http://WWW.CABARE.NET ©

Installation Réseau Serveur Windows 2008 & 2008 R2 – sys 22 – cours -

Installer serveur 2008 windows

Michel Cabaré – Ver 2.2 – mai 2010-

Installation réseau Serveur Windows 2008 & 2008R2

Cours

Michel Cabaré – Ver 2.2 – Mai 2010

www.cabare.net ©

La formation à pour but de vous initier avec les logiciels Microsoft Windows 2008 et Windows 2008 R2 Serveur (version 6.0-6001 et 6.1-7600) sur environnement P.C.

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

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

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

Bon Travail

Michel Cabaré

TABLE DES MATIÈRES

LES CLIENTS WINDOWS 7
CONFIGURATION MINIMALE: 7
CLIENT RESEAU WINDOWS: 7
SERVICES RESEAU WINDOWS: 8
NOM DE POSTE WINDOWS : 8

VOISINAGE – FAVORIS RESEAU 10
RESEAU SEVEN EN WORKGROUP : 10
FAVORIS RESEAU XP EN WORKGROUP : 10
FAVORIS RESEAU 2000 : 12
VOISINAGE RESEAU WINDOWS NT: 12

RECHERCHER UN POSTE 14
POURQUOI JE NE VOIS PAS TEL OU TEL POSTE ?: 14
S'assurer alors qu'un poste est bien présent sur SEVEN : 14
S'assurer alors qu'un poste est bien présent sur xp : 15
S'assurer alors qu'un poste est bien présent sur 2000 : 15
S'assurer alors qu'un poste est bien présent sur NT : 16

AUTORISATIONS DE PARTAGE - PERMISSIONS D'ACCES (NTFS) 17
AUTORISATION DE PARTAGE : 17
PARTAGE ET SECURITE: 17
En système FAT: 17
En système NTFS : 17
SECURITE OU PARTAGE: 17

AUTORISATIONS DE PARTAGE 18
DESACTIVER LES PARTAGES SIMPLIFIES: 18
EFFECTUER UN PARTAGE: 18
DONNER UNE AUTORISATION DE PARTAGE: 19
Les 3 "faux types" et 2 "vraies" Autorisations de Partage 20
Le refus de Partage 20
COMBINAISON D'AUTORISATIONS DE PARTAGE : 21
PLANIFICATION DES AUTORISATIONS DE PARTAGES: 21
Exemple 1 : 21
Exemple 2 : 22
GESTION DES PARTAGES 22
SPECIFICITE WINDOWS 2008 - SEVEN ET MOT DE PASSE VIDE : 23

PARTAGES - LECTEURS RESEAUX SEVEN 24
CONNECTER UN LECTEUR RESEAU : 24
SE CREER UN RACCOURCIS SUR UN LECTEUR / REPERTOIRE RESEAU : 25
GERER LES PARTAGES: 26
LISTER LES LECTEURS RESEAUX EN COURS: 26

"TOPOLOGIE DE RESEAU" SEVEN 27
CENTRE RESEAU ET PARTAGE : 27

PARTAGES SIMPLIFIES XP 29
LES NIVEAUX PRE-DEFINIS SOUS XP : 29
LES 5 NIVEAUX PRE-DEFINIS SOUS XP : 29

Niveau 1 ..... *29*
Niveau 2 (par défaut) *30*
Niveau 3 ..... *30*
Niveau 4 (partage sur le réseau en lecture seule) *30*
Niveau 5 (partage sur le réseau en lecture ecriture) *31*
CONSEQUENCES DES PARTAGES SIMPLIFIES – "FORCE-GUEST": 31
PARTAGES SIMPLIFIES "FORCE-GUEST" **32**
ENVIRONNEMENT ACCES RESEAU SOUS XP : 32
Compte invité : *32*
Stratégie locale – droits utilisateurs – refuser accès réseau : *32*
Assistant partage accès réseau sous XP : *33*
DESACTIVATION PARTAGES SIMPLIFIES : 33
Utiliser le compte invité : *34*
SYNCHRONISATION SOUS XP **35**
AUTORISATION LORS DU PARTAGE : 35
PARAMETRAGE DU CLIENT : 36
DEMANDE DE MISE EN CACHE : 36
MACHINE DISTANTE INACCESSIBLE - PARAMETRAGE: 37
SUPPRIMER DES FICHIERS HORS CONNEXION: 37
WORKSGROUP & DOMAINES **38**
WORKSGROUP GROUPE DE TRAVAIL: 38
APPARTENIR A UN WORKSGROUP AVEC SEVEN: 38
APPARTENIR A UN WORKSGROUP AVEC WINDOWS XP: 39
APPARTENIR A UN WORKSGROUP AVEC WINDOWS NT 2000 : 39
DOMAINE : 40
GESTION DE DOMAINE SOUS WINDOWS 2008: 41
ACTIVE DIRECTORY **43**
QU'EST-CE UN SERVICE D'ANNUAIRE ?: 43
LA STRUCTURE LOGIQUE D'ACTIVE DIRECTORY DANS UN DOMAINE: 44
Domaine *44*
Annuaire & Espace de noms *44*
Active Directory & DNS *44*
Contrôleur de schéma *44*
Nom *45*
Objet *45*
Conteneur UO *46*
LA STRUCTURE LOGIQUE AU SEIN DE PLUSIEURS DOMAINES: 46
Arbres-arborescence de domaines *46*
Forêts *47*
Catalogue Global *48*
Relations d'approbation *48*
LA STRUCTURE PHYSIQUE D'ACTIVE DIRECTORY: 48
Sites *48*
ASSISTANT ACTIVE DIRECTORY & DCPROMO **49**
DCPROMO ET SERVICES DE DOMAINE ACTIVE DIRECTORY ADDS 2008: 49
"PROMOTION" WINDOWS 2008 R2: 50
OPTIONS DISPONIBLE AVEC DCPROMO /ADV 55
"RETROGRADATION" WINDOWS 2008 - 2008R2: 56
DCPROMO SERVEUR 2003: 58
"PROMOTION" WINDOWS 2003 : 58
"RETROGRADATION" WINDOWS 2003 : 62
GESTIONNAIRE DE SERVEUR **64**
LANCER LA MMC GESTIONNAIRE DE SERVEUR: 64
ROLES SERVICES ET FONCTIONALITES 66
PRESENCE DU DNS **67**

LANCER LA MMC DNS: 67
VERIFIER LA PRESENCE DE AD ET DU SERVEUR: 67
VERIFICATION PARAMETRE IP SERVEUR : 68
PRESENCE DE AD 69
LANCER LA MMC AD: 69
PRESENCE DU COMPTE ADMINISTRATEUR: 70
STRATEGIES DE DOMAINE 71
STRATEGIE MOT DE PASSE SUR DOMAINE: 71
ADHESION A UN DOMAINE 73
APPARTENIR A UN DOMAINE DEPUIS UN CLIENT SEVEN - XP : 73
1-m Création du compte ordinateur sur le serveur (manuelle) 73
1-a Création du compte ordinateur (à la volée) 74
2 –m Création de l'enregistrement hôte dans le DNS (manuelle) 75
2 –a Création de l'enregistrement hôte dans le DNS (à la volée) 75
3 Saisie dans les paramètres Tcp-ip et vérification du nom machine 75
4 Demande d'adhésion au Domaine 76
OUVERTURE DE SESSION 78
DERNIER LOGIN UTILISE : 78
OUVERTURE DEPUIS SEVEN : 79
OUVERTURE DEPUIS XP : 79
COMPTES UTILISATEURS DE DOMAINE 80
COMPTES UTILISATEURS PREDEFINIS : 80
CREER UN COMPTE UTILISATEUR SUR LE DOMAINE: 81
PROPRIETE COMPTE UTILISATEUR DE DOMAINE: 82
Compte Utilisateur onglet Général : 83
Compte Utilisateur onglet Compte : 83
Compte Utilisateur onglet Profil : 84
Compte Utilisateur onglet Membre de : 85
GROUPES LOCAUX 86
GROUPES LOCAUX PREDEFINIS : 86
GROUPES SPECIAUX 88
GROUPES GLOBAUX-UNIVERSELS 90
GROUPES LOCAUX - GLOBAUX - UNIVERSELS: 90
GROUPES GLOBAUX PREDEFINIS 91
INCLUSIONS ENTRE GROUPES SOUS NT 92
WINDOWS 2000 – 2003 MIXTE NATIF 93
QUELQUES REGLES POUR CREER DES GROUPES : 95
EXEMPLE : UTILISATEUR DE DOMAINE - UTILISATEUR AVEC POUVOIR 95
EXEMPLE ACCES RESSOURCES : 96
EXEMPLES 3 : 96
EXEMPLE : GROUPES ADMINS DE DOMAINE & ADMINISTRATEURS: 97
CREATION – GESTION DE GROUPES 98
GROUPE LOCAL SUR UN POSTE: 98
GROUPE LOCAL – GLOBAL SUR UN SERVEUR CD: 98
MEMBRES D'UN GROUPE: 99
GERER - INFORMATION SUR LES GROUPES - 100
SUPPRESSION D'UN GROUPE 100
REPERTOIRE DE BASE 101
REPERTOIRE DE BASE OU D'ACCUEIL : 101
MISE EN PLACE : 101
Avant la création des comptes 101
Pendant la création d'un compte 102
RESULTAT : 103

MODIFIER LE REPERTOIRE DE BASE : 104
REMARQUES SUR LE REPERTOIRE DE BASE : 104
SCRIPT D'OUVERTURE DE SESSION 105
OBJECTIF : 105
INDIQUER UN SCRIPT D'OUVERTURE DE SESSION : 105
ECRITURE DE SCRIPTS : 106
création de lecteur logique 106
COMMANDE NET 107
CONVENTION D'ECRITURE : 107
COMMANDES NET UTILISABLES : 107
NET USE : 108
NET SEND : 110
NET USER 111
NET VIEW: 112
PROFILS SEVEN - XP 113
OBJECTIF : 113
LES DIFFERENTS PROFILS: 114
Profil local : 114
Profil par défaut local : 114
Profil par défaut de réseau : 114
Profil itinérant : 114
Profil obligatoire : 114
Profil super-obligatoire : 114
PROFILS LOCAUX SEVEN: 115
RAPPELS PROFILS LOCAUX XP-2000: 116
Différence entre 2000 et XP : 116
PROFILS PAR DEFAUT LOCAL : 117
PROFILS PAR DEFAUT RESEAU : 117
CONFIGURER LES PROFILS ERRANT SUR LE SERVEUR: 118
CONFIGURER LES PROFILS ERRANT POUR LES COMPTES UTILISATEURS: 119
SUPPRESSION PROFIL ERRANT SUR UN POSTE CLIENT: 120
SUPPRESSION PROFIL ERRANT STOCKE SUR LE SERVEUR: 120
SUPPRIMER TOUS LES PROFILS LOCAUX D'UNE MACHINE: 121
PROFIL ERRANT OBLIGATOIRE (MANDATORY) : 122
PROFIL ERRANT SUPER OBLIGATOIRE SEVEN: 122
COPIE DE PROFIL LOCAL EN ERRANT : 123
TRANSFERT DE PROFIL LOCAL SUR UN AUTRE PROFIL : 123
HORODATAGE ET PROFILS : 124
LOGIQUE DE GESTION DES PROFILS : 124
LOGIGRAMME GESTION DES PROFILS : 125
IMPRIMANTE RESEAU 126
INSTALLER UNE IMPRIMANTE RESEAU : 126
PARTAGER UNE IMPRIMANTE LOCALE / RESEAU: 127
ACCEDER A UNE IMPRIMANTE DEJA INSTALLEE SUR LE RESEAU : 127
GERER UNE IMPRIMANTE RESEAU 129
GESTIONNAIRE D'IMPRESSION: 129
AUTORISATION SUR IMPRIMANTE: 130
PLUSIEURS IMPRIMANTE SECURISEES DIFFEREMMENT : 130
POOL D'IMPRIMANTE: 131

LES CLIENTS WINDOWS

Configuration minimale:

Une réseau doit être installée,

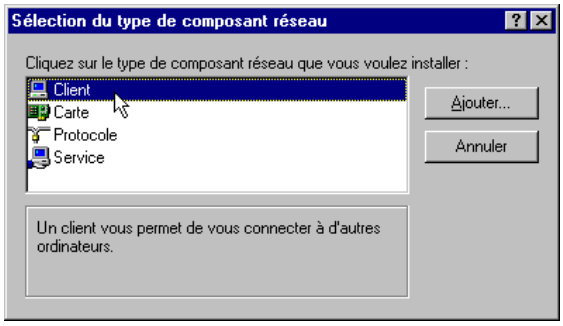
TCP-IP le protocole choisit

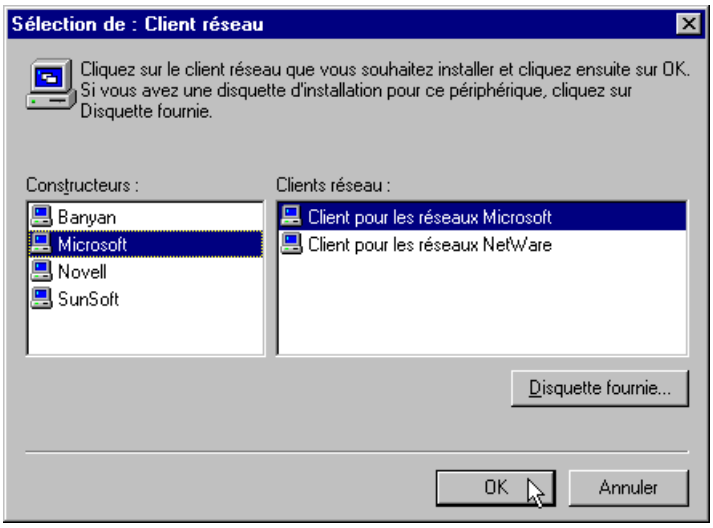
Des adresses IP correctes doivent être validées

Client réseau Windows:

Sous Windows faut spécifier:

- si nous souhaitons utiliser des ressources réseau : **"notion de client"**

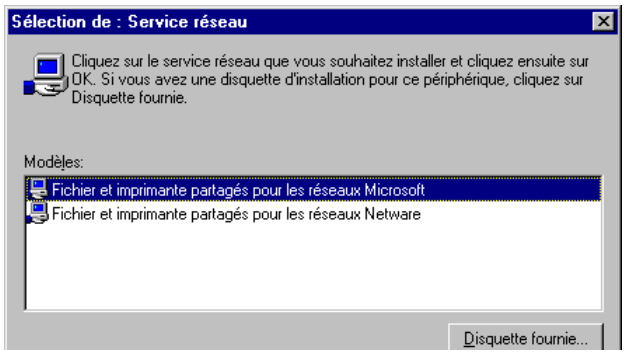




N.B: si on n'installe pas de client, alors on ne pourra pas aller chercher des ressources sur d'autres machines présentes réseau. Indépendamment de toutes notions de partages, login et autres…

Services réseau Windows:

- si l'on souhaite mettre en oeuvre des services pour les autres machines du réseau: **"notion de service"**



N.B: si on n'installe pas de services, alors on ne pourra pas être utilisé par d'autres machines sur le réseau. Et l'option partage ne sera pas disponible dans les menus . Indépendamment de tous autres réglages …

Nom de poste Windows :

Cette étape n'est pas à négliger sinon beaucoup de soucis guettent…A noter qu'un nom d'hôte et un nom d'ordinateur (nom netbios) sont deux choses différentes, même si par défaut, dans un réseau microsoft, ce sont les mêmes.

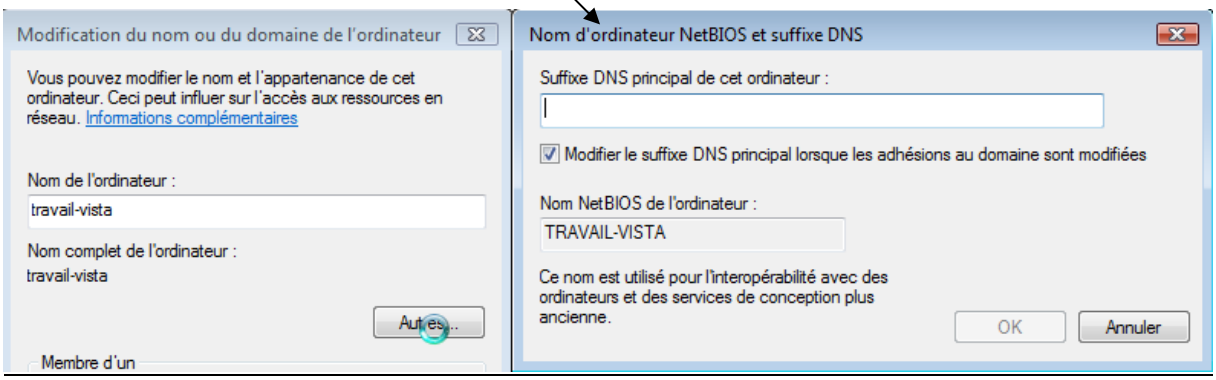
En toute rigueur, ils se définissent ainsi :

98-NT4 Nom netbios :
Propriétés **Voisinage réseau**
Onglet **identification**
Nom d'ordinateur

N98-NT4 nom d'hôte :
Propriété **TCP/IP**
onglet **DNS**
Hôte

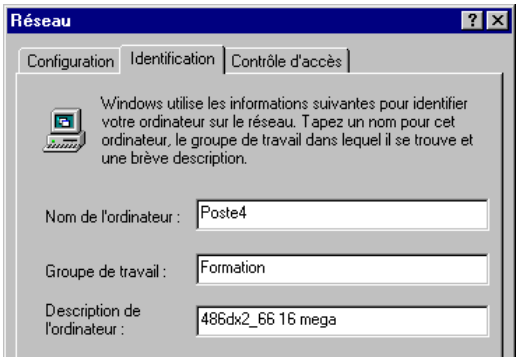
2000 Nom netbios = **Nom d'hôte** Par défaut, (par traduction automatique) :
Propriétés **Poste de Travail**
Onglet **identification réseau**
Nom d'ordinateur

XP-SEVEN Nom netbios = **Nom d'hôte** Par défaut, (traduction automatique) :
mais on peut en spécifier un différent



trois particularités :

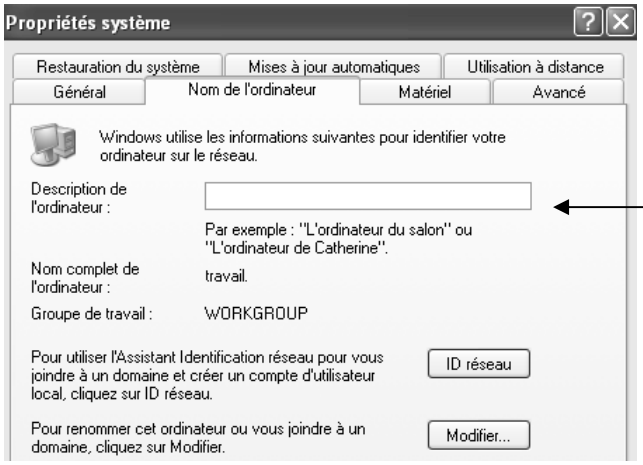
Sous windows 9x:



la notion de domaine NT n'existe pas.

Un poste 95-98 ne peut que faire partie d'un **Workgroup** c.a.d. **Groupe de Travail**

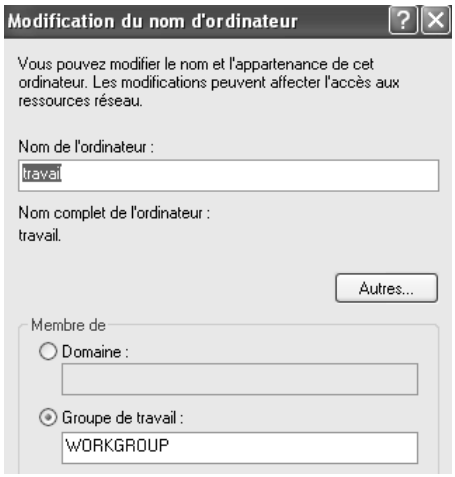
Sous windows XP:



Apparition d'une zone "**Description de l'ordinateur**"

A ne pas confondre avec le nom de l'ordinateur

Accessible par **Modifier…**

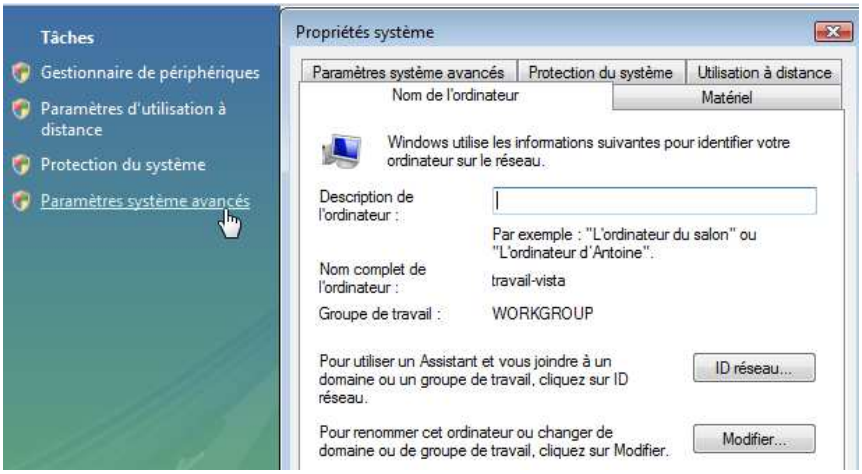


N.B: ne jamais rentrer une **Description de l'ordinateur** différente du **Nom de l'ordinateur**

N.B: ne jamais suivre l'exemple, mais utiliser les règles classiques (- de 15 caractères… etc…)

Sous windows SEVEN :

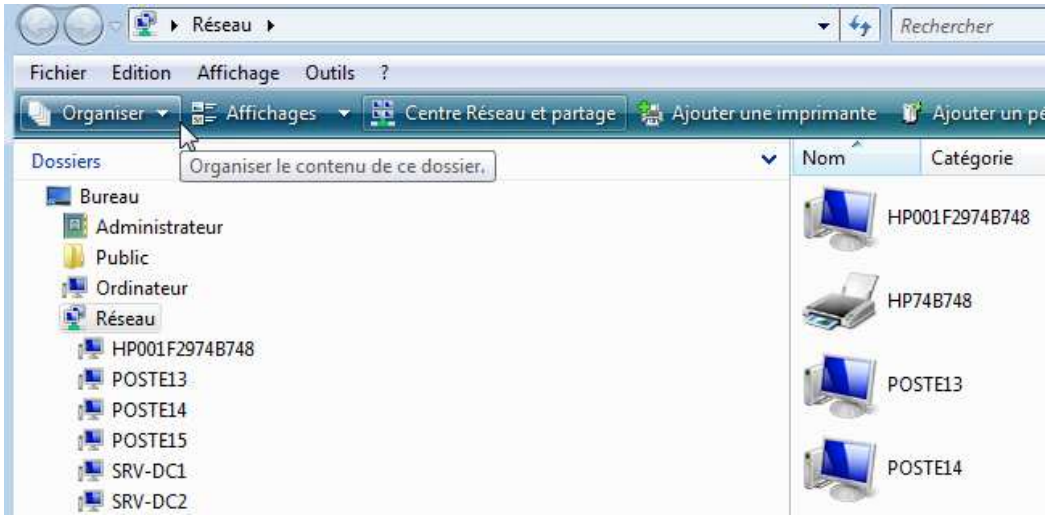
même situation que sous XP



VOISINAGE – FAVORIS RESEAU

Réseau SEVEN en Workgroup :

Si on est sur un poste Windows SEVEN installé correctement, au niveau de l'icône **Réseau** on devrait voir

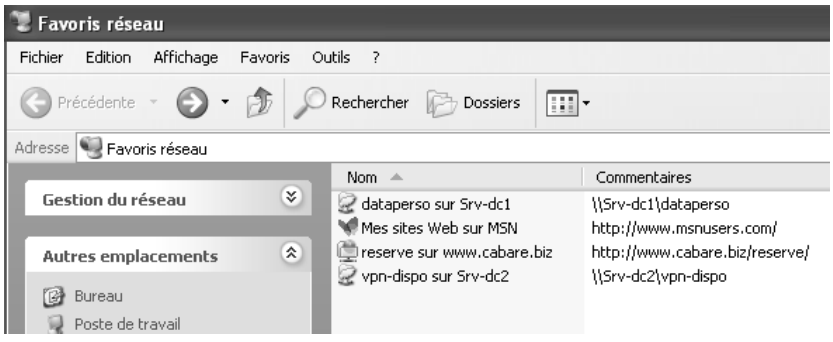


Dans la partie haute, une liste déroulante est disponible

Et on peut bien sur taper les noms UNC des postes que l'on souhaite atteindre…

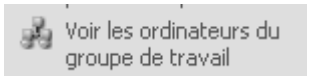
Favoris réseau XP en Workgroup :

Si on est sur un poste Windows XP installé correctement, au niveau de l'icône **favoris réseau** on devrait voir

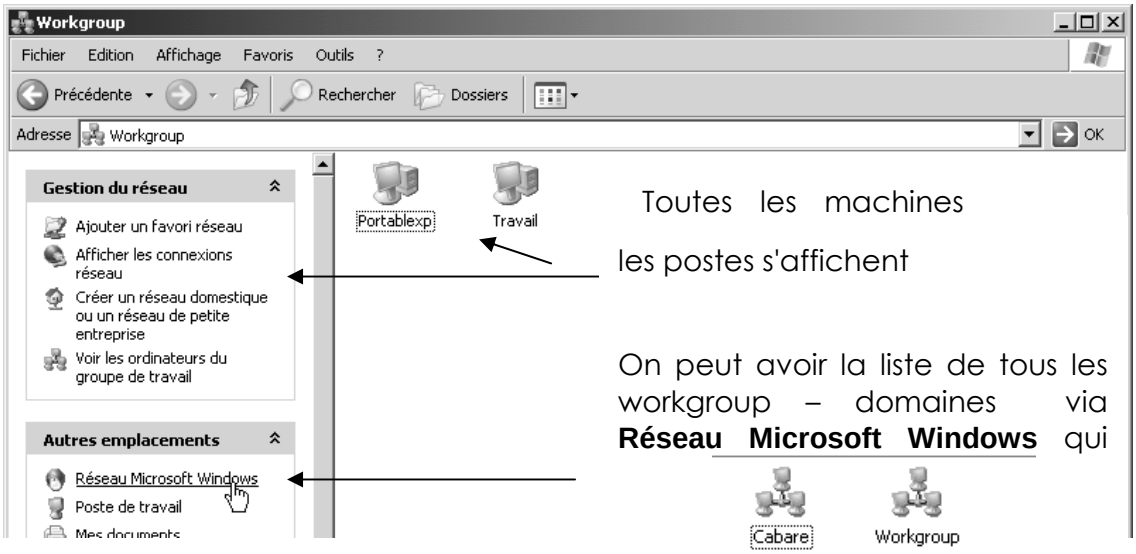


Ce qui peut être assez déroutant…

Pour voir les connexions possibles, il faut demander dans

Gestion du réseau et ensuite 

Si on demande d'afficher notre **workgroup** alors



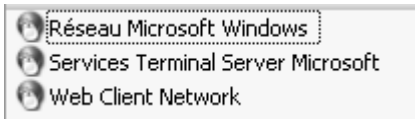
Toutes les machines les postes s'affichent

On peut avoir la liste de tous les workgroup – domaines via **Réseau Microsoft Windows** qui

donne

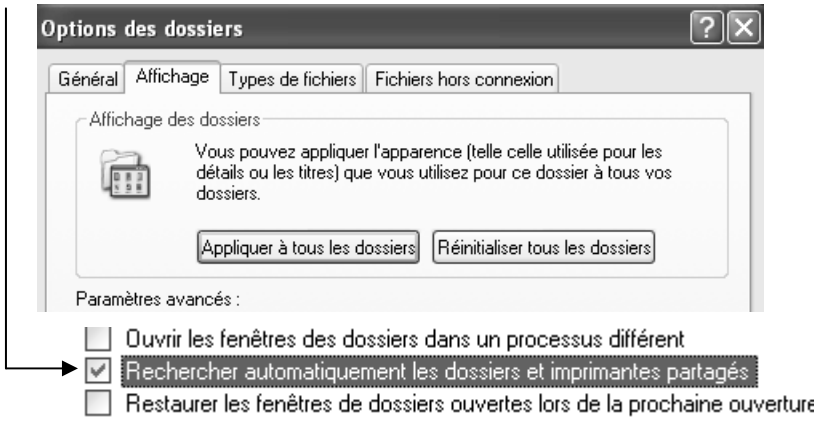
ensuite on pourrait également

via

obtenir 

N.B: Dans XP, afin d'alléger l'affichage, il faut impérativement demander de pas afficher "tout" ce que l'on peut atteindre, ce qui s'obtient via les options

Outils / Options des dossier onglet **Affichage / Paramètres avancés**



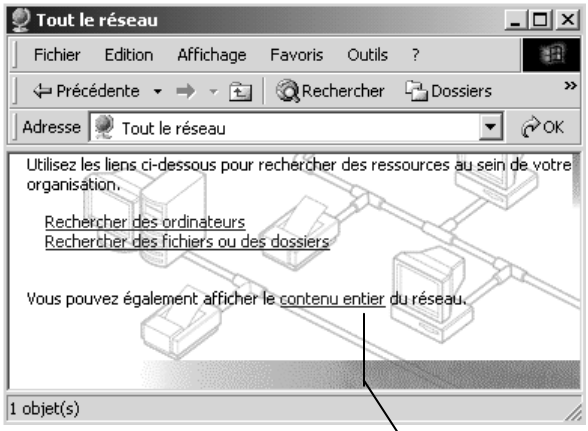
il faut décocher cette option

Favoris réseau 2000 :

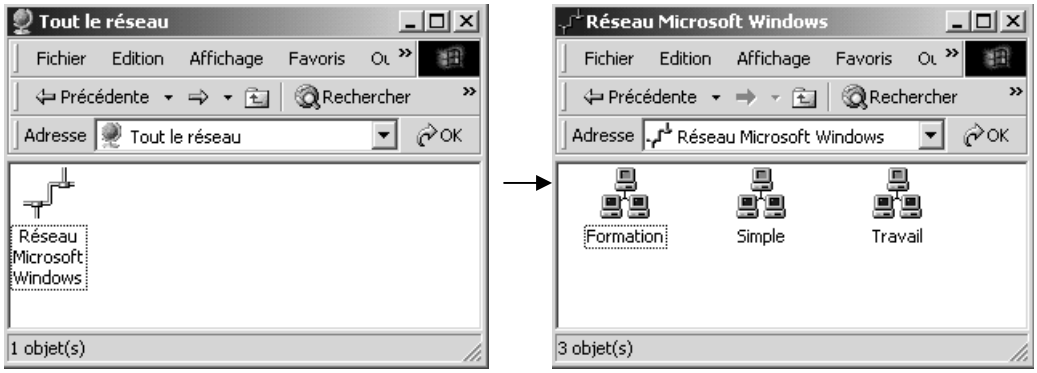
La notion de **favoris Réseau** apparaît avec 2000.

donnant

donnant

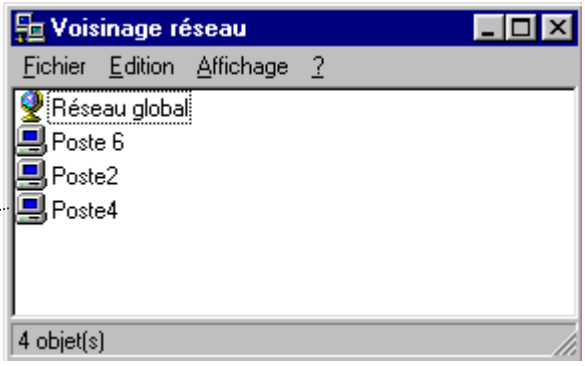


En demandant Contenu entier du réseau on retrouve



Voisinage réseau windows NT:

Si on est dans un poste Windows NT installé correctement avec une carte réseau, et relié au serveur, alors au niveau de l'icône voisinage réseau on devrait voir l'image suivante



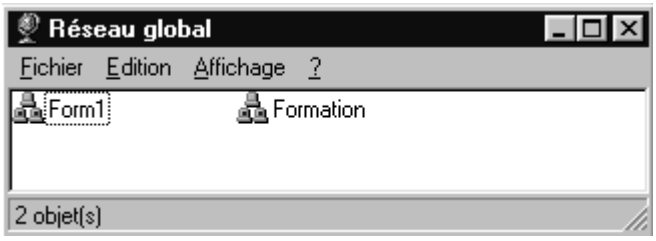
Les ordinateurs visibles en première instance dans voisinage réseau sont les ordinateurs faisant partie du même groupe de travail, ou d'un Domaine ayant un nom « homonyme »

Si le poste n'était relié a aucun autre poste, il n'y en aurait aucun

Par **réseau global** on entends la visualisation de tous les **groupes de travail** éventuellement définis et accessibles, et bien sûr de tous les **domaines**, donc notamment le serveur NT que l'on vient de monter

Ils s'agit en fait de tous ce qui est accessible au sens large et qui correspond à la notion de Domaines-Workgroup sous NT

Tous les "Domaines-Workgroup" apparaîtront sous forme de trois postes en triangle



NB : Depuis une machine Windows, on voit autant de regroupement que de nom de workgroup out de domaines différents

RECHERCHER UN POSTE

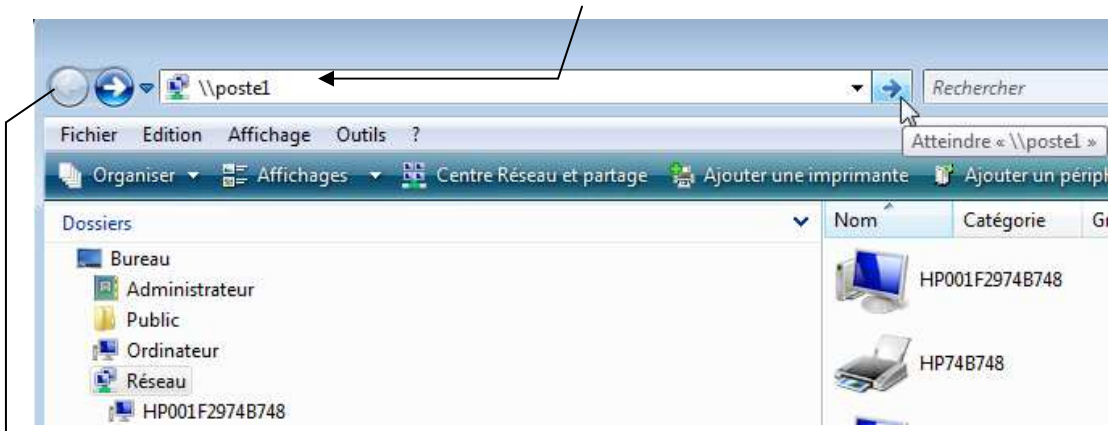
Pourquoi je ne vois pas tel ou tel poste ?:

Souvent, un poste est long à apparaître, puis il apparaît comme par « magie » au bout d'un délai qui semble interminable. Il faut bien penser que les postes font autre chose de temps en temps que d'envoyer des trames sur le réseau dans le seul but de mettre à jour l'affichage !

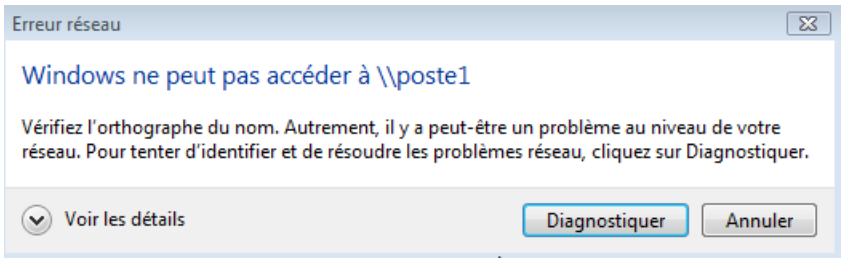
S'assurer alors qu'un poste est bien présent sur SEVEN :

On peut lorsque l'on demande de voir le réseau, demander alors d'atteindre une machine particulière

il suffit de taper le nom netbios UNC, sous la forme **\\nom-machine** dans la barre de titre



Si le nom n'existe pas (ou ne peut être trouvé) alors on obtient un message



si le nom est correct, le poste s'affiche…

N.B: on peut aussi taper une adresse ip

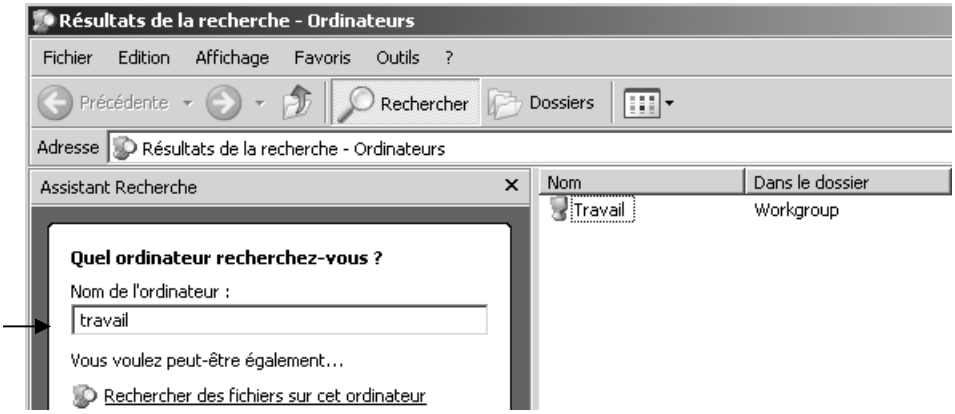
S'assurer alors qu'un poste est bien présent sur xp :

On peut lorsque l'on demande de voir tout le réseau, demander alors **Rechercher des ordinateurs,**

soit clic droit sur **Favoris réseau / Rechercher des ordinateurs**

et on obtient

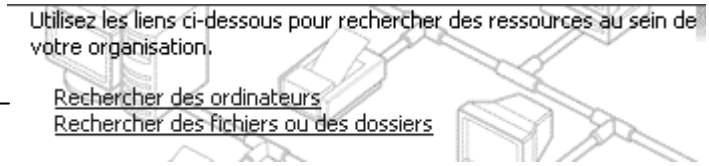
On cherche un nom machine précis



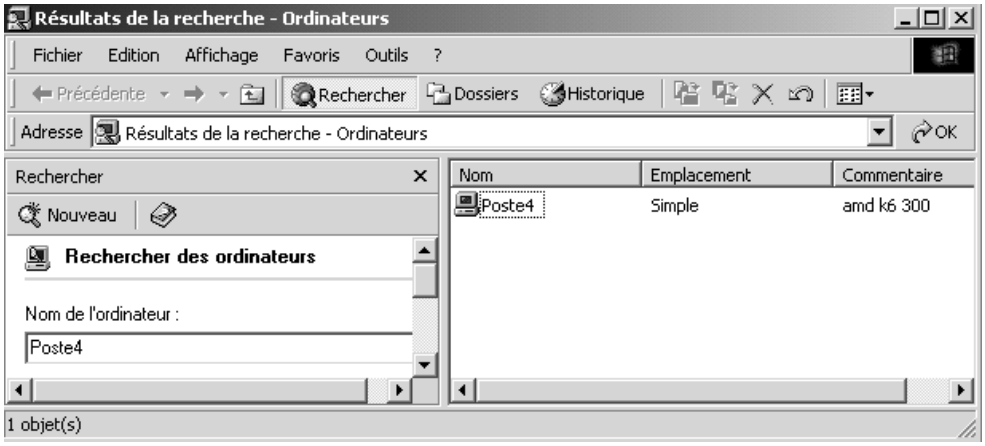
On a dans **Emplacement** le nom du Workgroup ou Domaine...

S'assurer alors qu'un poste est bien présent sur 2000 :

On peut lorsque l'on demande de voir tout le réseau, demander alors **Rechercher des ordinateur**

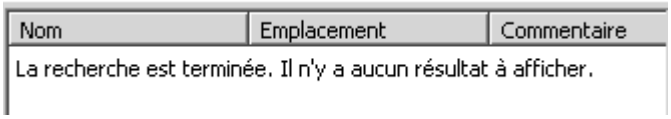


Si on obtient



on a dans **Emplacement** le nom du Workgroup ou Domaine...

Mais si on obtient

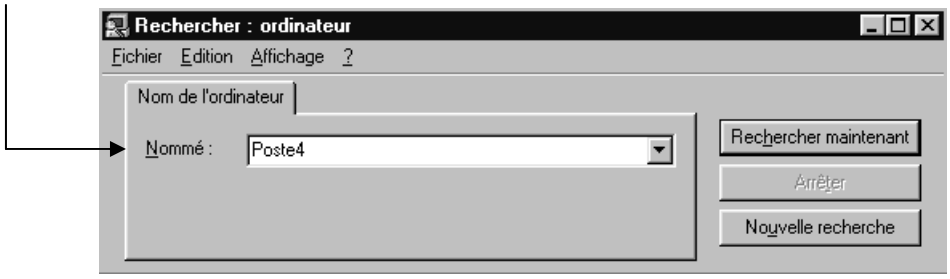


il ne faut pas d'attendre !!!!

S'assurer alors qu'un poste est bien présent sur NT :

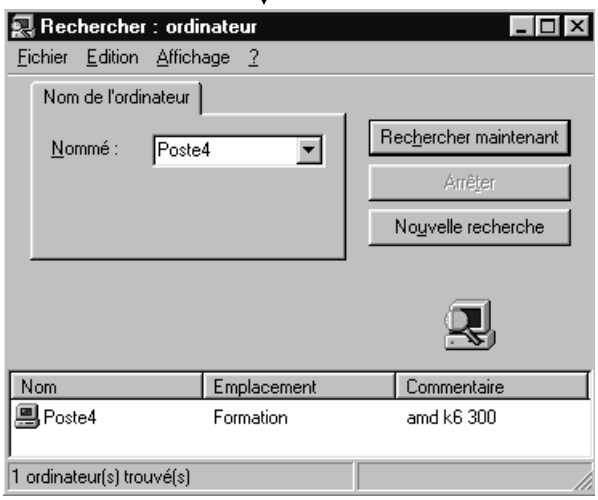
Démarrer / Rechercher / Ordinateur...

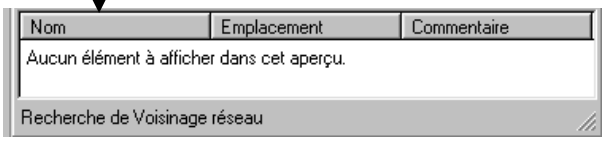
et on donne le non de l'Ordinateur cherché



On donne le Nom d'Ordinateur

Si on obtient ↓ mais si on a ↓ attendre est inutile





on a dans **Emplacement** le nom du workgroup ou Domaine, et l'affichage n'est plus qu'une question de délai...

AUTORISATIONS DE PARTAGE - PERMISSIONS D'ACCES (NTFS)

Autorisation de Partage :

Toute personne connectée sur le réseau est un utilisateur qui peut accéder à des ressources qui ont été au préalable partagée.

Que le disque soit en FAT, FAT32 ou NTFS on doit forcément le partager pour pouvoir y accéder depuis le réseau

Les autorisations de partages s'appliquent également sur des ressources qui ne sont pas des espaces de stockage, comme des imprimantes ou des lecteurs de CDROM....

Partage et Sécurité:

C'est à ce niveau là qu'il va y avoir une différence entre des systèmes disques montés en FAT, ou des systèmes disques montés en NTFS....

