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

Centre Régional de CNAM

# WINDOWS NT 2000:
# Travaux Pratiques

## -S4-

Michel Cabaré

Juin 2003 ver 1.4

**CUEFA** - Département Formation Continue

BP 68

38402 ST MARTIN D'HÈRES

# TABLE DES MATIÈRES

# RESEAU « SIMPLE » MANUELLEMENT

**Objectifs et fonctionnalités :**

Il s'agit de présenter ici un réseau local, constitué d'un seul Domaine, On va essayer de faire le plus d'étapes manuellement… Le Serveur NT 2000 nommé **s1-man** et de clients tantôt Windows 95-98 nommés **win-man1**, **win-man2** tantôt NT 2000 professionnel nommés **win2k-1**, **win2k-2**

le protocole choisit est TCP/IP, Les adresse IP sont donnée manuellement avec **192.168.1.X** où X sera le n° de la machine sur laquelle on travaille, le masque de sous-réseau sera pour tous **255.255.255.0**

**N.B** : *pour se « mettre » en situation d'un Contrôleur nouvellement installé, il suffit d'exécuter **DCPROMO** pour rétrograder le serveur, en précisant bien qu'il s'agit du dernier contrôleur de Domaine, et de demander de désinstaller DHCP et DNS dans **Ajouter/supprimer des composants windows*** du panneau de configuration, en demandant 

*puis Détail et décocher DNS et éventuellement DHCP !*
*on peut finir le "ménage" en supprimant dans Winnt\system32\ le contenu des dossiers DNS et DHCP éventuels*

**Création du domaine manuel.net :**

**Démarrer/Exécuter** et tapez ensuite **dcpromo**. Dans l'« **l'assistant installation Active directory** » il faut alors répondre

1. Contrôleur de domaine pour un nouveau domaine
2. Créer une nouvelle arborescence de domaine
3. Créer une nouvelle forêt d'arborescence de domaines
4. Donner le nom DNS en **manuel.net**
5. Accepter le nom Netbios proposé , pour nous ici **manuel**
6. Choisir un emplacement pour les fichiers stockant Active Directory, comme **…\WINNT\NTDS** (accepter l'emplacement proposé)
7. indiquer le lecteur NTFS comme destination du dossier Sysvol de publication d'Active Directory **…\WINNT\SYSVOL**
8. lorsque l'assistant détecte que il n'y a pas de DNS disponible, **ne pas demander d'en créer un**
9. Autoriser la compatibilité avec les versions antérieures de NT
10. indiquer un mot de passe de restauration de service d'annuaire, par exemple **zk28a**

**Puis re démarrer le poste**

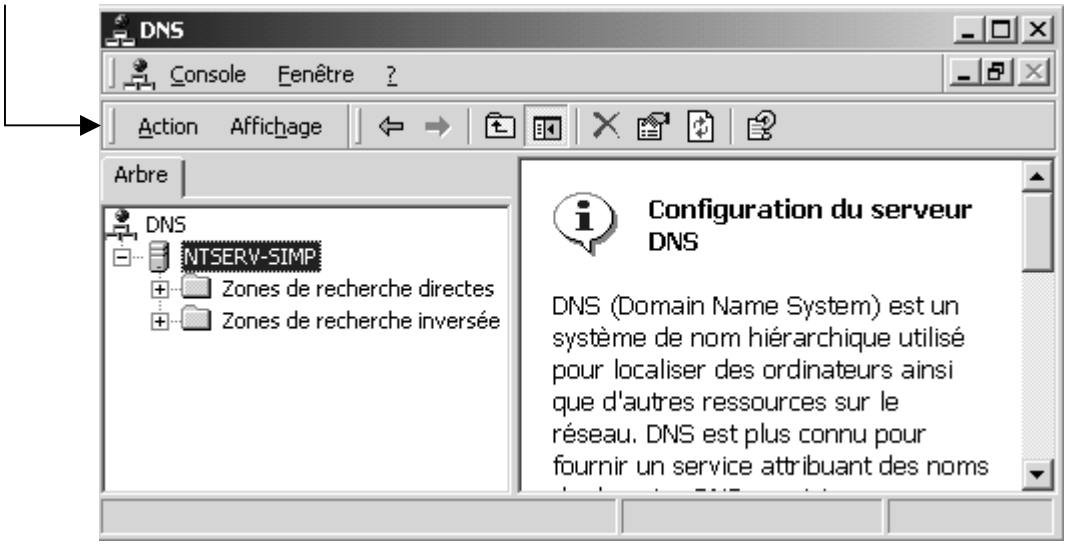
**Installation du serveur DNS :**

Pour installer un serveur DNS sur un serveur NT2000 Server il faut aller dans **Ajouter/supprimer des composants windows** du panneau de configuration, en demandant


puis Détail et cocher **DNS** ! (le CD est nécessaire)

**Configuration du serveur DNS :**

On a installé un serveur DNS ; reste à l'installer soit via l'assistant en se positionnant dessus (après avoir lancé la console d'administration DNS par **démarrer / programme / Outils d'administration / DNS** ) et en demandant le menu **Action / Configurer le serveur**




Dans les boites de « **l'assistant configuration de serveur DNS** » on réponds :

1. Ceci est le premier serveur DNS sur le réseau
2. Créer une zone de recherche directe
3. en Zone principale standard
4. donner le nom de la zone, ici pour nous **manuel.net**
5. accepter de créer le nouveau fichier **manuel.net.dns**
6. Créer une zone de recherche inversée
7. en Zone principale standard
8. avec un ID réseau de **210.200.200**
9. accepter de créer le nouveau fichier **210.200.200.in-addr.arpa.dns**

**Inscription du DC dans le serveur DNS :**

A l'heure actuelle on a un serveur 2000, C.D. et sur ce serveur 2000 on dispose d'un serveur DNS opérationnel

Il faut "inscrire tous les enregistrements SRV correpondant à mon domaine dans le DNS

Après s'être bien assuré que la zone accepte les mises à jours dynamiques,

Exemple ici pour une zone nommée dom1.com


on lance sur le serveur une commande

**net stop netlogon**

```
C:\>net stop netlogon
Le service Ouverture de session réseau s'arrête.
Le service Ouverture de session réseau a été arrêté.
```

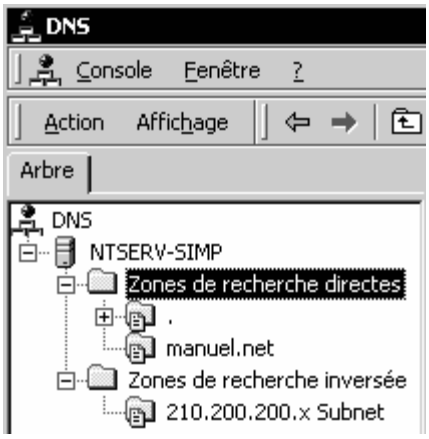
suivit de

**net start netlogon**

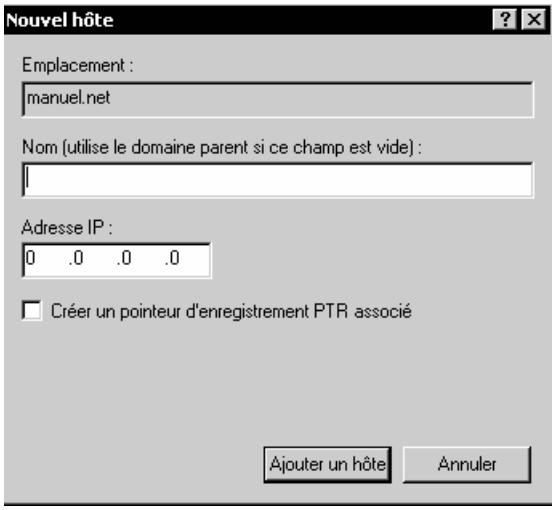
```
C:\>net start netlogon
Le service Ouverture de session réseau démarre.........
Le service Ouverture de session réseau a démarré.
```

## Ajouter les Hôtes et tester le serveur DNS :

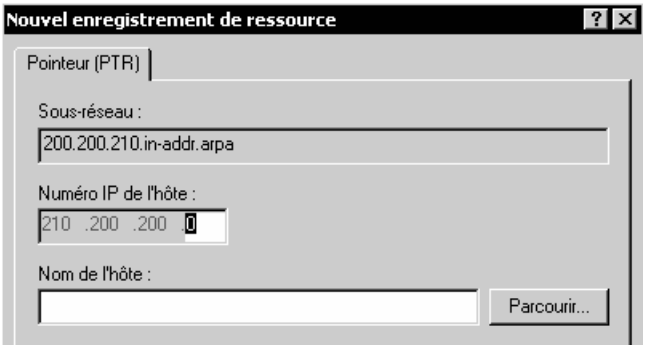
Se plaçant sur le zone de résolution crée, on demande soit




Pour une Zone de recherche Directe **Action/ nouvel hôte**




Pour une Zone de recherche inversée **Action/ nouveau pointeur**

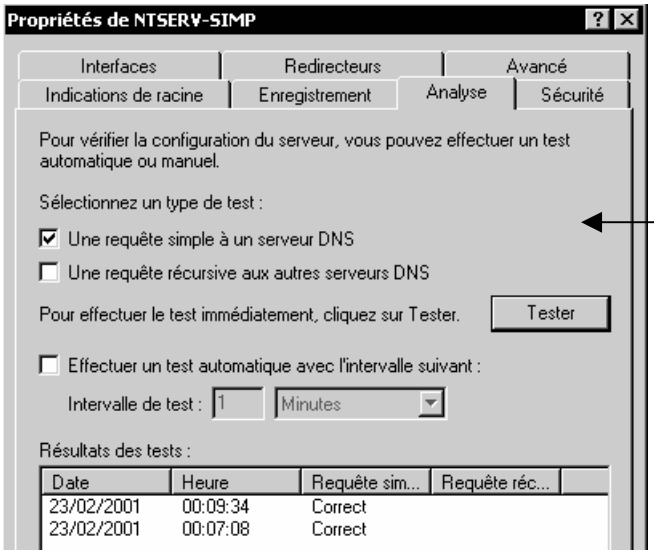


# TEST DE DNS

**Test DNS et Paramétrage TCP/IP des clients du domaine :**

Le paramétrage de l'adresse du serveur DNS sur les clients peut se tester via **IPCONFIG/ ALL** ou **Winipcfg**

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

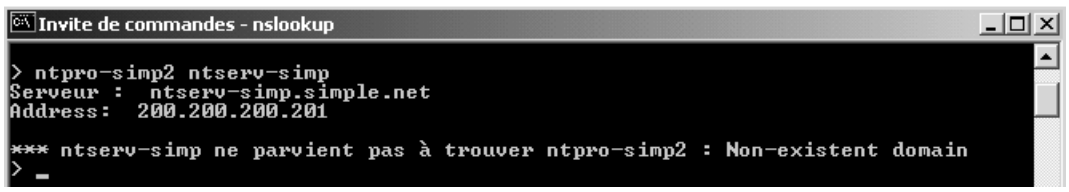

Onglet **Analyse**

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**

**nslookup :**

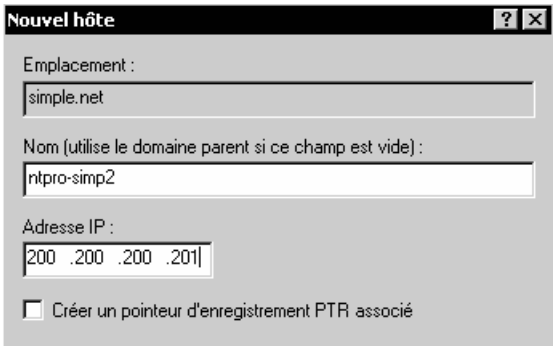
Par exemple on teste que le client nommé ntpro-simp2 d'adresse 200.200.200.202soit bien résolu sur notre serveur DNS **ntserv-simp**

Ici on ne trouve pas de résolution…

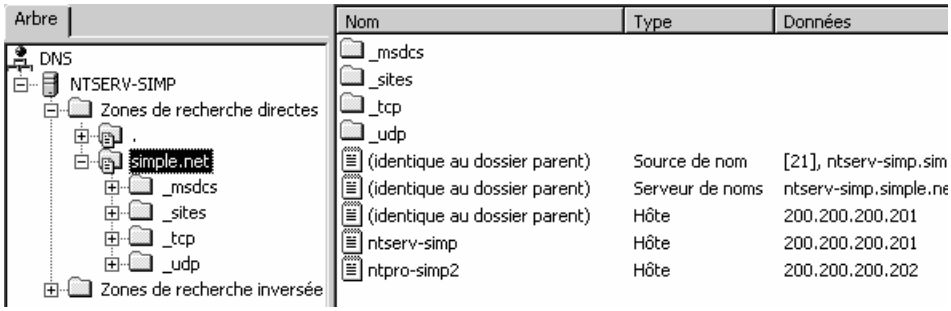


Normal, encore faut il :

1. dans le serveur DNS rentrer le poste dans la zone de recherche



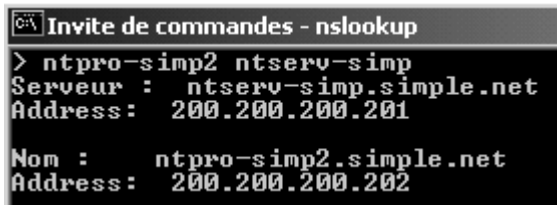

de manière à obtenir




2. préciser sur le client l'adresse du serveur DNS à contacter…

et lorsque l'on re-teste que le client nommé ntpro-simp2 d'adresse 200.200.200.202soit bien résolu sur notre serveur DNS ntserv-simp

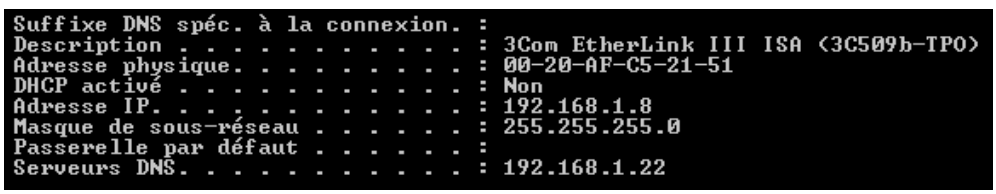
Cela marche !!!…



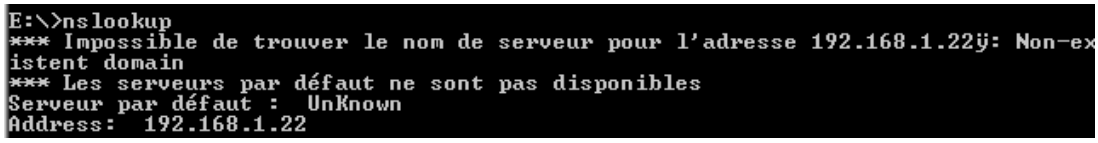

**Test de résolution inverse :**

La **résolution inverse** n'est pas nécessaire au fonctionnement des mécanismes 2000, et pourtant elle peut expliquer par exemple pour quoi on a un message d'erreur lorsque l'on lance nslookup…

Ainsi sur la machine ci dessous sur laquelle on a fait un **ipconfig /all**



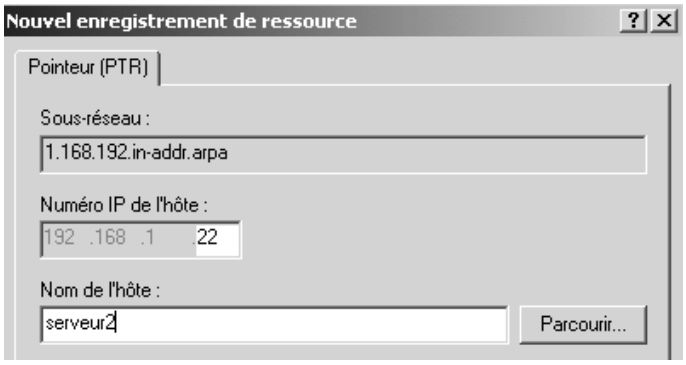

puis un **nslookup**, on obtient



pourquoi ?

parce que on essaye de faire un résolution inverse de l'adresse 192.168.1.22 qui est notée comme étant l'adresse du serveur DNS à interroger.

Pour que cela fonctionne, il faut sur le serveur DNS, se créer une zone de recherche inversée, et y rentrer ensuite



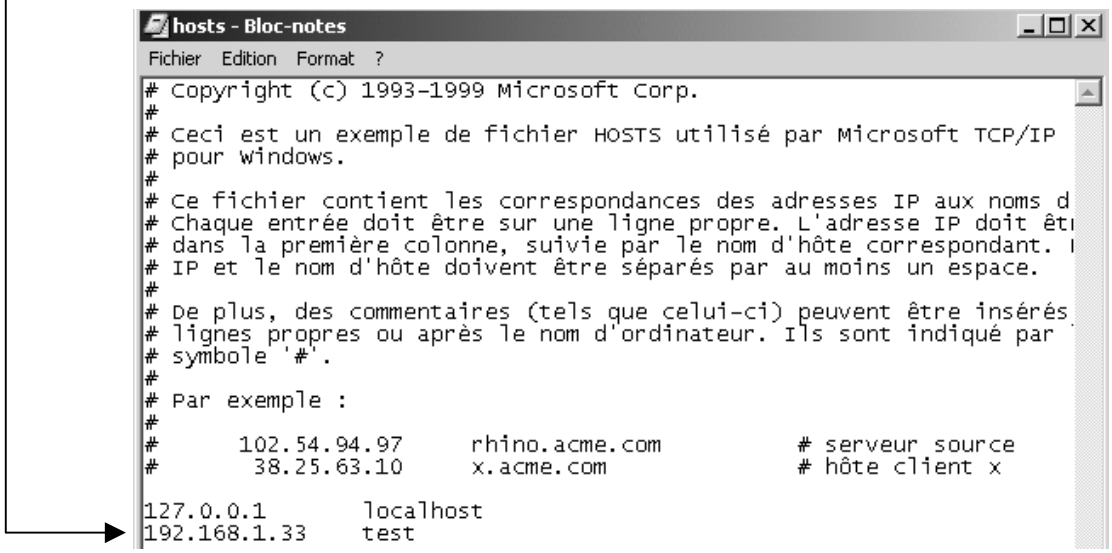

alors on pourra obtenir lors de l'appel à nslookup

# MODIFIER LE FICHIER HOSTS

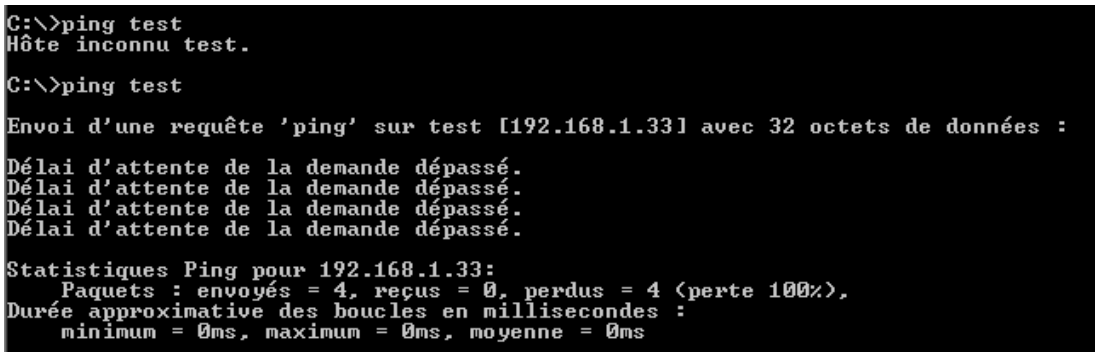
**Inscrire une machine dans hosts :**

Le fichier est fournit directement dans les postes 2000, ou avec une extension **.sam** sur les postes win98

Inscrivons le poste nommé **test** d'adresse **192.168.1.33** dans la table de résolution locale



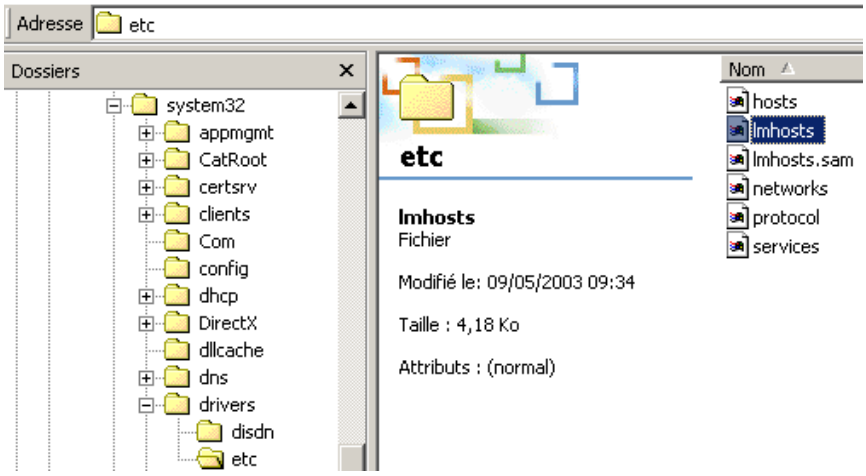

du coup si avant o n'avait aucune possibilité , on peut désormais au moins envoyer la trame…



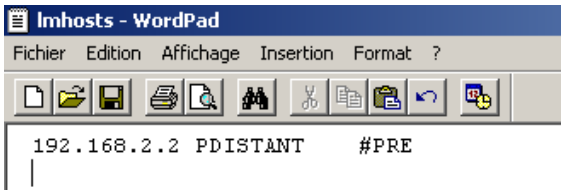
# MODIFIER LE FICHIER LMHOSTS

**Inscrire une machine simple dans lmhosts :**

Inscrivons le poste nommé **pdistant** d'adresse **192.168.2.2** dans la table préchargée de résolution de nom netbios d'une machine:




Il suffit d'éditer le fichier texte et d'y inscrire la ligne suivante




On recharge par la commande **nbtstat –R**

```
C:\>nbtstat -R
    Purge et préchargement de la table nom de cache distant NBT terminés.
```

et on visualise par la commande **nbtstat –c**:

```
C:\>nbtstat -c

Accton:
Adresse IP du noud : [192.168.1.30] ID d'étendue : []

                Table de nom de cache distant NetBIOS

      Nom               Type         Adresse d'hôte    Vie [sec]
    ---------------------------------------------------------------
    PDISTANT       <03>  UNIQUE          192.168.2.2          -1
    PDISTANT       <00>  UNIQUE          192.168.2.2          -1
    PDISTANT       <20>  UNIQUE          192.168.2.2          -1
```

**Inscrire un Contrôleur de Domaine dans lmhosts :**

En général, on n'a pas besoin d'inscrire des postes génériques, mais plutôt un contrôleur de domaine…

Dans ce cas la ligne se complique un petit peu puisqu'il est nécessaire d'indiquer le nom de domaine en plus….

Il faut effectuer donc 2 entrées, une pour le PDC et l'autre pour le nom de domaine.

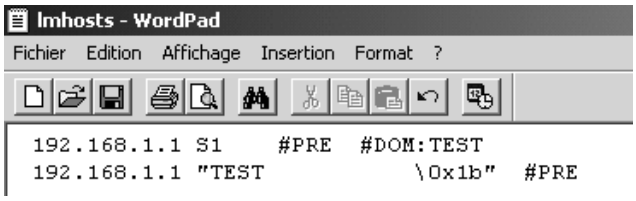
```
10.0.0.1   PDCName   #PRE #DOM:Domain-name
10.0.0.1   "Domain-name    \0x1b"   #PRE
```

**N.B** : Le nom de domaine dans cette entrée respecte la casse.

**N.B:** L'espacement de ces entrées est obligatoire.

Remplacez **10.0.0.1** par l'adresse IP de votre contrôleur principal de domaine,
**PDCName** par le nom NetBIOS de votre contrôleur principal de domaine,
**Domain** par le nom de domaine de Windows NT.

Inscrivons le contrôleur de domaine **TEST** nommé **S1** d'adresse **192.168.1.1** dans la table préchargée de résolution de nom netbios d'une machine:




avec pour vérification


**NB**: Au total il doit y avoir 20 caractères à l'intérieur des guillemets
(le nom de domaine, +
le nombre d'espaces appropriés pour obtenir 15 caractères, +
la barre oblique inverse, +
la représentation hexadécimale NetBIOS du type de service).

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

Ainsi une simple erreur de nombre de caractère (différent de 20 ici)

```
192.168.1.1 S1     #PRE   #DOM:TEST
192.168.1.1 "TEST              \0x1b"       #PRE
```

ne génère aucun message d'erreur, mais simplement une mauvaise inscription :

```
C:\>nbtstat -c

Accton:
Adresse IP du noud : [192.168.1.2] ID d'étendue : []

                Table de nom de cache distant NetBIOS

        Nom               Type         Adresse d'hôte   Vie [sec]
    ---------------------------------------------------------------
    S1             <03>  UNIQUE          192.168.1.1          -1
    S1             <00>  UNIQUE          192.168.1.1          -1
    S1             <20>  UNIQUE          192.168.1.1          -1
    TEST           <1C>  GROUP           192.168.1.1          -1
    TEST           <03>  UNIQUE          192.168.1.1          -1
    TEST           <00>  UNIQUE          192.168.1.1          -1
    TEST           <20>  UNIQUE          192.168.1.1          -1
```

# TEST INSTALLATION DE AD

**Vérification configuration IP:**

Au niveau IP, Il faut que le paramétrage serveur DNS soit configuré pour pointer vers lui-même… avec 127.0.0.1

Si ce n'est pas le cas, rafraîchir le cache avec la commande

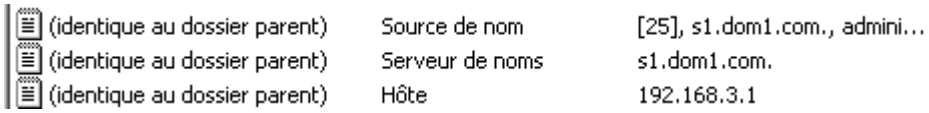
**ipconfig /flushdns**

```
C:\>ipconfig /flushdns

Configuration IP de Windows 2000

Cache de résolution DNS vidé.
```

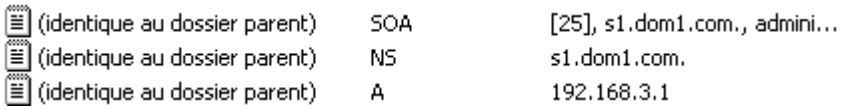
suivie de la commande **ipconfig /registerdns**

```
C:\>ipconfig /registerdns

Configuration IP de Windows 2000

L'inscription des enregistrements de ressource pour toutes les cartes de cet ord
inateur a été initiée. Toute erreur sera signalée dans l'Observateur d'événement
s dans 15 minutes.
```

dans la console DNS on doit voire 3 enregistrement minimum…un Hôte pour le nom du serveur, un serveurs de nom et un source de nom.




en affichage détaillé cela donnerait




**Vérification des enregistrement de ressource SRV**

On regarde si les 4 dossiers suivants on été crées dans la zone DNS principale


et on liste les enregistrements de type SRV par un commande nslookup avec

**ls –t SRV domaine**

voire si on veut en garder une trace dans un fichier

**ls –t SRV domaine >nomfich**

et on peut décrypter un peu les enregistrement SRV à l'aide des informations suivantes

| Enregistrement SRV | Critères de recherche |
|---|---|
| **ldap._tcp.***Domaine_DNS.* | Permet à un ordinateur de trouver un serveur LDAP dans le domaine |
| **_ldap._tcp.***Site.***_sites.dc._msdcs.***Domaine_DNS.* | Permet à un ordinateur de trouver un contrôleur de domaine sur le même site |
| **_gc._tcp.***Forêt_DNS.* | Permet à un ordinateur de trouver un serveur de catalogue global |
| **_gc._tcp.***Site.***_sites.***Forêt_DNS* | Permet à un ordinateur de trouver un serveur de catalogue global sur le même site |
| **_kerberos._tcp.***Domaine_DNS.* | Permet à un ordinateur de trouver un serveur KDC dans le domaine |
| **_kerberos._tcp.***Site.***_sites.***Domaine_DNS.* | Permet à un ordinateur de trouver un serveur KDC sur le même site |

- **Les contrôleurs de domaine exécutant Windows 2000 inscrivent d'autres enregistrements SRV dans le sous-domaine _msdcs au format :**

  *_Service._Protocole.DcType.***_msdcs.***Domaine_DNS*

DcType pouvant valoir :

**dc** pour Domain Controller

**gc** pour Global Catalog

pour reconstruire la liste des enregistrement correspondant à AD dans le DNS on peut, après s'être bien assuré que la zone accepte les mises à jours dynamiques,

Exemple ici pour une zone nommée dom1.com


on lance sur le serveur une commande

**net stop netlogon**

```
C:\>net stop netlogon
Le service Ouverture de session réseau s'arrête.
Le service Ouverture de session réseau a été arrêté.
```

suivit de

**net start netlogon**

```
C:\>net start netlogon
Le service Ouverture de session réseau démarre.........
Le service Ouverture de session réseau a démarré.
```

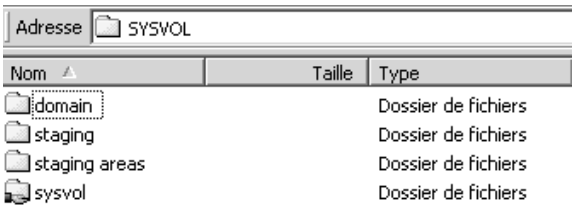
**N.B:** si le pb persiste on supprime la zone , puis on la recrée…

## Vérification du dossier SYSVOL

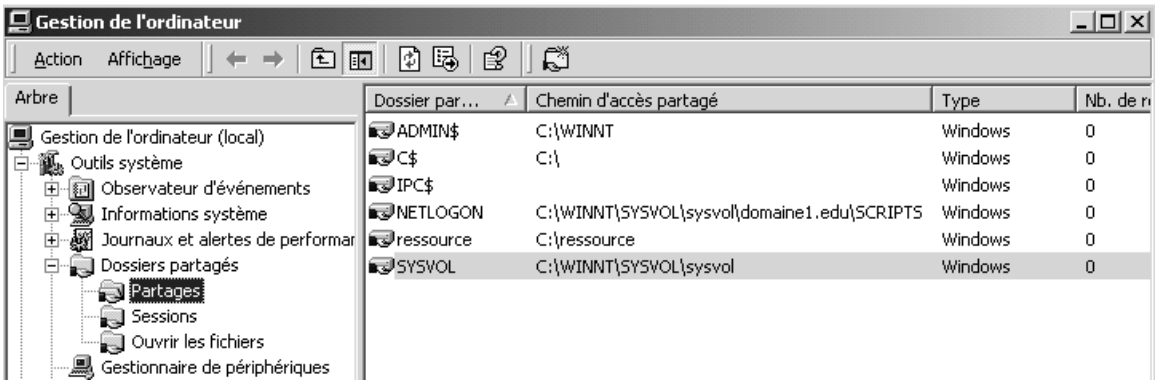
Pour vérifier que le dossier SYSVOL à bien été crée il faut regarder si dans le dossier principal de NT on trouve le dossier **sysvol**….

Ce qui peut aussi se faire plus rapidement via


dans lequel on doit trouver les 4 sous dossier suivants




La vérification du partage peut se faire rapidement via

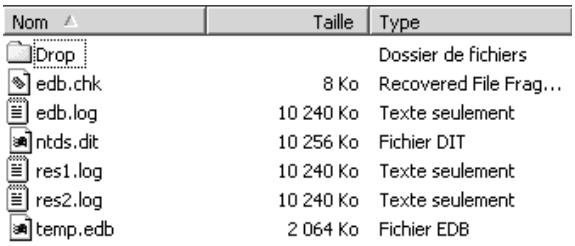



## Vérification de la base de donnée d'annuaire et des fichiers journaux

Pour vérifier que la base de donnée à bien été crée il faut regarder si dans le dossier principal de NT on trouve le dossier **ntds**….

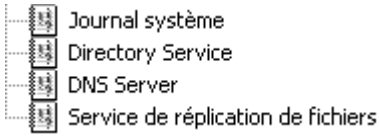
Ce qui peut aussi se faire plus rapidement via


comprenant les fichiers suivants




## Vérification des journaux d'événement

Essentiellement les 4 suivants



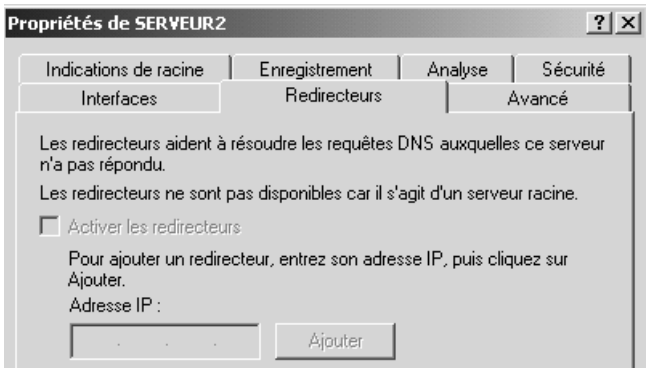
# ACCES A INTERNET

**Après installation d'un serveur DNS :**

Si vous installez DNS au cours du processus dcpromo, vous obtiendrez une zone racine. Celle-ci indique à votre serveur DNS qu'il est un serveur Internet racine. Par conséquent, votre serveur DNS n'utilisera pas de redirecteurs ou d'indications de racine lors du processus de résolution de noms.

Ce qui pour aller sur internet risque de poser probleme.

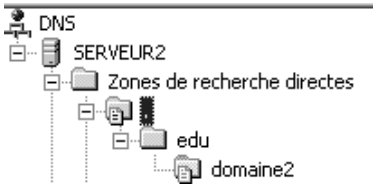
on ne peut pas spécifier les redirecteurs (ils sont grisés)



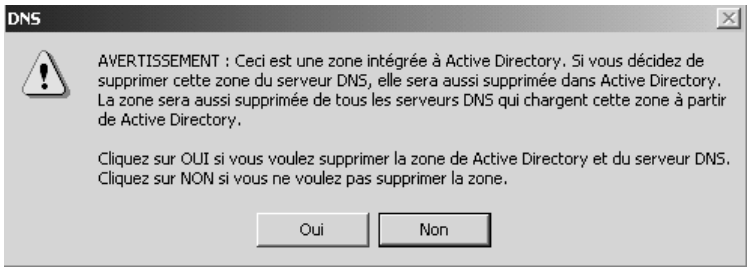

**Suppression de la zone DNS racine**

Dans le Gestionnaire du DNS, développez l'objet **Serveur DNS** Développez le dossier **Zones de recherche directe**.

Cliquez avec le bouton droit sur la zone **" . "**, puis demandez **Supprimer**.




Le serveur DNS va demander confirmation sur une action qui est irreversible



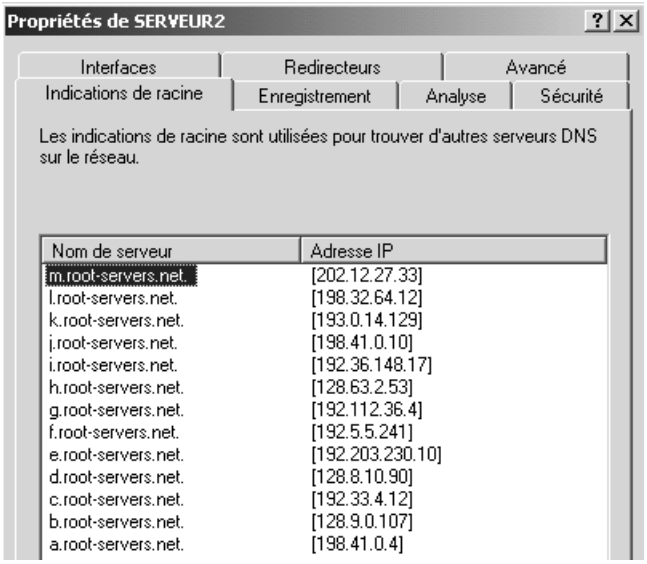

**N.B**: il faut bien penser à faire **F5** pour que le DNS soit réactualisé !

## Utilisation des indications de racine

A partir du moment ou la zone racine n'existe plus , les indications de racine sont utilisables par notre serveur DNS

Avantage : on est standard, et on de dépends pas des DNS du FAI

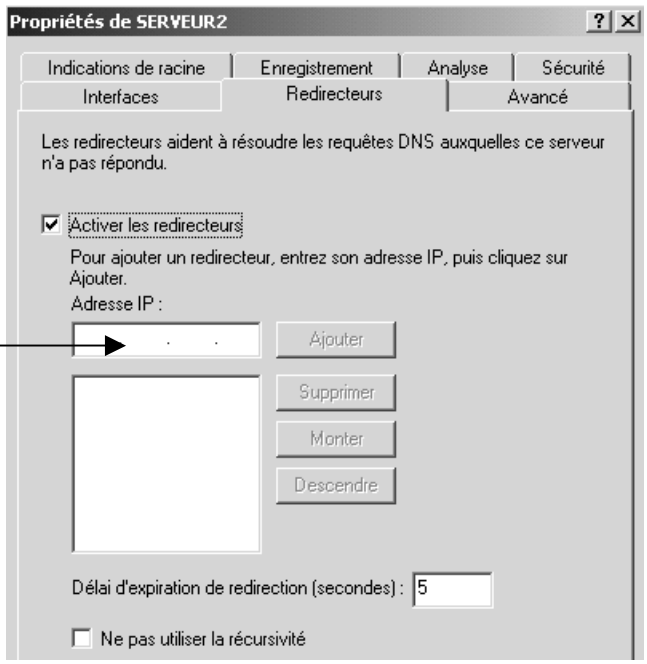
Inconvénient : cela génère un fort traffic




## Utilisation des redirecteurs

A partir du moment ou la zone racine n'existe plus , les redirecteurs sont utilisables

Il faut indiquer ceux du FAI ...




**N.B:** Attention, pour éviter les prises de lignes intempestives par le DNS, il est préférable utiliser les redirecteurs pointant vers les DNS du FAI, supprimer les indications de racine et lire l'article **F246804** de la Base de connaissance pour limiter les connexions du serveur DNS dynamique de windows !

## Indication de la passerelle à utiliser

Bien sûr les clients indiques comme serveur DNS le serveur 2000 et pas celui du FAI...

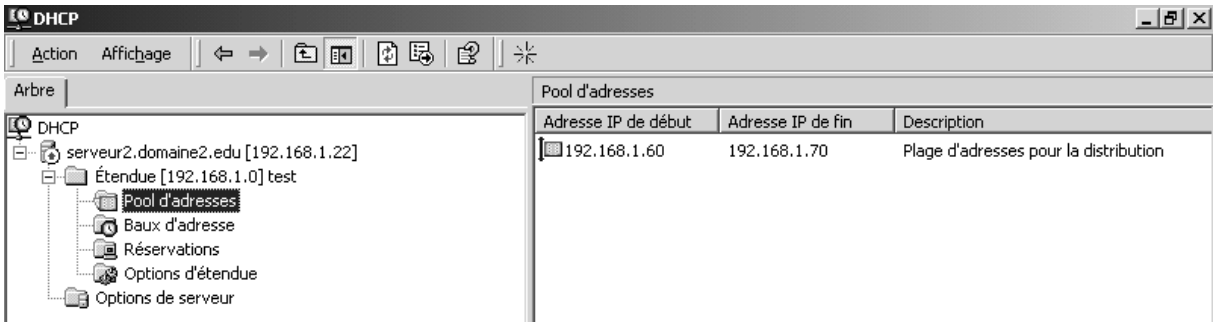
Bien sûr, que ce soit sur le serveur DNS ou les clients, il ne faut pas oublier d'indiquer en paramètres TCP/IP l'adresse du routeur que l'on prendra pour sortir physiquement....

