TP 6 : Installation d'un contrôleur de domaine

1. But du TP

A l'issue de ce TP, l'étudiant sera capable d'effectuer les tâches suivantes :

- Installation et configuration du contrôleur de domaine
- Tests d'ouverture de session
- Intégrer des stations au domaine
- créer des restrictions de groupe
- configurer les services d'impression
- Créations d'approbations

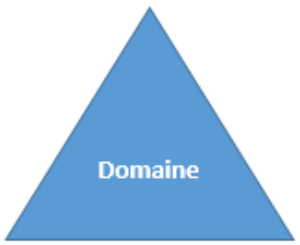
2. Modèle « *Groupe de travail* »

Toutes les machines sous Windows sont par défaut dans un **groupe de travail** nommé « ***WORKGROUP*** ». ce dernier permet de mettre en relation des machines d'un même groupe de travail, notamment pour le partage de fichiers, mais il n'y a pas de notions **d'annuaire**, ni de **centralisation** avec ce mode de fonctionnement (chaque machine contient sa propre base d'utilisateurs indépendante les unes des autres.). Par conséquence, ce modèle devient très vite inadapté dès que le nombre de postes et d'utilisateurs augmente, car cela devient lourd en administration et les besoins différents.

3. Modèle « *Domaine* »

Un domaine se réfèrent à un regroupement logique de serveurs et de machines clientes dans un réseau local. Il est géré par un serveur appelé **contrôleur de domaine**, qui est chargé d'autoriser les machines à rejoindre le domaine et d'autoriser les utilisateurs à accéder aux ressources de l'ensemble du domaine. Les domaines sont principalement utilisés dans le cadre des entreprises, pour gérer de manière centralisée les utilisateurs, les machines, etc.

Le domaine permet à l'administrateur système de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données (**annuaire**) stockée dans un **contrôleur de domaine**.

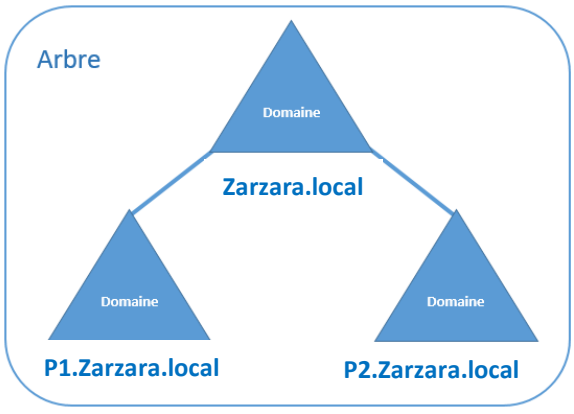


Symbolisation d'un domaine

4. Contrôleur de domaine

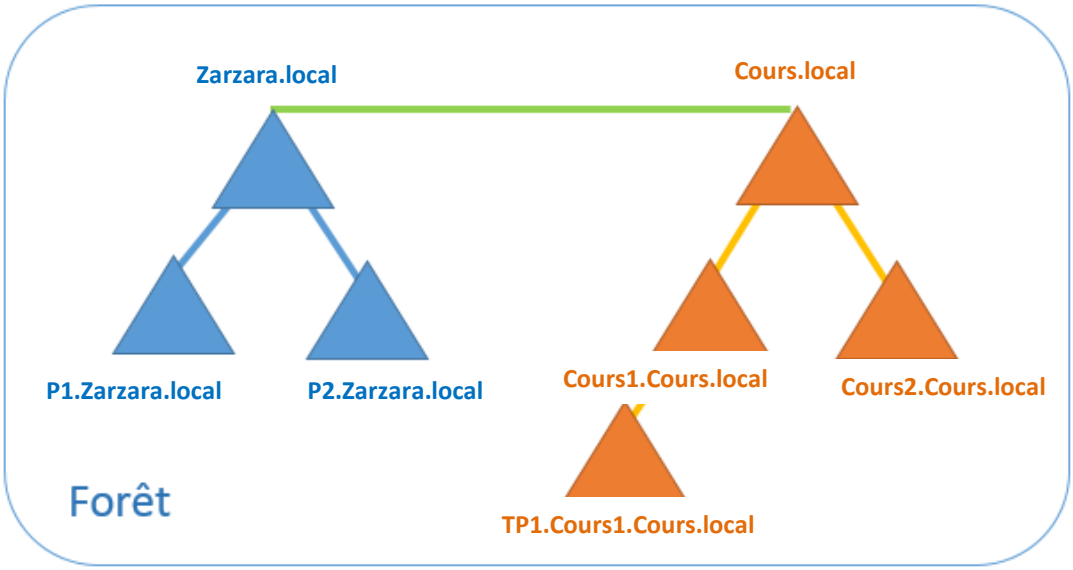
Lorsque l'on crée un domaine, le serveur depuis lequel on effectue cette création est promu au rôle de « **contrôleur de domaine** » du domaine créé. Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine. De ce fait, il devra vérifier :

- les identifications des objets (utilisateurs, ordinateurs, groupes, etc.),
- traiter les demandes d'authentification,
- veiller à l'application des stratégies de groupe
- stocker une copie de **l'annuaire Active Directory**.



5. Arbre : Un arbre est un regroupement hiérarchique de plusieurs domaines.

6. **Forêt :** En effet, une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs **arbres**. Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt. Les domaines d'une forêt fonctionnent de façon indépendante, mais la forêt facilite les communications entre les domaines, c'est-à-dire dans toute l'architecture.



Conclusion : Une **forêt** est un ensemble d'arbres, qu'un **arbre** est constitué d'une racine et potentiellement de branches qui sont représentées par des **domaines** et des **sous-domaines**.

7. **Active Directory :**

L'Active Directory est un **annuaire LDAP** (***Lightweight Directory Access Protocol***) pour les systèmes d'exploitation Windows, le tout étant créé par Microsoft. Cet annuaire contient différents objets, de différents types (utilisateurs, ordinateurs, etc.), l'objectif étant de centraliser deux fonctionnalités essentielles : l'**identification** et l'**authentification** au sein d'un système d'information.

Au sein de l'annuaire Active Directory, il y a différents types d'objets, comme par exemple les utilisateurs, les ordinateurs, les serveurs, les unités d'organisation ou encore les groupes. En fait, ces objets correspondent à des **classes**, c'est-à-dire des objets disposant des mêmes **attributs**.

La base de données Active Directory est divisée de façon logique en trois partitions de répertoire (appelé « **Naming Context** »). Ces trois partitions sont la partition de **schéma**, la partition de **configuration**, et la partition de **domaine**.

1. **La partition de schéma** : cette partition contient l'ensemble des définitions des classes et attributs d'objets, qu'il est possible de créer au sein de l'annuaire Active Directory. Cette partition est unique au sein d'une forêt.

2. **La partition de configuration :** cette partition contient la topologie de la forêt (informations sur les domaines, les liens entre les contrôleurs de domaines, les sites, etc.). Cette partition est unique au sein d'une forêt.

3. **La partition de domaine :** cette partition contient les informations de tous les objets d'un domaine (ordinateur, groupe, utilisateur, etc.). Cette partition est unique au sein d'un domaine, il y aura donc autant de partitions de domaine qu'il y a de domaines.

Active Directory s'appuie donc sur organisation des machines en domaines **DNS**, dont il assure la bonne intégration ; sur une centralisation des informations des membres du réseau (machines, utilisateurs, ….) dans un **annuaire LDAP** ; sur une sécurisation forte par le protocole d'authentification **Kerberos** ; sur des partages de ressources (dossiers, imprimantes,…) par le protocole **SMB/CIFS**.

Travail demandé

Pour effectuer ce TP nous aurons besoin d'utiliser trois machines virtuelles, un serveur Windows 2003, et deux machine Windows 7 (version **Professionnel**) selon la topologie réseau suivante.

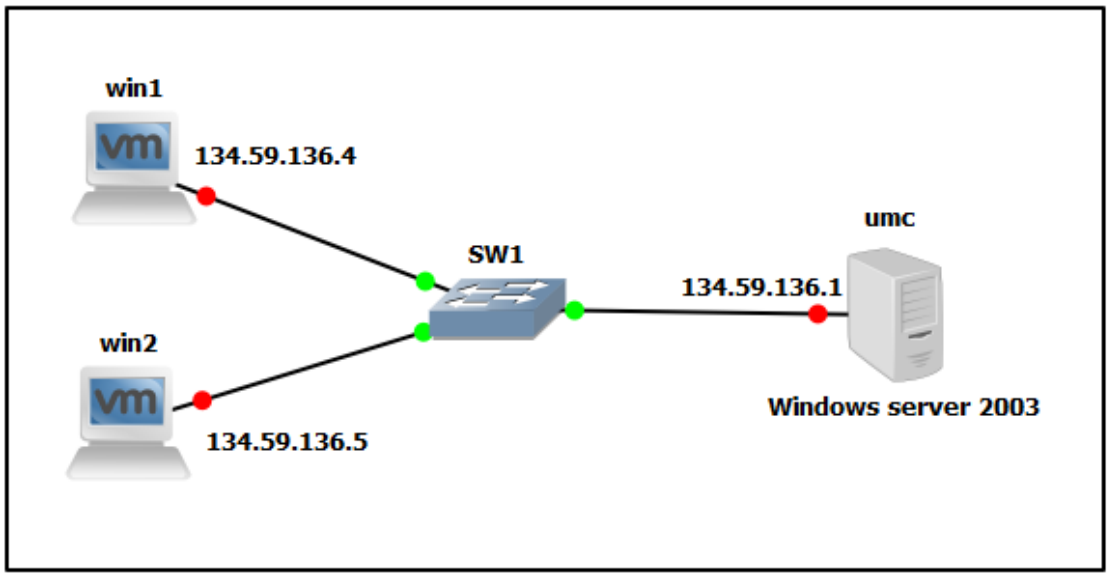


Figure 1 : Topologie réseau du TP 6 réaliser sous GNS3

1. Configurer la machine serveur « *Windows server 2003* » en **contrôleur de domaine Active Directory** et les autres machines virtuelles en **membres du domaine**.
   - Le nom de domaine est : zarzara.edu
   - Nom NetBios :zarzara
   - Niveau fonctionnel : Windows 2003
   - Les autres options seront laissées par défaut.
2. Créez les trois unités organisationelles (U.O) Electronique, Mécanique et G-transport dans le domaine zarzara.edu.
3. Dans l'U.O. **Electronique**, créez le groupe **Cours** et le groupe **TP**.
4. Dans l'U.O. **Mécanique**, créez le groupe **accueil** et le groupe **laboratoires**.
5. Dans l'U.O. **G-transport**, créez le groupe **développeurs** et le groupe **techniciens**.
6. Dépalcer la machine virtuelle « win1 » vers l'U.O. Electronique.

7. Créez les comptes utilisateurs suivant : **AMIRA KOKO**, **MERIEM MIMI, AHMED RIDA** et **ANIS FOFO.**
8. Ajouter les utilisateurs **AMIRA KOKO** et **MERIEM MIMI** au groupe cours de l'U.O. Electronique.
9. Ajouter l' utilisateurs **AHMED RIDA** au groupe TP de l'U.O. Electronique.
10. Ajouter l' utilisateurs **ANIS FOFO** au groupe laboratoires de l'U.O. Mécanique et au groupe techniciens de l'U.O. G-transport.
11. Faites en sorte que les utilisateurs du groupe **cours** ne puissent se connecter que de 8^h à 18^h.
12. Créer une nouvelle stratégie du groupe pour l'U.O. Electronique avec les paramètres suivants :
    1. Désactiver la connexion au domaine depuis un compte **invité.**
    2. Renommer le compte administrateur à **admin-electronique.**
    3. Désactiver l'exécution de **Windows Massenger.**
    4. Interdire aux utilisateurs de partager des fichiers de leur profil.
    5. Interdire le menu contextuel (clic droit) dans Internet Explorer

La console **gpedit.msc** (à lancer depuis Démarrer → Exécuter) permet d'éditer individuellement les stratégies de groupes locales. Cette console existe pour **tous les Windows** y compris les versions clientes.

Devoir maison (10pts)

1- Créez l' unités organisationelles (U.O) **Etablissement**, puis ajouter a cette dernière les groupes **enseignants** et **étudiants,** l'ordinateur **win2** et le compte utilisateur **CHEF** qui est un compte administrateur **(1pt)**.

2- Ajouter au groupe « **enseignants »** les utilisateurs **ens1, ens2** (administrateur) et **ens3** (utilisateur). Et au groupe « **étudiants »** les utilisateurs **etu1, etu2** et **etu3** (utilisateur) **(1pt).**

3- Ouvrez une session du domaine sur la machine **win2** avec le compte « **CHEF** » **(1pt)**.

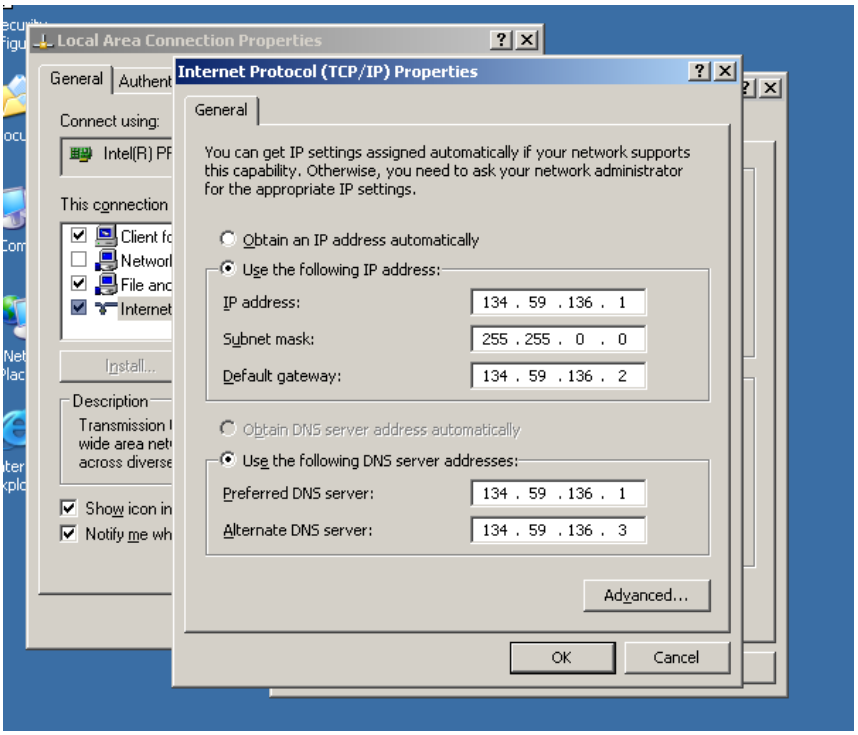
4- On souhaite imposer à l' unités organisationelles (U.O) **Etablissement** les règles suivantes :

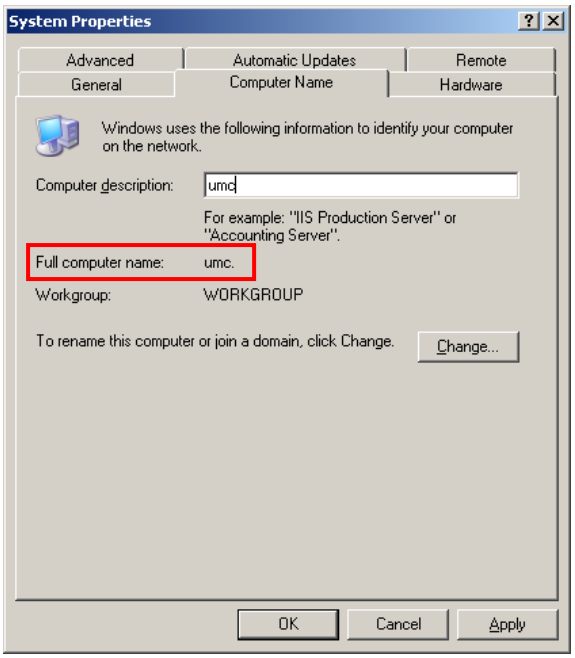
   1) Un étudiant est autorisé à réinitialiser les mots de passe des autres étudiants **(1pt)**.
   2) Aucun étudiant et aucun enseignant n'a de commande « **Exécuter** » dans son menu « **Démarrer** » **(1pt)**.
   3) On souhaite partager un dossier nommé « **Cours** » situé à la racine de c:\ sur **win2** de façon à ce que les **enseignants et le CHEF** aient les accès en contrôle total au partage Alors que les **étudiants** aient uniquement accès en « lecture /affichage » du contenu du dossier **(2pts)**.
   4) Empêcher les étudiants d'accéder à internet **(1pt)**.
   5) Un enseignant ne pouvant ouvrir de session que sur la machine **win2** aux horaires de travail (du Dimanche au Jeudi de 8h à 17h) **(2pt)**.