En système FAT:

- La seule sécurité possible sur une partition FAT est celle apportée par les mécanismes de partage de répertoire
- Par conséquent rien n'est prévu pour limiter les accès depuis une session locale

En système NTFS :

- Les mécanismes de partage de répertoire existent sur un système NTFS pour réguler les tentatives d'accès depuis le réseau
- Mais les fichiers et les dossiers sur une partition NTFS peuvent se voir attribuer des permissions d'accès **indépendamment de leurs partages**, par conséquent NTFS est prévu pour limiter les accès aussi depuis une session locale

Sécurité ou Partage:

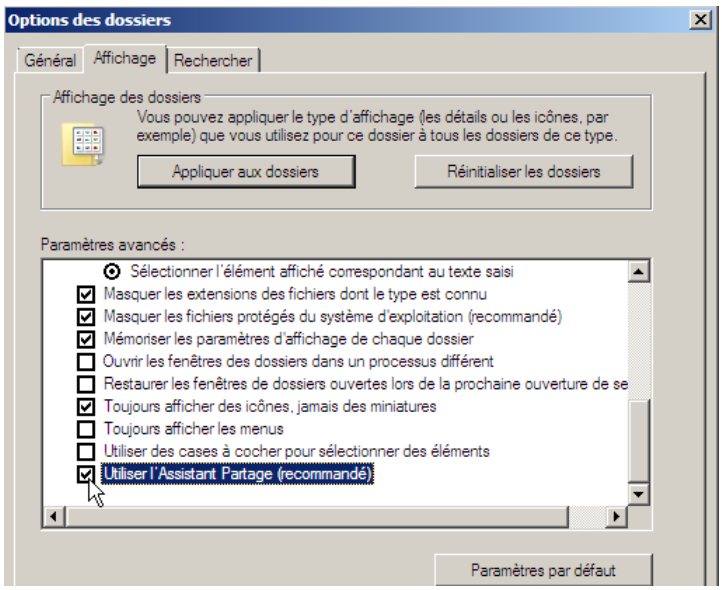
Sans refaire un chapitre en NTFS, il est clair que si la sécurité NTFS est disponible, alors au niveau des partages on laissera systématiquement Tout le Monde en Contrôle Total (ou en Lecture seule à la limite)

Et le chapitre suivant est … inutile !

AUTORISATIONS DE PARTAGE

Désactiver les partages simplifiés:

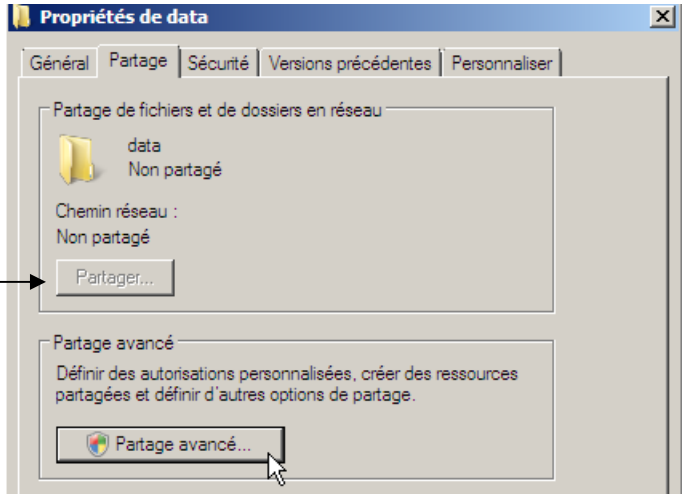
Afin de pouvoir travailler correctement, il faut désactiver la gestion simplifiée des partages, pour ne plus avoir accès à l'assistant…



Effectuer un partage:

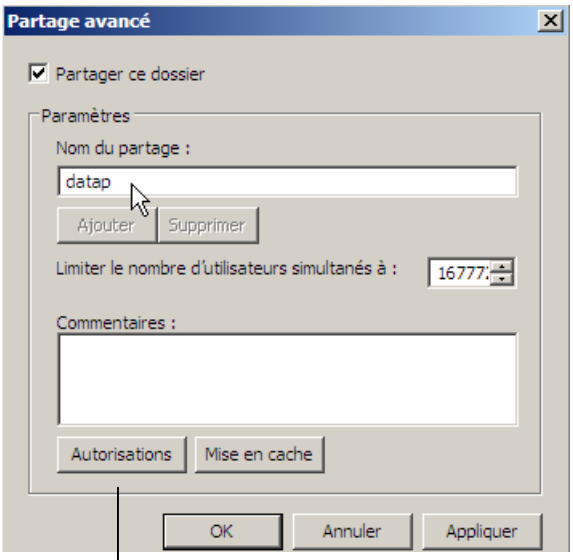
Il suffit de se placer sur la ressource à partager, puis de demander le menu contextuel de la souris, à savoir **Partage…**

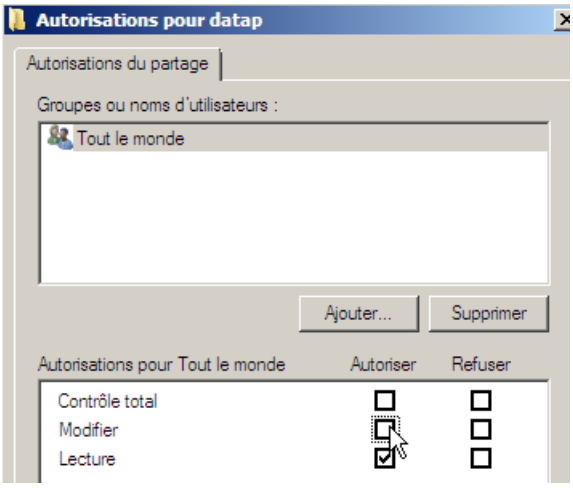
l'assistant est dévalidé, cela tombe bien, il ne faut pas s'en servir !



on demande **Partage avancé**…

On obtient

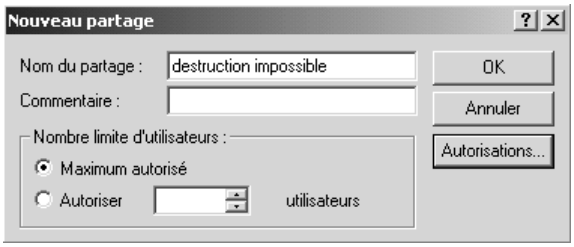




Si on veut en réserver l'accès à certains comptes utilisateurs ou à certains groupes, il va falloir travailler sur les autorisations de partage en cliquant sur **Autorisations** ...

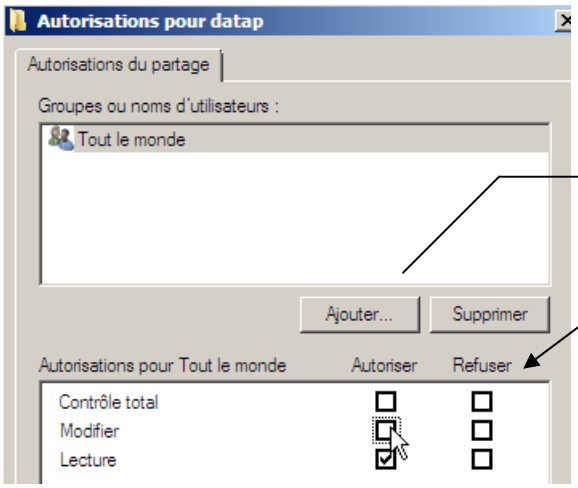
Attention : une ressource peut être partagée plusieurs fois par **Nouveau partage** sous des noms différents avec des autorisations différentes…

Dans un premier temps partagez une ressource que sous un seul nom !



Donner une Autorisation de Partage:

Ce sont les **Autorisations** que l'on doit donner pour filtrer qui peut accéder à cette ressource depuis le réseau



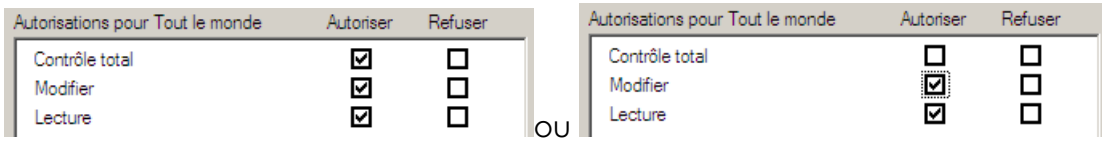
On peut Ajouter d'autres Groupes ou Utilisateurs par le bouton **Ajouter**

Sur lequel on appliquerait ensuite des Autorisations

(ou des Refus !)

Le **Groupe Spécial Tout le Monde** est inclus par défaut ...en **Lecture**

Mais on peut aussi donner



Attention aux valeurs des partages par défaut:

- Sous 2000 Pro - Serveur un partage par défaut est de type **Tout le Monde** en **Contrôle Total**
- Sous XP Pro - 2003 et 2008 Serveur un partage par défaut sera de type **Tout le Monde** en **Lecture Seule**

Les 3 "faux types" et 2 "vraies" Autorisations de Partage

Lire

Autorise :

- Affichage des noms de fichier et de sous-répertoire.
- Modification des sous-répertoires du répertoire partagé.
- Affichage des données dans des fichiers et exécution des fichiers d'application.

Modifier

Autorise :

- Affichage des noms de fichier et de sous-répertoire.
- Modification des sous-répertoires du répertoire partagé.
- Affichage des données dans des fichiers et exécution des fichiers d'application.
- Ajout de fichiers et de sous-répertoires au répertoire partagé.
- Modification des données dans des fichiers.
- Suppression de sous-répertoires et de fichiers.

Contrôle total (Total)

Autorise :

- Affichage des noms de fichier et de sous-répertoire.
- Modification des sous-répertoires du répertoire partagé.
- Affichage des données dans des fichiers et exécution des fichiers d'application.
- Ajout de fichiers et de sous-répertoires au répertoire partagé.
- Modification des données dans des fichiers.
- Suppression de sous-répertoires et de fichiers.

→ **Modifier** et **Contrôle Total** sont équivalent en partage…

Le refus de Partage

Le refus de partage « passe avant toute autre autorisation ».

Par exemple si un individu isolé dans un groupe ne doit pas faire une action, on lui appliquera un refus de partage juste à lui…, le fait que son groupe ait l'autorisation n'est pas gênant.

Combinaison d'autorisations de partage :

deux règles régissent les combinaisons de permission

1. la permission effective de l'utilisateur est la permission la moins restrictive obtenue par la combinaison des différentes permissions
2. si une permission "refuser » est donnée, cette dernière masque toutes les autres permissions, et la permissions effective résultantes est donc "aucun accès"

Donc si l'utilisateur est membre de plusieurs groupes, il hérite de toutes les permissions définies à travers chacun des groupes, sauf si la permission "refuser" est spécifiée pour au moins un groupe !

planification des autorisations de partages:

Il est capital que au niveau de l'arborescence, les dossiers nécessitant d'un **niveau de sécurité identique**, soit **crées à un niveau identique**

le dossier partagé apparaît en tant que "racine", et si on peut voir la totalité de ce dossier, et de ses éventuels sous-dossiers, on ne peut pas en "sortir"

donc, on peut accéder au contenu d'un dossier partagé (et donc à la totalité des sous-dossiers) , mais on ne peut pas accéder aux dossiers situés à un niveau plus élevé, ni aux dossiers de même niveau

N.B: Il ne faut donc jamais partager tous les dossiers individuellement, mais seulement le point d'entrée de la hiérarchie pour laquelle on souhaite laisser un accès.

N.B: Dans le cas on l'on ne dispose pas de volume NTFS on peut alors partager tous les dossiers individuellement, afin de construire une ébauche de sécurité…. MAIS CELA RESTE INCOMPLET ET PENIBLE.

Exemple 1 :

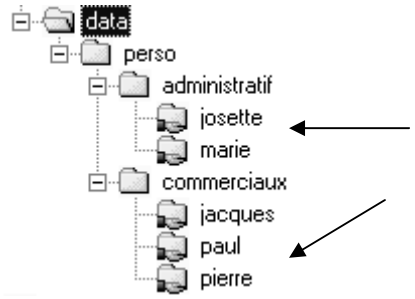
pierre, paul et jacques doivent avoir chacun un dossier personnel, sur lesquels l'administrateur à un droit de visite.

on commence par créer les dossiers personnels et les partages pour chacun

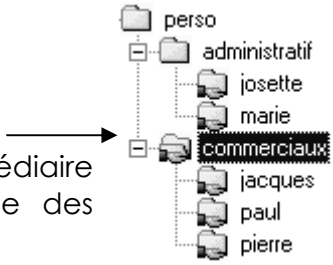
puis on partage au niveau supérieur (ici perso) pour l'administrateur : il verra toute la hierarchie et y aura accès !

Exemple 2 :

pierre, paul, jacques marie et josette doivent avoir chacun un dossier personnel . Pierre, paul et jacques commerciaux, doivent avoir chacun un dossier personnel, sur lesquels les administratifs marie et josette ont un droit de regard. l'administrateur à un droit total sur tout le monde, ….



on commence par créer les dossiers personnels et les partages pour chacun



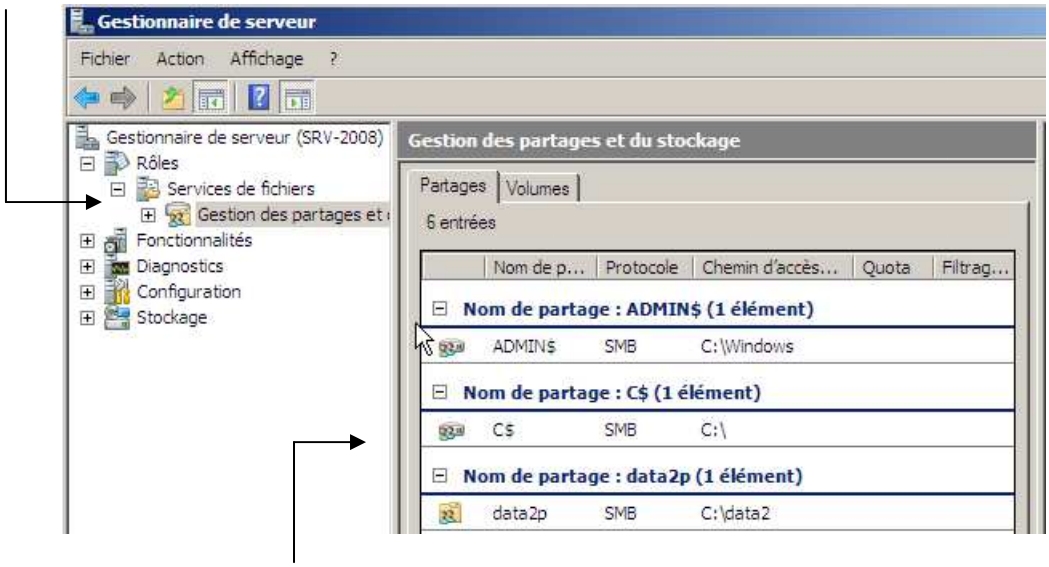
puis on partage au niveau intermédiaire (ici commerciaux) pour le groupe des administratifs (marie + josette)

et enfin au niveau supérieur pour l'administrateur

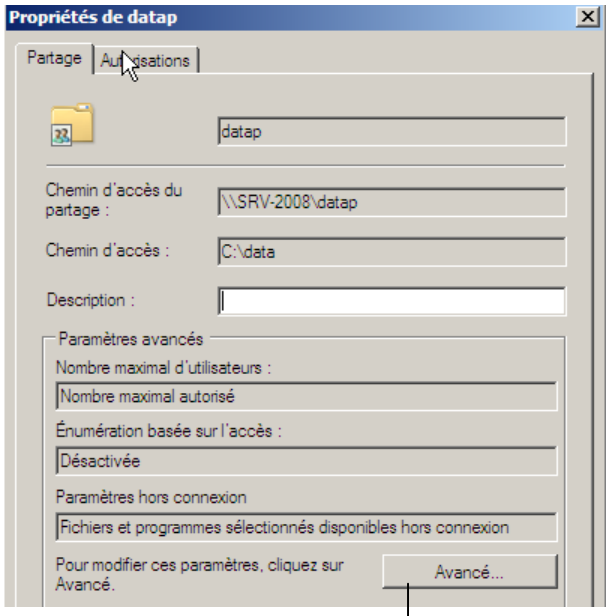
Gestion des partages

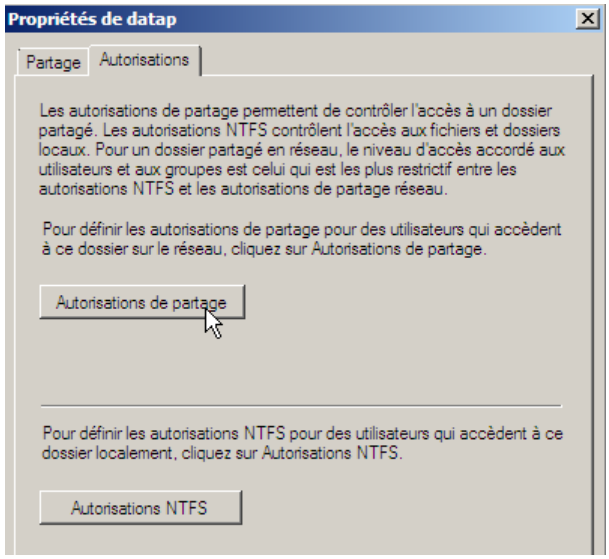
soit par l'icone de la barre des tâches gestionnaire de Serveur

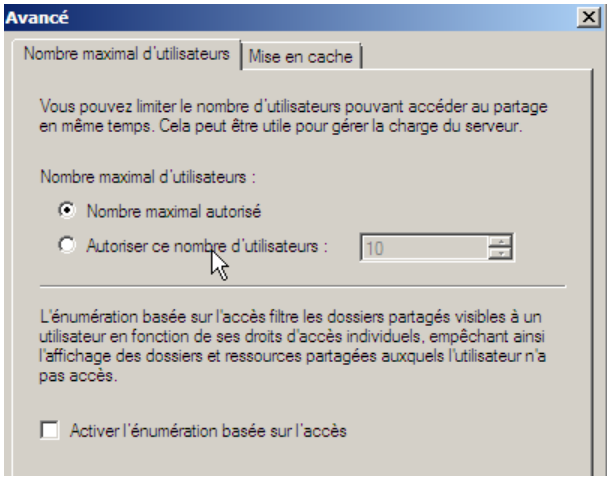
soit **clic droit / gérer** du **poste de travail**, on obtient le **Gestionnaire de serveur**



on peut ensuite sur un partage demander les **propriétés** ...



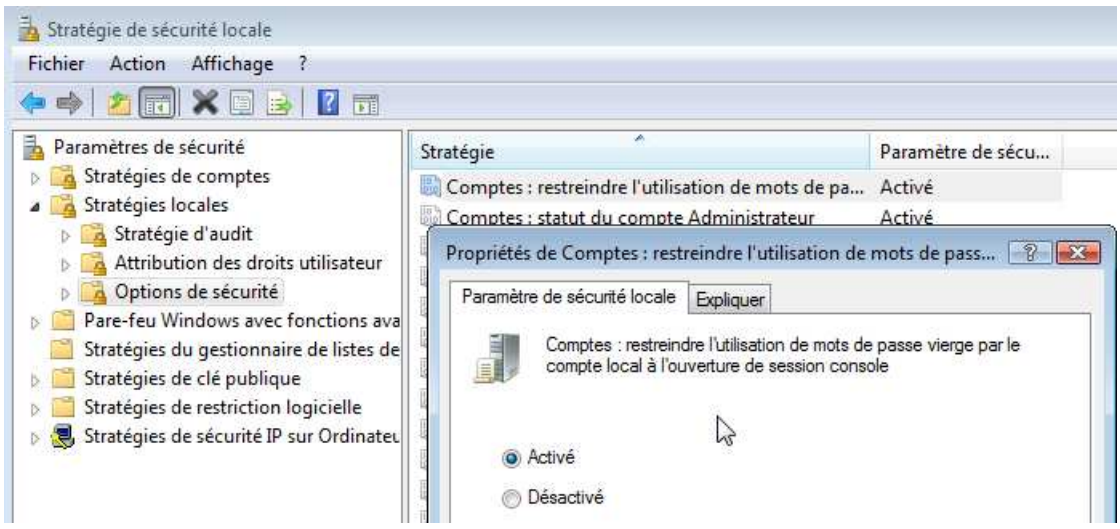




Spécificité Windows 2008 - SEVEN et mot de passe vide :

Les utilisateurs distants ne peuvent pas s'authentifier en utilisant un compte avec un mot de passe vide. Cette sécurité de l'authentification est configurée dans une **stratégie de sécurité locale**…

Paramètres de Sécurité / Stratégies locales / Options de sécurité / Comptes:



PARTAGES - LECTEURS RESEAUX SEVEN

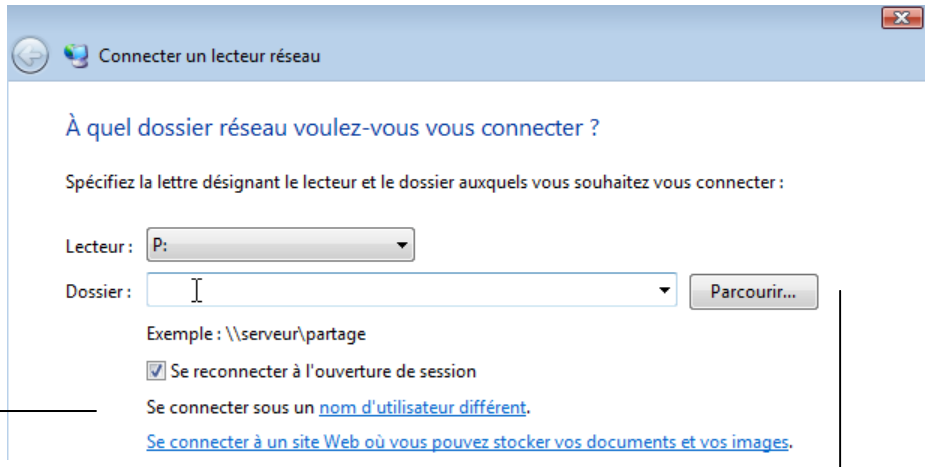
Connecter un lecteur réseau :

N.B : il faut bien sûr que le partage ait été fait sur le poste serveur

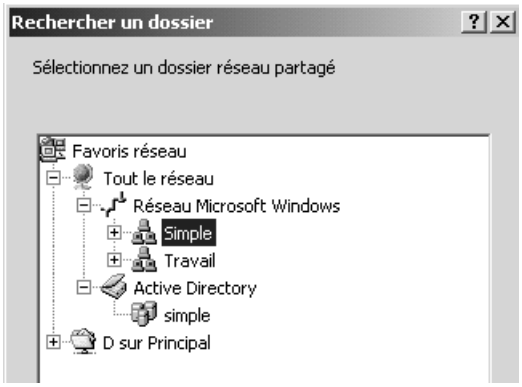
On accède à l'assistant connection de lecteur réseau en demandant le menu contextuel **Propriété** de l'icône **Favoris réseau** du bureau

(on peut aussi se placer directement sur la ressource à connecter… ou demander le menu **Outils / Connecter un lecteur Réseau**)

Pour obtenir alors cette boite de dialogue



on peut demander **Parcourir…**

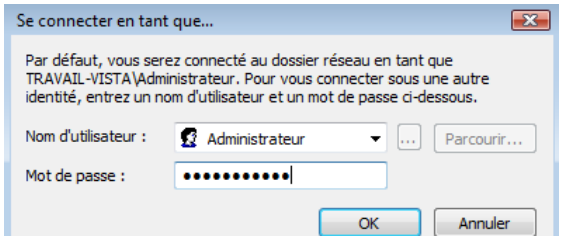


Mais on peut aussi sans attendre

L'interface graphique entrer directement dans **Dossier** une invite du genre

\\nomserveur\nompartage

On peut demander une autre authentification pour ce lecteur…



Se Créer un raccourcis sur un lecteur / répertoire réseau :

Il faut bien sûr que le partage ait été fait sur le serveur

Pour pouvoir créer un raccourci sur un répertoire partagé,

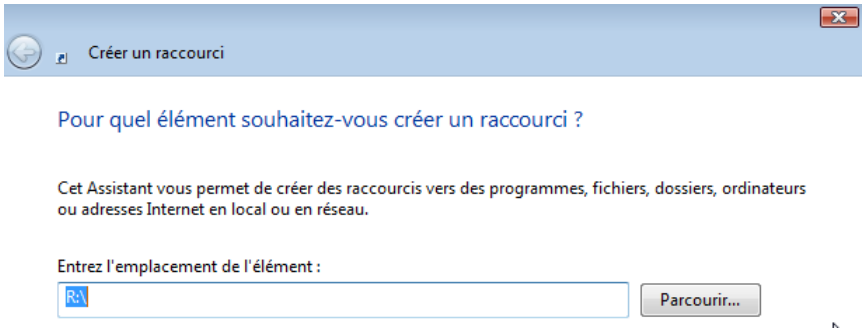
il suffit de lancer l'explorateur puis de visualiser la ressource à atteindre,

Un clic droit de la souris amène le menu contextuel:

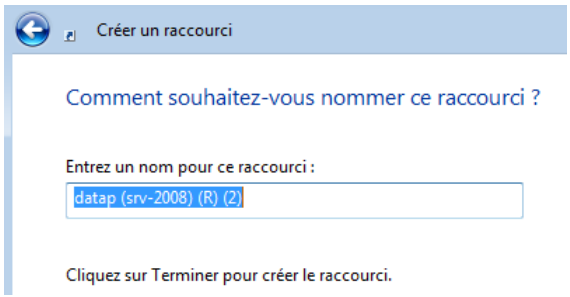
On demande **Créer un raccourci**

Il suffit de placer ensuite le raccourci sur le bureau (ou ailleurs…)

Pour pouvoir créer un raccourci sur un lecteur réseau, on demande avec le clic droit de créer un raccourci, et on complète



on peut aussi indiquer un chemin réseau directement sous la forme **\\poste\partage**...



on obtient alors

N.B : l'icône peut être différente, selon que vous ayez saisit le nom UNC, taper la lettre d'un lecteur réseau pré-existant, ou demandé parcourir le réseau…

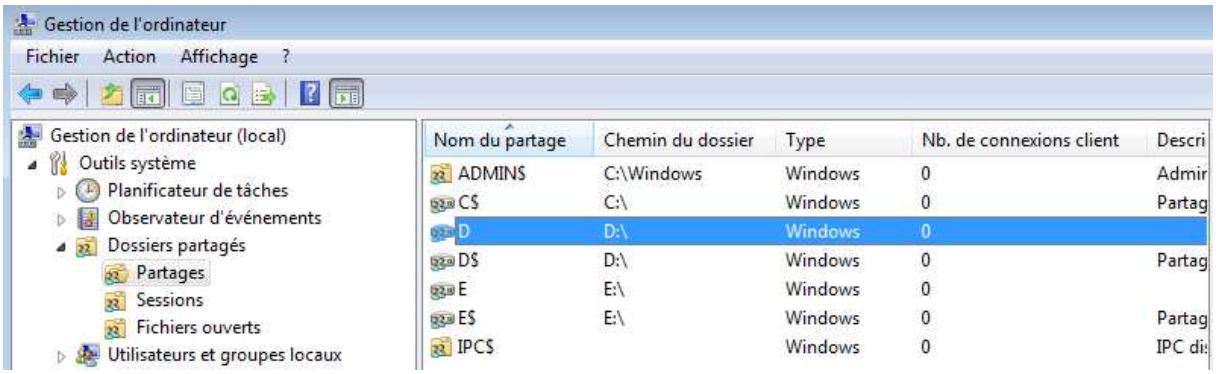
N.B : lors d'une session ultérieure, si c'est un autre utilisateur qui se connecte sur le poste SEVEN, il ne verra rien des raccourcis crées par son collègue, car ses modifications sont stockées dans les profils

Gérer les partages:

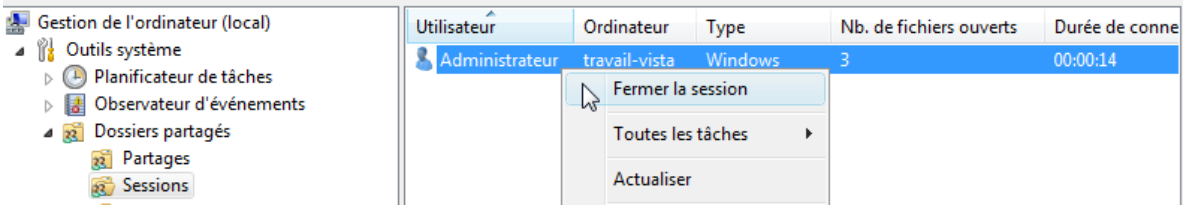
Il s'agit de gérer les partages réalisés sur le poste SEVEN, (et non pas les partages auxquels on a accès depuis le poste SEVEN)

Depuis le **Poste de Travail** clic droit **gérer**

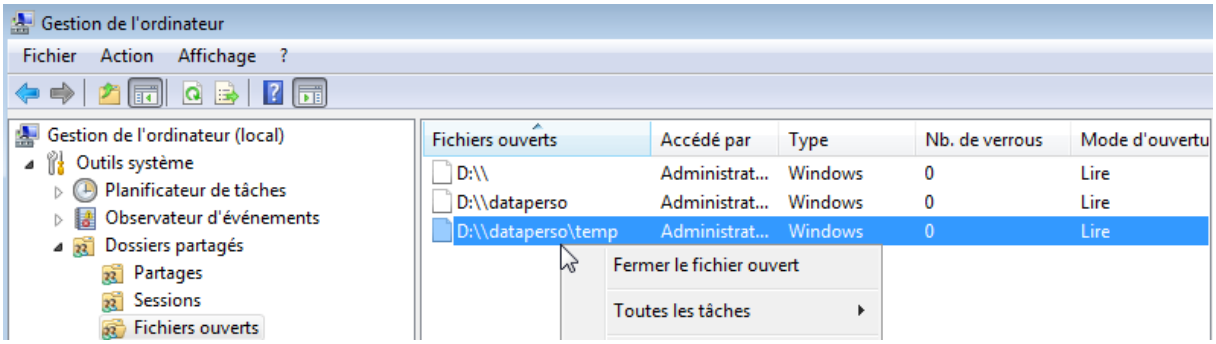
Onglet **Partages**



Onglet **Sessions**



Onglet **Fichiers ouverts**



N.B : Sur Windows **SEVEN** il existe **10** session maxi…

Lister les lecteurs réseaux en cours:

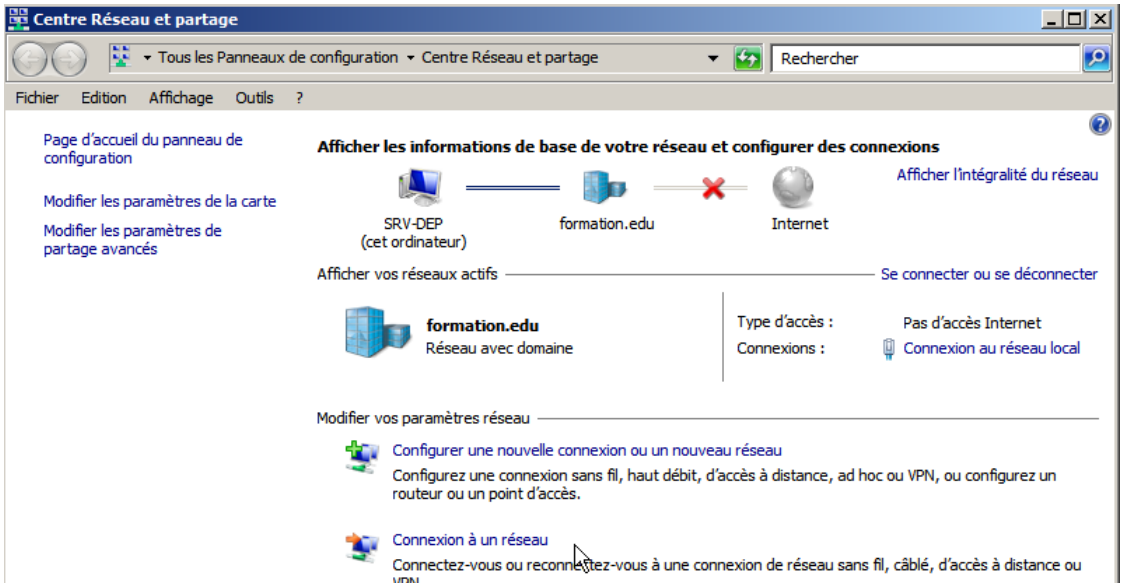
Il s'agit de lister les lecteur réseau utilisés (montés) à un moment donné, on peut passer la commande en invite :

net use

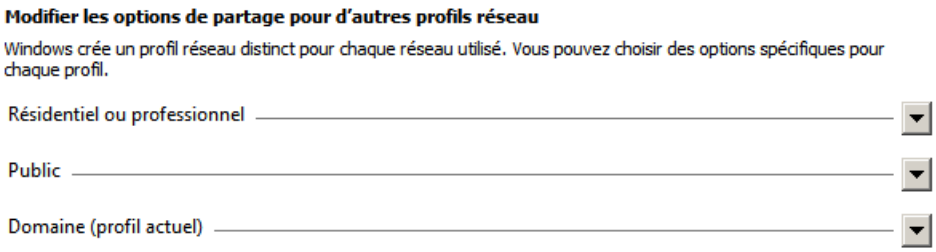
```
C:\Users\Administrateur>net use
Les nouvelles connexions seront mémorisées.

État         Local     Distant                   Réseau

-------------------------------------------------------------------------------
OK           R:        \\srv-2008\datap          Microsoft Windows Network
La commande s'est terminée correctement.
```

"TOPOLOGIE DE RESEAU" SEVEN

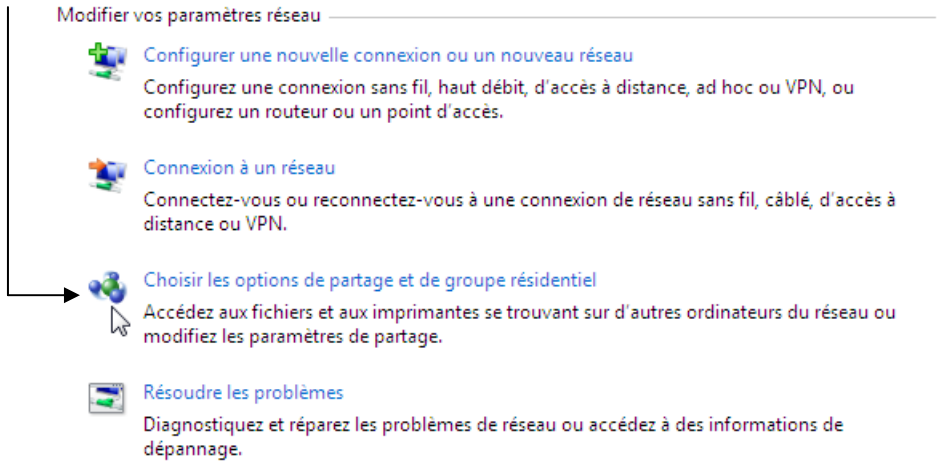
Centre Réseau et partage :



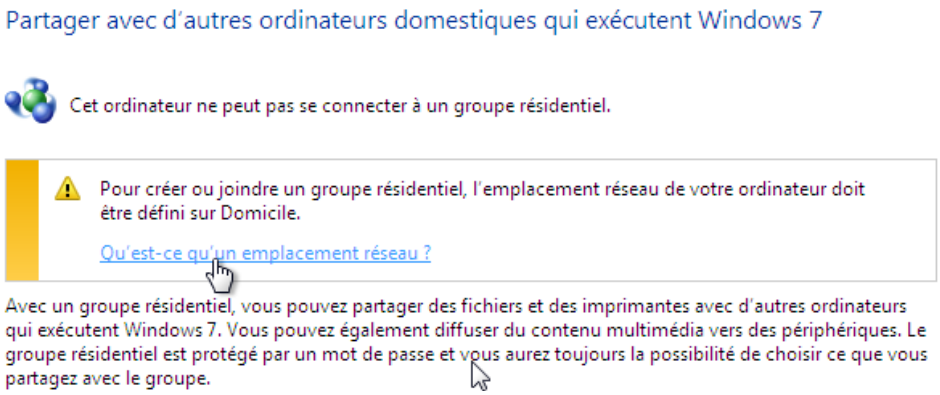
trois catégories de réseau sont possibles (2 si pas de domaine permettant chacune de définir les 3 réglages suivants



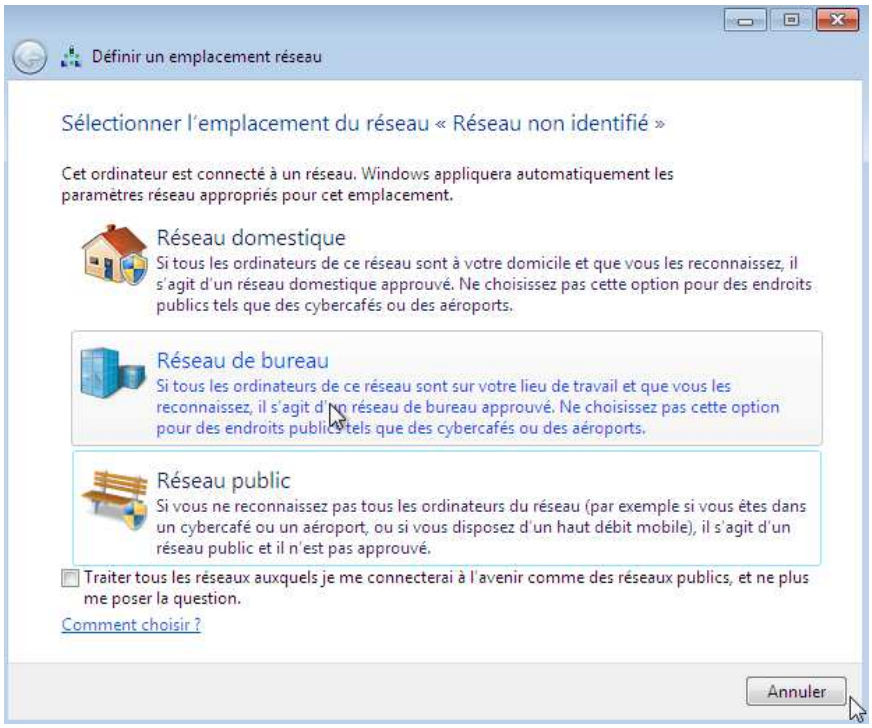
on y accède en demandant **choisir les options de partage et de groupe résidentiel**...



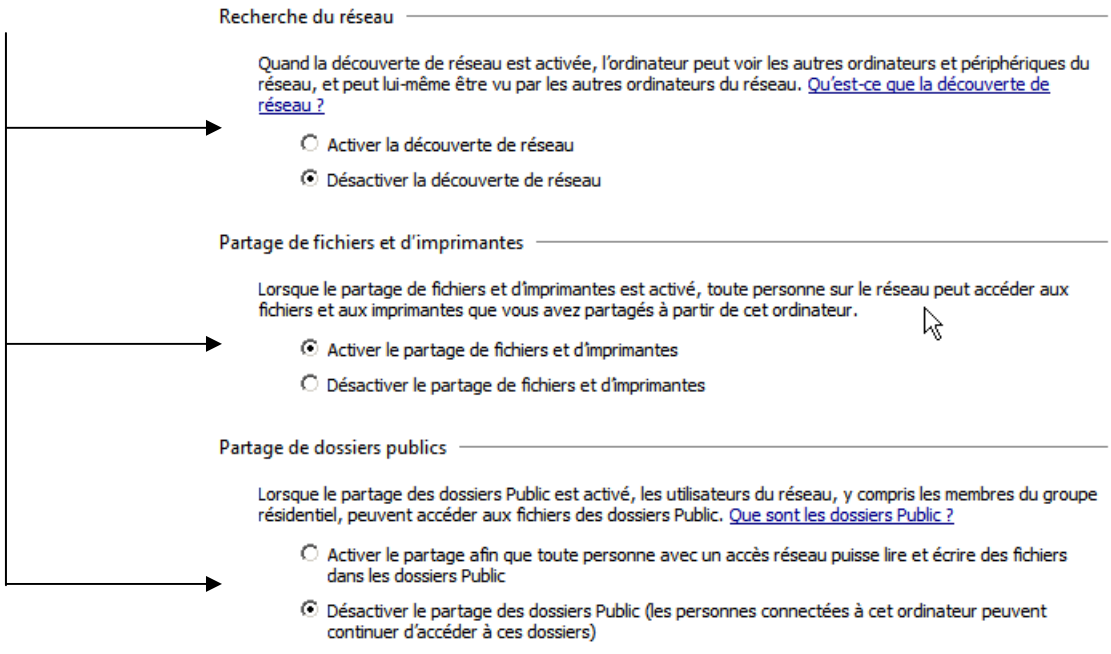
puis on demande



et on choisit son emplacement...



à chaque emplacement correspond un "jeu de réglage"



PARTAGES SIMPLIFIES XP

Les niveaux pré-définis sous XP :

Windows XP introduit une nouvelle interface utilisateur dans Windows XP Édition familiale et Windows XP Professionnel, connue sous le nom de **Partage de fichiers simple**

L'interface utilisateur Partage de fichiers simple est disponible dans les propriétés du dossier et configure à la fois les autorisations du système de **partage** et du système de fichiers **NTFS**

On peut désactiver cette fonctionnalité (voir chap suivant) mais par défaut elle est activée sur les postes XP…

Il existe 5 niveaux pré-définis

- **Niveau 1 :** Mes documents (confidentiel)
- **Niveau 2 :** Mes documents (par défaut)
- **Niveau 3 :** Fichiers dans les documents partagés disponibles pour les utilisateurs locaux
- **Niveau 4 :** Fichiers partagés sur le réseau (lisibles par tous)
- **Niveau 5 :** Fichiers partagés sur le réseau (lisibles et accessibles en écriture pour tous)

Correspondant à

Niveau d'accès	Tout le monde (NTFS/Fichier)	Propriétaire	Système	Administrateurs	Tout le monde (Partage)
Niveau 1	n/a	Contrôle total	Contrôle total	n/a	n/a
Niveau 2	n/a	Contrôle total	Contrôle total	Contrôle total	n/a
Niveau 3	Lecture	Contrôle total	Contrôle total	Contrôle total	n/a
Niveau 4	Lecture	Contrôle total	Contrôle total	Contrôle total	Lecture
Niveau 5	Modification	Contrôle total	Contrôle total	Contrôle total	Contrôle total

Les 5 niveaux pré-définis sous XP :

Niveau 1

la possibilité de rendre un dossier confidentiel (niveau 1) est uniquement disponible pour un compte d'utilisateur dans son dossier **Mes documents**

Pour configurer un dossier et tous les fichiers qu'il contient sur le niveau 1

1. Cliquez avec le bouton droit sur le dossier, puis cliquez sur **Partage et sécurité**.
2. Activez la case à cocher **Rendre ce dossier confidentiel**, puis cliquez sur **OK**.

Autorisations NTFS locales :

- Propriétaire : Contrôle total
- Système : Contrôle total

Autorisations de partage réseau :

- Non partagé

Niveau 2 (par défaut)

Il s'agit du paramètre par défaut pour tous les dossiers et les fichiers du dossier **Mes documents** de chaque utilisateur

Pour configurer un dossier et tous les fichiers qu'il contient sur le niveau 2

1. Cliquez avec le bouton droit sur le dossier, puis cliquez sur **Partage et sécurité**.
2. Assurez-vous que les cases à cocher **Rendre ce dossier confidentiel** et **Partager ce dossier sur le réseau** sont désactivées

Autorisations NTFS locales :

- Propriétaire : Contrôle total
- Administrateurs : Contrôle total
- Système : Contrôle total

Autorisations de partage réseau :

- Non partagé

Niveau 3

Les fichiers sont partagés entre les utilisateurs qui ouvrent une session sur l'ordinateur localement.

Les utilisateurs distants ne peuvent pas accéder aux dossiers ou fichiers du niveau 3. (Pour permettre à ceux-ci d'accéder aux fichiers, vous devez les partager sur le réseau avec le niveau 4 ou 5).

Pour configurer un fichier ou un dossier et tous les fichiers qu'il contient sur le niveau 3, démarrez l'Explorateur Windows, puis copiez ou déplacez le fichier ou le dossier vers le dossier Documents partagés sous le Poste de travail.

Autorisations NTFS locales :

- Propriétaire : Contrôle total
- Administrateurs : Contrôle total
- Utilisateurs avec pouvoir : Modification
- Utilisateurs avec accès restreint : Lecture
- Système : Contrôle total

Autorisations de partage réseau :

- Non partagé

Niveau 4 (partage sur le réseau en lecture seule)

Les fichiers sont partagés pour que chacun puisse les lire sur le réseau.

Pour configurer un dossier et tous les fichiers qu'il contient sur le niveau 4

1. Cliquez avec le bouton droit sur le dossier, puis cliquez sur **Partage et sécurité**.
2. Activez la case à cocher **Partager ce dossier sur le réseau**.
3. Désactivez la case à cocher **Autoriser les utilisateurs réseau à modifier mes fichiers**, puis cliquez sur **OK**.