# MISE EN ŒUVRE DHCP

**Installation d'un serveur DHCP :**

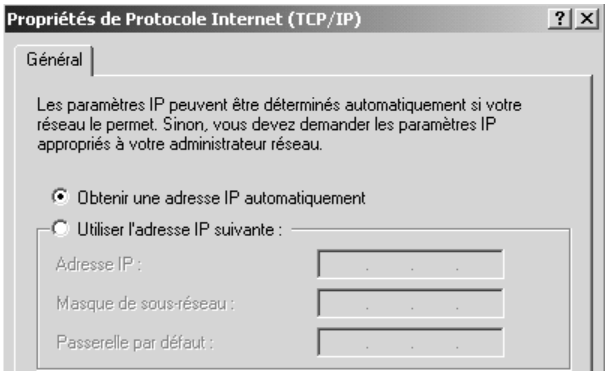
Installons sur le serveur 2000 un serveur DHCP distribuant des adresses comprises entre 192.168.1.60 et 192.168.1.70

Dans un premier temps, par de paramètres options de serveur…




activons l'étendue, puis le serveur DHCP

Vérifions si sur le client on récupère bien une adresse IP dynamiquement…

On demande donc 


Et on obtient **Adresse IP** et **Serveur DHCP**…ainsi que le **Bail**


Pour libérer une adresse on peut faire **IPCONFIG / RELEASE**… voire **/RENEW**

**Sécuriser un serveur DHCP :**

Je souhaite que n'importe qu'elle machine ne puisse plus récupérer une adresse ip au hasard. Par conséquent on va mettre en place une réservation d'adresse basée sur les adresses mac des clients que je pense avoir a terme.

Pour connaître l'adresse mac d'une machine, si je peux l'atteindre par un ping, la commande en ligne

**arp –a**

me donnera son adresse mac

Il ne me reste plus qu'a créer des reservation avec ces adresses.

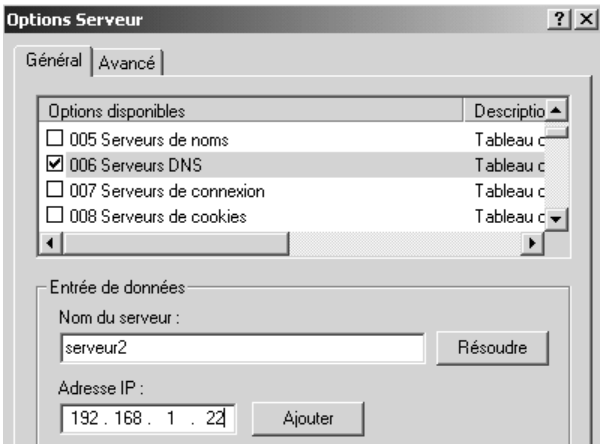
**Augmenter les sauvegardes automatique serveur DHCP :**

Modifier la clé de la base de registre afin que les sauvegardes s'effectuent de manière automatique toutes les 20 minutes (14 en hexa) au lieu de toutes les heures comme cela est prévu par défaut.

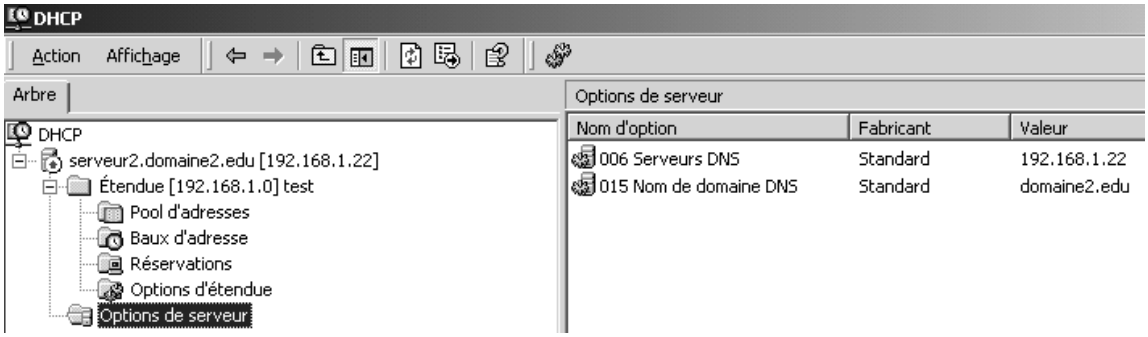
# MISE EN ŒUVRE DDNS

**Paramétrage d'un serveur DHCP :**

Il faut rajouter dans les options de serveur, l'adresse du serveur DHCP que l'on souhaite fournir aux clients DHCP…

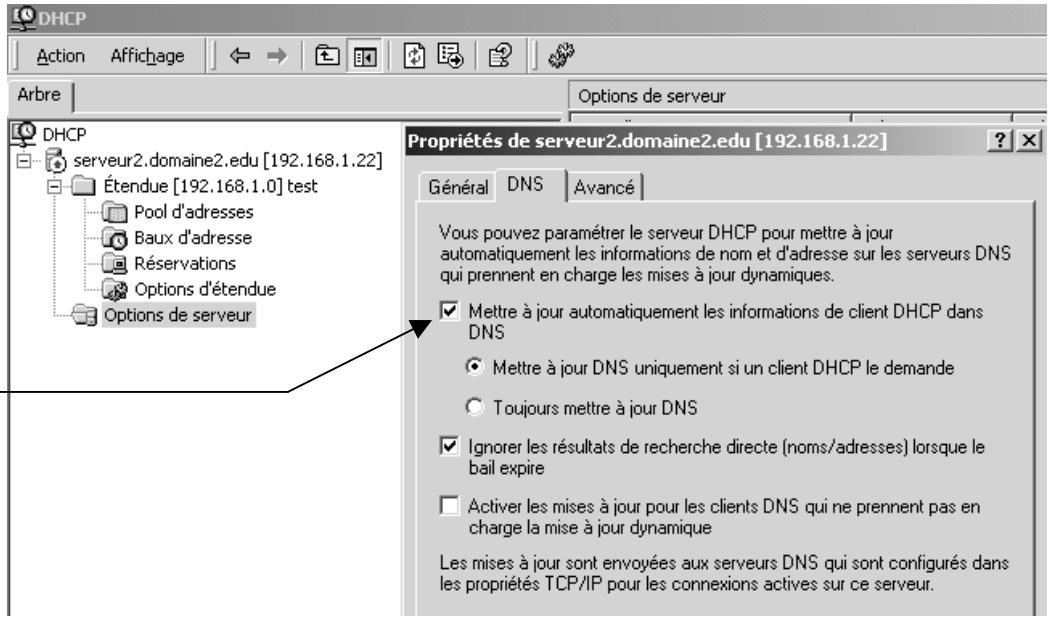



De manière à avoir



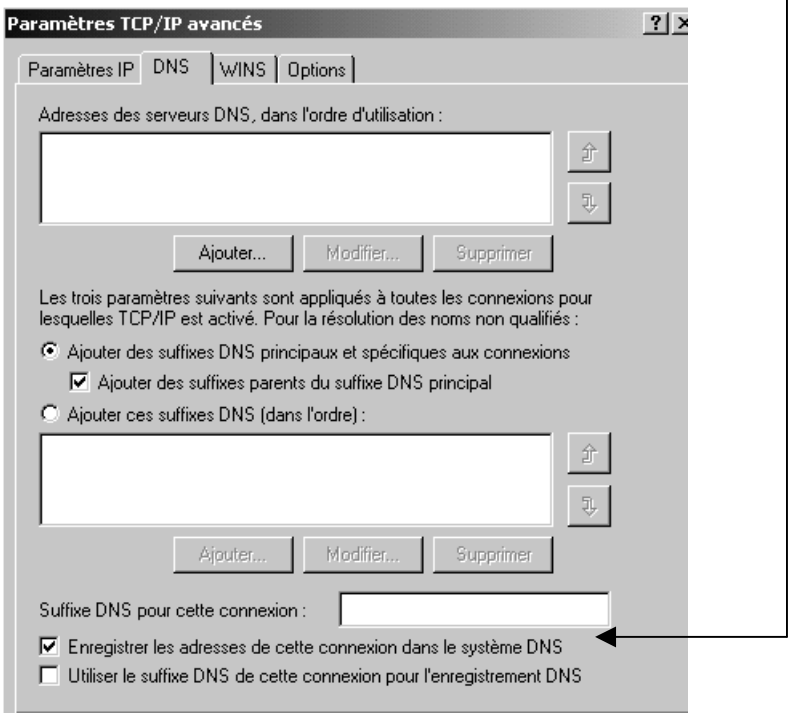

Puis il faut vérifier que les propriétés de ce serveur DHCP soient

Pour des clients 2000



**Paramétrage d'un client 2000 :**

Dans les propriétés avancées de TCP/IP, vérifier que l'on a




Ce qui fait que lorsque sur ce client on fait **IPCONFIG /RELEASE** on a

```
thernet carte Connexion au réseau local :

        Suffixe DNS spéc. à la connexion. :
        Description . . . . . . . . . . . : 3Com EtherLink III ISA (3C509b-TPO)
        Adresse physique. . . . . . . . . : 00-20-AF-C5-21-51
        DHCP activé . . . . . . . . . . . : Oui
        Autoconfiguration activée . . . . : Oui
        Adresse IP. . . . . . . . . . . . : 0.0.0.0
        Masque de sous-réseau . . . . . . : 0.0.0.0
        Passerelle par défaut . . . . . . :
        Serveur DHCP. . . . . . . . . . . : 255.255.255.255
        Serveurs DNS. . . . . . . . . . . :
```

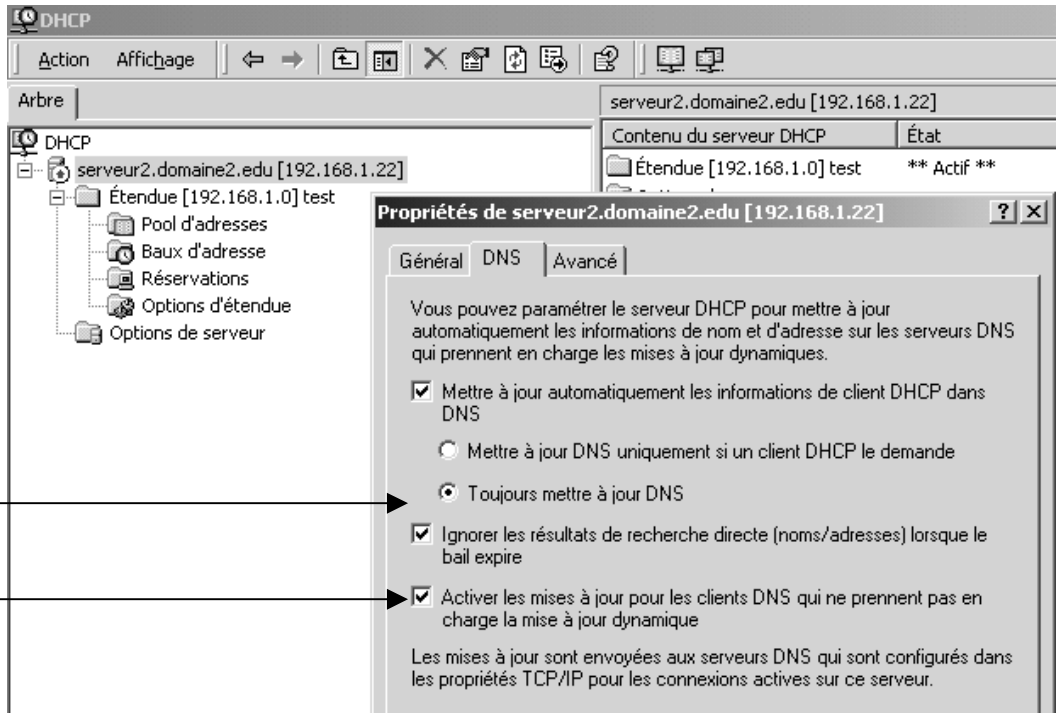
avec un **IPCONFIG /RENEW** on obtient

```
thernet carte Connexion au réseau local :

        Suffixe DNS spéc. à la connexion. : domaine2.edu
        Description . . . . . . . . . . . : 3Com EtherLink III ISA (3C509b-TPO)
        Adresse physique. . . . . . . . . : 00-20-AF-C5-21-51
        DHCP activé . . . . . . . . . . . : Oui
        Autoconfiguration activée . . . . : Oui
        Adresse IP. . . . . . . . . . . . : 192.168.1.60
        Masque de sous-réseau . . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . . :
        Serveur DHCP. . . . . . . . . . . : 192.168.1.22
        Serveurs DNS. . . . . . . . . . . : 192.168.1.22
        Bail obtenu . . . . . . . . . . . : mardi 4 juin 2002 01:31:47
        Bail expire . . . . . . . . . . . : mercredi 12 juin 2002 01:31:47
```

et surtout **l'enregistrement correspondant et crée dans le DNS…**

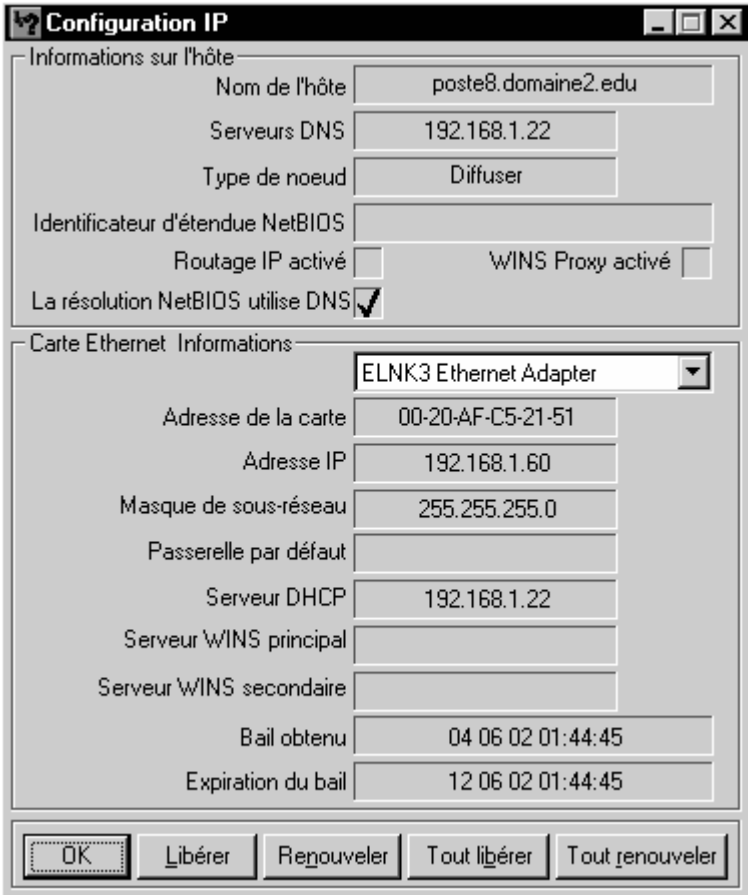
**Paramétrage d'un client non 2000 :**

Peu de modification, a dire vrai, vérifier que les propriétés de ce serveur DHCP soient




Pour des clients autres que 2000

et sur un client windows 98 on obtient par exemple



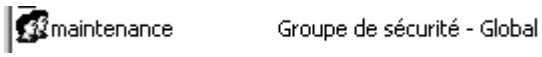

et surtout **l'enregistrement correspondant et crée dans le DNS…**

# PUBLICATION RESTREINTE DANS AD

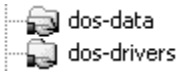
**Objectif :**

Dans un domaine, on souhaite faire que seuls les membre du groupe d'utilisateur "**maintenance**" puisse accéder à des ressources partagées avec le mot clé "**pilote**"…

On crée un groupe de sécurité global d'utilisateurs nommé **maintenance** à l'intérieur duquel on placera par exemple un utilisateur **bob**.



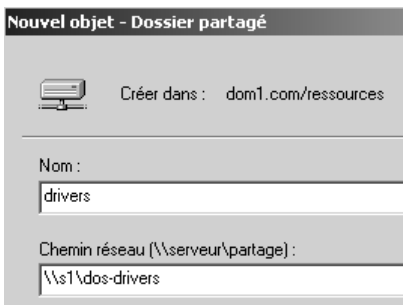

On partage 2 dossiers, un sous l'appellation **dos-drivers**, l'autre sous l'appellation **dos-data**, en imaginant que le premier contienne des sources de drivers, et le deuxième des données….

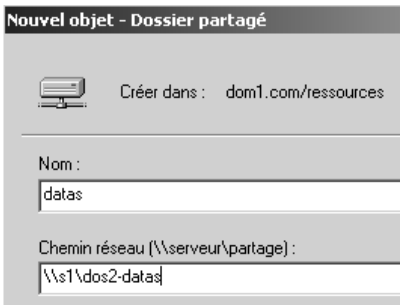



**N.B:** ces dossiers peuvent se trouver physiquement n'importe où dans mon domaine…

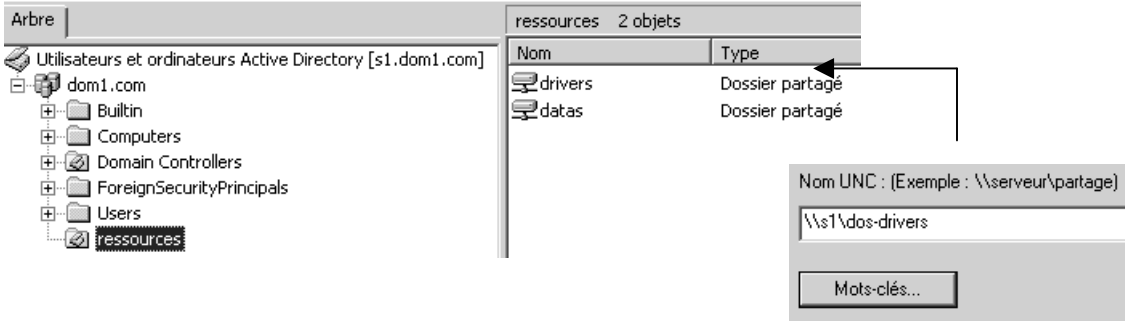
**Publication sélective dans A.D. :**

Pour publier ces dossiers dans AD on se place dons dans la mmc **Utilisateurs et ordinateurs Active Directory** et on crée une UO nommée par exemple **ressources** contenant mes 2 dossiers partagés



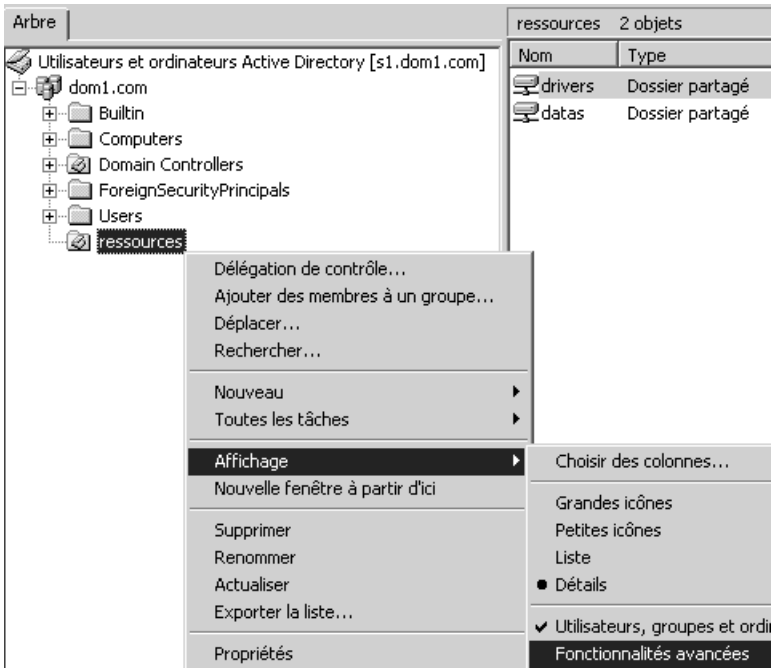




donc on obtient

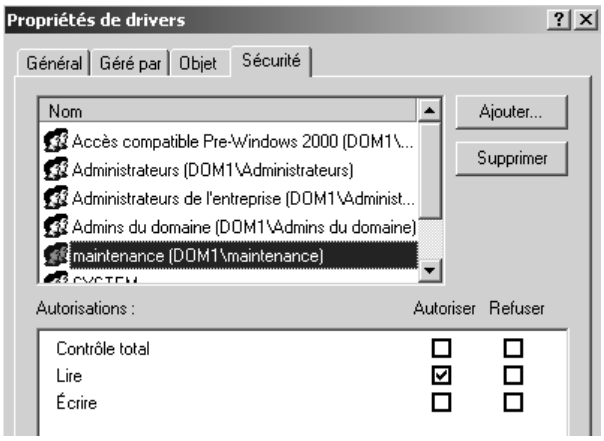



et on ajoute au dossier partagé drivers le mot clé "pilote"…

Pour modifier les permissions de sécurité des objets publiés, il est nécessaire de demander **Affichage / fonctionnalités avancées**




A partir de là on accède à l'onglet **Sécurité**



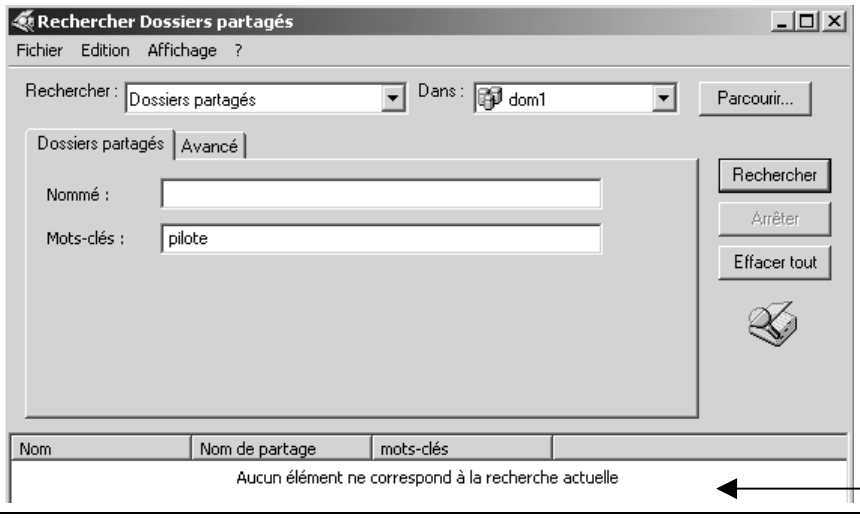

On y ajoute le groupe **maintenance**…

Et on supprime le groupe **Utilisateurs authentifiés**…

---

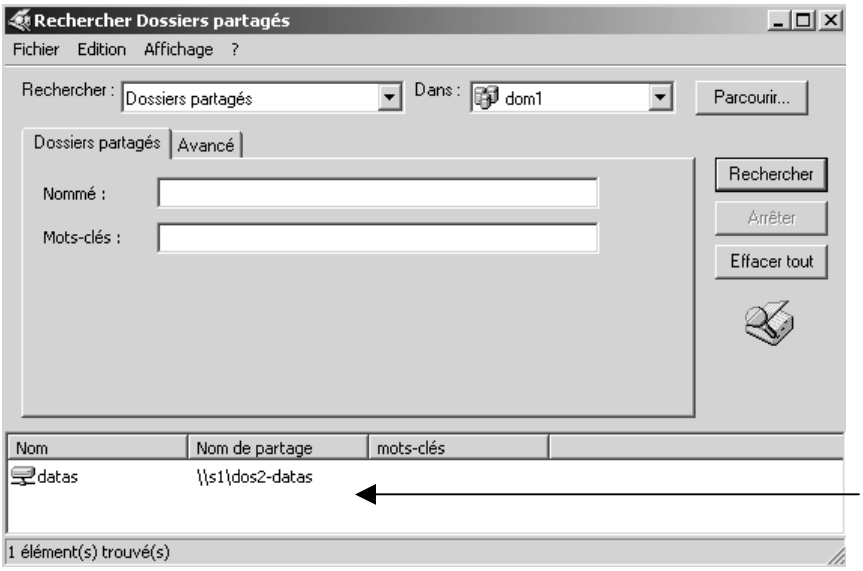
**Recherche de dossiers partagés :**

- Si un utilisateur simple (non membre du groupe maintenance) fait une recherche dans AD de tous les dossiers partagés avec le mot clé pilote…



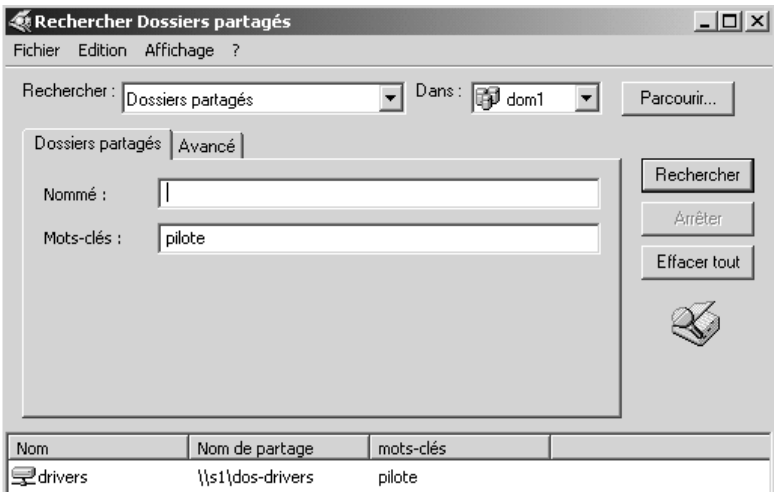

La recherche n'aboutit pas

- Si ce même utilisateur simple (non membre du groupe maintenance) fait une recherche dans AD de tous les dossiers partagés …

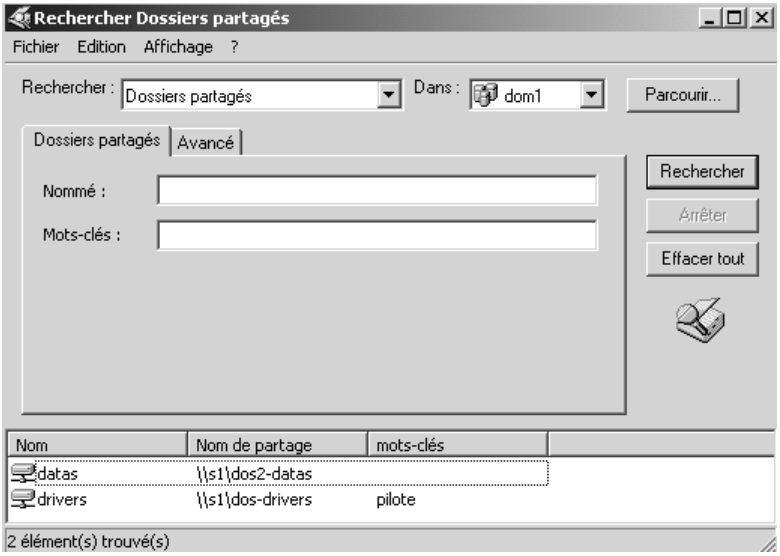



Seul le dossier datas paraît, La recherche n'aboutit pas pour drivers…

- Si bob, (membre du groupe maintenance) fait une recherche dans AD de tous les dossiers partagés avec le mot clé pilote…




- Si bob, (membre du groupe maintenance) fait une recherche dans AD de tous les dossiers partagés …



# DELEGATION COMPETENCE SUR UO

**Objectif :**

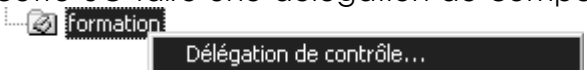
Dans un domaine, on souhaite faire que le service « **formation** », soit autonome quant à la gestion de ses utilisateurs, postes etc

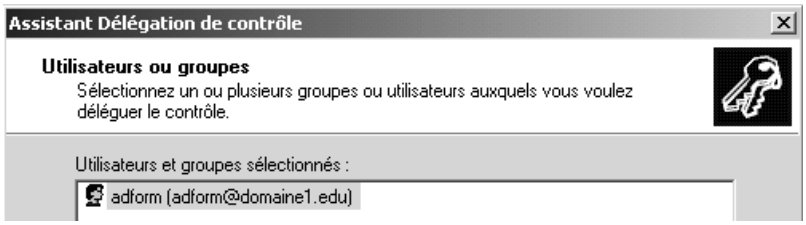
L'idée est de créer une OU sur laquelle on effectuera une délégation de compétence pour un compte particulier, nommé **adform**…

**Mise en place délégation :**

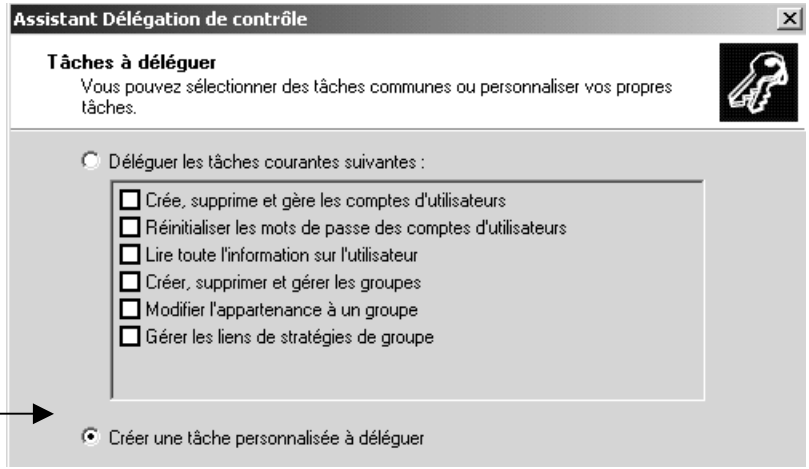
On va créer une UO **formation**, contenant un utilisateur **adform**,

puis on va pour cette UO faire une délégation de compétence complète à cet utilisateur…

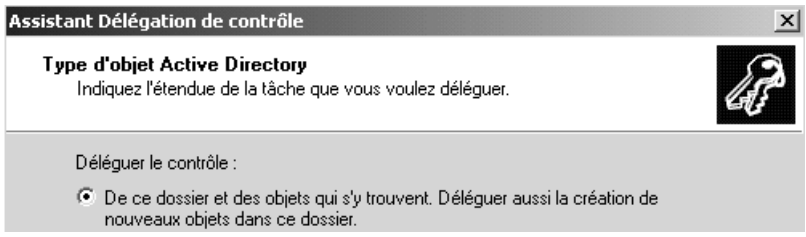


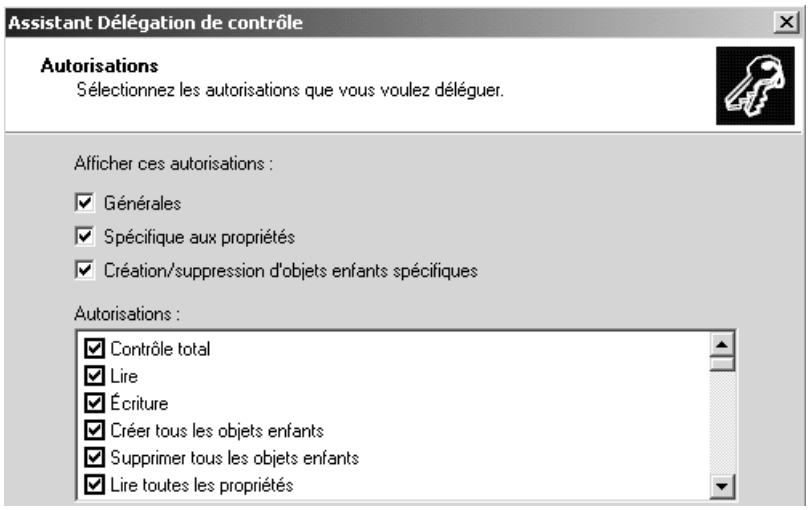

On veut « plus » que cela donc



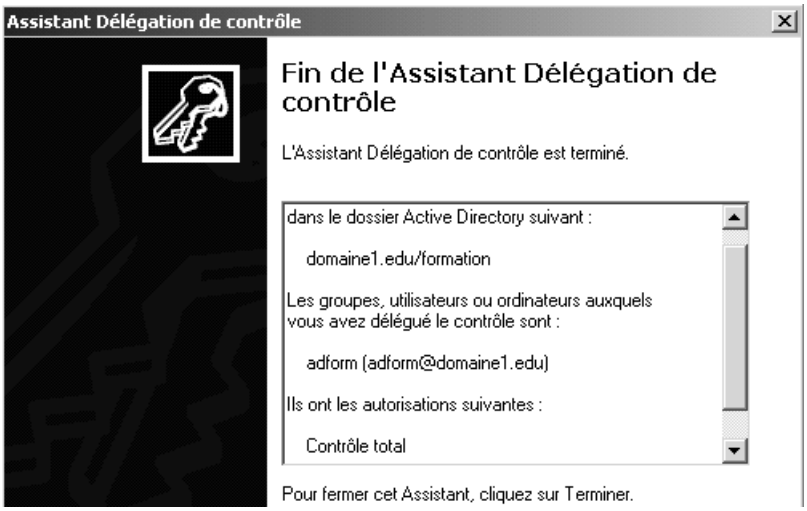

Délégation totale sur cette UO



En contrôle total




Ce que nous confirme l'assistant




**Utilisation de la délégation :**

Pour voir si cela fonctionne, il faut essayer d'administrer cette OU en tant qu'utilisateur **adform**.

Mais cet utilisateur n'est qu'un utilisateur classique au niveau des groupes de domaine, donc il ne peut pas ouvrir de session sur le CD. On peut soit modifier les stratégies de Contrôleur de Domaine pour lui permettre d'ouvrir une session locale sur le serveur (déconseillé) soit lui installer les outils d'administrations à distance sur son poste (mieux).

**N.B** : le fichier permettant l'installation des outils d'Administration, est stocké dans le CD de distribution 2000 serveur, dans i386... (fichier **Adminpak.msi)**

Depuis un client, et connecté en tant que **adform**, on lance la console **Utilisateurs et ordinateurs Active Directory**, on n'a d'action possible que sur l'UO **formation** …

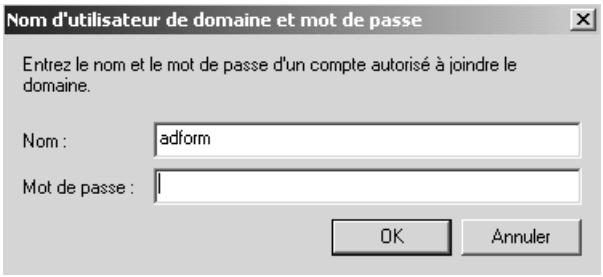
Ajoutons deux stagiaires **stg1** et **stg2**, (sans mot de passe) dans l'UO formation, cela est possible sans problèmes

Et un compte ordinateur **clientform** placé dans notre UO formation

Rattachons un nouveau poste nommé **clientform** (donc actuellement membre d'un workgroup) au domaine….

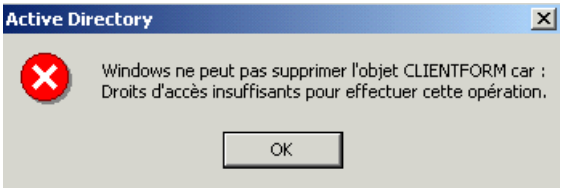

Il suffit après une ouverture de session locale en tant qu'administrateur du poste, de demander un rattachement domaine

en donnant comme identificateur le compte que l'on à crée comme administrateur de notre UO , c'est à dire **adform**




**N.B** : Si l'utilisateur **adform**, ne crée pas un compte ordinateur au préalable dans son UO formation, il pourra rattacher la station au domaine (a condition bine sur que l'enregistrement hôte ait été crée dans le dns…), et le compte ordinateur (crée au préalable dans le dns) ira se ranger dans le conteneur d'AD prévu par défaut à cet effet, c'est à dire **computers**…

Mais là, toute tentative de gestion de ce compte machine par notre **adform** se soldera par un échec, car ses droits sont limités a son UO **formation** !



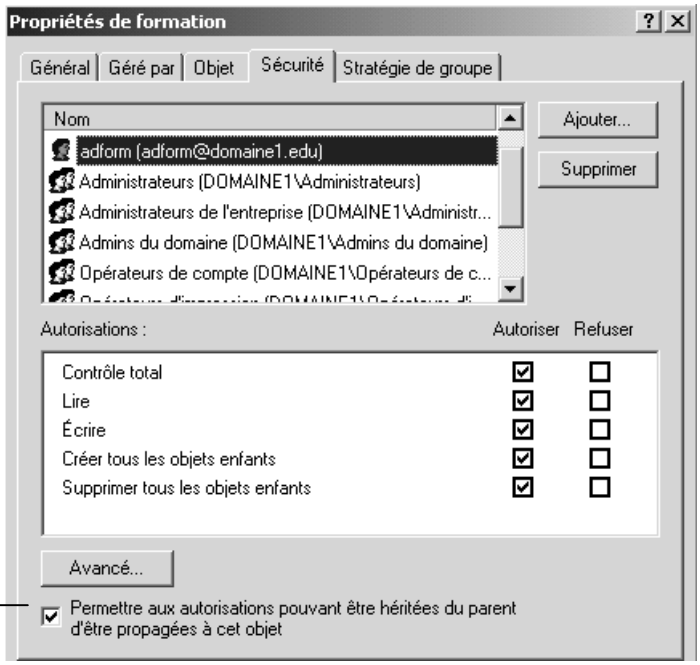

**Ajouter une délégation :**

On réutilise l'assistant de délégation

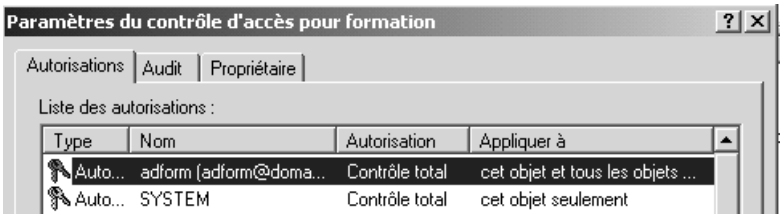
**Modifier-Supprimer une délégation :**

Il faut accéder aux propriétés de l'objet AD sur lequel la délégation à été faite. Seul le propriétaire de l'objet peut le faire.

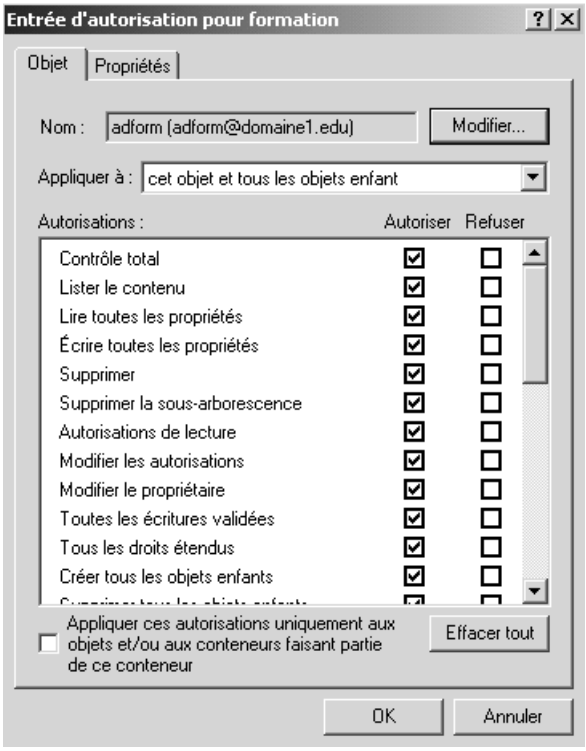
On demande les propriétés de l'UO **formation**, onglet **sécurité**




Puis si nécessaire **Avancé**




voire **Afficher/Modifier**

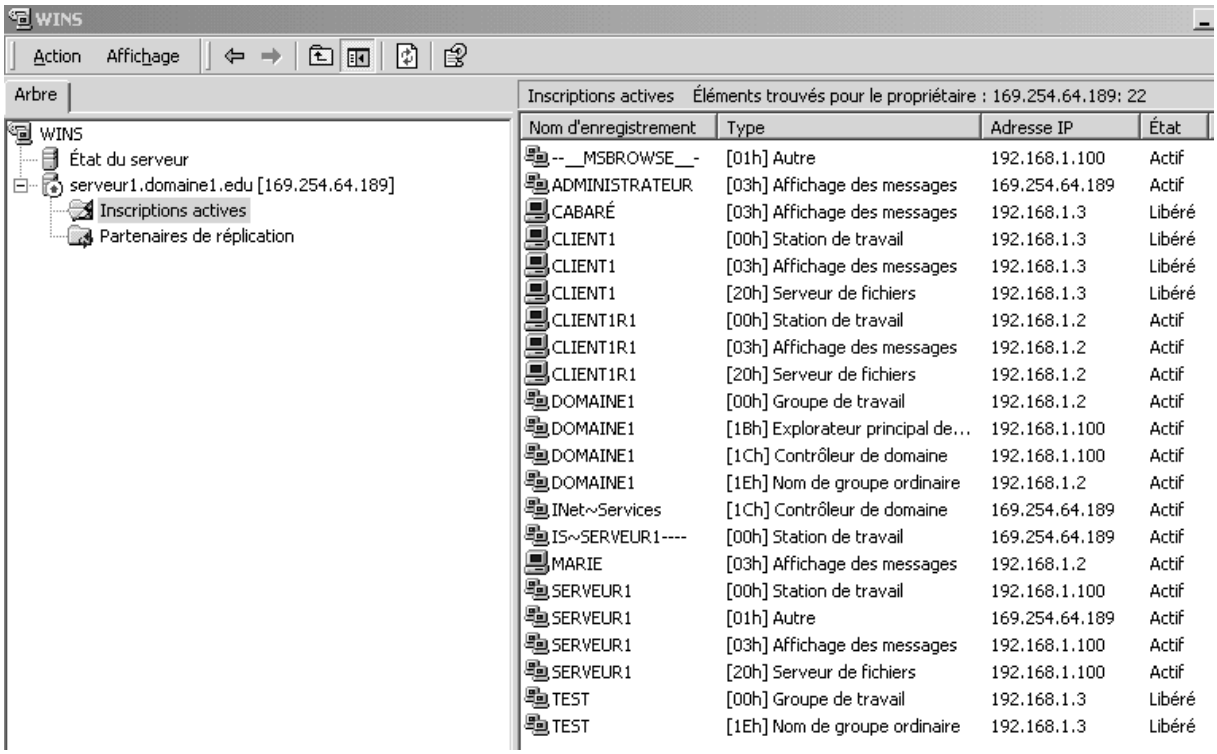


# COMMANDE NET SEND…

**La base de la commande Net send :**

Cette commande utilise des **noms netbios**… (le 16° caractère spécifie la nature du nom 03h affichage des messages…)

Que se passe-t-il si l'administrateur à ouvert une session sur le serveur est sur un client ? à qui sera envoyé le net send ? ….