Remarque: **Me rendre sur papier (Rapport) la démarche documentée de ce que vous avez fait.**

Solution

. Etape 01 : Configuration de l'adresse IP fixe et du serveur (umc)

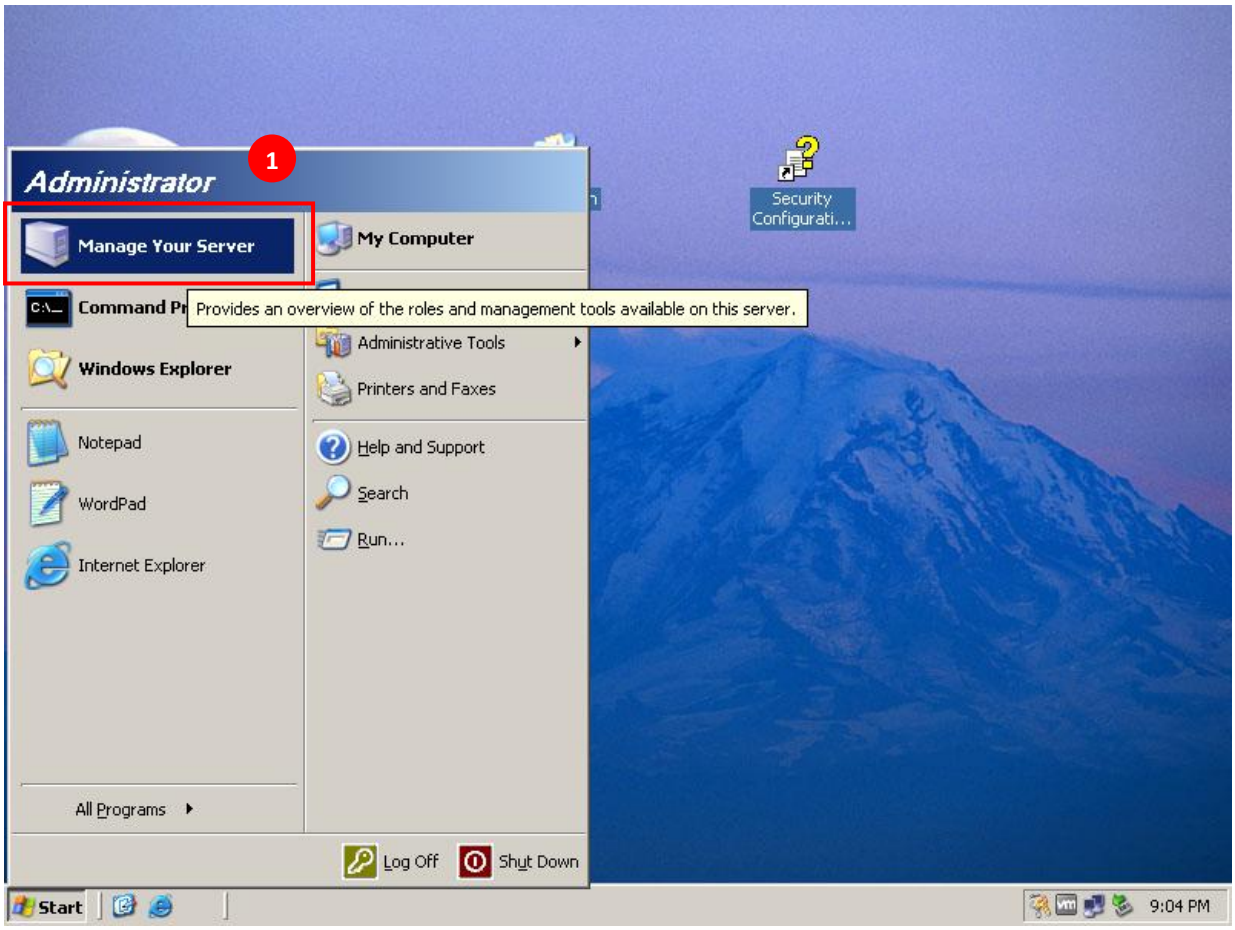




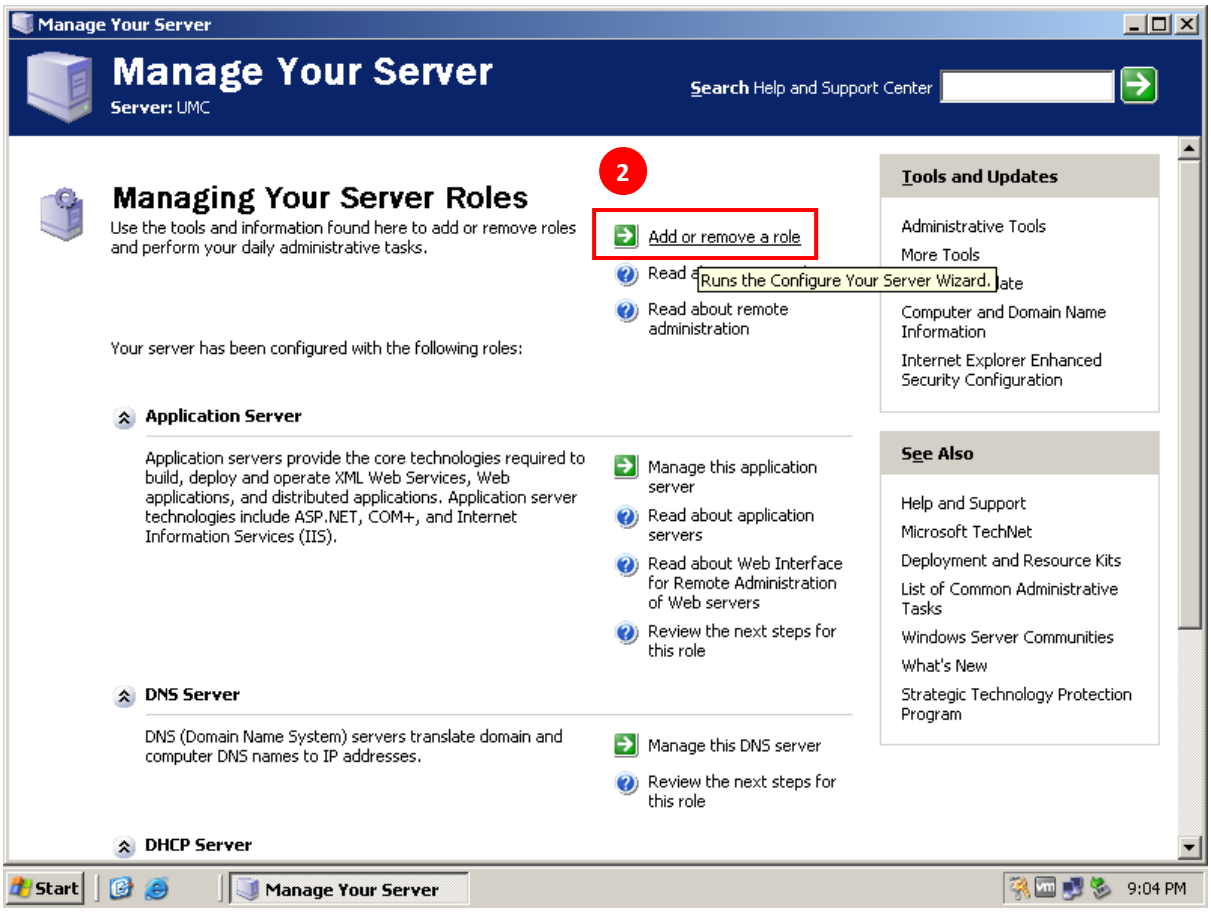
. Etape 02 : Installation du contrôleur du domaine Active Directory

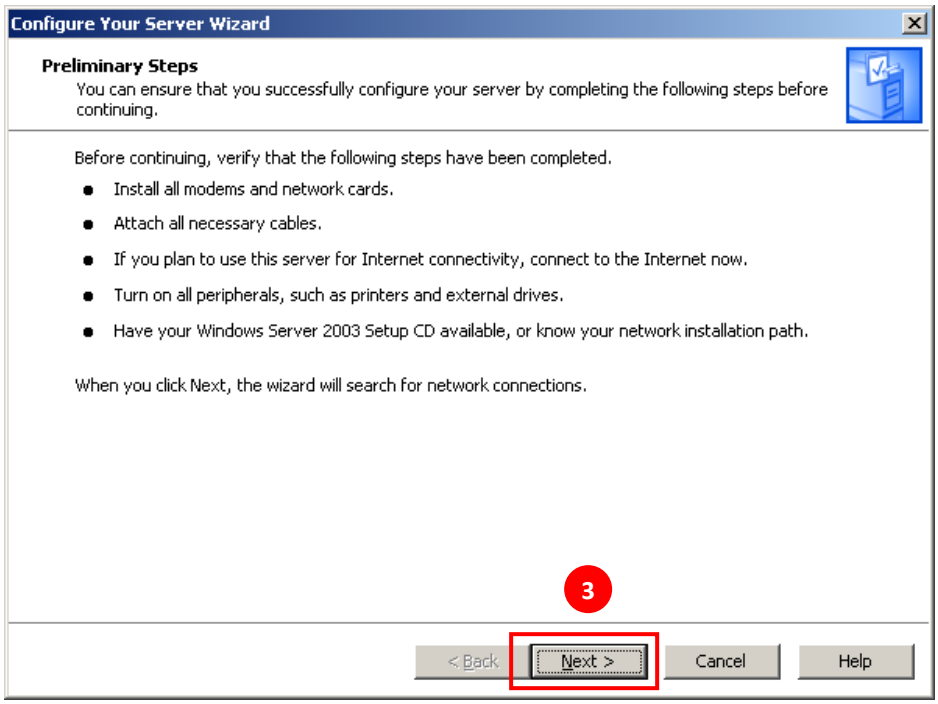
- Allez dans le gestionnaire de serveur puis faites un clic droit sur Rôles, Ajouter des rôles.

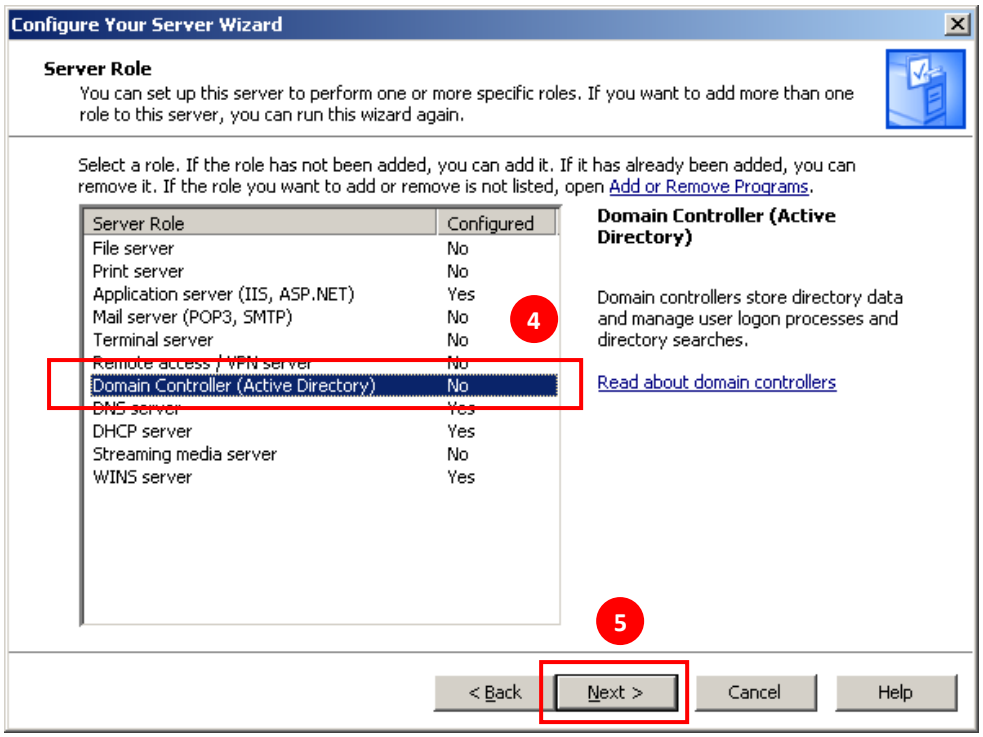
- Sélectionnez le rôle Services de domaine Active Directory et cliquez sur Suivant.
- Si vous n'avez rien installé précédemment sur votre serveur, vous devrez ajouter des fonctionnalités du framework.NET en cliquant sur Ajouter les fonctionnalités requises.

