

# Environnement

## Nom de domaine

Comme dans la capture ci-dessous de nom de domaine est "Scuolapro.local"

```
Nom de l'hôte . . . . . : ICT158-SRV03-1
Suffixe DNS principal . . . . . : Scuolapro.local
Type de nœud . . . . . : Inconnu
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS : Scuolapro.local
```

Le FQDN ou Fully Qualified Domain Controller est "ict158-srv03-1.scuolapro.local"

Propriétés de 5e514734-7b39-4d21-aff5-270ee42d3261

Nom canonique (CNAME) | Sécurité

Nom de l'alias (utilisez le domaine parent si ce champ est vide) :

5e514734-7b39-4d21-aff5-270ee42d3261

Nom de domaine pleinement qualifié (FQDN) :

5e514734-7b39-4d21-aff5-270ee42d3261.\_msdcs.Scuolapro.local

Nom de domaine pleinement qualifié (FQDN) pour l'hôte de destination :

ict158-srv03-1.scuolapro.local

Parcourir...

OK Annuler Appliquer

## IP

L'adresse du serveur est 10.1.1.20 avec comme passerelle par défaut 10.1.1.1 et le serveur DNS pointe sur lui même.

```
Adresse physique . . . . . : 00-0C-29-E0-10-3B
DHCP activé . . . . . : Non
Adresse IP . . . . . : 10.1.1.20
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 10.1.1.1
Serveurs DNS . . . . . : 10.1.1.20
```

L'adresse du client est 10.1.1.41, on peut constater également que l'adresse IP a bien été attribuée par le serveur DHCP et pas rentrer manuellement, la passerelle par défaut est 10.1.1.1 et le serveur DHCP et DNS pointe bien sur l'adresse du serveur windows 2003.

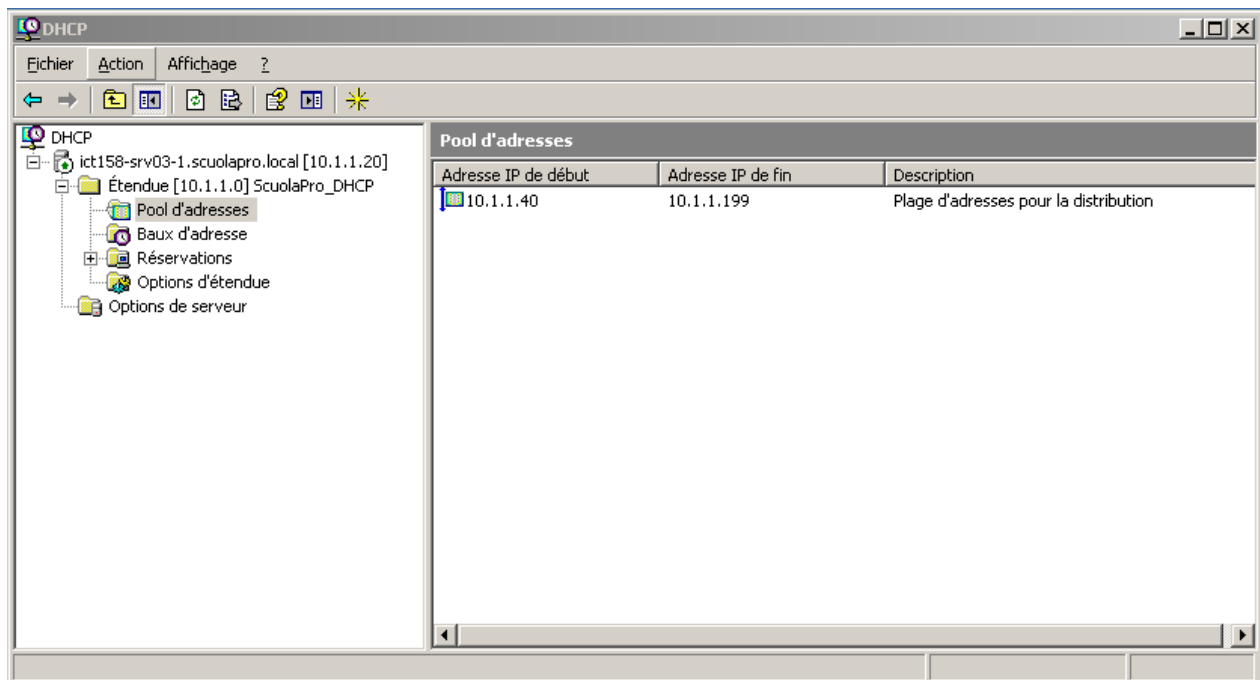
```
Adresse IPv4. . . . . : 10.1.1.41 (préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : mardi 9 février 2021 08:56:50
Bail expirant. . . . . : mercredi 17 février 2021 08:56:49
Passerelle par défaut. . . . . : 10.1.1.1
Serveur DHCP . . . . . : 10.1.1.20
IAID DHCPv6 . . . . . : 234884137
DUID de client DHCPv6. . . . . : 00-01-00-01-1F-70-66-1C-00-0C-29-B5-AD
-41
Serveurs DNS. . . . . : 10.1.1.20
```

## Réseau

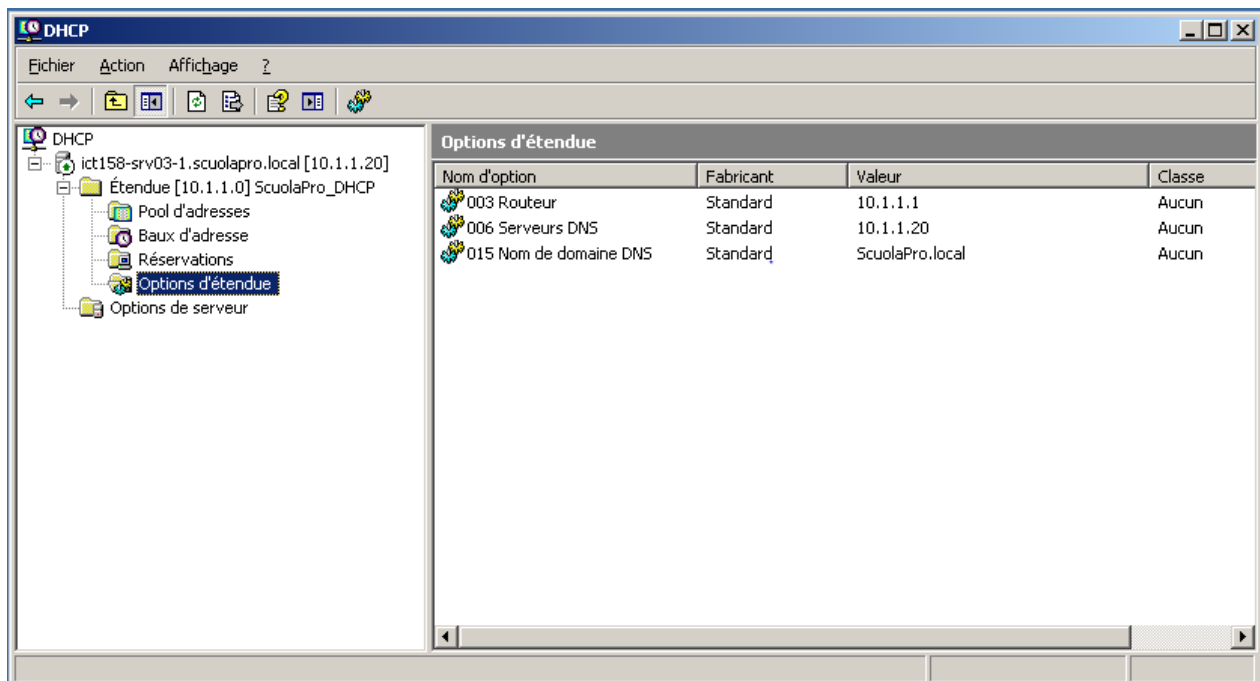
L'adresse du réseau est 10.1.1.0, le masque de sous réseau est 255.255.255.0 ou /24

```
Adresse physique . . . . . : 00-0C-29-E0-10-3B
DHCP activé. . . . . : Non
Adresse IP. . . . . : 10.1.1.20
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 10.1.1.1
Serveurs DNS . . . . . : 10.1.1.20
```

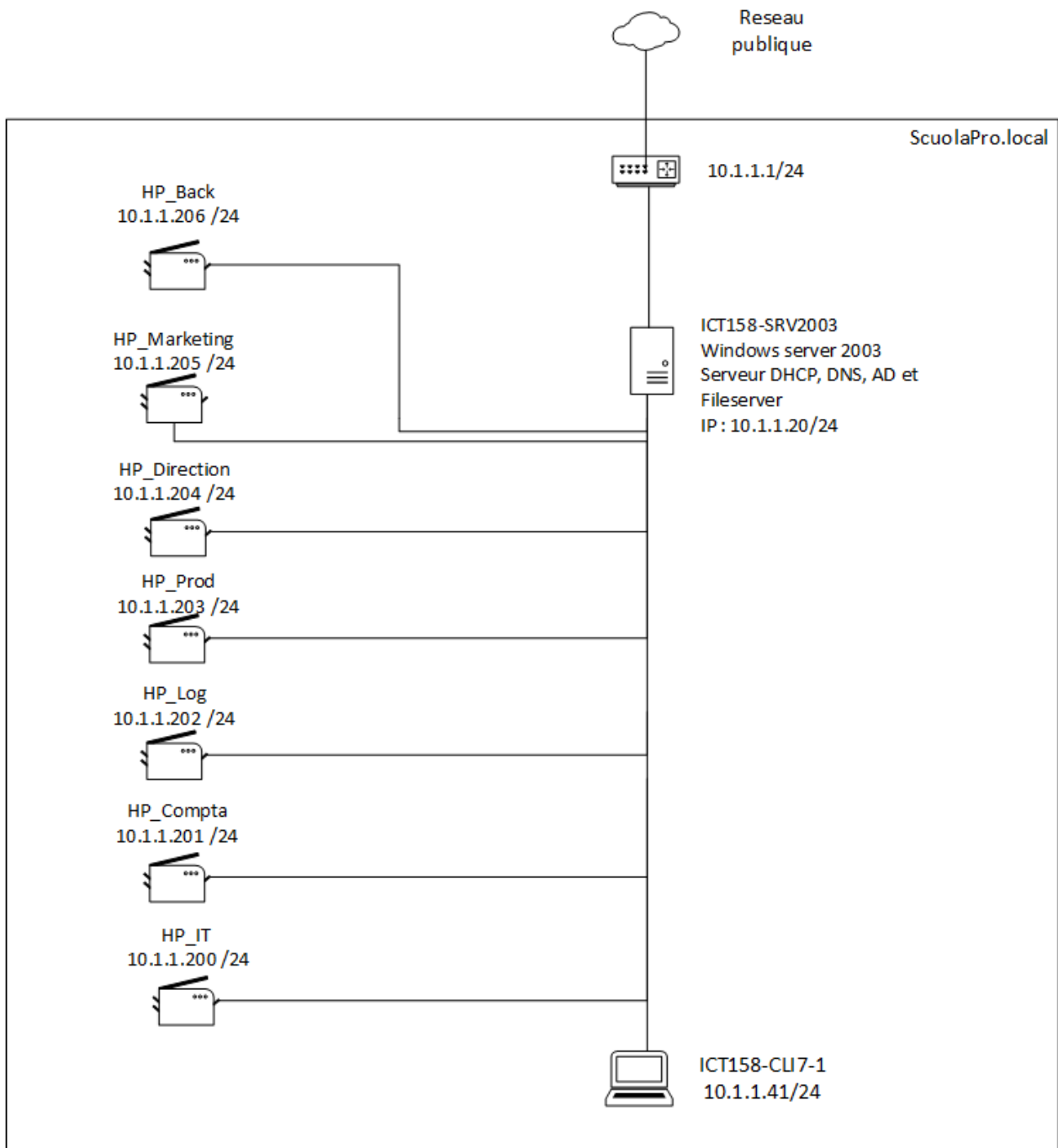
La pool d'adresse IP sont entre 10.1.1.40 et 10.1.1.199



Ici on peut voir que l'adresse du routeur est 10.1.1.1, l'adresse du DNS est 10.1.1.20 lui-même et le nom de domaine est "ScuolaPro.local".



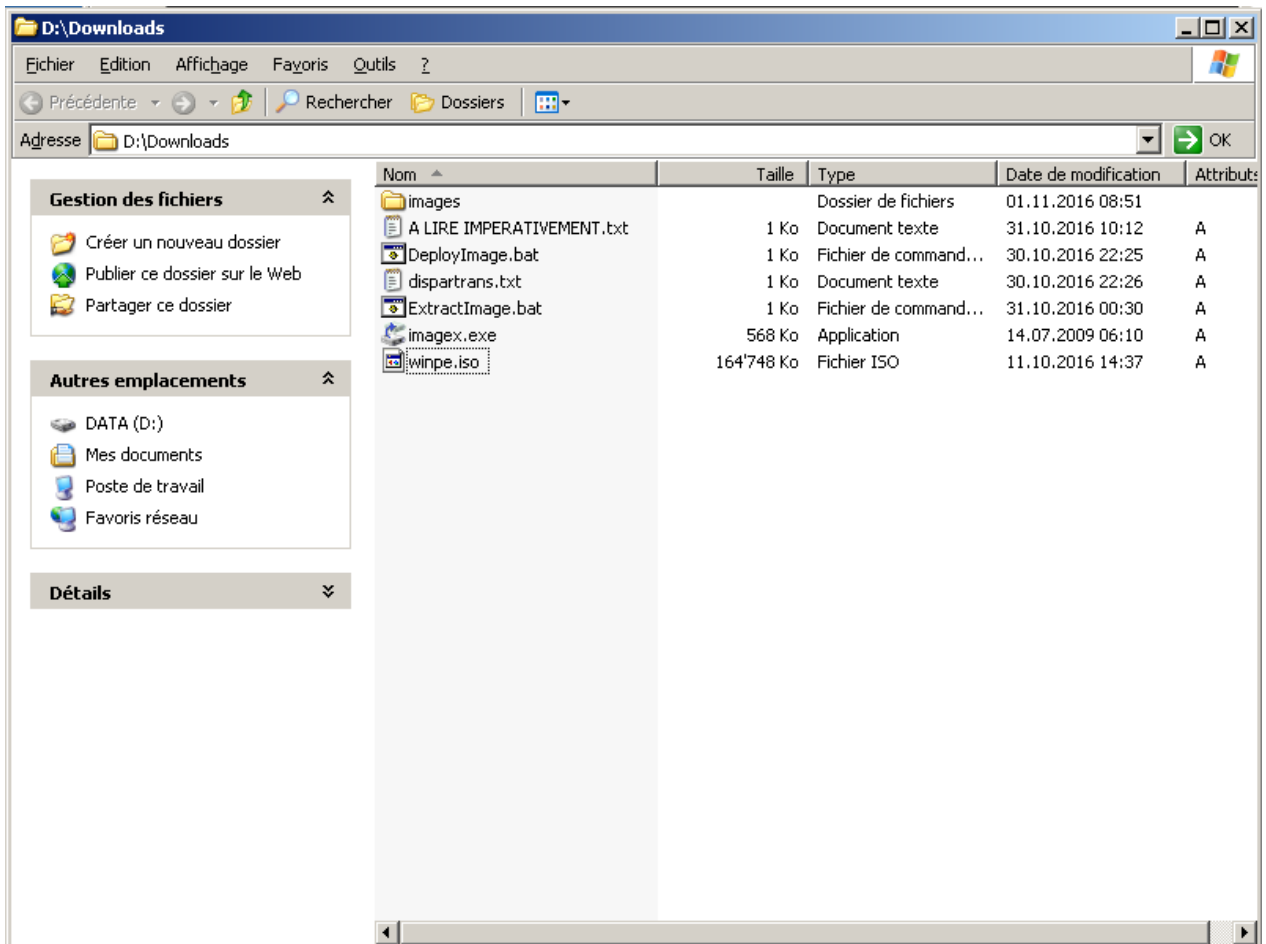
Voici un état des lieux du réseau actuelle.