Autorisations NTFS locales :

- Propriétaire : Contrôle total
- Administrateurs : Contrôle total
- Système : Contrôle total
- Tout le monde : Lecture

Autorisations de partage réseau :

- Tout le monde : Lecture

Niveau 5 (partage sur le réseau en lecture ecriture)

Tout utilisateur (local ou distant) peut lire, écrire, modifier ou supprimer un fichier dans un dossier partagé à ce niveau d'accès

Pour configurer un dossier et tous les fichiers qu'il contient sur le niveau 5

1. Cliquez avec le bouton droit sur le dossier, puis cliquez sur **Partage et sécurité**.
2. Activez la case à cocher **Partager ce dossier sur le réseau**, puis cliquez sur **OK**.

Autorisations NTFS locales :

- Propriétaire : Contrôle total
- Administrateurs : Contrôle total
- Système : Contrôle total
- Tout le monde : Modification

Autorisations de partage réseau :

- Tout le monde : Contrôle total

Conséquences des partages simplifiés – "force-guest":

Hors Domaine, lorsque le partage de fichiers simple est activé, tous les utilisateurs distants s'authentifient en tant qu'invité.

C'est ce que l'on appelle le "**force-guest**". Ceci étant dit, les comptes Invités ne disposant d'aucun privilège administratif les fonctionnalités suivantes ne marchent plus :

- l'administration à distance
- modification du Registre à distance
- connexions à des partages d'administration (tels que C$)
- les outils Dossiers partagés (Fsmgmt.msc) et Gestion de l'ordinateur (Compmgmt.msc) reflètent une interface utilisateur de sécurité et de partage plus simple

De plus :

- si vous configurez des entrées de contrôle d'accès utilisateur spécifiques, les utilisateurs distants ne sont pas affectés

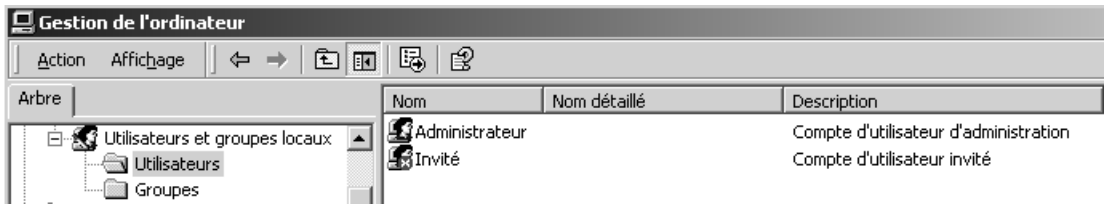
PARTAGES SIMPLIFIES "FORCE-GUEST"

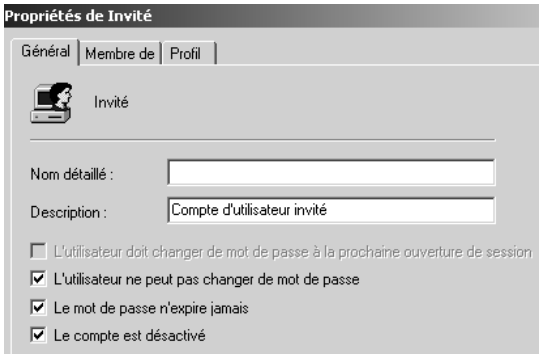
Environnement Accès réseau sous XP :

Les accès à travers le réseau (hors Domaine) dépends de :

Compte invité :

Ce compte utilisateur **Invité** est toujours présent, dans gestion des utilisateurs,
Par défaut: **désactivé**





Stratégie locale – droits utilisateurs – refuser accès réseau :

Il existe une **stratégie de sécurité locale** , dans **Attribution de droits des utilisateurs**, nommée **"refuser l'accès à cet ordinateur à partir du réseau**"

Par défaut: **invité** est **refusé**

Nb: ne pas confondre avec la stratégie "refus session locale…"

Assistant partage accès réseau sous XP :

par défaut, xp n'autorise l'accès réseau que pour les comptes invités, selon un principe connu sous le nom de **force-guest (**ceci pour éviter que les mots de passe ne circulent entre les machines....)

on voit en filigrane que on essaye d'accéder à la machine distante, à travers le compte invité....

Par ailleurs, l'assistant de partage qui se déclenche sous Xp peut modifier :

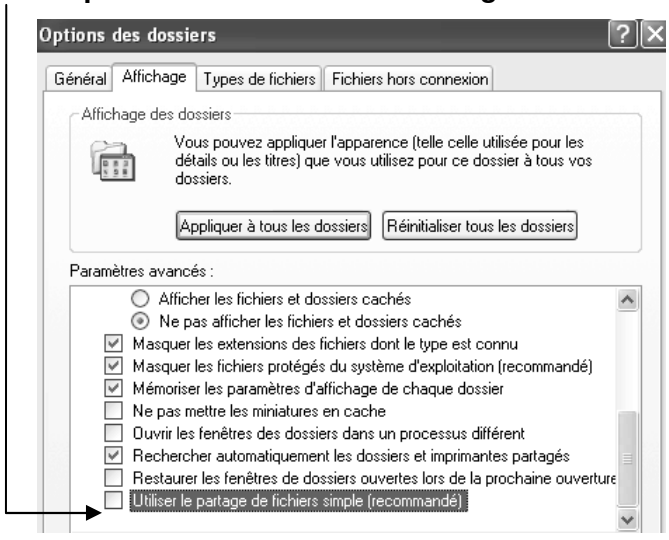
- Nom machine
- Workgroup
- Activation du compte invité
- Retrait du compte invité de la stratégie locale "refus l'accès réseaux"
- Stratégie réseau modèle; sélectionnée sur "invité seulement"
- Partage du dossier "documents partagés" sous le nom "sharedocs"
- Modification NTFS du dossier pour le groupe Tout le Monde

IL VAUT MIEUX NE PAS UTILISER CET ASSISTANT ET PARAMETRER MANUELLEMENT SON POSTE !

Désactivation partages simplifiés :

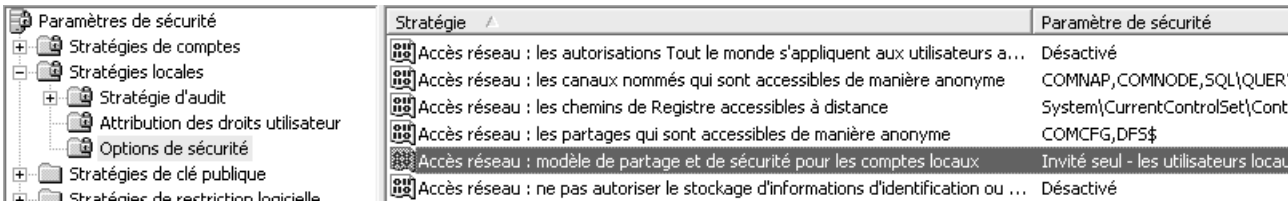
lorsque l'on désactive les partages simplifiés, dans le menu

outils / options des dossiers / affichage

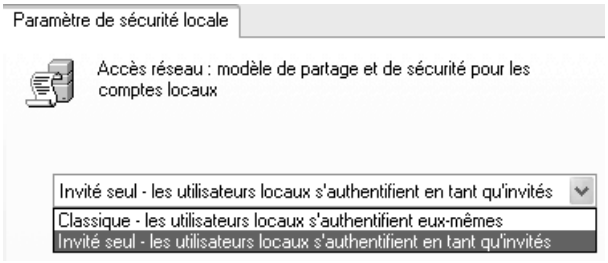


alors on va modifier la clé de stratégie locale suivante :

dans les **stratégies de sécurité locales**, / **options de sécurité**, on demande **accès réseau : modèle de partage et de sécurité pour les comptes locaux**,



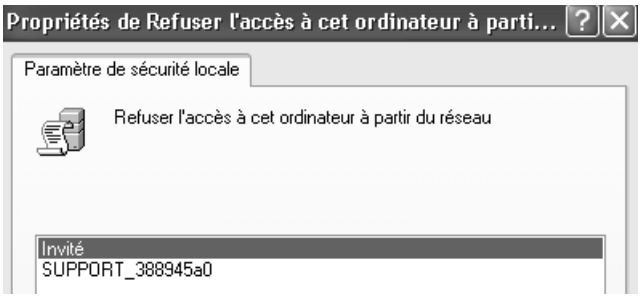
on choisit le type **classique** : authentification



Utiliser le compte invité :

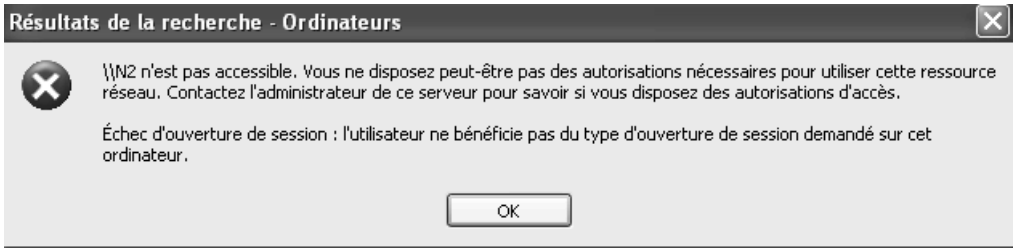
Si on veut utiliser le compte invité, alors il faut bien penser à

- activer le compte invité
  gérer du poste de travail, propriété du compte invité…
- sortir le compte invité de la stratégie "refus d'accès à travers le réseau"
  stratégies de sécurité locales, / **attributions des droits des utilisateurs**, on demande **refuser l'accès a cet ordinateur à partir du réseau**,



on supprime invité.

N.B: Si on ne fait que activer le compte invité, mais que l'on oublie de retirer le compte invité de la stratégie ""refuser l'accès ...", alors on obtient le message d'erreur suivant :



N.B : Si on accède à une machine via le compte invité, il faut aussi que les permissions NTFS soient positionnées (groupe **tout le monde**…)

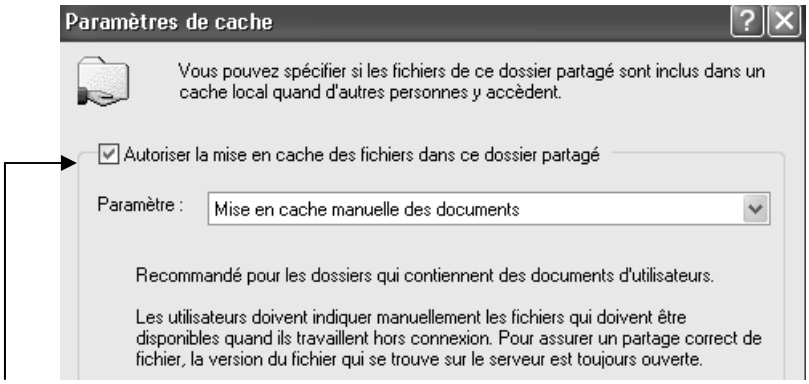
SYNCHRONISATION SOUS XP

Autorisation lors du Partage :

sous Windows XP, lorsque l'on partage un dossier, par défaut celui accepte les « futures » demandes de synchronisation hors connexion.

C'est le bouton **Mise en cache**

Qui gère de quelle manière on autorise ces futures demandes



Si on ne veut pas autoriser ces mises en caches, il suffit de dévalider la coche. Par défaut la mise en cache est possible si le client en fait la demande…

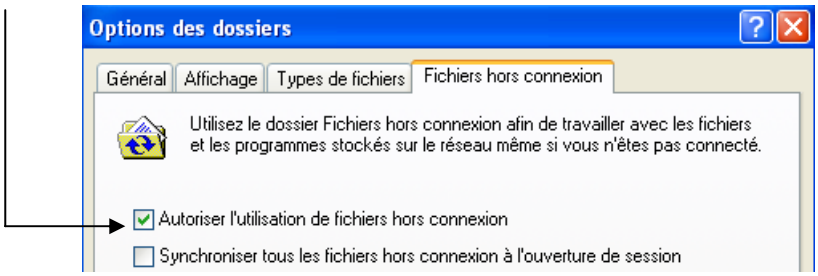
N.B : pour gérer ces fonctions l'affichage d'un dossier distant peut prendre jusqu'à 30 secondes, si on veut, on peut supprimer ces délais d'attente en supprimant la sous-clé suivante de
HKLM/Software/Microsoft/Windows/CurrentVersion/Explorer/RemoteComputer

Paramétrage du client :

sous Windows XP, le paramétrage par défaut autorise la mise en cache des documents. **IL VAUT MIEUX TRAVAILLER AU NIVEAU DOSSIER** (plutôt que fichier)

On peut s'en assurer via

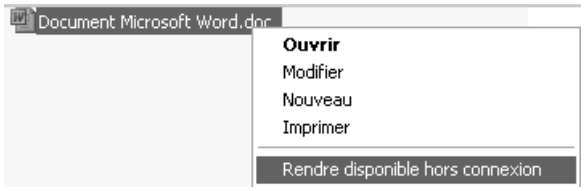
Outils / Options des dossiers onglet **Fichiers hors connexion**



Demande de mise en cache :

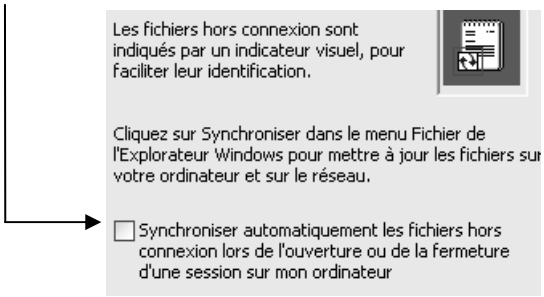
Lorsque l'utilisateur va mettre ou cherche un document dans le dossier partagé, il peut avec un clic contextuel demander de le

Rendre disponible hors connexion



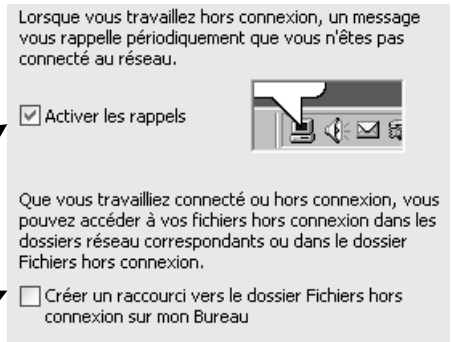
Un assistant se déclenche, Dans lequel on demande une synchro automatique

On peut forcer la synchronisation



On peut avoir un rappel visuel dans la barre des tâches

Et/ou demander un raccourci pour aller directement sur la ressource



Le dossier se voit marqué de manière particulière

Lors des prochaines **fermeture/ouverture de session** il y aura synchronisation, même s'il est possible de se synchroniser à tout moment.

Machine distante inaccessible - paramétrage:

Si un jour, on ouvre une session alors que le poste distant est inaccessible un message va apparaître, ainsi que un avertissement lors de la fermeture de session…

mais globalement je peux créer de nouvelles choses et utiliser les documents tels qu'ils étaient lors de mon dernier accès…

Lorsque le réseau sera rétabli, un synchronisation se refera automatiquement…

réglages via

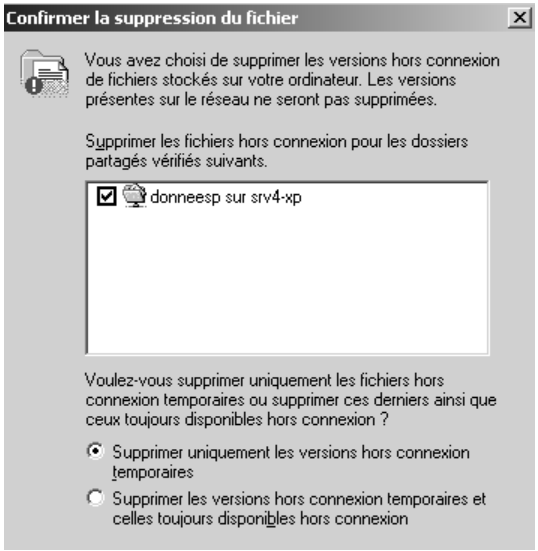
Outils / Options des dossiers onglet **Fichiers hors connexion**

Supprimer des fichiers hors connexion:

Si on souhaite arrêter cette fonctionnalité

Outils / Options des Dossiers onglet **Fichiers hors connexion**

Supprimer les fichiers…



N.B : les fichiers en cache synchronisés sont stockés en **%windir%CSC** et peuvent se gérer via un outils du Ressource Kit csccmd.exe (**Client-Side Caching Command-Line Options**)

WORKSGROUP & DOMAINES

Worksgroup Groupe de travail:

Cette notion est sensiblement la même depuis Windows Worksgroup 3.11 ou Windows 95-98. Un **groupe de travail** est un ensemble d'ordinateurs qui apparaît, pour des raisons pratiques, sous le même nom lorsque vous consultez les ressources réseau. Lorsque vous parcourez le réseau, les noms de tous les ordinateurs appartenant à votre groupe de travail s'affichent en premier dans le répertoire parcouru.

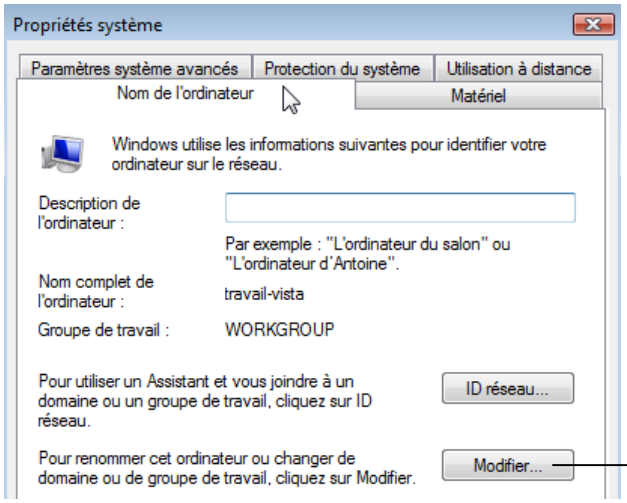
N'importe quel ordinateur peut devenir membre de n'importe quel groupe de travail unique.

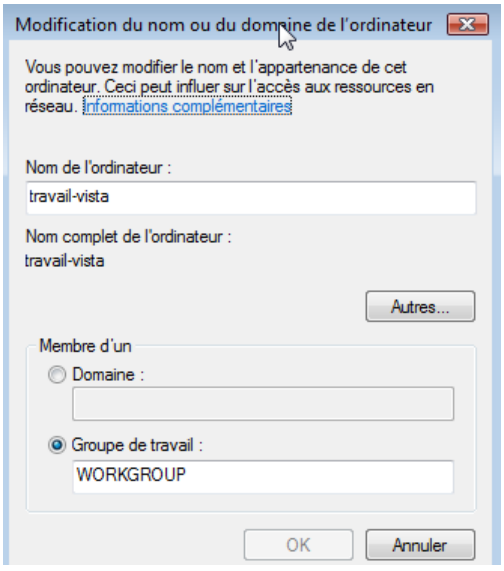
Appartenir à un Worksgroup avec SEVEN:

Sous SEVEN, la définition du groupe de travail se fait soit

- en demandant dans **le panneau de configuration** l'icône **système** puis on demande **Paramètres système avancés** / onglet **Nom de l'ordinateur**

- en faisant un clic droit sur l'icône **ordinateur** du bureau, et demander **propriété** puis l'onglet **Nom de l'ordinateur**





On peut changer le **Nom** du poste

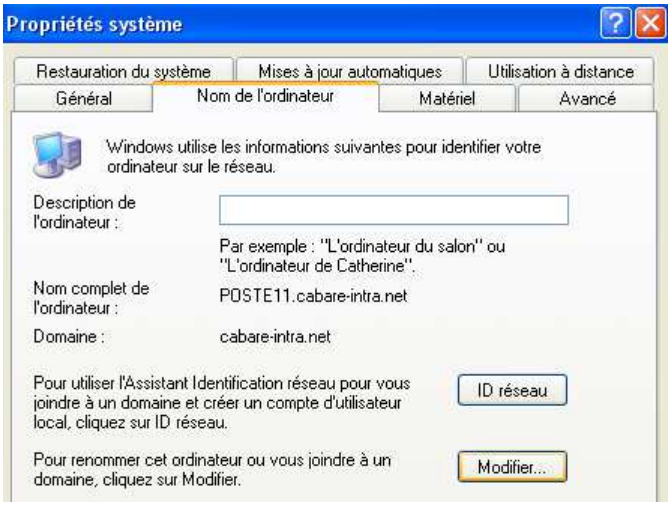
(il faut redémarrer impérativement)

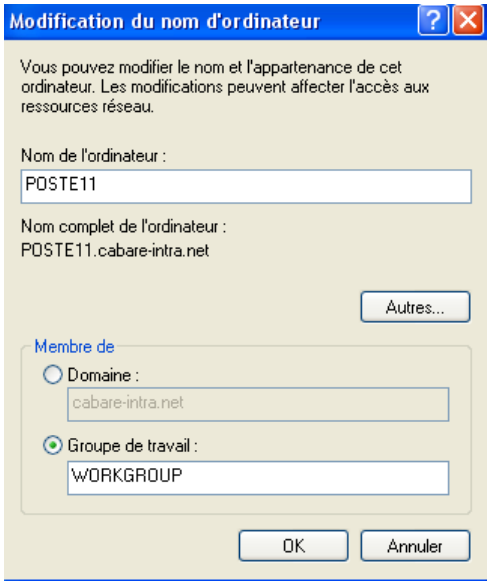
Et changer l'appartenance au un **Groupe de travail**.

Appartenir à un Worksgroup avec windows XP:

Sous Windows Xp, la définition du groupe de travail se fait soit

- en demandant dans le **panneau de configuration** l'icône **système** puis l'onglet **Nom de l'ordinateur**
- en faisant un clic droit sur l'icône **poste de travail** du bureau, et demander **propriété** puis l'onglet **Nom de l'ordinateur**





On peut changer le **Nom** du poste

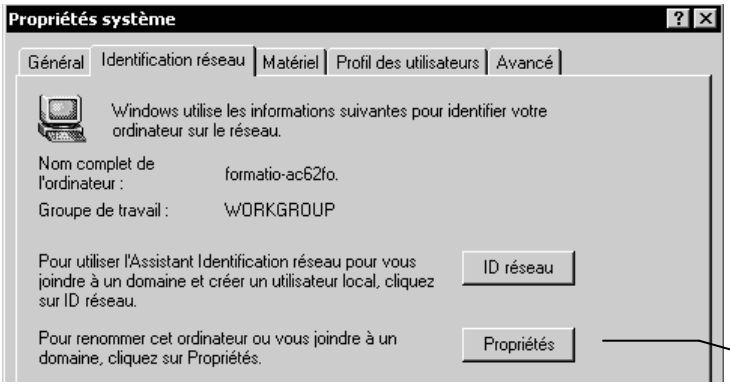
(il faut redémarrer impérativement)

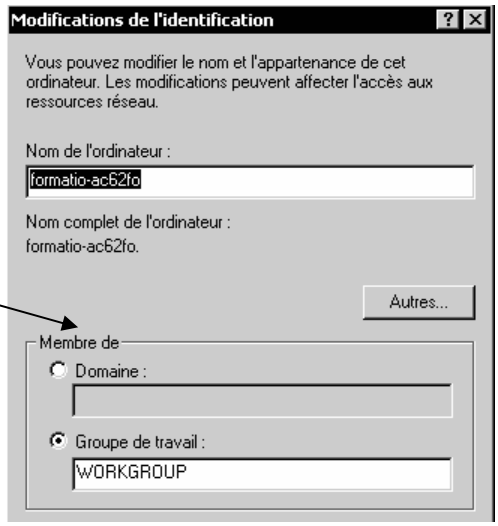
Et changer l'appartenance au **Groupe de travail**.

Appartenir à un Worksgroup avec windows NT 2000 :

Sous NT 2000 La définition du groupe de travail se fait soit

- en demandant dans le **panneau de configuration** l'icône **système** puis l'onglet **identification réseau**
- en faisant un clic droit sur l'icône **poste de travail** du bureau, et demander **propriété** puis l'onglet **identification réseau**





On peut changer le **Nom** du poste

(il faut redémarrer impérativement)

Et changer l'appartenance au **Groupe de travail**.

Domaine :

Cette notion n'existe pas sous Windows Worksgroup 3.11 ou Windows 95-98

Un **domaine** est un ensemble "logique" d'ordinateurs défini par l'administrateur d'un réseau Windows NT Server.

Un domaine permet en outre d'accéder aux comptes d'utilisateur et comptes de groupes centralisés gérés par l'administrateur de domaine

Ses paramètres ne sont plus sont stockés au sein de fichiers, tels que la base de donnée **SAM Security Account Manager** contenant l'ensemble des données des comptes utilisateur, mais hébergé dans une base de donnée stockée sur le serveur Contrôleur de Domaine et répliqués le cas échéant sur un ou plusieurs autres contrôleurs, dit « contrôleurs homologues ». Un domaine est donc l'unité de base de réplication et de sécurité d'un réseau Windows NT 2000. Un domaine partage une base de données d'annuaire centralisée nommée **Active Directory**

Contrairement à un groupe de travail, **un domaine doit déjà exister pour que vous puissiez en devenir membre**. Pour se joindre à un domaine au cours de l'installation, il est nécessaire d'avoir un **compte d'ordinateur** dans le domaine.

On peut imaginer que plusieurs domaines existent lors de la construction de grands réseaux, avec toute une gestion des relations entre eux, ce que l'on appelle les "approbations"

Pour des raisons de simplicité évidentes, nous nous limiterons à la gestion d'un seul domaine, définissant tous les comptes utilisateurs, tous les groupes et toutes les ressources

De même, un seul domaine ne veut pas forcément dire un seul contrôleur :

- Une organisation de petite taille qui utilise un réseau local unique peut nécessiter un seul domaine avec deux contrôleurs de domaine afin de garantir une disponibilité élevée et une tolérance de panne.
- Une organisation de grande taille avec plusieurs emplacements réseau nécessitera un ou plusieurs contrôleurs de domaine sur chaque emplacement afin de garantir une disponibilité élevée et une tolérance de panne.

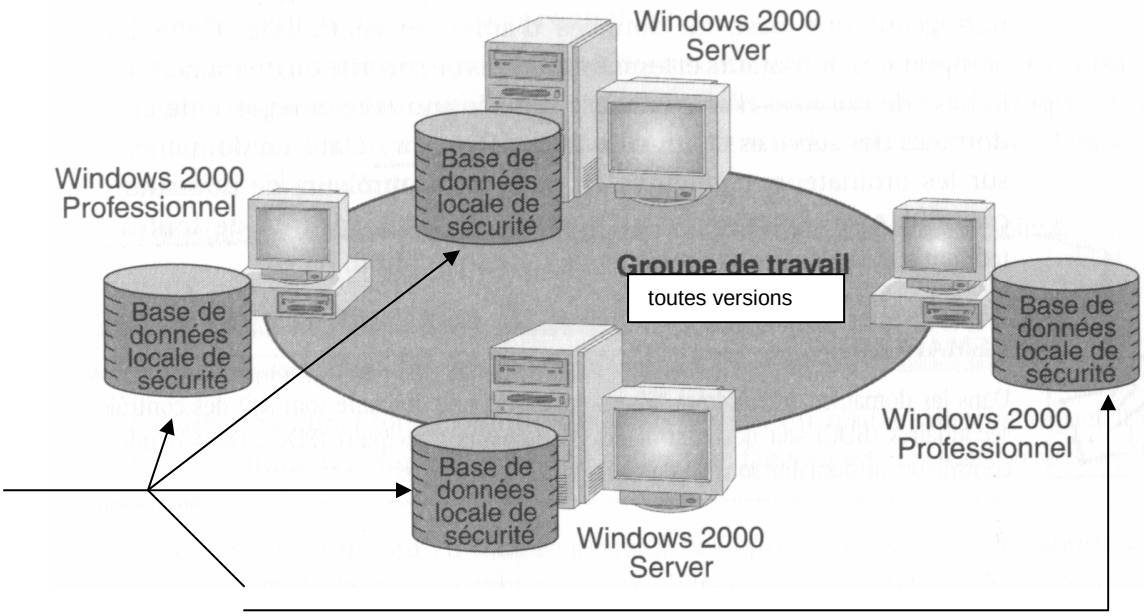
Mais ici encore, pour des raisons de simplicité, nous nous contenterons d'une situation avec un seul serveur dans notre domaine

Gestion de Domaine sous Windows 2008:

Dans un réseau sans domaine, c'est à dire constitué uniquement en Workgroups

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

la sécurité est gérée localement sur chaque poste du réseau

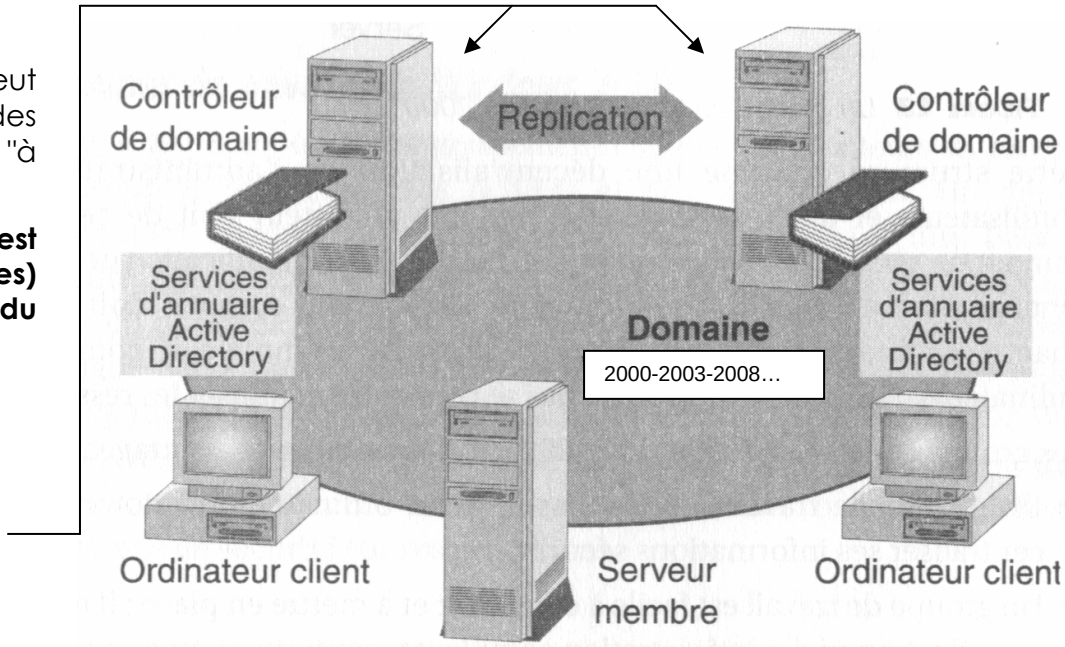


N.B: Dans le cas de machines Windows Server on parle alors de "**serveur autonome**"

Dans un réseau avec domaine, c'est à dire constitué avec un serveur 2000-2003-2008 faisant office de contrôleur de domaine

On ne peut trouver que des machines "à partir" de NT4.0

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



N.B: Dans un Domaine 2008 tous les "**contrôleurs de domaine**" de Active Directory sont **homologues**

Avec Windows 2008, un **serveur** peut avoir l'un des trois rôles suivants vis-à-vis du domaine :

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

Il est conseillé de planifier le rôle de chacun de vos serveurs dans les domaines Windows 2008 avant d'exécuter le programme d'installation. Mais toutefois, vous pouvez modifier ces rôles après l'installation.

Avec Windows SEVEN, un **client** peut avoir l'un des deux rôles suivants vis-à-vis du domaine :

- Poste appartenant à un domaine.
- Poste appartenant à un groupe de travail plutôt qu'à un domaine.

Différence avec NT 4.0 :

Les rôles des serveurs d'un domaine ne sont pas exprimés exactement de la même façon dans Windows 2000-2003 Server et dans Windows NT Server.

Avec Windows NT Server 4.0, les différents rôles possibles étaient les suivants :

- contrôleur principal de domaine (un seul par domaine),
- contrôleur secondaire de domaine
- serveur membre ou serveur autonome.

Windows 2008 propose un seul type de contrôleur de domaine (sans distinction de type « principal » ou « secondaire ») et inclut les rôles de serveur membre et de serveur autonome.

RÔLES SOUS WINDOWS NT 4.0	RÔLES SOUS 2008
Contrôleur principal de domaine	Contrôleur de domaine
Contrôleur secondaire de domaine	Contrôleur de domaine homologue
Serveur membre	Serveur membre
Serveur autonome	Serveur autonome

Les contrôleurs de domaine Windows 2008 introduisent des notions de rôles FSMO et de catalogue global, qui différencient en fait les serveurs homologues les uns des autres…

Sinon, la réplication d'annuaire Active Directory synchronise les données de l'annuaire sur chaque contrôleur de domaine, (Evolution du modèle de contrôleur principal de domaine et contrôleur secondaire de domaine utilisé dans Windows NT Server 4.0.)

ACTIVE DIRECTORY

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

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

On va définir un service d'annuaire tel que celui existant sous 2000-2003-2008 et portant le nom d'**Active Directory** par ses fonctions :

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

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

Ce qui fait que si AD est capable de trouver des ressources sur **tout système à la norme LDAP**, et si AD est interrogeable par tout **client LDAP**, on ne pourra **pas répliquer la structure AD de windows 2000-2003-2008 sur un autre système que Windows 2000-2003-2008**.

La structure Logique d'Active Directory dans un Domaine:

Domaine

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

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

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

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

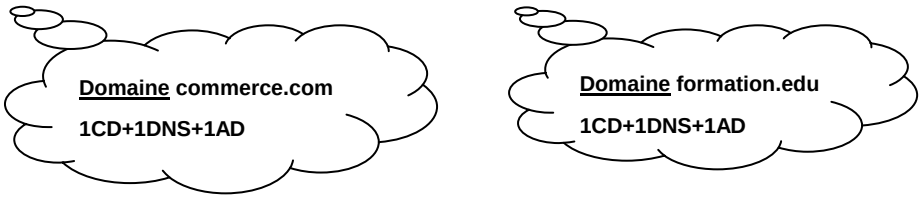
Annuaire & Espace de noms

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

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

Active Directory & DNS

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



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

Contrôleur de schéma

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

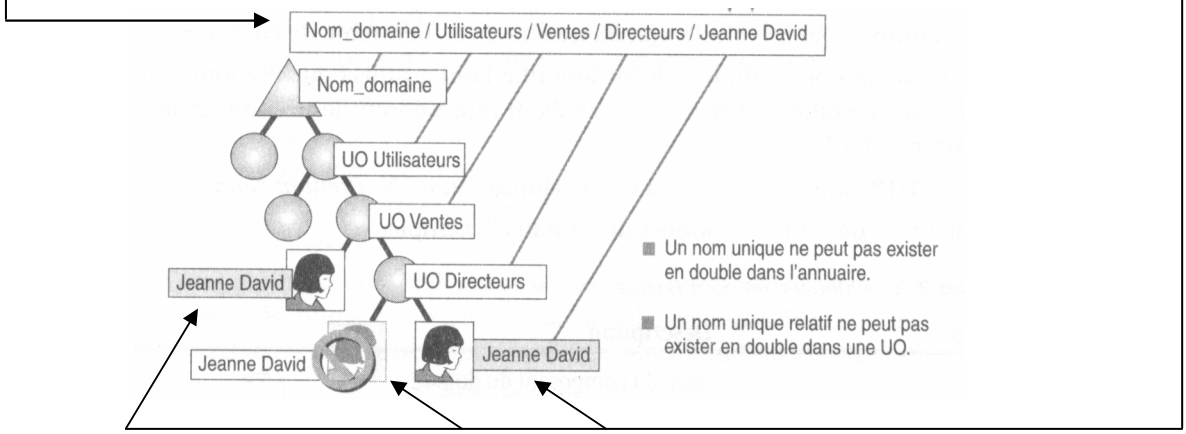
Nom

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

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

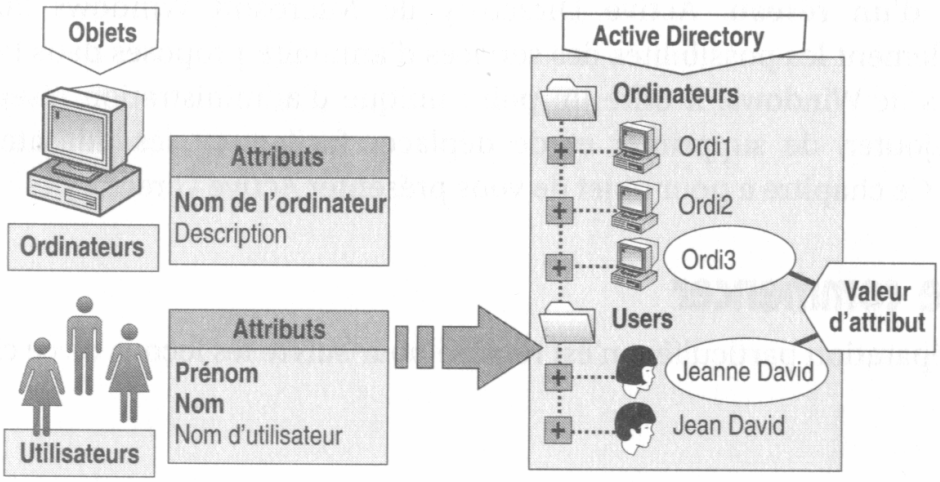
DC=Nom_Domaine//**OU**=Utilisateurs /**OU**=Ventes/**CN**=Jeanne David

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



Objet

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



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

Conteneur UO

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

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

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

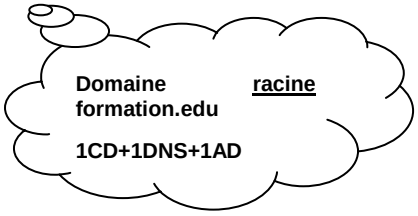
La Structure Logique au sein de plusieurs Domaines:

Arbres-arborescence de domaines

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

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

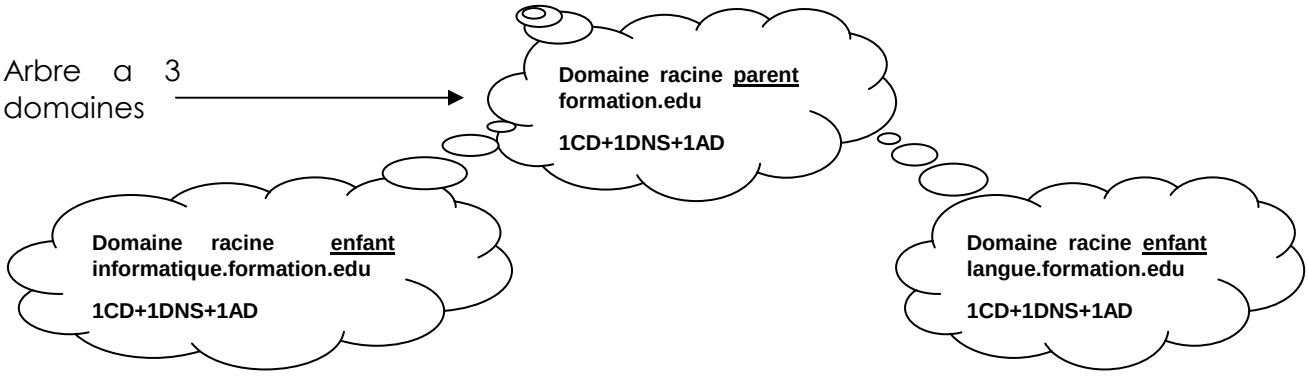
Arbre a 1 domaine



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

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

Arbre a 3 domaines

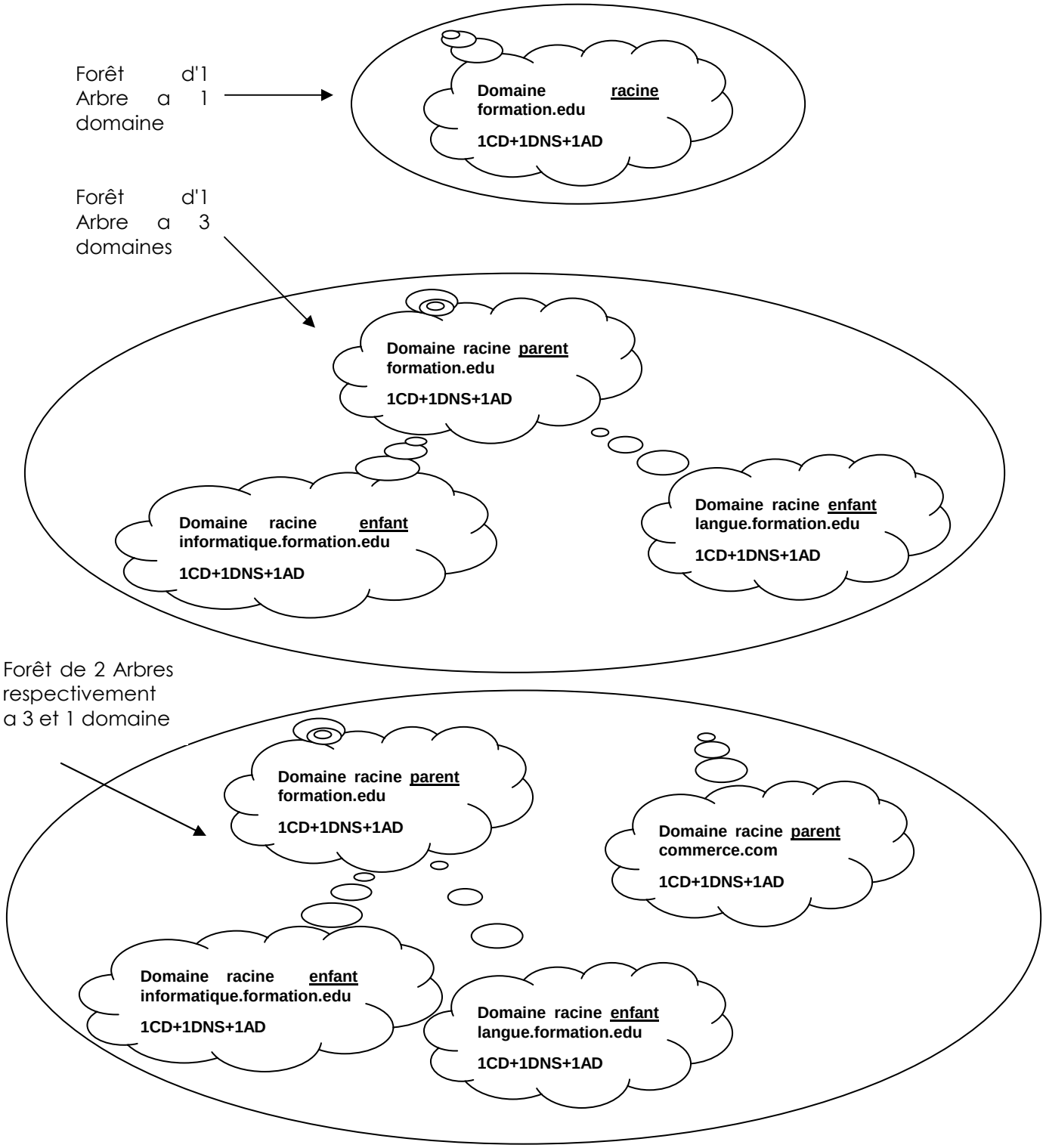


Une arborescence constitue un **espace de noms** hierarchisé et continu. Les serveurs DNS du (des) domaines enfants reprends le nom du serveur DNS de plus haut niveau (du parent)

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

Forêts

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



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

Les relations d'approbation sont bidirectionnelles et transitives Lorsque plusieurs arbres de domaines sont interconnectés pour former une forêt. les **arbres de domaine** de la forêt partagent un même **schéma**, et un même **catalogue global de AD**.

Catalogue Global

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

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

Relations d'approbation

Elles peuvent être **uni-directionelles**, c'est à dire que ce n'est pas parce que un domaine approuve un autre domaine, que la réciproque est vrai. (Si A approuve B, alors B n'approuve pas A)

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

Elles peuvent être **transitives** , c'est à dire que 2 chemins d'approbations permettent d'en définir un troisième (Si A approuve B, et B approuve C alors A approuve C…)

La structure Physique d'Active Directory:

Sites

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

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

Un site contient au minimum un contrôleur de Domaine.

