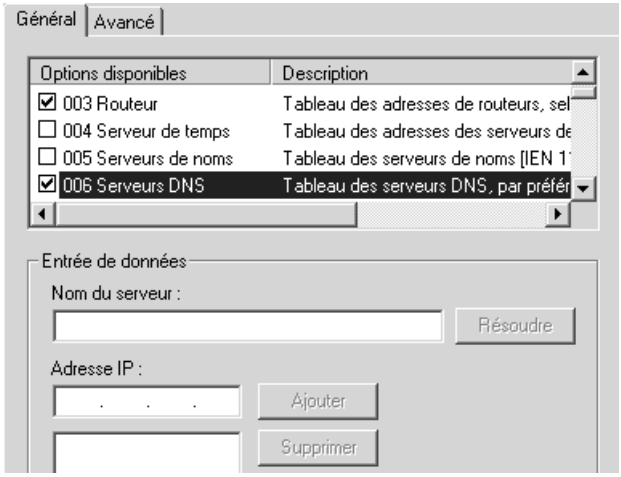
Dans la liste Options Disponibles, cochez l'option DHCP à configurer,:

Routeur :



Si besoin bien sûr…

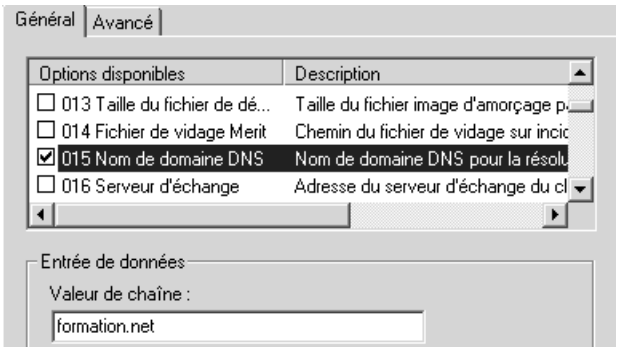
DNS :



Obligatoire si **DDNS** !

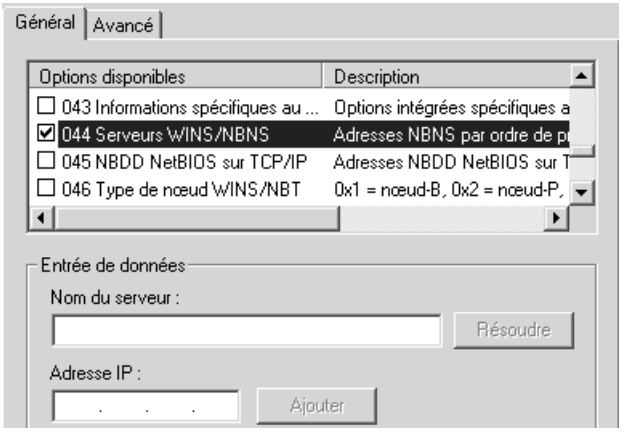
N.B : en général on y associe également l'entrée **15 Nom de domaine DNS (obligatoire si on utilise DDNS)**

Nom de domaine



Obligatoire si **DDNS !**

Serveur WINS



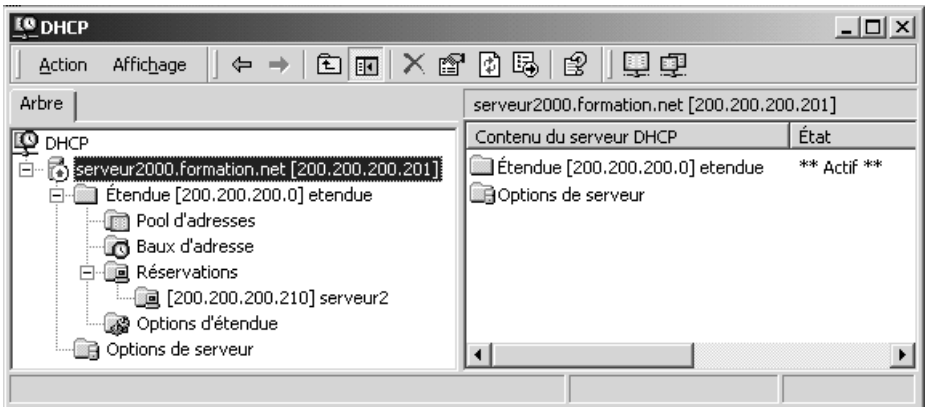
Si besoin bien sûr… et en général associé à

046 type de noeud ... **0x..**

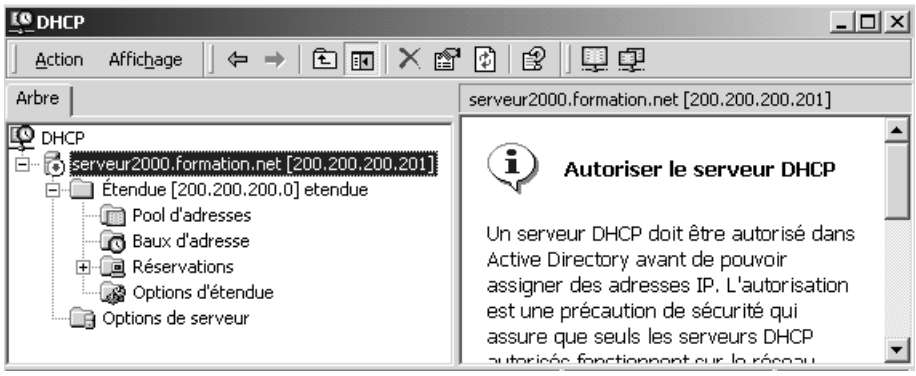
Autoriser / Interdire un serveur DHCP:

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

Action / Autoriser



Action / Interdire



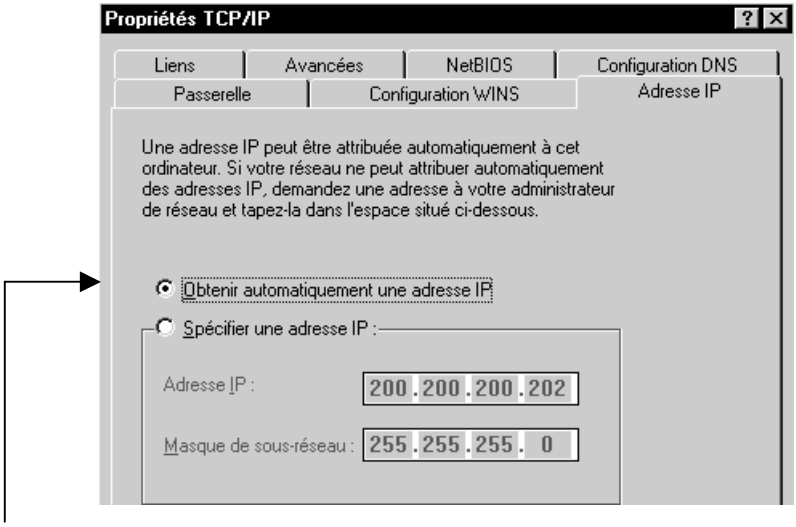
CLIENT DHCP

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



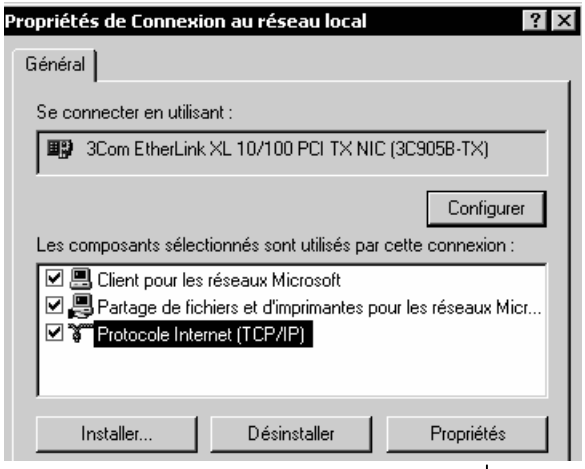
Lorsque on demande une adresse automatique, tout le reste du paramétrage IP devient "inactif"

Client DHCP NT 2000:

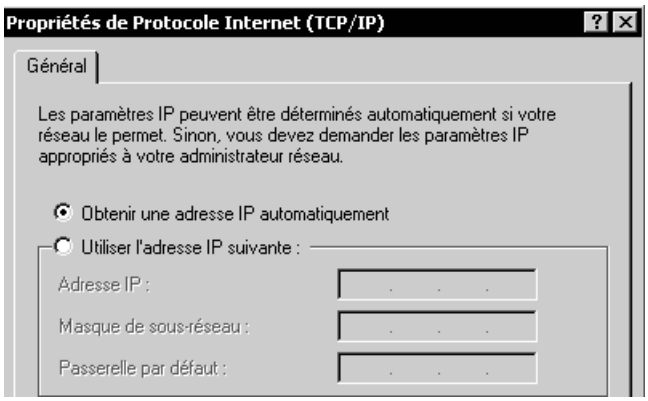
Un poste devient client DHCP simplement en demandant dans le paramétrage de TCP/IP « **Obtenir automatiquement une adresse IP** »

- 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 **/release /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 :

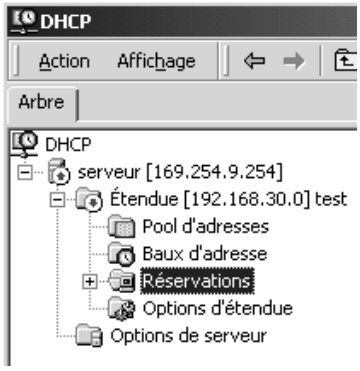
La fonctionnalité la plus importante, est celle de pouvoir connaître l'adresse Ip qui a été affectée à telle ou telle machine...

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.

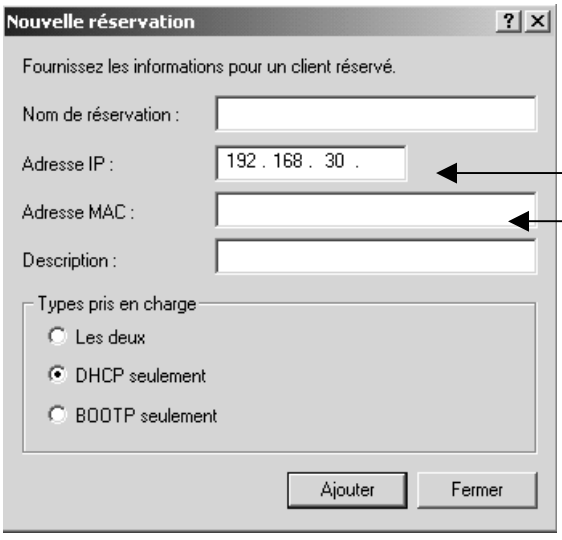
Reservation d'adresse :

Pour réserver une adresse, il est necéssaire 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 :

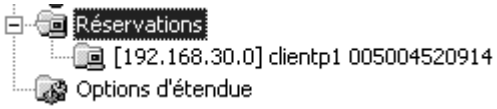
L'adresse ip

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

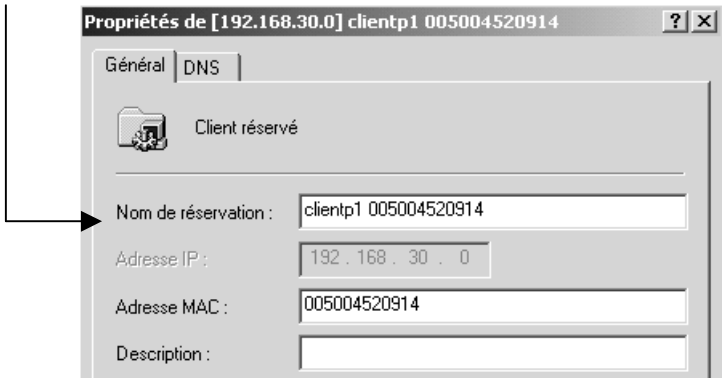
La reservation est faite. Désormais lorsque le poste ayant l'adresse physique xxxxxxxxxx fera sa demande d'adresse ip, il obtiendra toujours celle-là

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

Pour obtenir un affichage des reservation 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'interieur de system32. la sauvegarde s'effectue dans un dossier nommé backup/jet

Dossier DHCP en **system32\dhcp**

Dossier Sauvegarde en **\backup\jet**

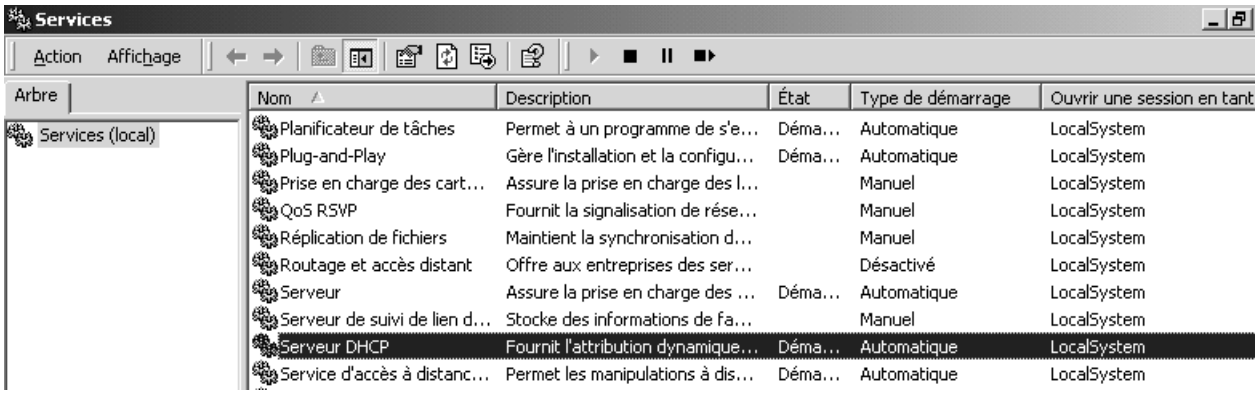
en cas de probleme detecté, win2000 peut essayer d'utiliser automatiquement cette sauvegarde.

Sauvegarde manuelle serveur DHCP :

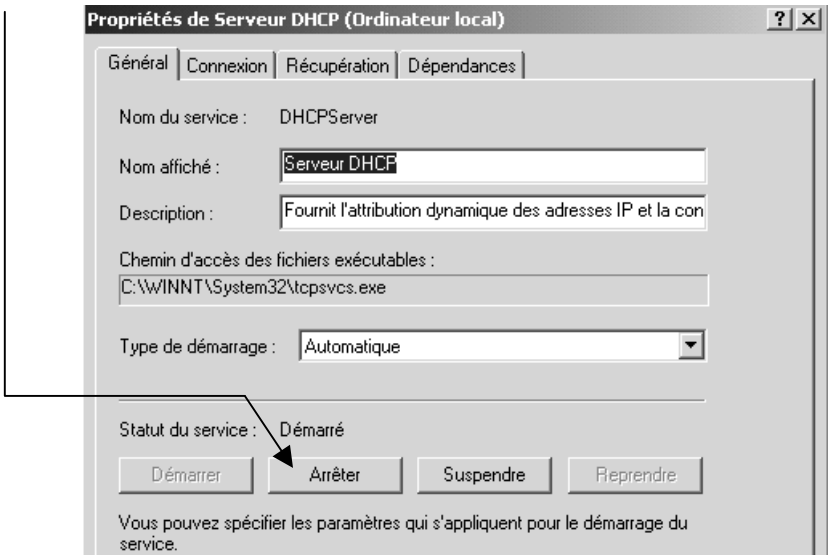
Il est possible de forcer une sauvegarde manuellement. Il va falloir arrêter le service DHCP, copier les fichiers de sauvegarde a leur emplacement d'origine, puis re-démarrer le serveur DHCP.

pour stopper le service dhcp on demande

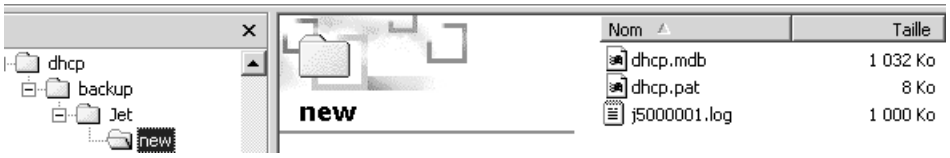
Programme / outils d'administration / services /



Dans les propriétés du service DHCP on arrête le service

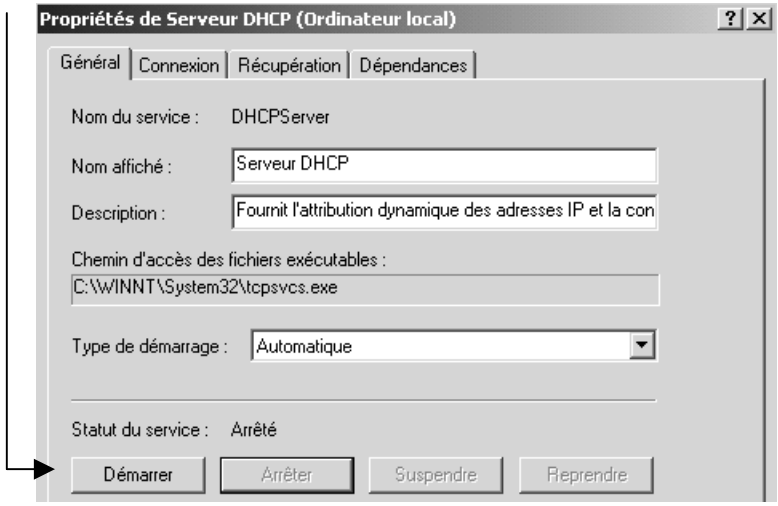


On copie le contenu du dossier **Winnt\system32\dhcp\backup\jet\new**



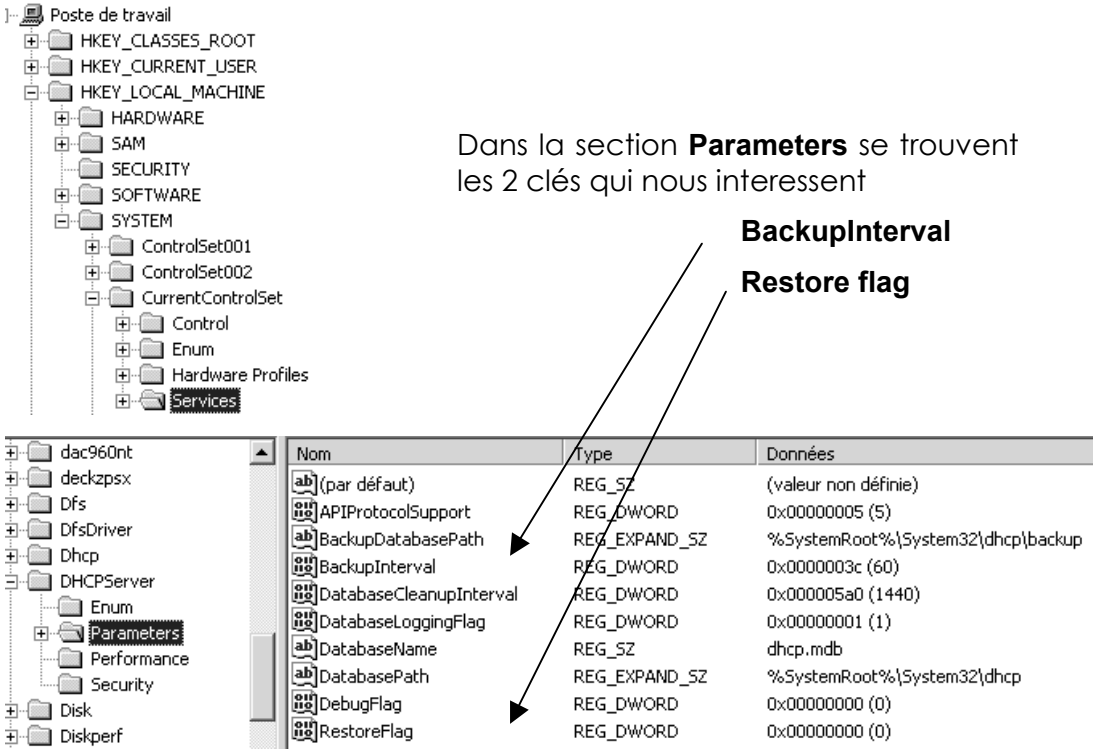
dans le dossier **Winnt\system32\dhcp**

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 combiens la restauration doit être effectuée.

Ici a été modifié à 10 mn...

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...

ADRESSES IP AUTOMATIQUES (APIPA)

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

DYNAMIC DNS WINDOWS 2000

Principe du DDNS :

Les systèmes prêts pour Windows 2000 exploitent une autre fonction DNS : DDNS. Lorsqu'un client Windows 2000 démarre, il demande à son serveur DNS local d'ajouter son nom dans la base de données. Même si les clients de versions antérieures à Windows 2000 ne savent pas demander au serveur DNS de les ajouter à la base de données de la zone, le serveur DHCP de Windows 2000 remplit cette tâche pour eux. Ainsi, même les anciens PC peuvent être ajoutés dynamiquement au fichier de zone

Pour utiliser cette fonction il faut travailler coté serveurs DHCP et Serveur DNS, mais aussi coté client, 2000 ou « autres ».

Coté serveurs DHCP & DNS :

Il faut effecteur une configuration sur les 2 serveurs conjointement :

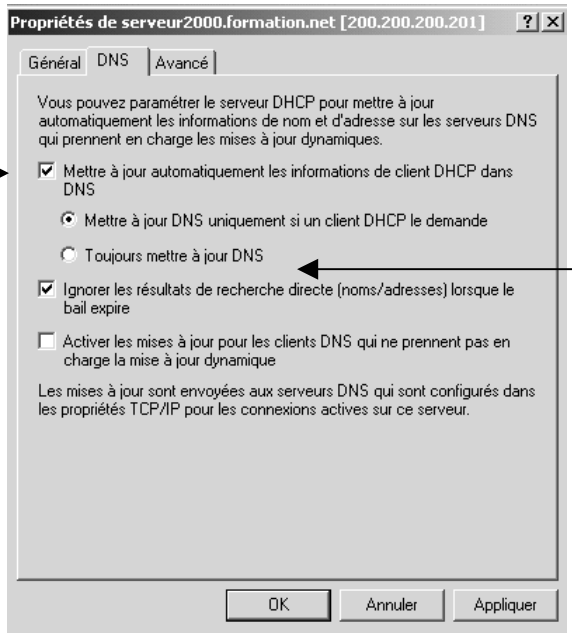
- Sur le **serveur DHCP** l'adresse du ou des **serveurs DNS à utiliser** pour cette opération, ainsi que le nom de domaine par défaut

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

- Un **serveur DHCP NT 2000** 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

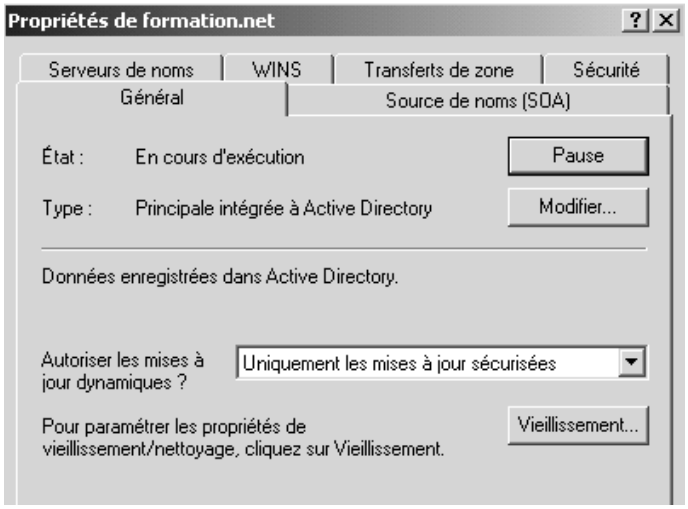


Donc, Par défaut un **serveur DHCP** NT2000 ***enregistre auprès du serveur DNS*** les **client DHCP** NT2000 qui en font la demande…

N.B : Si un client DHCP NT2000 avait sa case « demande d'enregistrement » non coché, on pourrait dans le serveur DHCP NT2000 demander de « **Toujours mettre à jour le DNS** »

- Sur le **serveur DNS** d'autoriser les mises à jours automatiques

Il faut demander le menu contextuel en étant dans la console sur DNS et demander **Propriété / onglet général**



Il faut autoriser les mises à jours dynamiques en

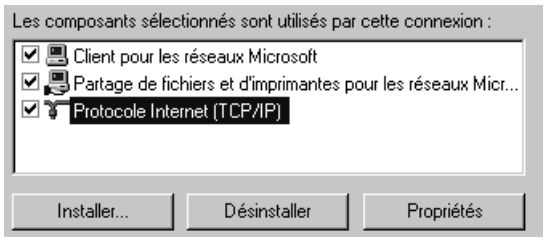
- "Oui" si on n'a pas intégré DNS à "Active directory"
- "Uniquement les mises à jour sécurisées" si le DNS est intégré à Active directory

---

Coté Clients:

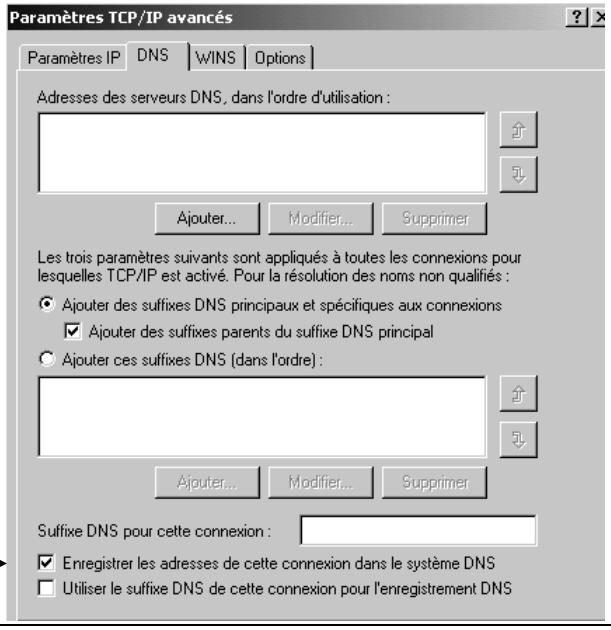
Fonctionnement standard depuis des machines NT2000 :

- Un **client DHCP NT 2000** est capable de demander la mise à jour dynamique de son enregistrement auprès du serveur DHCP. Son paramétrage <u>par défaut</u> 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** ...

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

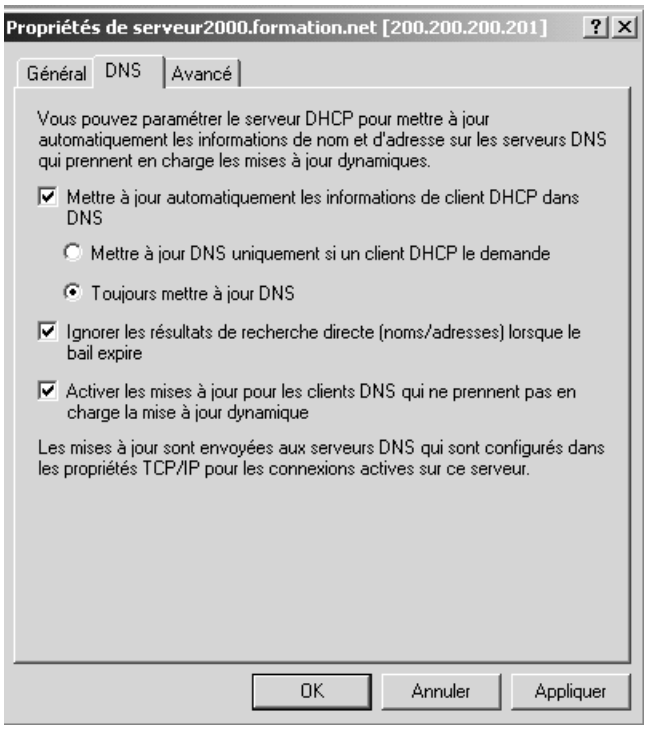
Fonctionnement depuis des machines « avant » NT2000 :

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**

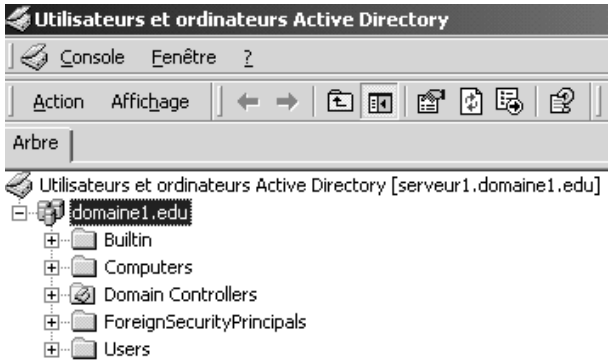


N.B: il est fondamental de distribuer par le DHCP deux paramètres qui sont le "*code 006 serveur DNS*" et le "*code 15 nom de domaine*". (cf chapitre DHCP)

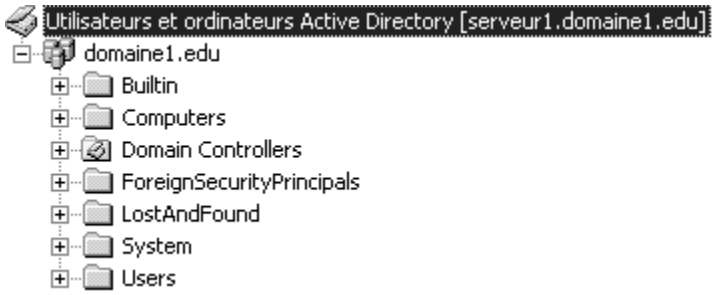
STRUCTURE PAR DEFAUT D'ACTIVE DIRECTORY

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 :

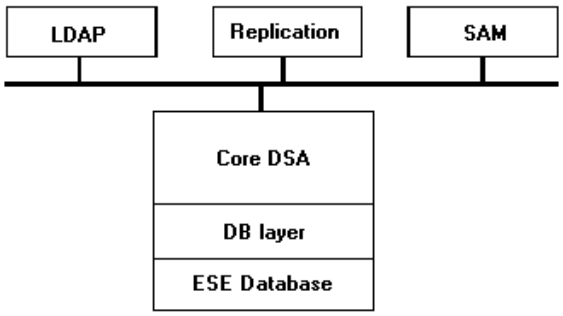
Le service Active Directory de Windows 2000 s'intègre dans le processus d'autorité de sécurité locale (**LSASS.EXE**) et peut ainsi gérer des informations confidentielles, telles que des mots de passe de comptes

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 9x avec le package client Active Directory.

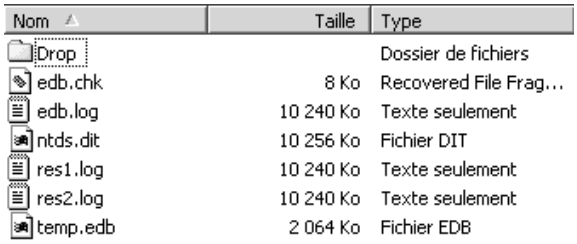
L'interface de Réplication assure la réplication d'annuaires avec d'autres contrôleurs de domaine Active Directory.

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*).

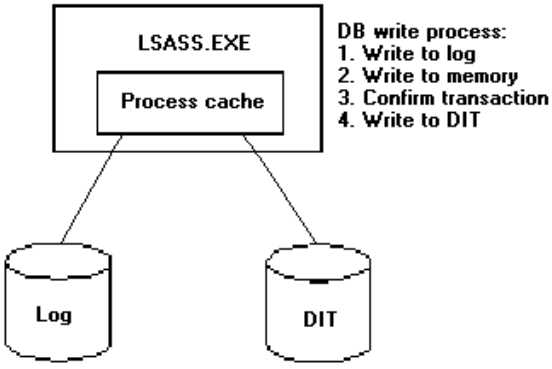
La base de données Active Directory est stockée dans le fichier **Ntds.dit** et des journaux de transactions sont stockés dans les fichiers **.log**



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

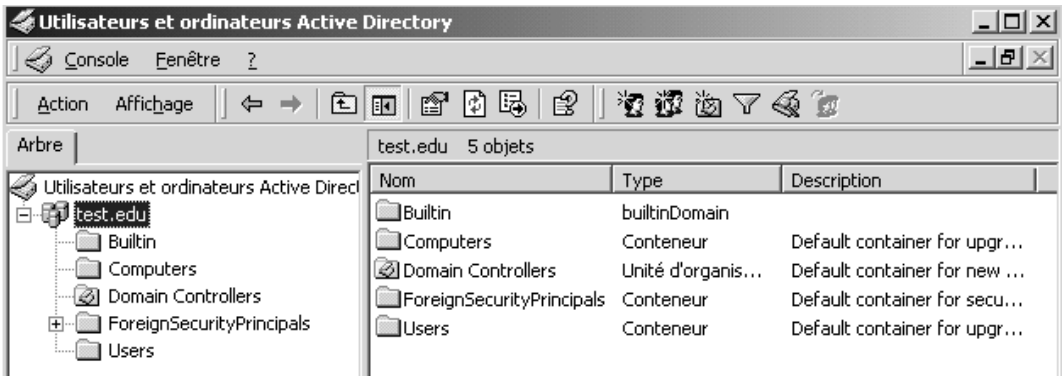
Les paramètres de stockage de la base de données Active Directory sont relativement prévisibles. De nombreuses sociétés n'atteindront peut-être jamais un annuaire de 100 000 utilisateurs et il convient donc de noter que (du point de vue de l'utilisation de l'espace disque) les besoins en matériel du 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

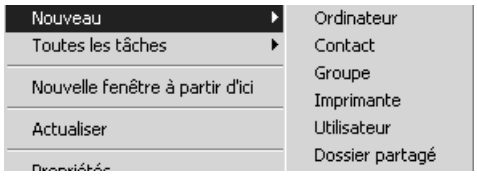
PUBLICATION DANS ACTIVE DIRECTORY

Publication d'un dossier partagé :

Il faut lancer la console Utilisateur et ordinateur Active Directory

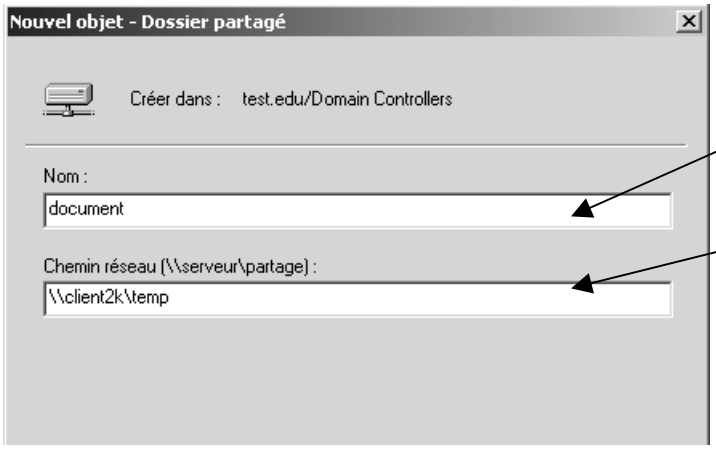


se placer dans l'arborescence là où l'on veut créer notre objet puis



ici par exemple un dossier partagé

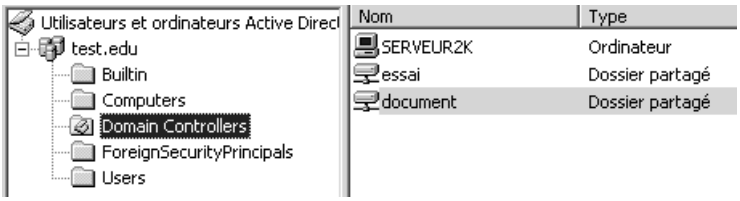
ce qui amène la boite suivante



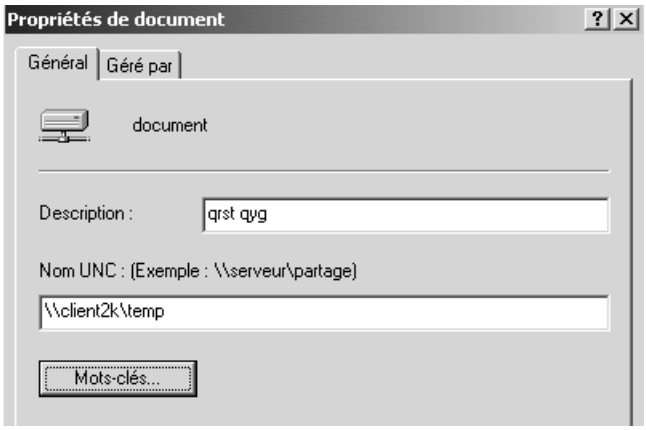
On indique le nom de l'objet que l'on publie

Et bien sûr on donne son chemin réseau….(une machine 2000 quelconque, mais ni windows98- ni NT4.0 !)

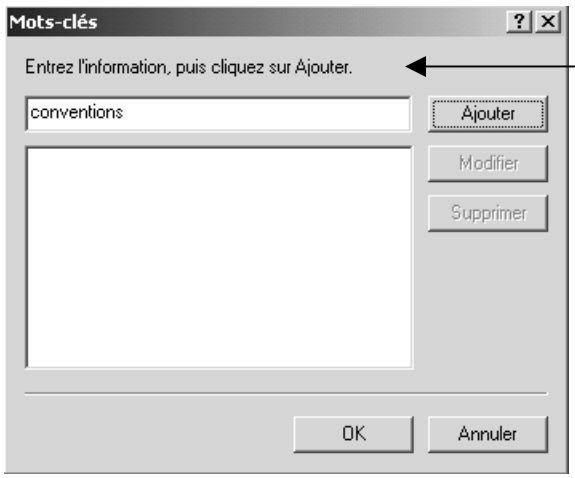
mon dossier partagé est "publié" désormais dans Active Directory



un double clic dessus, me permet de le paramétrer :

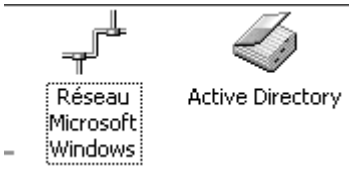


avec des mots clés :



Recherche d'un dossier partagé publié dans AD:

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

la recherche avec Active Directory se présente différemment

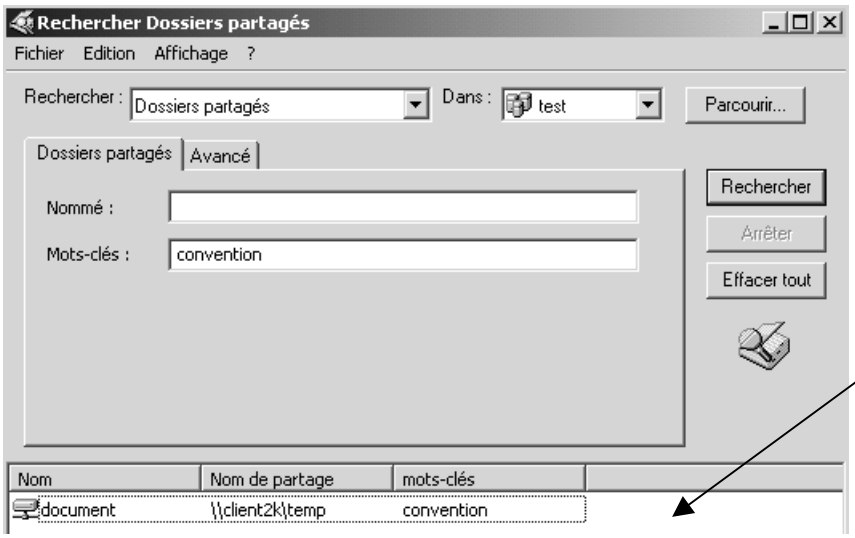
dans Active directory

clic bouton droit sur mon domaine, **rechercher…**

Je donne mon mot clé…

Et avec **Rechercher…**

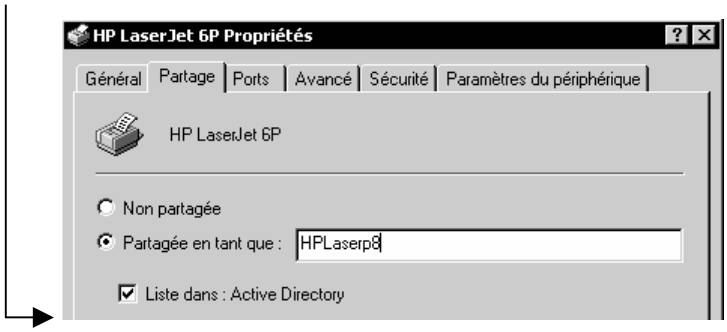
On obtient



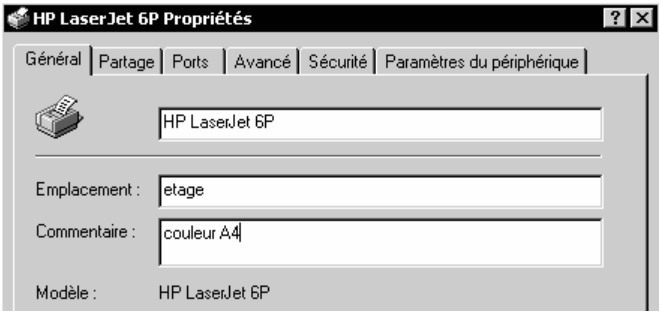
Publication d'une imprimante partagée sous 2000:

Sur un poste 2000, 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…

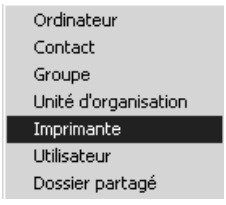


Publication d'une imprimante partagée sous windows95:

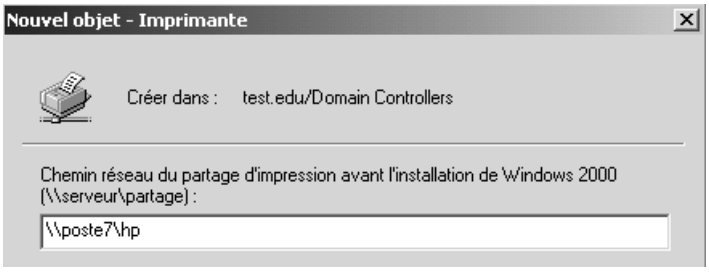
Sur un poste windows 95-98, ayant une imprimante installée localement,

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



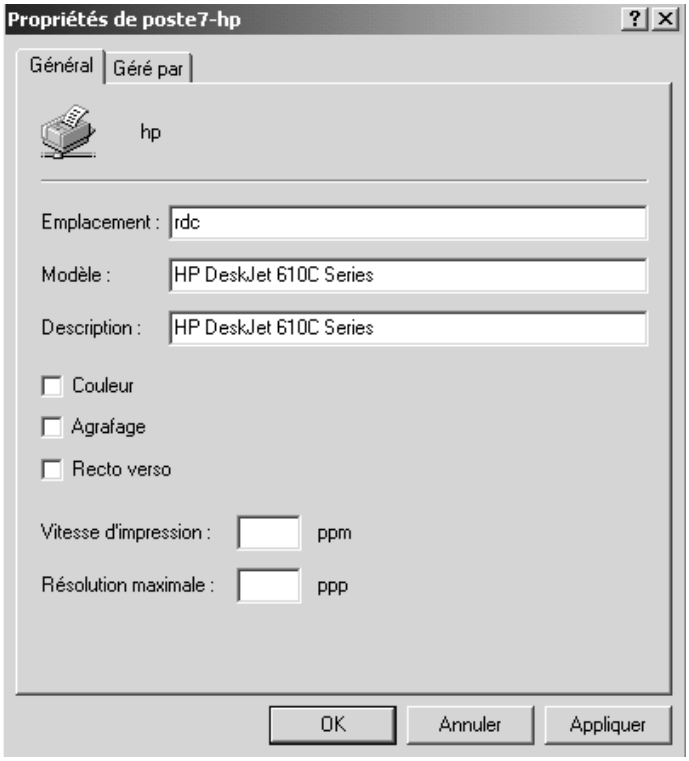
on obtient alors



on indique le chemin →

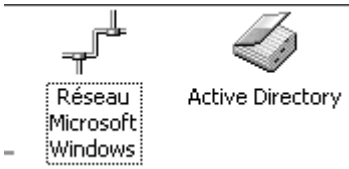
l'imprimante est "publiée"

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



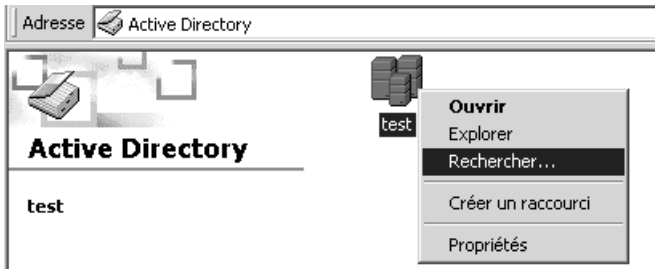
Recherche (voir) une imprimante publiée dans AD :

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 le nom du workgroup + nom machine + nom de partage de mon imprimante (système analogue a celui de la recherche d'un dossier partagé)

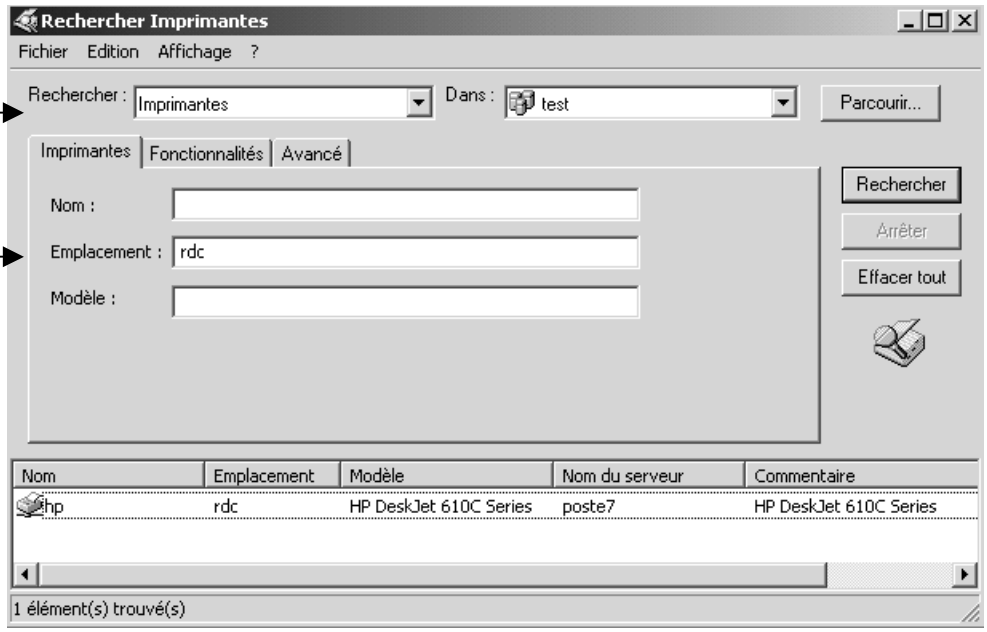
La recherche dans Active Directory se veut différente :



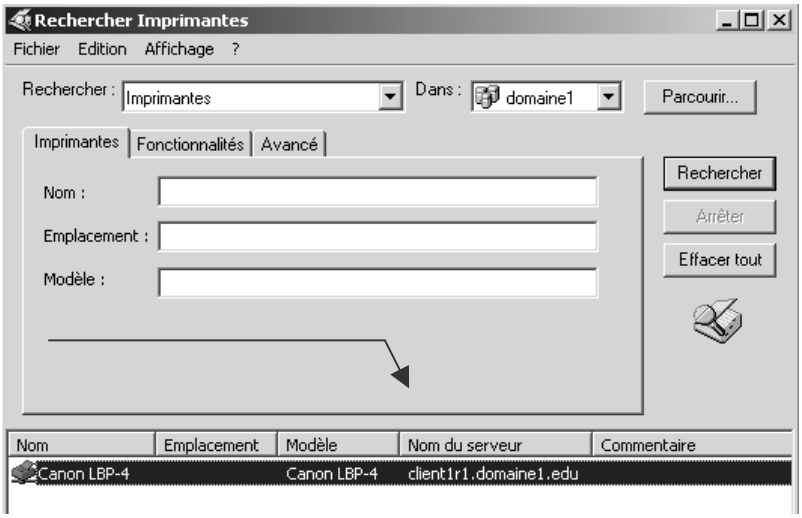
Et avec **Rechercher… Imprimante**

Et un mot clé

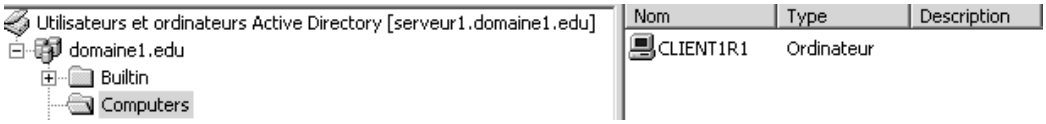
On obtient



N.B : 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 AD



Pour cela il faut demander le menu **Affichage / Utilisateurs, Groupes et Ordinateurs en tant que conteneur** qui amène

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 (voir chap admin à distance page 216)
- 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 :

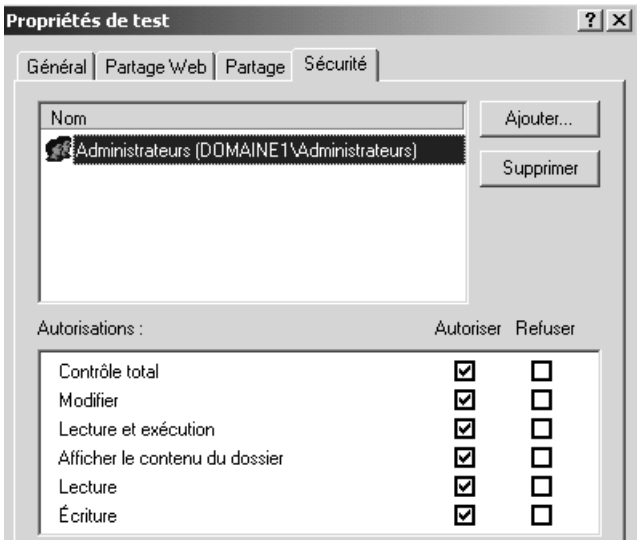
- Tous les postes 2000 utilisent AD
- Tous les clients windows 95-98 et NT4.0 peuvent effectuer des recherches plus sommaires s'ils ont installé les outils client AD (voir chap client-98-NT & AD page 91)

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**.

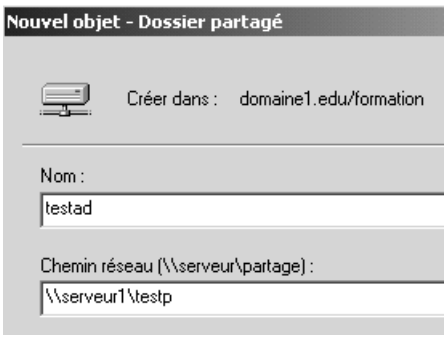
Permissions des Ressource partagée :

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,

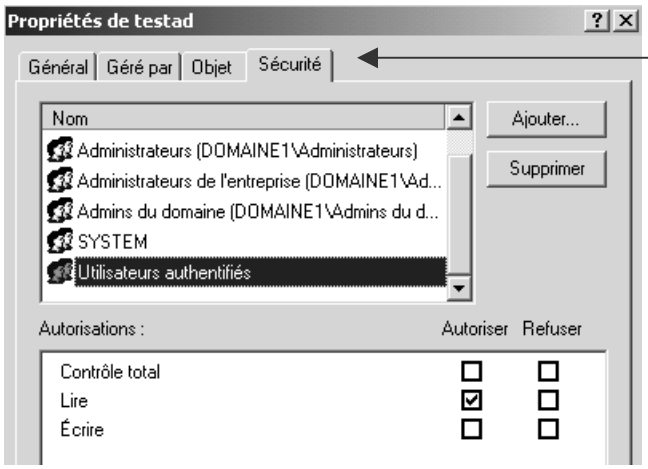


Permissions des Objets Publiés :

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**

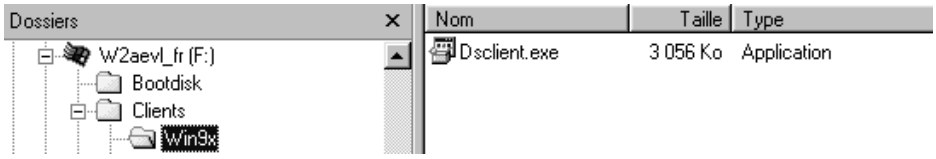
N.B : pour les objets publiés par défaut, ils seront toujours accessible à travers la recherche dans AD. Par contre pour les objets publiés manuellement (pas par l'installation par défaut) si la permission lire n'est pas donnée, ces objets n'apparaîtrons pas lors d'une recherche

(par exemple pour ce 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 publié ne donne rien, alors que si je suis logué en tant qu'administrateur, le même recherche aboutira…)

CLIENTS 95-98-NT & ACTIVE DIRECTORY

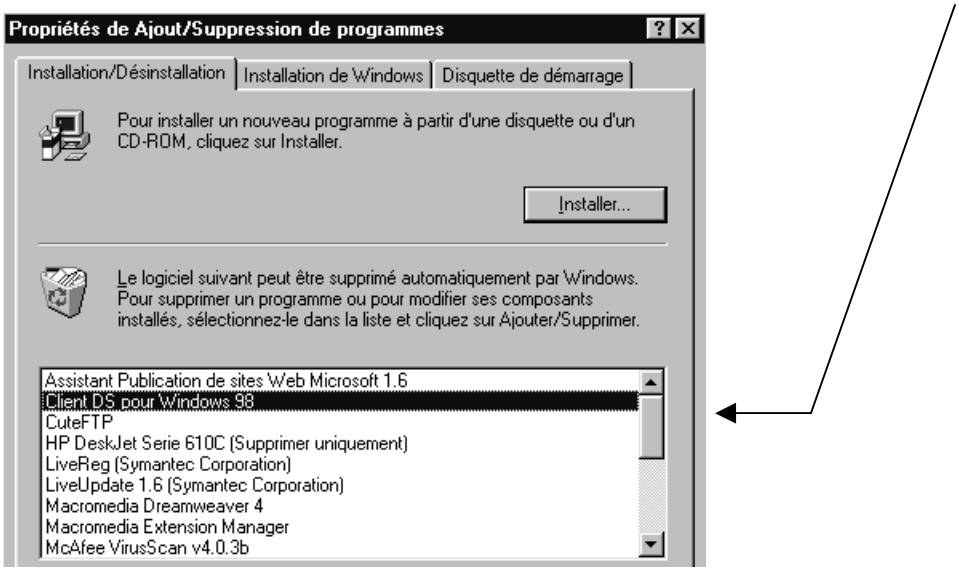
Extensions Client 95-98 Active directory :

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

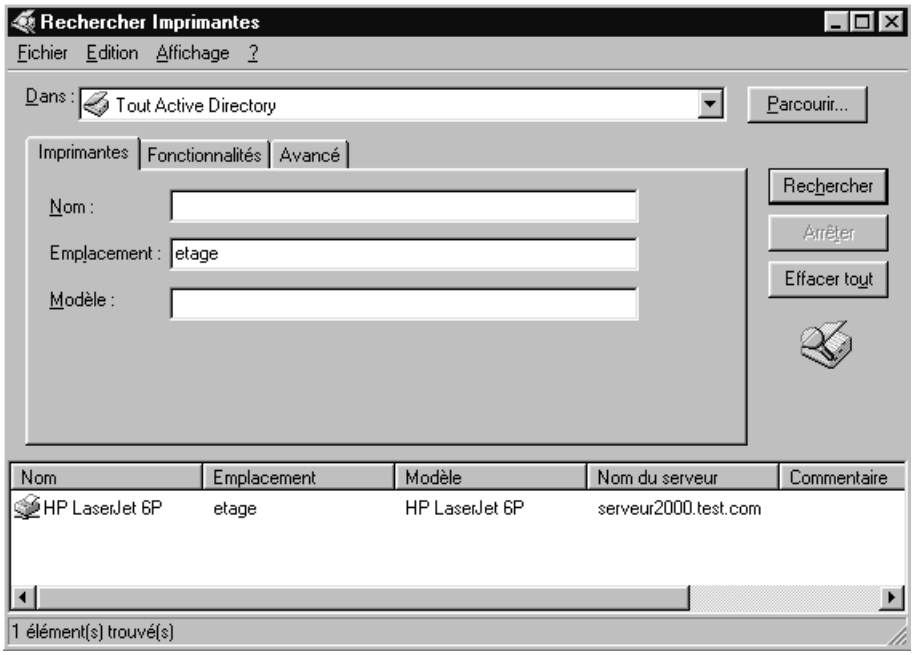


N.B: Ne pas oublier de faire que le client soit bien déclaré dans le DNS du domaine, (sur le serveur) et que son paramétrage IP indique le DNS du domaine…

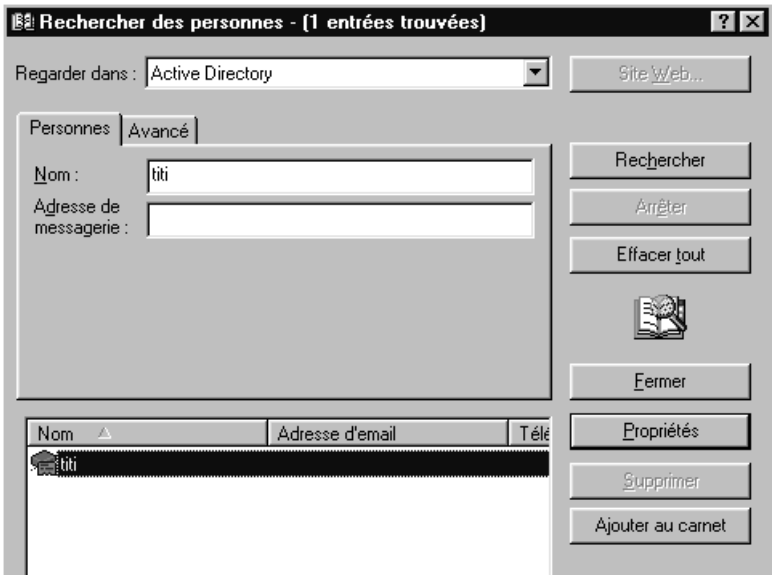
Utiliser Active Directory depuis 95-98 :

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

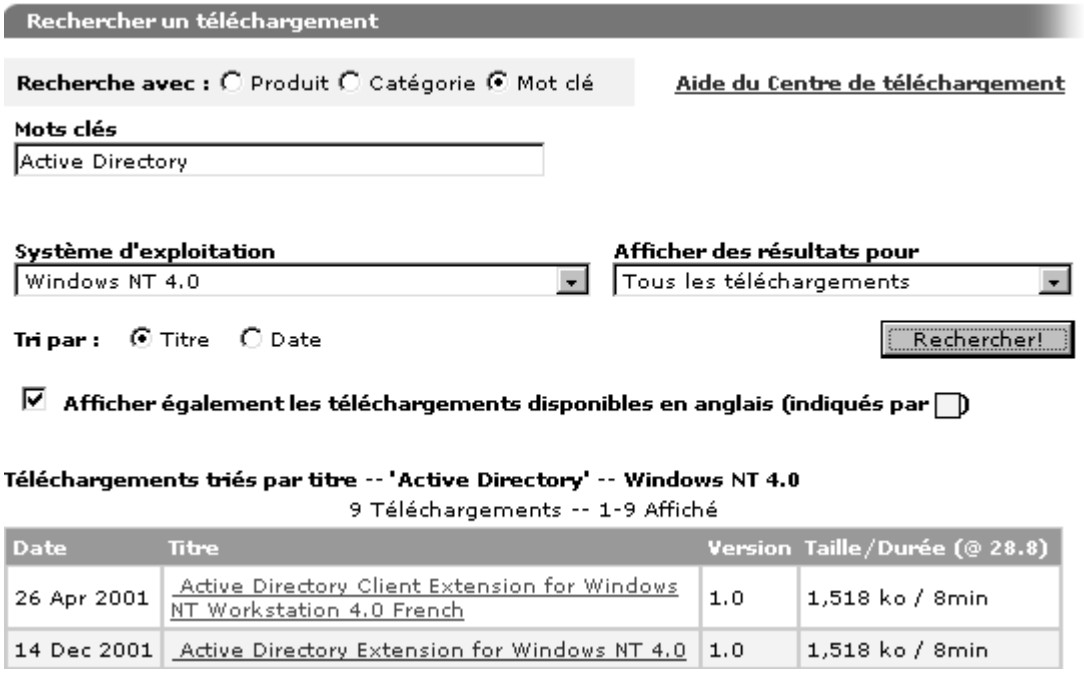


et la recherche des personnes s'étoffe quelque peu…



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 :

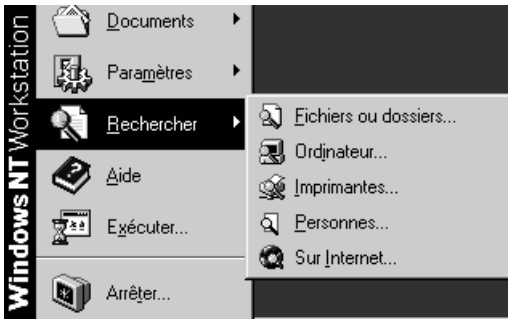
- le sp6 doit être installé
- IE ver 4.0 minimum doit être installé

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

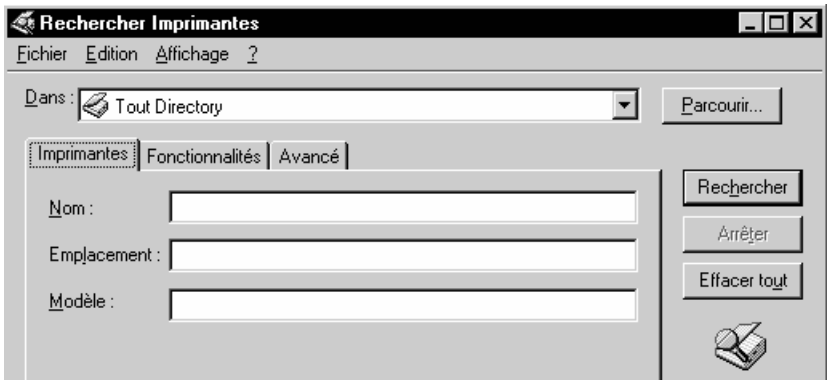
qui amène à …

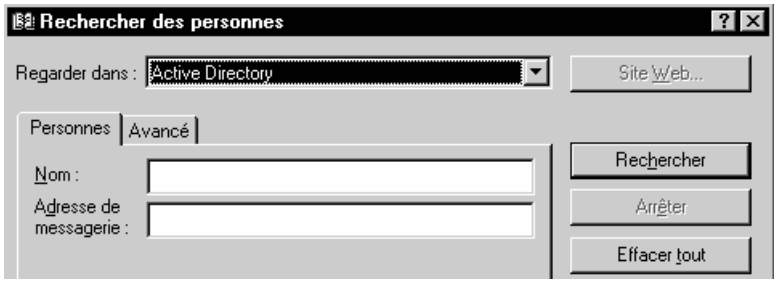
Utiliser Active Directory depuis NT4.0 Wks :

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



avec comme pour les client windows



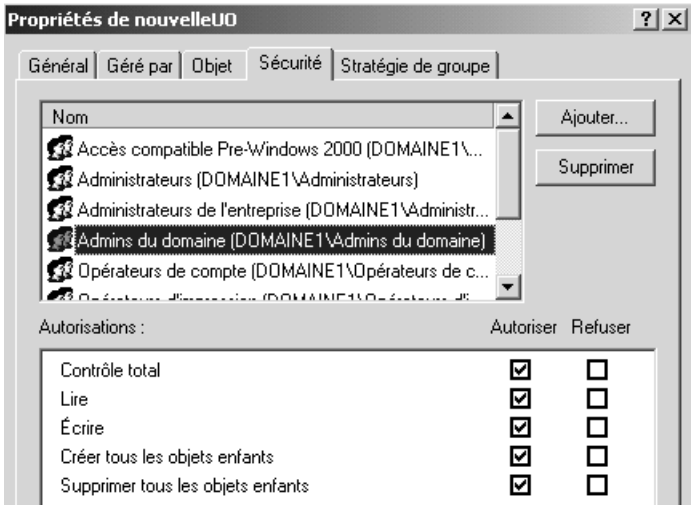


Encore faut il que cette station NT soit rattachée au domaine 2000 sur lequel on effectue une recherche avec Active Directory…!

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**

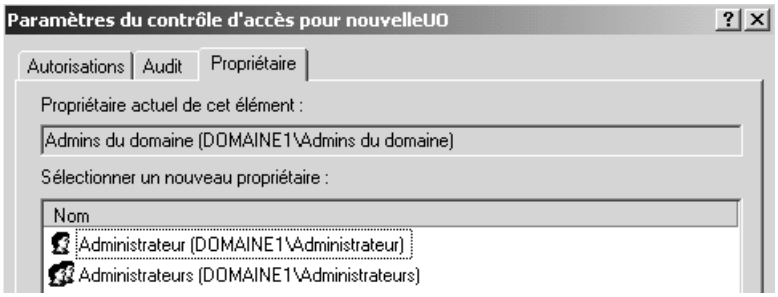


NB : la gestion des permissions se fait de manière identique a celle des permissions NTFS…

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 :

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 :

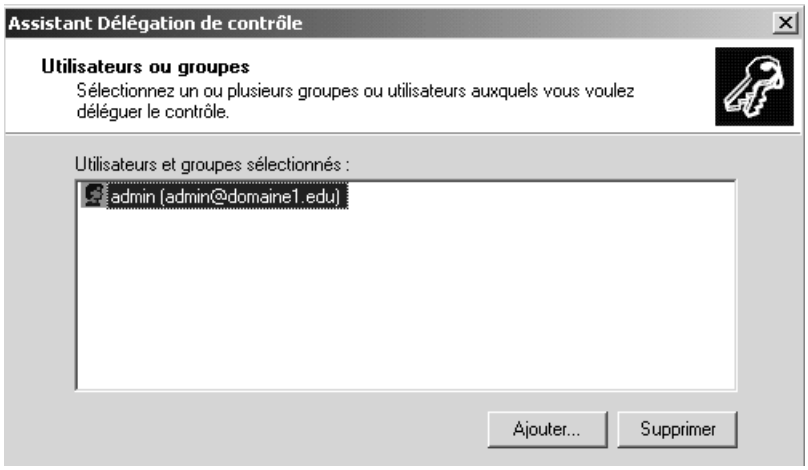
- Délégation de compétences au niveau d'une OU via l'assistant (conseillé)
- Attribution d'autorisations spécifiques sur des OU ou des objets (déconseillé)

On ne traitera ici que de la délégation de compétence 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**

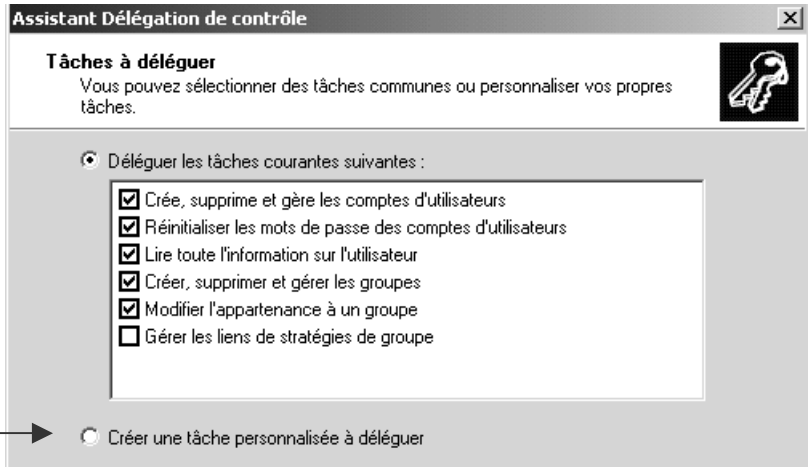
L'assistant se déclenche alors et nous demande successivement :

Pour qui on souhaite effectuer la délégation



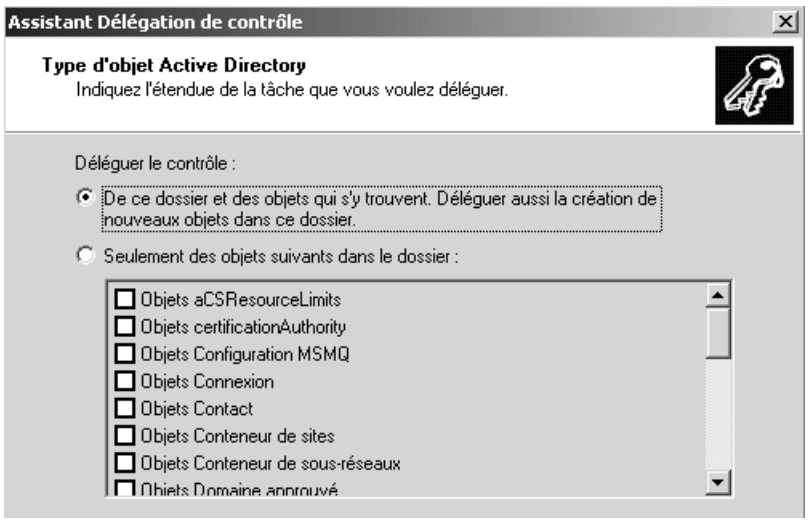
Si on veut accepter une tâche pré-définie, il suffit de choisir…

Sinon il faut cocher



Dans ce cas

Le plus simple est de déléguer un contrôle total…



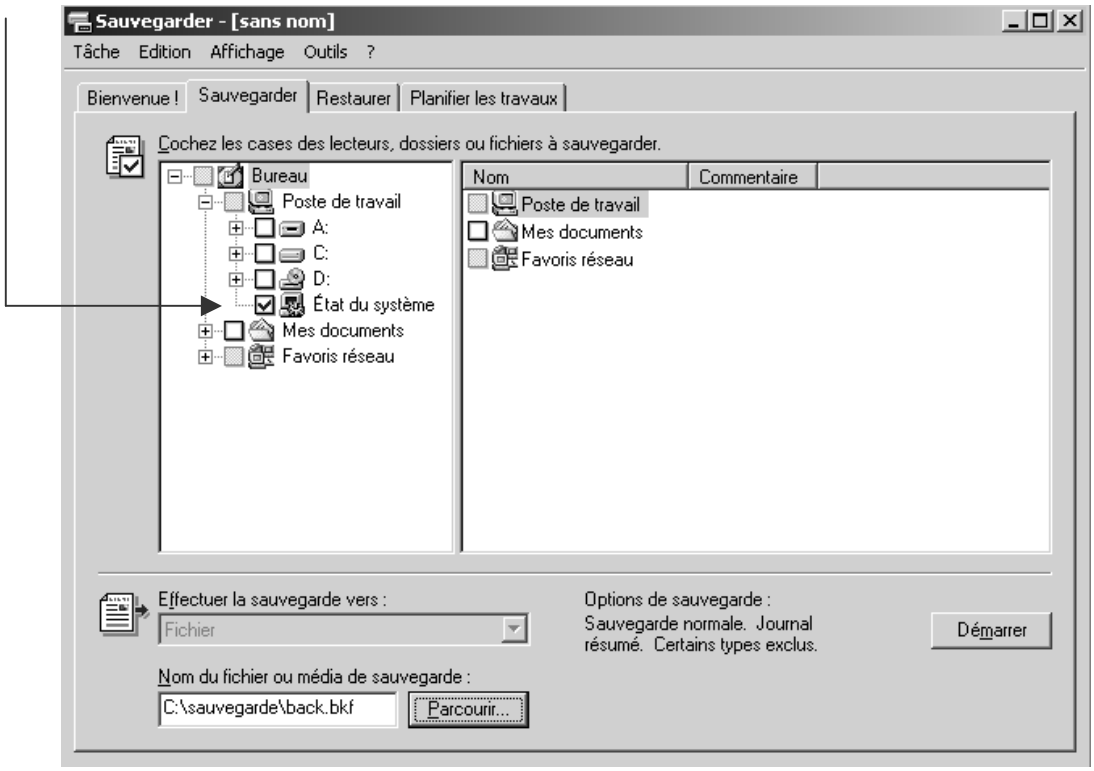
SAUVEGARDE-RESTAURATION DE A.D.

