http://WWW.CABARE.NET ©

Installation Réseau Serveur Windows 2008 & 2008 R2 – sys 22 – Travaux Pratiques

Installer serveur 2008 windows

Michel Cabaré – Ver 2.3 – juin 2010-

Installation réseau Serveur Windows 2008 & 2008R2
Travaux Pratiques

Michel Cabaré – Ver 2.3 – Juin 2010

www.cabare.net ©

TABLE DES MATIÈRES

DESACTIVER STRATEGIE MOT DE PASSE COMPLEXE

Probleme:

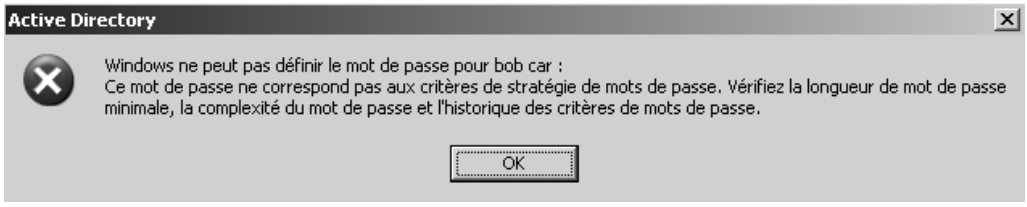
Par défaut sur un serveur 2003 une stratégie existe à propos des mots de passe, obligeant toute création à respecter les règles de complêxitée.

Ainsi la création d'un utilisateur

Login :**bob**

Pswd :**b**

Se voit refusée



Ces règles demandent à ce que par défaut un mot de passe :

- Contienne plus de 7 caractères
- Contienne au moins une minuscule, une majuscule, un chiffre, un signe de ponctuation
- Ne contienne pas le nom de l'utilisateur auquel il permet d'accéder

Dévalidation:

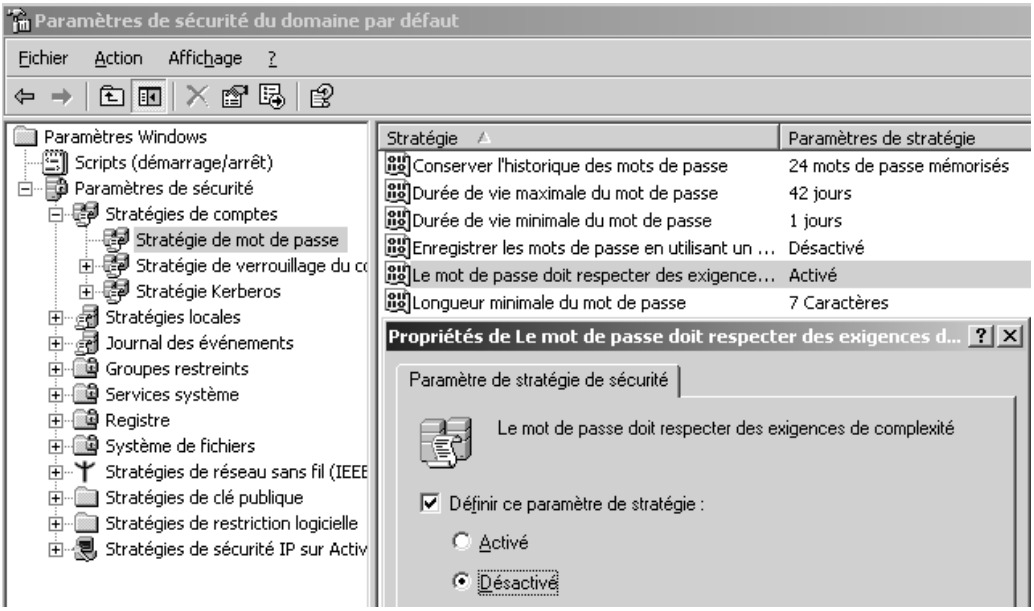
Sans rentrer dans le probleme des stratégies, pour travailler simplement, et toujours créer les login simple, on va dans

Outils d'administration /Stratégies de sécurité du domaine

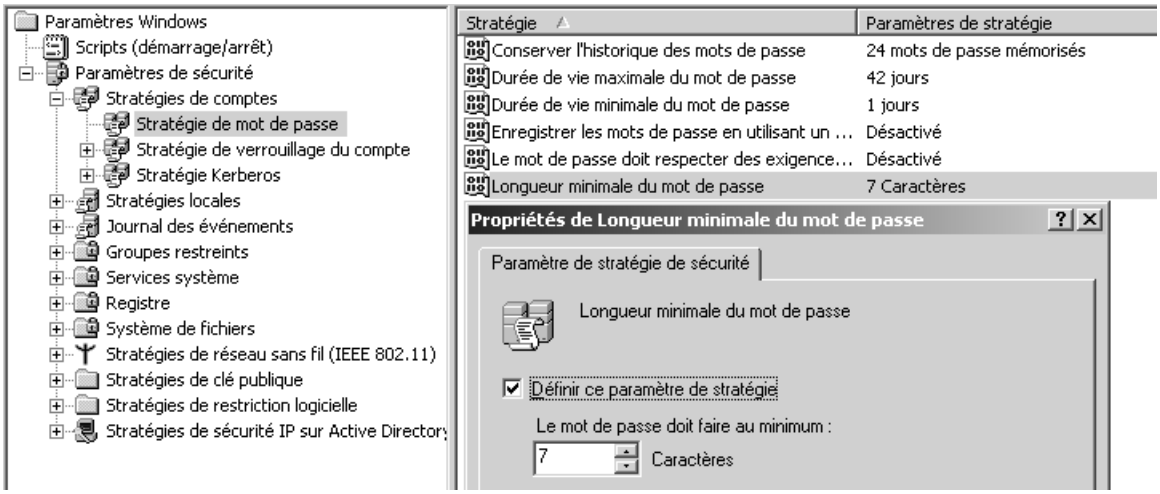
Dans **Paramètres windows / Paramètres de Sécurité / Stratégies de Compte / Stratégies de mot de passe**

On demande alors

Le mot de passe doit respecter des exigences de complexité



Longueur minimale du mot de passe



Suivit de **gpupdate /force**

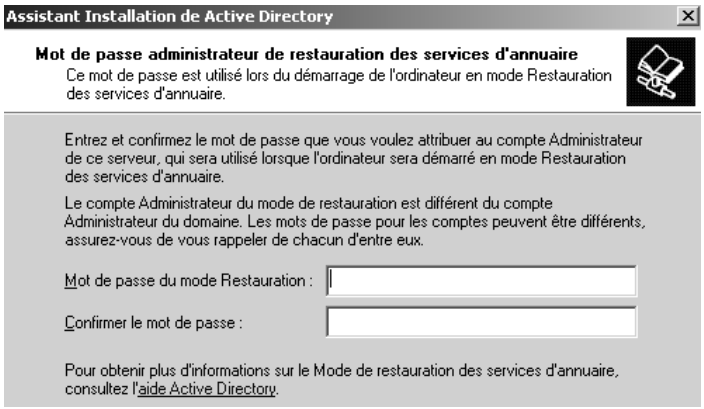
```
C:\Documents and Settings\Administrateur.SRV1-2003>gpupdate /force
Actualisation de la stratégie...

L'actualisation de la stratégie utilisateur s'est terminée.
L'actualisation de la stratégie ordinateur s'est terminée.

Pour vérifier des erreurs dans le traitement de la stratégie, consultez
l'Observateur d'événements.
```

