Université Pierre et Marie Curie – Sciences et Technologies

UFR 919 d'Ingénierie

Département de Licence (3) – mention : Informatique

Unité d'Enseignement : LI350-2015fev
Initiation à l'Administration de Systèmes

Systèmes "Windows" – Cours 4 : semaine 10

Active Directory (AD) - Group Policy Object (GPO)

Document (3W) **Malika Maoui Henda, Bruno Leseur**
(auteur originel : Laurent Gydé)

http://www-licence.ufr-info-p6.jussieu.fr/lmd/licence/2014/ue/LI350-2015fev/

année 2014-2015, semestre 2

Active Directory

Active Directory

- AD permet de :
  - centraliser
  - de structurer
  - d'organiser et de contrôler les ressources réseau dans les environnements Windows 2008
- AD est un annuaire des objets du réseau, il permet aux utilisateurs :
  - de localiser, de gérer et d'utiliser facilement les ressources

Schéma Active Directory

- Le schéma Active Directory stocke la définition de tous les objets d'Active Directory (ex : nom, prénom pour l'objet utilisateur).
- Il n'y a qu'un seul schéma pour l'ensemble de la forêt, ce qui permet une homogénéité de l'ensemble des domaines.

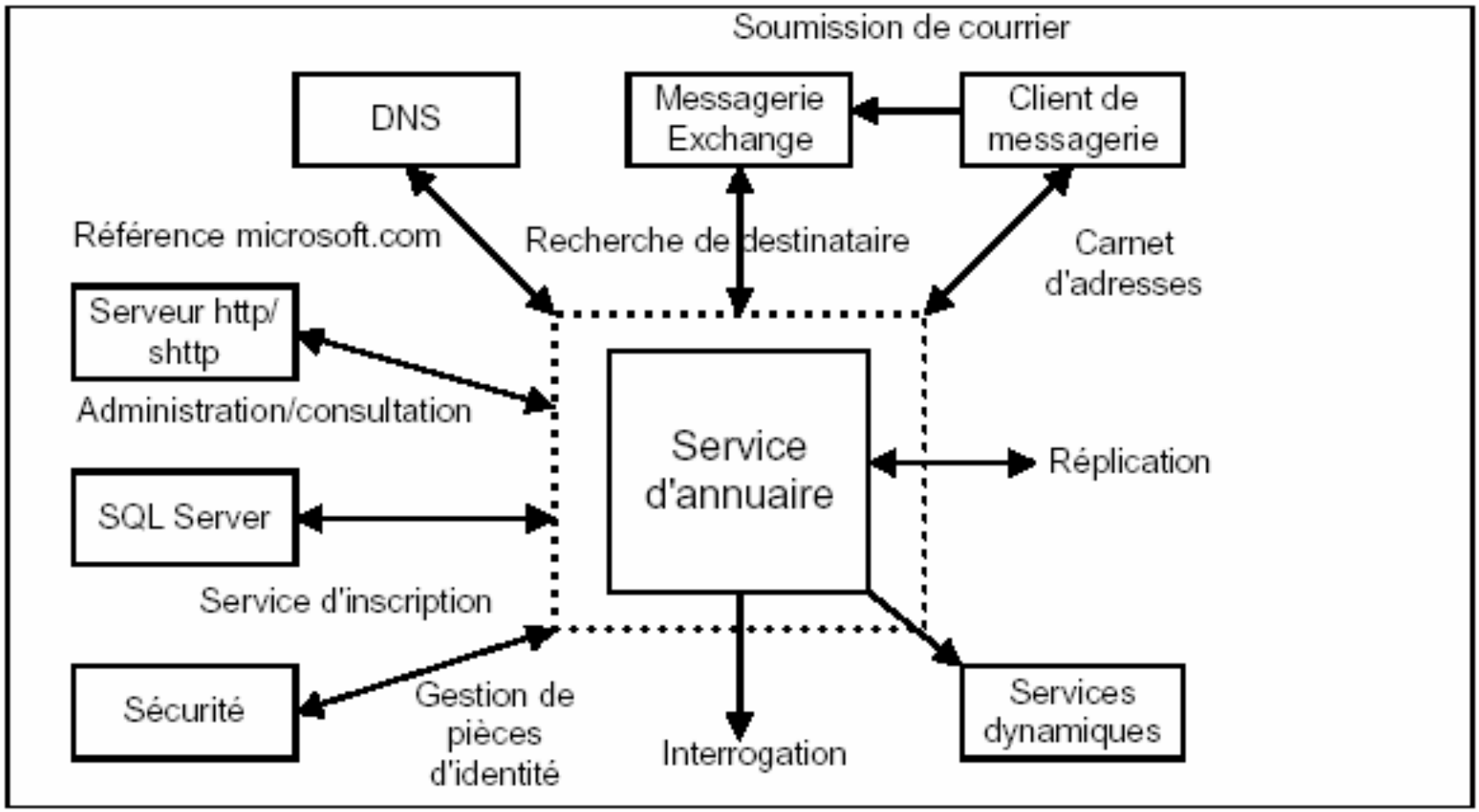
Catalogue global

- Le catalogue global contient une partie des attributs les plus utilisés de tous les objets Active Directory. Il contient aussi les informations nécessaires pour déterminer l'emplacement de tout objet de l'annuaire.
- Le premier contrôleur de domaine installé au sein d'une forêt est automatiquement serveur de catalogue global. Il est possible de configurer d'autres contrôleurs de domaine en tant que serveur de catalogue global afin de réguler le trafic.

Active directory

- Un chef d'orchestre chargé de la gestion d'un parc Informatique

Active Directory



Active Directory – AD

- Depuis Windows 2000, Active Directory est l'annuaire unique sous Windows pour la gestion des :
  - Utilisateurs
  - Groupes
  - Contacts
  - Serveurs
  - Ordinateurs
  - Imprimantes
  - Dossiers partagés
  - …

L'environnement Active Directory

- AD s'inscrit dans un environnement de services systèmes et réseau complet
  - TCP/IP
  - DHCP
  - DNS
  - SNTP
  - LDAP/LDIF
  - Kerberos/X509
  - NTFS
- Les services ci-dessus sont :
  - Soit indispensables pour installer AD
  - Soit dépendants de l'installation de AD

L'environnement Active Directory

- TCP/IP
  - Support natif de IPv4 et de IPv6
  - Ne peut pas être désinstallé
  - Il est toujours possible d'ajouter d'autres protocoles (NetBeui, NWLINK …)
- DHCP (Dynamic Host Configuration Protocol)
  - Récupération automatique des configurations réseau (IPv4 seulement), notamment l'adresse IP et les informations de résolution de nom
  - Configurable à l'intérieur d'Active Directory

L'environnement Active Directory

- DNS (Domain Name System)
  - Le service de DNS est obligatoire avec Active Directory
  - Il est utilisé pour la résolution des noms ET la résolution des services
  - On peut utiliser le DNS de Windows ou un autre DNS obligatoirement en mode dynamique
- SNTP (Simple Network Time Protocol)
  - Permet la synchronisation des horloges des systèmes (stockage de l'heure UTC, affichée en tenant compte du fuseau horaire)
  - Impératif pour le protocole d'authentification de Windows (Kerberos)

L'environnement Active Directory

- LDAP (Lightweight Directory Access Protocol)
  - LDAP est un protocole du service d'annuaire utilisé pour interroger et mettre à jour Active Directory.
  - LDAP est un standard d'accès à l'annuaire, AD est compatible LDAPv3 (en revanche, ce n'est pas un annuaire X.500)
  - LDAP permet des requêtes de gestion de la base de données d'AD pour des recherches, ajouts, modifications et suppressions d'objets

L'environnement Active Directory

- LDIF (LDAP Directory Interchange Format)
  - LDIF permet des importations, exportations et modifications d'Active Directory par fichiers de textes
  - Permet de charger AD à partir d'une base de données externe ou inversement (exemple, gestions des comptes utilisateurs à partir de la base de données du personnel)

L'environnement Active Directory

- Kerberos
  - Protocole d'authentification par défaut depuis Windows 2000 (remplace LM/NTLM utilisé jusqu'à NT4)
  - Compatible Kerberos V5 (MIT)
  - Authentification mutuelle du client et du serveur
  - Adresse du serveur Kerberos utilisé pour l'ouverture de session extraite du DNS

L'environnement Active Directory

- X.509
  - Windows Server propose les services de certificats compatibles X.509
  - Renforcement de la sécurité (authentification, intégrité, confidentialité, non répudiation)
  - Utilisable par les autres services
    - Authentification par carte à puce
    - Chiffrement de fichiers (EFS)
    - Chiffrement des données sur le réseau (IPSEC)

La structure logique Active Directory

- Forêt
  - C'est un ensemble de domaines n'ayant pas le même nom commun mais partageant un schéma et un catalogue global commun
  - Exemple : consulting.com et egilia.lan
  - Par défaut, les relations d'approbation entre les domaines au sein d'une forêt sont bidirectionnelles

La structure logique Active Directory

- Plusieurs arbres constituent une forêt, ils doivent partager :
  - Le schéma (modèle de données d'Active Directory)
  - La configuration de la forêt (domaine racine de la forêt)
  - Le catalogue global (groupes universels)
- Les racines des arbres sont reliées par des relations d'approbation

La hiérarchie logique Active Directory

- Domaine
  - C'est un ensemble de ressources et de services utilisant un même annuaire pour l'authentification et la gestion des accès (même notion qu'avec Windows NT4)
  - C'est un ensemble d'ordinateurs et /ou d'utilisateurs qui partagent une même base de données d'annuaire
  - Un domaine a un nom unique sur le réseau

La hiérarchie logique Active Directory

- Des domaines différents peuvent se communiquer des informations de sécurité grâce aux relations d'approbation
- Dans un domaine Windows 2008, tous les serveurs maintenant le domaine (contrôleurs de domaine) possèdent une copie de l'annuaire AD.
- Chaque contrôleur est capable de recevoir ou de dupliquer les modifications.

La hiérarchie logique Active Directory

- Arbre
  - Les domaines sont organisés selon une structure d'arbre doté de relations d'approbations
  - On ajoute un domaine dans un arbre en le désignant comme enfant d'un domaine déjà configuré
  - Le nommage des domaines est celui du DNS (pour ne pas être lié au « vrai » DNS de l'internet, exemple « .local »)

La hiérarchie logique Active Directory

- Unité Organisationnelle (UO)
  - L'UO est un objet conteneur utilisé pour organiser les objets au sein du domaine. Il peut contenir d'autres objets comme :
    - Comptes utilisateurs
    - Groupes
    - Ordinateurs
    - Imprimantes
    - Autres UO
    - ...

La hiérarchie logique Active Directory

- Les UO permettent :
  - d'organiser de façon logique les objets de l'annuaire
  - de faciliter la délégation de pouvoir selon l'organisation des objets et de contrôler l'environnement des utilisateurs et des ordinateurs grâce à l'application de stratégie de groupe (GPO)
  - On peut configurer certaines propriétés au niveau de l'UO
    - Délégation de l'autorité d'administration
    - Application de stratégies de groupes
    - …

La hiérarchie logique Active Directory

Rôles de maîtres d'opération

- Avec Windows NT 4.0, les contrôleurs de domaine suivent un schéma maître/esclave (PDC / BDC)
- Dans un domaine Windows 2000/2008, cette notion n'existe plus, on parle de contrôleurs de domaine multi-maîtres.
- Les modifications d'AD peuvent être faites sur n'importe quel contrôleur de domaine. Il existe des exceptions pour lesquelles les modifications sont réalisées sur un contrôleur de domaine spécifique.

- Ces exceptions sont nommées rôles de maître d'opération et sont au nombre de cinq :
- **Contrôleur de schéma** : C'est le seul contrôleur de domaine habilité à modifier et à mettre à jour le schéma.
- **Maître d'attribution des noms de domaine :** Il permet d'ajouter ou de supprimer un domaine dans une forêt.

- **Emulateur PDC :** Il gère également le processus de verrouillage des comptes utilisateurs, les changements de mots de passe et toutes les modifications faites sur des objets de stratégie de groupe.
- **Maître d'identificateur relatif ou maître RID:** Il distribue des plages d'identificateurs relatifs (RID) à tous les contrôleurs de domaine afin de générer les identificateurs de sécurité (SID)…

- **Maître d'infrastructure** : Il permet de mettre à jour les éventuelles références d'un objet dans les autres domaines lorsque cet objet est modifié (déplacement, suppression,…).
- Les deux premiers rôles sont assignés au niveau de la forêt et les trois derniers au niveau du domaine.
- Par défaut le premier contrôleur de domaine d'une nouvelle forêt cumule les cinq rôles.

Structure Physique

- **Contrôleurs de domaine**
- Un contrôleur de domaine est un ordinateur exécutant Windows 2000 Server ou Windows 2008 Server qui stocke un réplicat de l'annuaire
- Il assure l'authentification et l'ouverture des sessions des utilisateurs, ainsi que les recherches dans l'annuaire
- Un domaine peut posséder un ou plusieurs contrôleurs de domaine.

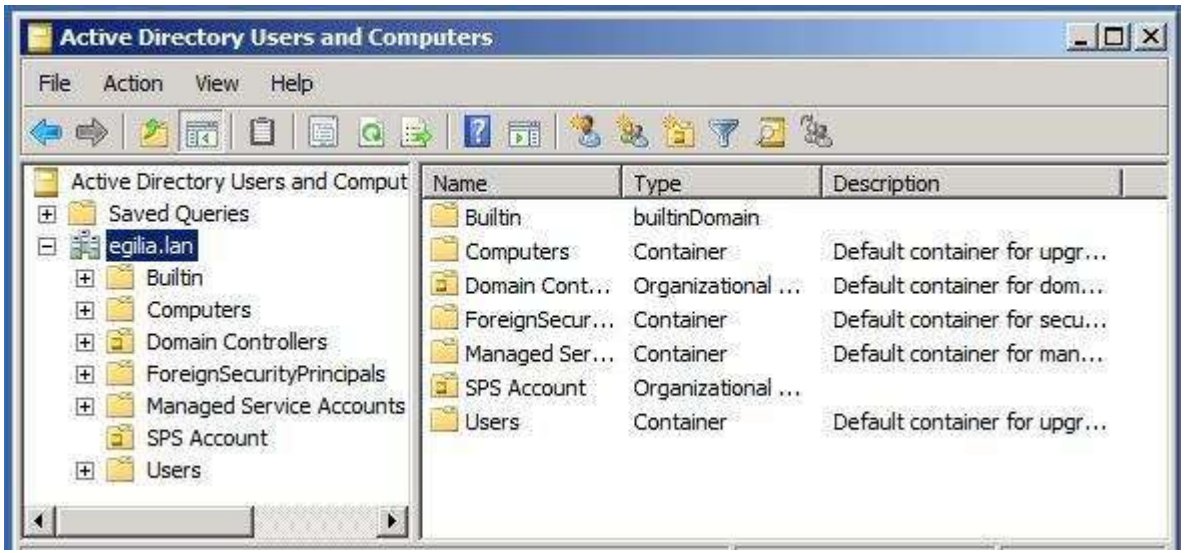
Méthodes d'administration

- **Utilisation d'Active Directory pour la gestion centralisée**
- Active Directory permet à un seul administrateur de centraliser la gestion et l'administration des ressources du réseau.
- Active Directory permet aussi d'organiser les objets de façon hiérarchique grâce aux conteneurs comme les unités organisationnelles, les domaines ou les sites.

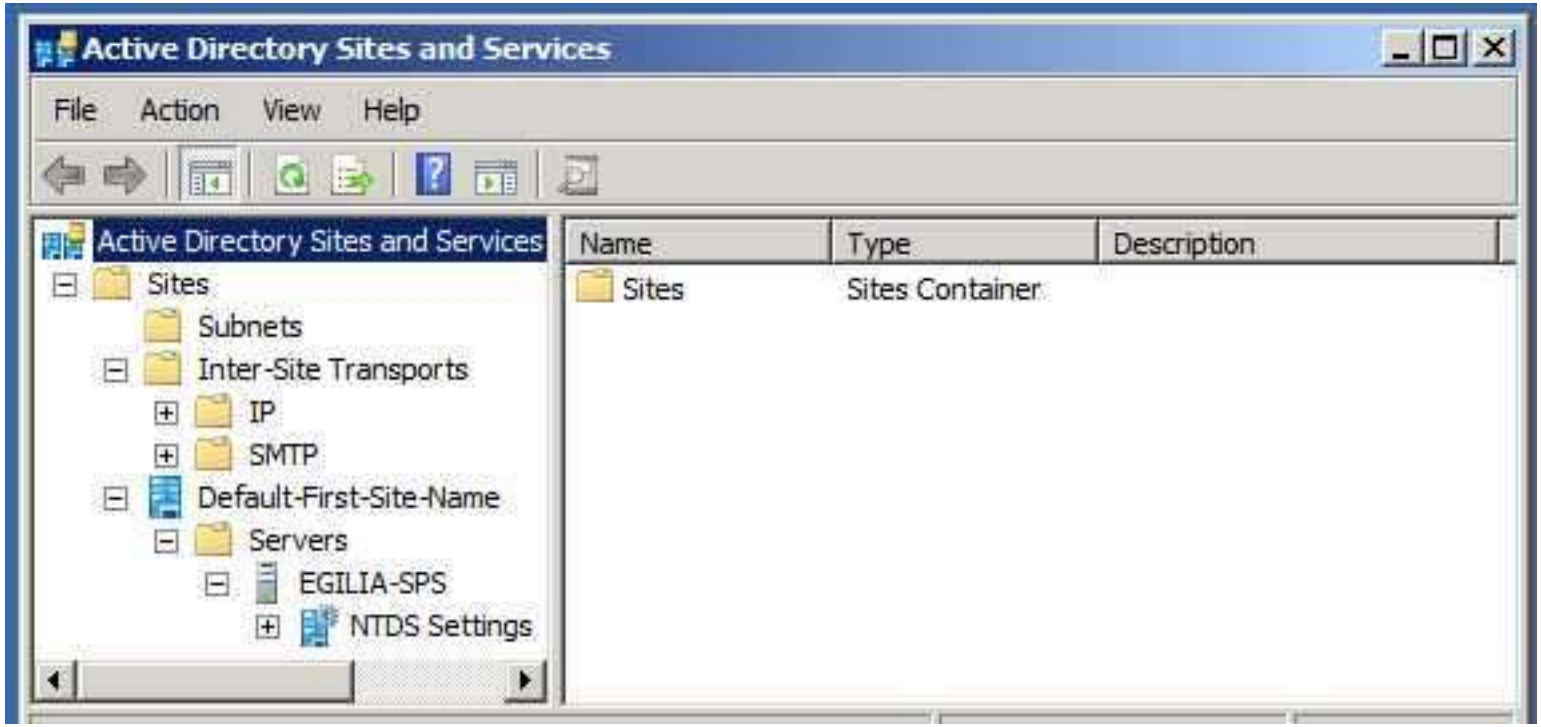
Les outils d'administration d'Active Directory

- L'administration du service d'annuaire Active Directory se passe par le biais de différentes consoles MMC :

- **Utilisateurs et ordinateurs Active Directory**: C'est le composant le plus utilisé pour accéder à l'annuaire. Il permet de gérer les comptes d'utilisateurs, les comptes d'ordinateurs, les fichiers et les imprimantes partagés, les unités d'organisation …



- **Sites et Services Active Directory** : Ce composant permet de définir des sites, des liens de sites et de paramétrer la réplication Active Directory.