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

N.B: il est conseillé de penser son réseau en Domaine, et de gérer ensuite les problèmes de géographie physique par la notion de site, que de faire autant de domaines que de sites géographiques.
Lorsque l'on fait plusieurs domaines, c'est plutôt que les modèles d'administration et de sécurité diffèrent entre les domaines…

ASSISTANT ACTIVE DIRECTORY & DCPROMO

DCPROMO et Services de Domaine Active Directory ADDS 2008:

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

Dans 2008 on distingue des **rôles** et des **fonctionnalités**

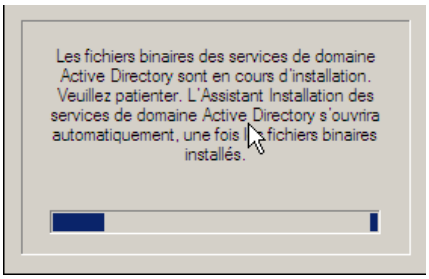
Les rôles dont on a besoin sont celui de **Service de Domaine Active Directory**, et celui de **Serveur DNS**…

Mais nous on veut créer le domaine… et pas seulement ajouter les rôles!

Si les services AD sont effectivement nécessaires sur un CD, ils ne permettent pas la création d'un domaine à proprement parler (ils sont par exemples nécessaires pour réaliser un CD en lecture seule...), création qui ne peut se faire que via une commande **dcpromo**...

"promotion" Windows 2008 R2:

la commande **dcpromo** (ou **dcpromo /adv** pour afficher toutes les options) exécute d'abords le désarchivage des fichiers nécessaires à l'installation



(si on veut désinstaller ces fichiers, il faudra désinstaller le rôle **AD DS** Service de domaine Active Directory manuellement...)

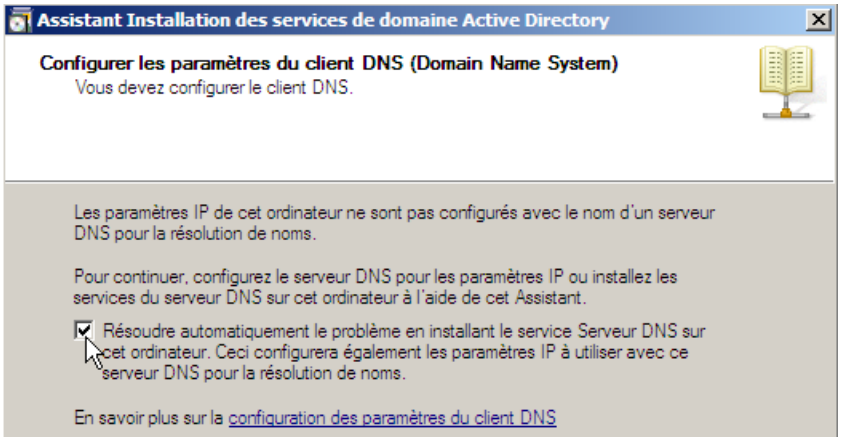
puis l'assistant se déclenche

soit on coche ici,

soit on demande **dcpromo /adv** pour vérifier ensuite le nom Netbios généré

La question du DNS se pose,

- si on n'a pas de serveur DNS renseigné au niveau de l'adresse IP, l'assistant demande tout de suite



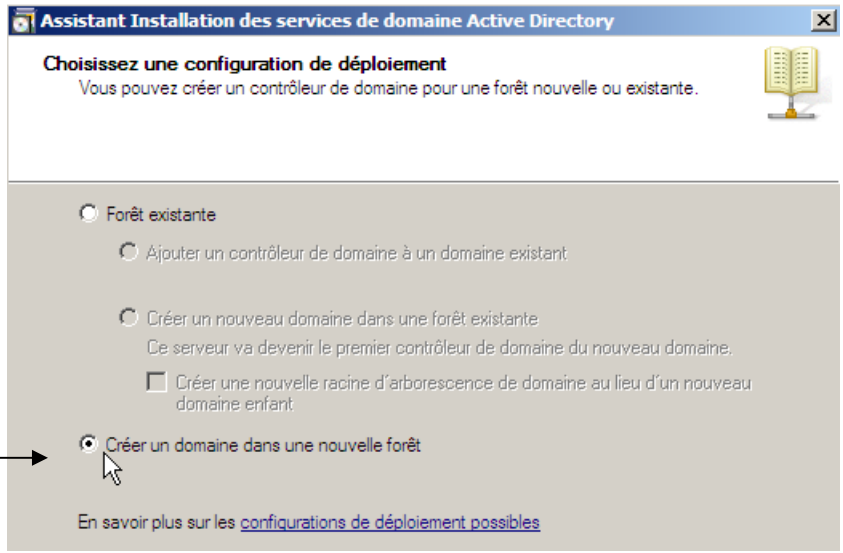
- si on à un e adresse IP de renseignée au niveau du DNS, on poursuit

une mise en garde s'affiche

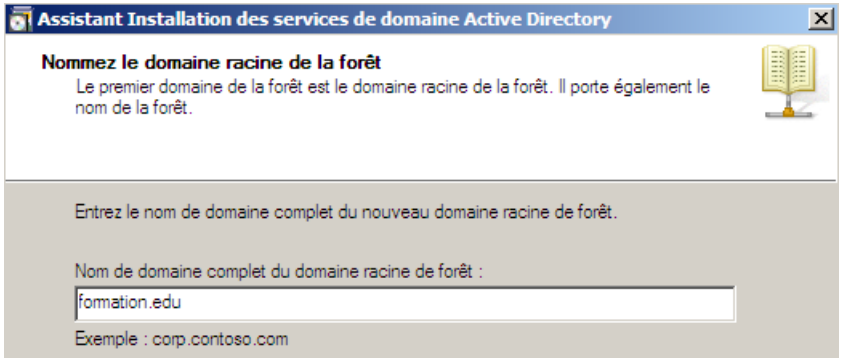
Si pas de migration automatique de prévue, et pas de NAS, on peut laisser tomber

On demande de créer une nouvelle forêt

On veut créer un nouveau « **Domaine dans une nouvelle forêt** »

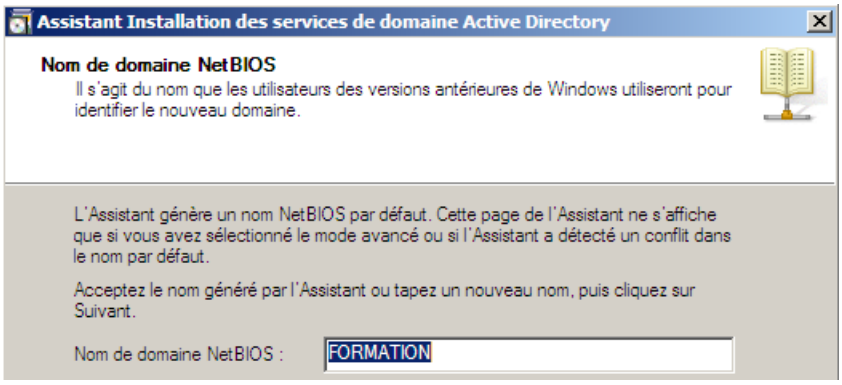


et on nomme le domaine



Un nom Netbios est proposé (15 premier caractères dans l'étendue des caractères autorisés par netbios). Il est déconseillé de donner un nom netbios différent de celui construit par défaut à partir du nom de Domaine.

N.B: Il serait bon que le nom netbios "ressemble" au nom DNS sans le domaine



Puis il faut choisir un niveau fonctionnel de Forêt et de Domaine…

3 niveaux de fait existent au niveau **forêt**

- 2000
- 2003-2008 (mêmes fonctionnalités mais permet de n'avoir que des domaines 2008… et plus de domaine 2003…)
- 2008R2 (corbeille…)

Niveau fonctionnel de forêt	Fonctionnalités activées	Systèmes d'exploitation de contrôleur de domaine pris en charge
Windows 2000	Toutes les fonctionnalités Active Directory par défaut	Windows 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2003	Toutes les fonctionnalités Active Directory par défaut, plus les fonctionnalités suivantes : • Approbation de forêt • Changement de nom de domaine • Réplication de valeurs liées (modifications d'appartenance de groupe pour stocker et répliquer des valeurs pour chaque membre au lieu de répliquer l'ensemble de l'appartenance comme une seule unité) Cela permet de moins utiliser le processeur et la bande passante réseau pendant la réplication et d'éliminer le risque de perdre des mises à jour lorsque des membres différents sont ajoutés ou supprimés simultanément de différents contrôleurs de domaine. • Possibilité de déployer un contrôleur de domaine en lecture seule	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2008	Toutes les fonctionnalités du niveau fonctionnel de forêt Windows Server 2003, mais pas de fonctionnalités supplémentaires. Toutefois, tous les domaines qui sont ultérieurement ajoutés à la forêt fonctionneront par défaut au niveau fonctionnel de domaine Windows Server 2008.	Windows Server 2008 Windows Server 2008 R2
Windows Server 2008 R2	Toutes les fonctionnalités du niveau fonctionnel de forêt Windows Server 2003, plus la fonctionnalité suivante : • Corbeille, qui permet de restaurer des objets supprimés en intégralité durant l'exécution des services AD DS.	Windows Server 2008 R2

N.B: le choix du niveau conditionne le type des autres serveurs…

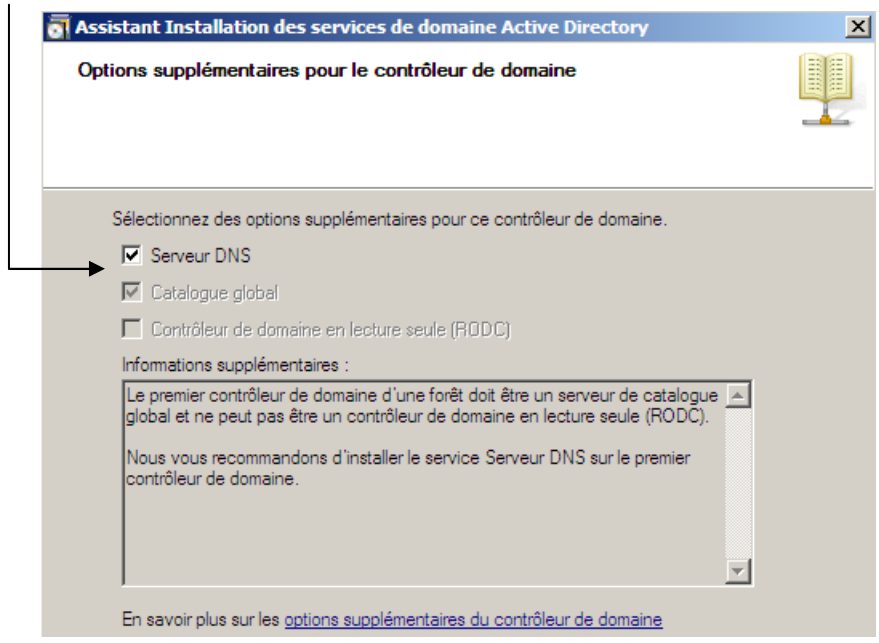
4 niveaux existent au niveau **domaine**

- 2000 natif
- 2003
- 2008
- 2008R2

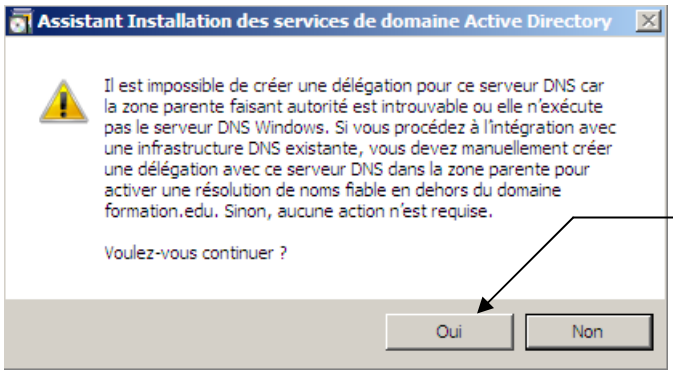
Niveau fonctionnel de domaine	Fonctionnalités activées	Systèmes d'exploitation de contrôleur de domaine pris en charge
Windows 2000 natif	Toutes les fonctionnalités Active Directory par défaut, plus les fonctionnalités suivantes : • groupes universels pour les groupes de distribution et les groupes de sécurité ; • imbrication de groupes ;	Windows 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2003	Toutes les fonctionnalités Active Directory par défaut, toutes les fonctionnalités du niveau fonctionnel de domaine Windows 2000 natif, plus les fonctionnalités suivantes : • Disponibilité de l'outil de gestion de domaines, Netdom.exe, pour préparer le changement de nom des contrôleurs de domaine.	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2008	Toutes les fonctionnalités Active Directory par défaut, toutes les fonctionnalités des niveaux fonctionnels de domaine Windows 2000 natif et Windows Server 2003, plus les fonctionnalités suivantes : • Prise en charge de la réplication du système de fichiers DFS (Distributed File System) pour SYSVOL, ce qui offre une réplication plus fiable et plus granulaire du contenu de SYSVOL. Il peut être nécessaire d'effectuer des opérations supplémentaires pour utiliser la réplication DFS pour SYSVOL. Pour plus d'informations, voir l'article consacré aux services de fichiers (http://go.microsoft.com/fwlink/?LinkId=93167) (éventuellement en anglais). • Prise en charge d'AES (Advanced Encryption Services) 128 et 256 pour le protocole Kerberos.	Windows Server 2008 Windows Server 2008 R2
Windows Server 2008 R2	Toutes les fonctionnalités Active Directory par défaut, toutes les fonctionnalités des niveaux fonctionnels de domaine Windows 2000 natif, Windows Server 2003 et Windows Server 2008, plus la fonctionnalité suivante : • assurance de mécanisme d'authentification, qui empaquète les informations relatives au type de méthode d'ouverture de session (carte à puce ou nom d'utilisateur/mot de passe)	Windows Server 2008 R2

N.B: le choix du niveau conditionne le type des autres serveurs…

La Question du DNS refait surface. Si on avait renseigné un adresse IP comme serveur DNS, alors la case à cocher Serveur DNS est optionnelle… (si on n'a pas d'adresse IP de renseignée comme DNS, on doit installer un DNS)



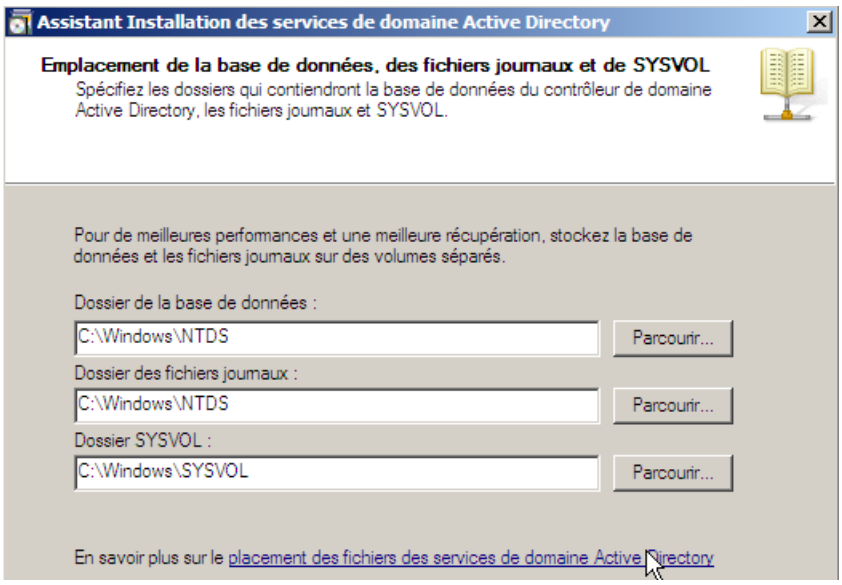
Une mise en garde apparaît



on réponds Oui

ensuite on demande l'emplacement des fichiers système

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



On peut garder les valeurs par défaut

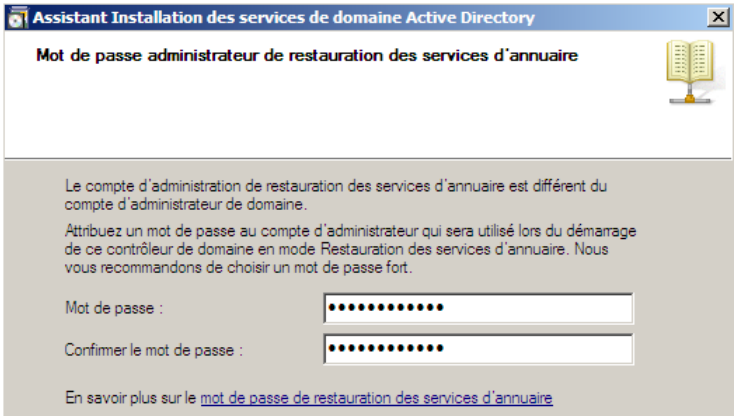
Si on veut affiner, il faut savoir que 5 "composants" existent

- Le volume système
- Le volume de démarrage
- Le volume qui héberge SYSVOL
- Le volume qui héberge la base de données Active Directory (Ntds.dit)
- Le volume qui héberge les fichiers journaux de la base de données Active Directory

et si plusieurs volumes (partitions) son disponibles : mettre sur le 1° disque les 3 premiers volumes (système-démarrage-sysvol), et sur le 2° disque les 2 derniers volumes (base AD et les fichiers journaux AD)

N.B: Si on veut prévoir une sauvegarde stockée localement, il faut un volume distinct pour son stockage

On peut prévoir ensuite un mot de passe ici différent de celui d'administration courant. En Effet lors d'une restauration des services d'annuaire, 2008 démarre sans charger Active Directory, et donc le mot de passe doit être stocké « en dehors » de AD.



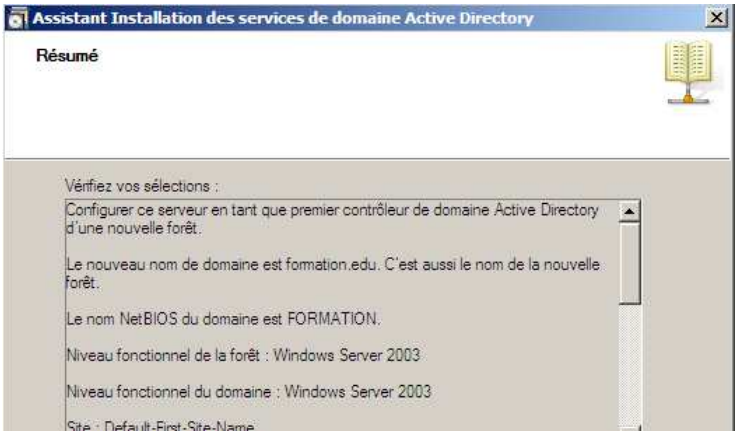
N.B : sous 2008 il existe un utilitaire **NTDSUTIL.exe** permettant de modifier ce mot de passe par une commande genre **Set DSRM Password**

puis **reset password on server null**

(ou **reset password on server nomhotedistant)**

```
ntdsutil: Set DSRM Password
Redéfinir le mot de passe administrateur DSRM : reset password on server null
Entrez le mot de passe du compte Administrateur du mode de restauration du
service d'annuaire : **********
Confirmez le nouveau mot de passe : **********
```

Après l'affichage d'un bref résumé



Un redémarrage du serveur sera nécessaire.

Options disponible avec dcpromo /adv

Configuration de déploiement	Pages d'installation en mode avancé de l'Assistant
Nouvelle forêt	**Nom de domaine NetBIOS**
Nouveau domaine dans une forêt existante.	Dans la page **Choisissez une configuration de déploiement**, l'option de création d'une nouvelle arborescence de domaine n'apparaît que pour une installation en mode avancé. **Nom de domaine NetBIOS** **Contrôleur de domaine source**
Contrôleur de domaine supplémentaire dans un domaine existant.	**Installation à partir du support** **Contrôleur de domaine source** **Spécifiez la stratégie de réplication de mot de passe** (pour l'installation d'un contrôleur de domaine en lecture seule uniquement)
Crée un compte pour l'installation d'un contrôleur de domaine en lecture seule.	**Spécifiez la stratégie de réplication de mot de passe**
Joint un serveur à un compte pour l'installation d'un contrôleur de domaine en lecture seule.	**Installation à partir du support** **Contrôleur de domaine source**

"Rétrogradation" Windows 2008 - 2008R2:

Si on souhaite enlever Active Directory d'un Contrôleur de domaine (voire supprimer un Domaine)

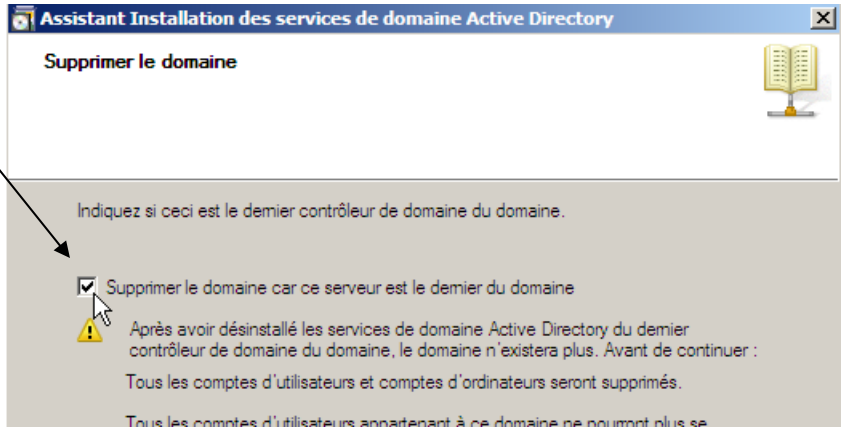
Démarrer/Exécuter et tapez ensuite **dcpromo**.

Une sérieuse mise en garde apparaît ainsi que un message indiquant la perte du catalogue global…

On demande de confirmer la suppression du Domaine

Et on demande de « confirmer » que

Ce serveur est le dernier contrôleur de domaine



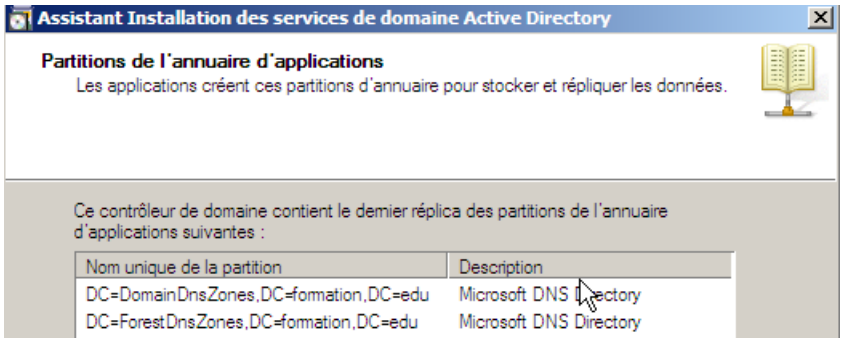
On demande de confirmer la suppression des partitions d'annuaire.

N.B: Une partition d'annuaire d'applications est une partition d'annuaire qui n'est répliquée que sur des contrôleurs de domaine spécifiques. Les partitions d'annuaire d'applications sont généralement créées par les applications qui les utilisent pour stocker et répliquer des données

Par exemple, deux partitions d'annuaire d'applications DNS sont créées par défaut sur les contrôleurs de domaine 2003 ou 2008 si ceux-ci hébergent également des zones DNS intégrées à Active Directory:

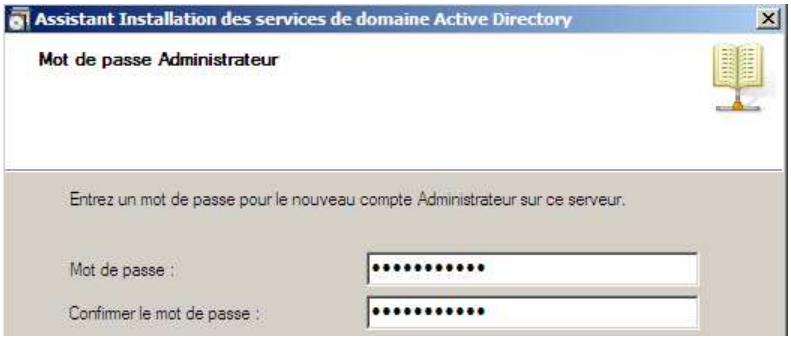
- **DomainDNSZones** : comprend des données DNS qui sont répliquées sur tous les contrôleurs de domaine du domaine
- **ForestDNSZones** : comprend des données DNS qui sont répliquées sur tous les contrôleurs de domaine de la forêt.

si d'autres partitions d'annuaires apparaissent, il faut s'assurer des conséquences de leur perte



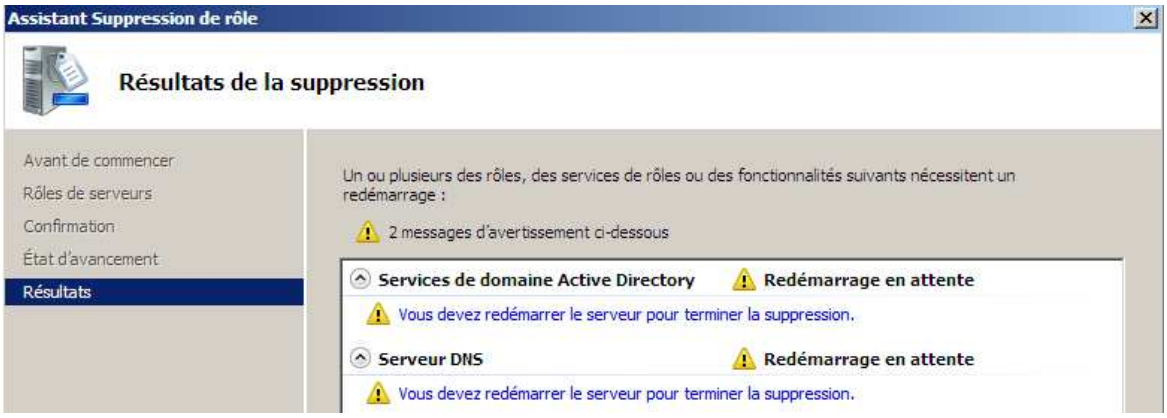
il faut confirmer

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



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

N.B: Pour retrouver réellement un serveur "avant" dcpromo, il faut désinstaller manuellement les **rôles DNS** et **ADDS** via le **gestionnaire de serveur**, **rôles**…ainsi que la fonctionnalité **Gestion des stratégies de groupes**…



ainsi que la fonctionnalité **Gestion des stratégies de groupes**…

DCpromo serveur 2003:

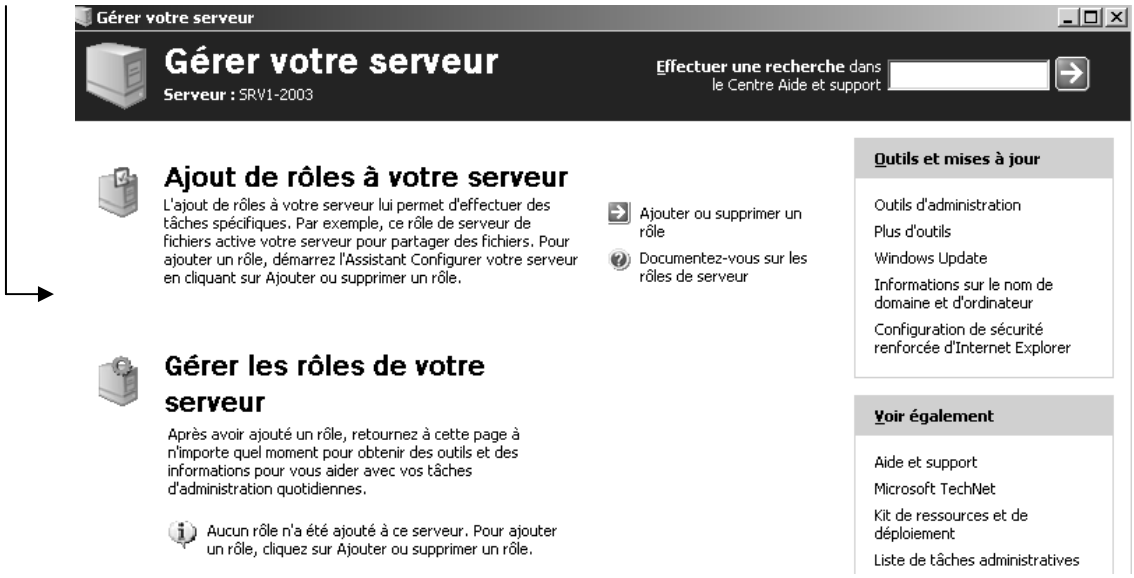
Pour créer un domaine, vous devez **promouvoir** un ou plusieurs ordinateurs exécutant **Windows Server** afin qu'ils deviennent un ou des contrôleurs de domaine.

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

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

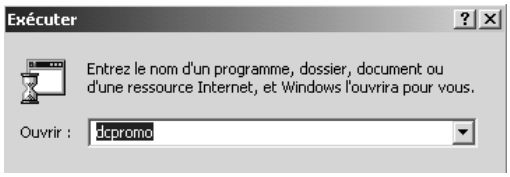
Démarrer/Programmes/Outils d'administration/Gérer serveur.

Cliquez sur **Ajouter ou Supprimer un rôle**



Ou mieux

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



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

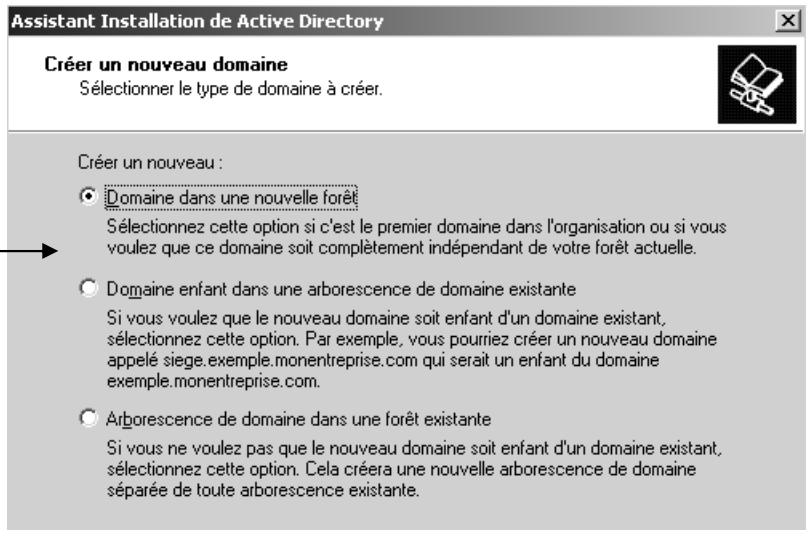
N.B: Une connexion réseau active doit exister !

"Promotion" windows 2003 :

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

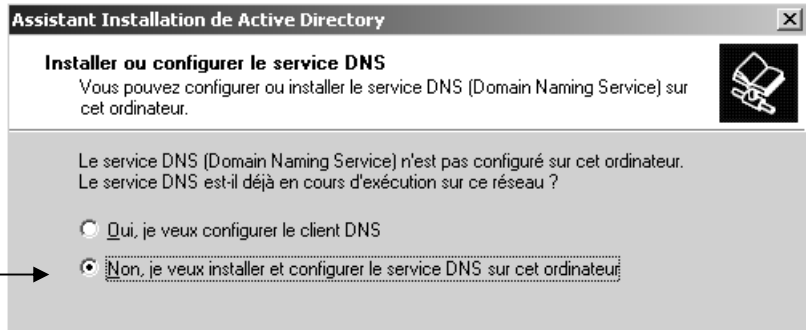
N.B : Serveur 2003 et clients 95, NT4 WKS. Les ordinateurs clients exécutant Windows pour Workgroups, Windows 95 sans le client Active Directory et Windows NT 4.0 Service Pack 2 (ou antérieur) ne prennent pas en charge la signature SMB et, par conséquent, ils ne peuvent pas se connecter aux contrôleurs de domaine Windows Server 2003

On veut créer un nouveau « **Domaine dans une nouvelle forêt** »



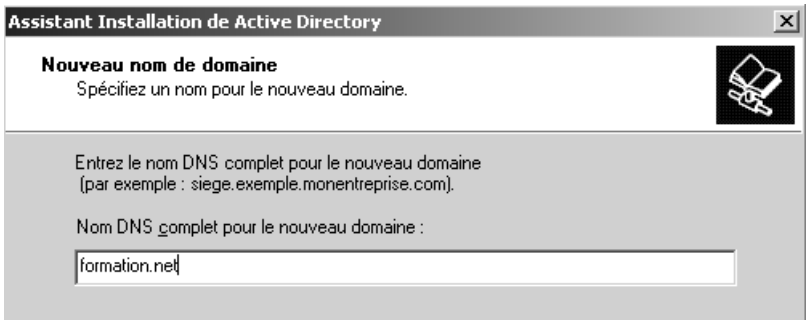
A la suite de quoi, 2003 demande comment on souhaite procéder pour le serveur DNS

On indique que l'on veut installer un serveur DNS « **Non, je veux installer et configurer le service DNS sur cet ordinateur** »



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

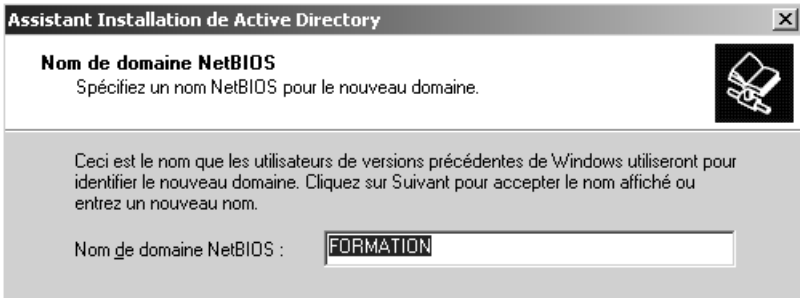
Par exemple **formation.net**



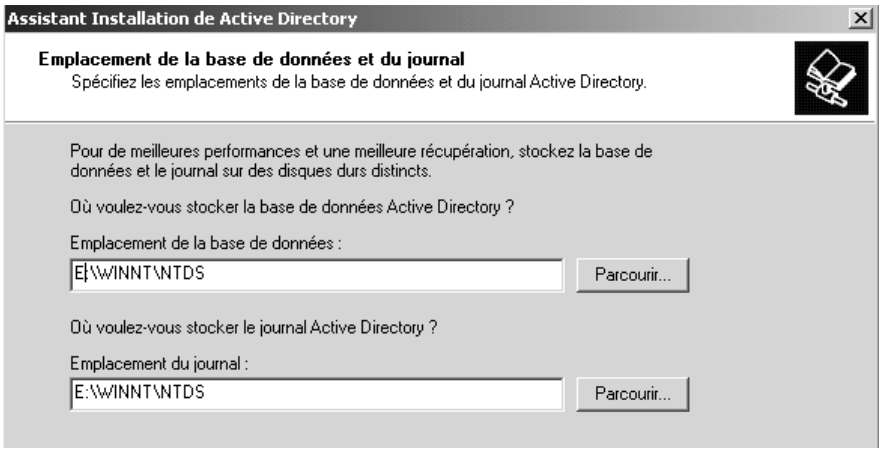
A partir duquel le nom Netbios est proposé (15 premier caractères dans l'étendue des caractères autorisés par netbios)

Il est très déconseillé de donner un nom netbios différent de celui construit par défaut à partir du nom de Domaine.

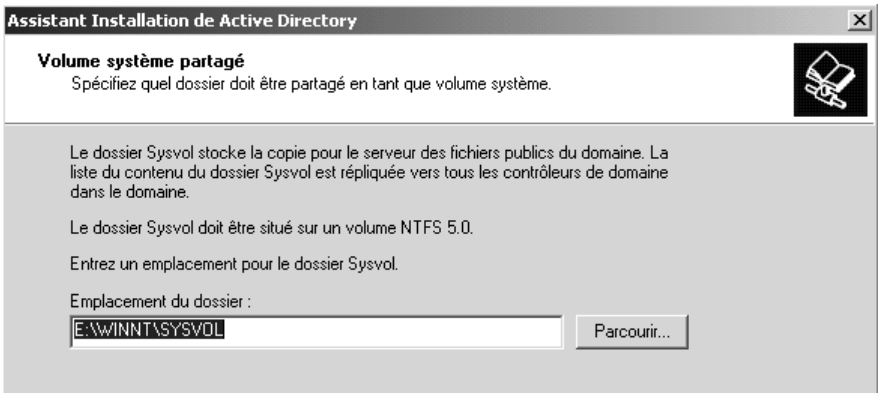
On accepte **formation**



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

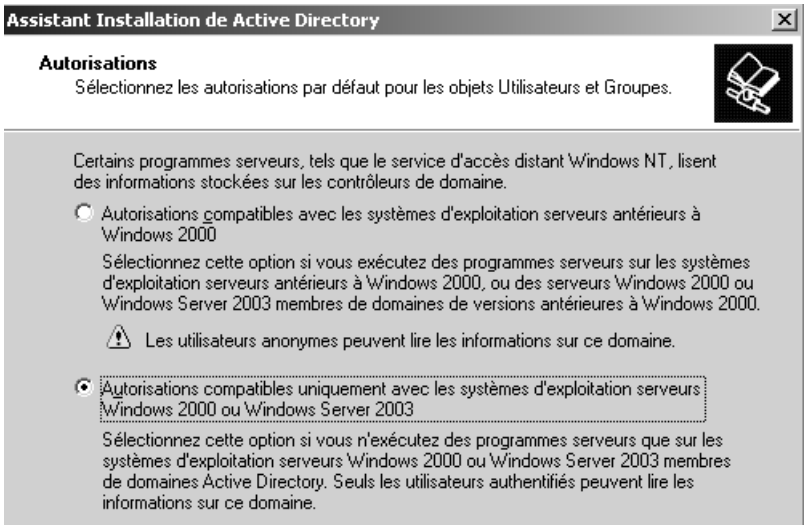


fichiers miroirs de l'Active Directory destinés à la lecture et réplication (on doit les mettre sur un volume NTFS)

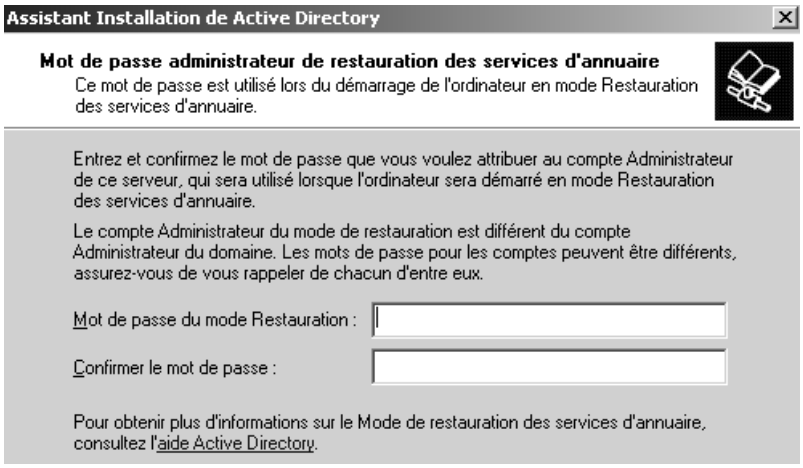


A la suite de quoi on choisit

Une raison pour garder des autorisations compatibles antérieur à 2000 c'est une mise à niveau d'un serveur NT4 vers 2003 avec des services RAS (ou des serveur NT4, évidemment…)



On peut prévoir ensuite un mot de passe ici différent de celui d'administration courant. En Effet lors d'une restauration des services d'annuaire, 2003 démarre sans charger Active Directory, et donc le mot de passe doit être stocké « en dehors » de AD.