CHANGEMENT MOT DE PASSE RESTAURATION AD

Perte mot de passe Restauration AD 2008:

Le mot de passe de restauration des services d'Annuaire qui est défini lors de l'installation d'un CD (et uniquement à ce moment là…)

A été perdu **Il faut le rétablir…**



En invite de commande on tape la commande **ntdsutil**

```
C:\Documents and Settings\Administrateur.SRV1-2003>ntdsutil
ntdsutil:
```

A l'invite de ntdsutil, on tape la commande **set DSRM password**

```
ntdsutil: set DSRM password
```

A l'invite de DSRM on tape la commande **reset password on server null**

```
Redéfinir le mot de passe administrateur DSRM : reset password on server null
```

A l'invite on tape et on confirme le nouveau mot de passe

```
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 : ******
Le mot de passe est correctement défini.

Redéfinir le mot de passe administrateur DSRM :
```

On ressort de la commande en tapant deux fois **quit**

```
Redéfinir le mot de passe administrateur DSRM : quit
ntdsutil: quit

C:\Documents and Settings\Administrateur.SRV1-2003>
```

ACCESS RESSOURCES SANS DOMAINE

Situation :

Il s'agit de savoir s'il est possible d'accéder à des ressources présentes sur un poste sécurisé, sans s'y être authentifié….

Cela peut correspondre :

- à un réseau en poste à poste entre machines XP,
- à la tentative d'accès depuis un poste XP hors domaine sur un serveur 2003 Contrôleur de Domaine

Entre un client XP et un serveur 2003 CD :

Soit sur le serveur des comptes de domaine existant

Administrateur/domaine

Bob/b

Soit sur le client des comptes locaux existant

Administrateur/local

Toto/t

Sur le client on ouvre une session en tant que Toto/t, lorsque l'on essaye d'accéder à un partage effectuer sur le serveur on obtient

Ici il faut donner un login valable sur la machine que l'on essaye d'atteindre (existant donc dans les comptes déclarés localement sur cette machine…)

Ce qui parait normal.

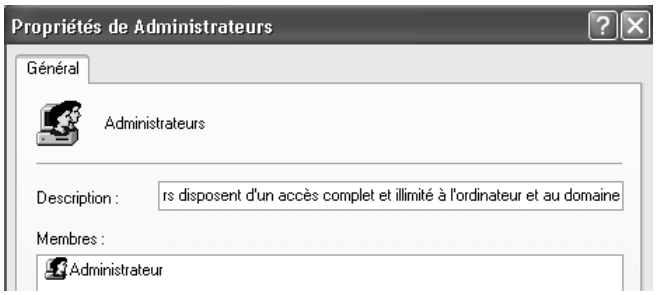
On est dans un contexte ou la sécurité est contrôlée par chaque machine, et aucune centralisation n'existe.

INCLUSION ENTRE GRP ADMINS

Qui est Administrateur d'un poste :

Sur une machine de type SEVEN ou XP on pourrait croire que c'est le compte utilisateur **Administrateur** qui à tous les pouvoirs.

S'il est vrai que ce compte utilisateur est un peu particulier, (par exemple c'est le seul compte à ne pas pouvoir être supprimé, ou bloquer en tentatives d'accès erronées…) il est surtout important car il faut partie du groupe local des **Administrateurs**



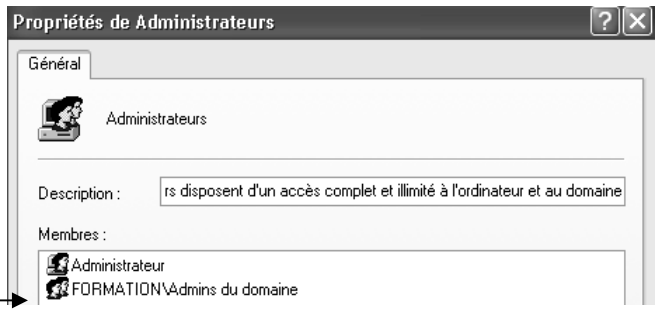
A tel point que on ne peut pas le sortir de ce groupe…

Raisonnement identique sur un serveur CD, ou les droits d'administration du serveur sont donnés au groupe local des **Administrateurs**, dont évidemment le compte utilisateur **administrateur** fait partie

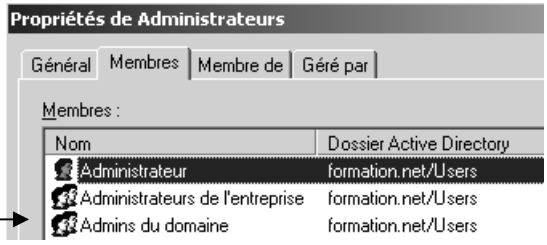
Conséquences de l'adhésion à un Domaine :

Lorsque un poste adhère à un domaine, automatiquement tous les membres du groupes **Admins de Domaine** font partie des administrateur de ce poste, car le groupe de Domaine **Admins de domaine** est inclus dans le groupe local des **Administrateurs** du poste

poste client



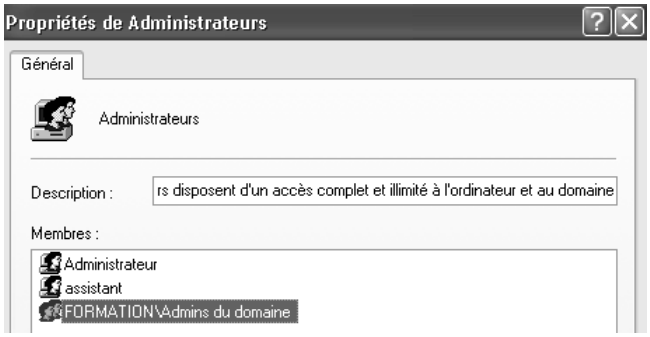
Serveur CD



Tentative de sécession ? :

En tant que administrateur local, on refuse de recevoir des administrateurs de domaine…

Rien de plus simple: il suffit dans gestion des utilisateurs de demander les membre du groupe des **Administrateurs** du poste



puis d'enlever le groupe des **Admins du domaine**

Désormais, notre poste fait toujours partie du Domaine, mais de nouveau seul le compte local Administrateur à les droits d'administration (et ici dans l'exemple un autre compte local assistant…)

Si l'Administrateur du Domaine vient ouvrir une session sur notre machine, cela sera possible, mais il va se retrouver simple utilisateur !

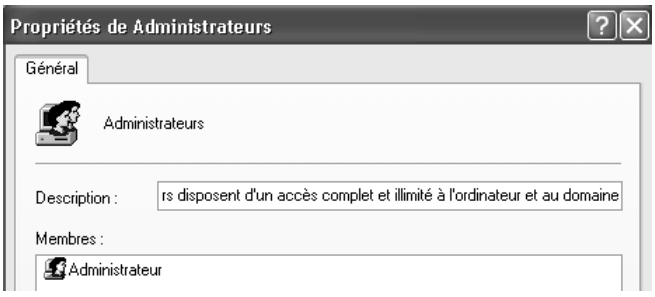
Quel sont ses moyens de mater la révolte ?