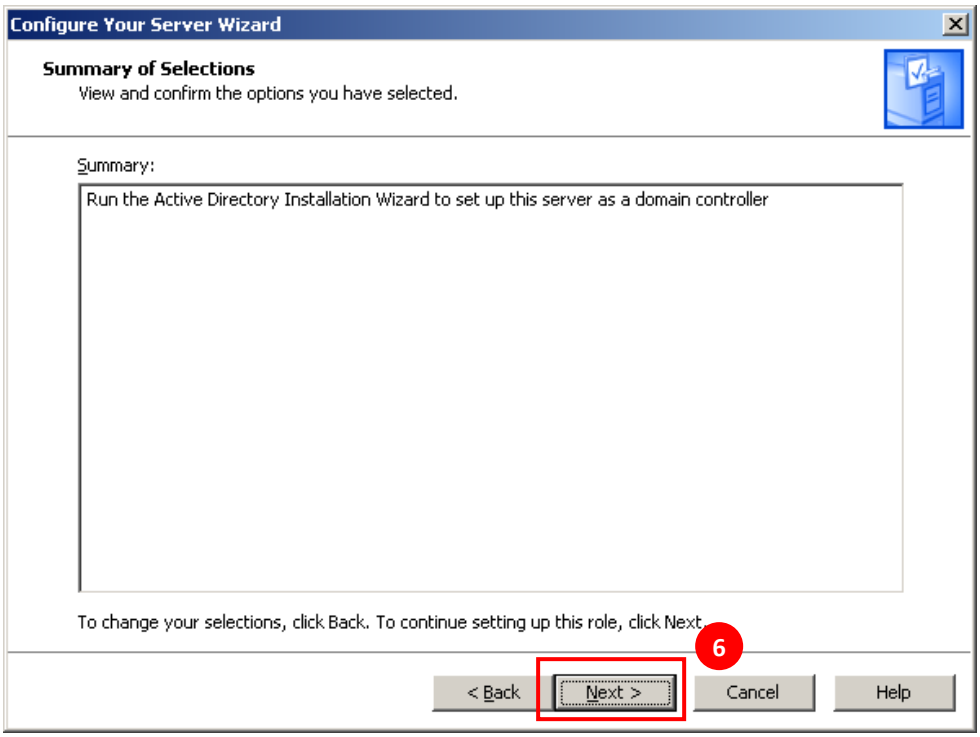


TP 6 : Installation d'un contrôleur de domaine

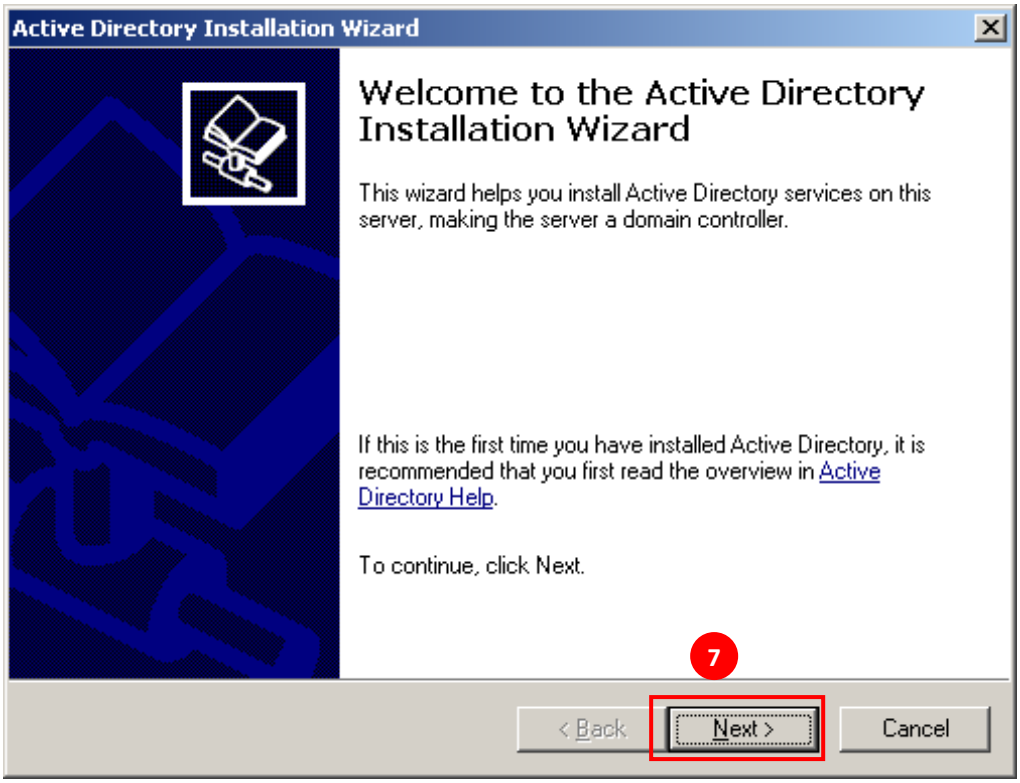


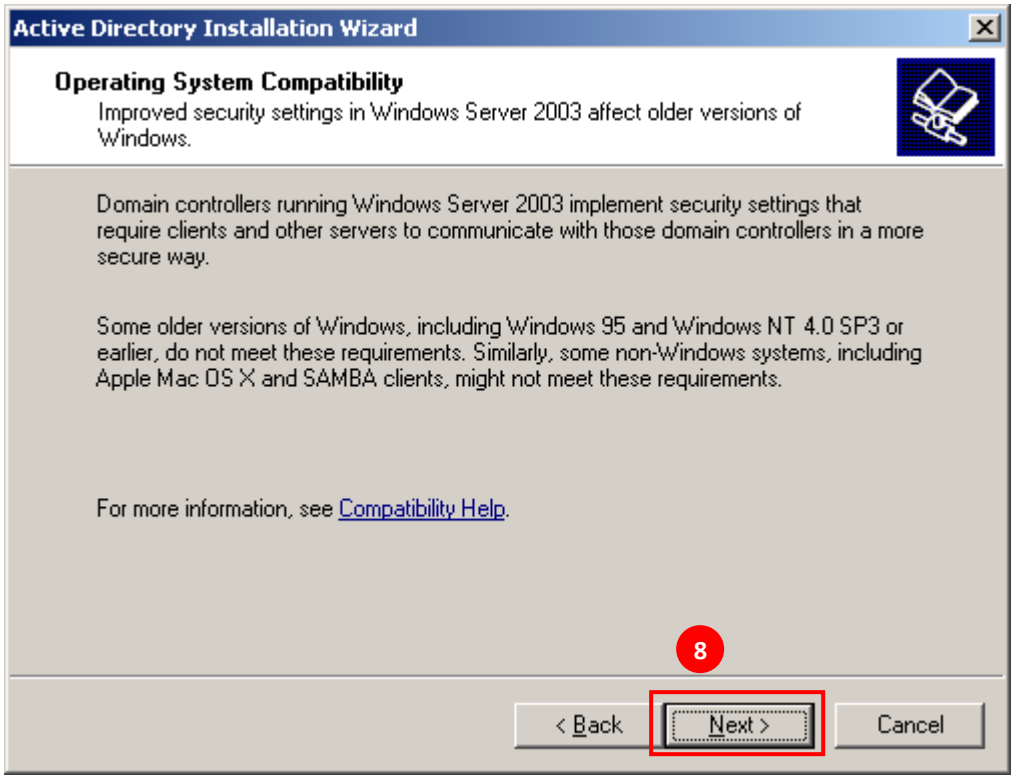


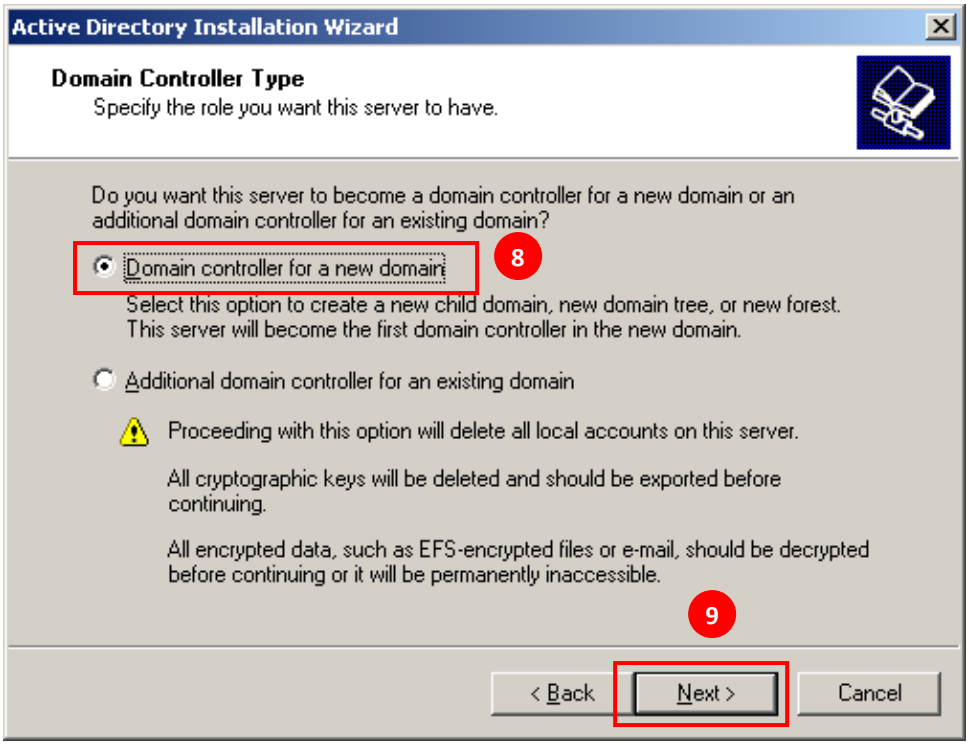


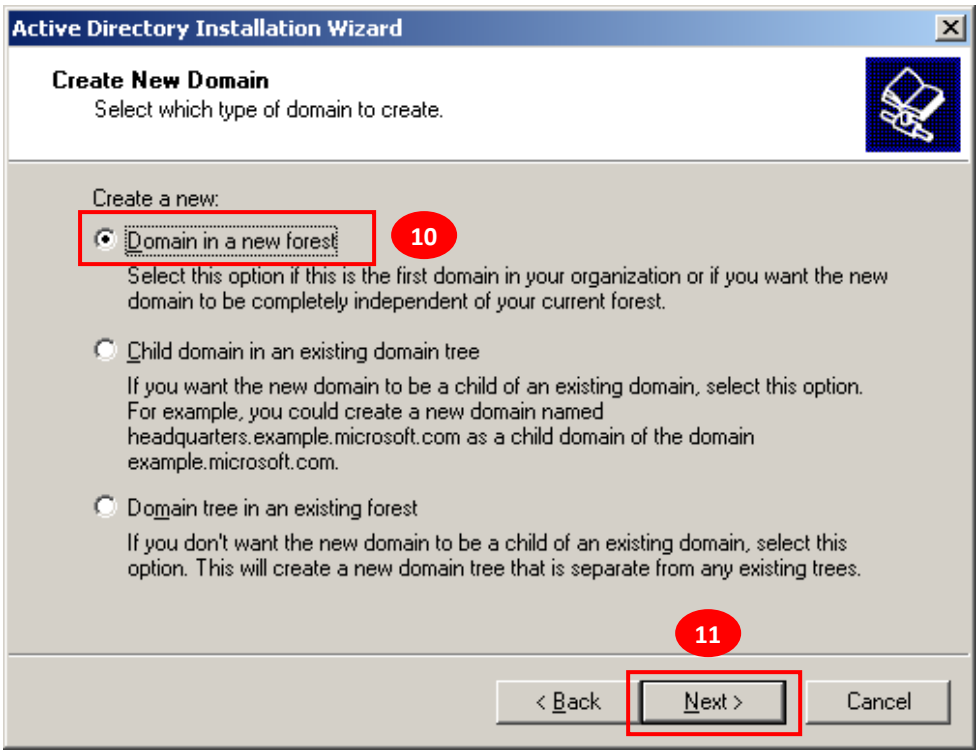


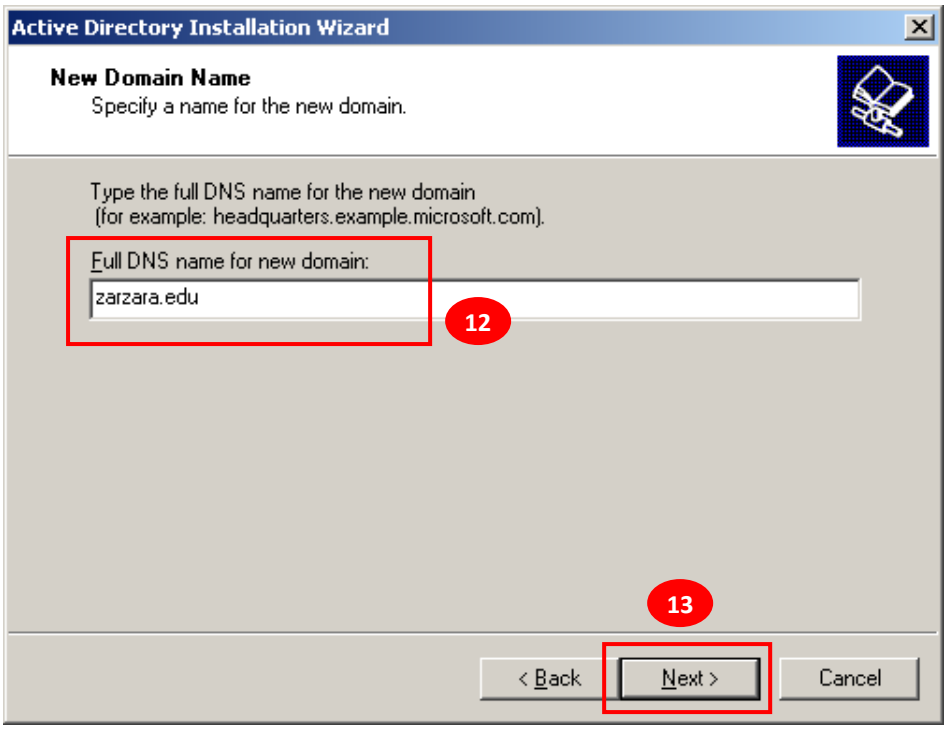
Nous allons maintenant commencer la création de votre Active Directory. Vous aurez le choix entre rejoindre une forêt existante ou créer un nouveau domaine dans une nouvelle forêt. Nous allons créer un nouveau domaine.

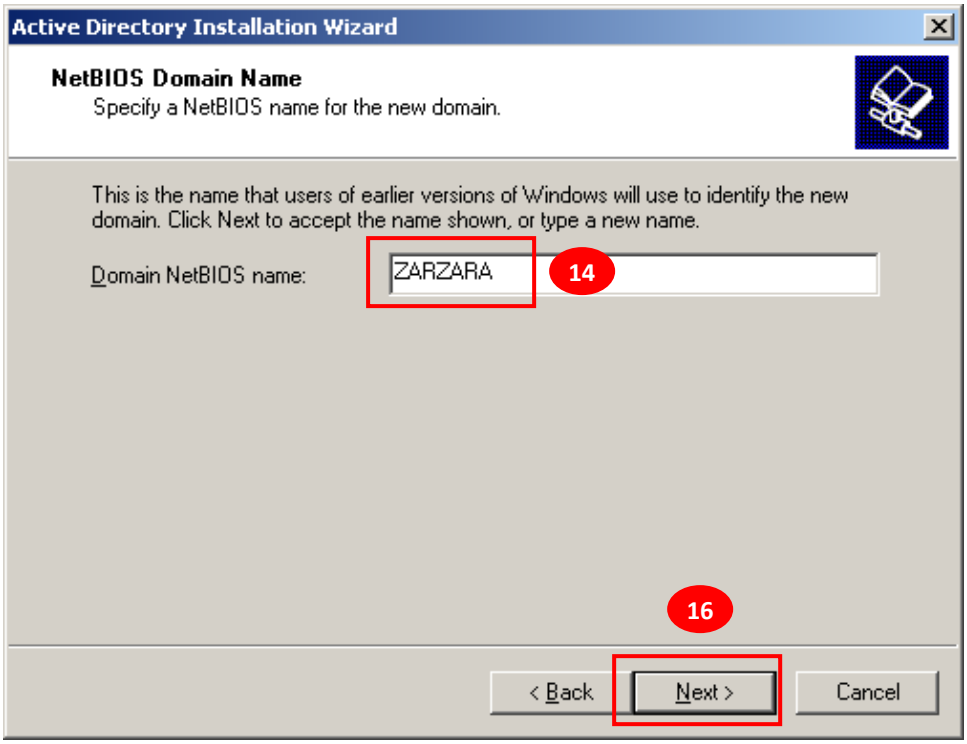

Active Directory Installation Wizard
Welcome to the Active Directory Installation Wizard
This wizard helps you install Active Directory services on this server, making the server a domain controller.
If this is the first time you have installed Active Directory, it is recommended that you first read the overview in Active Directory Help.
To continue, click Next.
7
< Back
Next >
Cancel

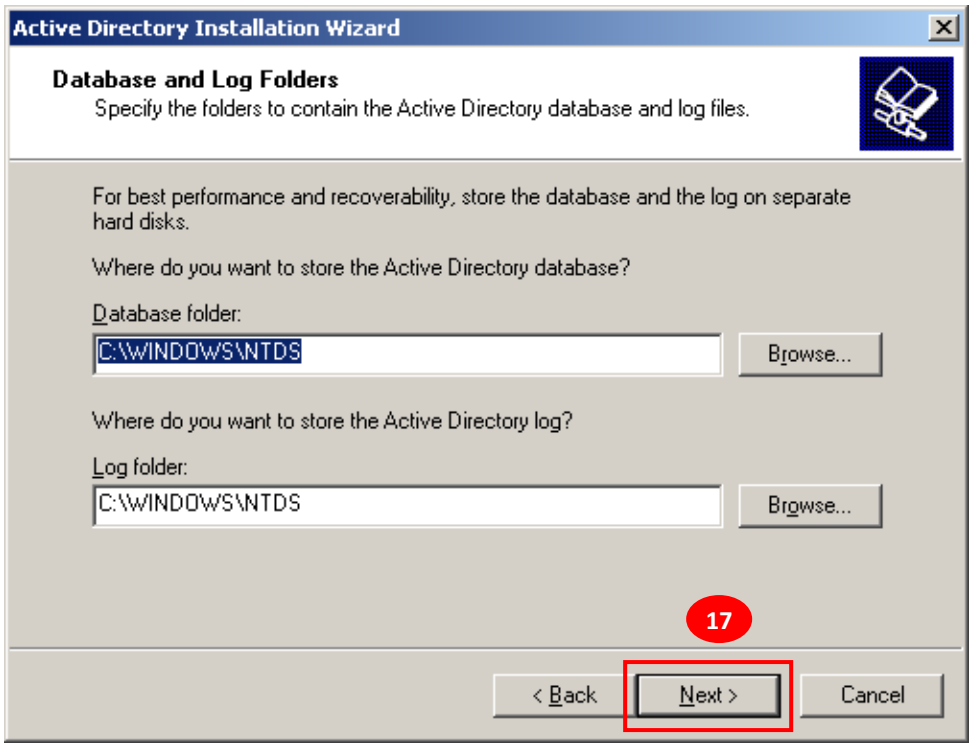

Active Directory Installation Wizard
Operating System Compatibility
Improved security settings in Windows Server 2003 affect older versions of Windows.
Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.
For more information, see Compatibility Help.
8
< Back
Next >
Cancel

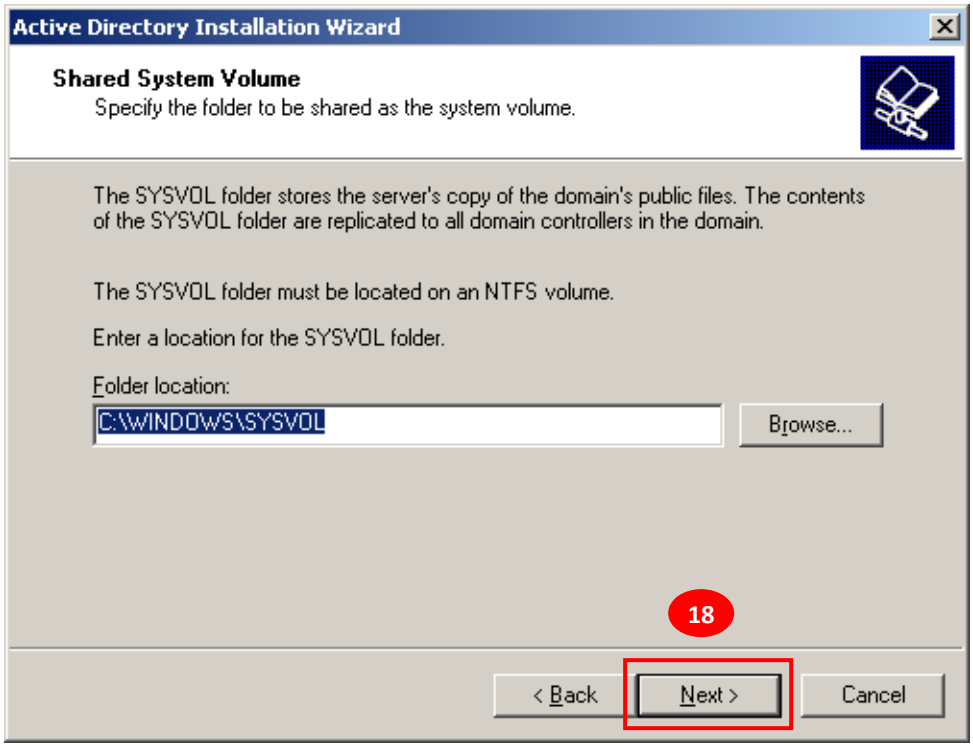

Active Directory Installation Wizard
Domain Controller Type
Specify the role you want this server to have.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?
Domain controller for a new domain
8
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
Additional domain controller for an existing domain
Proceeding with this option will delete all local accounts on this server.
All cryptographic keys will be deleted and should be exported before continuing.
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
9
< Back
Next >
Cancel