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 CD. (on verra plus loin la technique de duplication entre deux CD…)

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



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 !

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.

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 identifier comme **administrateur restauration service d'annuaire**
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 identifier 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 modifier par la replication 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, 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 **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 — **Restore database**

   Seulement une OU — **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

REPERTOIRE DE BASE

Répertoire de base ou d'Accueil :

Il peut être intéressant de fournir pour chaque utilisateur, un répertoire par défaut dans lequel les commandes de type **Fichier / Ouvrir** ou bien de type **Fichier / Enregistrer sous** iraient correctement se placer.

Ce répertoire par défaut, nommé répertoire de base ou répertoire d'accueil, peut être :

- placé sur la station locale où l'utilisateur ouvre sa session (on parle alors de « chemin local »)
- ou mieux, il peut être placé sur le serveur (on parle de « connecter »)

Si le client ouvre une session sur une machine de type 2000, un lecteur logique l'amenant directement sur son répertoire peut être automatiquement crée.

Si le client ouvre une session sur une machine de type windows 95-98, pour créer automatiquement un lecteur logique l'amenant directement sur son répertoire, il faut alors créer un script de connexion (voir script page)

Mise en Place :

Un certain nombre d'opérations doivent être effectuées, certaines avant la créations des comptes utilisateurs, et d'autres pendant la création de ces comptes.

Avant la création des comptes

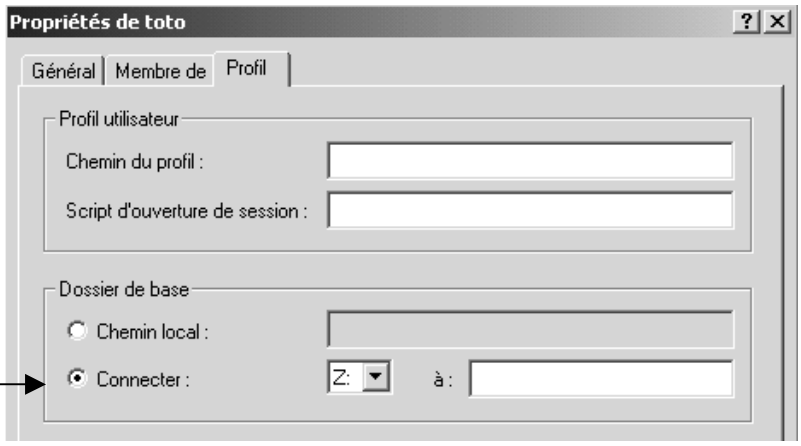
Il faut se créer la structure de rangement :

- Créer le dossier "racine" de la future arborescence pour les dossiers des utilisateurs, nommé par exemple **ressources (**mais il ne faut pas se créer soi-même les dossiers utilisateurs à l'intérieur ! **sauf si ce dossier est sur un volume FAT)**
- Il faut ensuite partager ce dossier **Ressource** en donnant une permission de type contrôle total à tous les utilisateurs à même d'y venir par la suite 

  N.B : par sécurité il vaut mieux donner contrôle total au **groupe Utilisateurs** plutôt qu'au **groupe Tout le monde**…ainsi seuls les utilisateurs ayant des comptes de domaine peuvent accéder au dossier partagé !

Pendant la création d'un compte

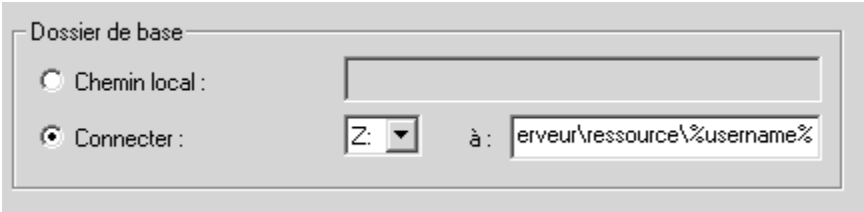
Lorsque ensuite l'on crée un compte Utilisateur, il faut demander les propriétés et demander l'onglet **Profil,**



Dans la boîte de dialogue il faut donner un nom et un emplacement au **dossier de base**, et choisir **Connecter**, puis choisir une lettre de lecteur logique associée à ce répertoire de base

N.B: si on utilise la variable **%username%**, celle-ci sera automatiquement remplacée par le nom de l'utilisateur qui à ouvert une session, et créera automatiquement un dossier du même nom

Ce système permet de créer un compte « modèle »



Noter que dans l'écriture du type:

\\serveur\ressource\%username%

on à selon les conventions de nom les valeurs suivante :

\\Serveur	nom d'identification du serveur sur lequel on crée les dossiers de stockage
\ressource	nom du dossier "racine" des dossiers de chaque Utilisateur. C'est le seul que l'on crée !
\%username%	Variable système prédéfinie

Résultat :

Si on crée un répertoire de base pour les utilisateurs, la structure suivante va se créer automatiquement au fur et à mesure de la création des comptes :

N .B : si le dossier est dans un support NTFS, lors de la première connection de cet utilisateur, un dossier à son nom sera créé dans ressources avec des droits **pour cet utilisateur et l'administrateur** uniquement

N .B : si le dossier est dans un support FAT, lors de la première connection de cet utilisateur, le dossier à son nom ne sera pas crée (**il faut le faire au préalable**, pour chaque utilisateur…)

Modifier le répertoire de base :

Il n'existe aucun moyen de modifier simplement de dossier de base pour plusieurs utilisateurs, si ce n'est de sélectionner tous les utilisateurs dont on veut modifier le dossier d'accueil, puis d'effectuer la modification

Rappels :

on peut trier les utilisateurs par leur nom, mais aussi par leur nom détaillé, (menu **Affichage /tri** dans le gestionnaire des utilisateurs…)

on peut en sélectionner plusieurs par la touche **CTRL**,

on peut en sélectionner tout un "paquet" en cliquant sur le 1°, en maintenant la touche **MAJ** appuyée, et en cliquant sur le dernier…

---

remarques sur le répertoire de base :

A noter que le répertoire de base est le répertoire dans lequel le profil des utilisateurs win 95-98 est stocké, lorsque l'on utilise cette fonctionnalité…

par conséquent un script permettant de créer un lecteur logique sur un autre répertoire de base lors de l'ouverture de session paraît à priori fort souhaitable…(voir script page 103)

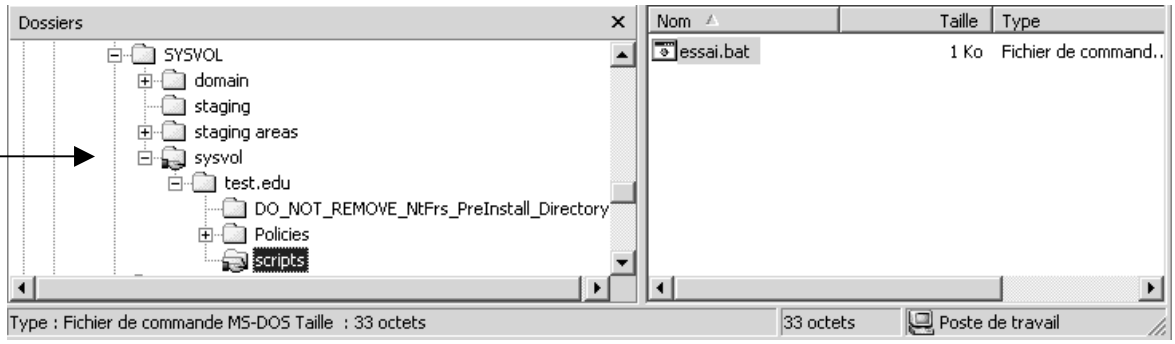
SCRIPT D'OUVERTURE DE SESSION

Objectif :

Un script d'ouverture de session est un fichier qui est exécuté chaque fois qu'un utilisateur ouvre une session. Il peut s'agir d'un fichier de commandes (portant une extension de nom de fichier**.bat** ou **.cmd**) ou d'un programme exécutable (portant une extension de nom de fichier**.exe**).

Un script d'ouverture de session est un fichier qui est exécuté chaque fois qu'un utilisateur ouvre une session. Il peut s'agir d'un fichier de commandes (portant une extension de nom de fichier**.bat** ou **.cmd**).

Pour les ordinateurs clients exécutant Windows95-98 ou WindowsNT4.0 ou Windows2000, le chemin d'accès du script d'ouverture de session sur un serveur 2000 est **Winnt\Sysvol\sysvol\domaine\scripts**. (sous NT4.0 server le chemin était généralement **Winnt\System32\Repl\Import\Scripts**.)



N.B: sous 2000, les client 2000 peuvent recevoir en plus a l'ouverture de session, une notion de stratégie. Ce qui fait que si un client est une machine windows95-98, ou NT 4.0, on ne peut travailler **qu'avec des scripts** (les stratégies 2000 ne marcheront pas pour ces clients), mais si un client est un poste 2000, alors celui-ci récupère lors de l'ouverture de session **les scripts et les stratégies 2000**…

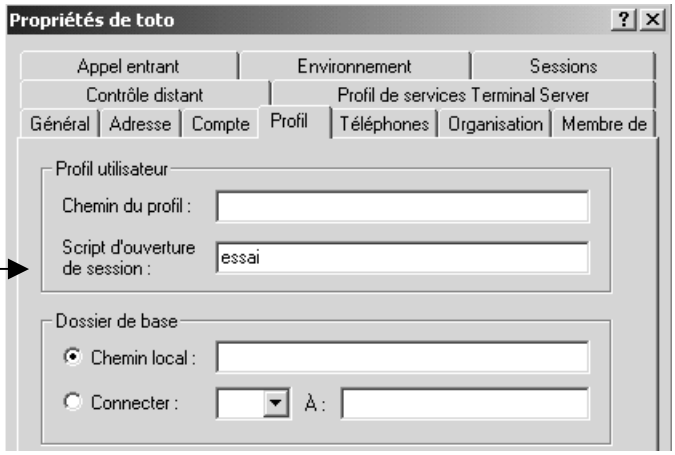
N.B : Si enfin, on utilise des stratégies sous NT4.0, (avec poledit), ces stratégies sont récupérées par les versions NT4.0 et win95-98, mais ne sont pas récupérées par les clients 2000…. Heureusement !

Indiquer un script d'ouverture de session :

Pour chaque utilisateur, il est possible d'indiquer le nom d'un script d'ouverture de session , dans les paramètres des utilisateurs, en demandant Profil

tapez le nom de fichier à exécuter (sans **.bat**) dans la zone Nom du script d'ouverture de session :

essai



Si le script d'ouverture de session se trouve dans un sous-répertoire du chemin de ce script, indiquez son **chemin relatif** avant le nom du fichier, par exemple s'il se trouve dans un dossier nommé **actuels** alors il faut entrer **actuels\essai** :

Ecriture de scripts :

Il existe parfois de légère (et parfois importantes) différences de syntaxe entre l'implémentation des commandes sous environnement 2000 et sous environnement windows 95-98…et la moindre erreur dans la syntaxe d'une commande fait que celle-ci ne s'exécute pas…

par conséquent il est tout à fait conseillé de tester localement un script dans l'environnement de destination, pour vérifier son bon déroulement, avant de le mettre à disposition sur le serveur…

création de lecteur logique

voilà un moyen simple de mettre en place le répertoire de base des clients windows 95-98 sur un serveur 2000 :

net use x: /home

avec x correspondant à la lettre du lecteur que l'on désire connecter en tant que partage de base

pour un client 2000 (mais non windows 95-98) on pourrait écrire

net use x: /home /persistent:no

mise à l'heure machine

voilà un moyen de mettre à l'heure des clients depuis un serveur 2000 :

net time \\serveur /set /y

N.B: pour utiliser la commande Net Time dans un login script afin de synchroniser l'heure d'une station 2000 avec un serveur, il faut que le groupe local utilisateur (de la station) ait le droit de modifier l'heure du système (dans le panneau de configuration, menu **stratégies locales/ droit de l'utilisateur / modifier heure système** et en ajoutant le groupe local utilisateurs authentifiés…).

Remarque sur les scripts pour les clients 95 -98:

les client windows 95 :

du propre aveux de microsoft, il existe un problème lorsque deux clients 95 essayent de partager au même moment le même script de connexion, voire simplement depuis le même client lors de deux ouvertures de session rapprochées…

"This problem can occur if multiple Windows 95 workstations try to run a logon script file (for example, the Winlogon.bat file) located on a single Windows NT domain controller at the same time. The first time a Windows 95 workstation access the logon script file, it does so in Read/Share/Exclusive mode. All subsequent accesses to the file are done in Read/Share/Deny None mode.

"An update to address this problem is now available, but is not fully regression tested and should be applied only to computers experiencing this specific problem. Unless you are severely impacted by this specific problem, Microsoft does not recommend implementing this update at this time. "

les client windows "Non NT-2000" en général :

on peut solutionner le problème en écrivant un script pour chaque utilisateur, (même s'il contient la même chose) de manière à ne pas avoir ce problème …

COMMANDE NET

Convention d'écriture :

Pour utiliser les commandes en ligne; il est nécessaire par rapport à la syntaxe normale des fichier BATCH dos, connaître quelques commandes spécifiques à NT, telles que NET ou AT

- Les même conventions que pour NTBACKUP sont utilisées:

Ainsi, la ligne de syntaxe ci-dessous :

NET COMMANDE [nom] {OPTION1 | OPTION2}

signifie que vous devez taper NET COMMANDE et soit OPTION1, soit OPTION2. Par contre, vous n'êtes pas obligé de fournir un nom.

- Quand ils sont tapés à l'invite de commande, les noms de service comprenant deux mots ou plus doivent être entre guillemets anglo-saxons (").

Par exemple, **NET START "Explorateur d'ordinateurs"** démarre le service d'exploration de l'ordinateur.

Commandes NET Utilisables :

Les commandes utilisables avec la commande Net sont :

ACCOUNTS	
COMPUTER	
CONFIG	
CONFIG SERVER	
CONFIG WORKSTATION	
CONTINUE	
FILE	
GROUP	
HELP	
HELPMSG	

LOCALGROUP	
NAME	
PAUSE	
PRINT	
SEND	
SESSION	
SHARE	Crée, supprime ou affiche des ressources partagées
START	
STATISTICS	
STOP	
TIME	Synchronise l'horloge de l'ordinateur avec celle d'un autre ordinateur ou d'un domaine.
USE	Liste, établit ou rompt une connexion d'une station de travail à une ressource partagée
USER	Liste, ajoute, modifie ou supprime un utilisateur
VIEW	Affiche la liste des domaines, des ordinateurs ou des ressources partagées par l'ordinateur spécifié

Pour plus de renseignement sur la syntaxe on peut taper

NET xxx /? voir **NET xxx /? |MORE**

exemple

NET USE /? voir **NET USE /? |MORE**

Net Use :

NET USE établit ou rompt une connexion d'une station de travail à une ressource partagée. Employée sans argument, NET USE liste les connexions de la station de travail.

Les paramètres utilisables avec la commande Net USE sont :

NET USE [nom de périph.|*] [\\Ordinateur\Partage[volume] [mot de passe | *]] [/USER:[nom de domaine\]nom d'utilisateur] [[/DELETE] | [/PERSISTENT:{YES | NO}]]

ou

NET USE [nom de périphérique | *] [mot de passe | *] [/HOME]

ou

NET USE [/PERSISTENT:{YES | NO}]

nom de périphérique	Spécifie le nom de périphérique affecté à la connexion à établir ou à rompre. Ce nom de périphérique désigne soit un lecteur de disque (de D: à Z:),soit une imprimante (de LPT1: à LPT3:). Mettez une astérisque pour affecter la première lettre disponible au périphérique.
\\Ordinateur	Est le nom du serveur qui gère la ressource partagée. Si ce nom contient des espaces, spécifiez-le, double barre oblique (\\) comprise, entre guillemets anglo-saxons ("). Le nom d'ordinateur peut contenir de 1 à 15 caractères.
\Partage	Est le nom réseau de la ressource partagée.
\Volume	Spécifie un volume NetWare sur le serveur. Vous devez avoir les services client pour NetWare (Windows NT Workstation)) installés
mot de passe	Est le mot de passe nécessaire pour accéder à la ressource.
*	Affiche un message demandant le mot de passe. Celui-ci n'est pas affiché lorsque vous le tapez.
/USER	Spécifie un nom d'utilisateur différent pour établir la connexion.
nom de domaine	Spécifie un autre domaine. Si cet argument est omis, le domaine où se déroule la session courante est utilisé.
nom d'utilisateur	Spécifie le nom d'utilisateur à employer pour la session.
/HOME	Connecte un utilisateur à son répertoire de base.
/DELETE	Rompt une connexion réseau et la supprime dans la liste des connexions persistantes.
/PERSISTENT	Permet de gérer les connexions réseau persistantes. La valeur par défaut est celle définie en dernier.
YES	Enregistre toutes les connexions à mesure que vous les établissez et les restaure à la session suivante.
NO	N'enregistre ni la connexion à établir, ni les suivantes ; les connexions existantes seront restaurées à la session suivante. Employez l'option /DELETE pour supprimer des connexions persistantes.

Net Time :

NET TIME synchronise l'horloge de la station de travail avec celle d'un serveur ou d'un domaine et sert à afficher l'heure d'un serveur ou d'un domaine. Employée sans argument, **NET TIME** affiche la date et l'heure courantes du serveur qui a été désigné comme serveur de synchronisation du domaine.

NET TIME [\\nom d'ordinateur | /DOMAIN[:nom de domaine]] [/SET]

\\nom d'ordinateur	Est le nom du serveur dont vous voulez connaître l'heure ou avec lequel vous voulez synchroniser votre station.
/DOMAIN[:nom de domaine]	Spécifie le domaine avec lequel vous voulez synchroniser votre station de travail.
/SET	Synchronise l'horloge de l'ordinateur avec celle de l'ordinateur ou du domaine spécifié.

Net Send :

disponible uniquement sur les postes Windows NT

net send {*nom* | ***** | **/domain**[:*nom*] | **/users**} *message*

Paramètres

nom

Spécifie le nom d'utilisateur, le nom d'ordinateur ou le nom de messagerie auquel le message doit être envoyé. S'il s'agit d'un nom d'ordinateur contenant des caractères blancs, placez-le entre guillemets (" ").

N.B : on parle ici de nom NetBios !

*****

Envoie le message à tous les noms de votre domaine ou votre groupe de travail.

/domain[:*nom*]

Envoie le message à tous les noms du domaine de l'ordinateur. Si *nom* est spécifié, le message est envoyé à tous les noms du domaine ou du groupe de travail indiqué.

/users

Envoie le message à tous les utilisateurs connectés au serveur.

message

Spécifie le texte du message à envoyer

Si le service de Messagerie est démarré (normalement il l'est en automatique)

net send nomposte "message"

permet d'envoyer un message à la machine nomposte. On peut mettre une * à la place du nom de la machine pour envoyer un message à toutes les machines…

```
D:\>net send * "arret serveur"
Le message a été envoyé au domaine STAGE.
```

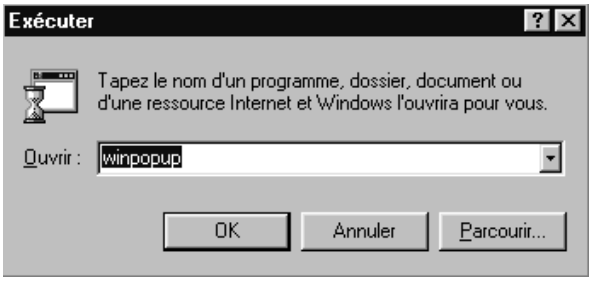
amène alors

Contacter les clients windows :

pour que la commande **Net send** soit aperçue depuis un poste windows, il faut activer sur chaque client un utilitaire qui s'appelle **winpopup.exe**

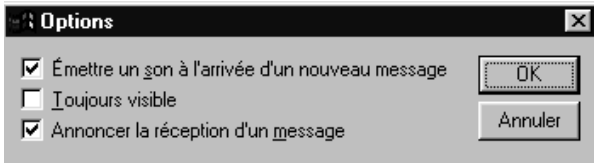
cet utilitaire est automatiquement installé sur un poste windows des que l'on demande d'installer le "client pour les réseaux microsoft"…généralement dans le dossier dans lequel windows est installé

Pour démarrer winpopup manuellement, il faut taper alors dans le menu **démarrer / exécuter**



Pour que winpopup démarre automatiquement il suffit de la placer dans le dossier **Démarrage** de l'ordinateur

dans le menu **Message / Options** on peut demander d'être alerté lors de l'arrivée d'un message



Bien sûr le poste doit ouvrir la session sur le domaine géré par le serveur…

Net User:

NET USER ajoute, modifie ou supprime un utilisateur. Employé sans argument, NET USER liste les paramètres de l'utilisateur

net user [*nom_utilisateur* [*mot_de_passe* | ***] [*options*]] [**/domain**]

net user *nom_utilisateur* {*mot_de_passe* | ***} **/add** [*options*] [**/domain**]

net user *nom_utilisateur* [**/delete**] [**/domain**]

Paramètres

Aucun

Utilisée sans paramètre, la commande **net user** affiche la liste des comptes d'utilisateurs sur l'ordinateur.

net users ou net user →

```
C:\>net users

comptes d'utilisateurs de \\SERVEUR1

-------------------------------------------------------------------------------
Administrateur           ajout                    Invité
IUSR_SERVEUR             IWAM_SERVEUR             krbtgt
marie                    TsInternetUser
La commande s'est terminée correctement.
```

nom_utilisateur

Indique le nom du compte d'utilisateur à ajouter, supprimer, modifier ou afficher. Ce nom peut comporter jusqu'à 20 caractères.

net users compte ou

net user compte →

```
C:\>net users administrateur
Nom d'utilisateur                       Administrateur
Nom complet
Commentaire                             Compte d'utilisateur d'administra
tion
Commentaires utilisateur
Code du pays                            000 (Valeur par défaut du système
)
Compte : actif                          Oui
Le compte expire                        Jamais

Mot de passe : dernier changmt.         11/25/2002 1:42 PM
Le mot de passe expire                  Jamais
Le mot de passe modifiable              11/25/2002 1:42 PM
Mot de passe exigé                      Oui
L'utilisateur peut changer de mot de passe  Oui

Stations autorisées                     Tout
Script d'ouverture de session
Profil d'utilisateur
Répertoire de base
Dernier accès                           12/8/2002 10:27 AM

Heures d'accès autorisé                 Tout

Appartient aux groupes locaux           *Administrateurs
Appartient aux groupes globaux          *Utilisa. du domaine
                                        *Propriétaires créateu
                                        *Administrateurs du sc
                                        *Administrateurs de l'
                                        *Admins du domaine
La commande s'est terminée correctement.
```

mot_de_passe

Assigne ou modifie le mot de passe du compte d'utilisateur. Il peut comporter jusqu'à 127 caractères. Toutefois, si vous utilisez Windows 2000 sur un réseau comportant aussi des ordinateurs qui utilisent Windows 95 ou Windows 98, veillez à ce que vos mots de passe n'excèdent pas 14 caractères.

*****

Produit une invite pour le mot de passe. Le mot de passe ne s'affiche pas quand vous le tapez à l'invite du mot de passe.

/domain

Exécute l'opération sur le contrôleur de domaine principal du domaine principal de l'ordinateur. Ce paramètre ne s'applique qu'aux ordinateurs Windows 2000 Professionnel qui font partie du domaine Windows 2000 Server. Par défaut, les ordinateurs Windows 2000 Server exécutent les opérations sur le contrôleur de domaine principal.

Cette action est appliquée au contrôleur de domaine principal du domaine principal de l'ordinateur. Il peut ne pas s'agir du domaine de connexion.

/add

Ajoute un compte d'utilisateur à la base de données de comptes d'utilisateurs.

/delete

Supprime un compte d'utilisateur de la base de données de comptes d'utilisateurs.

Net view:

NET view Affiche la liste des domaines, des ordinateurs ou des ressources partagées par l'ordinateur spécifié

net view [*nom_ordinateur* | **/domain**[**:***nom_domaine*]]

net view /network:nw [*nom_ordinateur*]

Paramètres

Aucun

Utilisée sans paramètre, la commande **net view** affiche la liste des ordinateurs de votre domaine en cours.

nom_ordinateur

Indique l'ordinateur pour lequel vous voulez afficher les ressources partagées.

/domain[**:***nom_domaine*]

Désigne le domaine dont vous voulez afficher les ordinateurs disponibles. Si *nom_domaine* est omis, tous les domaines du réseau sont affichés

LE SHELL DOS POUR LES SCRIPTS

Interpreteur de commande :

Le langage de scripts présenté ici est un langage existant depuis l'origine quasiment des système windows, car il est d'origine MSDOS.

Pour des raisons évidente de compatibilité, il vaut mieux baser nos scripts sur le tronc commun de la machine de plus "bas niveau" disponible…

Bien que désormais Microsoft tende à promouvoir un langage de script propre nommé WSH, les shell DOS ont encore de beau jours vu leur évidente simplicité de manipulation…

Par défaut, le sous-système MS-DOS utilise une version spéciale de **Command.com** fonctionnant de façon transparente pour les autres sous-systèmes de Windows 2000.

vous devez utiliser la version 32 bits (Cmd.exe), disponible sur le menu **Programmes**, et non pas la version 16 bits (Command.com).

echo :

```
E:\>help echo
Affiche des messages ou active/désactive l'affichage des commandes.

  ECHO [ON | OFF]
  ECHO [message]

ECHO sans paramètres affiche l'état en cours de la commande.
```

if :

```
E:\>help if
Lance l'exécution conditionnelle dans un programme de commandes.

IF [NOT] ERRORLEVEL nombre commande
IF [NOT] chaîne1==chaîne2 commande
IF [NOT] EXIST nom_de_fichier commande

  NOT                   Indique que Windows 2000 n'effectue la commande que si
                        la condition est fausse.

  ERRORLEVEL nombre     Condition vraie si le dernier programme exécuté a
                        retourné un code sortie supérieur/égal au nombre donné.
  commande              Spécifie la commande à exécuter si la condition est
                        satisfaite.

  chaîne1==chaîne2      Condition vraie si les chaînes spécifiées sont
                        identiques.

  EXIST nom_de_fichier  Condition vraie si le nom de fichier donné existe.

  commande              Spécifie la commande à exécuter si la condition est
                        vérifiée. Commande peut être suivi de la commande ELSE
```

N.B: uniquement sur 2000, else n'est pas valable sous win95-98...

for :

```
C:\>for /?
Exécute une commande sur chaque fichier d'un ensemble de fichiers.

FOR %variable IN (ens) DO commande [param]

  %variable  Paramètre remplaçable.
  (ens)      Ensemble de fichiers séparés par des espaces. Caractères
             génériques permis.
  commande   Commande à exécuter pour chaque fichier.
  param
      Paramètres ou commutateurs pour la commande spécifiée.

Pour utiliser FOR dans les fichiers de commandes, spécifiez %%variable
au lieu de %variable.
```

goto :

```
E:\>help goto
Dirige cmd.exe sur une ligne étiquetée dans le programme de commandes.

GOTO nom

  nom   Chaîne utilisée en tant que nom dans le programme de commandes.

Les noms sont seuls sur une ligne et commencent par le signe ':'
```

find :

```
E:\>help find
Recherche une chaîne de texte dans un ou des fichiers.

FIND [/V] [/C] [/N] [/I] "chaîne" [[lecteur:][chemin]nom_de_fichier[ ...]]

  /V         Affiche toutes les lignes ne contenant pas la chaîne spécifiée.
  /C         Affiche seulement le nombre de lignes contenant la chaîne.
  /N         Affiche les numéros de ligne avec les lignes affichées.
  /I         Ignore la casse lors de la recherche de la chaîne.
  "chaîne"   Spécifie la chaîne de texte à trouver.
  [lecteur:][chemin]nom_de_fichier
             Spécifie un ou des fichiers pour la recherche.

Sans nom de chemin, FIND recherche le texte tapé à l'invite ou redirigé depuis
une autre commande.
```

pause

```
E:\>help pause
Interrompt l'exécution d'un programme de commandes et affiche le message
    Appuyez sur une touche pour continuer...
```

call :

```
E:\>help call
Appelle un programme de commandes depuis un autre.

CALL [lecteur:] [chemin] nom_de_fichier [paramètres de commande]

  paramètres de commande      Paramètres requis par le programme de
                              commandes appelé.
```

rem :

```
E:\>help rem
Indique un commentaire dans un fichier de commandes ou dans CONFIG.SYS.

REM [commentaire]
```

Compléments du Resource Kit

Un utilitaire est fournis nommé **ifmember.exe** bien sur fonctionnant uniquement en environnement 2000 ou nt4.0

IfMember is a command-line tool that checks whether the current user is a member of a specified group. It is typically used in Windows logon scripts and other batch files.

IfMember uses its own process token to discover group membership, rather than querying the relevant domain controller each time it runs. While this has a significant performance benefit, it does mean that IfMember will only be aware of groups on the local computer, on the computer's domain, and on trusted domains.

IfMember Syntax

Open command prompt now.

---

ifmember [**/verbose**] [**/list**] [*groupname1*] [*groupname2*] ...

Where:

/verbose
prints all group matches

/list
lists all groups the user is in

groupname
specifies one or more group names (separated by a spaces)

LES LANGAGES DE SCRIPT : WSH

Dans le Resource Kit :

Il existe un langage de script complémentaire, présent pour les postes 2000 (et NT4.0) nommé **KIX32**…

Même si ce langage de script est plus complet que ce que l'on peut faire avec les commandes shell msdos, il comporte un inconvénient de taille, c'est de ne pouvoir fonctionner que sur des clients nt4.0 ou 2000

Windows Scripting Host :

Précédemment, le seul langage de script natif pris en charge par Windows était le langage de commande MS-DOS. Bien que rapide et concis, MS-DOS possède des fonctionnalités assez limitées, en comparaison de Visual Basic Script et de Java Script.

WSH est un hôte indépendant du langage utilisé pour les plates-formes Microsoft Windows 32 bits. Microsoft fournit avec l'environnement WSH les moteurs de script Visual Basic Script et Java Script.

WSH peut être exécuté à partir de l'hôte sous Windows (Wscript.exe) ou de l'hôte à base de shell de commande (Cscript.exe). Trois hôtes pour l'exécution de ces langages de scripts sur la plate-forme Windows existent :

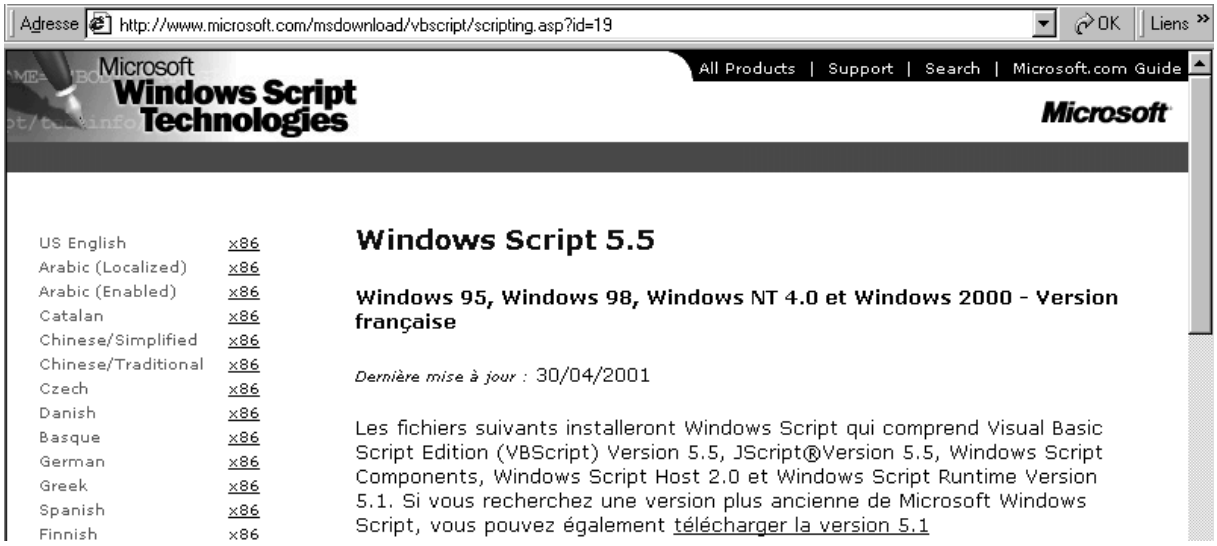
- **IE**
  Internet Explorer permet d'exécuter des scripts sur les postes clients à partir des pages HTML.
- **IIS**
  Internet Information Server prend actuellement en charge Active Server Pages, qui permet d'exécuter des scripts sur des serveurs Web ; il permet en d'autres termes d'écrire des scripts côté serveur sur Internet ou sur un réseau intranet.
- **WSH**
  WSH permet d'exécuter les scripts directement sur le bureau de Windows ou sur la console de commande sans qu'il soit nécessaire de les insérer dans un document HTML. WSH est un hôte de script à mémoire réduite idéal pour les besoins de scripts non interactifs, tels que les scripts de connexion, d'administration, etc.

En résumé, VBScript est utilisable par **plusieurs** environnements, dont le principal est **WSH** . **WSH** admet **plusieurs** langages de script, dont le principal est **VBScript**

Installation de Windows Scripting Host :

Pour pouvoir utiliser WSH, vous devez installer Microsoft Internet Explorer 3.0 ou version ultérieure. L'hôte de script utilise les moteurs Visual Basic Script et Java Script fournis avec Internet Explorer 3.0 ou version ultérieure. **WSH est installé en même temps** que Windows 98, Windows 2000 et Internet Information Server 4.0. Sous Windows 95, un programme d'installation spécial a été conçu.

On peut récupérer des mises à jours



Spécifications :
Windows Script est destiné à Windows 95, Windows 98, Windows NT 4.0 et Windows 2000.

Important : Les utilisateurs de Windows 95 doivent avoir installé OSR2 ou exécuter Microsoft Internet Explorer 4.0 ou supérieure pour que ces fichiers fonctionnent correctement. Les utilisateurs de Windows 95 sans Microsoft Internet Explorer 4.0 ni OSR2 devront installer DCOM avant d'utiliser ces fichiers. Les utilisateurs de Microsoft Windows NT 4.0 doivent avoir installé Microsoft Internet Explorer 3.02 ou Internet Explorer 4.0 avant d'utiliser ces fichiers.

For Windows 2000: scriptfr.exe
For Windows 95, 98 & NT 4: scr55fr.exe

Certains scripts **VBS** peuvent faire appel à **WMI** (***Windows Management Instrumentation***), qui est un fournisseur **d'informations** diverses sur le système d'exploitation (matériel - BIOS compris -, disques, mémoire, comptes, réseau, ...) . Cet ensemble est **installé d'origine** avec **Windows ME**, **Windows 2000** et **Windows XP**. Dans le cas de **Windows 95/98/98SE** et **Windows NT4**, il faut **l'installer** séparément, à partir d'un fichier auto extractible **téléchargeable** librement sur le site Microsoft :

Utiliser WSH ?:

C'est un vrai langage, avec une approche objet… dépassant le cadre de ce support, et méritant un support à part entière…

PROFILS SOUS 2000

Objectif :

Les profils d'utilisateur présentent plusieurs avantages :

- Lorsque les utilisateurs ouvrent une session sur leur station de travail, ils reçoivent les paramètres du bureau tels qu'ils existaient à la fermeture de la dernière session.
- Plusieurs utilisateurs peuvent utiliser le même ordinateur et chacun reçoit un bureau personnalisé lorsqu'il ouvre une session.
- Vous pouvez créer des profils d'utilisateur personnalisés et les attribuer à des utilisateurs, afin de leur fournir des environnements de travail cohérents qui correspondent aux tâches qui leur incombent.
- Vous pouvez spécifier des paramètres de groupe de programmes commun pour tous les utilisateurs.
- Vous pouvez attribuer des profils d'utilisateur obligatoires pour empêcher des utilisateurs de modifier les paramètres du bureau.

N.B: Les profils d'utilisateur peuvent être employés sur des ordinateurs exécutant Windows 95-98,. (cf chapitre suivant) pour d'autres systèmes (Windows 3.1 ou autre) il faut écrire des scripts de connexion

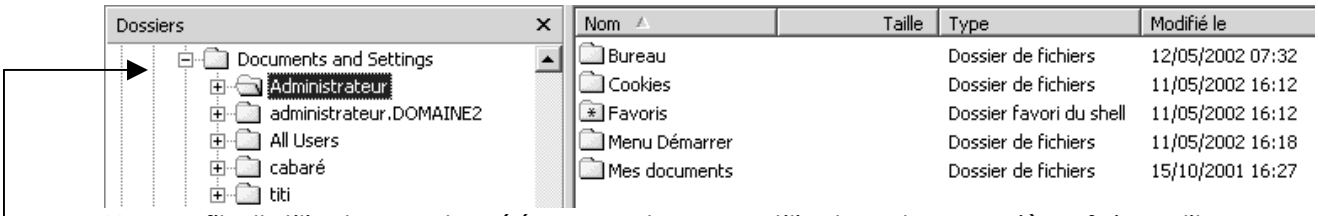
Les profils permettent de mémoriser notamment les paramètres suivant:

Explorateur Windows NT	Tous les paramètres définissables par l'utilisateur pour l'Explorateur Windows NT.
Barre des tâches	Tous les groupes de programmes personnels et leurs propriétés, tous les programmes et leurs propriétés, et tous les paramètres de la barre des tâches.
Paramètres d'imprimante	Connexions aux imprimantes du réseau.
Panneau de configuration	tout sauf polices / date-heure / affichage drivers / réseau /
Accessoires	Tous les paramètres d'application spécifiques à l'utilisateur qui affectent l'environnement Windows NT de l'utilisateur, tels que la Calculatrice, l'aspect de l'horloge, le Bloc-notes, Paint

Les profils peuvent être stockés sur un serveur afin d'être en mesure de suivre les utilisateurs sur n'importe quel ordinateur exécutant la plate-forme Windows 2000 sur le réseau. Ils sont appelés **Profils Errants**, par opposition aux profils crées automatiquement par défaut sous 2000 pour chaque utilisateur qui prennent alors le nom de **Profils Locaux**.

Profils Locaux :

Sur les ordinateurs Windows 2000 Pro ou Server, les profils d'utilisateur créent et conservent automatiquement les paramètres du bureau pour l'environnement de travail de chaque utilisateur sur l'ordinateur local.



Un profil d'utilisateur est créé pour chaque utilisateur la première fois qu'il ouvre une session sur un ordinateur 2000 et est stocké automatiquement dans un dossier **Document and Settings** du disque logique sur lequel 2000 est installé, (sous NT4 il était stocké dans **Winnt\Profiles**)

Il existe au minimum 2 dossier nommés :

All Users

Default User

Plus le profil de l' **Administrateur** (celui crée lors de l'instalation du poste)

leur signification est la suivante :

All Users : Les paramètres contenus dans le dossier **All Users** sont utilisés pour créer le profil utilisateur, il s'agit du groupe de programme communs, qui sont toujours disponibles quelle que soit la personne qui a ouvert la session. Seuls les membres du groupe Administrateur peuvent créer des groupes de programme commun

Default Users : C'est le profil d'utilisateur utilisé par défaut pour créer tout nouveau profil sur ce poste

Création d'un profil local :

A chaque nouvelle ouverture de session, un Profil commence par une copie du profil Utilisateur par défaut (Default users) et du profil des programmes communs (All users)

Bien qu'il ne soient pas copiées physiquement, les paramètres du dossier **All Users** et **Default User** sont utilisés pour créer le profil de l'utilisateur

Ainsi le profil d'utilisateur local est celui qui est stocké sous le nom de l'utilisateur dans le dossier **Profiles**

S'il n'existe pas de profil errant pour cet utilisateur, lors de sa première connexion un dossier à son nom est donc crée . Lorsque l'utilisateur ferme sa session, toutes les modifications apportées aux paramètres par défaut son enregistrées dans son dossier de Profil.

Ce système fonctionne tout seul, et c'est ce qui fait que les lecteurs logiques, et de manière générale toutes les modifications faites sous une session n'apparaissent pas pour une session d'un autre utilisateur;

A condition que l'utilisateur se connecte toujours sur la même station !

Profils Errant :

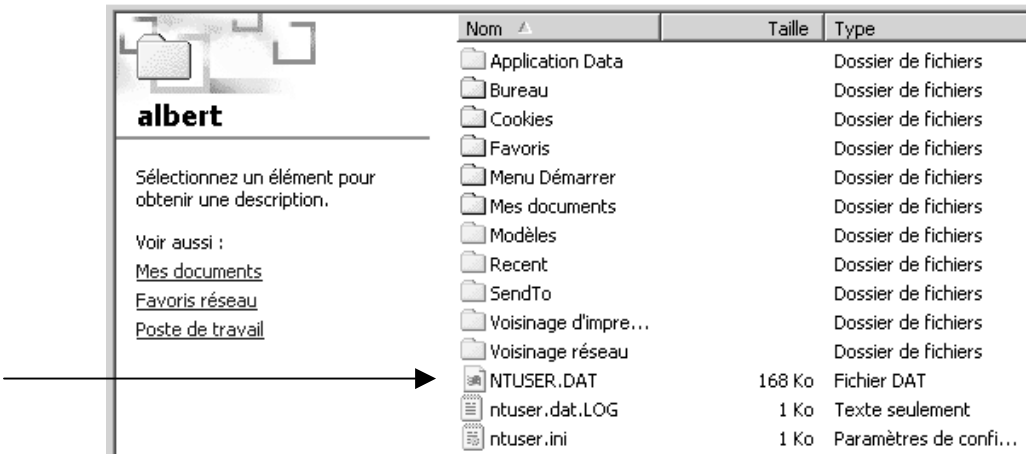
Contrairement au **profil local**, qui mémorise différents environnement pour un utilisateurs selon la machine sur laquelle il se connecte, un **profil errant** donne toujours le même environnement de travail, quelle que soit la machine NT sur laquelle celui-ci se logue.

Ce profil errant doit être enregistré de manière centralisée sur un dossier crée a cet effet sur le serveur. A terme ce dossier contiendra un sous-dossier par profil errant stocké, du nom de l'utilisateur,

Par exemple créons un dossier nommé **stock_profil** et partageons le pour tous les utilisateurs en contrôle total. Si on prévoit de gérer les profils pour **Albert** et **Bertrand** on aura a terme

Dans chacun de ces dossiers, on pourra retrouver tout l'environnement du bureau de l'utilisateur, ainsi qu'une copie de la base de registre du paramétrage (après une connexion déconnexion de l'utilisateur…)

fichier **ntuser.dat**



N.B: le nom du dossier dans lequel on s'apprête à stocker les profils n'a aucune importance…

N.B: si on ne veut pas que ce dossier soit visible, on peut faire terminer son nom par $

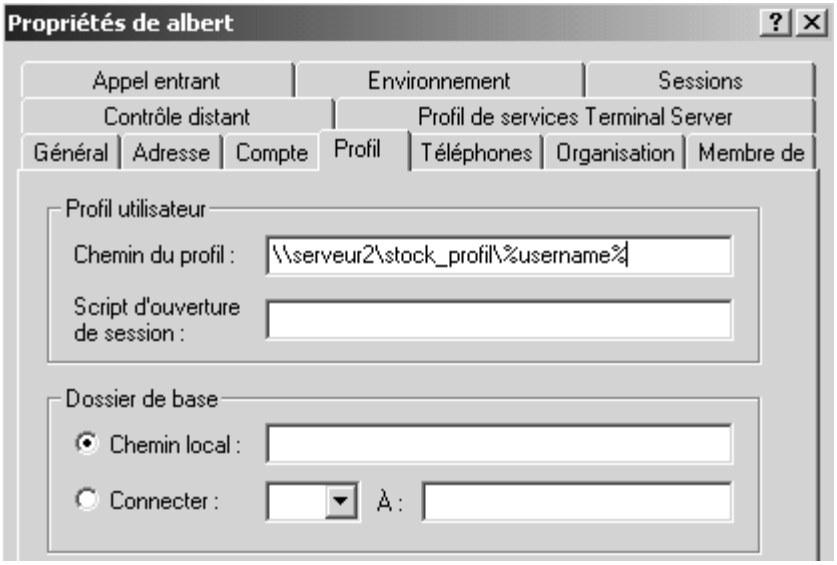
Profil Errant crée par l'utilisateur (vide au départ):

Il suffit d'ajouter un chemin de profil d'utilisateur à chaque compte d'utilisateur pour créer automatiquement un dossier de profil d'utilisateur vide nommé pour l'utilisateur à l'emplacement prévu du serveur et pour permettre au l'utilisateur de créer son propre profil

Le principe général de création d'un profil errant vide est celui-ci :

- Le compte utilisateur pour le profil voulu existant, faire apparaître via l'onglet **Profil** la boite de dialogue

Il faut ajouter un chemin d'accès complet dans chaque compte utilisateur du type



\\Serveur\Dossier\nomprofil

avec **Serveur** : le nom du serveur NT sur lequel les profils sont enregistrées (ici **SERVER2**)

avec **Dossier** : le nom du dossier partagé avec le groupe global prédéfini **Tout le monde** (ici **stock_profil**)

avec **nomprofil** : le nom d'utilisateur défini pour le compte Utilisateur (ici **albert**)
Il serait bien sûr plus intéressant de mettre ici **%username%** (pour pouvoir copier ce compte…)

- A partir de là, lors de la première connexion de Albert depuis n'importe quelle machine 2000, un dossier contenant son profil est automatiquement crée. Si Albert modifie son environnement de travail, lors de sa fermeture de session ces modifications seront stockées dans son profil

---

Profil Errant modifiable par l'utilisateur (copie de profil):

Le principe est donc exactement le même que celui pour crée un profil vide, modifiable par l'utilisateur, avec une seule différence, c'est au préalable de faire une copie d'un profil existant dans le profil de l'utilisateur afin de lui fournir une base

Un dossier du type

\\Serveur\Dossier\nomprofil

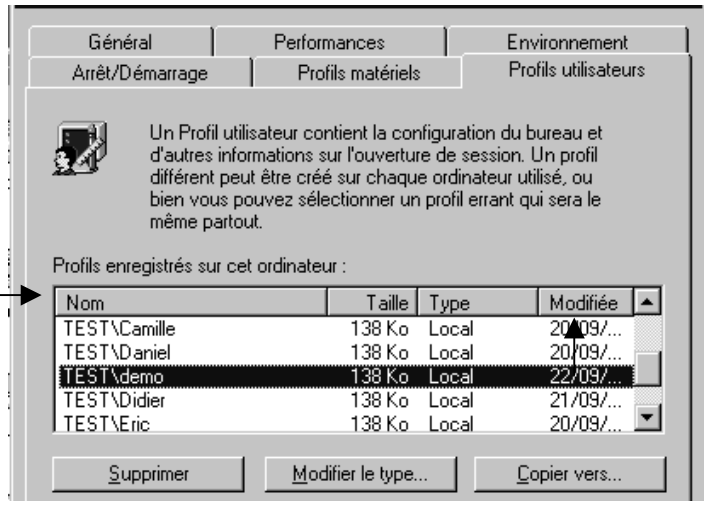
Doit donc déjà exister

De même il faut sur une machine NT disposer déjà d'un compte Utilisateur avec un profil existant localement. Ce profil c'est le modèle que l'on souhaite copier comme "base"

Pour copier un Profil, il faut se **mettre sur la machine sur laquelle le profil à copier se trouve**, puis ouvrir une session avec les droits d'Administrateurs

On demande ensuite dans **Panneau de configuration / Paramètre / Système**

l'onglet **Profil utilisateurs**

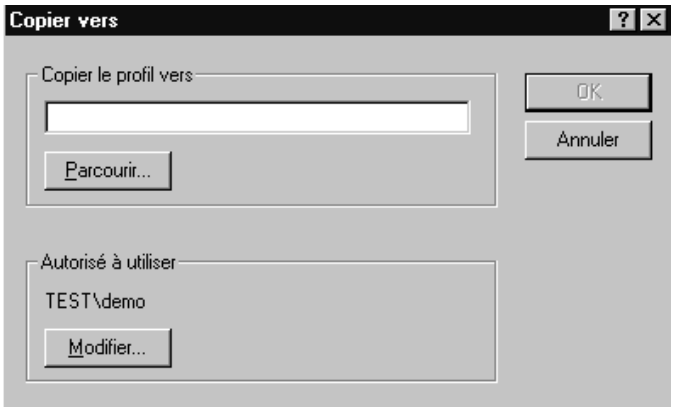


tous les profils utilisateurs existant sur cette machine apparaissent

Pour copier un profil (ici **Demo**), après l'avoir sélectionné il faut faire **Copier vers…**Pour obtenir

il faut indiquer ici le nom de la machine de destination avec le dossier dans lequel se trouvent le profil et le nom du profil

ou bien cliquer sur **Parcourir…**

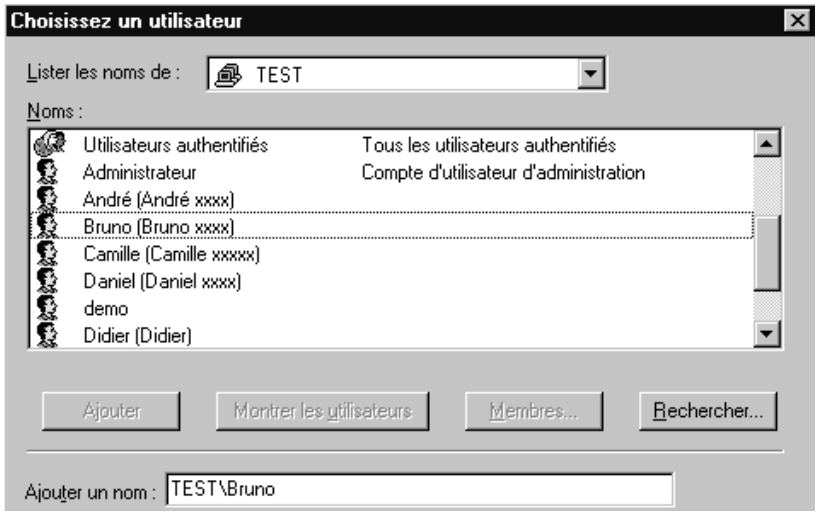


pour obtenir par exemple **\\Serveur\Dossier\Bruno**

Ce n'est pas tout, encore faut il autoriser le bon utilisateur pour ce profil

en demandant **Modifier…**

on obtient

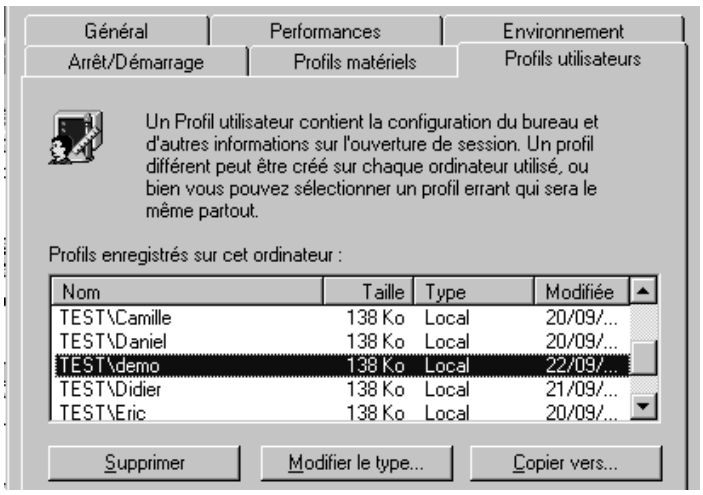


On ajoutera l'utilisateur souhaité de manière à avoir

Supprimer un Profil :

Dans **Panneau de configuration / Paramètre / Système**

l'onglet **Profil utilisateurs**



Pour Supprimer un profil (ici **Demo**), après l'avoir sélectionné il faut faire **Supprimer…**

Profils Errants Personnels ou Obligatoires :

Deux types de profils errant existent :

- Profil Personnel Errant : l'utilisateur peut le modifier, et son profil sera enregistré à chaque fermeture de session. Chaque utilisateur possède son profil personnel.
  ce profil est stocké dans un fichier **Ntuser.dat**
- Profil Obligatoire Errant : c'est un profil que l'utilisateur ne peut pas modifier, et qui donc peut servir pour plusieurs personne en même temps.
  ce profil est stocké dans un fichier **Ntuser.man**

Profil Errant obligatoire (non modifiable) :

IL faut renommer le fichier **Ntuser.dat** en **Ntuser.man** dans le profil d'utilisateur spécifié. Un profil d'utilisateur obligatoire sera alors créé

Le principe est donc exactement le même que celui pour crée un profil avec modèle, avec une seule différence, comme on l'a dit, c'est de renommer fichier **Ntuser.dat** en **Ntuser.man** dans le dossier du profil d'utilisateur

Profil Errant obligatoire identique pour un groupe:

Dans le cas d'un profil de groupe, il semble plus raisonnable de créer un profil non modifiable car toute personne du groupe aurait la possibilité de modifier le profil pour tout le groupe…

Création du profil type pour des « commerciaux »:

- créer sur le serveur un utilisateur **profil_commerciaux**
- lui indiquer un chemin de profil **\\serveur\Profil\%Username%**
- ouvrir une session avec sur un client 2000 et effectuer tous les changements nécessaires (bureau, mais aussi répertoire utilisateurs par défaut dans Word, etc..)
- créer sur le serveur un sous-dossier "**commerciaux**" dans le dossier **Profil**
- créer un groupe global **commerciaux** et y placer tous les utilisateurs nécessaires
- fermer la session en tant que utilisateur "**profil_commerciaux**"et en ouvrir une autre en tant qu'Administrateur (on va copier le profil crée localement)
- demander **paramètre / panneau de configuration / système / onglet profils utilisateurs**, visualiser le profil commerciaux, le copier dans le dossier commerciaux du dossier profil du serveur, soit **\\serveur\profil\commerciaux**, attribuer via le bouton **modifier** les droits d'utilisation à ce profil pour le groupe global des **commerciaux**
- Lorsque cela est fait, se loguer sur le serveur et aller dans ce dossier et renommer **Ntuser.dat** en **Ntuser.man**

maintenant le profil type pour les commerciaux est crée

pour chaque utilisateur commercial

- Pour chaque création d'un nouvel utilisateur, indiquer le répertoire **\\serveur\profil\commerciaux**
- ne pas oublier de placer l'utilisateur dans le groupe global commerciaux commerciaux (pour qu'il ait le droit d'utiliser le profil)

Horodatage et profils :

Quand l'utilisateur ferme sa session, windows place automatiquement un exemplaire mis à jour du profil dans le répertoire sur le serveur, mais uniquement si celui-ci est plus récent !

Ainsi dans le cas d'une station client qui retarde, lorsque l'utilisateur modifie son profil et quitte la session, 2000 constate que son profil est plus "ancien" que la copie dont il dispose sur le serveur, et donc ne récupère pas le nouveau profil !

On à donc intérêt à synchroniser systématiquement les machines via un script, par exemple

Logique de gestion des profils :

Lorsque l'utilisateur **ouvre une session** sur une machine 2000 :

- Si c'est la première connexion, et qu'il n'existe pas de profil, alors un profil local est crée sinon le profil errant est récupéré, et est copié dans un profil homonyme local
- Si ce n'est pas la première connexion, et qu'il n'existe pas de profil errant, le profil local est récupéré, s'il existe un profil errant celui est récupéré et remplace le profil homonyme local
- Si ce n'est pas la première connexion, et qu'il existe un profil errant mais que celui-ci ne peut être chargé (…) un profil local est crée (ou chargé s'il existe) mais lors de la fermeture de session il n'y a pas tentative de copier le profil local à l'emplacement d'origine du profil errant
- Si ce n'est pas la première connexion, et qu'il existe un profil errant mais que celui-ci n'a pu être chargé la dernière fois (…) un profil local existe et est peut plus récent que le profil errant. NT demande alors à l'utilisateur quel profil doit il ouvrir

Lorsque l'utilisateur **ferme une session** sur une machine 2000 :

- Si il n'y a pas eut chargement d'un profil errant, les modifications sont apportées au profil local
- Si il y a eut chargement d'un profil errant, les modifications sont apportées au profil local, puis ce profil est fermé et copié à l'emplacement d'origine du profil errant (s'il est plus récent que celui existant)

Supprimer tous les profils locaux d'une machine NT:

Tous les profils errants sont donc stockés sur le serveur, et celui-ci les copie sur la machine client lorsque l'utilisateur se connecte. Si un utilisateur s'identifie sur différentes machines, une copie de son profil sera présent sur toutes ces machines. Dans la même logique, si différents utilisateurs s'identifient sur une même machine, tous leurs profils seront copiés sur cette machine. Un profil pouvant atteindre 1 Méga, à terme il peut être nécessaire de faire le ménage.

Pour supprimer les profils locaux d'une machine, il est nécessaire de le faire un à un, depuis l'onglet Profil utilisateur de l' icône système du panneau de configuration. On peut aller plus vite en utilisant un exécutable du KIT DE RESSOURCE TECHNIQUE WINDOWS SERVER nommé **delprof.exe**

cet utilitaire permet de supprimer tous les profils locaux, avec confirmation éventuelle sur chacun (à l'exception bien sûr du profil de la session sur laquelle on est logué)

N.B : cet utilitaire existe à l'identique pour la version 4.0, mais ne peut s'appliquer sur un poste 2000 serveur

voilà quelques paramètres d'appel :

Delprof /p Demande confirmation pour chaque profil

Delprof /d:3 Ne traite que les profils vieux de plus de **3** jours. Si omis tous les profils sont traités

Delprof /q Ne demande pas de confirmation pour s'exécuter au départ

Delprof /c:\\nom Permet d'indiquer le **nom** de la machine sur laquelle on veut supprimer les profils locaux

Ainsi par exemple la ligne de commande

Delprof //p /c:\\nom permet de supprimer tous les profils locaux de la machine nom, en demandant au fur et à mesure, confirmation pour chacun d'eux. Pour peu que sur cette machine il n'y ait pas de session ouverte, alors tous les profils pourront être supprimés

```
A:\>delprof /p /c:\\poste5wks

Delete \\poste5wks\admin$\Profiles\Administrateur? (Yes/No/All) y
Deleting \\poste5wks\admin$\Profiles\Administrateur...    [Ok]
```

il est possible de demander de supprimer tous les profils en cache local, dans le poste NT (et donc forcer à télécharger le dernier profil stocké sur le serveur) en créant ou modifiant la clé de registre local

HKEY_LOCAL_MACHINE\software\Microsoft\WindowsNT\curentVersion\Winlogon

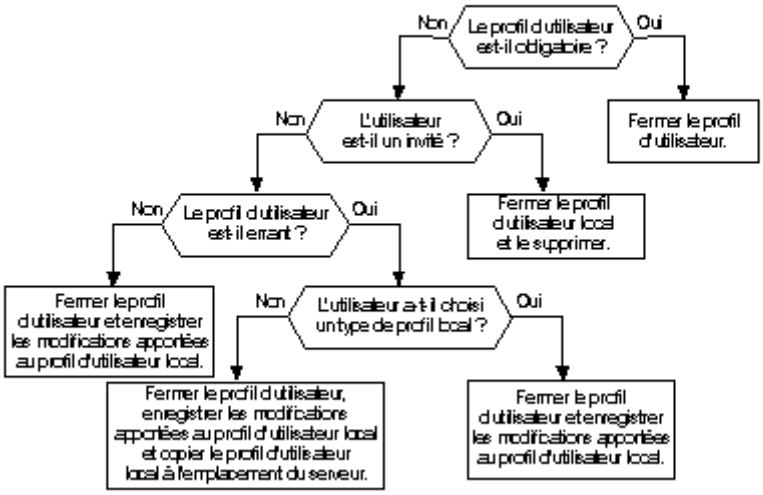
ajouter une valeur de type REG_DWORD **"DeleteRoaminCache" = 1** pour activer la suppression du cache

N.B: Ce qui peut d'ailleurs s'obtenir via une stratégie système d'ordinateur

---

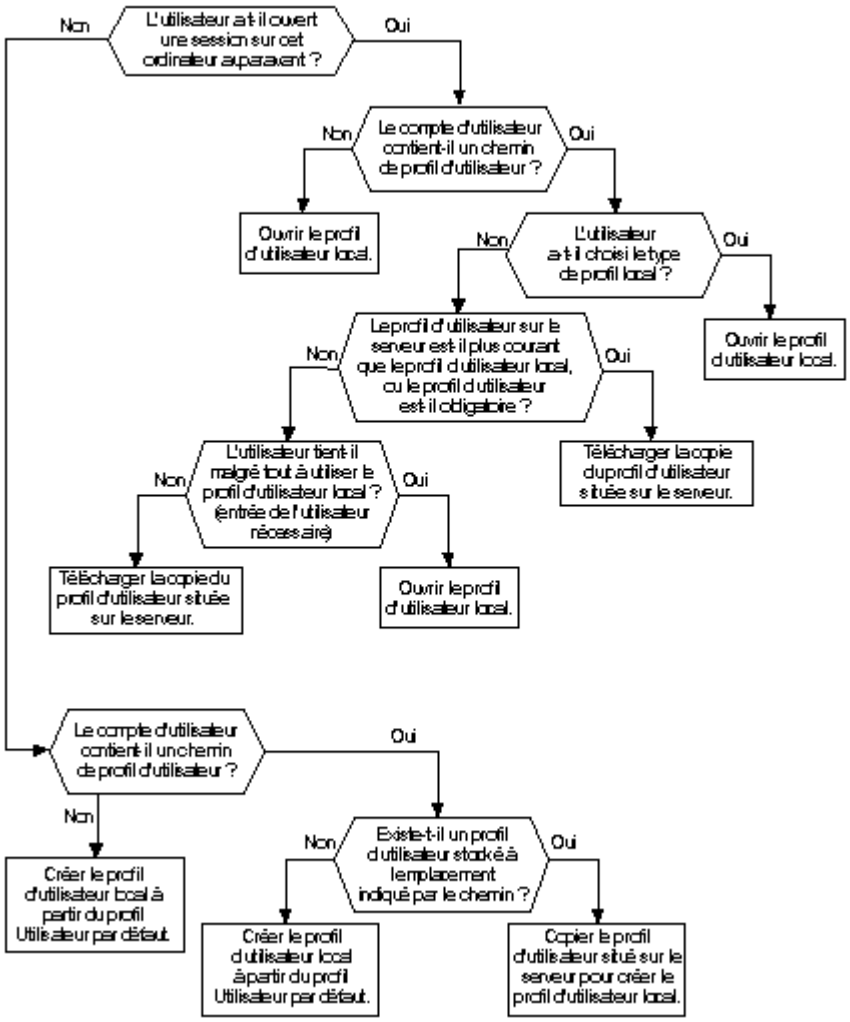
Séquence d'enregistrement de profil :

Le graphique suivant présente la séquence d'enregistrement de profils d'utilisateur à la fermeture d'une session.



Séquence d'ouverture de profil :

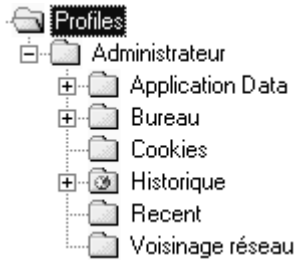
Le graphique suivant présente la séquence d'ouverture des profils d'utilisateur à l'ouverture d'une session.



PROFILS SOUS WIND 95-98

Création d'un Profil 95-98:

Les profils d'utilisateur locaux de Windows 95-98 fonctionnent de la même manière que les profils d'utilisateur sous Windows 2000



Chaque profil inclut plusieurs parties :

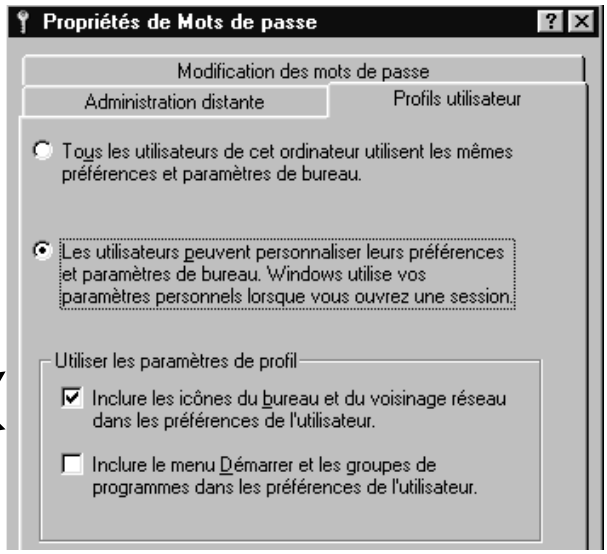
un fichier **USER.DAT**

Un dossier **Bureau**, **Recent, Menu Démarrer**… et pour wind98 quelques dossiers de plus pour les applications internet

Pour activer les profils il faut dans le panneau de configuration demander **Mot de passe**


Mots de passe

et dans l'onglet **Profils utilisateurs** demander de pouvoir personnaliser les préférences



Il faut cocher les options selon ce que l'on souhaite mémoriser

puis Arrêter et redémarrer l'ordinateur

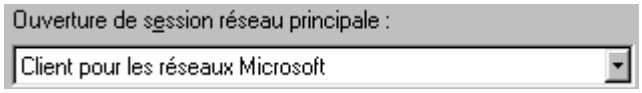
N.B: Lorsque on installe des profils en cochant les deux options, si une application est installée sous un profil, elle n'apparaîtra pas dans le menu démarrer d'un autre profil…(mais cela n'empêche pas d'y accéder si on est capable de la localiser et de créer un raccourci…)

Profils errant modifiables vers client windows :

Les profils d'utilisateur errants Windows peuvent être utilisés sur un réseau Windows 2000 sous 2 conditions :

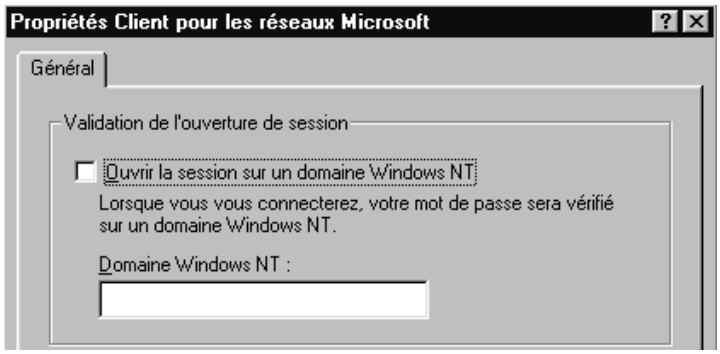
- si **Client pour les réseaux Microsoft** est choisi comme client principal de la session réseau

  Dans **propriété** de **Voisinage réseau**



- et si on a demandé d'ouvrir une session sur un domaine (bien sur avec le nom de domaine sur lequel on va stocker les profils)

  Dans **propriété** de **Client pour les réseau Microsoft**



De plus pour mettre en place des profils utilisateurs sur des clients 95-98 il faut

- Pour chaque ordinateur, s'assurer que les profils sont activés selon la technique des profils windows 95-98 (voir ci-dessus création d'un profil windows 95-98)
- Sur le serveur 2000, vérifier que chaque utilisateur à son répertoire de stockage personnel, c'est à dire qu'un dossier personnel à cet utilisateur existe et qu'il est paramétré comme dossier d'accueil (voir chapitre répertoire de base).
  CE NE DOIT PAS ETRE LE REPERTOIRE DE STOCKAGE DES PROFILS WINDOWS 2000

Ainsi si on veut créer un profil errant pour l'Utilisateur **Paul**, stocké sur le serveur **SERVER** pour des clients windows 95-98, il faut :

- Sur le serveur, créer un dossier **Paul**, dans lequel le profil de cet utilisateur sera stocké, par exemple si les dossiers d'accueil sont stockés dans le dossier **Perso** alors créer **Perso\Paul**
- Sur le serveur, créer bien sûr un compte utilisateur Paul avec comme répertoire d'accueil (dans le bouton Profil) **\\SERVER\Perso\Paul**
- Sur chaque poste windows sur lequel Paul est susceptible de se connecter, il faut demander d'ouvrir une session en tant que client pour les réseaux Microsoft, et demander de valider les mots de passe sur le Domaine géré par le serveur **SERVER** Les profils doivent être activés classiquement dans l'icône mot de passe du panneau de configuration

Quand l'utilisateur windows95-98 ferme sa session, windows place automatiquement un exemplaire mis à jour du profil dans le répertoire personnel de l'utilisateur sur le serveur, mais uniquement si celui-ci est plus récent !

Ainsi dans le cas d'une station client qui retarde, lorsque l'utilisateur modifie son profil et quitte la session, 2000 constate que son profil est plus "ancien" que la copie dont il dispose sur le serveur, et donc ne récupère pas le nouveau profil !

On à donc intérêt à synchroniser systématiquement les machines via un script, par exemple

---

Profils errant obligatoires vers client windows :

Les profils d'utilisateur obligatoires peuvent être utilisés, mais doivent être créés pour chaque utilisateur et placés dans chaque répertoire personnel

L'idée est analogue à ce qui existe pour les profils sous 2000, c'est à dire que il faut renommer le fichier **user.dat** en **user.man** dans le chemin de profil d'utilisateur stocké sur le serveur

---

Particularités des profils windows 95-98:

On ne peut pas créer de profils d'utilisateur pour des clients Windows 95-98 sur un ordinateur Windows 2000 car Les fichiers utilisés pour les profils d'utilisateur ne sont pas les mêmes sous Windows 95 et sous Windows 2000.

Windows 2000	Windows 95-98
Ntuser.dat	User.dat
Ntuser.man	User.man

Les profils de 2000 et de Windows 98 présentent les différences suivantes :

- Windows 98 ne prend pas en charge les groupes de programmes communs. Les profils d'utilisateur de Windows 98 ne copient pas tous les éléments du bureau, mais uniquement les fichiers de raccourcis (.lnk) et les fichiers d'informations sur les programmes (.pif).
- Les clients Windows 95-98 n'utilisent pas le chemin du profil de Windows NT Server pour obtenir des profils d'utilisateur errants. Ils ne peuvent être récupérés qu'à partir du répertoire de base de l'utilisateur.
- Pour utiliser des profils d'utilisateur obligatoires sur des ordinateurs Windows 95-98 sur un réseau Windows 2000 Server, un administrateur doit créer un profil d'utilisateur personnalisé pour chaque utilisateur et copier les fichiers de profils d'utilisateur dans le répertoire de base de chaque utilisateur.
- Ne pas mélanger de profils Windows95 avec des profils Windows 98 ?

OBSERVATEUR D'EVENEMENTS

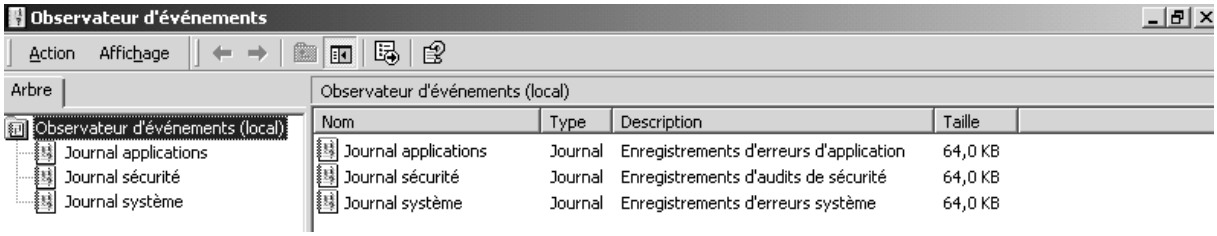
Principes et type des journaux :

Certaines activités peuvent être consignées dans un journal d'évènements, et il existe plusieurs types de journaux.