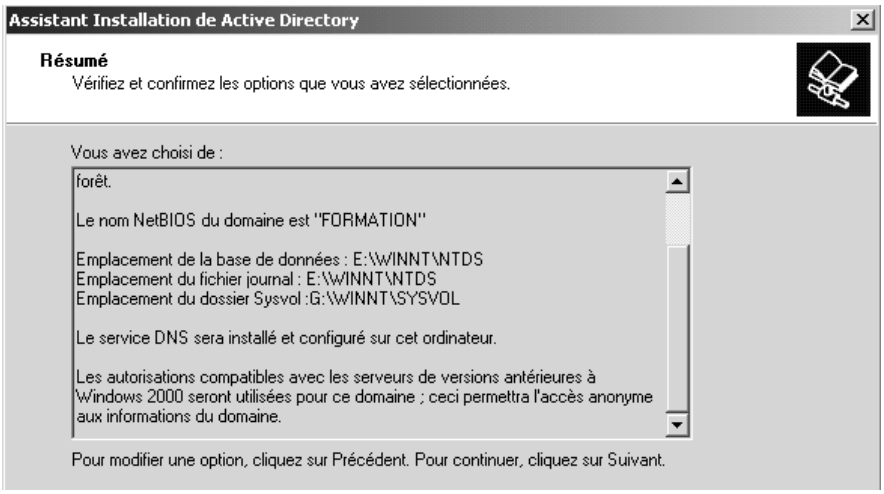
N.B : sous 2003 il existe un utilitaire **NTDSUTIL.exe** permettant de modifier ce mot de passe par une commande genre **Set DSRM Password**

puis **reset password on server null**

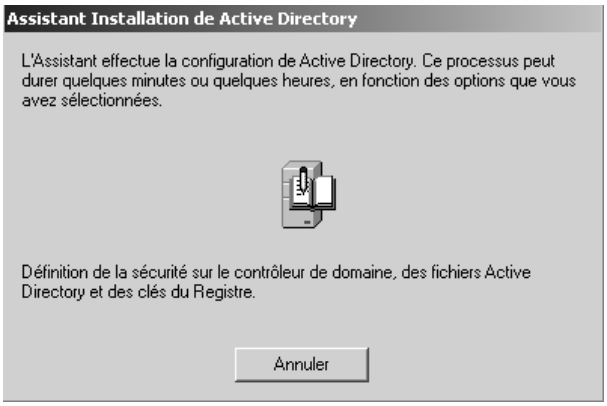
(ou **reset password on server nomhotedistant)**

```
ntdsutil: Set DSRM Password
Redéfinir le mot de passe administrateur DSRM : reset password on server null
Entrez le mot de passe du compte Administrateur du mode de restauration du
service d'annuaire : **********
Confirmez le nouveau mot de passe : **********
```

Après l'affichage d'un bref résumé



La transformation en **Contrôleur de Domaine** commence



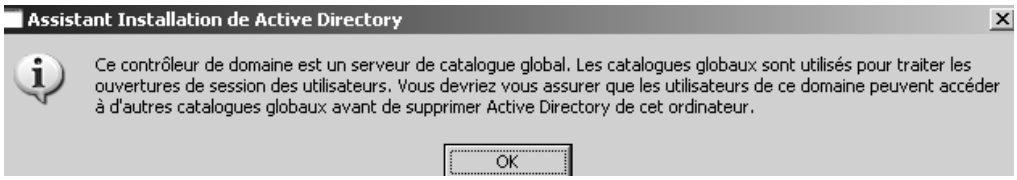
L'accès au CD source sera nécessaire, ainsi qu'un redémarrage du serveur

"Rétrogradation" Windows 2003 :

Si on souhaite enlever Active Directory d'un Contrôleur domaine(voire supprimer un Domaine)

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

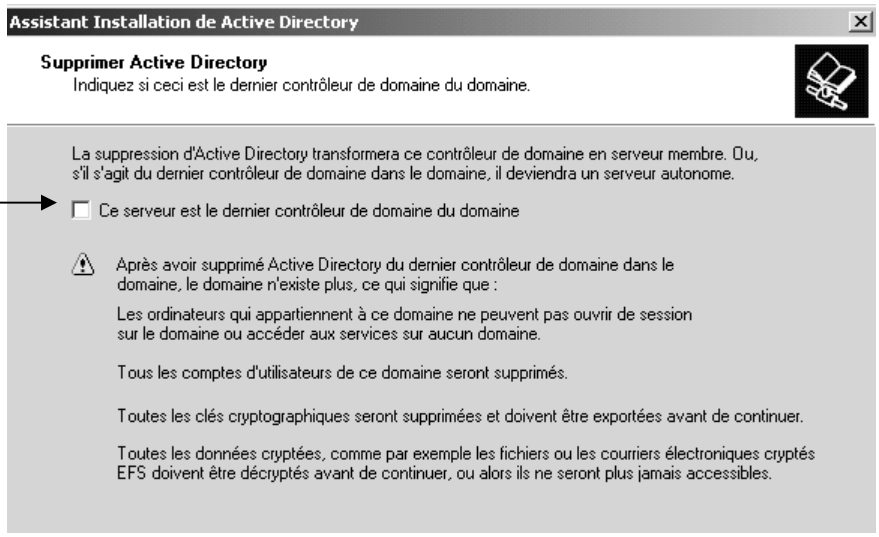
Une sérieuse mise en garde apparaît ainsi que un message indiquant la perte du catalogue global…



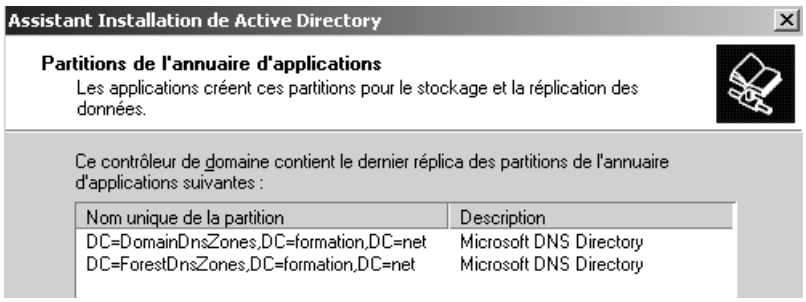
On demande de confirmer la suppression du Domaine

Et on demande de « confirmer » que

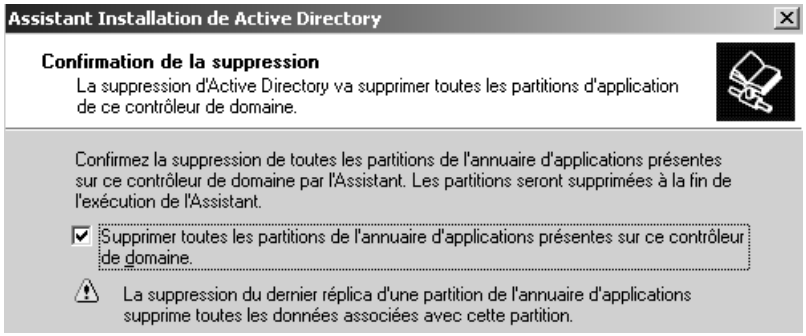
Ce serveur est le dernier contrôleur de domaine



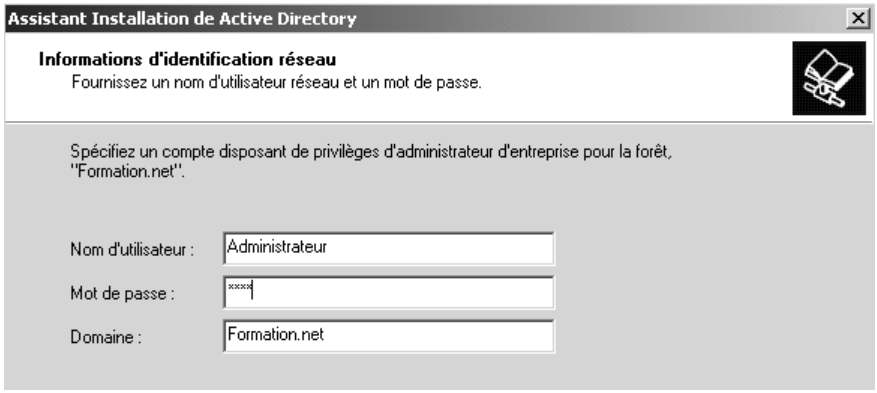
Dans ce cas les derniers réplicas vont être supprimés (2003)



On confirme (2003)



Il faut éventuellement s'identifier (2000)



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

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

N.B: parfois le temps de base imparti est insuffisant et un message d'erreur peut survenir. On enchaîne alors une 2° fois la commande **DCpromo** sans crainte…

GESTIONNAIRE DE SERVEUR

Lancer la mmc Gestionnaire de Serveur:

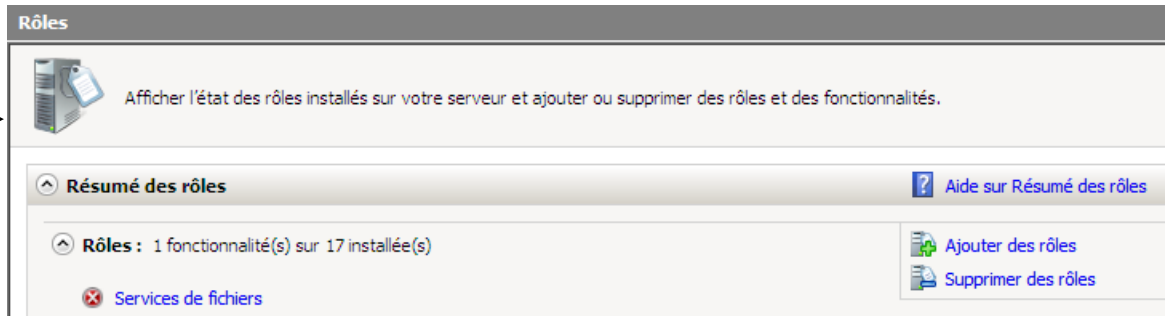
Depuis la barre des tâches

ou depuis icone **ordinateur** du bureau, via clic-droit **gérer**

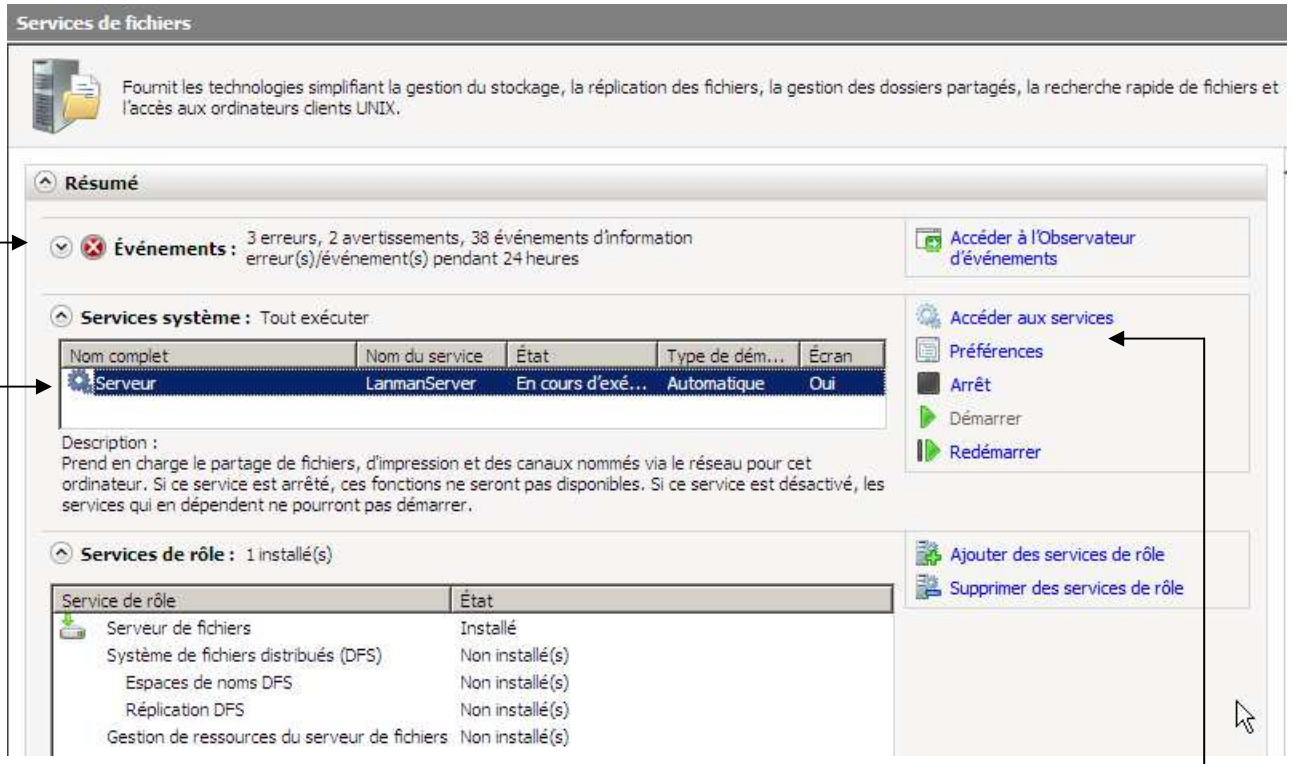
on accède au **gestionnaire de serveur**

en cliquant coté gauche, sur le noeuds, on obtient le détail, coté droit...

ainsi **Rôles**



lorsque l'on est sur un rôle, ici les **Services de fichiers**, on peut accéder au détail, en partie centrale,



on obtient directement le **nom du service** et son **paramétrage**...

et ses éventuels évènements...

le rôles peuvent se rajouter de manière automatique, comme par le service de fichier dès que l'on effectue un simple partage sur un dossier…

Roles services et fonctionalités

Un **rôle de serveur** est un ensemble de programmes logiciels qui, une fois installés et correctement configurés, permettent à un ordinateur de remplir une fonction spécifique

Une fois correctement installés et configurés, les rôles ont été conçus de manière à fonctionner automatiquement

Les **services de rôle** sont des programmes logiciels qui fournissent la fonctionnalité d'un rôle.

Certains rôles, tels que Serveur DNS, possèdent une seule fonction et ne disposent donc pas de services de rôle disponibles, mais en général Vous pouvez considérer un rôle en tant qu'un groupement de services de rôle étroitement associés et complémentaires

Les **fonctionnalités** sont des programmes logiciels qui, bien qu'elles ne fassent pas directement partie des rôles, peuvent prendre en charge ou augmenter la fonctionnalité d'un ou de plusieurs rôles, ou encore améliorer la fonctionnalité de la totalité du serveur, quels que soient les rôles installés

Actuellement 17 rôles existent, mais certains développement sont déjà prévus (wsus sp1...)

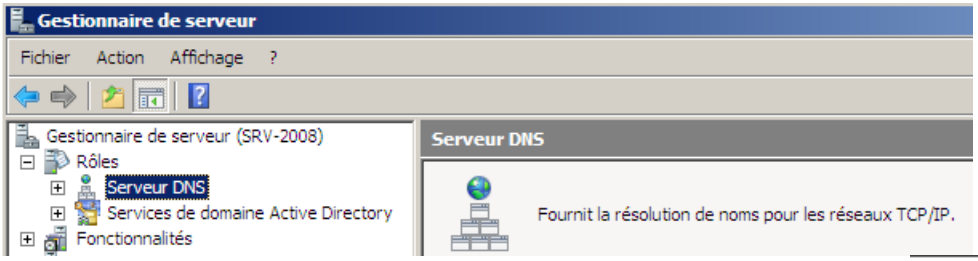
en **Core Mode** seuls 9 **rôles** sont possibles

- Hyper-V
- Serveur DHCP
- Serveur DNS
- Serveur WEB (sans ASP)
- Services AD LDS
- Services d'impression
- Services de domaine Active Directory
- Services de fichier

PRESENCE DU DNS

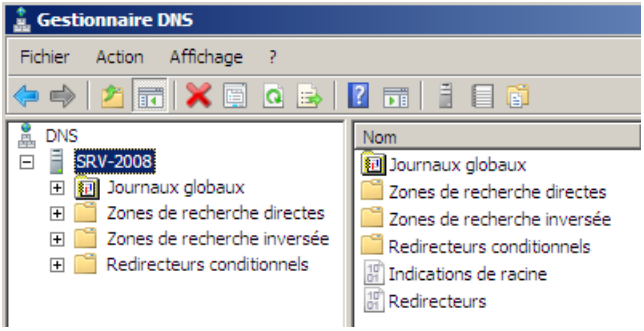
Lancer la mmc DNS:

On peut accéder au DNS soit par le biais du **Gestionnaire de serveur** dans les **Rôles**, **Serveur DNS**

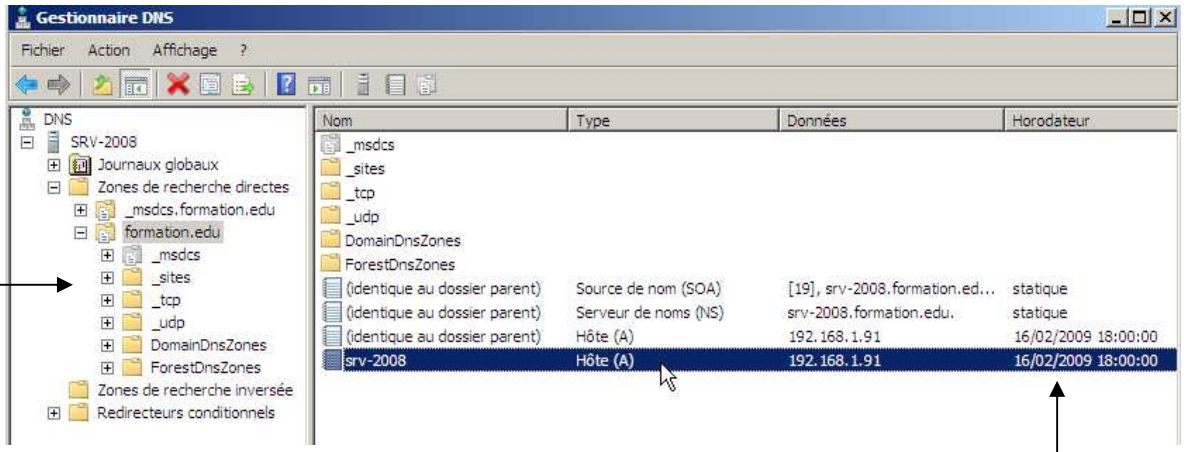


Soit depuis les outils d'administration

Panneau de configuration / outils d'Administration



Vérifier la présence de AD et du serveur:



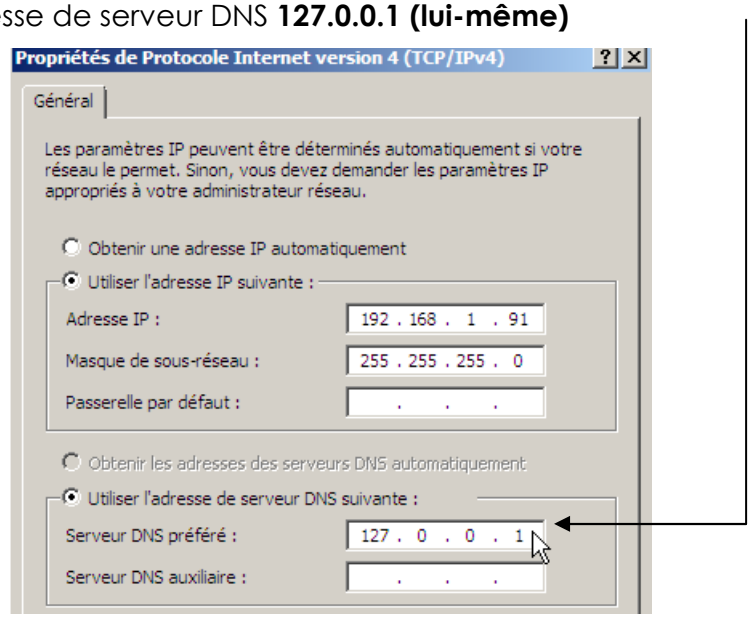
La présence de

- Un structure d'enregistrements de type SRV correspondant à AD
- L'enregistrement de notre serveur

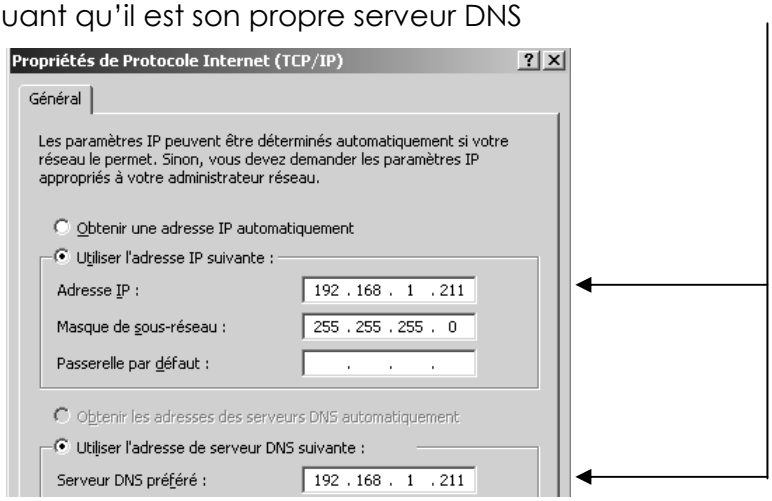
Devrait suffire pour l'instant pour valider notre serveur DNS

Vérification paramètre IP serveur :

Sous 2008, cette opération est effectuée automatiquement avec comme adresse de serveur DNS **127.0.0.1 (lui-même)**



Sur un serveur 2003, il est nécessaire de modifier le paramétrage IP en indiquant qu'il est son propre serveur DNS

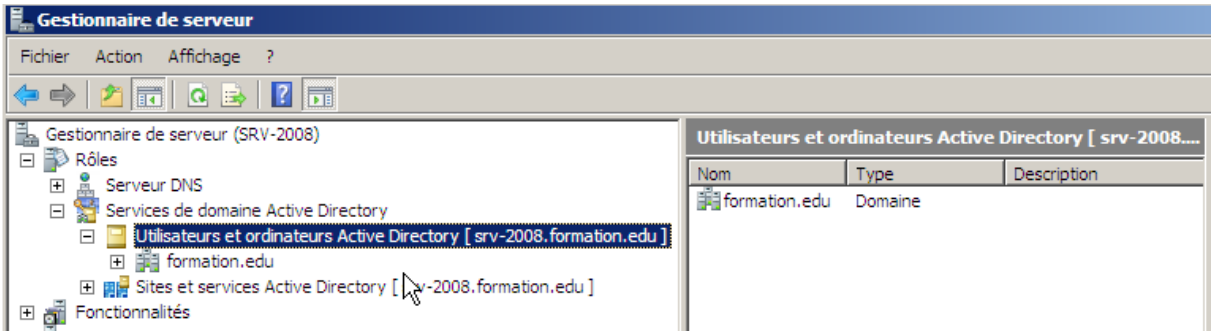


PRESENCE DE AD

Lancer la mmc AD:

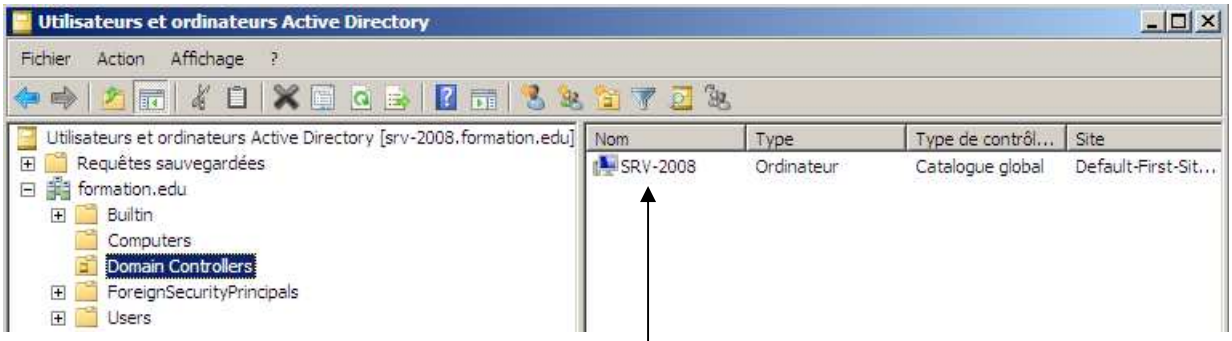
On peut accéder à la gestion de AD soit par le biais du **Gestionnaire de serveur**

dans les **Rôles**, **Services de domaine Active Directory**, **Utilisateurs et Ordinateurs Active directory**



Soit on visualise Active Directory par les outils d'administration

Panneau de configuration / outils d'Administration / Utilisateurs et Ordinateurs Active Directory



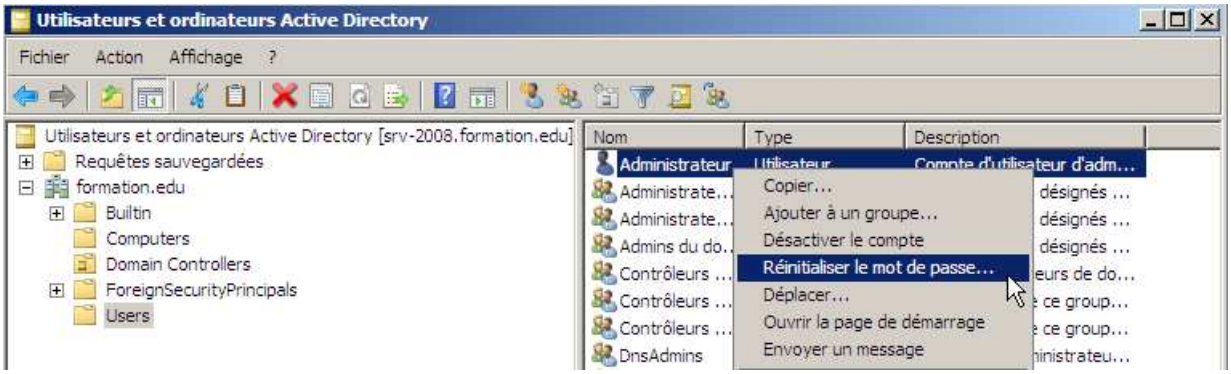
La présence :

- de notre Serveur (ici SRV1-2008) dans l'Unité Organisationnelle **Domain Controllers**
- du nom de Domaine dans l'arborescence
- Du compte Administrateur dans l'Unité Organisationnelle **Users**

devrait suffire à nous confirmer la création de notre domaine.

Présence du compte Administrateur:

Dans l'UO **Users**, on retrouve le compte **Administrateur**, il faut lui changer immédiatement de mot de passe, car désormais c'est un compte **Administrateur de Domaine**…

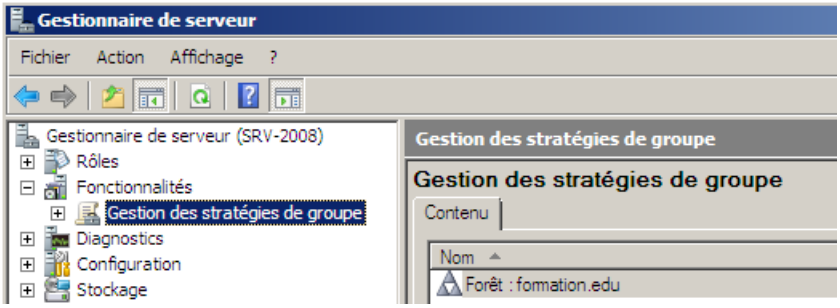


Attention aux stratégies de domaine par défaut…

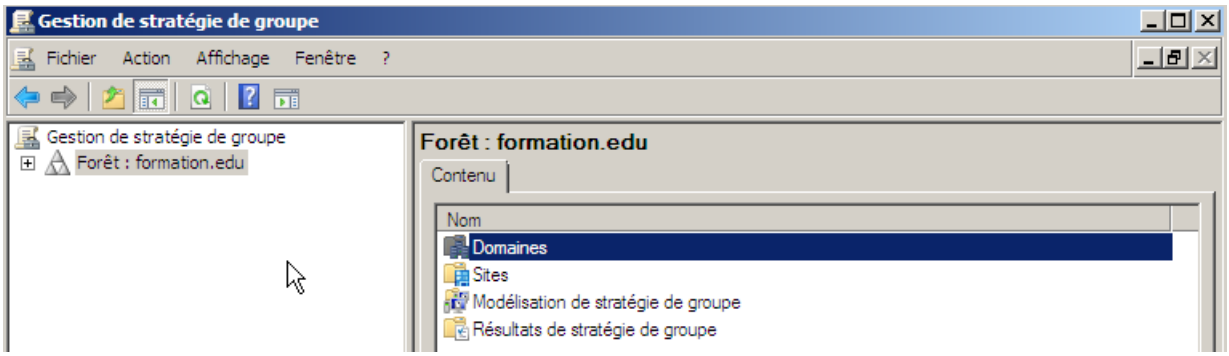
STRATEGIES DE DOMAINE

Stratégie Mot de Passe sur Domaine:

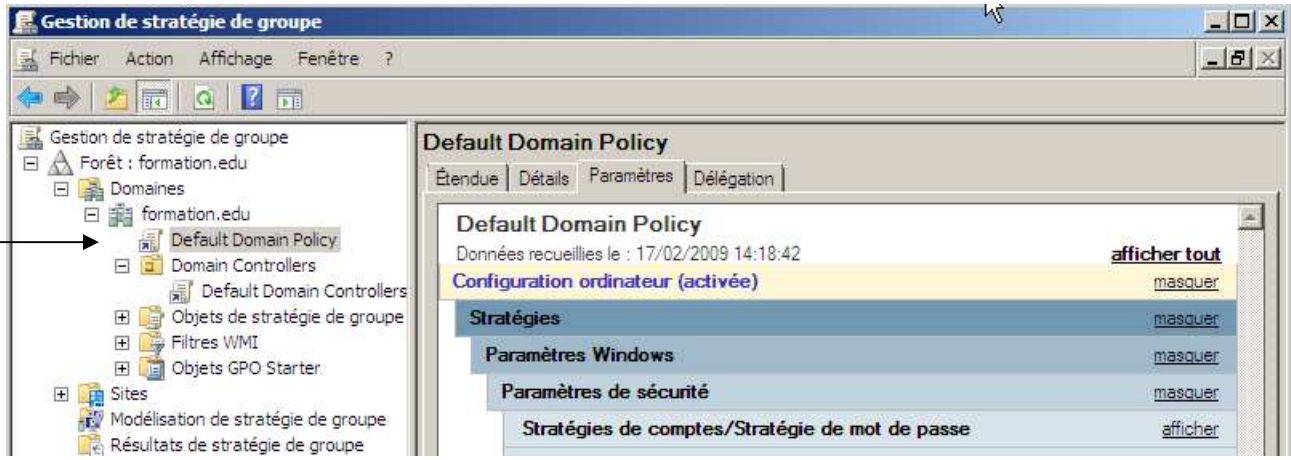
On peut accéder à la gestion des stratégies soit par le biais du **Gestionnaire de serveur / fonctionnalités / Gestion des stratégies de groupe**



soit depuis le **panneau de configuration**, **outils d'administration**, **Gestion de stratégie de groupe**



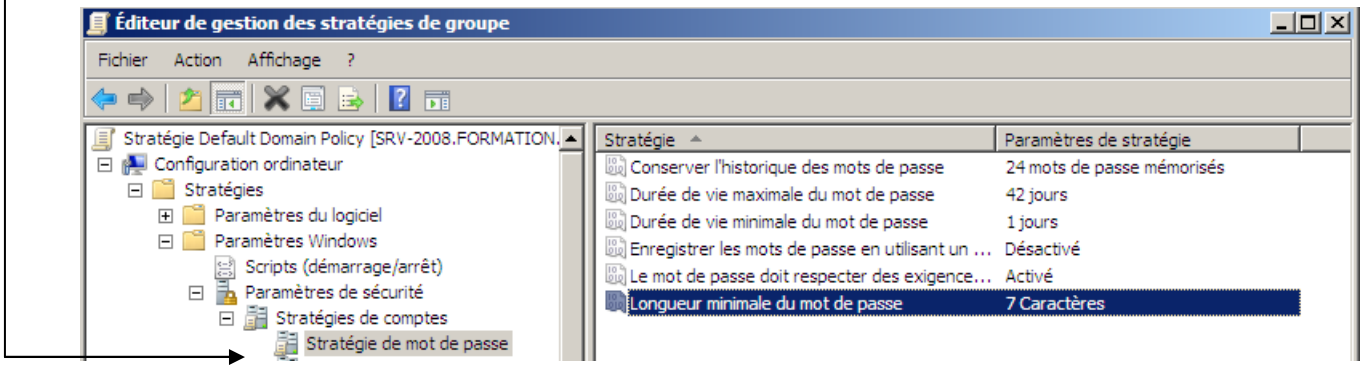
il faut se placer sur **default domain policy**



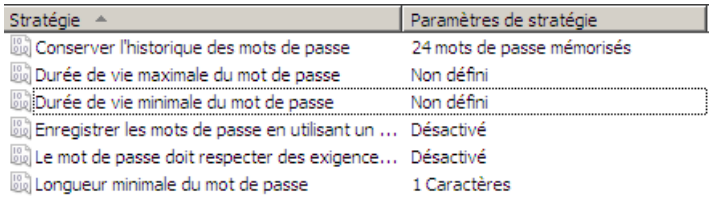
puis on demande l'onglet **Paramètres**, et clic droit / **modifier**

alors l'éditeur de stratégies apparait

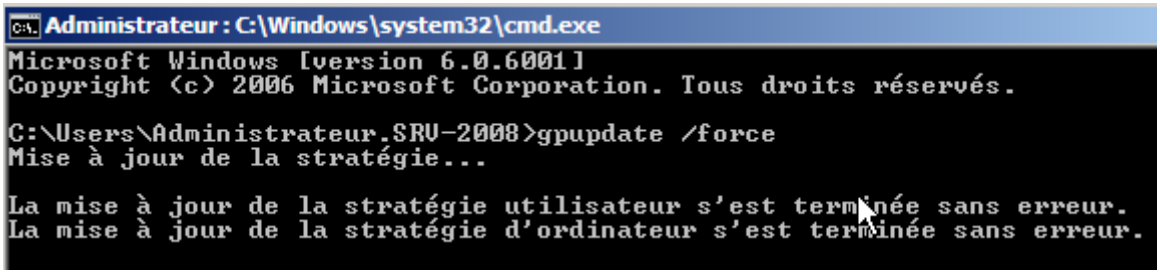
dans lequel on va chercher



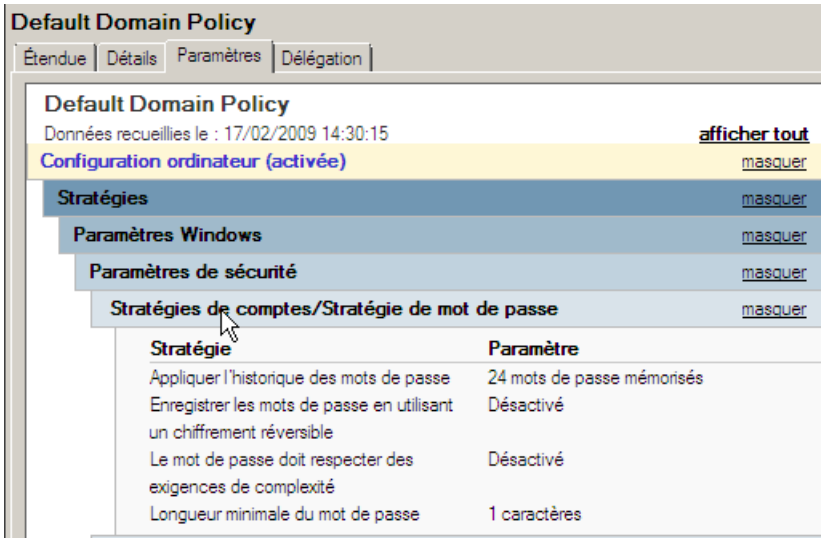
et on indique



après éventuelle propagation via **gpupdate/force**



on peut vérifier



ADHESION A UN DOMAINE

Appartenir à un Domaine depuis un client SEVEN - XP :

Pour qu'un client XP-SEVEN puisse faire partie d'un Domaine, il faut plusieurs conditions, réalisées (certaines peuvent se faire de manière plus ou moins automatique, mais détaillons de plus près:

1. Serveur : Dans A.D. un compte ordinateur ayant le même nom que le nom d'hôte du poste doit exister
2. Serveur : Dans la zone DNS de votre domaine, un enregistrement hôte correspondant a votre poste avec son adresse IP doit être saisit.
3. Client : l'adresse du serveur DNS doit être correctement renseignée, le nom machine doit correspondre a celui du compte d''ordinateur.
4. Client : une demande à se rattacher au domaine doit être faite.

Ces étapes peuvent se faire manuellement, ou peuvent être automatisées de certaines manières…

1-m Création du compte ordinateur sur le serveur (manuelle)

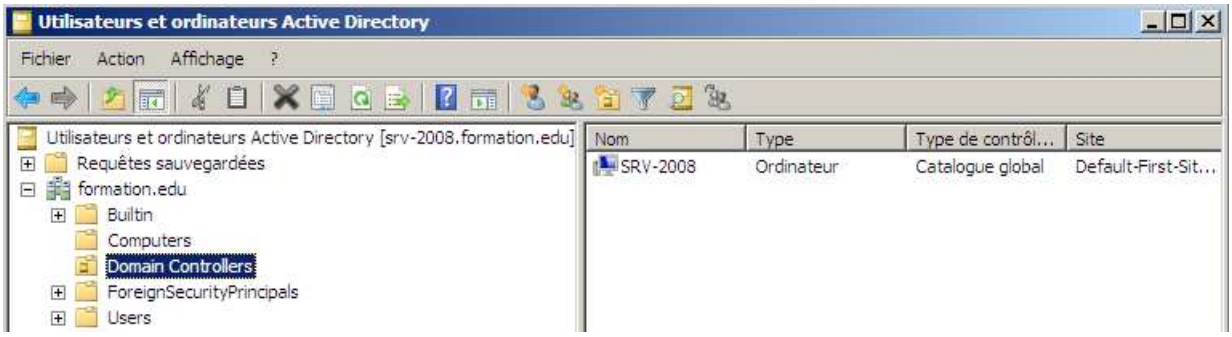
Les membres du groupe **Opérateurs de compte**, **Admins du domaine** peuvent créer des comptes ordinateurs

Par défaut, les utilisateurs authentifiés dans un domaine reçoivent le **droit d'utilisateur Ajouter des stations de travail au domaine** et ils peuvent créer jusqu'à 10 comptes d'ordinateurs dans le domaine

N.B: on peut aussi dans une unité d'organisation, attribuer à l'utilisateur ou au groupe l'autorisation **Créer des objets d'ordinateur**

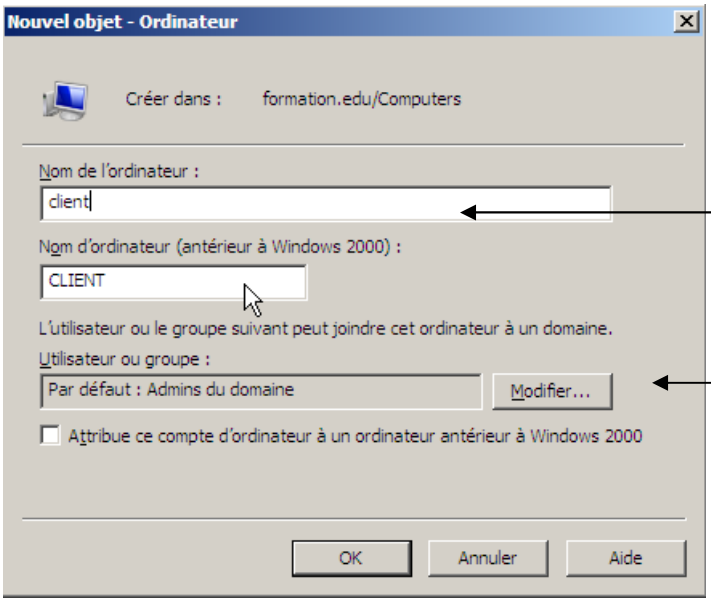
Pour créer un compte ordinateur, il faut lancer la console

Outils d'Administration / Utilisateurs et ordinateurs Active Directory



Se placer dans L'UO voulue (par exemple **Computers**) puis demander dans le menu

Action / Nouveau / Ordinateur un assistant se déclenche alors

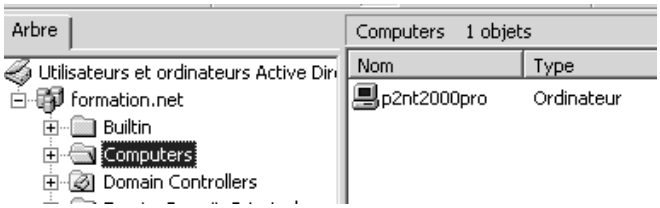


Et rentrer ici le nom machine du poste SEVEN XP qui va faire sa demande d'accès au Domaine

Ainsi que les comptes de domaines autorisés à ajouter ce PC au domaine : par défaut le groupe des

Admins du domaine…

Et le compte ordinateur se crée !



1-a Création du compte ordinateur (à la volée)

Windows 2008 accorde par défaut le droit d'ajouter des stations de travail à un domaine au groupe Utilisateurs authentifiés

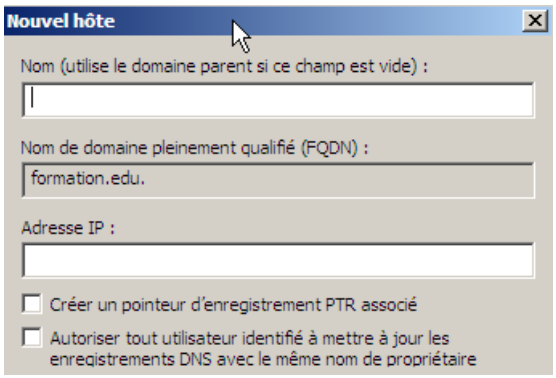
Un utilisateur authentifié peut joindre par défaut dix comptes d'ordinateur au maximum

Un administrateur de Domaine aussi

Lorsque un utilisateur authentifié crée a la volée un compte ordinateur, celui-ci est stocké dans l'**UO** par défaut **Computers**.

2 –m Création de l'enregistrement hôte dans le DNS (manuelle)

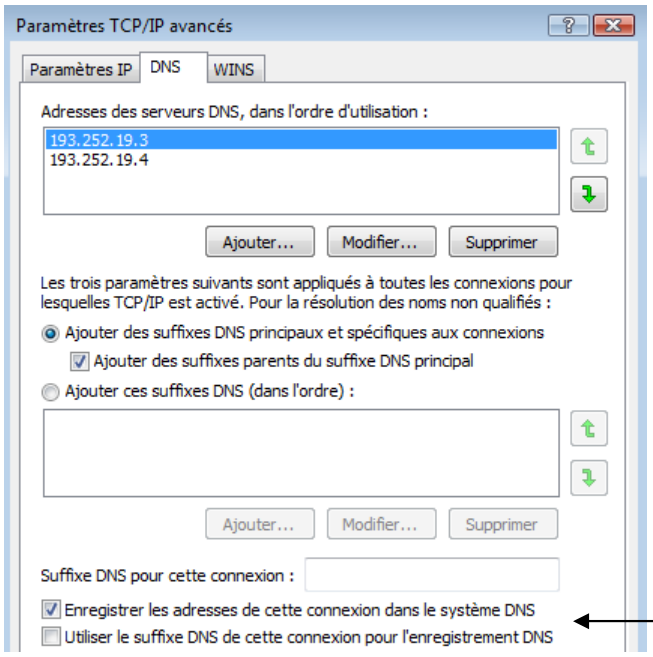
Dans le DNS on ajoute un hôte



2 –a Création de l'enregistrement hôte dans le DNS (à la volée)

Dans le cas d'un machine SEVEN ou XP Pro, et d'un serveur DDNS acceptant les mises à jours…,

et si dans les paramètres avancés tcp-ip, onglet **DNS**



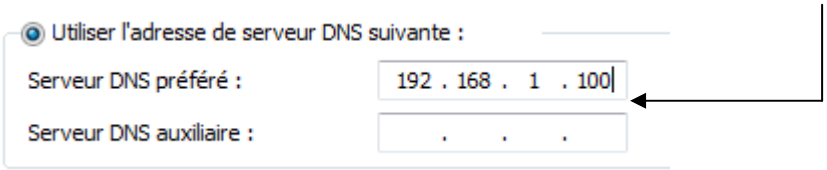
on a demandé

Enregistrer les adresses… dans le système DNS

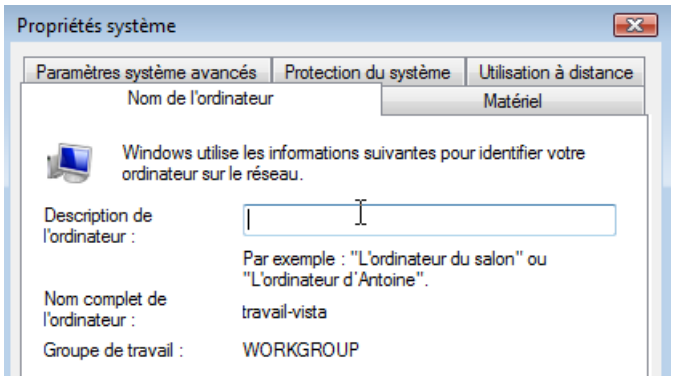
Alors l'enregistrement hôte peut de faire tout seul automatiquement.

3 Saisie dans les paramètres Tcp-ip et vérification du nom machine

il faut saisir l'adresse du serveur DNS dont le client va dépendre



et vérifier le nom machine



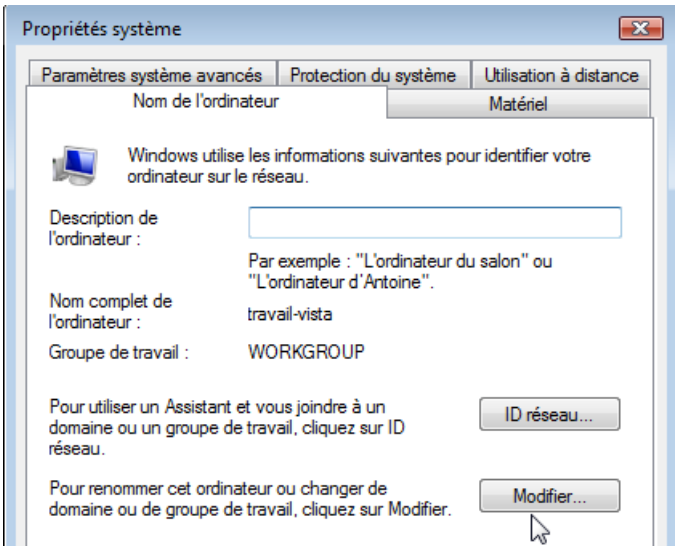
N.B: attention pour les postes SEVEN et XP, ne pas confondre le nom d'hôte (nom complet) utilisé et le nom indiqué en "description" dans les propriétés du poste de travail. ou système…

N.B: Si un changement de nom est nécessaire, il faut absolument rebooter le PC avant de faire la demande d'adhésion.

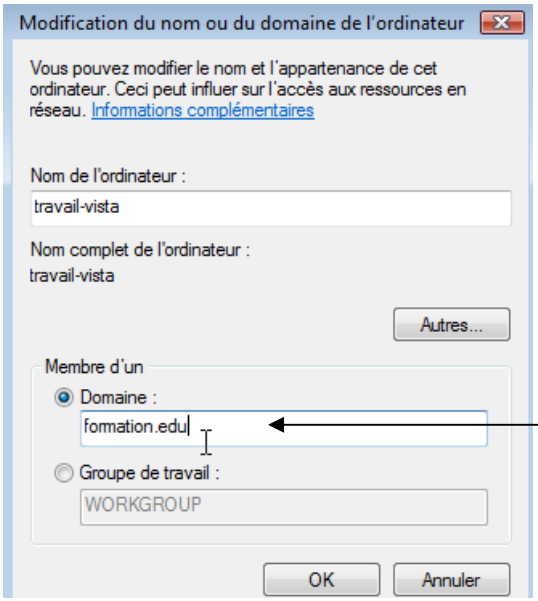
4 Demande d'adhésion au Domaine

Sous SEVEN XP l'appartenance au domaine se fait

- en demandant dans le panneau de configuration l'icône **système** puis l'onglet **identification réseau**
- en faisant un clic droit sur l'icône **ordinateur** du bureau, et demander **propriété** puis l'onglet **Nom de l'ordinateur**



on demande **Modifier…**



il faut rentrer un nom DNS !