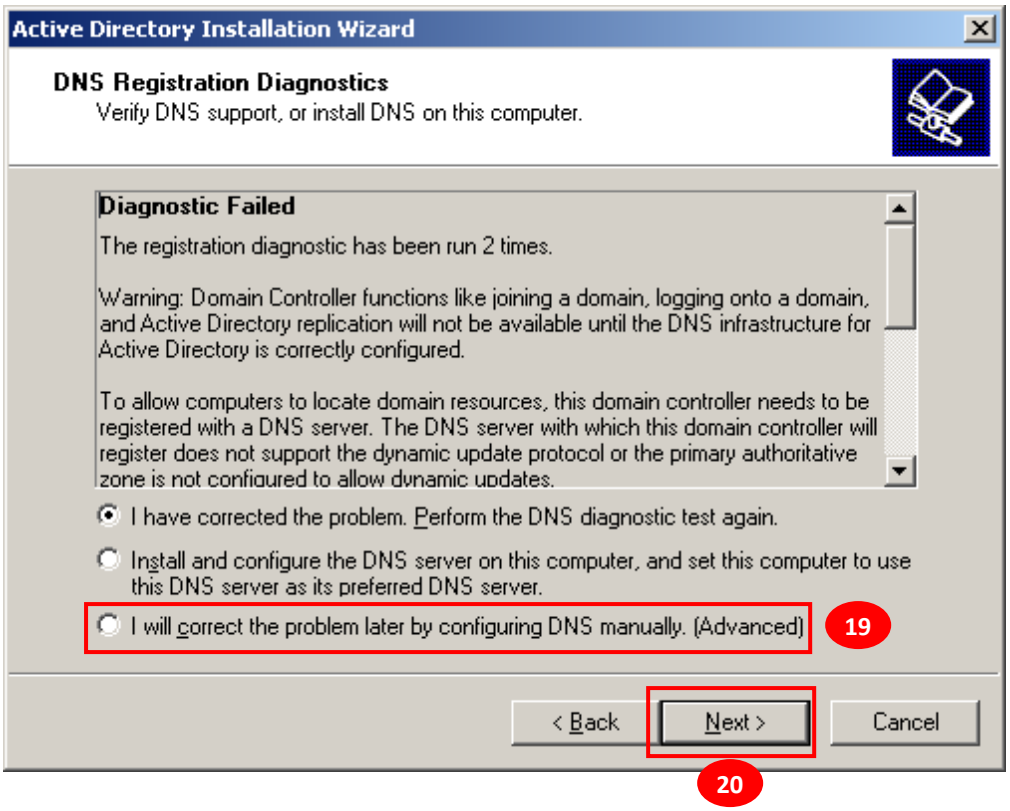

Active Directory Installation Wizard
Create New Domain
Select which type of domain to create.
Create a new:
Domain in a new forest
10
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
11
< Back
Next >
Cancel

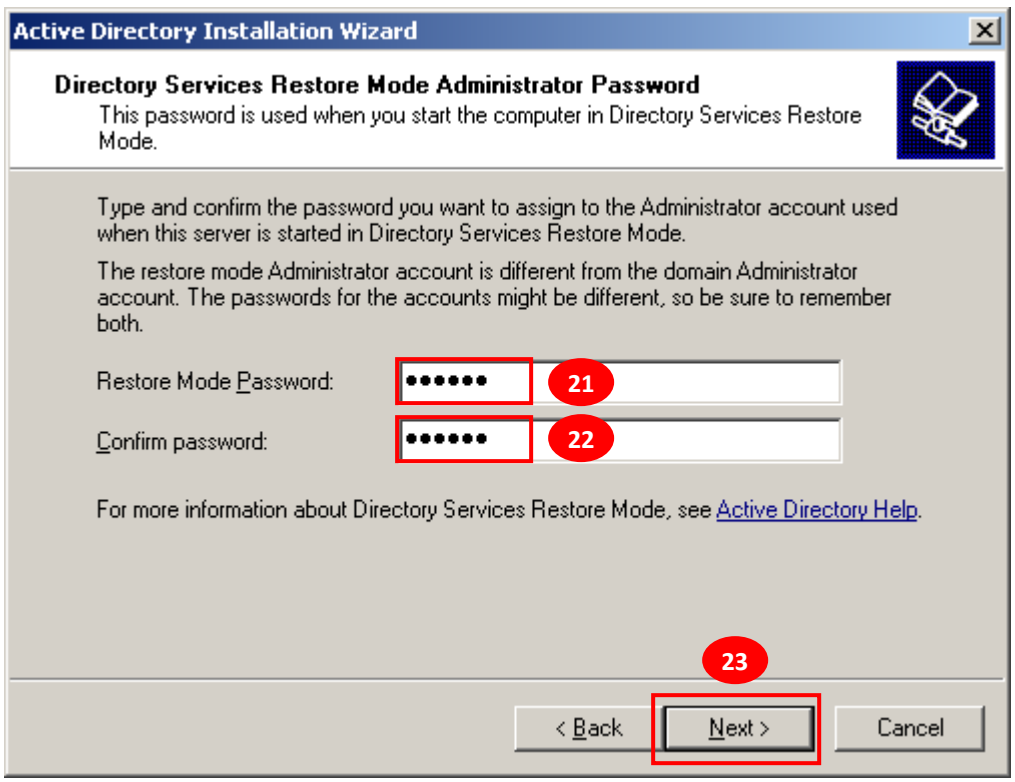

Active Directory Installation Wizard
New Domain Name
Specify a name for the new domain.
Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).
Full DNS name for new domain:
zarzara.edu
12
13
< Back
Next >
Cancel

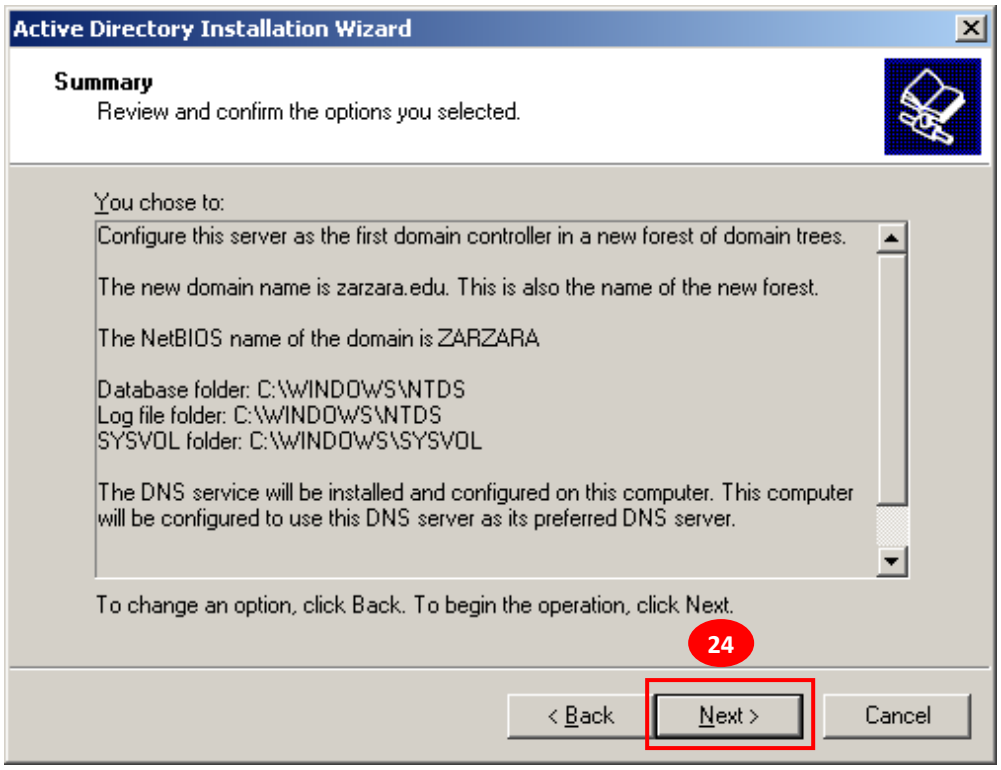

Active Directory Installation Wizard
NetBIOS Domain Name
Specify a NetBIOS name for the new domain.
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.
Domain NetBIOS name:
ZARZARA
14
16
< Back
Next >
Cancel

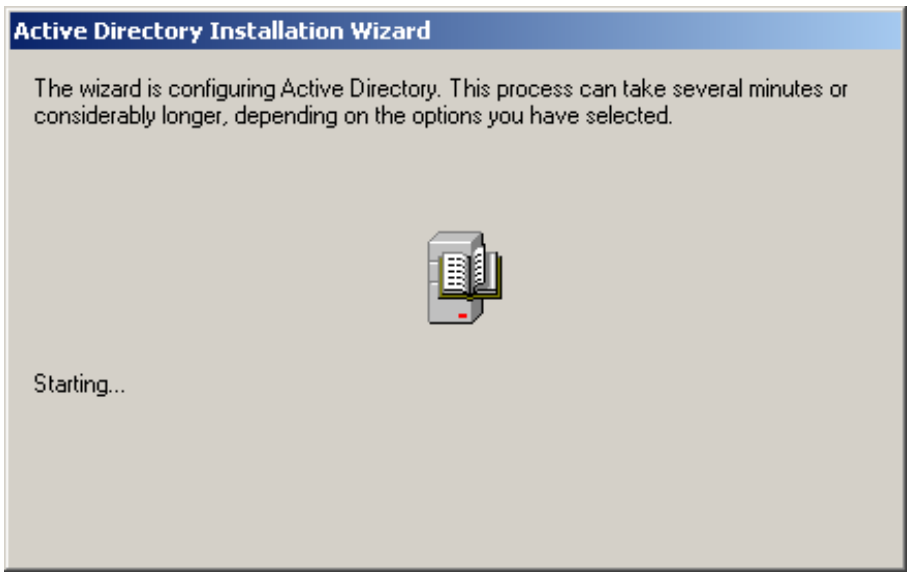

Active Directory Installation Wizard
Database and Log Folders
Specify the folders to contain the Active Directory database and log files.
For best performance and recoverability, store the database and the log on separate hard disks.
Where do you want to store the Active Directory database?
Database folder:
C:\WINDOWS\NTDS
Browse...
Where do you want to store the Active Directory log?
Log folder:
C:\WINDOWS\NTDS
Browse...
17
< Back
Next >
Cancel


Active Directory Installation Wizard
Shared System Volume
Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Folder location:
C:\WINDOWS\SYSVOL
Browse...
18
< Back
Next >
Cancel

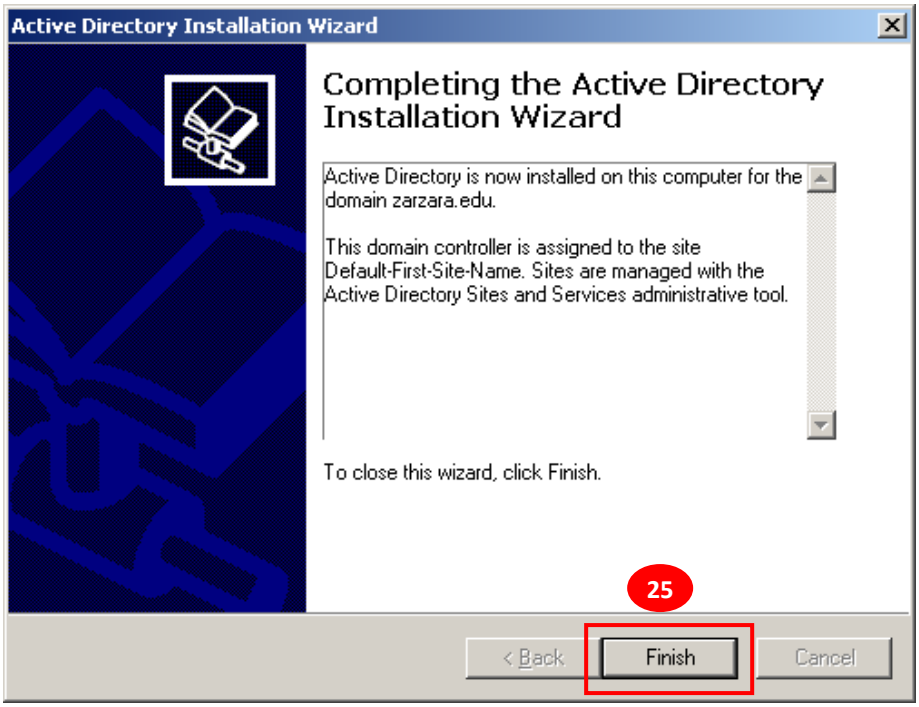

Active Directory Installation Wizard
DNS Registration Diagnostics
Verify DNS support, or install DNS on this computer.
Diagnostic Failed
The registration diagnostic has been run 2 times.
Warning: Domain Controller functions like joining a domain, logging onto a domain, and Active Directory replication will not be available until the DNS infrastructure for Active Directory is correctly configured.
To allow computers to locate domain resources, this domain controller needs to be registered with a DNS server. The DNS server with which this domain controller will register does not support the dynamic update protocol or the primary authoritative zone is not configured to allow dynamic updates.
I have corrected the problem. Perform the DNS diagnostic test again.
Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server.
I will correct the problem later by configuring DNS manually. (Advanced)
19
< Back
Next >
Cancel
20

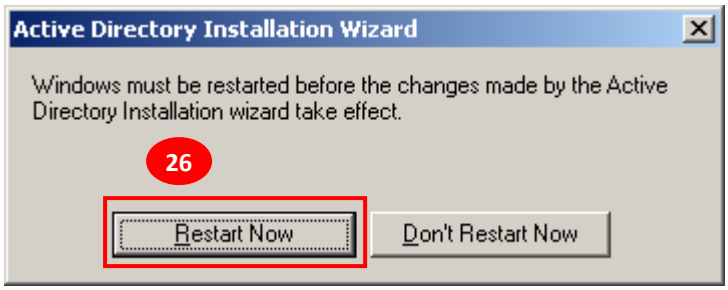

Active Directory Installation Wizard
Directory Services Restore Mode Administrator Password
This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
••••••
21
Confirm password:
••••••
22
For more information about Directory Services Restore Mode, see Active Directory Help.
23
< Back
Next >
Cancel