Pour envoyer le message " Réunion reportée à 15:00 au même endroit " à l'utilisateur marie, tapez :

**net send marie " Réunion reportée à 15:00 au même endroit. "**

Pour envoyer un message à tous les utilisateurs connectés actuellement au serveur, tapez :

**net send /users Ce serveur va s'arrêter dans 5 minutes.**

# COMMANDE NET USER...

**La base de la commande Net user :**

Ce qui est intéressant, c'est de pouvoir en ligne de commande, ajouter un utilisateur. Avec les paramètres de base :

- ajouter un compte d'utilisateur pour **Michel** et l'autorisez le à se avec le mot de passe obligatoire (**mc**):

```
C:\>net user michel mc /add
La commande s'est terminée correctement.
```

**Les paramètres optionnels :**

/fullname:"*nom*"

Spécifie le nom complet de l'utilisateur plutôt qu'un nom d'utilisateur. Placez le nom entre guillemets.

/passwordchg:{yes | no}

Indique si les utilisateurs peuvent modifier leur propre mot de passe. La valeur par défaut est yes.

/passwordreq:{yes | no}

Indique si un compte d'utilisateur doit posséder un mot de passe. La valeur par défaut est yes.

/times:{*heures* | all}

Précise quand l'utilisateur est autorisé à employer l'ordinateur. Le paramètre *heures* est exprimé en *jour*[*-jour*][*,jour*[*-jour*]] *,heure*[*-heure*][*,heure*[*-heure*]] et limité à des incréments d'une heure. Les jours peuvent être écrits en toutes lettres ou abrégés sous la forme lun, mar, mer, jeu, ven, sam et dim. Les heures peuvent être exprimées à l'aide de la plage 12 ou 24 heures. Pour la plage 12 heures, utilisez AM, PM ou A.M., P.M. La valeur all signifie qu'un utilisateur peut toujours se connecter. La valeur nulle (blanc) signifie qu'un utilisateur ne peut jamais se connecter. Séparez le jour et l'heure par des virgules et les unités du jour et de l'heure par des points-virgules (par exemple, L,4AM-5PM;Ma,1PM-3PM). N'utilisez pas d'espaces pour désigner les heures

/workstations:{nom_ordinateur[,...] | *}

Répertorie jusqu'à huit stations de travail à partir desquelles un utilisateur peut se connecter au réseau. Séparez les entrées multiples de la liste par des virgules. Si /workstations ne possède pas de liste ou si elle correspond à *, cela signifie que l'utilisateur peut se connecter à partir de n'importe quel ordinateur.

- supprimez ce compte, puis ajouter un compte d'utilisateur pour **Michel Cabare** et l'autorisez le à se avec le mot de passe obligatoire (**mc**):

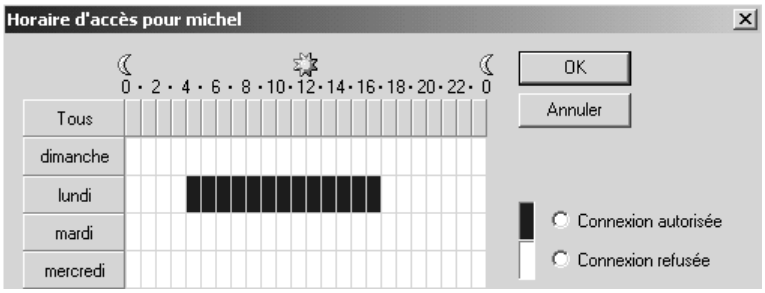
```
net user michel mc /add /fullname:"michel cabare"
```

- supprimez ce compte et ajouter un compte d'utilisateur pour **Michel Cabare** autorisé à se connecter **lundi** de **04:00 à 17:00** (pas d'espace dans la désignation des heures) avec le mot de passe obligatoire (**mc**):

Les 2 syntaxes équivalentes →

```
C:\>net user michel mc /add /times:L,4AM-5PM
La commande s'est terminée correctement.

C:\>net user michel mc /add /times:L,4-17
La commande s'est terminée correctement.
```

donnent



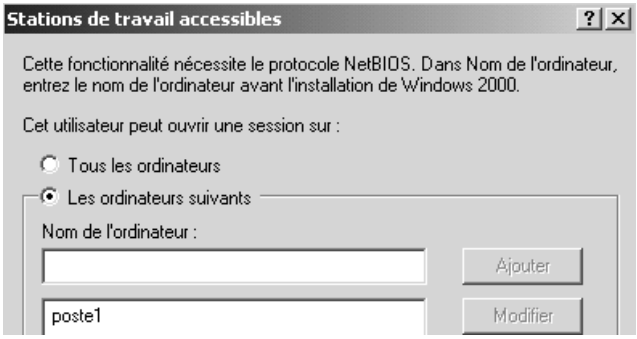

- supprimez ce compte et ajouter un compte d'utilisateur pour **Michel Cabare** autorisé à se connecter du **lundi au vendredi** de **08:00 à 17:00** (pas d'espace dans la désignation des heures) avec le mot de passe obligatoire (**mc**):

```
C:\>net user michel mc /add /times:L,8-17;MA,8-17;ME,8-17;J,8-17;V,8-17
La commande s'est terminée correctement.
```

**NB** : notez dans cette syntaxe la différence MA mardi et ME mercredi !

- supprimez ce compte et ajouter un compte d'utilisateur pour **Michel Cabare** autorisé à se connecter du **lundi au vendredi** de **08:00 à 17:00** (pas d'espace dans la désignation des heures) avec le mot de passe obligatoire (**mc**) depuis le poste **client1**:

```
C:\>net user michel mc /add /times:L,8-17;MA,8-17;ME,8-17;J,8-17;V,8-17 /worksta
tions:poste1
La commande s'est terminée correctement.
```



# SCRIPT SELON L'OS

**Détecter l'OS du client :**

Il est fréquent que certaine commandes ne soient pas traitées comprises de la même manière selon l'OS du client….ainsi, pour la création du lecteur logique, on sait que une lettre peut être attachée automatiquement au répertoire de base, mais on sait aussi que on peut via un script donner l'instruction suivante **net use g : /home**

Le problème dans ce cas c'est que ce script fait « double emplois » lors d'une exécution sur un client 2000.

On voudrait faire exécuter différent selon la nature du client :

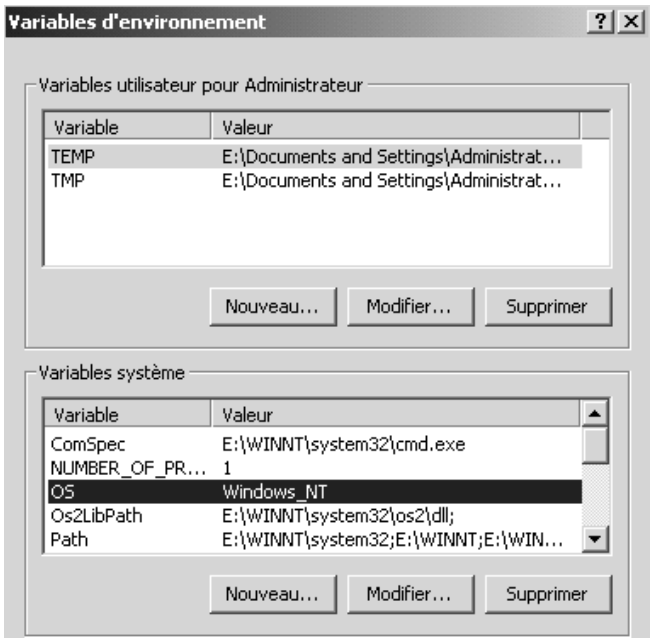
- Si le client est windows95-98, il faut créer un lecteur sur le dossier de base
- Si le client est 2000, il n'est pas nécessaire de créer ce lecteur logique, car il est crée automatiquement

**Variable d'environnement :**

Il existe une variable d'environnement nommée **%OS%**

Dans le **panneau de configuration / système** on trouve


dans lequel on voit que




Donc on peut dire que si on a **"%OS%"=="Windows_NT"** on est sur un client 2000 (ou NT4.0)

Soit donc un script avec les étiquettes **SUITE-FIN** suivantes :

```
If not "%OS%"=="Windows_NT" goto SUITE
REM partie qui va etre executée sur un client 2000

goto FIN:

REM partie qui va etre executée sur un client non 2000
:SUITE

:FIN
```

exercice : faire un script qui ne crée de lecteur réseau sur le répertoire de base que si le client n'est pas un client nt ou un client 2000….

---

**Version d'OS :**

cette variable d'environnement nommée **%OS%** est la même pour 2000 et pour NT4, ce qui fait que si l'on voulait descendre au niveau de la détection de la version de Windows il faudrait employer une commande **VER** qu'il faudrait rediriger ensuite avec une commande **FIND** de recherche de caractère…

en effet **ver** renvois les valeurs suivantes selon les versions de système

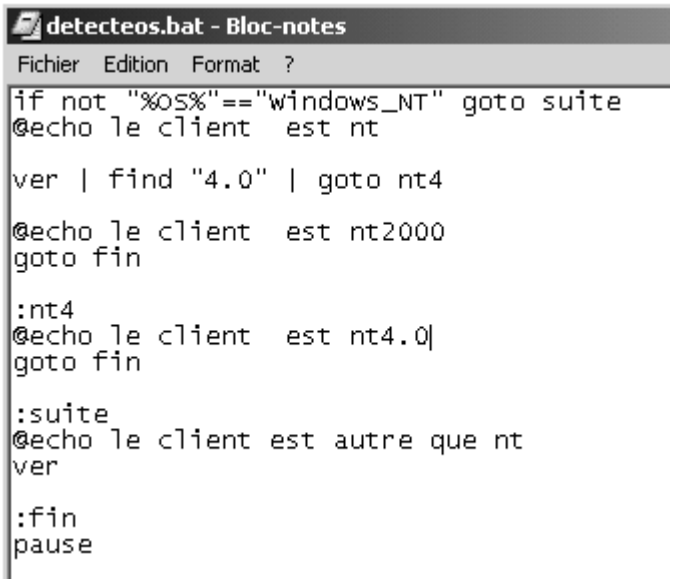
pour Windows NT 4.0 (wks ou srv)


pour Windows 2000 (pro ou server)


On peut donc rechercher la chaîne "4.0" pour savoir si on est sur un poste NT4.0 ou un poste 2000. Pour rediriger la sortie de la commande **ver** sur la commande **FIND** on utilise un **| (pipe)**, ce qui donnerait à peu près la ligne suivante

```
Ver | find "4.0" | goto nt4
```

exercice : faire un script qui détecte si le client sur lequel il s'exécute est un client windows95-98, nt4.0 ou 2000


detecteos.bat - Bloc-notes
Fichier Edition Format ?
if not "%OS%"=="Windows_NT" goto suite
@echo le client est nt
ver | find "4.0" | goto nt4
@echo le client est nt2000
goto fin
:nt4
@echo le client est nt4.0
goto fin
:suite
@echo le client est autre que nt
ver
:fin
pause

# SCRIPT GROUPE UTILISATEURS

**Tester l'appartenance à un groupe précis :**

Il est aussi fréquent que certaine commandes ne soient pas applicable à tous les utilisateurs, mais qu'elles aient un sens uniquement si l'utilisateur est membre de tel ou tel groupe…

Imaginons un fichiers **.bat** spécifique à des commerciaux, nommé **commercial.bat**, et un fichier **.bat** spécifique à des secrétaires, nommé **secretaire.bat**

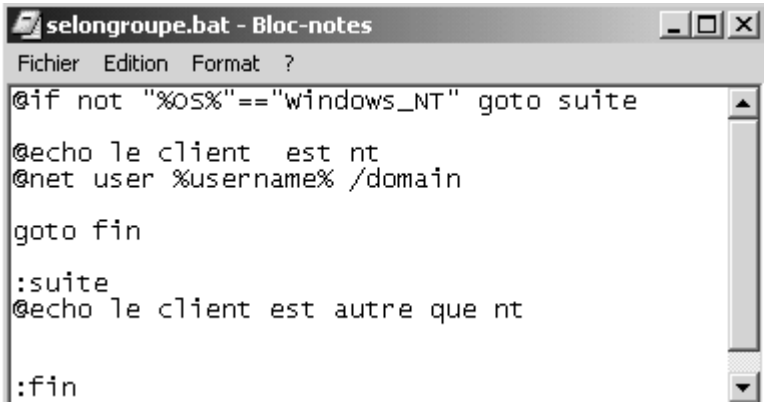
Ces deux fichiers sont appelables dans mon script via la commande **call** mais comment détecter l'appartenance d'un utilisateur à tel groupe ?

Cela n'est possible que si le client est un client NT…

**Solution native :**

On sait que **net user toto /domain** renvois alors les paramètres de cet utilisateur.

Un script permettant d'avoir les informations concernant l'utilisateur en train d'ouvrir la session ressemblerait donc à ceci :




soit l'utilisateur toto membre d'un groupe secretaire,

et titi membre d'un groupe commercial


alors ce script sur l'ouverture de titi amène l'info suivante :

```
La demande sera traitée sur contrôleur de domaine du domaine domaine2.edu.

Nom d'utilisateur                            titi
Nom complet                                  titi
Commentaire
Commentaires utilisateur
Code du pays                                 000 (Valeur par défaut du système
)
Compte : actif                               Oui
Le compte expire                             Jamais

Mot de passe : dernier changmt.              5/14/2002 12:49 PM
Le mot de passe expire                       6/26/2002 11:37 AM
Le mot de passe modifiable                   5/14/2002 12:49 PM
Mot de passe exigé                           Oui
L'utilisateur peut changer de mot de passe   Oui

Stations autorisées                          Tout
Script d'ouverture de session                selongroupe
Profil d'utilisateur
Répertoire de base                           \\serveur2\ressource\titi
Dernier accès                                5/14/2002 1:18 PM

Heures d'accès autorisé                      Tout

Appartient aux groupes locaux                *Utilisateurs
Appartient aux groupes globaux               *Utilisa. du domaine
                                             *commercial
La commande s'est terminée correctement.
```

Pour détecter l'appartenance à un groupe, il suffit maintenant d'utiliser **FIND** en récupération de la sortie du script précédant…

Et bien sur prévoir les 2 fichiers bat à exécuter…

```
@if not "%OS%"=="Windows_NT" goto suite

@echo le client  est nt
@net user %username% /domain | find /i "*commercial" && call commercial.bat
@net user %username% /domain | find /i "*secretaire" && call secretaire.bat
goto fin

:suite
@echo le client est autre que nt

:fin
```

## Avec le resource kit

Avec l'utilitaire nommé **ifmember.exe** qu'il faut installer sur tous les clients en \WINNT\SYSTEM32 (ou un chemin disponible dans les variables d'environnement système)

selonifmember.bat - Bloc-notes

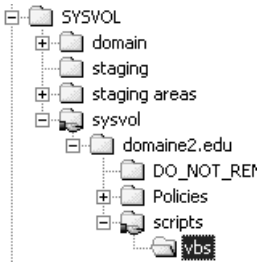
Fichier Edition Format ?

```
@if not "%OS%"=="Windows_NT" goto suite

@echo le client  est nt
ifmember "commercial"
if errorlevel 1 call commercial.bat
ifmember "secretaire"
if errorlevel 1 call secretaire.bat

goto fin

:suite
@echo le client est autre que nt
```

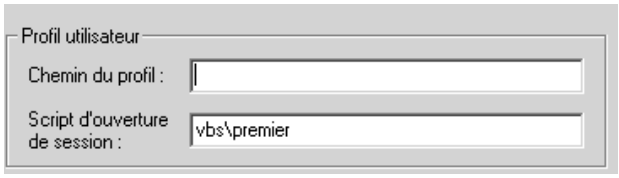
# SCRIPT WSH

## Mise en place des scripts :

On veut utiliser des scripts que l'on placera dans un dossier spécifique du serveur nommé par exemple vbs…de manière à ne pas les mélanger avec ceux existant.




il faudra du coup indiquer dans le profil utilisateur cette redirection



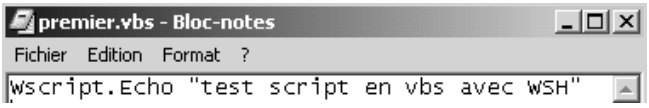

## 1° script en vbs :

La commande la plus simple que l'on puisse faire, comme d'habitude, c'est faire afficher un message.

En vbs la commande est la suivante :

**Wscript.Echo "test script en vbs avec WSH"**

On peut donc mettre cette ligne dans un fichier xxxx.vbs, par exemple **premier.vbs**




Bon, notre premier fichier en vbs à destination de WSH est prêt, mais comment l'exécuter sur le client ?

Le problème c'est que cette commande doit être exécutée via l'environnement 'en ligne de commande » de WSH, et non pas l'environnement graphique.

Comme on ne peut pas savoir si sur le client par défaut WSH est positionné en ligne de commande, ou en interface GUI, on faut lancer la commande avec des paramètres d'appel, du genre

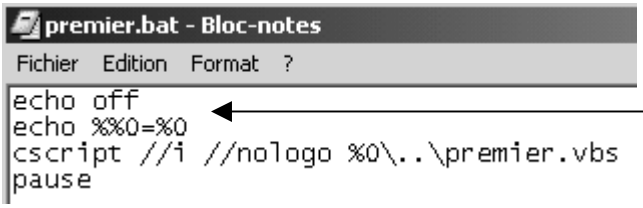
**cscript //i //nologo %0\\..\\premier.vbs**

l'utilisation des paramètres **//i** et de **//nologo** est simple, ces paramètres expriment en wsh le mode interactif, sans logo de démarrage, et sont possibles par l'appel de **cscript**….

Plus délicat la signification de **%0\\..\\premier.vbs**

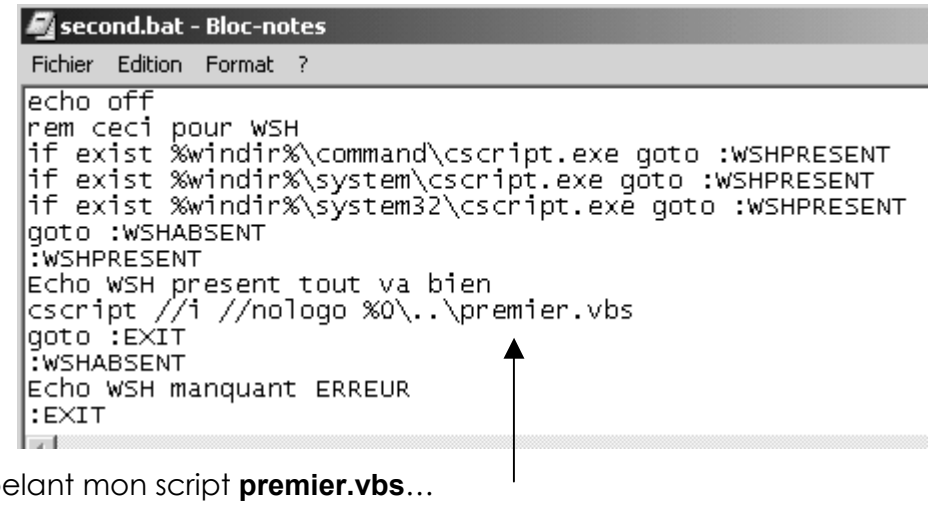
En effet le script que l'on écrit doit aller chercher le fichier **premier.vbs** à son emplacement d'origine, hors le client ne le connaît pas ! **%0** contient toujours le chemin complet vers le script en cours, de la on peut utiliser et écrire le chemin permettant de trouver **premier.vbs**

Par conséquent un script **premier .bat** et contenant




devrait donner à l'exécution sur un client « comprenant wsh » le résultat suivant :


Si on voulait vraiment, on pourrait affiner le test de la présence de WSH en testant la présence des fichiers système, par un script **second.bat** du genre :




appelant mon script **premier.vbs**…

En effet la présence de l'installation de WSH sur un OS est donnée ci-dessous

| Composant | Fichier clé | Emplacements |
|---|---|---|
| Windows Script Host | CSCRIPT.EXE | %windir%\command<br>%windir%\system<br>%windir%\system32 |
| VBScript | VBSCRIPT.DLL | %windir%\system<br>%windir%\system32 |
| ADSI | ADSNT.DLL | %windir%\system<br>%windir%\system32 |

**Un exemple en vbs :**

Soit le fichier **exemple.bat** permettant de lancer le script **exemple.vbs** suivant :

```
Dim variable

Wscript.Echo "exemple script en vbs avec WSH"

Set variable = WScript.CreateObject("WScript.Network")

Wscript.Echo "machine " & variable.ComputerName
Wscript.Echo "utilisateur " & variable.UserName
Wscript.Echo "domaine " & variable.UserDomain

variable.MapNetworkDrive "S:", \\serveur2\ressource

Wscript.Echo "fin test script en vbs avec WSH"
```

Bien sur il vaut mieux que ce partage ait été crée préalablement à l'exécution du script !

# ID ÉVÈNEMENT

**Signification d'un ID du gestionnaire évènement :**

Un site répertorie et traite une bonne partie des évènements qui surviennent au quotidien. Il s'agit du site **www.eventid.net**

Sur la page d'accueil, on ait une recherche par ID


Enter the event ID:

Enter event source (optional):

Search

| Event ID: 54 | |
|---|---|
| **Source** | w32time |
| **Type** | Warning |
| **Description** | The Windows Time Service was not able to find a Domain Controller. A time and date update was not possible. |
| **Comments** | A.G.: "As per Microsoft: This issue can occur because of repeated network issues or if the Time service has been unable to find a domain controller to synchronize with for a long time. To reduce network traffic, the Time service will wait 960 minutes before it tries again, and no synchronization takes place during this interval, even if network connectivity is restored after being in a disconnected state for an amount of time that is less than the synchronization interval."<br>A.G.: "Windows 2000 computers are attempting to synchronize their time with a domain controller. If none is found this message is generated. The domain controller must run the w32time service. This service can be syncronized with an external source (ie.atomic clocks like the one maintained by Navy Observatory). A syncronized time is very import for Active Directory implemenations due to its distributed nature." |
| **Links** | Q312534; Windows 2000 Time |
| **Contributors** | Adrian Grigorof |

des liens peuvent exister sur des articles de la FAQ Micosoft ou la doc en ligne…

| Event ID: 62 | |
|---|---|
| **Source** | w32time |
| **Type** | Error |
| **Description** | This Machine is a PDC of the domain at the root of the forest. Configure to sync from External time source using the net command, 'net time /setsntp:'. |
| **Comments** | **Adrian Grigorof**: The Time service is not configured to use a reliable source for synchronization. Try "net time /setsntp:ntp2.usno.navy.mil" followed by "w32tm /s" (Internet connectivity should be available between the server and the ntp2.usno.navy.mil NTP - Network Time Protocol server) |
| **Contributors** | Adrian Grigorof |

La commande pour qu'il y ait synchronisation serait

**Net TIME /SetSNTP:nomserveur**

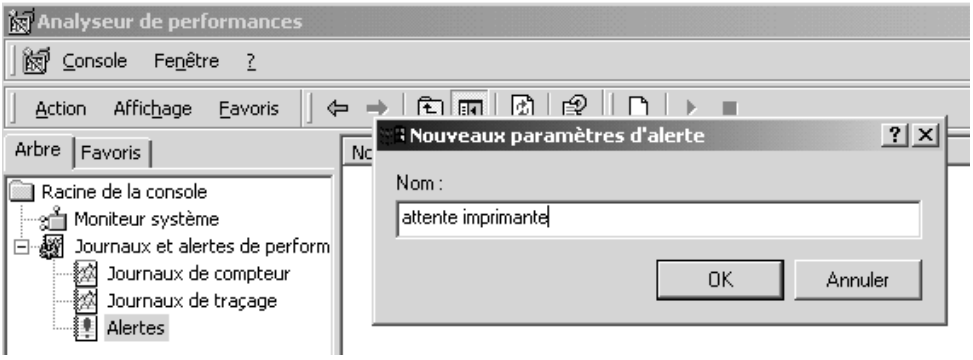
# MONITEUR SYSTEME : ALERTE SUR UNE IMPRIMANTE

**Paramétrage Seuil d'alerte :**

Soit une imprimante **HP laserjet 6P** définie sur une machine **client2kp7**. On tient à ce que l'on sache immédiatement **lorsque une attente de plus de 2 document existe sur ce périphérique**. On souhaite que cela soit **consigné dans le journal des évènements application** et qu'un message soit envoyé sur le poste de l'administrateur, situé en **Serveur2**…

Sur le client il faut d'abords définir l'imprimante…(pour les test on la mettra hors connexion **Utiliser l'imprimante hors connexion**)

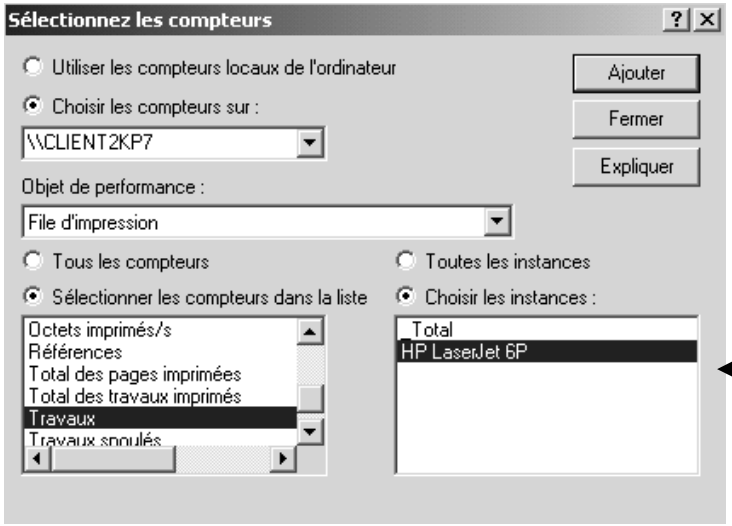

On crée sur le poste ou se trouve l'imprimante une nouvelle alerte, nommé par exemple"**attente imprimante**"




et on la configure de la manière suivante :

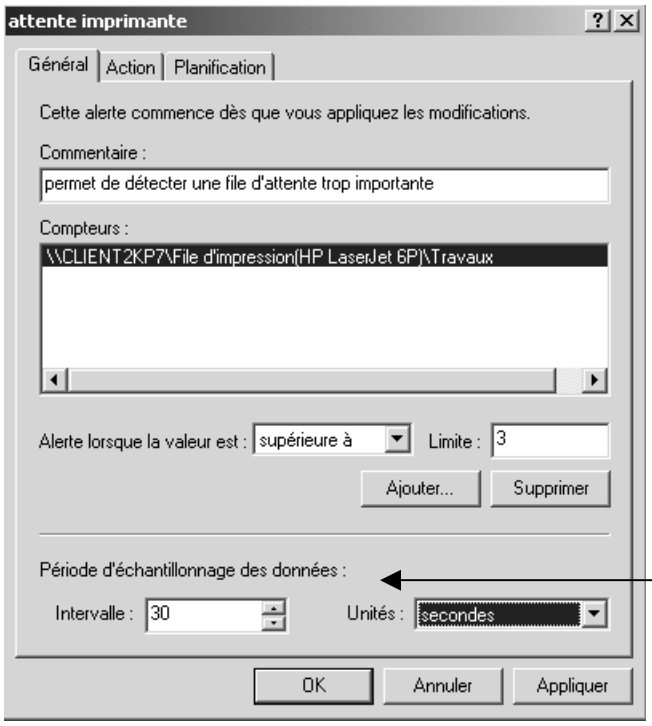
**Sur le poste**

Les travaux dans la file d'impression



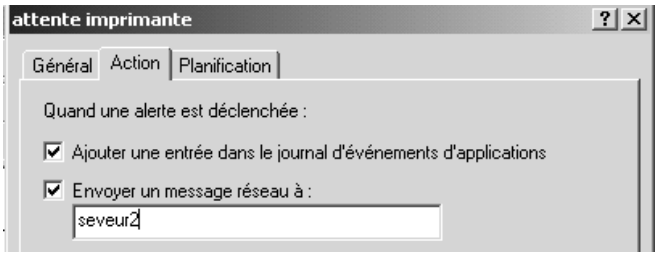

De l'imprimante HP Laserjet 6p

pour obtenir

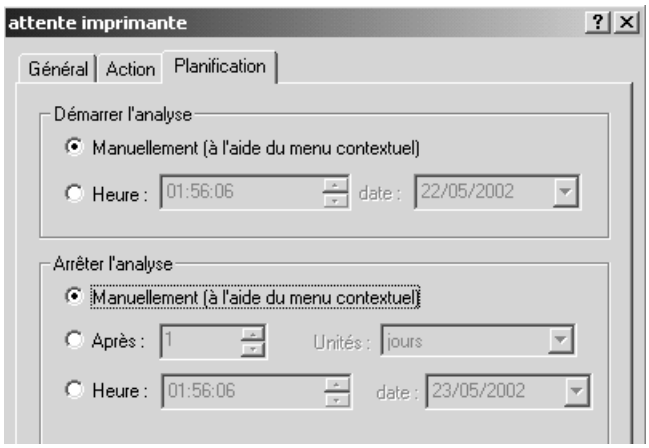



Indiquer ici un délai raisonnable…

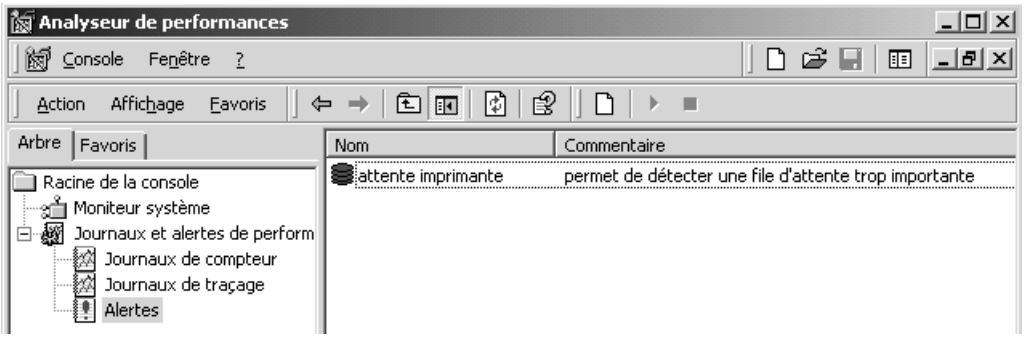
Au niveau de l'action on demandera :




et une planification manuelle

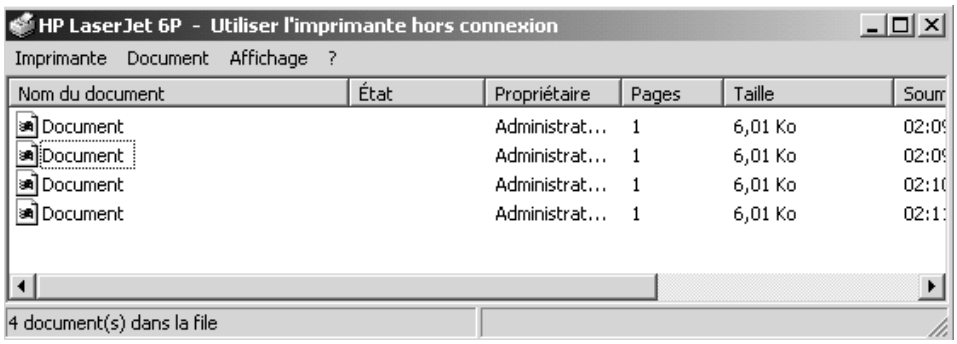



Il ne reste plus qu'à la démarrer, via le menu contextuel.

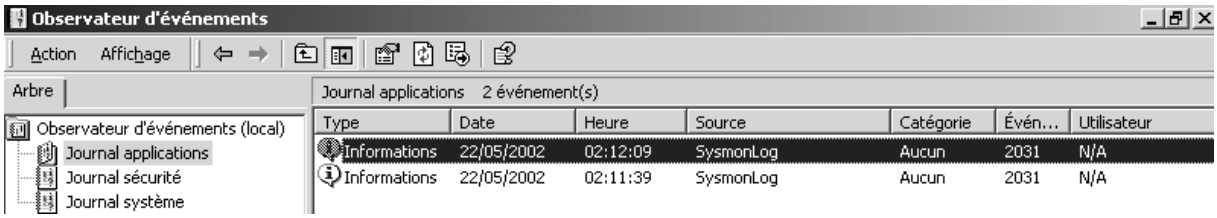


**Déclenchement Seuil d'alerte :**

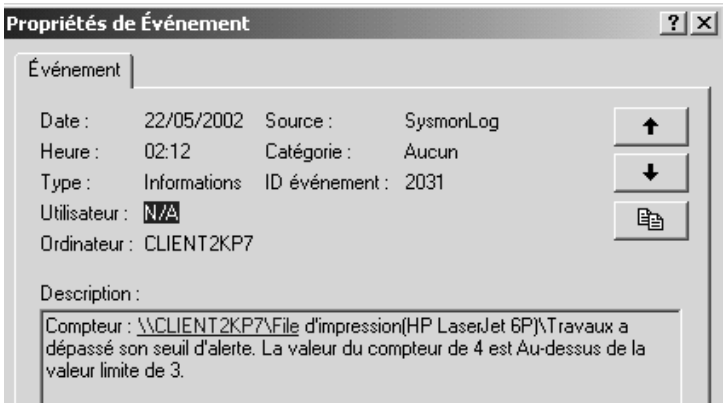
Après avoir mis l'imprimante hors connexion, il suffit de demander une impression de quelques documents pour obtenir :



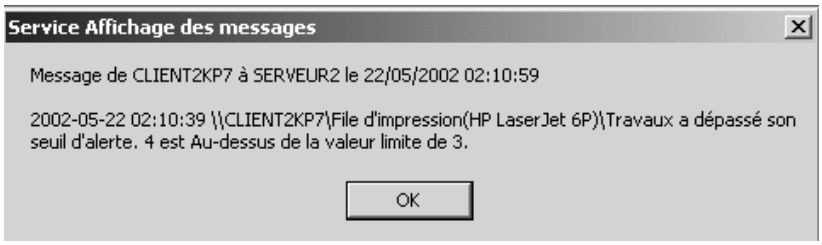

avec dans le journal d'événement **basé sur le poste**




avec le détail




et avec une notification **sur le serveur**




**N.B** : bien penser a placer les alertes sur les machines sur lesquelles on veut visualiser les évènements.

# MONITEUR SYSTEME DISQUE LOGIQUE

**Compteur sur disque logique :**

Par défaut, lorsque le système démarre, il active les compteurs d'analyse du disque par un pilote **Diskperf.sys**

Ce pilote par défaut active les compteurs uniquement sur les disques physiques, mais on peut par une ligne de commande, demander de l'activer aussi sur un lecteur logique…

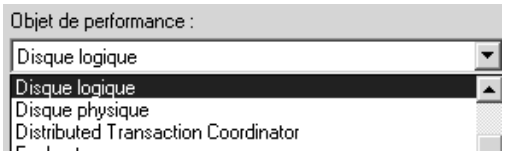
```
E:\>diskperf -?

DISKPERF====================

Démarre et arrête les compteurs de performance de disque système.

Utilisée sans commutateurs, DISKPERF rapporte quels disques
si les compteurs de performance sont activés sur l'ordinateur local ou spécifié.


Des compteurs de performance de disque peuvent être spécifiés pour rapporter les

performances des lecteurs physiques individuels, ou des lecteurs
logiques individuels ou des volumes de stockage. Notez que ces deux jeux de
compteurs de performance sont mesurés indépendamment. L'utilisateur
a le choix de les activer ou de les désactiver indépendamment
grâce aux commutateurs de la ligne de commande.

DISKPERF [-Y[D¦V] ¦ -N[D¦V]] [\\NomOrdinateur]

  -Y  Force le système à démarrer tous les compteurs de
      performance de disque quand le système est redémarré.

  -YD Active les compteurs de performance de disque pour les
      lecteurs physiques quand le système est redémarré.
  -YV Active les compteurs de performance de disque pour les
      disques logiques ou les volumes de stockage quand le
      système est redémarré.
  -N  Force le système à désactiver tous les compteurs de
      performance de disque quand le système est redémarré.

  -ND Désactive les compteurs de performance de disque pour les lecteurs
      physiques.
  -NV Désactive les compteurs de performance de disque pour les lecteurs
      logiques.
  \\NomOrdinateur      Nom de l'ordinateur dont vous voulez
                       paramétrer l'utilisation des compteurs de
                       performance de disque.
```

Ainsi la commande

**Diskperf.sys -YV** permet de disposer d'un compteur de plus, permettant d'afficher la place disponible sur un lecteur logique

```
E:\>DISKPERF -YV

Les compteurs de performance des disques logique et physique de ce système
sont maintenant initialisés pour être lancés lors du démarrage.
```

Après redémarrage, on aura dans l'analyseur de performance, la possibilité de demander un disque logique…



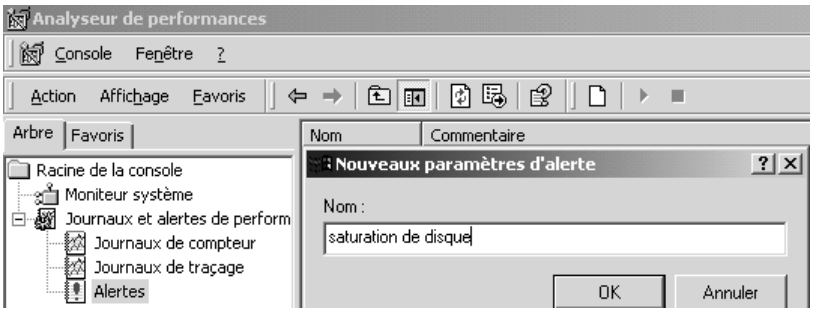

Et sur les disques logiques, on demande la taille disponible…

## Alerte saturation de disque :

Un fois que l'on sait comment demander d'activer un compteur pour les disques logiques sur un poste à distance,