Rétablissement de la situation :

Seul l'administrateur local peut rétablir la situation…

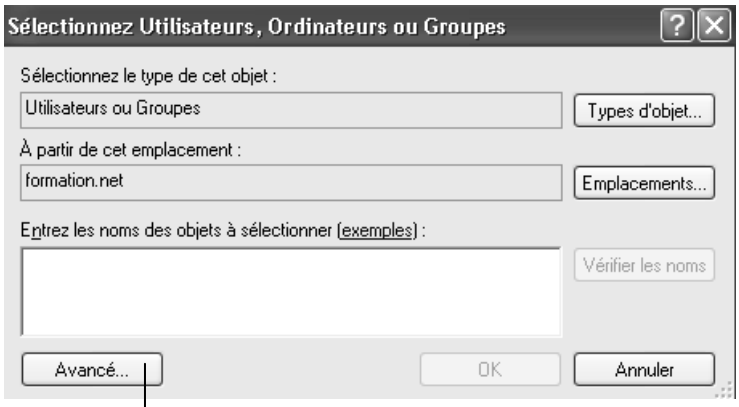
en redemandant depuis la gestion des utilisateurs de rajouter le groupe des **Admins du Domaine** dans le groupe des **Administrateurs** du poste.

Dans



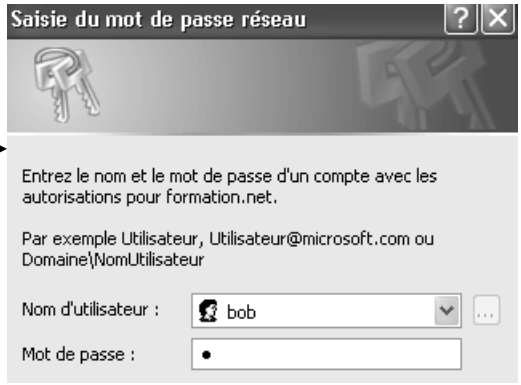
on demande

Ajouter…



Quand on demande **Avancé…**

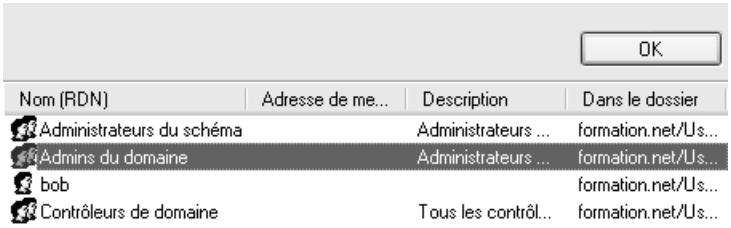
On à une demande d'authentification



Ce qui est normal, car on est inconnu sur le domaine

NB : à ce niveau, il n'est pas du tout nécessaire de sortir un login Administrateur de Domaine, un login quelconque utilisateur de domaine suffira !

Il ne reste plus qu'à ajouter le groupe des **Admins du domaine**



Ouf !

STOCKAGE PROFILS DISCRET

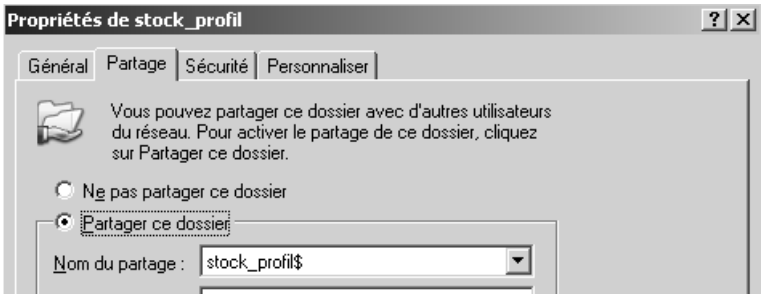
Objectifs et fonctionnalités :

On veut gérer les profils pour quelques utilisateurs, mais de manière discrète et sécurisée, c'est-à-dire que

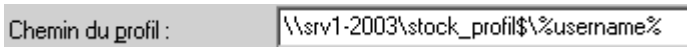
- on ne veut pas que le dossier de stockage des profils soit visible
- on ne souhaite pas garder une copie des profils errants sur les machines sur lesquelles les utilisateurs se sont connectés.
- On souhaite avoir un profil obligatoire

Dossier de stockage caché :

Il suffit de partager le dossier avec un nom se terminant par **$**



Et d'utiliser ce nom de partage ensuite dans les comptes utilisateurs



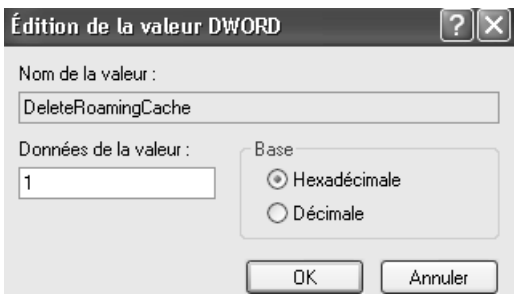
Non stockage des profils errant :

Sur tous les postes sur lesquels on l'on ne souhaite pas garder une copie des profils errants, on modifie 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**

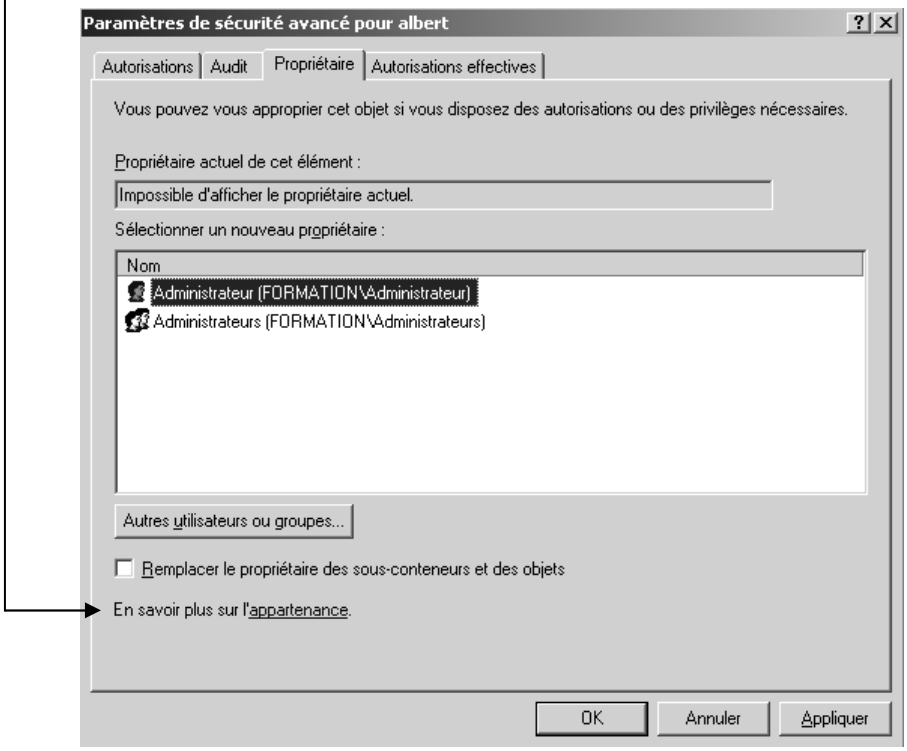


Création du profil obligatoire :