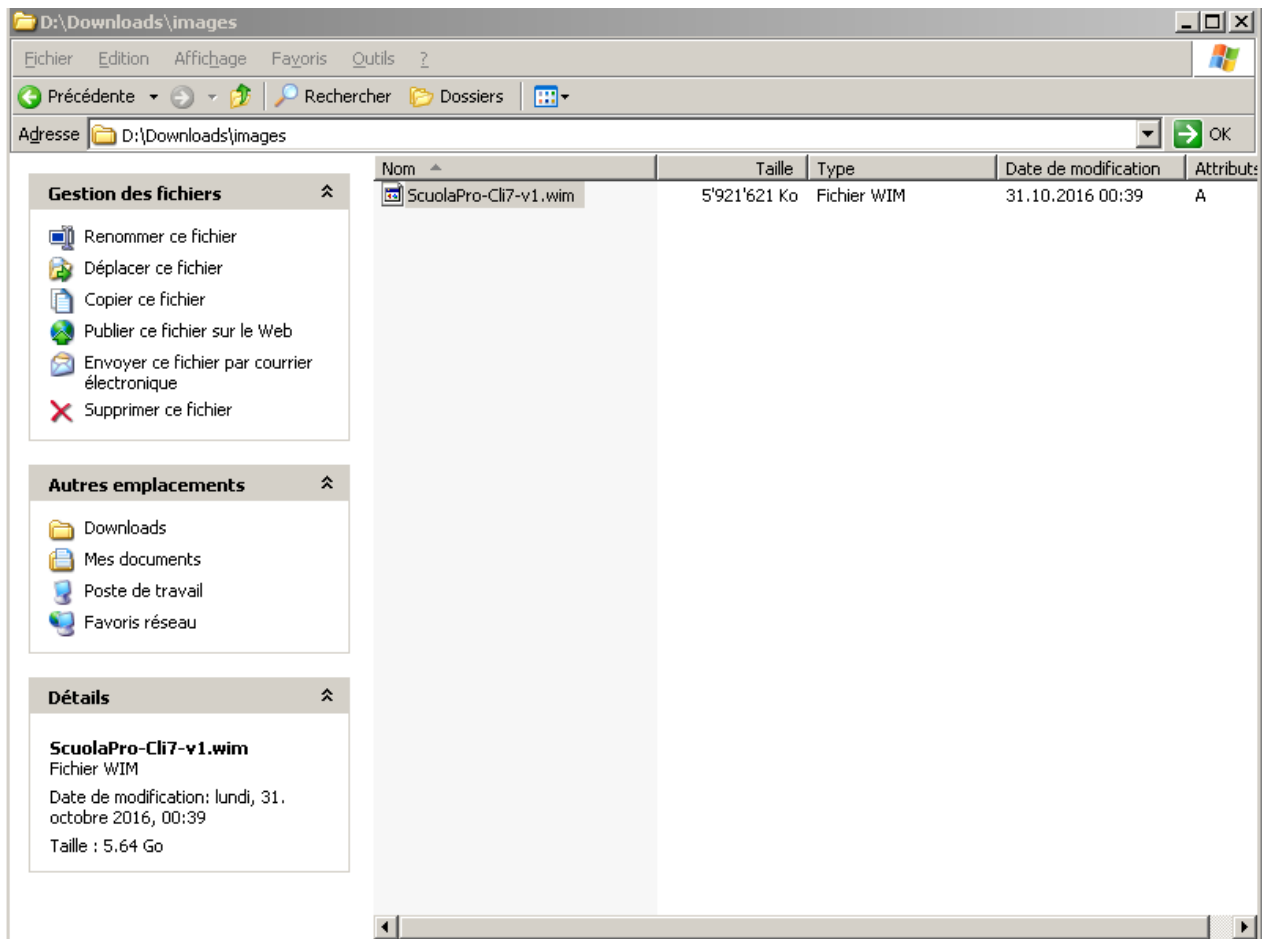
Il y a actuellement 6 imprimantes connectés au serveur puis à un routeur ainsi qu'une machine cliente également connectée au serveur.

## Déploiement auto \*wim

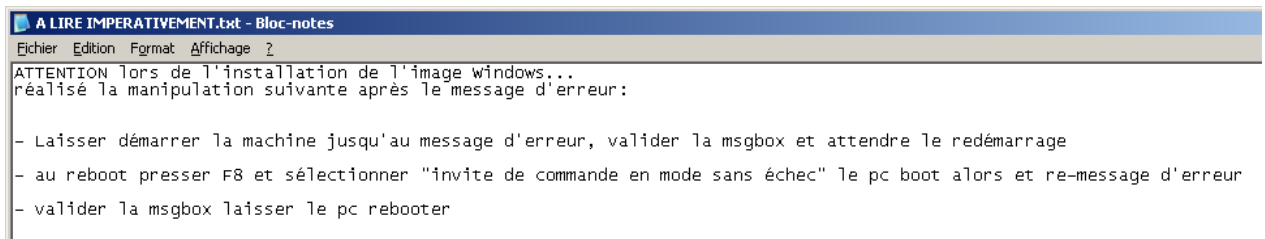
Sur le bureau du windows server 2003 il y a un raccourci qui mène au déploiement d'os qui est visiblement situé dans le fichier download du disque D:



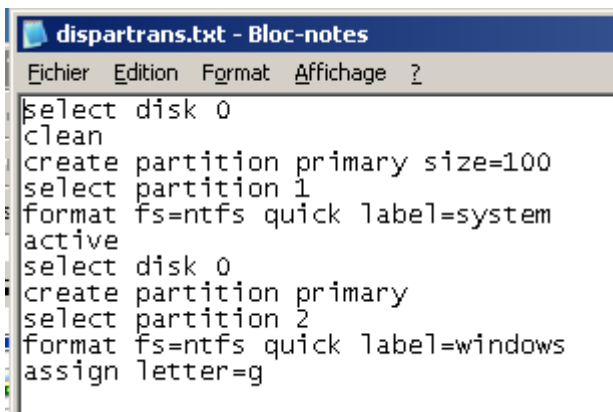
Dans le dossier images il y a l'image windows 7 qu'utilise la machine cliente.



En revenant sur le dossier on peut y trouver un fichier texte à lire



Egalement un autre fichier texte qui semble contenir un code comme un script mais il est en fichier texte, il semble qu'il sert à créer deux partitions différentes.



Sinon il ne reste que deux script en .bat, "DeployImage", qui j'imagine sert à déployer l'image windows du client.

```

DeployImage.bat - Bloc-notes
Fichier  Edition  Format  Affichage  ?
@echo off
diskpart /s z:\dispartrans.txt
z:
imagex /apply z:\images\ScuolaPro-Cl17-v1.wim 1 g:
g:\windows\system32\bcdboot g:\windows
g:\windows\system32\shutdown /r /t 0

```

et "ExtractImage" qui sert à enlever l'image de la machine

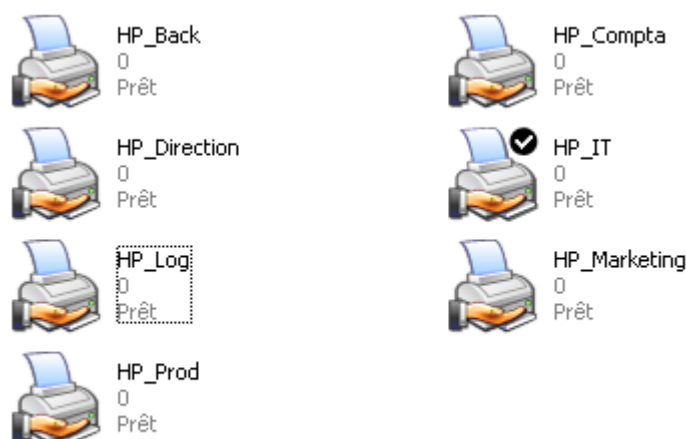
```

ExtractImage.bat - Bloc-notes
Fichier  Edition  Format  Affichage  ?
@echo off
imagex.exe /capture d: z:\Images\ImagescuolaPro.wim "ICT15-CL12" /verify

```

## Imprimantes

Il y a un total de 7 imprimantes connecté sur le même réseau, une pour chaque département.



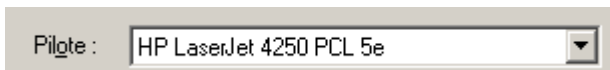
Les printers sont tous des HP LaserJet 4250 PCL 5e, pour l'instant seulement une seule imprimante est utilisée, la HP\_IT.

Dans cette capture nous pouvons voir les quelles adresses IP correspond à quelle imprimante ainsi que le port utilisé TCP/IP.

Port	Description	Imprimante
<input type="checkbox"/> IP_10.1.1.200	Standard TCP/IP Port	HP_IT
<input type="checkbox"/> IP_10.1.1.201	Standard TCP/IP Port	HP_Compta
<input type="checkbox"/> IP_10.1.1.202	Standard TCP/IP Port	HP_Log
<input type="checkbox"/> IP_10.1.1.203	Standard TCP/IP Port	HP_Prod
<input type="checkbox"/> IP_10.1.1.204	Standard TCP/IP Port	HP_Direction
<input type="checkbox"/> IP_10.1.1.205	Standard TCP/IP Port	HP_Marketing

Port	Description	Imprimante
<input type="checkbox"/> FILE:	Impression dans un fich...	
<input checked="" type="checkbox"/> 10.1.1.206	Standard TCP/IP Port	HP_Back

Toutes les imprimantes utilisent le même pilote, le "HP Laserjet 4350 PCL 5e".



Il y a trois pilote d'impression différent d'installé sur le serveur d'impression, celui qu'utilisent les imprimantes ont la version 64 bits et 32 bits.

Nom	Processeur	Version
HP LaserJet 4050 Serie...	x86	Windows 2000, Window...
HP LaserJet 4250 PCL 5e	x64	Windows XP et Window...
HP LaserJet 4250 PCL 5e	x86	Windows 2000, Window...

## Serveurs

---

### Hardware

---

Checker la documentation dans ce repository, ce document repertorie tout le type d'hardware disponible pour ce type de serveur, difficile de dire les vrais composants du serveur puisqu'il d'agit d'une machine virtuel, les composants ne sont pas les mêmes :

[https://github.com/Vinkhey/ICT-158/blob/main/Doc%20Machines/doc\\_HPServer.pdf](https://github.com/Vinkhey/ICT-158/blob/main/Doc%20Machines/doc_HPServer.pdf)

D'après la capture ci-dessous l'os installé est "Microsoft windows server 2003 Standard Edition", la version du système est "5.2.3790 Service Pack 2 version 3790"



```
C:\ Invite de commandes
Microsoft Windows [version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrateur.SRU2003.000>systeminfo

Nom de l'hôte:                ICT158-SRU03-1
Nom du système d'exploitation: Microsoft(R) Windows(R) Server 2003,
Standard Edition
Version du système:           5.2.3790 Service Pack 2 version 3790

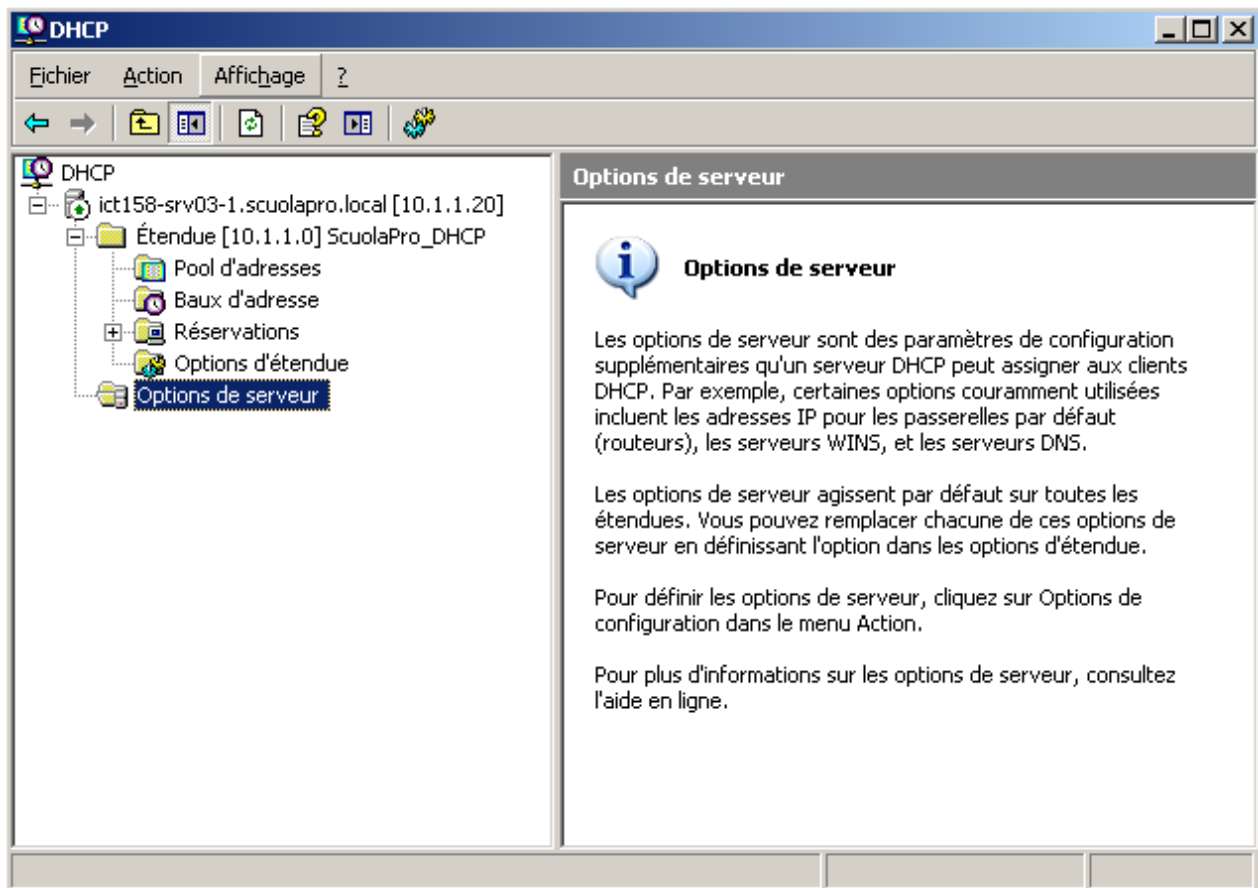
Fabricant du système d'exploitation: Microsoft Corporation
Configuration du système d'exploitation: Contrôleur principal de domaine
Type de version du système d'exploitation: Uniprocessor Free
Propriétaire enregistré:     Ste-Croix
Organisation enregistrée:    CPNU
Identificateur de produit:    69891-640-0588025-45468
Date d'installation originale: 02.10.2016, 19:08:21
Temps d'activité système:    0 jours, 0 heures, 29 minutes, 49 se
condes
Fabricant du système:        VMware, Inc.
Modèle du système:           VMware Virtual Platform
Type du système:             X86-based PC
Processeur(s):               1 processeur(s) installé(s).
[01]: x86 Family 6 Model 94 Stepping
3 GenuineIntel ~3408 MHz
Version du BIOS:             INTEL - 6040000
Répertoire Windows:          C:\WINDOWS
Répertoire système:          C:\WINDOWS\system32
Périphérique d'amorçage:      \Device\HarddiskVolume1
Option régionale du système: fr-ch;Français (Suisse)
Paramètres régionaux d'entrée: fr-ch;Français (Suisse)
Fuseau horaire:              (GMT+01:00) Amsterdam, Berlin, Berne
, Rome, Stockholm, Vienne
Mémoire physique totale:      511 Mo
Mémoire physique disponible:  299 Mo
Fichier d'échange : taille maximale: 1'254 Mo
Fichier d'échange : disponible: 1'022 Mo
Fichier d'échange : en cours d'utilisation: 232 Mo
Emplacements des fichiers d'échange: C:\pagefile.sys
Domaine:                     Scuolapro.local
Serveur d'ouverture de session: \\ICT158-SRU03-1
Correctif(s):                 3 Corrections installées.
[01]: Q147222
[02]: SP1 - SP
[03]: KB914961 - Service Pack
1 carte(s) réseau installée(s).
[01]: VMware Accelerated AMD PCNet A
dapter
Nom de la connexion : Connexion au réseau local
DHCP activé : Non
Adresse(s) IP
[01] : 10.1.1.20

C:\Documents and Settings\Administrateur.SRU2003.000>
```