**Diskperf.sys –YV \\nomposte**

installer une alerte ne devrait pas poser de problème

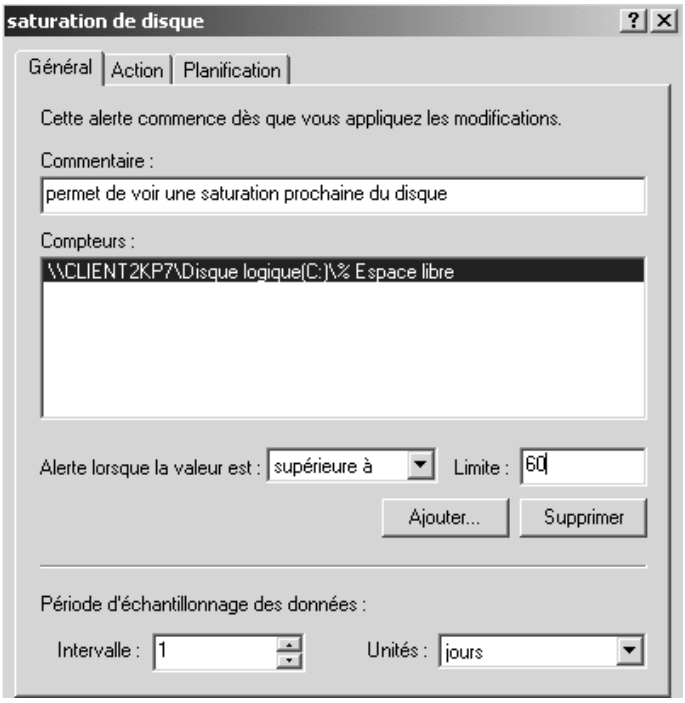


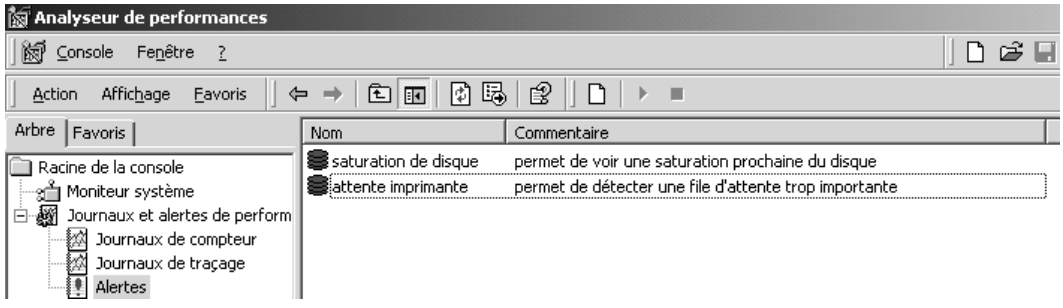

Avec les paramètres suivants

Sur la machine [\\client2kp7](\\client2kp7)

Lorsque l'on a 60% de plein…

Tester 1 fois pas jour

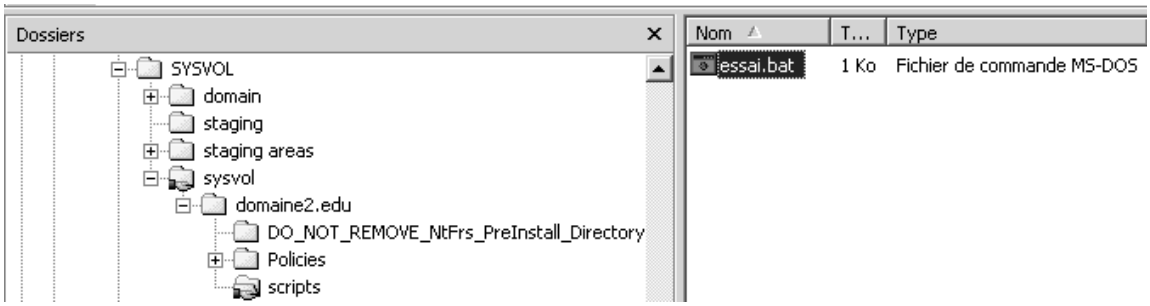


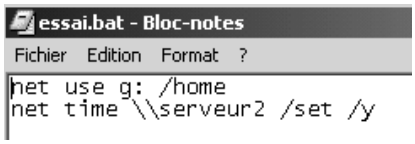
# SCRIPT DE MISE A L'HEURE

**Création du script :**

Un petit script de mise à l'heure fonctionnera très simplement à partir du moment ou il est stocké dans le dossier adéquat du serveur 2000,




et qu'il contiendra des instructions du type :

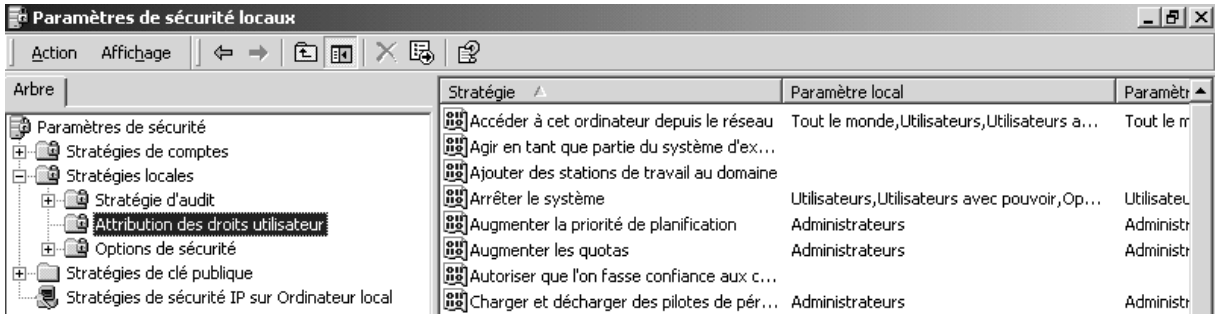



**Droit de modification de l'heure système :**

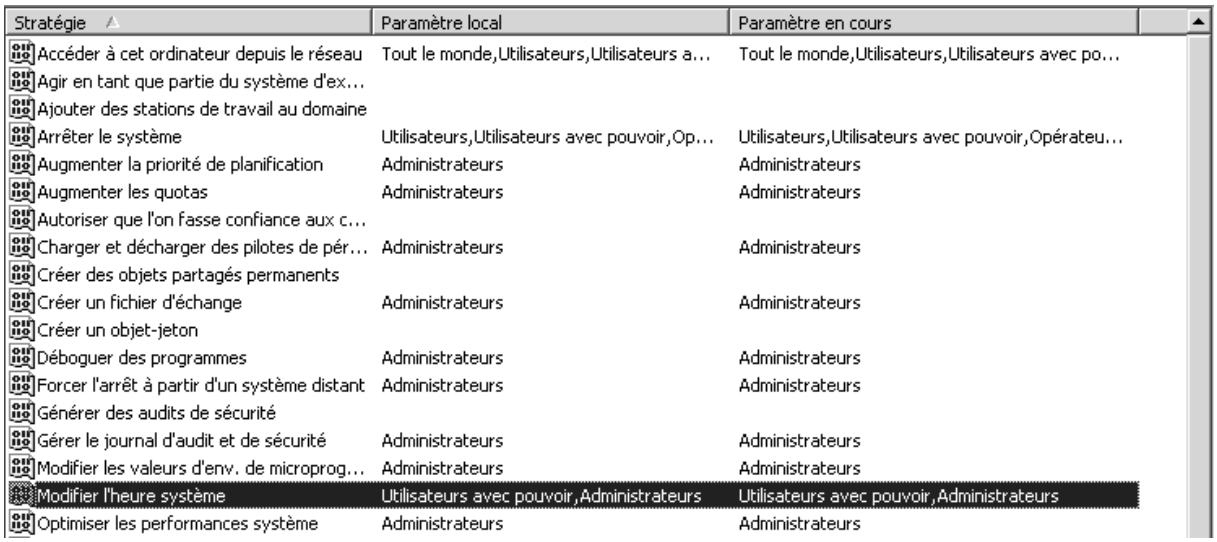
Bien sûr sur une machine windows, le script s' exécutera sans problème, car tout le monde a le droit de modifier cette heure système.

Mais il n'en va pas de même pour un client 2000, sur lequel nativement un tel script n'a aucun effet…

En effet il faut aller voir dans
**panneau configuration / outils d'administration/ Stratégies locales**, et vérifier qui peut modifier l'heure système…


o
on peut alors voir que



| Stratégie | Paramètre local | Paramètre en cours |
|---|---|---|
| Accéder à cet ordinateur depuis le réseau | Tout le monde,Utilisateurs,Utilisateurs a… | Tout le monde,Utilisateurs,Utilisateurs avec po… |
| Agir en tant que partie du système d'ex… | | |
| Ajouter des stations de travail au domaine | | |
| Arrêter le système | Utilisateurs,Utilisateurs avec pouvoir,Op… | Utilisateurs,Utilisateurs avec pouvoir,Opérateu… |
| Augmenter la priorité de planification | Administrateurs | Administrateurs |
| Augmenter les quotas | Administrateurs | Administrateurs |
| Autoriser que l'on fasse confiance aux c… | | |
| Charger et décharger des pilotes de pér… | Administrateurs | Administrateurs |
| Créer des objets partagés permanents | | |
| Créer un fichier d'échange | Administrateurs | Administrateurs |
| Créer un objet-jeton | | |
| Déboguer des programmes | Administrateurs | Administrateurs |
| Forcer l'arrêt à partir d'un système distant | Administrateurs | Administrateurs |
| Générer des audits de sécurité | | |
| Gérer le journal d'audit et de sécurité | Administrateurs | Administrateurs |
| Modifier les valeurs d'env. de microprog… | Administrateurs | Administrateurs |
| Modifier l'heure système | Utilisateurs avec pouvoir,Administrateurs | Utilisateurs avec pouvoir,Administrateurs |
| Optimiser les performances système | Administrateurs | Administrateurs |

Si on veut ajouter tous les utilisateurs authentifiés, par exemple, alors on fera la manipulation suivante :

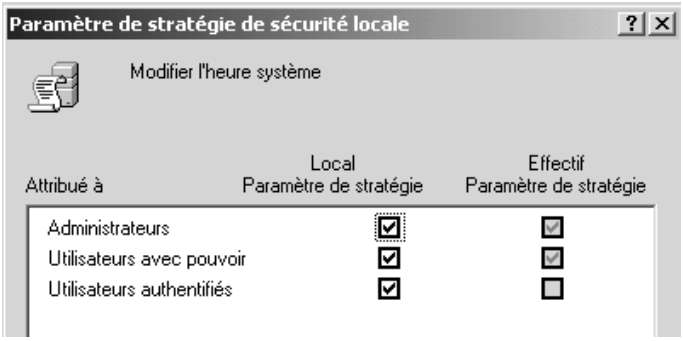
En double-cliquant dessus

On obtient

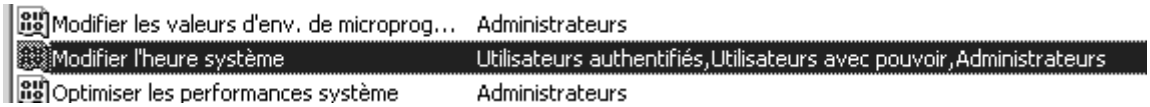

Dans lequel on Ajoute

Les utilisateur authentifiés


pour obtenir finalement




ou encore




**Exemple d'écrasement entre stratégie locale et stratégie de DC :**

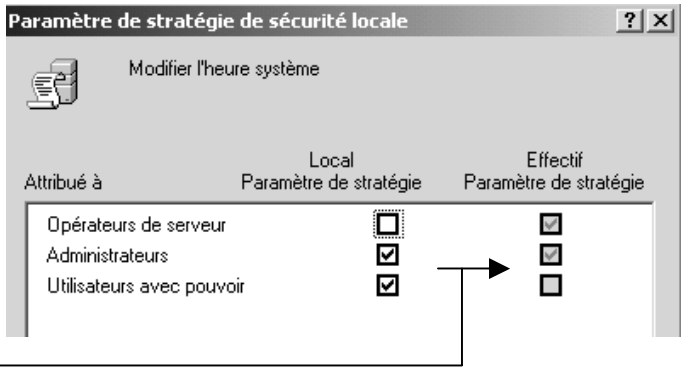
Regardons la même chose, à titre de curiosité sur le contrôleur de Domaine.

On a dit que les paramètres locaux sont modifiées dans cet ordre (si cela à un sens)

**stratégies locale – stratégie de Contrôleur de Domaine**

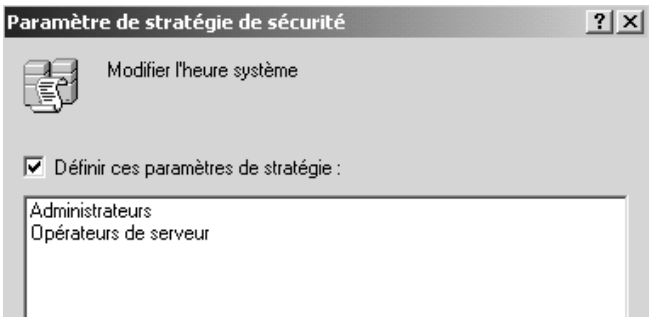
Par conséquent si on regarde les **stratégies locales** sur un contrôleur de domaine (notre serveur), en ce qui concerne **Modifier l'heure système** on va trouver alors

On retrouve « classiquement » les administrateur et les utilisateurs avec pouvoir, mais on s'aperçoit que les paramètres effectifs diffèrent !




En effet au niveau stratégie de contrôleur de Domaine on va trouver

Et les stratégies sont cumulatives !



# STRATEGIE LOCALE 1°

**Augmenter la sécurité :**

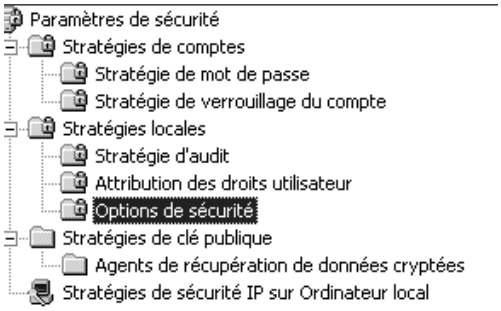
Pour augmenter la sécurité à propos de la connexion sur un réseau, on souhaite effectuer plusieurs modification de la sécurité d'une machine

1. Ne pas faire afficher le dernier identificateur de session utilisé sur cette machine


2. Ne pas permettre une ouverture de session si le contrôleur de domaine est indisponible

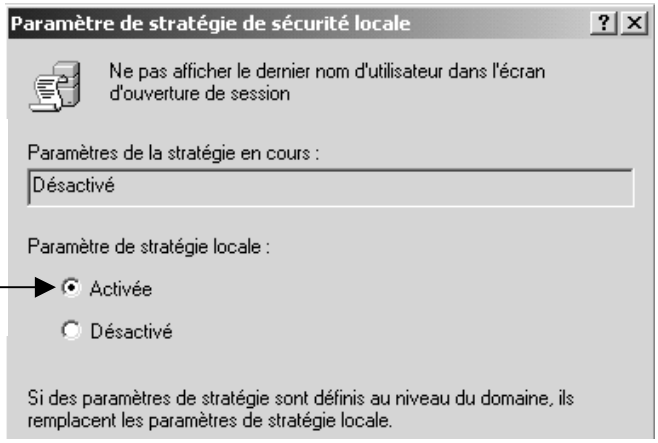

Mettez en œuvre localement cette stratégie, testez là, puis redonnez les valeurs par défaut…

Il faut aller dans les options de sécurité

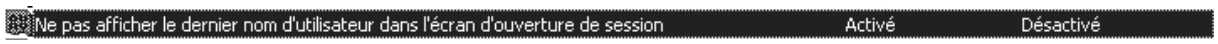



et demander pour

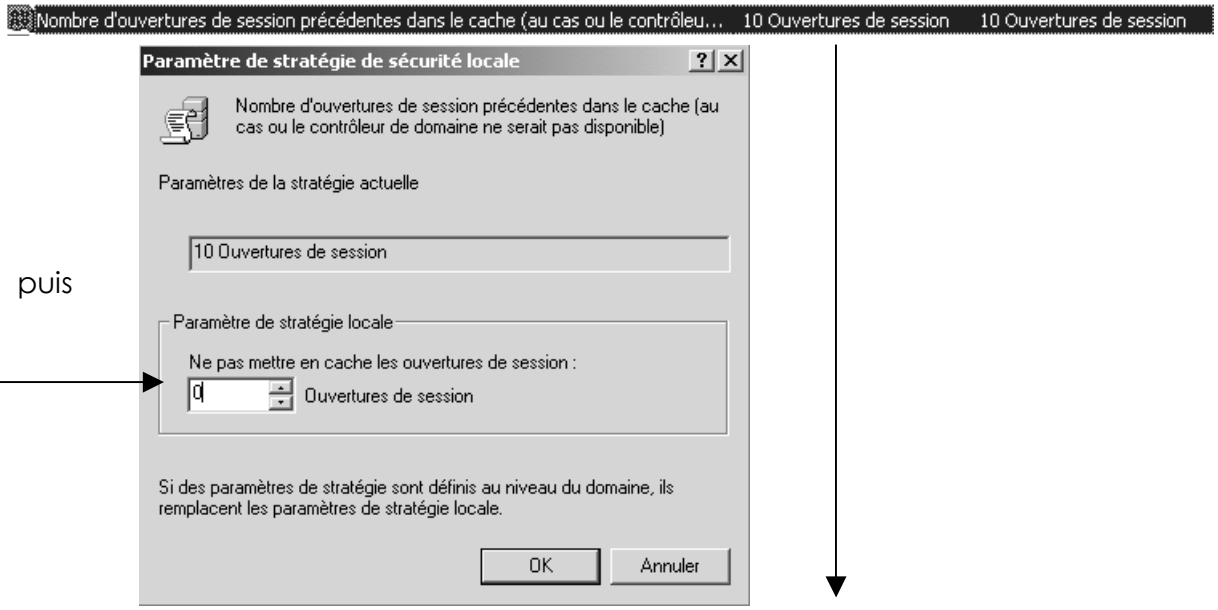

On double clic puis on demande **Activée**




on obtient alors



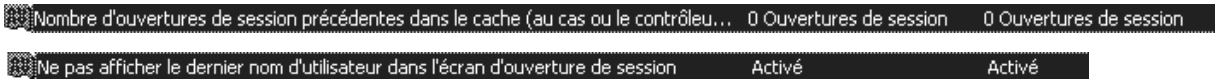
puis pour



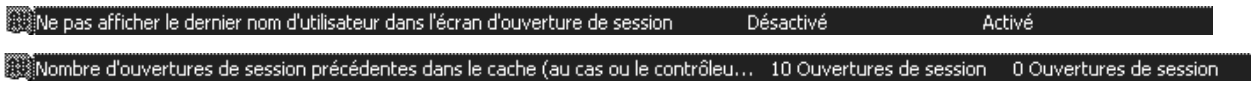

On double clic puis on demande **0**

on obtient alors


Après redémarrage du poste on aura bien




pour retrouver la situation initiale, il faut faire les manipulations inverses, de manière à obtenir




puis effectuer un re démarrage !

# STRATEGIE LOCALE 2°

**Pister les tentatives d'accès :**

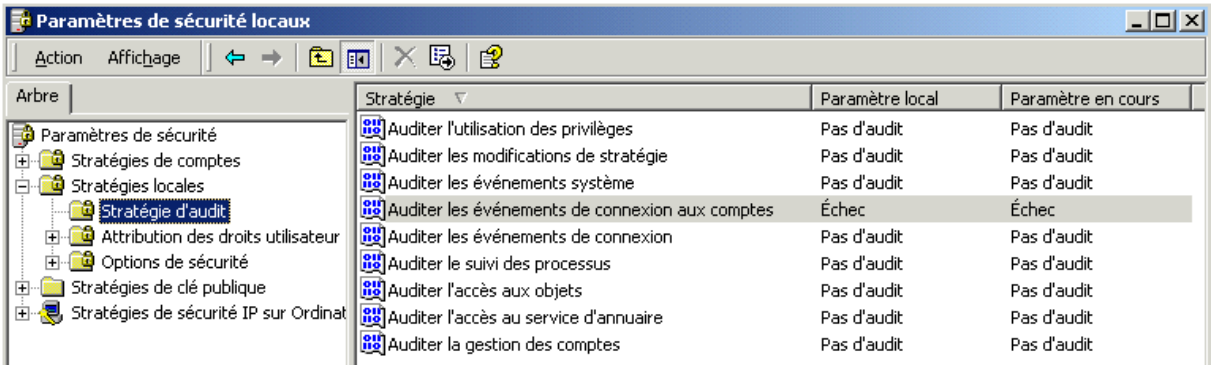
Dans une entreprise, on souhaite pister les tentatives d'accès infructueuses effectuées sur le réseau. On souhaite avoir des renseignements lorsque on a des tentatives de connexion qui échouent….

Le principe va consister à armer une stratégie d'audit basée sur les **évènements de connexion aux comptes**.

Par définition on n'auditera que les tentatives qui échouent, en sachant que l'événement est enregistré sur la machine sur laquelle l'identification se fera…

**Audit sur le client :**

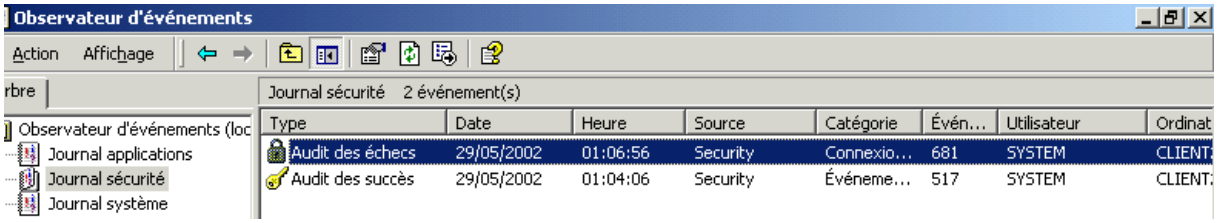
On suppose que les tentatives de connexions se font depuis une machine isolée dans un bâtiment, la nuit. On va placer dessus donc un audit sur les echec.



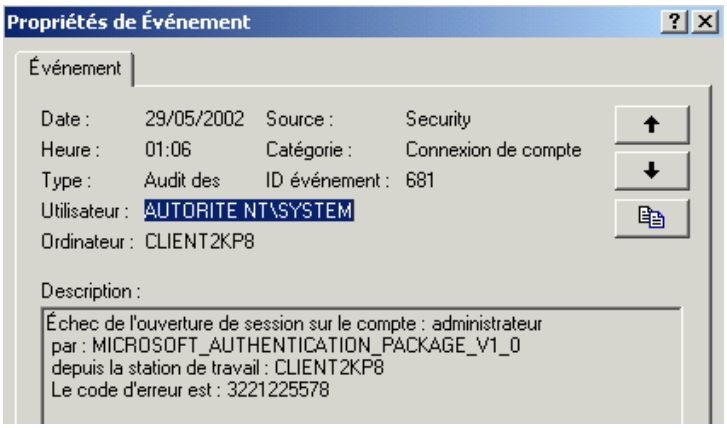

Essayez d'ouvrir une session en tant qu'administrateur du domaine, en vous trompant . Que lisez vous dans le journal d'événement ?

…

Les évènements sont consignés sur le système qui effectue l'authentification, par conséquent ce n'est que **si on se trompe en essayant d'ouvrir une session locale**, que l'on pourra observer alors dans le journal sécurité

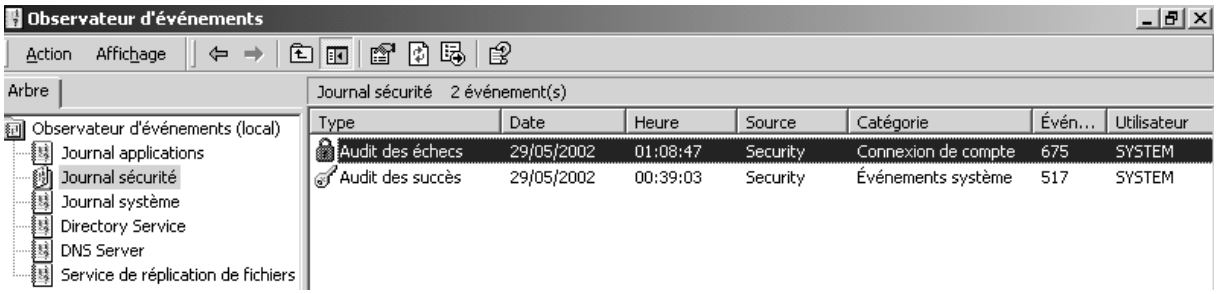


avec comme explication

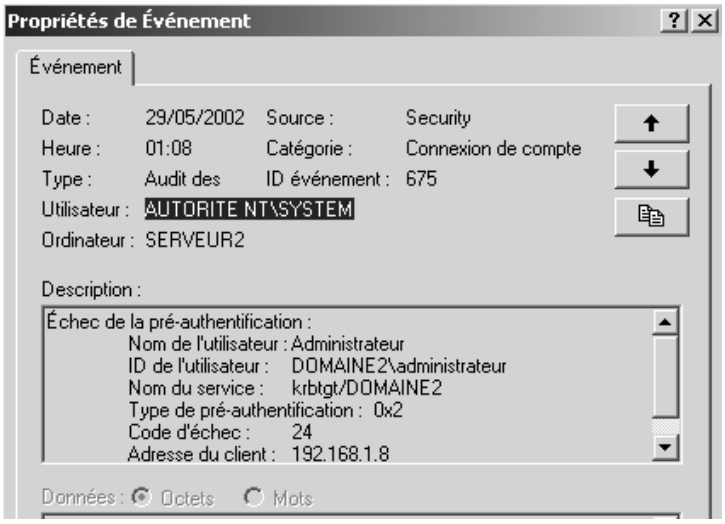



**Audit sur le serveur :**

Si on veut une trace des tentatives infructueuses sur le domaine, il faut auditer le contrôleur de domaine, on se place sur le contrôleur, on active les stratégies de sécurités locale…..




avec comme explication



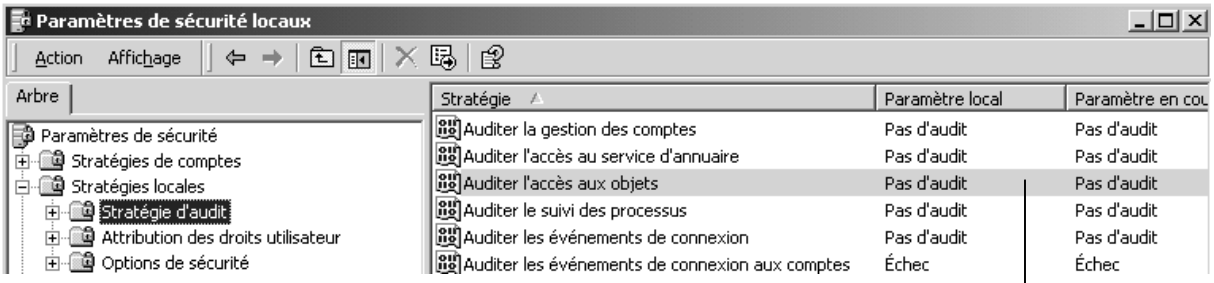

**N.B**: on s'apperçoit que les sratégies définies sur les contrôleurs de Domaines viennent "écraser" les stratégies définies localement.

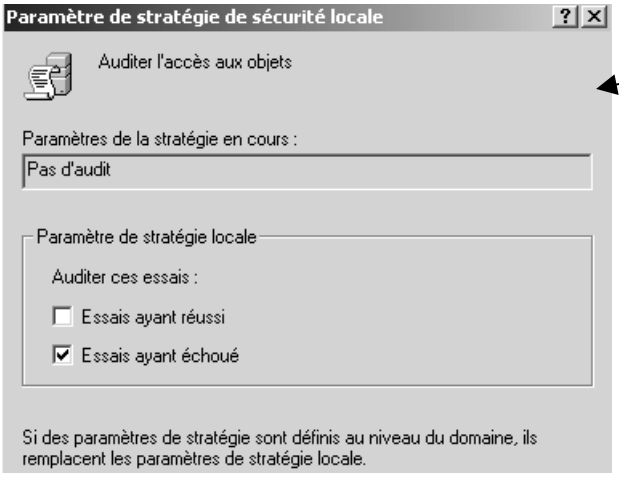
# STRATEGIE AUDIT ACCES DOSSIER

**Objectif :**

On veut savoir qui essaye d'utiliser (alors qu'il n'en a pas le droit) le dossier de pierre, qui contient des documents confidentiels mis à disposition pour certains de ses collègues.

Il faut d'abords sur la machine sur laquelle le dossier existe, activer l'audit au niveau des ressources de manière générale.

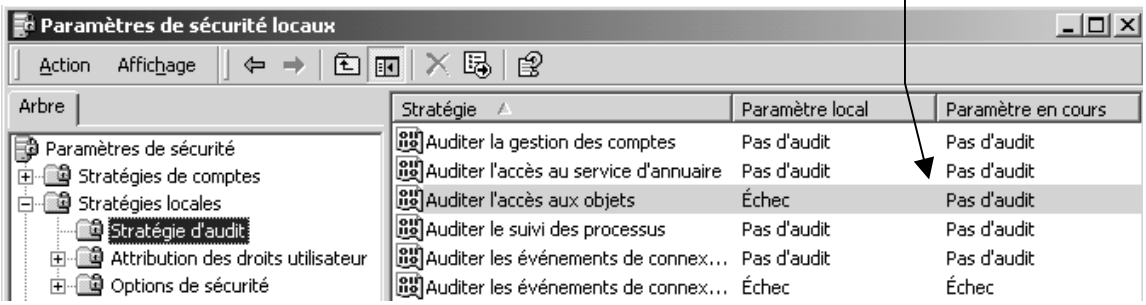


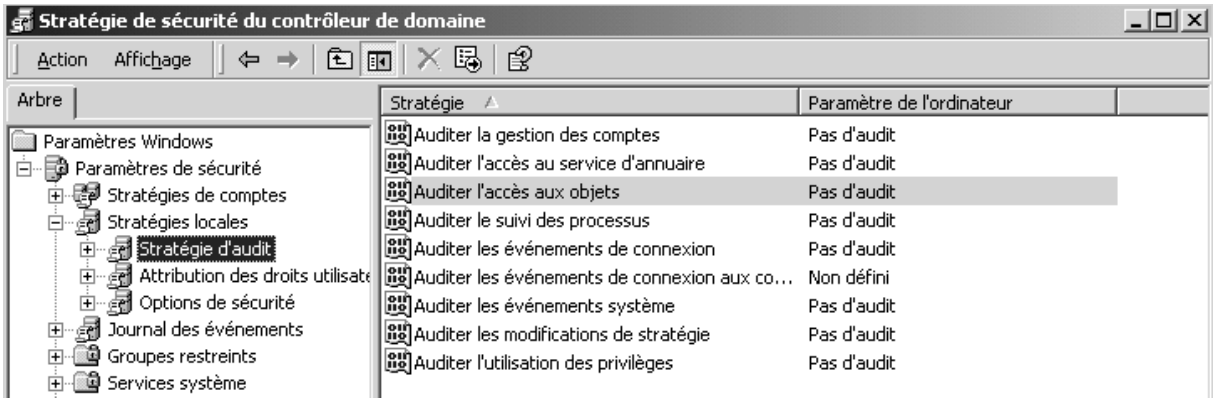

redémarrer

Mais là on obtient une surprise de taille, c'est que la boite de dialogue sécurité locale affiche une information un peu déroutante :

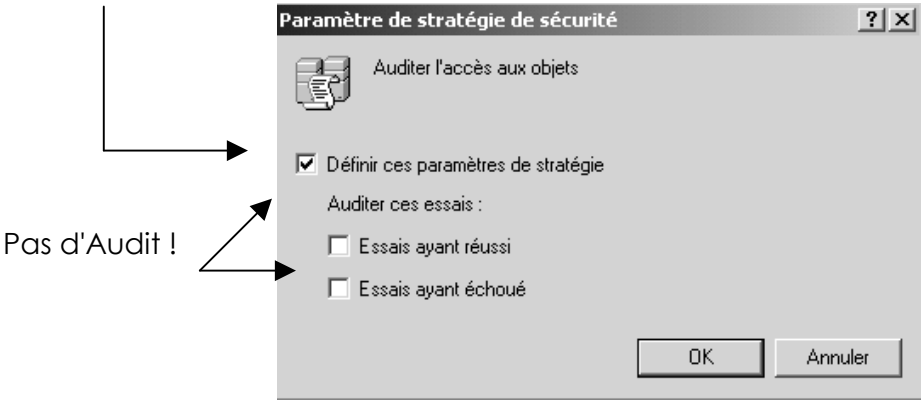
On a bien demandé **Audit sur Echec**, mais **en cours** il y a **pas d'audit** !



Cela provient du fait que pour les contrôleur de domaine, il existe des paramètres que l'on gère dans la mmc **Outils Administration / Stratégie de Sécurité du contrôleur de domaine** passant après les paramètres de sécurité locaux d'une machine…



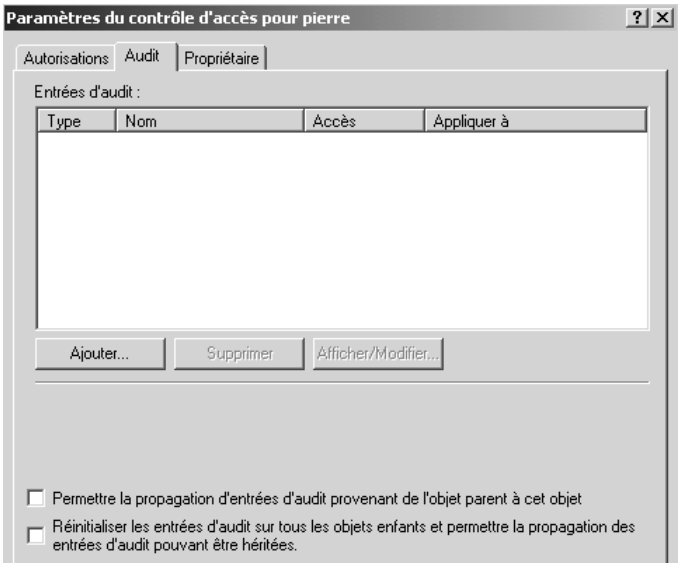

Or ceux-ci sont positionné par défaut à




Soit on demande de désactiver à ce niveau, et on garde la commande dans les permissions de sécurités locales, soit on "force" ici en demandant d'activer l'audit sur les ressources en cas d'Echec…

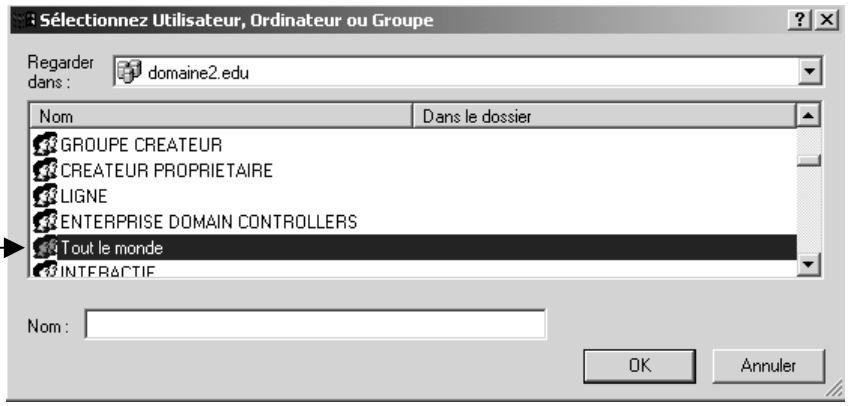
puis il faut pour le dossier de pierre accéder aux permissions NTFS et demander **Avancée**

on a alors

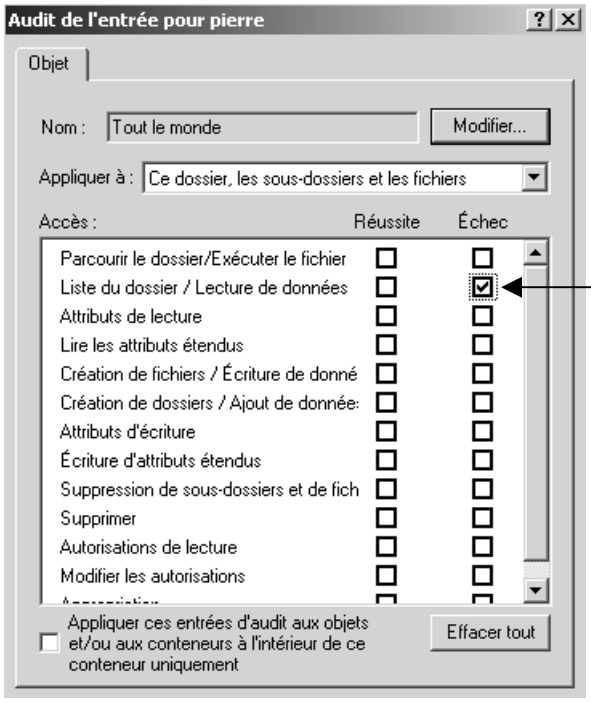



Dans laquelle il faut **Ajouter**

Le groupe prédéfini **Tout le monde**

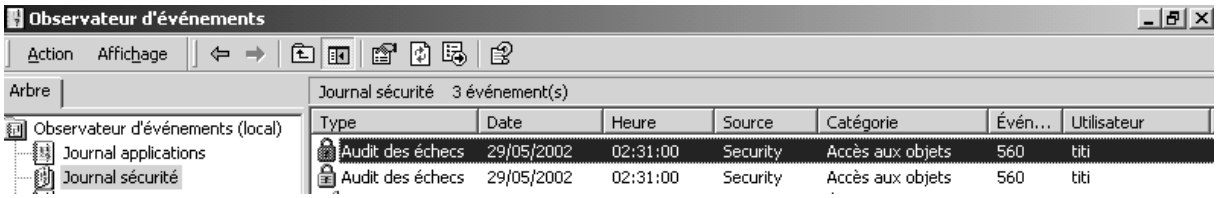



et en indiquant l'audit voulu :

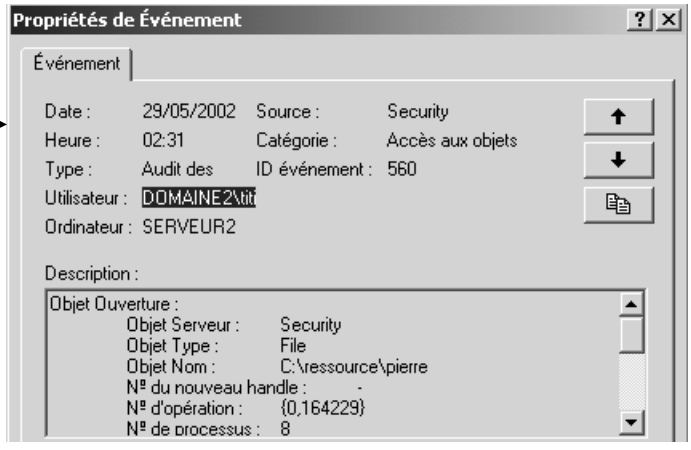



Audit sur **Echec** pour la lecture (tentative...)

Lorsqu'un utilisateur non autorisé tente la lecture du dossier de pierre,




L'événement est consigné



# STRATEGIE AUDIT IMPRIMANTE

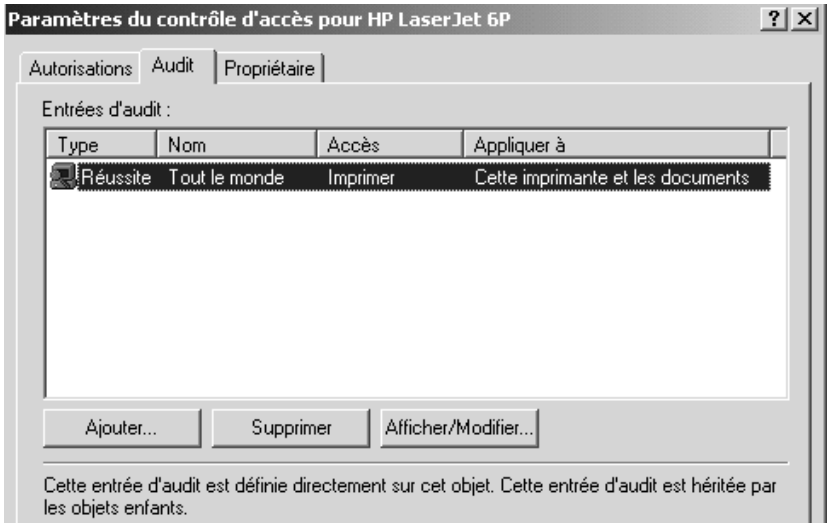
**Savoir qui imprime :**

Il faut activer l' Audit "**Accès aux objets**" dans les stratégies locales de l'ordinateur sur lequel l'imprimante est connectée.