Après authentification obligatoire, on pourra alors finir la procédure

Et changer l'appartenance ou non à un Domaine

et si tout se passe bien on a

OUVERTURE DE SESSION

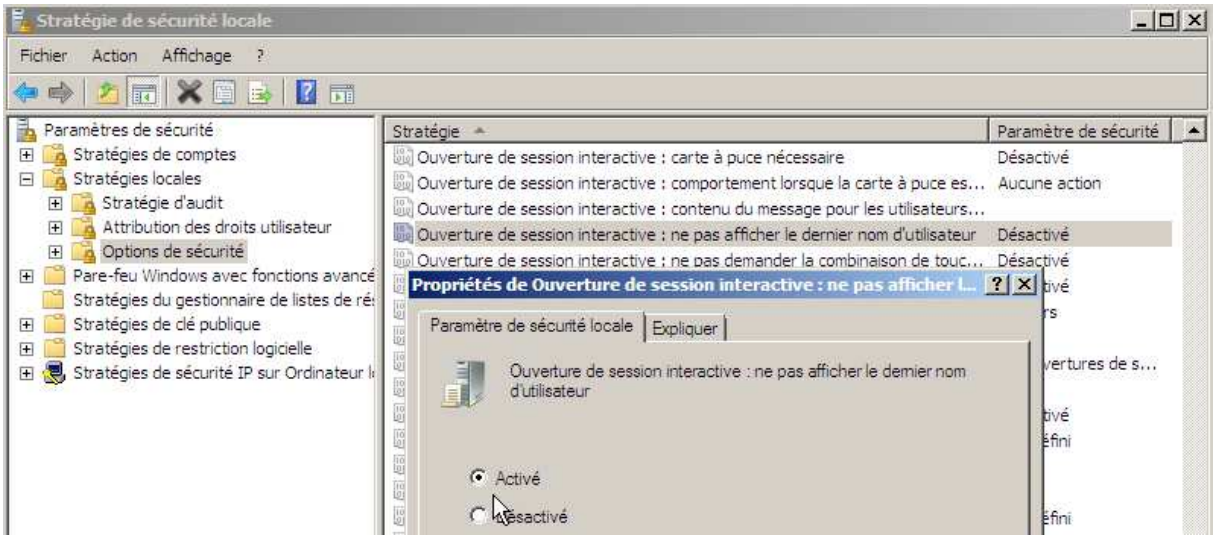
Dernier login utilisé :

Par défaut, SEVEN et XP re-proposent de visualiser le dernier utilisateur ayant ouvert une session.

Par sécurité, ou simplement par commodité (pour changer de login sous SEVEN il faut demander expressément **autre utilisateur** dans le fenêtre de login…)

il est possible de désactiver cette fonction via les stratégies de locales de sécurité

Panneau de configuration / outils d'administration / stratégies de sécurité locale



N.B : par ailleurs il est fortement déconseillé de garder la possibilité d'ouvrir des sessions multiples sur un poste en domaine, cela ne peut que amener des perturbations…

Ouverture depuis SEVEN :

Une fois le poste SEVEN raccordé au domaine…

Si le poste client se nomme « **client-SEVEN »**

Et le domaine se nomme« **formation.edu »** nom netbios « **formation »**

On peut taper un nom de la forme : **NOM\LOGIN**

client-SEVEN\administrateur	admin local du poste
formation.edu\administrateur	admin domaine,
formation\administrateur	admin domaine (nom NETBIOS)

On peut taper un nom de la forme : **LOGIN@NOM** (domaine uniquement)

administrateur@formation.edu	admin domaine
administrateur@formation	admin domaine (nom NETBIOS)
administrateur@client-SEVEN	ne marche pas

Ouverture depuis XP :

Une fois le poste XP raccordé au domaine…

Si ce n'est pas le cas, on demande le choix du domaine via **Options>>**

Dans **Se connecter à** :
2 choix existent :

- **Domaine**
- **Cet Ordinateur**

Il faudra alors choisir si on demande de s'authentifier sur le domaine ou sur le poste localement à travers cette liste déroulante.

COMPTES UTILISATEURS DE DOMAINE

Comptes Utilisateurs Prédéfinis :

Sous 2008 Serveur Il existe 2 Comptes Utilisateurs prédéfinis

Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'administration
Invité	Utilisateur	Compte d'utilisateur invité

Le **Compte Administrateur** :

C'est la personne qui aura le pouvoir maximal sur la station de travail, et pourra gérer la configuration du système

Ce compte ne peut être supprimé, mais peut être renommé

Le **Compte Invité** :

Sert pour des utilisateurs occasionnels ayant un minimum de droits sur le système

Ce compte par défaut est inactivé

Sous Windows 2003 Serveur un nouveaux compte est crée, il n'existe plus sous Windows 2008 Serveur

Le **Compte Support** :

Ce compte par défaut est inactivé

N.B Sur un Serveur CD, les comptes sont représentés par une icône , car ce sont forcement des **Comptes de Domaine**

Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'administration
Invité	Utilisateur	Compte d'utilisateur invité

N.B : sur un client SEVEN ou XP, un compte utilisateur est représenté avec une icône devant une machine, car il s'agit forcement d'un **Compte local**

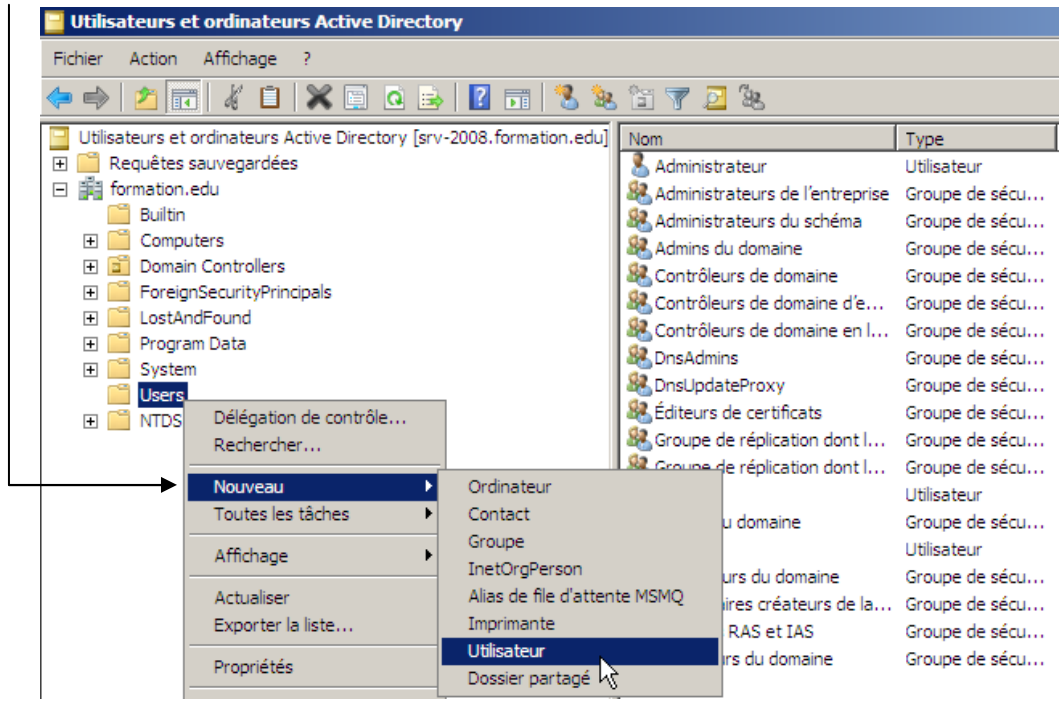
Nom	Nom complet	Description
Administrateur		Compte d'utilisateur d'administration
Invité		Compte d'utilisateur invité

Créer un Compte Utilisateur sur le Domaine:

Dans **Utilisateur et Ordinateurs Active Directory**

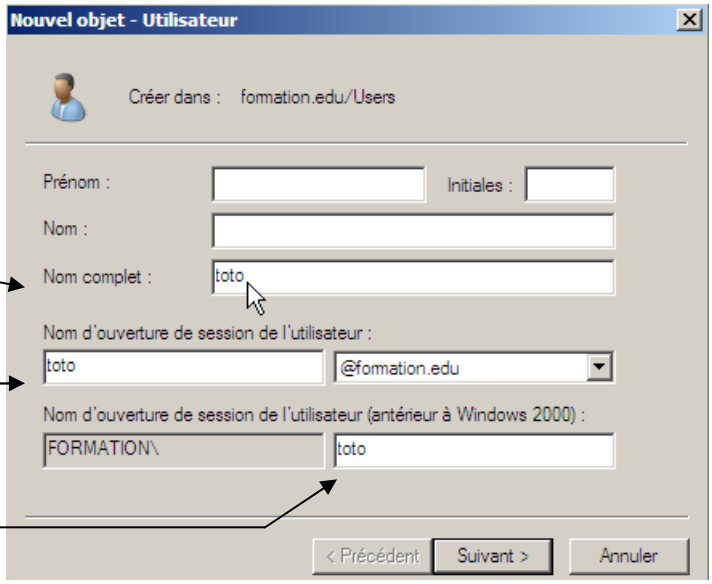
On se place dans l'unité organisationnelle voulue, par exemple **Users** et on demande ensuite

Clic droit , **Nouveau / Utilisateur**



Un assistant se déclenche alors

Les 3 renseignements requis au minimum sont



Nom complet

Nom d'ouverture de session de l'utilisateur

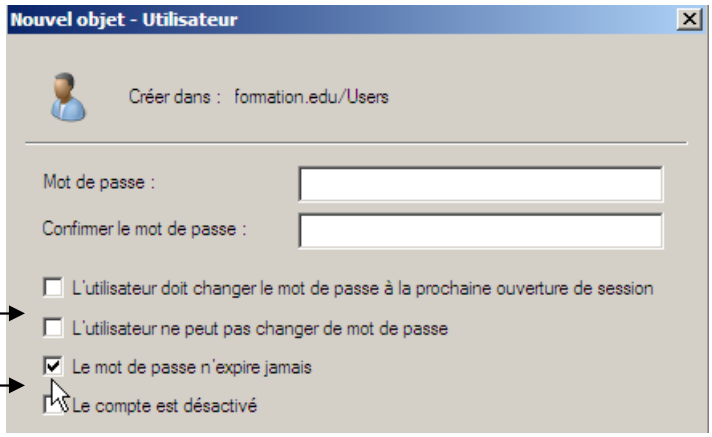
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)

Et le mot de passe

On peut choisir ses réglages…

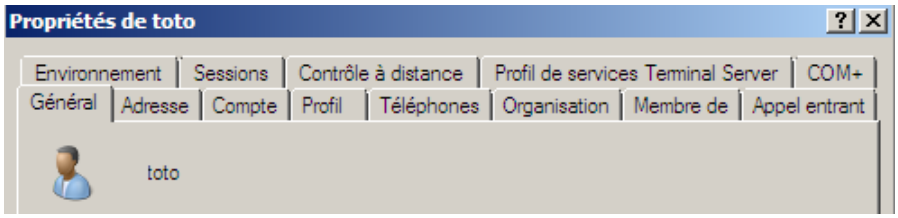
il vaut mieux éviter de demander de changer le mot de passe à la première ouverture de session, surtout en formation…

durée par défaut :45j



Propriété Compte Utilisateur de Domaine:

Il faut se placer sur le compte utilisateur voulu et demander le menu contextuel **propriété…**



Parmi les onglets existants, certains sont indispensables au quotidien,

Général

Compte

Profil

Membre de

d'autres correspondent à des fonctionnalités plus spécifiques

Environnement

Sessions

Contrôle à distance

Profil de services Terminal Server

Com+

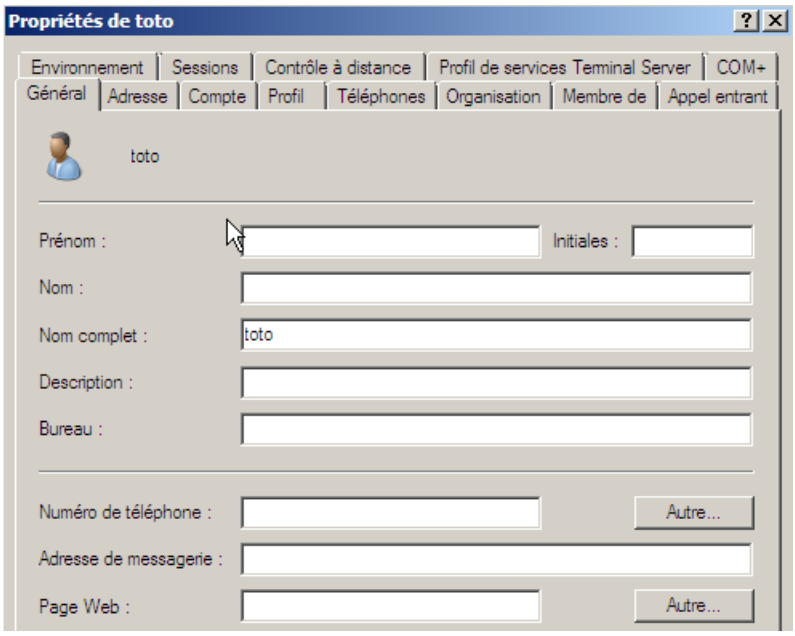
Adresse

Téléphones

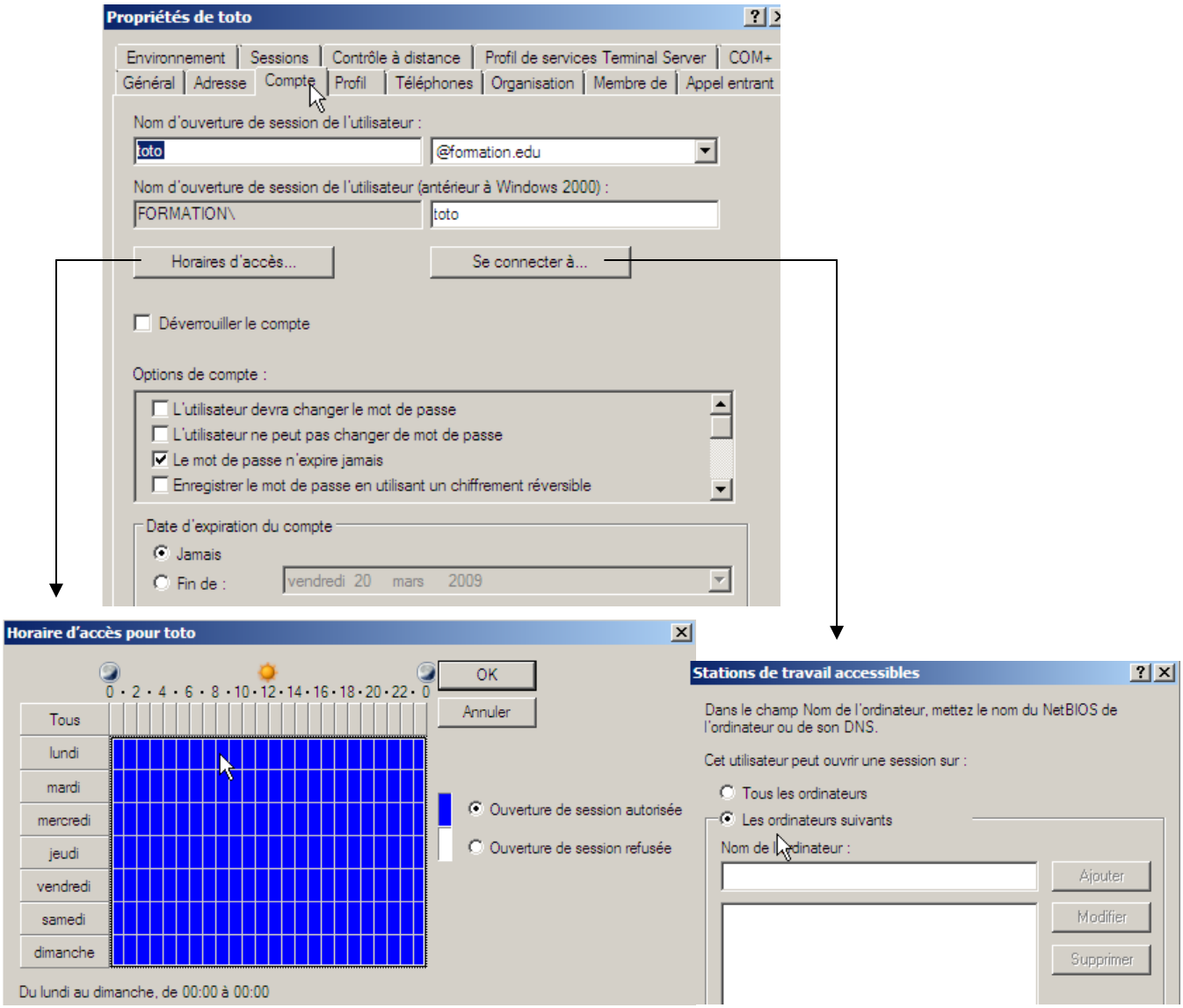
Organisation

Appel entrant

Compte Utilisateur onglet Général :

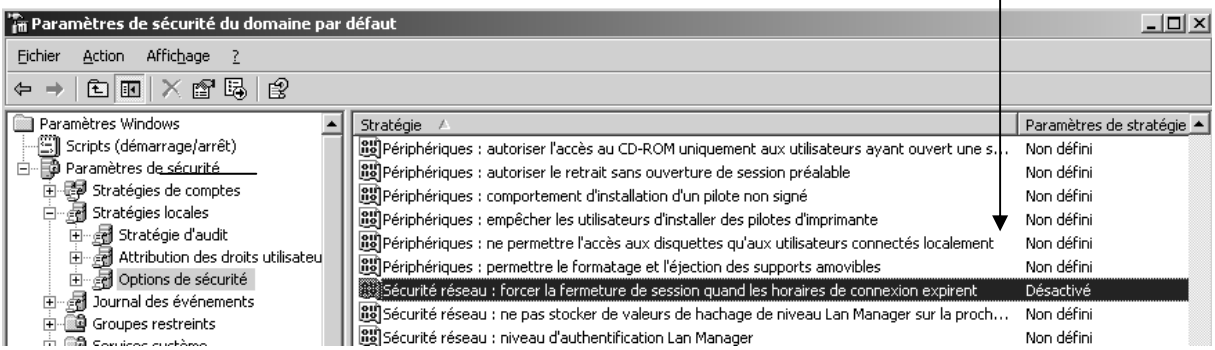


Compte Utilisateur onglet Compte :



Horaire d'accès

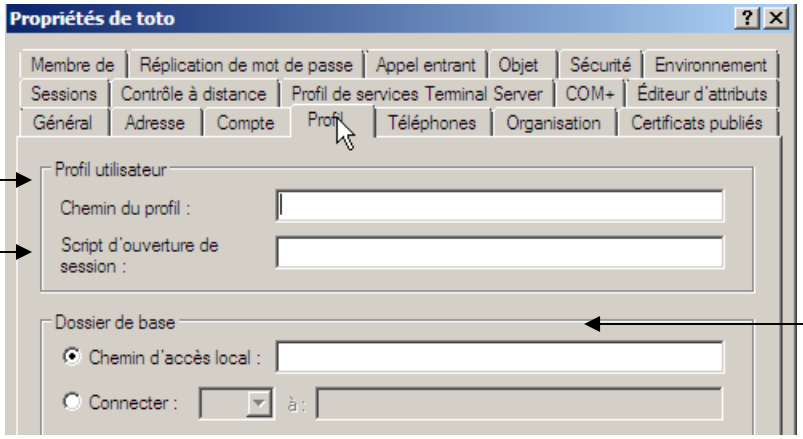
Si jamais un utilisateur reste en session après les horaires convenus, par défaut il ne sera pas déconnecté. Cela est modifiable par une **stratégie de Domaine**



Se connecter à

Si le nom Netbios est utilisé, donc cela s'applique aussi à des postes Windows 9.x, même si dans ce cas on ne pourra pas garantir le poste (comme avec SEVEN ou XP…)

Compte Utilisateur onglet Profil :



Profil utilisateur

Il est possible de définir des profils errants, et des profils obligatoires non modifiables (cf chapitre profil page 113)

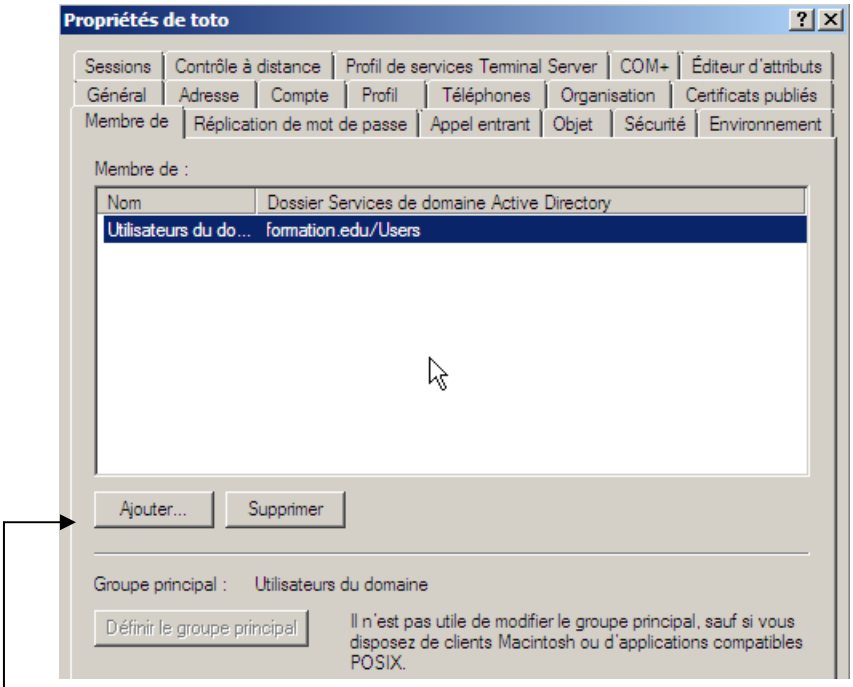
Script d'ouverture de session

On peut développer des scripts se déclanchant au moment de l'ouverture de session de cet utilisateur sur le client (cf chapitre script page 105)

Dossier de base

Une facilité de création de répertoire sécurisé pour cet utilisateur peut être mise en place (cf chapitre répertoire de base page 101)

Compte Utilisateur onglet Membre de :



Ajouter / Supprimer : Il est possible de visualiser / modifier l'appartenance de l'utilisateur à un groupe local – global – universel…

GROUPES LOCAUX

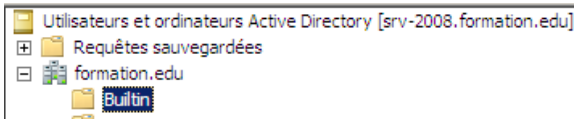
Groupes Locaux Prédéfinis :

Les droits d'un utilisateur sont souvent déterminés par le groupe auquel il appartient, un **groupe** étant un ensemble d'utilisateur ayant les mêmes droits, ou mieux, un ensemble de droits et de permissions bien définis, dont on bénéficiera lorsque l'on en fait partie.

Un groupe local à un symbole qui est sur un serveur 2008

Il existe un certain nombre de **groupes prédéfinis** dans Windows, depuis le groupe **Administrateurs** (disposant de tous les droits) jusqu'au groupe Invité (ayant les droits les plus faibles)

Sous 2008 SRV les groupes locaux prédéfinis sont stockés essentiellement dans l'UO **Builtin**

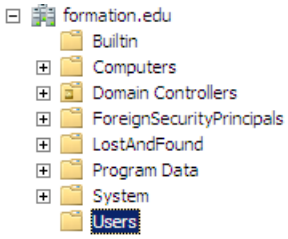


Nom	Type
Accès compatible pré-Windows 2000	Groupe de sécurité - Domaine local
Accès DCOM service de certificats	Groupe de sécurité - Domaine local
Administrateurs	Groupe de sécurité - Domaine local
Duplicateurs	Groupe de sécurité - Domaine local
Générateurs d'approbations de forêt entrante	Groupe de sécurité - Domaine local
Groupe d'accès d'autorisation Windows	Groupe de sécurité - Domaine local
IIS_IUSRS	Groupe de sécurité - Domaine local
Invités	Groupe de sécurité - Domaine local
Lecteurs des journaux d'événements	Groupe de sécurité - Domaine local
Opérateurs d'impression	Groupe de sécurité - Domaine local
Opérateurs de chiffrement	Groupe de sécurité - Domaine local
Opérateurs de compte	Groupe de sécurité - Domaine local
Opérateurs de configuration réseau	Groupe de sécurité - Domaine local
Opérateurs de sauvegarde	Groupe de sécurité - Domaine local
Opérateurs de serveur	Groupe de sécurité - Domaine local
Serveurs de licences des services Terminal Server	Groupe de sécurité - Domaine local
Utilisateurs	Groupe de sécurité - Domaine local
Utilisateurs de l'Analyseur de performances	Groupe de sécurité - Domaine local
Utilisateurs du Bureau à distance	Groupe de sécurité - Domaine local
Utilisateurs du journal de performances	Groupe de sécurité - Domaine local
Utilisateurs du modèle COM distribué	Groupe de sécurité - Domaine local

N.B : Les groupes prédéfinis suivant n'existent pas sous Windows 2003 Serveur

- IIsiusr
- Accès DCOM service de certificat
- Opérateurs de chiffrement
- Lecteurs des Journaux d'évènements

Sous 2008 SRV certains groupes locaux prédéfinis sont aussi stockés dans l'UO **Users**



Nom	Type
DnsAdmins	Groupe de sécurité - Domaine local
Éditeurs de certificats	Groupe de sécurité - Domaine local
Groupe de réplication dont le mot de passe RODC e...	Groupe de sécurité - Domaine local
Groupe de réplication dont le mot de passe RODC e...	Groupe de sécurité - Domaine local
Serveurs RAS et IAS	Groupe de sécurité - Domaine local

N.B : Les groupes prédéfinis suivant n'existent pas sous Windows 2003 Serveur

- Groupe de réplication mot de passe RODC autorisé
- Groupe de réplication mot de passe RODC refusé
- TelnetClients

Groupe Local Administrateurs

Contient : Compte **Administrateur** (de la machine locale)

+ Groupe Global **Admins du Domaine**

Membres :

Nom	Dossier Services de domaine Active Directory
Administrateur	formation.edu/Users
Administrateurs de l'entreprise	formation.edu/Users
Admins du domaine	formation.edu/Users

Utilisation : Tout faire sur la machine locale (si la machine est un contrôleur de domaine, on peut tout faire sur le domaine)

Groupe Local Utilisateurs

Contient : Tous les comptes crées sur la machine

Groupe Global **Utilisateurs du Domaine**

Membres :

Nom	Dossier Services de domaine Active Directory
INTERACTIF	AUTORITE NT
Utilisateurs authentifiés	AUTORITE NT
Utilisateurs du domaine	formation.edu/Users

Utilisation : Faire ce que on leur a accordé et accéder aux ressources que on leur a partagé

Groupe Local Invités

Contient : Compte **Invité**

+ Groupe Global **Invités du Domaine**

Membres :

Nom	Dossier Services de domaine Active Directory
Invité	formation.edu/Users
Invités du domaine	formation.edu/Users

Utilisation : Faire ce que on leur a accordé et accéder aux ressources que on leur a partagé. Mais les membres de ce groupe ne peuvent pas modifier de manière permanente leur environnement

Opérateur de sauvegarde

Contient : Vide

Utilisation : Sauvegarder et restaurer des fichiers sur la machine locale (via le gestionnaire de sauvegarde)

Opérateur de Serveur

Contient : Vide

Utilisation : Les membres peuvent administrer les serveurs de domaine

Groupe Local Utilisateurs Bureau à Distance

Contient : Vide

Utilisation : Utiliser le bureau à Distance

Groupe Local Opérateurs de configuration réseau

Contient : Vide

Utilisation : Droits de configuration réseau (changement adresse IP)

Groupe Local Utilisateurs avec Pouvoir (que sous SEVEN - XP)

Contient : Tous les comptes autorisés manuellement

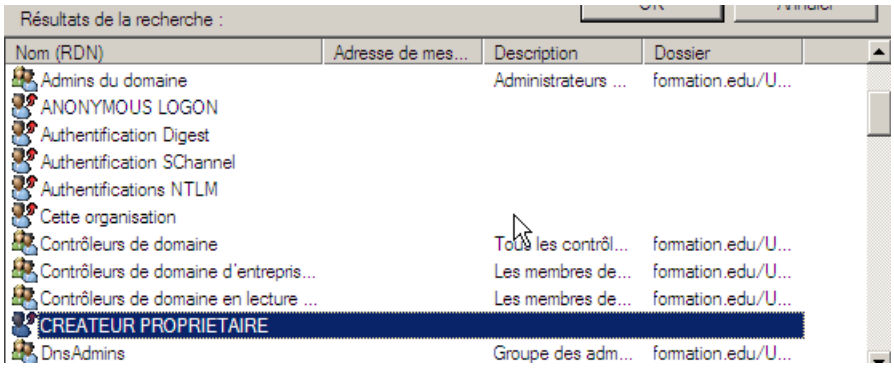
(+ Groupe Global **Utilisateurs du Domaine)**

Utilisation : Faire ce que on leur a accordé et accéder aux ressources que on leur a partagé

N.B: En général beaucoup de groupes prédéfinis par rapport aux besoins de gestion d'un réseau local classique, et que il paraît souhaitable de n'utiliser que les groupes importants

Groupes Spéciaux

Ces groupes Spéciaux prédéfinis, l'administrateur lui même ne peut les détruire ni les renommer, et **on les voit apparaître nottament lors du partage d'accès aux ressources**.



Autrement dit **ce n'est pas vous qui gérez les groupe spéciaux prédéfinis, mais vous pouvez vous en servir….**

En effet, selon ce qu'un utilisateur est en train de faire, il devient automatiquement membre (ou est supprimé) d'un groupe Spécial

Seuls deux de ces groupes présentent un intérêt dans un premier temps

Tout le monde

Contient : Tous les utilisateurs travaillant sur une machine, y compris les invités.

Utilisation : Accorder des droits à tous les utilisateurs

Créateur propriétaire

Contient : L'utilisateurs ayant crée ou pris possession d'un ressource (en NTFS)

Utilisation : gérer les accès au fichiers et aux dossiers sur des disques NTFS

Anonymous Logon

Ouverture de session anonyme

Contient : Ce groupe représente les utilisateurs et les services qui accèdent à un ordinateur et à ses ressources par l'intermédiaire d'un réseau sans utiliser un nom de compte, un mot de passe ou un nom de domaine

Sur Windows NT et des versions antérieures, le groupe Ouverture de session anonyme est un membre par défaut du groupe Tout le monde.

Sur Windows Server 2008 ou 2003, le groupe Ouverture de session anonyme n'est pas un membre par défaut du groupe Tout le monde.

Réseau

Contient : utilisateurs qui accèdent à une ressource donnée sur le réseau, par opposition aux utilisateurs qui accèdent à une ressource en se connectant localement à l'ordinateur contenant la ressource. Chaque fois qu'un utilisateur accède à une ressource donnée sur le réseau, l'utilisateur est ajouté automatiquement au groupe Réseau

Interactifs

Contient : Ce groupe représente tous les utilisateurs qui sont actuellement connectés à un ordinateur particulier et qui accèdent à une ressource donnée sur cet ordinateur, par opposition aux utilisateurs qui accèdent à la ressource sur le réseau

GROUPES GLOBAUX-UNIVERSELS

Groupes locaux - globaux - universels:

En fait deux catégories de groupes existent par défaut sur les serveurs 2003:

- Les **Groupes Globaux :** contiennent les utilisateurs du domaine, c'est à dire définissent les groupes de personnes qui auront les même droits et permissions sur tout le Domaine
- Les **Groupes Locaux :** sont généralement associés à une machine, et définissent les droits d'accès se rapportant à des ressources locales, c'est à dire sur une machine

  N.B: il existe des **Groupes Locaux de Domaine**, et des **Groupes Locaux hors Domaine**.
  En effet si un groupe local est défini sur un contrôleur de Domaine, il existera sur tous les contrôleurs de domaine, alors qu s'il est défini sur une machine autre, il n'existera que sur cette machine

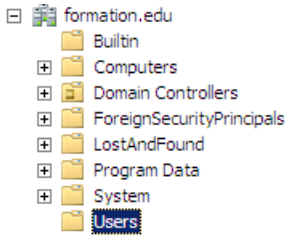
Et trois catégories sur les serveurs 2008, car un nouveau type de groupe apparaît:

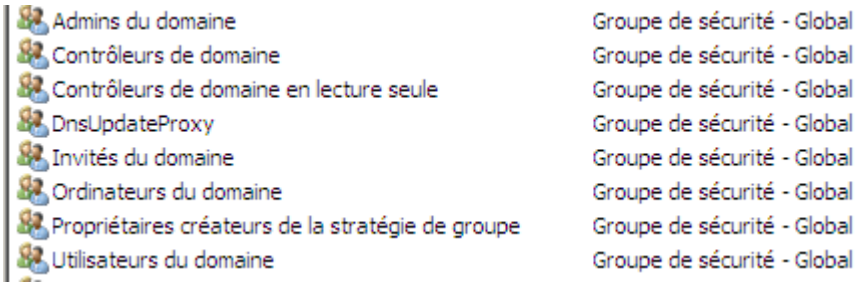
- Les **Groupes Universels :** permettent de consolider les groupes qui s'étendent sur plusieurs domaines. Pour ce faire, ajoutez les comptes aux groupes à étendue globale et insérez ces groupes dans des groupes à étendue universelle

Un **groupe global** – **Universel** à un symbole qui est sur un serveur 2008

Nom	Type	Description
Administrateurs de l'entreprise	Groupe de sécurité - Universel	Administrateurs désignés de l'entreprise
Administrateurs du schéma	Groupe de sécurité - Universel	Administrateurs désignés du schéma
Admins du domaine	Groupe de sécurité - Global	Administrateurs désignés du domaine
Contrôleurs de domaine	Groupe de sécurité - Global	Tous les contrôleurs de domaine du domaine
Contrôleurs de domaine d'e...	Groupe de sécurité - Universel	Les membres de ce groupe sont des contrôle...
Contrôleurs de domaine en l...	Groupe de sécurité - Global	Les membres de ce groupe sont des contrôle...
DnsAdmins	Groupe de sécurité - Domaine local	Groupe des administrateurs DNS

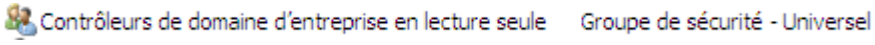
Sous 2008 SRV les **groupes globaux** et **Universels** prédéfinis sont stockés essentiellement dans l'UO **Users**





Sur un serveur 2003, les 2 groupes **Administrateur de l'entreprise**, **Administrateur du schéma**, peuvent exister en tant que **Groupe Global** si on choisit un niveau fonctionnel 2000…

Le groupe **Contrôleur de domaine d'entreprise en lecture seule**, **Administrateur** ne peut exister que sur un serveur 2008

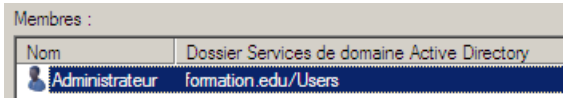


Groupes Globaux prédéfinis

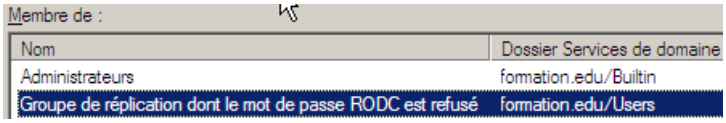
Sur tout poste NT Server 2000 2003 Contrôleur de Domaine

Admins du Domaine

Contient : Compte **Administrateur**



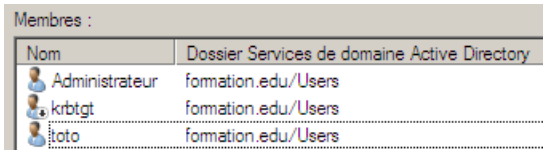
Inclus dans : Groupe Local **Administrateurs** de toute poste du domaine



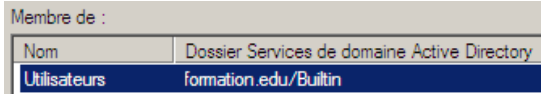
Utilisation : Tout faire sur la machine locale et sur le domaine

Utilisateurs du Domaine (Utilisa. du Domaine sous 2003)

Contient : Automatiquement tous les comptes crées sur le domaine , on ne peut les supprimer de leur groupe principal



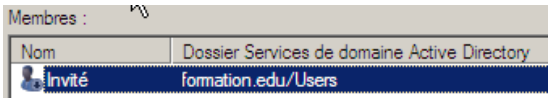
Inclus dans : Groupe Local **Utilisateurs** de chaque machine du domaine, y compris serveurs



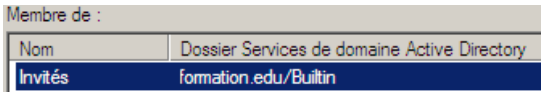
Utilisation : Faire ce que on leur à accordé et accéder aux ressources que on leur à partagé

Invités du Domaine

Contient : Compte Invité



Inclus dans : Groupe Local **Invité** de chaque machine du domaine, y compris serveurs



Utilisation : Faire ce que on leur à accordé et accéder aux ressources que on leur à partagé. Mais les membres de ce groupe ne peuvent pas modifier de manière permanente leur environnement

Inclusions entre groupes sous NT

Un intérêt majeur de la notion de groupe, réside dans l'idée de pouvoir inclure des groupes dans des groupes, ainsi que des utilisateurs dans des groupes.

Cela permet de structurer les accès aux ressources et les attributions de droits de manière plus fiable et rationnelle, plutôt que de travailler au niveau de l'individu.

Sous Windows NT 4.0

Utilisateur - Groupe	Peut contenir	Peut être membre
Utilisateur	-	Groupe Local Groupe Global
Local	Utilisateur Groupe Global	-
Global	Utilisateur	Groupe Local

N.B: Noter que ce sont les groupes Globaux qui peuvent faire partie des groupes Locaux, et jamais l'inverse

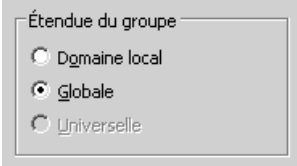
N.B: Noter que les groupes Locaux ne peuvent contenir que des groupes Globaux, et jamais d'autres groupes Locaux

Sous Windows 2000, apparaît un nouveau type de Groupe, le **groupe Universel**, Ce groupe permet des portée à l'intérieur d'une forêt et non pas simplement d'un Domaine.

Mais ce groupe ne peut être utilisé si il existe ne serait-ce que un seul serveur NT4 faisant partie du Domaine…

Par conséquent lorsque l'on installe un Domaine, par défaut celui-ci est dit en **mode mixte** pour les domaine 2000 et **mode interim** (…) pour les domaines 2003

Dans cette situation l'accès aux groupes universels est désactivé

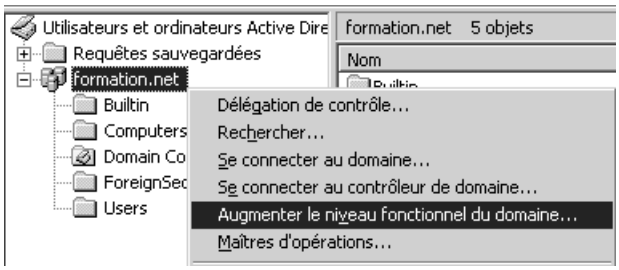


Mode de Domaine	Serveur CD Possibles
2000 Mixte (par défaut)	Windows Nt 4.0 Windows 2000 Windows 2003
2000 natif	Windows 2000 Windows 2003
2003 Interim	Windows Nt 4.0 Windows 2003
2003 natif	Windows 2003
2008 natif	Windows 2008

Pour passer en mode 2000 natif (ou 2003) il faut dans

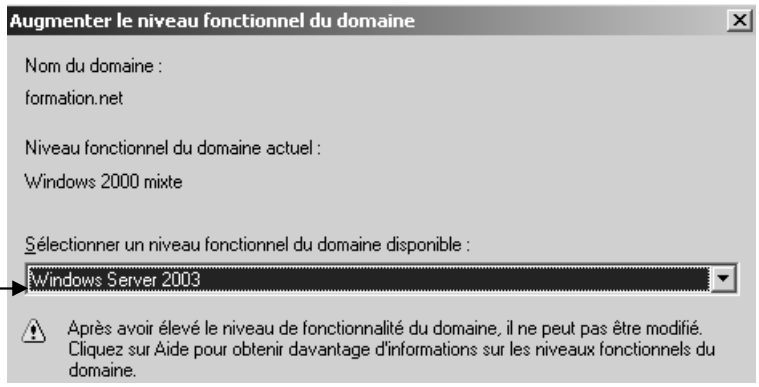
Outils d'Administration / utilisateur et ordinateurs Active Directory, sélectionner le domaine et demander par clic droit

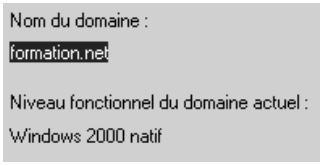
Augmenter le niveau fonctionnel du domaine…



N.B : Après changement de niveau fonctionnel, tout retour en arrière est impossible !

On choisit le niveau que l'on peut atteindre





En mode natif il est possible désormais de :

- Inclure des groupes Locaux dans des groupes Locaux
- Inclure des groupes Globaux dans des groupes Globaux
- Créer des groupes Universels
- Changer de Nom de Domaine (…)

Sous Windows 2000-2003-2008 (mixte-natif)

Type de Groupe	Peut contenir (**en Mixte-NT4**)	Peut contenir (***en natif***)	Peut être membre de (**en Mixte-NT4**)	Peut être membre de (***en natif***)
G-LOCAL	**Utilisateur** **G-Global**	**Utilisateur** **G-Global** ***G-Local*** ***G-Universel***	**-**	***G-Local***
G-GLOBAL	**Utilisateur**	**Utilisateur** ***G-Global***	**G Local (mixte)**	**G Local** ***G-Global*** ***G Universel***
G-UNIVERSEL	-	***Utilisateur*** ***G-Global*** ***G-Universel***	**-**	***G-Local*** ***G Universel***

Quelques règles pour créer des groupes :

L'administration d'un réseau Windows repose sur une analyse en 3 étapes

1. Définir les diverses fonctions ou types d'utilisateurs intervenant sur le réseau, pour permettre la définition des droits et des permissions des Groupes Globaux
2. Définir les diverses fonctions et ressources utilisables localement sur un poste selon des besoins des différents types d'utilisateur pour créer les Groupes Locaux
3. Faire de ces Groupes Globaux des membres des Groupes Locaux

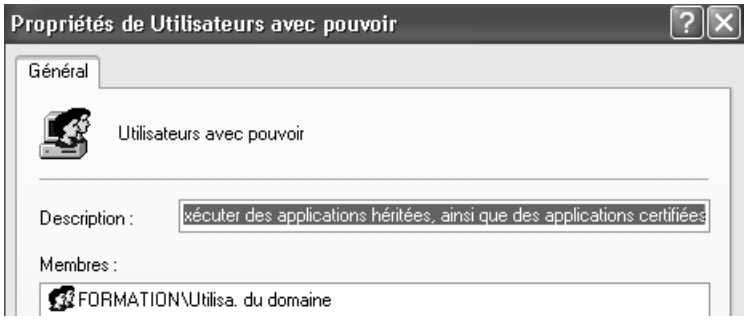
- Pour Créer des Groupes il faut faire partie d'un des groupes prédéfinis suivant : **Administrateurs**, **Opérateurs de Compte**
- Les noms de groupe doivent être uniques au sein du Domaine, être différents des noms des comptes utilisateurs ne pas dépasser 20 caractères ni contenir les caractères suivants :
  ? \ * " < > | / [ ] ; : + =
- Regroupez logiquement tous les utilisateurs du domaine en fonction de leurs besoins commun:
  Par exemple tous ceux devant utiliser une imprimante couleur, tous ceux devant accéder en lecture à tous les fichiers…
- Créez d'abords les Groupes Globaux logiques d'utilisateurs, puis ajoutez ensuite dans chaque groupe les comtes utilisateurs nécessaires
- Créez des Groupes Locaux en fonction des besoins d'accès aux ressources
- Affectez aux groupes locaux les permissions adéquates
- Incluez les Groupes Globaux dans les groupes locaux

Exemple : Utilisateur de Domaine - Utilisateur avec pouvoir

On souhaite qu'un utilisateur, des qu'il est crée, soit reconnu sur tous les postes du domaine avec des droits du niveau utilisateurs avec Pouvoir

Au niveau de chaque poste membre du domaine, il faut les configurer avec comme membre du groupe local des **Utilisateurs avec Pouvoir**

Le groupe des **Utilisateurs du domaine**



Exemple accès ressources :

Si les chefs de service (regroupés dans un **Groupe Global** "***Chef de service***") doivent accéder à tous les fichiers

Et les commerciaux (regroupés dans un **Groupe Global** "***Commerciaux***") ne doivent que pouvoir les lire,

Alors il faut créer deux **Groupes Locaux** là où sont stockés les fichiers: un pour l'accès complet (nommé "***Accès complet***") , l'autre pour l'accès en lecture seule (nommé "***Accès lecture***").