Un fois la session ouverte avec Albert, et tous les paramétrages effectués,

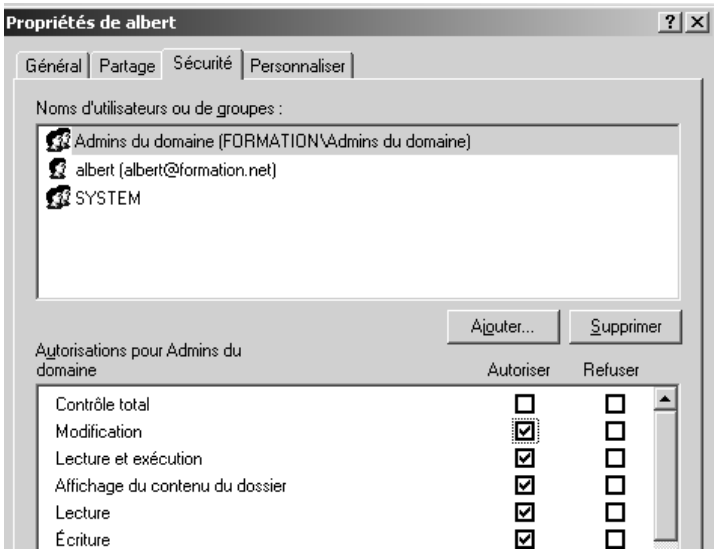
Il faut pouvoir Accéder au dossier de stockage du profil errant de Albert, de manière à changer le fichier **Ntuser.dat** en **Ntuser.man**

MAIS en NTFS il ne faut pas s'approprier tout le profil, mais juste le dossier de départ, dans lequel ensuite on va se rajouter en Modifier



Puis par rapport à la sécurité posée par défaut

on vient se rajouter en **Modifier**



Tout cela devrait nous permettre désormais d'accéder au dossier du profil.

Pour modifier NTUSER.DAT il peut être nécessaire de modifier la sécurité du fichier, avant d'avoir la possibilité de changer son extension.

N.B : si on commet l'erreur de manipulation de s'approprier la totalité du dossier-profil, ce profil deviendra inutilisable pour l'utilisateur.

1. Un fois le fichier renommé sur le serveur,
2. il faut ouvrir une session sur le client
3. apporter une modification a son environnement,
4. refermer la session,
5. ré-ouvrir une session et constater que les modifications apportées en 3) ont été perdues

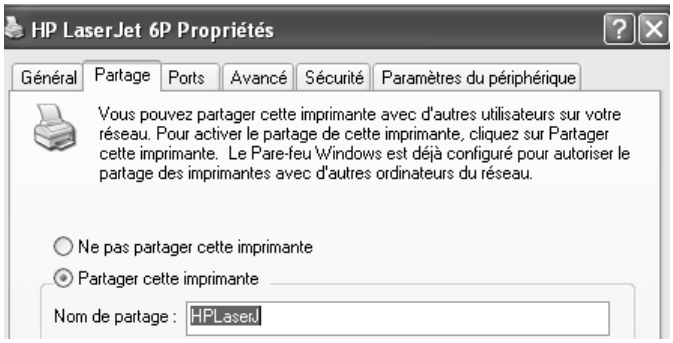
GESTION IMPRIMANTE

Accès imprimante partagée :

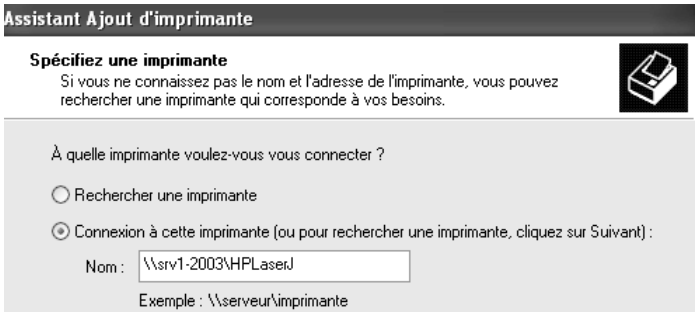
Si on veut accéder à une imprimante "régulée" par Windows, il est alors évident que on doit absolument

1. La partager sur le serveur d'impression
2. Aller la chercher depuis le "client"

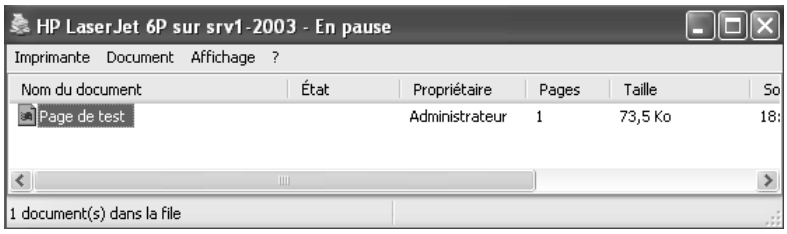
Sur un serveur on partage une imprimante HP laserjet 6p



On y accède depuis le client en installant une imprimante réseau



Pour procéder au TP, il suffit de mettre en pause l'imprimante… toutes les impressions étant bloquées, elles se mettrons en file dans de gestionnaire !



Il n'est même pas nécessaire d'avoir une imprimante physique de reliée…

RESEAU DE BASE
« FORMATION.EDU »

Objectifs et fonctionnalités :

Il s'agit de présenter ici un réseau local, constitué d'un seul Domaine, que l'on nommera **formation.edu**

Les noms à donner pour les utilisateurs sont

Poste 1	Nom : "**André**"	Nom détaillé :"André+*nom*"
	Mot de Passe : "**a**"	
Poste 2	Nom : "**Bruno**"	Nom détaillé :"Bruno+*nom*"
	Mot de Passe : "**b**"	
Poste 3	Nom : "**Claude**"	Nom détaillé :"Claude+*nom*"
	Mot de Passe : "**c**"	
Poste 4	Nom : "**Denis**"	Nom détaillé :"Denis+*nom*"
	Mot de Passe : "**d**"	
Poste 5	Nom : "**Etienne**"	Nom détaillé :"Etienne+*nom*"
	Mot de Passe : "**e**"	etc...

Sur le serveur, on prévoira un dossier nommé « **Ressource Formation** » contenant :

- un espace disque commun pour tous les utilisateurs nommé **Global** et partagé sous l'appellation **Commun**
- un espace disque réservé à chacun (nommé du nom de connexion ;**André, Bruno, Claude...**)

Sur le serveur les accès aux dossiers doivent êtres réalisés ainsi :

- Chaque utilisateur doit avoir accès à son propre dossier
- Chaque utilisateur doit avoir accès àu dossier commun
- les administratifs **André** et **Claude** doivent avoir accès en lecture seule aux dossiers de **Bruno** et **Denis**, commerciaux,
- **Etienne**, responsable doit avoir accès en lecture seule a tous les dossiers

Sur le serveur, les accès aux programmes doivent êtres réalisés ainsi :

- **André** et **Claude**, administratifs, doivent avoir accès à **Wordpad** et la **Calculette**, mais ne peuvent se connecter que depuis leur station d'attribution et pendant les heures de bureau (**8h00 à 17h30**)
- **Bruno** et **Denis**, commerciaux, ne doivent avoir accès qu'au **Solitaire** (la société n'est pas très sollicitée !), mais peuvent se connecter depuis n'importe quel poste
- **Etienne**, responsable peut utiliser aussi bien **Wordpad** que la **calculette** ou le **solitaire**, et peut se connecter bien sûr depuis n'importe quel poste

Chaque utilisateur doit disposer de raccourcis sur le bureau sur les logiciels qu'il peut utiliser, ainsi que deux lecteur logiques :

- un "**Y:**" sur son espace direct
- un "**Z:**" amenant au dossier Global

Un compte **Administrateur** avec mot de passe **domaine** sera créé avec droit total sur toutes les ressources et pouvant évidemment se connecter depuis n'importe quel poste

---

Analyse des Comptes :

On va lister tous les comptes nécessaires, par exemple :