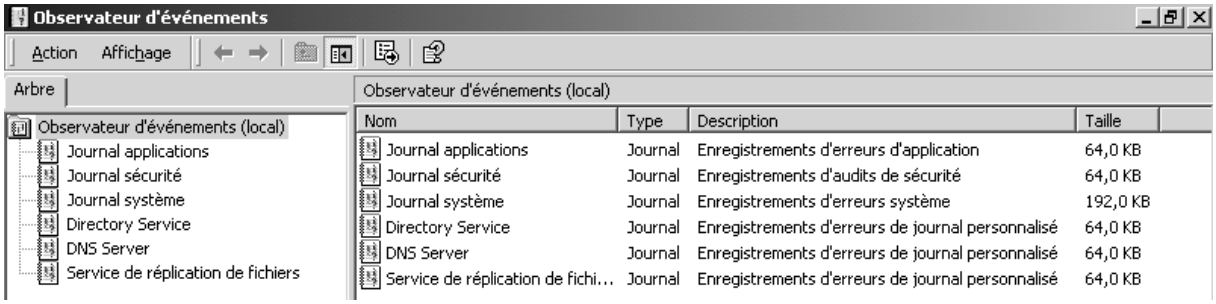
Ces journaux sont accessibles via le menu

Démarrer / Programme / Outils d'administration / Observateur d'évènement

Sur un 2000 Pro on aura



Sur un 2000 Serveur on aura



avec en plus un journal spécifique pour l'AD, le DNS et la réplication des AD entre les différents serveurs du Domaine

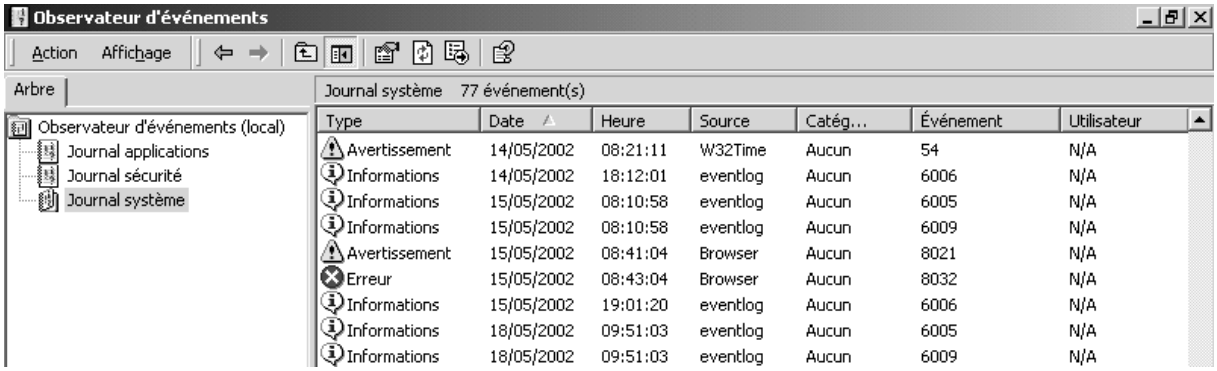
Lecture du journal à distance :

Si on a un compte autorisé, on peut dans l'observateur d'événement indiquer le poste sur lequel on souhaite travailler

Par le menu contextuel on peut choisir un poste du domaine

Lecture du journal d'évènement :

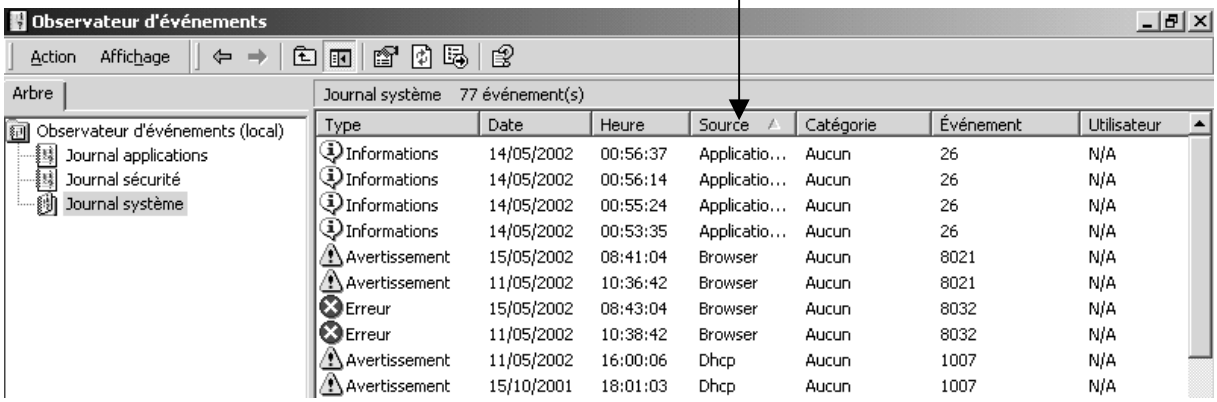
Un double –clic sur le journal, permet de "lire" le journal



Type	Date	Heure	Source	Catég...	Événement	Utilisateur
Avertissement	14/05/2002	08:21:11	W32Time	Aucun	54	N/A
Informations	14/05/2002	18:12:01	eventlog	Aucun	6006	N/A
Informations	15/05/2002	08:10:58	eventlog	Aucun	6005	N/A
Informations	15/05/2002	08:10:58	eventlog	Aucun	6009	N/A
Avertissement	15/05/2002	08:41:04	Browser	Aucun	8021	N/A
Erreur	15/05/2002	08:43:04	Browser	Aucun	8032	N/A
Informations	15/05/2002	19:01:20	eventlog	Aucun	6006	N/A
Informations	18/05/2002	09:51:03	eventlog	Aucun	6005	N/A
Informations	18/05/2002	09:51:03	eventlog	Aucun	6009	N/A

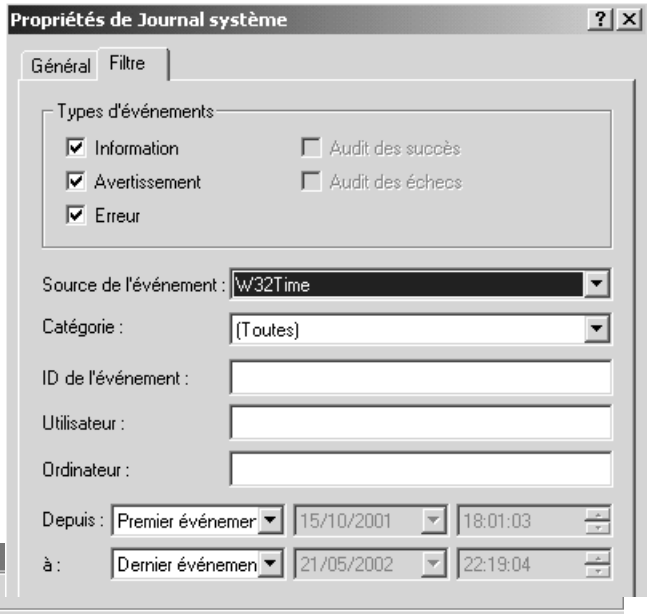
On peut trier le journal,

Ici par **Source**, il suffit de cliquer sur la colonne



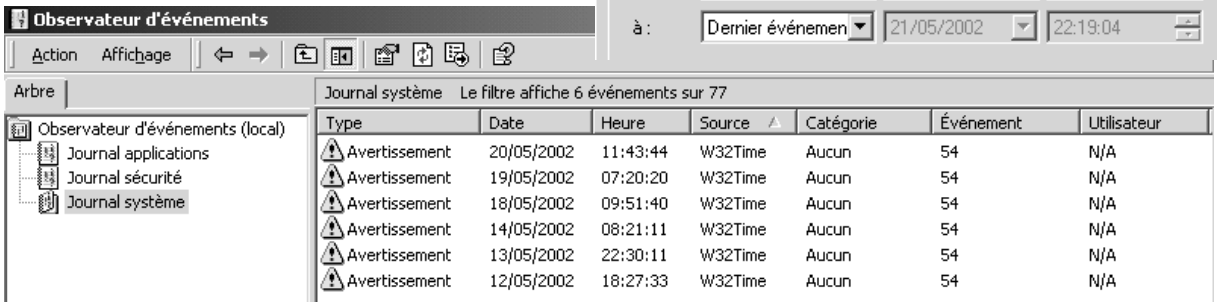
Type	Date	Heure	Source	Catégorie	Événement	Utilisateur
Informations	14/05/2002	00:56:37	Applicatio...	Aucun	26	N/A
Informations	14/05/2002	00:56:14	Applicatio...	Aucun	26	N/A
Informations	14/05/2002	00:55:24	Applicatio...	Aucun	26	N/A
Informations	14/05/2002	00:53:35	Applicatio...	Aucun	26	N/A
Avertissement	15/05/2002	08:41:04	Browser	Aucun	8021	N/A
Avertissement	11/05/2002	10:36:42	Browser	Aucun	8021	N/A
Erreur	15/05/2002	08:43:04	Browser	Aucun	8032	N/A
Erreur	11/05/2002	10:38:42	Browser	Aucun	8032	N/A
Avertissement	11/05/2002	16:00:06	Dhcp	Aucun	1007	N/A
Avertissement	15/10/2001	18:01:03	Dhcp	Aucun	1007	N/A

On peut filtrer le journal en passant par le **Affichage / Filtre**, on obtient alors



Dans lequel on peut exprimer une recherche…

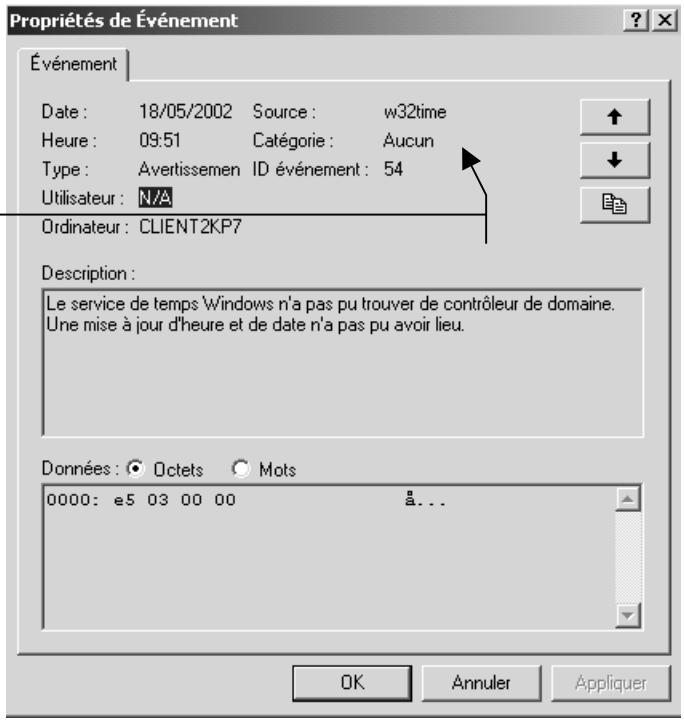
Ici tout ce qui touche a l'horloge de temps…



Type	Date	Heure	Source	Catégorie	Événement	Utilisateur
Avertissement	20/05/2002	11:43:44	W32Time	Aucun	54	N/A
Avertissement	19/05/2002	07:20:20	W32Time	Aucun	54	N/A
Avertissement	18/05/2002	09:51:40	W32Time	Aucun	54	N/A
Avertissement	14/05/2002	08:21:11	W32Time	Aucun	54	N/A
Avertissement	13/05/2002	22:30:11	W32Time	Aucun	54	N/A
Avertissement	12/05/2002	18:27:33	W32Time	Aucun	54	N/A

Identification du problème :

Ce n'est pas une chose très aisée…car le détail de l'événement n'est pas toujours d'une clarté biblique.



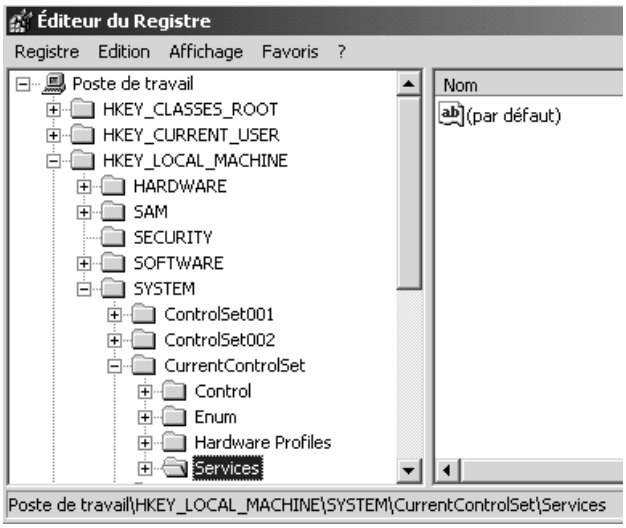
On dispose en général

D'un ID : ici **54**

D'une source : ici **w32time**

Localisation de la source

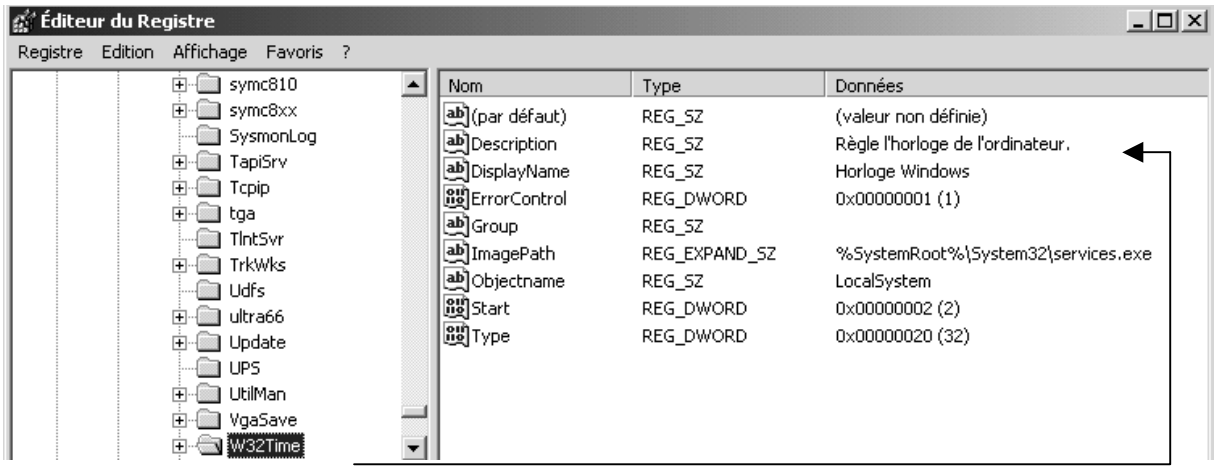
La source peut être parfois plus lisiblement traduite en faisant une recherche dans la base de registre : ainsi **w32time** peut être trouvé



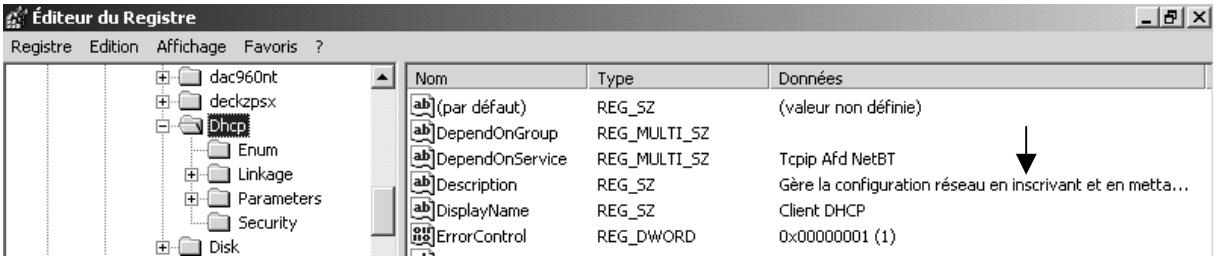
On se place sur la ruche

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services et on effectue une recherche de w32time…

on peut trouver une description



ou encore avec dhcp, par exemple



ID événement

Cet ID peut servir pour une recherche sur Technet, ou sur la base de connaissance en ligne de microsoft ou sur le site **www.eventid.net**

Par exemple le message concernant W32time à deux identificateurs, selon qu'ils apparaissent sur un poste 2000, **ID 54**, **(warning**) et selon qu'ils apparaissent sur un serveur Contrôleur de Domaine, **ID 62 (error)**

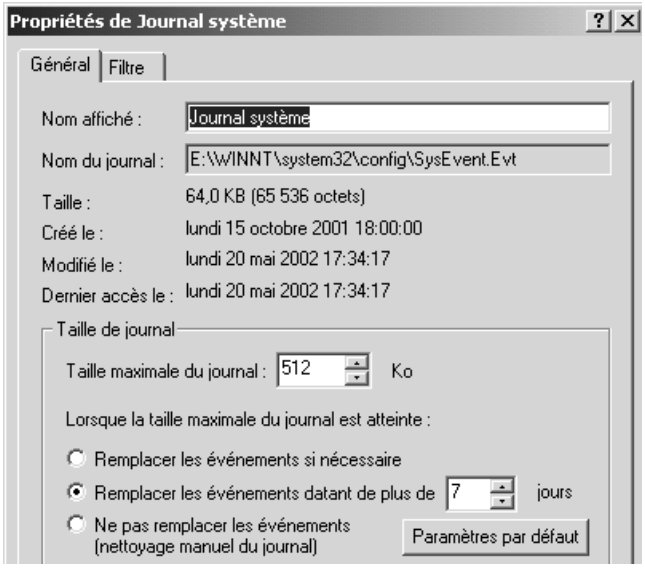
La commande pour qu'il se synchroniserait serait :

Net TIME /SetSNTP:nomserveur

Gestion des journaux :

Il est possible dans le menu **Action / …** d'effectuer une purge d'un journal, de le vider ou de l'archiver

Lorsque l'on est sur un journal on peut demander par le menu contextuel **propriété** pour définir sa taille (entre 64k et 4 Giga), quoi faire lorsque l'on atteint cette taille…

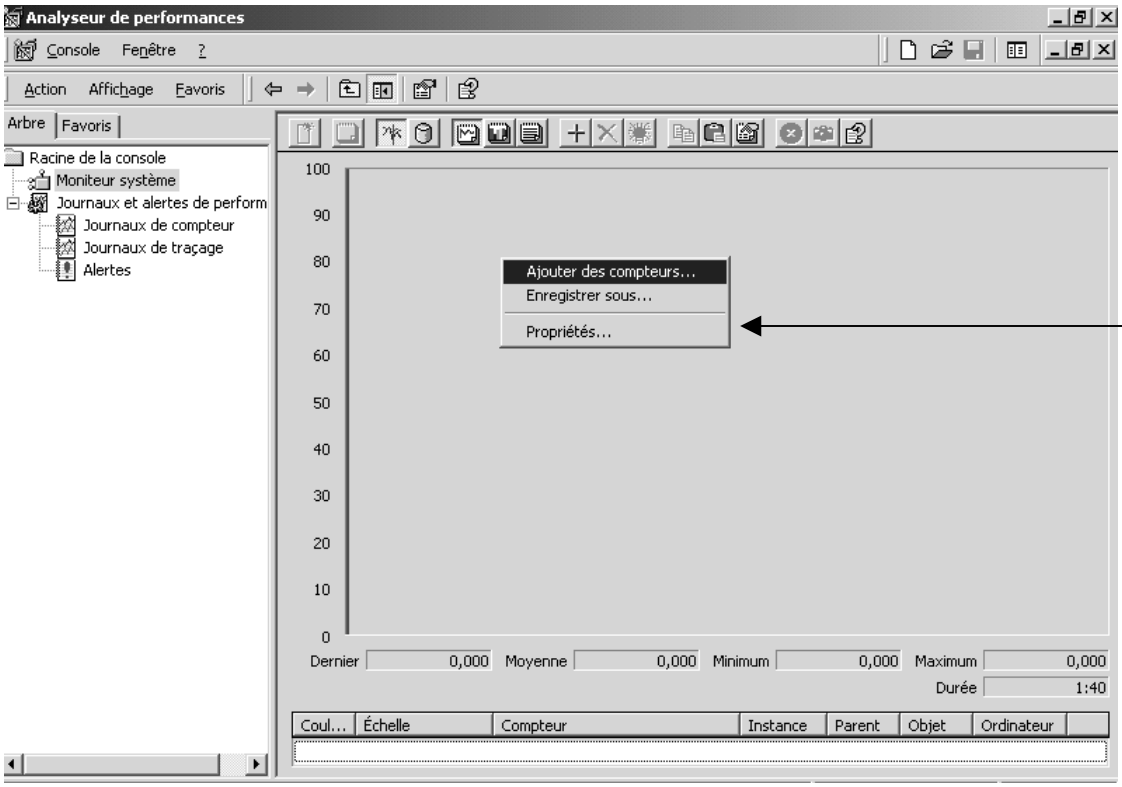


MONITEUR SYSTEME

L'analyseur de performance :

Il se lance depuis le menu

Outils d'Administration / Analyseur de performance

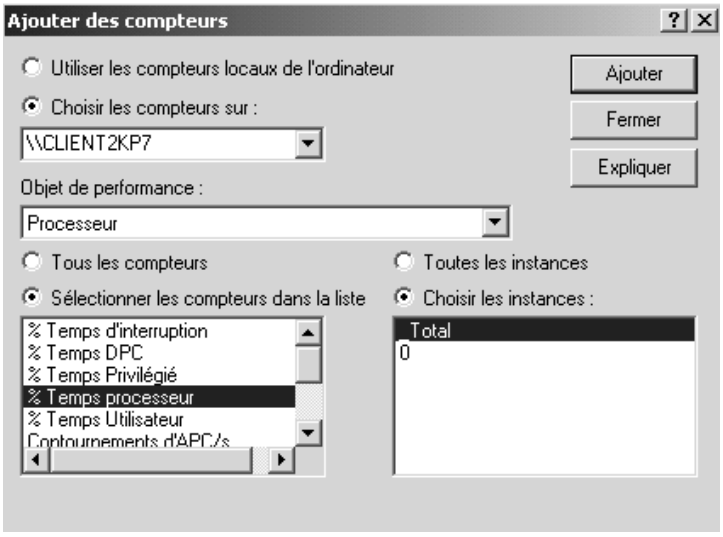


On ajoute des compteurs en demandant un menu contextuel à droite …

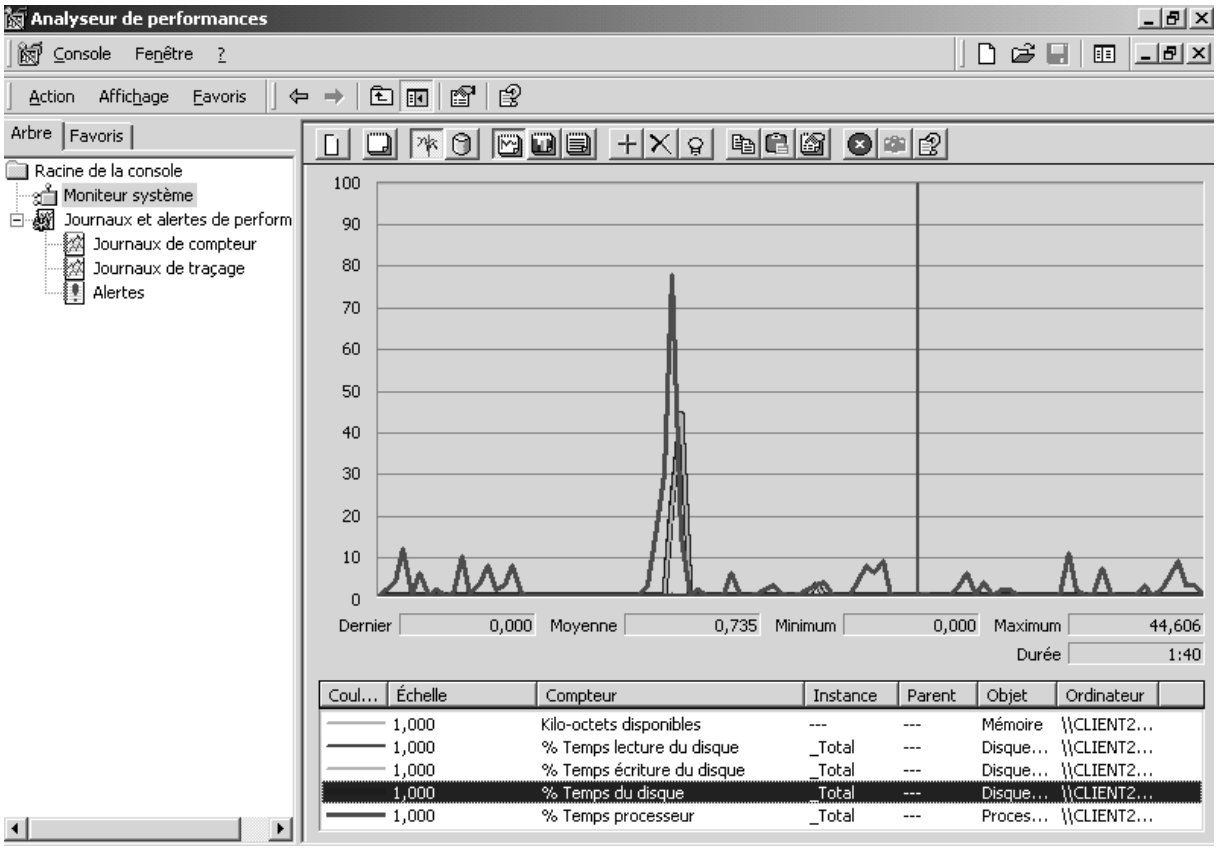
Et on peut créer des compteurs sur toute machine sur laquelle on peut accéder

Par exemple classiquement :

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



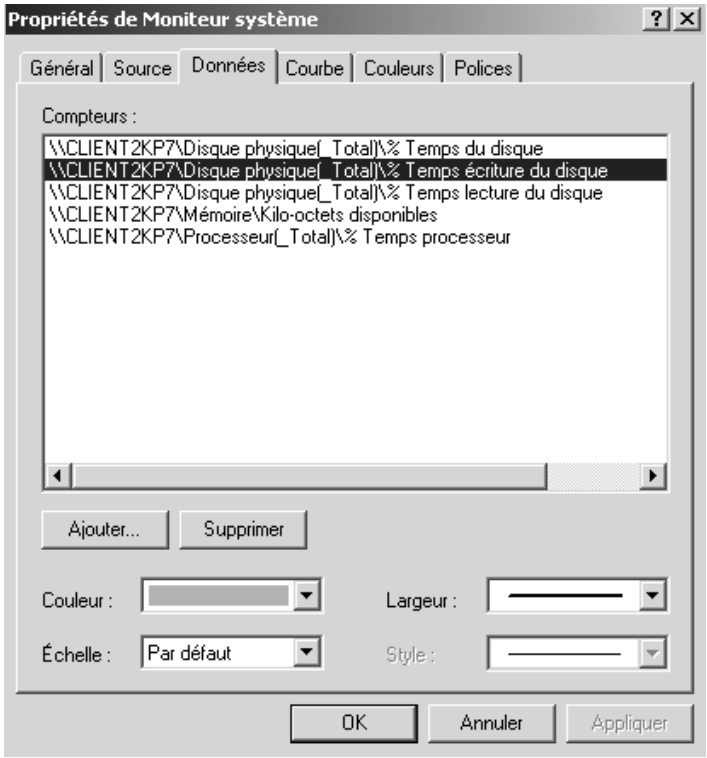
Créons un moniteur système surveillant ces points sur notre machine



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…

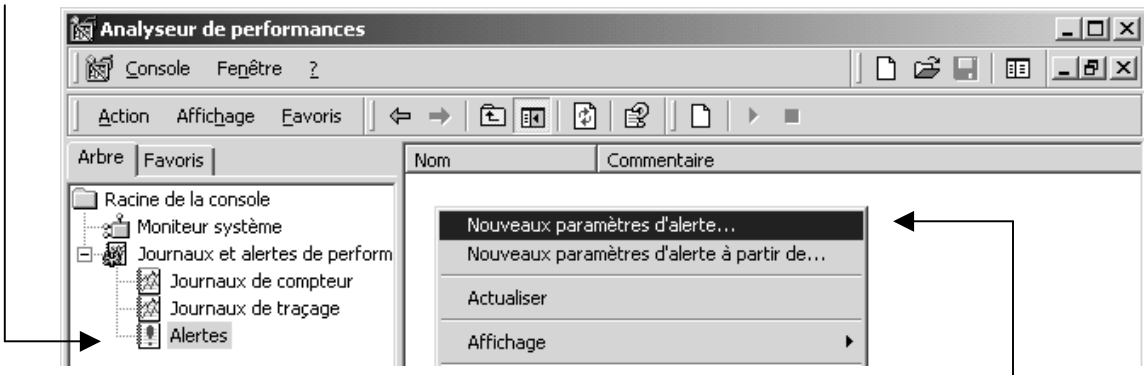


NB: Ajouter visuellement des compteurs, ne charge pas le processeur, car les compteurs sont renseigné automatiquement par le système, il s'agit ici simplement de décider de les afficher visuellement, ou non…

Gestion des alertes :

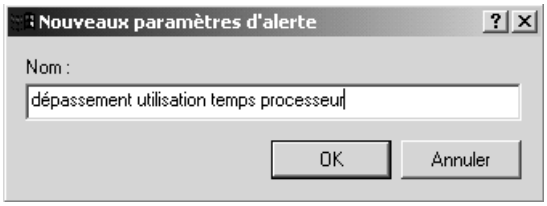
Ce qui est très intéressant, dans l'analyseur de performance, c'est la possibilité de configurer des alertes…permettant d'avoir une information comme quoi tel ou tel seuil est atteint ou dépassé !

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

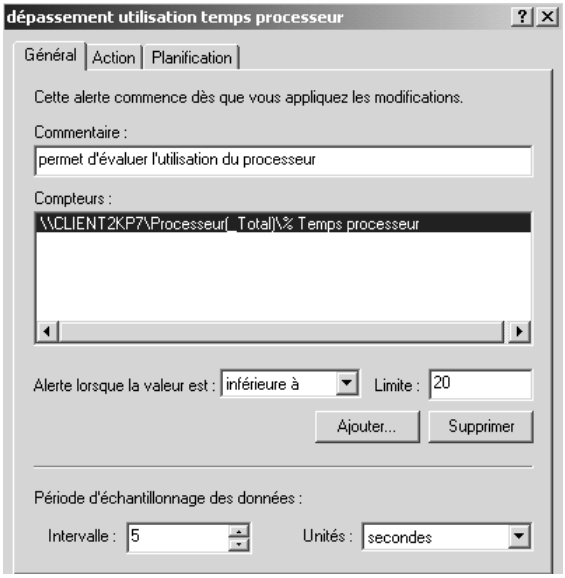


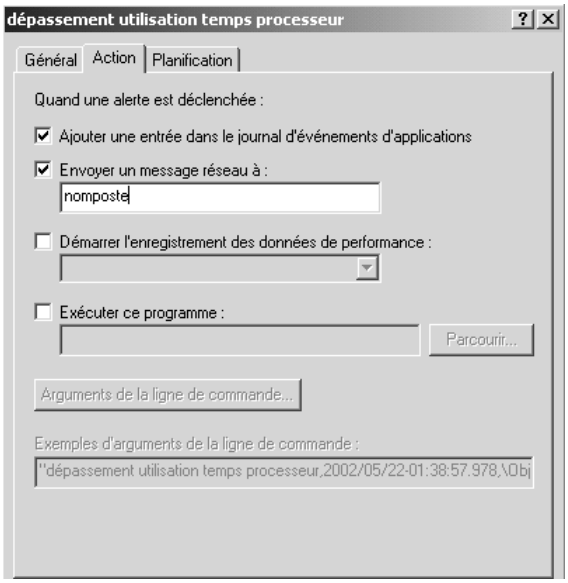
et demander à droite via le menu contextuel, **Nouveau paramètres d'alerte**

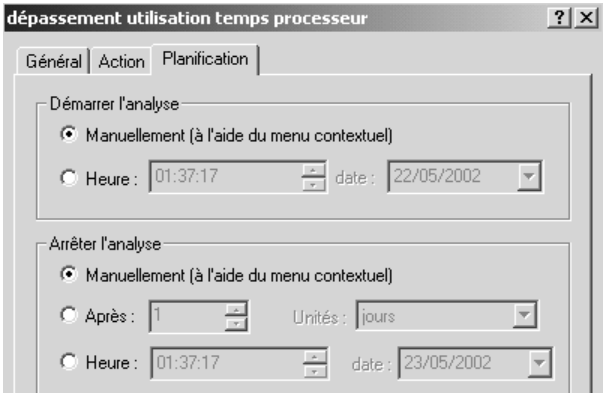
il faut donner un nom a notre détection d'alerte



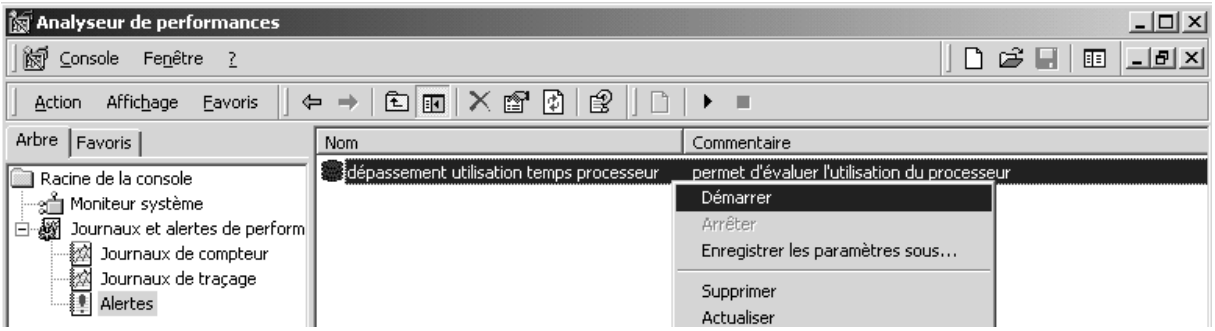
puis la paramétrer avec les 3 onglets **Général**, **Action** et **Planification**







Enfin il faut la démarrer avec le menu contextuel



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

STRATEGIES LOCALES 2000

Types de stratégie :

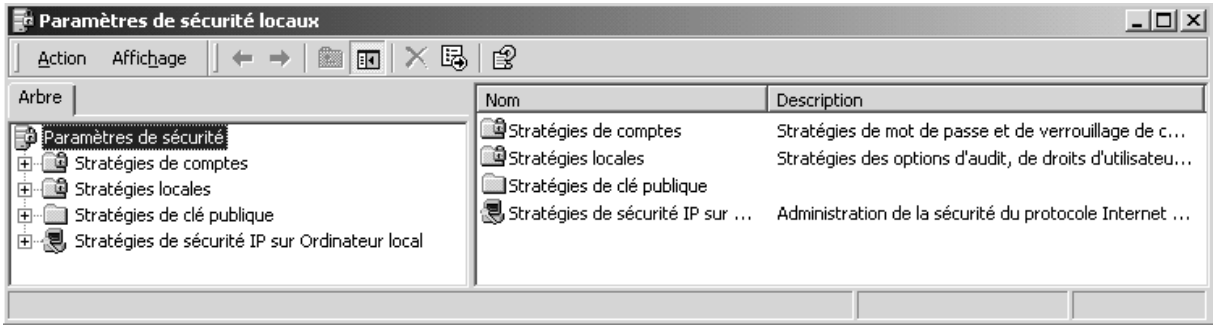
Les stratégies de sécurité permettent d'éviter que des utilisateurs modifient involontairement (ou volontairement) la configuration d'un ordinateur.

il existe essentiellement 2 méthodes pour implémenter des stratégies sur des postes 2000, par le biais d'une **stratégie système locale** appliquée sur un ordinateur unique, ou par le biais d'une **stratégie de groupe** appliquée dans un domaine et déployée sur plusieurs ordinateurs…

Stratégies sur un ordinateur local (cf microsoft GPO hors AD):

Lorsque un ordinateur n'appartient à aucun domaine, pour configurer une stratégie il faut obligatoirement passer par une stratégie locale…

Il faut passer par les **Outils d'administration / Stratégies de sécurités locales**,



Ces stratégies locales sont disponibles sur un poste 2000, (qu'il soit membre d'un domaine ou non) et sur un serveur 2000 (s'il n'est pas contrôleur de domaine). Mais lorsque l'on est dans un domaine, ces stratégies locales peuvent être écrasées par des stratégies de plus haut niveau.

Et que donc les paramètres locaux sont modifiées par stratégies dans cet ordre

stratégies locale – stratégie Contrôleur de Domaine /ou stratégies de Domaine

Stratégies de Groupe GPO (cf microsoft GPO dans AD):

Lorsque un ordinateur appartient à un domaine, pour configurer une stratégie on peut alors utiliser les stratégies de groupes dites GPO. Même si les stratégies de groupes seront étudiées ultérieurement, il faut savoir que l'on peut poser des stratégies de groupes à différents niveaux,

Et que donc les paramètres locaux sont modifiées par des GPO dans cet ordre

GPO Contrôleur de Domaine /ou GPO de Domaine – GPO d'U.O.

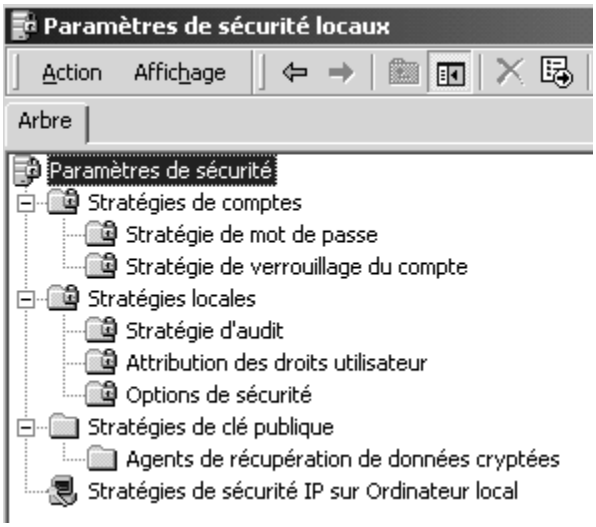
Configurer des stratégies localement :

Il ne faut pas confondre "*configurer des stratégies localement*", qui suppose que l'action soit faite localement sur chaque machine, avec la notion de "*paramètres de stratégie locale*".

En effet Les paramètres de stratégie locale sont configurables en partie localement depuis la console mmc "**Stratégie de sécurité locale**" mais aussi dans une **stratégie de groupe GPO**, définie au niveau du domaine ou d'une UO…

dans ce cas ces paramètres se superposent voire écrasent les valeurs définies via la console de stratégie se sécurité locale…

Les paramètres communs aux **Stratégie de sécurité locale** et aux **Stratégie de groupe GPO** sont donc les suivants:



- **Stratégies de compte**

  (~gestion utilisateur)
- **Stratégies locales**

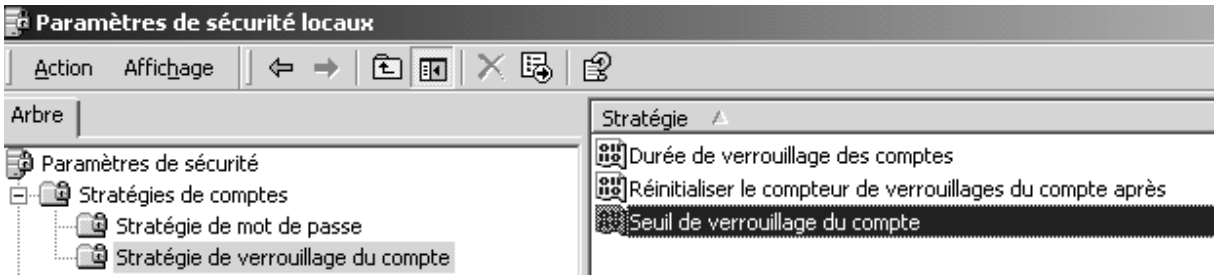
  (~qui peut ouvrir session locale)
- **Stratégies de clé publique**

  (agent de récupération)
- **Stratégies IPSEC**

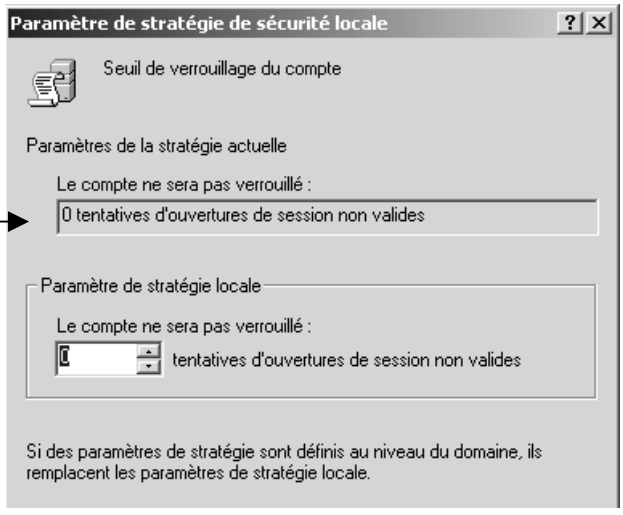
  (cryptage IP)

On se déplace alors dans l'arborescence proposée, et on visualise sur la droite les différentes composantes modifiables…

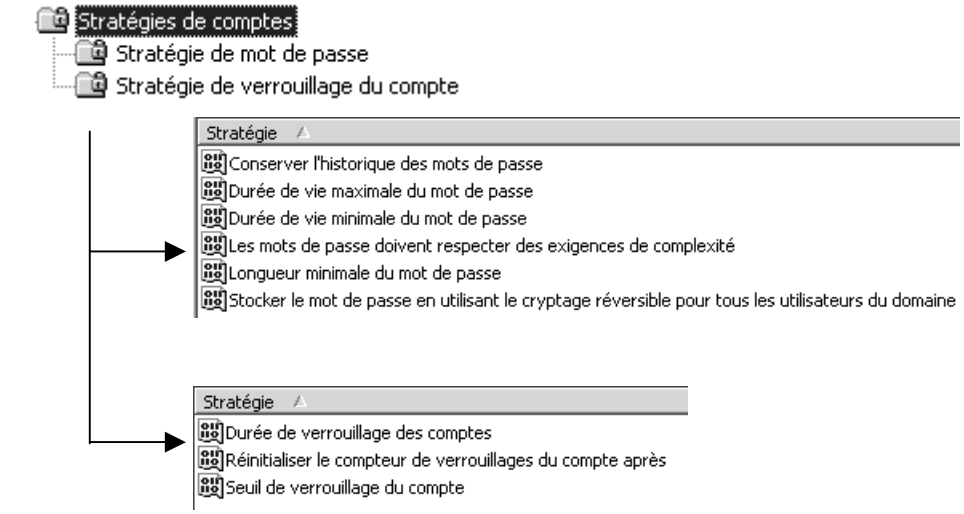
Par exemple, dans **Stratégies de compte, Stratégies de verrouillage du compte**

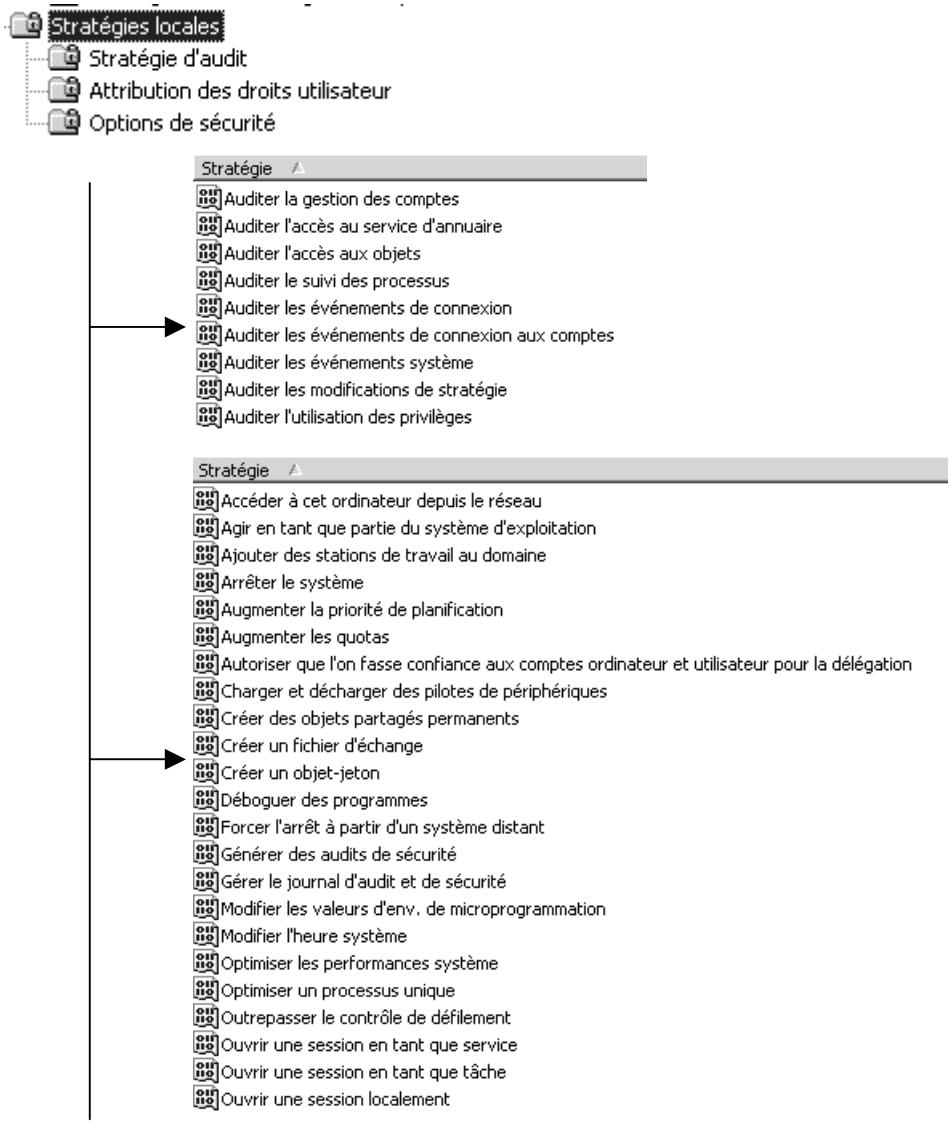


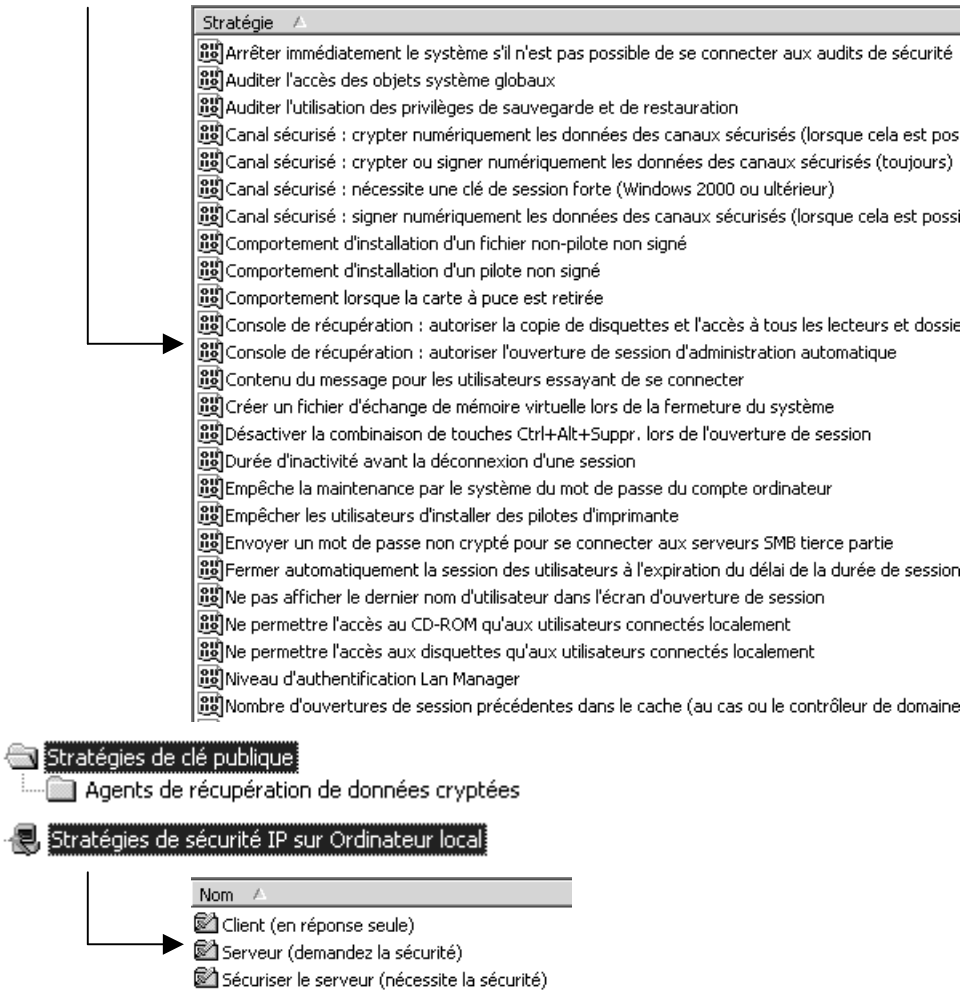
Sur lequel un double-clic amène



Contenu des Paramètres locaux de sécurité :







T.P: *script de mise à l'heure*

T.P: *stratégies locales 1°*

AUDIT (POSTE LOCAL)

Principe de l'audit :

Il est possible par un audit de suivre les évènements qui surviennent de la part d'un utilisateur, ou du système d'exploitation, sur **une machine donnée**.

Chaque événement est consigné dans un des journaux, appelé **journal de sécurité.**

Une **stratégie d'audit**, définit les type d'événement que l'on veut surveiller dans la liste suivante les moins importants sont présentés entre parenthèses():

- **Gestion des comptes** : un administrateur gère un compte ou un groupe, un compte est modifié (mot de passe…)
- **Accès à AD** : un utilisateur accède à AD (l'audit doit être posé sur les objets AD)
- **Accès aux objets** : un utilisateur accède à une ressource fichier, dossier, imprimante. (l'audit doit être posé sur chaque objet à auditer)
- **(Suivi des processus)** : uniquement pour les développeurs…
- **Connexion** : enregistre les sessions sur le poste, que celle-ci soient locales ou via le réseau, qu'elles utilisent un compte local ou de domaine, (l'audit est posé sur la station)
- **Connexion compte** : enregistre les demandes d'identification. Si la demande d'ouverture de session se fait sur le domaine, elle est reçue par un contrôleur de domaine ,l'audit doit être posé sur le contrôleur. Si elle est locale, l'audit doit être posé localement
- **(Evènements système)** : démarrage ou arrêt du poste…
- **(Modification de stratégie)** : modification aux options de sécurité ou aux stratégies …. D'audit
- **Utilisation de privilèges** : comme la possibilité de modifier l'heure système, ou lorsque un administrateur s'approprie un fichier

De manière générale donc, pour installer un audit, il va falloir :

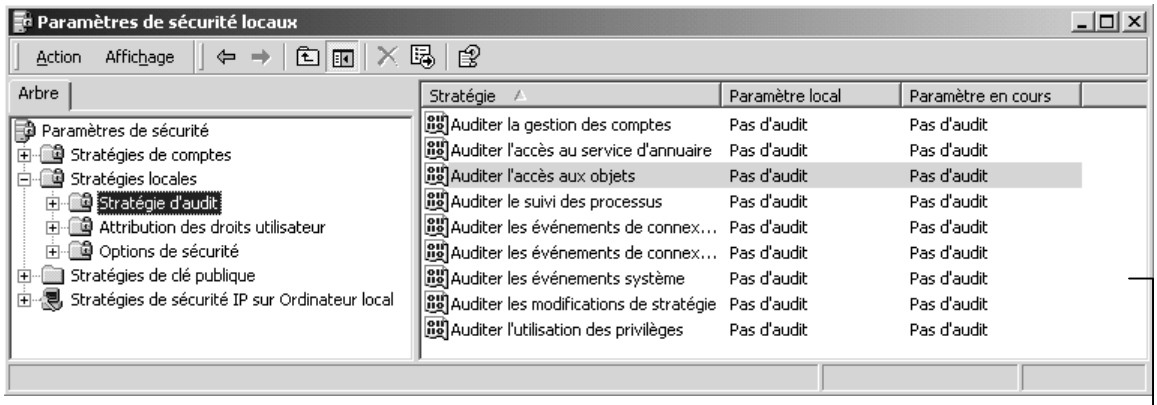
1. Choisir les postes où installer l'audit
2. Déterminer les évènements à auditer
3. Indiquer si on veut auditer les succès ou les échec

Installer un audit sur une machine:

Il faut passer par les **Stratégies de sécurités locales**,

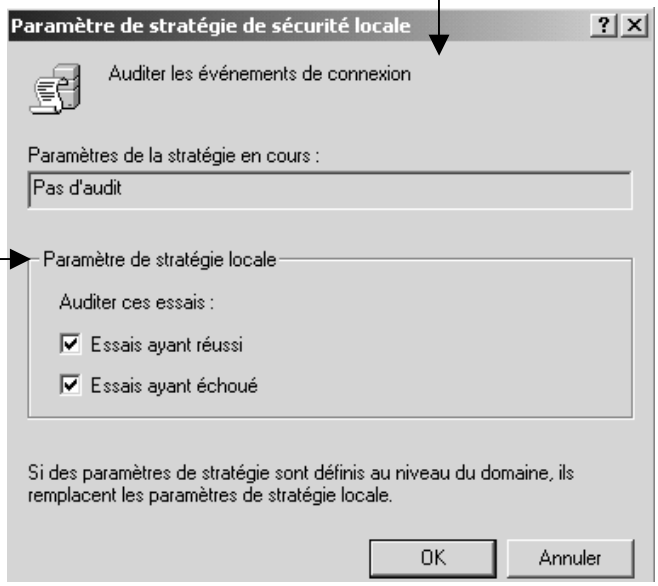
dans laquelle Il faut développer la clé

Stratégies locales / Stratégies d'audit



par exemple sur **connexion**

et en demandant d'auditer les réussites et les échec…



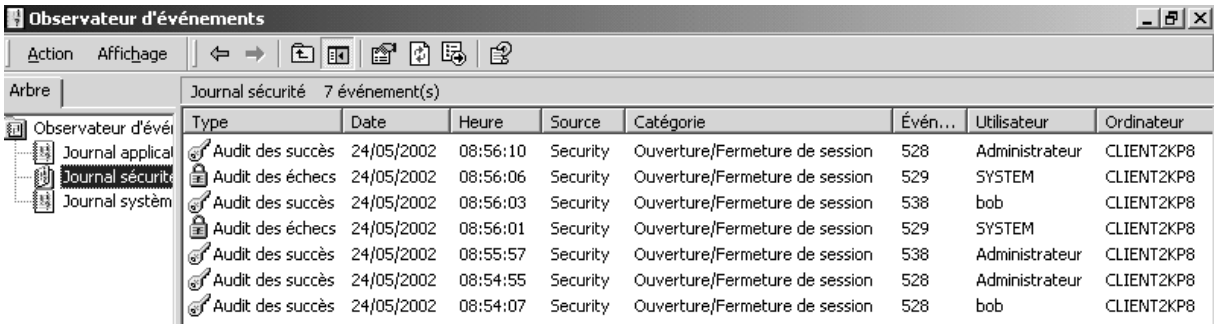
L'audit étant posé , mais non enregistré

il faut fermer la console pour que les modifications soient prises en compte et re-démarrer

…dans ce cas si on re-ouvre la console on voit alors

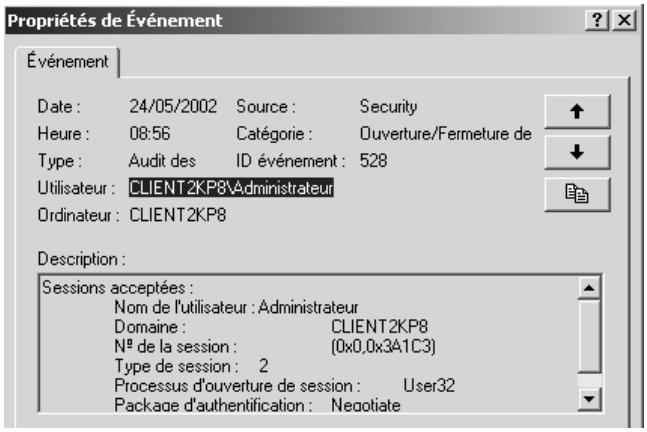
Lire le journal de sécurité:

Ensuite les évènements de sécurité sont consignés dans le journal d'événement



Dans lequel un double clic sur l'événement donne le détail

Audit succès



Audit Echec

T.P: *stratégies locales 2°*

Installer un Audit sur des ressources:

Lorsque l'on souhaite installer un **Audit sur des ressources**, l'opération se fait en deux temps. En effet il ne suffit pas de demander d'activer l'audit sur telle ou telle type d'événement (comme cela était le cas pour les session, ou les identification du chapitre précédant), mais il va falloir aussi activer l'audit sur les ressources que l'on veut observer…

Il faut donc :

1. activer le type d'audit souhaité , c'est à dire Audit "**Accès aux objets**"dans les stratégies locales de l'ordinateur
2. activer ensuite "**pour chaque ressource**" l'audit particulier

Audit sur un dossier

Il faut

1. activer l' Audit "**Accès aux objets**"dans les stratégies locales de l'ordinateur sur lequel le dossier de Pierre se trouve
2. sur le dossier de Pierre activer les propriétés avancées NTFS et demander Audit pour tout le monde en Echec

T.P: *stratégies audit acces dossier*

Audit sur une imprimante

On veut savoir qui utilise l'imprimante :

Il faut

1. activer l' Audit "**Accès aux objets**"dans les stratégies locales de l'ordinateur sur lequel l'imprimante est connectée
2. sur cette imprimante demander Audit pour tout le monde en réussite

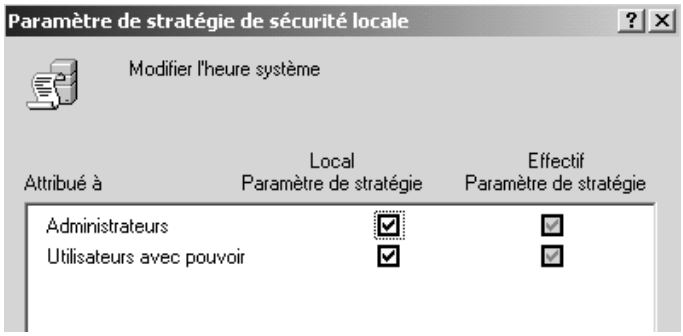
STRATEGIES DE DOMAINE OU DE CD

Stratégies de Domaine :

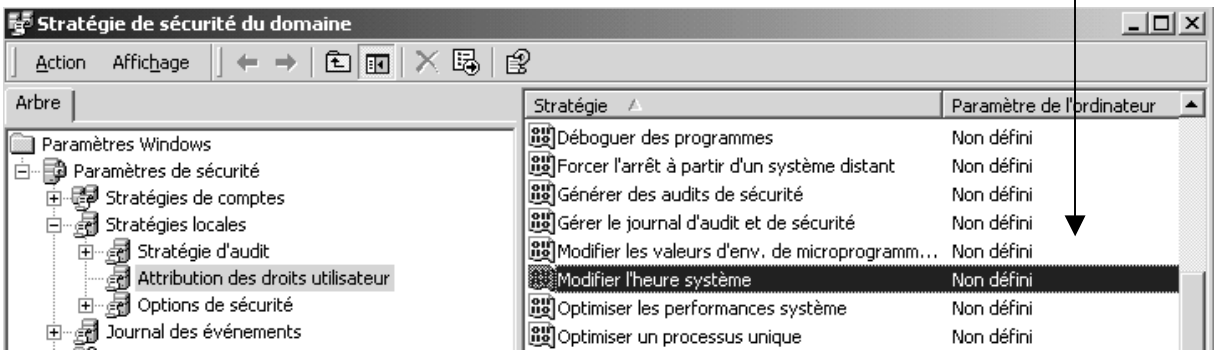
Lorsque l'on configure une stratégie de domaine, cela signifie que l'on souhaite que cette stratégie s'applique à toutes les machines de notre domaine.

Encore faut-il que cette stratégies soit définies au bon endroit, et transmise….

Sur un client du domaine, voila l'aspect de la **stratégie locale** concernant qui peut mettre à l'heure la machine....

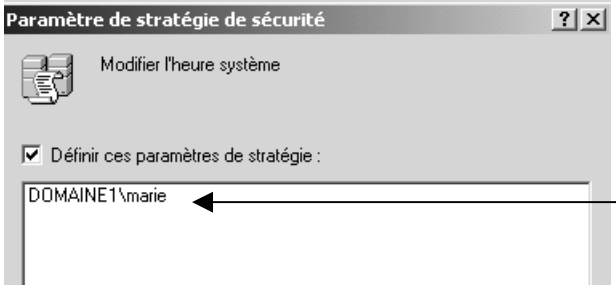


Sur le serveur de Domaine, on définit une **stratégie de domaine** qui par défaut est non activée



en spécifiant que l'utilisateur marie a ce droit de mise à l'heure…

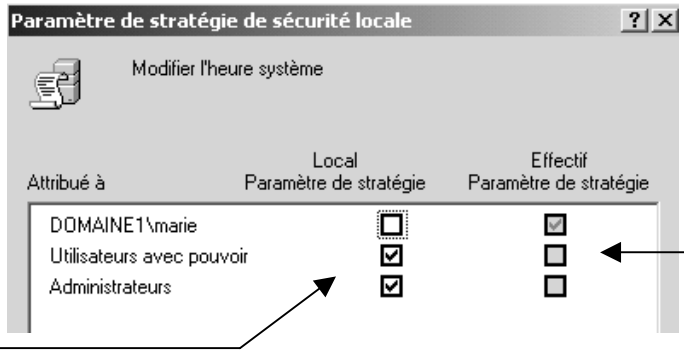
N.B : On active cette stratégie →



← Avec un utilisateur

Lorsque la stratégie de domaine à pu se propager, normalement sur le client la visualisation des stratégies locales devrait donner :

Pas de changement localement



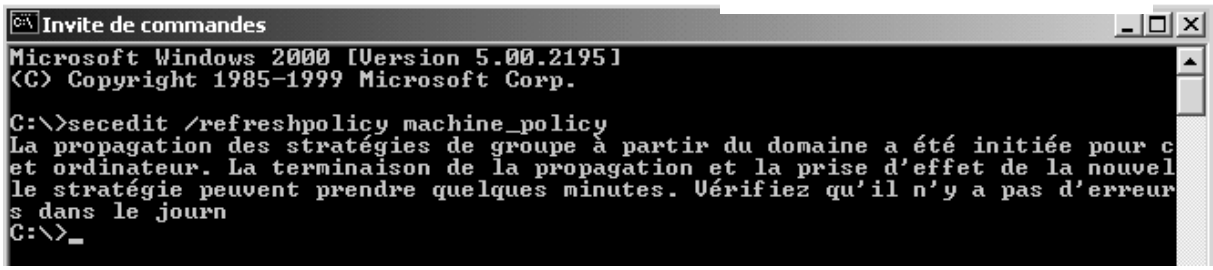
Mais ici on a récupéré la stratégie de domaine

N.B: Normalement une stratégie se propage à **chaque démarrage de poste**, puis **toutes les 5 à 60 voire 90 minutes**, et lorsque les paramètres de sécurité locale sont modifiés…

Il est bien sûr toujours possible de forcer le rafraîchissement à l'aide de la commande

Secedit /refreshpolicy machine_policy

(Voir détail de la commande secedit dans le chapitre sur les GPO…)

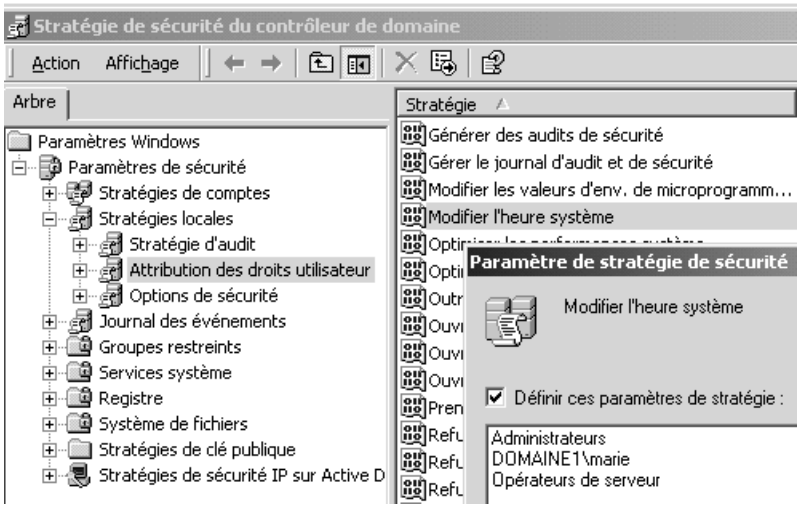


effectivement, dans le journal on peut observer

Stratégies de Contrôleur de Domaine :

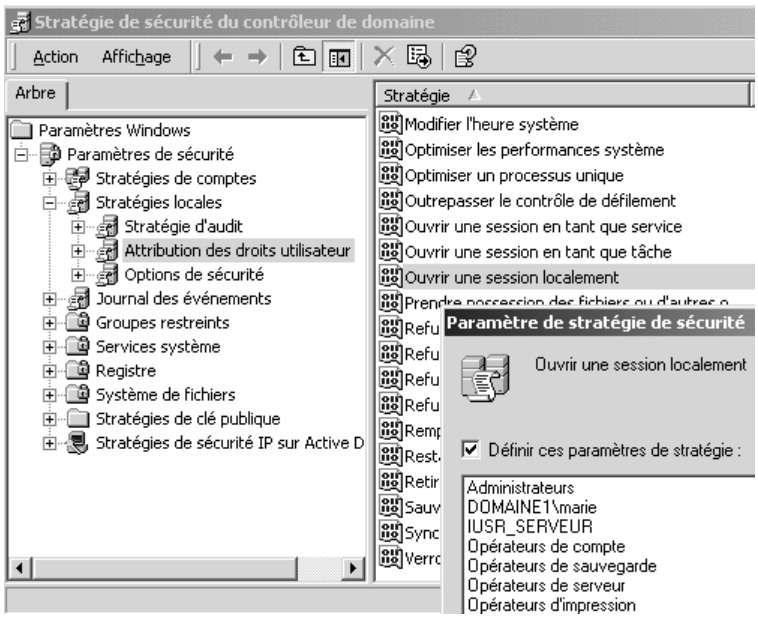
Lorsque l'on configure une stratégie de Contrôleur de domaine, cela signifie que l'on souhaite que cette stratégie s'applique à toutes les machines ayant ce rôle, et uniquement celles-ci. (cela peut représenter uniquement notre serveur CD)

Sur le serveur de Domaine, on définit une **stratégie de contrôleur de domaine** qui par défaut est non activée

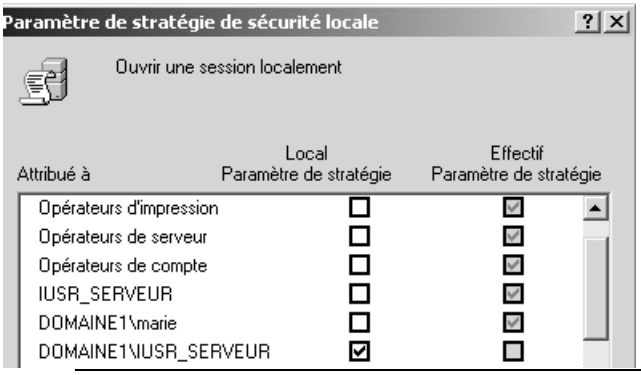


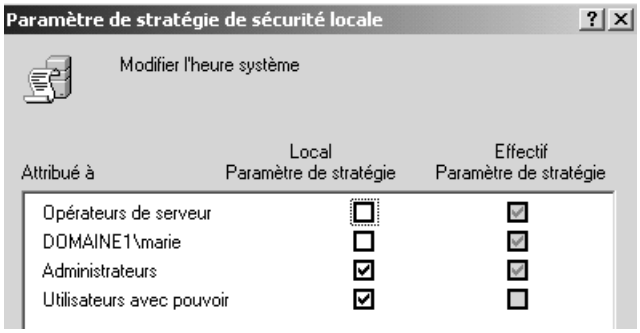
en spécifiant que l'utilisateur marie a ce droit de mise à l'heure…

Mais qu'elle dispose aussi du droit d'ouverture de session locale



Sur le serveur de Domaine, on visualise alors une **stratégie locale** qui montre les options reçuent au niveau du CD :





MODELE DE STRATEGIES

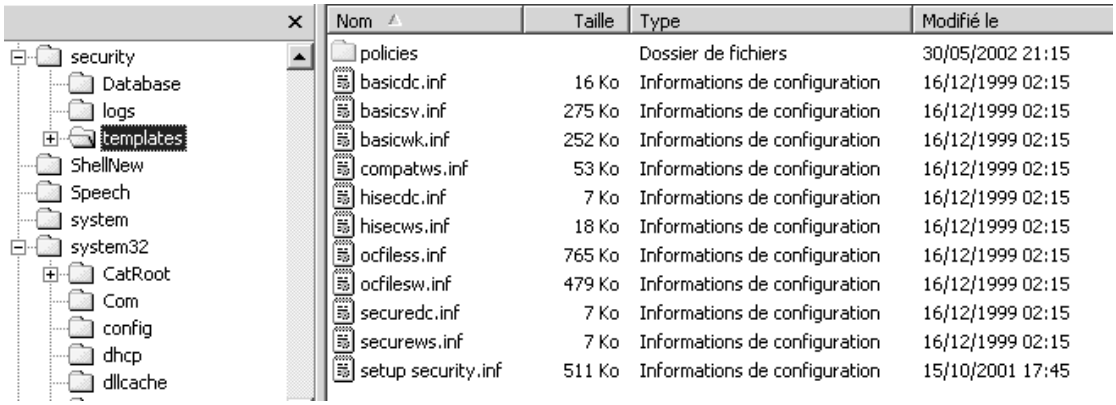
Les modèles de stratégie de sécurité:

N.B: La notion existe déjà sous NT4 avec les fichiers **Ntconfig.pol**, que l'on créait avec le poledit de NT, voire sous win95-98 avec les fichiers **Config.pol** que l'on créait avec le poledit de windows…
on peut continuer à s'en servir en plaçant ces fichiers dans **SYSVOL\Sysvol\domaine\Scripts**…(là où l'on met les scripts de connexion)

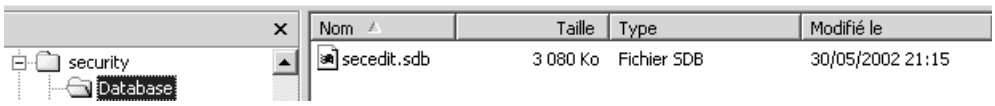
Par rapport aux variables modifiables via les paramètres de sécurité locale, les stratégies de groupes nommées aussi GPO fonctionnent avec une notion de modèle. Ce modèle étant exportable, on pourra, dans le chapitre suivant, voir comment créer des GPO de domaine , ou d'Unité Organisationelle…

Pour l'instant, on va dire que **un modèle de stratégie**, permet **de modifier globalement la sécurité d'une machine par l'application d'un modèle pré-défini** (ou bien défini par nous même), alors que les paramètres de sécurité locale nécessitaient une modification manuelle de chaque valeur…

Les modèles de stratégie sont définis dans des fichiers xxxx**.inf** stockés en général dans **Winnt\Security\Templates**



La base de donnée dans laquelle on utilise le modèle est unique (une seule base par machine), et se trouve dans un fichiers **xxxxx.sdb** dans le dossier **Winnt\Security\Database**



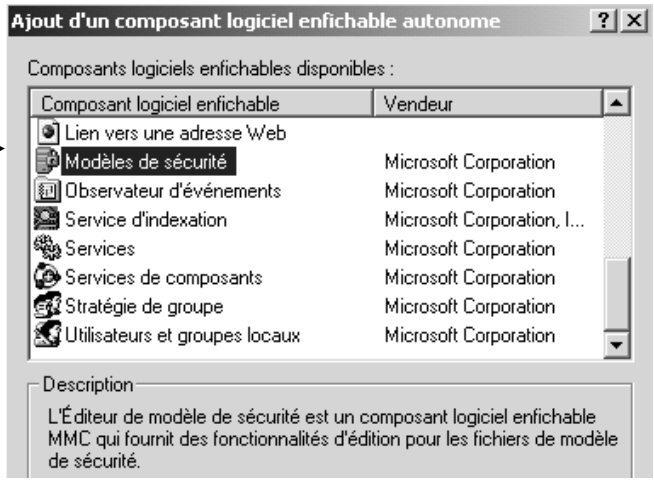
Il va falloir :

1. se créer un modèle (ou prendre un modèle prédéfini)
2. ouvrir le modèle dans la base de donnée de sécurité
3. appliquer la base de sécurité au poste

Création d'un modèle:

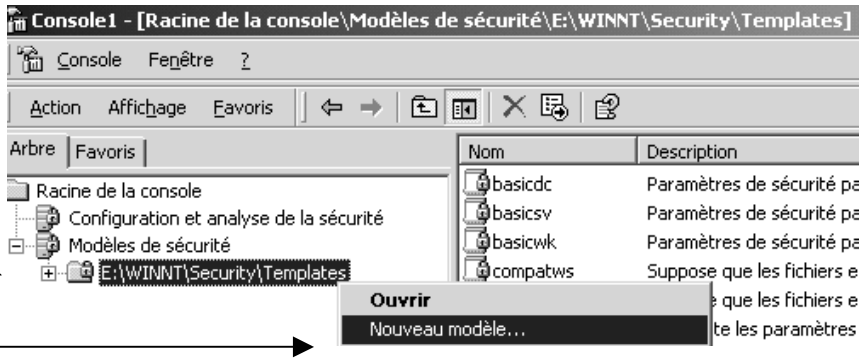
Il faut avoir une mmc permettant de gérer les modèles, cette mmc se nomme

Modèles de sécurité



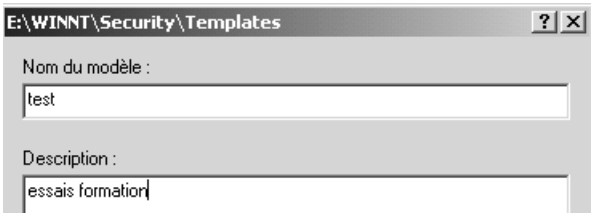
Dans cette mmc tous les modèles prédéfinis apparaissent évidemment on décide de se créer un modèle personnalisé

Clic droit sur le dossier dans lequel les modèles sont stockés



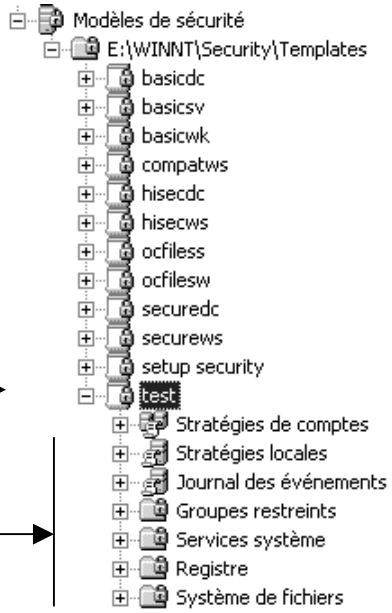
puis

Nouveau modèle



et on lui donne un nom

On obtient alors notre modèle de sécurité



Dans lequel on reconnaît les paramètres de sécurité que l'on modifiait en local, ainsi que les autres…

Effectuons une modification, pour l'instant un peu… futile

Dans les **stratégies locales / options de sécurité**

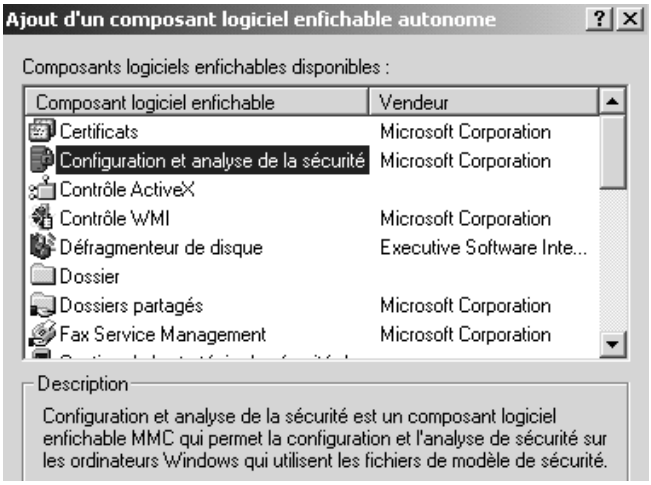
on prévoit de donner un message :"*super, bravo*", sans oublier le titre qui va avec

Pour enregistrer le modèle, il faut se placer sur le modèle et demander **clic droit, enregistrer…**

Création d'une base locale de sécurité:

Il faut avoir une mmc permettant de gérer les bases, cette mmc se nomme

Configuration et analyse de la sécurité ⟶



Cette console permet d'ouvrir une base de donnée existante (pour la manipuler) ou en crée une nouvelle à l'aide d'un modèle…

Pour ouvrir une base de donnée existante

1. Cliquez-droit sur l'élément étendu de *Configuration et analyse de la sécurité*.
2. Cliquez sur **Ouvrir la base de données**
3. Sélectionnez une base de données et cliquez sur **Ouvrir**

Pour créer une nouvelle base de données

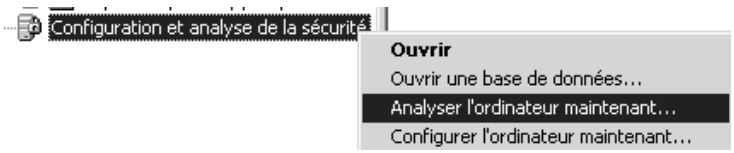
1. Cliquez-droit sur l'élément d'étendue *Configuration et analyse de la sécurité*.
2. Cliquez sur **Ouvrir la base de données**
3. Entrez un nouveau nom de base de données et cliquez sur **Ouvrir**.
4. Sélectionnez un fichier de configuration de sécurité à importer puis cliquez sur **Ouvrir**.