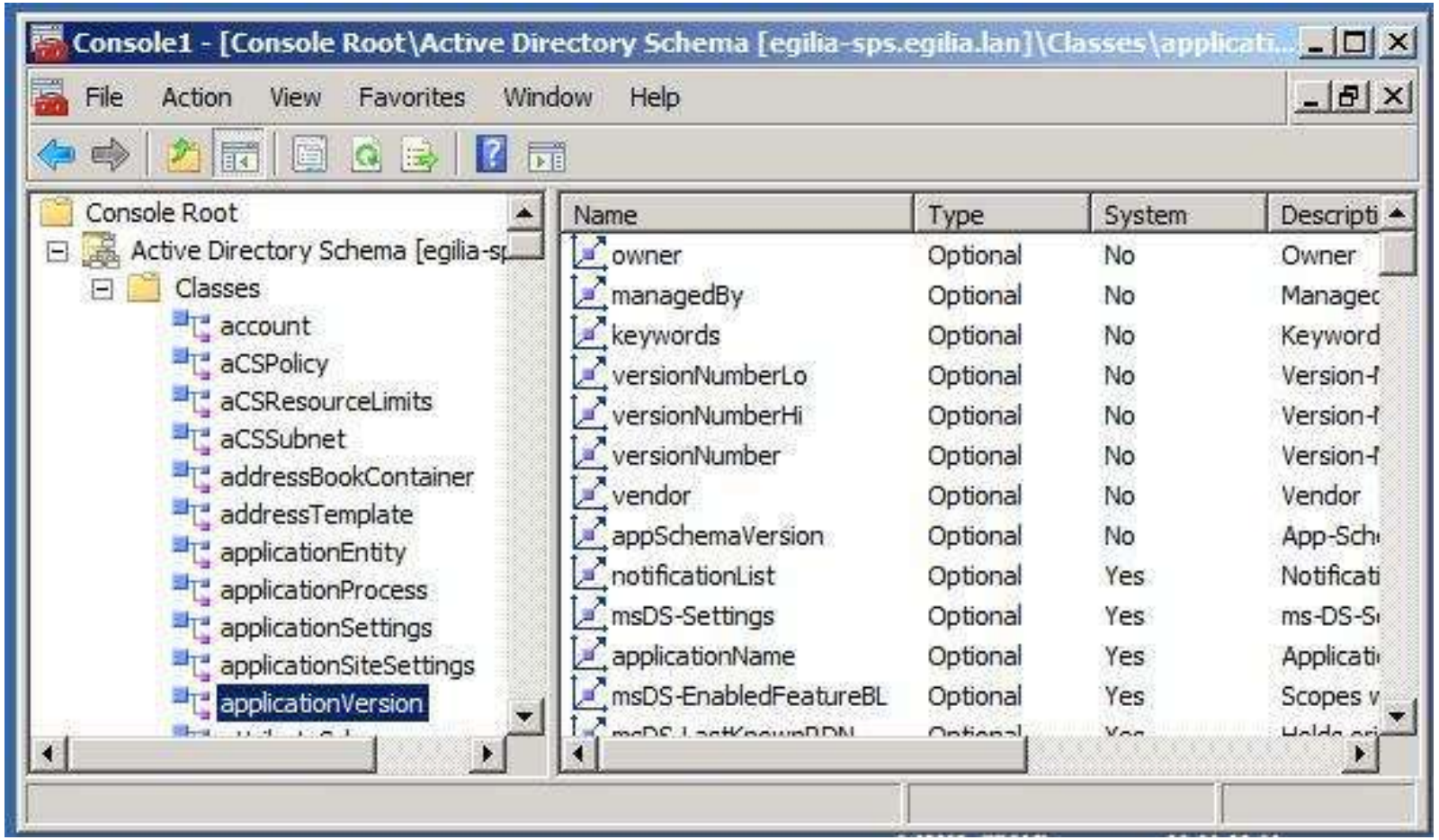


- **Domaines et approbations Active Directory**

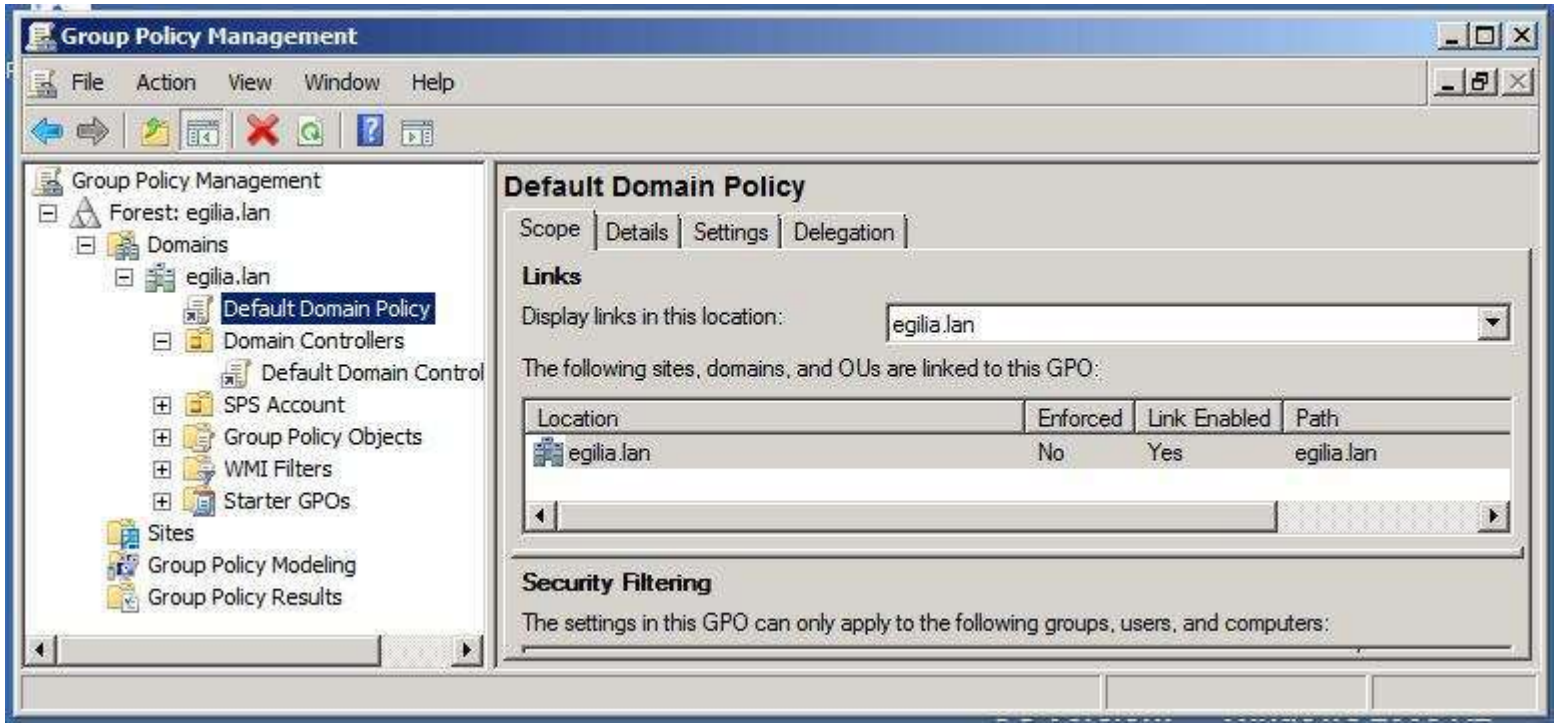
: Ce composant permet de mettre en place les relations d'approbations et les suffixes UPN. Il propose aussi d'augmenter le niveau fonctionnel d'un domaine ou d'une forêt.

- **Schéma Active Directory** : Ce composant permet de visualiser les classes et les attributs de l'annuaire. Pour pouvoir accéder à la console Schéma Active Directory, il faut dans un premier temps enregistrer une DLL. Pour cela, il vous faut ouvrir une invite de commande et taper la commande :

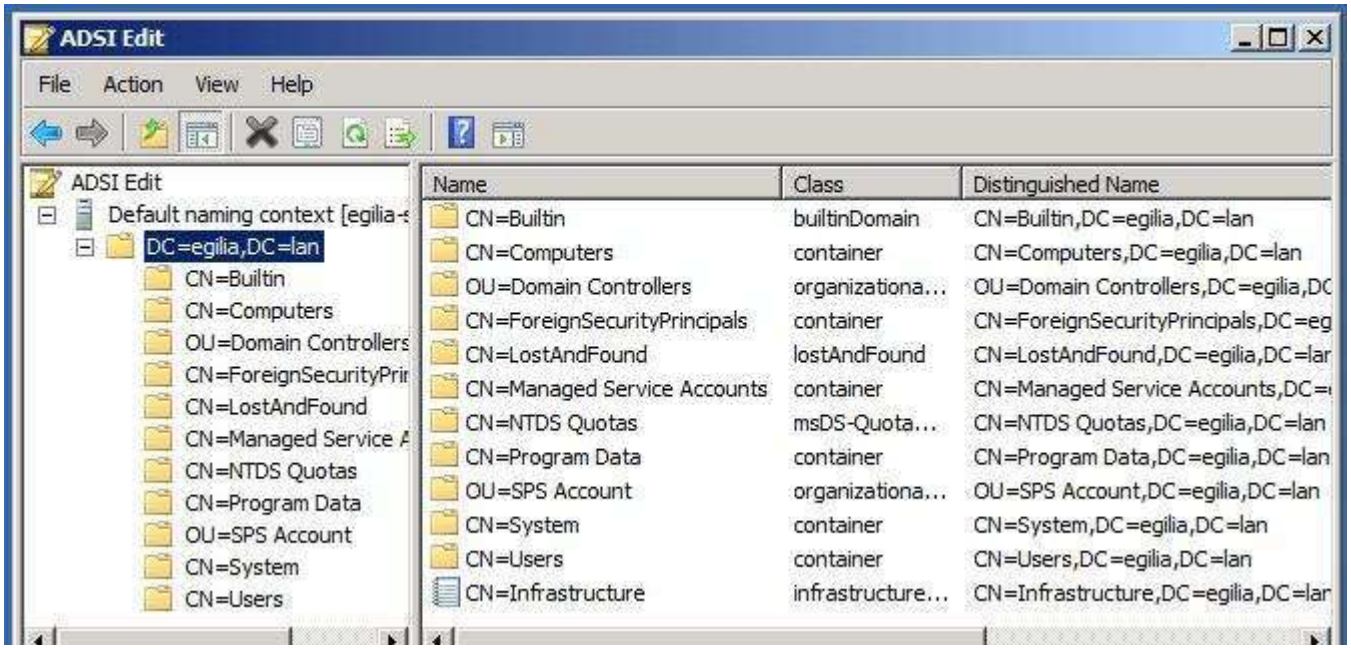
  regsvr32 schmmgmt.dll


Console1 - [Console Root\Active Directory Schema [egilia-sps.egilia.lan]\Classes\applicati...
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Schema [egilia-sp
Classes
account
aCSPolicy
aCSResourceLimits
aCSSubnet
addressBookContainer
addressTemplate
applicationEntity
applicationProcess
applicationSettings
applicationSiteSettings
applicationVersion
Name
Type
System
Descripti
owner
Optional
No
Owner
managedBy
Optional
No
Manage
keywords
Optional
No
Keyword
versionNumberLo
Optional
No
Version-
versionNumberHi
Optional
No
Version-
versionNumber
Optional
No
Version-
vendor
Optional
No
Vendor
appSchemaVersion
Optional
No
App-Sch
notificationList
Optional
Yes
Notificati
msDS-Settings
Optional
Yes
ms-DS-S
applicationName
Optional
Yes
Applicati
msDS-EnabledFeatureBL
Optional
Yes
Scopes v

- **Gestion des Stratégies de Groupe** : Ce composant permet de centraliser l'administration des stratégies de groupe d'une forêt, de vérifier le résultat d'une stratégie de groupe ou bien encore de comparer les paramètres de deux stratégies de groupe. Ce composant n'est pas disponible sur le CD-ROM de Windows 2008 Server, il doit être téléchargé sur le site de Microsoft.

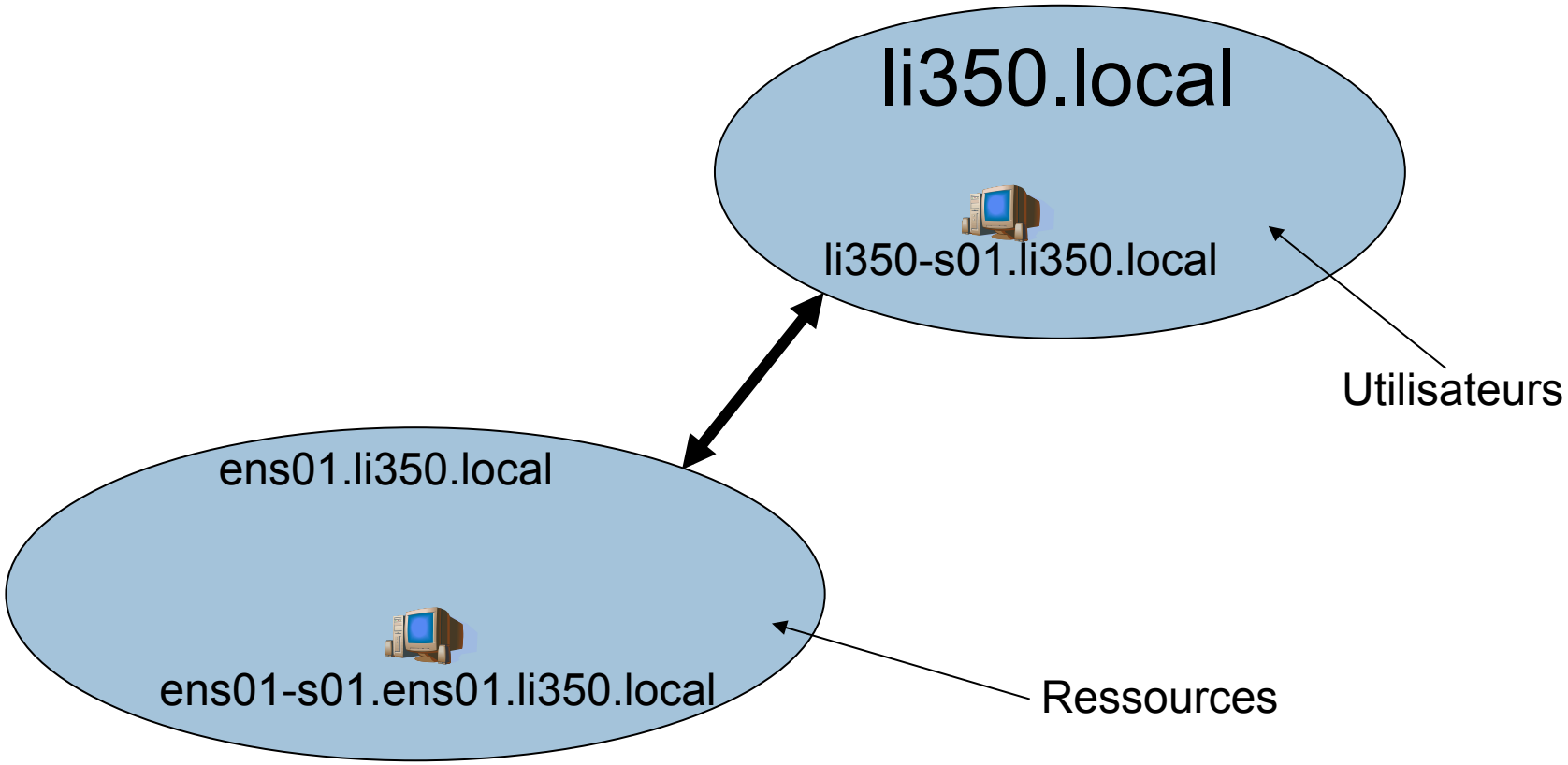

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: egilia.lan
Domains
egilia.lan
Default Domain Policy
Domain Controllers
Default Domain Control
SPS Account
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Default Domain Policy
Scope Details Settings Delegation
Links
Display links in this location: egilia.lan
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
egilia.lan No Yes egilia.lan
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:

- **ADSI Edit** : Ce composant permet de visualiser l'arborescence LDAP réelle du service d'annuaire. Elle peut s'avérer utile pour lire ou modifier certains attributs ou certains objets de l'annuaire.



La hiérarchie Active Directory

- Exemple de démarrage d'une forêt Active Directory



Les pré requis pour installer Active Directory

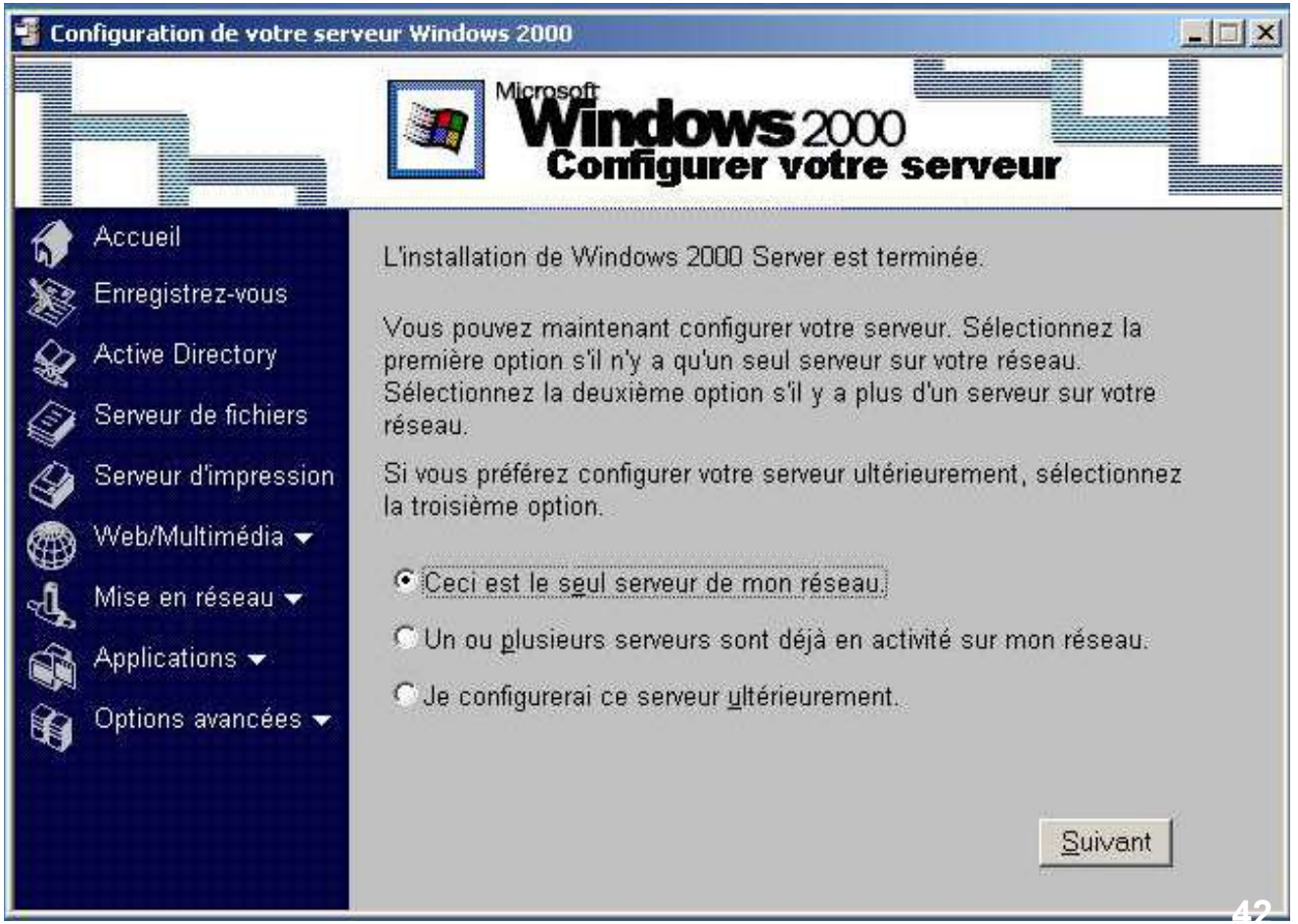
- Un ordinateur exécutant Windows 2008 Standard Edition, Enterprise Edition ou Datacenter Edition. Attention, le service d'annuaire Active Directory ne peut pas être installé sur Windows 2008 Server Web Edition.
- 250 Mo d'espace libre sur une partition ou un volume NTFS
- Les paramètres TCP/IP configurés pour joindre un serveur DNS.
- Des privilèges administratifs suffisants pour créer un domaine.