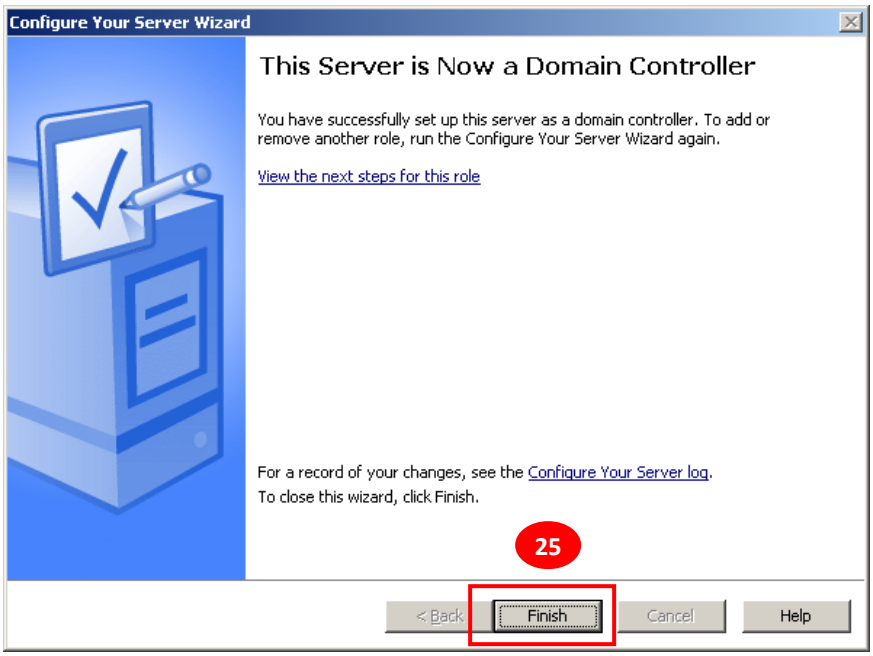




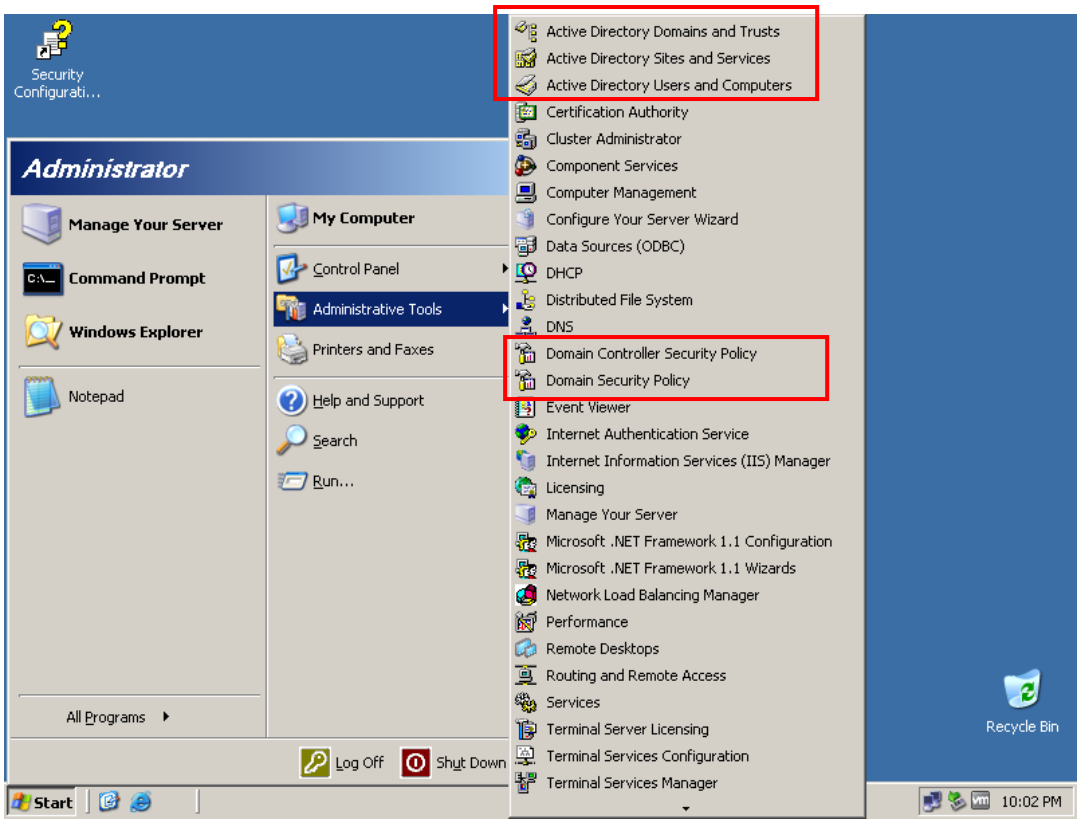
Installation de l'active Directory

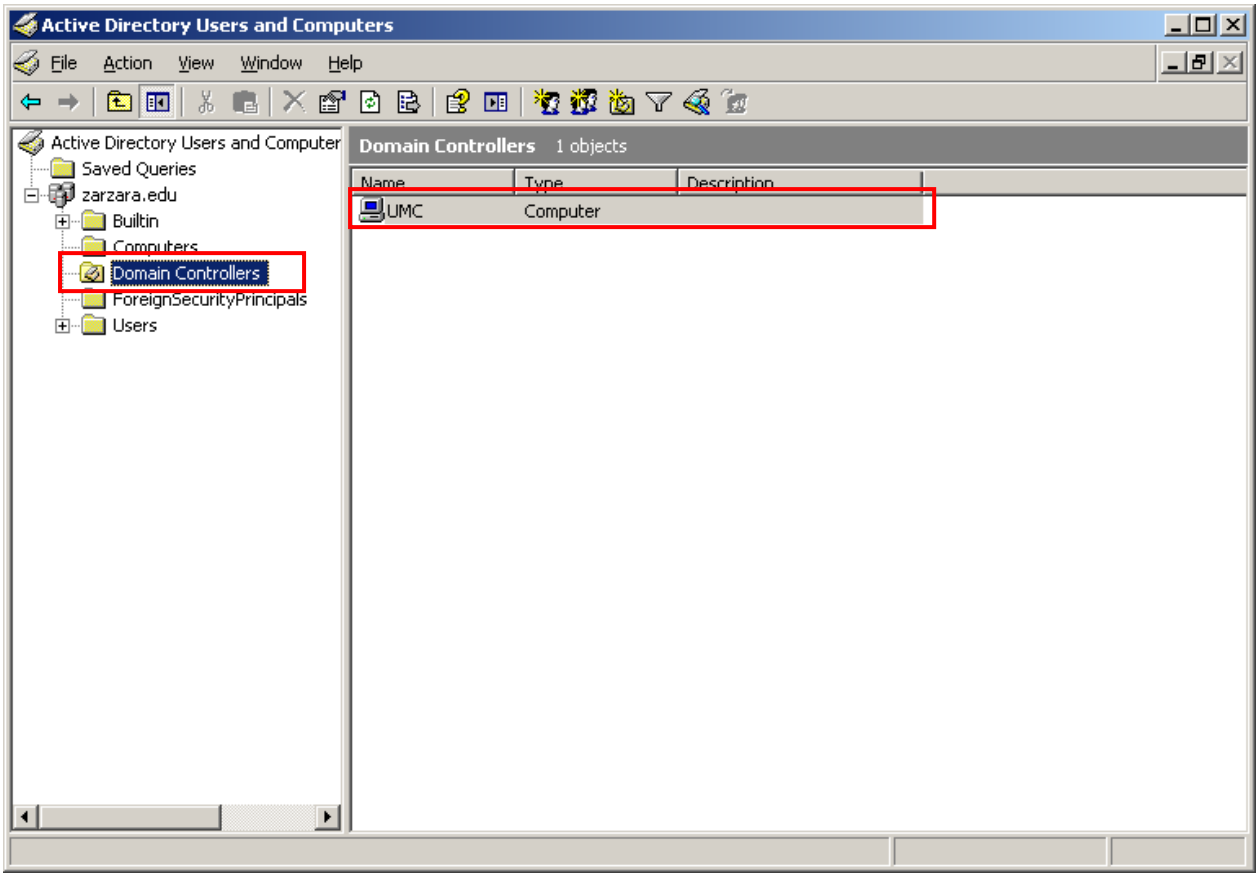

Active Directory Installation Wizard
Completing the Active Directory Installation Wizard
Active Directory is now installed on this computer for the domain zarzara.edu.
This domain controller is assigned to the site Default-First-Site-Name. Sites are managed with the Active Directory Sites and Services administrative tool.
To close this wizard, click Finish.
25
< Back
Finish
Cancel


Active Directory Installation Wizard
Windows must be restarted before the changes made by the Active Directory Installation wizard take effect.
26
Restart Now
Don't Restart Now


Configure Your Server Wizard
This Server is Now a Domain Controller
You have successfully set up this server as a domain controller. To add or remove another role, run the Configure Your Server Wizard again.
View the next steps for this role
For a record of your changes, see the Configure Your Server log.
To close this wizard, click Finish.
25
< Back
Finish
Cancel
Help

TP 6 : Installation d'un contrôleur de domaine

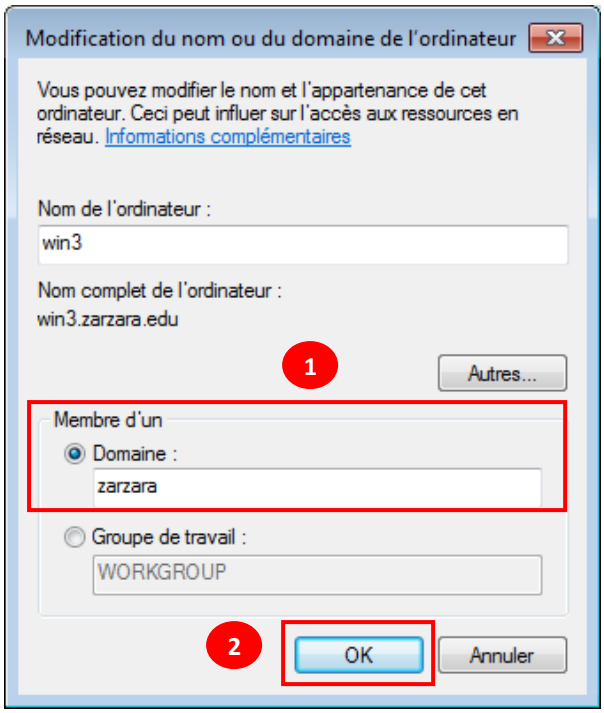




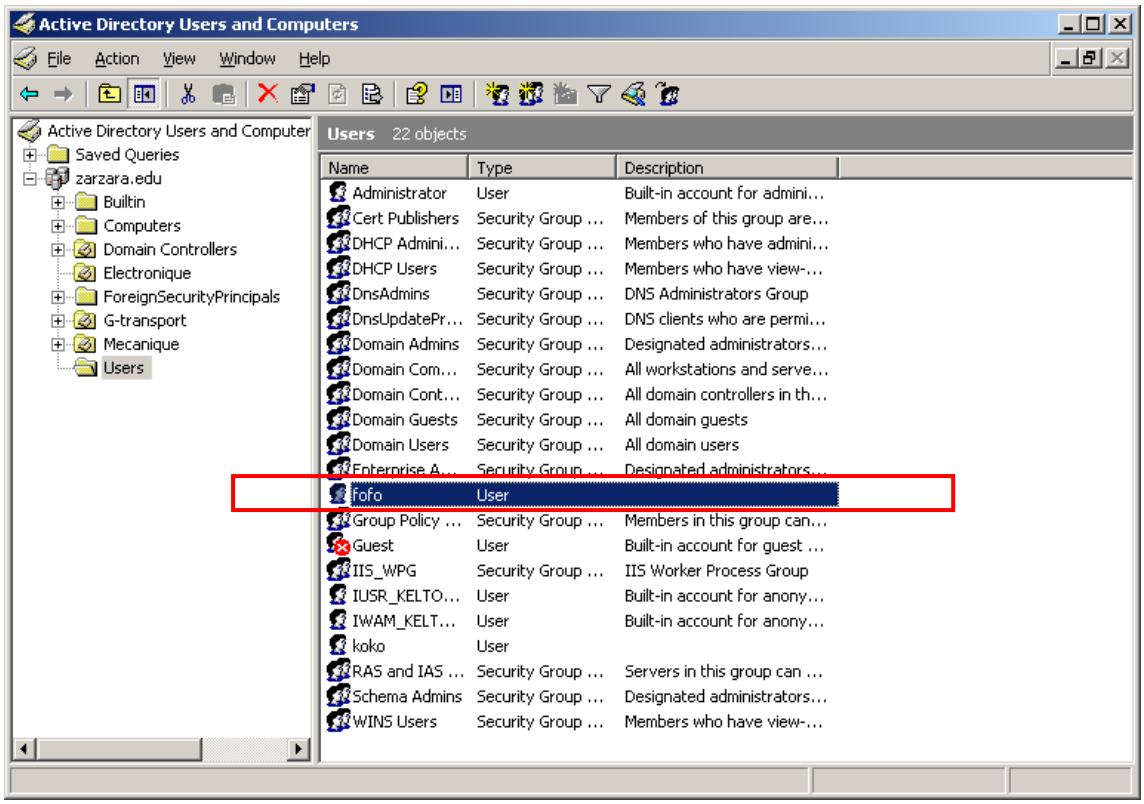
A la fin de la configuration, vous pouvez vérifier le bon fonctionnement de votre **contrôleur du domaine** via la fenêtre « ***Active Directory Users and Computers*** » → «***Domain Controllers*** ».

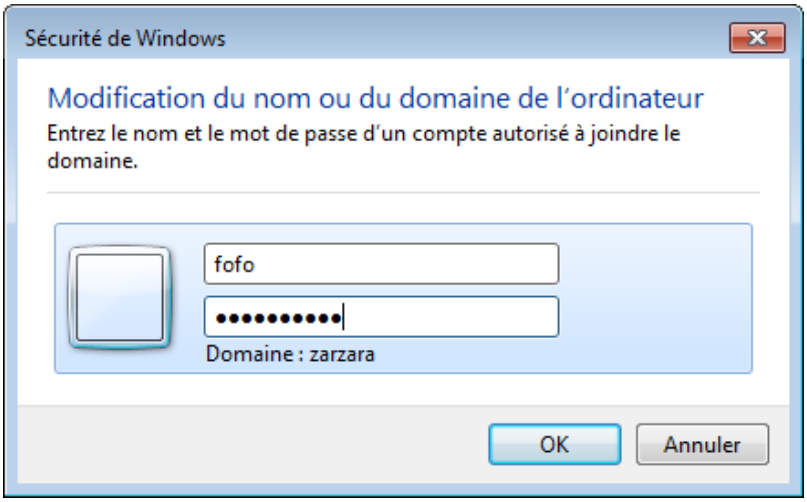
Etape 03 : Intégration des machines clientes comme membres du domaine Active Directory.

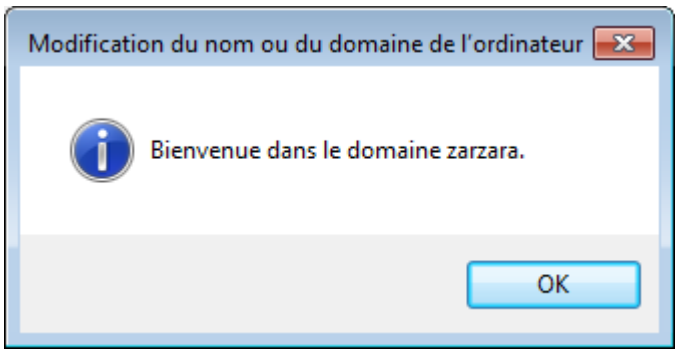
- Dans de la machine **win1**, « clic sur démarrer → poste de travail→ clic droit → propriétés →Paramètres système avancés → nom de l'ordinateur ».



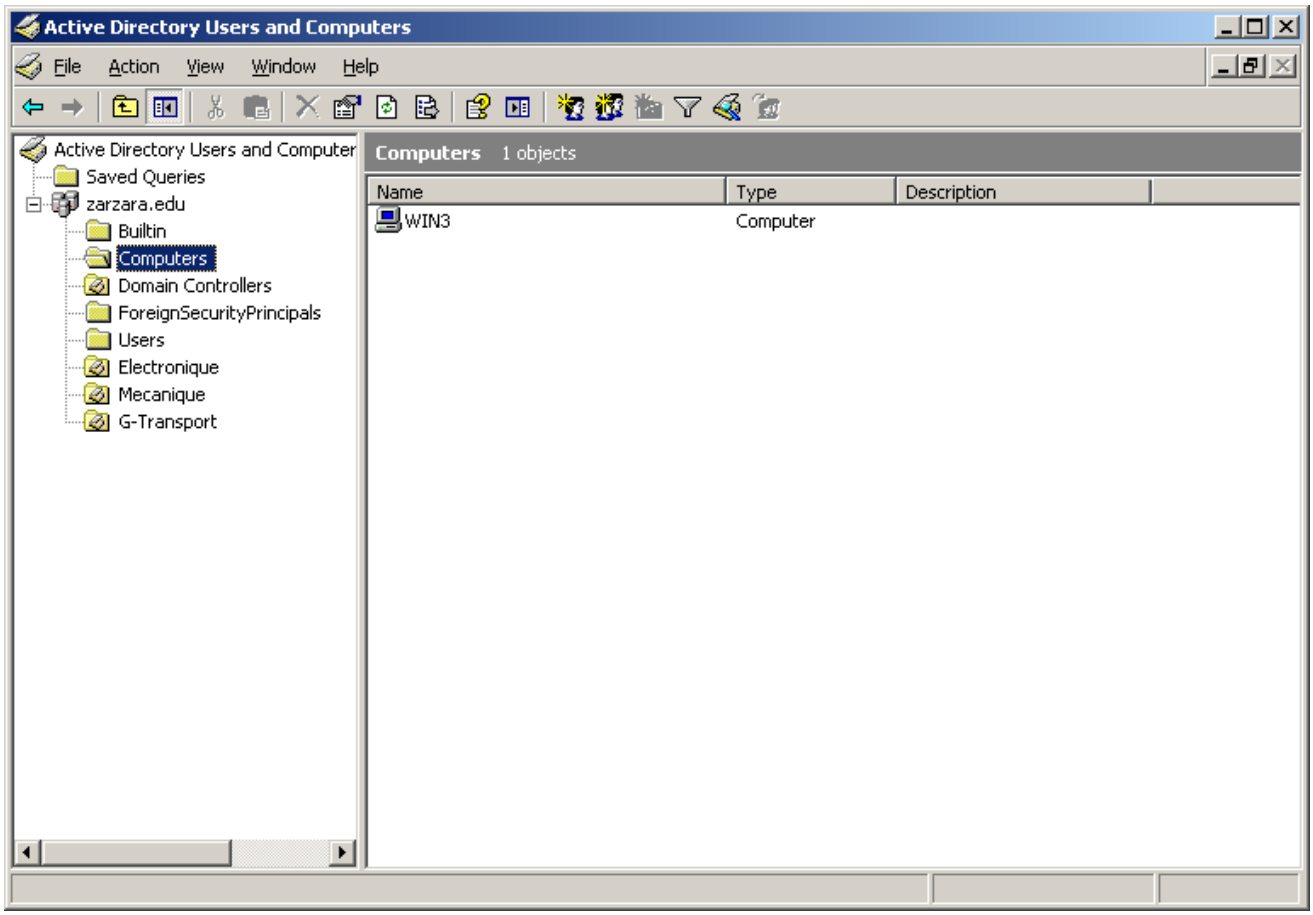
Pour Ouvrir une session du domaine sur la machine **win2,** il faut utiliser un compte utilisateurs qui déjà existe dans le domaine. (Nom : fofo et mot de passe Koko123456).


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
zarzara.edu
Builtin
Computers
Domain Controllers
Electronique
ForeignSecurityPrincipals
G-transport
Mecanique
Users
Users 22 objects
Name Type Description
Administrator User Built-in account for admini...
Cert Publishers Security Group ... Members of this group are...
DHCP Admini... Security Group ... Members who have admini...
DHCP Users Security Group ... Members who have view-...
DnsAdmins Security Group ... DNS Administrators Group
DnsUpdatePr... Security Group ... DNS clients who are permi...
Domain Admins Security Group ... Designated administrators...
Domain Com... Security Group ... All workstations and serve...
Domain Cont... Security Group ... All domain controllers in th...
Domain Guests Security Group ... All domain guests
Domain Users Security Group ... All domain users
fofo User
Group Policy ... Security Group ... Members in this group can...
Guest User Built-in account for guest ...
IIS_WPG Security Group ... IIS Worker Process Group
IUSR_KELTO... User Built-in account for anony...
IWAM_KELT... User Built-in account for anony...
koko User
RAS and IAS ... Security Group ... Servers in this group can ...
Schema Admins Security Group ... Designated administrators...
WINS Users Security Group ... Members who have view-...