"**Administrateurs du Domaine**"	Compte prédéfini lors de l'install

puis les comptes Utilisateurs crées suivant

"**Etienne**"		Compte prédéfini lors de l'install
"**André**"	(Administratif)	Compte avec connexion depuis une station fixe, horaires de bureau et mot de passe fixé
"**Bruno**"	(Commercial)	Compte avec obligation de changer le mot de passe
"**Claude**"	(Administratif)	Compte copié depuis André avec changement (station, mot passe)
"**Denis**"	(Commercial)	Compte copié depuis Bruno…

Analyse des Groupes :

On va représenter sur un schéma toutes les contraintes, par exemple

Un groupe global pré defini :

"**Admins du Domaine**" avec 1 compte utilisateur l'Administrateur

trois Groupe Globaux :

"**Responsable**" contenant le compte Etienne

"**Administratif**" contenant le compte André et Claude

"**Commerciaux**" contenant le compte Bruno et Denis

trois Groupes Locaux :

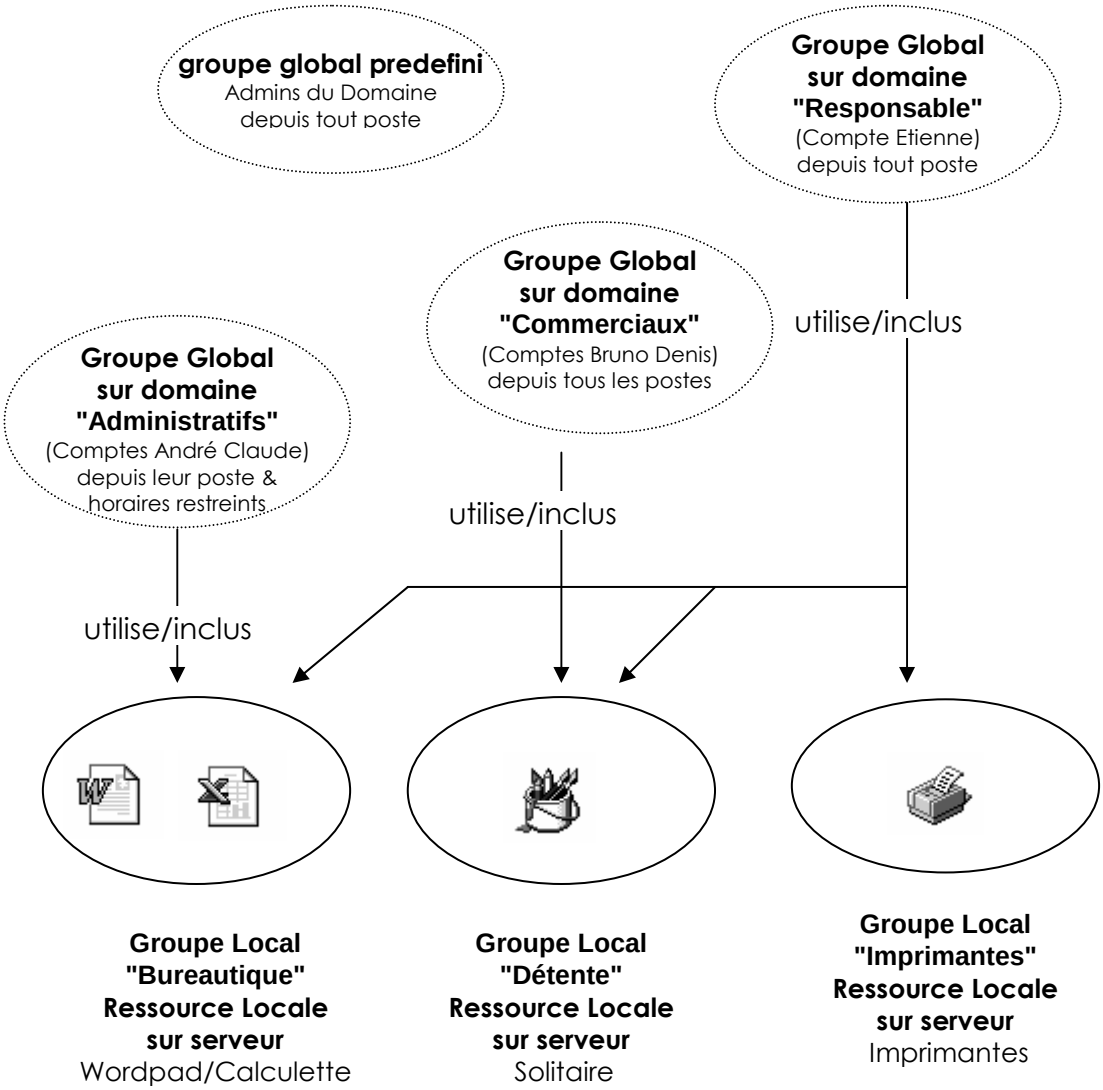
"**Bureautique**", pour l'utilsation de Wordpad + Calculette

"**Detente**", , pour l'utilsation du Solitaire

"**Impression**" pour l'utilisation des imprimantes

On intégrera un groupe global dans les groupes locaux dont il à l'usage,

Par exemple :



Pour les dossier, les permissions pourraient être attribuées Par exemple :

Ressource Formation

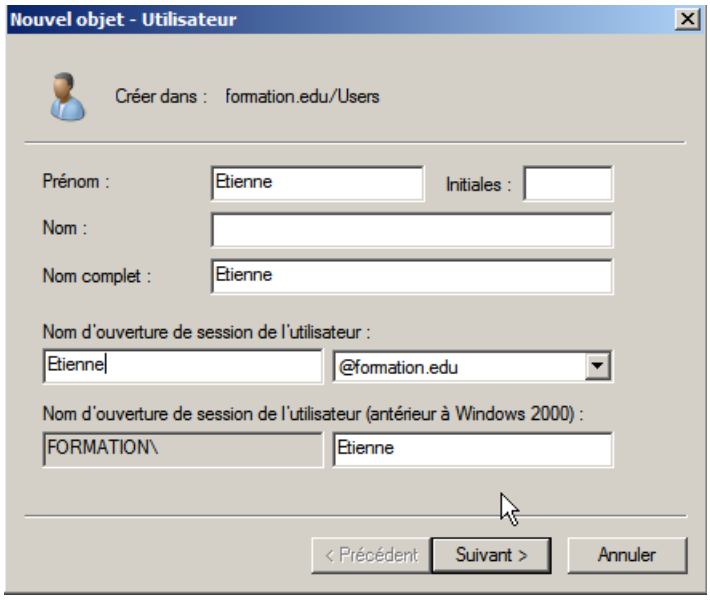
André	Compte Utilisateur "André"	Accès "Total"
	Groupe Global "Responsable"	Accès "Lecture"
	Groupe Global "Admins du Domaine"	Accès "Total"
Bruno	Compte Utilisateur "Bruno"	Accès "Total"
	Groupe Global "Responsable"	Accès "Lecture"
	Groupe Global "Administratif"	Accès "Lecture"
	Groupe Global "Admins du Domaine"	Accès "Total"
Claude	Compte Utilisateur "Claude"	Accès "Total"
	Groupe Global "Responsable"	Accès "Lecture"
	Groupe Global "Admins du Domaine"	Accès "Total"
Denis	Compte Utilisateur "Denis"	Accès "Total"
	Groupe Global "Responsable"	Accès "Lecture"
	Groupe Global "Administratif"	Accès "Lecture"
	Groupe Global "Admins du Domaine"	Accès "Total"
Etienne	Compte Utilisateur "Etienne"	Accès "Total"
	Groupe Global "Admins du Domaine"	Accès "Total"
Global	Groupe Global "Tout le monde"	Accès "Total"