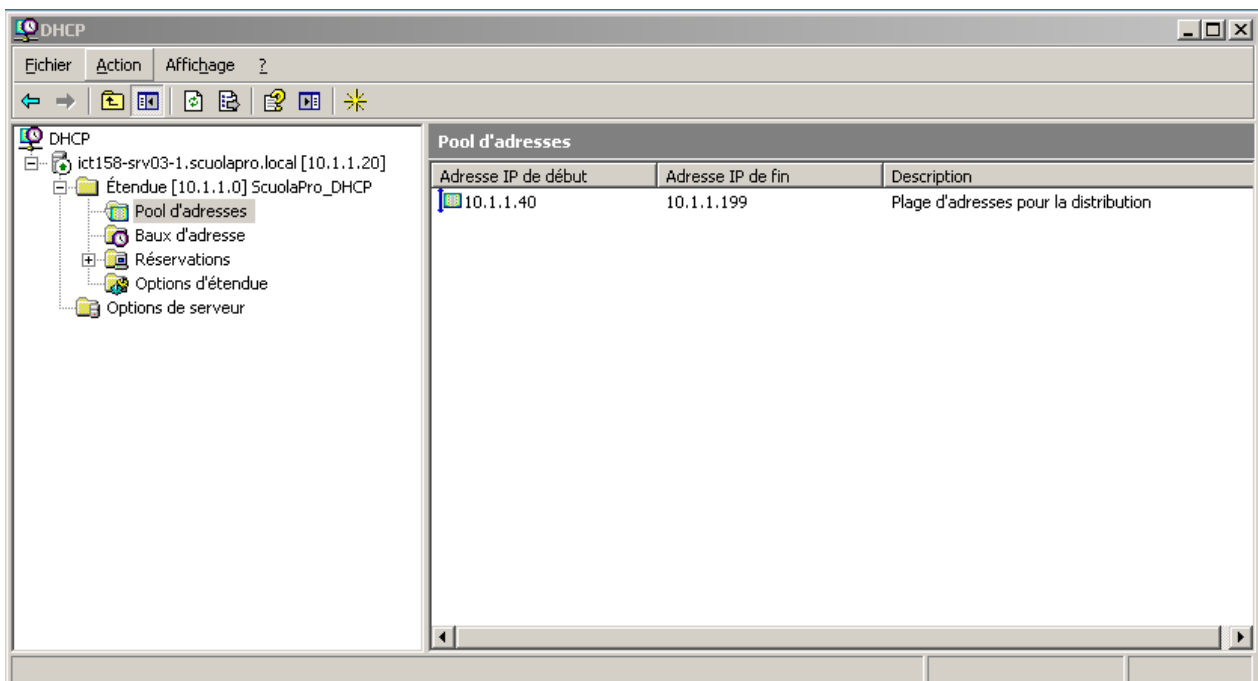
## Services

### DHCP

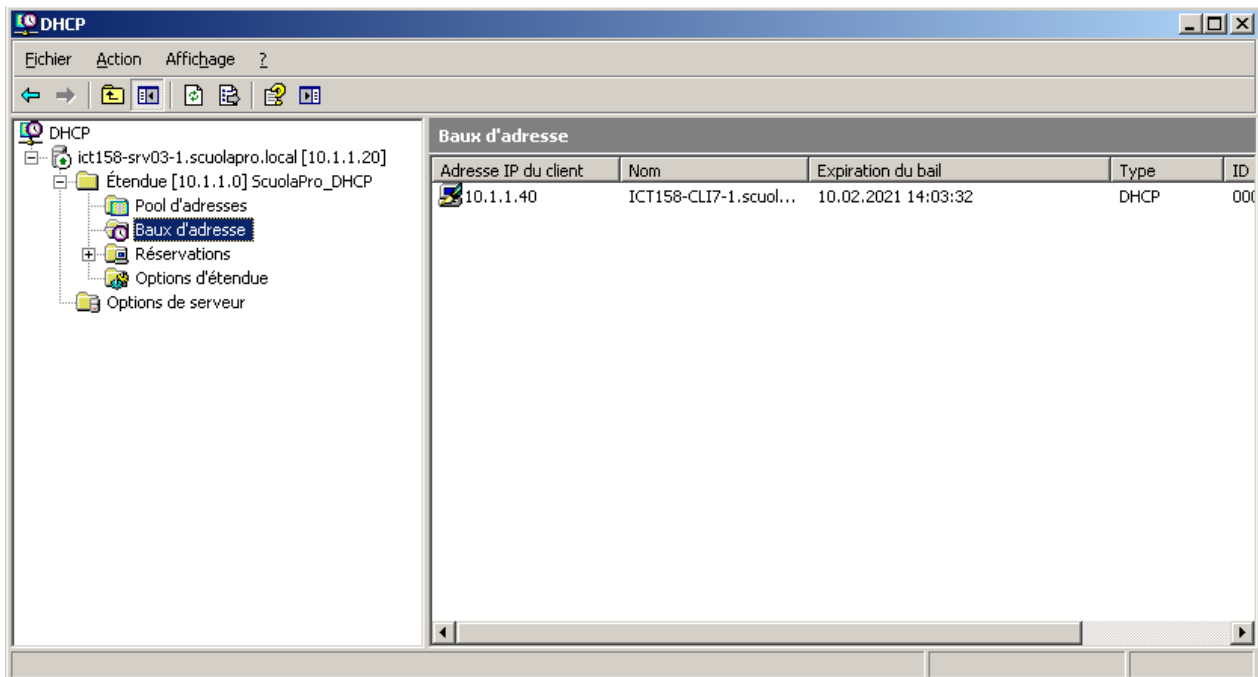
Comme indiqué plus haut dans le document, il y a une étendue "ScuolaPro\_DHCP" sur l'adresse 10.1.1.0, le serveur DHCP est le serveur lui-même en 10.1.1.20



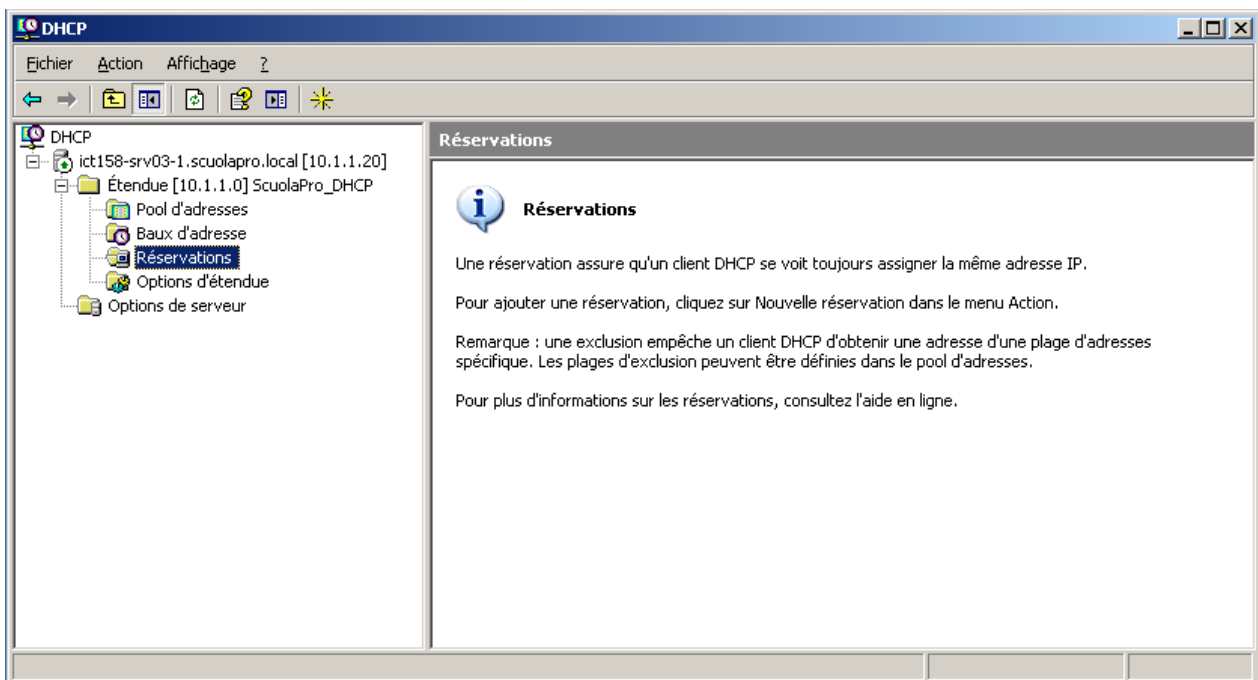
La Pool d'adresse distribuable est entre les adresses 10.1.1.40 et 10.1.1.199



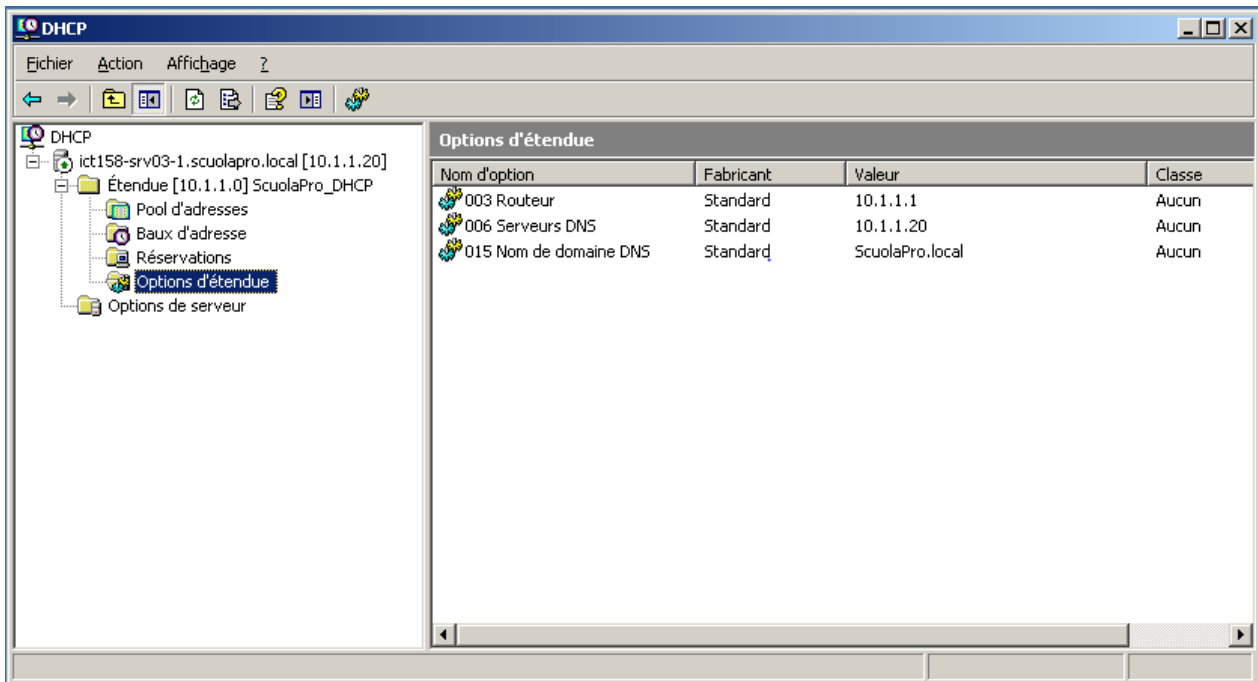
On peut constater qu'une adresse IP à déjà été attribuée à la machine cliente avec pour adresse 10.1.1.40 est la fin du bail d'une durée de 8 jours.



Aucune réservation d'adresse IP n'a été effectuée.



Ici on peut constater les options d'étendues, le routeur avec l'adresse 10.1.1.1 et le serveur DNS en 10.1.1.20 avec comme nom de domaine ScuolaPro.local



Aucune option de serveur n'a été effectuée



## AD

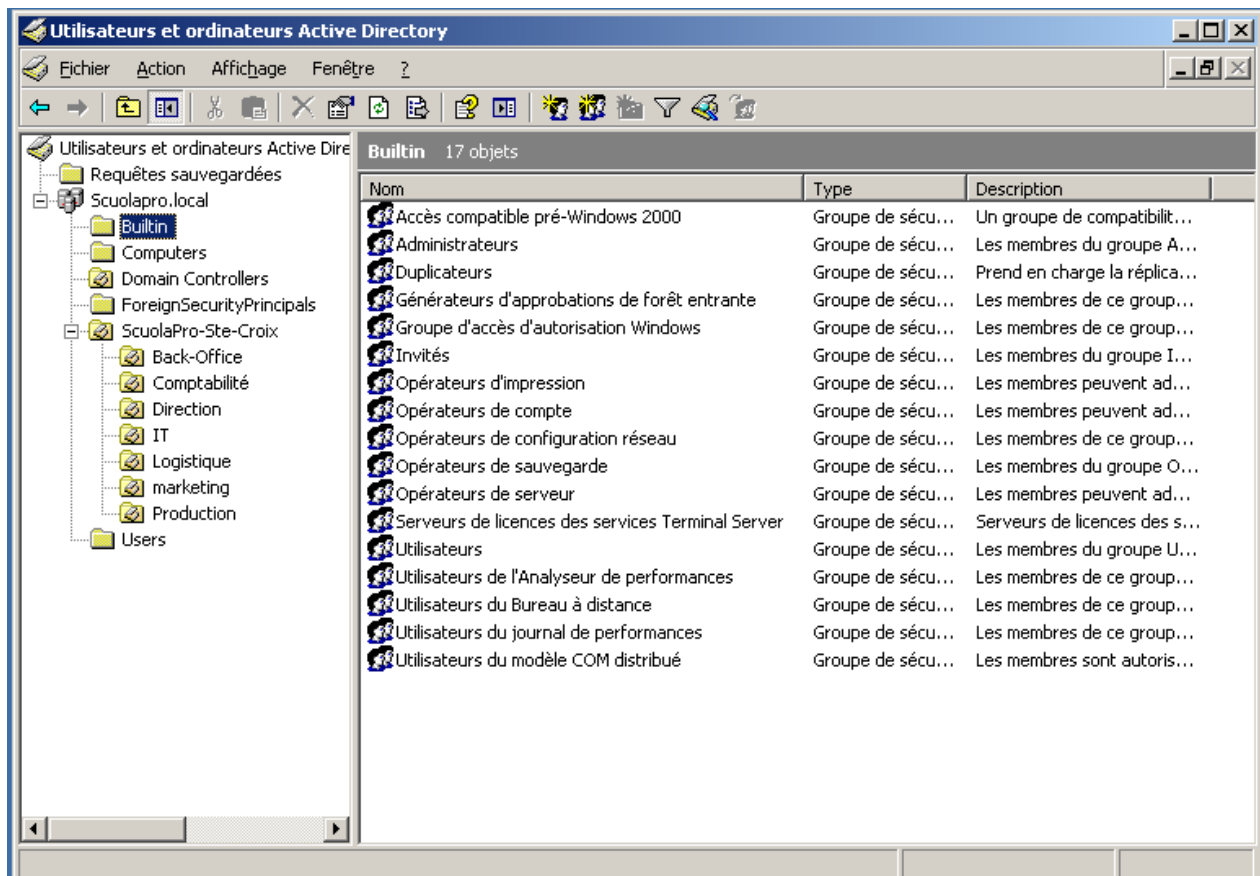
Comme mentionné au début de ce document le nom de domaine est "ScuolaPro.local" et le FQDN est "ict158-srv03-1.scuolapro.local", le contrôleur de domaine est "ScuolaPro.local", il n'y a pas de sous-domaine.

Le niveau fonctionnel est windows 2000 mixte et le niveau de la forêt est windows 2000.

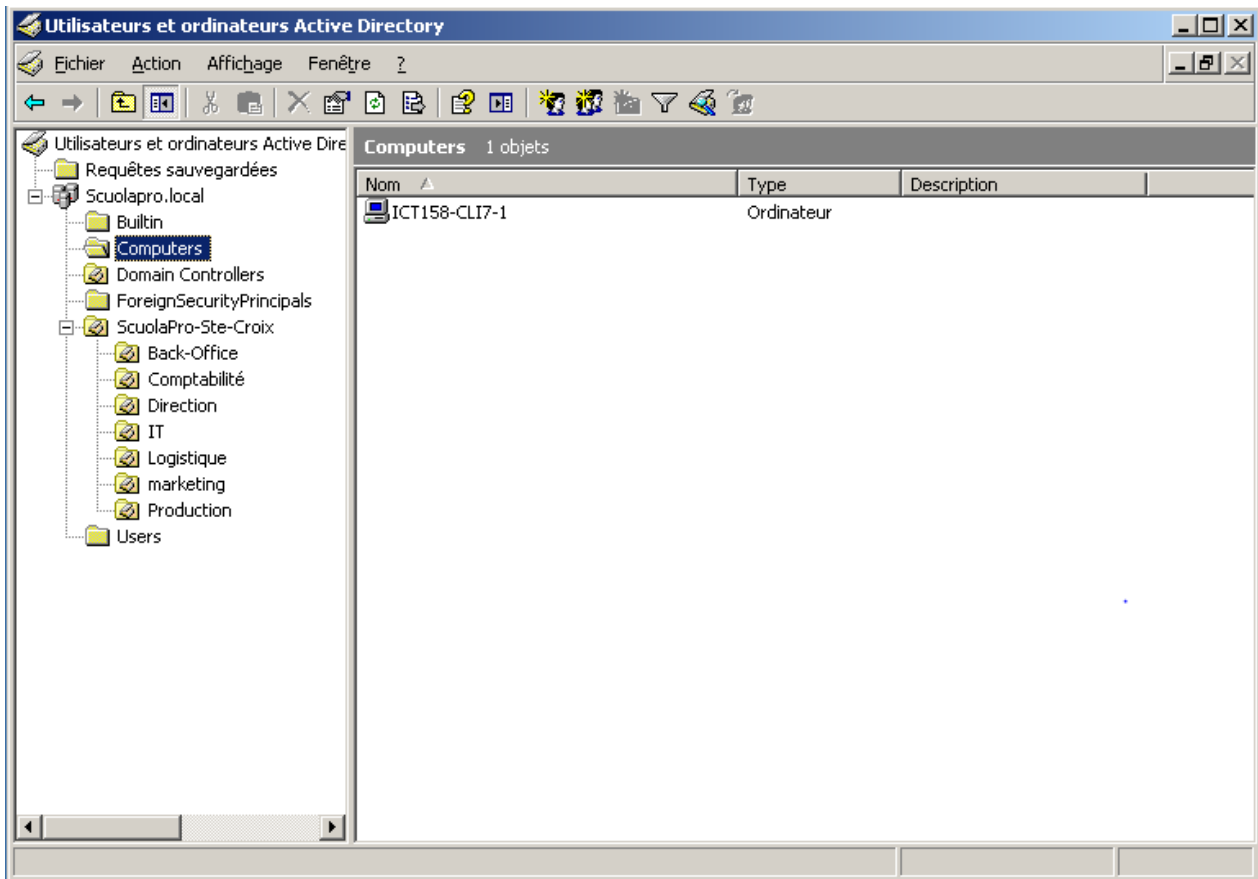
Niveau fonctionnel du domaine :  
Windows 2000 mixte