Nous avons besoin de la créer donc on va Ouvrir la base, lui donner le nom **essais.sdb** et sélectionner le fichier **test.inf** crée auparavant…

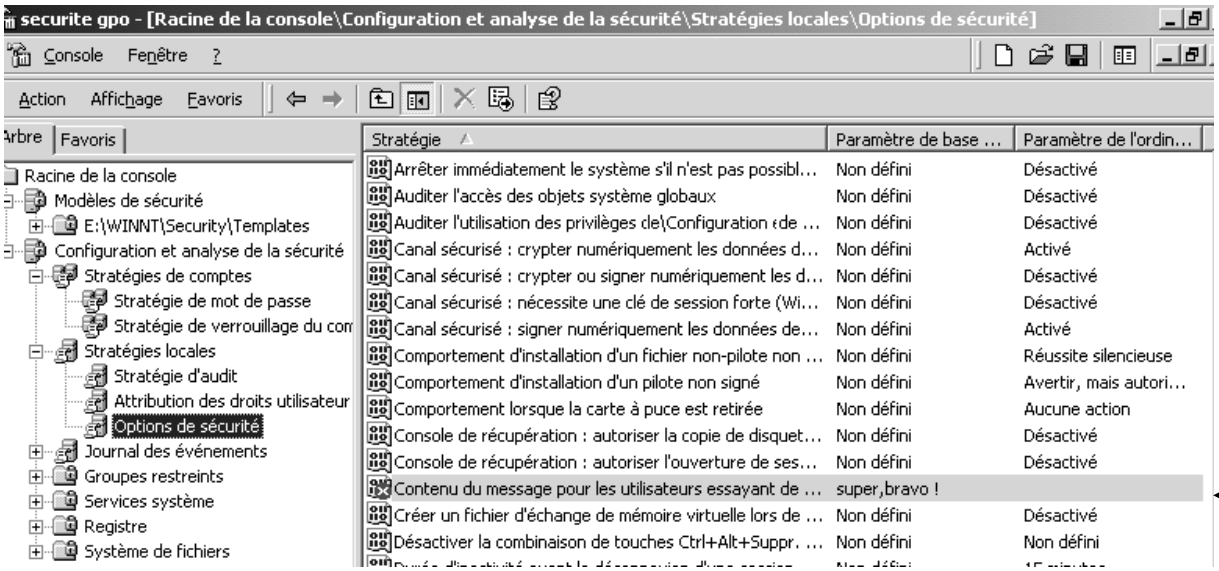
Maintenant nous avons une base de donnée crée avec un modèle chargé !

Vérification modèle - poste:

Il est possible désormais soit d'appliquer notre modèle à l'ordinateur, soit de **analyser la configuration** actuelle de l'ordinateur…. C'est plus prudent !



on accepte le chemin du journal par défaut puis on peut parcourir l'arborescence **pour visualiser les différences entre le modèle chargé, et la configuration actuelle**!

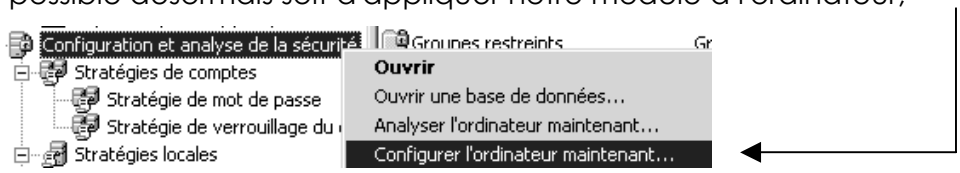


NB: toutes les différences sont marquées d'une croix rouge

Lorsque l'on est content, on peut appliquer notre modèle + base à notre machine

Application du modèle sur le poste

Il est possible désormais soit d'appliquer notre modèle à l'ordinateur,



Si on effectue une vérification après application, les modification sont marquées d'une coche verte…

Modification du modèle

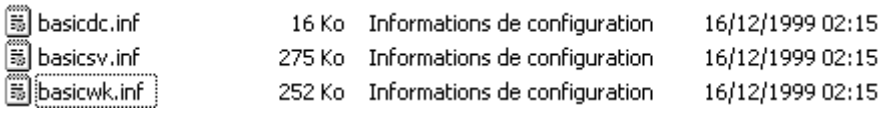
Si on souhaite modifier notre structure, on modifie le modèle, puis dans la base actuelle on importe la nouvelle mouture du modèle…

On peut aussi se créer une nouvelle base, pour être sûr de partir sur le bon pieds…

Suppression d'une stratégie

Si on veut "sortir" une machine du réseau, et permettre de retrouver un poste standard, il faut annuler notre stratégie…

Cela peut se faire en appliquant les modèle de sécurité de base

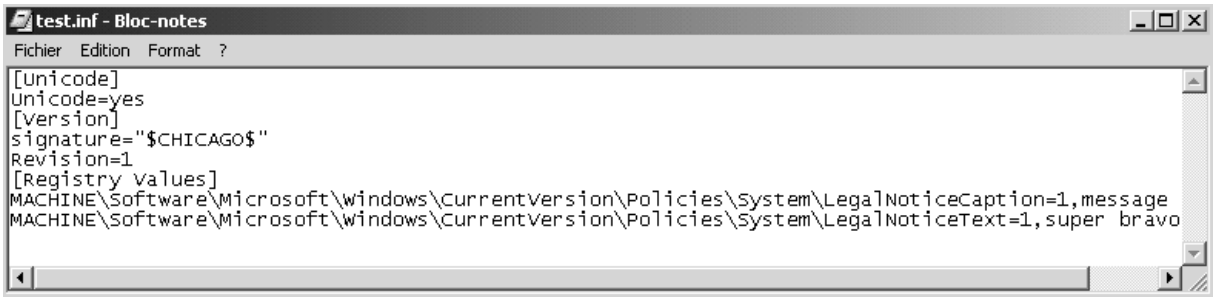


Ainsi par exemple pour une station 2000 le modèle se nomme **basicwk.inf**

Il suffira d'importer ce modèle dans notre base, et de l'appliquer à notre machine…

Clés de registre… d'une stratégie

On peut avoir une idée des modification apportées au niveau de la base de registre, en visualisant le contenu de notre modèle…



Résumé

On se: crée un modèle xxxxx.inf (rien ne se passe)

On ouvre/crée une base de donnée xxxx.sdb (rien ne se passe)

On importe un modèle (rien ne se passe)

On analyse différence entre base et registre (rien ne se passe)

On configure le poste (on modifie la base de registre)

N.B: à partir du moment ou l'on a configuré le poste, la base contient des informations différentes du modèle utilisé, car elle est un résultat de (modèle+registre). Dans le doute, refaire une base avec une copie propre du modèle et recommencer. A la limite, appliquer le modèle de sécurité de base, puis réappliquer le modèle spécifique

N.B: Faire attention aux modèles dans lesquels on ne spécifie rien pour une clé, cela ne rétablira pas la clé dans sa valeur par défaut, mais cela la laissera en l'état

T.P: *modèle de stratégie*

GPO D'UNITE ORGANISATIONELLE

Types et niveaux de stratégie :

GPO signifie Group Policy Object

On l'a déjà dit mais rappelons que l'on peut poser des stratégies à différents niveaux, (dites aussi GPO hors domaine) pour être complet, on dira donc les paramètres locaux sont modifiées par stratégies dans cet ordre

stratégies locales – stratégies CD /ou de Domaine

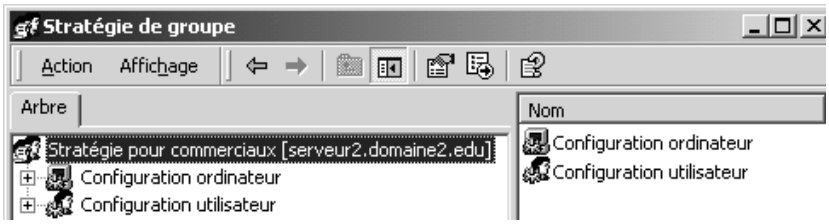
Alors que les stratégies GPO s'appliquent donc dans cet ordre

GPO de site – GPO de Domaine/ou de CD – GPO d' Unité Organisationnelle

Pour un ordinateur on aura donc alors

Stratégies locales – stratégies CD /ou de Domaine – GPO de site – GPO de Domaine/ou de CD – GPO de Unité Organisationnelle

Les GPO de domaine (ou d'Unité Organisationelle) se décomposent en deux catégories



Les paramètres de **stratégie de groupe pour les ordinateurs** (valables a la mise sous tension du poste, puis lors de rafraîchissement périodiques… cf secedit…)

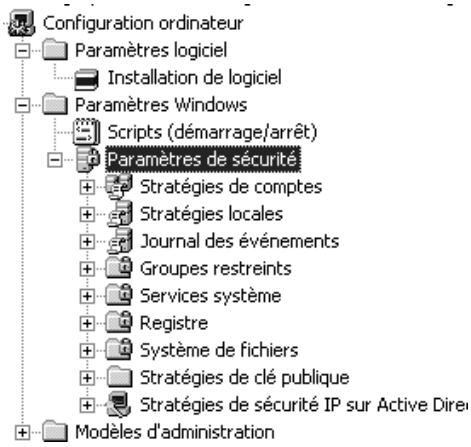
Les paramètres de **stratégie de groupe pour les utilisateurs** (valables a chaque ouverture de session puis lors de rafraîchissement périodiques… cf secedit…)

Par défaut, les stratégies de groupes ont un traitement synchrone, c'est à dire :

- les **stratégie de groupe pour les ordinateurs** s'exécutent avant que le message de bienvenue dans windows ne s'affiche.
- les **stratégie de groupe pour les utilisateurs** s'exécutent avant que l'interpréteur de commande du système ne soit activé et mis à la disposition de l'utilisateur.

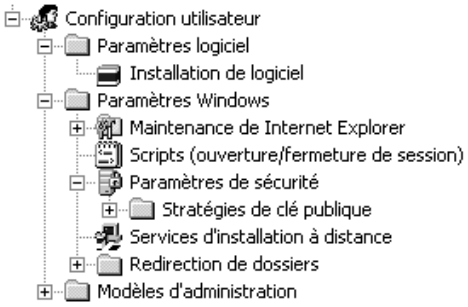
Les ajouts notables dans les **stratégie de groupe pour les ordinateurs** sont:

1. les scripts de machine, avec les scripts de démarrage et les scripts d'arrêt…
2. l'installation de logiciel



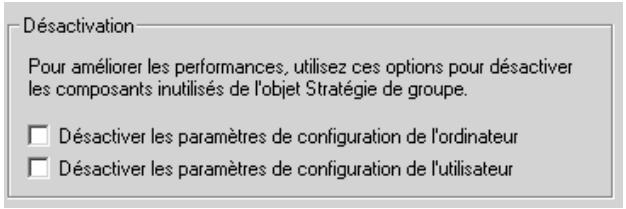
Les ajouts notables dans les **stratégie de groupe pour les utilisateurs** sont:

1. Les installations de logiciels
2. les scripts d'ouverture et de fermeture de session (doublon avec compte util…)
3. redirection de dossier



N.B: les scripts qui sont gérés par les stratégies ne sont pas récupérés par les clients autres que 2000

N.B: Dans une stratégie on peut au niveau de ses propriétés invalider la catégorie que l'on ne pense pas utiliser (amélioration de la vitesse de connexion)



Niveau de modification dans la base de registre

Lorsque l'on manipule les paramètres de **stratégies de sécurité locale**, (ce qui ne peut se faire que depuis le poste, comme on l'a vu dan le chapitre des stratégies locales…) on fixe les modifications dans la base de registre au niveau des clés

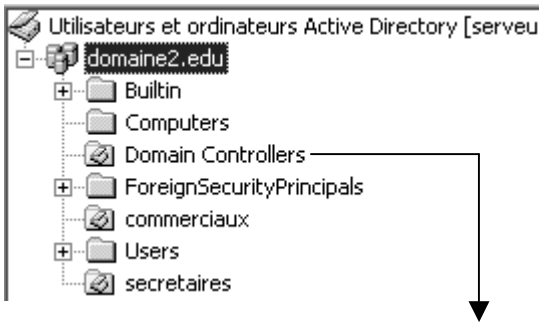
HKEY_LOCAL_MACHINE Et **HKEY_CURRENT_USER**

Ces modifications sont permanentes sur la machine, que cette machine soit membre d'un domaine ou non. C'est pour cette raison que ces **stratégies de sécurité locale** sont le seul moyen de gérer la sécurité sur des machines seules, hors domaine.

Lorsque l'on manipule les paramètres de **stratégies de sécurité de groupe**, on fixe les modifications dans la base de registre au niveau des clés qui seront effacées si la GPO ne s'applique plus, en clair les paramètres de stratégies GPO ne s'appliquent plus, et on retrouvera les paramètres de stratégie locale.

Stratégies Prédéfinies existantes :

SI on regarde dans **Utilisateur et ordinateurs Active Directory**

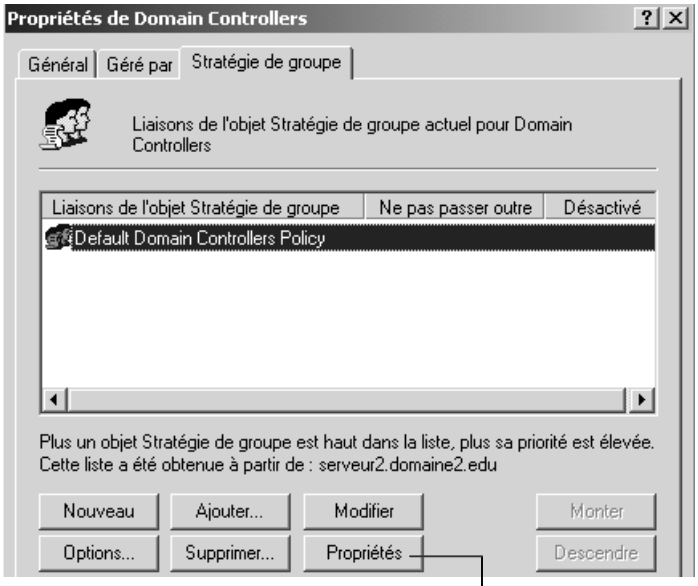


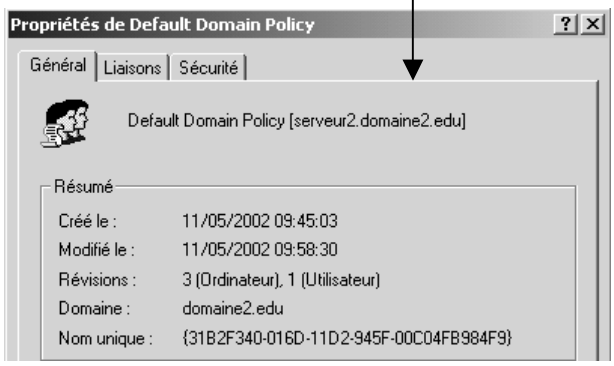
Il existe une GPO pour le **Domain**

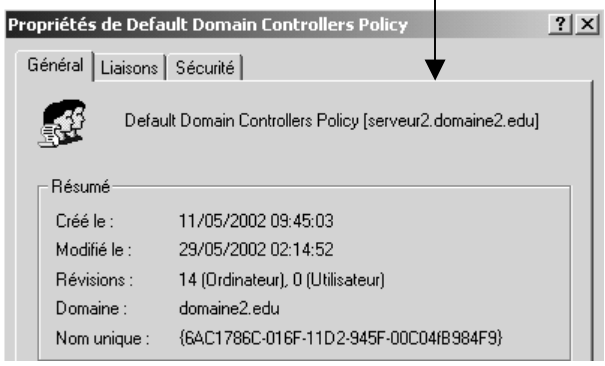
(ici le pointeur)

Et Il existe une GPO pour **Domain Controllers**

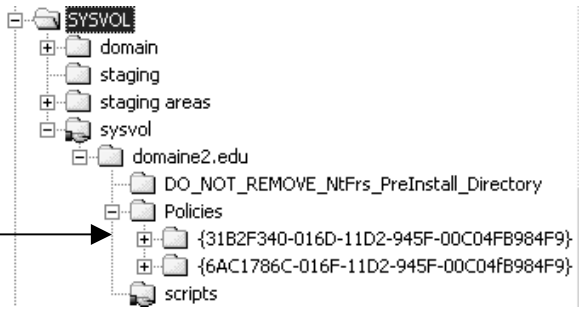
(ici le pointeur)







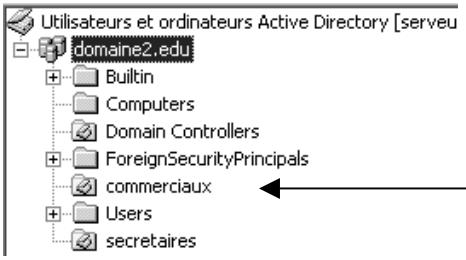
Stockées physiquement dans sysvol (qui est répliqué entre CD../..)



N.B: les stratégies de groupes sont aussi visibles depuis la mmc **Utilisateur et ordinateurs Active Directory** en demandant **Affichage / fonctionnalité avancées**, dans le conteneur **Domaine, System, Policies** (il s'agit en fait de pointeurs sur les GPO physiquement stockées dans sysvol)

Définir une Stratégie de Groupe sur une U.O :

Ayant ouvert une session sur un serveur contrôleur de domaine, il faut lancer la mmc **Utilisateur et ordinateurs Active Directory**

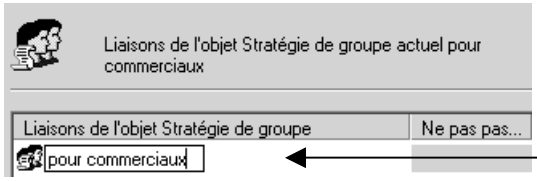


En se plaçant sur l'Unité voulue, il faut demander propriété :

Exemple ici commerciaux

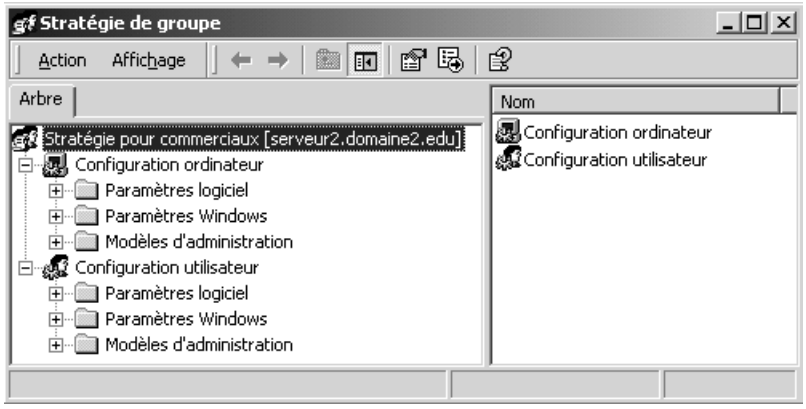
et demander **Stratégies de groupe**

Il faut se créer une nouvelle stratégie via **Nouveau**



De préférences lui donner un nom en relation avec l'UO qu'elle gère par exemple ici "pour commerciaux"

puis modifier



Il faut enfin déplacer (ou créer si besoin) dans l'UO les éléments dont on veut qu'ils héritent la stratégie…par exemple un compte ordinateur si la stratégie travaille dans le registre configuration ordinateur.

N.B: il est toujours déconseillé de poser des stratégies au niveau des OU prédéfinies, il vaut mieux créer ses propres OU et poser des stratégies dessus.

L'utilitaire en ligne Secedit

Cette commande analyse ou configure la sécurité du système en appliquant un modèle stocké.

Configurer la sécurité du système

secedit /configure

Cette commande configure la sécurité du système en appliquant un modèle stocké.

Syntaxe

secedit /configure [**/DB** *NomFichier*] [**/CFG** *NomFichier*] [**/overwrite**][**/areas** *Zone1 Zone2...*] [**/log** *CheminJournal*] [**/verbose**] [**/quiet**]

secedit /validate

Cette commande valide la syntaxe d'un modèle de sécurité que vous souhaitez importer dans une base de données en vue d'une analyse ou d'une application à un système.

Syntaxe

secedit /validate *NomFichier*

Analyser la sécurité du système

secedit /analyze

Cette commande analyse la sécurité du système.

Syntaxe

secedit /analyze [**/DB** *NomFichier*] [**/CFG** *NomFichier*] [**/log** *CheminJournal*] [**/verbose**] [**/quiet**]

Parameters

:**/DB** *NomFichier*
Indique le chemin de la base de données qui contient la configuration stockée par rapport à laquelle l'analyse sera effectuée. Cet argument est obligatoire. Si *NomFichier* indique une nouvelle base de données, l'argument **CFG** *NomFichier* doit également être spécifié.

/CFG *NomFichier*
Cet argument est uniquement valide lorsqu'il est utilisé avec le paramètre **/DB**. Il s'agit du chemin d'accès du modèle de sécurité qui sera importé dans la base de données en vue d'une analyse. Si cet argument n'est pas spécifié, l'analyse sera effectuée par rapport à n'importe quelle configuration déjà stockée dans la base de données.

/log *CheminJournal*
Chemin du fichier journal du processus. Si cet argument n'est pas spécifié, le fichier par défaut sera utilisé.

/verbose
Demande des informations détaillées sur la progression au cours de l'analyse.

/quiet
Supprime les sorties écran et journal. Vous pouvez toujours afficher les résultats de l'analyse à l'aide de la Configuration et analyse de la sécurité.

secedit /validate

Cette commande valide la syntaxe d'un modèle de sécurité que vous souhaitez importer dans une base de données en vue d'une analyse ou d'une application à un système.

Syntaxe

secedit /validate *NomFichier*

Il est possible aussi avec cette option **/refreshpolicy** de forcer la propagation d'une stratégie de groupe.

N.B: Normalement une stratégie se propage à **chaque démarrage de poste**, puis **toutes les 5 à 60 voire 90 minutes**, et lorsque les paramètres de sécurité locale sont modifiés…

Actualiser les paramètres de sécurité

secedit /refreshpolicy

Cette commande actualise la sécurité du système en appliquant à nouveau les paramètres de sécurité à l'objet Stratégie de groupe.

Syntaxe

secedit /refreshpolicy {**stratégie_ordinateur** | **stratégie_utilisateur**} [**/enforce**]

Parameters

stratégie_ordinateur
Actualise les paramètres de sécurité pour l'ordinateur local.

stratégie_utilisateur
Actualise les paramètres de sécurité pour le compte d'utilisateur local qui conduit actuellement une session sur l'ordinateur.

/enforce
Actualise les paramètres de sécurité, même si aucune modification n'a été apportée aux paramètres de l'objet Stratégie de groupe.

Non erreur doc: **machine_policy**

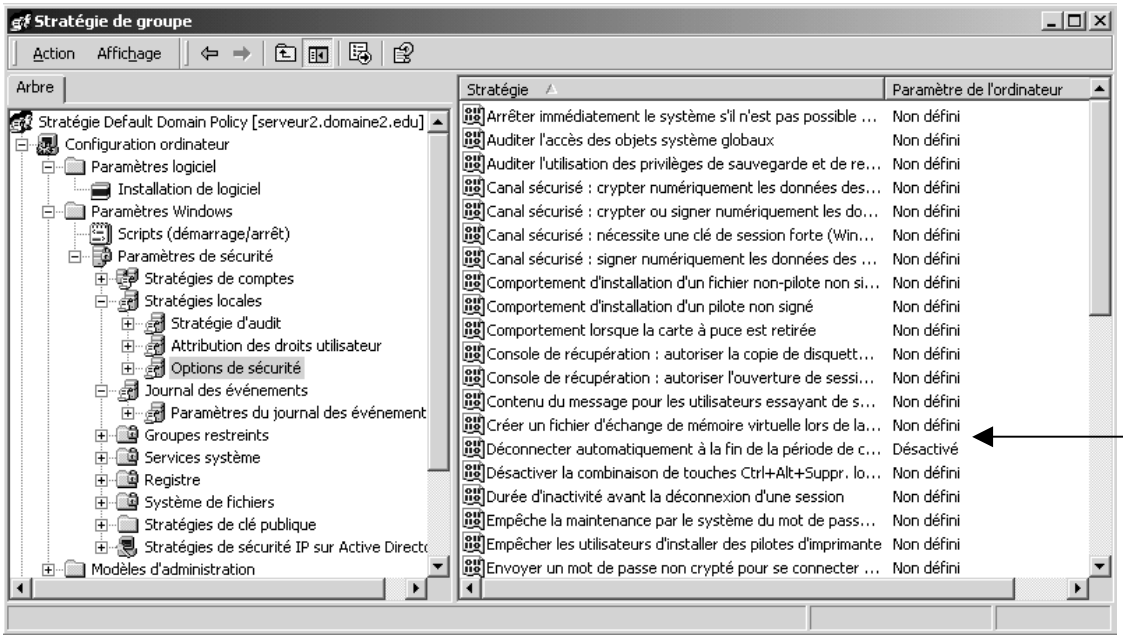
Non erreur doc: **user_policy**

GPO DE DOMAINE, DE CONTROLEUR

Mise en oeuvre :

On l'a déjà dit, il existe une GPO par défaut pour le domaine nommée **Default Domain Policy**, Default Domain Policy et une GPO par défaut pour les contrôleur de Domaine nommée **Default Domain Controllers Policy**. Default Domain Controllers Policy

Ces stratégies existent, mais sont très permissives, dans le sens ou la plupart de leur composant sont non spécifiés…voire spécifié avec une valeur désactivée…



N.B: toutes les stratégies définies par défaut dans la GPO de domaine, s'appliquent à la GPO des Controlleurs de Domaine.

Si on modifie ou ajoute une stratégie au niveau du domaine ou des contrôleur, ceux-ci doivent attendre 5 minute avant d'en recevoir les effets…

Il es bien sûr toujours possible de forcer le rafraîchissement à l'aide de la commande

Secedit /refreshpolicy machine_policy

ou

Secedit /refreshpolicy user_policy

LIAISON - HERITAGE – BLOCAGE - FORCER DES GPO

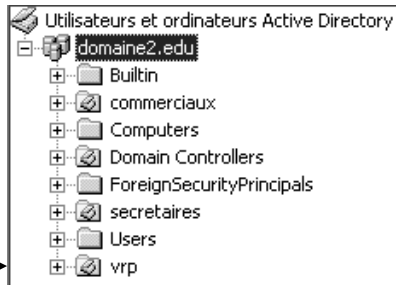
Liaison de GPO :

On a compris que lorsque l'on définissait une GPO sur une UO, celle-ci s'appliquait a tous les éléments posés dans l'UO.

Si on souhaite appliquer la même GPO à deux UO différentes, il semble inutile de créer deux GPO différentes, (avec tous les risques de fausse manipulation…) avec les mêmes paramètres, s'appliquant chacune à une UO différente.

Il est possible de spécifié pour une UO d'utiliser une GPO déjà existante, c'est ce que l'on appelle lier une GPO…

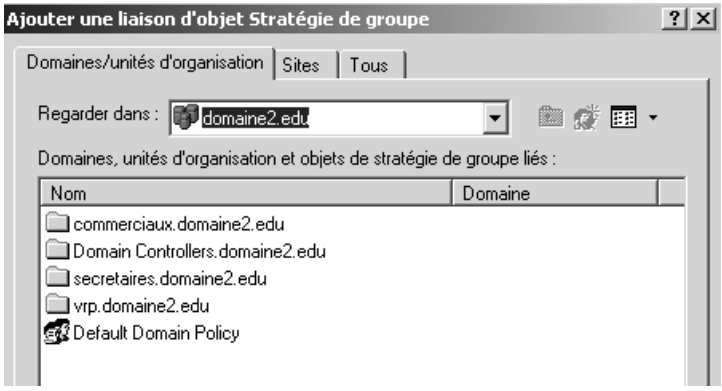
Imaginons que nous devions créer une nouvelle UO pour les **VRP**, celle-ci devant suivre les même consigne de stratégie que les commerciaux…



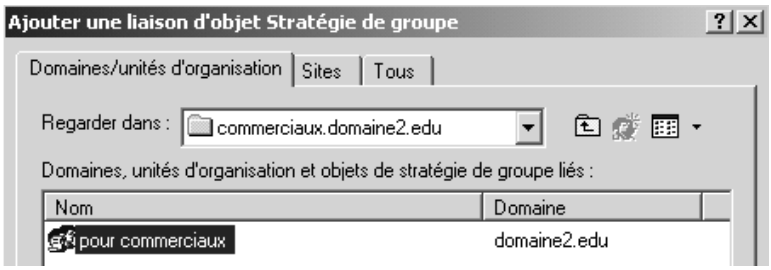
Lorsque je demande les **Stratégies de groupe** pour cette UO

On ne demande pas Nouveau, mais **Ajouter…**

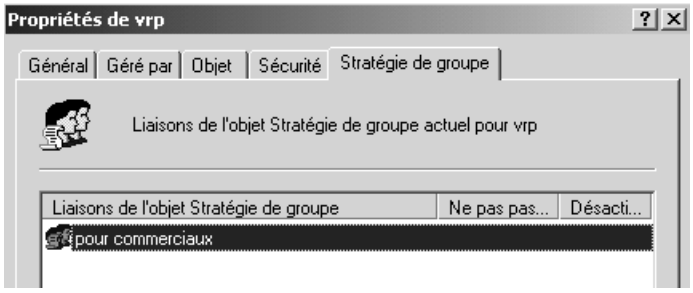
La liste de toutes les GPO de domaine et d'UO apparaît



Et il faut aller la GPO qui nous intéresse…

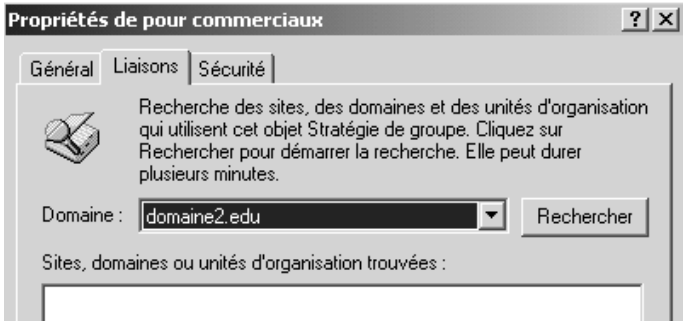


pour obtenir finalement

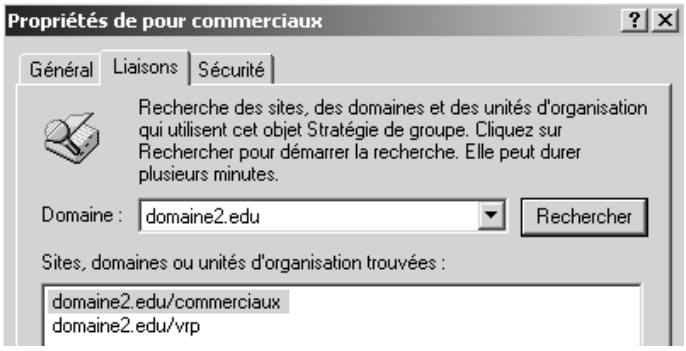


N.B: Attention, a partir de maintenant, toute modification de la GPO intitulé "pour commerciaux" et posée initialement sur l'UO commerciaux, s'applique bien sûr aussi à l'UO VRP

N.B: Rien ne permet facilement de savoir "*si une GPO est utilisée sur d'autres UO que celle sur laquelle elle est crée*".
Le seul moyen de le savoir, c'est de se placer sur la GPO, pour nous ici "pour commerciaux" dans l'UO commerciaux, et demander **propriétés** :



Puis on demande **Rechercher**



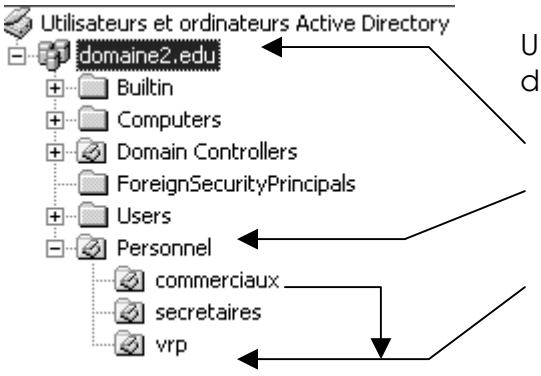
On a la liste de toutes les UO utilisant cette GPO

évidemment l'UO **commerciaux** utilise cette GPT

mais aussi l'UO **vrp** !

héritage et blocage d'héritage:

On le sait, lorsque l'on crée des UO, les GPO s'appliquent de manière hiérarchique.



Un élément placé dans l'UO **vrp** reçoit donc ici :

- la GPO de domaine par défaut
- La GPO de Personnel (si elle existe)
- La GPO de vrp et celles liées (par exemple celle de commerciaux

N.B: En cas de conflit sur un même élément défini à différents niveaux, le principe étant de dire "c'est le dernier qui cause, qui a raison" une exception, lorsque les paramètres qui rentrent en conflits sont exprimés dans des paramètres utilisateurs, et des paramètres ordinateurs. dans ce cas, généralement les paramètres d'ordinateurs priment ! mais cela doit être vérifié dans les explications des propriétés…

Il est possible de bloquer l'héritage au niveau d'un objet GPO, il suffit simplement de demander sur cet objet "**bloquer l'héritage**":

N.B: On ne peut pas bloquer l'héritage des stratégies de domaine pour l'UO prédéfinie Domain Controller… **par conséquent toutes les stratégies définies au niveau du domaine s'appliquent aussi aux controlleurs** !

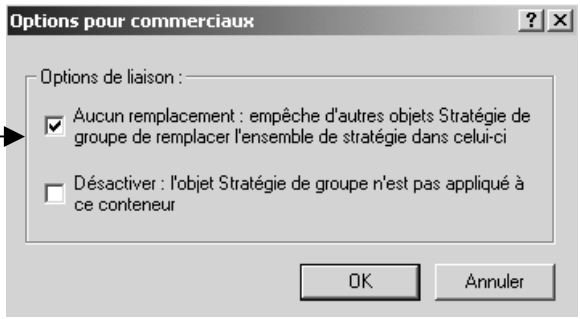
N.B: lorsque l'on bloque un héritage, on bloque cet héritage pour toutes les stratégies qui pourraient venir… sauf celles qui ont été spécifiées avec la mention "**aucun remplacement**" (cf chapitre suivant)

Interdire le blocage d'héritage :

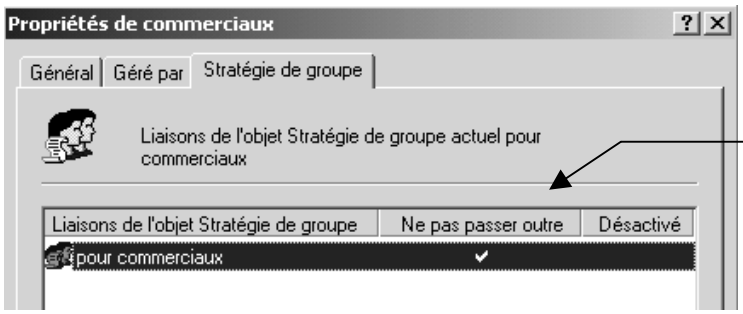
Il est possible dans une stratégie de spécifier que cette stratégie ne peut pas être bloquée par une stratégie ultérieure (on peut donc forcer l'héritage…)

Pour forcer une stratégie à être appliquée, on peut donc demander sur cette stratégie, **Option**

Et demander alors **Aucun remplacement**



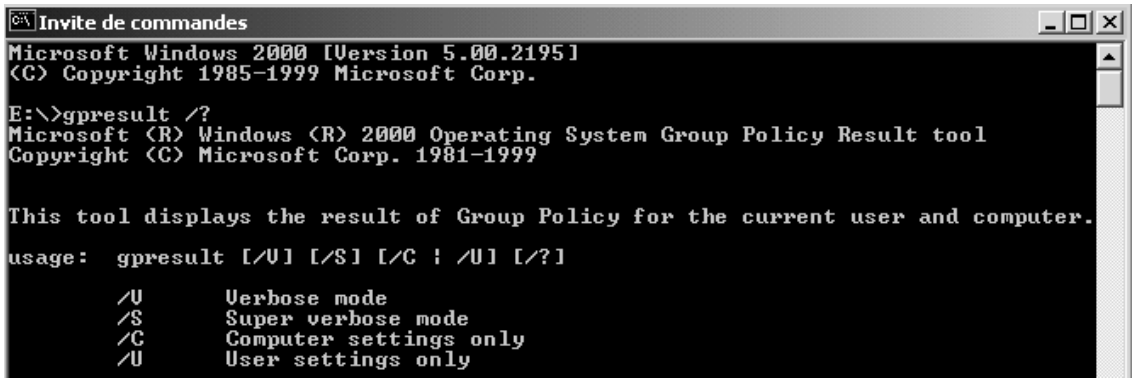
Cela se visualise ensuite sous la forme d'une coche **Ne pas passer outre**



L'utilitaire Gpresult.exe du kit de ressource

Il existe un utilitaire du kit d ressource technique permettant d'avoir un compte rendu sur une machine des GPO sui se sont appliquées

Il se lance en ligne de commande par **gpresult.exe**



GPO ET MODELES D'ADMINISTRATION

Les Modèles présents

Maintenant que l'on a compris comment donner et faire appliquer des GPO sur des UO ou dans un domaine, on peut regarder de plus près ce qui leur est spécifique, par rapports aux sécurité locales.

On a regroupé dans les modèles d'administration, toute une série de paramètres, disponibles tantôt pour la partie ordinateur, utilisateur, ou les deux...

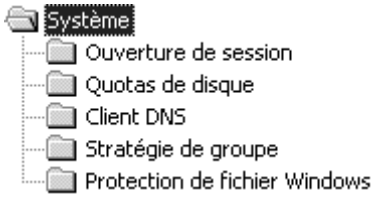
Type de paramètre	Éléments contrôlés	Disponible pour
Composants Windows	Les parties de Windows 2000 et ses outils et composants auxquels les utilisateurs peuvent accéder, y compris la console MMC	
Système	Les procédures d'ouverture et de fermeture de session, la console Stratégie de groupe, les quotas de disque et le traitement par boucle	
Réseau	Les propriétés des connexions réseau et des connexions d'appel entrant	
Imprimantes	Les paramètres d'imprimante qui peuvent obliger les imprimantes à être publiées dans Active Directory et désactiver l'impression à partir d'un navigateur Web	
Menu Démarrer et barre des tâches	Les fonctionnalités auxquelles les utilisateurs peuvent accéder à partir du menu **Démarrer** et les options qui rendent le menu **Démarrer** en lecture seule	
Bureau	Le bureau Active Desktop, y compris ce qui apparaît sur les bureaux, et ce que les utilisateurs peuvent faire avec le dossier Mes documents	
Panneau de configuration	L'utilisation des applications Ajout/Suppression de programmes, Imprimantes et Affichage du Panneau de configuration	

aller regarder un peu l'éventail des possibilités…

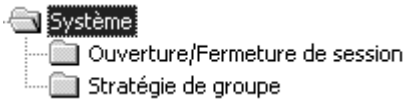
Composant **Windows** ordinateur

utilisateur

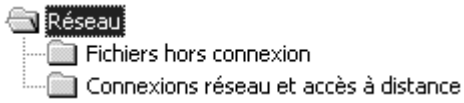
Composant **Système** ordinateur



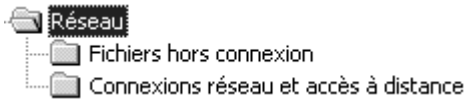
utilisateur



Composant **Réseau** ordinateur



utilisateur

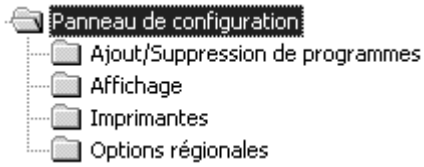


Composant **Imprimante** ordinateur

Composant **Menu Démarrer barre tâche** utilisateur

Composant **Bureau** utilisateur

Composant **Panneau de configuration** utilisateur



GPO ET SCRIPTS

Scripts de démarrage – arrêt – fin de session :

Lorsque l'on met en œuvre des scripts via les GPO, il est possible de placer trois nouveaux type de scripts

- Script de démarrage : s'exécute lors de l'allumage du poste
- Script de fermeture de session : s'exécute lors d'une fermeture de session
- Script d'arrêt : s'exécute lors d'un arrêt de la machine

Mais on peut aussi placer un script de type classique

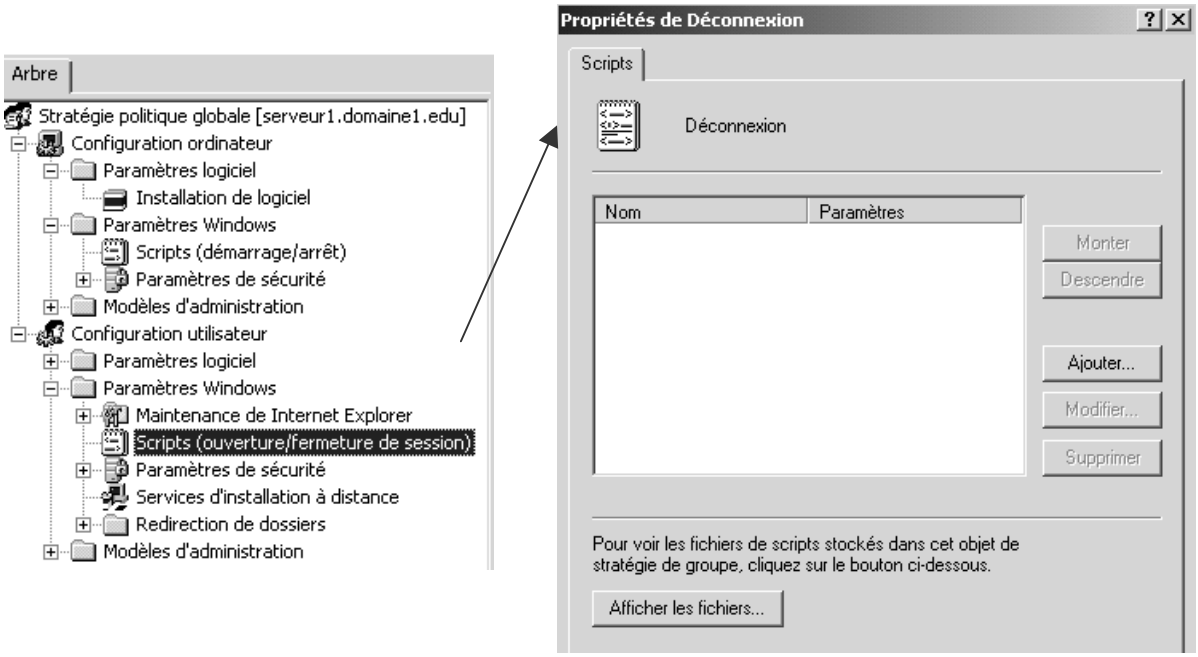
- Script d'ouverture de session : s'exécute lors d'une ouverture de session

Par défaut chaque script est réalisé avant la fin de l'autre (on parle de traitement synchrone). Les scripts GPO sont traités avant les scripts utilisateurs classiques.

Par défaut les scripts de démarrage sont masqués.

Scripts de fin de session :

pour utiliser un script de fin de session dans une GPO, le script étant déjà écris dans un fichier **.bat** ou **.vbs**,

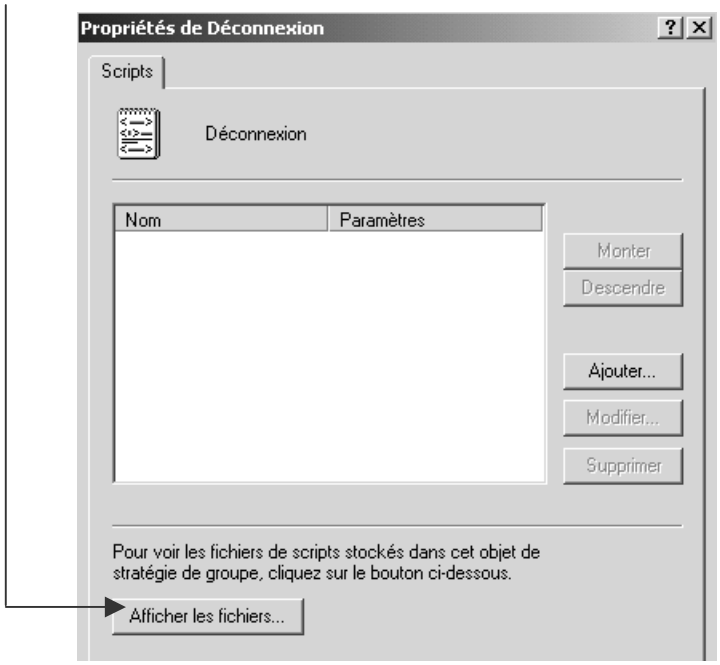


Il faut effectuer une maneuvre en deux temps :

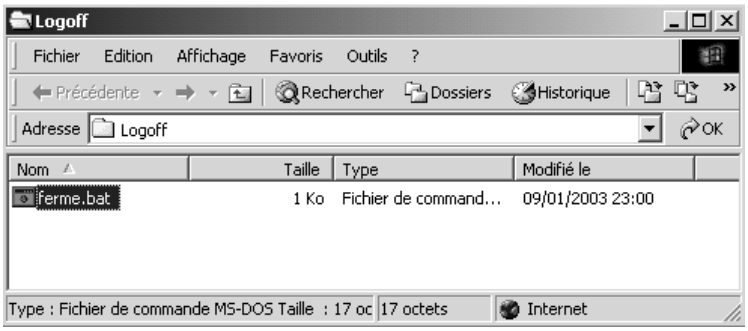
1. D'abords il faut copier le script dans la GPO
2. Puis il faut dire à la GPO d'utiliser ce script…

Copier le script dans la GPO

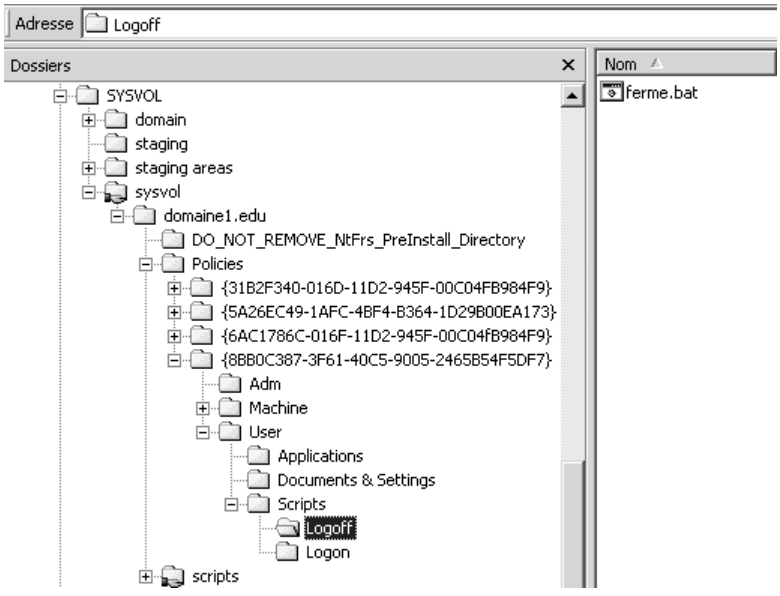
depuis la GPO, on demande le bouton **Afficher les fichiers…**



Une fenêtre s 'ouvre dans laquelle il faut copier notre script (ici **ferme.bat**)

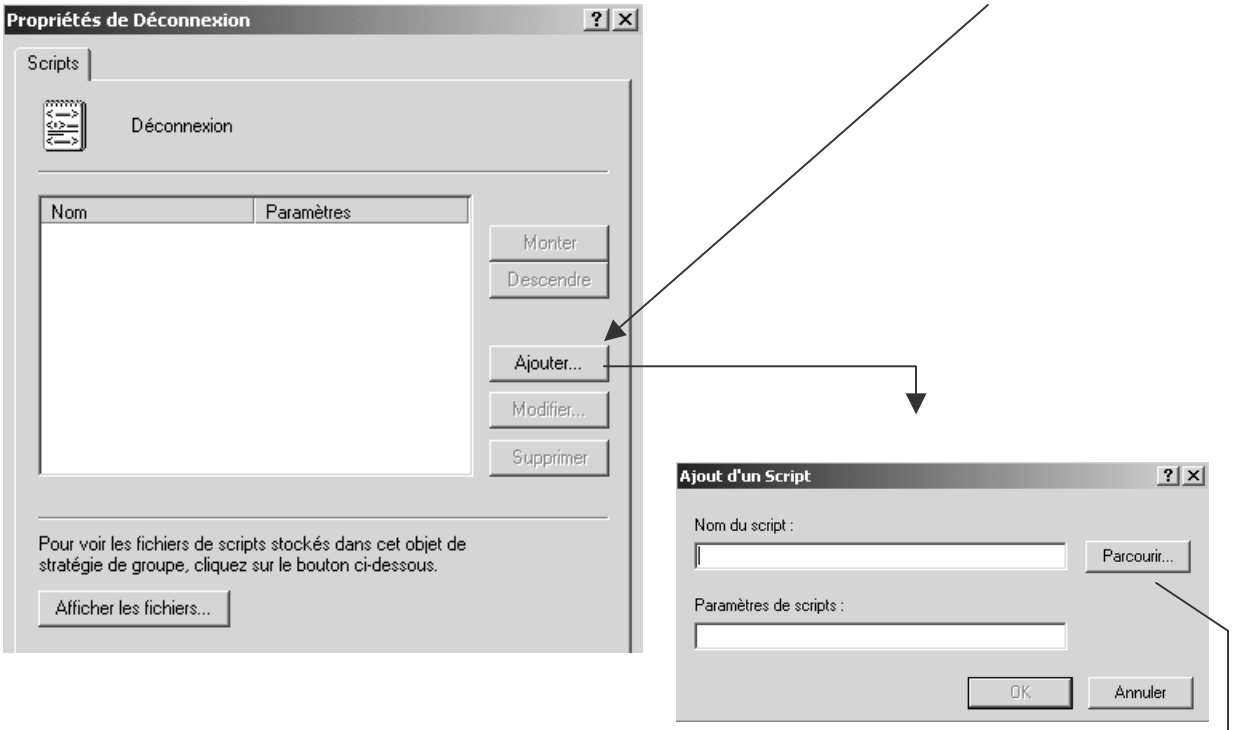


N.B : cette opération a simplement pour but de stocker dans notre GPO une copie du script, qui physiquement se trouve dans la policy…



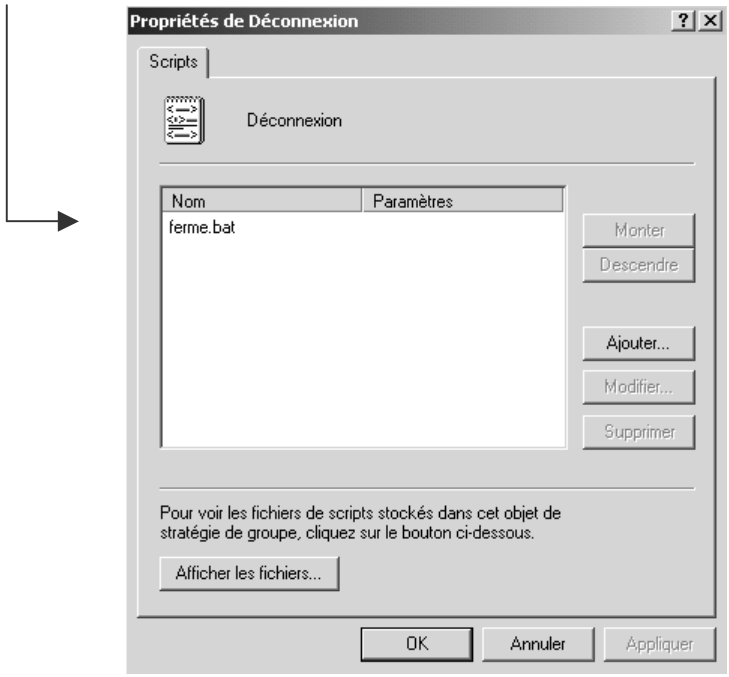
Utiliser le script dans la GPO

Pour utiliser le script dans la GPO, depuis la GPO, on demande le bouton **Ajouter**



Et via **Parcourir** on prends un script parmi ceux existant dans la GPO (donc précédemment copiés)

Maintenant on a un script de déconnexion….



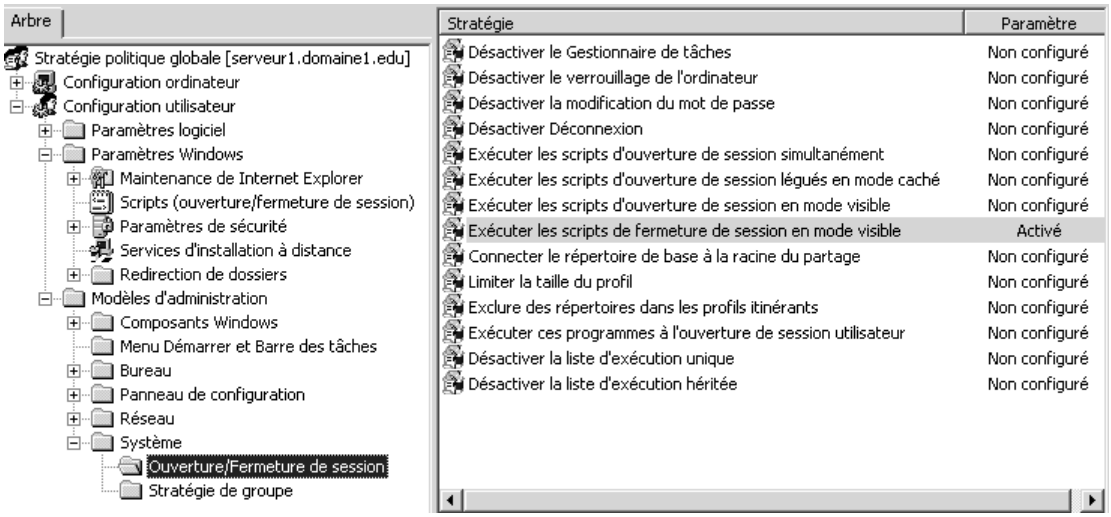
test et visualisation :

les scripts de déconnexion s'exécutent par défaut en **mode caché**…

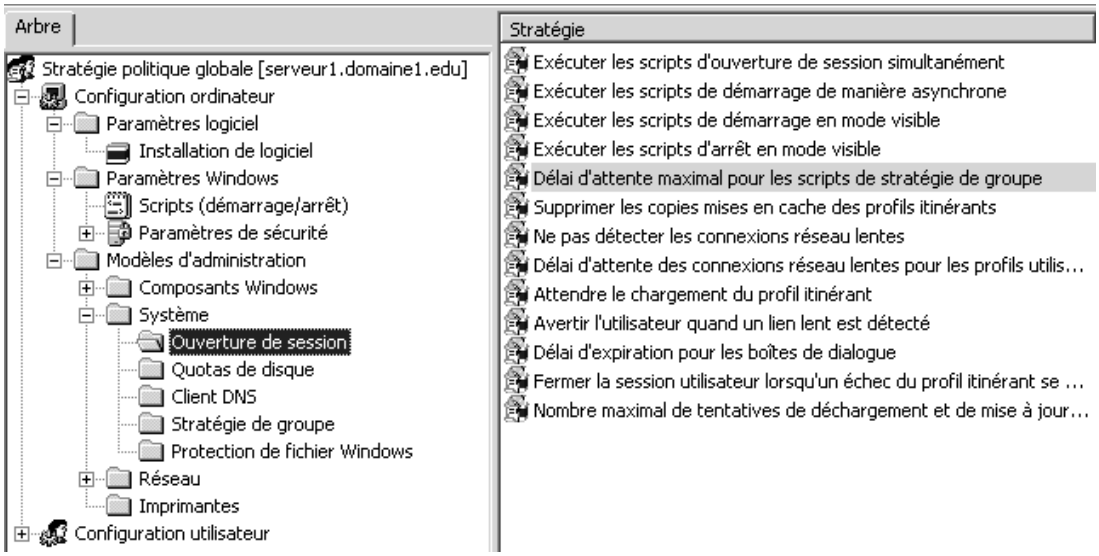
les scripts disposent de **10 minutes** pour se réaliser, avant d'être interrompus.

Ainsi, une bête commande **pause**, dans un script de déconnexion, provoque le blocage du poste pendant 10mn, puisque personne ne peut appuyer sur la touche fatidique…

Il existe un modèle de stratégie utilisateur, permettant **d'exécuter les scripts de fermeture de session en mode visible**…



Il existe un modèle de stratégie ordinateur, permettant de paramétrer le **délai d'attente maximal pour les scripts** (tous les scripts) (et 0 donnera une attente infinie…)



GPO ET INSTALLATION DE LOGICIELS

Les 3 éléments Winstaller – GPO - AD

Un nouveauté de windows2000 consiste en un système d'installation et de maintenance de logiciel, utilisant AD (Active Directory), les GPO (stratégies de groupe), et Windows installer

L'ordre logique dans lequel ces fonctionnalités vont jouer est le suivant :

1. Windows Installer est utilisé pour l'installation de logiciel
2. Les GPO sont utilisées pour définir une stratégie quant à cette installation
3. Active Directory est là pour déployer cette stratégie

On a déjà suffisamment parlé de AD et des GPO, la grosse nouveauté ici réside dans **Windows Installer**

Windows installer et fichiers msi

Le service **Windows installer** est un service client automatisant entièrement la procédure d'installation et de désinstallation de logiciel, à condition d'avoir un « package windows installer » correspondant à l'application à installer. Ce package est plus connu sous l'appellation du **fichier MSI** (**Microsoft installer**)

Le fichier MSI est donc en fait un fichier de réponse automatisé et contenant tous les fichiers nécessaires à l'installation de l'application…

Les fichiers MSI font toujours des installations **classiques locales** de tout logiciel, grâce à la présence dans l'OS du composant Windows Installer.

- Si l'OS n'a pas **Windows Installer**, une **mise à niveau du système sera nécessaire**
  C'est pour cette raison que certaines installations demande un redémarrage du poste, car d'abords en fait elles installent Windows installer, puis elles font « lire le fichier msi par le Windows installer pour installer l'application proprement dite.
- Si l'on **veut une installation réseau**, type installation administrative d'office, les fichiers msi et windows installer **ne savent pas faire**

La présence de Windows installer est vérifiable par la présence du fichier **msiexec.exe,** présent en général dans le dossier système.

Aujourd'hui toutes les applications récentes sont livrées avec un fichier MSI destiné à être interprété par un Windows installer

Si on n'a pas de fichier Msi, il est impossible de se créer une stratégie d'installation automatisée.

Il existe des outils professionnels permettant de créer des fichier msi, et il y en à 1 livré dans le dossier du CD de 2000

\ValueADD\3RDPARTY\MGMT\WINSTLE

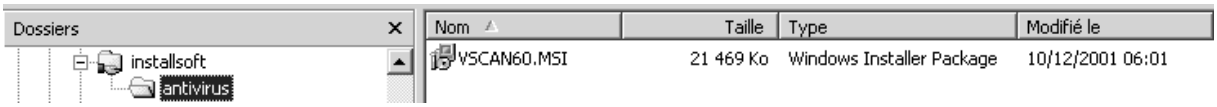
Procédure d'installation et de maintenance logiciels

Il va falloir exécuter les 4 étapes suivantes :

1. Il faut créer une GPO qui installe le logiciel sur l'ordinateur, soit lors du démarrage du poste, soit lors du « lancement » de l'application (qui paraît comme disponible) de la part de l'utilisateur.
   cette phase peut être qualifiée de déploiement .
2. Le logiciel déployé peut être mis automatiquement à niveau, ou redéployé au démarrage du poste ou lorsqu'un utilisateur lance sa session.
   cette phase peut être qualifiée de maintenance .
3. Le logiciel peut être automatiquement supprimé au démarrage du poste ou lorsqu'un utilisateur lance sa session.

Création du point d'installation de logiciel

Il faut copier les package Windows installer, c'est à dire le fichier **msi** vers le **point de distribution** du logiciel.



Ce point de distribution est généralement un dossier partagé sur le serveur. On peut donner des permissions en lecture seule…, partager le dossier de manière administrative ($), pour le rendre invisible…

Affectation - Publication de logiciel

L'affectation permet d'être sur que le logiciel est présent sur l'ordinateur voulu. On peut affecter les logiciels à des utilisateurs, ou a des ordinateurs.

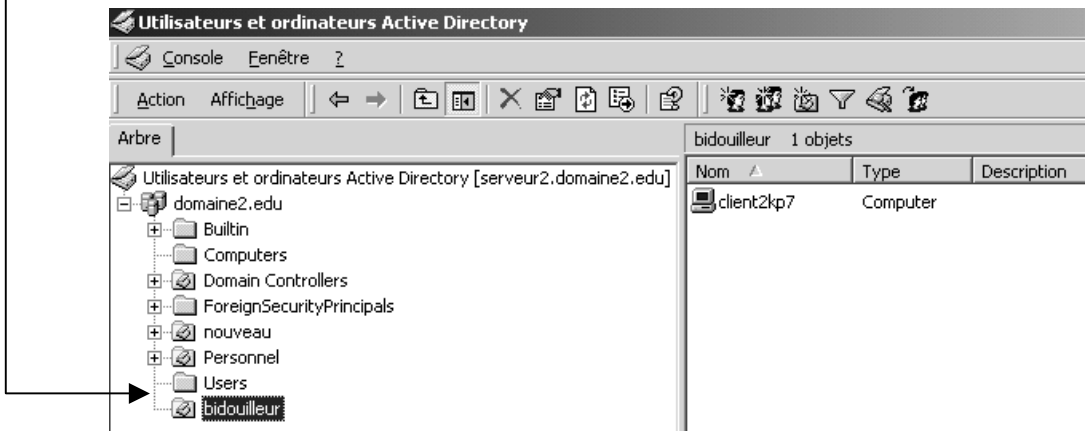
- Si on les affectent à des **ordinateurs** : il n'y a pas d'annonce, le logiciel est automatiquement installé lors de l'allumage du poste. (sauf pour les CD)
- Si on les affectent à des **utilisateurs** : lorsque l'utilisateur ouvre un session, le logiciel est annoncé (raccourcis présents) , mais l'installation ne débute réellement que si l'utilisateur clique sur l'application ou double-clique sur un fichier associé.

La Publication permet que le logiciel soit instalable sur l'ordinateur voulu. On peut publier des logiciels que pour des utilisateurs, mais pas pour des ordinateurs.

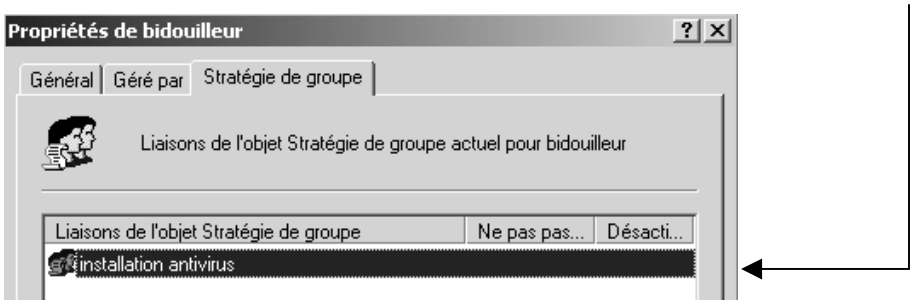
En effet lors de la publication de logiciels, il n'y a pas d'annonce. L'utilisateur peut installer l'application en passant par ajout/suppression programme, ou l'installation se fait automatiquement via un double clic sur un fichier associé

Stratégie de déploiement de logiciel

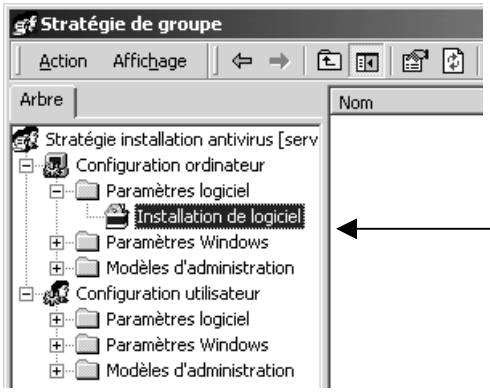
On va créer une **GPO** sur une **OU** contenant les machines des **bidouilleurs**, et leur installer un antivirus dès le démarrage du poste



Sur cette OU on va poser une GPO que l'on nomme de manière explicite

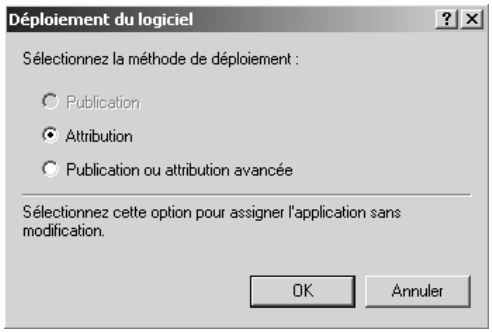


Cette GPO contient une définition de **Paramètres logiciel** dans **Configuration d'utilisateur (ou ordinateur)**

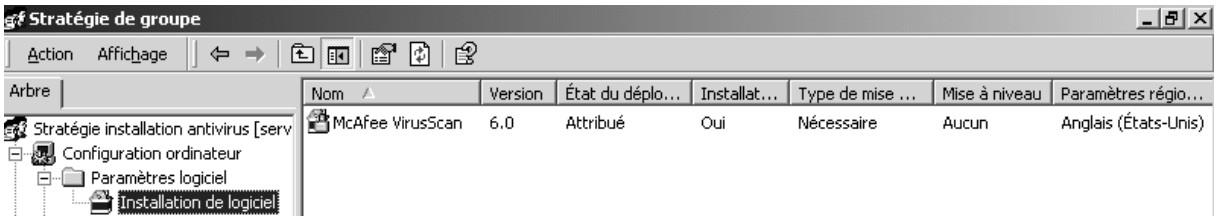


Pour laquelle on demande via un clic droit **nouveau package** et on va chercher le chemin du dossier de distribution (via le réseau bien sûr)

puis



on obtient finalement



NB: si on travaille au niveau de la configuration d'utilisateur, à l'ouverture de session on récupèrer le MSI

NB: si on travaille au niveau de la configuration d'ordinateur, il faut arrêter et re-démarrer le poste pour récupérer le MSI

STRATEGIES SYSTEME CLIENTS NON-2000: "POLEDIT"

Que sont les stratégies système :

Une stratégie système est une restriction imposée à un utilisateur ou à l'ordinateur d'un utilisateur pour limiter sa capacité à accéder aux ressources ou à configurer l'ordinateur. (ne plus pouvoir accéder au panneau de configuration, enlever la commande exécuter du menu démarrer, etc etc…

Ces restrictions sont obtenues via la modification de la base de registre de la machine sur laquelle la session est ouverte, et l'utilitaire **POLEDIT** permet de modifier la base de registre en utilisant une interface graphique…

Mais même si POLEDIT permet de modifier la base de registre locale, (et à fortiori une base de registre quelconque de n'importe qu'elle machine du domaine) POLEDIT devrait être utilisé essentiellement pour créer une fichier de configuration. Ce fichier de configuration sera stocké sur le serveur, et téléchargé sur chaque client à l'ouverture de session : il prévaudra alors sur les inscriptions locales de la base de registre locale !