Création des Comptes :

Au niveau des comptes, on peut dire que trois types de compte existent ,

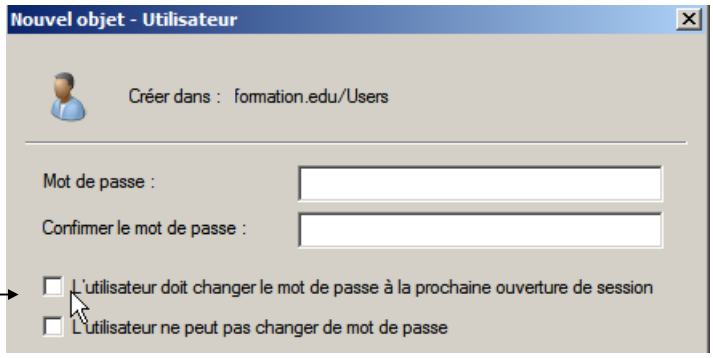
- un pour les administratifs (accès depuis leur poste et horaires classiques, mot de passe fixé),
- un pour les commerciaux (gestion du mot de passe forcée)
- un pour le responsable (gestion du mot de passe libre)

Créons le compte du responsable par Utilisateurs et **Ordinateurs Active Directory**, via le menu **Action Nouveau / Utilisateur**:

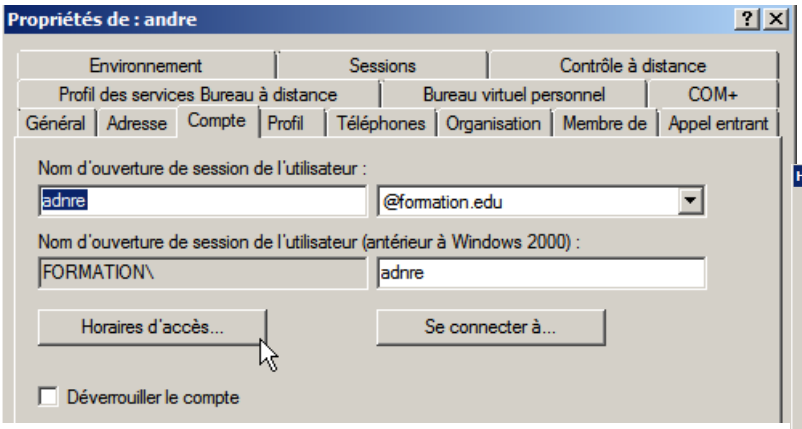


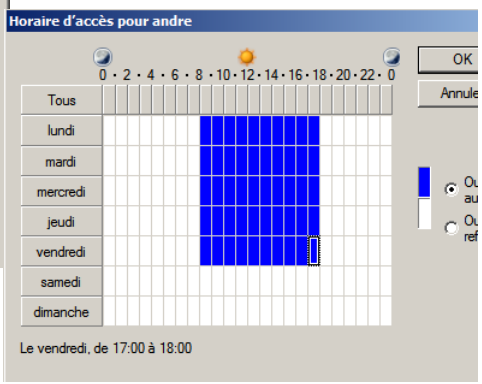
puis

Plus pratique



Créons un compte Administratif type pour **André** de la même manière, puis modifions ses propriétés en ce positionnant dessus par le menu contextuel:





pour créer le deuxième compte Administratif de Claude, il est préférable de partir du compte administratif existant de André et de demander une copie par le menu contextuel **copier**....

et de ne changer que ce qui doit être changé (la station de connexion)

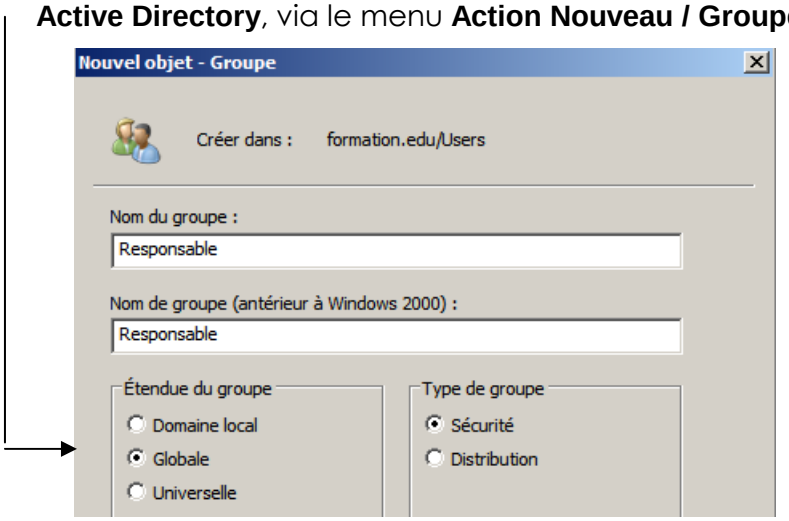
Idem pour le compte Commercial type pour **Bruno** que l'on recopiera, et de ne changer que ce qui doit être changé (station de connexion) pour Claude

Création des Groupes Globaux :

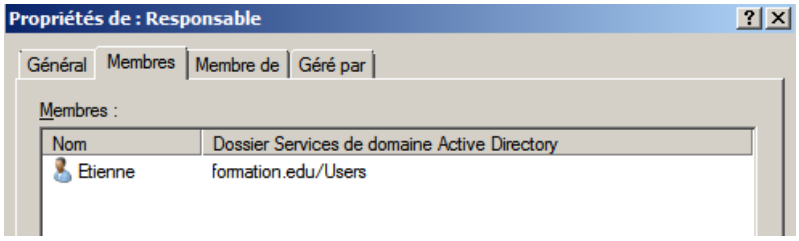
Le groupe Global "**Admins du Domaine**" existe, et contient déjà le compte utilisateur de l'"**Administrateur**" avec son mot de passe (domaine)

Il faut créer le groupe Global **Responsable**

Sur le serveur créons le Groupe Global par **Utilisateurs et Ordinateurs Active Directory**, via le menu **Action Nouveau / Groupe**:



Dans lequel on va rajouter le compte Etienne



Créons ensuite le groupe Global **Administratifs** par exemple

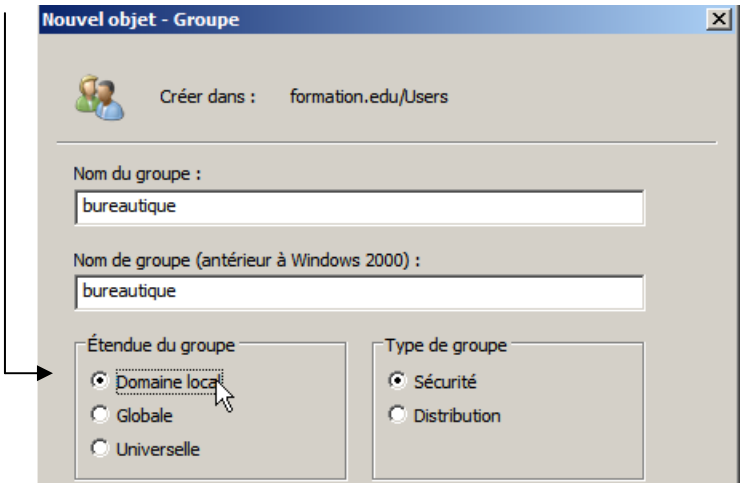
contenant **André** et **Claude**

Puis le groupe Global **Commerciaux** :