Le **Groupe Global** "***Chef de service***" sera inclus dans le **Groupe Local** "***Accès complet***",

le **Groupe Global** "***Commerciaux***" sera inclus dans le **Groupe Local** "***Accès lecture*** "

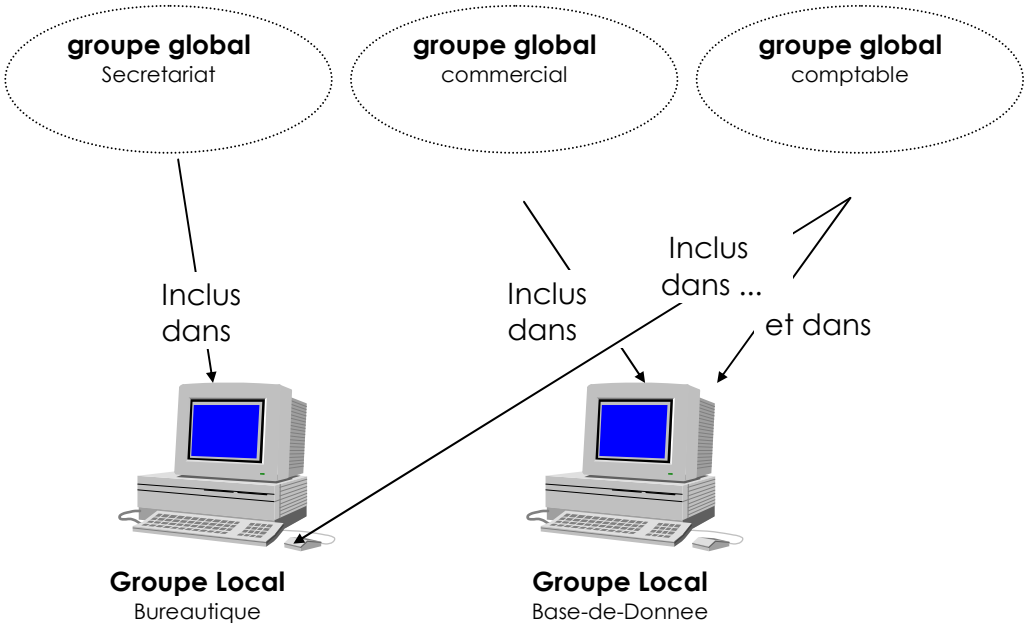
Exemples 3 :

On a besoin de créer au niveaux des utilisateurs une fonction de Secrétariat une fonction de Commercial et une fonction de comptable. Les Logiciels installé sont des logiciels de bureautique ou de gestion de base de donnée.

trois groupes globaux "**Secretariat**",
"**Commercial**"
"**Comptable**" correspondant aux fonctions ,

ainsi que deux groupes locaux définissant le type de ressources que l'on peut avoir besoin d'utiliser, à savoir "**Bureautique**"
"**Base-de-Donnee**"

On intègrera chaque groupe global dans les groupes locaux dont il à l'usage, par exemple



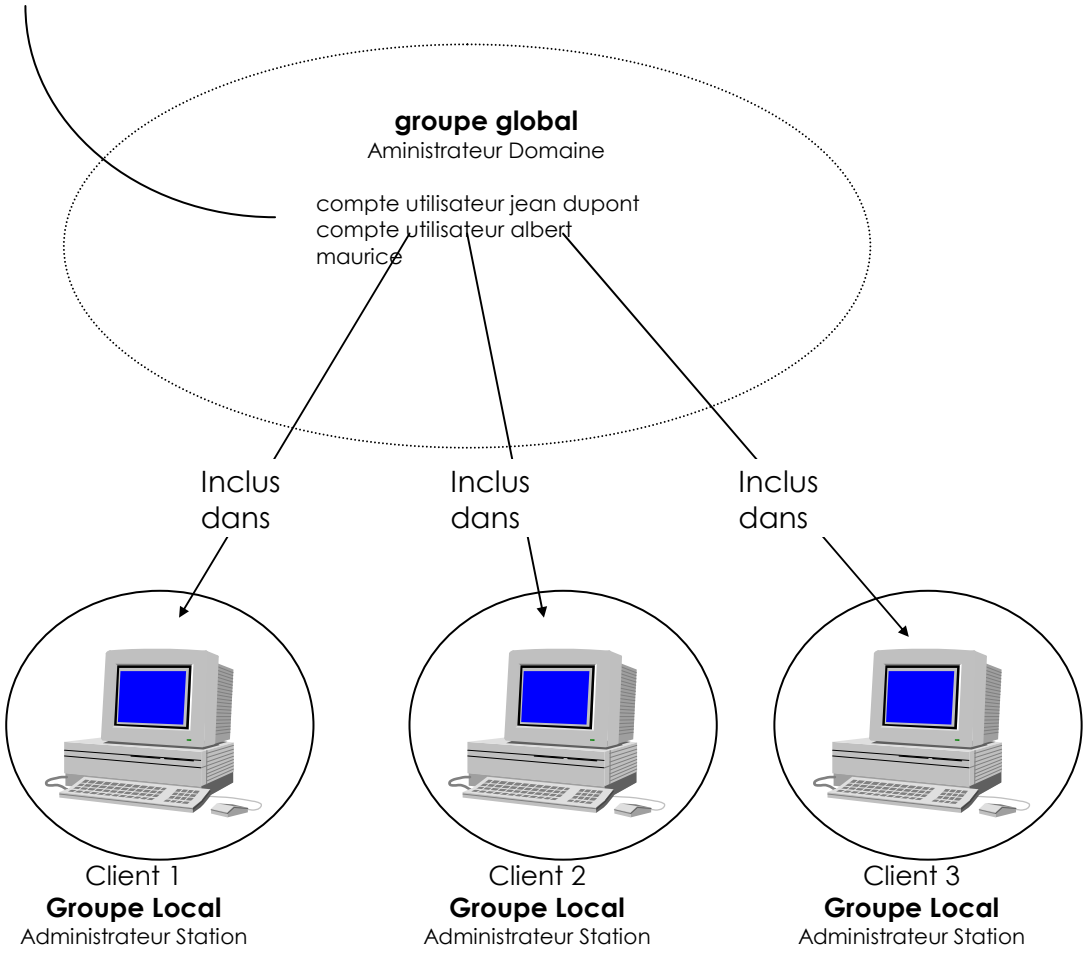
- Si un Commercial arrive, en le mettant dans le grpe Global "**Commercial**" il récupère tous les droits sur les logiciels qu'il peut avoir besoin d'utiliser...

Exemple : Groupes Admins de Domaine & Administrateurs:

Dans un domaine, on a besoin de créer au niveau des utilisateurs une fonction d'Administrateur, il existe par conséquent un groupe global "**Admins du Domaine**" correspondant à la fonction d'administration sur tout le domaine en général

Au niveau des stations il existe un groupe local "**Administrateurs** " ayant tous les droits et les permissions possibles et imaginables mais limitées à la station

Le Groupe Global "**Admins du Domaine**" est intégré dans le groupe Local "**Administrateurs** " de façon à ce que les administrateurs du domaine soient également administrateur de la station



- Si on relie une nouvelle station, le groupe Global "**Admins du Domaine**" est placé dans le groupe Local "**Administrateurs** " et très simplement, les membres du groupe des administrateur de domaine ont tous les droit sur la station
- Si un nouvel Administrateur est embauché, il suffit de le placer dans le groupe Global "**Admins du Domaine**" pour qu'il récupère automatiquement tous les droits sur toutes les stations...

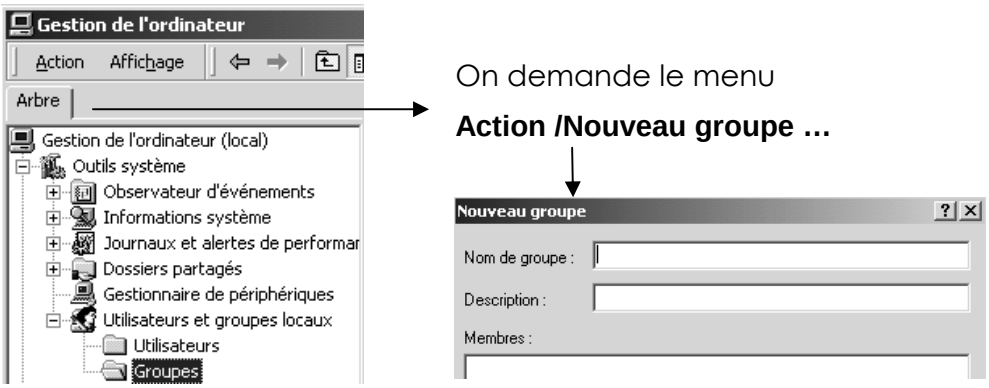
N.B : Si on avait travaillé au niveau des comptes directement, il aurait fallut insérer le nouvel administrateur dans chaque station au lieu de simplement l'ajouter dans le groupe Global "**Admins de Domaine**"

CREATION – GESTION DE GROUPES

Groupe local sur un poste:

l'outil pour faire cela se trouve dans le menu

Démarrer / Programme / Outils d'Administration/ gestion de l'ordinateur

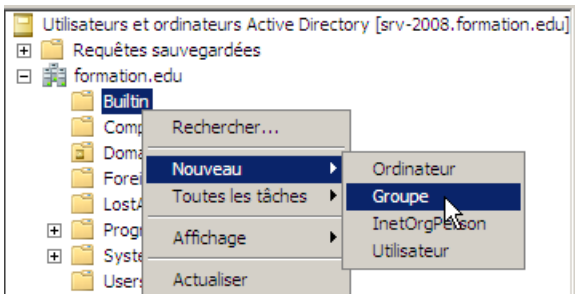


Groupe local – Global sur un Serveur CD:

Sur le serveur contrôleur de domaine on demande

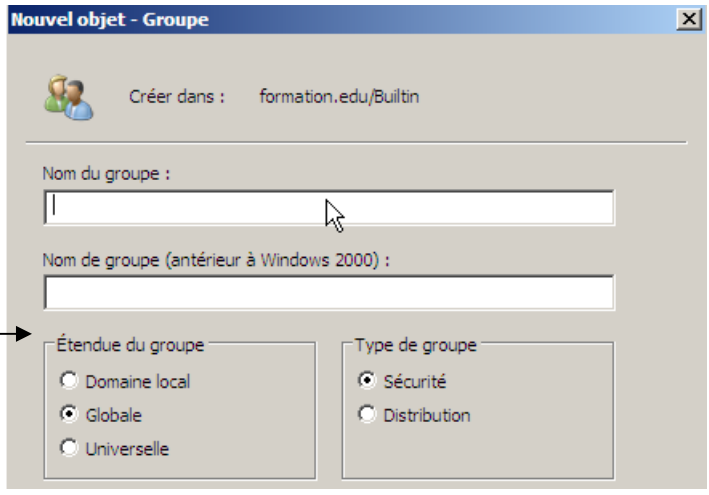
Utilisateurs et ordinateurs Active Directory

puis dans le gestionnaire MMC On se place par exemple sur l'UO **Builtin**



et on demande le menu **Action / Nouveau / Groupe** (ou clic droit, …)

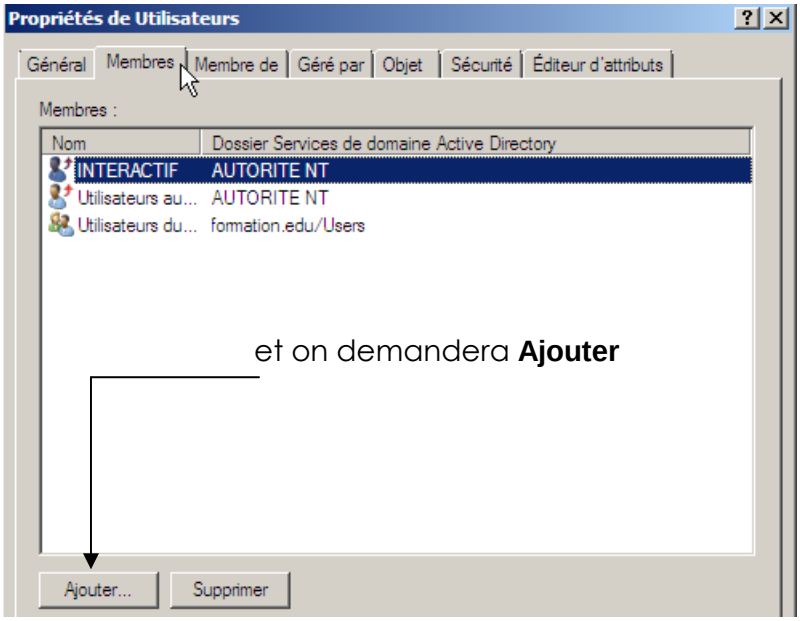
On demande un groupe dont la portée est **Local ou Globale**



puis OK

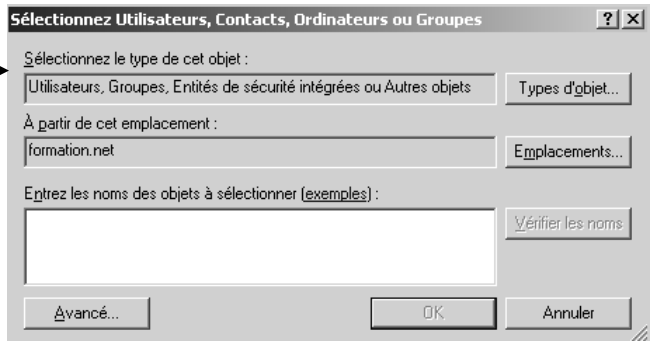
Membres d'un groupe:

- Sur un poste **V2008 ou SEVEN** on fera un double clic sur le groupe que l'on souhaite gérer, deux onglets apparaissent, on choisit l'onglet **Membres** et on demandera **Ajouter**



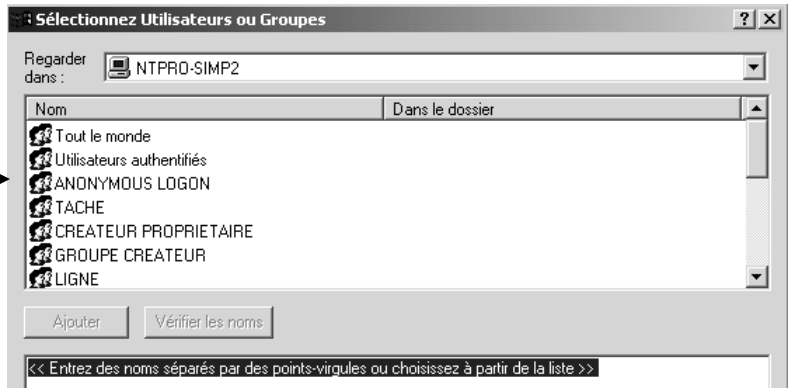
- Sur un poste **XP** on fera un double clic sur le groupe local que l'on souhaite gérer, onglet **Membres** et on demandera **Ajouter**

On obtiendra alors la boite de dialogue suivante :



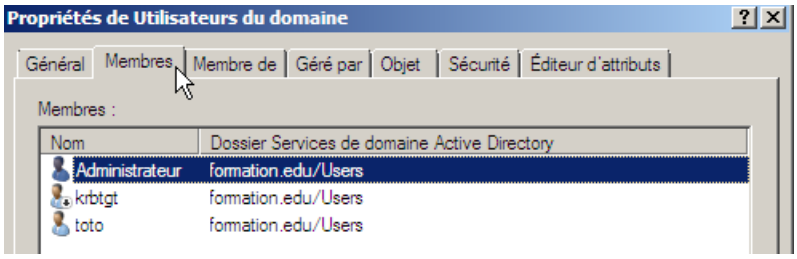
Proposant un certain nombre de Utilisateurs, **groupes locaux, globaux ou Universel**, selon le domaine dan lequel on effectue la recherche

Ou

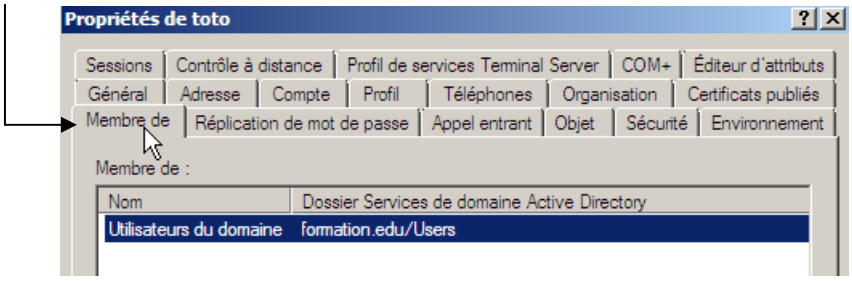


Gérer - Information sur les groupes -

Si on peut savoir quels sont tous les utilisateurs membre d'un groupe, en double-cliquant sur le groupe et en demandant **Membres**



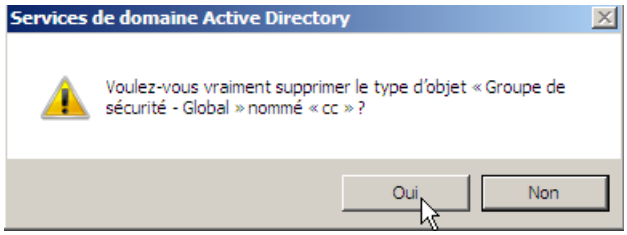
On peut aussi savoir quels sont tous les groupes dont un compte Utilisateur est membre en double-cliquant sur le compte Utilisateur, puis demander **Membres de,** on obtient alors



Suppression d'un groupe

Il faut sélectionner le groupe que l'on veut supprimer et demander **Supprimer ...**

Un message de mise en garde apparaît informant du coté irréversible de la commande



Il faut parfois encore confirmer (sur AD un simple Confirmation est demandée)

REPERTOIRE DE BASE

Répertoire de base ou d'Accueil :

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

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

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

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

Mise en Place :

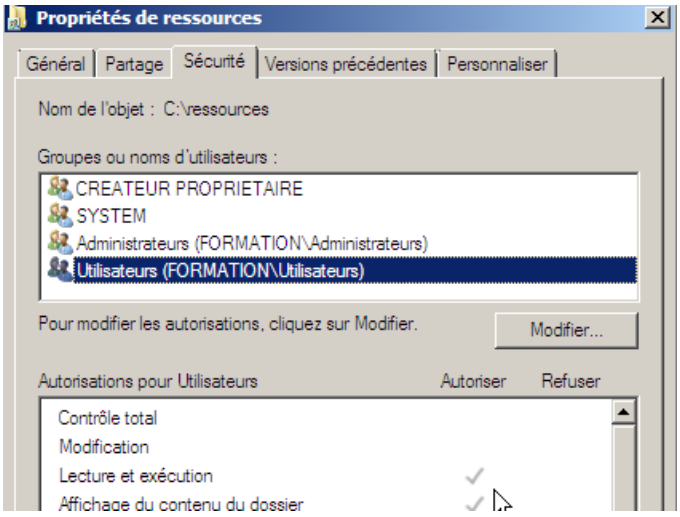
Un certain nombre d'opérations doivent être effectuées, certaines avant la création des comptes utilisateurs, et d'autres pendant la création de ces comptes.

Avant la création des comptes

Il faut se créer la structure de rangement :

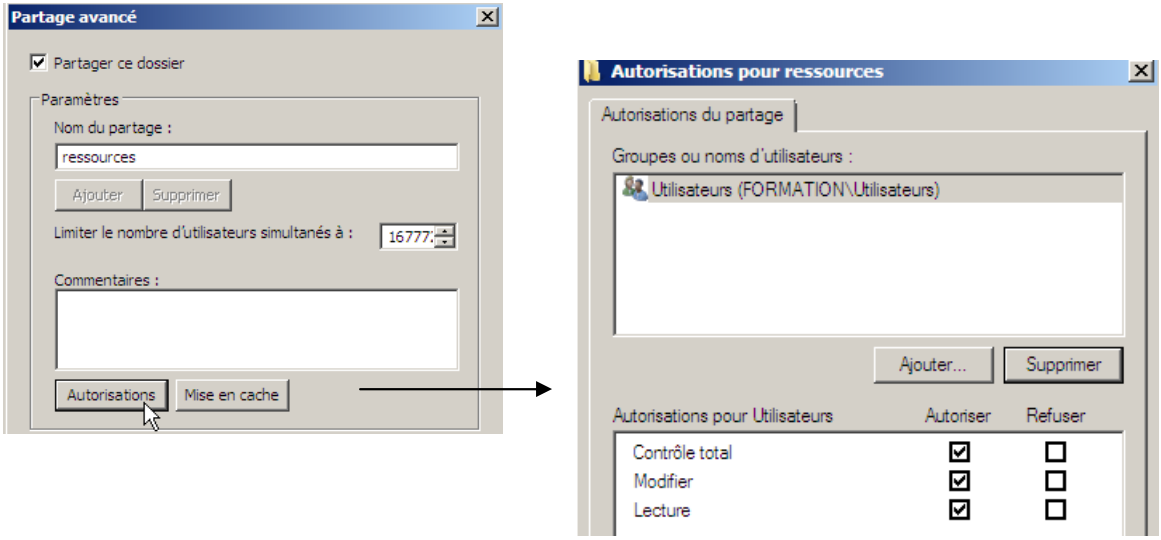
- Créer le dossier "racine" de la future arborescence pour les dossiers des utilisateurs, nommé par exemple **ressources (**mais il ne faut pas se créer soi-même les dossiers utilisateurs à l'intérieur ! **sauf si ce dossier est sur un volume FAT)**

Les permissions de sécurité NTFS sont les permissions par défaut

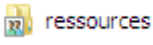


- Il faut ensuite partager ce dossier **Ressource** en donnant une permission de type **contrôle total** à tous les utilisateurs à même d'y venir par la suite

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

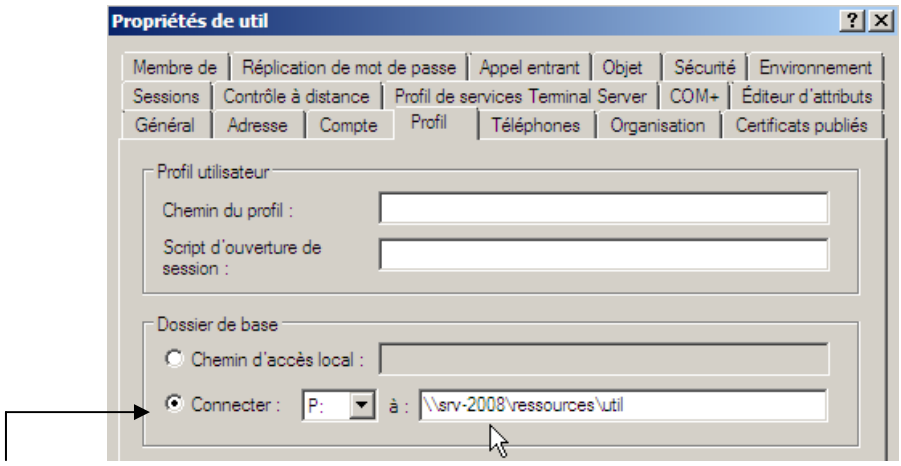


L'icône de partage apparaît

ou


Pendant la création d'un compte

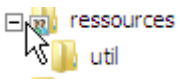
Lorsque ensuite l'on crée un compte Utilisateur, il faut demander les propriétés et demander l'onglet **Profil,**



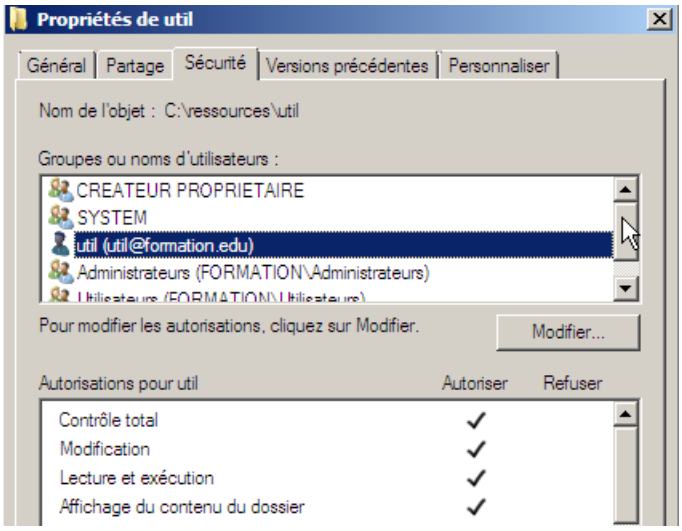
Dans la boîte de dialogue il faut donner un nom et un emplacement au **dossier de base**, et choisir **Connecter**, puis choisir une lettre de lecteur logique associée à ce répertoire de base (ici **P:** par exemple)

Après ouverture de session de **Util** sur un client, celui-ci devrait automatiquement voir apparaître

Sur le serveur un dossier perso pour util est crée…



La sécurité NTFS est posée par héritage, plus **util** en accès **contrôle total**



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

Cela permet de créer un compte « modèle » utilisable ensuite par copier

Noter que dans l'écriture du type:

\\serveur\ressource\%username%

on à selon les conventions de nom les valeurs suivante :

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

Résultat :

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

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

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

Modifier le répertoire de base :

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

Rappels :

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

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

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

Remarques sur le répertoire de base :

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

par conséquent un script permettant de créer un lecteur logique sur un autre répertoire de base lors de l'ouverture de session paraît à priori fort souhaitable

SCRIPT D'OUVERTURE DE SESSION

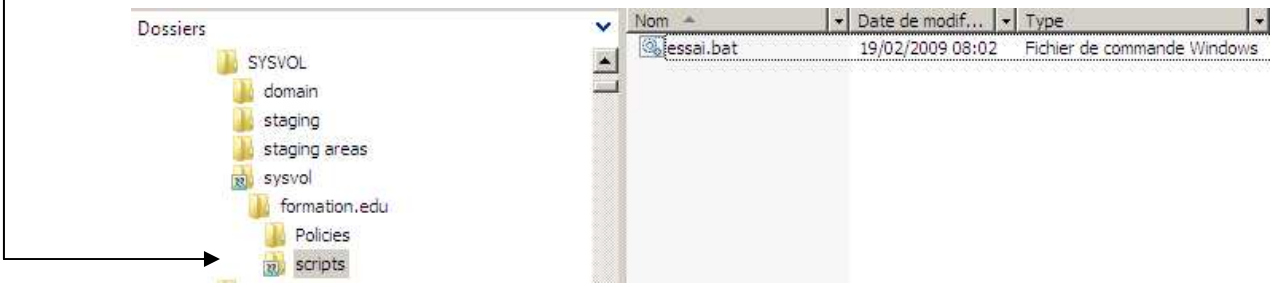
Objectif :

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

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

Pour les ordinateurs clients, le chemin d'accès du script d'ouverture de session sur un serveur 2008-2003 est **Winnt\Sysvol\sysvol\domaine\scripts**.

(sous NT4.0 server le chemin était généralement **Winnt\System32\Repl\Import\Scripts**.)



N.B: sous 2008-2003, les client SEVEN et XP peuvent recevoir en plus à l'ouverture de session, une notion de stratégie. Ce qui fait que si un client est une machine windows95-98, ou NT 4.0, on ne peut travailler **qu'avec des scripts** (les stratégies SEVEN, Xp ou 2000 ne marcheront pas pour ces clients).

Donc si un client est un poste SEVEN, Xp ou 2000, alors celui-ci récupère lors de l'ouverture de session **les scripts et les stratégies**…

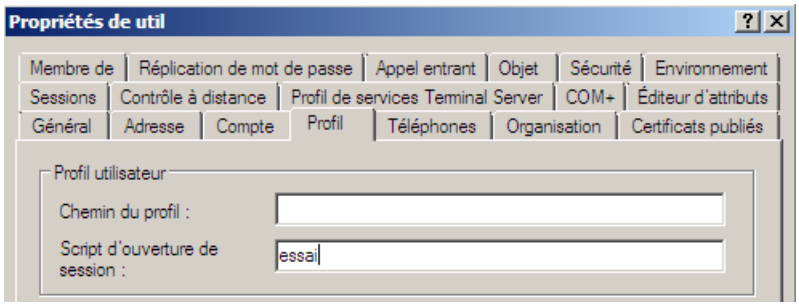
N.B : Si enfin, on utilise des stratégies sous NT4.0, (avec poledit), ces stratégies sont récupérées par les versions NT4.0, mais ne sont pas récupérées par les clients SEVEN ou Xp…. Heureusement !

Indiquer un script d'ouverture de session :

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

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

essai



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

Ecriture de scripts :

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

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

création de lecteur logique

commande de base

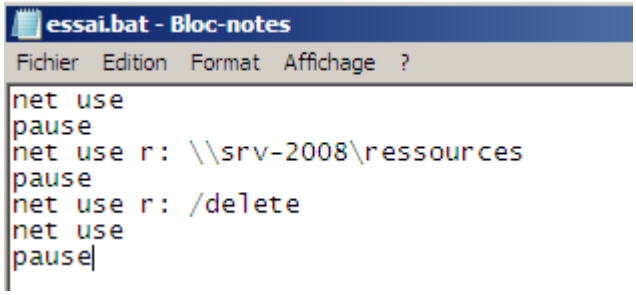
net use x: /home

ou

net use x: \\nomposte\nompartage

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

voici un exemple de script permettant de visualiser, créer, et effacer un lecteur réseau



COMMANDE NET

Convention d'écriture :

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

- Les mêmes conventions que pour NTBACKUP sont utilisées:

Ainsi, la ligne de syntaxe ci-dessous :

NET COMMANDE [nom] {OPTION1 | OPTION2}

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

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

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

Commandes NET Utilisables :

Les commandes utilisables avec la commande Net sont :

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

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

Pour plus de renseignement sur la syntaxe on peut taper

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

exemple

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

Net Use :

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

Les paramètres utilisables avec la commande Net USE sont :

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

ou

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

ou

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

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

Net Send :

Disponible uniquement sur les postes Windows XP-2000-NT, retiré sous les postes SEVEN

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

Paramètres

nom

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

N.B : on parle ici de nom NetBios !

*****

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

/domain[**:***nom*]

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

/users

Envoie le message à tous les utilisateurs connectés au serveur.

message

Spécifie le texte du message à envoyer

Si le service de Messagerie est démarré (normalement il l'est en automatique sous 2000, mais non sous XP)

net send nomposte "message"

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

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

amène alors

net send /users "message"

permet d'envoyer un message à tous les utilisateurs connectés

Net User

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

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

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

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

Paramètres

Aucun

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

net users ou net user →

```
C:\>net users

comptes d'utilisateurs de \\SERVEUR1

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

nom_utilisateur

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

net users compte ou

net user compte →

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

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

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

Heures d'accès autorisé                 Tout

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

mot_de_passe

Assigne ou modifie le mot de passe du compte d'utilisateur.

*

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

/domain

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

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

/add

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

/delete

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

Net view:

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

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

net view /network:nw [*nom_ordinateur*]

Paramètres

Aucun

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

nom_ordinateur

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

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

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

PROFILS SEVEN - XP

Objectif :

Les profils d'utilisateur présentent plusieurs avantages :

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

Les profils permettent de mémoriser notamment les paramètres suivants:

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

Les profils peuvent être stockés sur un serveur afin d'être en mesure de suivre les utilisateurs sur n'importe quel ordinateur exécutant la plate-forme Windows SEVEN-XP sur le réseau.

Evidemment le mélange de profils selon les OS est déconseillé… comment gérer un profil SEVEN sur une machine 2000 et qui repartirait sur un poste XP ?

Dans un premier temps, si on gère les profils, on gèrera des profils entre machines ayant même système client Windows…

Les différents Profils:

Les profils d'utilisateur existent sous plusieurs forment

Profil local :

C'est le profil créer automatiquement par défaut pour chaque utilisateur qui ouvre une session sur un poste. Il prend alors le nom de **Profil Local**.

Le profil local peut être créé à partir :

- D'un profil local par défaut (modèle) stocké sur la machine, dans un dossier **Default User** (sous XP) ou **Default** (sous SEVEN)
- D'un profil par défaut de réseau si cette fonction est mise en place sur le serveur CD et que le client est un client SEVEN.
- A partir d'une copie stockée sur le serveur (cf profil errant)

Profil par défaut local :

Lorsque on ouvre une session de domaine sur un client SEVEN ou Xp, Si aucun profil local existe, le nouveau profil est créé à partir du profil local par défaut, stocké en **Default User** (sous XP) ou **Default** (sous SEVEN)

Profil par défaut de réseau :

Lorsque on ouvre une session de domaine sur un client SEVEN, SEVEN essaye de trouver un profil par défaut de réseau sur le serveur.

Si ce profil existe, il est chargé et devient le profil local de l'utilisateur,

Si ce profil n'existe pas, le profil par défaut de la machine locale devient le profil local de l'utilisateur

Profil itinérant :

Fondamentalement une copie du profil local est stockée sur le serveur. Cette copie est utilisée ensuite lorsque l'utilisateur ouvre une session sur une autre machine pour créer le profil local.

Lors de la fermeture de session, les éventuelles modifications apportées au profil sont sauvées sur le serveur, pour être récupérables lors de la prochaine ouverture de session.

Profil obligatoire :

Il s'agit d'une variante du profil itinérant, dans laquelle toute modification du profil en cours est possible, mais aucune enregistrement ne se fait en fin de session. Par conséquent on est sûr du profil que l'on transmet – récupère la prochaine fois !

Profil super-obligatoire :

Il s'agit d'une variante du profil obligatoire. dans laquelle si, pour une raison ou une autre, on ne peut pas récupérer le profil lors de l'ouverture de session, la session est impossible !

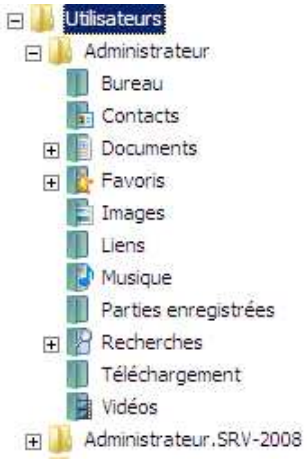
Profils Locaux SEVEN:

Par rapport aux profils XP, les différences suivantes existent :

- Le dossier Racine des profils devient « visuellement » le dossier **\Utilisateurs** (selon la regionalisation française) mais se trouve être le dossier **\users** (anciennement **\Document and Settings)**

```
C:\>dir /al
 Le volume dans le lecteur C n'a pas de nom.
 Le numéro de série du volume est 144A-3A67

 Répertoire de C:\

19/01/2008  15:23    <JONCTION>     Documents and Settings [C:\Users]
               0 fichier(s)                0 octets
               1 Rép(s)   8 068 775 936 octets libres
```

- Les préfixes **mes** et **ma** sont supprimes des dossiers **document** ou **musique** (à la place de **mes document** ou **ma musique**
- Les dossiers **document** ou **musique…** ne sont plus des sous-dossiers du dossier mes documents, mais sont directement crées à la racine du dossier profils (en quelque sorte remise à plat de l'arborescence…)
- Des nouveaux dossiers apparaissent dans le profil



Nouveau dossier dans un profil sous SEVEN

Contacts
Liens
Parties enregistrées
Téléchargement
Recherches

Lles noms des dossiers physiques ne correspondent pas forcément

```
<REP>          Contacts
<REP>          Desktop
<REP>          Documents
<REP>          Downloads
<REP>          Favorites
<REP>          Links
<REP>          Music
<REP>          Pictures
<REP>          Saved Games
<REP>          Searches
<REP>          Videos
```

Noms réels « hors régionalisation » du gestionnaire de fichier SEVEN

En plus de un dossier par profil, il existe d'autres dossiers

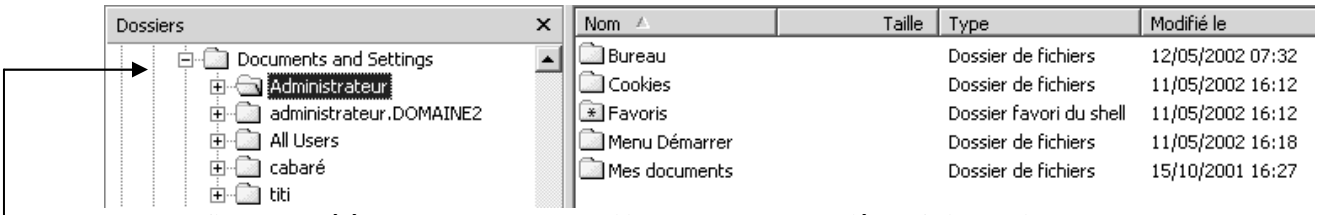
Le dossier **Default** correspondant au dossier **Default User** sous XP contient le profil par défaut

Le dossier **Public** correspondant au dossier **All User** sous XP contient uniquement les paramètres fusionnés avec tous les autres profils, car les donnée d'applications (qui y étaient stockées sous XP) sont désormais redirigées dans le dossier **ProgramData**

```
C:\Users>dir /al
 Le volume dans le lecteur C n'a pas de nom.
 Le numéro de série du volume est 144A-3A67