Installation ou suppression de Active Directory sur un serveur Windows 2000 et +

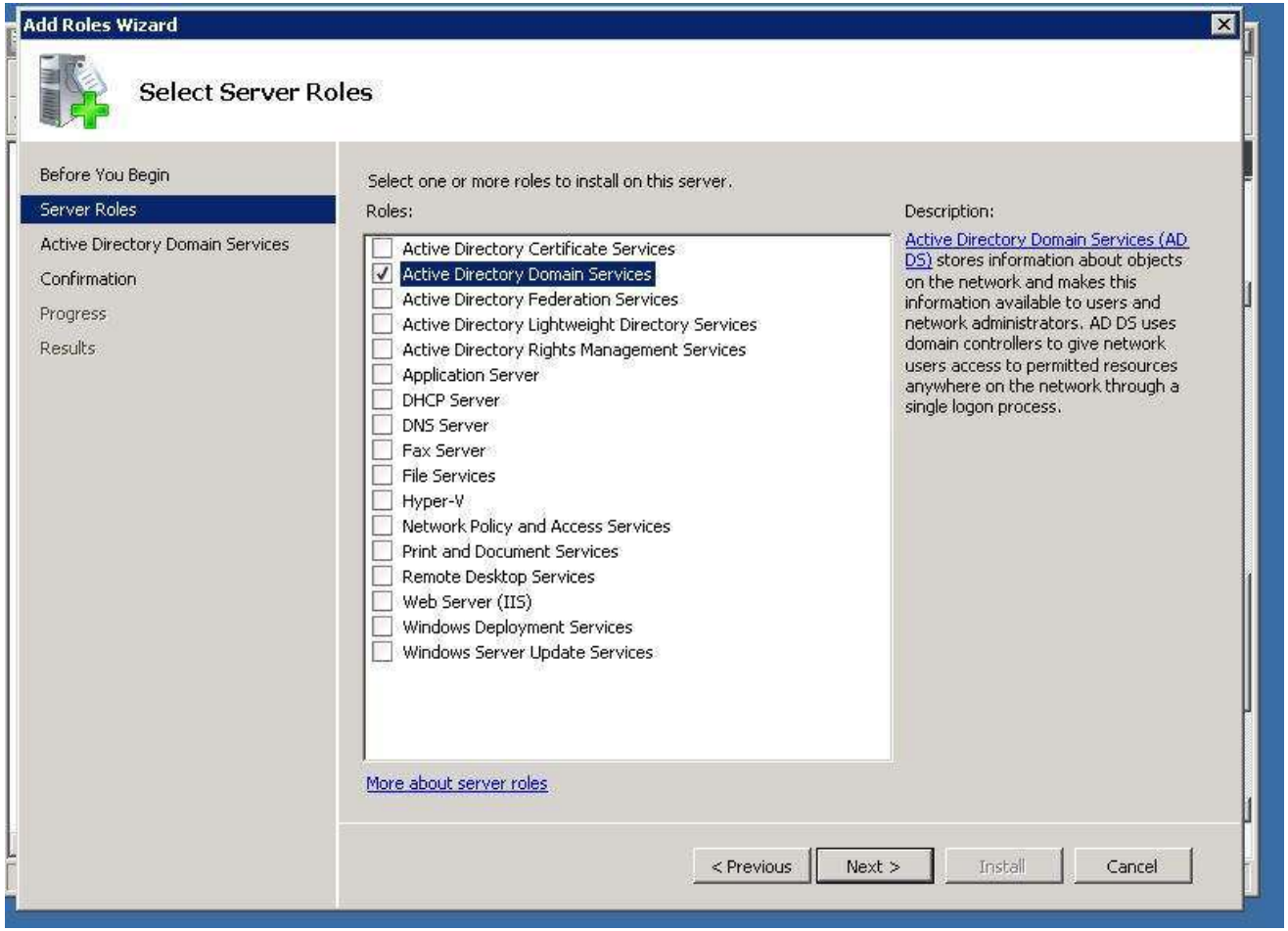
- Outil de gestion du serveur ou Dcpromo.exe
- Permet d'installer ou de supprimer Active Directory
- Si la machine est le dernier contrôleur du domaine, le domaine disparaît et le serveur devient alors un serveur autonome

La hiérarchie Active Directory

- Installation d'AD sur li350-s01.li350.local (1/4)



Ajouter le rôle AD Domain Services



Installation d'Active Directory

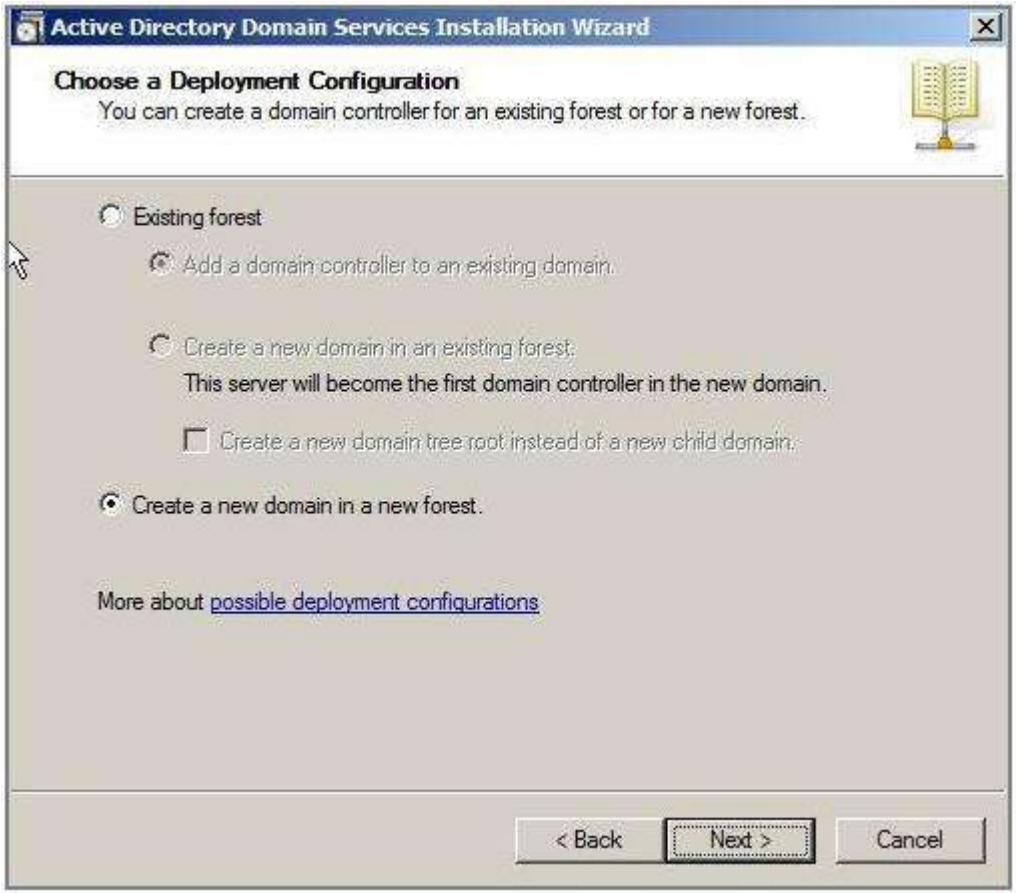
- La première étape consiste à **exécuter la commande dcpromo.**

Installation d'Active Directory

- Côchez la case "Utiliser les options avancées" de manière à avoir un maximum d'options...

Installation d'Active Directory

- un nouveau domaine dans une nouvelle forêt



Installation d'Active Directory

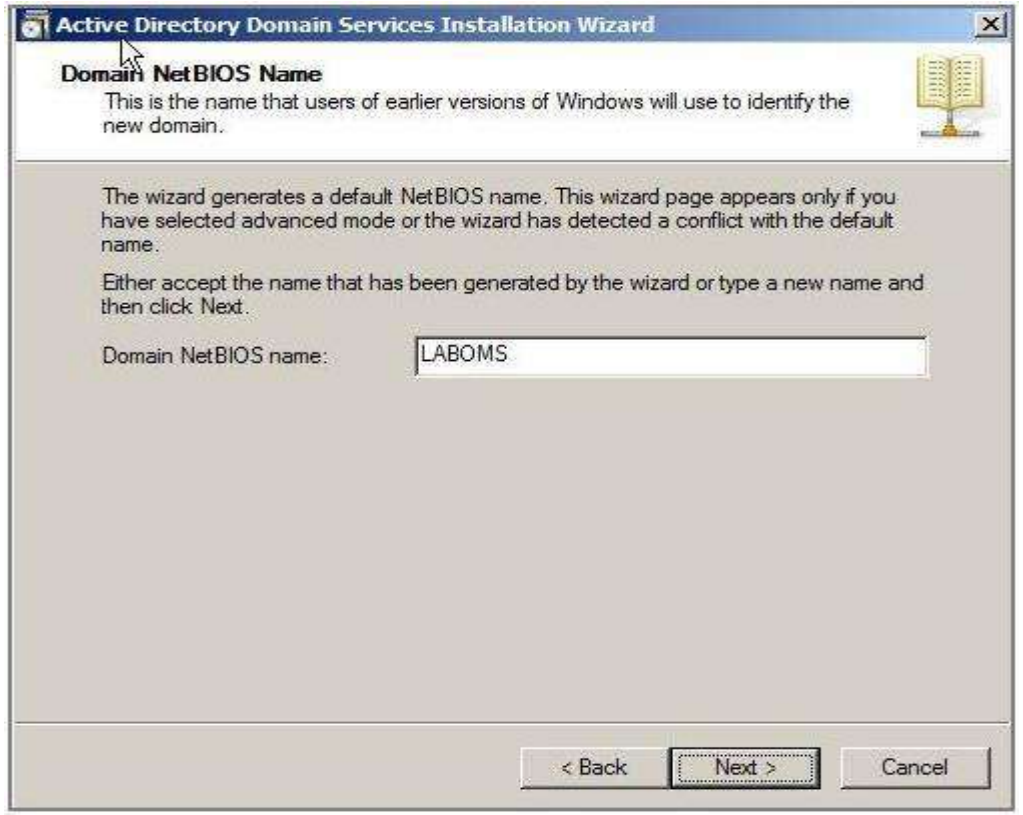
- le compte administrateur local deviendra administrateur du domaine une fois le service d'annuaire Active Directory installé

Installation d'Active Directory

- Il faut ensuite définir le nom DNS du domaine
- il n'est pas recommandé d'utiliser un domaine DNS *à seul niveau comme LABOMS*. Mieux vaut utiliser un nom de domaine à deux niveaux ou plus

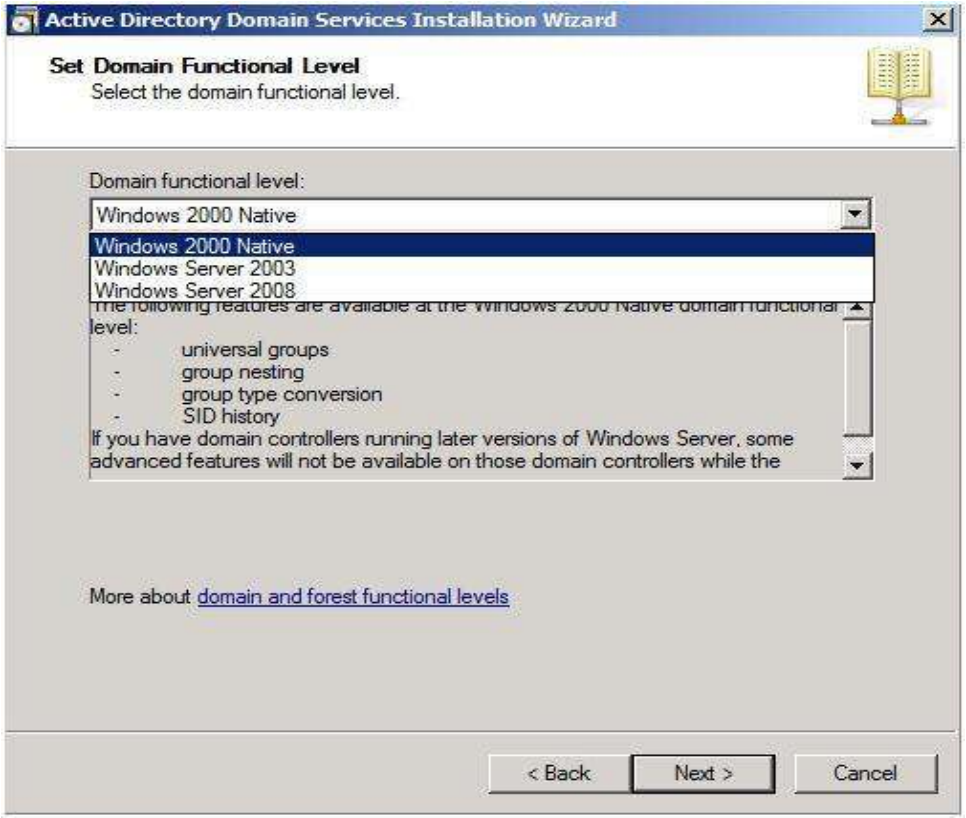
Installation d'Active Directory

- Une petite fenêtre apparaît ensuite pendant que l'installeur explore le réseau pour savoir si le nom NetBIOS existe déjà.



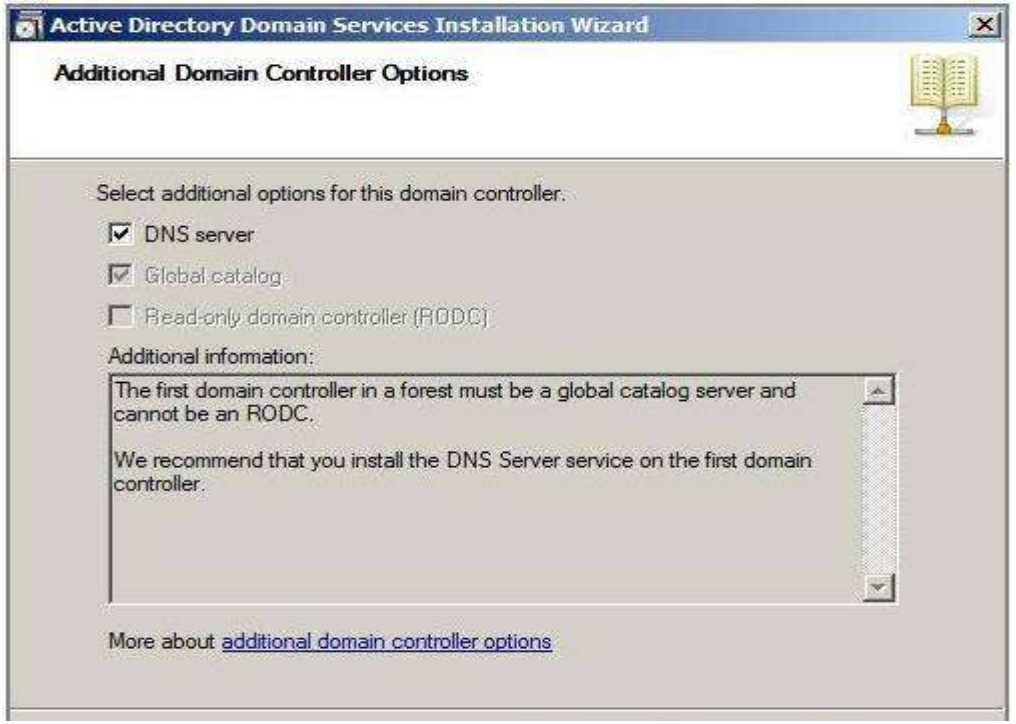
Installation d'Active Directory

- Etant donné que l'on crée une nouvelle forêt, l'administrateur doit choisir le niveau fonctionnel de cette dernière.



Installation d'Active Directory

- La page de l'assistant nous propose d'installer les rôles suivants : **"Serveur DNS", "Serveur de catalogue global", "contrôleur de domaine en lecture seule".**

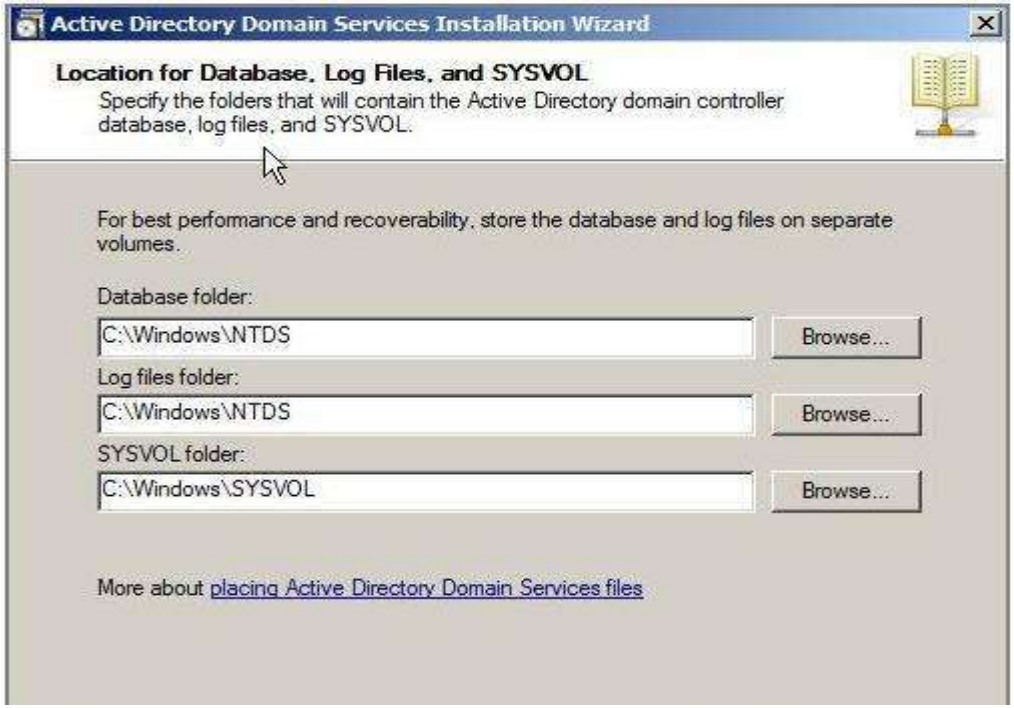


Installation d'Active Directory

- Dans mon exemple la case catalogue global est obligatoirement cochée étant donné qu'il s'agit du premier DC de la forêt (*pour la même raison il m'est impossible de cocher la case "contrôleur de domaine en lecture seule"*).