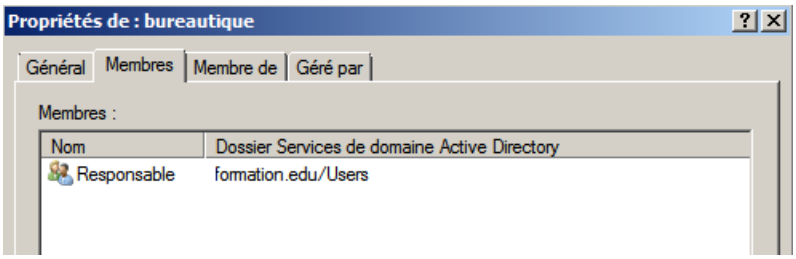
contenant **Bruno** et **Denis**

Création des Groupes Locaux :

pour créer le groupe local **Bureautique** on demande dans **Utilisateurs et Ordinateurs Active Directory**, le menu **Action Nouveau / Groupe**:



Pour ajouter des groupes globaux ou des utilisateurs, on demande **Propriétés…** et on obtient alors la boite de dialogue suivante



On fera de même pour créer le groupe local **Detente** :

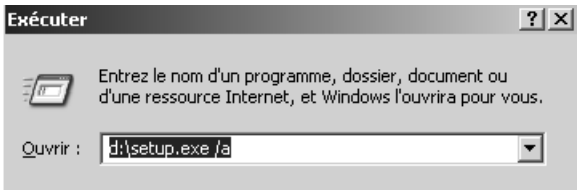
ainsi que pour créer le groupe local **Imprimante** :

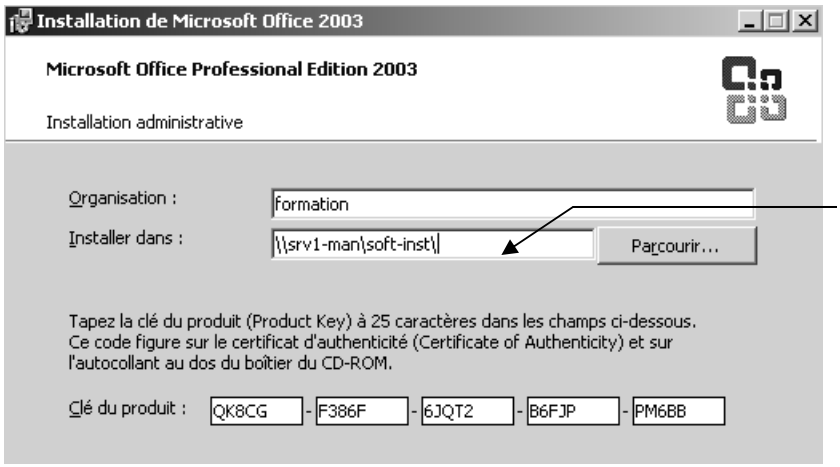
Création du point d'installation administrative

Sur le serveur, l'administrateur définit le point d'installation administrative en créant les dossiers qui contiendront les logiciels Office et à partir desquels les installations client seront réalisées. On parle d'**Installation Administrative**

- **700 Mo sont nécessaires**

On lance le nom du fichier **setup.exe / a** (uniquement depuis une version licence en nombre, impossible depuis une licence simple exemplaire)



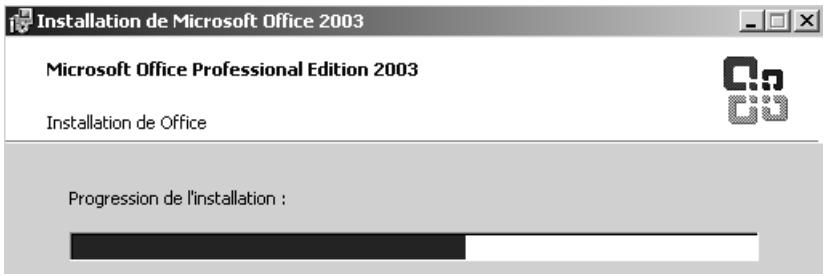


avec le chemin du point de distribution administratif…

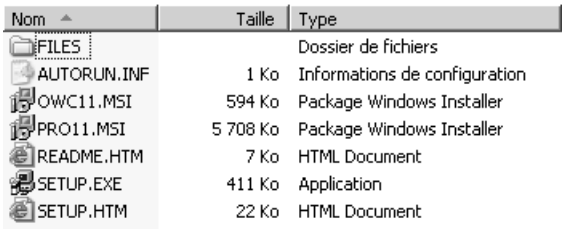
N.B : Il est conseillé que l'on ait un sous dossier en dessous du partage …

On accepte la licence…

Ce qui a pour effet de copier office 2003 (et non pas d'installer)



Plus de 4000 fichiers et 200 dossiers sont stockés sur le serveur dans une structure genre



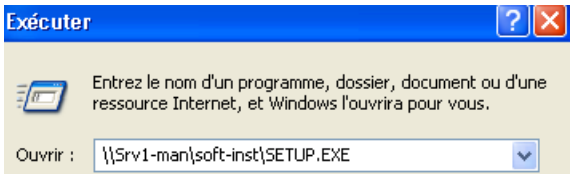
Installation client « manuelle »

L'installation client manuelle depuis une installation administrative de office 2003 effectuée auparavant, peut permettre de

- Se passe d'un lecteur de CDROM sur els clients
- Harmoniser l'installation de office 2003
- Donne une option d'installation office 2003 à minima localement sans passer par la gestion du fichier MSI… et les fichiers MST…

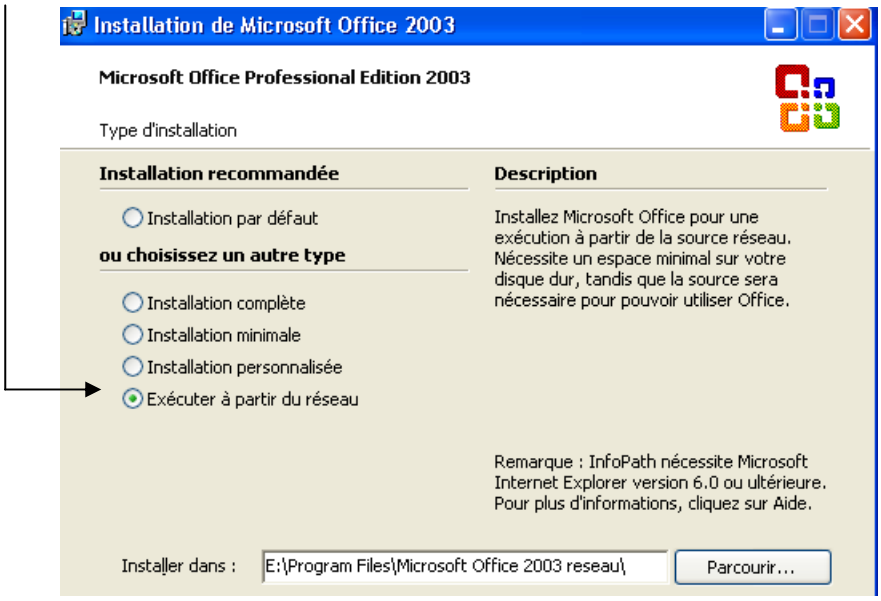
Depuis le client, il faut ouvrir une session en administrateur du poste (et client de domaine minimum).