Il existe fondamentalement deux type de stratégies système, :

la stratégies système des utilisateurs

la stratégies système des ordinateurs

La stratégie système des utilisateurs :

remplace les paramètres définis dans la zone relative à l'utilisateur courant du registre (HKEY_CURRENT_USER), elle s'applique par défaut à tous les utilisateurs, et par conséquent aussi à l'administrateur.

La stratégie système des ordinateurs :

remplace les paramètres définis dans la zone relative à l'ordinateur local (HKEY_LOCAL_MACHINE), elle s'applique par défaut à toutes les machines, même les serveurs, quel que soit l' utilisateur qui ait ouvert la session.

N.B: On peut donc considérer les stratégies système d'ordinateur par défaut comme un ensemble de stratégies à plus petit dénominateur commun.

Installer l'éditeur de stratégie :

ATTENTION : l'éditeur de stratégies est un outils puissant, son emplois doit être limité aux seuls administrateurs des machines

Il faut donc limiter son emplois en ne **l'installant pas sur toutes les machine !**

par précaution on peut toujours sauvegarder les fichiers User.dat et system.dat dans \windows (base de registre)

Pour installer l'éditeur, la situation n'est pas la même selon que l'on se trouve sur une machine NT ou Windows 95-98

Sur un serveur Windows NT :

Sur un **serveur NT** l'installation se fait en standard, et on peut lancer l'éditeur de stratégies système via

… / Programme / Outils d'administration (commun) / Editeur de stratégie système

Sur un client Workstation NT :

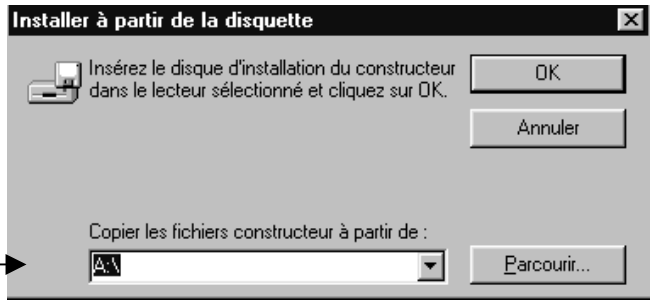
Sur une **workstation NT** il faut le récupérer soit depuis le CDROM NT serveur, mais il faut le décompresser, soit en copiant simplement les fichiers depuis le serveur **Poledit.exe** et éventuellement **Poledit.hlp**

On peut ensuite bien sûr se créer se créer un raccourci …

Pour la désinstallation il suffit de supprimer les deux fichiers en question…

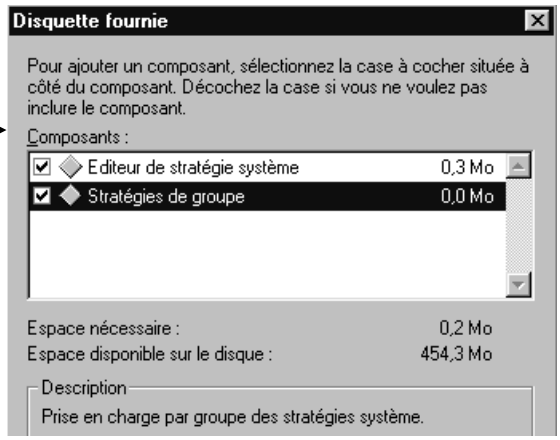
Sur un poste Windows 95-98 :

Pour installer cet outil sur votre disque dur local, ou pour installer le support pour les stratégies de groupe, utilisez l'option **Ajout/Suppression** de programmes du **Panneau de configuration**, sélectionnez l'onglet **Installation de Windows**, et cliquez sur le bouton **Disquette fournie**,



- pour windows 95 procédez à l'installation à partir du répertoire **ADMIN\APPTOOLS\POLEDIT**
- pour windows 98 procédez à l'installation à partir du répertoire **TOOLS\RESKIT\NETADMIN\POLEDIT**

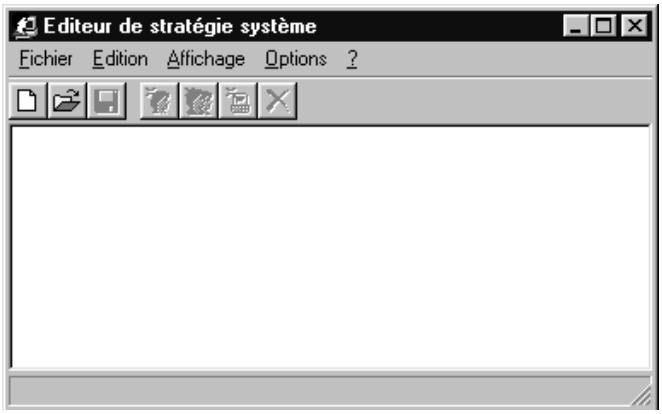
Dans l'installation bien cocher les deux cases



Désormais l'éditeur de stratégie est disponible dans le menu

… / Programme / Accessoires / outils systèmes / Editeur de stratégie système

Lorsqu'on le lance, on obtient



Pour plus d'informations sur les stratégies système et sur cet éditeur, consultez les rubriques correspondantes dans le Kit de ressources Windows 95 (**WIN95RK.HLP**) ou Windows 98 (**WIN98RK.HLP**).

Pour la désinstallation il suffit de demander le menu

Démarrer / panneau de configuration / Ajouter / suppression programme

Une entrée libellée "éditeur de stratégies système" apparaît

il suffit de demander de la désinstaller

STRATEGIE LOCALE OU MODELE

POLEDIT permet de modifier la base de registre locale, (et à fortiori une base de registre quelconque de n'importe qu'elle machine du domaine)

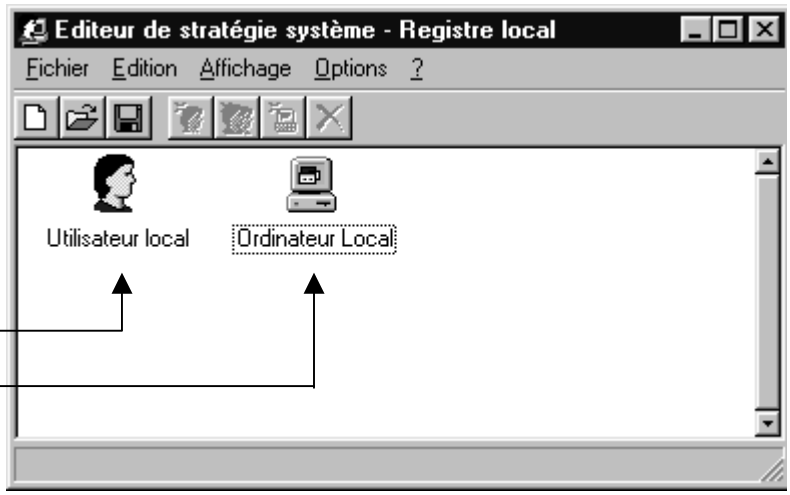
POLEDIT peut aussi créer un fichier de configuration. Ce fichier de configuration sera stocké sur le serveur, et téléchargé sur chaque client à l'ouverture de session : il prévaudra alors sur les inscriptions locales de la base de registre locale

Stratégie locale ou "mode registre" :

En mode registre, on édite donc directement le registre, et les modifications sont à priori directement visualisables

il n'est pas nécessaire de fermer la session en cours ou de re-démarrer l'ordinateur pour visualiser les effets

par le menu :
Fichier / Ouvrir la base de registre

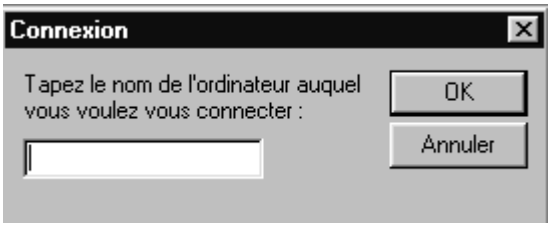


on édite la base de registre locale à travers :

l'**Utilisateur local**

ou l'**Ordinateur local**

par le menu :
Fichier / Connecter

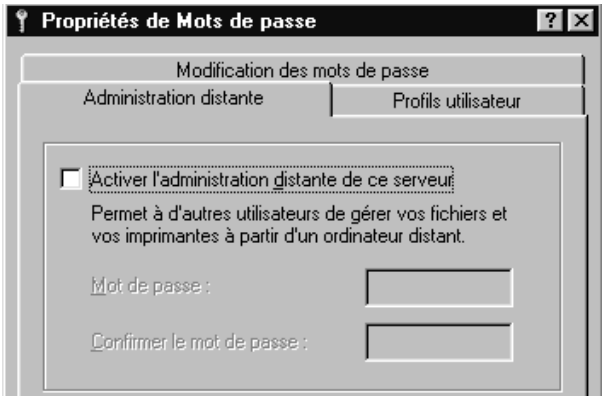


on peut éditer le registre d'une machine distante, à condition que sur cette machine un certain nombre de manipulation ait été faites :

1. l'**Administration distante** doit avoir été activée , via le menu

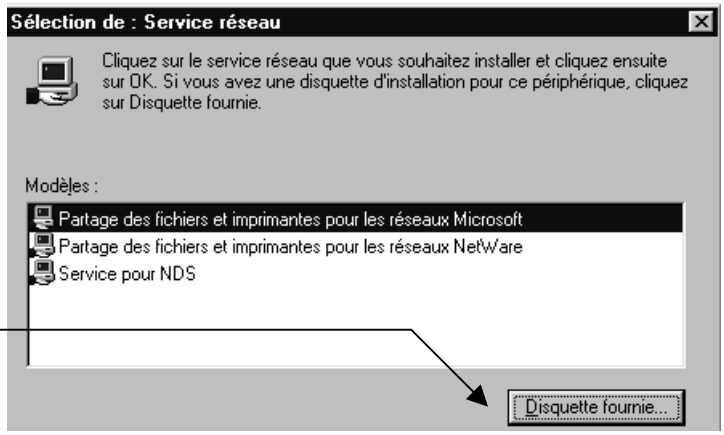
/démarrer / panneau de configuration / Mot de passe

onglet **Administration distante**



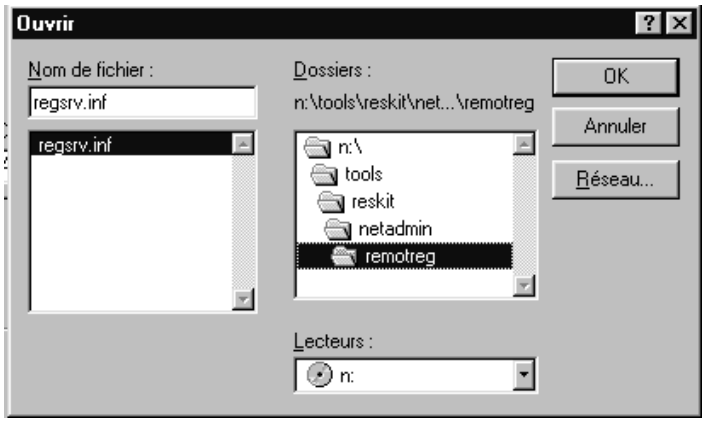
(ce qui est fait de manière implicite si on est Administrateur d'un domaine et que le client 98 est rattaché au domaine)

2. Le service **Registre distant** soit installé, via le menu contextuel de **voisinage réseau / propriété /** dans lequel on demande d'ajouter un service spécifique, que l'on prends via "disquette fournie"



- dans le dossier **TOOLS\RESKIT\NETADMIN\REMOTEREG**

Uniquement sur windows 98



pour plus re renseignement cf "Paramétrage de l'Administration à distance" du **Kit de ressource technique de windows 98**

N.B: MAIS DE MANIERE GENERALE IL EST DECONSEILLE D'UTILISER LE MODE REGISTRE. SI UNE INCOMPATIBILITE SE PRESENTE SPECIFIQUE A UN ORDINATEUR OU UN UTILISATEUR IL EST RECOMMANDE DE CREER DANS LE DOMAINE UNE STRATEGIE SPECIFIQUE POUR CET ORDINATEUR OU CET UTILISATEUR

Fichier de stratégie ou "mode stratégie":

Vous pouvez créer des fichiers de stratégies ou bien utiliser les exemples qui vous sont fournis dans le dossier ADMIN\RESKIT\SAMPLES\POLICIES.

En mode fichier de stratégie, on édite un fichier caractérisé par le fait que son extension est **xxxxx.POL**

Pour qu'un tel fichier de stratégie soit effectif, il est nécessaire que plusieurs conditions soient requises :

- le fichier de stratégie a été sauvegardé dans le dossier partagé du serveur NT CPD nommé **Netlogon**, sous le nom réservé :
  - ✓ **Ntconfig.pol** s'il a été crée via l'éditeur de stratégie NT et se destine à gérer tous les clients NT ouvrant leur session sur ce serveur CPD
  - ✓ **Config.pol** s'il a été crée via l'éditeur de stratégie windows 95-98 et se destine à gérer tous les clients windows 95-98 ouvrant leur session sur ce serveur de domaine
- l'utilisateur à ouvert une nouvelle session sur le domaine géré par le CPD depuis que le fichier de stratégie y a été placé

N.B: LES STRATEGIES SYSTEMES CREES SOUS L'EDITEUR DE STRATEGIE NT NE PEUVENT S'APPLIQUER QUE SUR LES MACHINE NT ET JAMAIS SUR DES CLIENTS WINDOWS 95-98.

DE MEME LES STRATEGIES SYSTEMES CREES SOUS L'EDITEUR DE STRATEGIE WINDOWS NE PEUVENT S'APPLIQUER QUE SUR LES MACHINE WINDOWS ET JAMAIS SUR DES CLIENTS NT.

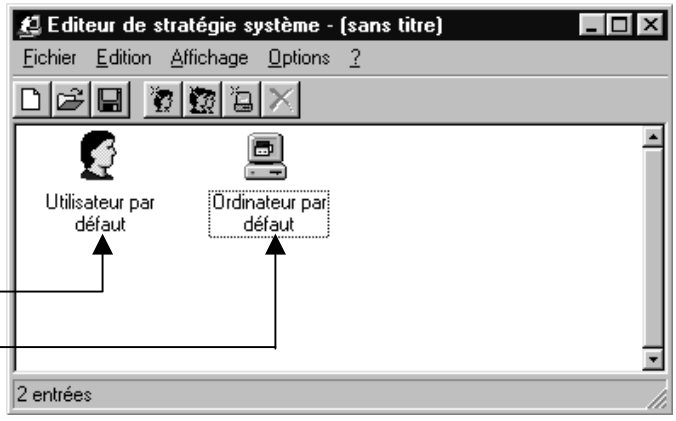
SI ON A UN PARK MIXTE IL FAUT SE CREER 2 FICHIERS DE STRATEGIES DISTINCTS A PARTIR DE L'EDITEUR SPECIFIQUE A CHAQUE ENVIRONNEMENT

par le menu :
Fichier / Nouveau

On cré un fichier de stratégie comprenant 2 entrées:

l'**Utilisateur par défaut**

ou l'**Ordinateur par défaut**



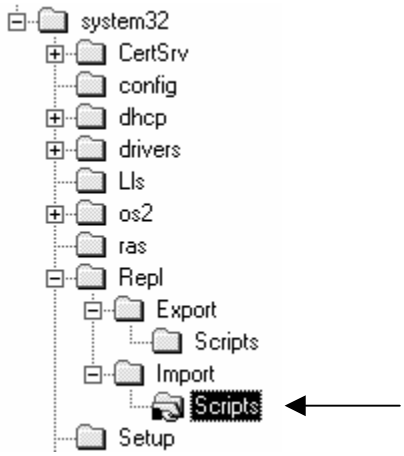
Il faudra bien sûr enregistrer ce fichier avec un nom adéquat ou temporaire classiquement, via le menu **fichier / enregistrer sous**…

STRATÉGIE SOUS WINDOWS NT4.0

Nom et emplacement :

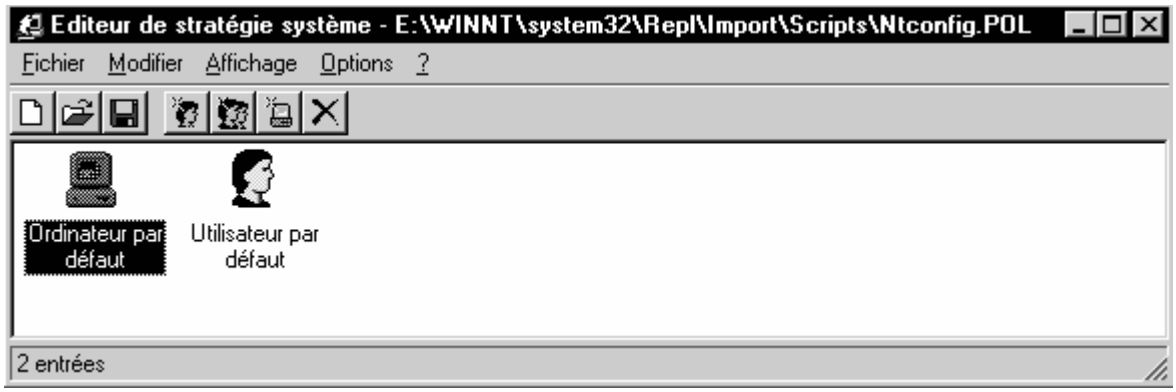
On l'a vu, le fichier de stratégie doit se nommer obligatoirement **Ntconfig.pol** et être sauvegardé dans le dossier partagé du serveur NT CPD nommé **Netlogon**

Le dossier qui apparaît pour les clients sous le nom **NETLOGON** est en fait un dossier situé dans le dossier principal dans lequel windows NT est installé



Winnt\system32\Repl\Import\Scripts

POLEDIT permet de se créer autant de fichier de stratégie que l'on souhaite, mais seul le fichier nommé **Ntconfig.pol** sera chargé et pris en compte par les clients NT

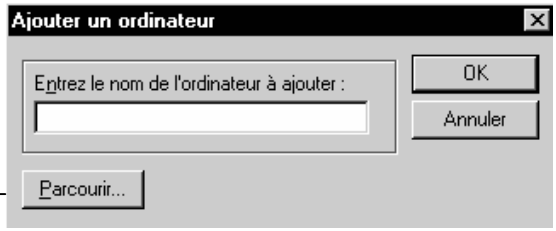


Stratégie d'Ordinateur:

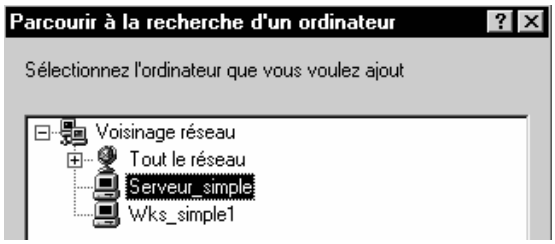
Les stratégies d'ordinateurs s'appliquent à tous les ordinateurs du domaine, et si l'on veut gérer différemment une machine particulière, il faudra inclure "l'exception "dans la stratégie système

pour gérer un poste différemment il faut dans le menu

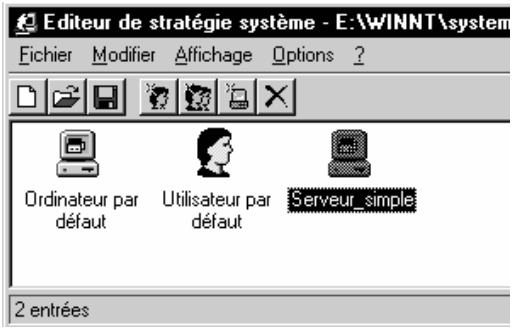
Modifier / Ajouter un ordinateur



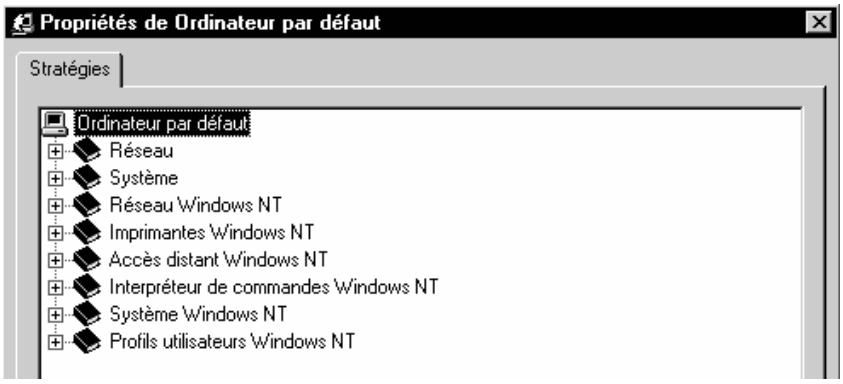
rentrer le nom de la machine à traiter différemment



de manière à visualiser le cas particulier dans l'éditeur de stratégie :



Les stratégies possible apparaissent alors listées:



3 valeurs peuvent être prises par les cases à cocher de l'éditeur de stratégies :

cochée : la stratégie est implémentée

grise : la clé de registre n'est pas modifiée

blanche : la statégie n'est pas implémentée

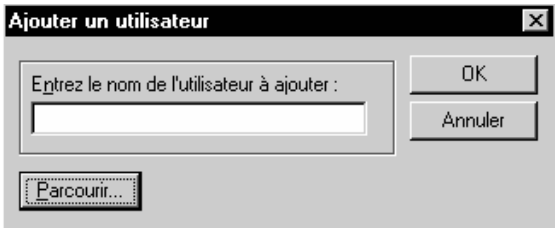
Stratégie d'Utilisateur:

Les stratégies d'Utilisateurs s'appliquent à tous les Utilisateurs du domaine, et si l'on veut gérer différemment un utilisateur

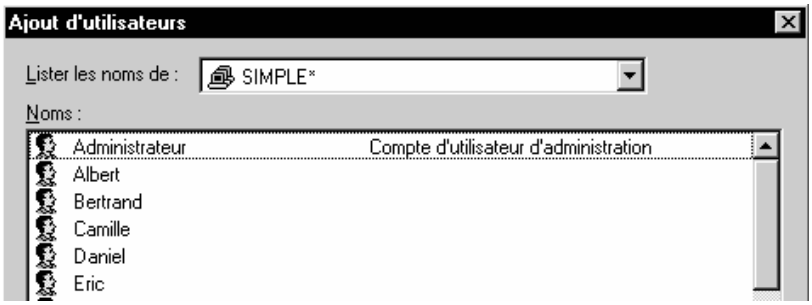
particulier ou un groupe, il faudra inclure "l'exception "dans la stratégie système

pour gérer un utilisateur différemment il faut dans le menu

Modifier / Ajouter un utilisateur

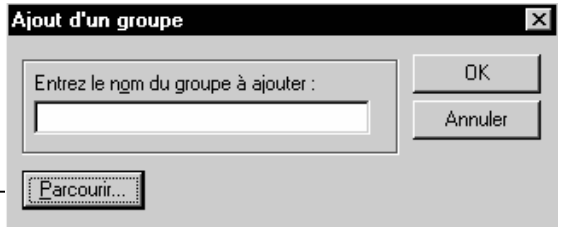


rentrer le nom de l'utilisateur à traiter différemment

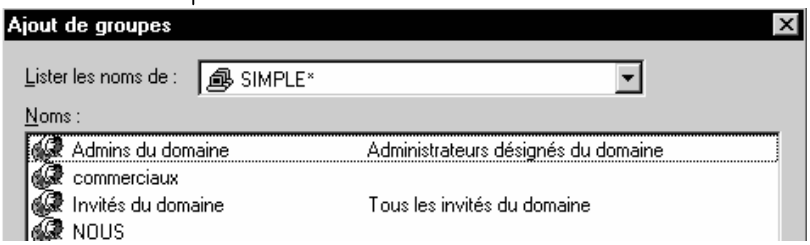


pour gérer un groupe différemment il faut dans le menu

Modifier / Ajouter un groupe



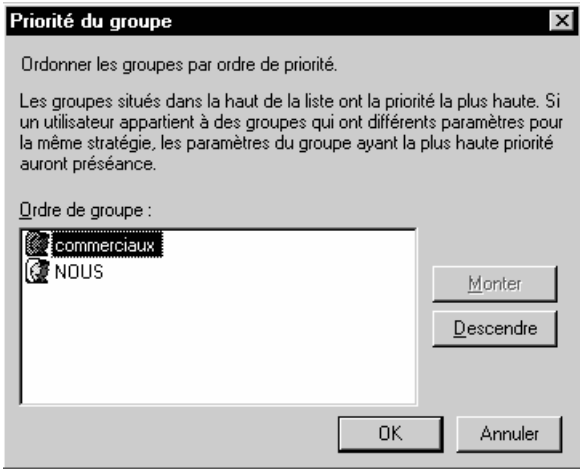
rentrer le nom du groupe à traiter différemment



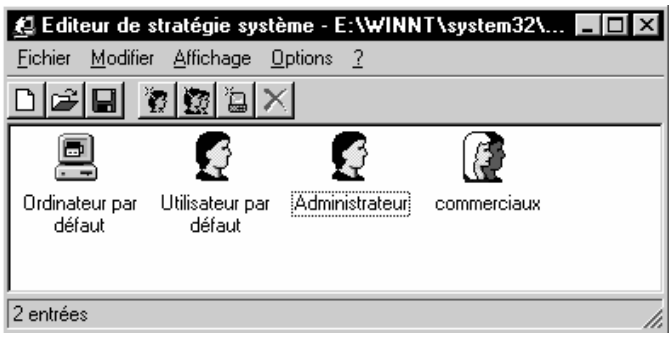
Evidemment un utilisateur pouvant faire partie de plusieurs groupes, on peut définir le groupe dont l'appartenance sera capitale pour décider de la stratégie à utiliser.

En se positionnant sur un groupe dans l'éditeur de stratégie et en demandant le menu **Option / Priorité du groupe**

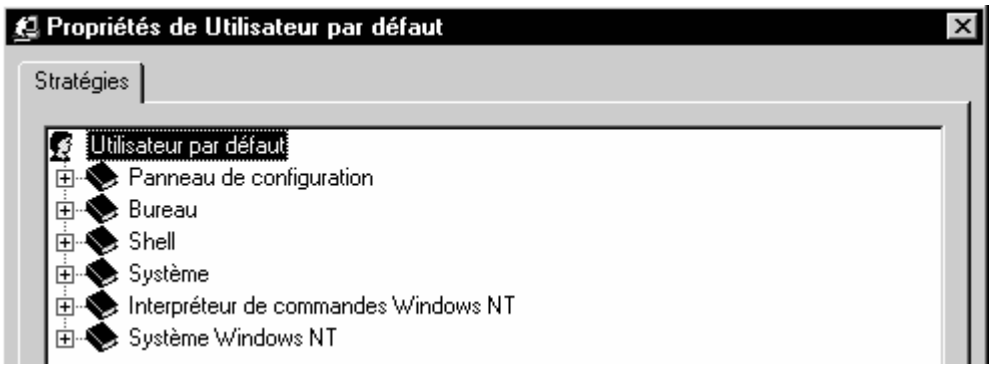
.



On visualise ainsi les cas particuliers dans l'éditeur de stratégie :



Les stratégies possible apparaissent alors listées:



3 valeurs peuvent être prises par les cases à cocher de l'éditeur de stratégies :

☑	cochée :	la stratégie est implémentée
▩	grise :	la clé de registre n'est pas modifiée
☐	blanche :	la statégie n'est pas implémentée

Logique de gestion des stratégies d'Utilisateur :

Lorsque l'utilisateur ouvre une session sur une machine NT :

- le profil éventuel est chargé, puis Windows NT cherche le fichier Ntconfig.pol sur le CPD qui a authentifié l'ouverture de session
- si une stratégie **spécifique à l'utilisateur** a été définie, celle-ci est fusionnée dans la base de registre HKEY_CURRENT_USER, elle à la **priorité sur toutes les autres ! (prendre l'habitude d'en définir une pour l'admin…)**
- si **aucune stratégie d'utilisateur n'a été définie**, mais qu'il y a un stratégie de groupe, on utilise une combinaison de toutes les stratégie de groupe, et si il y a certains conflits sur une stratégie, on applique celle du groupe ayant la plus haute priorité auquel l'utilisateur appartient pour la fusionner dans la base de registre HKEY_CURRENT_USER
- si aucune stratégie spécifique n'est définie, la stratégie de l'utilisateur par défaut est fusionnée dans la base de registre HKEY_CURRENT_USER

Logique de gestion des stratégies d'Ordinateur :

Lorsque l'utilisateur ouvre une session sur une machine NT :

- le profil éventuel est chargé, puis Windows NT cherche le fichier Ntconfig.pol sur le CPD qui a authentifié l'ouverture de session
- si une stratégie spécifique à l'Ordinateur a été définie, celle-ci est fusionnée dans la base de registre HKEY_LOCAL_MACHINE
- si aucune stratégie d'Ordinateur particulière n'a été définie, on utilise la stratégie de l'Ordinatuer par défaut qui est fusionnée dans la base de registre HKEY_LOCAL_MACHINE

Remarques sur les stratégies :

les stratégies s'ajoutent aux profils, et ont des objectifs de restrictions d'utilisation de la machine pouvant être souvent interprétées comme des disfonctionnement du poste de la part de l'utilisateur

Il peut être bon lors de l'utilisation de stratégies d'informer systématiquement l'utilisateur lors de l'ouverture de la session que des stratégies sont en œuvres…Cependant il faut prévoir un message générique, car la bannière fait partie des stratégies d'ordinateur, donc à moins de prévoir machine par machine qui va ouvrir une session, la personnalisation du message devient difficile…

Attention à ne pas inclure l'administrateur dans un groupe pour lequel une stratégie restrictive aurait été définie, celui-ci en bénéficierais automatiquement… **IL VAUT MIEUX DONC SE CREER UNE STRATEGIE SPECIFIANT TOUS LES DROITS POUR L'ADMINISTRATEUR (TOUTES LES RESTRICTIONS DEVALIDEES) , DE MANIERE A EVITER CETTE ERREUR**

De même faire très attention à ne pas se tromper sur le serveur entre **stratégie locale** et sur **domaine**, car le serveur deviendrait vite inaccessible ! (la stratégie locale modifiant la base de registre locale, donc celle du CPD…) On peut améliorer la sécurité en installant l'éditeur de stratégie sur une autre machine NT et en copiant ensuite le fichier **Ntconfig.pol** dans le dossier **Netlogon** du serveur, ainsi en cas de "plantage" on ne se trouve pas sur le serveur !

Pour annuler une stratégie il ne suffit pas de griser forcément la case correspondante, en effet cela signifie alors que l'on ne veut pas modifier la clé correspondante de la base de registre, et si cette clé avait été modifié précédemment , on ne rétablie pas la situation…

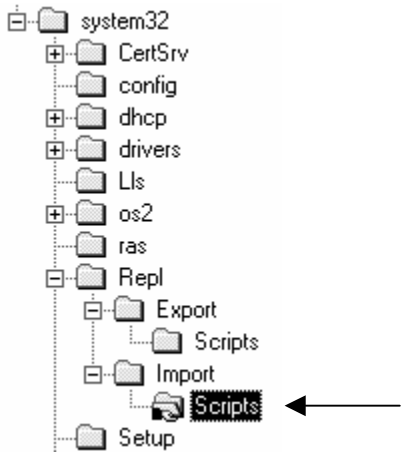
On crée alors facilement une situation confuse, dans laquelle il faut désactiver la clé de cette stratégie, ouvrir une session pour valider cette modification sur chaque client, refermer la session sur chaque client puis revenir dans le fichier de stratégie pour remettre la clé en grisé…

STRATEGIE SOUS WINDOWS 95-98

Nom et emplacement :

On l'a vu, le fichier de stratégie doit se nommer obligatoirement **Config.pol** et être sauvegardé dans le dossier partagé du serveur NT CPD nommé **Netlogon**

Le dossier qui apparaît pour les clients sous le nom **NETLOGON** est en fait un dossier situé dans le dossier principal dans lequel windows NT est installé



Winnt\system32\Repl\Import\Scripts

POLEDIT permet de se créer autant de fichier de stratégie que l'on souhaite, mais seul le fichier nommé **Config.pol** sera chargé et pris en compte par les clients windows.

Comme ce fichier doit être généré sur une machine Windows, le problème se pose de récupérer ce fichier sur le serveur… En effet les droit en accès au dossier **NETLOGON** sont en **lecture seule**, même pour l'Administrateur… Il faudra alors ouvrir une session sur le serveur et "aller chercher" le fichier sur la machine windows sur lequel il aura été fabriqué !

Stratégie d'Ordinateur:

C'est exactement le même principe que sous NT, aux possibilités près

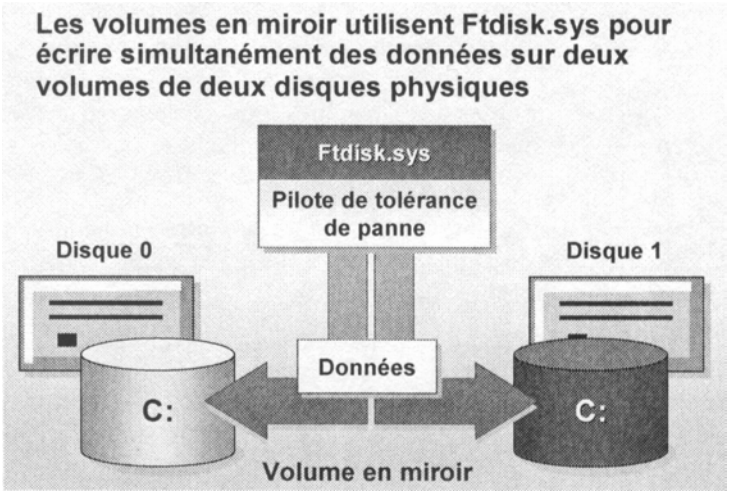
Stratégie d'Utilisateur:

C'est exactement le même principe que sous NT, aux possibilités près

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…

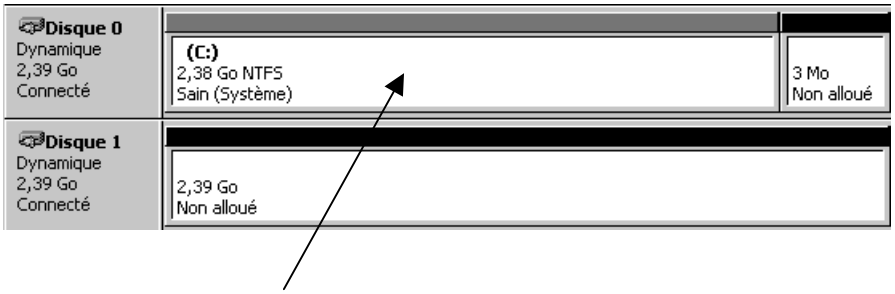
Ce système est préconisé pour les partitions système, et supporte les système de fichier FAT et NTFS

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) :

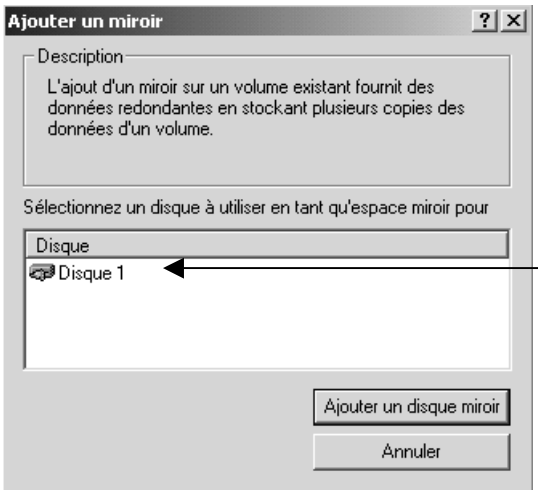
cela ne peut se faire que sur des disques dynamiques, en FAT ou NTFS, et le 2° disque doit être de capacité **>=** au premier...



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

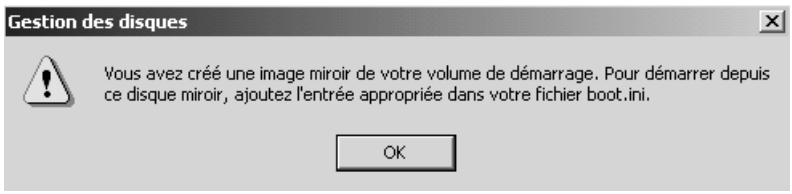
Ajouter un disque miroir

On obtient alors

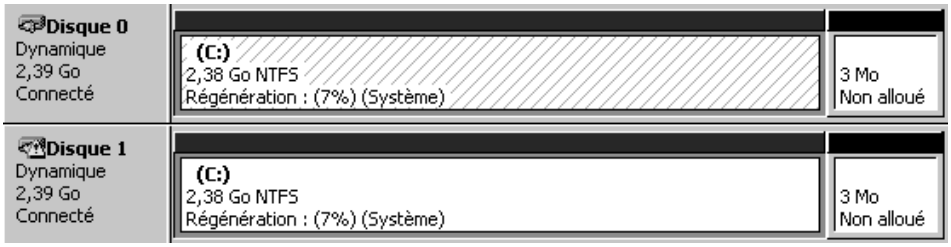


Dans laquelle il faut choisir le disque à utiliser pour construire le mirroir

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 :

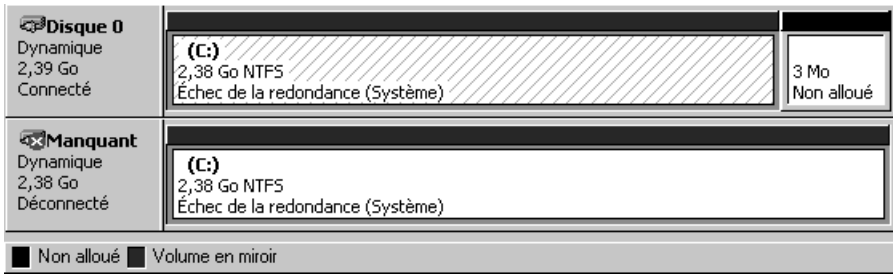
lorsque un panne arrive, la solution dépends du disque sur lequel la panne arrive.... Sur un système de base, avec sur la carte mère 1 les deux contrôlleurs IDE pilotant chacun un disque IDE configuré en maître on peut alors dire que NT étant installé (par exemple) sur le premier disque.

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

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

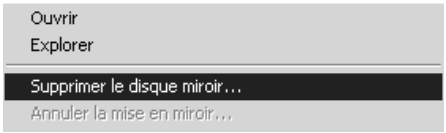
1° cas : panne du disque 2 "miroir"

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

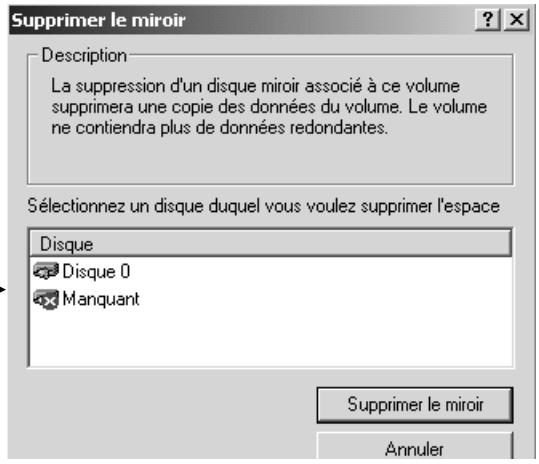


mais partons du principe que le 2° disque est irrémédiablement endommagé. Il va falloir briser le miroir, puis le reconstruire lorsque l'on aura introduit un nouveau 2°disque en état de marche.

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

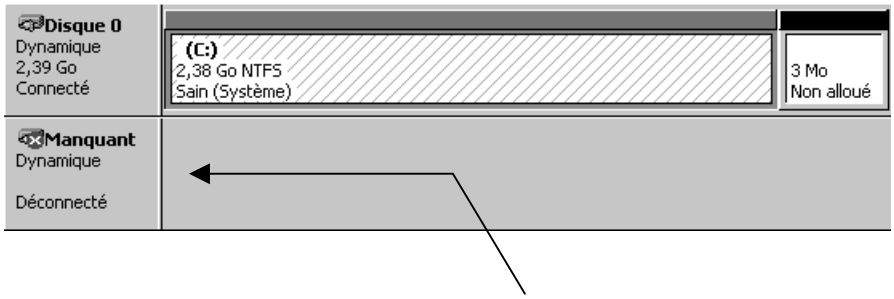


il faut choisir le disque sur lequel on veut supprimer le miroir



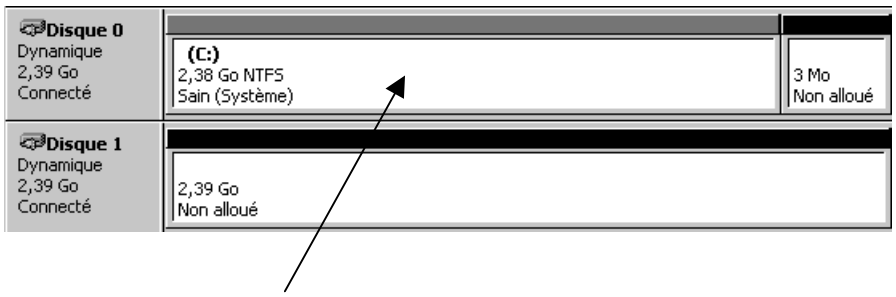
et confirmer

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 !!!!

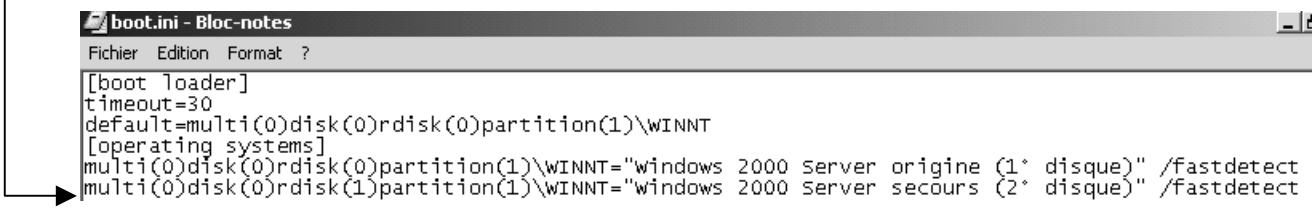
2° cas : panne du disque 1 "boot"

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 :

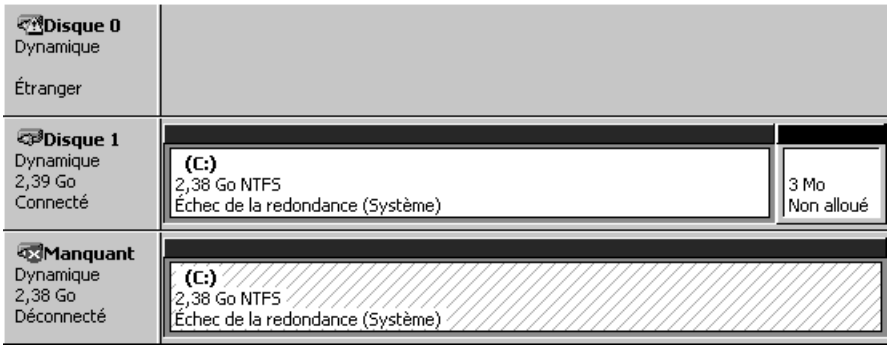
- formater la disquette **depuis NT** (pour que celle-ci cherche automatiquement un ntldr...)
- copier dessus les 3 fichiers minimum que sont **ntdetect.com**, **ntldr** et **boot.ini**
- modifier le fichier boot.ini en y rajoutant l'entrée permettant de booter sur un 2° disque, soit



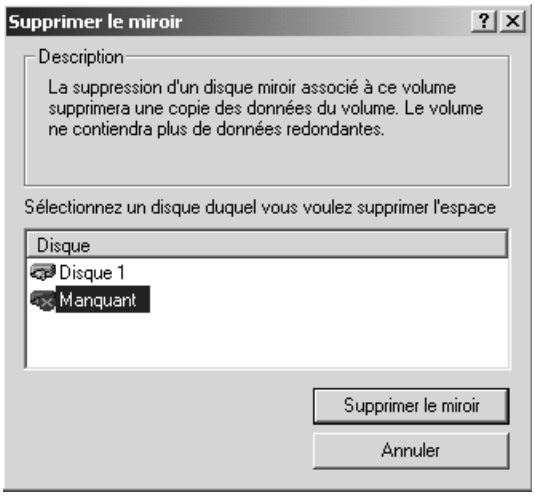
lorsque le 1° disque tombe en défaillance, il faut booter sur la disquette, et demander de démarrer sur Windows de secours.... (ou alors enlever physiquement le disque défaillant....) et le tour est joué !

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

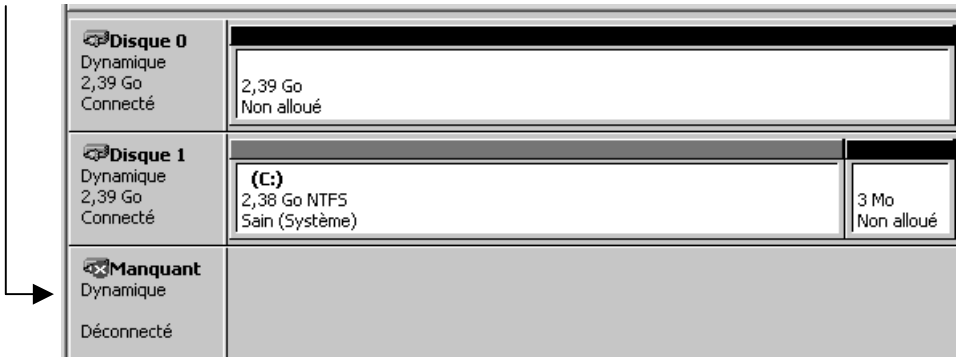
on prends alors la main, et dans le gestionnaire de disque on peut voir



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



puis supprimer le disque manquant,



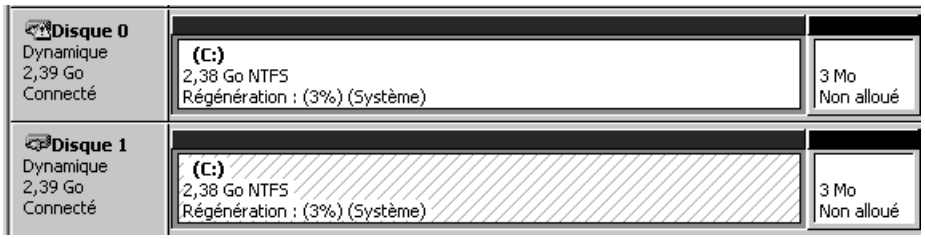
pour retrouver

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

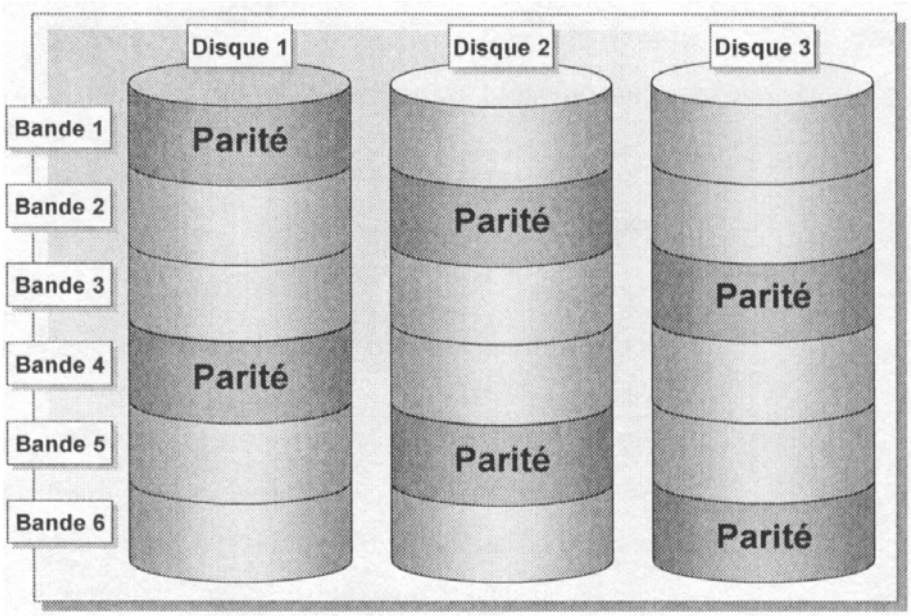
Le reste est classique !!!!



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…

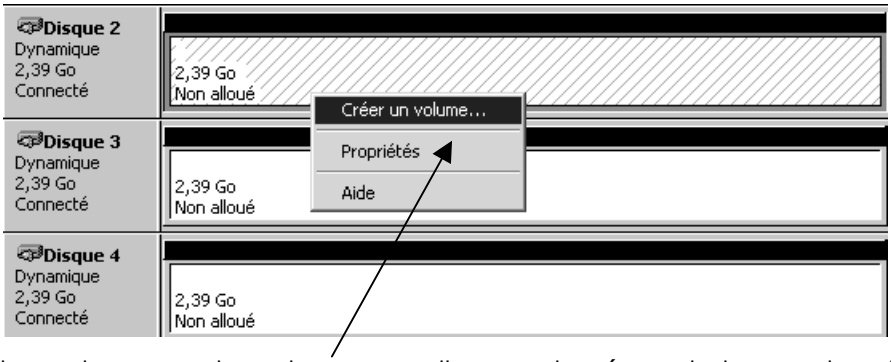
Le calcul de la place consommée et de 1 disque par système RAID5 mis en place…. L'ajout de disques supplémentaire ne modifie pas la sécurité, mais augmente la place disque de stockage et la vitesse d'accès au données.

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 :

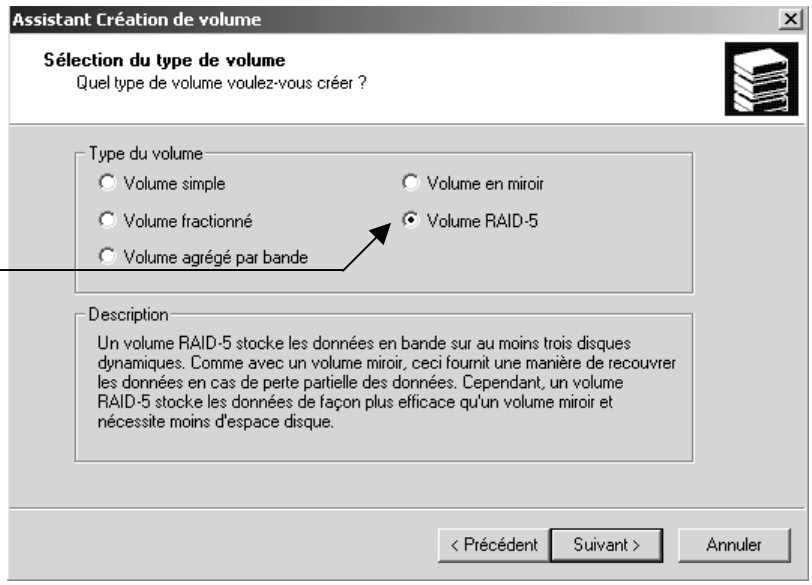
cela ne peut se faire que sur des disques dynamiques, en FAT ou NTFS, et les 3° disques (minimum)doivent être de capacité **équivalente**...



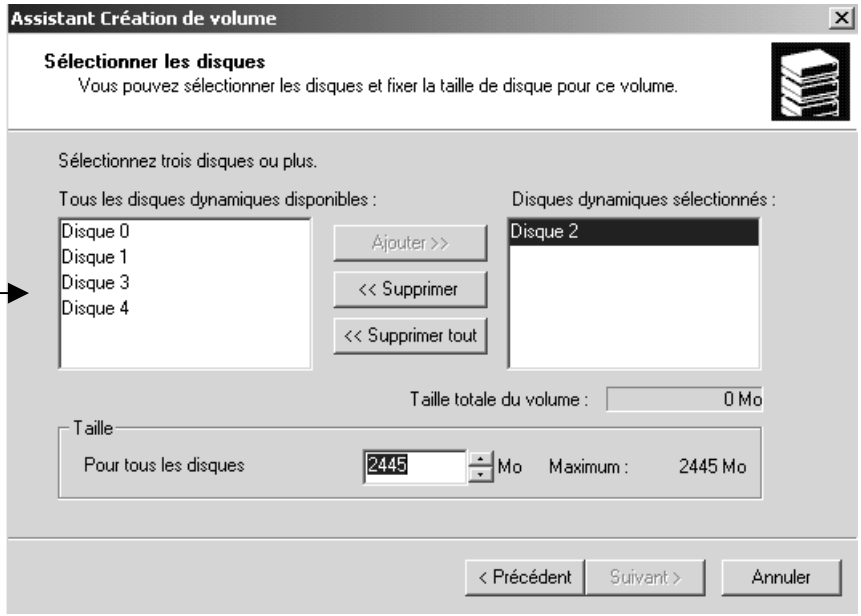
il faut se placer sur le volume que l'on veut créer, et demander via un clic droit de la souris

Créer un volume

de type **RAID-5**

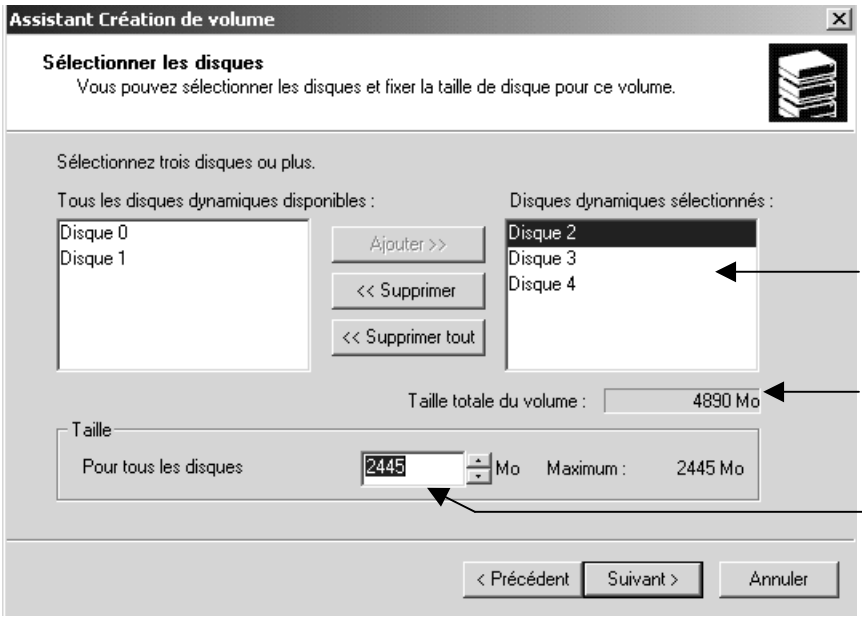


Puis dans l'étape suivante de l'assistant



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

Une fois ce choix fait, on a alors

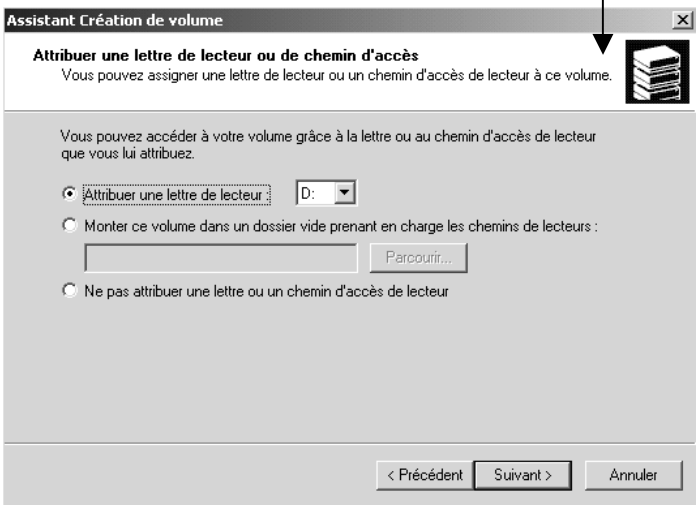


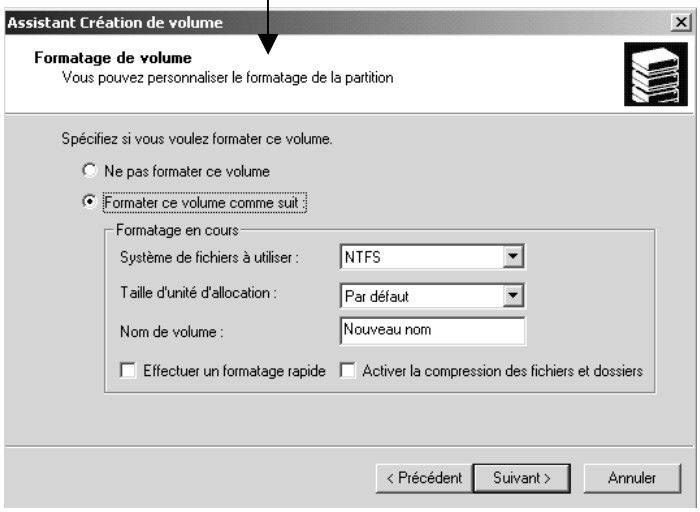
Liste des disques participant au RAID5

Volume global du RAID 5

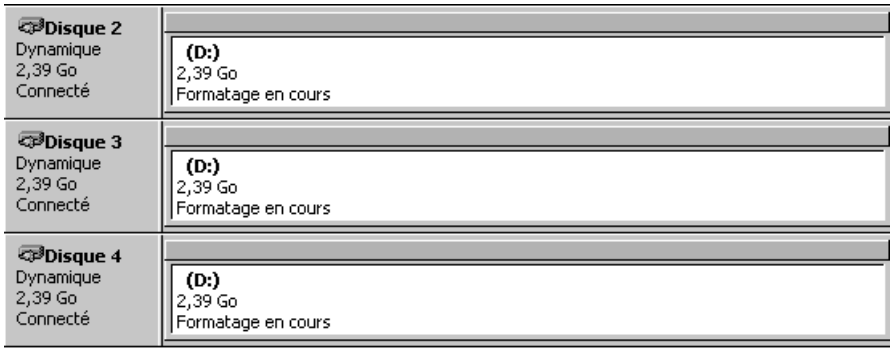
Volume pris sur chaque disque

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





et la construction du volume RAID s'effectue

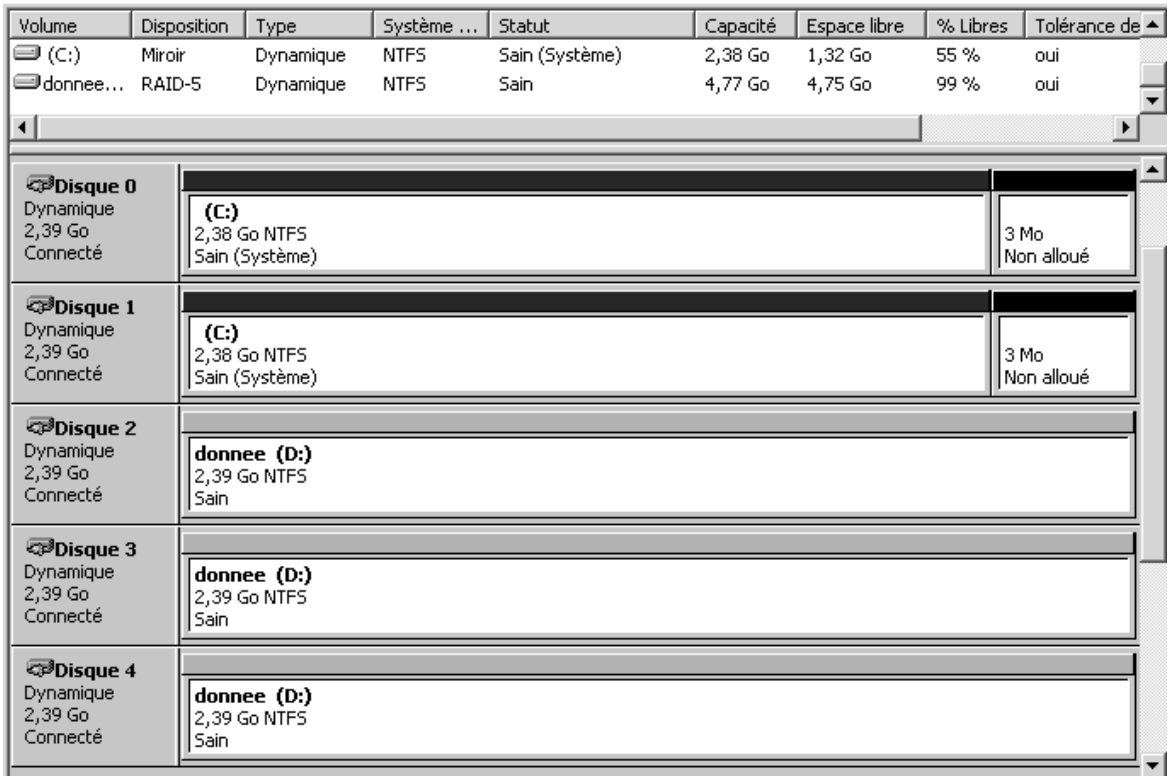


pour obtenir finalement dans le gestionnaire de disque

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 !

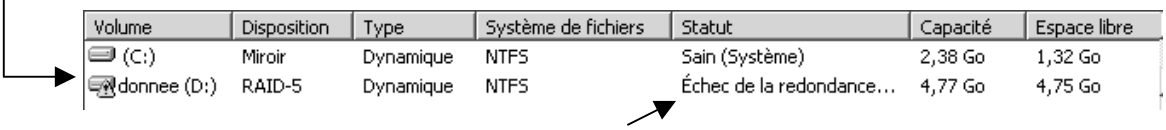
A partir de la on peut faire ce que l'on veut des volumes récupérés !

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

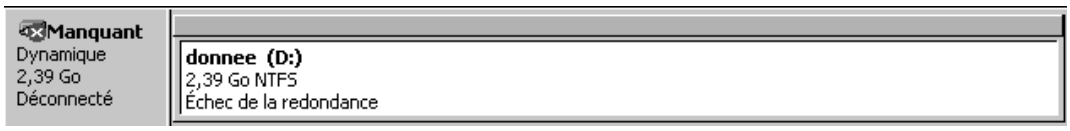


Volume	Disposition	Type	Système de fichiers	Statut	Capacité	Espace libre
(C:)	Miroir	Dynamique	NTFS	Sain (Système)	2,38 Go	1,32 Go
donnee (D:)	RAID-5	Dynamique	NTFS	Échec de la redondance...	4,77 Go	4,75 Go

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

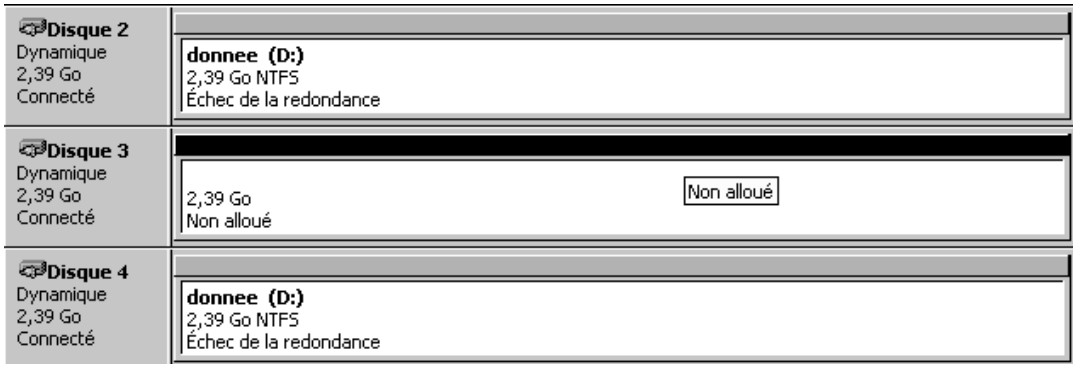
le disque posant problème est celui affichant

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 …

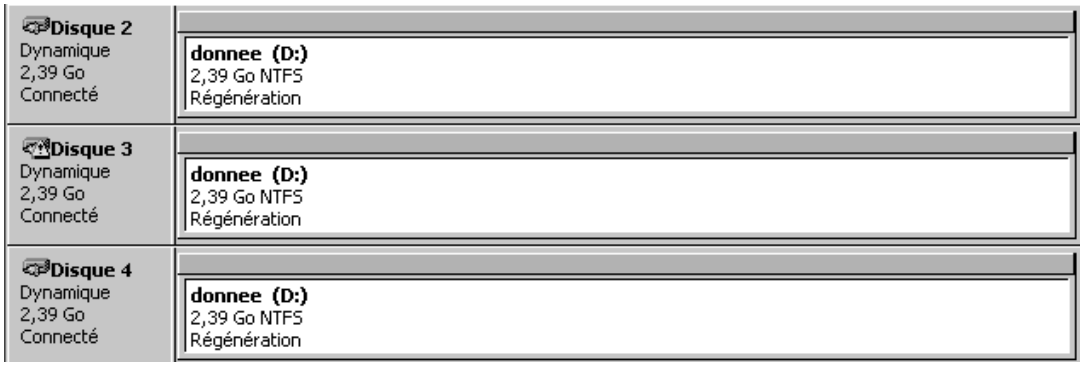


on se place sur le disque posant problème

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 EFS

EFS ou Système de Fichier Encrypté :

Le service **EFS** permet d'appliquer un cryptage au niveau des fichiers NTFS, reposant sur l'utilisation d'une clé publique…

Il existe des outils permettant de passer outre NTFS, mais il n'existe pas (encore ?) d'outils permettant de passer outre EFS

NB : cryptage et compression NFTS sont incompatibles

Différence entre une signature, et l'encryptage :

Une signature numérique, c'est un système qui assure que l'identité de l'expéditeur est bien celle supposée, est c'est un système qui vérifie que l'intégrité du message a été respectée (autrement dit on sait que le message nous vient bien de "untel" est qu'il n'a pas été modifié " en route")

Mais un message signé numériquement reste lisible par un éventuel pirate… (non modifiable, mais lisible…). Le cryptage, permet d'éviter à une tierce personne de lire le message au passage.

Mécanisme de clé secrète (symétrique) :

La même clé est utilisée pour coder – décoder le fichier. Elle doit rester forcément secrète pour assurer la fiabilité. Environ 1000 fois plus rapide que la clé symétrique. EFS crypte les fichiers avec une clé symétrique, amis crypte cette clé symétrique avec une clé asymétrique dans les certificats…

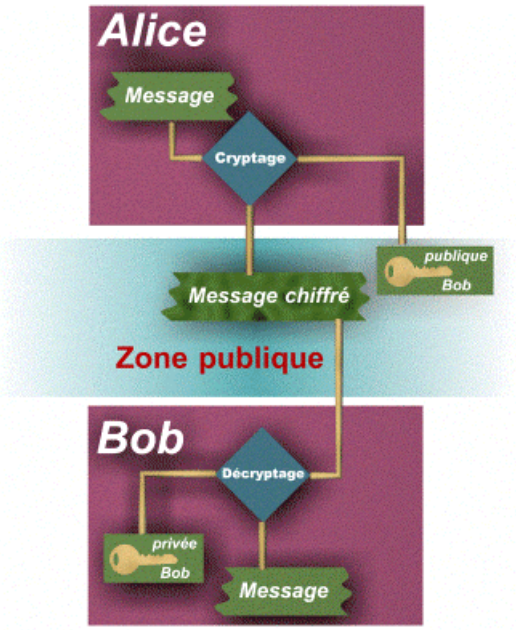
Mécanisme de clé publique – clé privée (asymétrique):

En effet comme il est impossible de prévenir d'une interception frauduleuse des données il faut donc rendre ces informations illisibles par son intercepteur. Pour cela RSA a développé en 1977 un système de cryptage dit "a clé publique" qui répond parfaitement à ce besoin

Il est important de bien comprendre le fonctionnement d'un tel algorithme de cryptage : Cet algorithme fonctionne a l'aide de 2 clés une publique et une privée, tout phrase cryptée par la clé publique ne peut être décryptée que par la clé privée et vice-versa.

Grâce a ce principe, nous pouvons établir une transmission sécurisée (voir schéma 1) de Alice a Bob.

- Bob diffuse sa clé publique
- Alice crypte le message qu'elle désire envoyer à Bob avec cette clé.
- Bob pourra décrypter ce message. (et que lui)

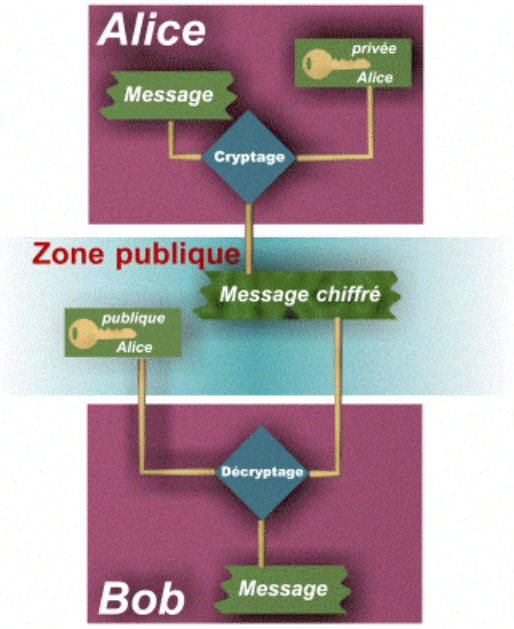


Transmission de Alice a Bob sécurisée

N.B: Bien sur il faut s'assurer que la clé présente dans la zone publique est bien celle de Bob pour cela il existe un **mécanisme de certificat**

Il est aussi possible grâce a ce principe de signer électroniquement (voir schéma 2) .

- En effet si Alice crypte un message avec sa clé privée
- seulement sa clé publique pourra le décrypter…
- Bob est donc sûr que c'est Alice qui a signé ce message.



Signature électronique d'Alice

Mécanisme de Certificat :

Comme nous avons vu , il n'est pas possible de garantir qu'une clé présente dans la zone publique appartient bien à la personne que vous désirez contacter de manière sécurisée. Pour cela nous avons besoin d'un tiers de confiance qui va lui assurer l'appartenance des clés publiques

Donc il vous faut impérativement un certificat. Le format des certificats est défini par la norme **X509**.

Le procédé de certification est assez simple : vous contactez **un tiers** certificateur, vous lui transmettez vos coordonnées et votre clé publique et celui-ci, après s'être assuré de la validité de ces informations, vous donne une chaîne de caractère qui est en fait le certificat crypté par la clé privée de ce **tiers** (sa signature électronique lisible avec sa clé publique…)

Donc pour récupérer votre clé publique, il faut que votre « contact » montre patte blanche auprès de **ce tiers**, afin que celui-ci le reconnaisse et lui délivre votre clé publique, c'est la rançon à payer pour être sûr de votre clé publique

Donc en fait les deux interlocuteurs doivent passer par un tiers auprès duquel il se sont enregistrés, de manière à être surs des provenances des clé publiques respectives. Ces deux interlocuteurs s'assurent de l'identité du tiers car toutes les informations qu'ils reçoivent de ce tiers (et notamment leurs clés publiques respectives) sont cryptée et décodables uniquement avec la … clé publique du tiers !