Niveau fonctionnel de la forêt :  
Windows 2000

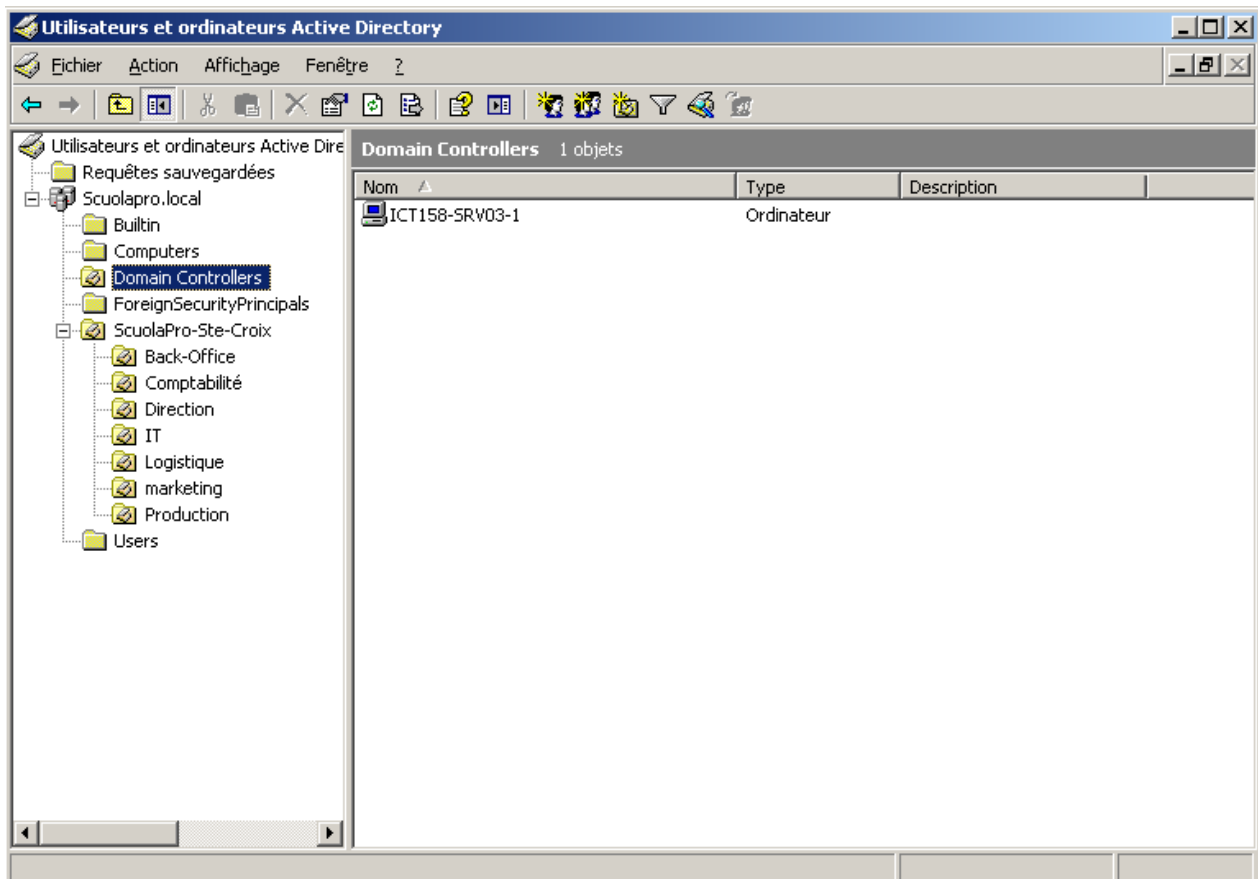
Ici on peut retrouver les groupes utilisateurs créés par défaut par l'OS.



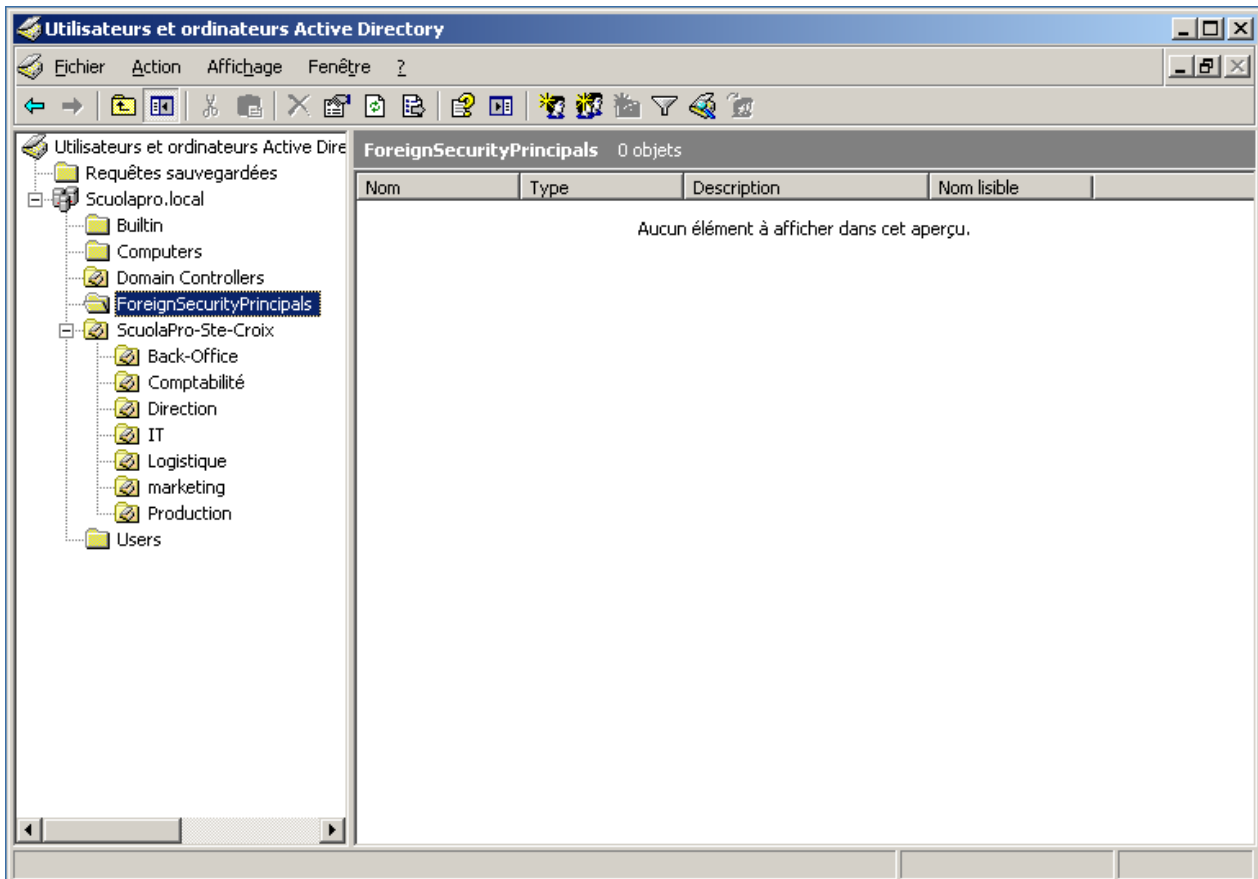
Ici on retrouve les machines du réseau.



Ici on retrouve le contrôleur de domaine qui est le serveur lui-même.



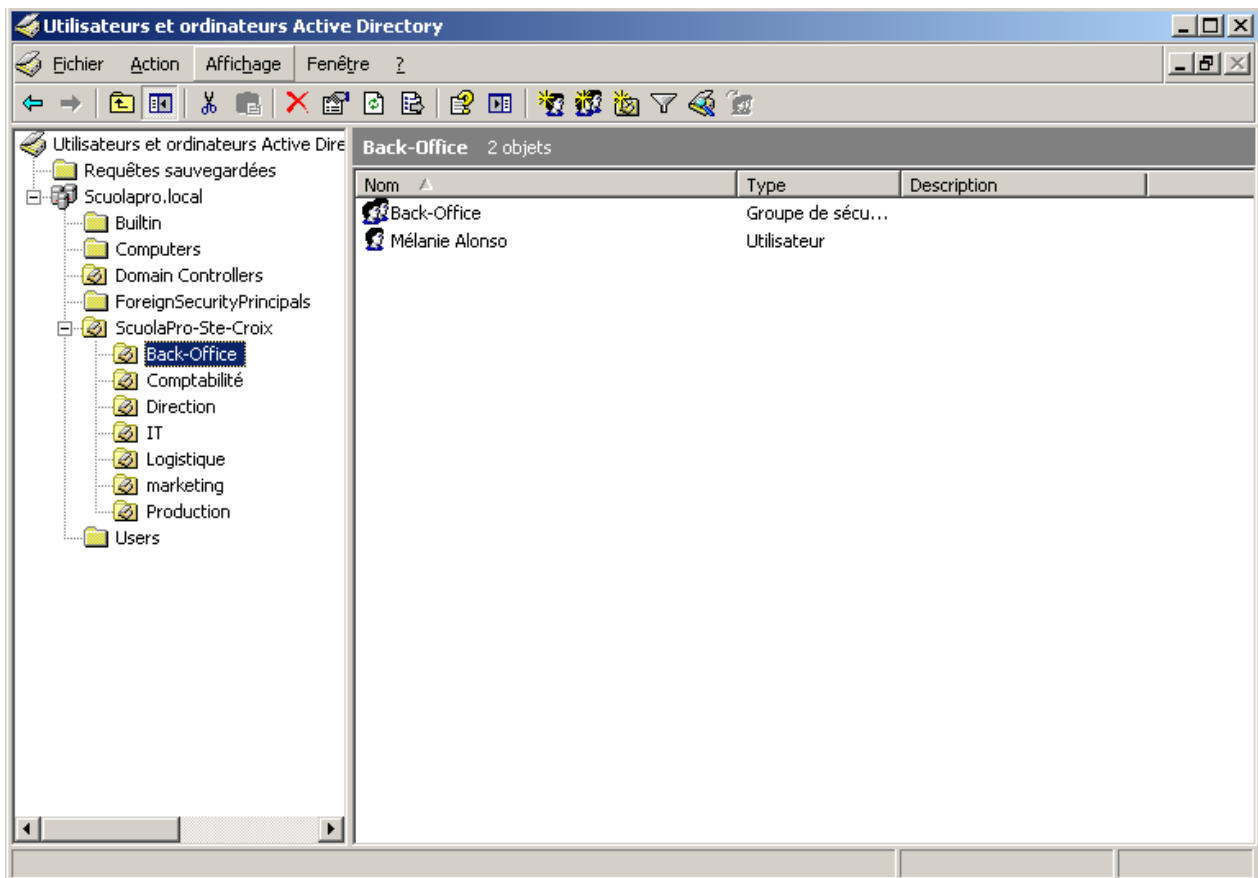
Aucun principe de sécurité étrangère



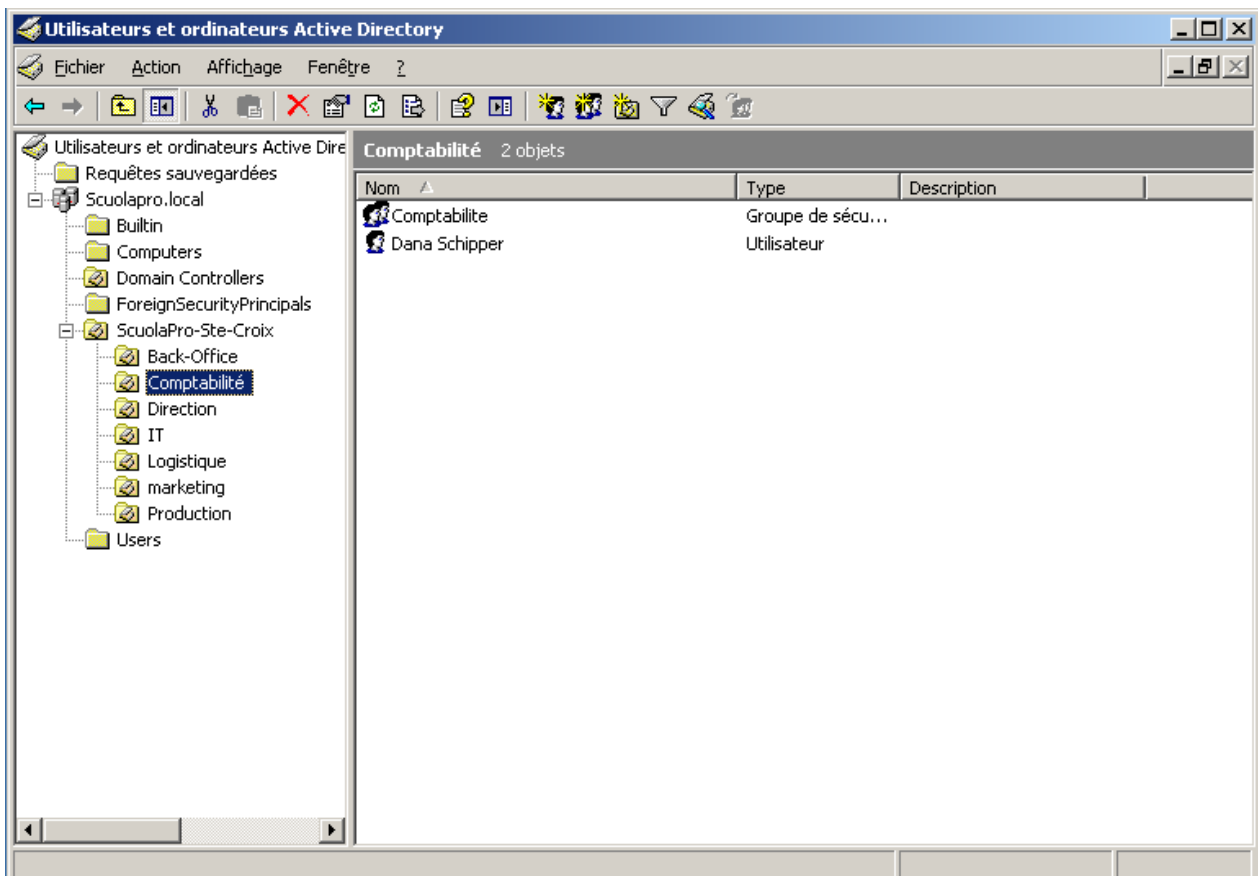
## Unité d'organisation

Dans l'unité d'organisation "ScuolaPro-Ste-Croix", on peut retrouver un groupe pour chaque département contenant les utilisateurs concernés.

Dans Back-office, le groupe Back-Office et L'utilisatrice Mélanie-Alonso, le groupe Back-Office ne possède actuellement aucun membre et Mélanie ne fait partit d'aucun autre groupe

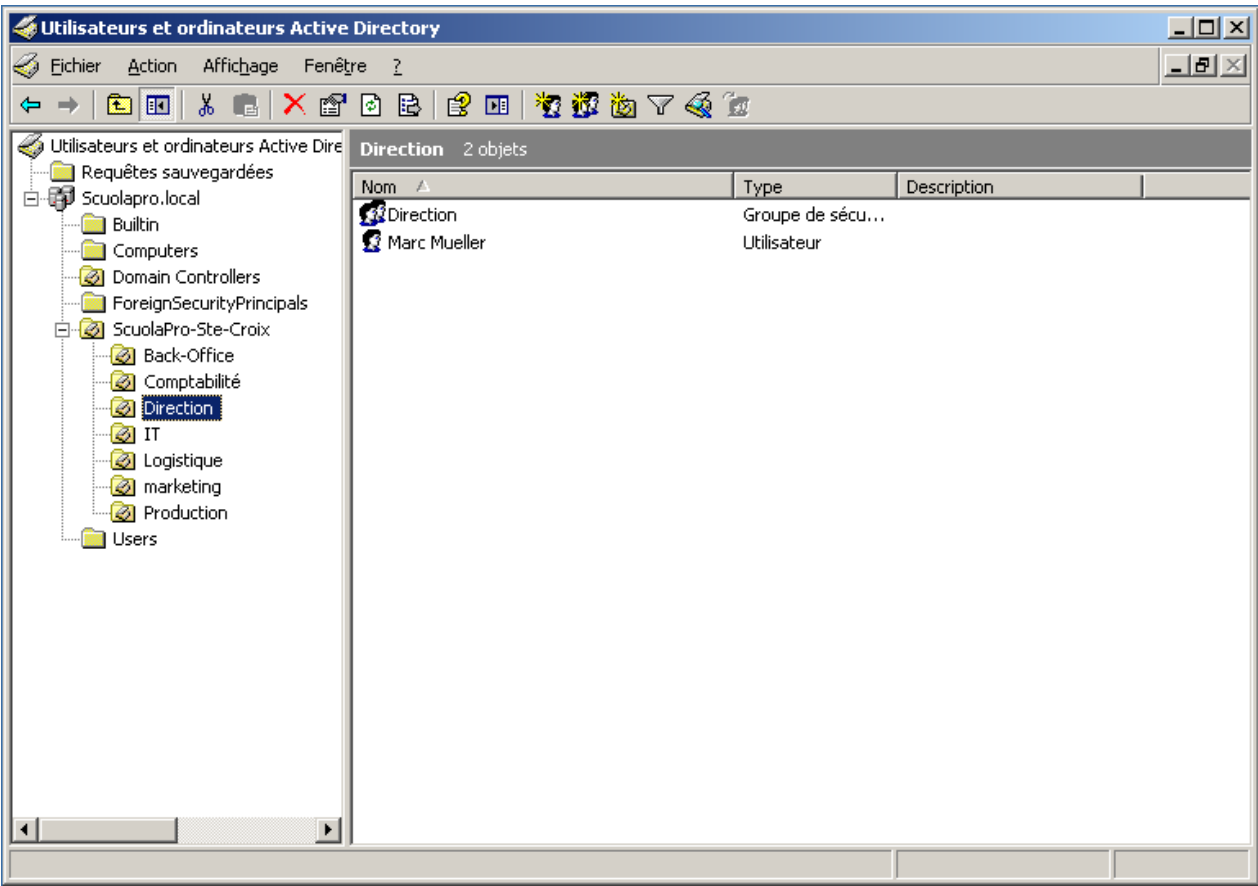


Dans Comptabilité, le groupe Comptabilite et L'utilisatrice Dana Schipper, le groupe Comptabilite ne possède actuellement aucun membre et Dana ne fait partit d'aucun autre groupe