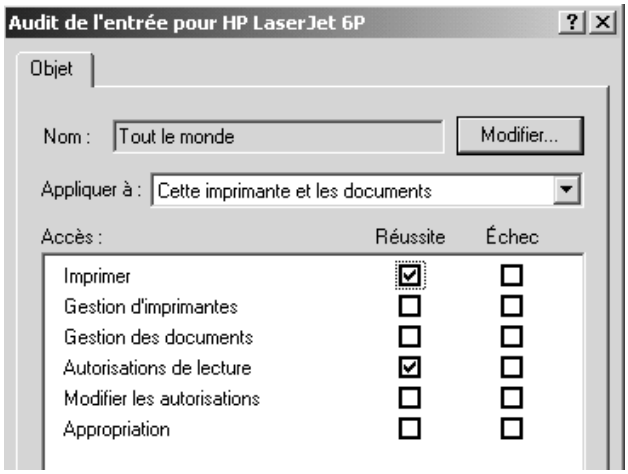
On doit demander **Audit sur Réussite**

Ensuite il faut se placer sur l'imprimante que l'on souhaite auditer, et demander dans les propriétés de l'imprimante:

onglet **Sécurité / Avancées** et onglet **Audit**…



avec



# MODELE DE STRATEGIE LOCALE

**Objectif :**

Obtenir sur disquette 3 modèles de stratégie locale, permettant de définir via un message qui s'afficherait avant l'invite d'ouverture de session, l'appartenance de la machine a un groupe particulier…

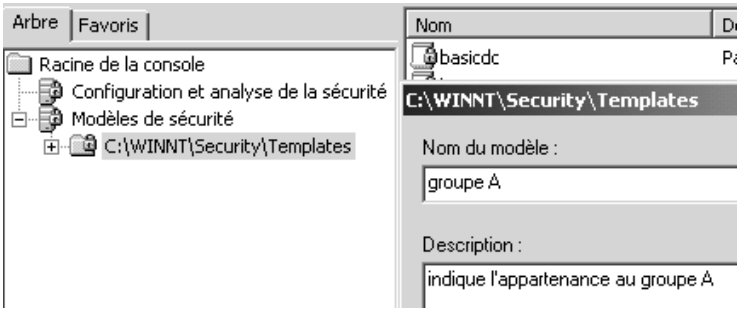
On pourrait ainsi disposer de 3 modèles :

1. Un modèle affichant l'appartenance à un « groupe A »
2. Un modèle affichant l'appartenance à un « groupe B »
3. Un modèle n'affichant plus aucune appartenance (efface les effets des modèles précédents…)

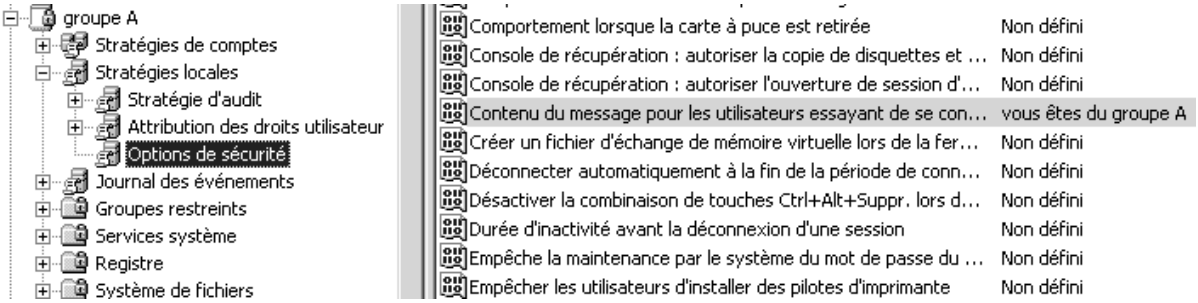
Rappelez vous que les stratégies sont définies dans des fichiers xxxx**.inf** stockés en général dans **Winnt\Security\Templates**

**Création et sauvegarde d'un modèle :**

Après avoir lancé (crée ?) la console , on se crée un nouveau modèle correspondant au groupe A…

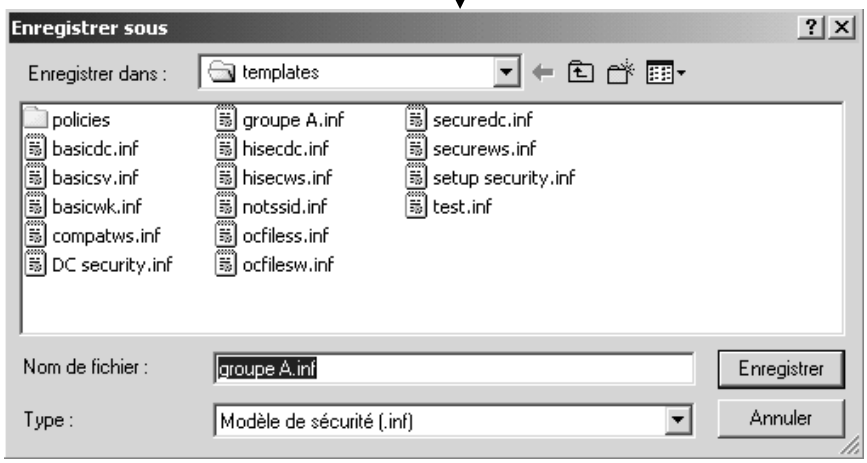



dans lequel on défini uniquement le titre et le contenu du message pour les utilisateurs essayant de se connecter



pour enregistrer le modèle on peut bien sur enregistrer classiquement, puis copier manuellement le fichier sur disquette, mais on peut aussi demander directement **enregistrer sous**…


Et choisir classiquement !

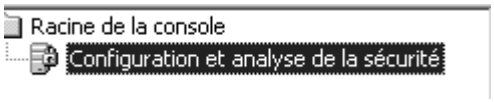



Si on a appliqué le modèle, il est possible de demander **exporter le modèle**…

---

**Récupération et utilisation d'un modèle :**

Après avoir lancé (crée ?) la console ,

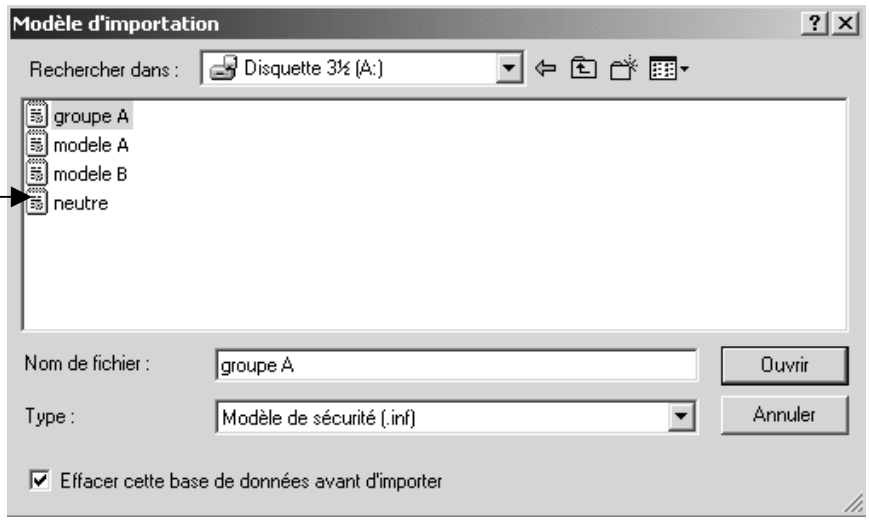



un fois une base de donnée crée (ouverte) il faut récupérer notre modèle.

via le menu contextuel **importer un modèle**...

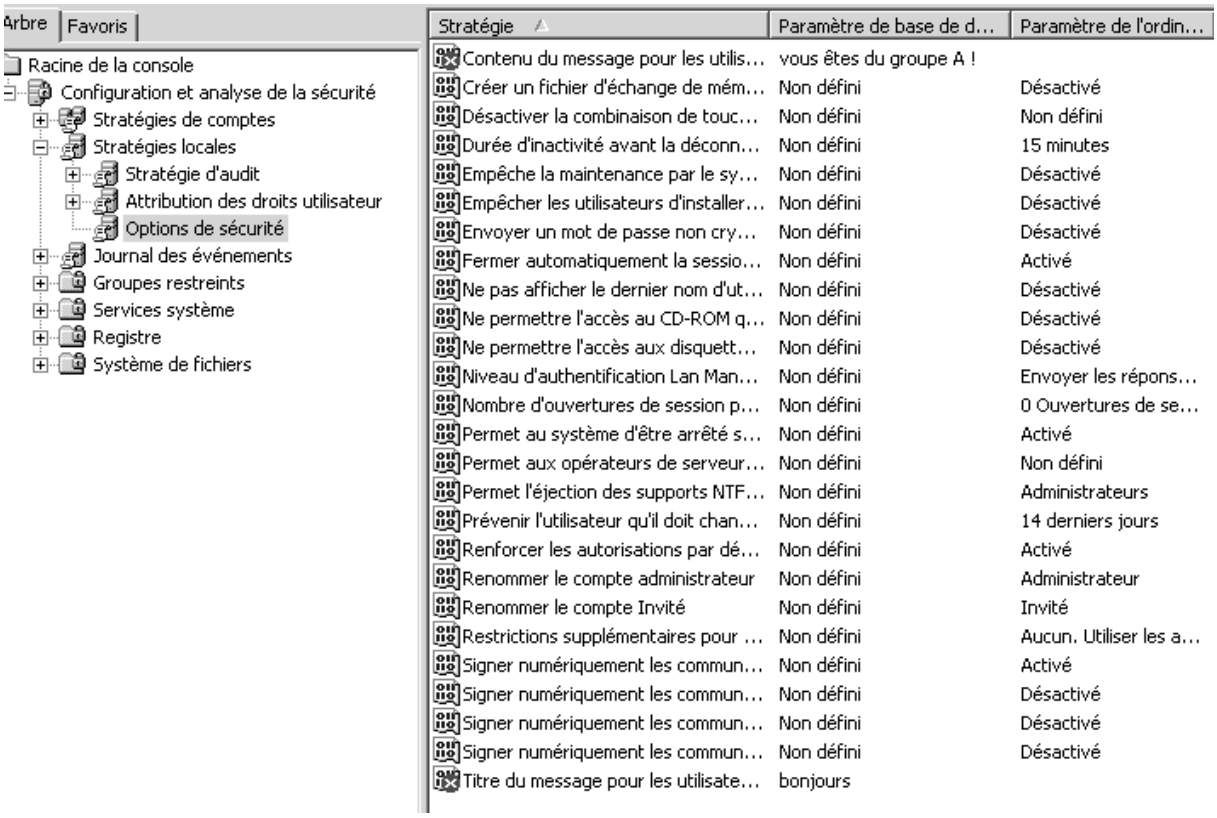
Et choisir classiquement !

On peut si on le veut effacer la modèle pré-existant …



il ne reste plus que l'analyse,

via le menu contextuel **analyser l'ordinateur maintenant**...




et l'application

via le menu contextuel **configurer l'ordinateur maintenant**...

**N.B** : pensez a vérifier l'application de votre modèle….

**N.B** : chargez le modèle de sécurité basic sur votre poste de travail basicwk , analysez votre machine (mais n'appliquez pas….) que peut on dire ?

# CREATION DE GPO SUR UNE UO

**Objectifs :**

Dans le domaine, on dispose de deux services, un service pour les commerciaux, et un autre pour les secrétaires.

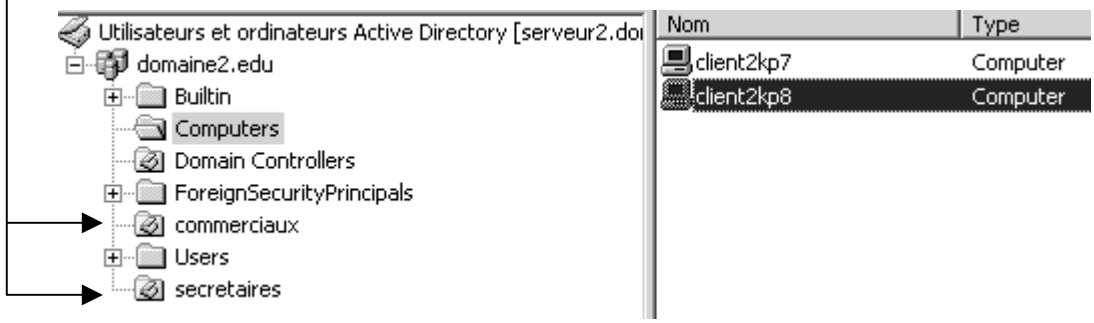
A terme, le gestion des postes des commerciaux est radicalement différente de celle des postes des secrétaires, par conséquent on va se créer des UO et des GPO pour chacune de ces entitées.

- Vérifier que lorsqu'un ordinateur fait partie d'une UO (commerciaux par exemple), il récupère automatiquement sa stratégie…
- Vérifier que pour récupérer la stratégie de l'autre UO (secretaire donc), il suffit de déplacer le compte ordinateur dans l'OU adéquate…

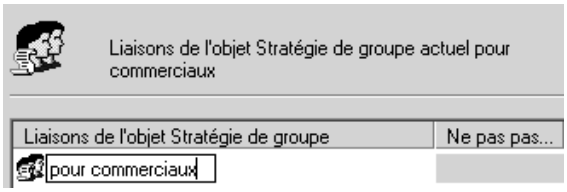
Le but ici étant pédagogique, les GPO n'auront pas d'autres effet que d'annoncer lors d'un message apparaissant à la mise sous tension l'appartenance à telle ou à telle entité (du genre, "bonjours, votre poste est régit par le modèle de sécurité affecté aux commerciaux/ *(ou)secrétaires*….")

**Définir 2 UO dans AD , et créer leur GPO :**

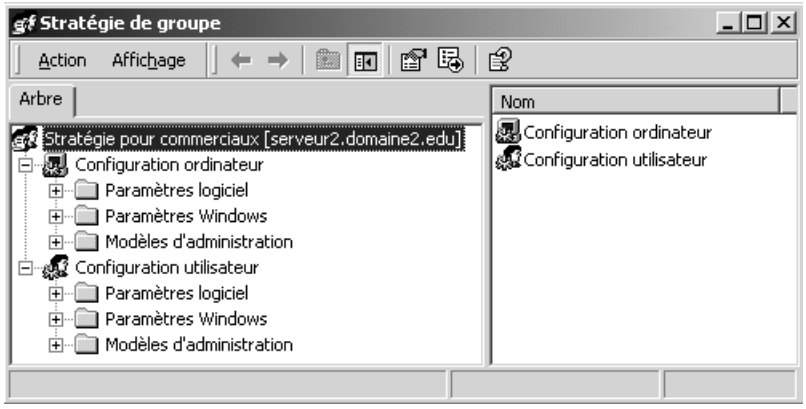
Il faut commencer par se créer deux UO commerciaux et secretaires



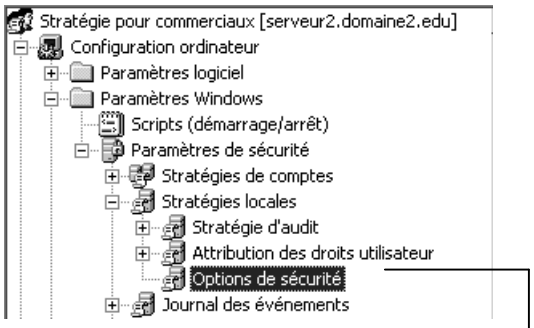

On se place ensuite sur l'UO des commerciaux, et on demande propriété, puis onglet **Stratégie de groupe/ Nouveau**




puis modifier

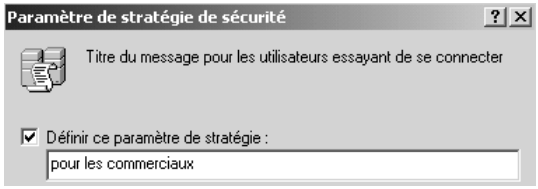


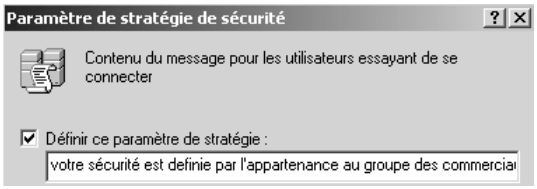

On va créer notre GPO pour les commerciaux affichant notre appartenance au groupe des commerciaux



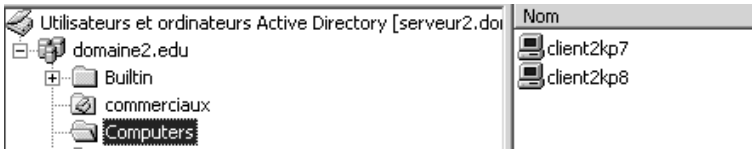

Changeons pour l'exemple uniquement :

1. Titre du message pour…
2. Contenu du message pour…

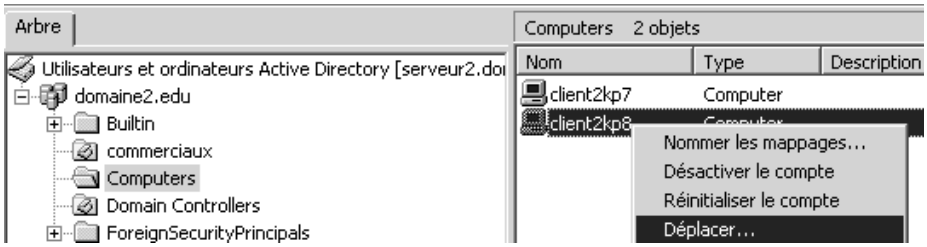


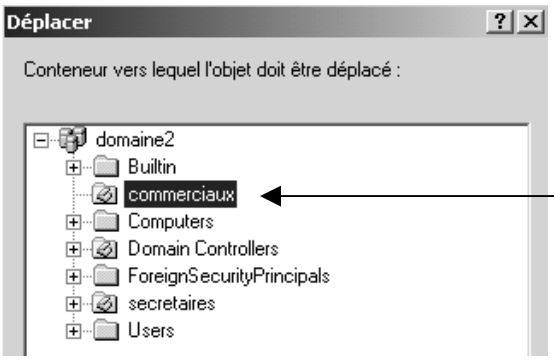

Si on se place sur l'UO prédéfinie **Computers**, on voir normalement tous les postes du domaine…



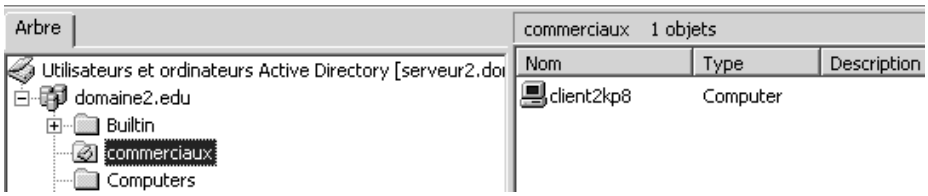

Il est nécessaire de déplacer les postes faisant partie de la section des commerciaux dans leur UO pour qu'ils héritent de leur stratégie. Prenons par exemple client2kp8



on obtient alors




On indique sa nouvelle UO d'appartenance




- vérifier que lorsque l'on démarre le poste, un message indique bien l'appartenance aux commerciaux…

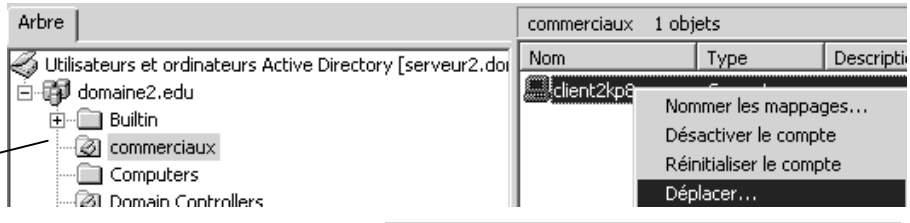
---

**Changer d'UO = changer de GPO :**

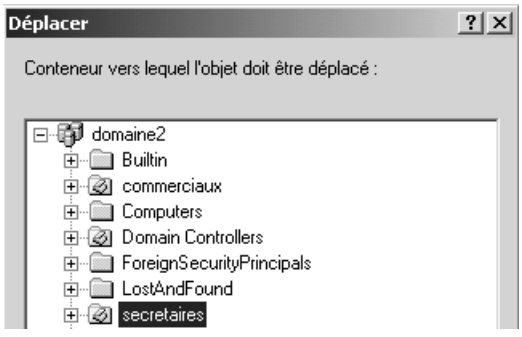
On va créer une GPO pour les secretaire affichant notre appartenance au groupe des secretaire.

Donc on procède de manière identique a ce que l'on a fait précédemment


Puis on déplace le poste faisant partie de la section des commerciaux dans leur UO pour qu'ils héritent de leur stratégie. Prenons par exemple client2kp8, qui "passe" dons de commercial à secretaire…




On indique sa nouvelle UO d'appartenance, de commerciaux on la passe dans secretaire



- vérifier que lorsque l'on ouvre une session, un message indique toujours l'appartenance aux commerciaux…et non pas aux secretaires !

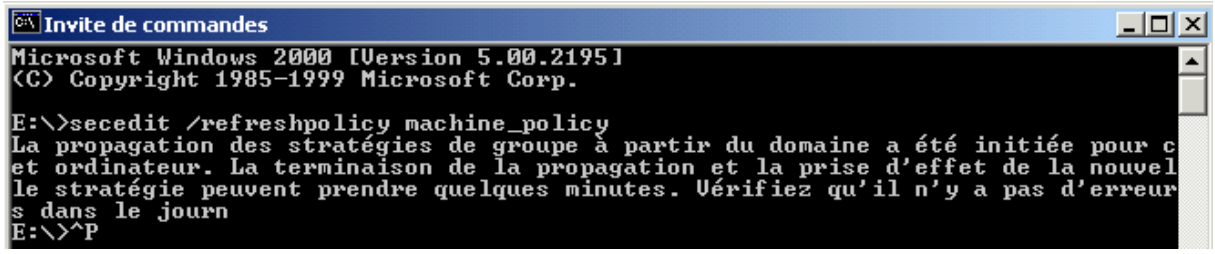
---

**Forcer une application de GPO avec secedit :**

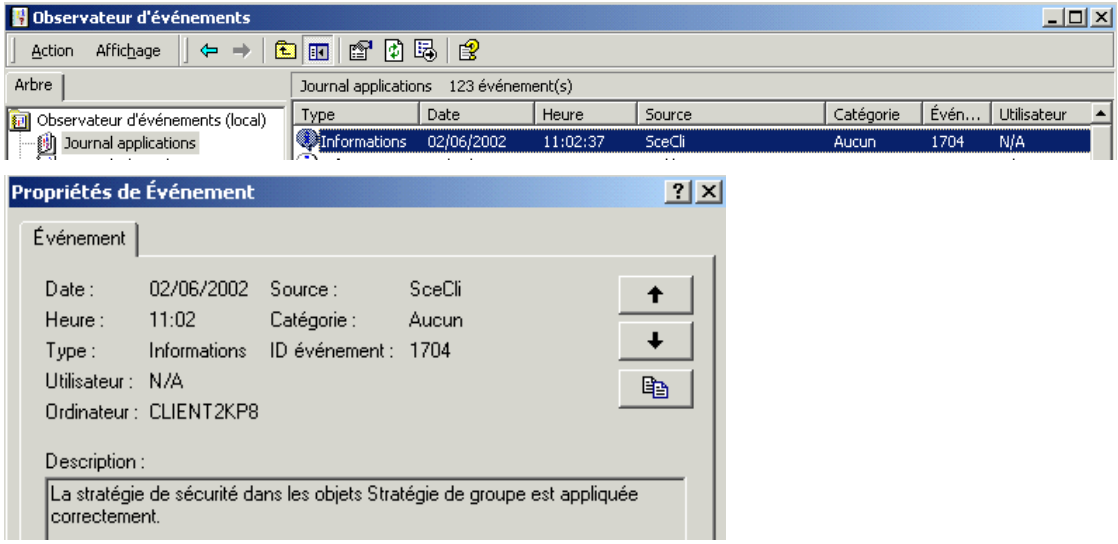
La GPO que l'on construit avec l'UO secretaire et commerciaux, est une GPO d'ordinateur, donc pour être prise en compte, elle nécessite un re-démarrage du poste.

Il est possible avec Secedit de forcer la propagation de cette stratégie, avec la commande :

**Secedit /refreshpolicy machine_policy**




On vérifie dans le journal d'événement que cela s'est bien passé




- vérifier que lorsque l'on ouvre une session, un message indique maintenant l'appartenance aux secretaires !

# GPO MODELE D'ADMINISTRATION DE DOMAINE

**Objectifs :**

Dans un domaine, on souhaite pour tous les utilisateurs du domaine sauf l'administrateur (si on ne veut pas quelle s'applique à l'administrateur, il faut le placer dans une UO spécifique et bloquer l'héritage sur cette UO...) la GPO suivante :

1. Supprimer le menu **exécuter** du menu **Démarrer**
2. Désactiver **Active desktop**
3. Désactiver l'accès au **Panneau configuration affichage**
4. Exécuter uniquement les applications prévues
5. Désactiver **Windows Update**

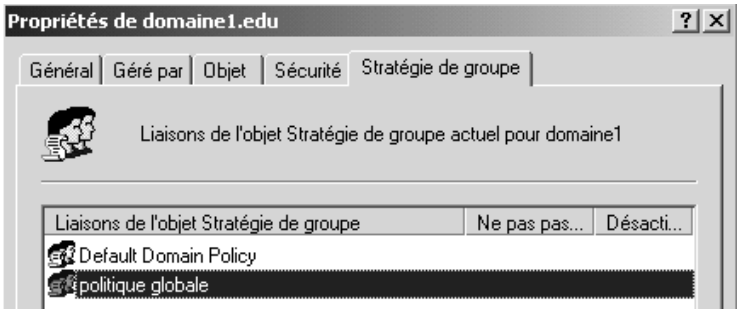
**Blocage de la stratégie pour l'administrateur:**

Puisque l'on va définir une GPO sur des utilisateurs, on bloque l'héritage sur une l'UO que l'on définie manuellement, dans laquelle tous les utilisateurs sur lesquels on ne veut pas que notre GPO de domaine s'applique …( a savoir pour nous l'administrateur)


on bloque l'héritage de L' UO contenant l'administrateur…

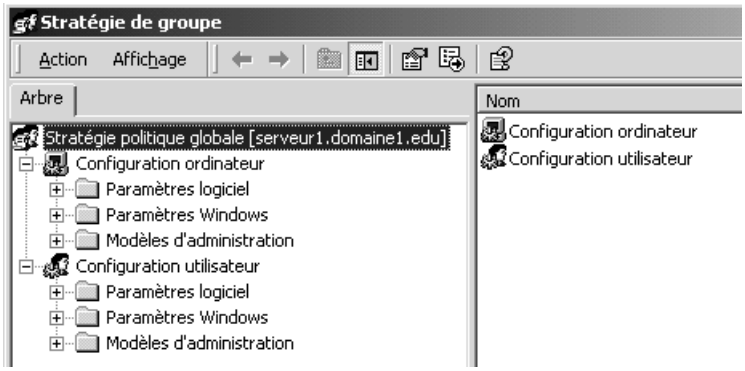
**Mise en oeuvre de la stratégie de domaine :**

En se plaçant sur le domaine, on grée une nouvelle GPO nommée « **politique globale** »




**N.B** : Il vaut mieux créer une nouvelle GPO que modifier la GPO **Default Domain policy** existante par défaut…

Puis on demande **modifier**…




Bien sûr il faut appliquer cette GPO sur le client, soit on attends le temps de propagation standard, soit on force depuis le client via la commande

**Secedit /refreshpolicy machine_policy** (si c'est une config ordinateur)

**Secedit /refreshpolicy user_policy** (si c'est une config utilisateur)

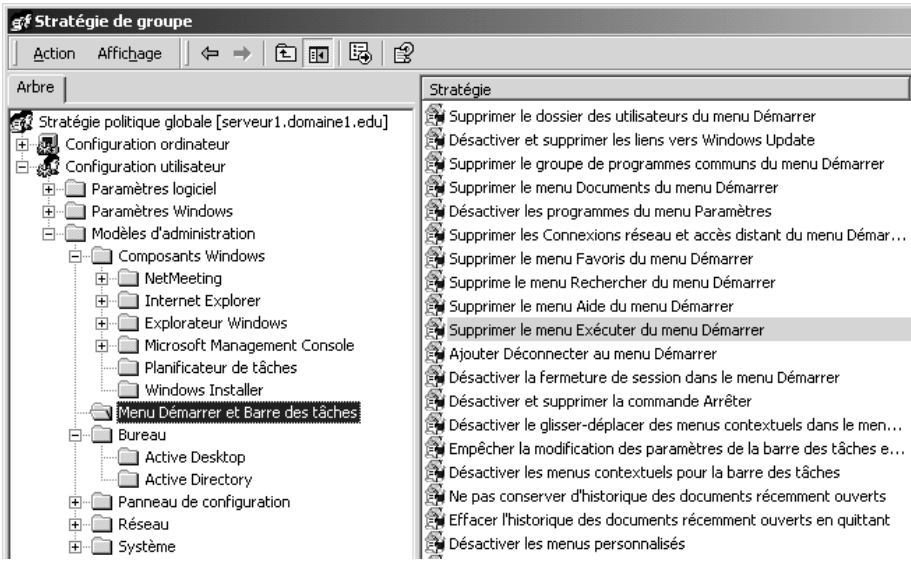
1. Supprimer le menu exécuter du menu Démarrer…

Configuration utilisateur,

Modèles d'administration,

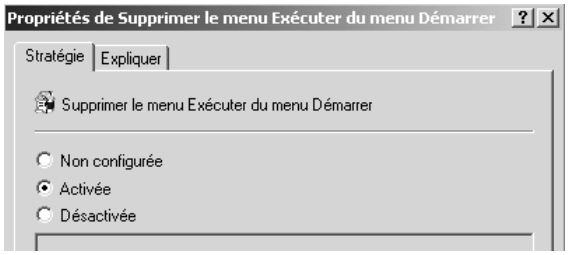
Composants Windows,

Menu Démarrer & barre des tâches

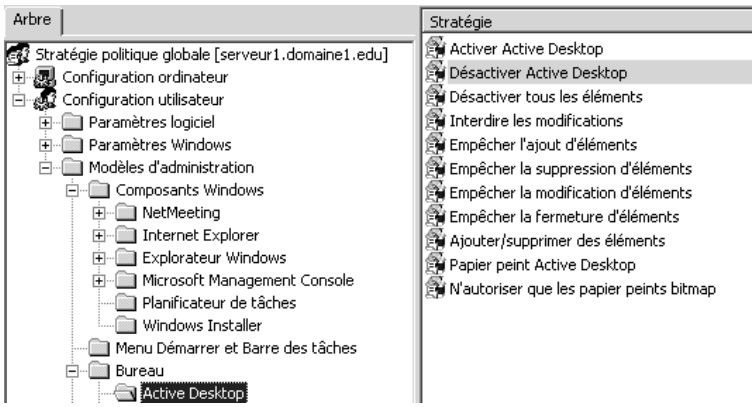



on demande d'activer la GPO,

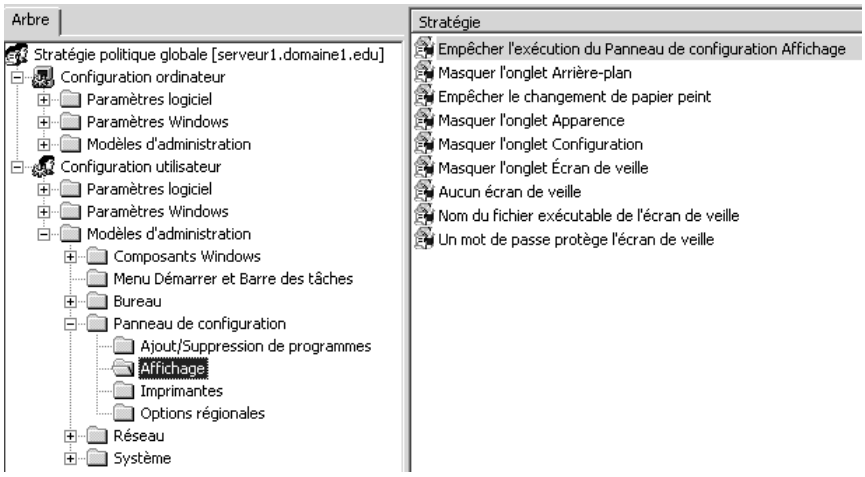
qui supprime le menu



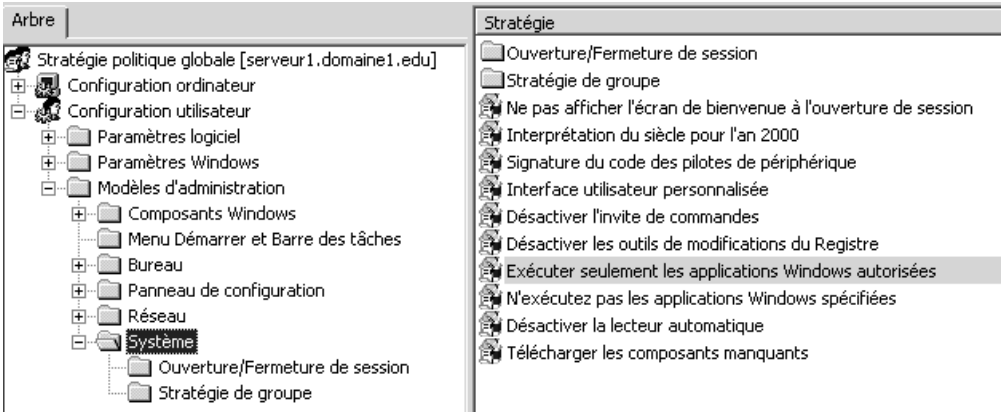
2. Désactiver **Active Dekstop**

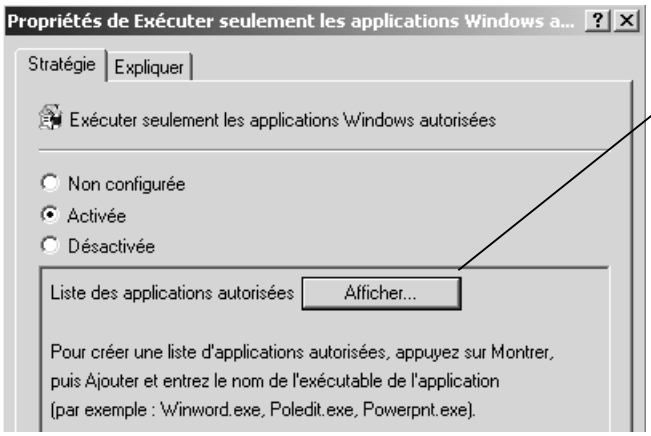



3. Désactiver l'accès au **Panneau configuration affichage**



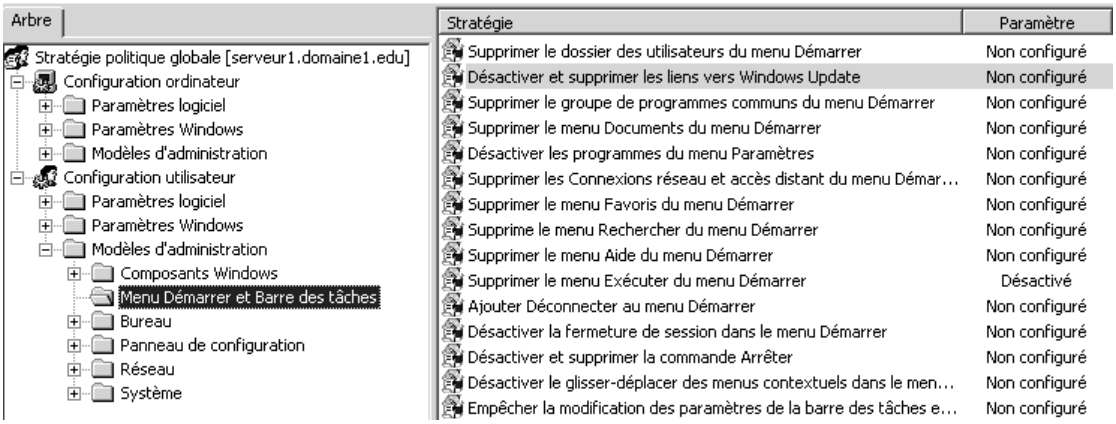

4. Exécuter uniquement les applications prévues !




On spécifie tous les exécutables pouvant être lancés

5. Désactiver **Windows Update**



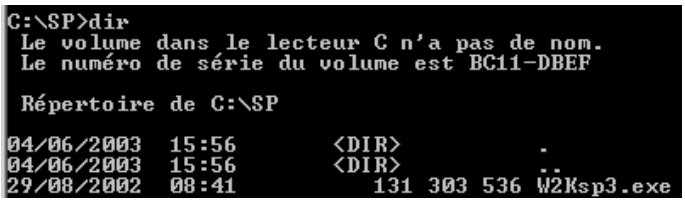
# GPO DEPLOIEMENT DE SERVICE PACK

**Objectifs :**

Déployer automatiquement un SP sur un ensemble de machine …

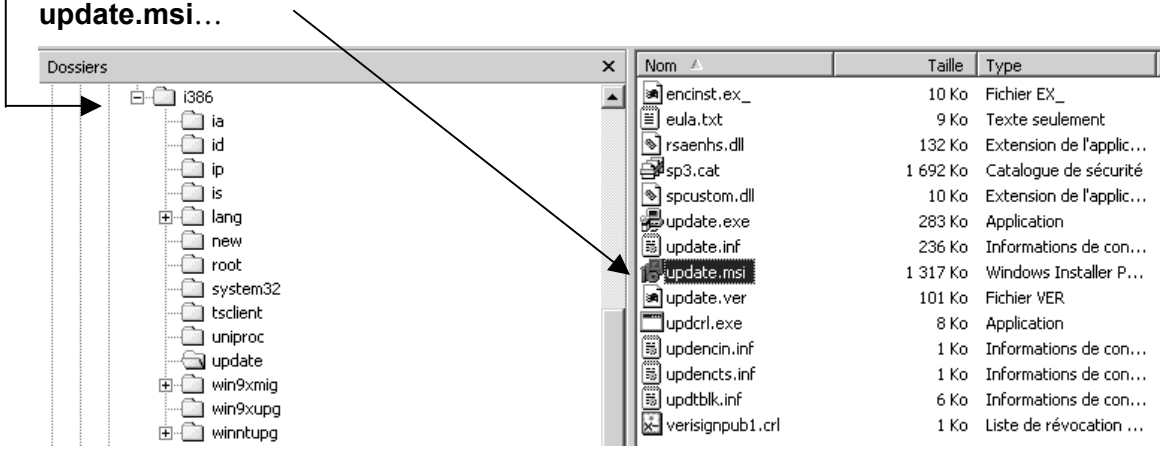
**Mise en oeuvre :**

Dans un dossier que l'on partage en lecture seule, on copie le source du SP3,

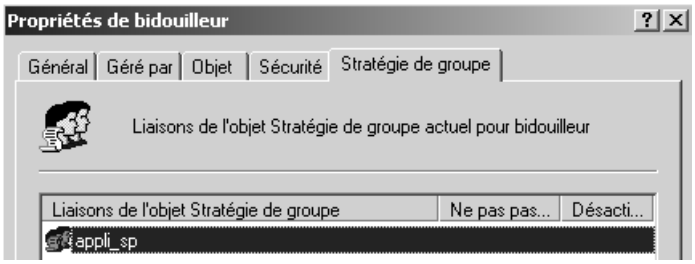



que l'on explose via la commande **w2ksp3.exe –x** dans le même dossier…

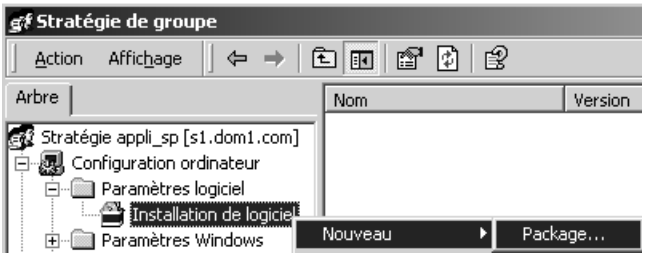
on peut observer qu'un dossier **/i386/update** est crée contenant un fichier **update.msi**…




On se crée ensuite une GPO

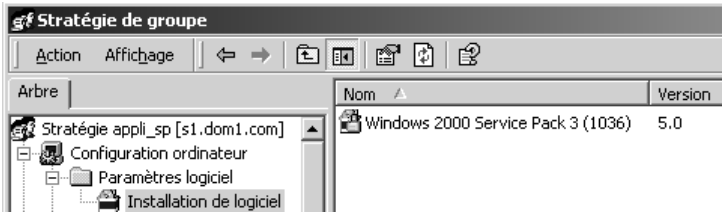



dans laquelle on va choisir une **configuration d'ordinateur**…




on va chercher un chemin réseau amenant à notre **\\serveur\Sp\i386\update\update.msi**

on devrait arriver à cela




| État du déploie... | Installation automatique | Type de mise à niveau | Mise à niveau | Paramètr... | Source |
|---|---|---|---|---|---|
| Attribué | Oui | Nécessaire | Aucun | Français ... | \\S1\sp\i386\update\update.msi |

Il n'y a plus qu'à disposer les UC voulues dans notre UO... et redémarrer les postes...