Fonctionnement d' EFS :

Le système **EFS** inclus dans windows2000 permet donc à un utilisateur de chiffrer un fichier de manière a ce que celui-ci ne puisse pas être lu par quelqu'un d'autre que lui (saut un compte particulier, appelé **agent de récupération**, généralement un administrateur…)

Sans la « clé », le fichier est véritablement indécryptable, même par l'administrateur. Seul un agent de récupération peut être alors utilisé pour relire le fichier. POUR LIRE UN FICHIER EFS, même si ont dispose de tous les droits NTFS, même si on s'est approprié le fichier , IL EST NECESSAIRE DE DISPOSER DE LA CLE PRIVEE (ou d'être AGENT DE RECUPERATION). Ainsi un disque « démonté et remonté sur un autre système » ou un portable reste protégé.

EFS fonctionne en arrière plan, et stocke dans le fichier lui-même un certain nombre d'informations (qui a chiffré, avec quelle clé, liste des agents de récupération…).

N.B: certaines applications peuvent sauvegarder des fichiers temporaires, et donc risquent de laisser des traces lisibles de vos fichiers, il vaut mieux pour éviter cela **demander de crypter tout un dossier, plutôt que uniquement un fichier**…. (dans ce cas, chaque fichier posé dans ce dossier sera automatiquement chiffré avec la clé de son propriétaire…)

Pour qu'EFS fonctionne il est nécessaire que :

- Vous soyez sur un volume NTFS 2000
- L'utilisateur ait un certificat valide d'utilisateur EFS
- Un compte d'agent de récupération d'EFS au moins ait un certificat valide de récupération d'EFS
  (une autorité de certification n'est pas nécessaire, EFS produit automatiquement ses propres certificats pour les utilisateurs et les comptes d'agent de récupération…)

Lorsque EFS chiffre un fichier :

Lorsque un utilisateur chiffre un fichier, les opérations suivantes sont exécutées :

- Production d'une clé de chiffrement
- Chiffrage du fichier avec cette clé de chiffrement
- Chiffrage de cette clé de chiffrement avec la clé publique de l'utilisateur (si nécessaire création de cette clé et du certificat associé)
- Stockage de cette « clé de chiffrage chiffrée » dans le fichier dans une zone nommée DDF (une par fichier)

Résultat : lorsque l'on essayera de lire un fichier chiffré, seul le possesseur de la clé privée de cet utilisateur, peut déchiffrer la clé de chiffrage employée lors du codage. Ce ne peut être que l'utiliateur

Mais n'oublions pas que EFS permet à des comptes définis d'agent de récupération de déchiffrer et de récupérer le fichier, au cas ou la clé privée serait détruire (exemple, un utilisateur renvoyé crypte tous ses fichiers avent de partir…)

Donc lorsque un utilisateur chiffre un fichier les opérations suivantes sont aussi exécutées :

- Chiffrage de cette clé de chiffrement avec la clé publique de chaque agent de récupération
- Stockage de cette « clé de chiffrage chiffrée » dans le fichier dans une zone nommée DRF (une ou plusieurs par fichier)
- Chaque fois que l'on manipule ce fichier, copie, ouverture, modification, la zone DRF est mise à jour selon les besoins

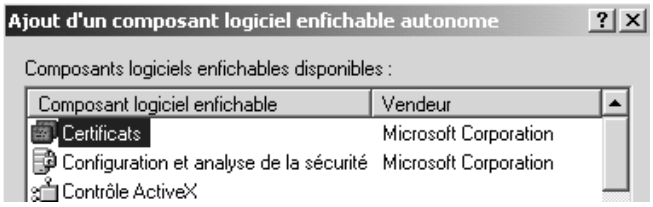
Résultat: seul le possesseur de la clé privée des agents de récupération peu lire le fichier

Mise en oeuvre :

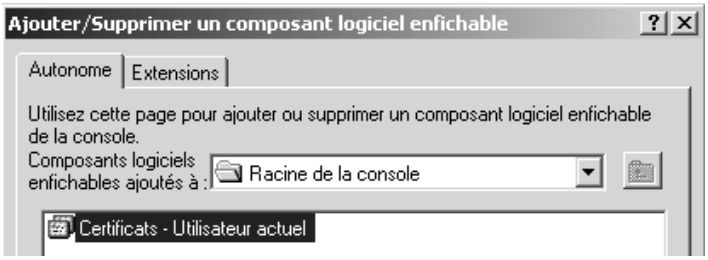
Soit 2 utilisateurs sur un poste 2000, andré et bruno,

Vérifions d'abords par exemple pour andré que celui-ci ne possède pas de certificat permettant de stocker une clé publique (il n'a jamais chiffré de fichier, et n'a donc jamais eut besoin d'une clé privée+clé publique…)

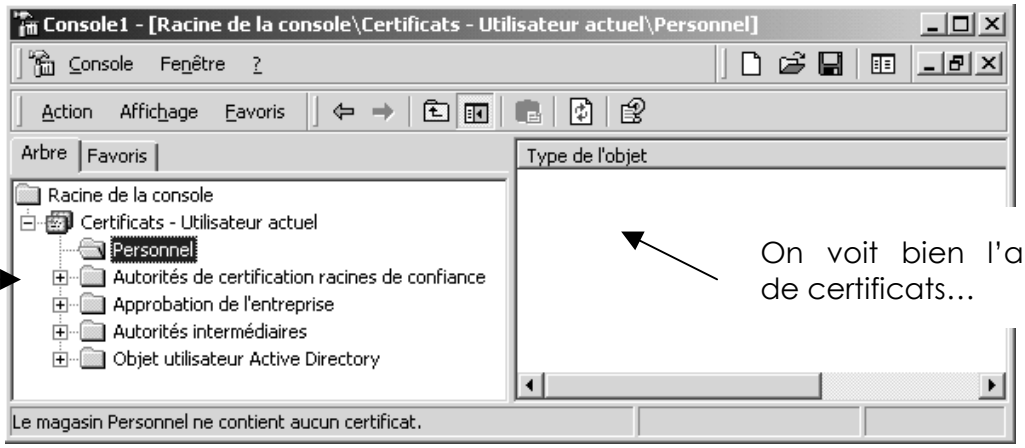
Il suffit de créer une **mmc** avec le composant **Certificats**



pour obtenir



Dans la console en se plaçant sur **Personnel**

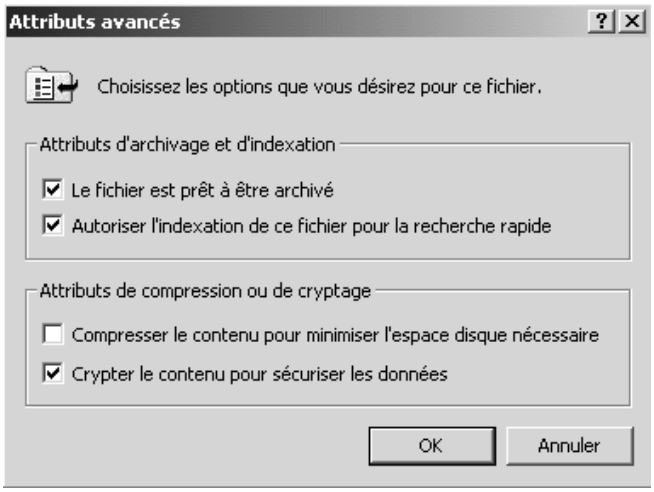


On voit bien l'absence de certificats…

dans un dossier que vous nommez **testefs**, andré crée un fichier nomme **essais andré**

puis il le chiffre... par **propriété** sur ce fichier, et **avancée**

On demande un cryptage via EFS en cochant cette case

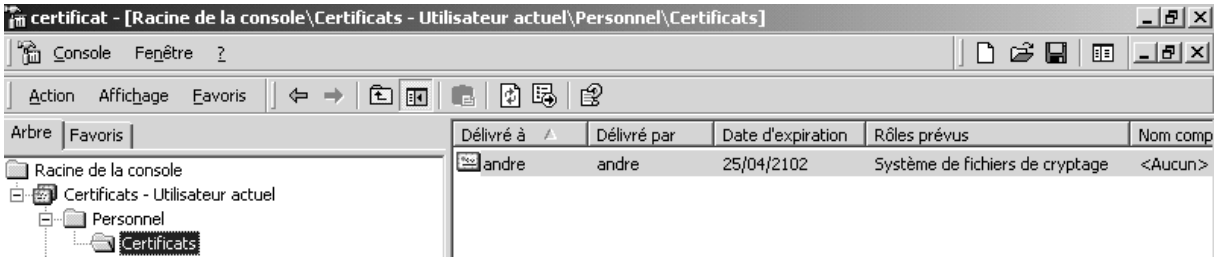


Une mise ne garde concernant le cryptage fichier ou dossier apparaît

et voilà !

A partir de maintenant, indépendamment des droits NTFS, Bruno ne peut plus ouvrir le fichier **essais andré**

Automatiquement, lors du premier appel à EFS de la part de André, une création de clé a été effectuée, et un certificat a été délivré…



par ailleurs il y a forcément un agent de récupération, on peut le connaître en utilisant un utilitaire du kit nommé **esfinfo.exe** dont l'appel en ligne de commande via **esfinfo** ou **esfinfo /r** donne

```
C:\testefs>efsinfo

C:\testefs\

essai andre.rtf: Encrypted
  Users who can decrypt:
    PROS1\andre (CN=andre,L=EFS,OU=EFS File Encryption Certificate)

C:\testefs>efsinfo /r

C:\testefs\

essai andre.rtf: Encrypted
  Recovery Agents:
    PROS1\Administrateur (OU=EFS File Encryption Certificate, L=EFS, CN=Administ
rateur)
```

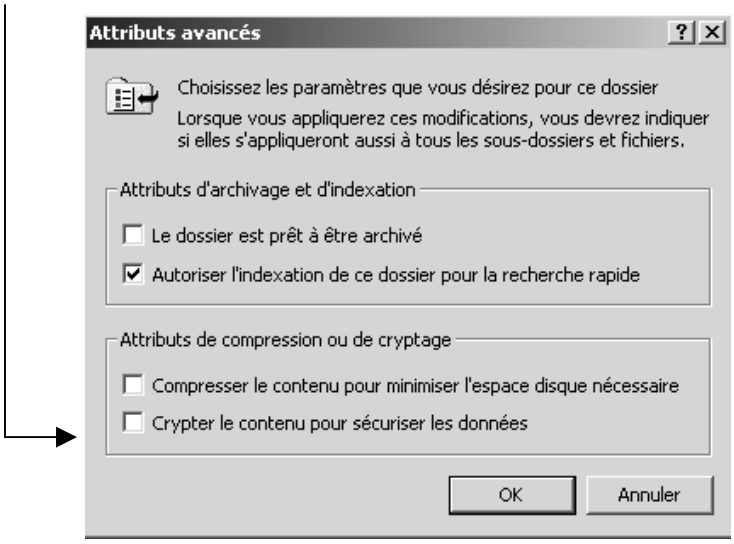
Si on souhaite que un autre utilisateur (a part l'agent de récupération) puisse modifier le fichier, il faut exporter la clé privée de l'utilisateur qui a chiffré le fichier, et l'importer pour l'utilisateur à qui on veut fournir l'accès…(Voir TP)

Donc un fichier crypté dans un domaine, pourra être "lu" sur n'importe quelle machine, a partir du moment ou l'on ouvre une session du domaine… Si on se transfère sur une autre machine (autre domaine ou chez soi) il faut emporter aussi le certificat avec la clé privée, et être repéré comme agent de récupération !

SI la clé privée est inutilisable, (utilisateur inexistant) l'agent de récupération peut ouvrir le fichier en utilisant sa propre clé cryptée. Si l'agent de récupération se trouve sur un autre ordinateur, il faut lui envoyer le fichier à décrypter, plutôt que l'agent vous envois sa propre clé cryptée…

Décryptage d'un fichier

De manière générale, lors d'une manipulation, pour décrypter un fichier il suffit de décocher la case **crypter le contenu**… dans avancée



On peut aussi utiliser une commande en ligne **cipher** dont l'aide donne :

```
E:\>cipher /?
Affiche ou modifie le cryptage de répertoires [fichiers] sur partitions NTFS.

  CIPHER [/E | /D] [/S:dir] [/A] [/I] [/F] [/Q] [/H] [/K] [Chemin [...]]

    /E      Crypte les répertoires spécifiés. Les répertoires seront marqués
            afin que les fichiers ajoutés ultérieurement soient cryptés.
    /D      Décrypte les répertoires spécifiés. Les répertoires seront marqués
            afin que les fichiers ajoutés ultérieurement ne soient pas cryptés.
    /S      Effectue l'opération spécifiée sur les répertoires dans le
            répertoire donné et tous ses sous-répertoires.
    /A      Traite aussi bien les fichiers que les répertoires. Le fichier
            crypté peut devenir décrypté s'il est modifié et que le répertoire
            parent n'est pas crypté. Il est recommandé de crypter le fichier
            et le répertoire parent.
    /I      Poursuit l'opération spécifiée même si des erreurs se sont
            produites. Par défaut, CIPHER s'arrête lorsqu'une erreur se
            produit.
    /F      Force l'opération de cryptage sur tous les objets spécifiés, y
            compris ceux qui sont déjà cryptés. Les objets déjà cryptés sont
            ignorés par défaut.
    /Q      Signale uniquement les informations les plus importantes.
    /H      Affiche les fichiers dont l'attribut est Caché ou Système. Ces
            fichiers sont omis par défaut.
    /K      Crée une nouvelle clé de cryptage pour l'utilisateur exécutant
            CIPHER. Si cette option est choisie, toutes les autres sont
            ignorées.
    Chemin  Spécifie un motif, un fichier ou un répertoire.

    Utilisé sans paramètres, CIPHER affiche l'état de cryptage du répertoire
    en cours et des fichiers qu'il contient. Vous pouvez utiliser plusieurs
    noms de répertoires et des caractères génériques. Vous devez placer des
    espaces entre chaque paramètre.
```

ainsi **cipher** donnerait:

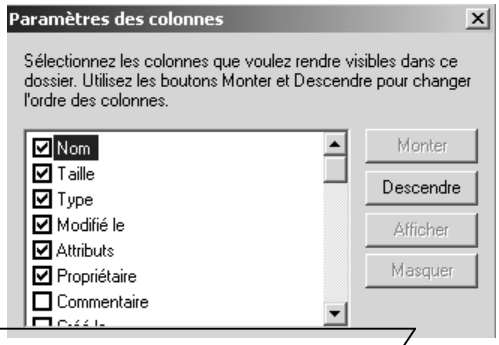
E pour encrypté

```
F:\newdata2>cipher

 Liste F:\newdata2\
 Les nouveaux fichiers ajoutés à ce répertoire ne seront pas cryptés.

U commerciaux
E Nouveau Texte seulement.txt
U secretaires
```

N.B : l'attribut E peut apparaître aussi dans l'explorateur de fichier

Il faut demander dans l'explorateur le menu :

Affichage / Choisir des colonnes



Nom	Taille	Type	Modifié le	Attributs
commerciaux		Dossier de fichiers	26/06/2001 19:50	A
secretaires		Dossier de fichiers	26/06/2001 19:50	A
Nouveau Texte seulement.txt	0 Ko	Texte seulement	19/05/2002 07:33	AE

Puis demander dans le menu :

Outils / Option des dossiers Comme de dossier actuel

Manipuler un fichier crypté

Lorsque l'on effectue les manipulations sur les fichiers cryptés, de manière générale, le fichier est décrypté, modifié, puis recrypté sous sa nouvelle forme ou destination si cela est possible

Ainsi lorsque l'on :	le chiffrage est
• Change le nom	maintenu
• Déplace Copie le fichier	maintenu si cible sur NTFS2000
• Déplace vers un autre PC	si la cible accepte EFS, maintenu avec la clé publique de l'expediteur. L'ordinateur cible doit être approuvé pour la délégation (voir dans Utilisateur et Ordinateur Active Directory, dossier Computer, propriété de l'ordinateur sur lequel on veut effectuer le transfert, onglet Général, la case à cocher Approuver l'ordinateur pour la délégation
• Sauvegarde	avec l'outils backup maintenu

« Philosophie » dans la méthode de cryptage :

lorsque l'on crypte, on peut crypter un fichier ou un dossier

Si on crypte que le fichier, les conséquences sont claires

Si on crypte le dossier alors on aura :

- Tous les fichiers existants sont protégés par notre clé (mais que si on peut écrire dedans au niveau des ACL)
- Tout ce qui sera crée ou copié plus tard dans ce dossier par nous sera protégé par notre clé
- Tout ce qui sera crée par un autre utilisateur sera protégé par sa clé
- Tout ce qui sera déplacé restera inchangé (au niveau cryptage)

IL VAUT MIEUX POSER UN CRYPTAGE PAR DOSSIER VIDE AVANT TOUTE UTILISATION

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 !**

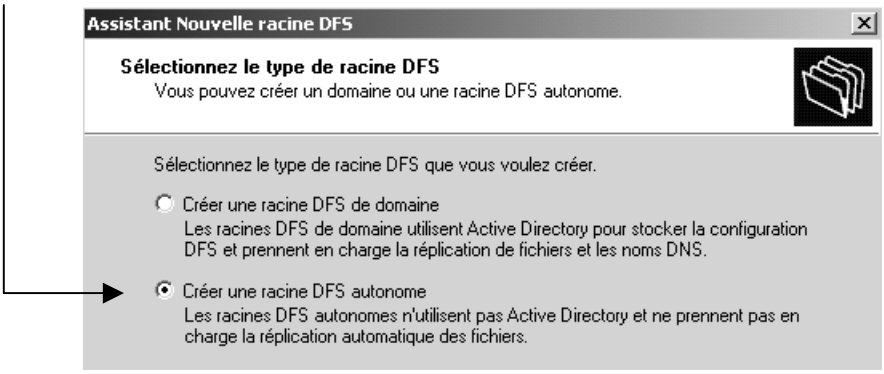
Il existe des racines **DFS de Domaine**, c'est à dire hébergées sur plusieurs serveurs du domaine, la topologie étant stockée dans Active Directory

Création d'une racine DFS autonome :

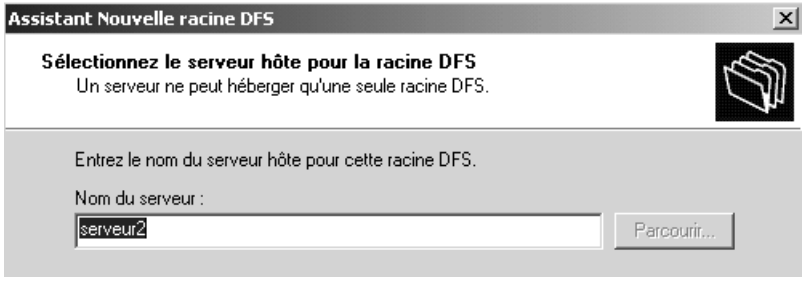
Il faut lancer dans les outils d'administration **Système de fichiers distribués**

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

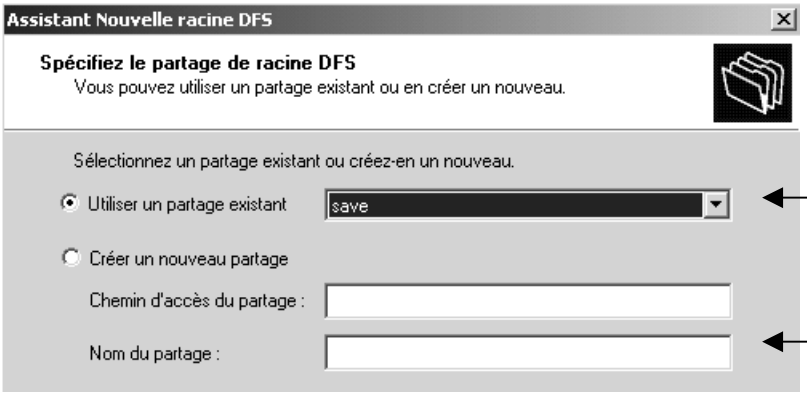
Dans lequel on va demande de créer une racine autonome



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



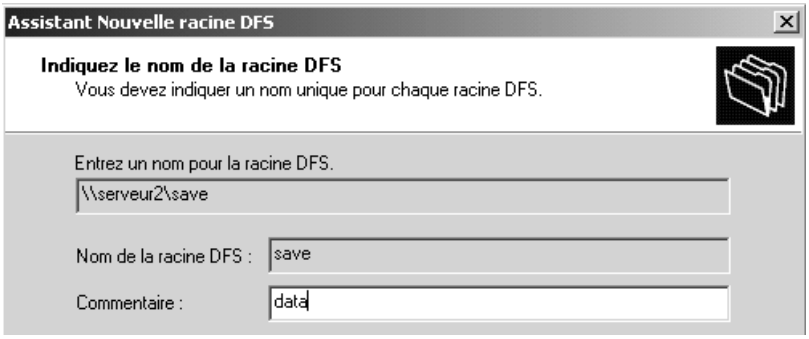
Et indiquer le partage que l'on veut rendre racine DFS



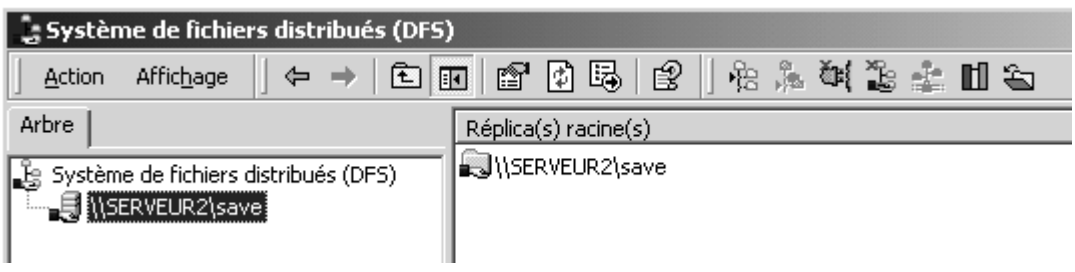
Ici apparaît une liste de tous les partages existants sur ce serveur...

Mais on peut s'en créer un à la volée

Il faut ensuite confirmer le nom de la racine DFS

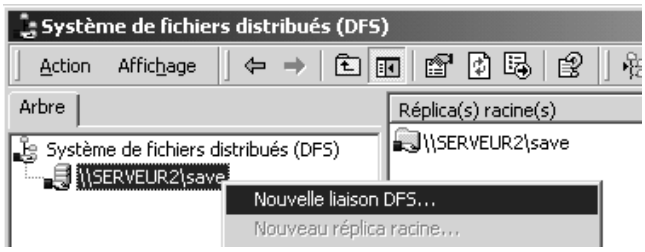


pour obtenir enfin notre structure :



Ajout d'un lien dans une arborescence DFS autonome :

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

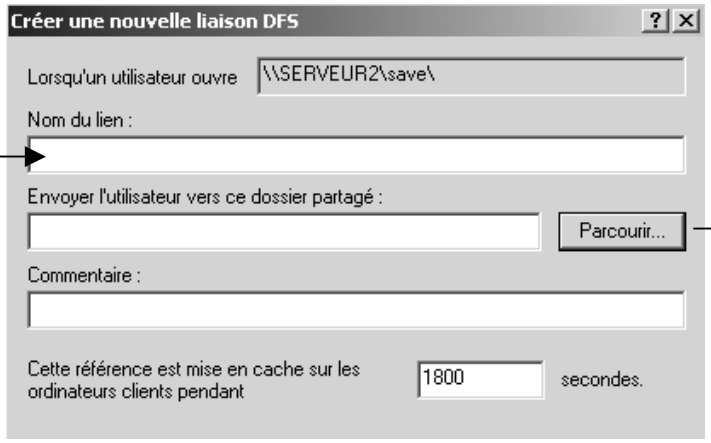


On se place sur notre racine...

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

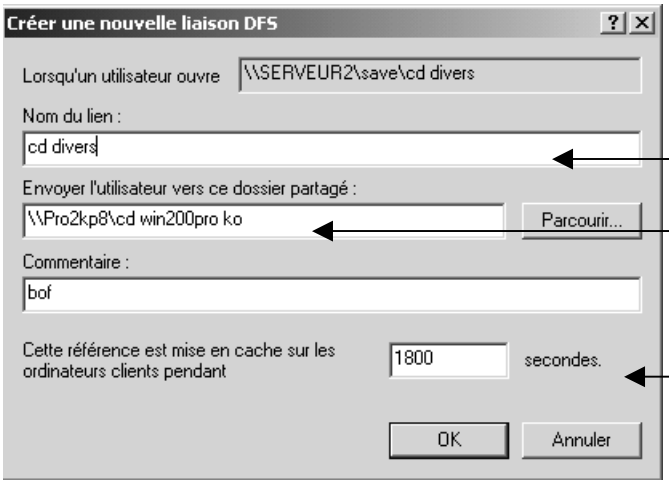
Dans la boite de dialogue qui apparaît

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



Et définir quel dossier partagé correspond

Pour obtenir par exemple

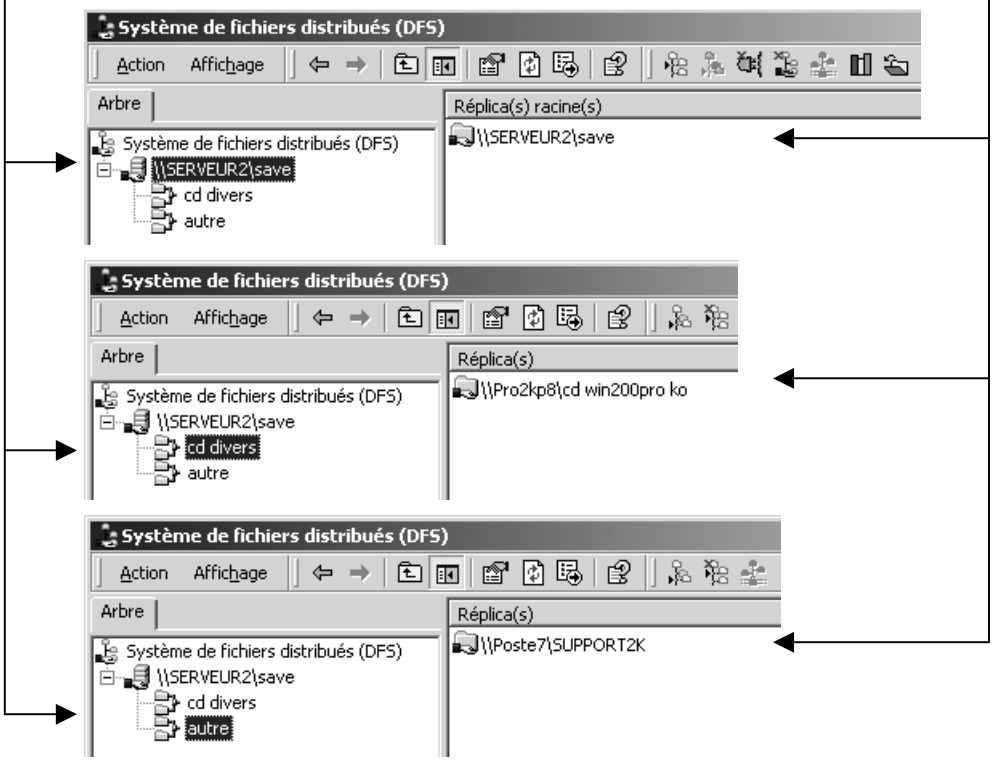


A un **Nom de lien DFS**

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...

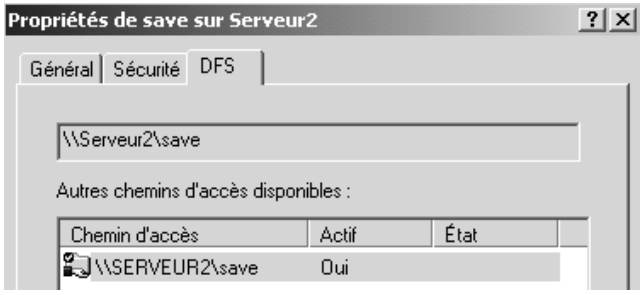


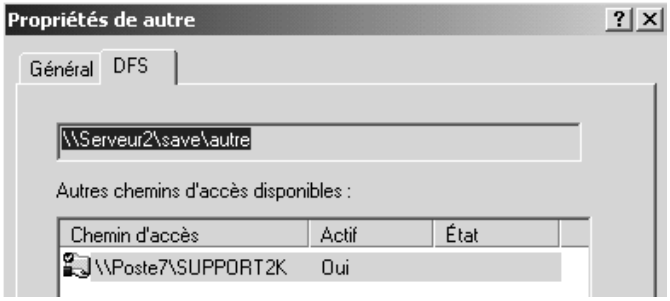
Utilisation d'une arborescence DFS autonome :

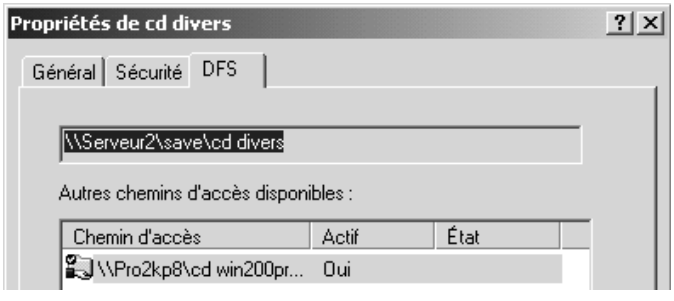
La seule chose que l'utilisateur doivent savoir, c'est où se trouve la racine de l'arborescence DFS, (c'est à dire son nom de partage sur le serveur...)

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

par propriété que alors on voit l'emplacement



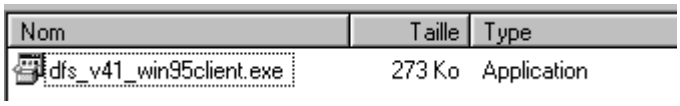




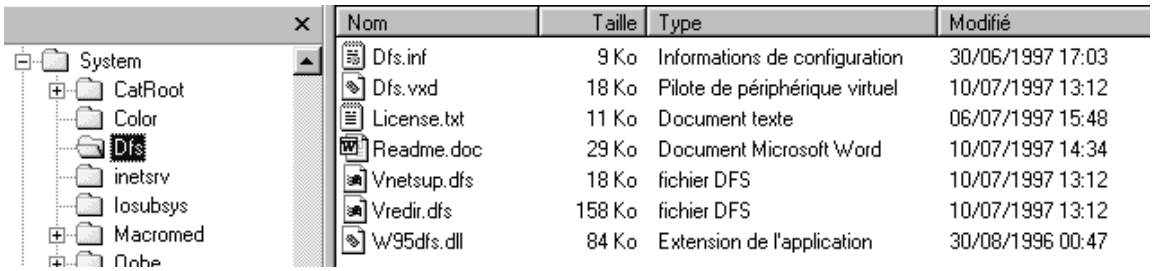
Utilisation de DFS depuis un poste Win95 :

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

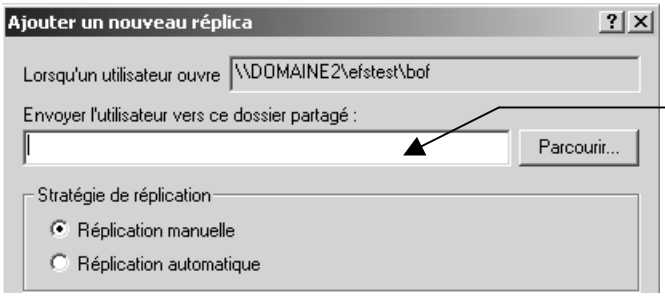
Création de réplica:

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**…



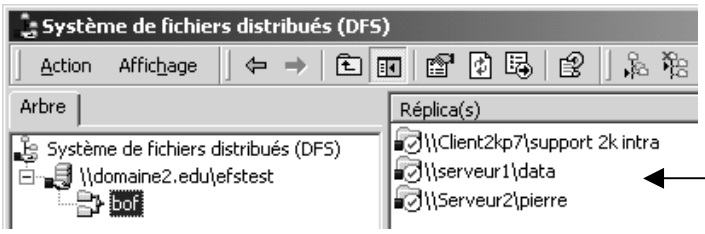
On indique ici le partage sur un autre poste…

Chaque lien DFS peut avoir 32 réplicas…

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

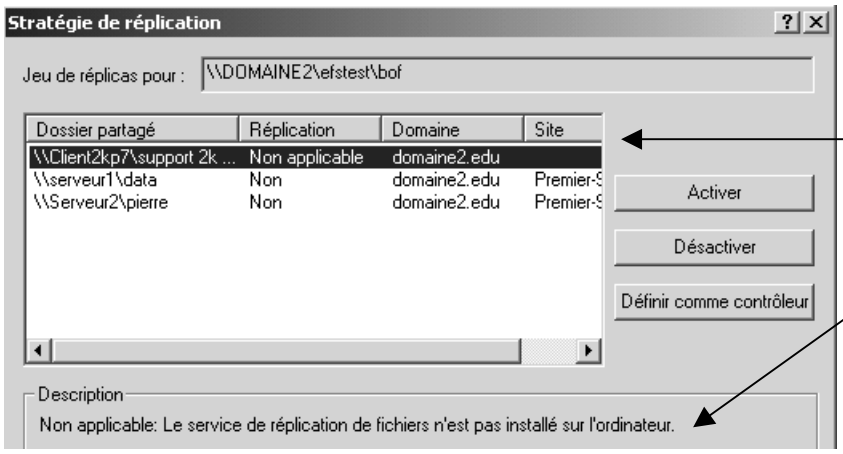
Il existe un mécanisme de réplication que l'on peut mettre en œuvre, mais uniquement si les réplicas sont sur des **serveurs 2000** et dans **1 domaine**.

Soit un lien DFS ici avec 3 réplicas



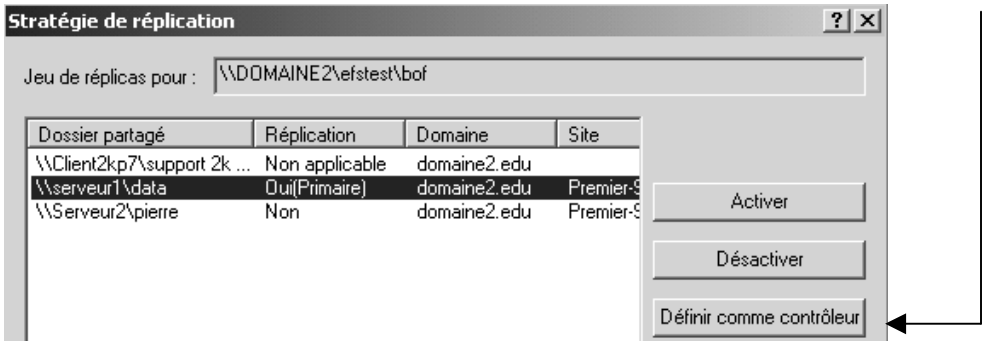
2 réplicas sur serveur et 1 réplica sur un client 2000

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

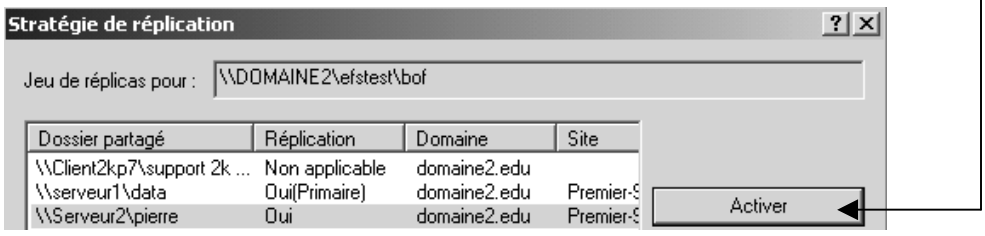


On ne peut pas faire de stratégie de réplication si le poste n'est pas un serveur 2000

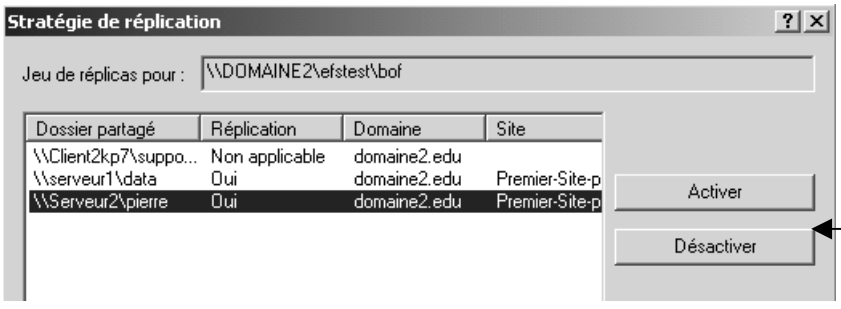
Il va falloir décider qui est contrôleur de la duplication (pour le 1° échange)



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

TERMINAL SERVER

Principe de base :

Chaque machine sous Windows 2000 peut être transformée en **serveur d'applications**. Ce système permet à chaque membre du réseau d'exécuter des programmes directement sur le serveur plutôt que sur son propre poste, baptisé à l'occasion client léger.

En effet, ce dernier n'abrite plus les applications sur son disque dur, puisque celles-ci sont désormais centralisées sur le serveur. Le client accède à l'application par une fenêtre qui lui donne l'impression que tous les traitements sont effectués sur sa machine. (Une utilisation de terminal server, peut être par exemple de permettre d'administrer à distance un serveur depuis n'importe quel client 2000)

le client se connecte au serveur sur lequel il fait tourner une application. Il lui envoie des informations telles les déplacements de la souris et les frappes au clavier. Le serveur interprète ces événements et exécute les requêtes comme si elles étaient effectués sur le poste client.

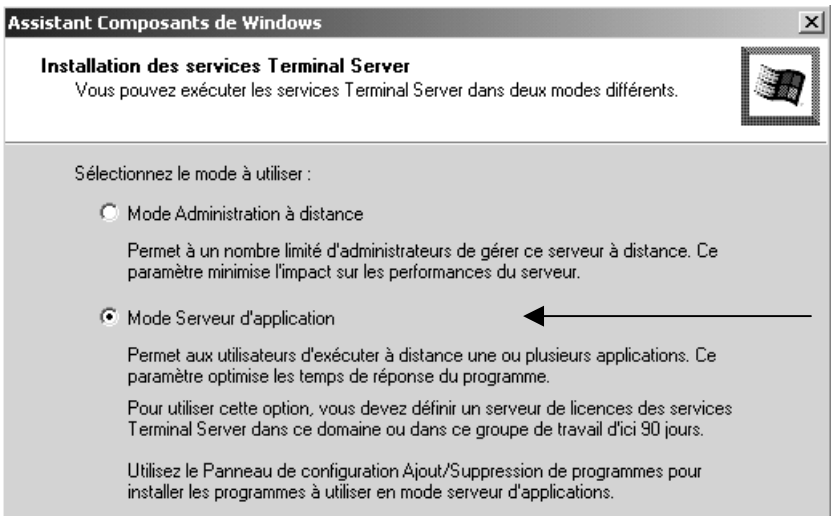
L'avantage de ce système repose sur la rapidité d'exécution de l'application. Celle-ci dépend en fait de la capacité du serveur, généralement largement plus puissant qu'un poste client. **Ceci permet aux utilisateurs de machines peu puissantes d'utiliser des logiciels réclamant des ressources qu'ils ne possèdent pas sur leurs machines**. Mais si trop de clients sont connectés au serveur, cette rapidité d'exécution tourne à une lenteur intolérable ! En caricaturant on peut avoir 50 clients sous windows 3.1 utilisant word2000 ! bien sûr il faut que le serveur soit capable de supporter 50 instances de Word 2000 !

Installation composant service Terminal Server:

Dans **Ajout/Suppression de programmes**. on demande **Ajouter/Supprimer des composants Windows** avec

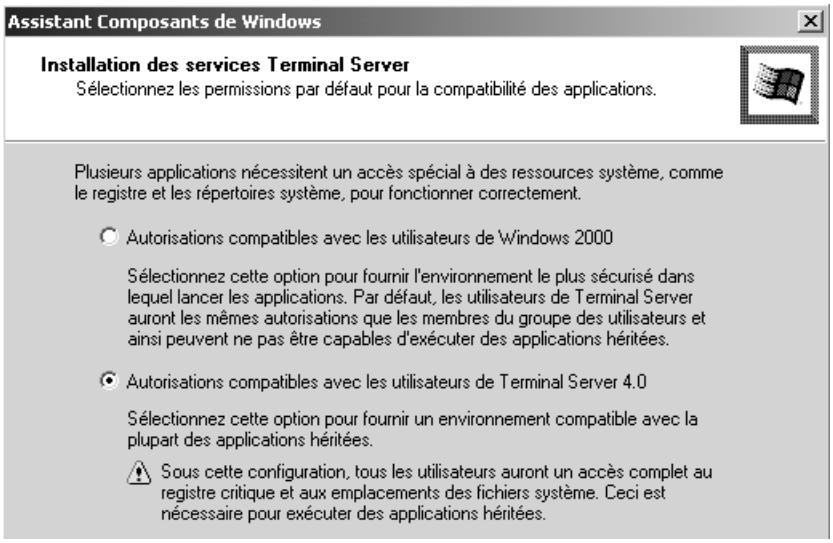
- **Services Terminal Server**
- **Gestionnaire de licences des services Terminal Server**

Deux modes de fonctionnement sont proposés.



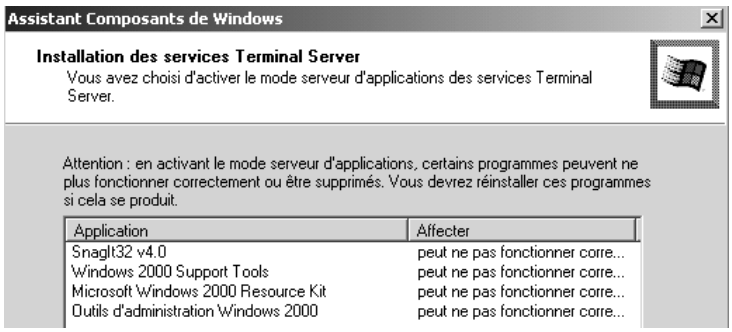
Le Mode **Serveur d'application** incorpore le Mode **Administration à distance**…

Choisissez **Serveur d'applications**, qui permettra d'installer les services de clients légers . Ensuite on demande de confirmer l'option de sécurité



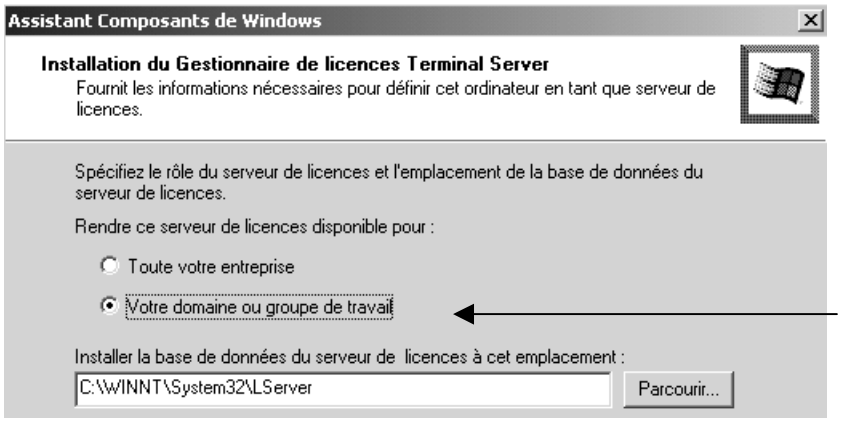
Et on nous informe que certains programmes risquent de poser problème : ce sont tous les programmes déjà installés sur ce serveur !

De manière générale, sur un serveur avec Terminal Server installé, **il faut ensuite lorsque l'on installe un nouveau logiciel que l'on veut mettre à disposition via termina server, passer par panneau de configuration ajouter / supprimer un programme**.



N.B : Si on installe un programme « directement » sur le serveur (avec sa procédure propriétaire), celui ne sera probablement pas appelable via Terminal Server

Ensuite on demande de confirmer l'option de sécurité



On donne le domaine

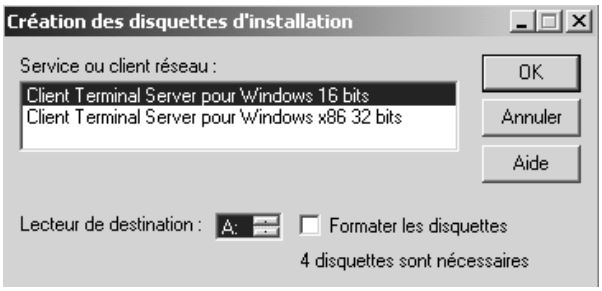
Après redémarrage du serveur 4 nouvelles mmc sont disponibles

Installation client Terminal Server:

Deux méthodes sont possibles pour installer un client TS

- A partir de disquettes :

Ces disquettes doivent être générées sur le serveur Terminal Server via la mmc **Créateur de client Terminal Server**

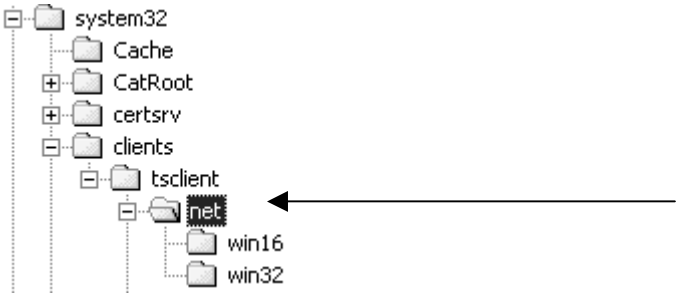


2 disquettes sont nécessaires pour les clients32 (win95 nt 2000)

4 disquettes sont nécessaires pour les clients16 (win3.11)

- A partir du serveur

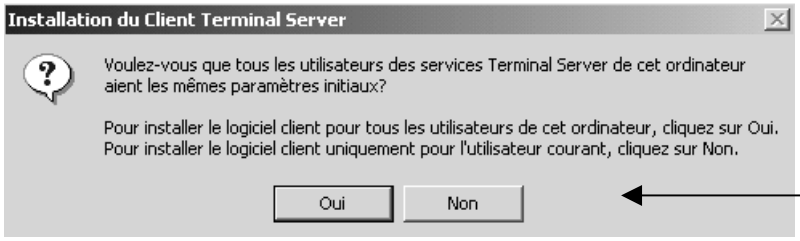
Un copie de ces disquette s trouver sur e serveur Terminal Server dans un sous dossier u dossier système **clients\tsclient\net**



Il faut partager le dossier **net** sous un nom clair pour tout le monde en lecture seule…

l'installation se lance via un fichier **setup.exe**

Il faut s'identifier avec un compte autorisé à faire une installation, et préciser si on veut le client TS pour tous les utilisateur de ce poste, ou uniquement pour le compte dont on vient de donner les références…



Oui On installe le client pour tous les utilisateurs…

Connexion du client sur le serveur Terminal Server:

Après installation du client, on trouve dans **Démarrer / Programmes**

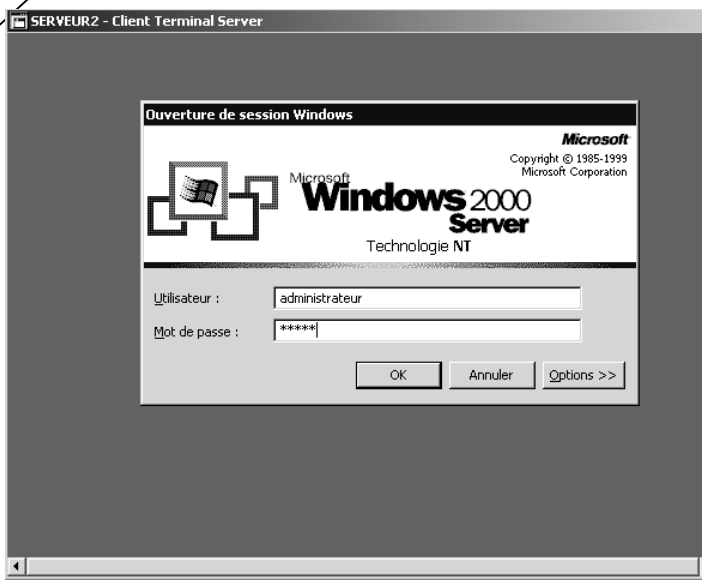
Lorsque l'on demande **Client Terminal Server** on obtient

On choisit notre serveur

Ici **Serveur2**

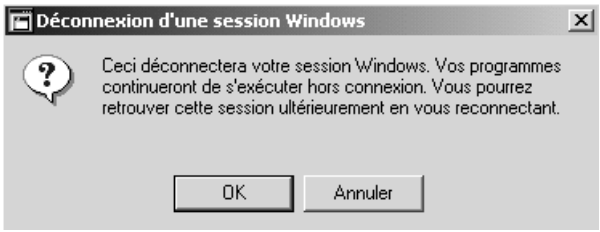
Puis **Connecter**

Dans la fenêtre Terminal qui apparaît il faut s'identifier…



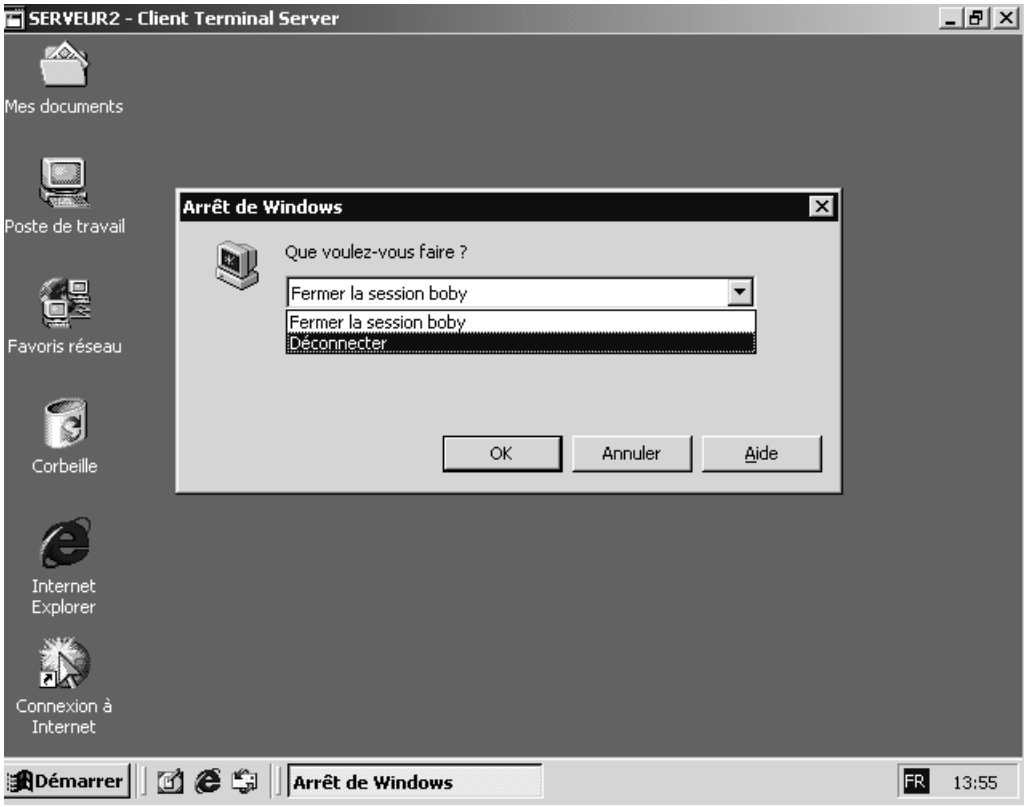
Fin de session - Deconnexion:

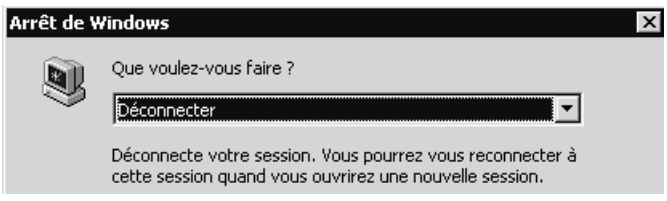
Pour arrêter une session **terminal server**, si on ne ferme que la fenêtre Terminal server, on se déconnecte, mais les applications restent ouvertes sur le serveur …

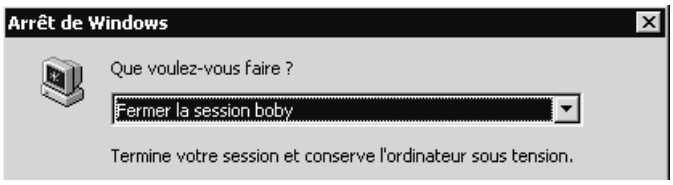


Il faut pour fermer les applications, bien demander à travers la session terminal server :

démarrer arreter fermer la session, et non pas déconnecter !







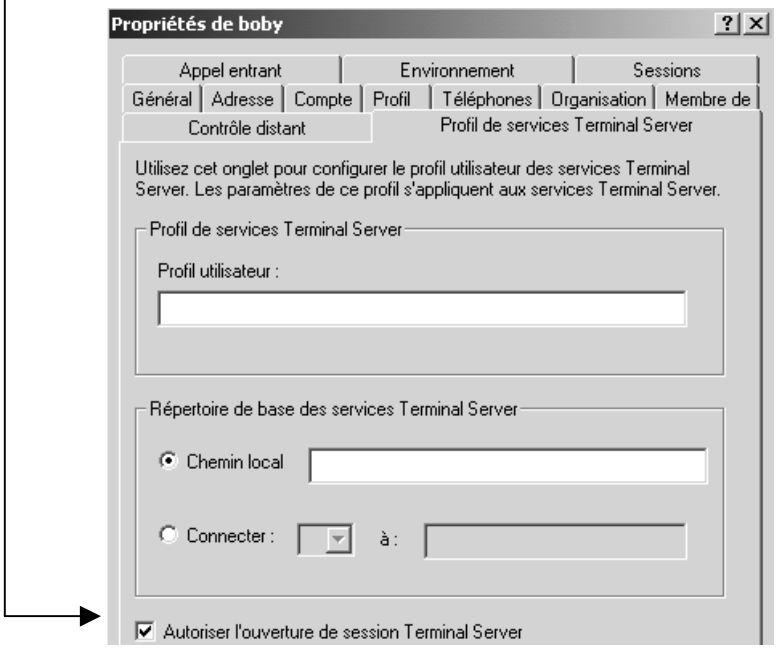
Toutes le applications tournent Toujours sur le serveur

les applications sont fermées

Autorisation de compte sur le serveur Terminal Server:

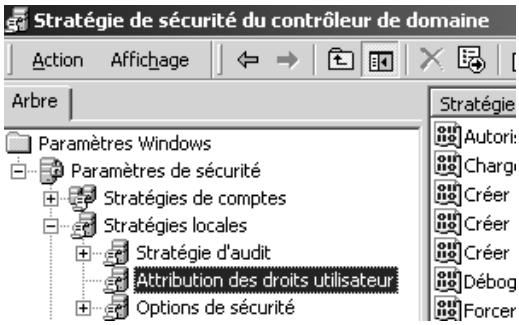
Le seul compte pour l'instant à pouvoir ouvrir une session à travers Terminal server c'est le compte Administrateur

En effet tous les autres comptes de domaine **sont autorisés par défaut** dans Terminal server, On peut le vérifier dans les propriété des comptes, dans l'onglet **Profil de services Terminal Server**



mais **ne sont pas autorisés par défaut** à ouvrir de session sur le serveur CD !. D'ailleurs si on essaye d'ouvrir une session terminal server depuis un client avec un compte utilisateur, le message parle de stratégies, et non pas d'autorisation de Terminal server…

ceci peut dépendre du fait que **terminal server** est ici installé sur le **CD. Dans ce cas il faut autoriser le compte à ouvrir une session locale, dans les Stratégies de sécurité du contrôleur de domaine !**



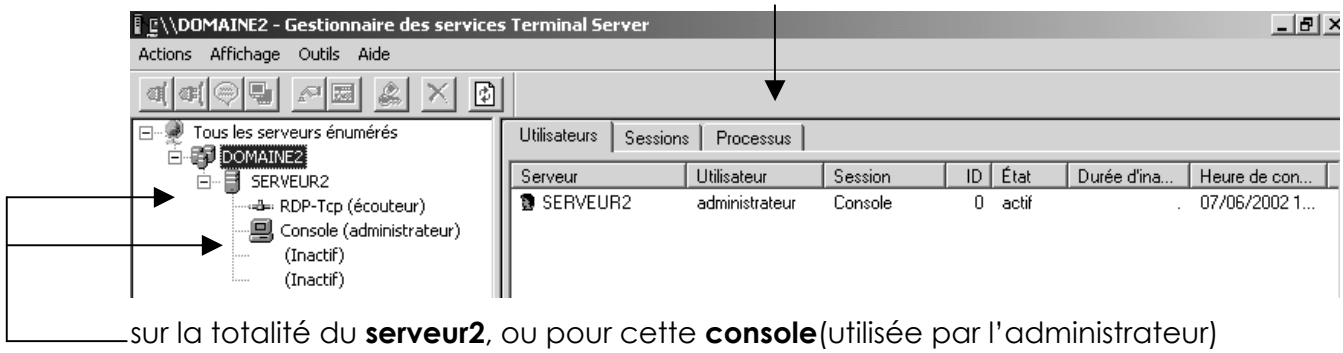
N.B : il est déconseillé d'installer Terminal Server sur le CD !

Vérification des session en cours:

Si on veut savoir actuellement quelles sont les sessions en cours via Terminal Server, on peut sur le serveur ou TS est installé lancer la mmc **Gestionnaire de services Terminal Server**

Cette console visualise tous les clients TS

Trois types d'information sont disponibles : **Utilisateur – Sessions - Processus**

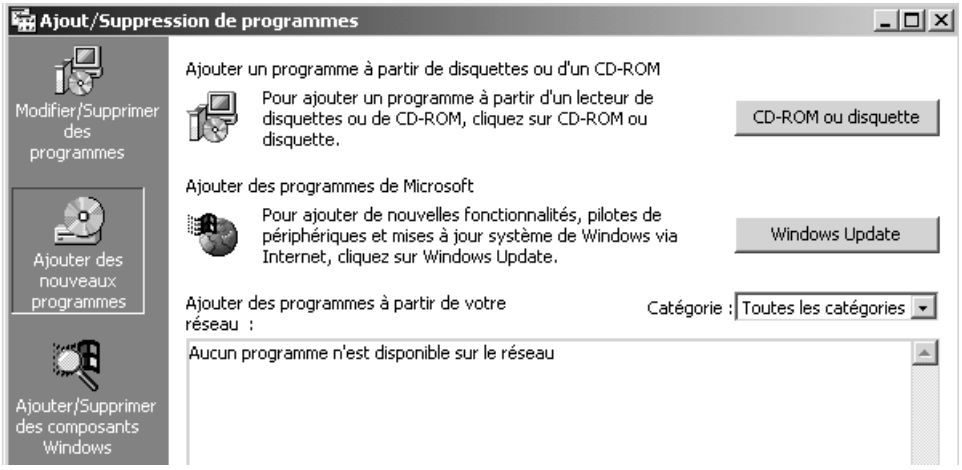


sur la totalité du **serveur2**, ou pour cette **console**(utilisée par l'administrateur)

Installer une application dans Terminal Server:

Si on veut installer une application, et faire qu'elle soit disponible dans **Terminal server**, deux méthode existent

Normalement il faut passer par



Dans le cas ou cette méthode échoue, il faut lancer alors la commande en ligne **change user**

```
C:\Documents and Settings\Administrateur>change user /?
Mode Modification de l'installation.

CHANGE USER {/EXECUTE | /INSTALL | /QUERY}

  /EXECUTE  Active le mode exécution (mode par défaut).
  /INSTALL  Active le mode installation.
  /QUERY    Affiche les paramètres actuels.
```

il faut :

1. taper change user /install
2. installer l'apllication localement
3. taper change user /execute

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…

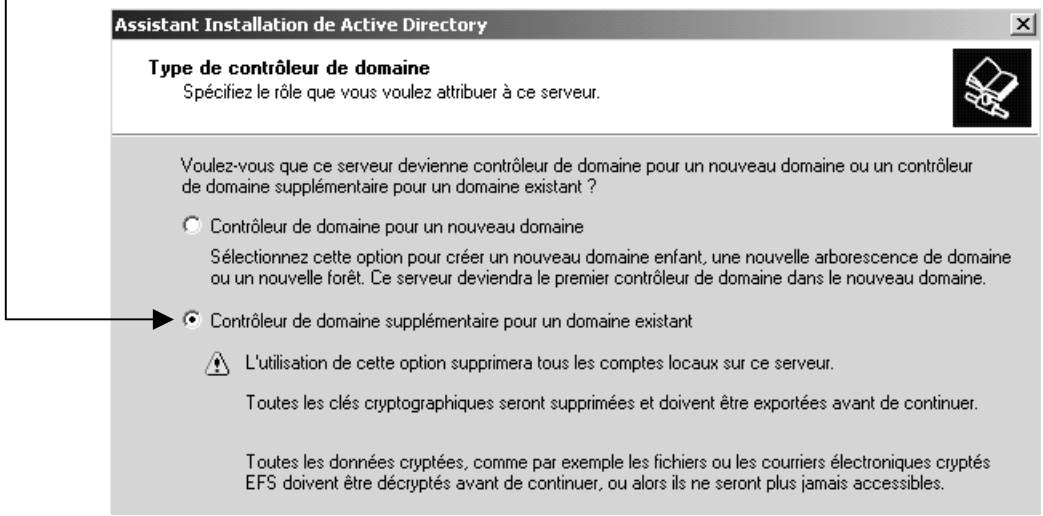
Lorsque l'on va exécuter **DCPROMO**, on va convertir l'ordinateur en Contrôleur de Domaine, et l'on va y dupliquer Active Directory

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….

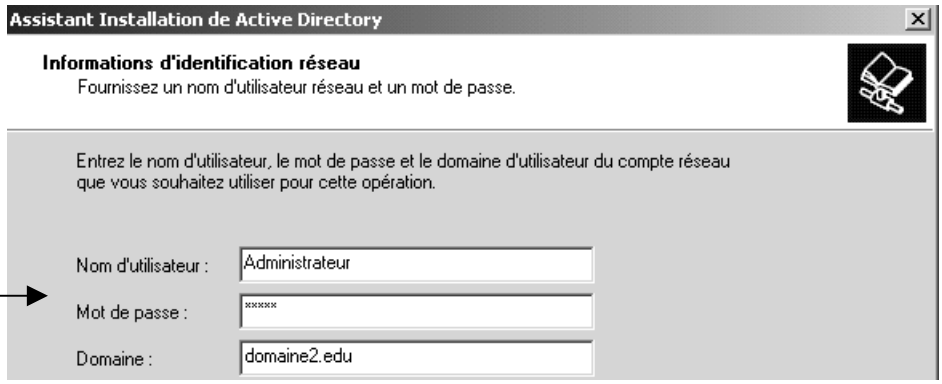
N.B: si on veut mettre toutes les chances, soyons progressif, rentrons le serveur autonome sur le domaine, puis executons un **dcpromo**…

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

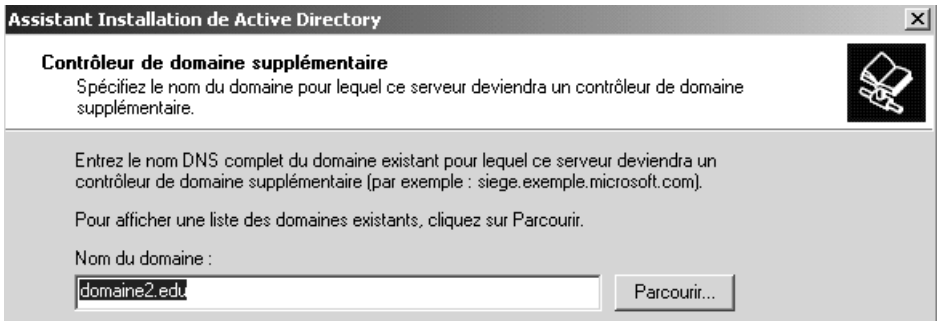


et pour pouvoir faire cela il faut s'identifier…

Identification sur le domaine…

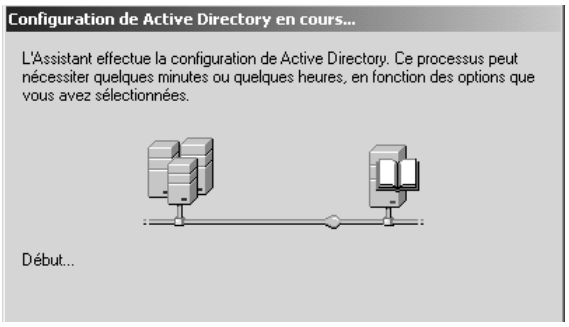


et spécifier a quel Domaine notre contrôleur de domaine veut participer



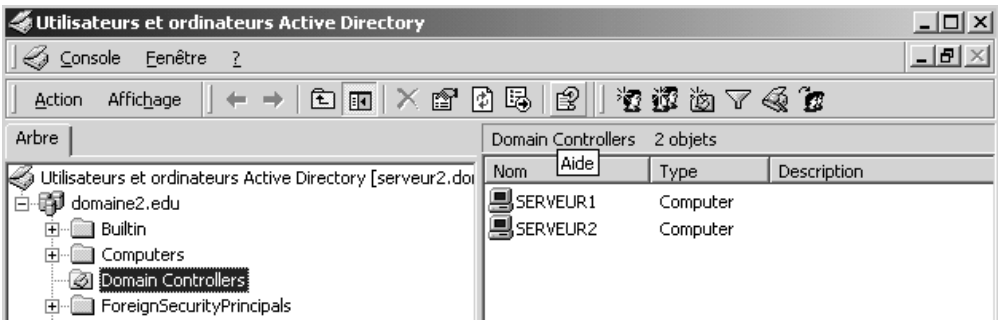
Le reste de l'assistant est identique à celui qui se déroule lors d'un DCPROMO de création de domaine…

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 Controlers**…



AJOUTER UN 2° SERVEUR 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…

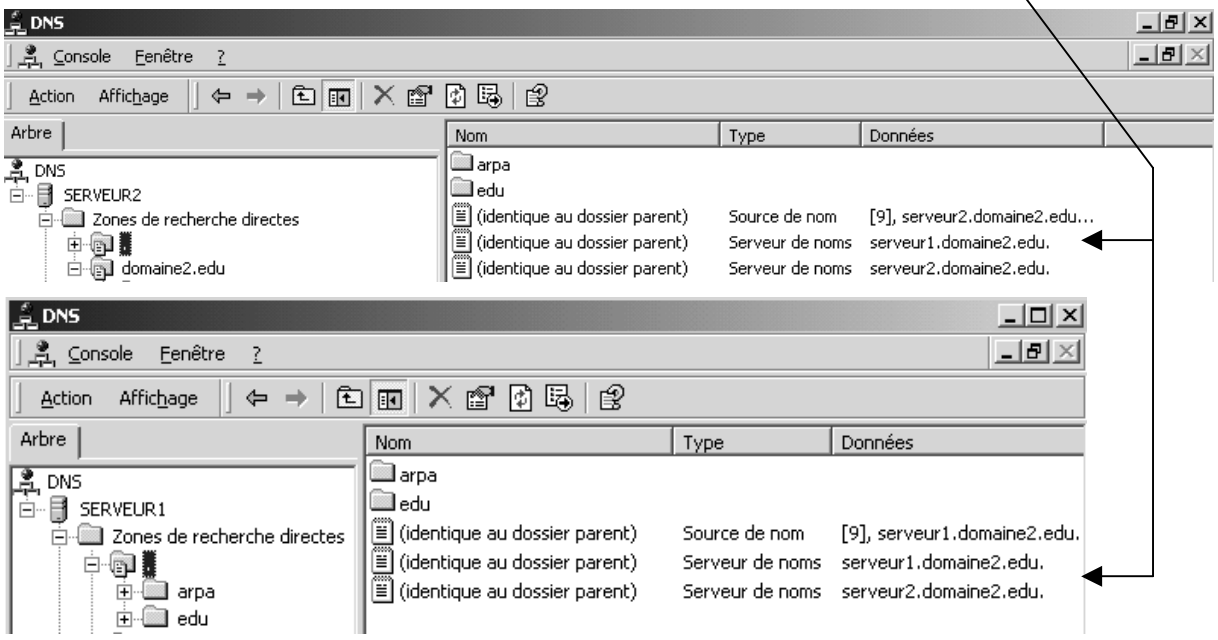
Il faut donc **installer un serveur DNS** sur notre 2° C.D.

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

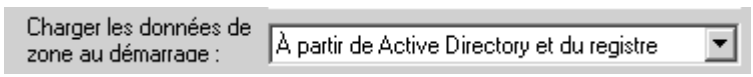
On installe classiquement notre serveur DNS sur notre 2° serveur C.D. (Ajout/Supression de services de mise en réseau, système de nom de domaine…)

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



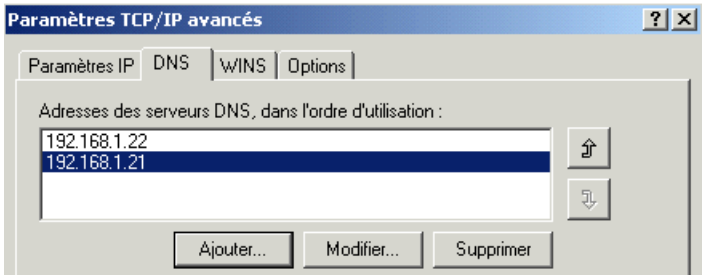
on peut aussi demander a un serveur DNS de recharger sa zone…

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

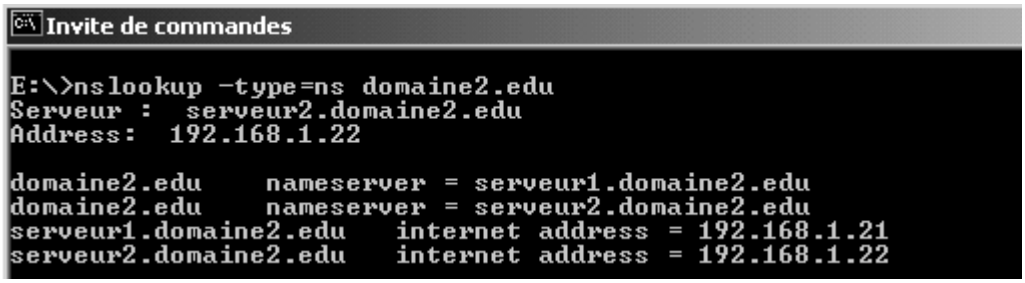


Liste de tous les serveurs DNS disponibles sur le domaine :

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)



AJOUTER UN 2° SERVEUR 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 …**

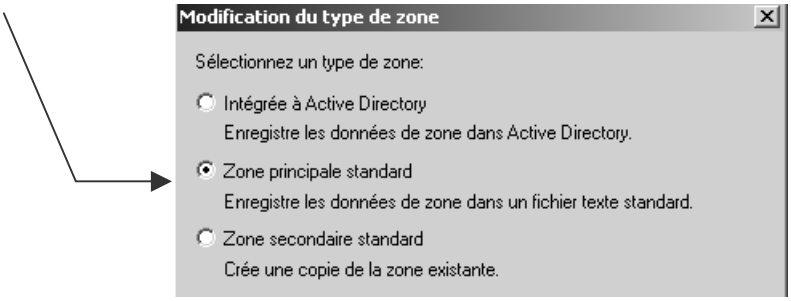
On installe classiquement notre serveur DNS sur notre 2° serveur C.D. (Ajout/Suppression de services de mise en réseau, système de nom de domaine…)

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…

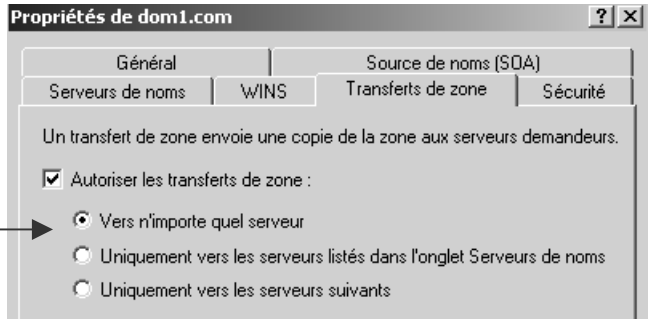
- Sur le CD "principal", il faut vérifier que le type de zone soit bien "**zone principale standard**…



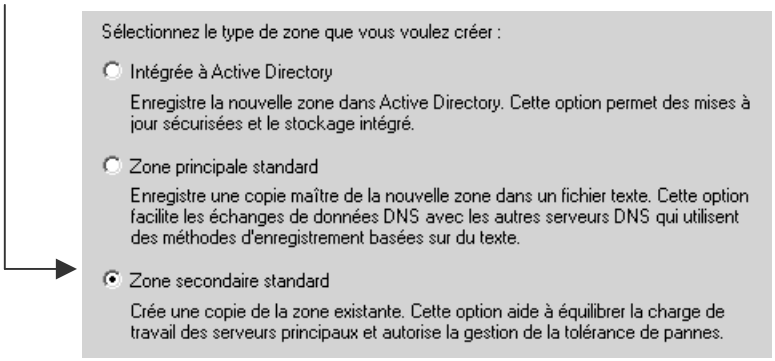
valider la manipulation avec **ipconfig /flushdns** puis **ipconfig /registerdns**, voire un vidage du cache ou un restart….