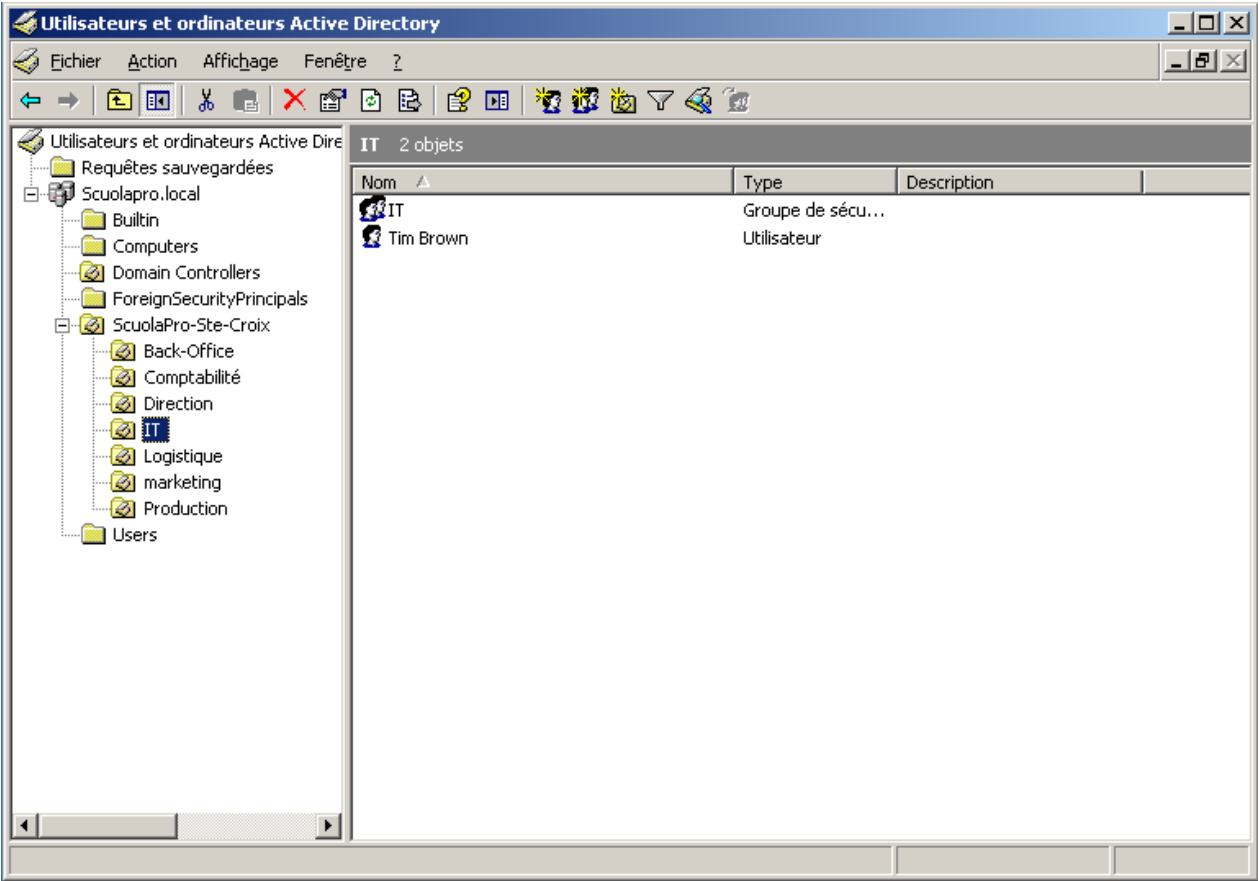




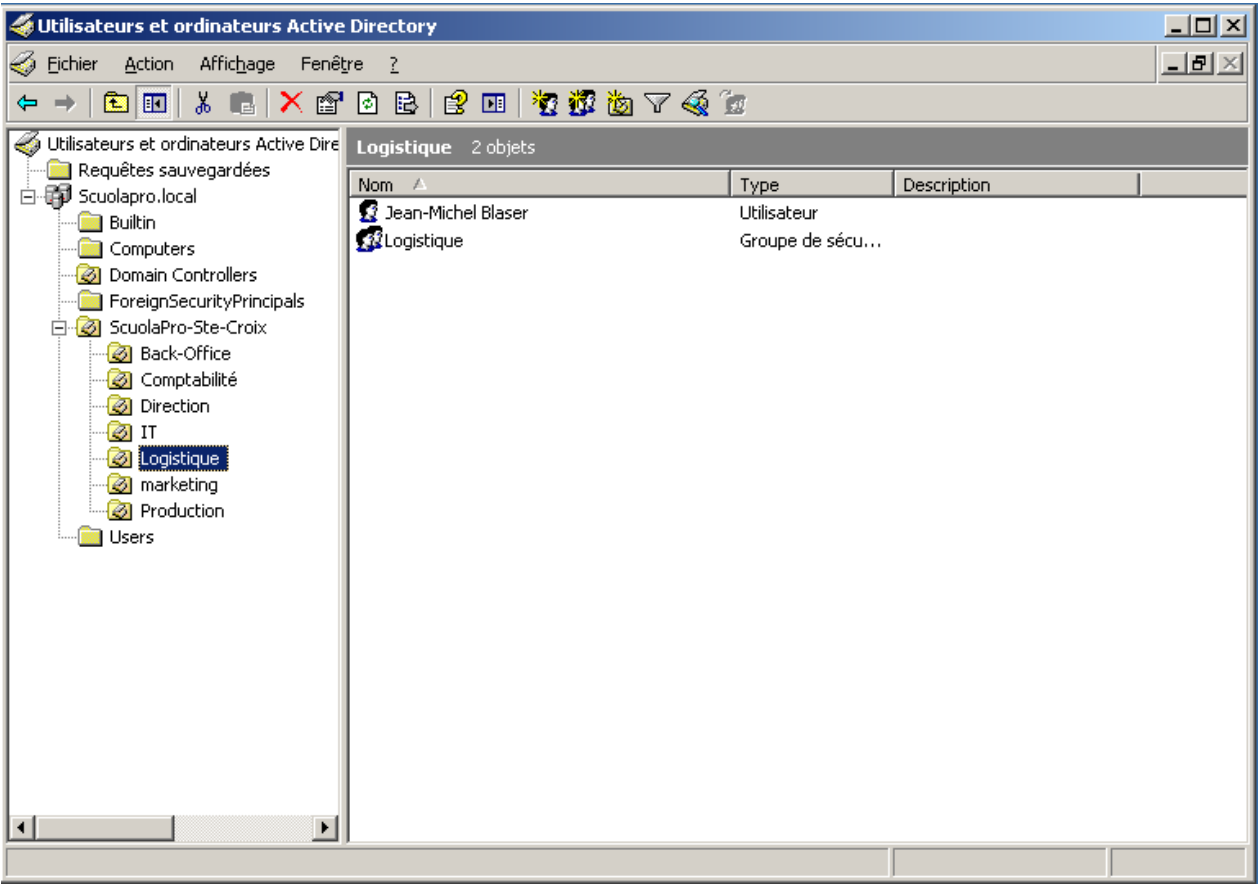
Dans Direction, le groupe Direction et L'utilisateur Marc Mueller, le groupe Direction ne possède actuellement aucun membre et Marc ne fait partit d'aucun autre groupe



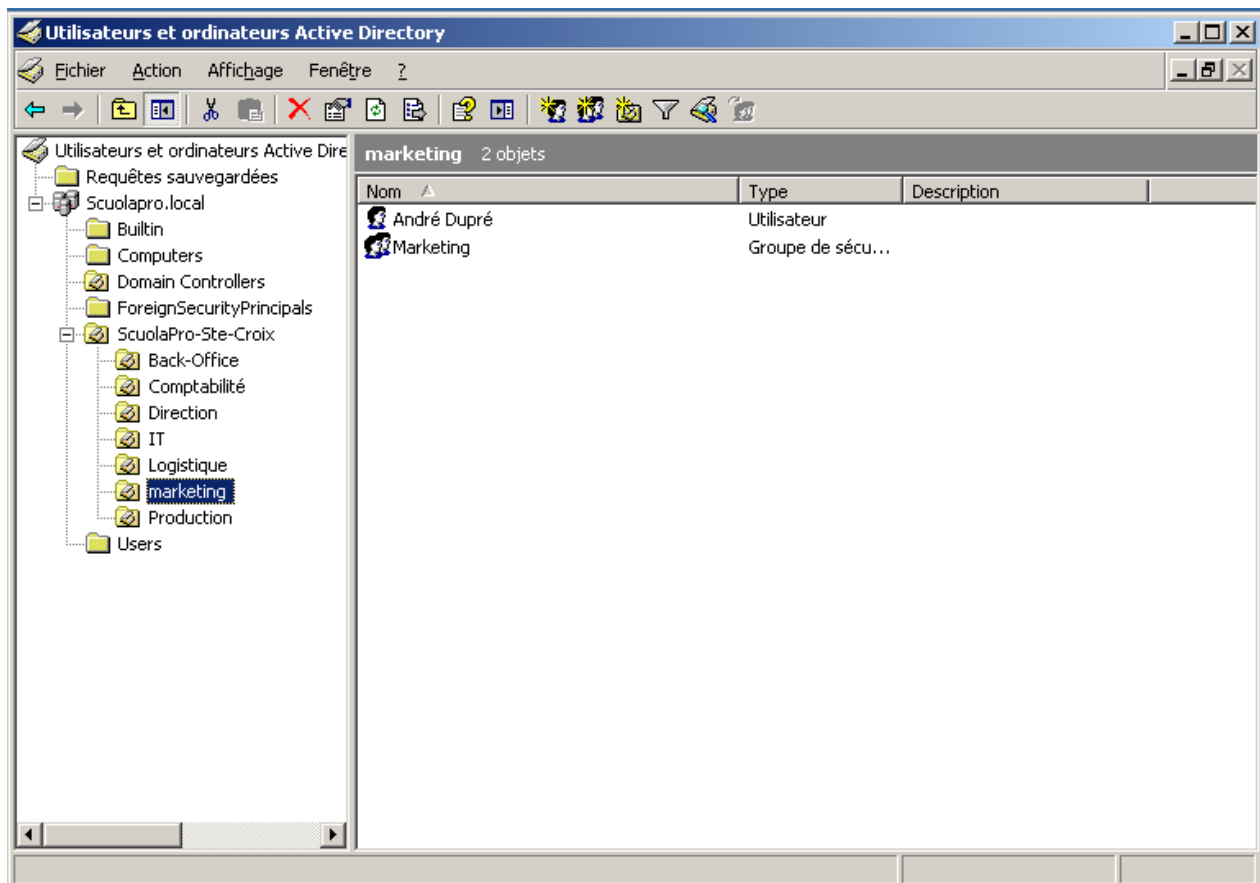
Dans IT, le groupe IT et L'utilisateur Tim Brown, il fait bien partit du groupe IT et aucun d'autre.



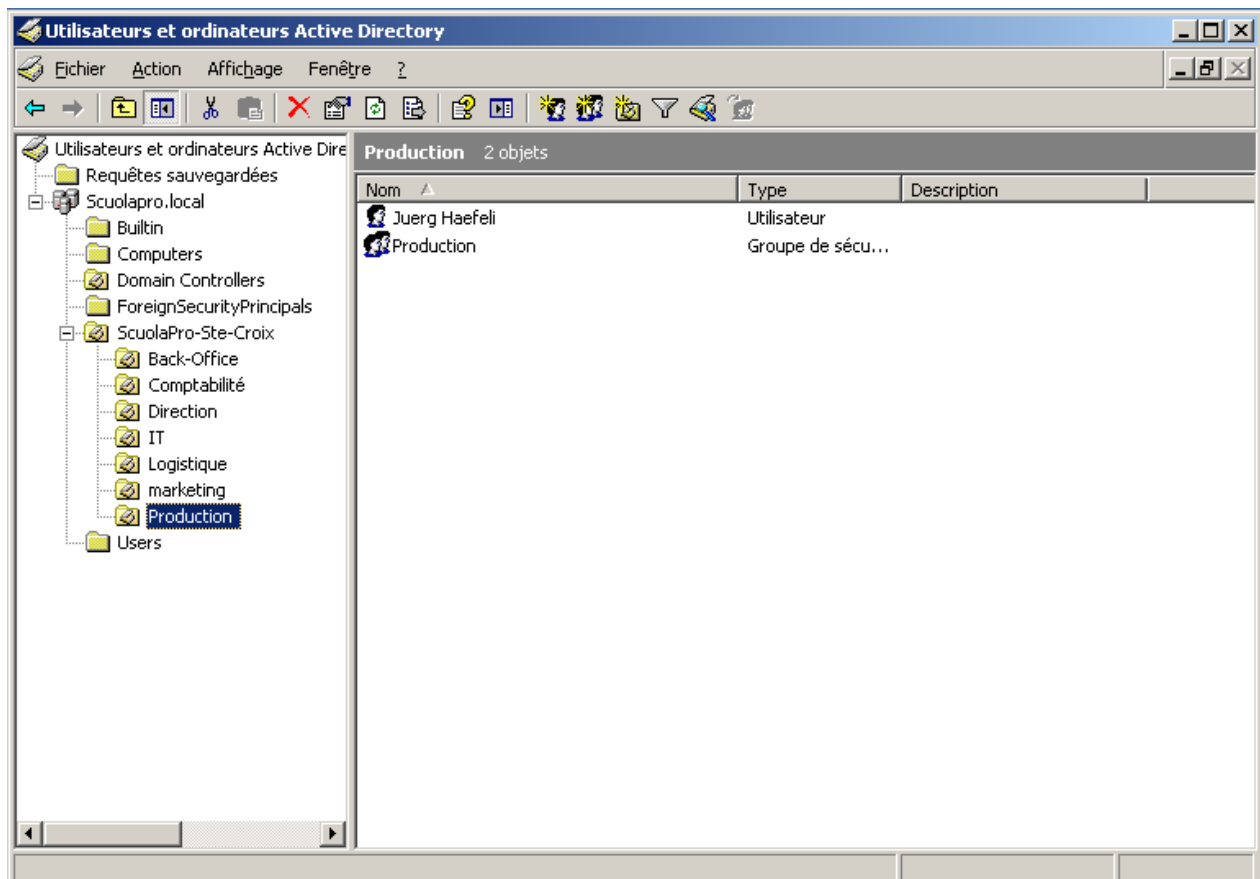
Dans Logistique, le groupe Logistique et L'utilisateur Jean-Michel Blaser, il fait bien partit du groupe Logistique et aucun autre.



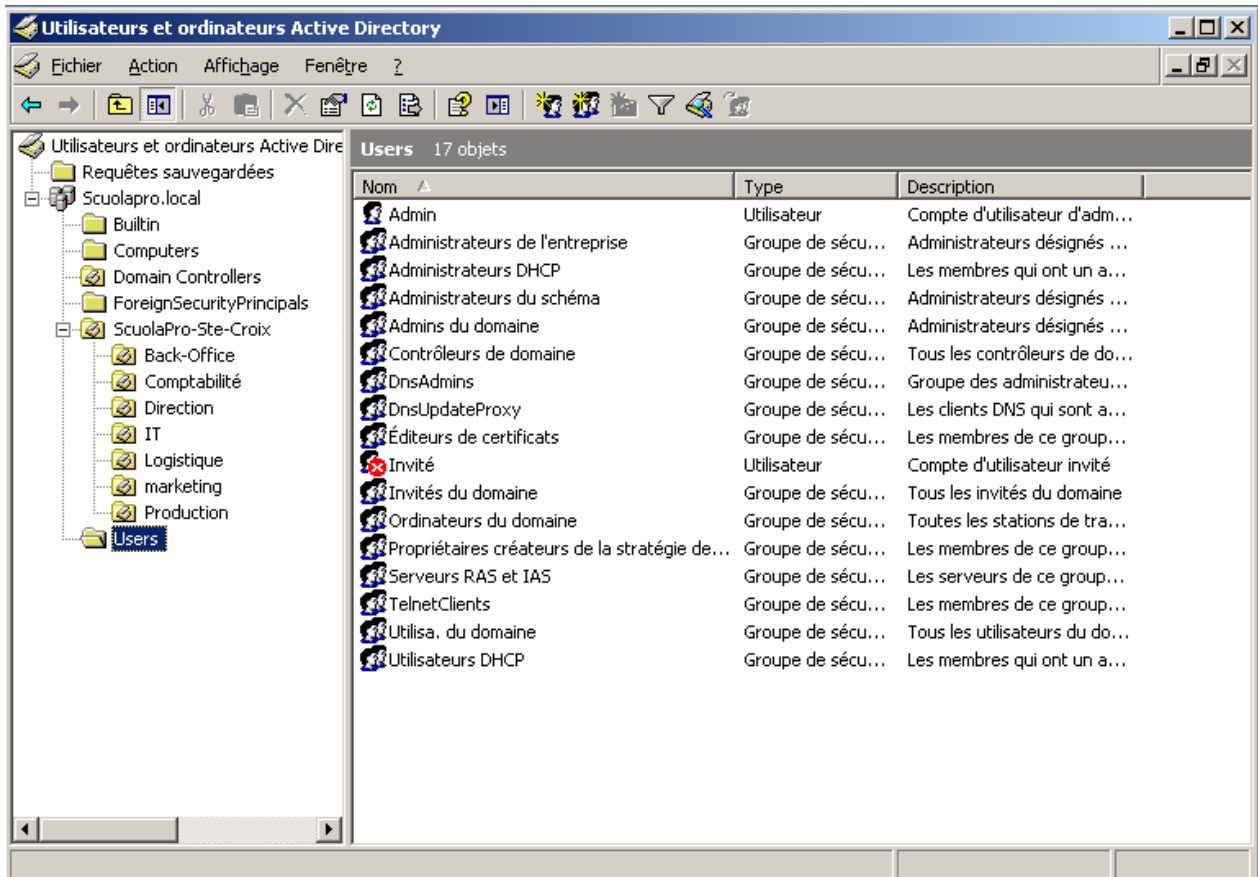
Dans marketing, le groupe Marketing et L'utilisateur André Dupré, le groupe Marketing ne possède actuellement aucun membre et André ne fait partit d'aucun autre groupe



Dans Production, le groupe Production et L'utilisateur Juerg Haefeli, le groupe Comptabilite ne possède actuellement aucun membre et Dana ne fait partit d'aucun autres groupes.