Installation d'Active Directory

- La page de l'assistant est dédiée au choix de **l'emplacement de la base de données, du journal des transactions et du partage SYSVOL** (sous Windows Server 2003, ces emplacements étaient configurés via 2 pages de l'assistant).

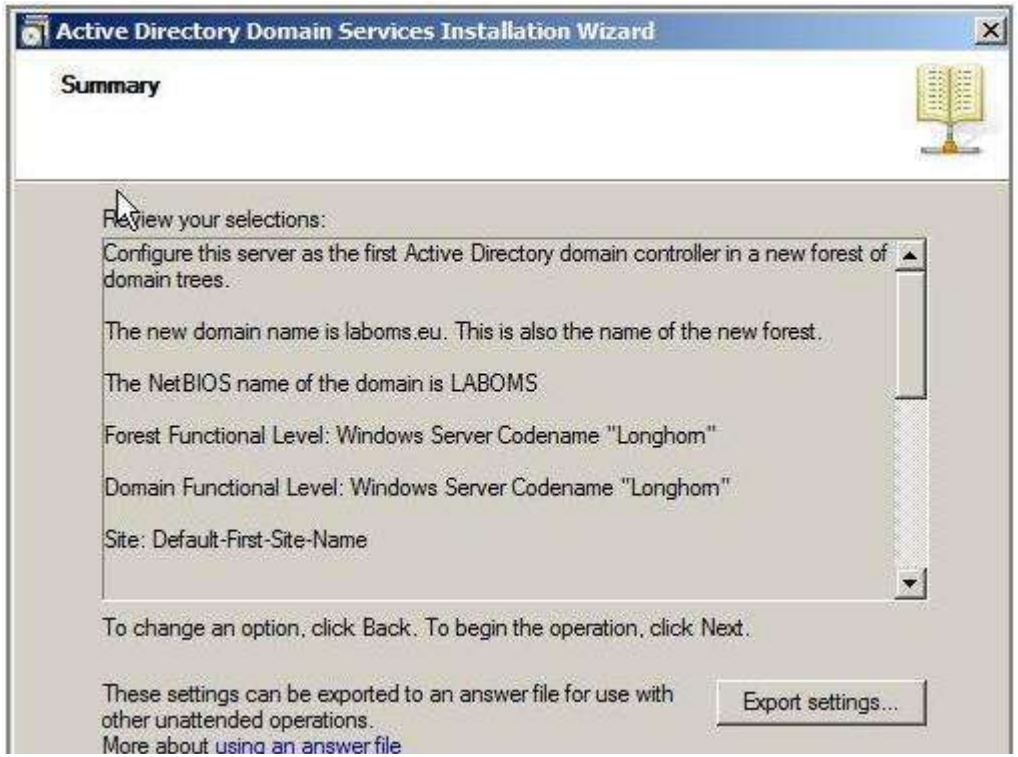


Installation d'Active Directory

- Une page nous propose d'entrer le mot de passe du compte de restauration.

Installation d'Active Directory

- La dernière page de l'assistant récapitule toutes les options sélectionnées. Il ne reste plus qu'à cliquer sur le bouton **"Suivant"** pour lancer l'installation.

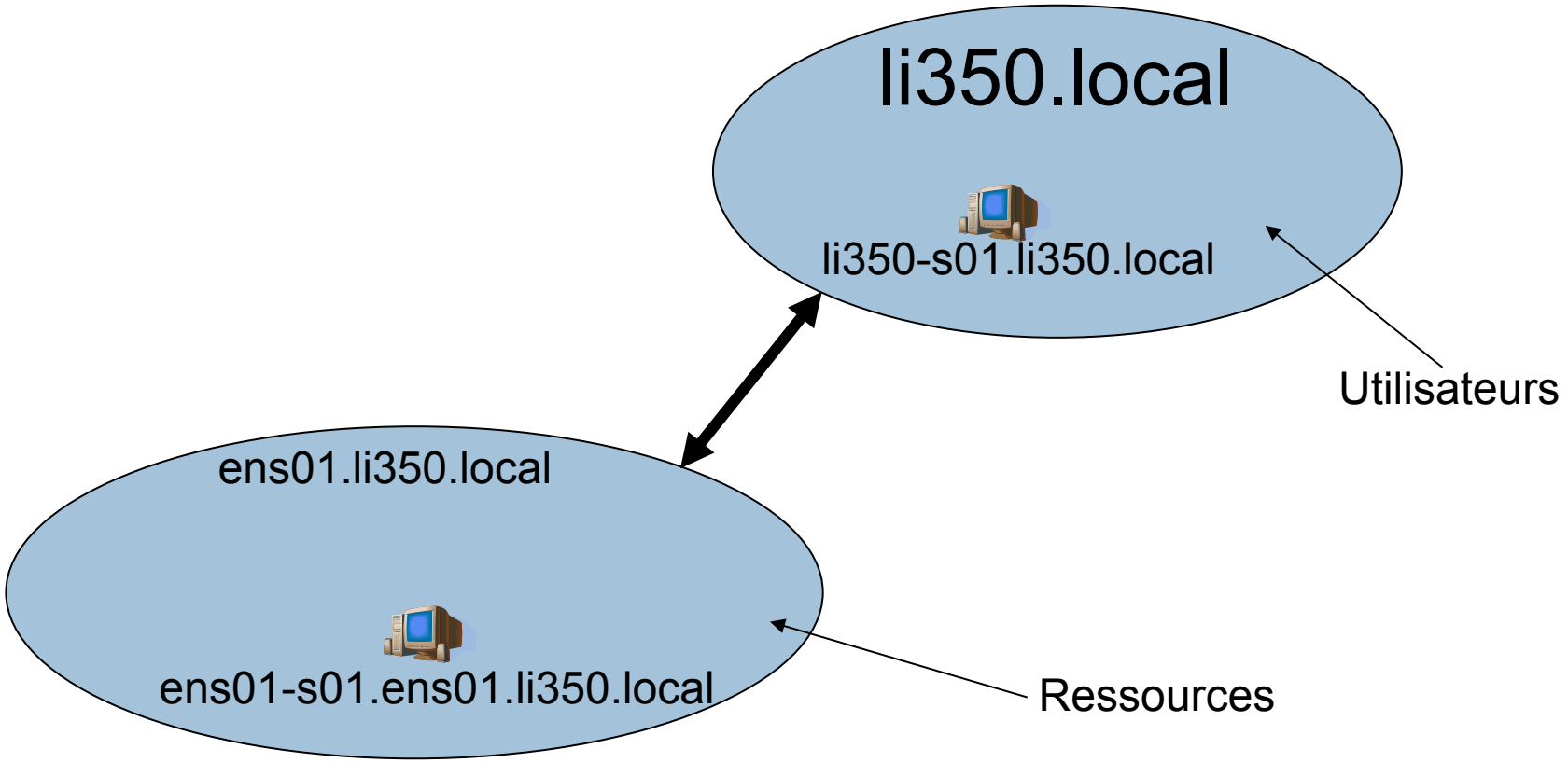


Installation d'Active Directory

- Dans tous les cas, le redémarrage reste obligatoire pour que l'annuaire soit fonctionnel.

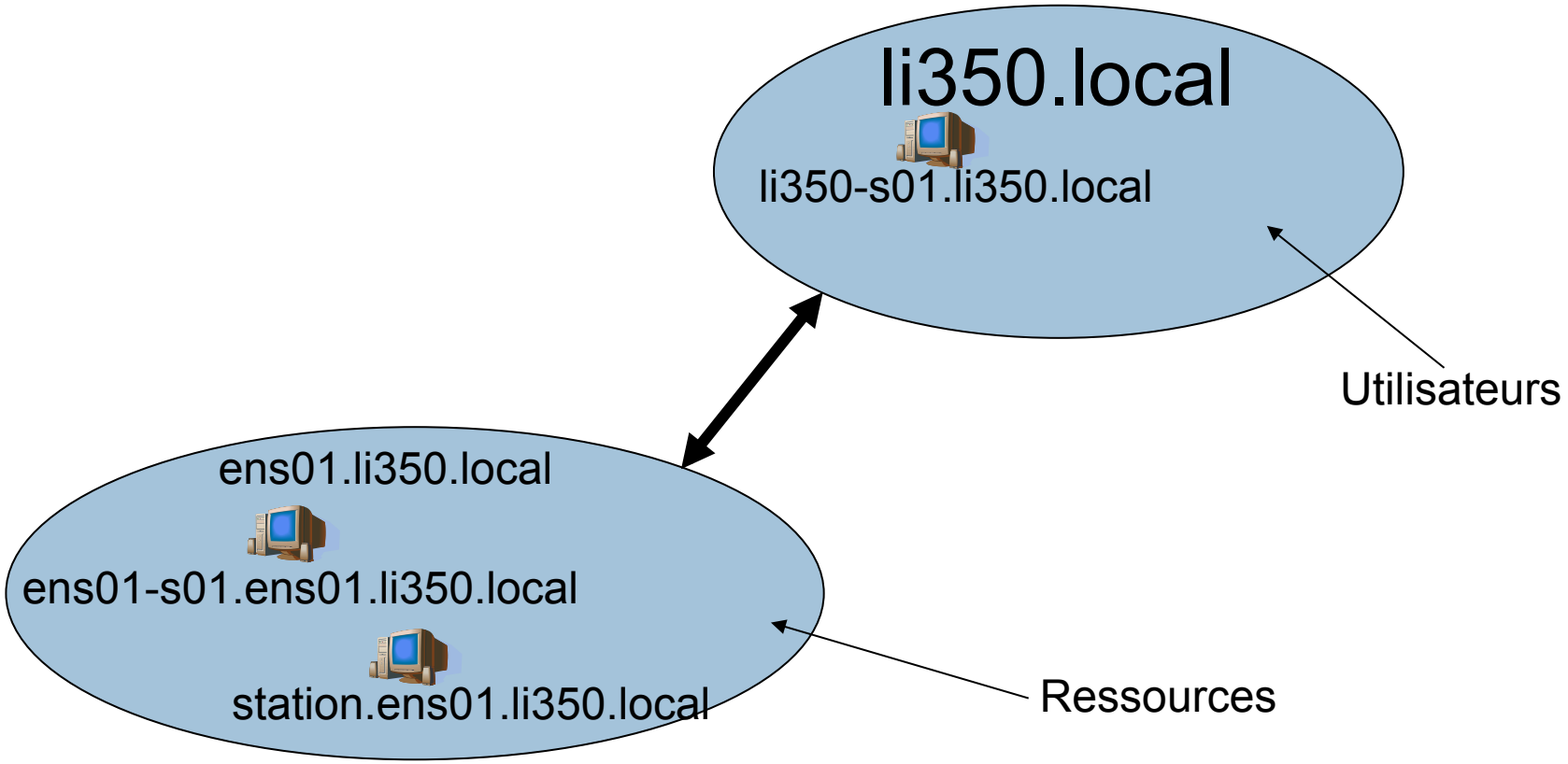
La hiérarchie Active Directory

- Exemple de démarrage d'une forêt Active Directory



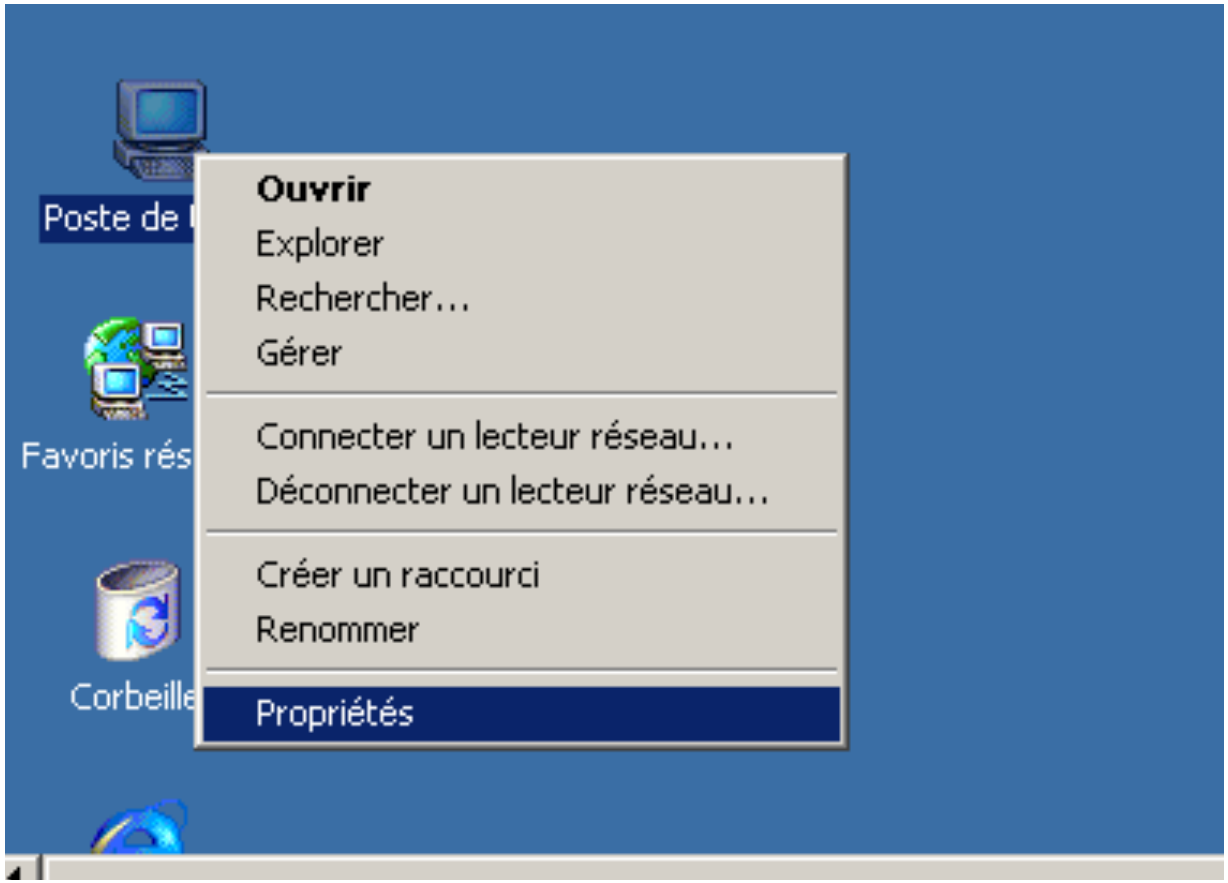
La hiérarchie Active Directory

- Exemple de démarrage d'une forêt Active Directory – Ajout d'une station



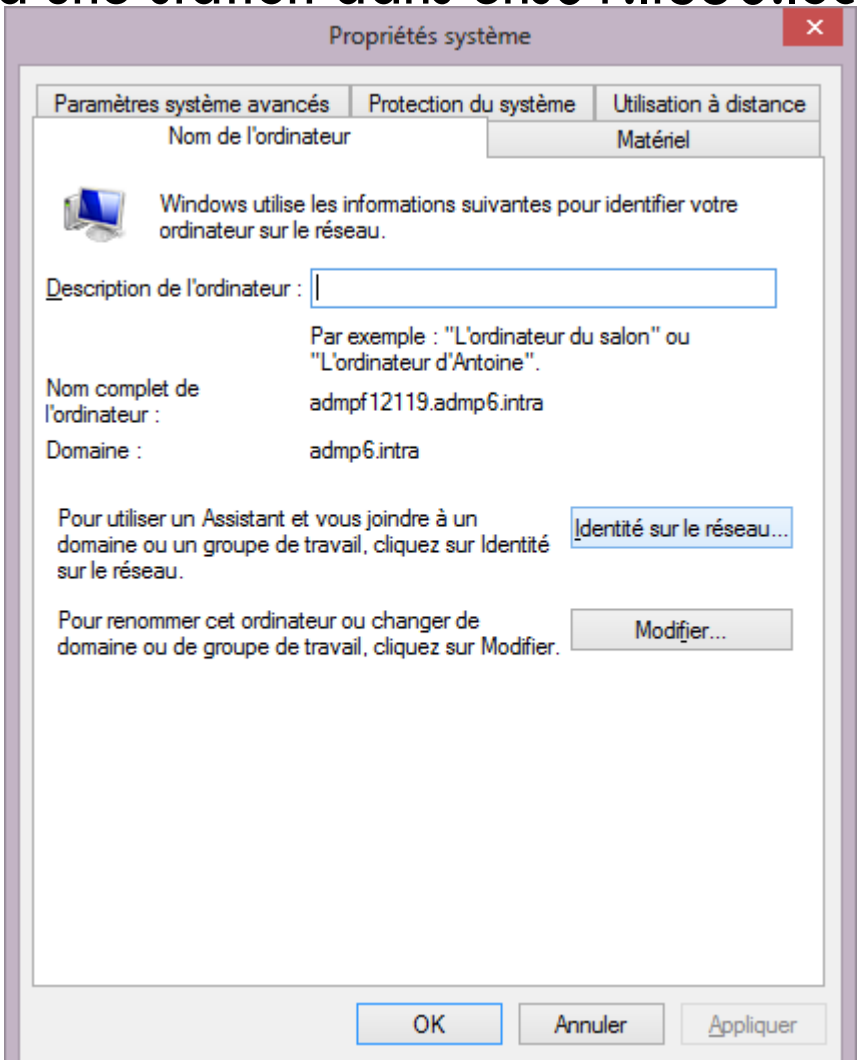
La hiérarchie Active Directory

- Ajout d'une station dans ens01.li350.local



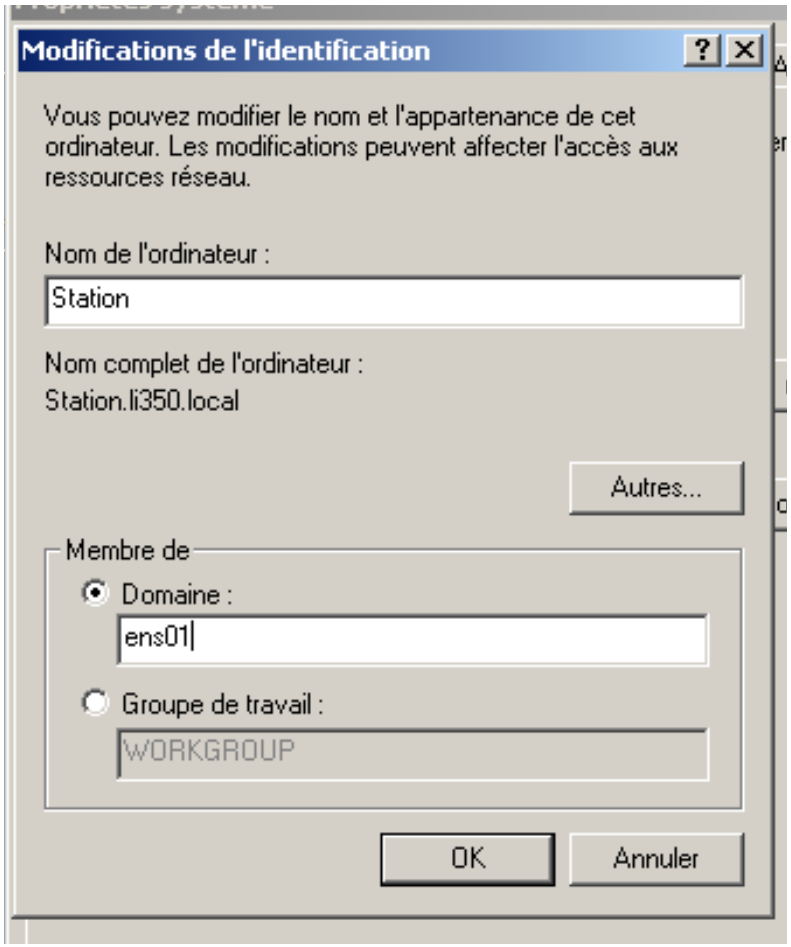
La hiérarchie Active Directory

- Ajout d'une station dans ens01.li350.local (2/9)