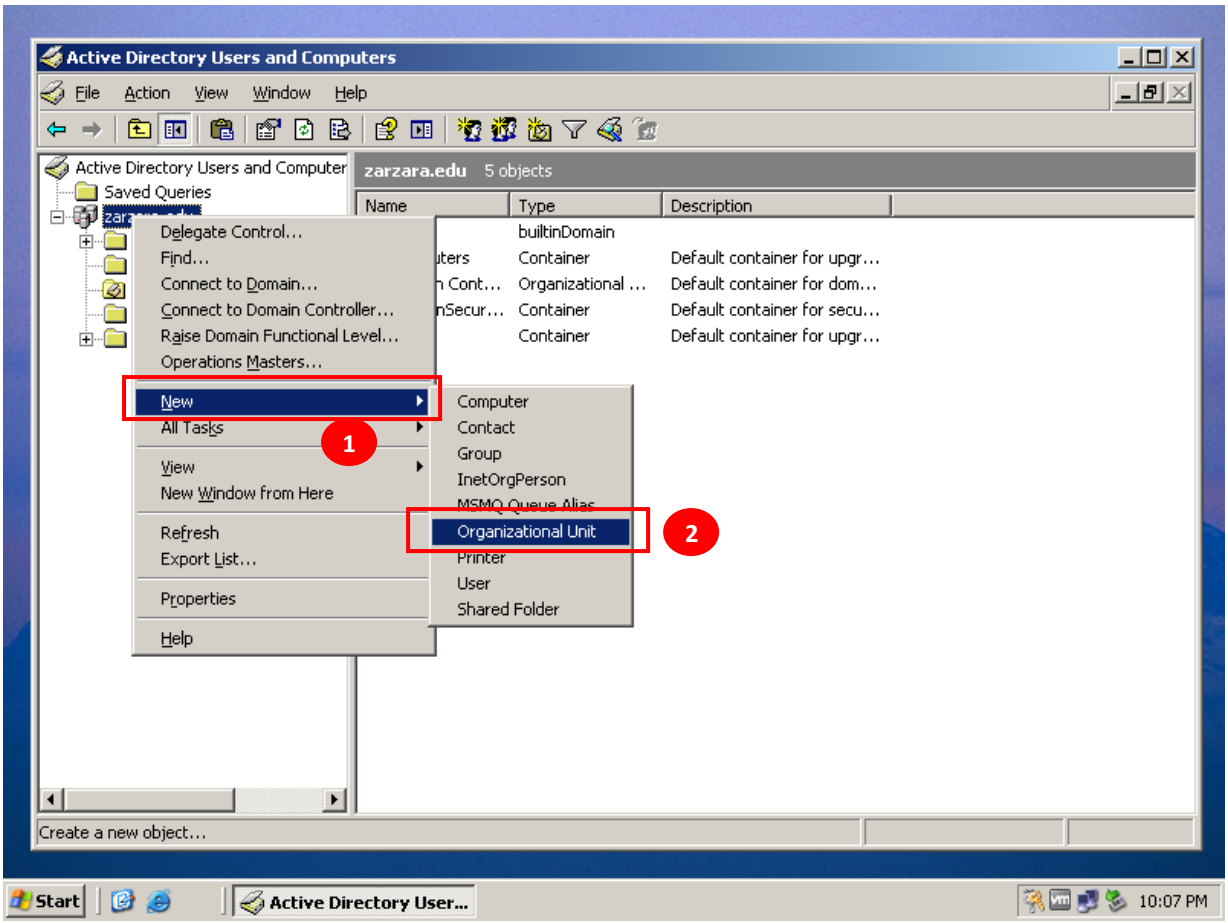

Sécurité de Windows
Modification du nom ou du domaine de l'ordinateur
Entrez le nom et le mot de passe d'un compte autorisé à joindre le domaine.
fofo
Domaine : zarzara
OK
Annuler

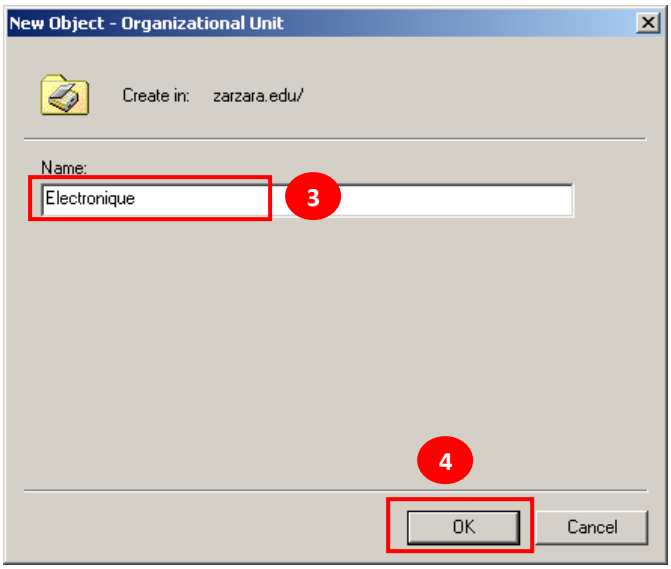

Modification du nom ou du domaine de l'ordinateur
Bienvenue dans le domaine zarzara.
OK

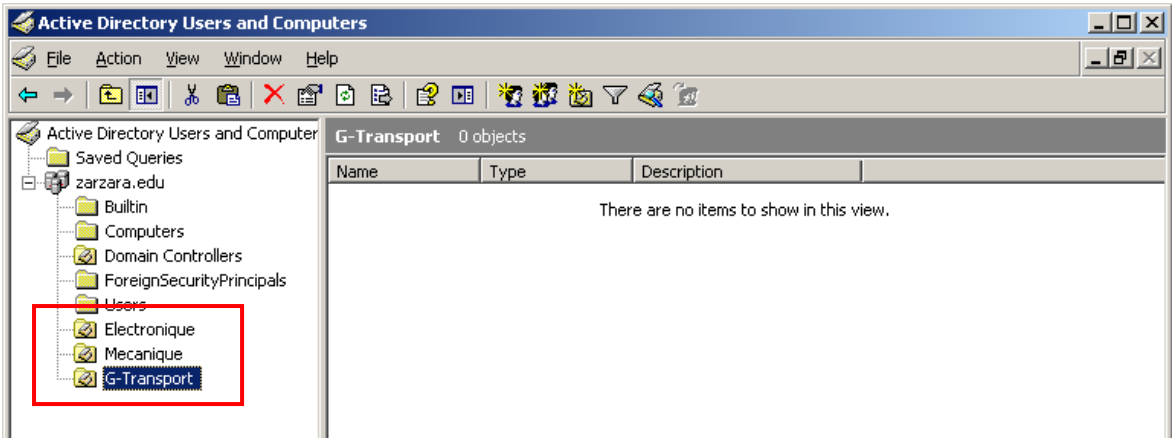
A la fin de la configuration, vous pouvez vérifier les machine du domaine via la fenêtre « ***Active Directory Users and Computers*** » → «***Computers*** ».



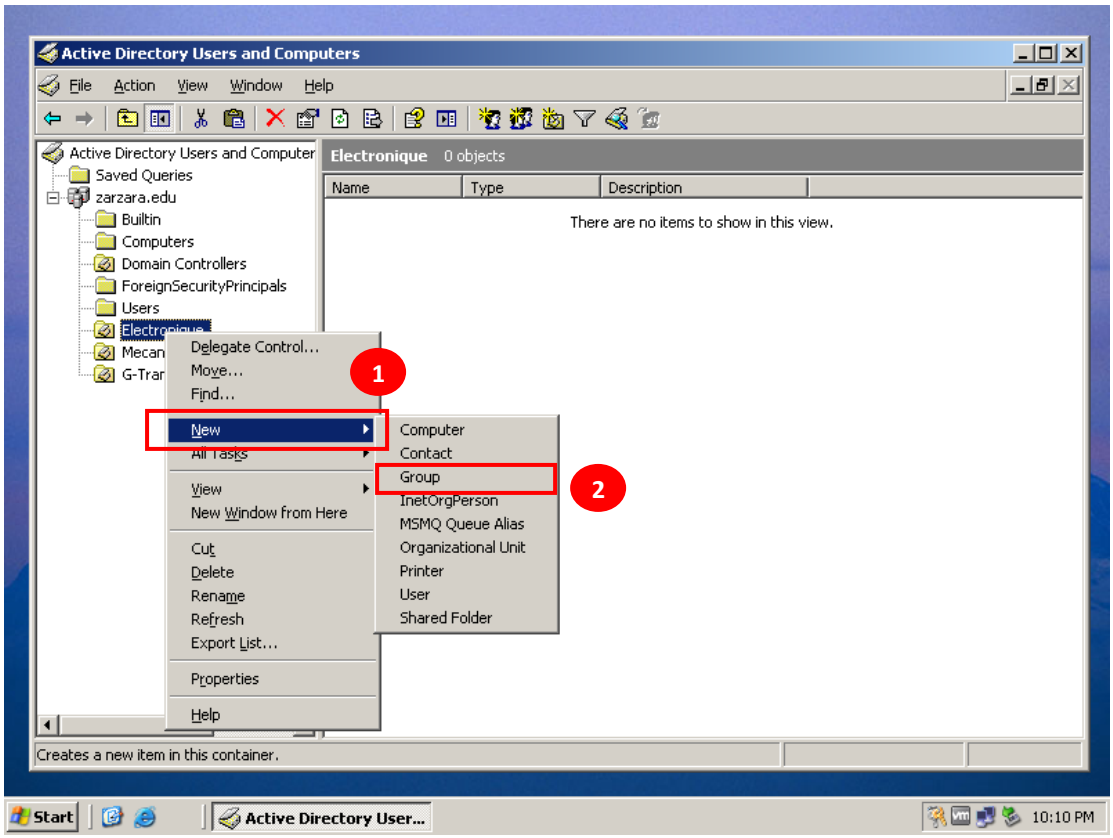
Etape 04 : Création des unités organisationnelles U.O

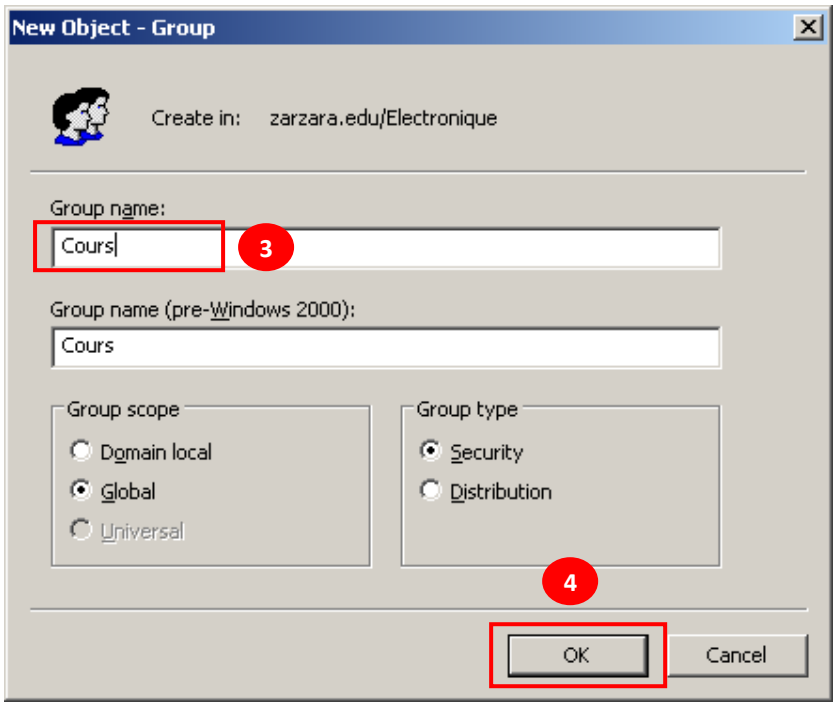


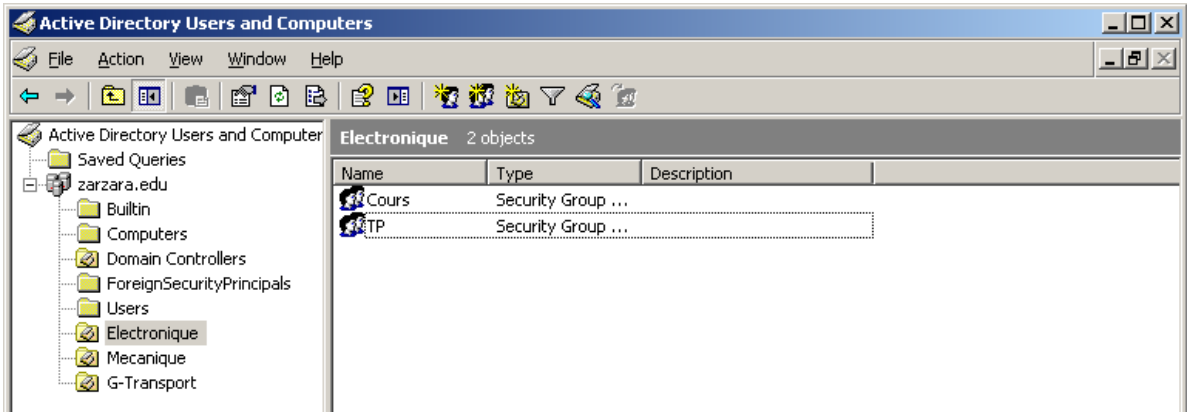


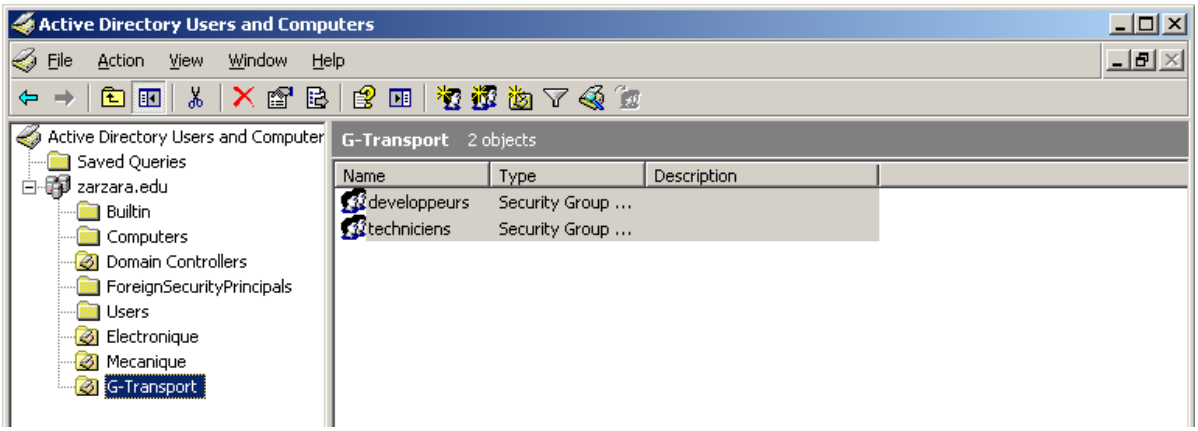


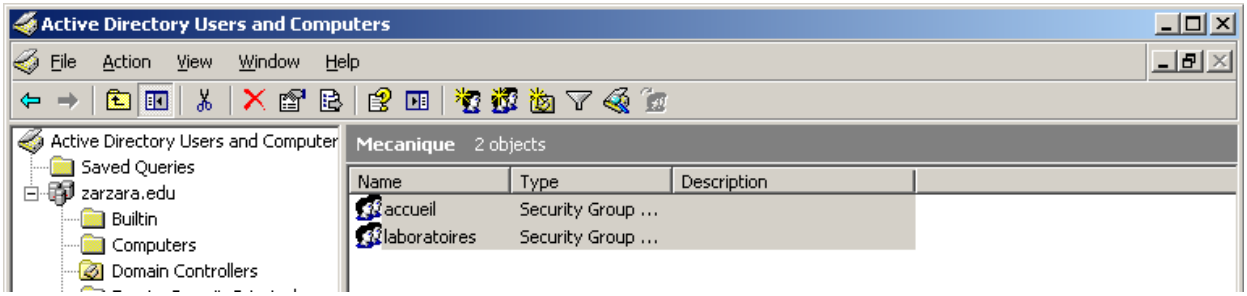
Etape 05: Création groupes



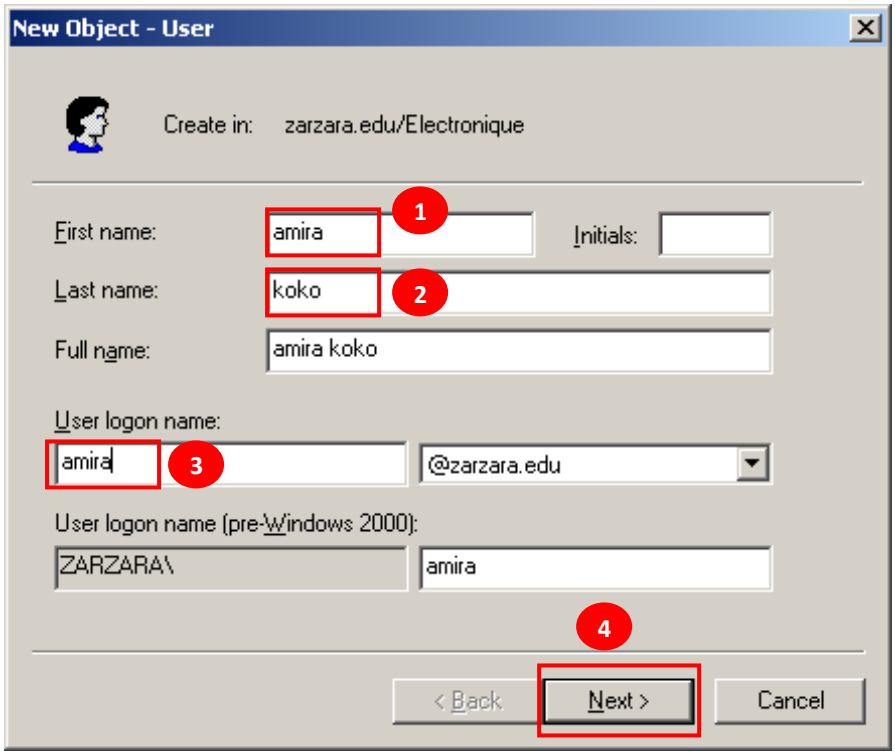

New Object - Group
Create in: zarzara.edu/Electronique
Group name:
Cours
3
Group name (pre-Windows 2000):
Cours
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
4
OK
Cancel