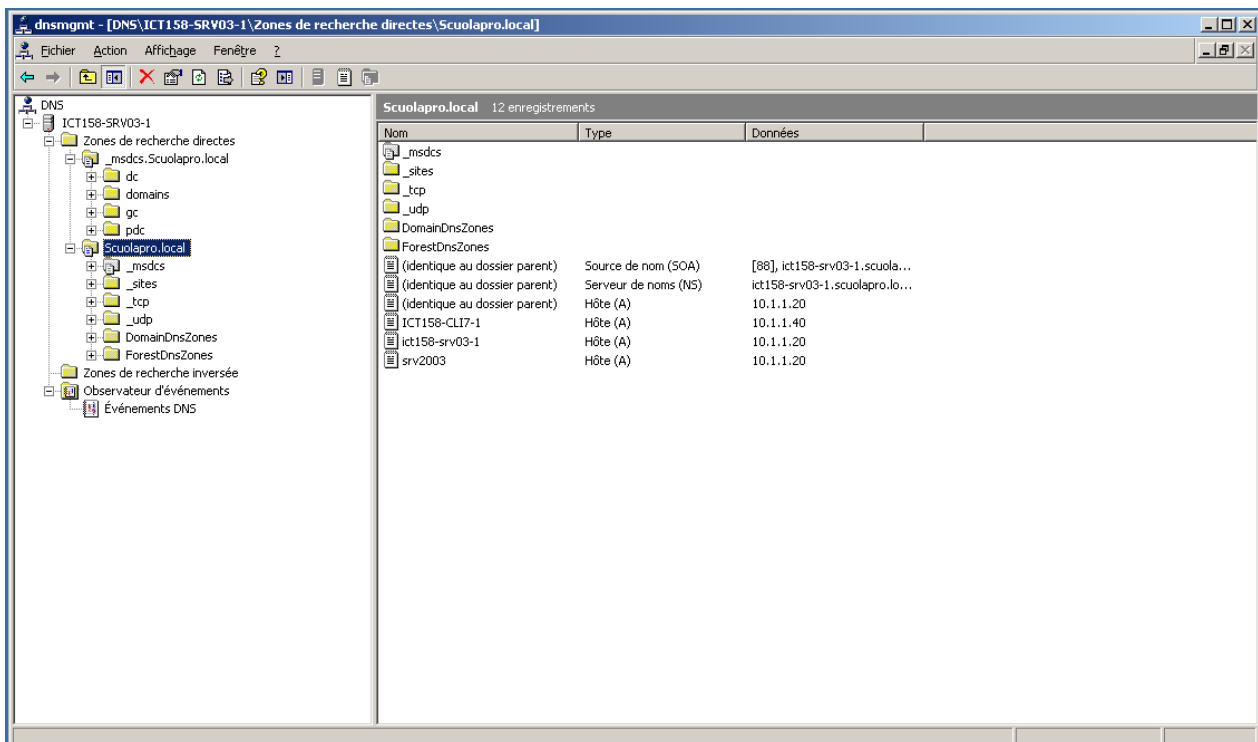


Ici on peut retrouver les différents autres groupes.

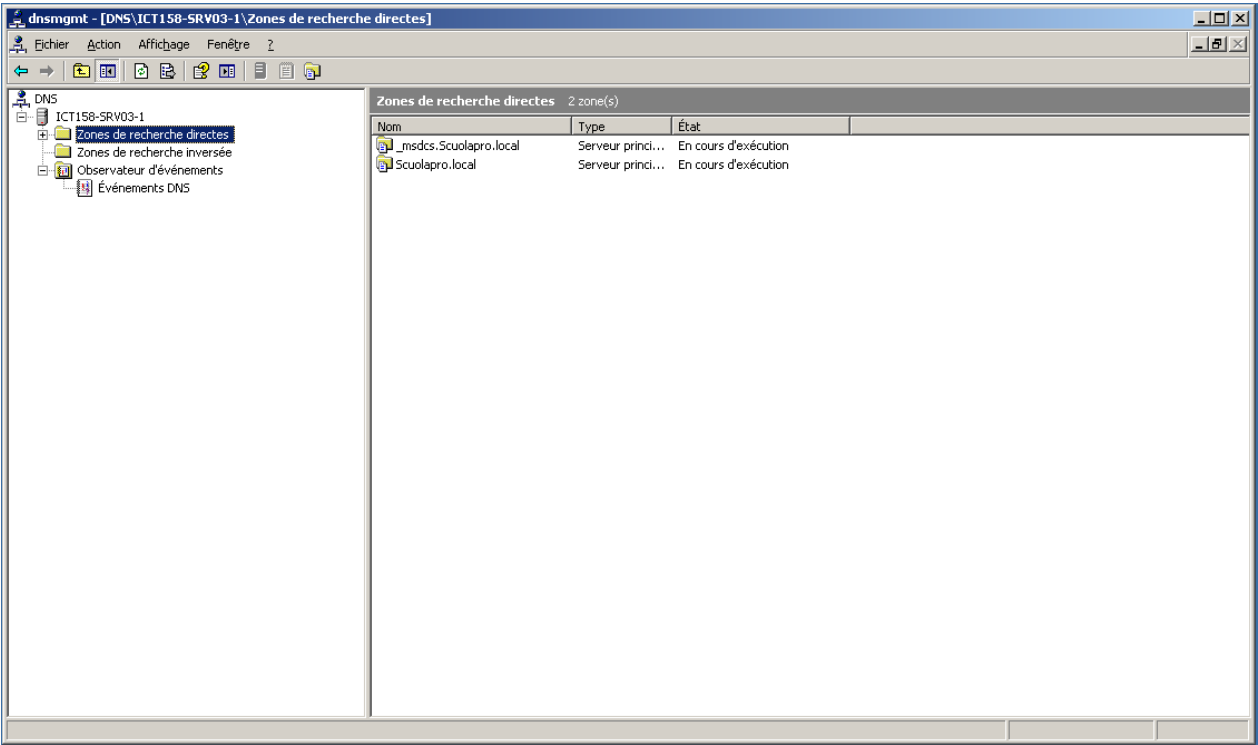


## DNS

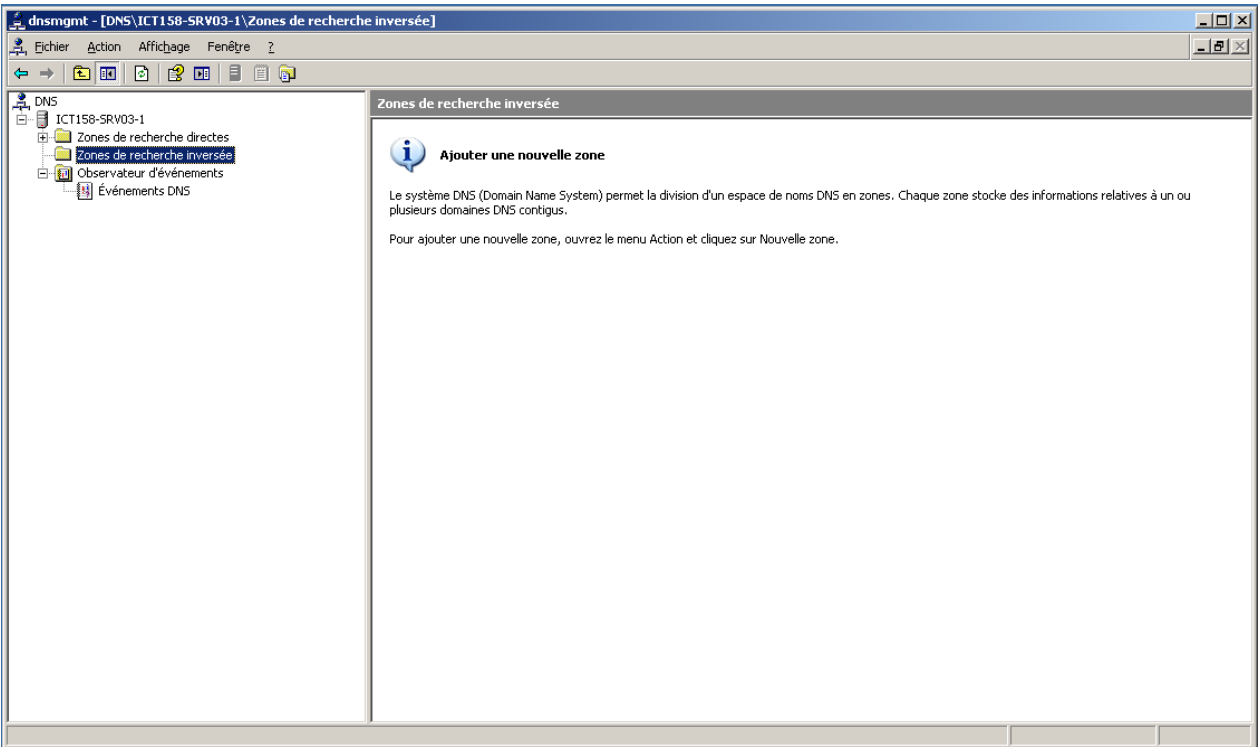
Les options du serveurs DNS :



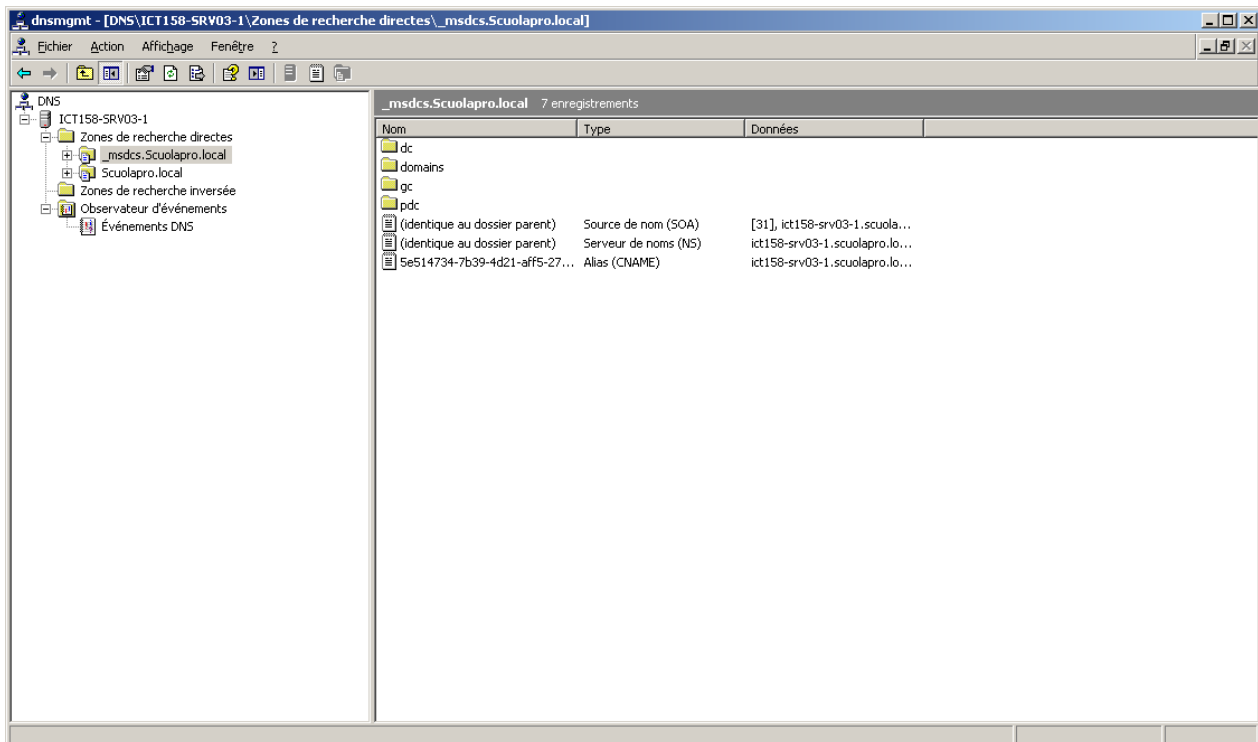
Dans la zone de recherche directe, le domaine ScuolaPro.local



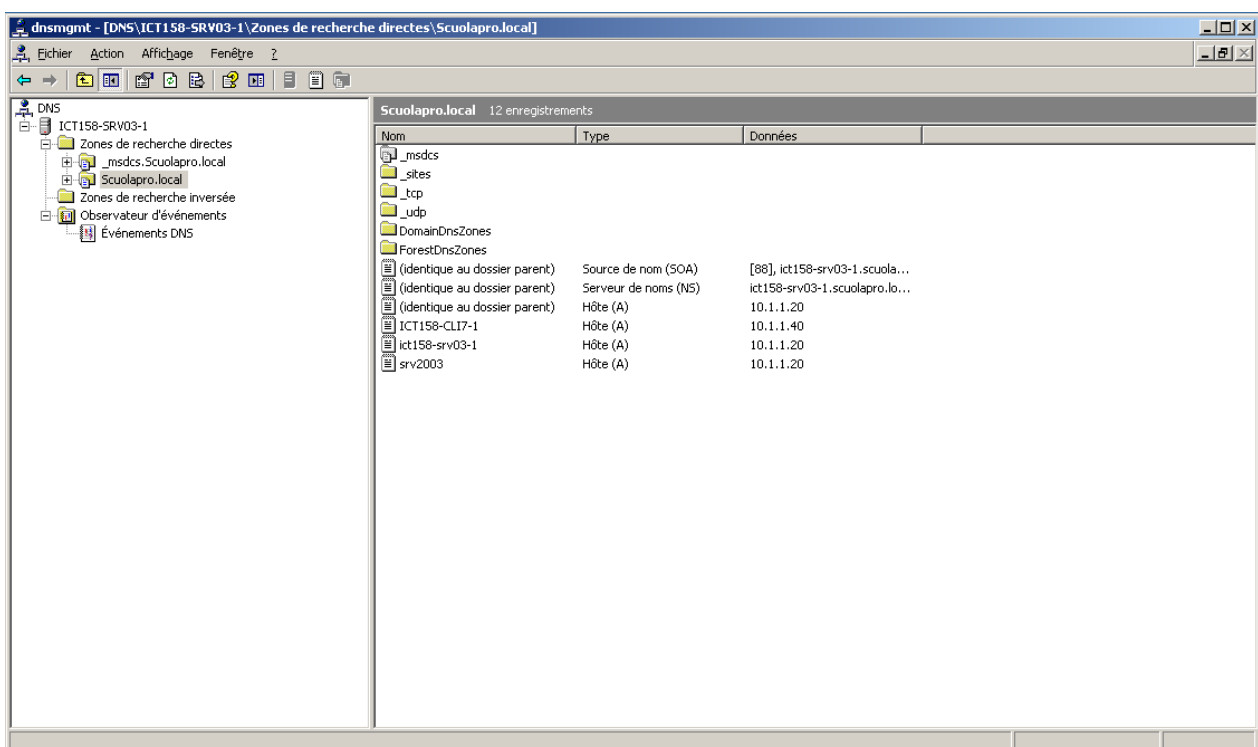
Aucune zone de recherche inversée



Ici on peut notamment retrouver le FQDN du domaine, il y a également un alias CNAME "5e514734-7b39-4d21-aff5-270ee42d3261.\_msdcs.Scuolapro.local"



Ici on peut retrouver tout les hotes du domaine.



## File Server

Les partages local, il y un total de 12 partages différents, un partage caché pour le disque C avec droits de lecture et exécution pour tout les utilisateurs, tout les partages ont tout les droits pour le groupe administrateurs.

Un partage caché pour le disque D: sans droits particuliers.

Un partage sur le dossier Downloads, les créateurs de fichiers et dossiers n'ont aucun droits.

Un partage sur le dossier Echange, les créateurs de fichiers et dossiers n'ont aucun droits.

Un partage caché IPC aucune idée de quoi il s'agit.

Un partage NETLOGON, avec comme droits de lecture et exécution pour le groupe utilisateurs authentifiés et opérateurs de serveurs, aucun droits pour les créateur propriétaire.