# CREATION D'UN LOT MSI

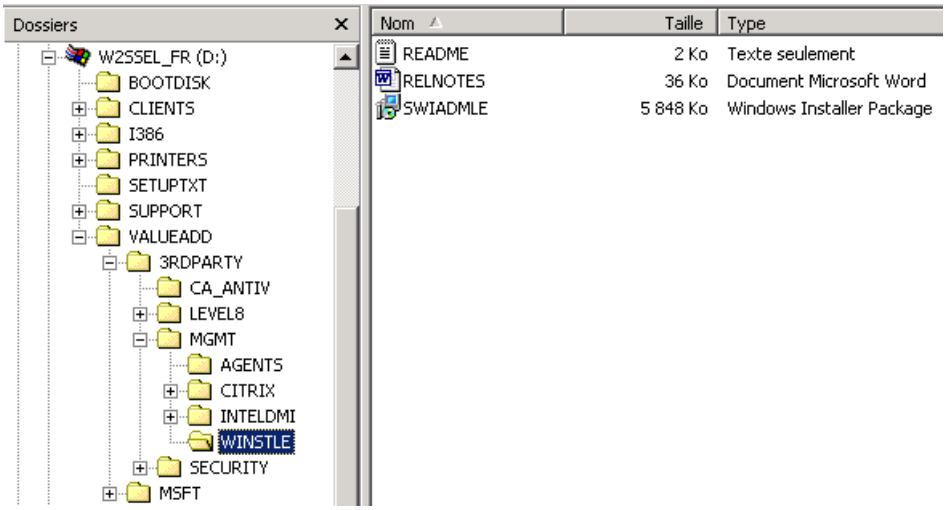
**Objectifs :**

Dans le but d'effectuer un déploiement par GPO, il nous faut un fichier MSI adéquat…

Il est possible de s'en créer un, soit avec des outils professionnels, soit avec un outils livré en "démo" avec windows 2000…

**Installation du logiciel création de msi :**

Il est stocké sur tous les CD 2000, on prends le fichier **SWIADMLE.MSI**…




on obtient de nouveaux raccourcis:

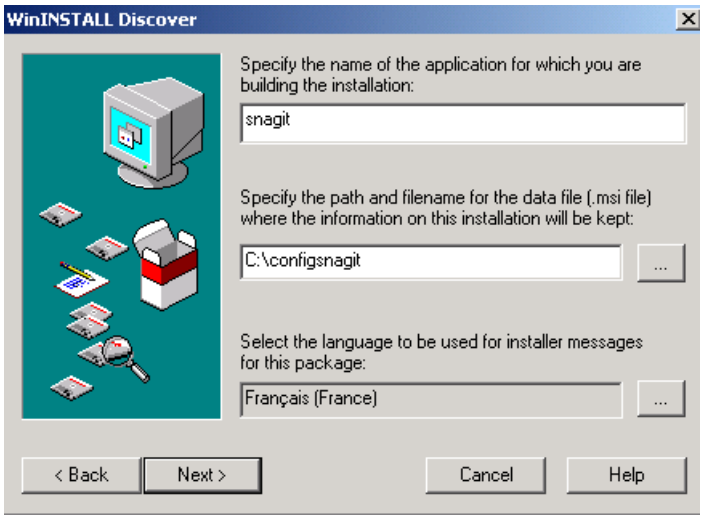

Le principe de création d'un fichier msi est le suivant:

1. il va falloir faire un instantané du système "avant" l'installation du programme pour lequel on veut faire un fichier msi,
2. puis un instantané "après" l'installation du programme
3. et le soft crée un différentiel entre les deux…

**N.B:** Bien sûr ceci doit se faire sur une machine dont la configuration logicielle est la plus proche possible de celle des machines cibles…

**instantané avant:**

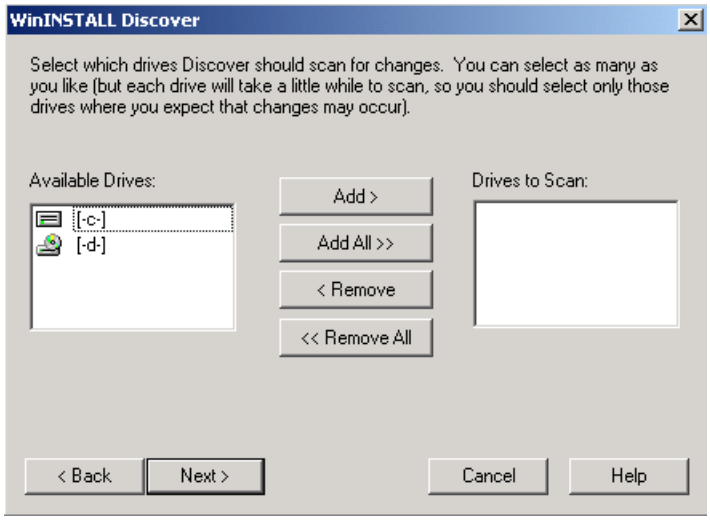
on démarre Veritas Discover, puis NEXT, puis



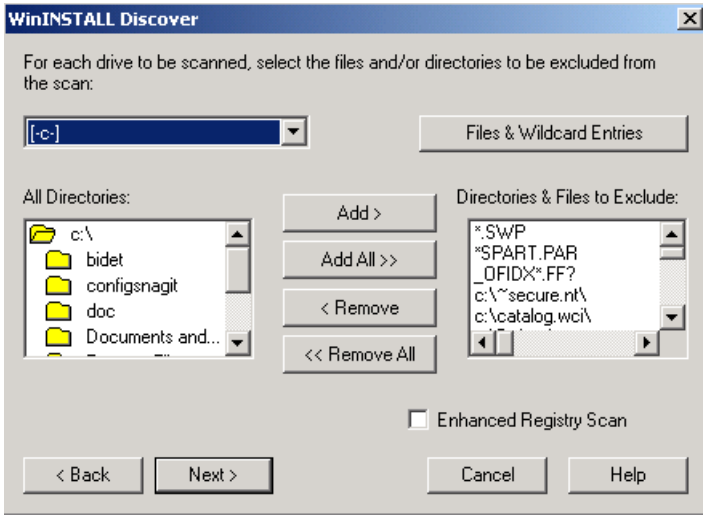

On indique le nom de l'application

Et l'endroit ou le MSI doit être crée à terme…

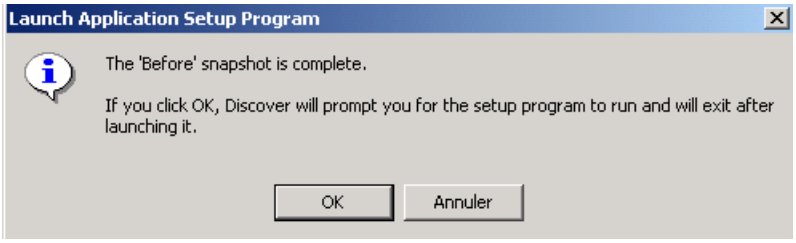
on choisit un disque ou il y a de la place (pour stocker les fichiers d'enregistrement de config) et ensuite on précise puis les disques a surveiller...




et s'il faut exclure certains dossiers de … "la surveillance"

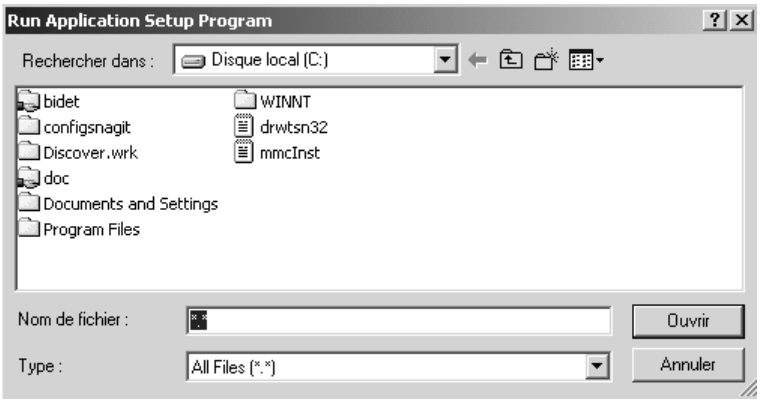


puis le travail se fait et un message comme quoi la configuration actuelle est mémorisée apparaît.




**Installation du logiciel pour lequel on veut un msi :**

Dans la foulée,




et on peut paramétrer le logiciel, et ses points de lancement (raccourcis, modif de menu…)

**instantané après:**

l' instantané après se lance comme pour l'instantané de début …

on obtient dans le dossier indiqué au début (pour nous le dossier **C:\configsnagit** ) la totalité de ce que l'on doit publier y compris le fichier msi de départ… !

le reste est désormais routinier….

# EFS - CRYPTAGE DE FICHIER

**3 utilisateurs indépendants :**

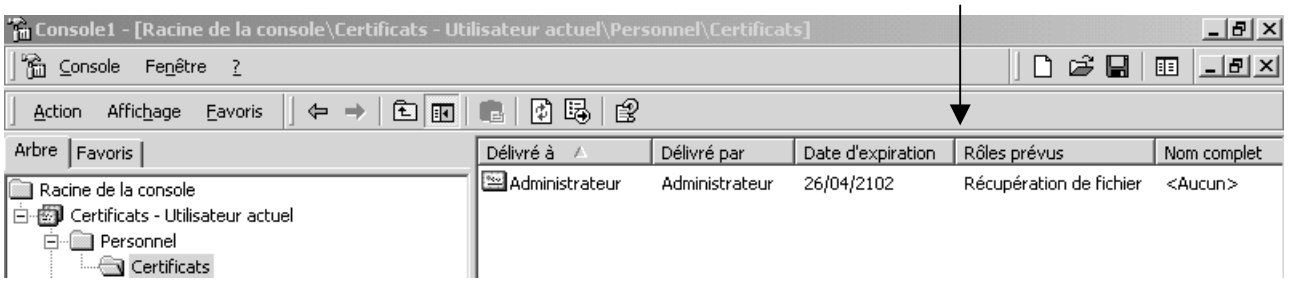
Soit sur une machine 3 utilisateurs farouchement indépendants, pierre, paul jacques, pour lesquels il faut s'assurer que ils ne puissent absolument aller lires leurs documents respectifs…

On décide que le dossier dans lequel ils doivent poser leurs document est le dossier DATA, sur lequel on activera le cryptage. En tant qu'administrateur du poste, on active le cryptage du dossier DATA…

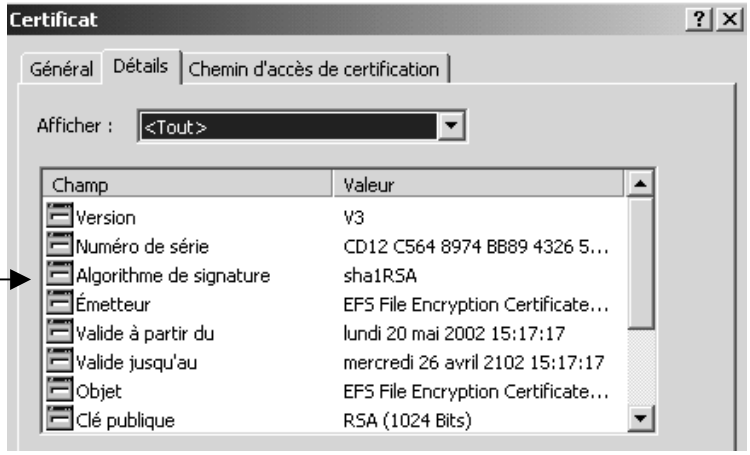
Vérifier que lorsqu'un document y à été crée par pierre il y est automatiquement crypté avec la clé personnelle privée de pierre, et par conséquent ni paul ni jacques ne peuvent y accéder…. (mais que l'administrateur, agent de récupération par défaut, peut)

## sur une machine autonome

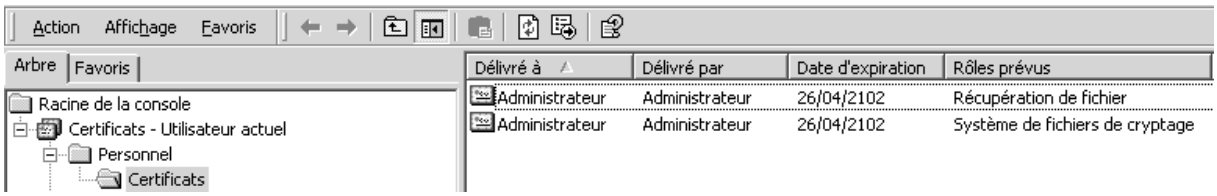
sur une machine autonome, c'est l'administrateur qui est agent de récupération : ici on a ouvert une mmc avec ses certificats. par défaut




et dans les propriétés on voit bien que le système EFS a demandé le certificat lors de l'installation du poste




Si l'administrateur crypte lui même un dossier, il se voir attribuer un certificat d'identification pour la diffusion de sas clé publique…




## Dans un domaine

```
E:\>cd data

E:\data>efsinfo

E:\data\

pierre.doc: Encrypted
  Users who can decrypt:
    CLIENT2KP8\pierre (CN=pierre,L=EFS,OU=EFS File Encryption Certificate)

E:\data>efsinfo /r

E:\data\

pierre.doc: Encrypted
  Recovery Agents:
    DOMAINE2\Administrateur (OU=EFS File Encryption Certificate, L=EFS, CN=Admin
istrateur)

E:\data>_
```

**N.B** : dans cet exemple, le fichier crypté par l'utilisateur local **pierre** du poste **client2kp8** est crée sur une machine **appartenant à un domaine DOMAINE2**. Par conséquent seul l'administrateur de domaine est l'agent de récupération. une fois que le fichier sera placé sur la machine contrôleur de domaine (le serveur initial de config de domaine, car seulement sur cette machine il y a le certificat de l'administrateur du domaine). Si cela ne convient pas, et que l'on veut ouvrir le fichier sur le poste ou il a été crée, il faut y ouvrir une session en tant qu'administrateur du domaine, et y ajouter les certificats préalablement exportés depuis le contrôleur de domaine : A NE PAS FAIRE POUR DES RAISONS DE DISPERTION DES CERTIFICATS !)

**N.B** : Si le poste se **déconnecte** du domaine, on n'aurait alors plus d'agent de récupération pour ce fichier… (si on s'y reconnecte, on retrouve notre agent de récupération)

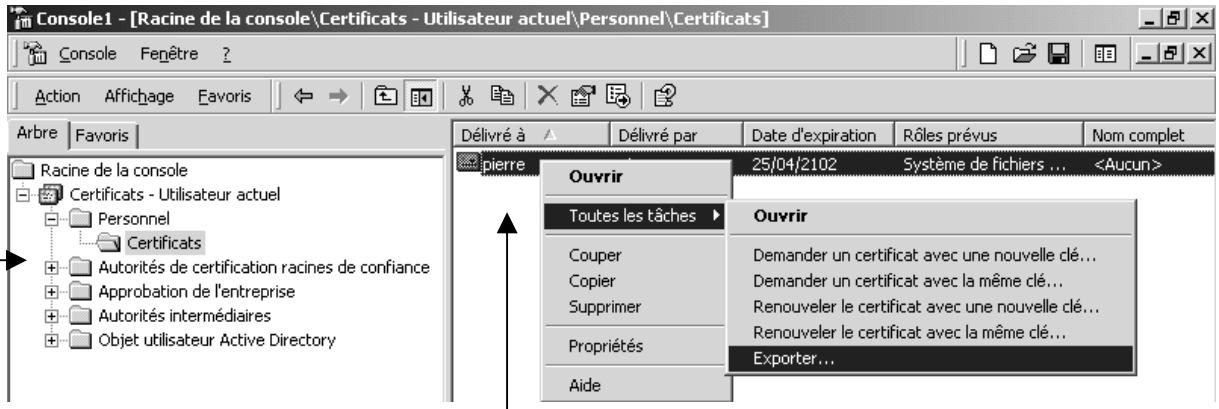
```
E:\data>efsinfo /r

E:\data\

pierre.doc: Encrypted
  Recovery Agents:
    Unknown (OU=EFS File Encryption Certificate, L=EFS, CN=Administrateur)
```

**Exportation Import de certificat :**

Pour pouvoir faire en sorte que paul puisse modifier le fichiers cryptés par pierre, il faut exporter le certificat de pierre, et l'importer pour paul

## Exportation du certificat de pierre sur disquette

Ayant une session pour pierre, on crée une mmc certificats

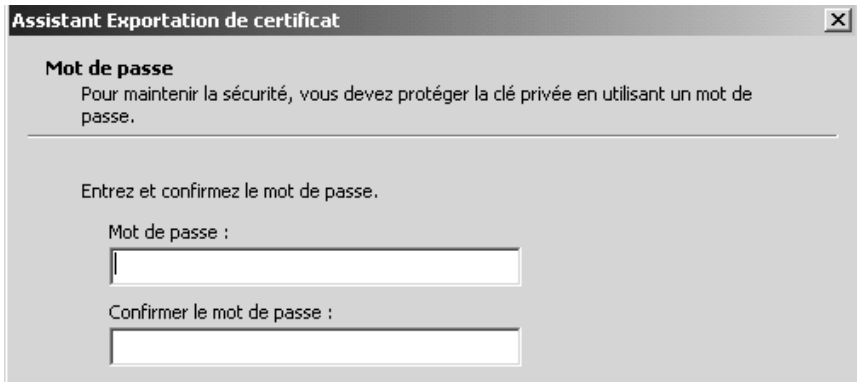



On se place sur certificats à gauche, puis menu contextuel sur le certificat de pierre

Dans laquelle on va enclencher l'exportation de certificat avec la clé privée de Pierre

Les étapes sont claires


Avec exportation de la clé privée

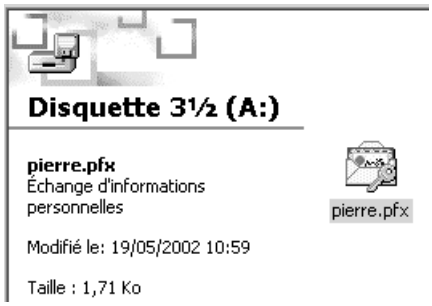




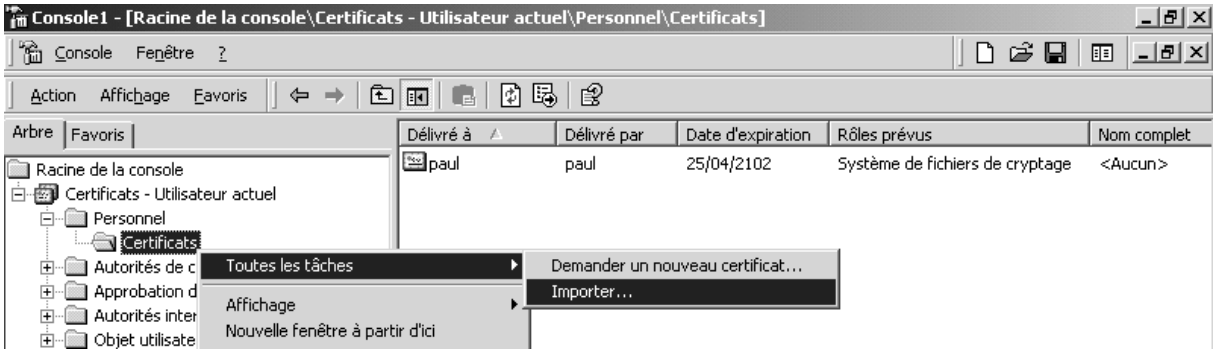
A partir de là, on dispose du certificat de pierre (et de sa clé privée) sur une disquette. Il reste à le donner à paul…

## Importation du certificat de pierre dans paul

Ayant une disquette contenant le certificat de pierre,

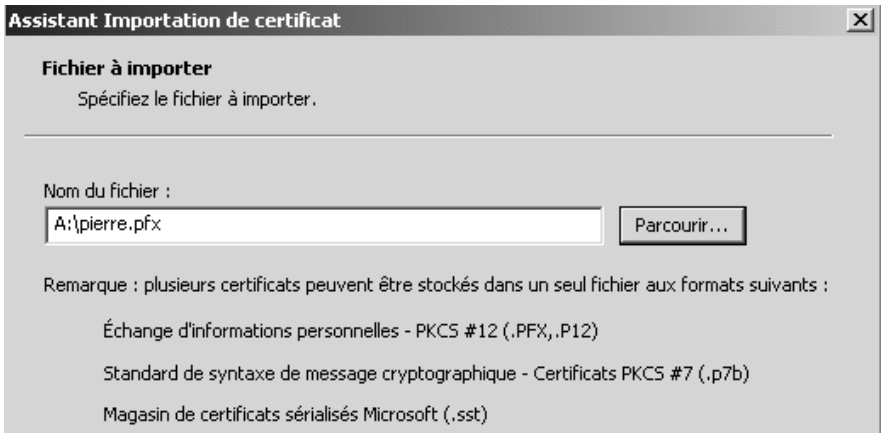


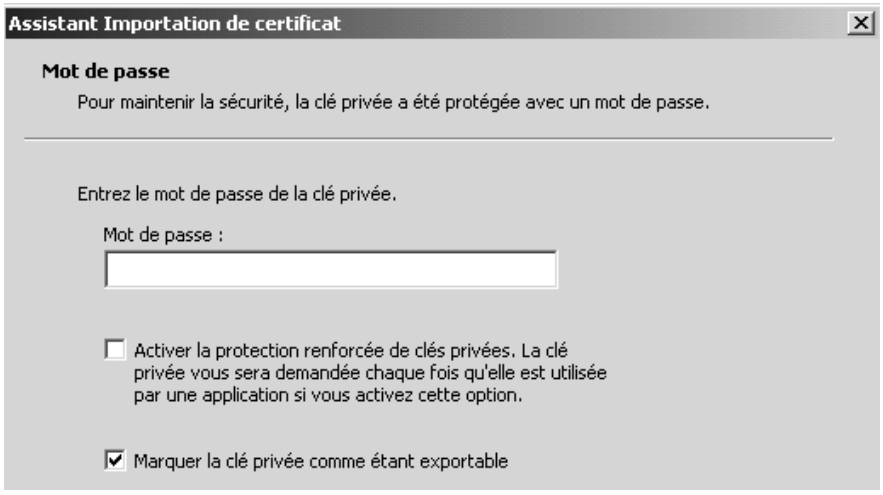

et ayant ouvert une session pour paul, on crée une mmc certificats



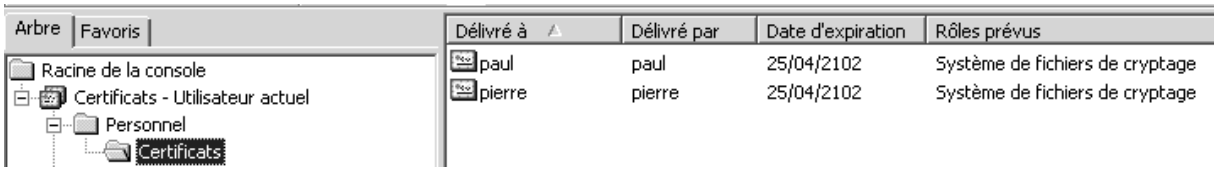

On se place sur certificats à gauche, puis avec le menu contextuel

on va enclencher l'importation de certificat avec la clé privée de Pierre…




Lorsque l'assistant se termine on devrait avoir

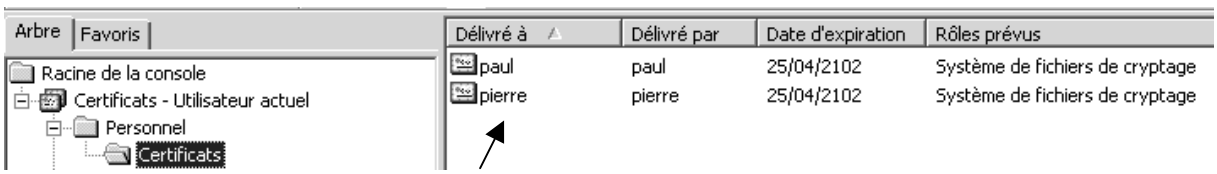



et paul peut désormais modifier les documents de pierre

## Annulation non rétro-active de l'import de certificat

Le temps passe, et paul se fâche avec pierre, comment peut on empêcher paul d'accéder aux fichiers de pierre ?

Il faut ouvrir une session en tant que Paul, aller dans les certificats…




et supprimer le certificat de pierre dans sa liste de certificats…

Pourquoi Pierre peut il toujours modifier les documents déjà existant de pierre ? car s'il les a déjà ouvert, leur champs liste DRF (liste des agents récupérateurs) inclus l'utilisateur Pierre comme personne habilité à les gérer.

Par contre, si maintenant Paul crée d'autres documents, ceux-ci sont inutilisables à Pierre

# EFS – SECURISER UN POSTE

**Vol d'un poste (portable ?) :**

Si on a compris le principe de la sécurisation, on a compris que sur une machine, par défaut le Compte de l'Agent de récupération par défaut est celui de l'Administrateur de Domaine (dans le cas d'une machine faisant partie d'un domaine) ou le compte de l'Administrateur Local…

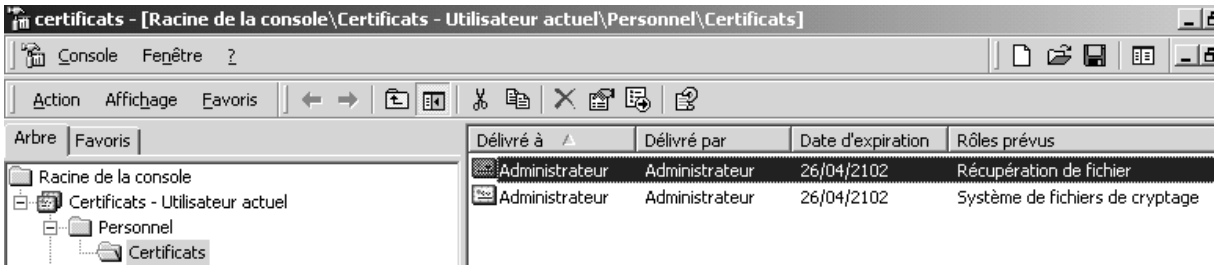
Si on sécurise le dossier mes documents par exemple, le seul compte permettant de visualiser tous les fichiers est donc celui de l'agent de récupération…

Pour sécuriser au maximum une machine, il suffit d'exporter le certificat du compte de l'agent de récupération, en exportant sa clé privée en un endroit sûr, par exemple une disquette que l'on stockera en un lieur sur !

A partir de la , l'agent de récupération n'existe plus !!!!! il faut pour le « reconstruire » que l'on importe le certificat et sa clé privée, ce qui suppose d'avoir accès à la disquette ….

**Export du certificat de l'agent de récupération d'un poste autonome :**

Le poste étant autonome (hors Domaine), il faut ouvrir une session en tant qu'administrateur local…

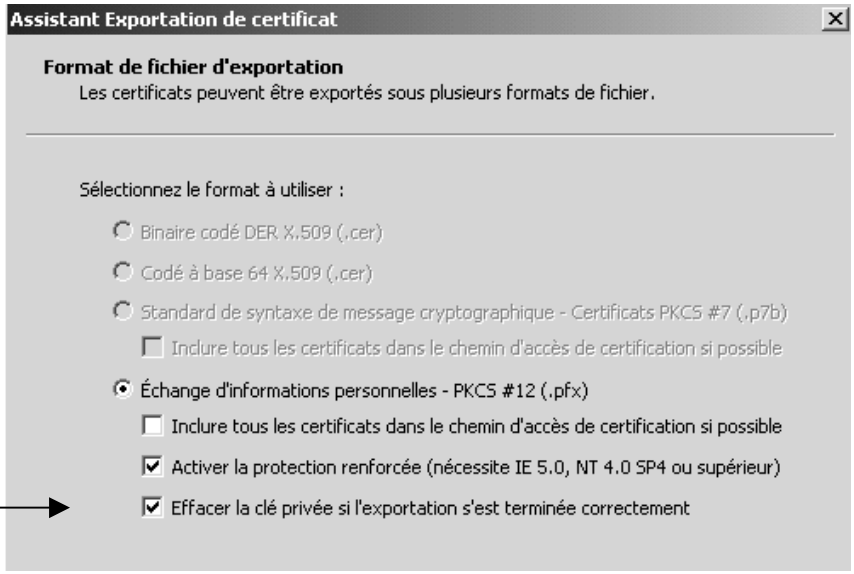



et demander d'exporter

dans l'assistant il faut indiquer alors


et surtout

Sinon la clé est laissée localement

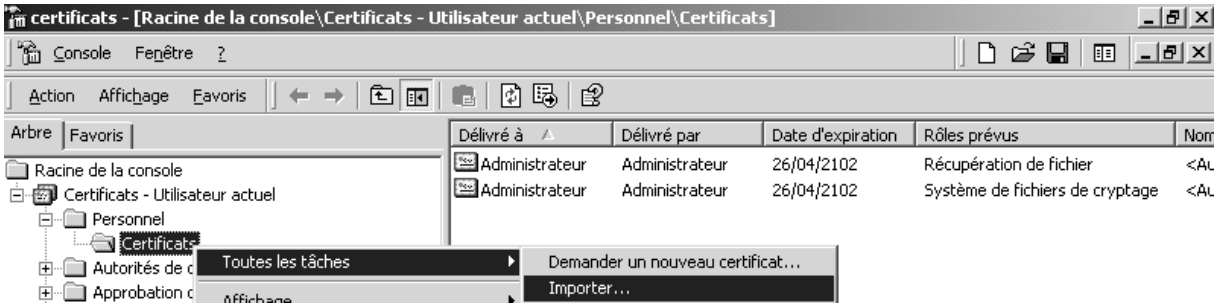



Vérifier que désormais l'administrateur n'est plus agent de récupération (ou plutôt il est **toujours agent de récupération**, mais ne **dispose plus de la clé privée**…)

---

**Import du certificat de l'agent de récupération d'un poste autonome :**

En cas de problème, on ouvre une session en tant qu'administrateur et on demande d'importer la clé




depuis la disquette…


**N.B** : pour que cela marche, la clé ne suffit pas, il faut la réimporter dans le compte qui est agent de récupération par défaut… (ici administrateur local). Ainsi une tentative d'import de la clé dans un autre compte quelconque du poste , se solderait par un échec de la lecture des fichiers cryptés !

donc deux choses importantes :

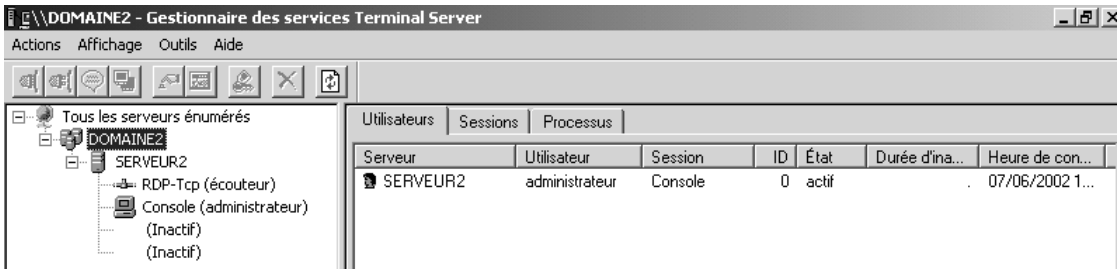
**le compte administrateur (agent de récupération)**

**la clé privée exportée dans la disquette**

# SESSION TERMINAL SERVER

**Analyser une session TS :**

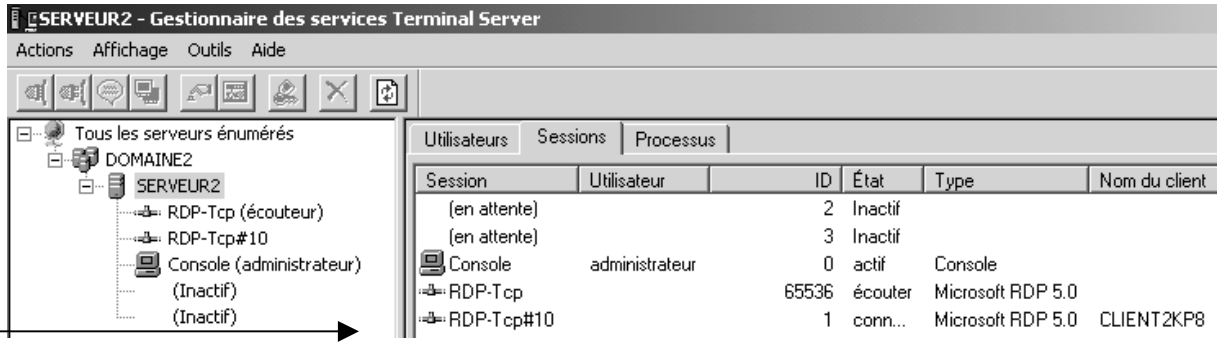
on veut savoir actuellement quelles sont les sessions en cours via Terminal Server, on peut sur le serveur ou TS est installé lancer la mmc **Gestionnaire de services Terminal Server**



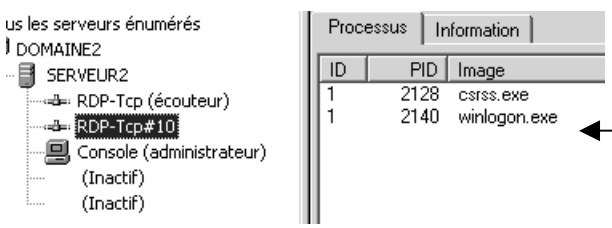

Soit un utilisateur boby, pour lequel on a donné les autorisations nécessaires… Regardons à travers le gestionnaire des services Terminal server, une session depuis le poste **client2kp8**, d'un utilisateur **boby** lançant **wordpad** sur le serveur2…

Lorsque boby sur le client demande une session Terminal Server, avant même qu'il ait pu s'identifier, le simple fait de demander

**Démarrer / Programmes** puis **Client Terminal Server** donne dans le gestionnaire de service

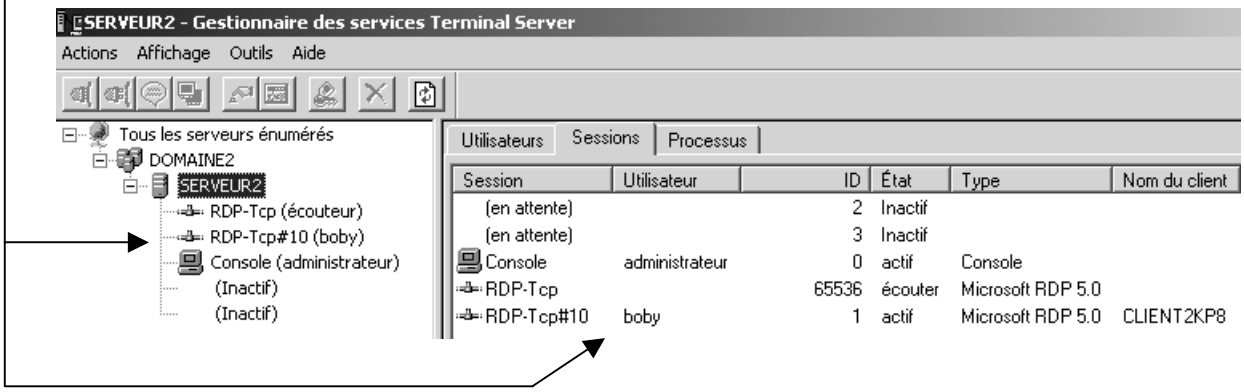



évidemment les processus en cours de cette session **RDP-TCp#10** sont peu nombreux



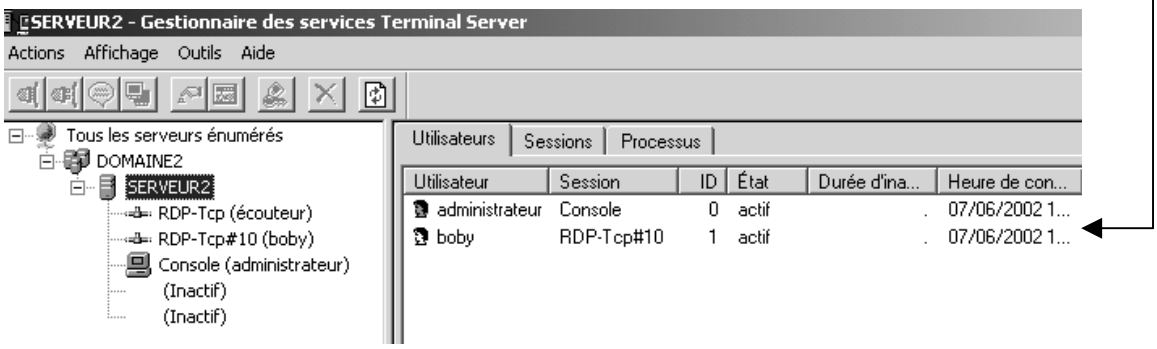

On voit bien une ouverture de session en cours… plus d'info sont disponibles dans l'onglet **Information…**

lorsque boby s'identifie correctement sur le client, on peut alors voir sa session

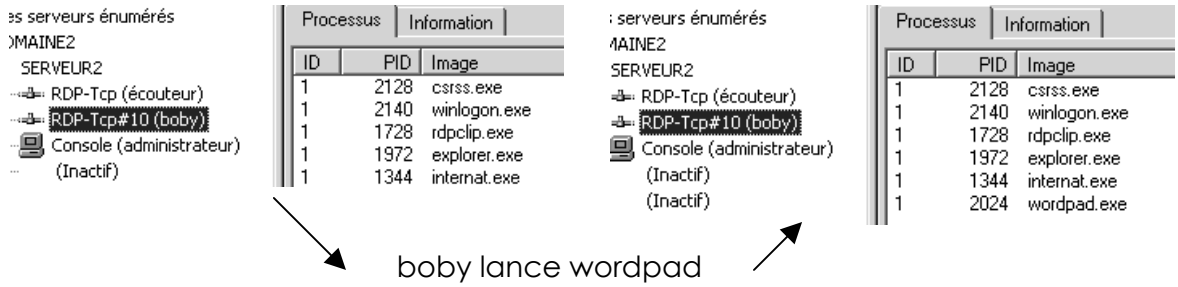



Une vue des session en cours pour le domaine ou le serveur est disponible :

Ici l'administrateur depuis le gestionnaire (localement) et boby…

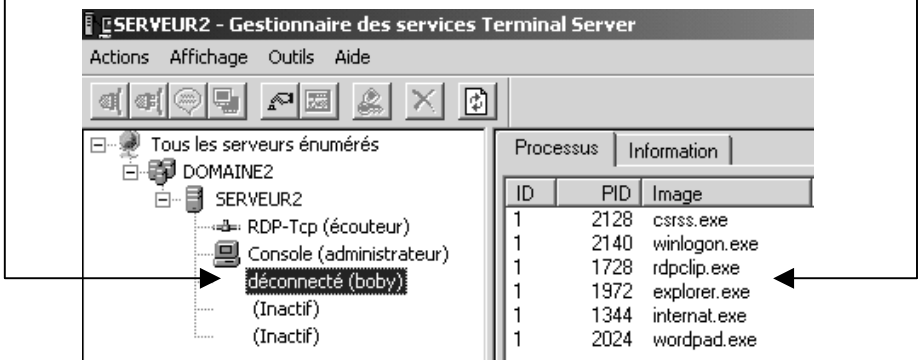



On peut suivre précisément ce que fait boby par les processus qu'il lance



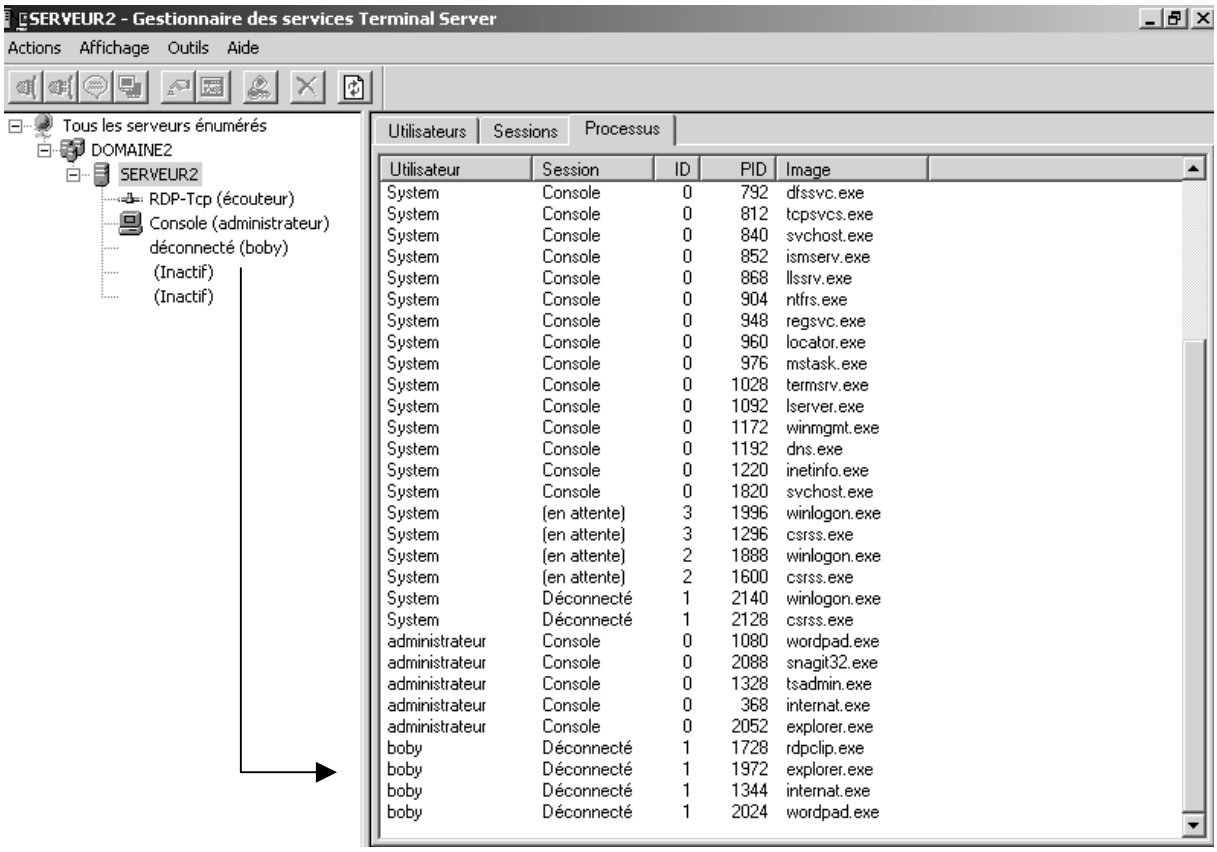

boby lance wordpad

Puis boby commet l'erreur classique de fermer sa fenêtre , donc il se **déconnecte**, mais **ses processus tournent toujours**..