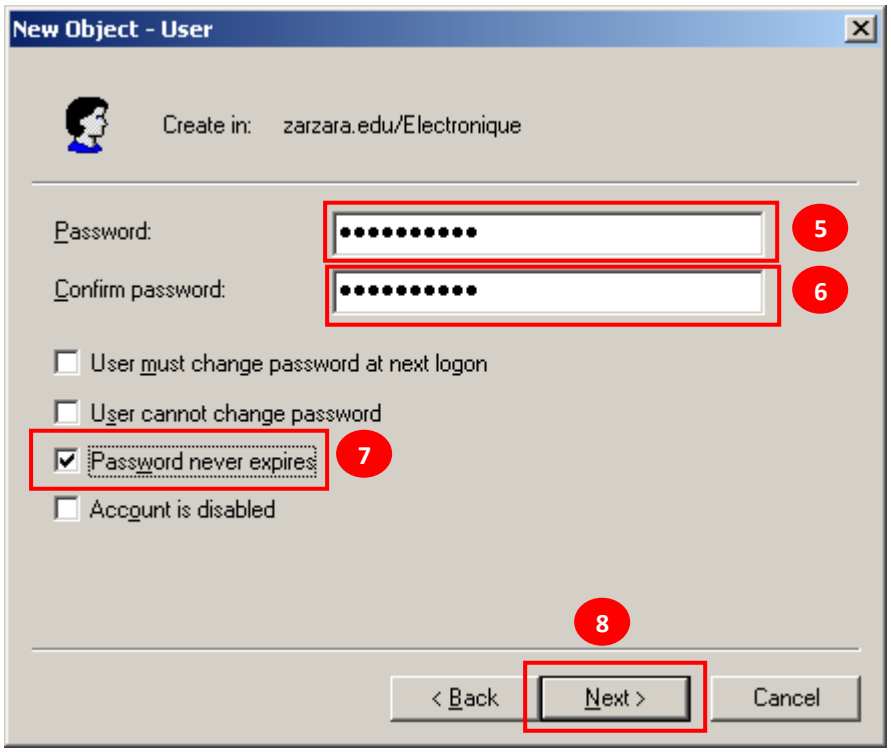

Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
zarzara.edu
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Electronique
Mecanique
G-Transport
Electronique 2 objects
Name Type Description
Cours Security Group ...
TP Security Group ...


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
zarzara.edu
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Electronique
Mecanique
G-Transport
G-Transport 2 objects
Name Type Description
developpeurs Security Group ...
techniciens Security Group ...

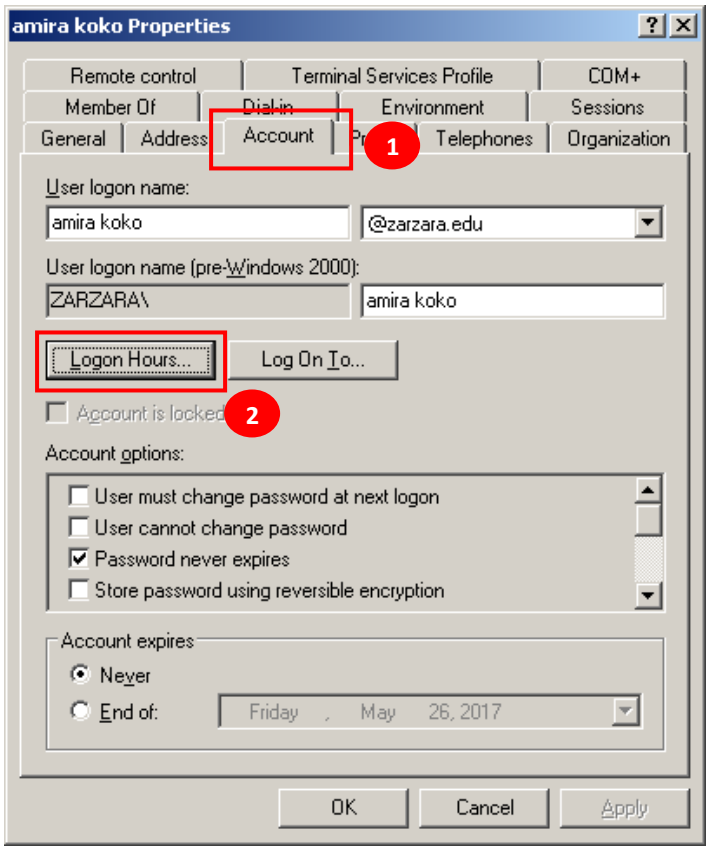


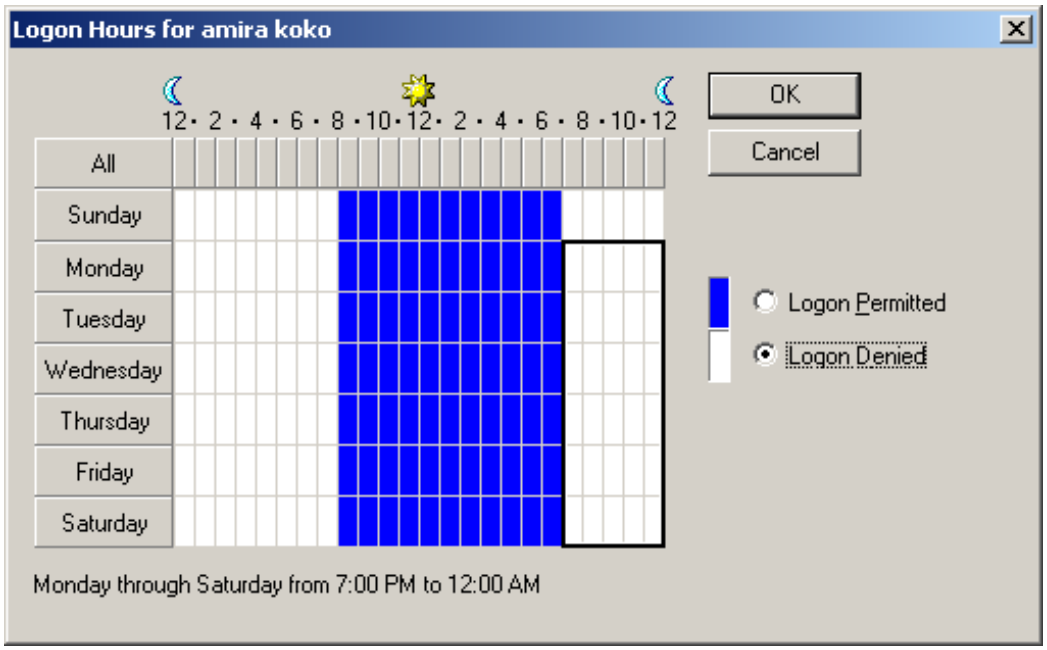
Etape 06: Création des comptes utilisateurs



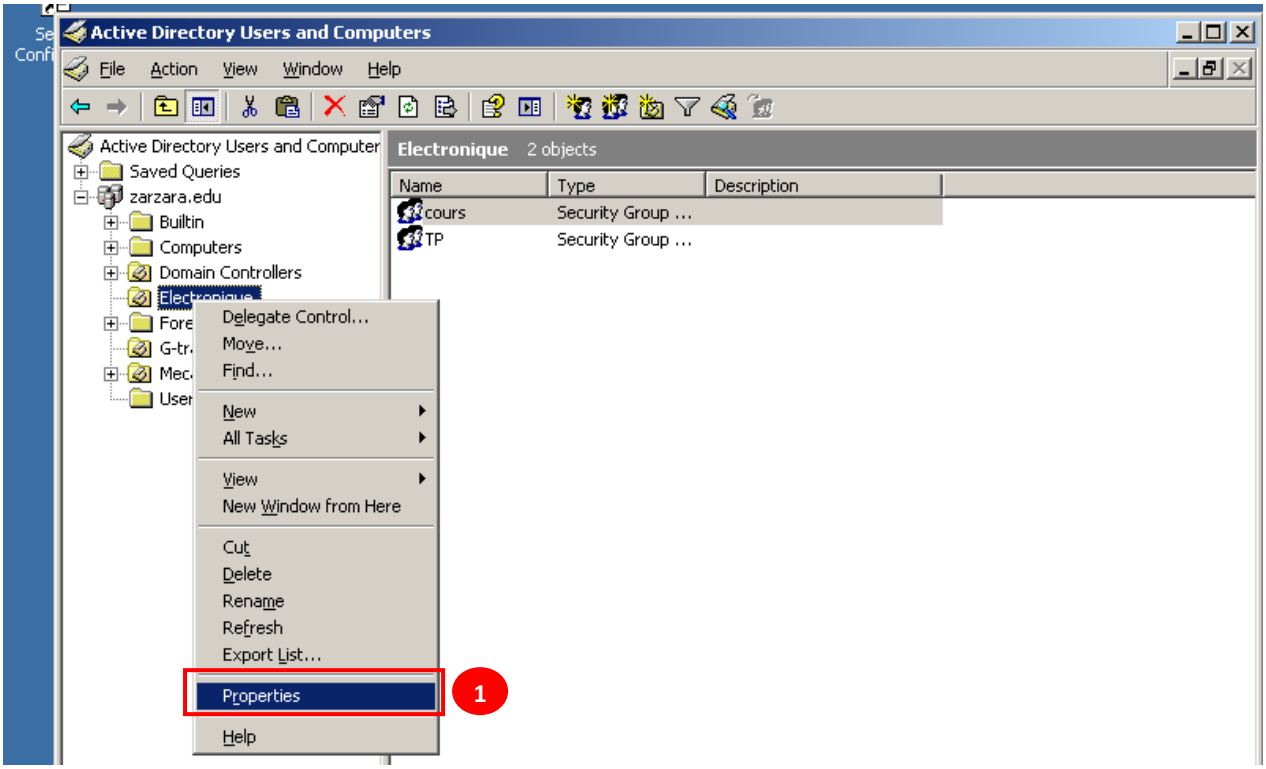


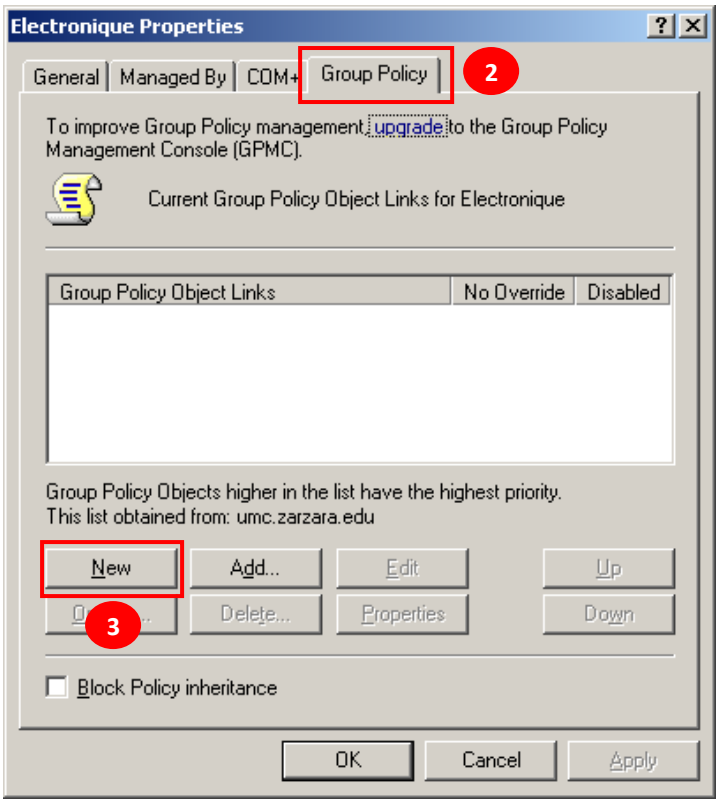
1. Faites en sorte que les utilisateurs du groupe **cours** ne puissent se connecter que de 8^h à 18^h.

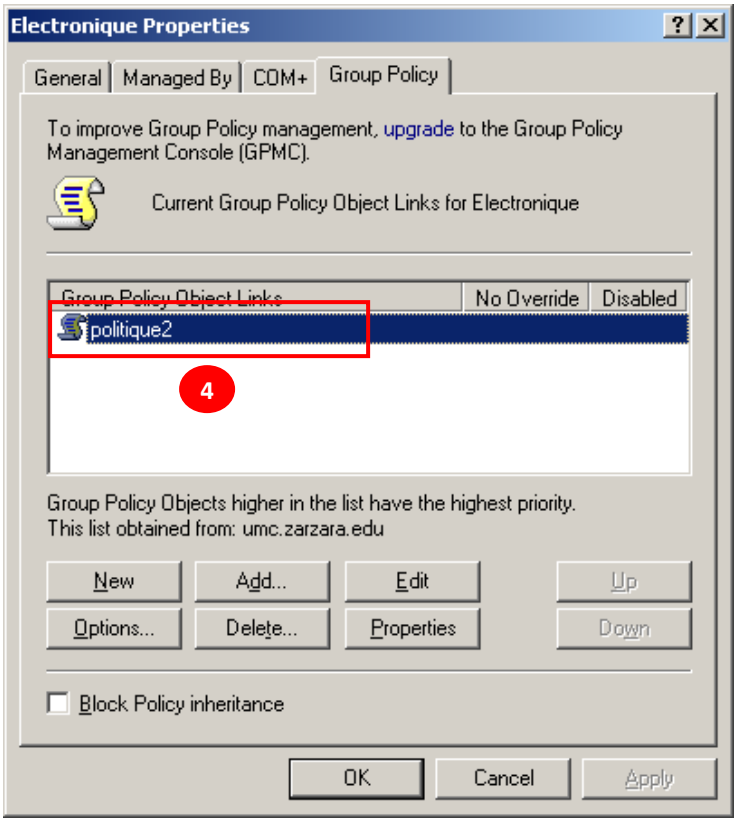


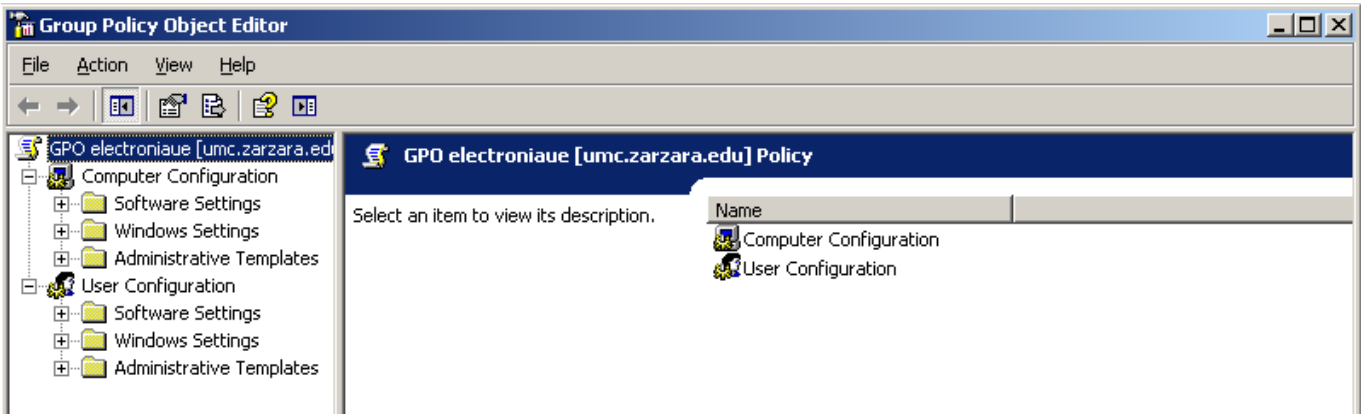


Création d'une nouvelle stratégie de la sécurité

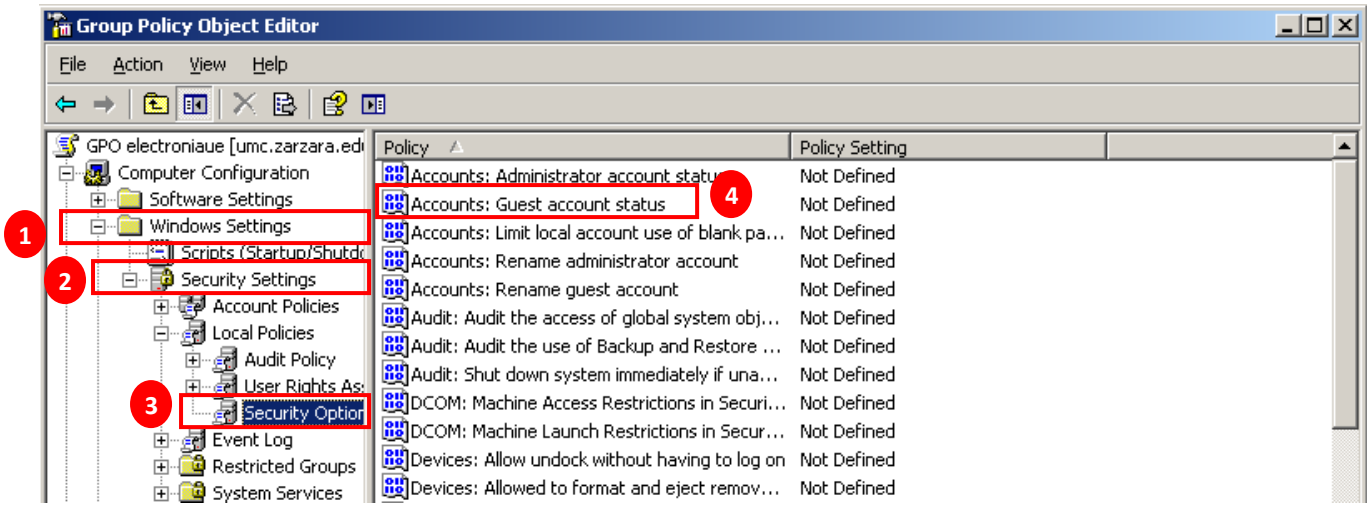


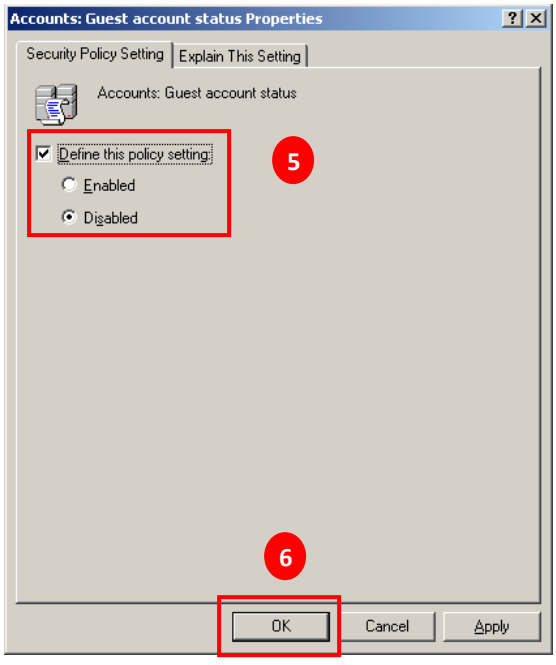

Electronique Properties
General
Managed By
COM+
Group Policy
2
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).
Current Group Policy Object Links for Electronique
Group Policy Object Links
No Override
Disabled
Group Policy Objects higher in the list have the highest priority.
This list obtained from: umc.zarzara.edu
New
Add...
Edit
Up
Delete...
Properties
Down
3
Block Policy inheritance
OK
Cancel
Apply