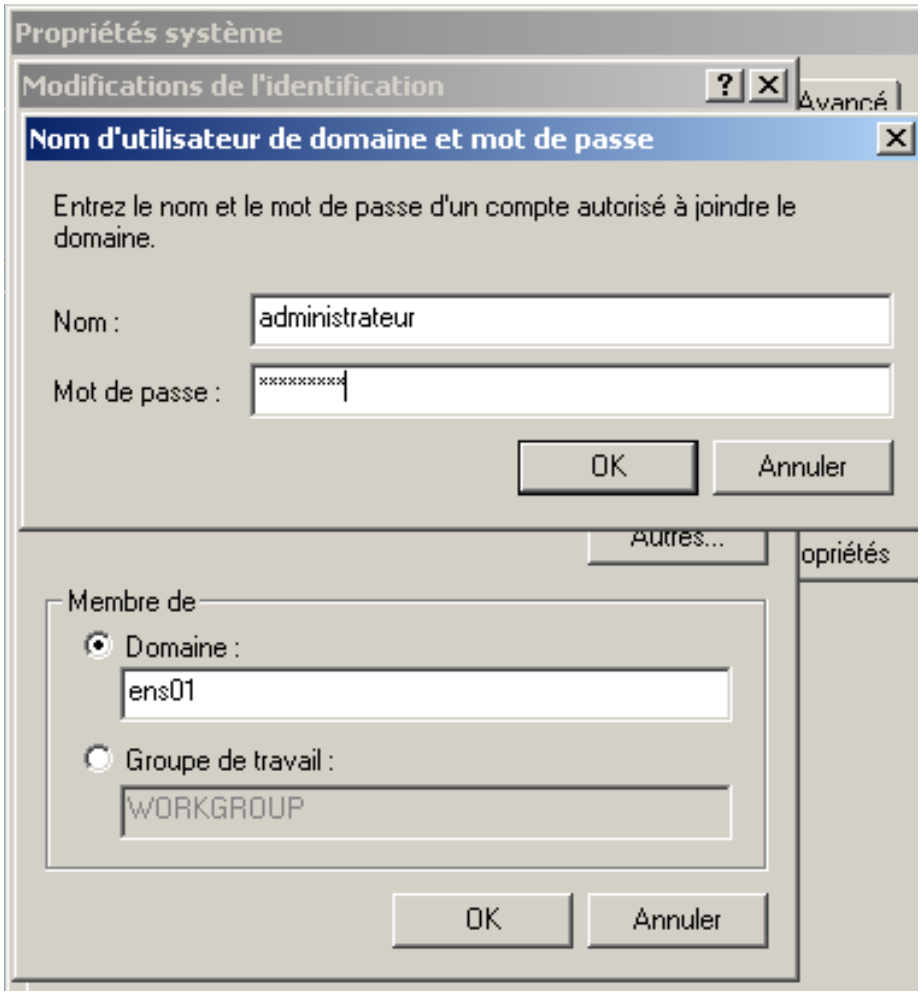
La hiérarchie Active Directory

- Ajout d'une station dans ens01.li350.local (3/9)



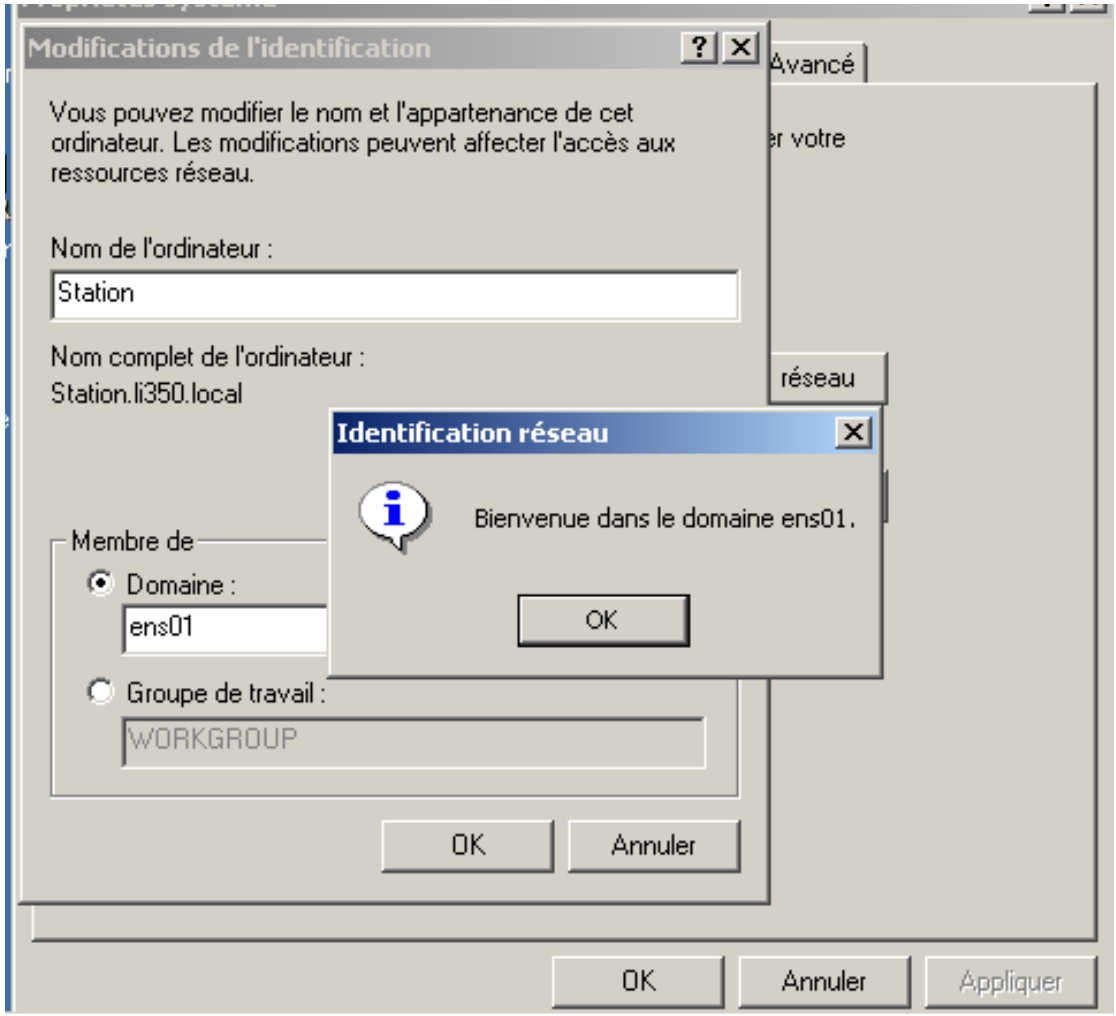
La hiérarchie Active Directory

- Ajout d'une station dans ens01.li350.local (4/9)



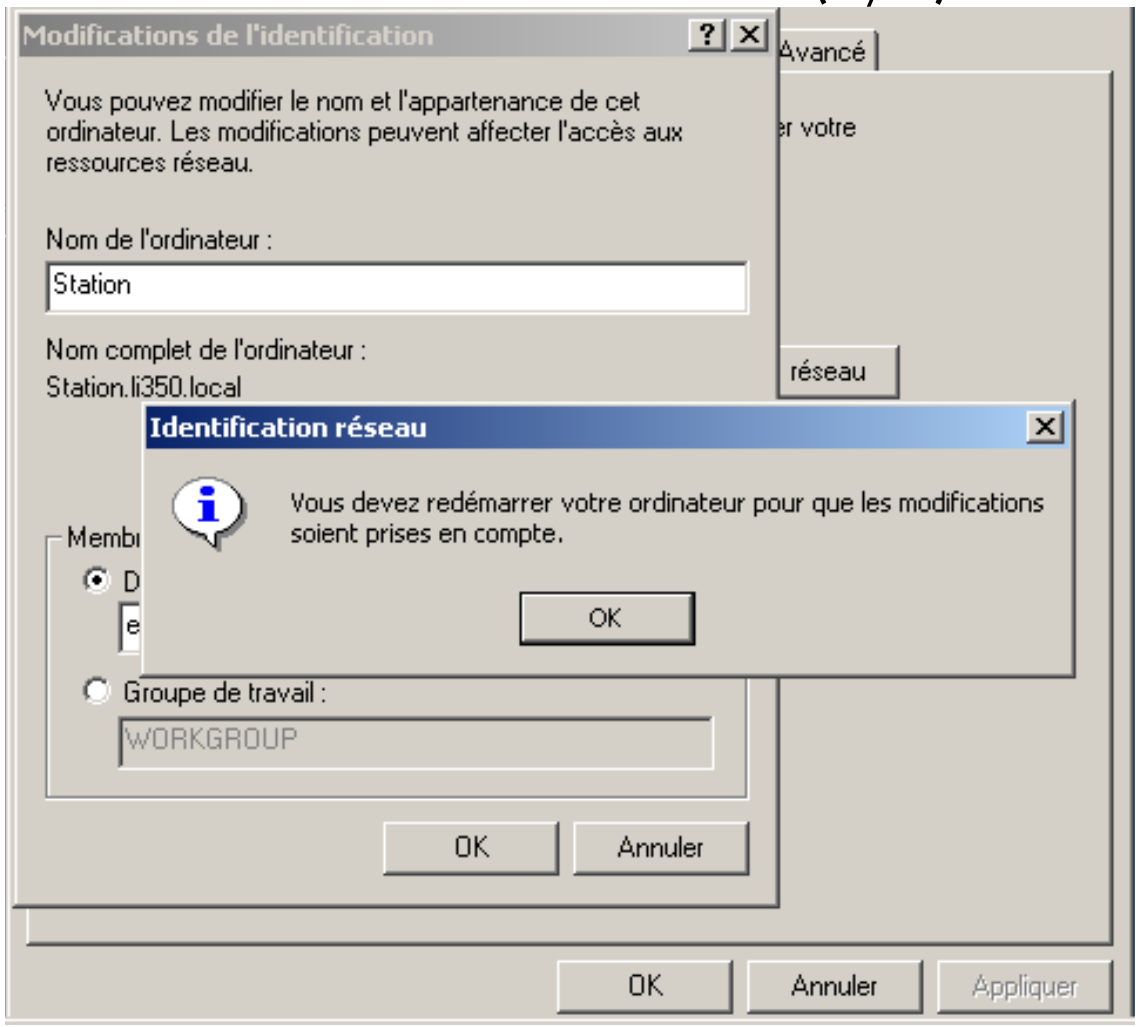
La hiérarchie Active Directory

- Ajout d'une station dans ens01.li350.local (5/9)



La hiérarchie Active Directory

- Ajout d'une station dans ens01.li350.local (6/9)



La hiérarchie Active Directory

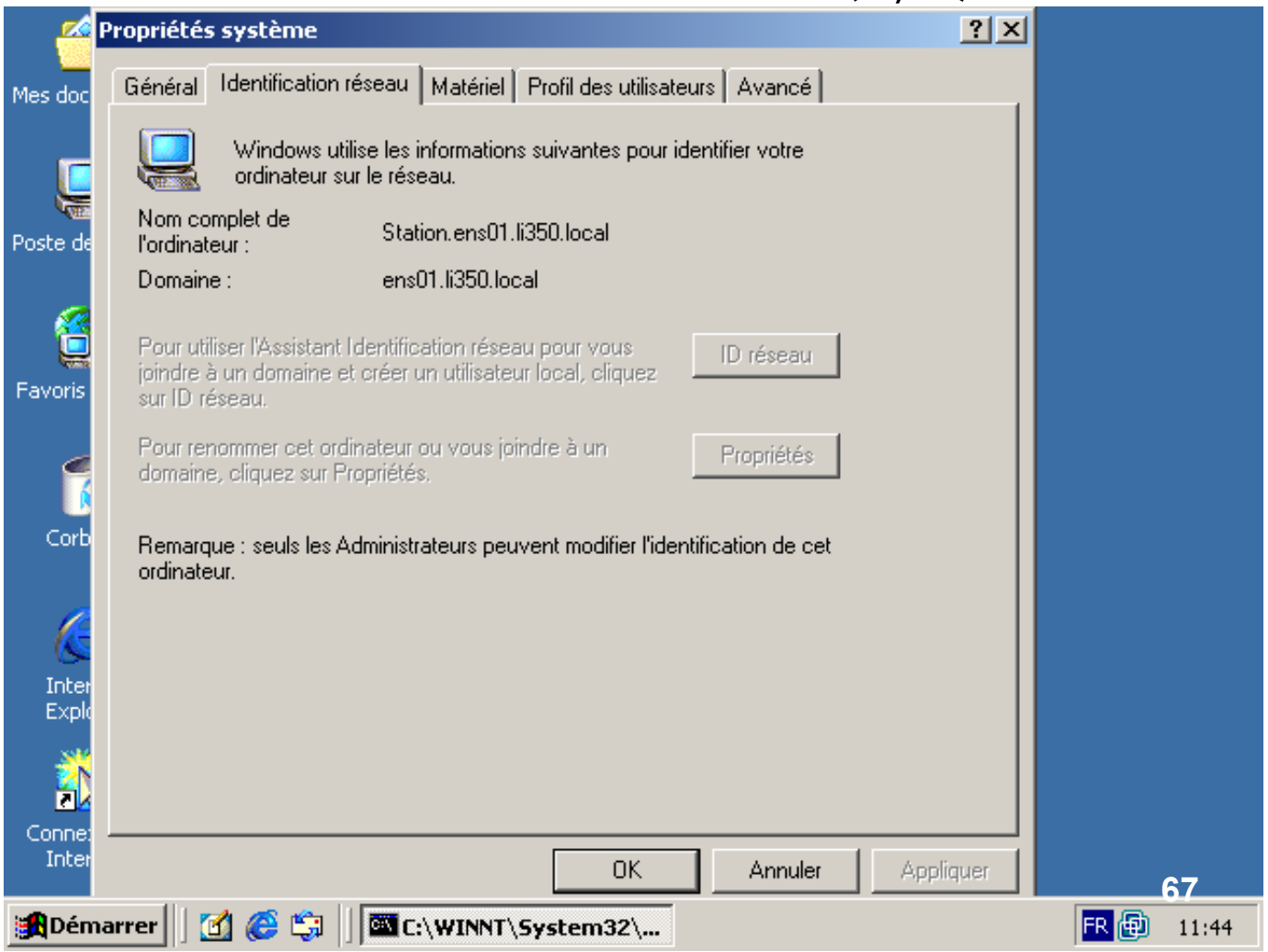
- Ajout d'une station dans ens01.li350.local (7/9)

La hiérarchie Active Directory

- Ajout d'une station dans ens01.li350.local (8/9)

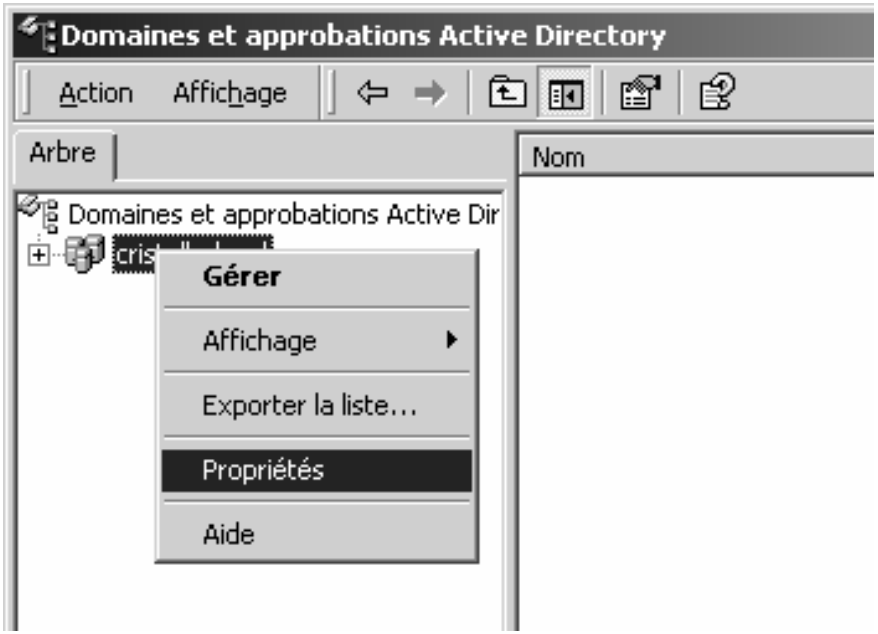
La hiérarchie Active Directory

- Ajout d'une station dans ens01.li350.local (9/9)

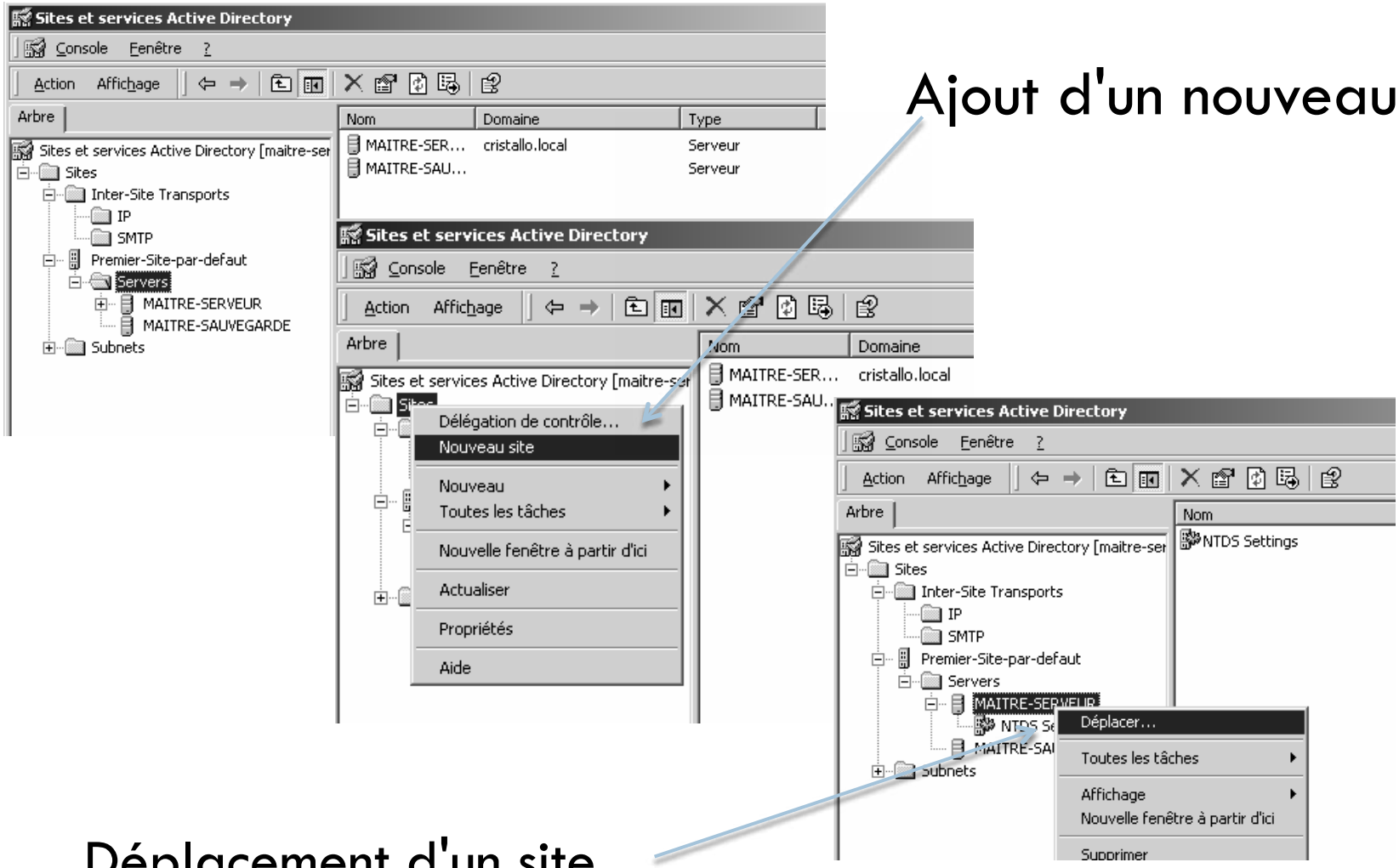


Approbation Active Directory : Outil

- Notion de mode
  - Natif (serveurs et stations uniquement Windows 2000 et ultérieurs)
    - La sécurité est maximale
  - Mixte (serveurs ou clients antérieurs à Windows 2000)
    - Les fonctionnalités de gestion des groupes sont réduites
    - *La sécurité correspond à celle d'un NT4*