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

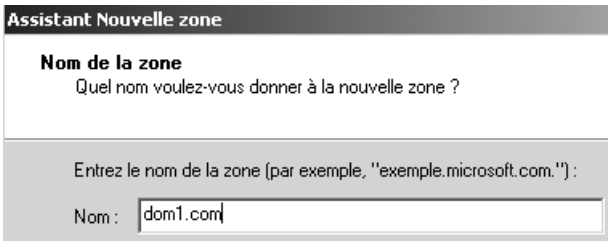
Dans un 1° temps autoriser les transferts vers tous les serveurs



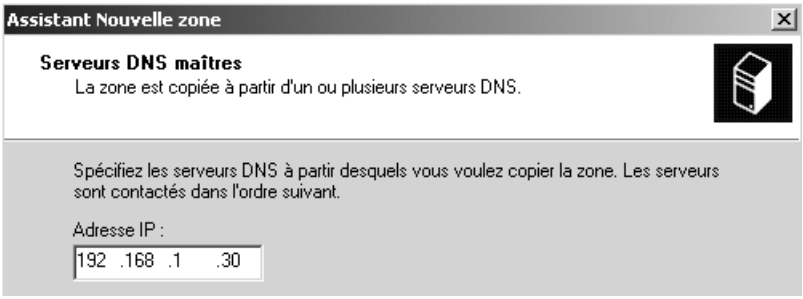
- Sur l'autre CD "backup", il faut créer une zone de type **Zone secondaire standard**. Cela se fait via l'assistant création de zone



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…

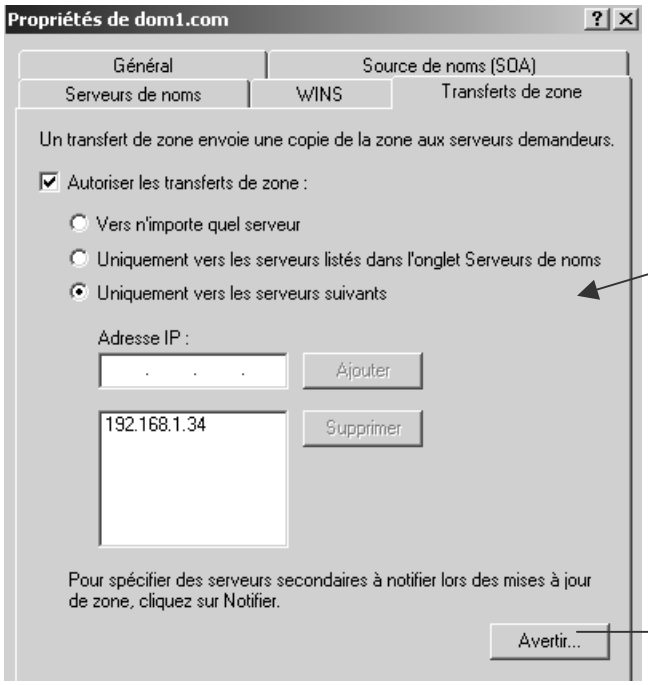


L'assistant terminé, on devrait voir remonter une copie de la zone….

Affinage de la duplication :

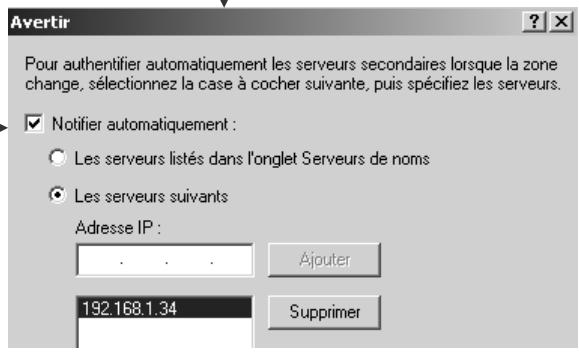
une fois les réplications de base vérifiées, on peut optimiser et sécuriser un peut…

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.**

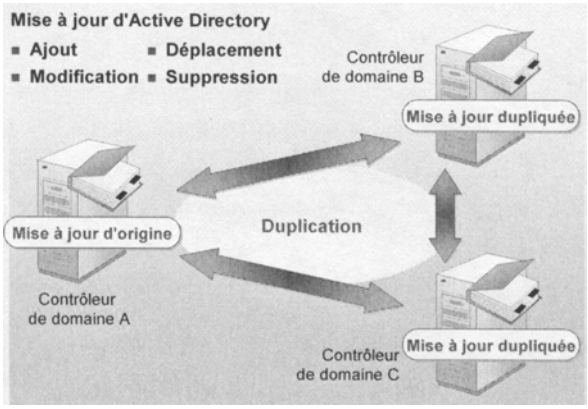
La **duplication** des informations stockées dans les AD de chaque contrôleur de Domaine, prends alors le nom de **Duplication intrasite**

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:

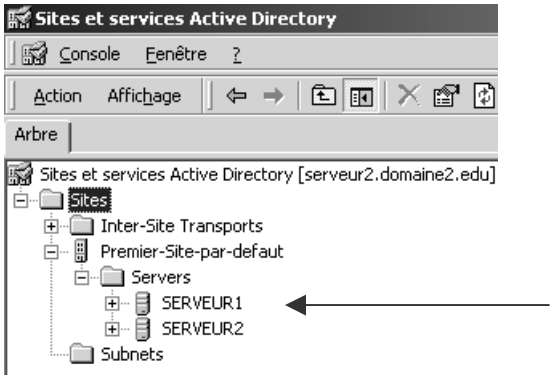
Le principe de mise à jour des modifications entre les copies des AD étant dit de «**duplication multi-maître** », 2 CD peuvent effectuer une demande de duplication au même moment, avec des AD ayant des objets différents…

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 la mmc **sites et services Active Directory**, sur le serveur dont on souhaite activer la réplication,



On demande le menu contextuel

Répliquer maintenant

DUPLICATION AD INTER-SITE

Utilité d'un Site :

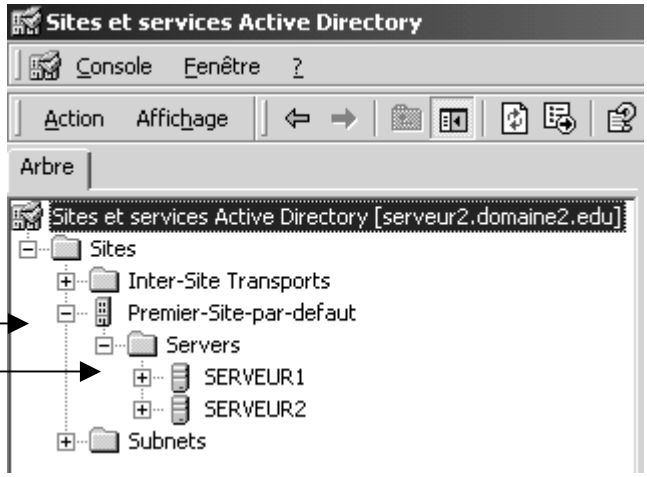
Si on ne spécifie rien lors de l'installation des DC, par défaut on se retrouve systématiquement dans un site par défaut, nommé **Premier-Site-par-défaut**, et contenant tous mes serveurs CD.

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. En effet entre deux sites on pourra 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.

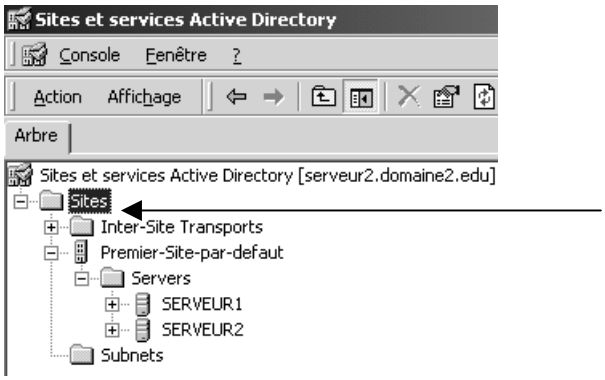
Un site est défini par une plage d'adresses TCP-IP suivant les règles .

- 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.

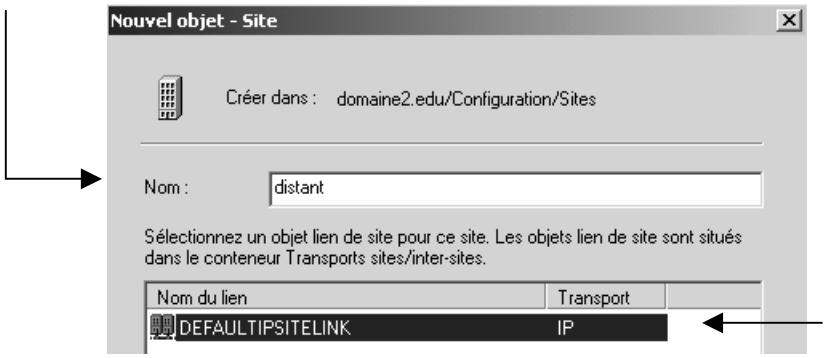
Pour créer un nouveau site, il faut se mettre sur le dossier **Sites**



Et demander clic droit

Nouveau site

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



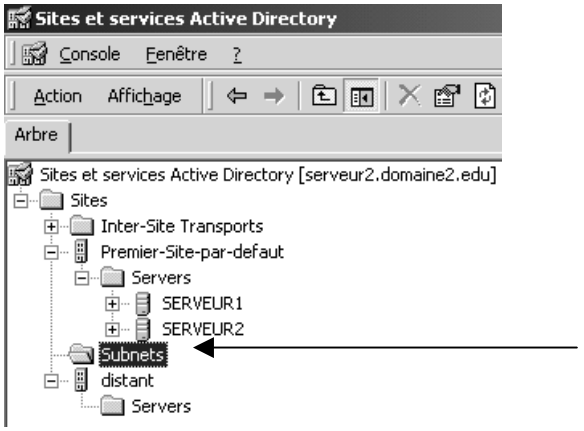
Et sélectionner le lien par défaut

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 :

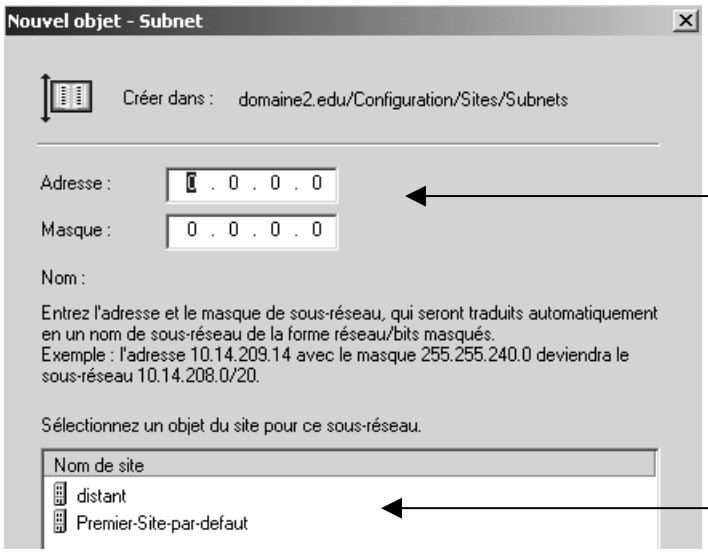
Pour créer un sous-réseau, il faut se mettre sur le dossier **Subnets**



Et demander clic droit

Nouveau Subnet

on obtient



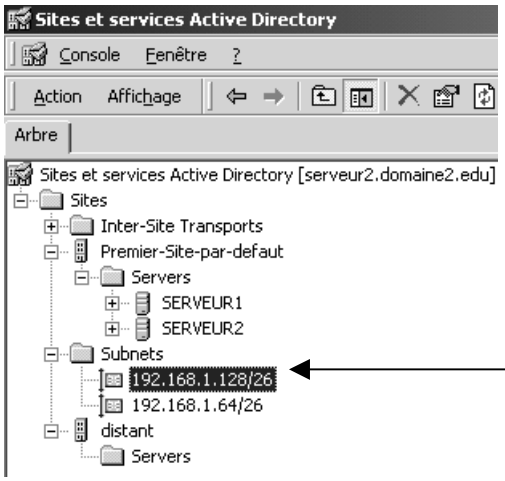
Il faut rentrer là les adresses et les masques de sous-réseau correspondant aux sites que l'on doit gérer…

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:

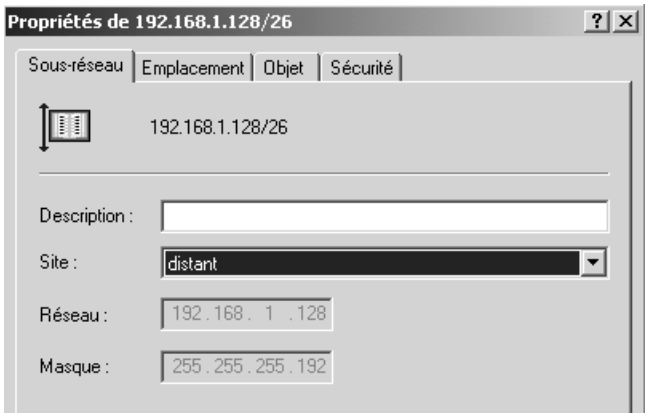
Pour associer une plage d'adresse à une notion de site, , il faut se mettre sur chaque sous réseau à associer, et demander **Propriétés**



Et demander clic droit

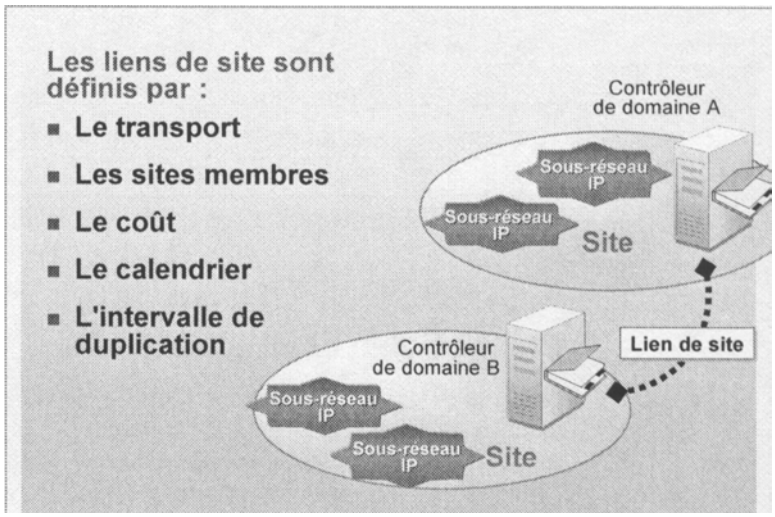
Propriétés

Vérifier que ce sous réseau soit bien associé à un site



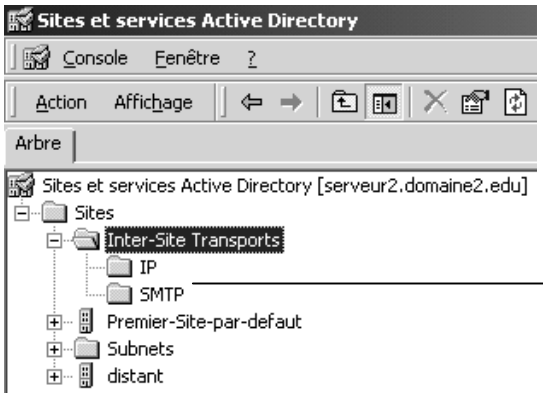
Création des liens de site:

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 :

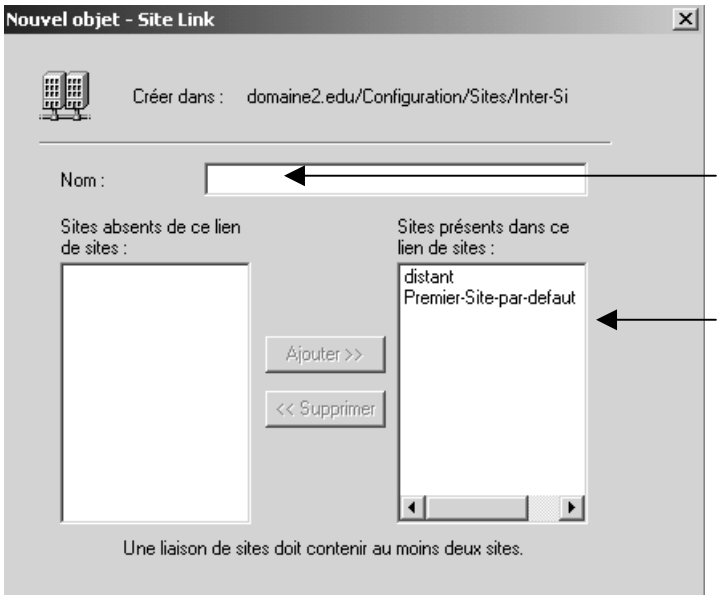
- **IP (RPC)** protocole **Remote Procedure Call** par défaut
- **SMTP** protocole **Simple MAIL Transfer Protocol** moins utilisé en l'espèce.

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

Et demander clic droit

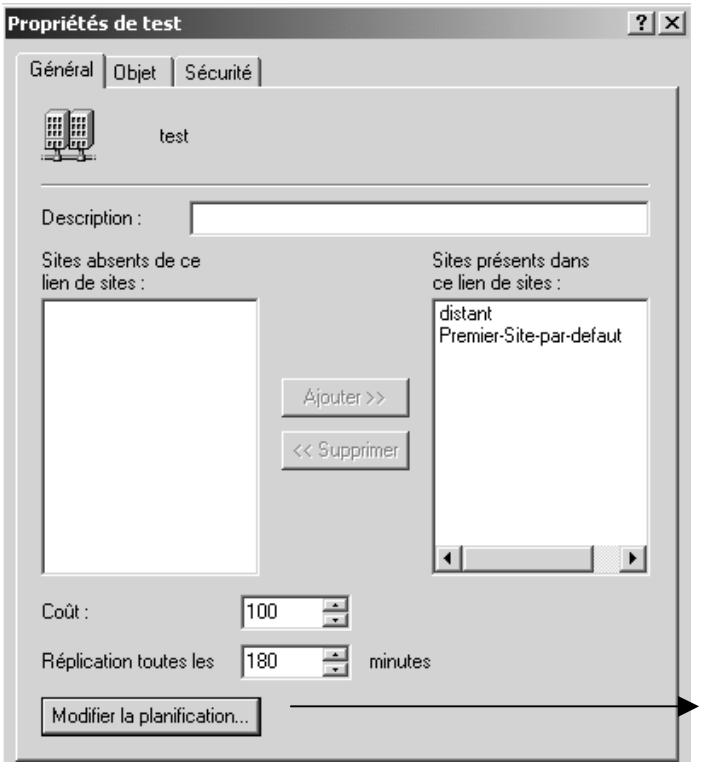
Lien vers un nouveau site

On va créer un nouvel objet Lien

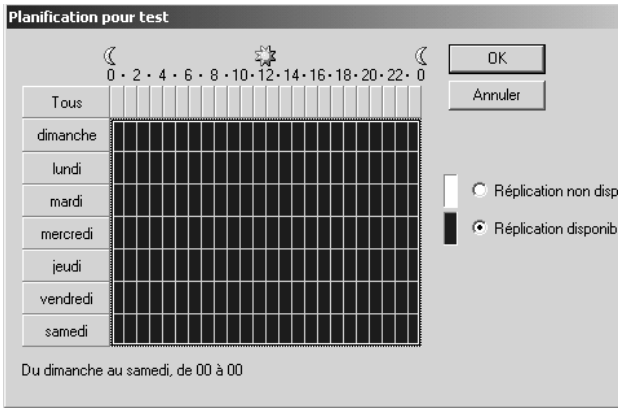


Que l'on doit nommer

Et dans lequel if faut inclure au moins 2 sites

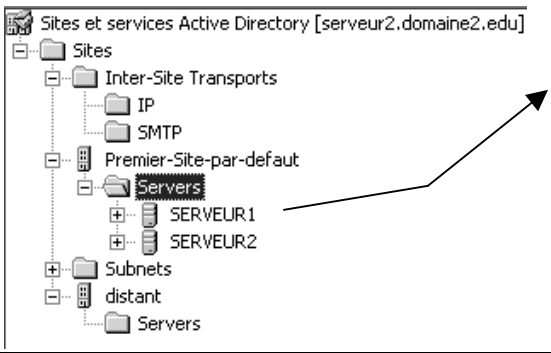


et pour lequel ensuite les propriétés vont permettre de configurer un certains nombre de choses…

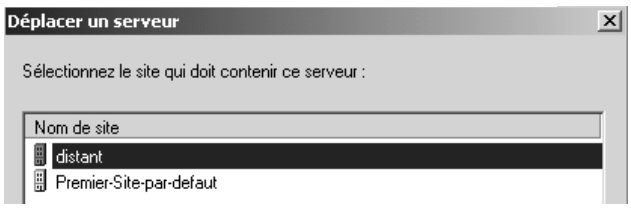


Mettre un **CD** dans chaque site:

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**

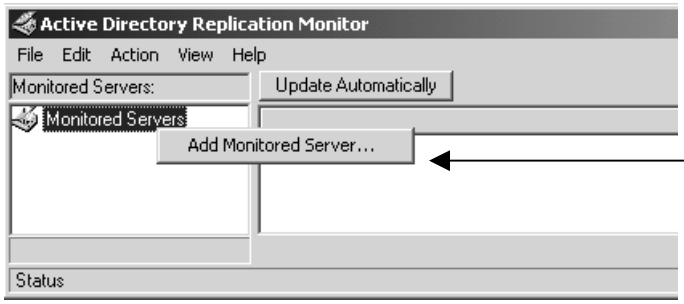


Visualiser le schéma de la duplication :

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**

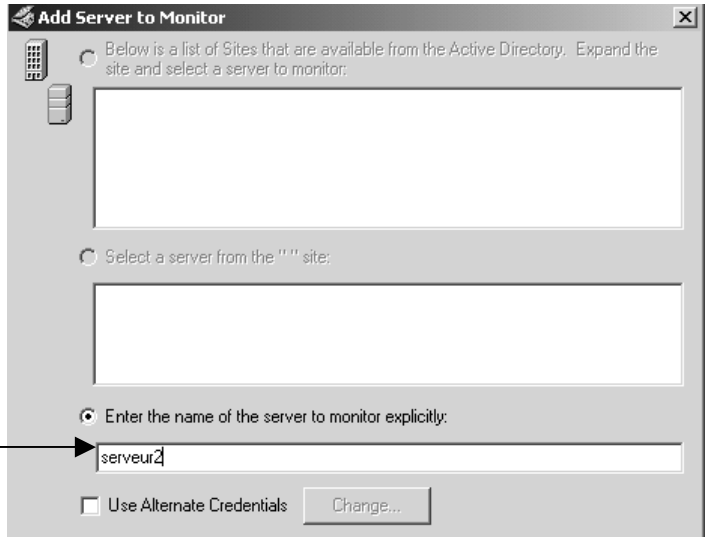


On demande un clic droit sur **monitored served** et on demande d'ajouter notre serveur…

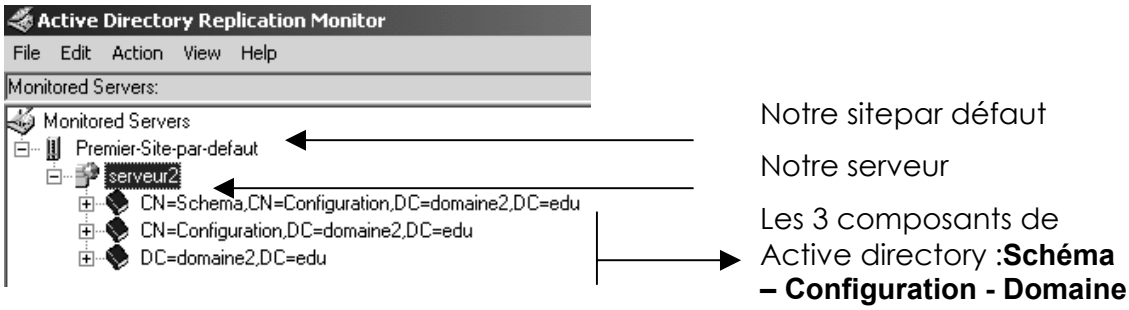
on obtient alors

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

et on y ajoute notre machine



on à alors une vision de la réplication de AD :

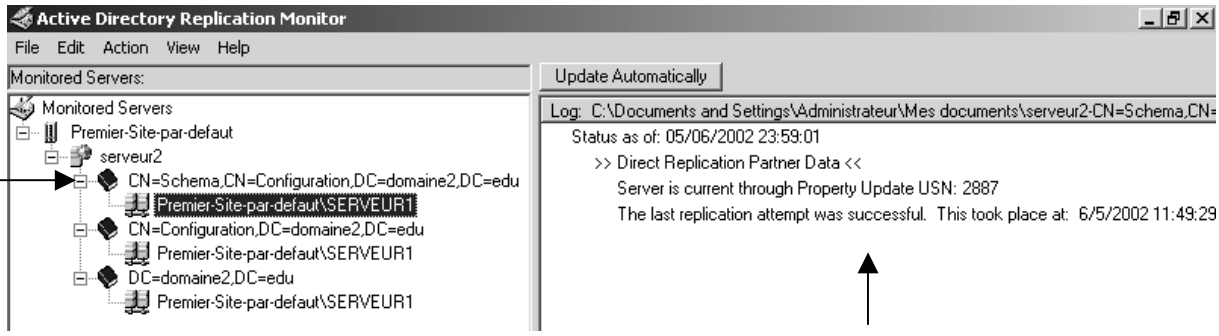


Le schéma : définition des règles de construction de AD, c'est la structure de AD, qui est unique dans tout le domaine, la forêt (éventuellement répliquée entre tous les DC de la forêt). *Unique !*

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,



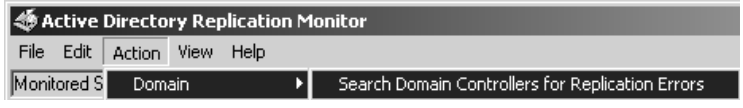
on à l'information "en clair"

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

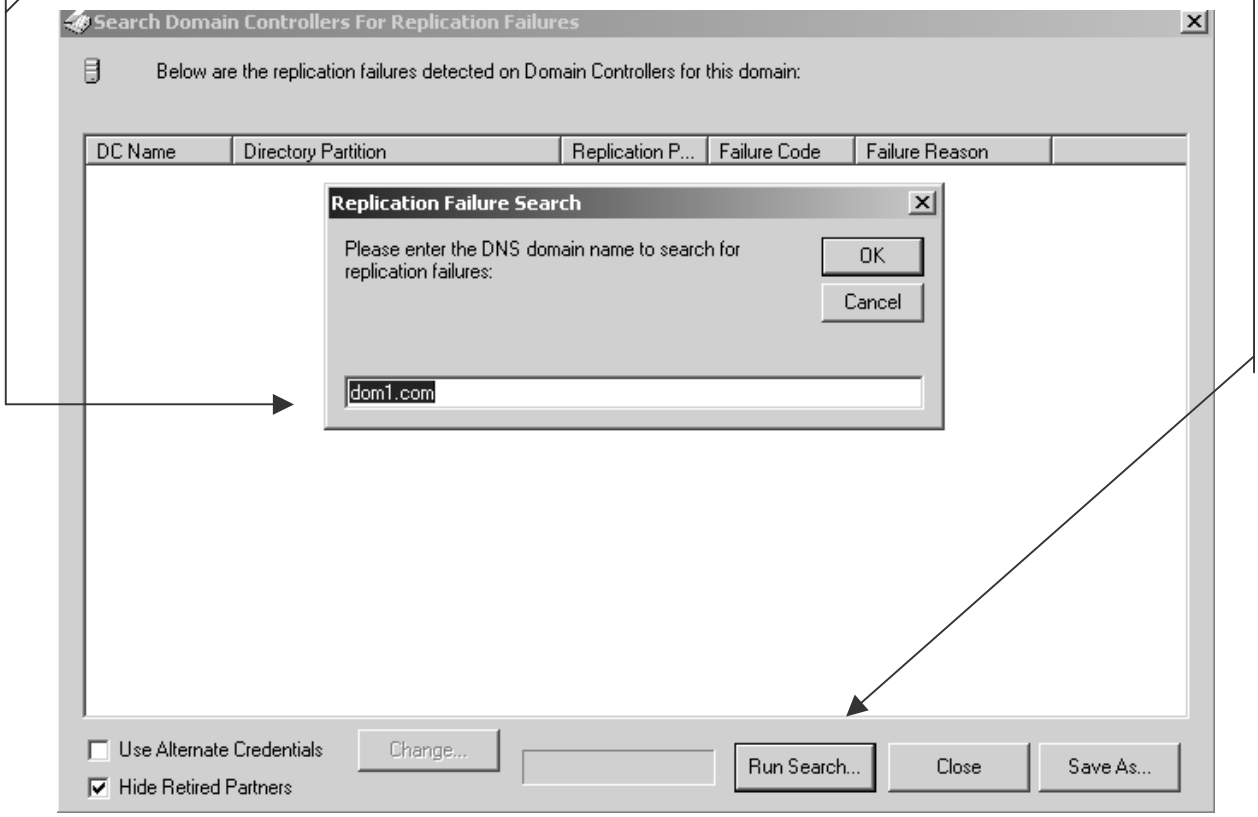
Vérification Recréer le schéma de la duplication :

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**

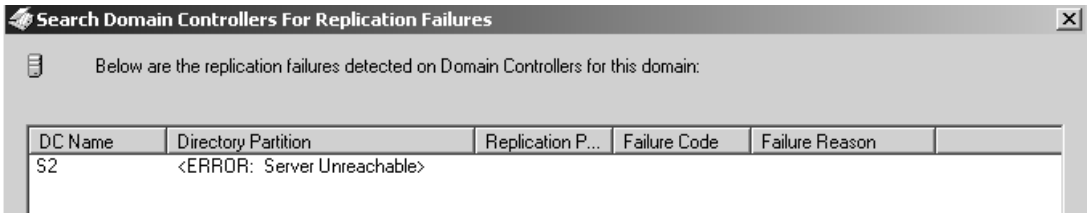
On installe ces outils avec les options par défaut…puis et on ajoute les serveurs dans notre visualisation. Puis on demande



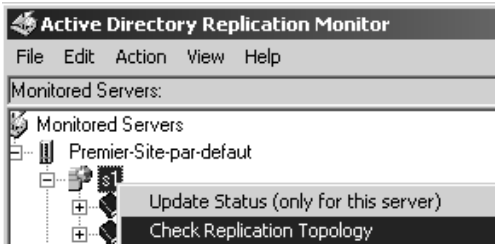
Dans la boite de dialogue, on demande alors **Run Search** et on indique le **domaine** pour lequel on veut effectuer la réplication…



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 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

1 & 2 sont **uniques pour la forêt**

3. Emulateur CPD (NT 4.0)
4. Maître identificateur Relatif RID
5. Maître d'infrastructure

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)

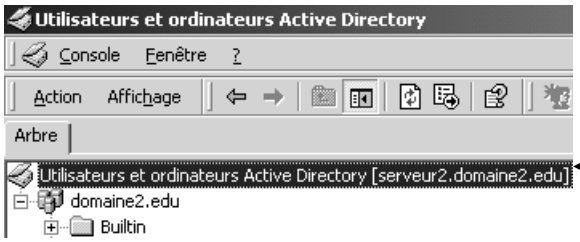
Met à jours les références d'objets d'un domaine aux autres domaines.

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 :

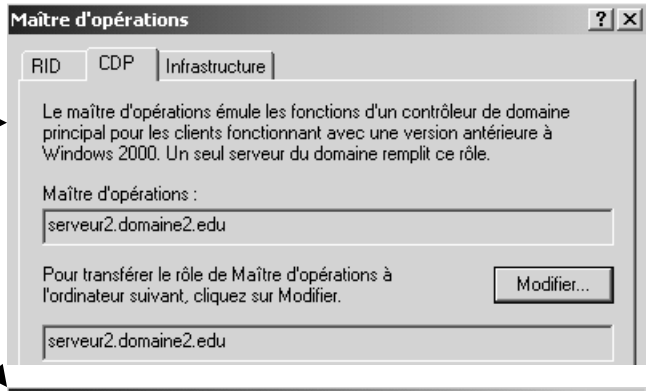


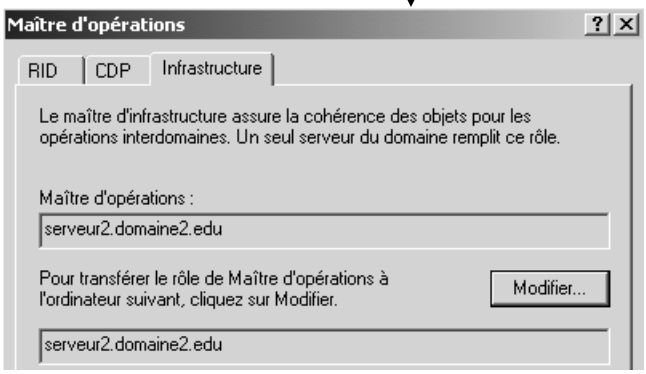
En se plaçant sur **Utilisateur et ordinateurs Active Directory** on demande clic droit **Maîtres d'opérations…**

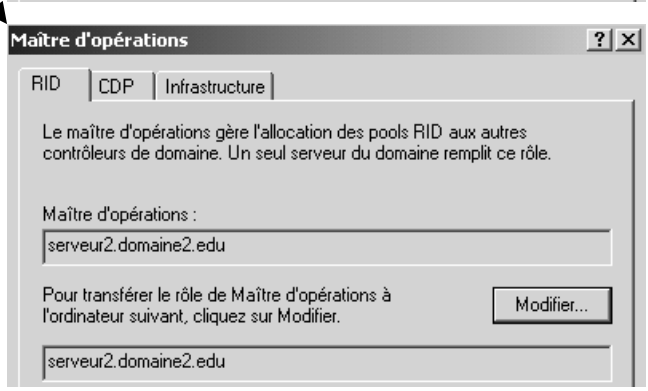
pour obtenir un boîte à 3 onglets

Les 3 rôles de domaine

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

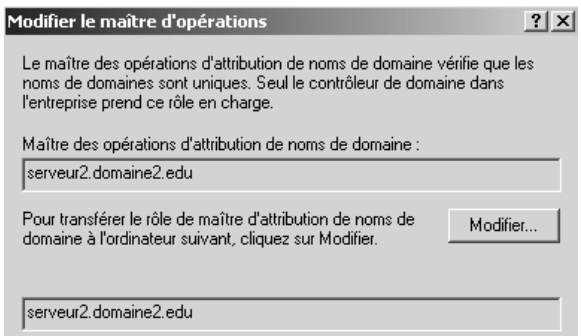






Avec la console **Domaine et approbation Active Directory** on peut trouver qui est maître d'attribution de Domaine

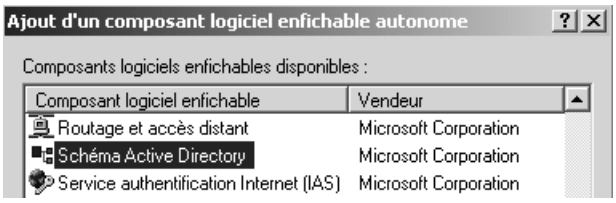
En se plaçant sur **Domaines et approbations Active Directory** on demande clic droit **Maîtres d'opérations…**



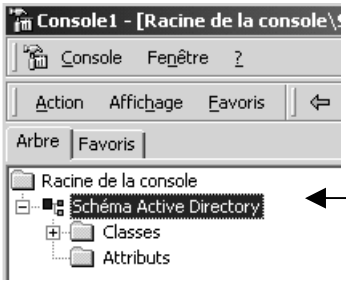
Pour localiser le maître de schéma, c'est le plus difficile. Il d'abords créer l'exécutable qui pourra ouvrir la console mmc

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 **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 même 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

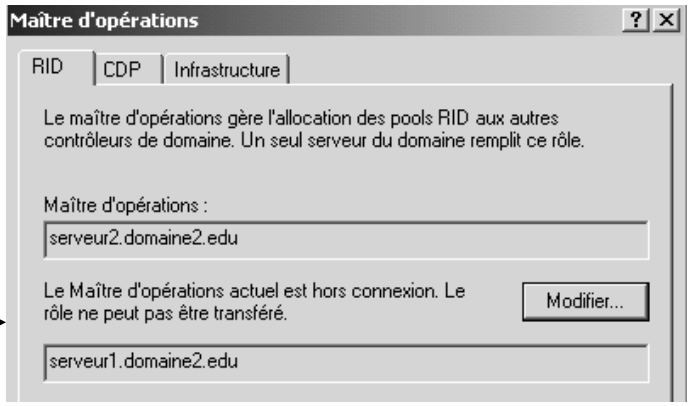
N.B : Si on est sur le serveur maître d'opération, il faut alors d' abords se connecter sur le serveur sur lequel on veut effectuer le transfert

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….

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
- 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....
- 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 même 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

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 outils est de localiser plus rapidement tous les objets d'une foret.

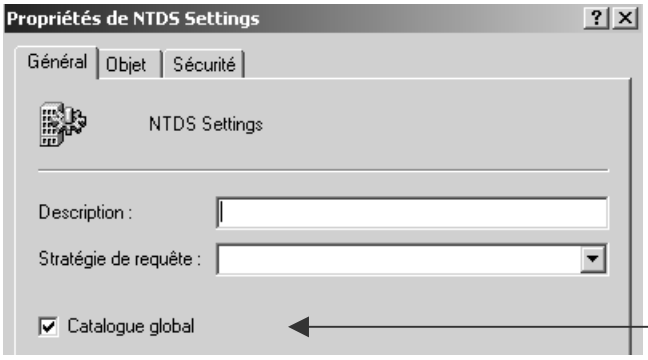
Il sert aussi sur des domaines en mode natif pour vérifier l'appartenance aux groupes universels. Si d'ailleurs il n'est pas disponible les utilisateurs non administrateur ne peuvent plus ouvrir de session. (plus avec Windows 2003)

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? :

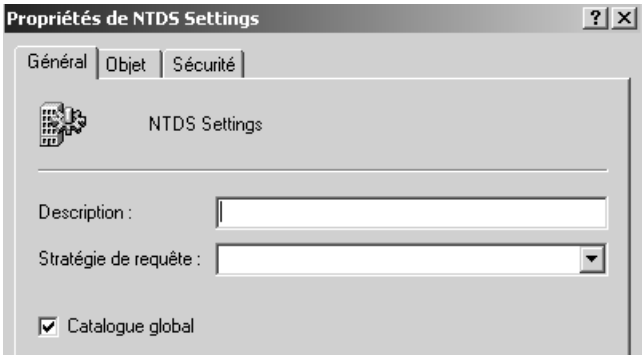
- Si plusieurs domaines existent dans la forêt, les serveur ayant le rôle de Maitres d'infrastructure ne doivent pas être serveur de GC. Car il travaillent sur les mêmes types d'objets. Si cette règle n'est pas observée, le transfert d'un objet entre 2 domaine risque de poser pb…
- Le maître d'attribution 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 déja 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**

de cocher 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 application devrait consigner l'opération

Pour désinstaller un serveur, on décoche la case…

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

1. on en active un 2°,
2. on attends 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

---

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 (…)

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

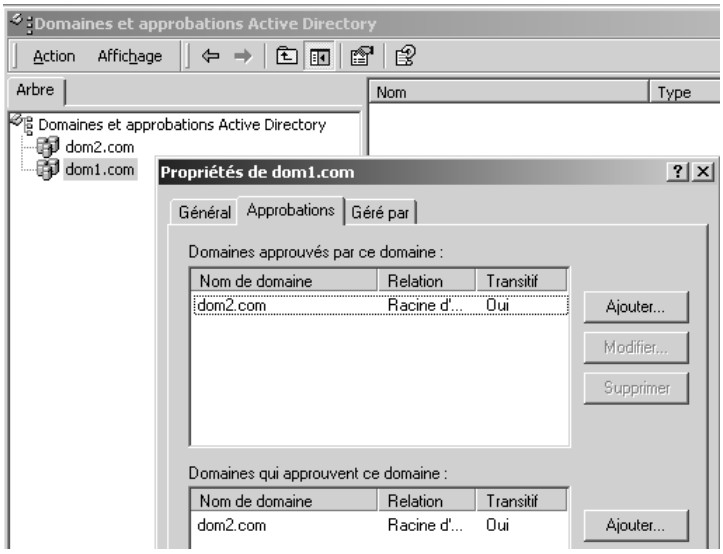
Mise en oeuvre

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

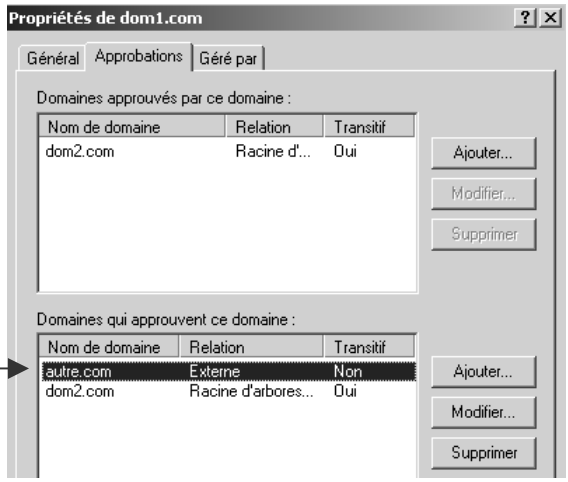
Domaines qui approuvent

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 !

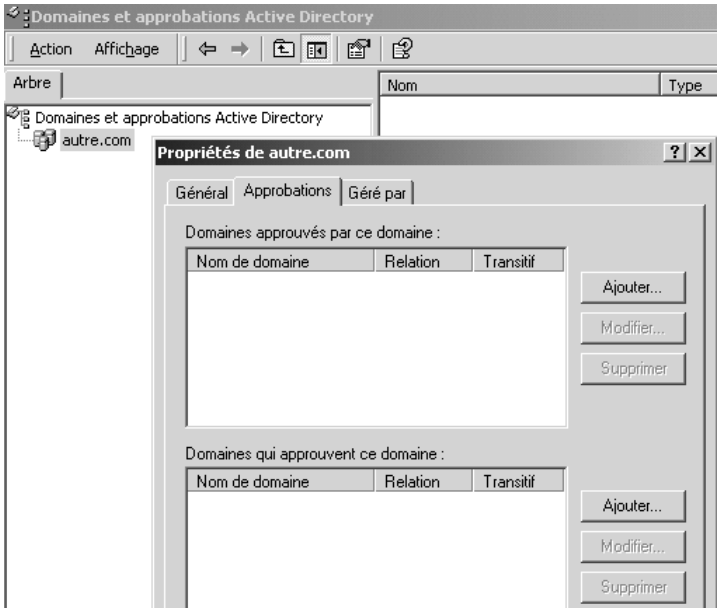
Voici donc notre nouvelle relation d'approbation avec le domaine AUTRE.COM



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)

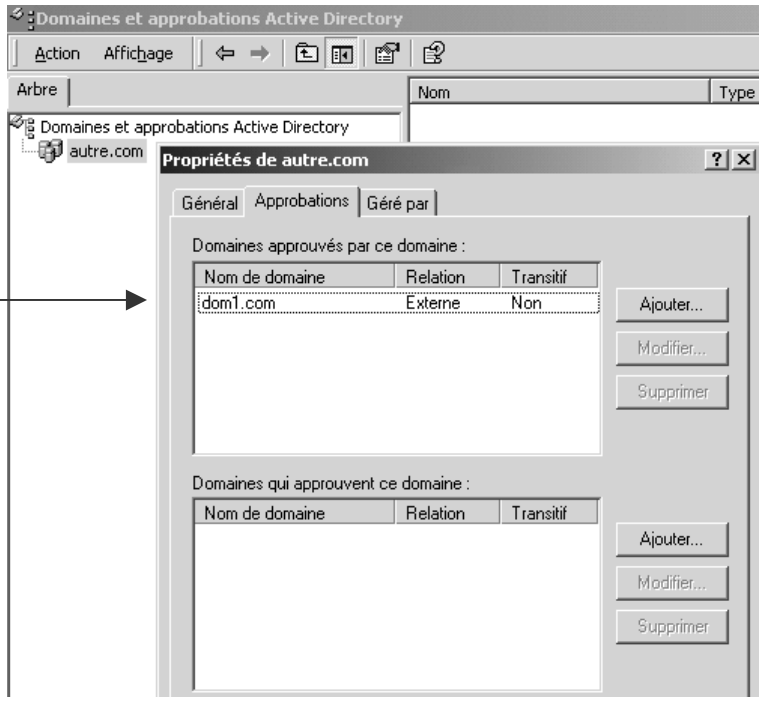
N.B: le mot de passe demandé ici est lié à la relation d'approbation uniquement

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

3. ok et on doit obtenir un message de confirmation

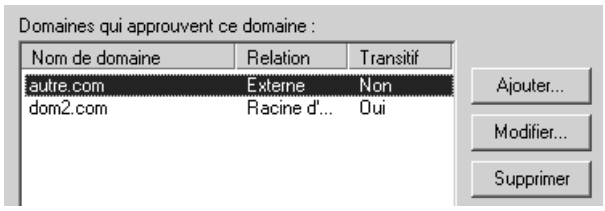
et notre relation doit apparaître ainsi :

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



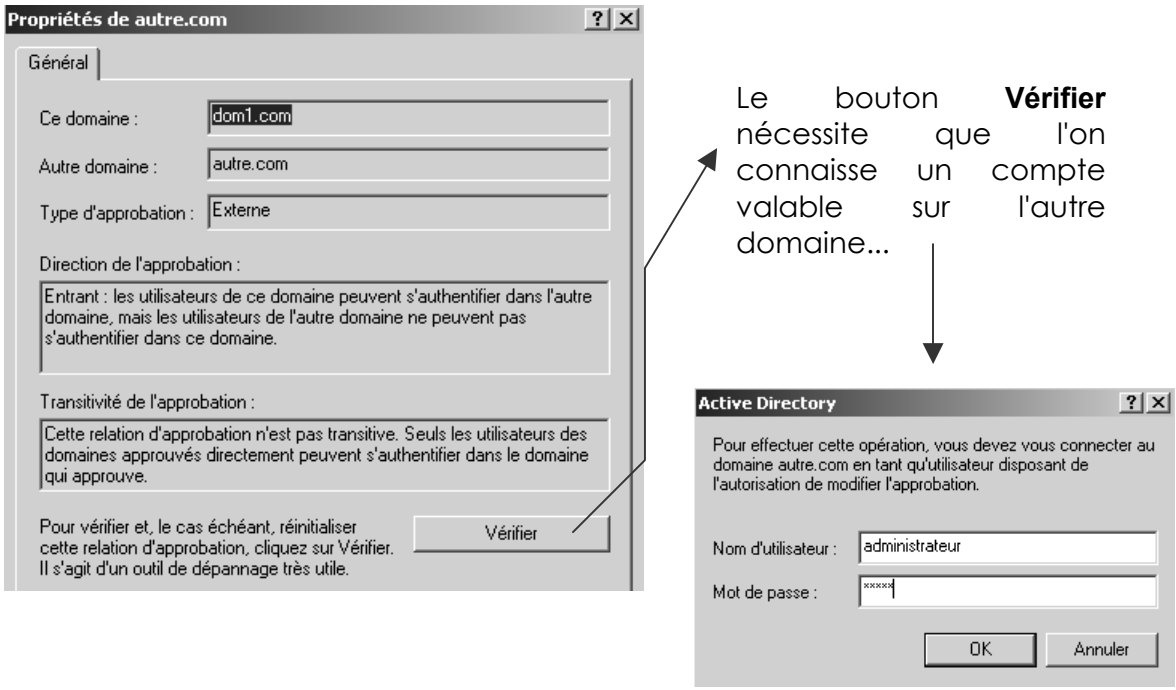
Tester la relation

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…)

ADMINISTRATION A DISTANCE

Principe de base :

Normalement, sous 2000, 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, et ce de deux manière principales :

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

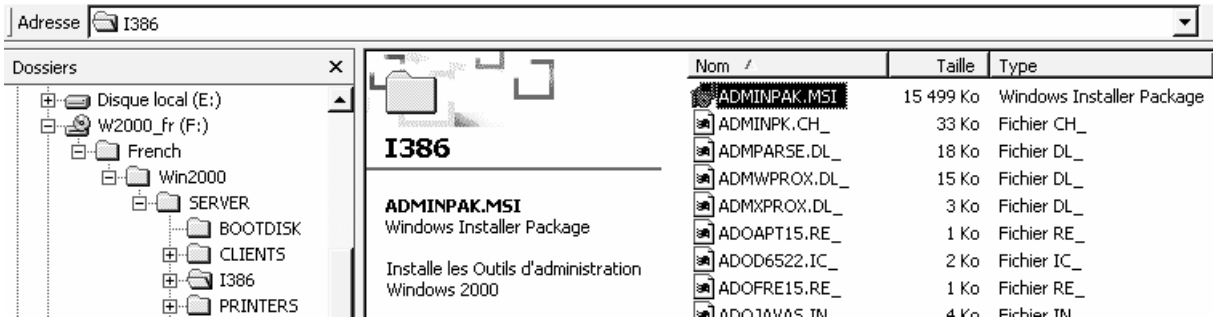
La première méthode n'offre pas la totalité de l'administration du serveur, mais elle permet de cibler les machines utilisables.

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 !

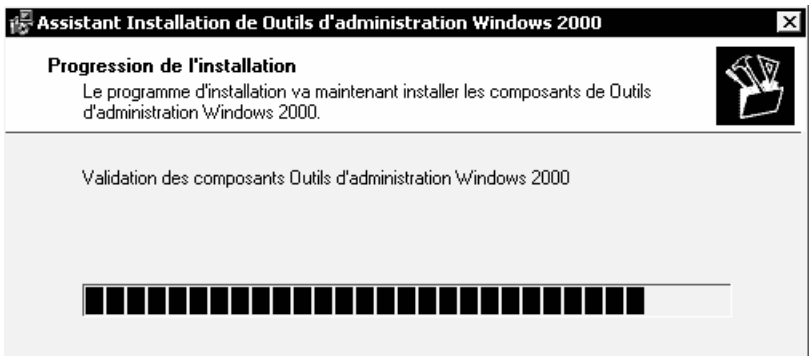
Installer les outils depuis le CD serveur 2000 :

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 :

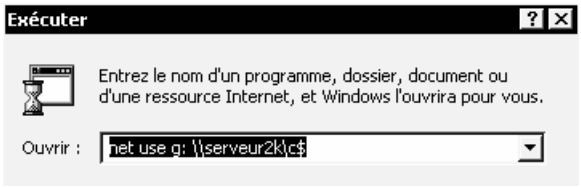
Si on n'a pas un CD 2000 server sous la main, il faut savoir que dans le dossier système du serveur c'est à dire en standard dans **Winnt/system32** le fichier **Adminpak.msi** est également stocké...

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**

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**.

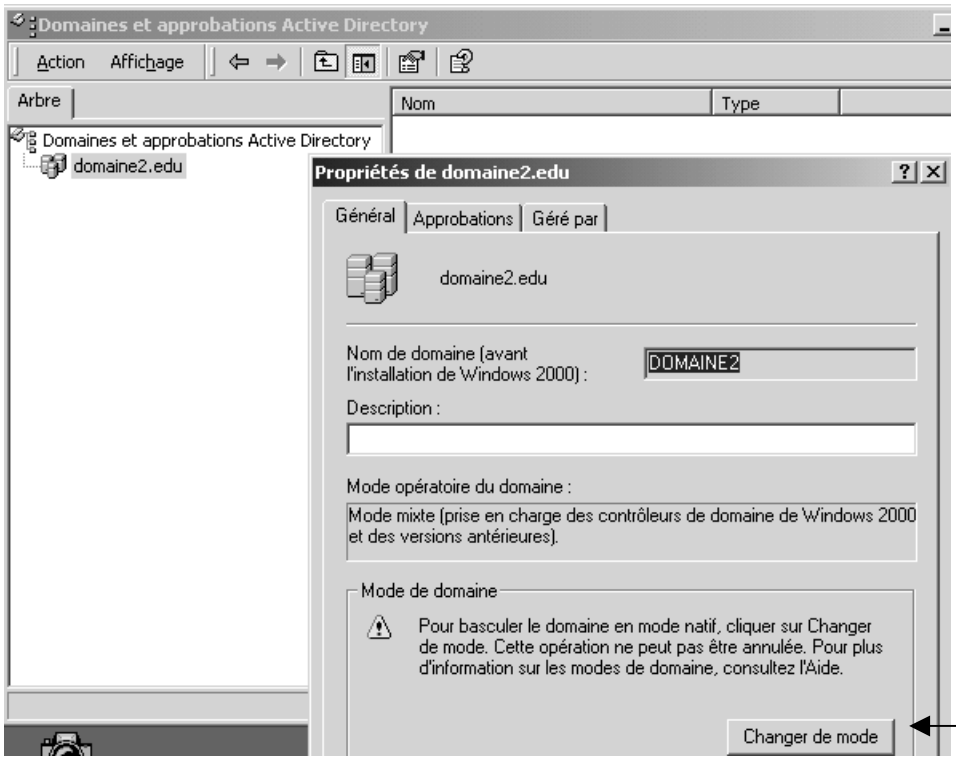
Les raisons de rester en mode mixte

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



INSTALLER NT EN MODE SILENCIEUX

Principes et variantes

En utilisant un fichier de réponse, les administrateurs de réseau et les utilisateurs expérimentés peuvent effectuer une nouvelle installation en mode sans assistance. En mode sans assistance, nulle intervention de l'utilisateur n'est nécessaire pendant l'installation car le fichier de réponse contient toutes les informations dont le programme d'installation a besoin,

Trois types d'installation en "mode silencieux" ou assimilés sont disponibles :

- **Unattended installation** :
  C'est véritablement une installation complète qui va chercher dans un fichier spécifique tout ou partie des réponses (selon le paramétrage que l'on choisit d'adopter) que l'on doit fournir d'habitude au programme d'installation.
  Peut s'appliquer sur des machines de configuration différentes (mais avec un OS déjà installé), soit avec un CD d'origine et une disquette (sur laquelle le fichier de réponse sera stocké) soit en venant chercher sur le réseau les fichiers \i386 du CD d'origine, ce que l'on appelle un dossier de distribution.

- **Sysprep installation** :
  Ce n'est pas véritablement une installation complète mais plutôt un système de clonage de disque intégrant un mécanisme de gestion /changement du SID lors de l'ouverture de la première session. **Ne peut s'appliquer que sur des machines de même configuration !**

- **Remote installation** :
  permet d'installer NT sur une machine nue (sans système d'exploitation) et sans accès CD local NT d'effectuer une installation en générant une disquette "cliente" qui permettra d'ouvrir une session sur le réseau et de faire une installation depuis un point de distribution crée au préalable
  Peut s'appliquer sur toute machines ayant une carte réseau connue ! (à condition qu'un **serveur DNS +** un **serveur DCHP** soient disponibles à **l'intérieur d'un Domaine,** et que le **volume de distribution** sur lequel on ira chercher les fichier du dossier \i386 se trouve dans un **volume NTFS différent du volume dans lequel le serveur est installé**)

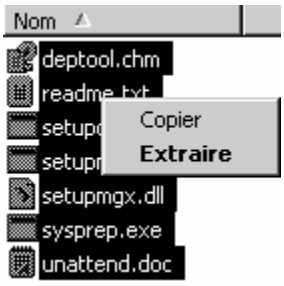
  N.B: Si l'on ne dispose pas des pré-requis énoncés, voir (chap " création client réseau v 3.0" via l'administrateur NT4.0" page 273)

Installer Setup Manager Wizard

Le **Setup Manager Wizard** permet de créer un script pour une installation personnalisée de NT2000 sans se préoccuper de la syntaxe

Pour le copier il suffit de récupérer le fichier **Deploy.cab** qui se trouve dans le dossier **Support/Tools** du CD d'installation NT

Un double clic dessus suffit à visualiser le contenu de ce fichier compressé au format Cabinet

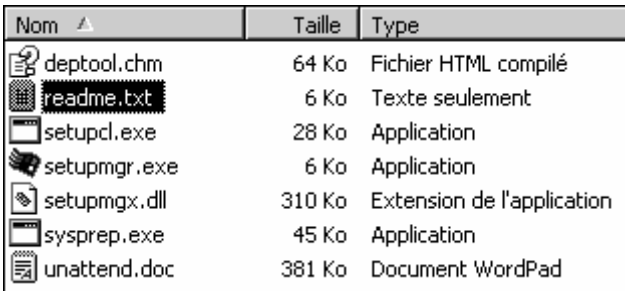


Il faut sélectionner tous les fichiers puis demander via un clic droit souris **Extraire**

NB ; on se sera au préalable crée un dossier de destination spécifique pour répondre à la question de **où doit on les extraires**…

Et voilà les 7 fichiers dont le

Setumgr.exe



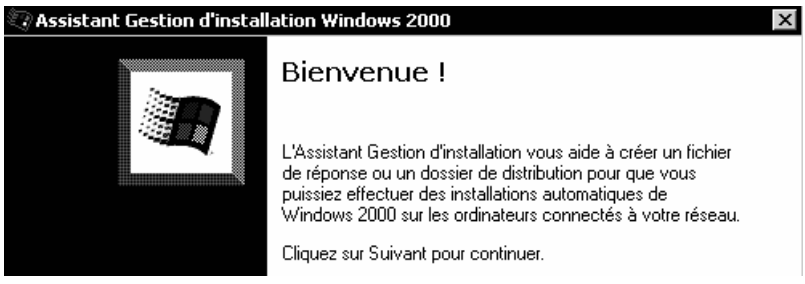
Nom	Taille	Type
deptool.chm	64 Ko	Fichier HTML compilé
readme.txt	6 Ko	Texte seulement
setupcl.exe	28 Ko	Application
setupmgr.exe	6 Ko	Application
setupmgx.dll	310 Ko	Extension de l'application
sysprep.exe	45 Ko	Application
unattend.doc	381 Ko	Document WordPad

Setup Manager Wizard et Unattented Mode

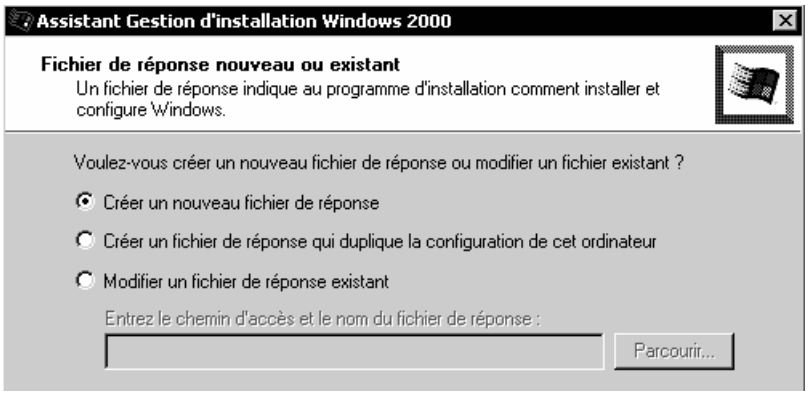
Le **Setup Manager Wizard** permet de créer un script pour une installation personnalisée de NT2000 sans surveillance.

Simultanément un **dossier de distribution** et un **fichier .udf** peuvent être crées

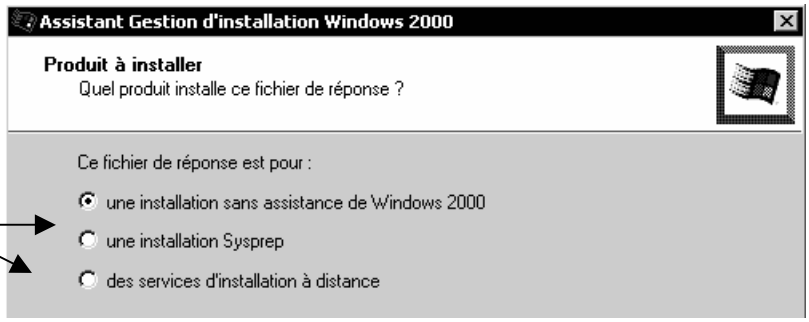
Il faut lancer le fichier **setupmgr.exe** en double-cliquant dessus



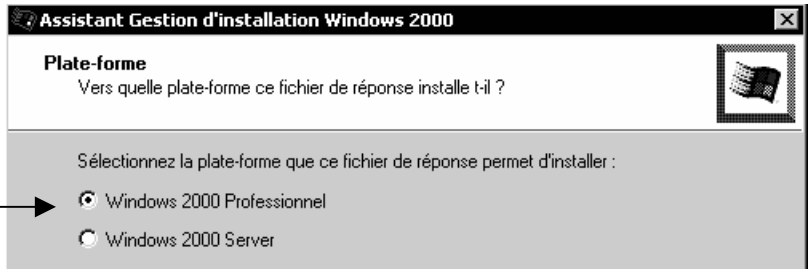
En général on peut se créer plusieurs fichiers de réponses selon les modalité d'utilisation...



C'est ici que l'on choisit une des 3 variantes **Unattended** - **Sysprep** - **Remote** - Installation

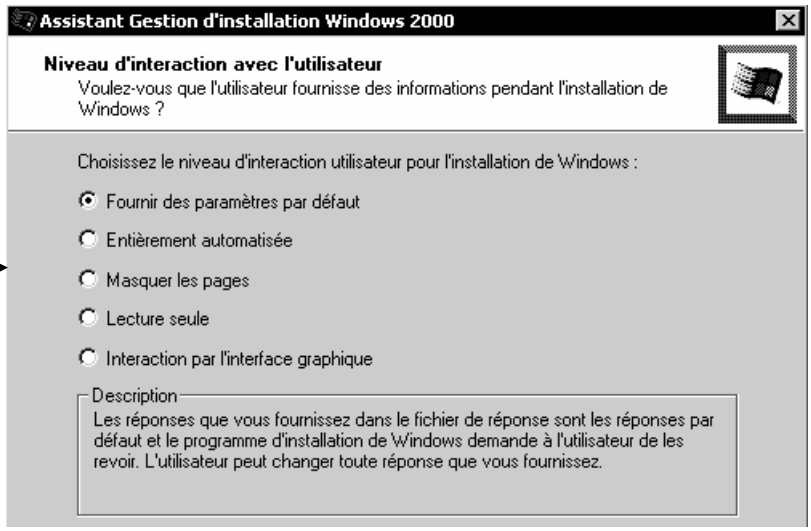


On installe des "client" Windows 2000 Professionnal, (car les serveurs doivent être configurés...)



Le choix est vaste !

Principalement on utilisera une des 3 premières options :



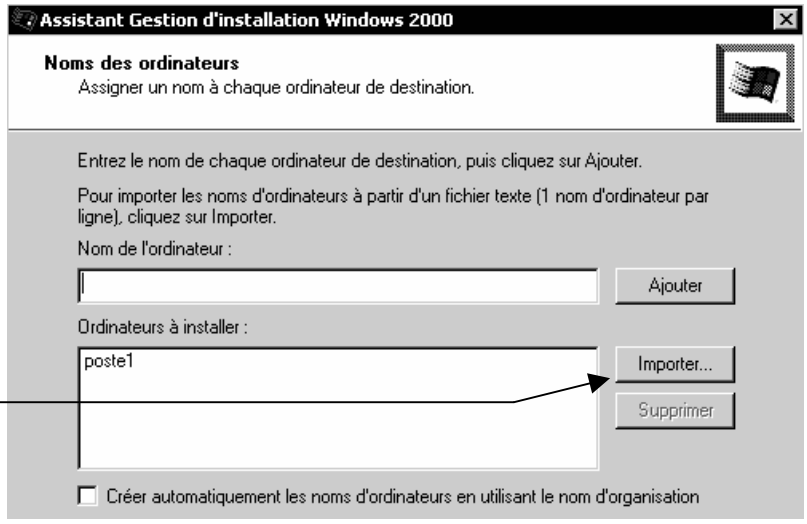
Fournir des paramètres par défaut : (on peut les modifier lors de l'install)

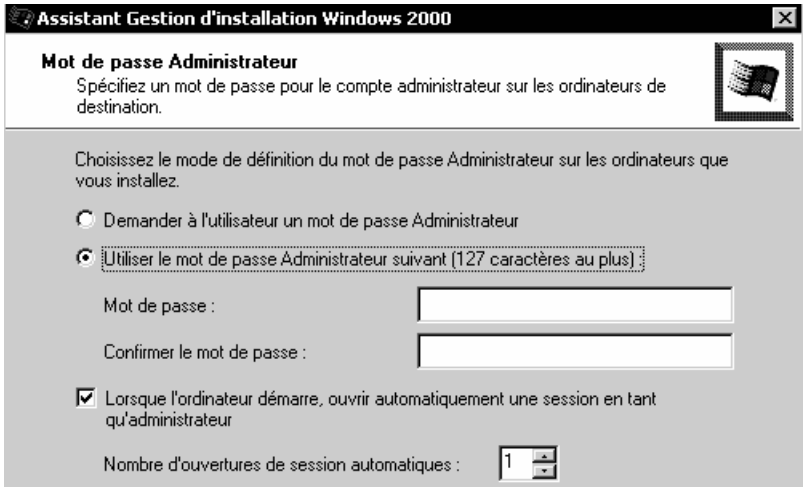
Entièrement automatisé : (l'install totalement automatique)

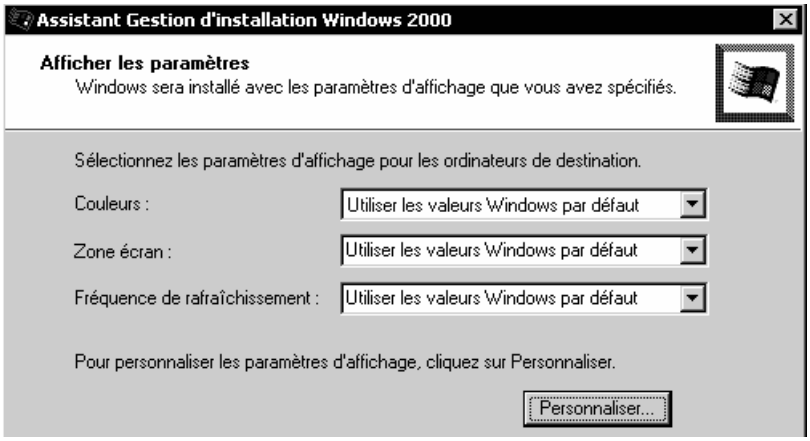
Masquer les pages : (seuls les paramètres non renseignés lors de la création du fichier de réponse restent accessibles lors de l'install)

Si on prévoit une liste de nom possibles, alors il y à création d'un fichier **.udf**

On peut ici associer un fichier texte dont chaque ligne peut correspondre à un nom machine

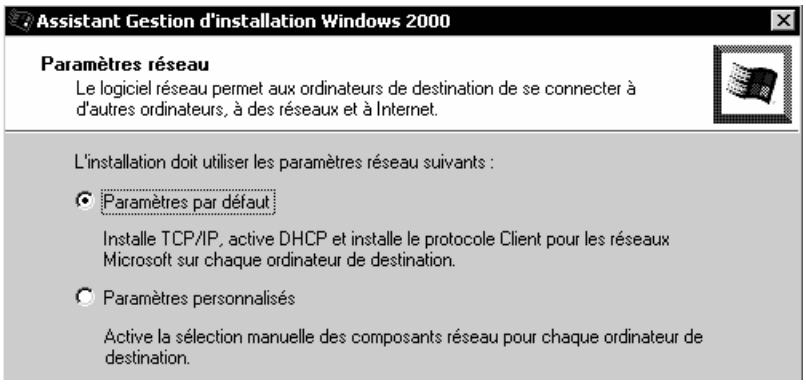




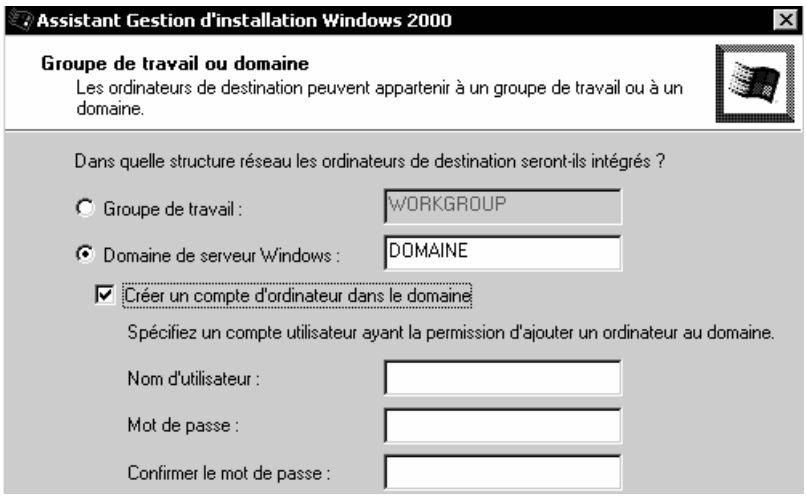


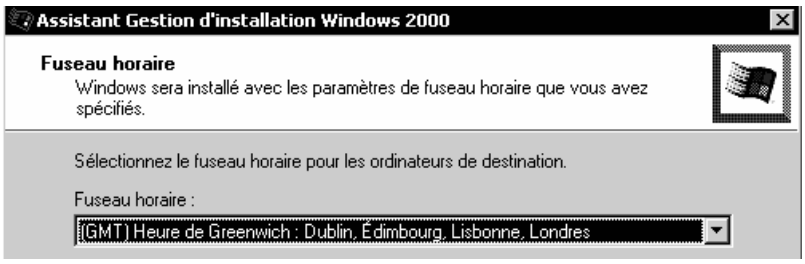
les Paramètres par défaut correspondent à 3 choix :

- protocole TCP/IP
- client réseau Microsoft
- client DHCP

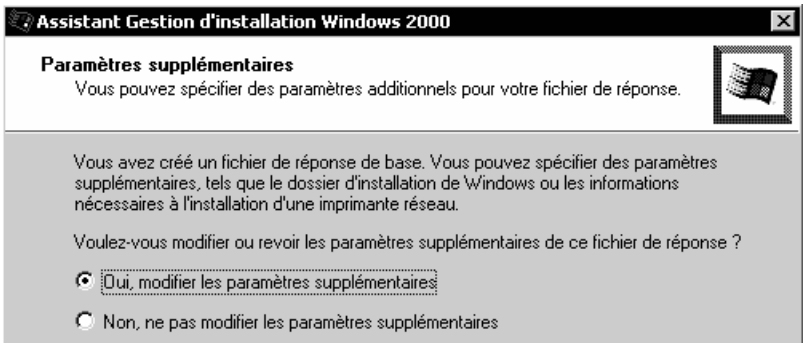


Cela peut être délicat, et on conseille d'abords de se joindre à un Groupe de travail ...