L'installation se lance en allant chercher le point de distribution administratif

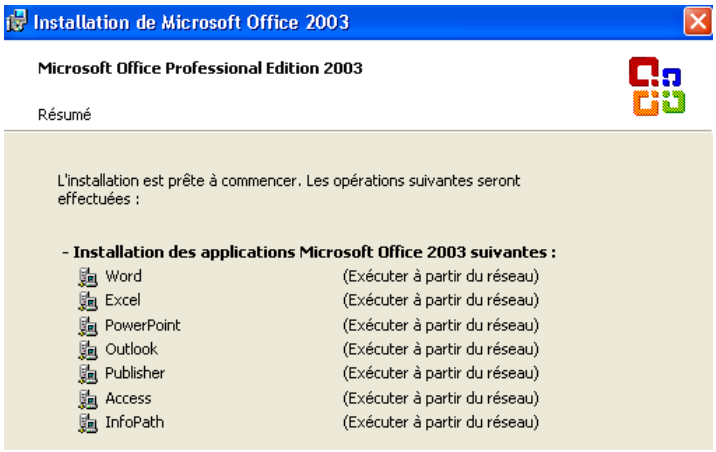


L'assistant se déclanche

Évidemment celle-ci nous intéresse particulièrement

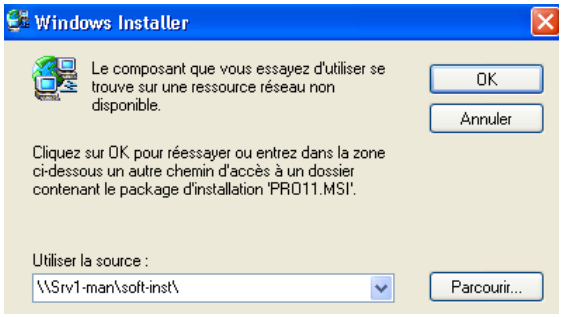


et on obtient une boite de dialogue de confirmation



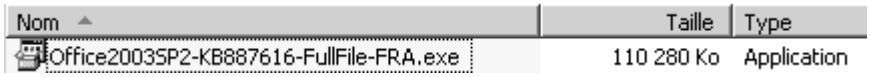
et 150 Mo pour office 2003 complet, c'est appréciable ! d'autant plus que la configuration est « figée »..

mais le problème c'est que il faut absolument que le serveur soit disponible pour utiliser office...sous peine d'obtenir un message du genre



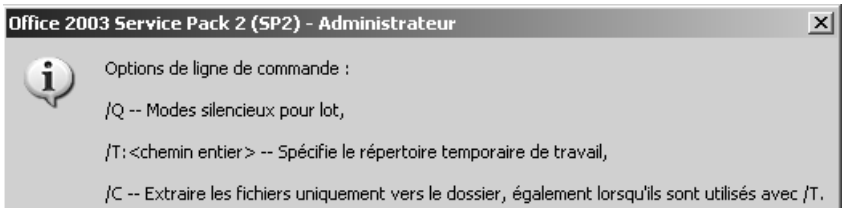
Intégration du Service Pack 2 de office 2003

Pour intégrer le Sp2 de office 2003 il faut récupérer le service pack complet version « administratif »



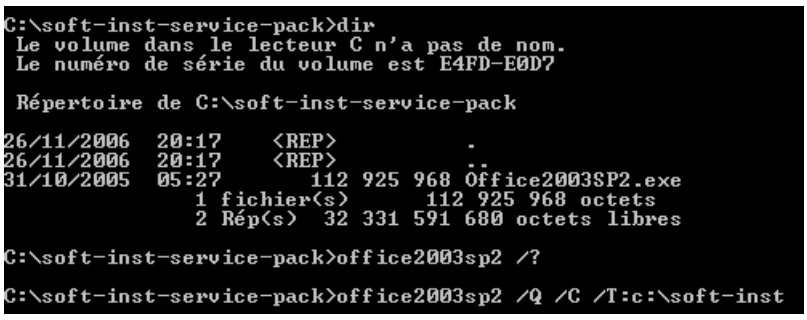
Pour plus de commodité on le renomme

Puis on l'extrait



Par **Office2003sp2.exe /Q /C /T :[chemin de destination]**

Donc



Notre dossier qui contenait

Nom	Taille	Type
FILES		Dossier de fichiers
AUTORUN.INF	1 Ko	Informations de configuration
modif-2003-formation.MST	13 Ko	Fichier MST
OWC11.MSI	594 Ko	Package Windows Installer
PRO11.MSI	5 708 Ko	Package Windows Installer
README.HTM	7 Ko	HTML Document
SETUP.EXE	411 Ko	Application
SETUP.HTM	22 Ko	HTML Document

désormais contient

FILES		Dossier de fichiers
AUTORUN.INF	1 Ko	Informations de configuration
MAINSP2ff.msp	101 010 Ko	Correctif Windows Installer
modif-2003-formation.MST	13 Ko	Fichier MST
ohotfix.exe	125 Ko	Application
ohotfix.ini	8 Ko	Paramètres de configuration
ohotfixr.dll	16 Ko	Extension de l'application
OWC11.MSI	594 Ko	Package Windows Installer
OWC11SP2ff.msp	6 118 Ko	Correctif Windows Installer
OWC102003SP2ff.msp	5 643 Ko	Correctif Windows Installer
PRO11.MSI	5 708 Ko	Package Windows Installer
README.HTM	7 Ko	HTML Document
SETUP.EXE	411 Ko	Application
SETUP.HTM	22 Ko	HTML Document

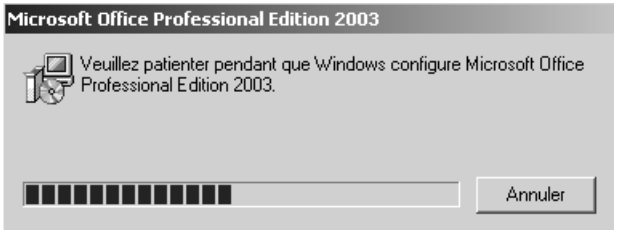
Extraction du service pack 2 de office 2003

Pour intégrer notre sp2 à office 2003 il faut deux commandes basées sur la syntaxe suivante

miexec /p [chemin]MAINSP2ff.msp /a [chemin]PRO11.msi SHORTFILENAMES=TRUE /qb

```
C:\soft-inst-service-pack>msiexec /p C:\soft-inst\MAINSP2ff.msp /a C:\soft-inst\
PRO11.msi SHORTFILENAMES=TRUE /qb
```

Amenant

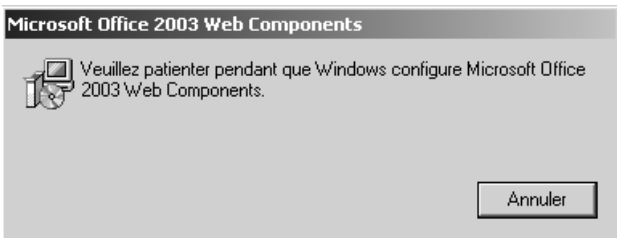


Et

miexec /p [chemin]OWC11SP2ff.msp /a [chemin]OWC11.msi SHORTFILENAMES=TRUE /qb

```
C:\soft-inst-service-pack>msiexec /p C:\soft-inst\OWC11SP2ff.msp /a C:\soft-inst
\OWC11.msi SHORTFILENAMES=TRUE /qb
```

Amenant



N.B : il est tout a fait possible d'extraire le service pack dans un dossier a part, afin de mieux l'effacer à la fin de l'intégration