Gestion des serveurs et services

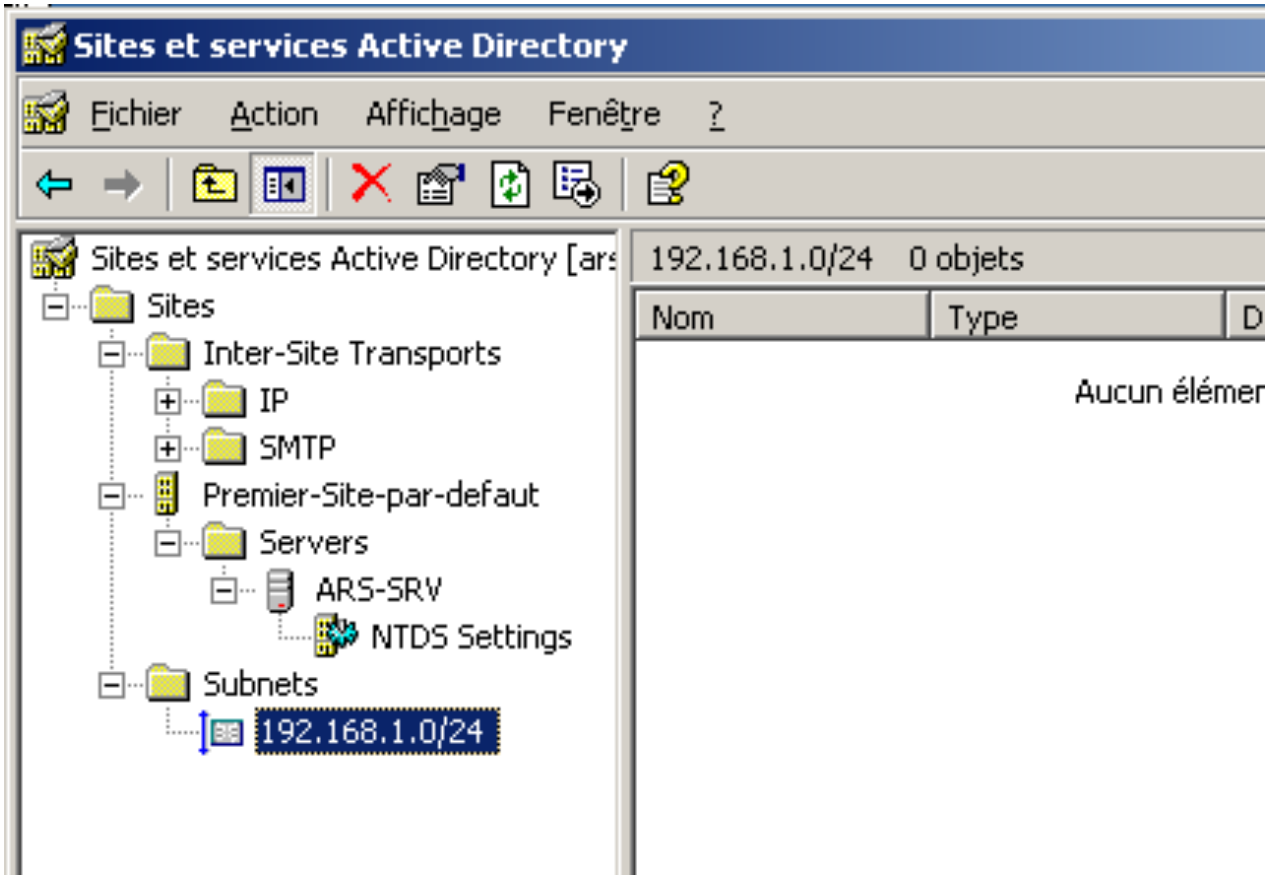


Ajout d'un nouveau site

Déplacement d'un site

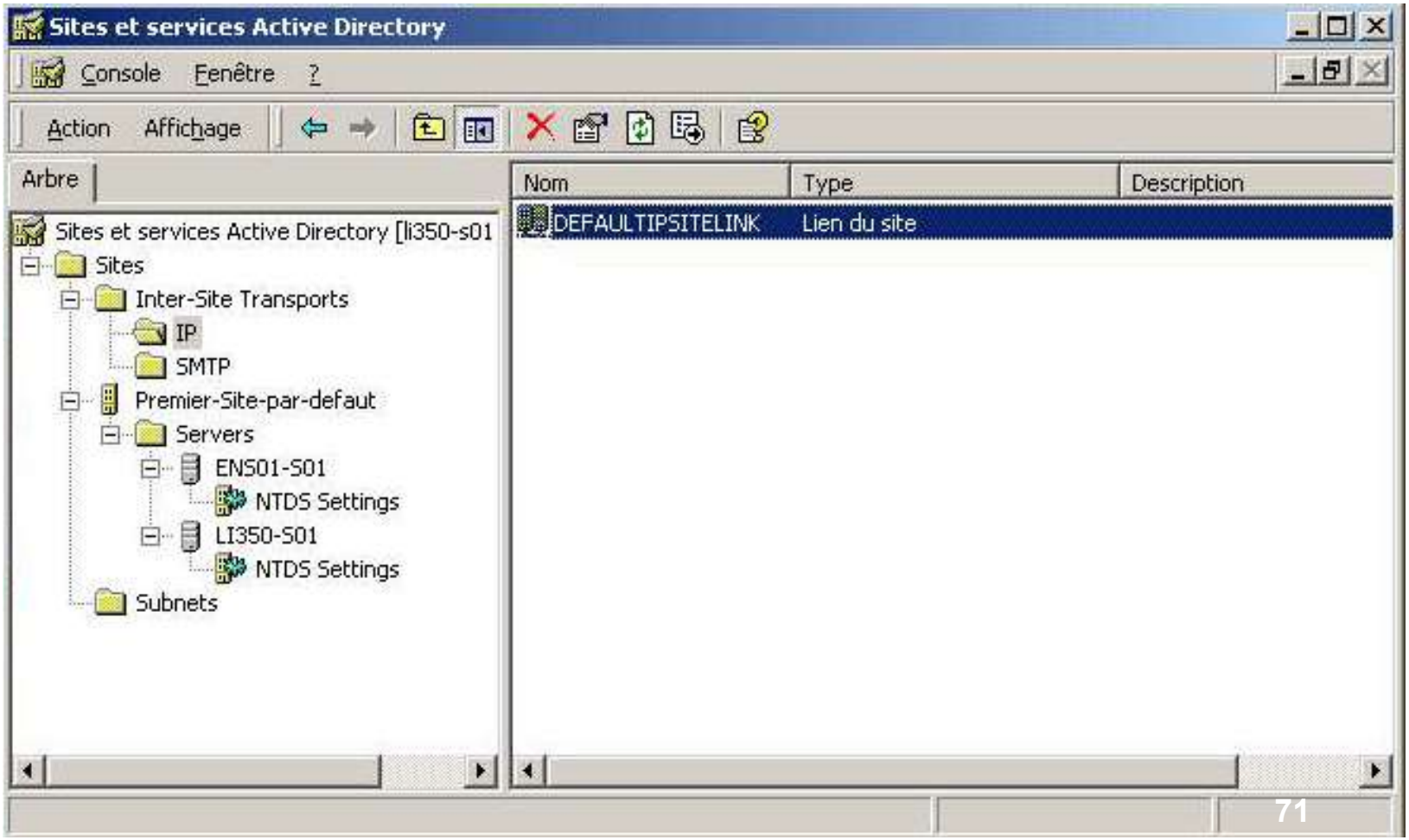
Gestion des serveurs et services

- Les ordinateurs sont affectés à un site en fonction de leur adresse IP



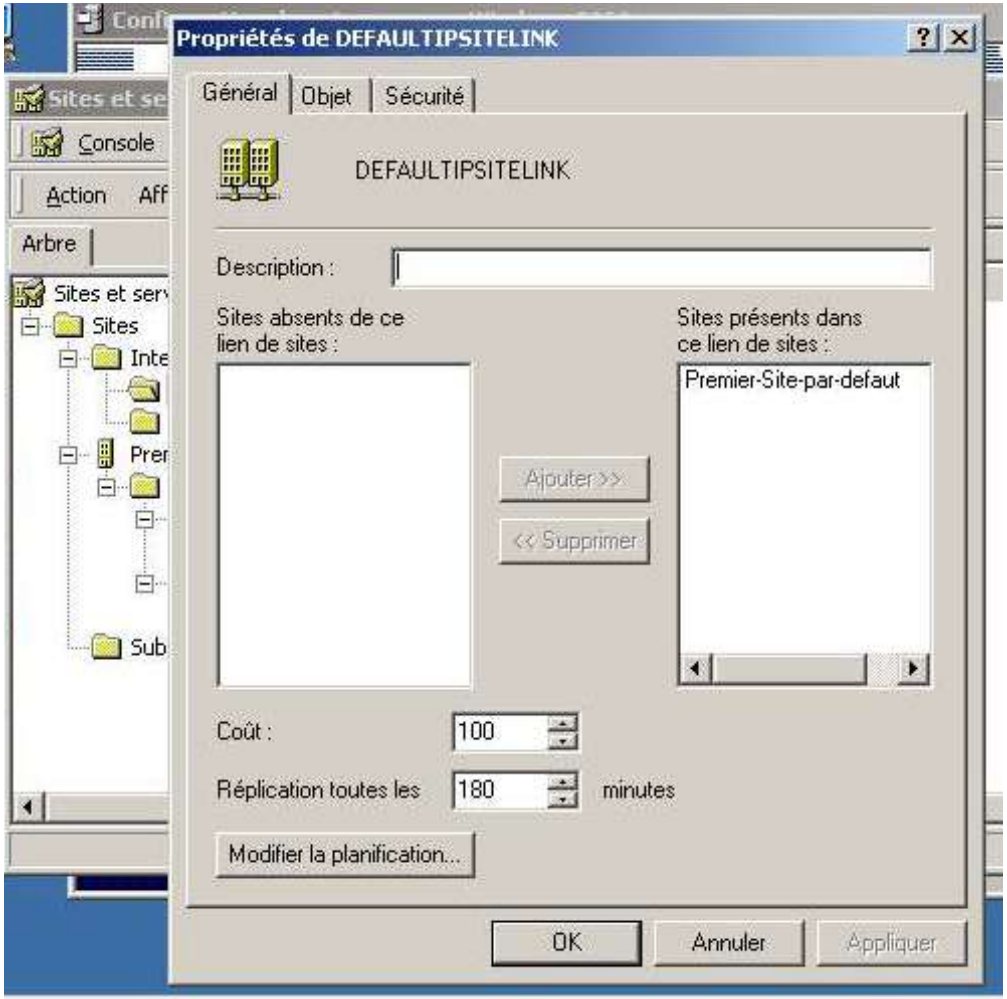
L'organisation physique du réseau dans Active Directory

- L'utilitaire Sites et Services Active Directory



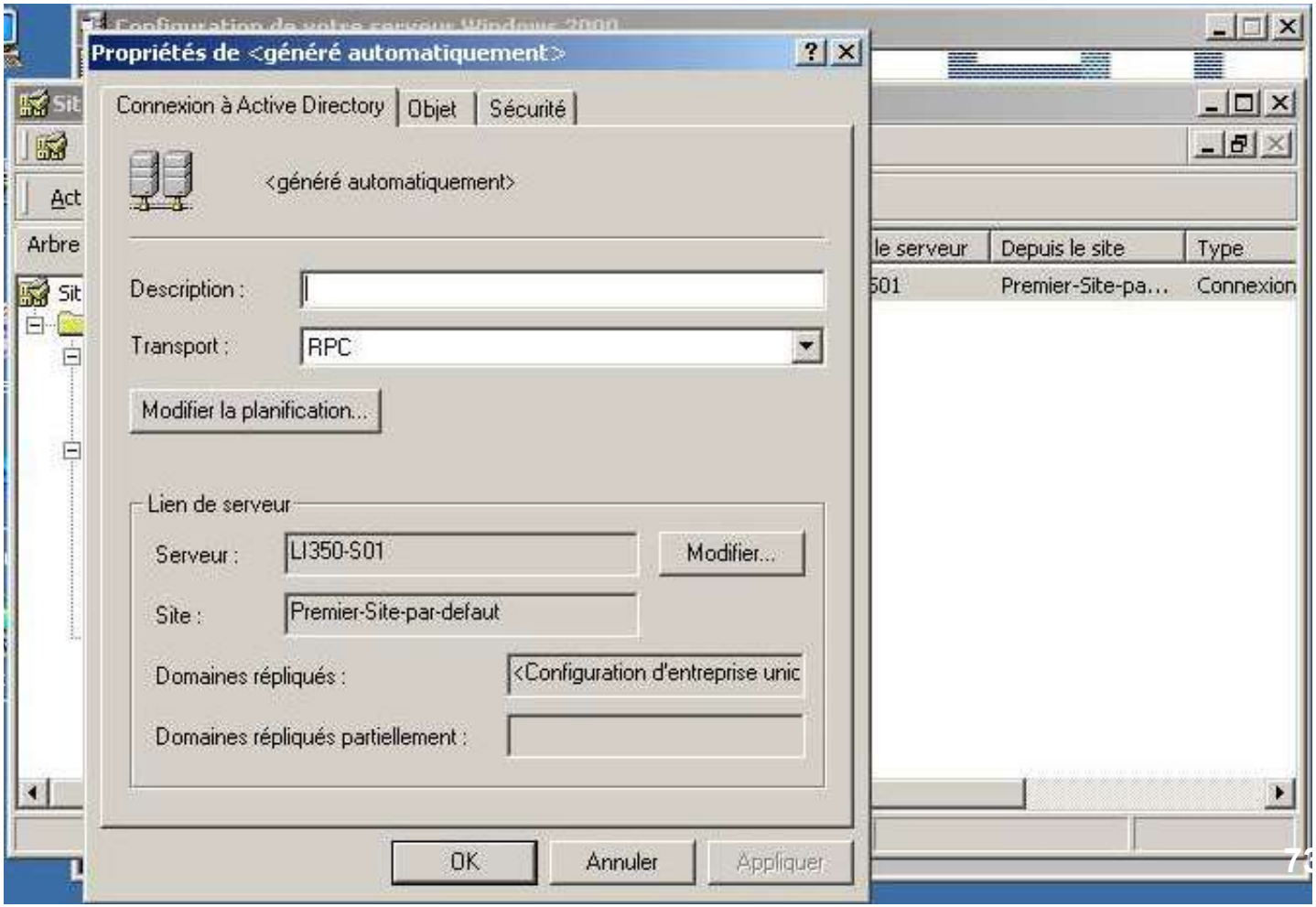
L'organisation physique du réseau dans Active Directory

- L'utilitaire Sites et Services Active Directory



L'organisation physique du réseau dans Active Directory

- L'utilitaire Sites et Services Active Directory



Base de comptes locale

- N'existe pas sur les contrôleurs de domaine
  - La base de compte locale est supprimée lors de l'ajout du rôle Active Directory
- Utilisable sur les serveurs et les stations de travail
- Ne permet qu'un accès aux ressources locales
- Les groupes locaux peuvent contenir des objets (utilisateurs et groupes) issus d'AD
- Administration par la console de gestion de l'ordinateur

Utilisateurs et groupes Active Directory

- Base de comptes dupliquée sur l'ensemble des contrôleurs AD
- Utilisable par toutes les ressources et services du domaine
- Administration par la console Utilisateurs et Ordinateurs Active Directory

Utilisateurs et groupes

- La ligne de commande pour la gestion des comptes sous Windows 2000
  - Net user
  - Net group
- Permet la gestion des comptes pour la machine locale et le domaine local
- Ne permet pas de gérer les comptes d'autres machines ou domaines

Utilisateurs et groupes

- La commande net user - **Exemples**
  - Afficher la liste de tous les comptes d'utilisateurs pour l'ordinateur local :
    - **net user**
  - Afficher des informations sur le compte d'utilisateur robertf :
    - **net user robertf**
  - Ajouter un compte d'utilisateur pour Suzanne Duprez et l'autoriser à ouvrir une session entre 08:00 et 17:00, du lundi au vendredi (pas d'espace dans la désignation des heures) avec le mot de passe obligatoire (suzanned) et le nom complet de l'utilisateur, tapez :
    - **net user suzanned /add /passwordreq:yes /times:lundi-vendredi, 8:00-17:00 /fullname:"Suzanne Duprez"**
  - Pour définir l'heure de connexion de johnsw (08:00 à 17:00) dans la plage 24 heures, tapez :
    - **net user johnsw /time:M-F,08:00-17:00**
  - Pour définir l'heure de connexion de johnsw (08:00 à 17:00) dans la plage 12 heures, tapez :
    - **net user johnsw /time:M-F,8am-5pm**
  - Pour autoriser marysl à se connecter entre 04:00 et 17:00 le lundi, entre 13:00 et 15:00 le mardi et entre 08:00 et 17:00 du mercredi au vendredi, tapez :
    - **net user marysl /time:L,4:00-17:00;Ma,13:00-15:00;Me-V,8:00-17:00**

Utilisateurs et groupes

- La commande net group - **Exemples**
  - Afficher la liste de tous les groupes figurant sur le serveur local :
    - **net group**
  - Ajouter le groupe Cadres à la base de données des comptes d'utilisateur locale :
    - **net group Cadres /add**
  - Ajouter le groupe Cadres à la base de données du domaine :
    - **net group Cadres /add /domain**
  - Ajouter les comptes d'utilisateur existants alainbo, fabriced et isabelb au groupe Cadres sur l'ordinateur local :
    - **net group Cadres alainbo fabriced isabelb /add**
  - Ajouter les comptes d'utilisateur existants alainbo, fabriced et isabelb au groupe Cadres dans la base de données du domaine :
    - **net group Cadres alainbo fabriced isabelb /add /domain**
  - Afficher les utilisateurs du groupe Cadres :
    - **net group Cadres**
  - Ajouter un commentaire à l'enregistrement du groupe Cadres :
    - **net group Cadres /comment:"La direction"**