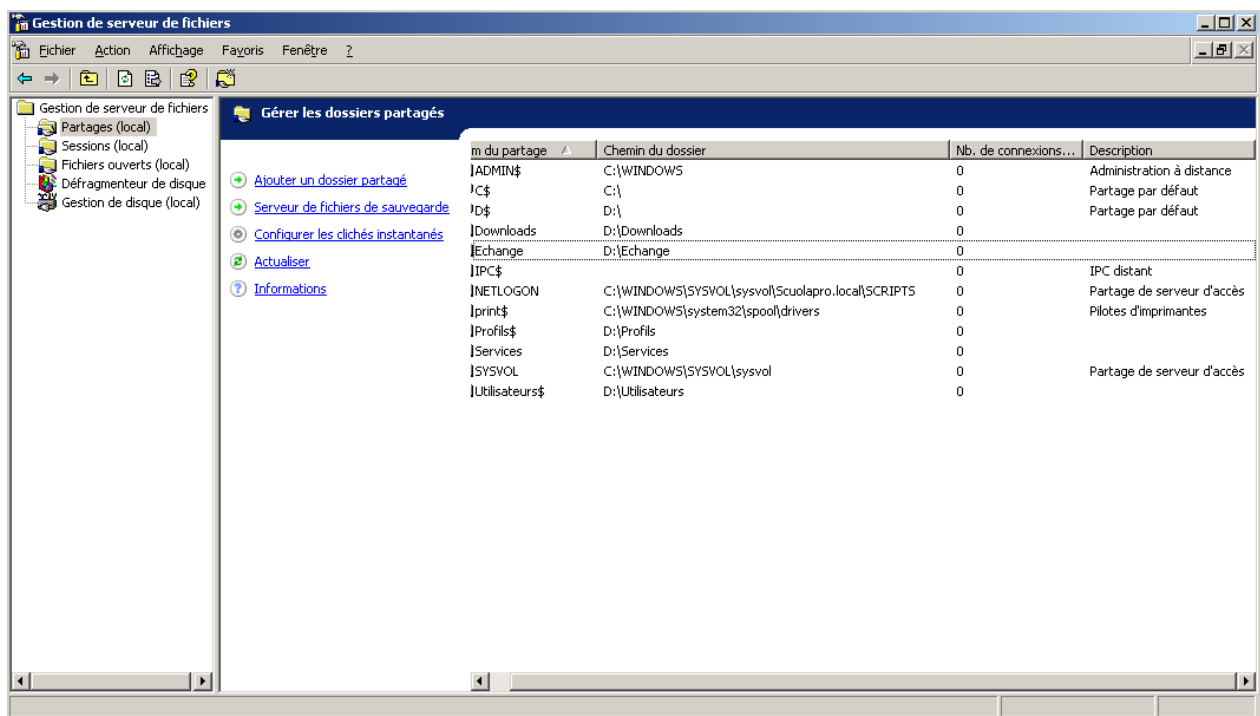
Un partage caché pour le dossier print qui contient les spools d'impression, createur propriétaire aucun droit, opérateur de serveur Modification, opérateur d'impression tout les droits, tout le monde droits de lecture et exécution et utilisateurs authentifiés également droit de lecture et exécution.

Un partage caché profil, créateur propriétaire aucun droit, utilisateur du domaine droit de modification.

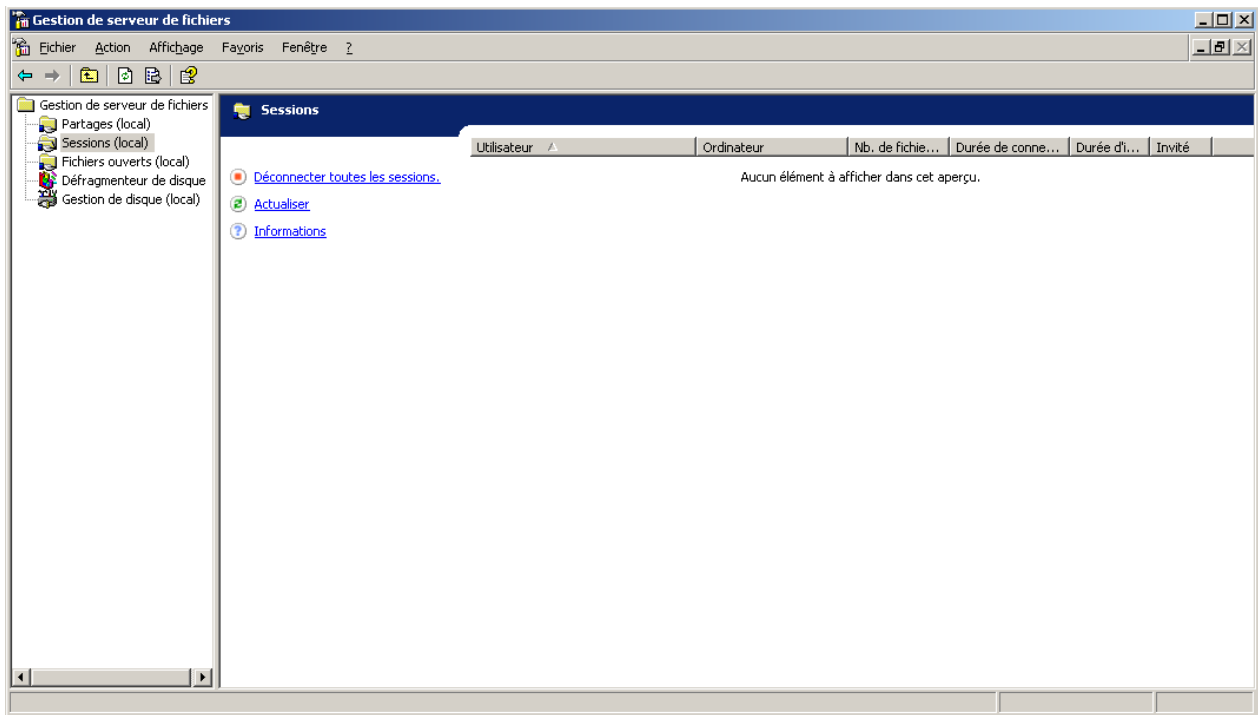
Un partage Services, créateur propriétaire aucun droits.

Un partage SYSVOL, créateur propriétaire aucun droit, opérateur de serveur et utilisateurs authentifiés droits de lecture et exécution.

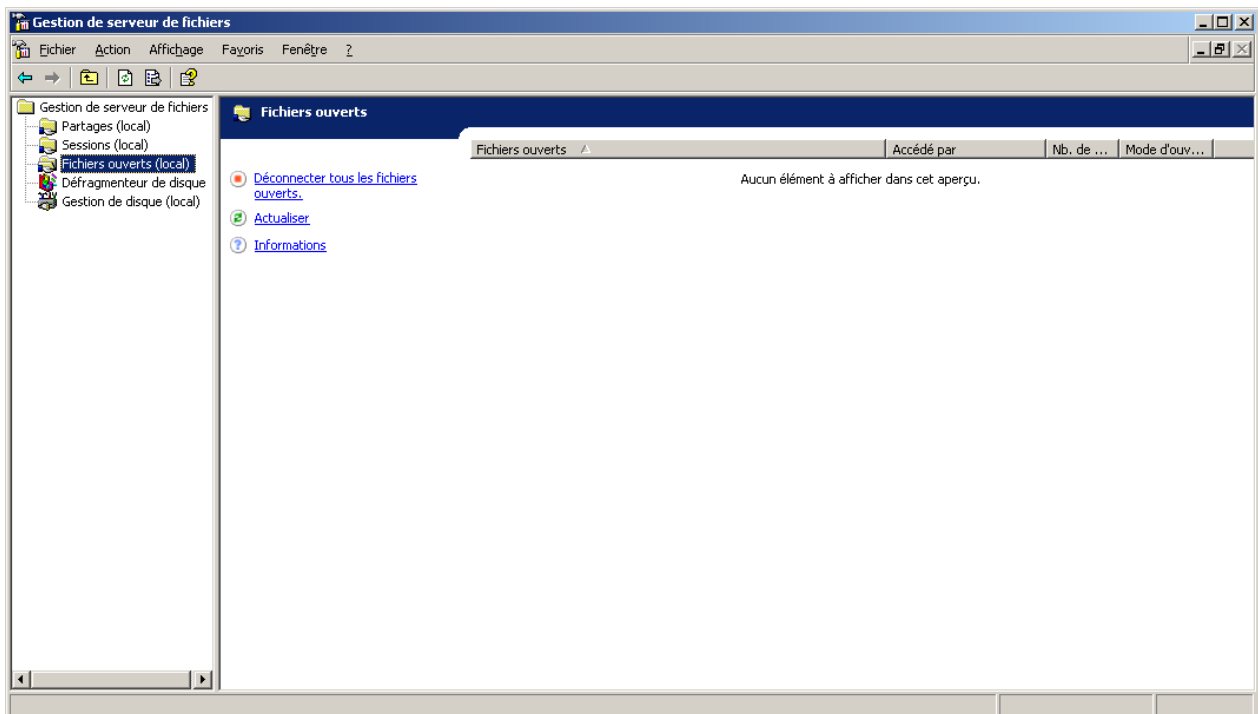
Un partage caché utilisateur, créateur propriétaire aucun droits.



Aucune Session locale :

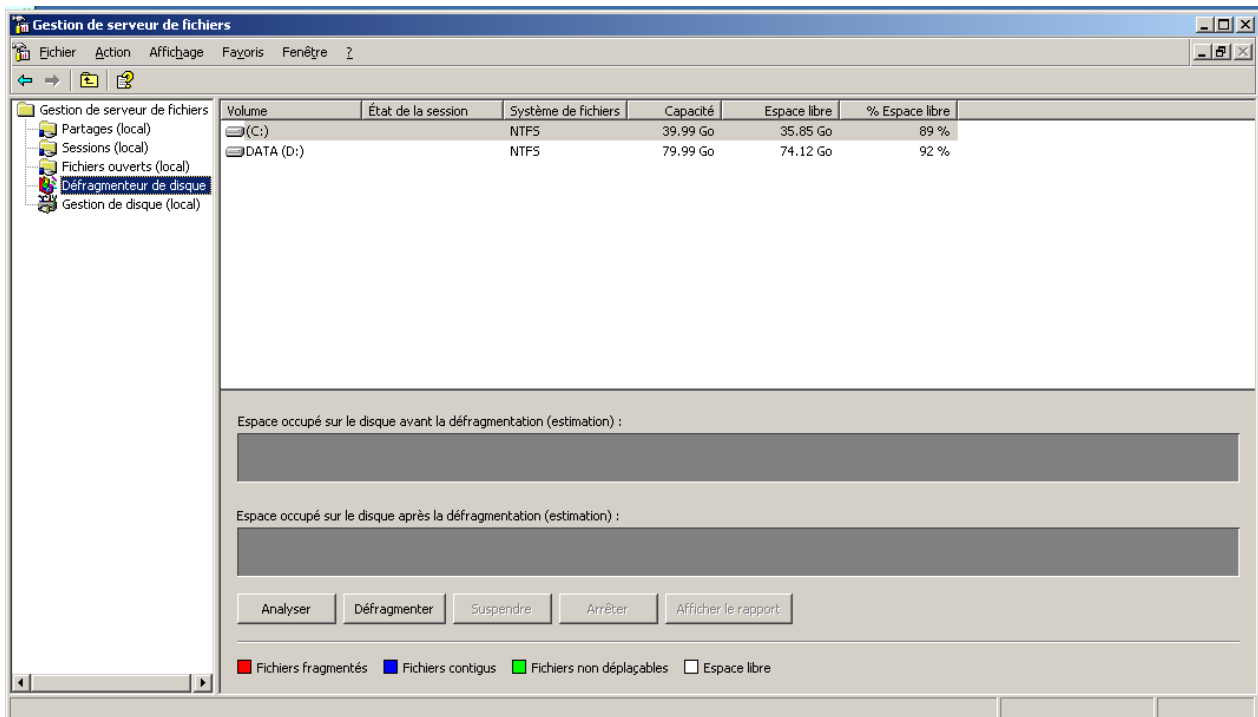


aucun fichiers d'ouverts :

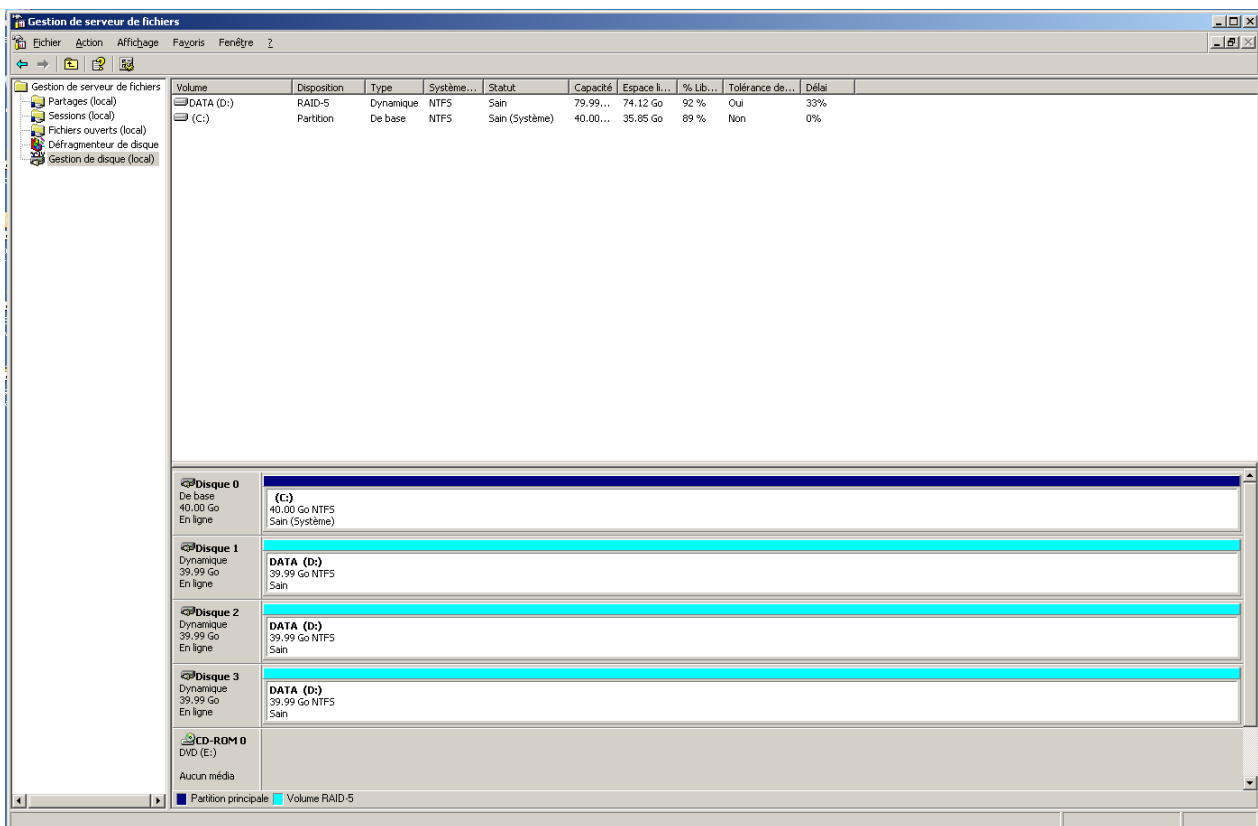


Pour défragmenter les disques :



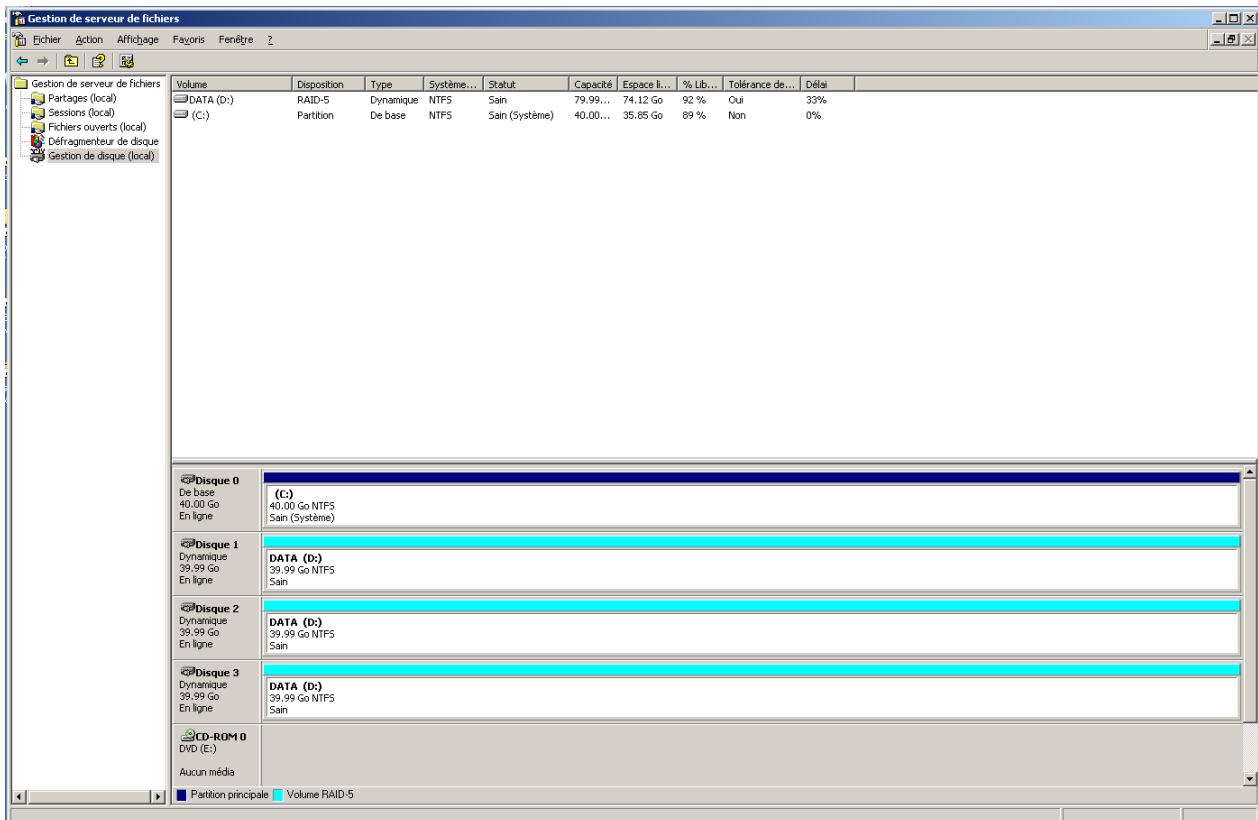


Les options de partitions de disques :