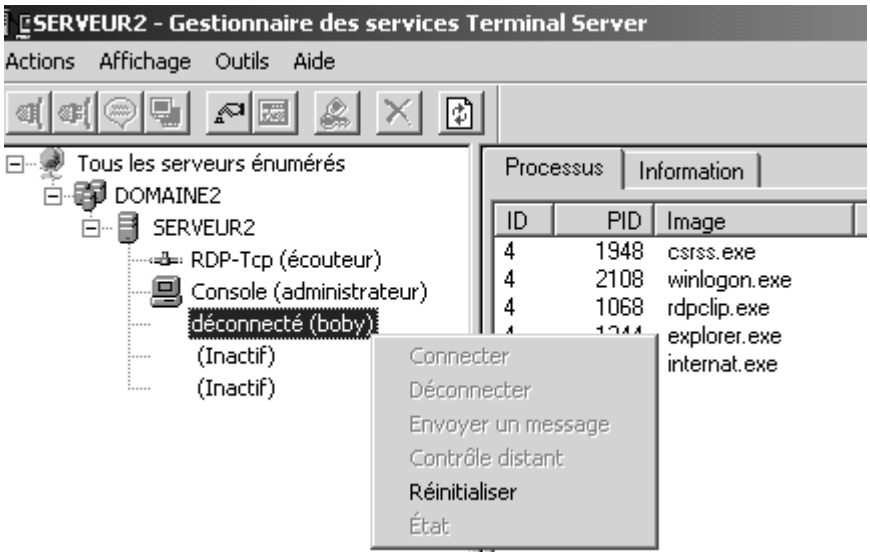

Si ici boby se reconnecte, il retrouve son environnement , et toutes ses applications…

On peut sur le serveur voir les processus de  sessions déconnectées




Si boby se reconnecte, et demande **démarrer /arreter / fermer la session** tout rentre dans l'ordre

Mais on peut aussi depuis le serveur « faire le ménage »

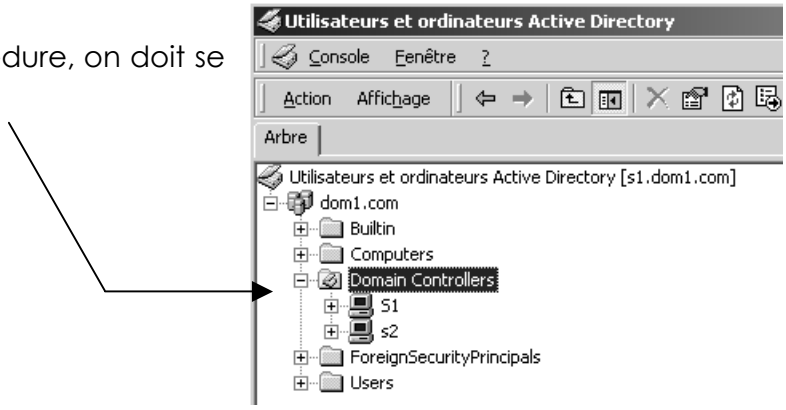


# TEST DE DUPLICATION D'AD

**Créer un 2° CD sur notre Domaine :**

Dans un domaine **dom1.com** on doit se créer un 2° CD à partir d'un serveur 2000 nommé **S2**…. pour venir épauler notre premier CD nommé **S1**.

A la fin de la procédure, on doit se retrouver avec




Un fois le 2° Contrôleur de Domaine opérationnel, par exemple **S2**, on crée sur ce serveur un compte **Nouveau**, mot de passe **n**.

Essayez d'ouvrir un session avec ce compte **Nouveau** depuis une machine du domaine: bien sûr cela marche !

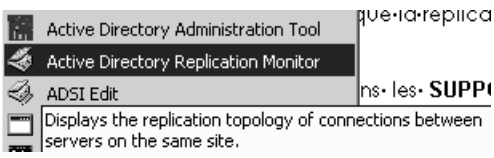
Revenons sur le premier serveur **S1**, le compte utilisateur Nouveau n'apparaît pas. Il n'apparaîtra que dans un délais d'environ **5 mn** !

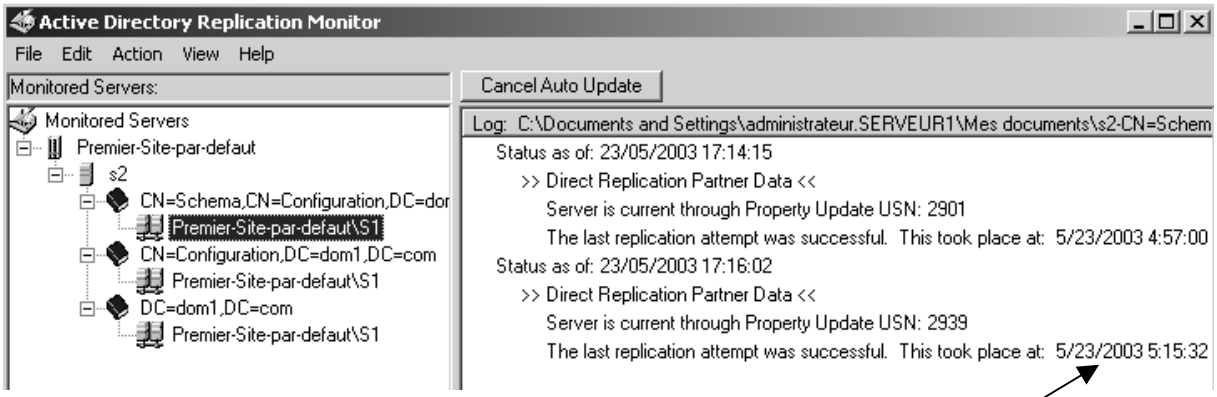
**Visualisation du trafic de duplication :**

Visualiser le trafic entre 2 nos CPD et forcer la mise a jour sans attendre les 5 mn, pour vérifier à des fins de test que la réplication est bien opérationnelle.

Le fichier sur le CD se trouve dans les **SUPPORT\TOOLS\SETUPEXE** et se nomme **replmon.exe.**

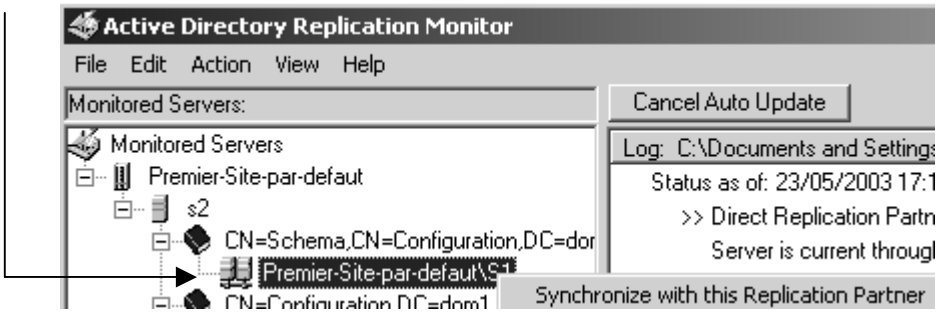
Une fois l'installation effectuée on lance **Active Directory Replication Monitor**



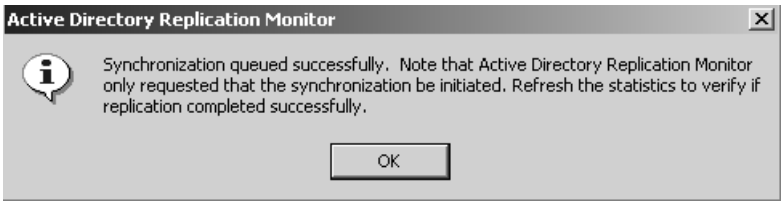



on voit que la dernière synchronisation s'est faite le **23/05 à 5h15:32**

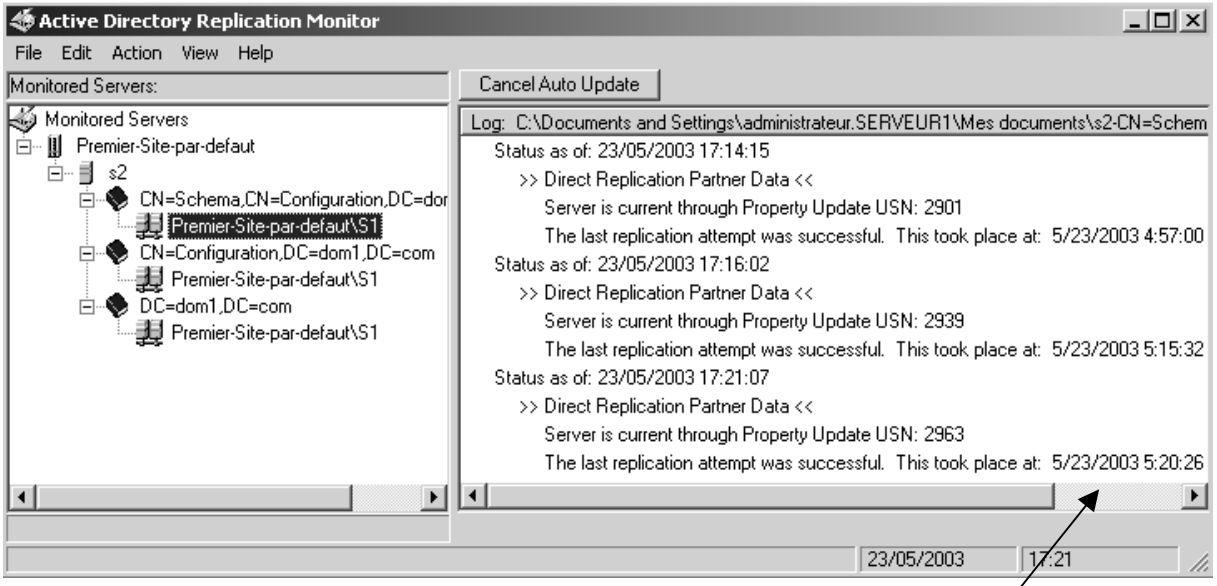
on se place sur l'ensemble des 3 composants Schéma-Configuration-Domaine et on clique avec le bouton contextuel, **Synchronize…** ou via le menu **Action / Replication partner / Synchronise with…**




un message de confirmation apparaît




et si on demande de rafraîchir via le menu **view refresh**




on voit que la dernière synchronisation s'est faite le **23/05 à 5h20:26**

# REPLICATION INTER-SITE

**Créons 2 sites distants de 62 machines maximum relié par RNIS:**

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

Si on veut **2 sous réseaux** comportant chacun **62 machines maximum**, on pourra prendre alors comme masque de sous réseau **255.255.255.192**

- **Id réseau**
  pour trouver les Id réseau je dois trouver toutes les combinaisons de **2 bits** de 11 à 00 en laissant tomber les valeurs n'ayant que des 0 ou que des 1 (non autorisée).J'obtient 10-01-soit en décimal 128-64.

  que je rajoute à mon Id réseau d'origine 192.168.1.xx soit donc les Id réseau suivantes :

  192.168.1.**128** 192.168.1.**64**

- Id hôte valide
  un petit calcul nous donne :

| sous-réseau | 1° adresse IP | dernière adresse IP |
|---|---|---|
| 192.168.1.**64** | 192.168.1.65 | 192.168.1.127 |
| 192.168.1.**128** | 192.168.1.129 | 192.168.1.191 |

**Créer les sites nécessaires :**

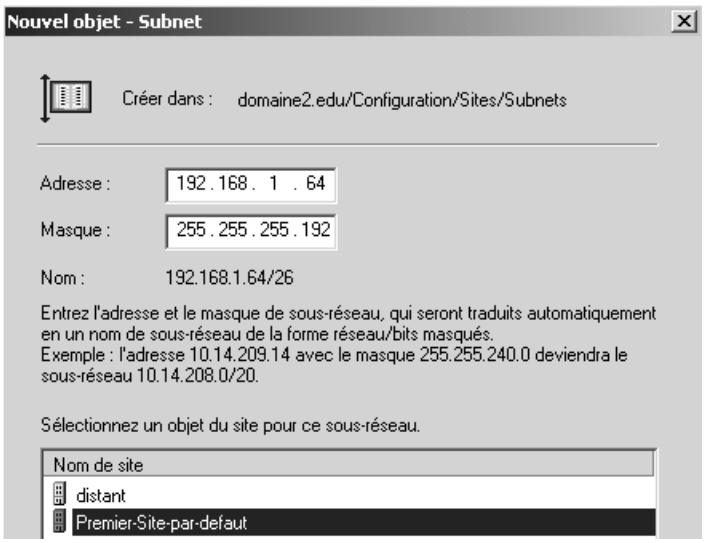
Dans la mmc **Sites et services Active Directory** on crée le site **distant** (puisque le premier site par défaut existe déjà)

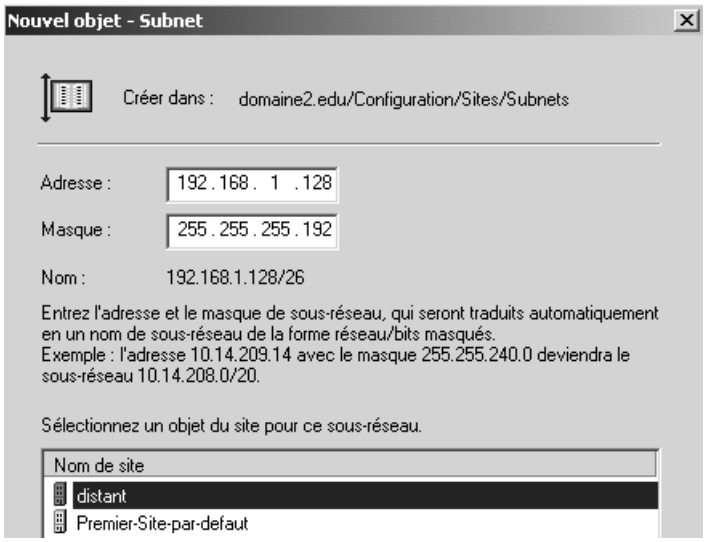
## Définir un sous -réseau :

Dans la mmc **Sites et cervies Active Directory**

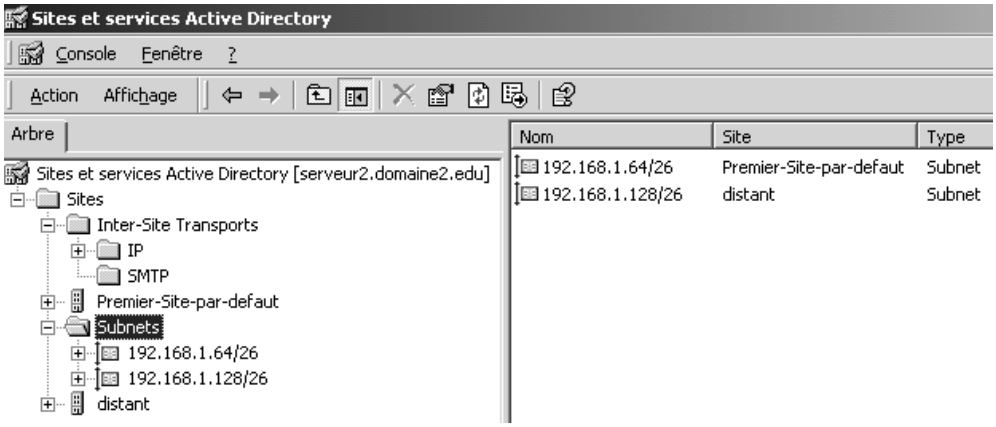
Pour créer les deux sous-réseaux nécessaires, il faut se mettre sur le dossier **Subnets**

et demander clic droit **Nouveau / subnet**



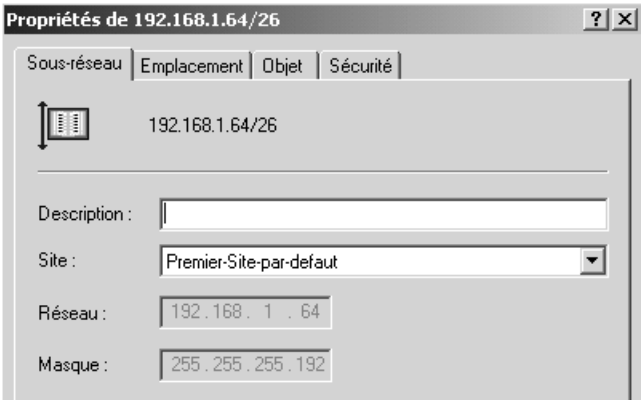



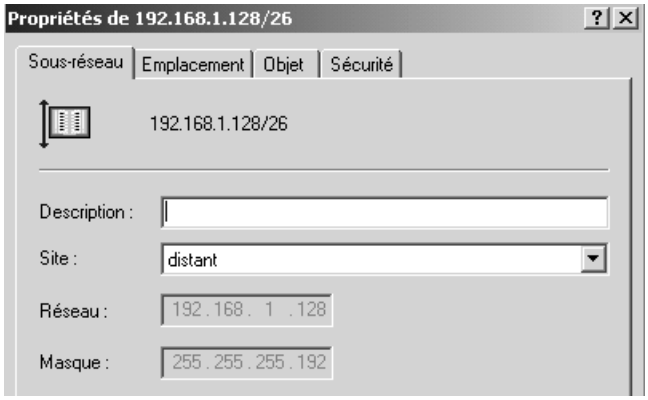

De manière à obtenir




## Associer un sous -réseau à un site:

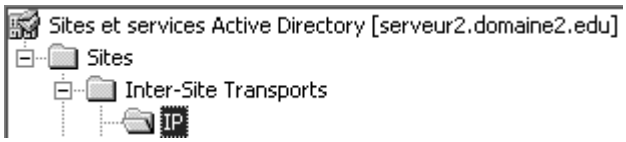
On vérifie que l'on a bien

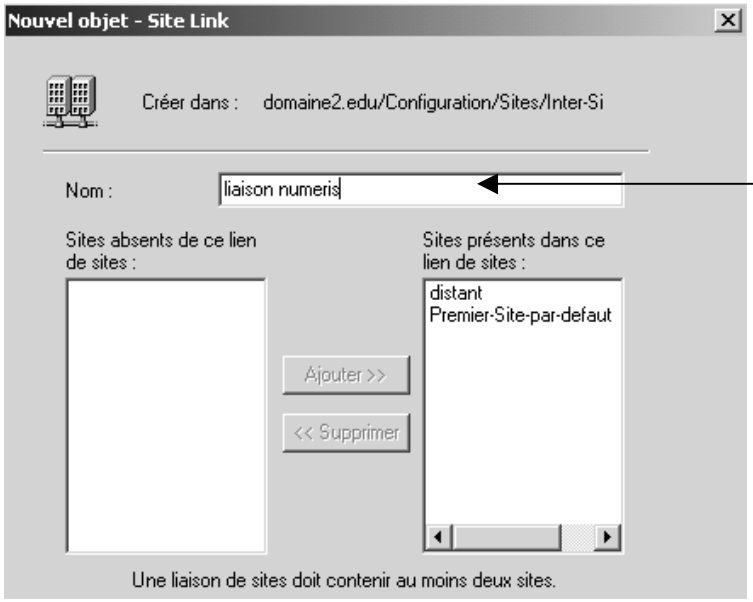


**Création des liens de site:**

Il faut créer un lien de site entre notre **premier-site-par-defaut** et notre site **distant.** On se place sur le protocole IP

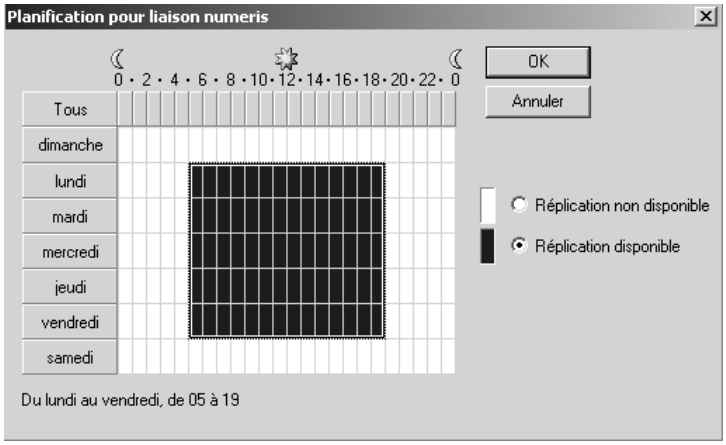



On nomme notre liaison

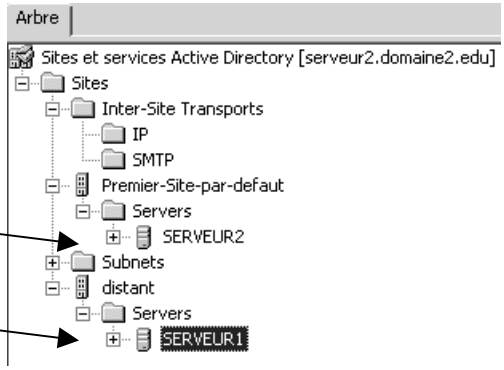
**liaison numeris**

et dans les propriétés on planifie quelques économies…




**On oublie pas de poser un Contrôleur de domaine dans chaque site:**

on place un Cd par site



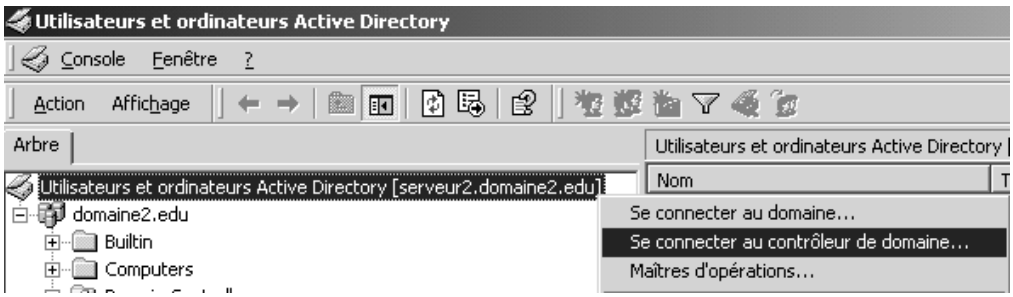
# TRANSFERT DE MAITRE D'OPERATION

**Objectif :**

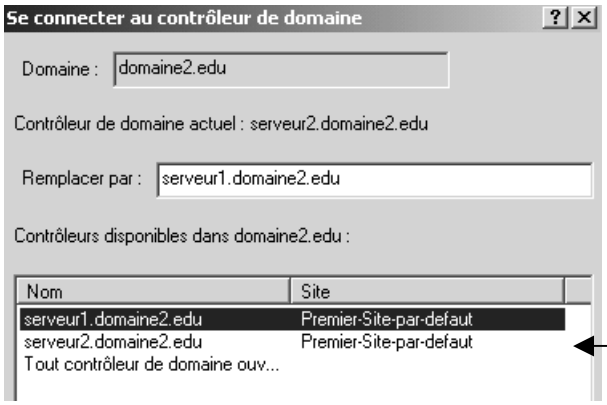
Imaginons par exemple le transfert de **l'Emulateur CPD** depuis un contrôleur nommé **serveur2** vers un contrôleur nommé **serveur1**.

On est sur le CD **serveur 2**

Dans la mmc **Utilisateurs et ordinateurs Active Directory** on essaye déjà de se connecter sur le serveur sur lequel on souhaite effectuer le transfert, c'est à dire pour nous **serveur1**




on obtient alors

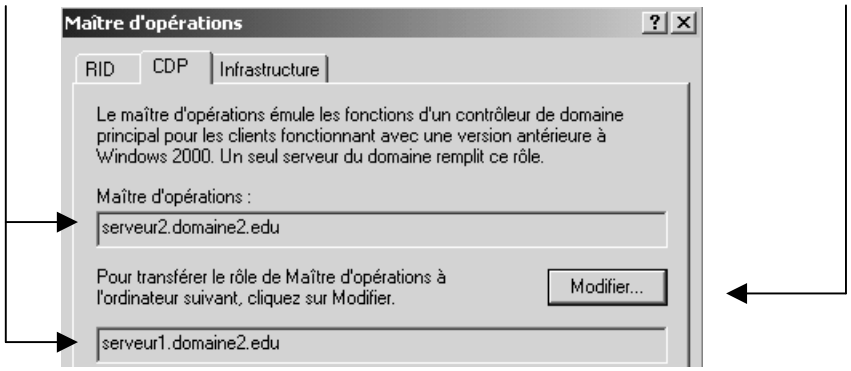



Tous les CD du Domaine apparaissent

étant maintenant placé sur le CD sur lequel on souhaite transférer le maître d'opération


On demande **Maîtres d'opérations…**

On vérifie bien ce que l'on veut faire, …. Et on demande **Modifier**




Un fois l'opération réalisée, refaite là dans l'autre sens pour retrouver la situation initiale

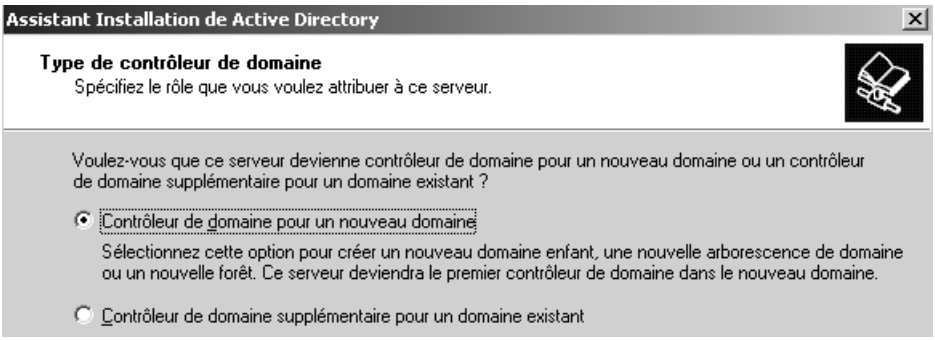
Essayez pour le contrôleur de schéma !

# CREATION D'UN DOMAINE ENFANT

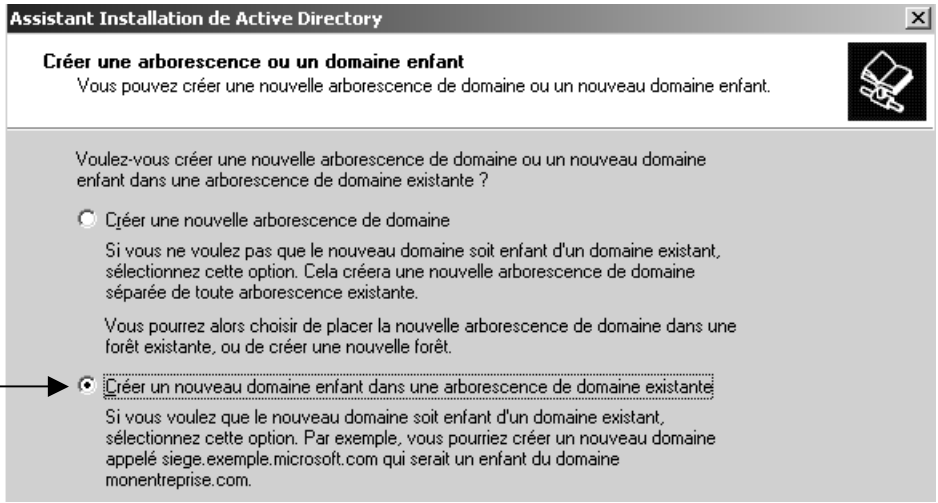
**Création du C.D. "enfant.dom1.com" sur serveur S4 :**

Il faut bien sûr que l'on ait de la connectivité IP et que l'on ait comme adresse de serveur DNS un serveur DNS du domaine parent…

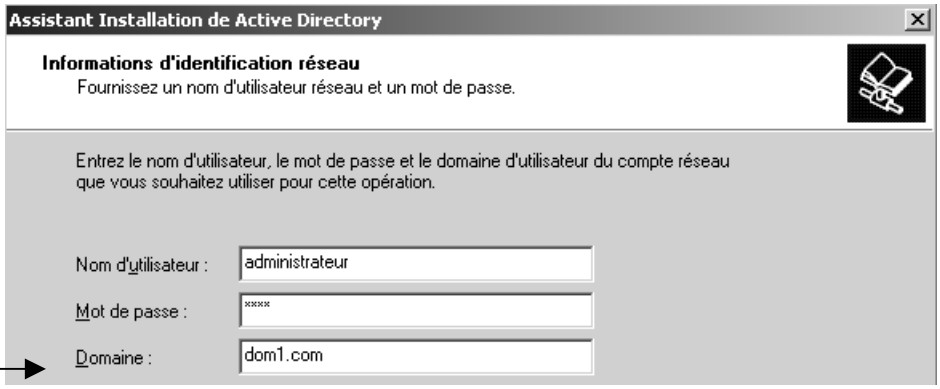
Ensuite on peut lancer le **DCpromo**



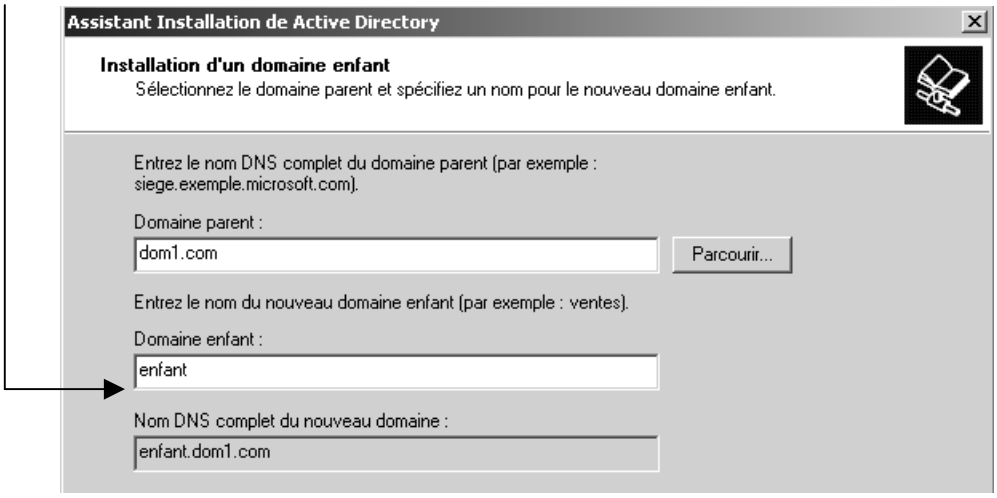

ici on demande



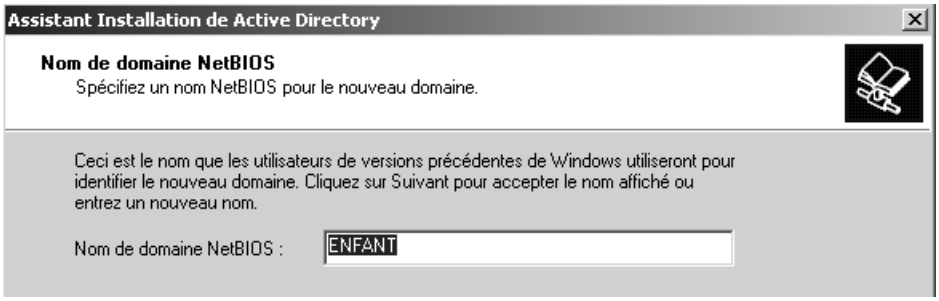

On précise le domaine "parent"



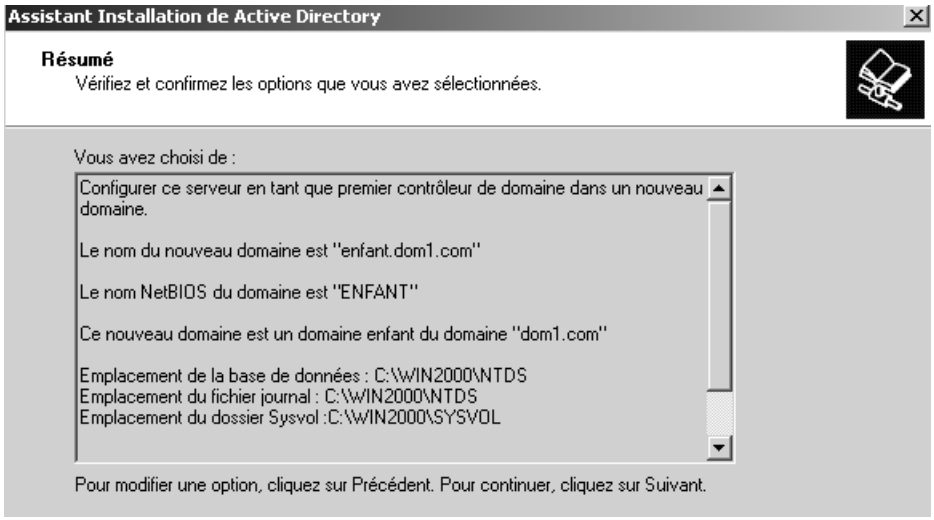
et on donne ensuite le nom du domaine "enfant"




un nom netbios va être proposé,




et tout l'assistant dcpromo est désormais classique pour aboutir au résumé final….




la création du domaine enfant se fait de manière automatique,

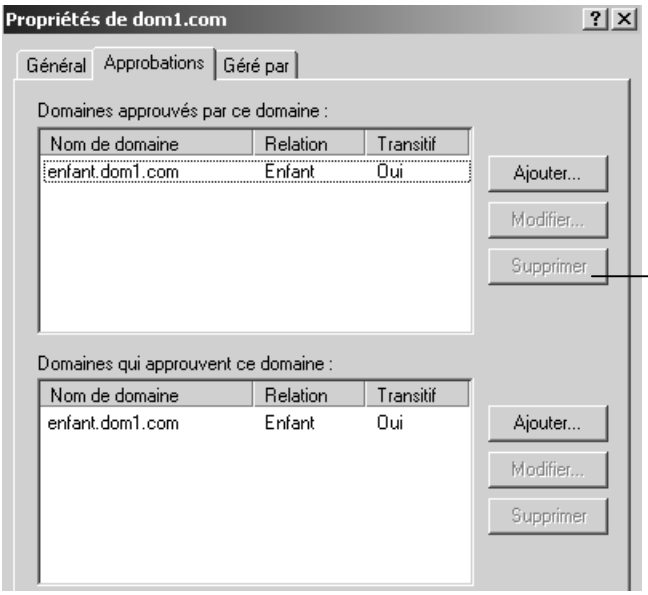
- ce serveur devient CD ,
- et les relations d'approbations entre le domaine enfant et le domaine parent sont automatiquement construites., à savoir :
  - le domaine enfant approuve le domaine parent
  - le domaine parent approuve le domaine enfant

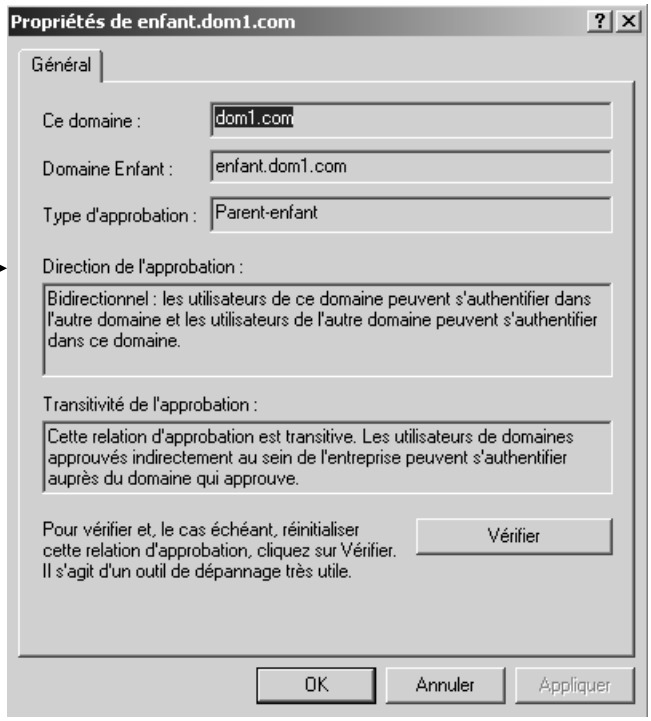
**Vérification des relations d'approbations :**

si tout se passe bien, lorsqu'l on ouvre la session sur le serveur CD du domaine enfant, on peut ouvrir la session sur un des deux domaines existants...

on peut vérifie dans **outils d'administration / Domaines et approbations active directory**


SI on demande les **propriétés** de dom1.com

## Gestion de zone DNS :

Maintenant réfléchissons : on a un domaine enfant, mais ce domaine ne dispose pas de son propre serveur DNS, il utilise le serveur DNS du domaine parent….