Utilisateurs et groupes

- La ligne de commande sous Windows 2003 pour active directory
  - Dsadd Ajoute des objets à l'annuaire
  - Dsmod Modifie des attributs spécifiques d'un objet existant dans l'annuaire
  - Dsmove Déplace un objet vers un conteneur
  - Dsquery Recherche des objets dans l'annuaire correspondant à des critères de recherche spécifiés
  - Dsget Affiche les propriétés des objets dans l'annuaire
  - Dsrm Supprime un objet et/ou toute la sous-arborescence d'un objet dans l'annuaire
- Possibilité d'agir en local (par défaut) ou sur un domaine spécifié
- Permet d'agir sur tous les attributs AD

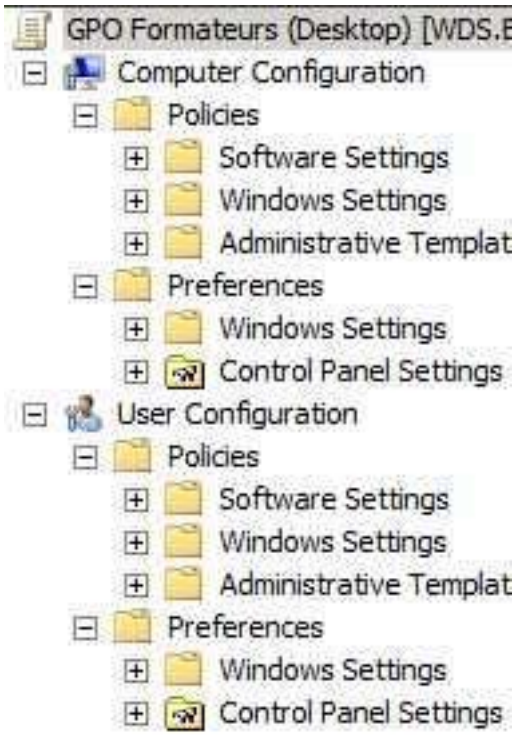
Utilisateurs et groupes

- La commande dsadd user :

Dsadd user *NUUtilisateur* [**-samid** *NomSAM*] [**-upn** *NPU*] [**-fn** *Prénom*] [**-mi** *Initiale*][**-ln** *Nom*][**-display** *NomAffiché*][**-empid** *IDEmployé*][**-pwd** {*Mot_de_passe* | *}][**-desc** *Description*] [**-memberof** *Groupe;…*][**-office** *Bureau*][**-tel** *NuméroTéléphone*][**-email** *CourrierElectronique*][**-fax** *NuméroTélécopie*][**-iptel** *NuméroTéléphoneIP*][**-webpg** *PageWeb*][**-title** *Titre*][**-dept** *Département*][**-company** *Société*][**-mgr** *Directeur*] [**-hmdir** *RépertoireBase*][**-hmdrv** *LettreLecteur:*][**-profile** *CheminProfil*][**-loscr** *CheminScript*][**-mustchpwd** {yes|no}][**-canchpwd** {yes|no}] …… ……[{**-s** *Serveur* | **-d** *Domaine*}]

Les stratégies de groupes

- Une stratégie de groupes est un objet Active Directory qui va contenir un ensemble de paramètres.



Les stratégies de groupes

- Ces paramètres vont permettre d'agir sur l'environnement d'un utilisateur ou d'un ordinateur en déployant une configuration qui ne sera pas modifiable
- Une stratégie de groupe peut aussi être appelée GPO (Group Policy Object)
- Cet objet de stratégie de groupe va ensuite être lié à un conteneur site, un domaine ou une unité d'organisation. Cela va permettre d'appliquer les paramètres de stratégie de groupe aux objets contenu dans ces conteneurs.

Les stratégies de groupes

- Applicables à différents conteneurs
  - Domaines
  - Sites
  - Unités Organisationnelles (UO)
  - A la machine locale
- Pour les utilisateurs et les ordinateurs

  (priorité aux stratégies définies sur les ordinateurs en cas de conflit)
- Héritables dans la hiérarchie des conteneurs AD

Les stratégies de groupes

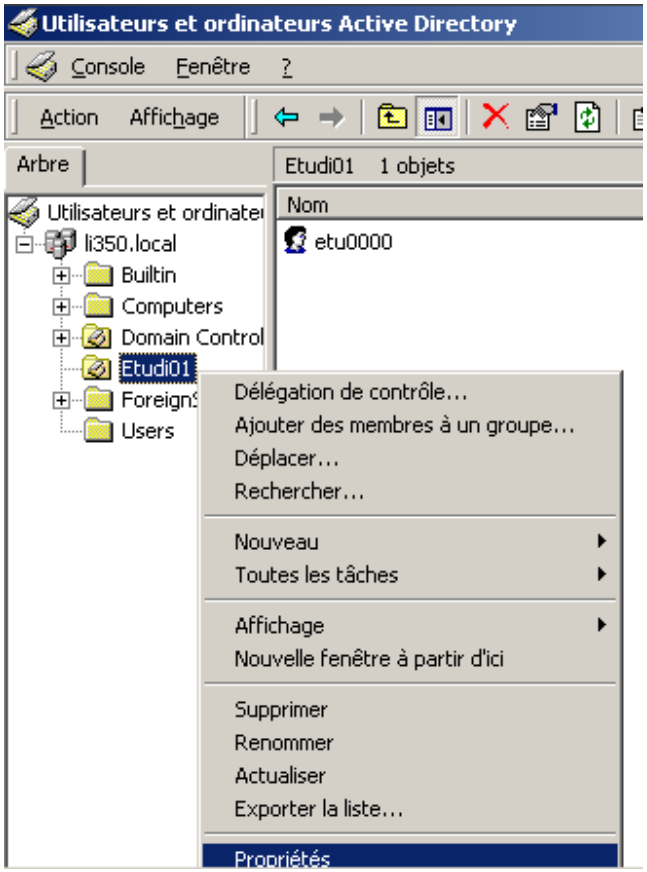
- Modèles d'administration
  - Accès au bureau
  - Barre des tâches
  - Panneau de configuration
  - Windows update
  - Planification
- Sécurité
  - Mots de passe
  - Audits de sécurité
- Installation automatique de logiciels

Les stratégies de groupes

- Scripts (en plus de celui associé au profil)
  - Ouverture/Fermeture de session
  - Démarrage/Arrêt de l'ordinateur local
- Service d'installation à distance
  - Uniquement avec les packages d'installation MSI
- Paramétrage de l'explorateur internet
- Redirection de dossiers
  - Mes documents
  - Bureau
  - …

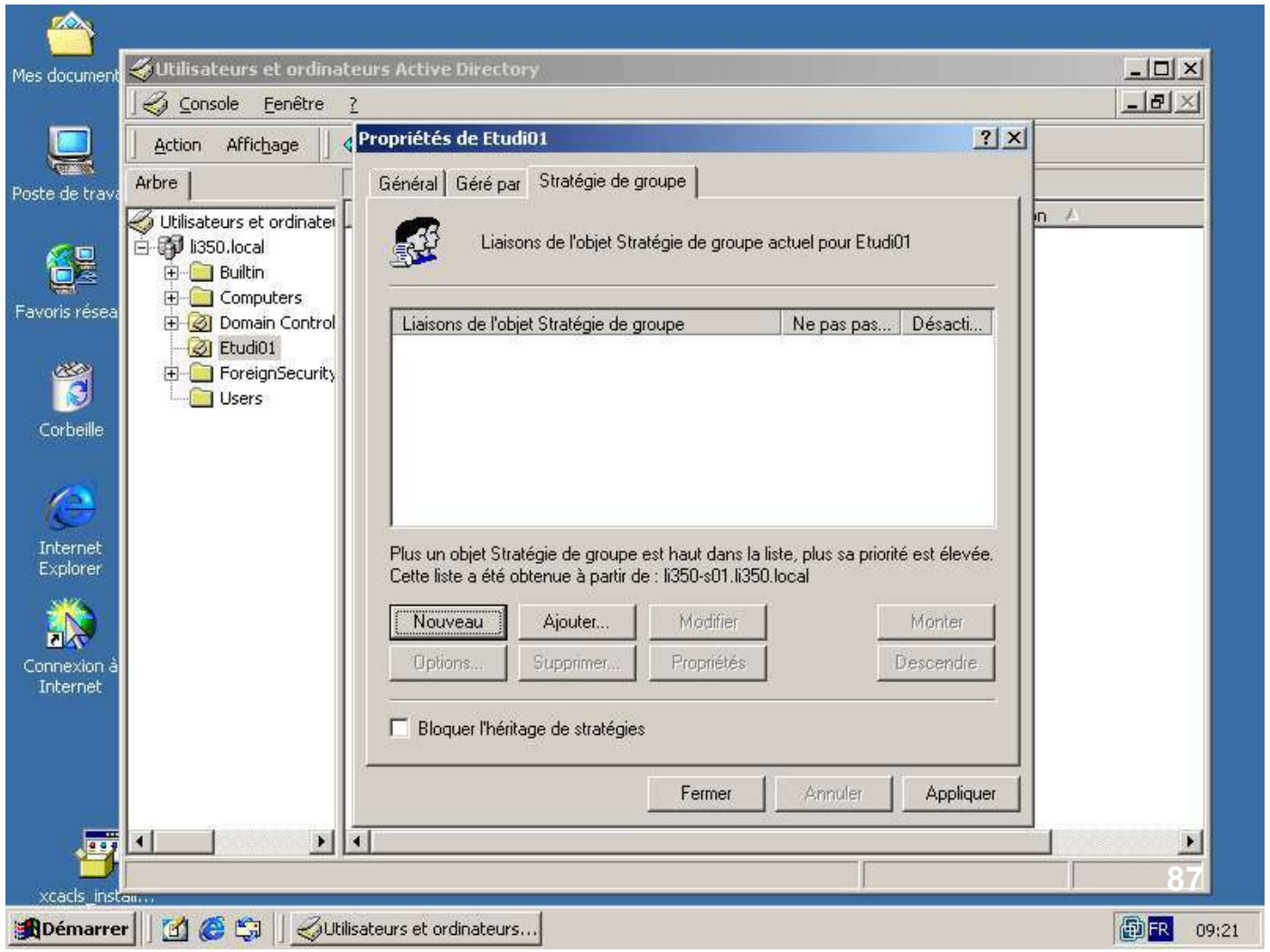
Les stratégies de groupes

- Mise en place d'une stratégie de groupe sur les objets d'une Unité Organisationnelle (UO)



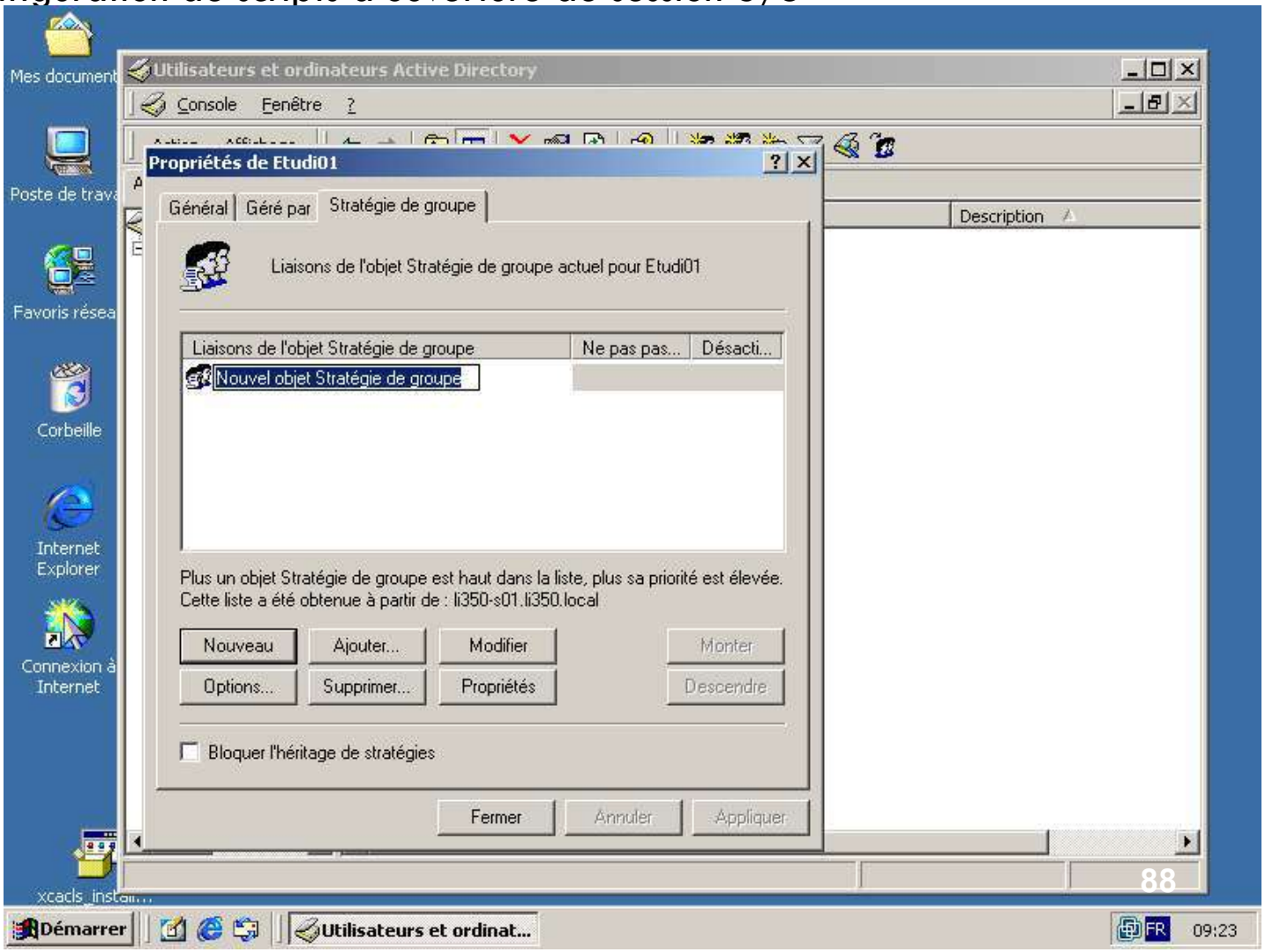
Les stratégies de groupes

- Configuration de scripts d'ouverture de session 2/5



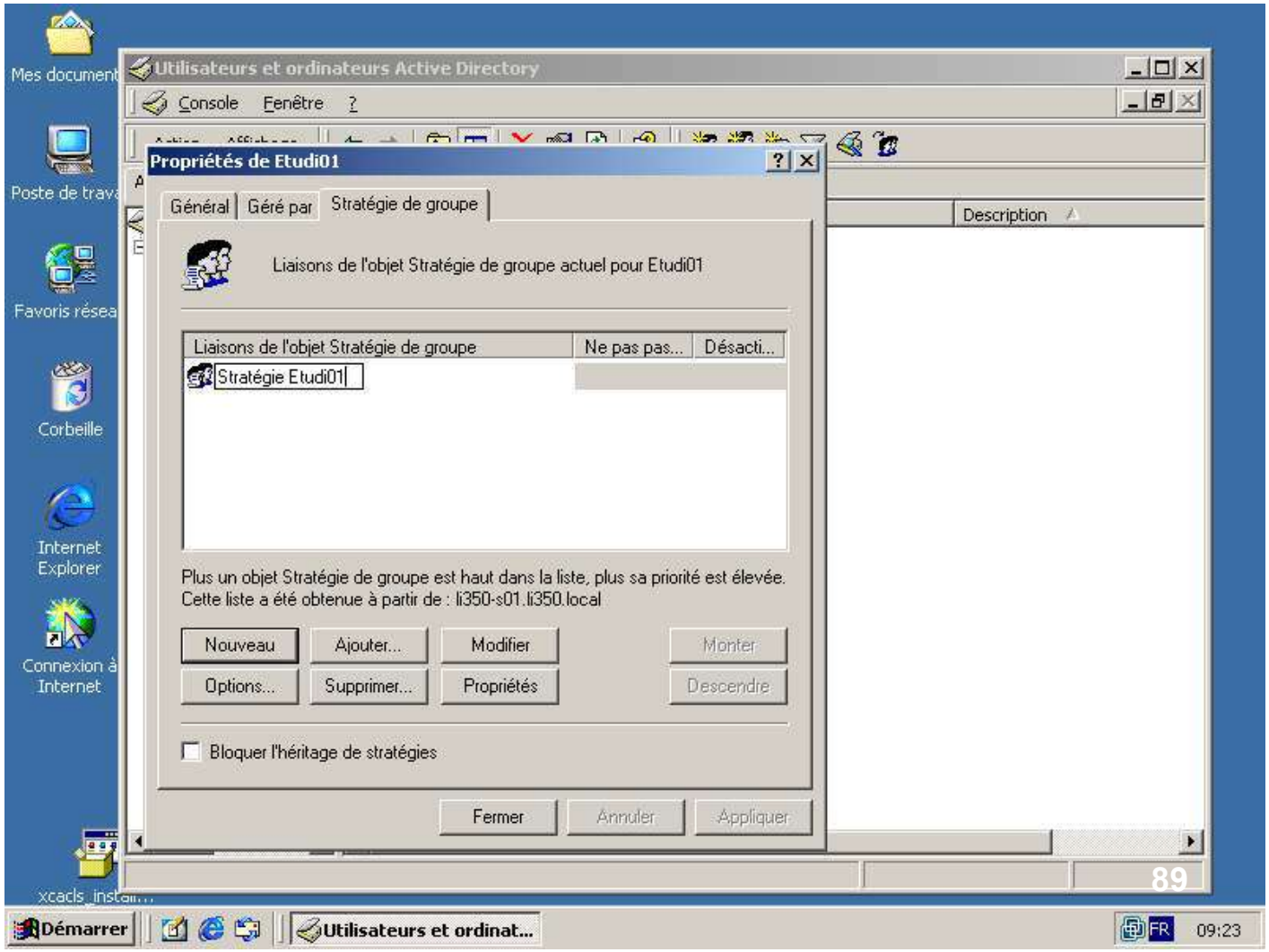
Les stratégies de groupes

- Configuration de scripts d'ouverture de session 3/5



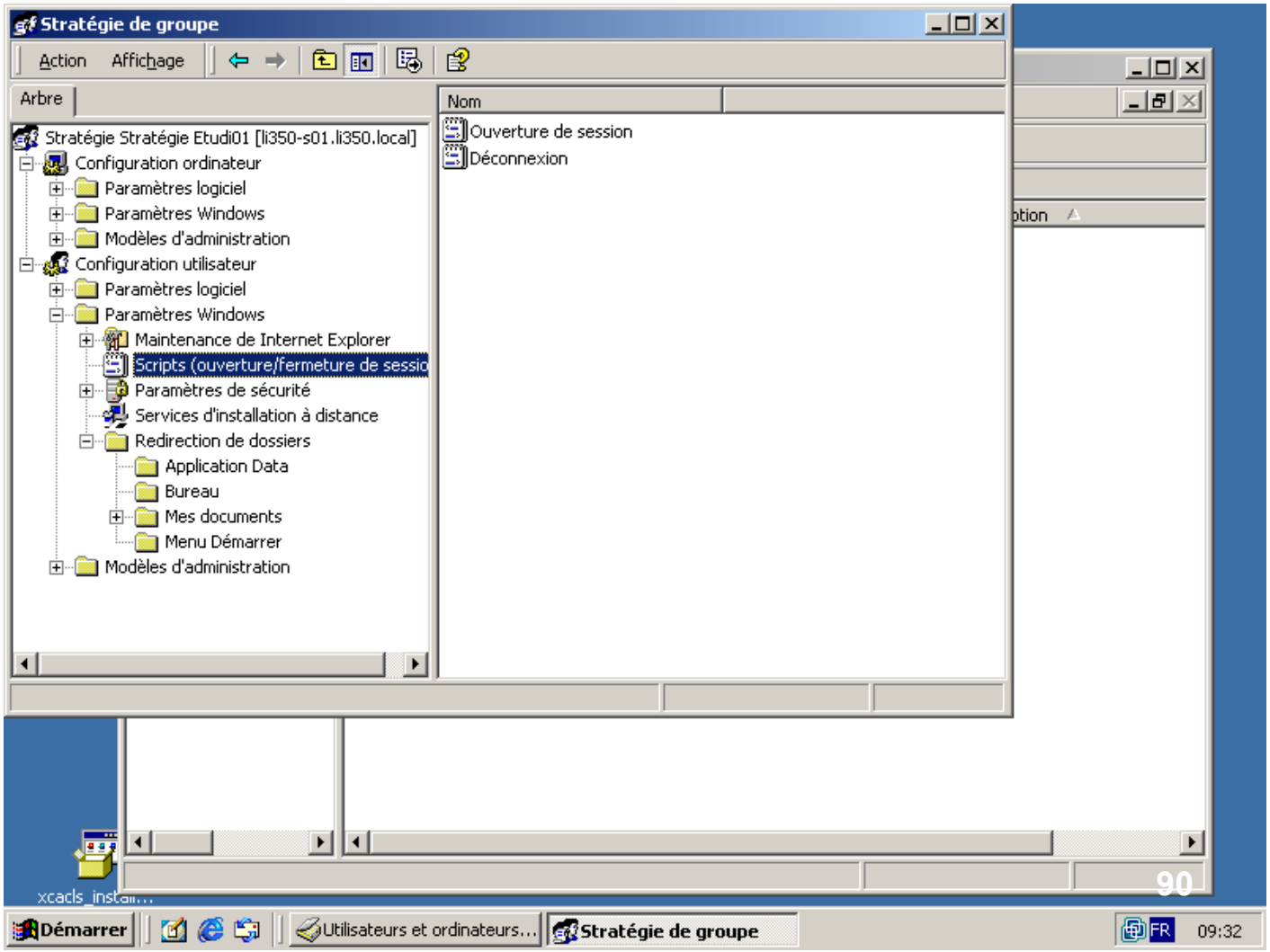
Les stratégies de groupes

- Configuration de scripts d'ouverture de session 4/5



Les stratégies de groupes

- Configuration de scripts d'ouverture de session 5/5



Autres paramètres de stratégie

- Il y en a plus de 500…
- Attention aux héritages de stratégie entre Unités d'Organisation
  - Une stratégie de haut niveau peut empêcher l'application d'une autre stratégie.
- Voir les stratégies comme un arbre ou chaque nœud (modification de stratégie) comporte 500 paramètres!
- Faire simple…