 Répertoire de C:\Users

19/01/2008  15:23    <SYMLINKD>     All Users [C:\ProgramData]
19/01/2008  15:23    <JONCTION>     Default User [C:\Users\Default]
```

Rappels Profils Locaux XP-2000:

Depuis Windows 2000, les profils d'utilisateur créent et conservent automatiquement des paramètres et des données chaque utilisateur.



Un profil est créé pour chaque utilisateur la première fois qu'il ouvre une session sur un ordinateur 2000-XP et est stocké automatiquement dans un dossier **Document and Settings** du disque sur lequel l'OS est installé, (sous NT4.0 il était stocké dans **Winnt\Profiles**).

Il existe au minimum 2 dossiers nommés :

All Users

Default User

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

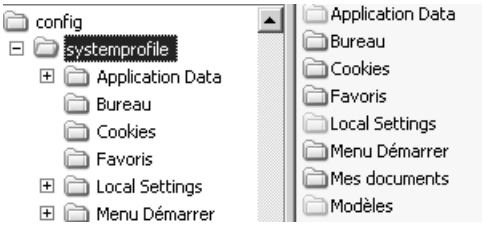
leur signification est la suivante :

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

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

Sous XP deux dossiers supplémentaires **localservice** et **Networkservice** sont crées pour gérer l'hébergement de services qui ne nécessiteraient pas d'être programmés en tant que service système interne…

Cependant ces deux profils sont gérés par Xp et n'apparaissent pas parmi les profils gérables du poste de travail…



De même un nouveau profil existe pour le système stocké en **system32/config/systemprofile**

Différence entre 2000 et XP :

Il existe des différences entre un profil 2000 et un profil XP, et de l'aveu même de Microsoft, il y aurait des risques d'effet de bords à récupérer un profil XP à la place d'un profil 2000

- Mais on n'a pas la possibilité de différencier les profils 2000 des profils XP, ceux-ci sont stockés et gérés de manière identique
- Alors que bien sur les profils Nt4 et 9x sont différentiables.

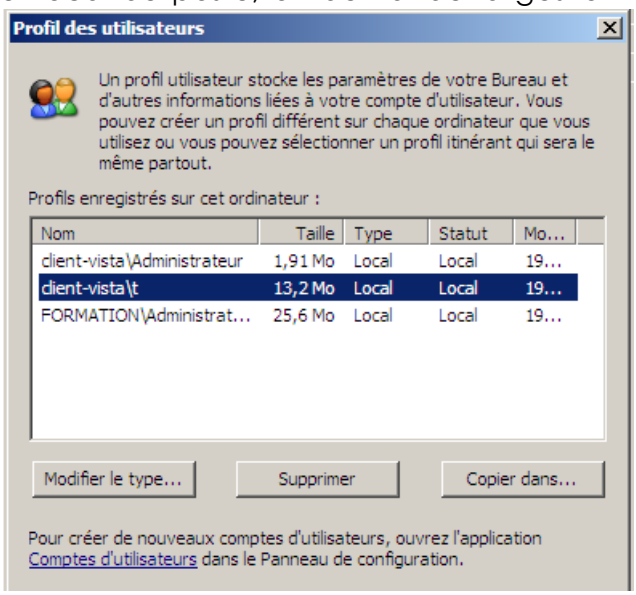
Il serait souhaitable d'utiliser des profils sur des systèmes identiques…

Profils par défaut local :

Pour créer un **profil local par défaut**, qui prépare l'environnement pour un utilisateurs à venir, le plus simple consiste à créer un utilisateur temporaire (ici par exemple nommé t…) , ouvrir une session avec et créer simplement le profil voulu…

Ensuite en tant que administrateur local du poste, on demande la gestion des profils, via

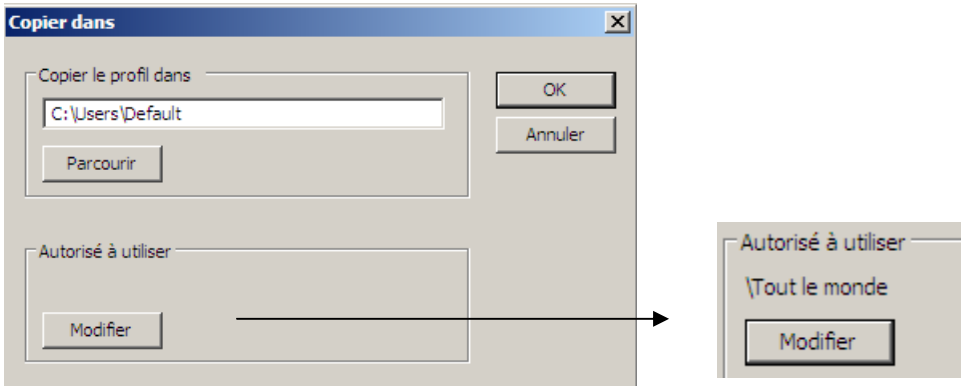
Propriétés de Ordinateur/ Paramètres systèmes avancés / profils des utilisateurs,



On choisit le profil qui va devenir notre « profil par défaut »

Et on demande **Copier dans…**

Il faut chosir le dossier **C:\Utilisateur\Default**, soit en fait **C:\Users\Default**

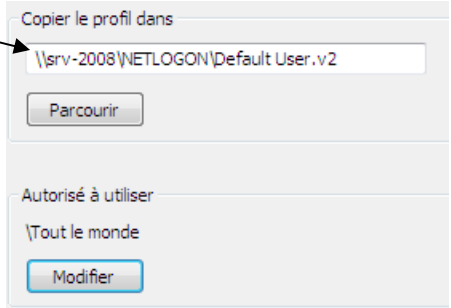


N.B : Il faut bien penser à indiquer Tout le monde comme identifiant autorisés à utiliser ce profil.

Profils par défaut réseau :

Le principe est de copier un profil local par défaut, dans le dossier **netlogon** du serveur, sous une appellation bien particulière

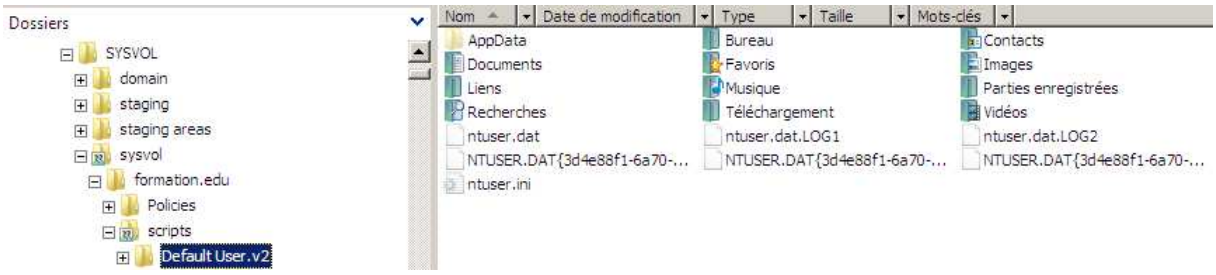
Default User.v2



Après création du futur profil par défaut de réseau sur un poste, il faut ouvrir une session sur ce poste an tant qu'administrateur de domaine, et copier ce profil dans le dossier

Netlogon\Default User.v2, et donner les autorisations à **Tout le monde**

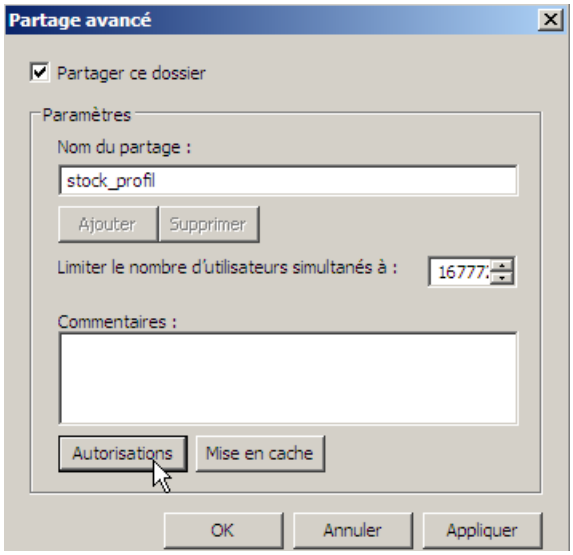
Ce qui devrait sur le serveur donner



N.B: pour des profils réseau par défaut pour des clients XP, le nom du dossier créé ne comporte pas **.V2,** et donc on crée simplement **Netlogon\Default User**

Configurer Les Profils Errant sur le Serveur:

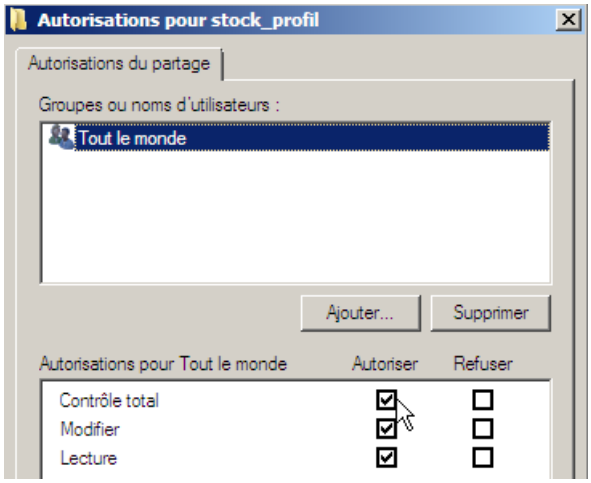
Contrairement au **profil local**, qui mémorise l'environnement pour un utilisateurs selon la machine sur laquelle il se connecte, un **profil errant** donne toujours le même environnement de travail pour l'utilisateur, quelle que soit la machine sur laquelle celui-ci se logue.



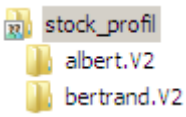
Ce profil errant doit être enregistré de manière centralisée sur le serveur. Par exemple créons un dossier nommé **stock_profil**

Les permissions de sécurité par défaut de 2008 conviennent

et partageons le pour tous les utilisateurs en **contrôle total**.



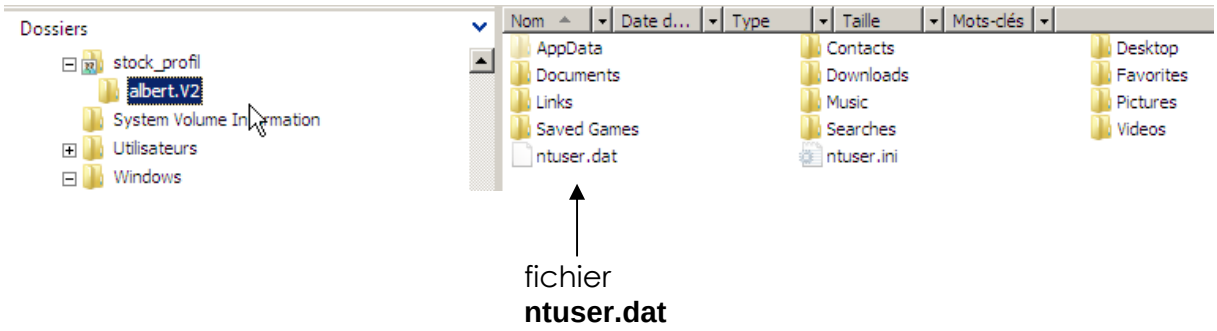
Si on prévoit de gérer les profils pour **Albert** et **Bertrand** on aura a terme un sous-dossier par profil errant stocké, du nom de l'utilisateur suivit de **.v2** .



N.B: le nom du dossier dans lequel on stocke les profils importe peu…

N.B: si on veut cacher ce dossier, on peut faire terminer son nom par **$**

Dans chacun de ces dossiers, on retrouvera le profil, ainsi qu'une copie de la base de registre des modifications (après 1 connexion/déconnexion …)



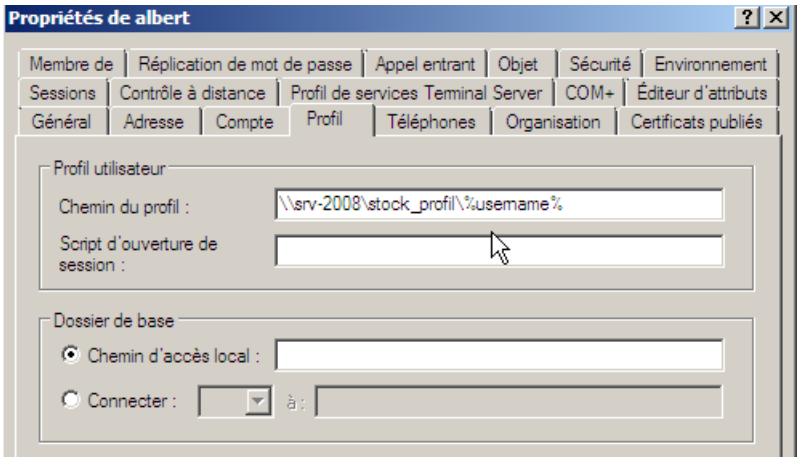
N.B: pour des profils XP, le nom du dossier créé ne comporte pas **.V2**

Configurer Les Profils Errant pour les comptes Utilisateurs:

Il suffit d'ajouter un chemin de profil d'utilisateur à chaque compte d'utilisateur, pour créer automatiquement le dossier de profil d'utilisateur vide (nommé pour cet utilisateur à l'emplacement prévu du serveur)

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

- Sur le compte utilisateur pour lequel on veut gérer le profil, demander **propriétés**, onglet **Profil** la boite de dialogue



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

  \\Serveur\Dossier\nomprofil

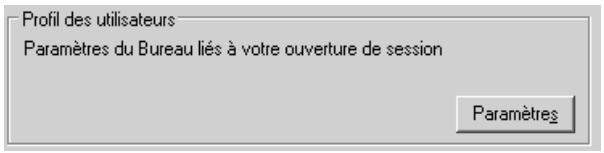
  avec **Serveur** : le nom du serveur NT sur lequel les profils sont enregistrées (ici **srv-2008**)

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

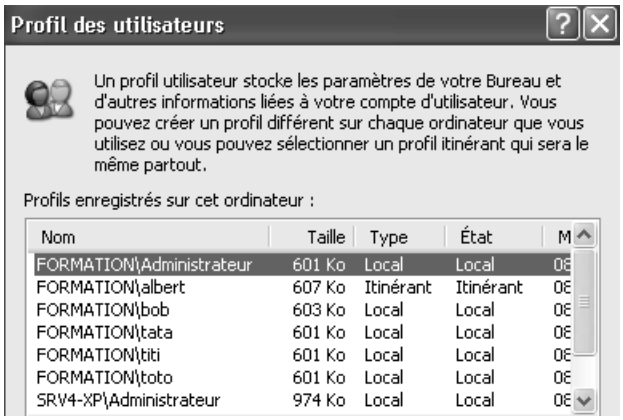
  avec **nomprofil** : le nom d'utilisateur défini pour le compte Utilisateur (ici **albert**)
  Il serait bien sûr plus intéressant de mettre ici **%username%** (pour pouvoir copier ce compte…)

Suppression Profil errant sur un poste client:

Dans **Poste de travail / Propriétés** l'onglet **Avancé** puis **Profil utilisateurs**

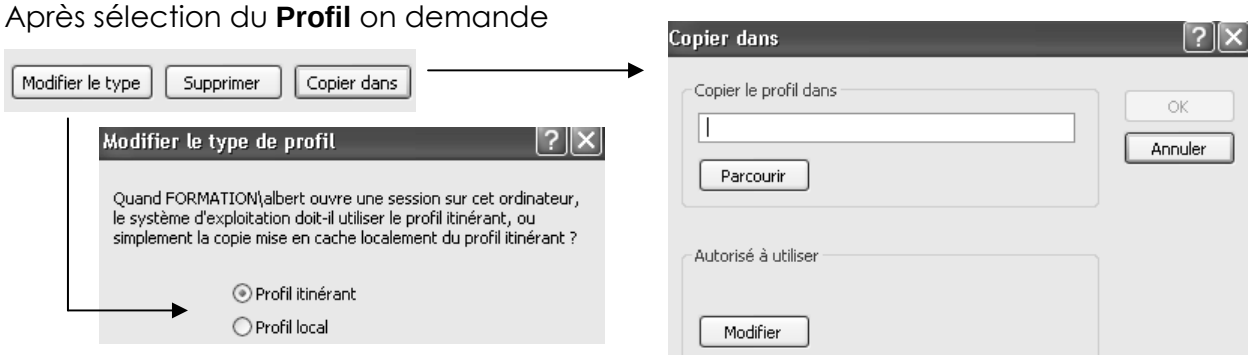


On obtient alors



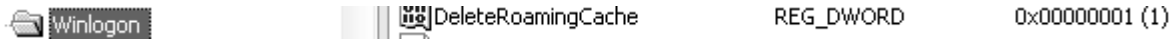
On peut voir si un profil est **local** ou **itinérant**

Après sélection du **Profil** on demande



N.B : Sur tous les postes sur lesquels on l'on ne souhaite pas garder une copie des profils errants, on peut effectuer une modification de la base de registre. Dans la clé **HKLM/Software/Microsoft/WindowsNT/CurrentVersion/Winlogon**

On crée une nouvelle valeur de type DWORD avec la valeur **DeleteRoamingCache = 1**



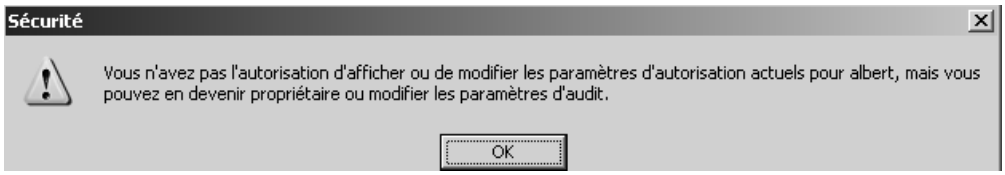
Suppression Profil errant stocké sur le serveur:

Fondamentalement il s'agit de supprimer le dossier homonyme de l'utilisateur, ainsi pour supprimer le profil d'albert, il suffirait de supprimer le dossier **albert** dans le dossier général **stock_profil**

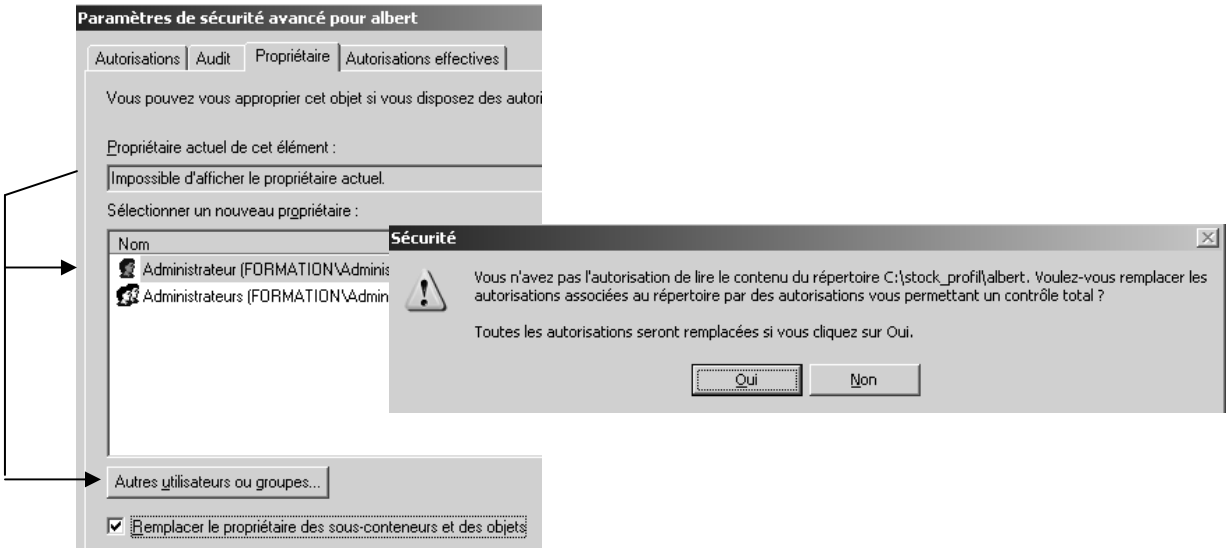
Mais ce n'est pas si simple, car la sécurité NTFS est posée par défaut sur un profil de manière à ce que uniquement l'utilisateur puisse accéder à son profil.

Il faut donc pour pouvoir effacer ce dossier, d'abords approprier le dossier Albert et tous son contenu

Lorsque l'on sélectionne le dossier



Il faut demander **Paramètres Avancés…**, onglet **Propriétaire**



Supprimer tous les profils locaux d'une machine:

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

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

voilà quelques paramètres d'appel :

Delprof /p	Demande confirmation pour chaque profil
Delprof /d:3	Ne traite que les profils vieux de plus de **3** jours. Si omis tous les profils sont traités
Delprof /q	Ne demande pas de confirmation pour s'exécuter au départ
Delprof /c:\\nom	Permet d'indiquer le **nom** de la machine sur laquelle on veut supprimer les profils locaux

Ainsi par exemple la ligne de commande

Delprof //p /c:\\nom permet de supprimer tous les profils locaux de la machine nom, en demandant confirmation pour chacun d'eux.

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

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

Profil Errant obligatoire (mandatory) :

Deux types de profils errant existent :

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

IL faut renommer le fichier **Ntuser.dat** en **Ntuser.man** dans le profil d'utilisateur spécifié.

Un profil d'utilisateur obligatoire sera alors créé des que on renomme le fichier **Ntuser.dat** en **Ntuser.man** dans le dossier du profil d'utilisateur

De manière analogue, renommer le fichier **Ntuser.man** en **Ntuser.dat** permettra à l'utilisateur de modifier de nouveau son profil.

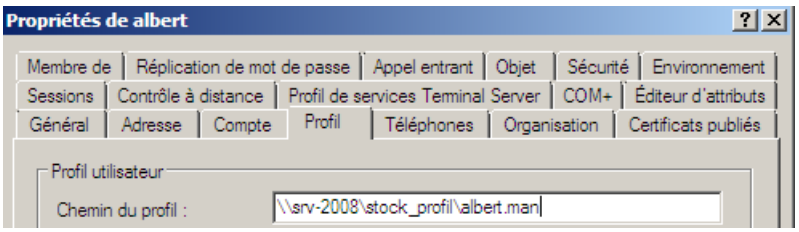
N.B : si la sécurité NTFS est présente sur le disque ou les profils errants sont stockés, alors elle ne vous laissera pas forcément travailler librement…

N.B : lors de l'appropriation des objets en NTFS, ne pas confondre **Administrateur** (local) et **Admins de Domaine** dans les droits !

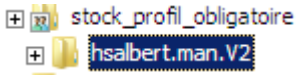
Profil Errant Super obligatoire SEVEN:

Si on veut en plus que lorsque (pour une raison ou une autre) le profil obligatoire ne puisse pas être chargé, alors l'ouverture de session soit refusée, il faut créer un profil super-obligatoire. Ces profils Super-obligatoires doivent être enregistrés de manière centralisée sur le serveur dans un dossier comportant **.man**

- Ainsi par exemple créons un dossier nommé **stock_profil**
- Une fois le profil obligatoire stocké dedans (avec renomage de user.dat en user.man)
- Il faut renommer le dossier profil utilisateur de **\albert.v2**en **\albert.man.v2**
- Et Sur le compte utilisateur pour lequel on veut APPLIQUER le profil, demander **propriétés**, onglet **Profil** la boite de dialogue



Pour tester, on renomme le dossier qui contient le profil obligatoire d'albert en hsalbert.man.v2



…on ne peut plus ouvrir de session avec albert !

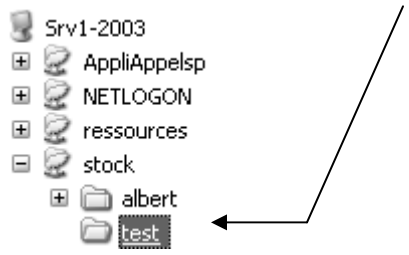
Copie de profil local en errant :

Le principe est basé sur un mélange des deux techniques, copier un profil local, et mettre en place les profils errants

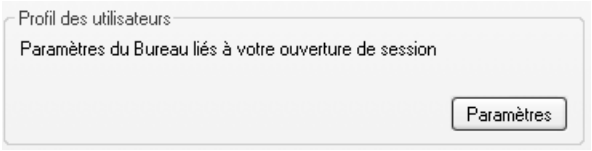
Au préalable sur un poste on ouvre une session et on crée un profil type avec un utilisateur **test** crée pour l'occasion

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

se préparer un dossier de stockage sur le serveur



sur le client, il faut demander la gestion des profils

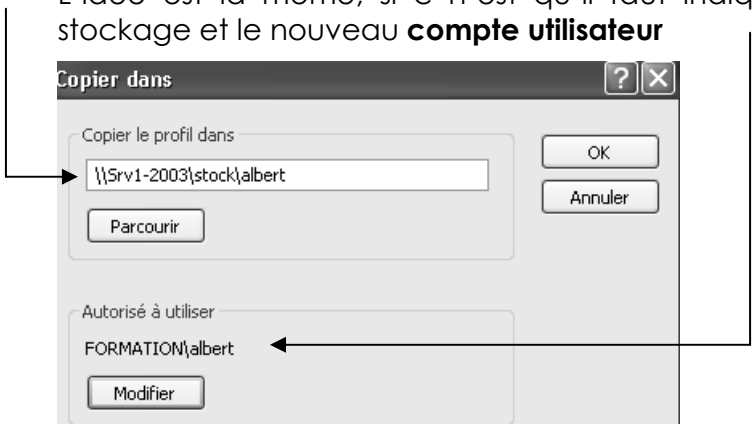


pour le profil **test** on demander **Copier dans**

On indique l'endroit préparé sur le serveur et on spécifie l'utilisateur

Transfert de profil local sur un autre profil :

L'idée est la même, si c n'est qu'il faut indiquer le nouveau dossier de stockage et le nouveau **compte utilisateur**



N.B : la situation peut se compliquer cependant si des documents existent dans les profils, auquel cas on risque très vite de ne plus rien comprendre

Horodatage et profils :

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

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

Une synchronisation correcte à l'intérieure du domaine est capitale

Logique de gestion des profils :

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

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

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

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

N.B: Les profils peuvent aussi se gérer via les stratégies, notamment via

Configuration d'ordinateur \ Modèles d'administration\ système\ profils des utilisateurs

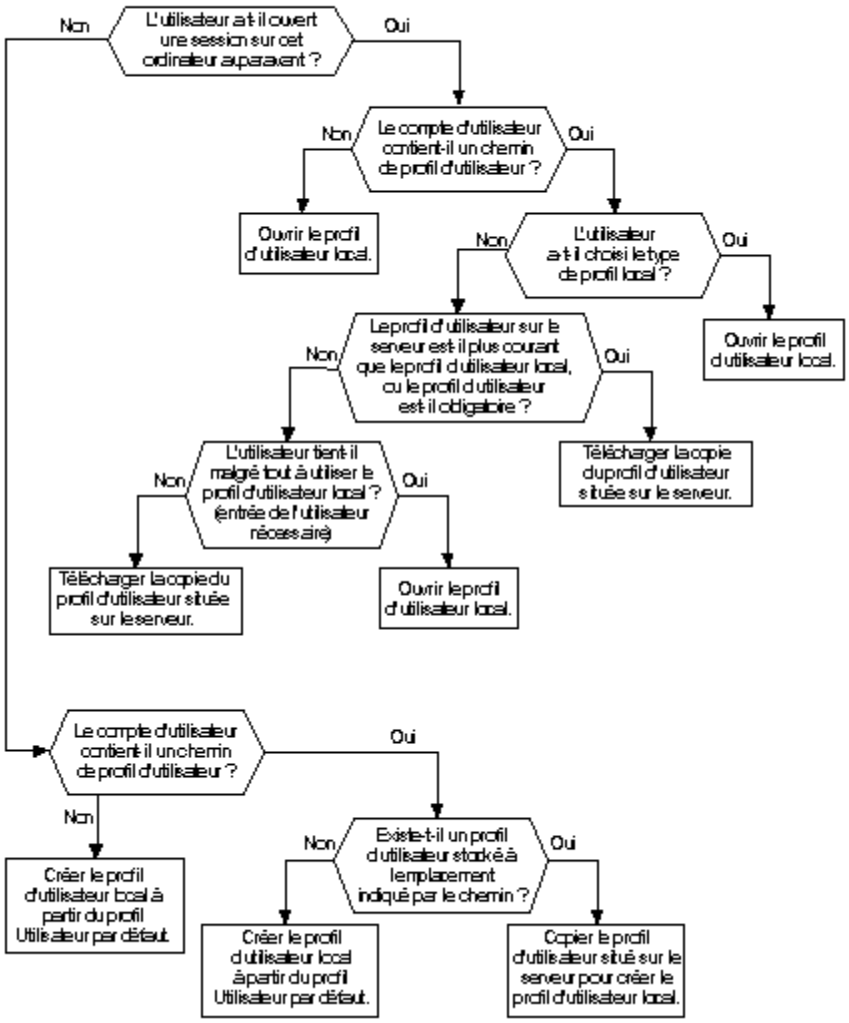
Et aussi

Configuration utilisateurs \ Modèles d'administration\ système\ profils des utilisateurs

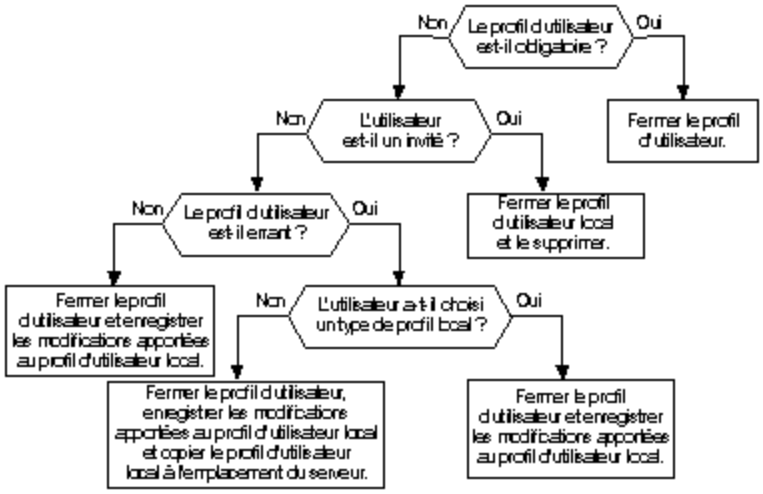
Logigramme gestion des profils :

Hors Profil Réseau par défaut…

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



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



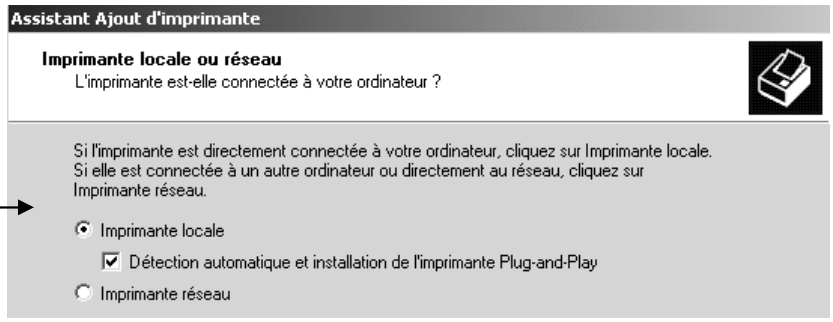
IMPRIMANTE RESEAU

Installer une imprimante réseau :

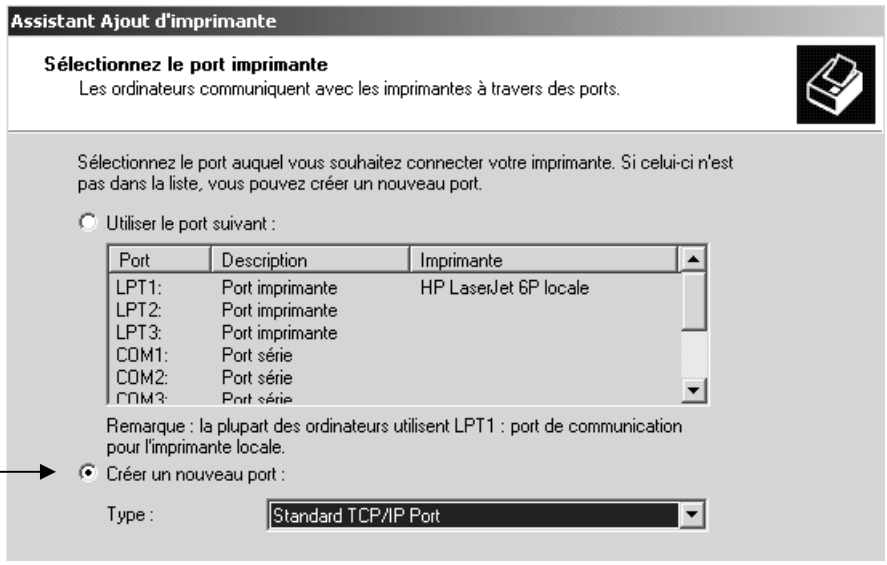
L'installation d'une imprimante réseau utilisant le protocole TCP/IP, ou d'un imprimante classique reliée à un boitier serveur d'impression utilisant TCP/IP comme protocole (boitier déjà configuré) est simple

Il faut demander dans le menu **Démarrer / Paramètres / Imprimantes** (ou dans le panneau de configuration) l'assistant **Ajout d'imprimante**…

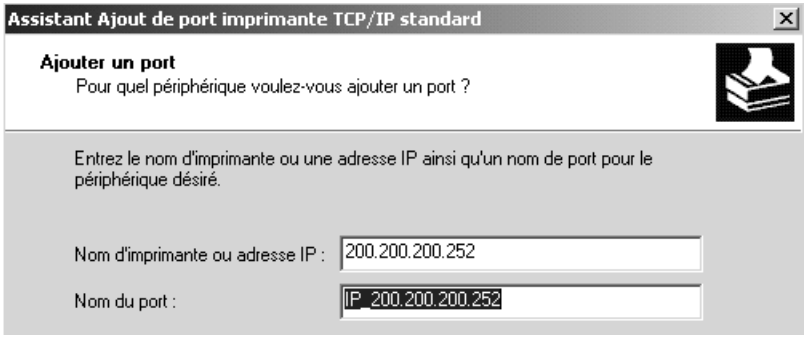
Il faut demander locale,



Mais en sélectionnant un port standard impression TCP/IP



Bien sûr il faut alors rentrer les paramètres TCP/IP de l'imprimante-boitier

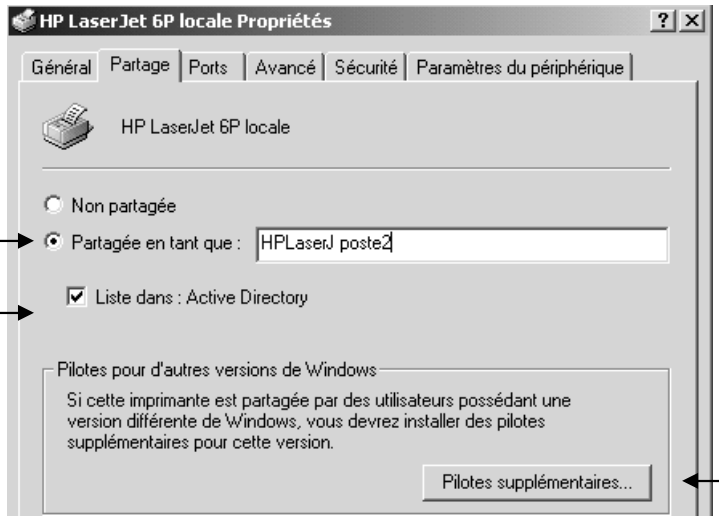


et c'est terminé !

Partager une imprimante locale / réseau:

L'imprimante étant installée, on la partage classiquement en la sélectionnant, et en demandant **partager** dans le menu contextuel

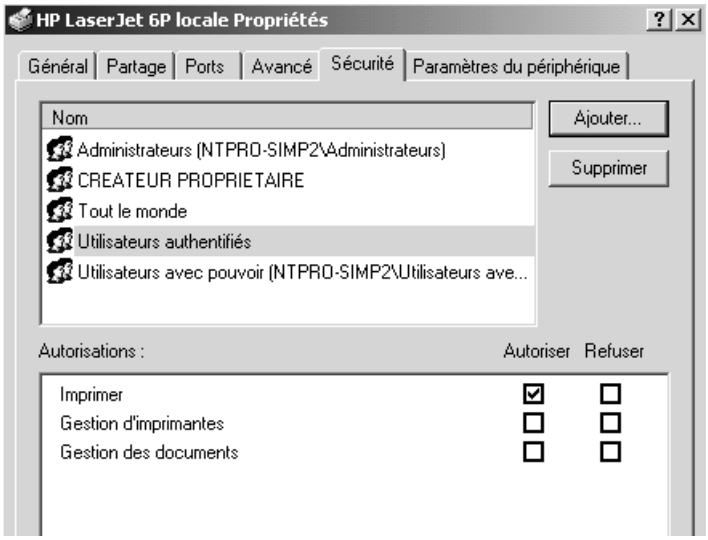
Nom de partage vu par ceux qui souhaiterons l'utiliser



Inscription dans Active Directory

Installation possibles de pilotes pour demandes d'impression depuis win95 ou NT4.0

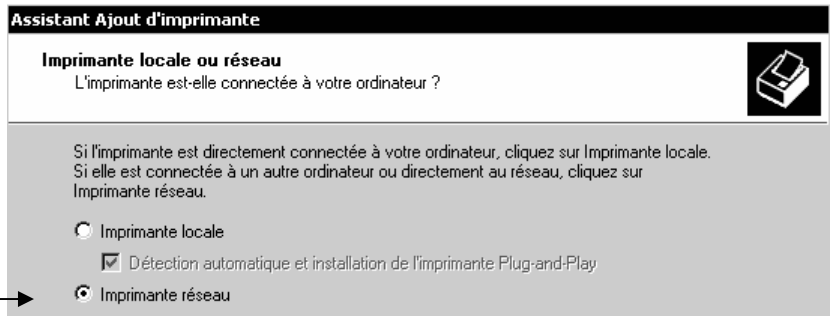
Ensuite en demandant propriété on peut gérer les autorisations de partage



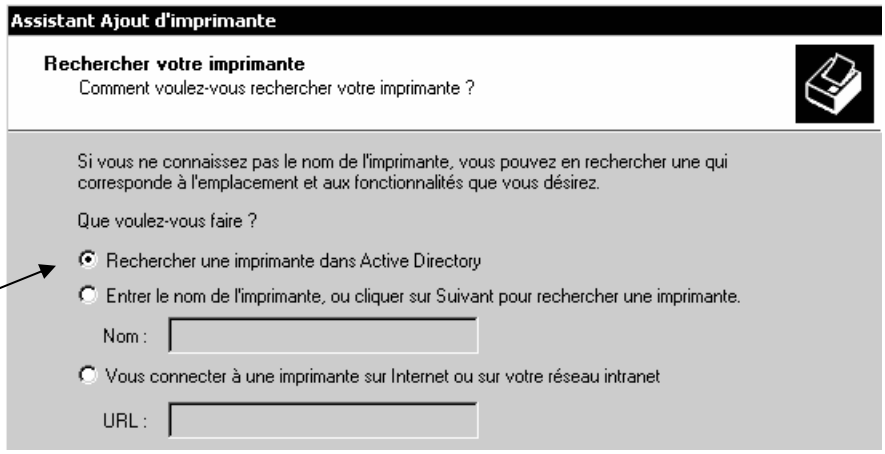
Accéder à une Imprimante déjà installée sur le réseau :

Il faut demander dans le menu **Démarrer / Paramètres / Imprimantes** (ou dans le panneau de configuration) l'assistant **Ajout d'imprimante**…

Il faut demander réseau,



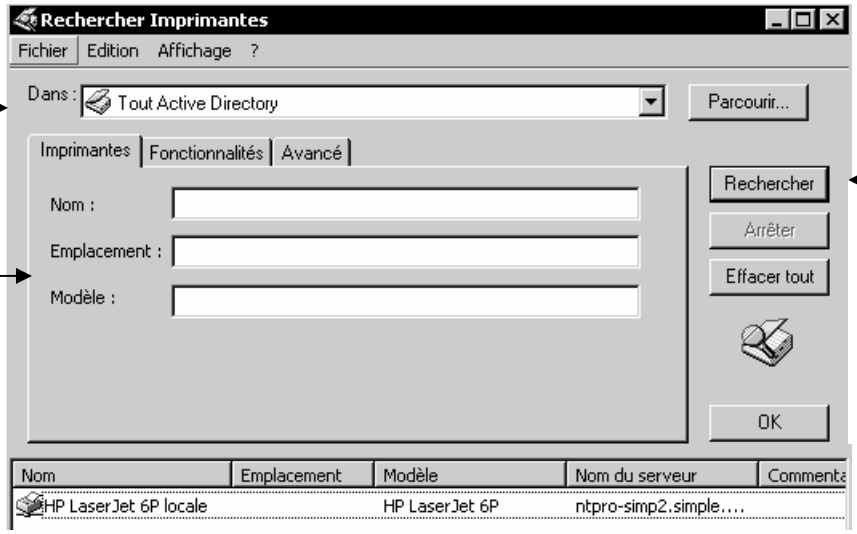
Si cette imprimante été inscrite dans Active Directory lors de son installation on peut alors demander



on obtient alors la boite de dialogue suivante

On précise où l'on cherche

Avec éventuellement des critères



Puis on demande Rechercher

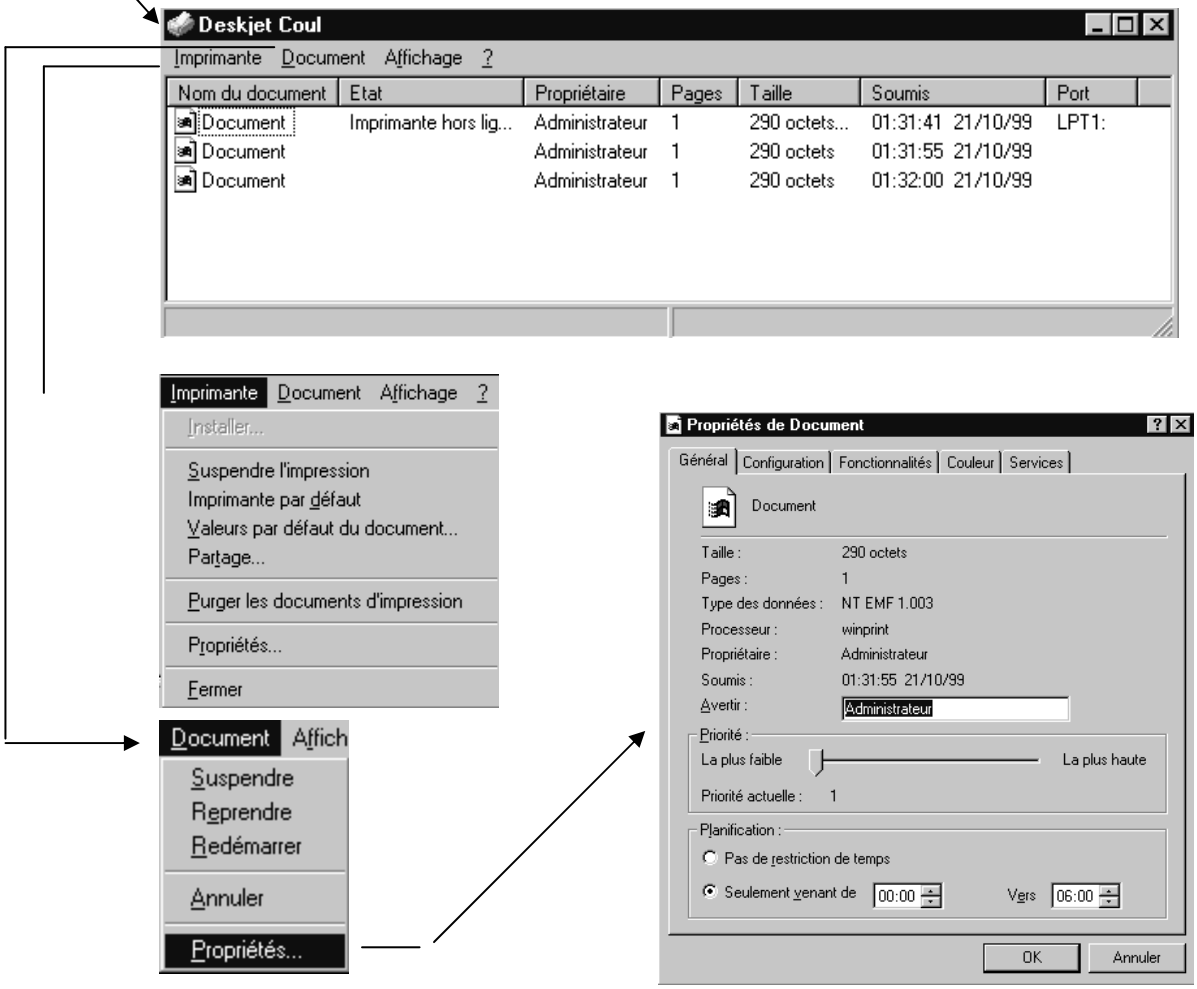
Il ne reste plus qu'à effectuer son choix dans la liste et demander OK

GERER UNE IMPRIMANTE RESEAU

Gestionnaire d'impression:

Quand un document est envoyé en file d'attente, il est donc "spooler" sur le disque dur de l'ordinateur sur lequel est présente l'imprimante logique. Ce fichier de Spool peut augmenter de manière conséquente et ralentir d'éventuels autres travaux sur cette machine

Chaque imprimante est associée à une file d'attente qui est gérée par le **gestionnaire d'impression**. Il suffit de double cliquer sur l'icône de l'imprimante dont on veut visualiser les files d'attente



N.B : lorsque une impression est en cours, le gestionnaire d'imprimante est disponible directement dans la barre des tâches

Autorisation sur Imprimante:

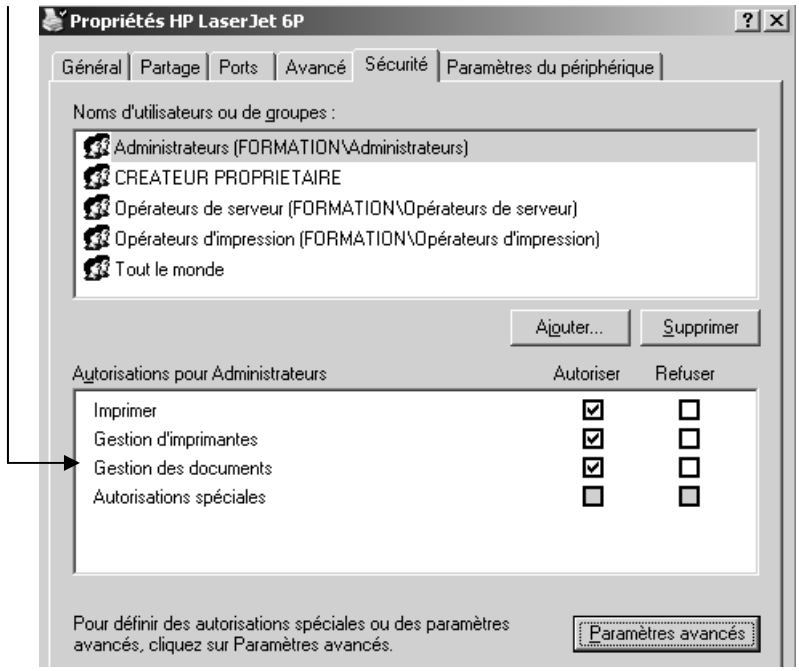
L'imprimante est un objet sur lequel on peut définir de la sécurité, en terme de qui à le droit de faire quoi…

Simplement par rapport aux Autorisations que l'on peut définir sur de dossiers ou des fichiers, il y a essentiellement 3 type autorisations

Gestion d'imprimantes

Gestion de document

Imprimer

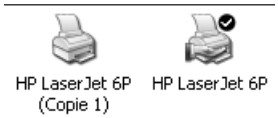


Windows affecte des autorisations d'imprimante à six groupes d'utilisateurs de la manière suivante :

Groupe	Imprimer	Gestion des documents	Gestion d'imprimantes
Administrateurs	X	X	X
Propriétaire créateur		X	
Tout le monde	X		
Utilisateurs avec pouvoir	X	X	X
Opérateurs d'impression	X	X	X
Opérateurs de serveur	X	X	X

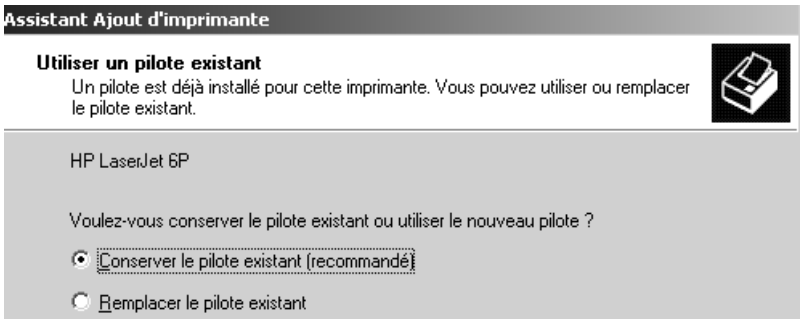
Plusieurs imprimante sécurisées différemment :

Il peut être intéressant de créer diverses imprimantes « logiques » pointant vers le même périphérique physique.



Cela permet une mise en place de paramétrages divers, clairement identifiables et… non modifiables !

Pour installer ces « copies » on procède comme si on installait un imprimante quelconque, puis on demande de **Conserver le pilote existant**



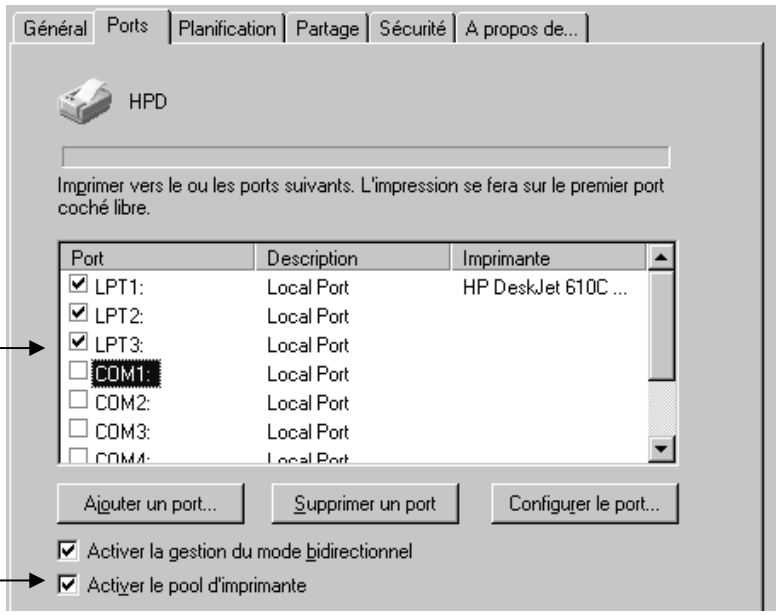
Il ne reste plus qu'a paramétrer chaque imprimante normallement

---

Pool d'imprimante:

Si plusieurs imprimantes sont identiques, ou du moins peuvent être pilotées par le même driver (voire en émulation…), créer un **Pool** d'imprimante fait que les documents à imprimer se répartissent automatiquement sur la première imprimante disponible du Pool, en assurant ainsi un flux régulier sans que l'utilisateur ait un choix à effectuer

Cela permet également un entretient ou une réparation d'une imprimante sans que le fonctionnement global soit perturbé

Un Pool de 2-3 imprimantes dans une pièce spécifique permet parfois un fonctionnement plus harmonieux qu'une seule imprimante plus puissante, dont l'arrêt peut paralyser toute l'activité

Il suffit de cocher les ports sur lesquels sont reliées les imprimantes faisant partie du Pool, de la plus rapide à la moins rapide…