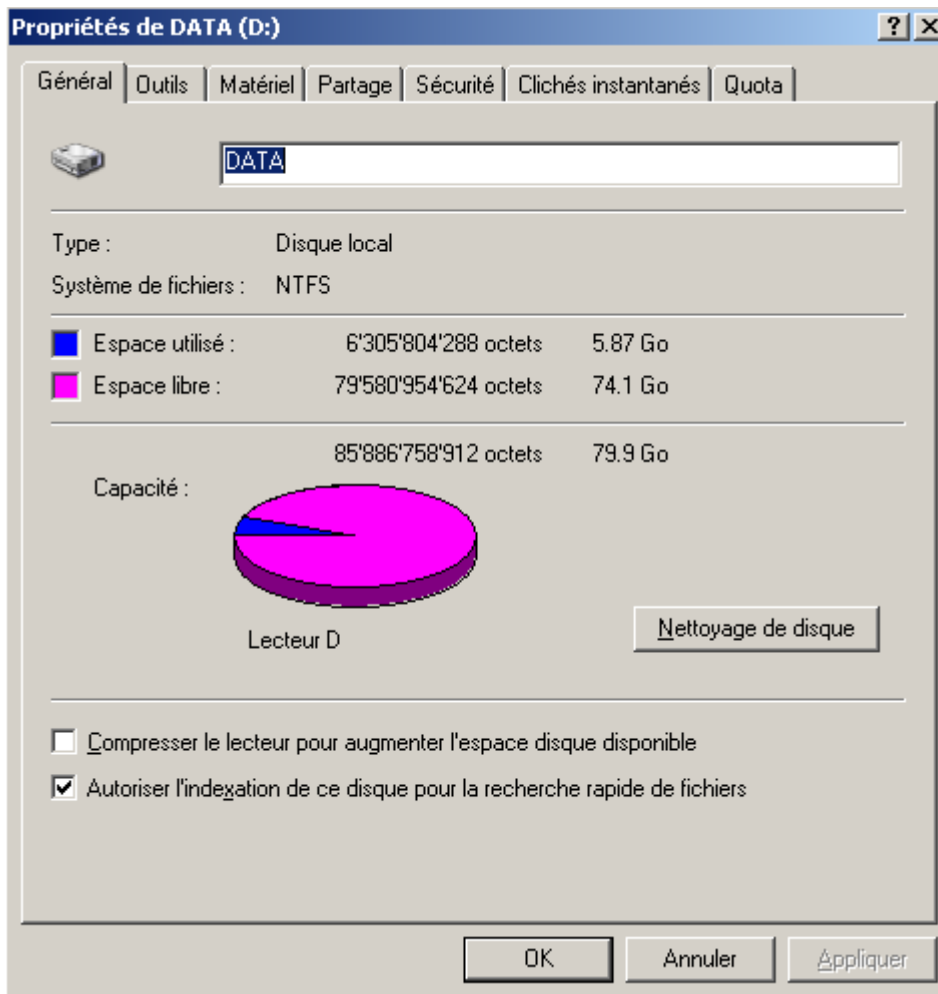


## Raid5

Le raid 5 est partagée en plusieurs partitions nommée Data avec comme lettre d: entre les disques 1 à 3 avec une capacité totale de 80 Go ainsi que de type NTFS et le disque c: de 40Go également de type NTFS.





Le disque D: possède 74.1 Go de disponible mais seulement 5.87 Go sont utilisés pour un total de 80 Go de base.



Le dossier Download contient un dossier image qui contient l'image du client windows 7.

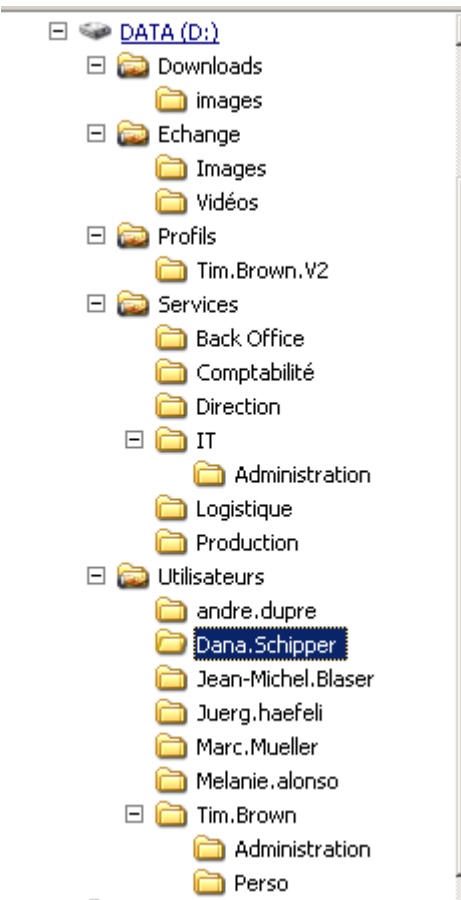
Le dossier Exchange contient un dossier Images et Vidéos qui sont vide les deux.

Le dossier Profils contient uniquement le dossier de Tim Brown, qui contient lui même un dossier Administration vide et un dossier Perso également vide.

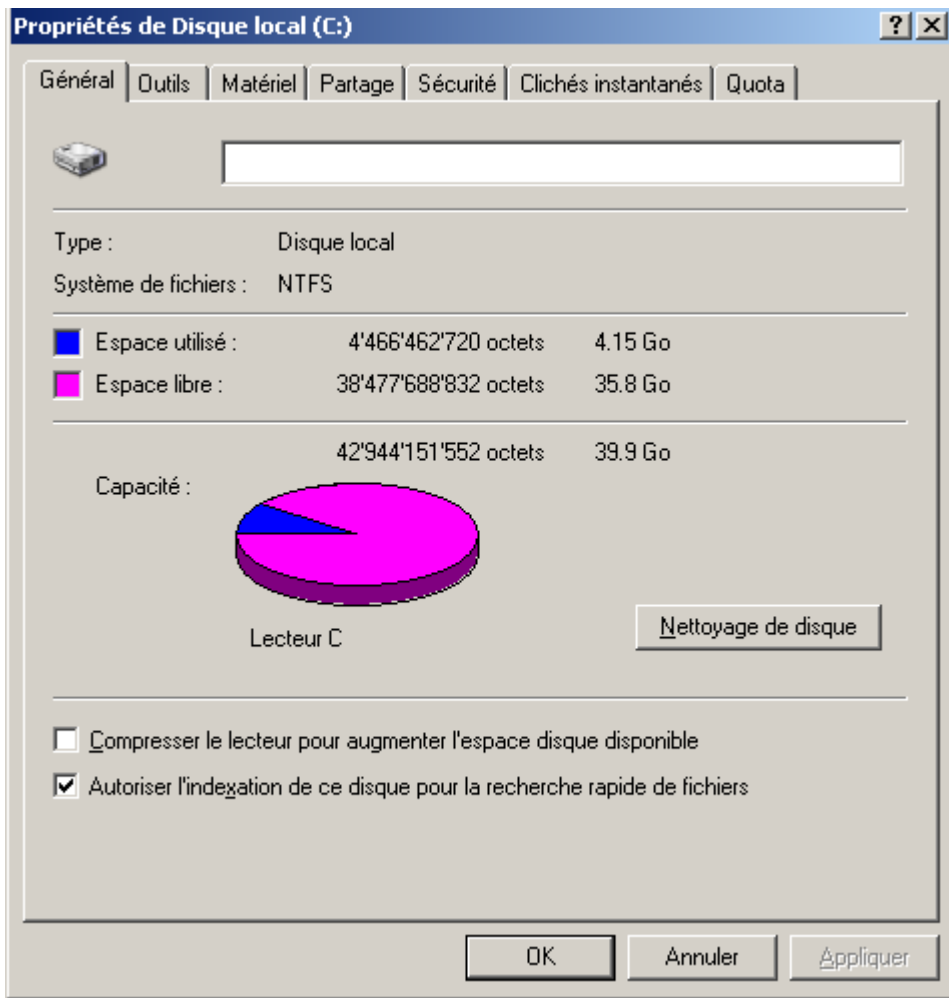
 Administration	03.10.2016 01:18	Dossier de fichiers
 Perso	03.10.2016 01:18	Dossier de fichiers

Le dossier Services contient tout les services de l'entreprise, seul le dossier IT contient un dossier Administration vide.

Le dossier Utilisateur contient tout les dossiers des utilisateurs de l'entreprise, seul le dossier de Tim Brown contient comme mentionné auparavant un dossier administration et Perso qui sont les deux vides.



Le disque C: qui possède 35.8 Go de libre et 4.15 Go d'utilisés pour un total de 40Go de base.



Il contient tout les fichiers systèmes destinés au fonctionnement du serveur.

Il y a également un lecteur disquette(A:) ainsi qu'un lecteur de disque DVD (E:).

## Client

### Hardware :

- 35 machines clientes de type [Dell Latitude E6510](#) cliquez sur le nom pour afficher la documentation Dell. Le Dell latitude E6510 est incompatible avec Windows 10.
- 10 machines clientes de type [Dell Latitude E6530](#) cliquez sur le nom pour afficher la documentation Dell. Le Dell latitude E6530 est compatible avec Windows 10.
- 5 machines clientes de type [Dell Optiplex 990](#) cliquez sur le nom pour afficher la documentation Dell. Le Dell Optiplex 990 n'est pas compatible avec Windows 10. Car Dell n'a pas mis à disposition des pilotes qui supportent Windows 10 sur ces PC.

### OS de la machine client :

Windows 7 Entreprise 64 bits [Service Pack 1](#)

### Réseau :

---

Nom de l'hôte : ICT158-CLI7-1

Suffixe DNS Principal : Scuolapro.local

Adresse physique : 00-0C-29-D6-17-2F

Adresse IPv4 : 10.1.1.41

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : 10.1.1.1

Serveur DHCP : 10.1.1.20

Serveur DNS : 10.1.1.20

## Logiciels :

---

### Office :

Version Office : 11.5604.5606

Office 2003 est compatible avec Windows 10.

### Antivirus :

Nom : Avira Antivirus

Version du produit : 15.0.20.59 -> Date : 25.08.2016

License : Version gratuite

### Bureau à distance :



### Adobe reader :

FireFox :

Version : 49.0.1

XMind :

Version : 7.5 Update 1 (R3.6.51.201607142338)

License : Pas de license

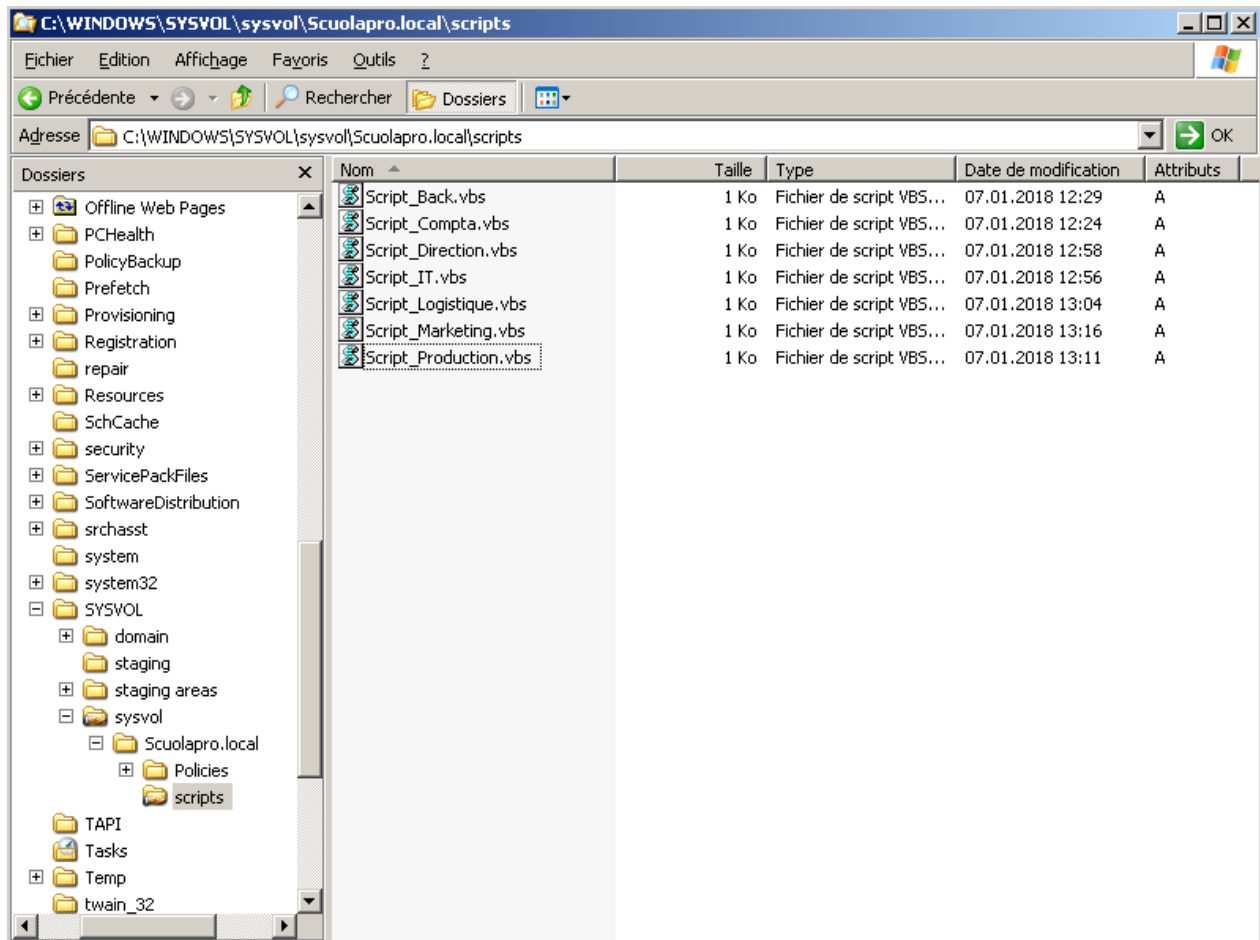
UltraVNC :

Version : 1.2.1.1

## Script Logon

Il y a un script différent pour chaque utilisateur selon son affiliation aux départements, pour l'instant le seul profil de créer et celui de Tim Brown, aucun autre profil ne figure dans le dossier Profils.

Le chemin où sont stocker tout les scripts :



Le contenu du script Back, servant à créer la session pour l'utilisatrice Melanie Alonso comme il s'agit de l'unique membre du Back Office. On peut voir que le script mappe un lecteur E: avec le contenu du dossier Back-Office et le script ajoute également l'imprimante HP\_Back, chaque script fait les mêmes actions mais en changeant à chaque fois d'utilisateurs et d'imprimantes en fonction des affiliations.

```
Script_Back.vbs - Bloc-notes
Fichier Edition Format Affichage ?
Option Explicit

Dim WSHNetwork, oNet, Printers, user

set WSHNetwork = wscript.CreateObject("wscript.Network")
Set oNet = CreateObject("wscript.Network")

'contrôle de l'utilisateur
user = WSHNetwork.UserName

' et transformation du username en majuscule
user = UCase(user)

select Case user

Case "MELANIE.ALONSO"

    oNet.MapNetworkDrive "E:", "\\ICT158-SRV03-1\Services\Back-office"
    WScript.Echo "User Name = " & user
    Printers = "\\ICT158-SRV03-1\HP_Back"
    WSHNetwork.AddWindowsPrinterConnection Printers

    WSHNetwork.SetDefaultPrinter Printers

Set Printers = nothing
WScript.Quit
```

## Profils itinérants

Dans cette capture on peut voir le chemin du profil de l'utilisateur, ils ont tous le même chemin mais en changeant juste le chemin selon leur prénom et nom, comme mentionné auparavant seul le profil de Tim Brown a été créé, il contient aucun octet de données.

Profil utilisateur	
Chemin du profil :	<input type="text" value="\\ICT158-SRV03-1\Profils\$\Melanie.alonso"/>
Script d'ouverture de session :	<input type="text" value="Script_Back.vbs"/>

## Dossier personnel

Chaque dossier perso des utilisateurs est monté sur un lecteur U:, changeant également nom en fonction de leur prénom et nom, seul le dossier de Tim Brown contient des dossiers, les dossiers Administration et Perso qui sont les deux vides, tout les dossiers possèdent 0 octets de données.

Dossier de base	
<input type="radio"/> Chemin d'accès local :	<input type="text"/>
<input checked="" type="radio"/> Connecter :	U: <input type="text" value="U:"/> à <input type="text" value="\\ICT158-SRV03-1\Utilisateurs\$\Melanie.alonso"/>