Ce qui pose un certain problème de fiabilité, ou de dépendance…

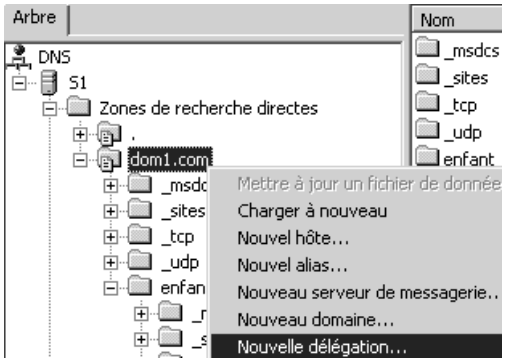
Pour délégué une zone vers un serveur DNS du domaine enfant, il va falloir suivre un mode opératoire précis :

1. Création d'une délégation pour le domaine enfant sur le serveur racine (parent)
2. Installation d'un serveur enfant dans le domaine enfant
3. Création d'une zone appropriée sur ce serveur
4. Reparamétrage du serveur DNS enfant

## Création d'une délégation sur le serveur DNS racine :

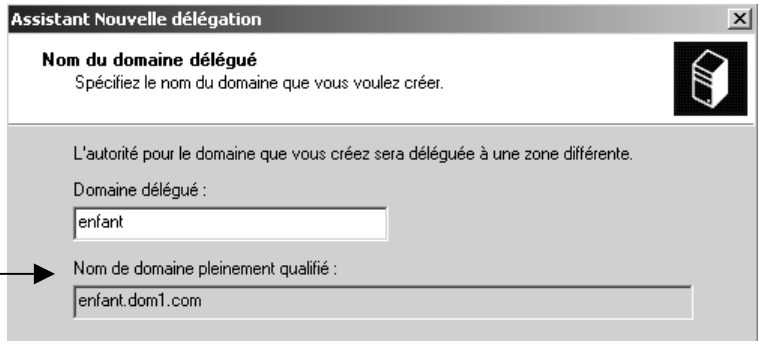
Sur le serveur DNS parent, que l'on appelle également serveur racine (à ne pas confondre avec la zone DNS racine ".") il faut créer une délégation correspondant au domaine enfant.

Cela correspond à une zone que l'on ne souhaite plus prendre en charge, car elle va être gérée a terme sur le serveur DNS du domaine enfant.

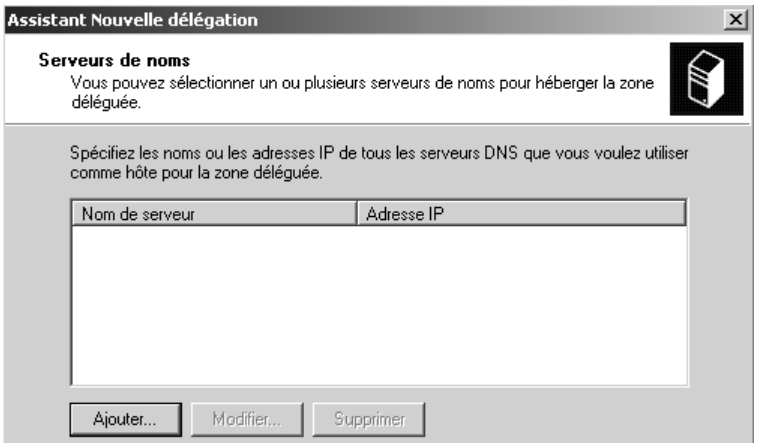


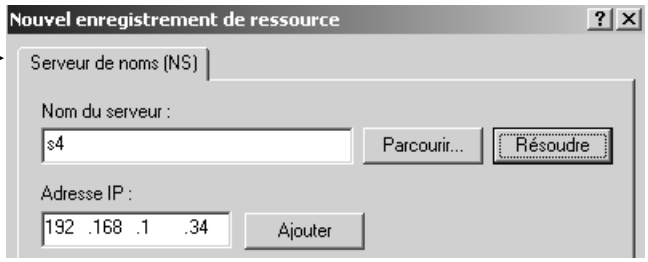

On se place sur notre zone parent et on demande via le menu contextuel **Nouvelle délégation**….

Un assistant se déclenche et demande le nom du domaine enfant



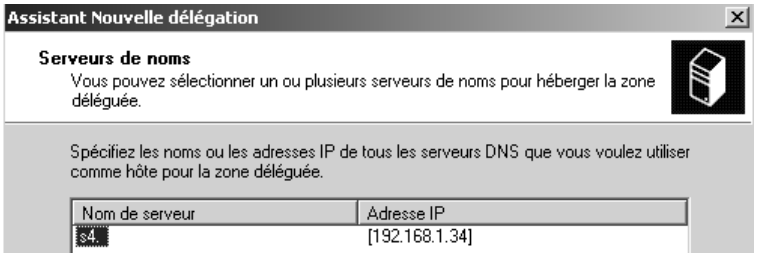

puis il faut donner l'adresse IP du serveur DNS qui va héberger la zone enfant via **Ajouter**



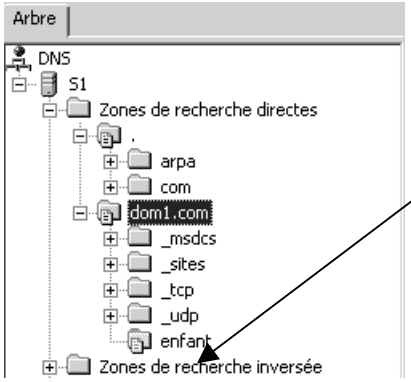




Il faut rentrer ici un nom adresse IP du serveur DNS, on ne peut pas le trouver (résoudre) ….

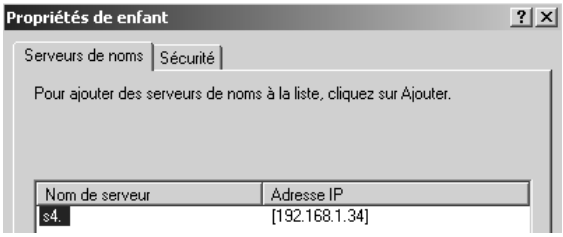
de manière à obtenir




Lorsque l'on valide ensuite l'assistant, après rafraîchissement de notre serveur DNS on obtient




Une zone "enfant" apparaît, sans que son contenu ne soit présent dans notre serveur DNS…

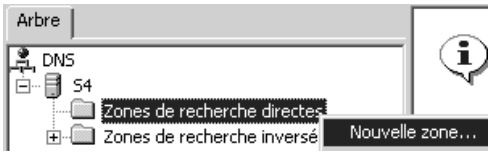



Désormais, à ce niveau, on ne tient plus compte de ce qui se trouve dans la zone enfant, celle-ci étant gérée sur un autre serveur DNS (pour nous ici S4), on ne fait que renvoyer les demandes de résolution. On dit que notre serveur **ne fait plus autorité pour cette zone**…

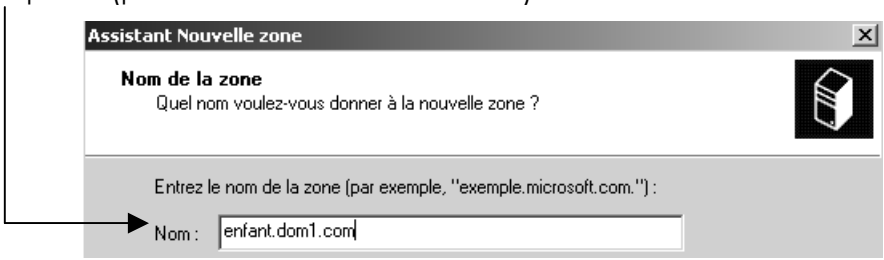
**Installation du serveur DNS enfant :**

Sur le serveur CD de la zone enfant, (pour nous S4), il faut donc installer un serveur DNS **faisant autorité** pour la zone enfant…

- L'installation d'un serveur DNS est classique, et la création d'une nouvelle zone aussi

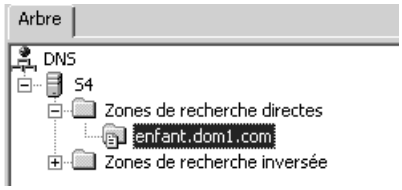


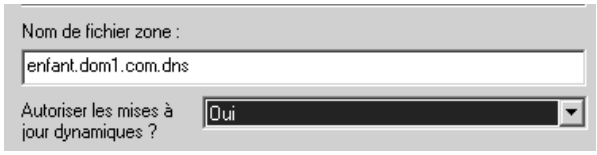

on demande de créer une **zone principale**, en spécifiant bien son nom complet…(pour nous **enfant.dom1.com**)




le reste se valide avec les options par défaut classiques.

- La zone étant crée, il va falloir lui autoriser les mises à jour dynamique, et l'intégrée à Active Directory…

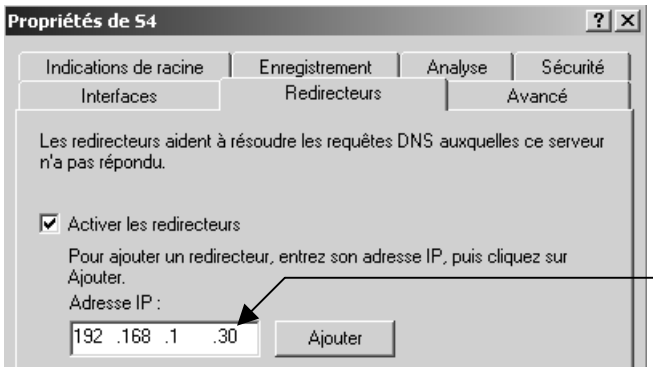



- Il faut ensuite modifier le serveur s4 pour qu'il se référence lui-même comme étant son propre serveur DNS...(adresse IP DNS…)

A l'heure actuelle, notre serveur DNS va prendre en charge tous les enregistrement de la zone enfant, mais il ignore tout de la zone parent…

- Il faut ensuite indiquer au serveur DNS enfant l'adresse du serveur DNS parent comme redirecteur à utiliser…




Il faut donner ici l'adresse du serveur DNS de la zone parent, pour nous S1 …

puis redémarrer…

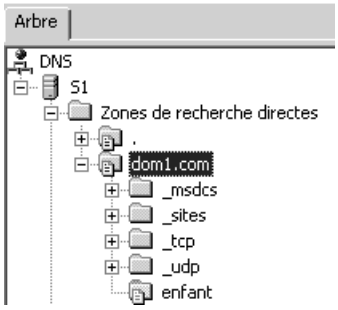
**test des zones DNS parent et enfant :**

Si on se résume,

On a un **domaine parent**, nommé **dom1.com.**

le serveur DNS installé sur une machine nommée **S1** d'adresse **192.168.1.30** a une zone principale intégrée à active directory

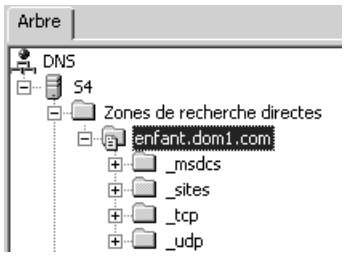
Sur cette zone on a une délégation pour une zone nommé **enfant**




on a un **domaine enfant**, nommé **enfant.dom1.com.**

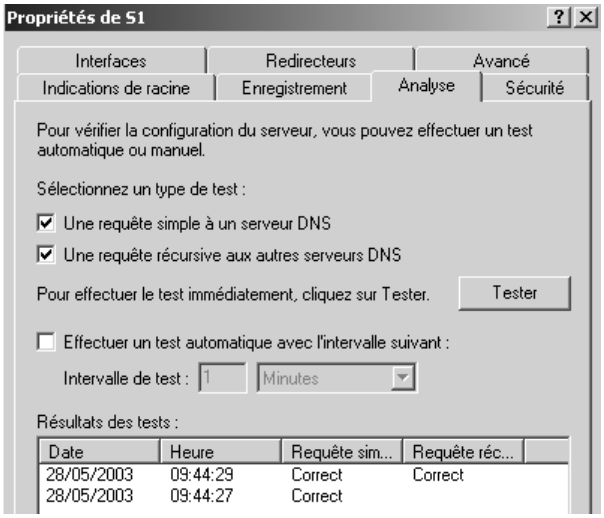
le serveur DNS installé sur une machine nommée **S4** d'adresse **192.168.1.34** a une zone principale intégrée à active directory

Sur ce serveur on a des redirecteurs actifs, pointant vers le serveur DNS parent en 192.168.1.30




**Tests sur la zone parent**

On peut déjà tester le fonctionnement du serveur DNS via l'onglet Analyse…




Puis on va utiliser nslookup

la résolution de **S1** sur **lui-même** devrait donner

```
> s1 s1
Serveur :  s1.dom1.com
Addresses:  192.168.3.1, 192.168.1.30

Nom :    s1.dom1.com
Addresses:  192.168.3.1, 192.168.1.30
```

la résolution de **S2** (autre machine du domaine dom1.com) devrait donner

```
> s2 s1
Serveur :  s1.dom1.com
Addresses:  192.168.3.1, 192.168.1.30

Nom :    s2.dom1.com
Address:  192.168.1.32
```

par contre il est normal que si on tente de résoudre **S4** l'on ait …

```
> s4 s1
Serveur :  s1.dom1.com
Addresses:  192.168.1.30, 192.168.3.1

*** s1 ne parvient pas à trouver s4 : Non-existent domain
```

il faut tester **S4.enfant** ou **S4.enfant.dom1.com** (en spécifiant le domaine)

```
> s4.enfant s1
Serveur :  s1.dom1.com
Addresses:  192.168.3.1, 192.168.1.30

R'ponse ne faisant pas autorit'ÿ:
Nom :    s4.enfant.dom1.com
Address:  192.168.1.34
```

On a cette info depuis un serveur auquel on a délégué…

**Tests sur la zone enfant**

On peut tester le fonctionnement du serveur DNS via l'onglet Analyse…

Puis on peut utiliser nslookup

la résolution de **S4** sur **lui-même** devrait donner

```
> s4 s4
Serveur :  s4.enfant.dom1.com
Address:  192.168.1.34

Nom :    s4.enfant.dom1.com
Address:  192.168.1.34
```

par contre il est normal que si on tente de résoudre **S2** (une machine du domaine parent) l'on ait tout de suite la réponse. (on utilise un système de redirection pour tout appel non résolu…)

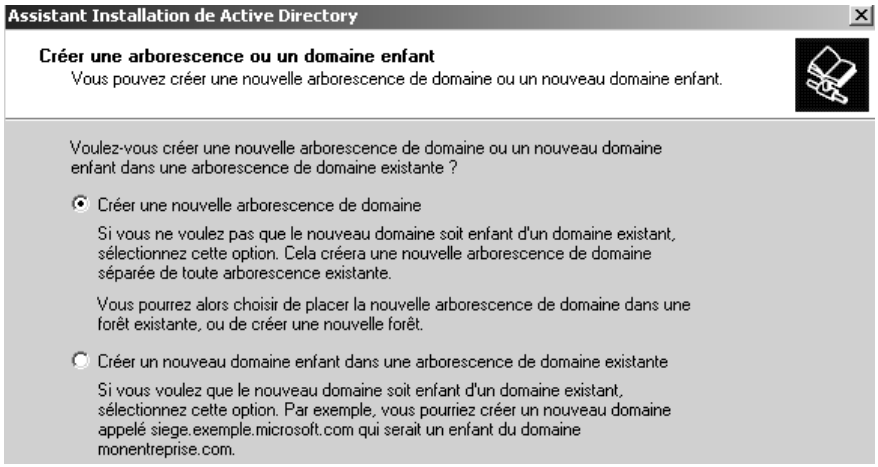
```
> s2 s4
Serveur :  s4.enfant.dom1.com
Address:  192.168.1.34

R'ponse ne faisant pas autorit'ÿ:
Nom :    s2.dom1.com
Address:  192.168.1.32
```

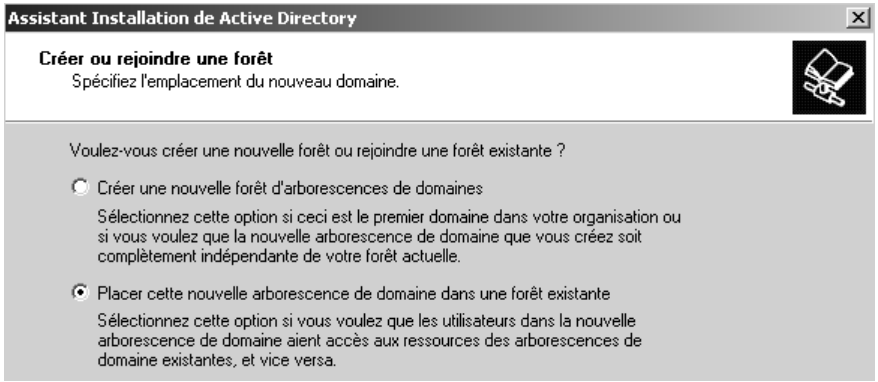
# CREATION D'UN DOMAINE DANS LA FORET

**Création du C.D. "dans la forêt dom2.com" sur serveur S5:**

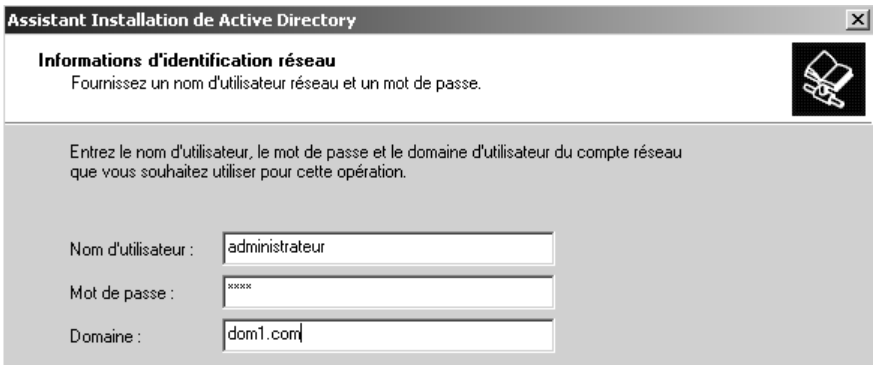
Il faut bien sûr que l'on ait de la connectivité IP et que l'on ait comme adresse de serveur DNS un serveur DNS du domaine voisin…

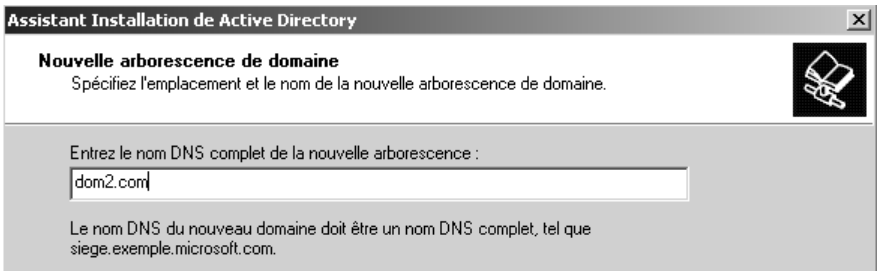
Lors de l'assistant DC promo, on réponds alors ainsi :

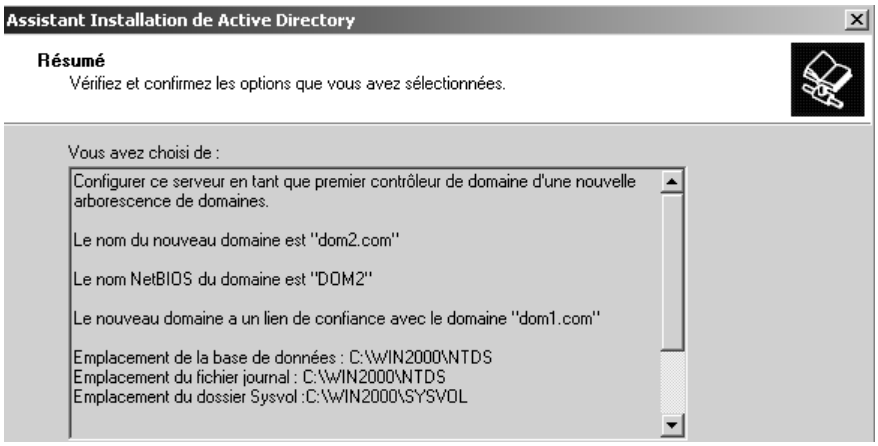



Evidemment il faut connaître un compte d'administrateur du domaine racine de la forêt






le reste est tout à fait standard…

la création du domaine dans la même forêt se fait de manière automatique,

- ce serveur devient CD
- et les relations d'approbations entre les deux domaines de la forêt sont automatiquement construites., à savoir :
  - le domaine racine approuve le domaine parent
  - le domaine parent approuve le domaine enfant
- le serveur ayant le rôle de contrôleur de schéma et de Maître d'attribution de nom de domaine est "dupliqué" sur le nouveau CD du nouveau domaine (mais l'original reste sur le CD d'origine…)

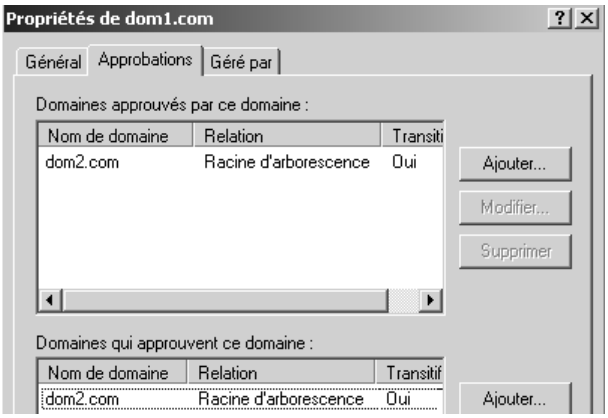
---

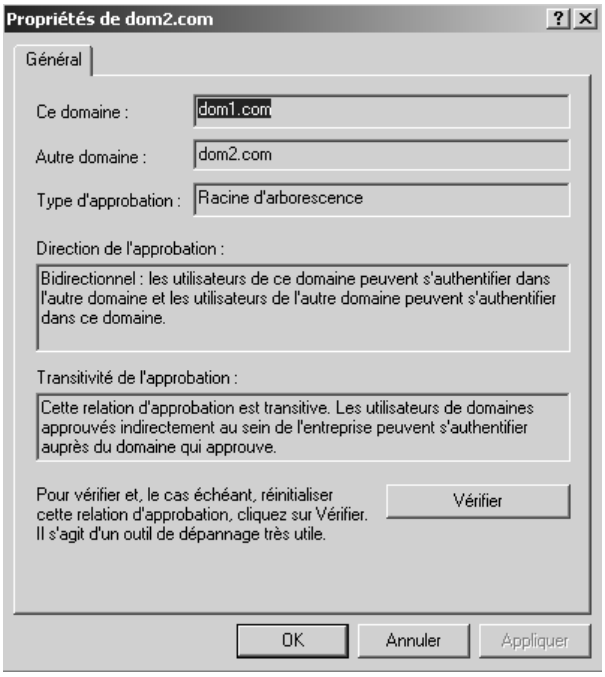
**Vérifions les relations d'approbation :**

Depuis un CD du domaine racine, on peut voir

on peut vérifier dans **outils d'administration / Domaines et approbations active directory**

SI on demande les **propriétés** de dom1.com



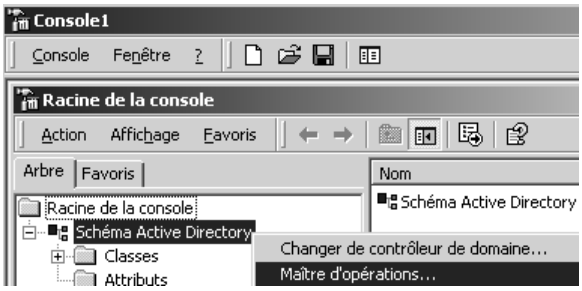

**Localisation des maîtres d'opération :**

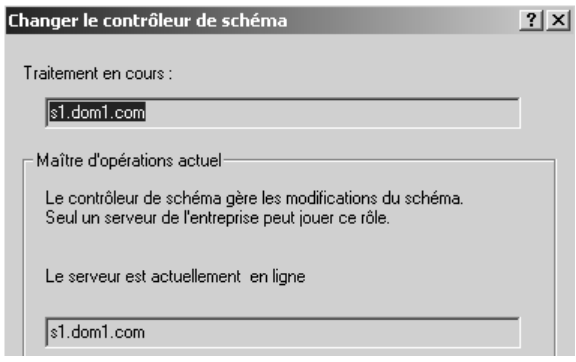
On se trouve dans le cas où on a une forêt à 2 domaines, par conséquent

- les 2 rôles **Contrôleur de schéma** et **Maître d'attribution de nom de domaine** doivent <u>être restés sur le 1° CD du domaine</u> (**serveur S1**) racine de la forêt **dom1.com**
- les 3 rôles **Emulateur CPD**, **RID** et **maître d'infrastructure** pour le domaine **dom1.com** <u>n'ont pas bougé</u> du serveur 1° CD du domaine (**serveur S1**)
- les 3 rôles **Emulateur CPD**, **RID** et **maître d'infrastructure** ont <u>étés crées</u> sur le 1° CD du domaine (**serveur S5**) qui a rejoint la forêt…

Vérifions :

le rôle **Contrôleur de schéma** <u>depuis le CD sur S5 (par exemple)</u> pour le nouveau domaine rallié dans la forêt, on exécute la mmc **Schéma Active directory**

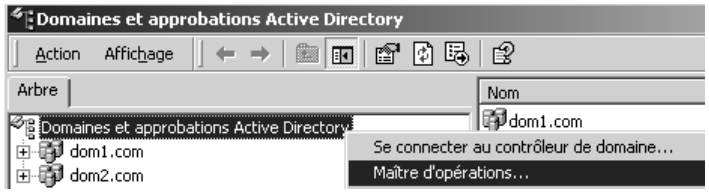



on constate qu'il est toujours sur **S1**

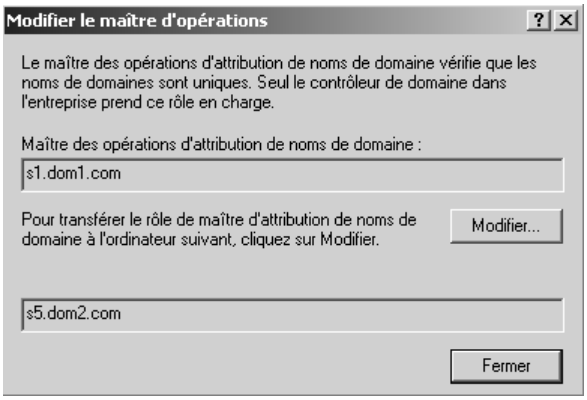
(et pour le transférer il faut appartenir au groupe **maître de schéma**)

le rôle **Maître d'attribution** depuis le CD sur S5 (par exemple) on exécute la mmc **Domaine et approbation Active Directory**

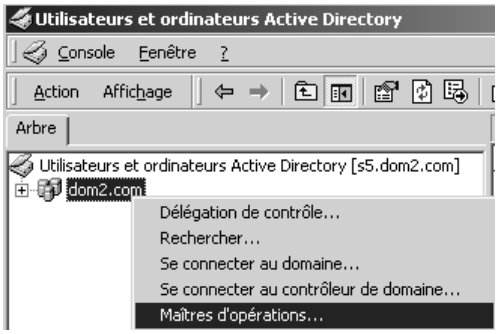


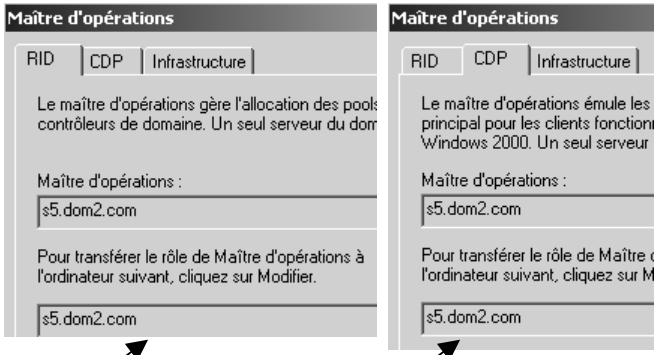

on constate qu'il est toujours sur **S1**

(on pourrait le transférer…)



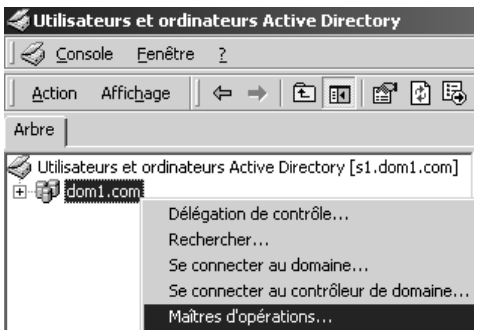

les 3 rôles **Emulateur CPD**, **RID** et **maître d'infrastructure** pour le domaine **dom2.com** on exécute depuis le CD sur S5 la mmc **Utilisateur et ordinateur Active Directory**

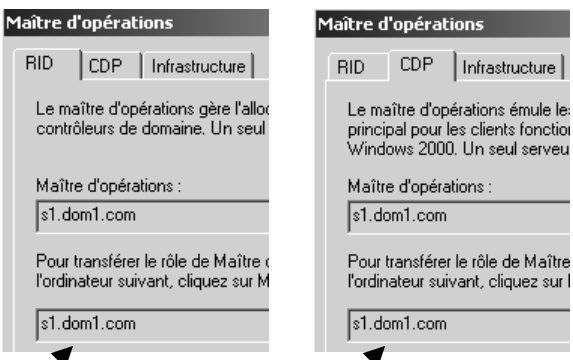



on constate qu'ils sont crées sur **S5**

les 3 rôles **Emulateur CPD**, **RID** et **maître d'infrastructure** pour le domaine **dom1.com** on exécute depuis le CD sur S1 la mmc **Utilisateur et ordinateur Active Directory**



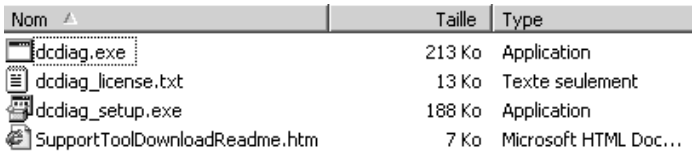

on constate qu'ils sont restés sur **S1**

# L'UTILITAIRE DCDIAG

**Récupération de l'utilitaire dcdiag :**

On récupère cet utilitaire dans un fichier


puis on l'installe en l'auto-décompressant, ce qui amène un éxécutable et une notice d'installation ...




**Quelques test possibles :**

Voici quelques test possibles à imaginer avec cet utilitaire...

Création du premier Contrôleur de domaine dans une nouvelle forêt Active Directory

**dcdiag /test:dcpromo /dnsdomain:example.microsoft.com /newforest**

```
C:\test>dcdiag /test:dcpromo /dnsdomain:dom1.com /newforest
   Starting test: DcPromo
      Messages logged below this line indicate whether this domain controller
      will be able to dynamically register DNS records required for the
      location of this DC by other devices on the network. If any
      misconfiguration is detected, it might prevent dynamic DNS registration
      of some records, but does not prevent successful completion of the Active
      Directory Installation Wizard. However, we recommend fixing the reported
      problems now, unless you plan to manually update the DNS database.

      DNS configuration is sufficient to allow this domain controller to
      dynamically register the domain controller Locator records in DNS.

      ..................... s1 passed test DcPromo
```

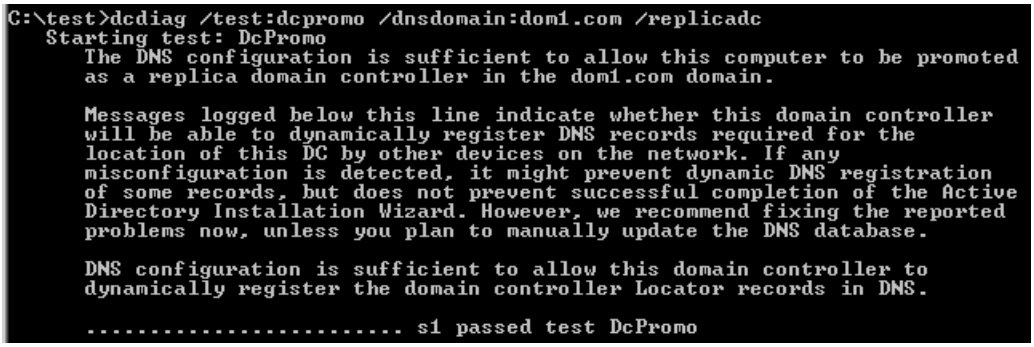
Test de l'enregistrement DNS dynamique

**dcdiag /test:registerindns /dnsdomain:example.microsoft.com**

```
C:\test>dcdiag /test:registerindns /dnsdomain:dom1.com
   Starting test: RegisterInDNS
      DNS configuration is sufficient to allow this domain controller to
      dynamically register the domain controller Locator records in DNS.

      ..................... s1 passed test RegisterInDNS
```

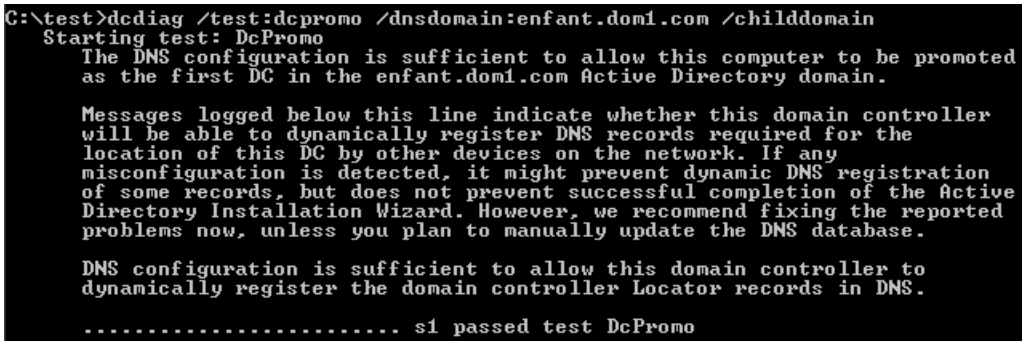
Ajout d'un contrôleur de domaine supplémentaire à un domaine existant (réplique du contrôleur de domaine)

**dcdiag /test:dcpromo /dnsdomain:example.microsoft.com /replicadc**



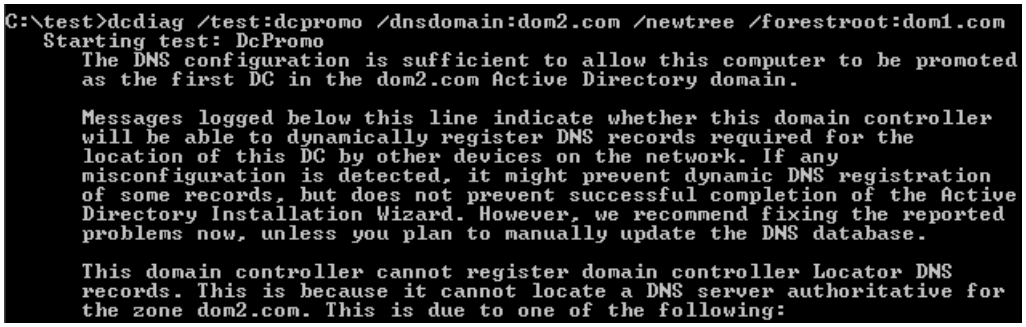

Ajout d'un domaine enfant à un arbre dans une forêt Active Directory existante

**dcdiag /test:dcpromo /dnsdomain:test.example.microsoft.com /childdomain**




Ajout d'un nouvel arbre de domaine à une forêt Active Directory existante

**dcdiag /test:dcpromo /dnsdomain:test.example.microsoft.com /newtree forestroot:example.microsoft.com**



# INSTALLATION MUETTE DEPUIS CD

**Objectifs et fonctionnalités :**

On veut réaliser une installation de Windows NT 2000 Professionnel à l'aide du CD mais sans que aucune question ne se pose à "l'installateur".

On va par conséquent créer un fichier **winnt.sif** et **winnt.bat** via le programme **Setup manager wizard**

On l'exécutera ensuite par le biais de **winnt.bat**

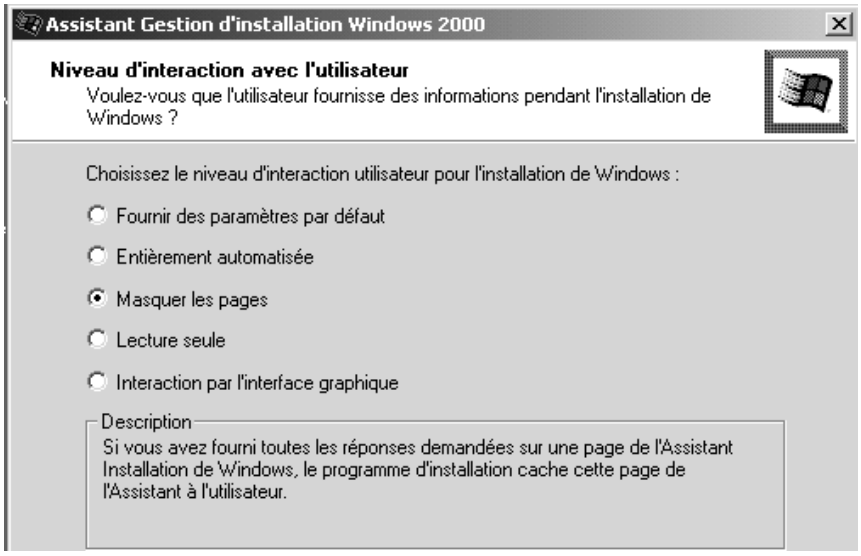
Il faut qu'aucune question ne se pose lors de l'installation, et que la configuration donnée au final à notre poste Nt2000 soit la suivante :

- personnalisation au nom de : cabaré – formation
- nom machine : postentauto
- mot de passe de l'administrateur : zk29
- paramètres TCP-IP par défaut : (client DHCP +, rés microsoft)
- connexion Groupe de Travail : Formation
- heure : Greenwich

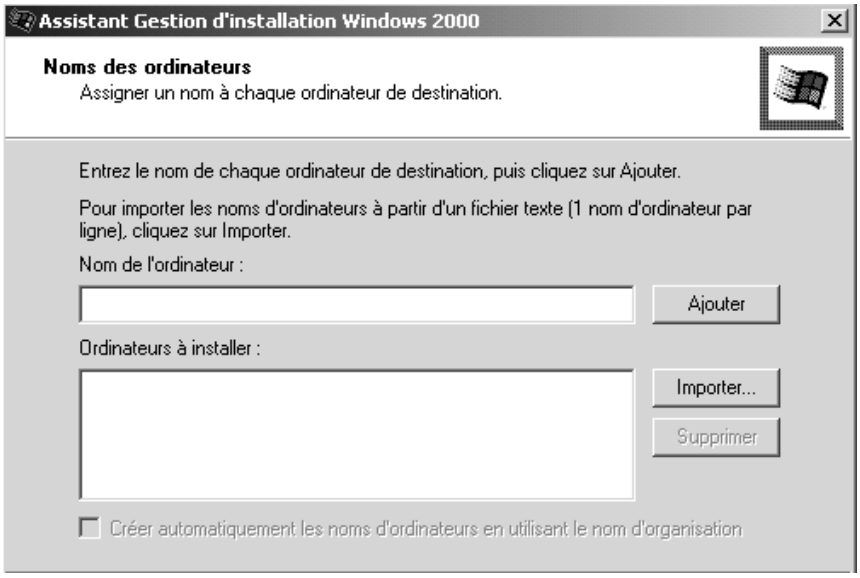
Serait il difficile de laisser en libre saisie uniquement le nom machine ?

**Réponse :**

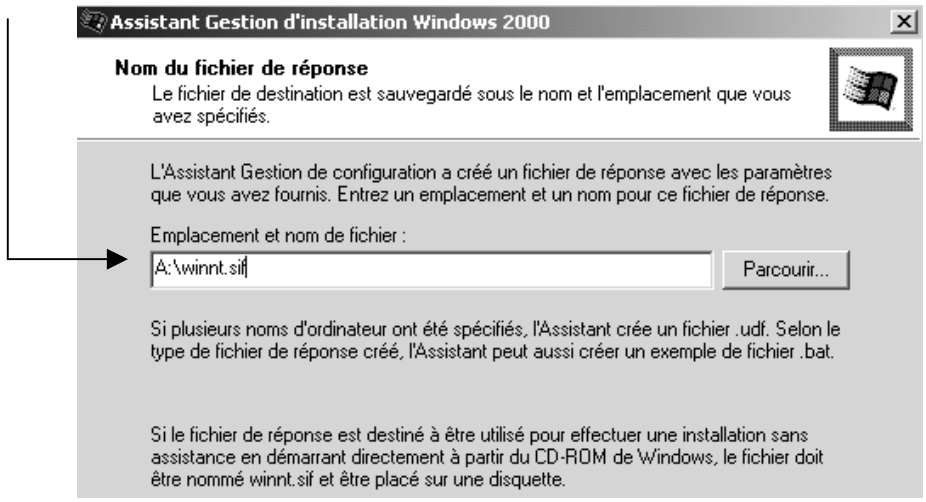
Le mode Masquer les pages convient



en prenant soin de ne pas renseigner la boite de dialogue **Noms des ordinateurs** lors de la création du fichier **winnt.sif**




Attention à bien indiquer le bon nom de fichier




Et à vérifier dans **winnt.bat** le chemin du CD sur la machine de destination...