Electronique Properties
General
Managed By
COM+
Group Policy
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).
Current Group Policy Object Links for Electronique
Group Policy Object Links
No Override
Disabled
politique2
4
Group Policy Objects higher in the list have the highest priority.
This list obtained from: umc.zarzara.edu
New
Add...
Edit
Up
Options...
Delete...
Properties
Down
Block Policy inheritance
OK
Cancel
Apply

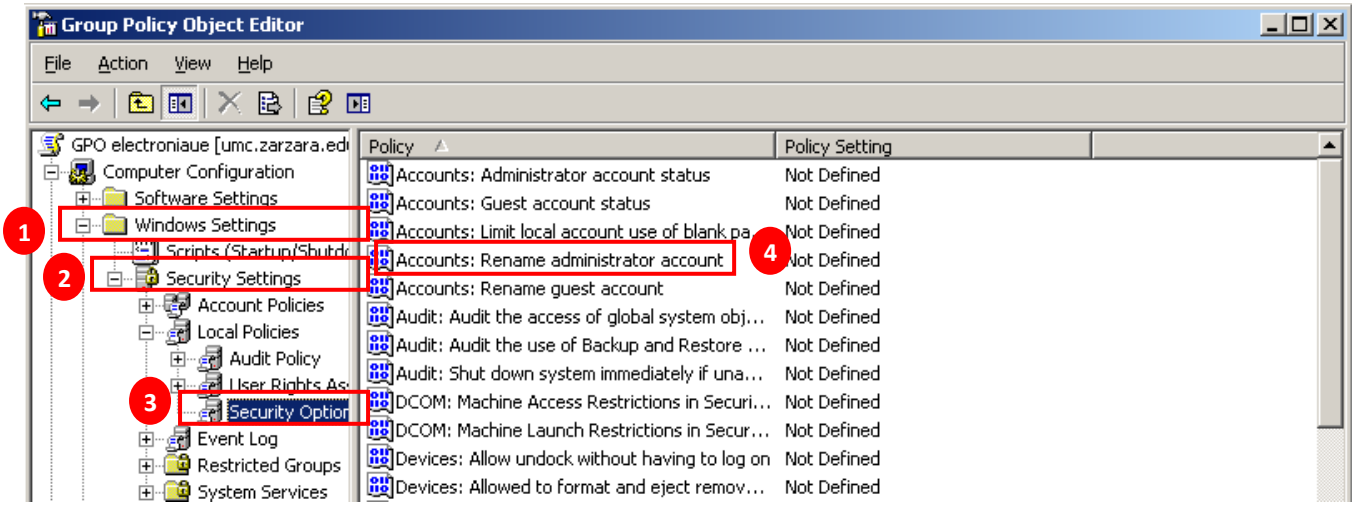


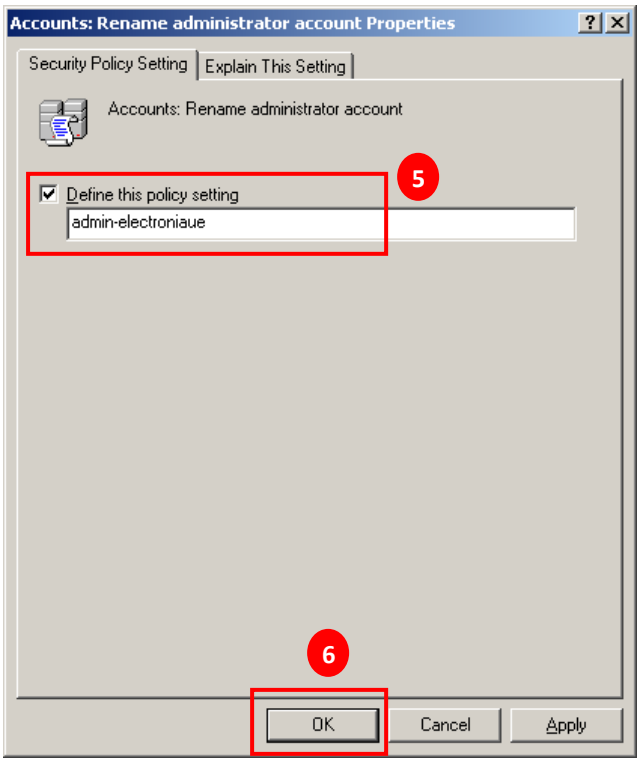
1. Règle 01 : Désactiver la connexion au domaine depuis un compte **invité**



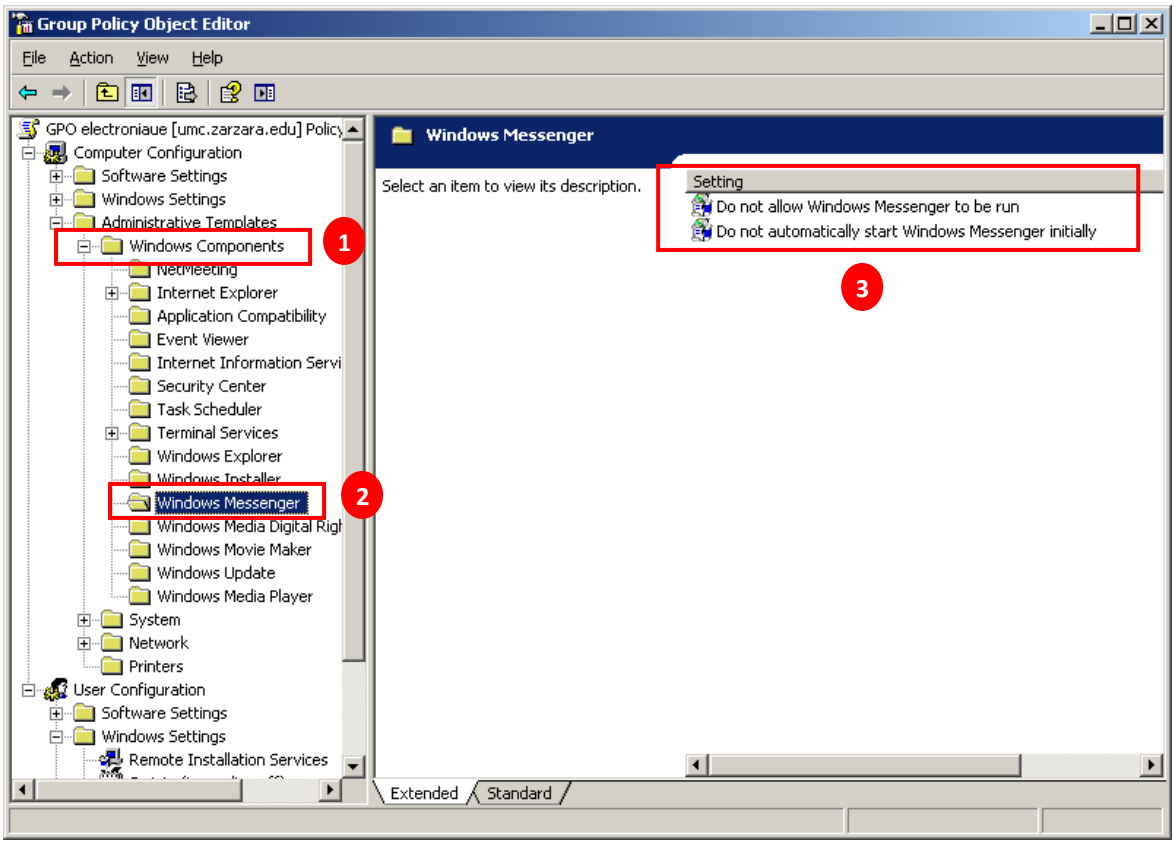


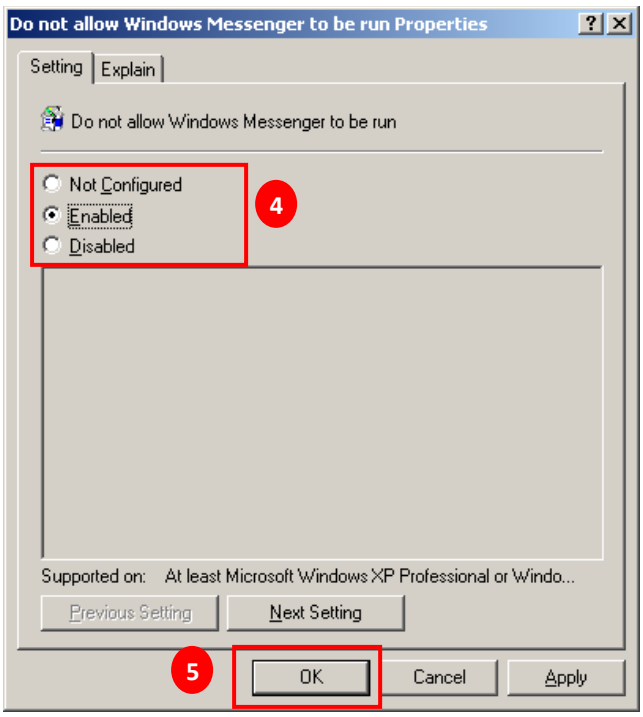
2. **Règle 2** : Renommer le compte administrateur à **admin-electronique.**

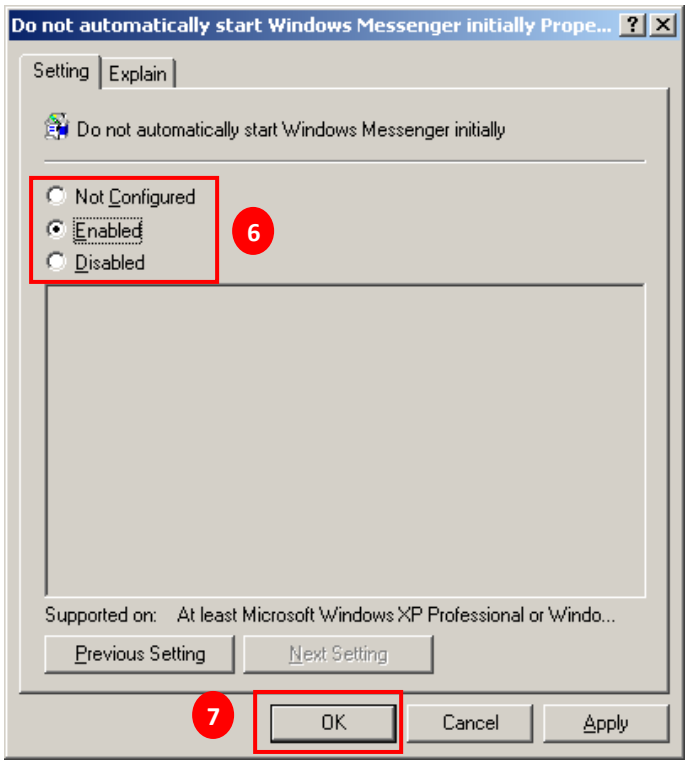




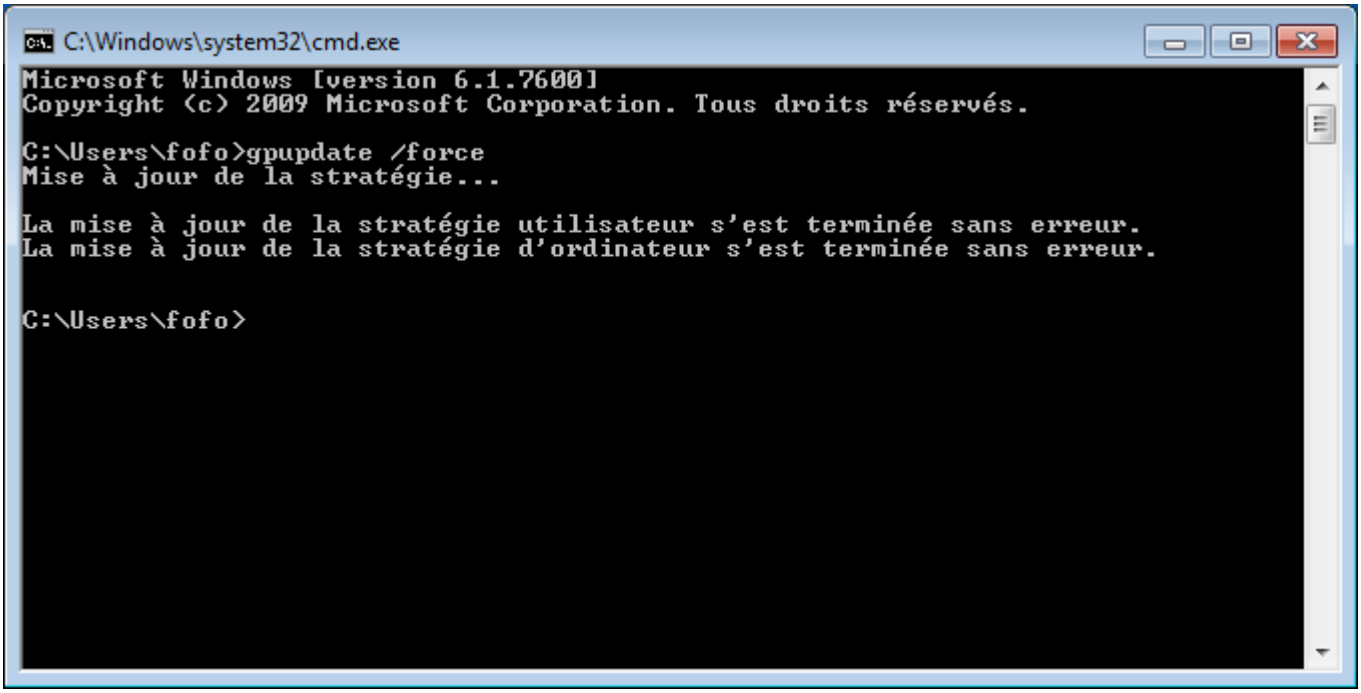
3. Règle 3 : Désactiver l'exécution de **Windows Massenger.**


Group Policy Object Editor
File Action View Help
GPO electroniaue [umc.zarzara.edu] Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Components
NetMeeting
Internet Explorer
Application Compatibility
Event Viewer
Internet Information Servi
Security Center
Task Scheduler
Terminal Services
Windows Explorer
Windows Installer
Windows Messenger
Windows Media Digital Rigl
Windows Movie Maker
Windows Update
Windows Media Player
System
Network
Printers
User Configuration
Software Settings
Windows Settings
Remote Installation Services
Windows Messenger
Select an item to view its description.
Setting
Do not allow Windows Messenger to be run
Do not automatically start Windows Messenger initially
Extended
Standard
1
2
3


Do not allow Windows Messenger to be run Properties
Setting
Explain
Do not allow Windows Messenger to be run
Not Configured
Enabled
Disabled
Supported on: At least Microsoft Windows XP Professional or Windo...
Previous Setting
Next Setting
OK
Cancel
Apply
4
5



Appliquer la mise à jour de la stratégie dans la machine **win1**



TP 6 : Installation d'un contrôleur de domaine