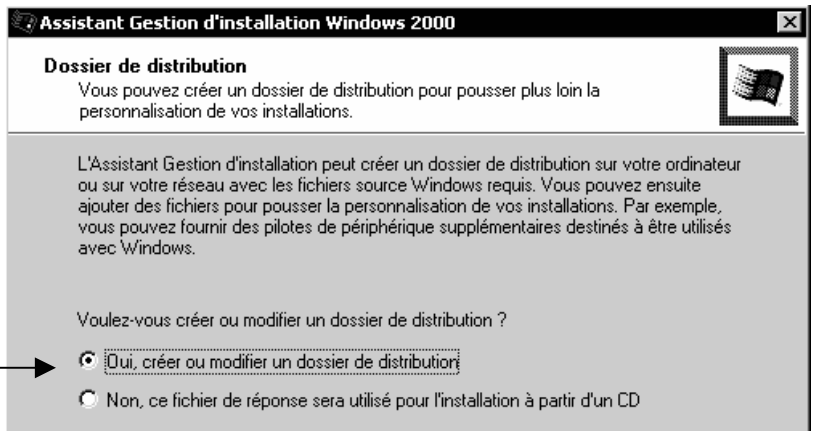




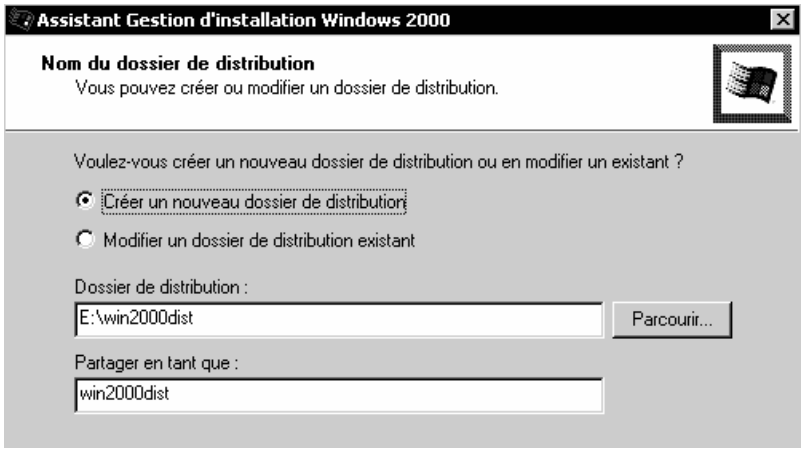
par défaut on propose de modifier des paramètre supplémentaires, non !



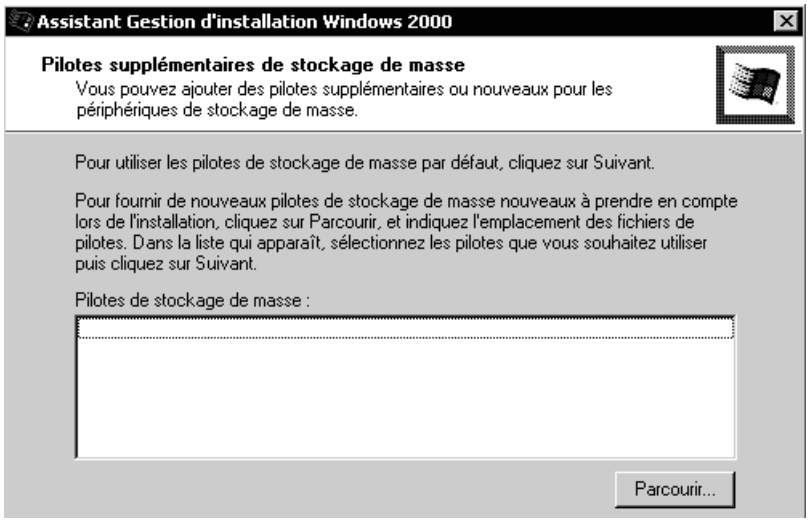
c'est un choix important !



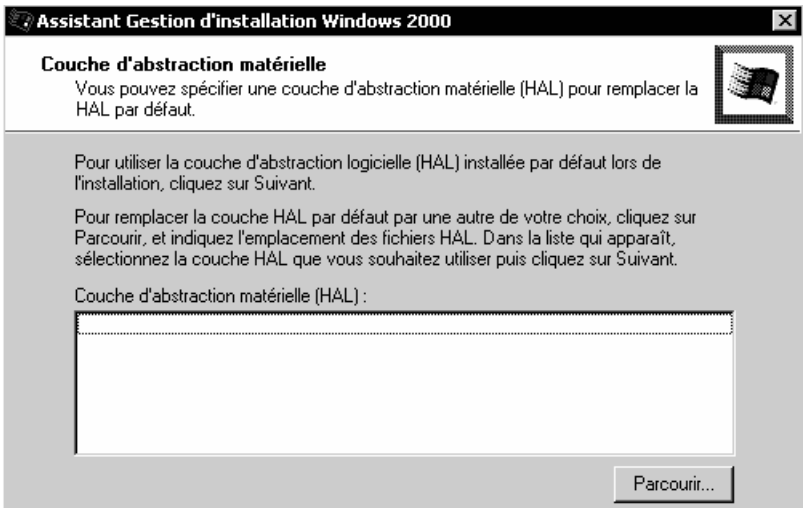
uniquement si on décide de fonctionner avec un dossier de distribution...



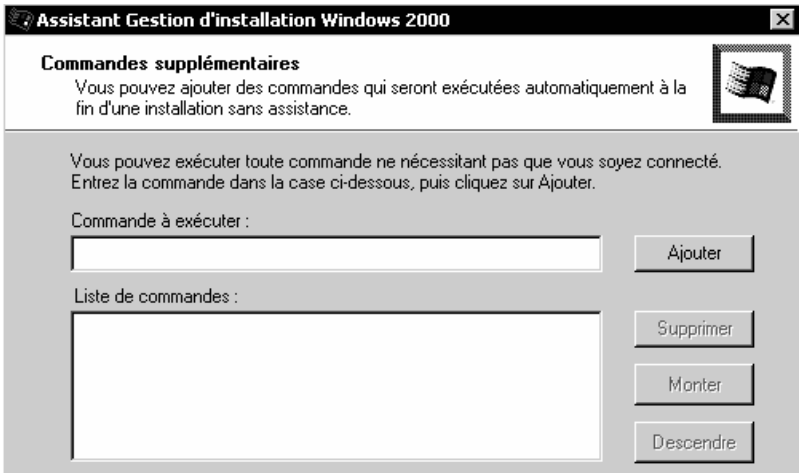
Utiliser les pilotes par défaut...



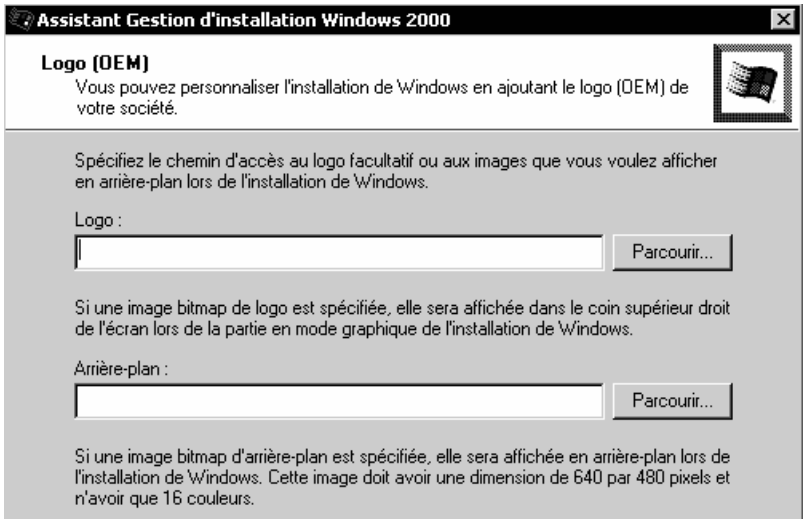
non en général...



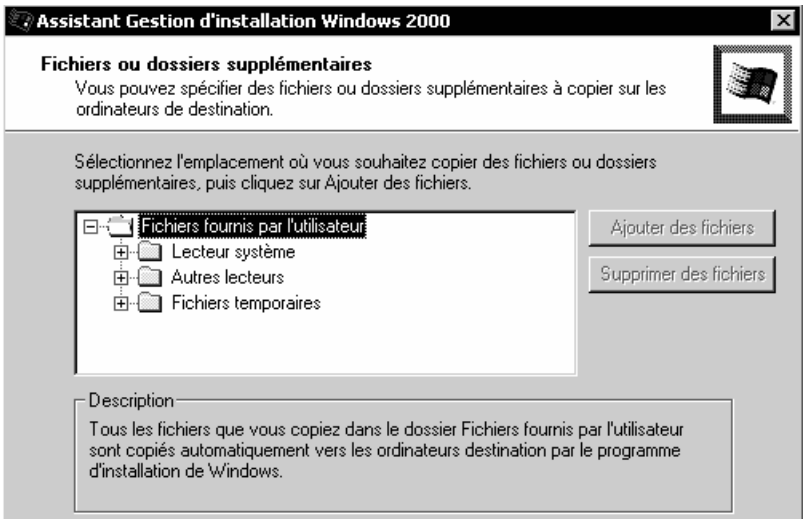
non en général...



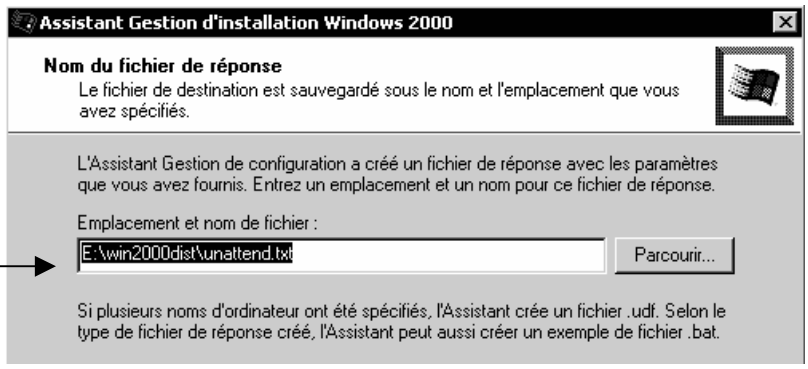
est-ce bien nécessaire ?



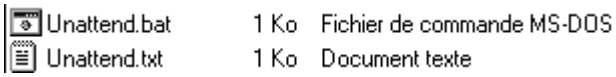
non en général...



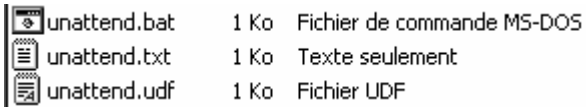
Pour un fichier destiné à être utilisé avec une distribution, en général on crée un fichier **unattend.txt**



Dans le cas d'une utilisation avec un **dossier de distribution** il a création de



Ou de



Le fichier **Unattend.txt** (similaire à **winnt.sif** au niveau de la structure) peut avoir l'aspect suivant :

```
;SetupMgrTag
[Data]
   AutoPartition=1
   MsDosInitiated="0"
   UnattendedInstall="Yes"
[Unattended]
   UnattendMode=ProvideDefault
   OemPreinstall=Yes
[GuiUnattended]
   AdminPassword=zk29
[UserData]
   FullName=cabaré
   OrgName=formation
   ComputerName=Postent2000prof
[SetupMgr]
   DistFolder=E:\win2000dist
   DistShare=win2000dist
dentification]
   JoinWorkgroup=formation
[Networking]
   InstallDefaultComponents=Yes
```

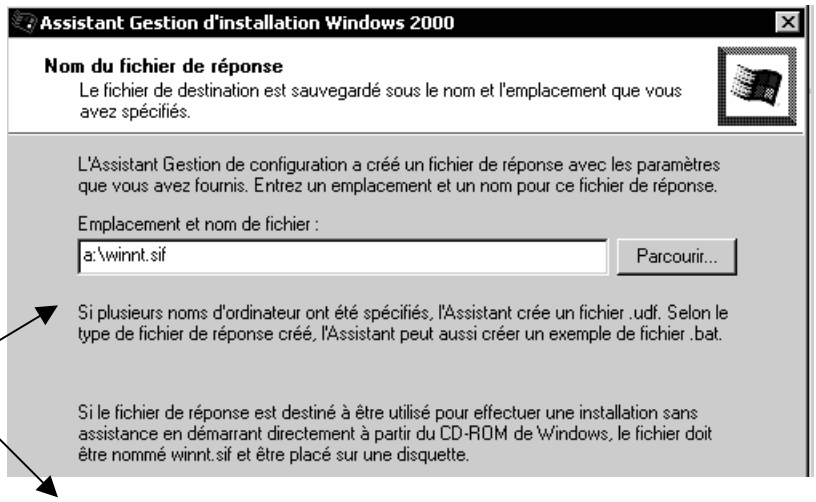
Il peut être utilisé avec un fichier **Unattend.bat** du type

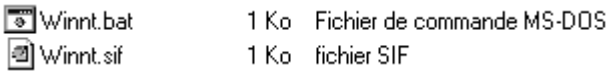
```
set AnswerFile=.\winnt.sif
set SetupFiles=H:\i386
H:\i386\winnt32 /s:%SetupFiles% /unattend:%AnswerFile%
```

N.B: la syntaxe complète de la structure du fichier **Unattend.txt** se trouve dans le fichier **Unattend.doc** situé parmis les fichiers récupérés depuis **Deploy.cab** 'qui se trouve dans le dossier **Support/Tools** du CD NT)

Dans le cas d'une utilisation avec le **CDROM source** NT

Il faut bien indiquer **A:\winnt.sif**





Le fichier **winnt.sif** (similaire à **unattend.txt** au niveau de la structure) peut être utilisé avec un fichier **winnt.bat** du type

```
set AnswerFile=.\winnt.sif
set SetupFiles=H:\i386
H:\i386\winnt32 /s:%SetupFiles% /unattend:%AnswerFile%
```

N.B: pour utiliser le fichier **winnt.sif** et **winnt.bat** il faut bien penser à éviter que la machine ne re-démarre la disquette étant toujours installée dans le lecteur, par conséquent :

- soit il faut être là, et la mettre et l'enlever lorsque c'est nécessaire
- soit dans le **SETUP du PC** au niveau de l'ordre de Boot il faut indiquer **C: - A:** au lieu du classique **A: - C:**

Setup Manager Wizard et Remote Installation

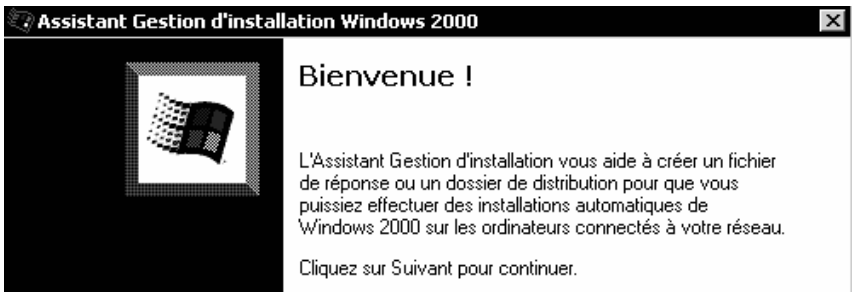
L'installation à distance ne peut fonctionner que si sur le réseau sur lequel on travaille sont opérationnels un **SERVEUR DNS** et un **SERVEUR DHCP**

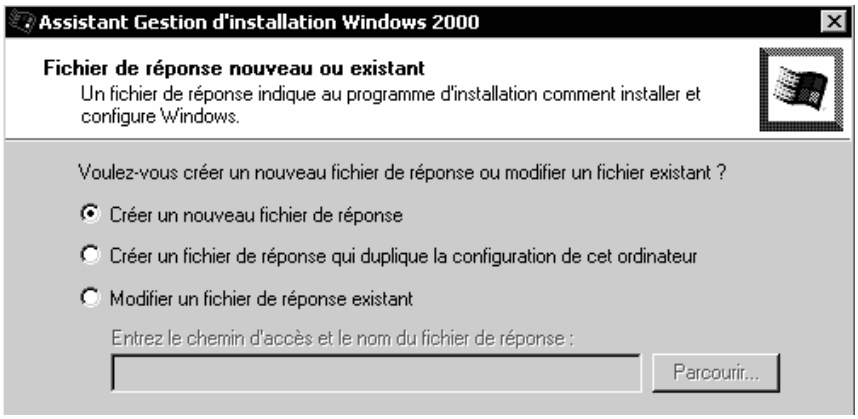
L'installation à distance ne peut fonctionner que si le client depuis lequel on lance l'installation est conforme à la spécification **NETPC**, ou possède une carte réseau équipée d'une **ROM de démarrage PXE**. Dans les autres cas, une **carte réseau simple** et une **disquette de démarrage spécifique** (émulant une ROM au standard PXE) pourront toujours suffire à condition que cette carte réseau soit ***compatible avec la liste des cartes que le générateur de disquette possède*** !

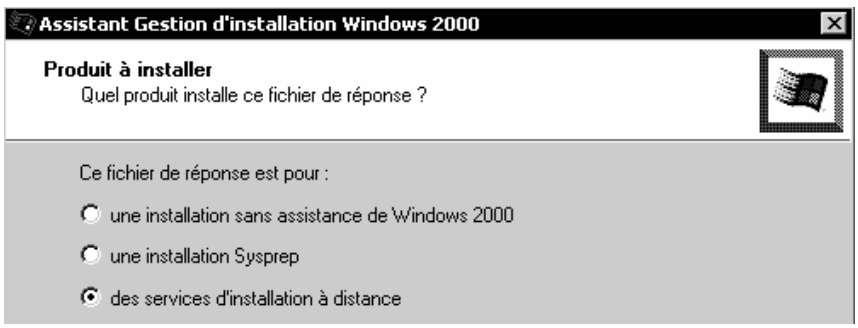
Le **Setup Manager Wizard** permet de créer un script pour une installation à distance.

Simultanément un **dossier de distribution** et un **fichier .udf** est crée

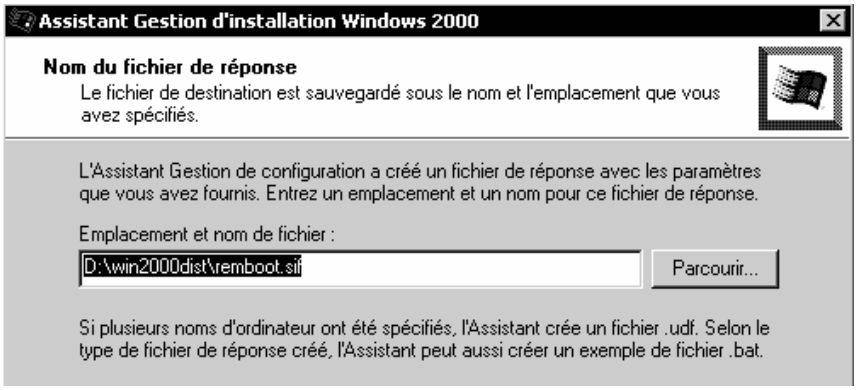
Il faut lancer le fichier **setupmgr.exe** en double-cliquant dessus







puis la fin se termine par



Le fichier **remboot.sif** (similaire à **unattend.txt** au niveau de la structure) peut être utilisé avec une disquette cliente qui pour être générée demande l'installation des **services d'installation à distance**

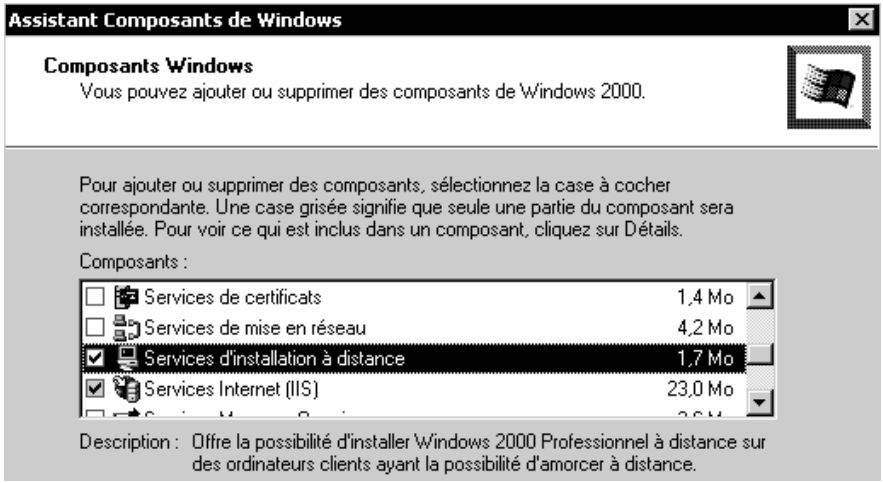
Mise en place des services d'installation à distance

Ces services ne peuvent être mis en place que sur des postes Serveur NT2000, et non sur des postes NT professionnel.

De plus ces services pour être fonctionnels nécessitent qu'il y ait

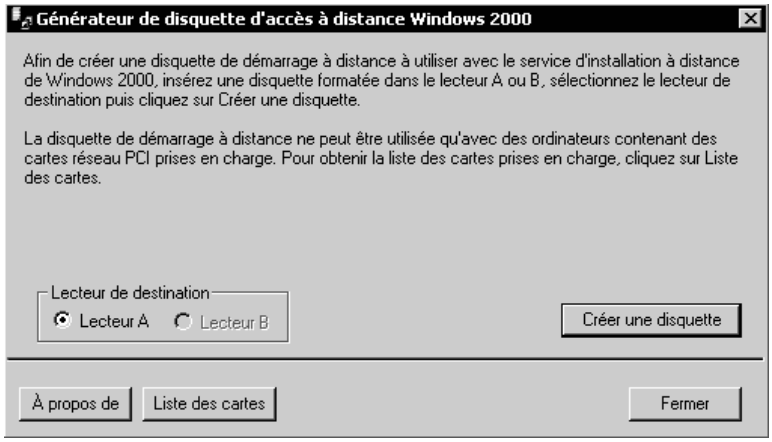
- un **Domaine**
- un **serveur DNS** installé et opérationnel
- un **serveur DCHP** installé et opérationnel
- un **volume de distribution** sur lequel on ira chercher les fichier du dossier \i386 se trouvant dans un **volume NTFS différent du volume dans lequel le serveur est installé**)

N.B: Si on souhaite effectuer une installation via réseau sur une machine nue et que l'on ne dispose pas des pré-requis énoncés, voir (chap " création client réseau v 3.0" via l'administrateur NT4.0" page 273)



Création d'une disquette cliente d'émulation ROM carte réseau PXE

Il faut lancer le programme **rbfg.exe**



CREATION CLIENT RESEAU VER 3.0

Installer Administrateur de client réseau NT 4.0:

Pour récupérer l'administrateur depuis le CD NT server 4.0 il faut

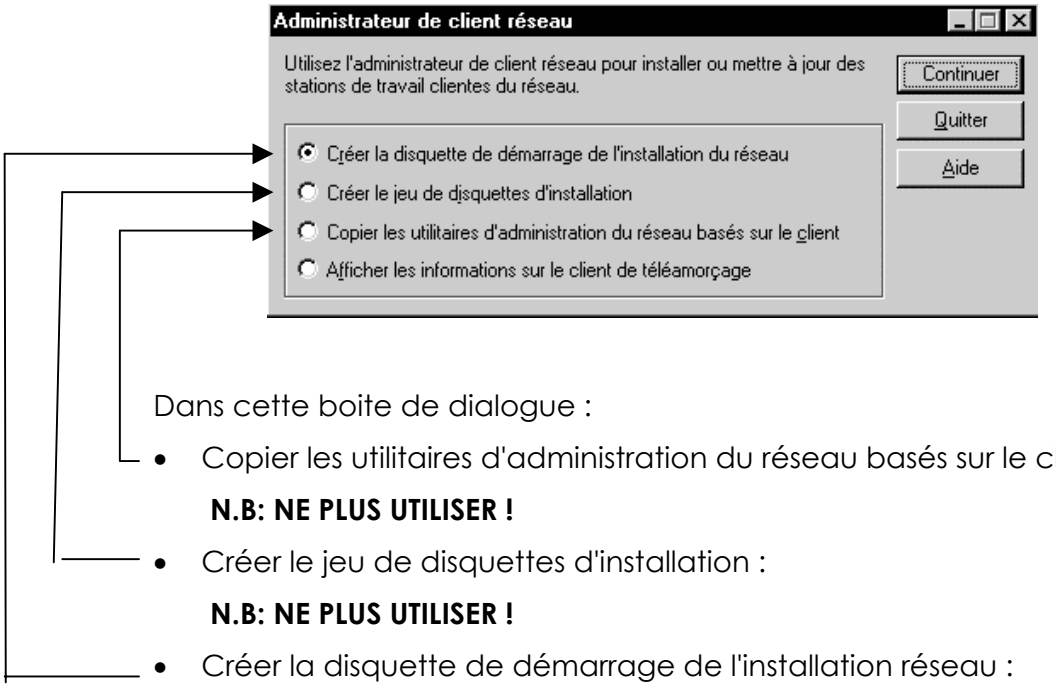
- Créer un dossier spécifique **C:\Ncadmin**
- copier depuis le CD NT server 4.0 les fichier du dossier i386 :
  Ncadmin.cn_ Ncadmin.ex_ Ncadmin.hl_
- taper en ligne de commande :
  expand –r ncadmin.*

Lancer Administrateur de client réseau NT 4.0:

Essentiellement cet outils va nous permettre d'installer sur des postes les composants qui leurs permettrons de devenir "client" du serveur

double cliquer sur le fichier

Ncadmin.exe



Dans cette boite de dialogue :

- Copier les utilitaires d'administration du réseau basés sur le client :

  N.B: NE PLUS UTILISER !

- Créer le jeu de disquettes d'installation :

  N.B: NE PLUS UTILISER !

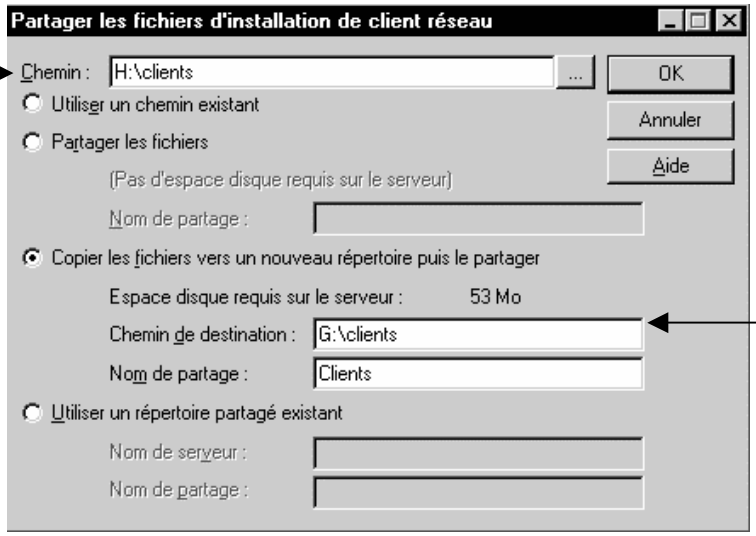
- Créer la disquette de démarrage de l'installation réseau :

  Signifie créer des disquettes amorçables permettant d'installer sur un poste client et depuis les fichier copiées une fois pour toute sur le serveur serveur des Systèmes tels que des Postes Workstation NT, Windows 95-98

1° Utilisation Copie & Partage des fichiers :

Lors de la première utilisation (et quel que soit le choix demandé), l'administrateur de clients réseaux va en général proposer de copier depuis le CD d'origine les fichiers nécessaires dans un dossier et le partager, ceci pour accélérer la vitesse de fonctionnement et pour éviter d'avoir à gérer le CD lors de prochaines opérations similaires

Dossier d'origine sur le CD NT



Dossier de destination sur le serveur NT

Il s'agit donc de copier les répertoires et fichiers du répertoire \Clients du CD de WindowsNT Server vers un dossier d'un disque du serveur partagé en général sous le nom "Clients"

Le tableau suivant décrit l'emplacement et la taille des fichiers d'installation dans le répertoire \Clients du CD de WindowsNT Server.

Client proposé d'office

Description	Répertoire	Taille
LAN Manager pour MS-DOS	\Lanman	3,5 Mo
LAN Manager pour MS OS/2	\Lanman.OS2	3,5 Mo
Network Client pour MS-DOS	\Msclient	4 Mo
RAS pour MS-DOS	\Ras	2,5 Mo
Utilitaires d'administration réseau pour les clients pour Windows NT	\Srvtools\winnt	11 Mo
Utilitaires d'administration réseau pour les clients pour Windows 95	\Srvtools\win95	2,5 Mo
TCP/IP-32 pour Windows pour Workgroups	\Tcp32wfw	2,5 Mo
Windows 95	\Win95	33 Mo

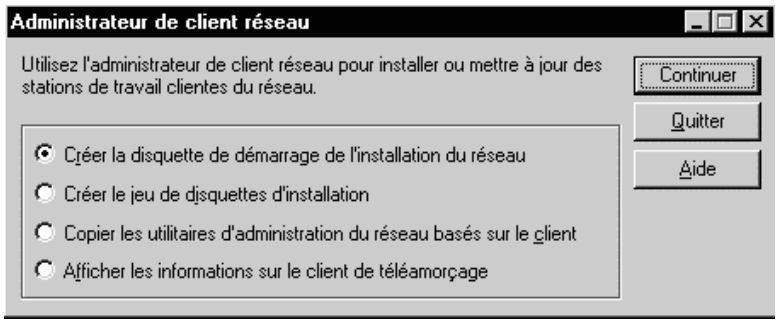
Choix proposés en standard et occupant au total 53 Mo sur le disque

Pour optimiser l'espace du disque dur, on peut supprimer tous les répertoires dont on ne se sert pas.

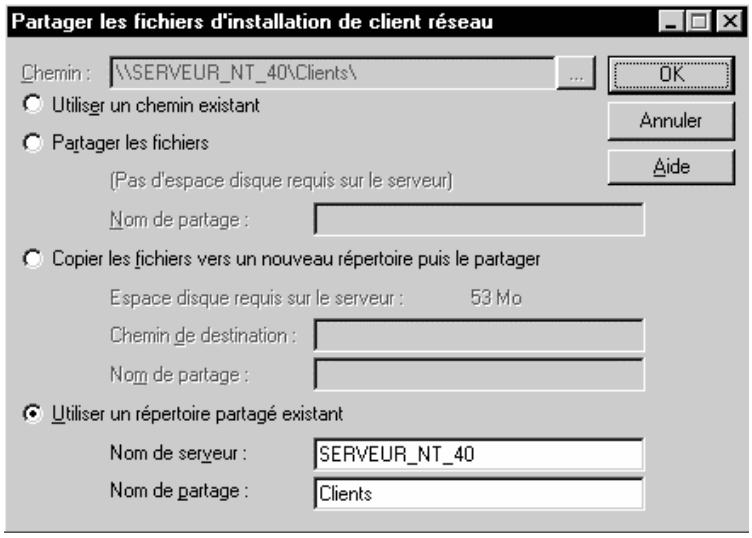
Toutefois, si on veut créer des disquettes de démarrage d'installation réseau, ne pas supprimer **\Clients\Msclient\Netsetup**. Les fichiers se trouvant dans ce répertoire permettent de créer des disquettes de démarrage d'installation réseau pour des Client MS-DOS.

Installation d'un Client Réseau 3.0 :

- Exécutez l'Administrateur de client réseau
- Cliquez sur Créer une disquette de démarrage d'installation, puis sur Continuer



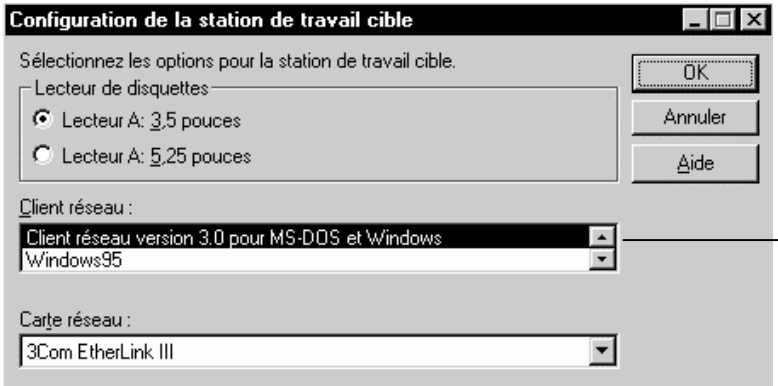
- Cliquez sur Utiliser le répertoire partagé existant, puis sur OK



- Choisissez le lecteur de disquette de la taille adéquate et la carte réseau qui convient

  N.B: On devra se créer un jeu de disquette pour chaque type de carte réseau utilisée sur les clients !

- Choisissez toujours clients MSDOS Windows dans la zone Client réseau et cliquez sur OK



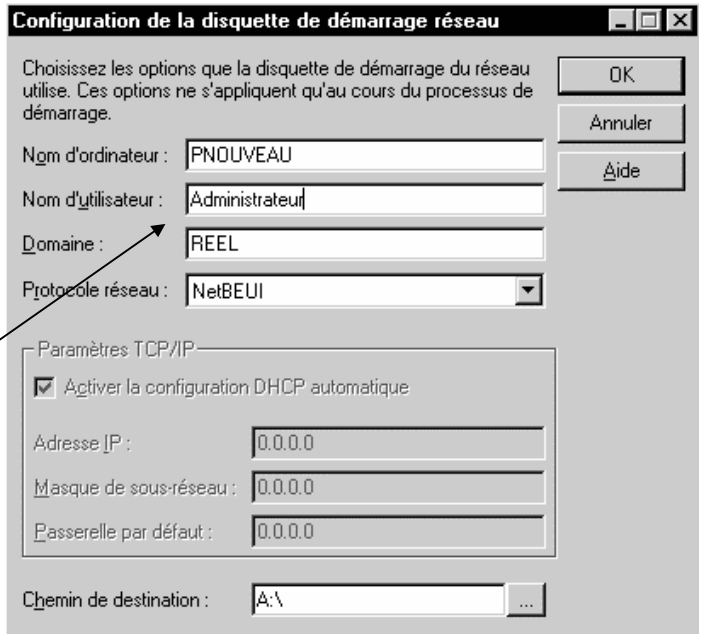
Bien identifier la carte

N.B: NT Server, NT Workstation et Worksgroup apparaitrons si on à chargé leurs fichiers dans le répertoire clients du serveur

- Un message demande ensuite de donner les paramètres pour construire la disquette,

Penser à un nouveau nom pour chaque installation...

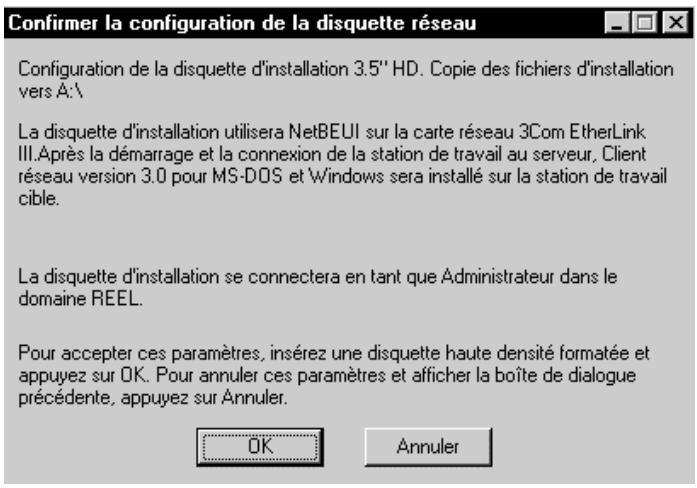
Se connecter avec un compte ayant suffisamment de droit dans le domaine !



Si possible demander NETBEUIL, c'est le plus "léger"

TCP/IP oblige à un véritable casse-tete de taille sur la disquette !

- demande de confirmation à laquelle on répondra en donnant un disquette système (formatée via **FORMAT a: /S**)



- Il ne reste plus qu'a redémarrer le futur poste client à partir de notre disquette de démarrage et enchaîner si tout se passe bien par une installation identique à ce qui se ferait depuis le CD d'origine !

  En effet la disquette comporte un autoexec.bat tel que :

```
path=a:\net
a:\net\net start
net use z: \\SERVEUR\Clients
z:\winnt\netsetup\winnt.exe /B /S:Z:\WINNT\NETSETUP
```

Option /B et /S d'installation...depuis disque z:\winnt\netsetup

On peut sans problème ne laisser que les deux premières lignes

ATTENTION AUX DIFFERENCES CLAVIER US / FR pour le mot de passe !

ensuite **NET USE Z: \\SRVNT40\Clients**

pour attribuer un lecteur **"Z:"** correspondant au dossier partagé **"Clients"** du poste serveur nommé **"SRVNT40"**

ou **NET USE Z: \\SRVNT40\G\I386**

pour attribuer un lecteur **"Z:"** correspondant au dossier **"I386"** d'un CD dans le lecteur de CDROM partagé sous **"G"** du poste serveur nommé **"SRVNT40**"

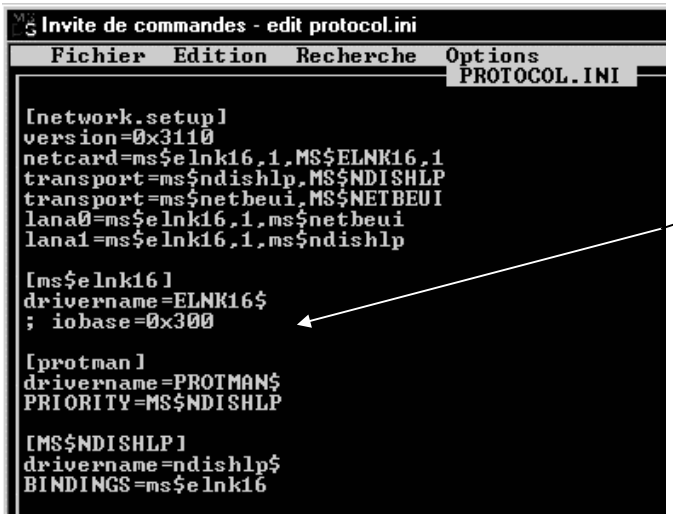
pour plus de renseignements sur la commande **NET** taper NET /? Sous Dos

---

Problèmes d'installation des clients 3.0:

Si des problèmes surviennent lors du redémarrage du PC avec la disquette crée, il faut vérifier les points suivants

- S'assurer d'avoir les permissions suffisantes pour accéder au répertoire partagé CLIENTS sur le serveur
- S'assurer d'entrer un nom d'ordinateur unique sur la disquette de démarrage pour chaque machine configurée via le réseau
- Si on a sélectionné NetBEUI en tant que protocole pour installer le client par l'intermédiaire du réseau, la station de travail cible doit être sur le même réseau que le serveur (non routable)
- La carte réseau ayant été configurée en utilisant des paramètres par défaut. Vérifiez que les paramètres par défaut sont les paramètres qui doivent être utilisés et modifiez les si nécessaire dans le fichier **Protocol.ini, vérifier aussi si besoin le fichier system.ini (nom de driver)**



Vérifier l'adresse, éventuellement l'IRQ et la mise en commentaire par le "**;**"

- On peut avoir un message comme quoi il est nécessaire de verrouiller le disque sur lequel l'installation va se faire si un autre système d'exploitation est détecté sur la machine cliente, il suffit alors de verrouiller le disque en question par la commande

  LOCK C: (si le disque est le C)

  que l'on incorporera en majuscule dans l'autoexec.bat de la disquette de construction client, avant l'appel de l'installation du client proprement dite

Cartes réseaux non connues des clients 3.0:

1. Lancez l'administrateur de clients réseaux normalement et choisissez un carte réseau comparable a la votre.
2. Une fois la génération de disquette finie, recherchez la disquette de pilote fournie avec votre carte réseau
3. Sur la disquette, il doit se trouver un répertoire NDIS et une section DOS.
4. Copiez les fichiers .dos de votre disquette de pilote dans le répertoire Net de la disquette crée par l'administrateur de client réseau .
5. La disquette de pilote doit aussi contenir un exemple de fichier protocol.ini , ouvrez ce fichier et cherchez y une ligne avec un $ a la fin , par exemple :
   DriverName = "EL59X$"
   Notez cette ligne .
6. Insérez la disquette crée par l'administrateur de client réseau et allez dans le répertoire **\net**.
7. Ouvrez le fichier system.ini et modifiez la section drivers pour qu'elle se réfère aux fichiers .dos que vous venez de copier. Par exemple :
   [network drivers]
   netcard=EL59X.dos
8. Apres avoir enregistré le **system.ini**, ouvrez le protocol.ini (dans le même répertoire) et trouvez le paramètre "**DriverName**" , changez le alors pour le nom que vous avez noté a l'étape 5. Par exemple
   [ms$elnk3]
   DRIVERNAME=EL59X$
   Si la carte est PCI , vérifiez que les interruptions et les I/O sont bien mis en commentaire ou alors indiquez les valeurs correctes.

Le client réseau sur disquette est maintenant configuré pour utiliser votre carte réseau.

Le texte original de la question :[*http://www.ntfaq.com/ntfaq/install32.html*](http://www.ntfaq.com/ntfaq/install32.html)

ANNEXE ADRESSE IP

Adresse IP :

La version actuelle de ce protocole désormais quasi universel repose en partie sur la notion d'adresse **IP** (Internet Protocol) décernée de façon unique pour chaque élément matériel faisant partie d'une réseau

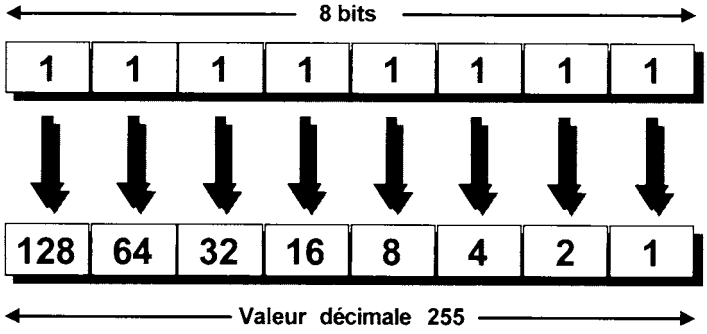
Ces adresses sont codées sur 32 bits, est sont représentées sous la forme de 4 nombre compris entre 0 et 255 (valeur d'un octet) et séparés par un point, soit (par exemple)

255.0.127.2 (ADRESSE DECIMALE)

On parle de bits de poids fort pour les nombres les plus à gauche

On parle de bits de poids faible pour les nombres les plus à droite

Chaque nombre décimal est la représentation d'un nombre binaire de 8 chiffres



On peut alors avoir aussi en notation binaire

11111111.00000000.01111111.00000010 (ADRESSE BINAIRE)

On parle de bits de poids fort pour les nombres les plus à gauche

On parle de bits de poids faible pour les nombres les plus à droite

On pourrait ainsi dire que les adresses IP varient de la plus petite 0.0.0.0 à la plus grande255.255.255.255

En fait toutes les combinaisons ne sont pas disponibles, et elles reflètent une certaine logique

ID réseau et ID hôte :

Les bits de poids fort définissent l'adresse du réseau, on parle de **ID réseau** et Les bits de poids faible définissent l'adresse d'un équipement dans le réseau on parle de **ID hôte**.

L' **ID réseau** identifie toutes les machines qui se trouvent sur le même réseau physique , encore appelé domaine de collision. Il s'agit d'un identifiant pour un réseau local , toutes les machines se trouvant "du même coté d'un routeur…

L' **ID hôte** identifie tout poste ou périphérique du réseau, il est unique à l'intérieur de tout **ID réseau**

Classes d'Adresse :

La limite entre poids fort et poids faible n'est pas toujours la même, c'est la notion de "**classe d'adresse**"

- plus les poids fort sont petits, et plus le nombre de machines dans un même réseau sera important, même si on aura peut de réseau
- plus les poids fort sont nombreux, on aura alors peut de machines connectable pour chacun de ces réseau, même s'il sont plus nombreux

Réseau de **Classe A** : (commence par **1** à **127**)

0XXXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

1° bit à 0

7 bits pour le réseau soit 2^7=127réseaux

24 bits pour le matériel soit 2^{24} (16 millions de machines)

Réseau de **Classe B** : (commence par **128** à **191**)

10XXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

1° bit à 1

2° bit à 0

14 bits pour le réseau soit 2^{14}=16384 réseaux

16 bits pour le matériel soit 2^{16} (65536 machines)

Réseau de **Classe C** : (commence par **192** à **223**)

110XXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

1° bit à 1

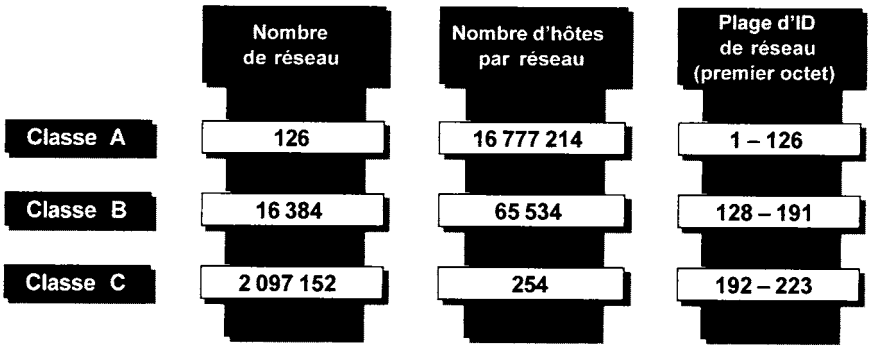
2° bit à 1

3° bit à 0

21 bits pour le réseau soit 2^{21}=2097152 réseaux

8 bits pour le matériel soit 2^8 (256 machines)

Soit en résumant



Avec quelques règles supplémentaires :

- l'**ID réseau 127**, est réservée pour les tests
- Un **ID réseau** composé exclusivement de 1 ou de 0 n'est jamais attribué
- Un **ID hôte** composé exclusivement de 1 ou de 0 n'est jamais attribué
- La valeur **255.255.255.255** correspond à une diffusion générale (**Broadcast**)

Adresses IP Privées :

Il est normal d'assigner des adresses globalement uniques à toutes les machines qui utilisent TCP/IP. Pour pouvoir étendre la durée de vie de l'adressage IPv4, les organismes d'enregistrement demandent plus de justifications qu'auparavant, rendant la tâche plus difficile à des organisations pour acquérir des adrresses supplémentaire [RFC1466].

Les machines de l'entreprise qui utilisent TCP/IP peuvent être divisées en 3 catégories:

- **Catégorie 1 :** les machines qui n'ont pas besoin d'accéder à des machines d'autres entreprises ou à l'Internet dans son ensemble. Les machines de cette catégorie peuvent utiliser des adresses IP qui sont uniques dans l'entreprise, mais qui peuvent être ambigues entre différentes entreprises.
- **Catégorie 2 :** les machines qui ont besoin d'accéder à un nombre limité de services extérieurs (ex: E-Mail, WWW, FTP) qui peuvent êtres servis par des passerelles applicatives. Pour beaucoup de machines dans cette catégorie, un accès non restreint (fourni par la connectivité IP) n'est pas forcément nécessaire et même quelque fois non désiré pour des raisons de sécurité. Pour les mêmes raisons que pour les machines de la première catégorie, de telles machines peuvent utiliser des adresses IP uniques dans l'entreprise, mais qui peuvent être ambigues entre différentes entreprises.

- **Catégorie 3 :** les machines qui ont besoin d'un accès réseau à l'extérieur de l'entreprise (fourni par la connectivité IP). Les machines de cette dernière catégorie ont besoin d'une adresse unique sur tout l'Internet.

On parle pour les machines des catégories 1 et 2 comme de machines "privées", et pour les machines de la 3eme catégorie comme des machines "publiques".

L'Autorité d'Affectation de Numéros sur Internet a réservé les 3 bloc suivant dans l'espace d'adressage pour des réseaux internes RFC 1918:

le premier bloc n'est rien d'autre qu'une classe A n° **10.**

10.0.0.0 - 10.255.255.255 (10/8 prefix)

le second, un ensemble de 16 classes B contiguës entre n° **172.16. et 172.31.**

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

N.B: pour **172.16.0.** le premier hote dispo sera .0.1 (éviter N° à 0 totalement)

et le troisième, un ensemble de 256 classes C de n° **192.168.0. à 192.168.255.**

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

N.B: pour **192.168.0.** le premier hote dispo sera .1 (éviter N° à 0 totalement)

Les **machines privées** peuvent communiquer avec toutes les autres machines de l'entreprise, à la fois publiques et privées. Néanmoins, elles ne peuvent avoir de connectivité IP avec une machine à l'extérieur de l'entreprise. Même si elles n'ont pas de connectivité IP vers l'extérieur, les machines privées peuvent toutefois avoir accès à des services extérieurs grâce à des passerelles (ex passerelles applicatives).

Pour connecter un réseau utilisant des adresse privées RFC 1918 sur internet, il est nécessaire de prévoir un système de traduction d'adresse (Network Address Translator) ou un système de proxy

Les **machines publiques** peuvent communiquer avec d'autres machines privées ou publiques à l'intérieur de l'entreprise et possèdent une connectivité IP avec les machines publiques extérieures à l'entreprise. Les machines publiques n'ont pas de connectivité avec des machines privées d'autres entreprises.

Masque de sous-réseau :

Le **masque de sous-réseau** permet de définir le découpage entre les bits de l'adresse qui servent à définir l'adresse de réseau, et ceux servant à définir l'adresse de la machine

En effet via un système de **ET bit à bit**, le **masque de sous-réseau** permet de distinguer l'**ID réseau** à partir de l'**Id hôte**, et par conséquent permet à **TCP/IP** de savoir si une **adresse IP** donnée se trouve sur le **réseau local** ou sur un **réseau distant**

Masque par défaut :

Ainsi dans des masques standards, tous les bits correspondants à l'**ID réseau** sont à 1, tous les bits correspondants à l'**ID hôte** sont à 0

Classe d'adresse	Bits utilisés pour le masque de sous-réseau				Notation décimale à points
Classe A	11111111	00000000	00000000	00000000	255.0.0.0
Classe B	11111111	11111111	00000000	00000000	255.255.0.0
Classe C	11111111	11111111	11111111	00000000	255.255.255.0

Masque personnalisé :

L'objectif est ici d'obtenir des adresses d'**ID réseau** et d'**Id hôte** groupées de manière un peu différente par rapport aux classes standardisées A-B-C qui servent de cadre

Pour définir des sous-réseaux personnalisé, il est nécessaire de bien définir deux points :

- Combien de réseau veut on gérer à l'intérieurs de la plage d'adresse attribuée
  N.B: en prévoyant un évolution future raisonnable !
- Combien d'hôtes maximum veut on gérer a l'intérieur d'un sous-réseau
  N.B: en prévoyant un évolution future raisonnable !

Puis travailler de la manière suivante :

- Définir le masque de sous-réseau qui donne le nombre de sous-réseau et d'hôte par sous-réseau voulu
- Déterminer les **ID réseaux** possibles à utiliser
  N.B: (cf tables page 286 pour savoir combien il y en a)
- Déterminer les **ID hôtes** possibles à utiliser
  N.B: (cf tables page 286 pour savoir combien il y en a)

Définir un masque de sous-réseau

On l'a dit, l'**ID réseau** se calcule en regardant le nombre de 1 du masque de sous-réseau.

Pour augmenter le nombre d'**ID réseau**, il faut ajouter des bits au masque de sous-réseau (Bien sûr si on augment le nombre d'**ID réseau**, on diminue le nombre d'**ID hôte**…)

De combien de bit faut-il augmenter le masque de sous-réseau ?

comme on travaille avec les puissances de 2, on augmente les combinaisons de 2 ^ nb bits ajoutés

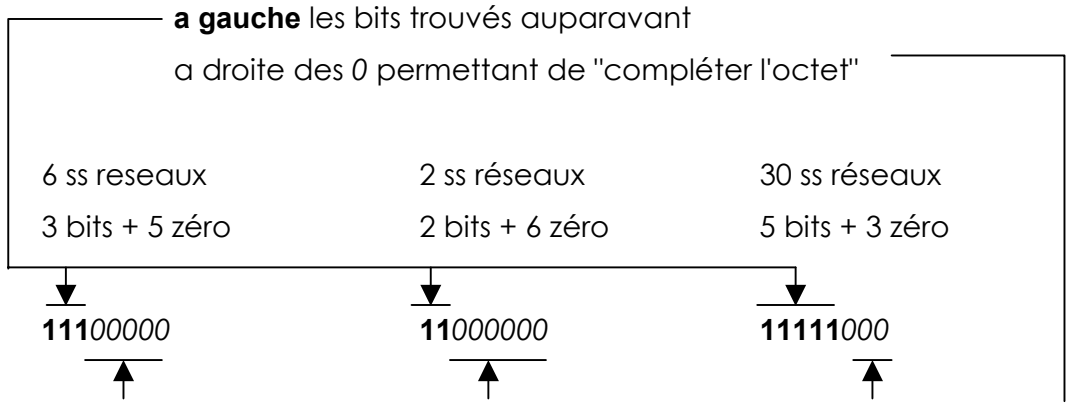
soit	1 bit	2 sous-réseaux
	2 bit	4 sous réseaux
	3 bits	8 sous réseaux
	4 bits	16 sous réseaux
	5 bits	32 sous réseaux
	x bits	2^x. sous-réseaux

mais rappelez vous, les adresse ne contenant que des 0 ou que des 1 ne sont pas autorisées, par conséquent il faut enlever les 2 adresses extrêmes possibles…ce qui nous donne

soit	**1 bit**	**impossible**	(2-2=0)
	2 bit	**2 sous réseaux**	(4-2)
	3 bits	**6 sous réseaux**	(8-2)
	4 bits	**14 sous réseaux**	(16-2)
	5 bits	**30 sous réseaux**	(32-2)
	x bits	(2^x)-2 sous-réseaux	

Comment calculer le nouveau masque de sous-réseau de mes réseaux?

1. Un foi trouvé le nombre de bits me permettant d'obtenir le nombre de sous-réseaux voulu, je dois créer un octet avec :



2. puis le convertir en décimal

111*00000*	**11***000000*	**11111***000*
=128+64+32	=128+64	=128+64+32+16+8
224	192	248

3. et remplacer dans la masque par défaut de ma classe d'adresse, le premier 0 par ce nombre…

6 ss reseaux	2 ss réseaux	30 ss réseaux
224	192	248

si l'adresse est de classe **A** cela donne par rapport au masque **255.0.0.0**

255.224.0.0	**255**.192.0.0	**255**.248.0.0

si l'adresse est de classe **B** cela donne par rapport au masque **255.255.0.0**

255.255.224.0	**255.255**.192.0	**255.255**.248.0

si l'adresse est de classe **C** cela donne rapport au masque **255.255.255.0**

255.255.255.224	**255.255.255**.192	**255.255.255**.248

Comment calculer les ID réseau de mes réseaux?

1. Recenser toutes les combinaisons possibles (en excluant donc celles n'ayant que des 1 ou des 0) de bits ajoutées au masque de sous-réseau précédemment et les convertir en décimal:

6 ss réseaux	2 ss réseaux	30 ss réseaux
(111)*00000*	**(11)***000000*	trop long !
110*00000*	**10***000000*	
101*00000*	**01***000000*	
011*00000*	**(00)***000000*	
100*00000*		
010*00000*		
001*00000*		
(000)*00000*		

2. Les convertir en décimal:

6 ss réseaux	2 ss réseaux
192	64
160	32

128

96

64

32

3. Ajouter ces valeurs a l'**ID réseau** d'origine:

Comment calculer les ID hôtes disponibles dans mes réseaux?

Les **ID hôte** commencent par la valeur .001 dans le dernier octet et augmentent 1 par 1 jusqu'à atteindre la valeur ID de sous-réseau du réseau suivant, -1

Bien sûr le dernier octet lui aussi ne peut pas être égal à 0 ou 255.

Tables de définition des sous-réseaux :

voilà le nombre de sous-réseau utilisables, avec le nombre d'hôte possible pour un masque de sous-réseau donné, et ce pour les

Adresses de classe A:

Bits supplémentaires (n)	*Nombre maximum de sous-réseaux (2^n-2)*	*Nombre maximum d'hôtes par sous-réseau (2^(24-n)-2)*	*Masque de sous-réseau*
0	0	16 777 214	255.0.0.0
1	invalide	invalide	invalide
2	2	4 194 302	255.192.0.0
3	6	2 097 150	255.224.0.0
4	14	1 048 574	255.240.0.0
5	30	524 286	255.248.0.0
6	62	262 142	255.252.0.0
7	126	131 070	255.254.0.0
8	254	65 534	255.255.0.0

Adresses de classe B:

Bits supplémentaires (n)	*Nombre maximum de sous-réseaux (2^n-2)*	*Nombre maximum d'hôtes par sous-réseau (2^(16-n)-2)*	*Masque de sous-réseau*
0	0	65 534	255.255.0.0
1	invalide	invalide	invalide
2	2	16 382	255.255.192.0
3	6	8 190	255.255.224.0
4	14	4 094	255.255.240.0
5	30	2 046	255.255.248.0
6	62	1 022	255.255.252.0
7	126	510	255.255.254.0
8	254	254	255.255.255.0

Adresses de classe C:

Bits supplémentaires (n)	*Nombre maximum de sous-réseaux (2^n-2)*	*Nombre maximum d'hôtes par sous-réseau (2^(8-n)-2)*	*Masque de sous-réseau*
0	0	254	255.255.255.0
1	invalide	invalide	invalide
2	2	62	255.255.255.192
3	6	30	255.255.255.224
4	14	14	255.255.255.240
5	30	6	255.255.255.248
6	62	2	255.255.255.252
7	invalide	invalide	255.255.255.254
8	invalide	invalide	255.255.255.255

Exemple 6 sous réseaux de 30 postes :

Si on veut **6 sous réseaux** comportant chacun 30 machines maximum, on pourra prendre alors comme masque de sous réseau **255.255.255.224**

- **Id réseau**
  pour trouver les Id réseau je dois trouver toutes les combinaisons de **3 bits** de 111 à 000 en laissant tomber les valeurs n'ayant que des 0 ou que des 1 (non autorisée).J'obtient 110-101-011-100-010-001 soit en décimal 192-160-128-96-64-32.

  que je rajoute à mon Id réseau d'origine 192.168.1.xx soit donc les Id réseau suivantes :

  192.168.1.**192** 192.168.1.**160** 192.168.1.**128** 192.168.1.**96**

  192.168.1.**64** 192.168.1.**32**

- Id hôte valide
  un petit calcul nous donne :

sous-réseau	**1° adresse IP**	**dernière adresse IP**
192.168.1.**32**	192.168.1.33	192.168.1.63
192.168.1.**64**	192.168.1.65	192.168.1.95
192.168.1.**96**	192.168.1.97	192.168.1.127
192.168.1.**128**	192.168.1.129	192.168.1.159
192.168.1.**160**	192.168.1.161	192.168.1.191
192.168.1.**192**	192.168.1.193	192.168.1.223

ANNEXE : STRATÉGIES WIN 98

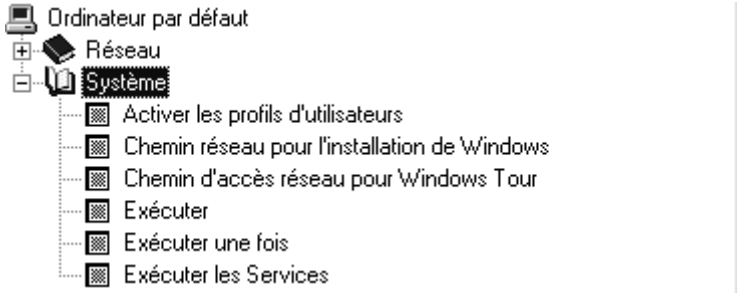
petit descriptif sommaire des stratégies disponibles sous windows 98

Stratégies d'Ordinateur Windows 98 :

L'éditeur de stratégie windows 98 présente au niveau **ordinateur** :

Réseau

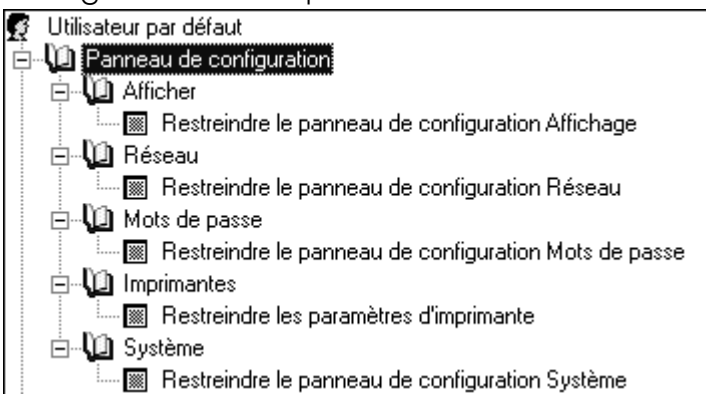
Système



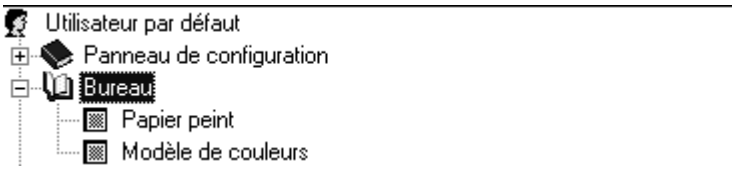
Stratégies d'Utilisateur Windows 98 :

L'éditeur de stratégie windows 98 présente au niveau **utilisateur** :

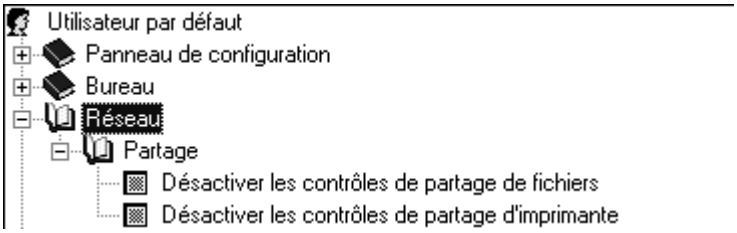
Panneau



Bureau

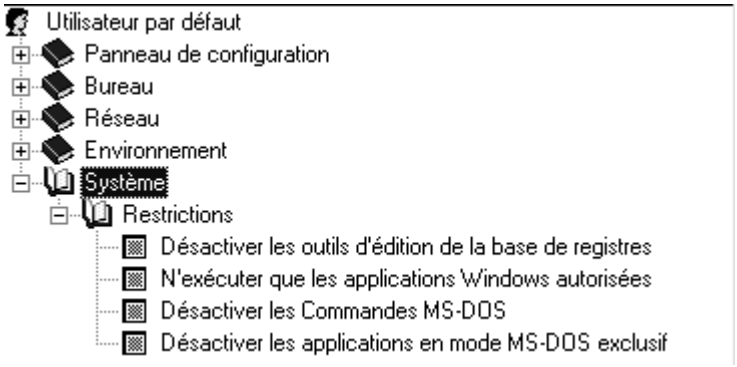


Réseau



Environnement

Système


Utilisateur par défaut
Panneau de configuration
Bureau
Réseau
Environnement
Système
Restrictions
Désactiver les outils d'édition de la base de registres
N'exécuter que les applications Windows autorisées
Désactiver les Commandes MS-DOS
Désactiver les applications en mode MS-DOS exclusif

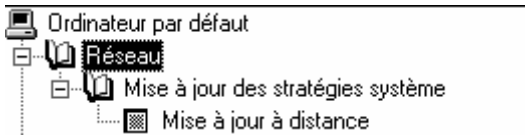
ANNEXE : STRATEGIES NT 4.0

petit descriptif sommaire des stratégies disponibles sous windows NT 4.0

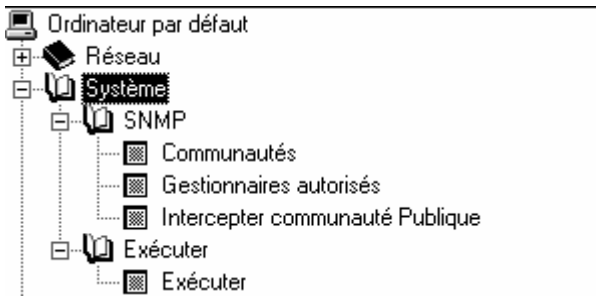
Stratégies d'Ordinateur Windows NT :

L'éditeur de stratégie windows NT présente au niveau **ordinateur** :

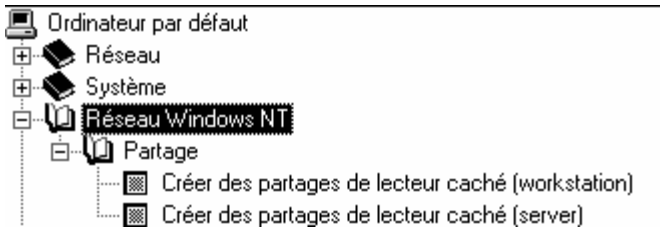
Réseau



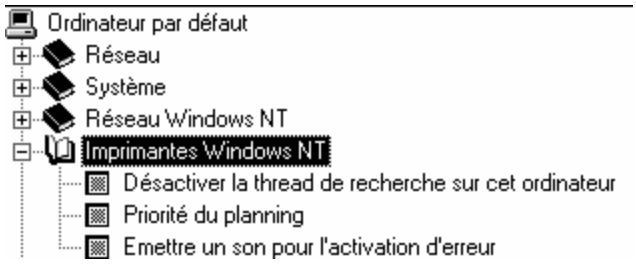
Système



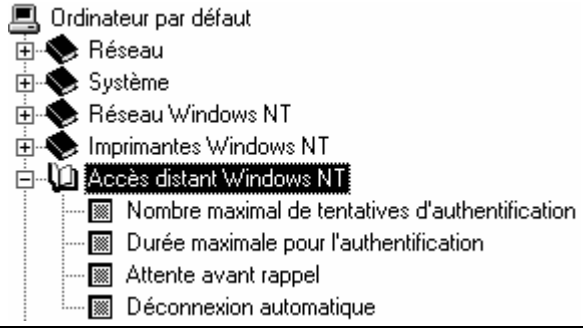
Réseau NT



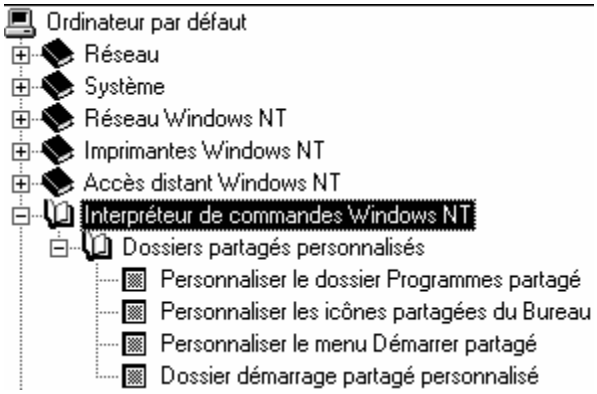
Imprim…



Accès



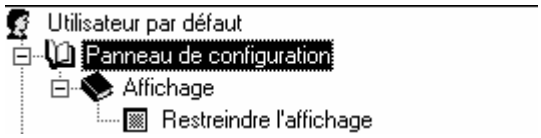
Commande



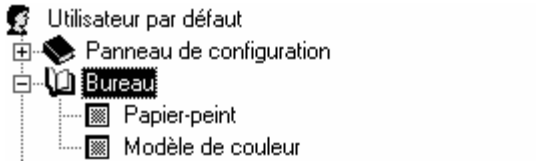
Stratégies d'Utilisateur Windows NT :

L'éditeur de stratégie windows NT présente au niveau **Utilisateur** :

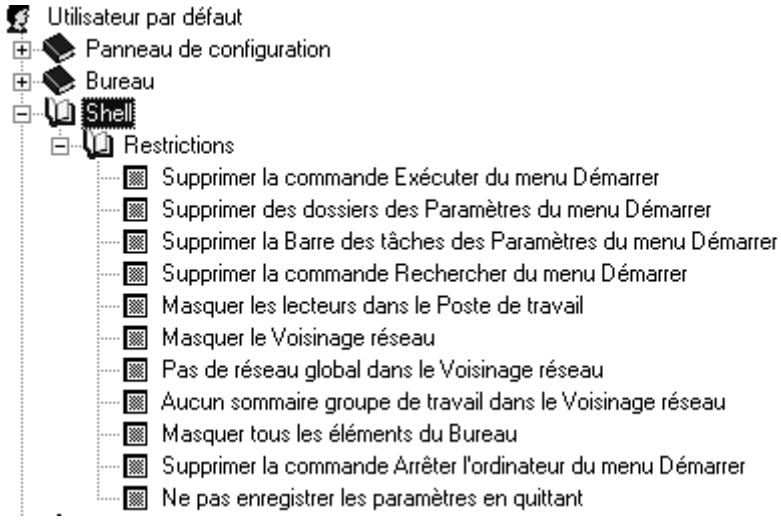
Panneau



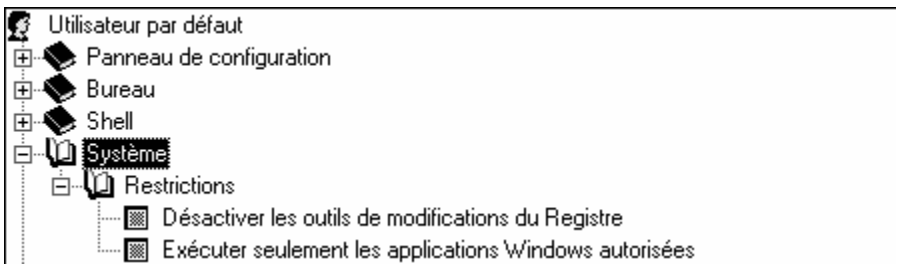
Bureau



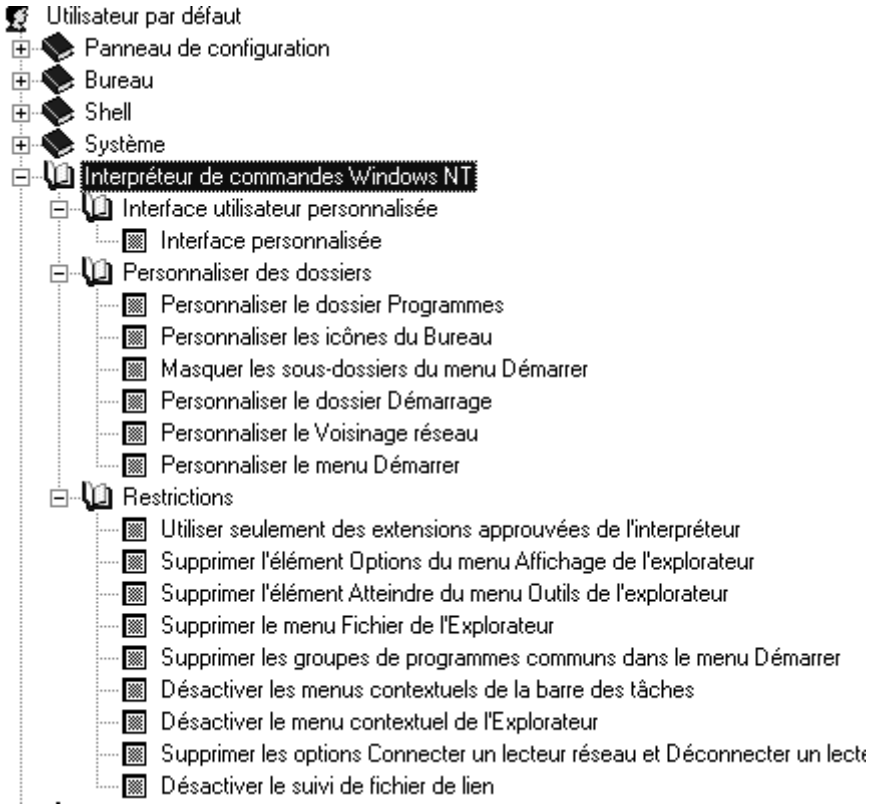
Shell



Système



Commande



Système NT