- Scripts
  - Démarrage
  - Arrêt
- Stratégie de comptes
  - Stratégie de mot de passe
    - Conserver l'historique des mots de passe
    - Durée de vie maximale du mot de passe
    - Durée de vie minimale du mot de passe
    - Les mots de passe doivent respecter des exigences de complexité
    - Longueur minimale du mot de passe
    - Stocker le mot de passe en utilisant le cryptage réversible pour tous les utilisateurs du domaine
  - Stratégie de verrouillage du compte
    - Durée de verrouillage des comptes
    - Délai de réinitialisation du compteur de verrouillages du compte
    - Seuil de verrouillage du compte

Stratégie locales

Stratégie d'audit

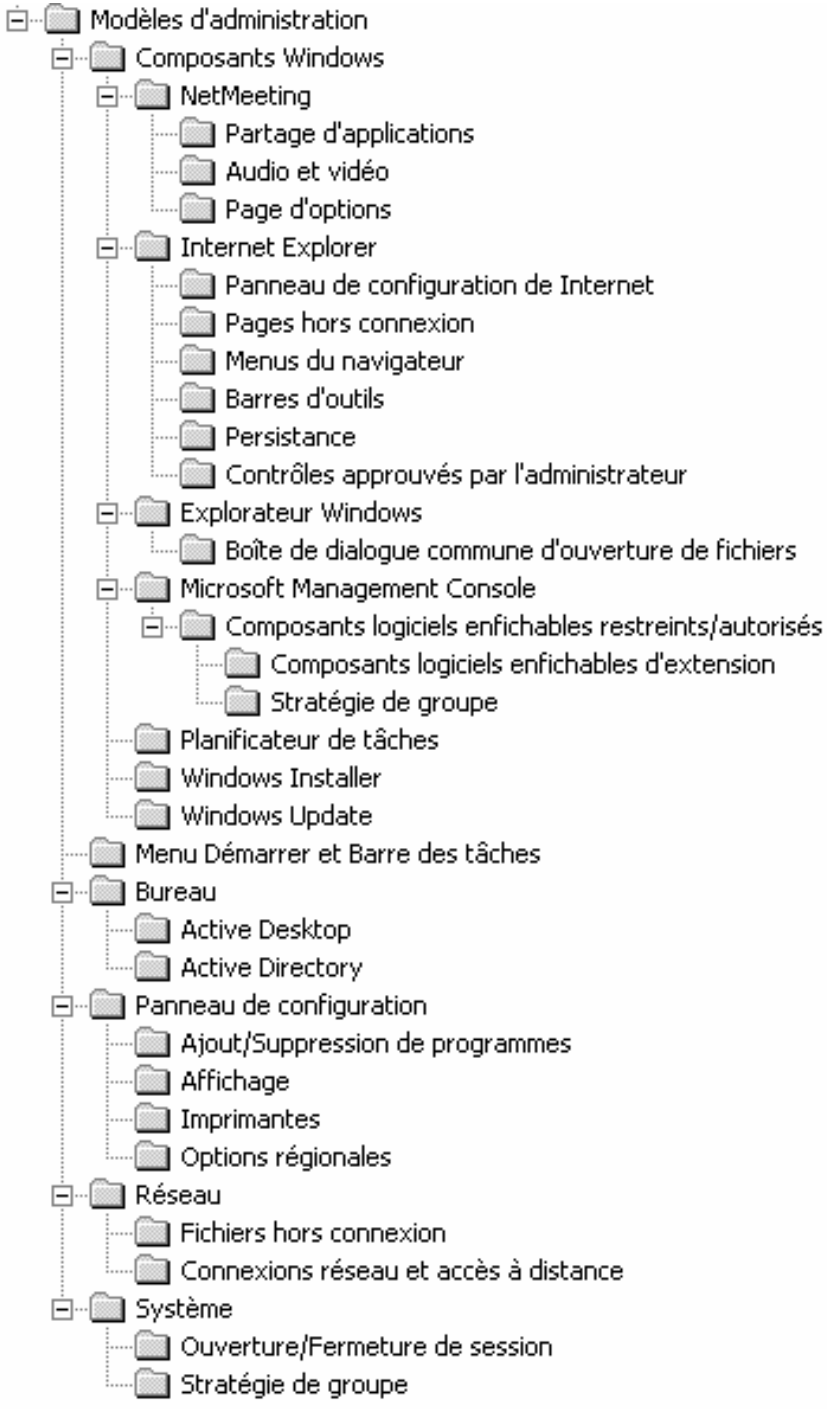
- Auditer la gestion des comptes
- Auditer l'accès au service d'annuaire
- Auditer l'accès aux objets
- Auditer le suivi des processus
- Auditer les événements de connexion
- Auditer les événements de connexion aux comptes
- Auditer les événements système
- Auditer les modifications de stratégie
- Auditer l'utilisation des privilèges

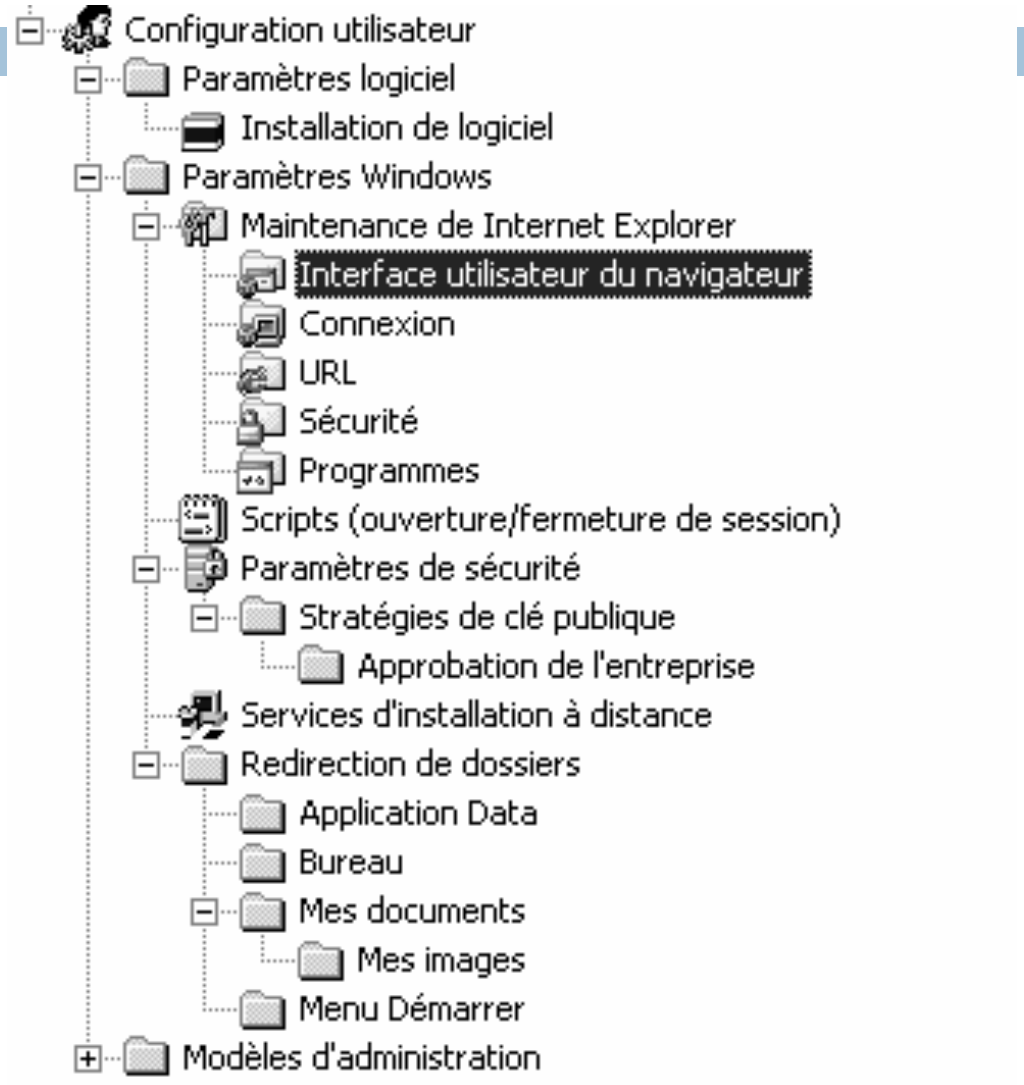
Attribution des droits utilisateur

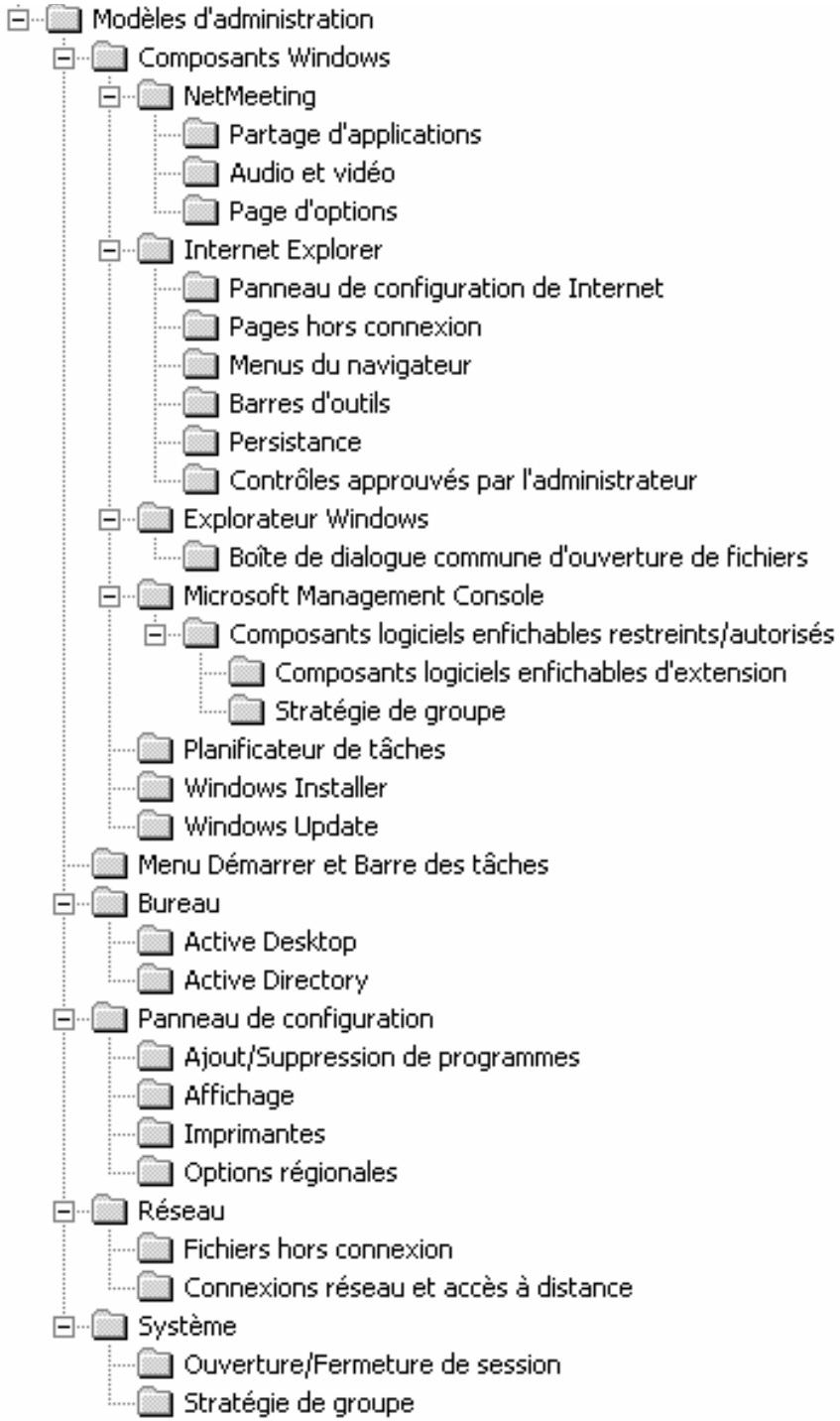
- Accéder à cet ordinateur depuis le réseau
- Agir en tant que partie du système d'exploitation
- Ajouter des stations de travail au domaine
- Arrêter le système
- Augmenter la priorité de planification
- Augmenter les quotas
- Autoriser que l'on fasse confiance aux comptes ordinateur et utilisateur pour la délégation
- Charger et décharger des pilotes de périphériques
- Créer des objets globaux
- Créer des objets partagés permanents
- Créer un fichier d'échange
- Créer un objet-jeton
- Déboguer des programmes
- Emprunter l'identité d'un client après l'authentification
- Forcer l'arrêt à partir d'un système distant
- Générer des audits de sécurité
- Gérer le journal d'audit et de sécurité

- Attribution des droits utilisateur (suite)
  - Modifier les valeurs d'environnement de microprogrammation
  - Modifier l'heure système
  - Optimiser les performances système
  - Optimiser un processus unique
  - Outrepasser le contrôle de défilement
  - Ouvrir une session en tant que service
  - Ouvrir une session en tant que tâche
  - Ouvrir une session localement
  - Prendre possession des fichiers ou d'autres objets
  - Refuser l'accès à cet ordinateur à partir du réseau
  - Refuser les ouvertures de session locales
  - Refuser l'ouverture de session en tant que service
  - Refuser l'ouverture de session en tant que tâche
  - Remplacer un jeton niveau de processus
  - Restaurer des fichiers et des répertoires
  - Retirer l'ordinateur de la station d'accueil
  - Sauvegarder des fichiers et des répertoires
  - Synchroniser les données de l'annuaire Active Directory
  - Verrouiller des pages en mémoire


Configuration ordinateur
Paramètres logiciel
Installation de logiciel
Paramètres Windows
Scripts (démarrage/arrêt)
Paramètres de sécurité
Stratégies de comptes
Stratégie de mot de passe
Stratégie de verrouillage du compte
Stratégies locales
Stratégie d'audit
Attribution des droits utilisateur
Options de sécurité
Journal des événements
Paramètres du journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de clé publique
Agents de récupération de données cryptées
Paramètres de demande automatique de certificat
Autorités de certification racines de confiance
Approbation de l'entreprise
Stratégies de sécurité IP sur Active Directory
Modèles d'administration


Modèles d'administration
Composants Windows
NetMeeting
Partage d'applications
Audio et vidéo
Page d'options
Internet Explorer
Panneau de configuration de Internet
Pages hors connexion
Menus du navigateur
Barres d'outils
Persistance
Contrôles approuvés par l'administrateur
Explorateur Windows
Boîte de dialogue commune d'ouverture de fichiers
Microsoft Management Console
Composants logiciels enfichables restreints/autorisés
Composants logiciels enfichables d'extension
Stratégie de groupe
Planificateur de tâches
Windows Installer
Windows Update
Menu Démarrer et Barre des tâches
Bureau
Active Desktop
Active Directory
Panneau de configuration
Ajout/Suppression de programmes
Affichage
Imprimantes
Options régionales
Réseau
Fichiers hors connexion
Connexions réseau et accès à distance
Système
Ouverture/Fermeture de session
Stratégie de groupe


Configuration utilisateur
Paramètres logiciel
Installation de logiciel
Paramètres Windows
Maintenance de Internet Explorer
Interface utilisateur du navigateur
Connexion
URL
Sécurité
Programmes
Scripts (ouverture/fermeture de session)
Paramètres de sécurité
Stratégies de clé publique
Approbation de l'entreprise
Services d'installation à distance
Redirection de dossiers
Application Data
Bureau
Mes documents
Mes images
Menu Démarrer
Modèles d'administration


Modèles d'administration
Composants Windows
NetMeeting
Partage d'applications
Audio et vidéo
Page d'options
Internet Explorer
Panneau de configuration de Internet
Pages hors connexion
Menus du navigateur
Barres d'outils
Persistance
Contrôles approuvés par l'administrateur
Explorateur Windows
Boîte de dialogue commune d'ouverture de fichiers
Microsoft Management Console
Composants logiciels enfichables restreints/autorisés
Composants logiciels enfichables d'extension
Stratégie de groupe
Planificateur de tâches
Windows Installer
Windows Update
Menu Démarrer et Barre des tâches
Bureau
Active Desktop
Active Directory
Panneau de configuration
Ajout/Suppression de programmes
Affichage
Imprimantes
Options régionales
Réseau
Fichiers hors connexion
Connexions réseau et accès à distance
Système
Ouverture/Fermeture de session
Stratégie de groupe

Performances de Active Directory

- La vitesse d'ouverture d'une session utilisateur est proportionnelle au nombre de groupes de sécurité auxquels il appartient
- Attention aux très gros sites!
  (500 dossiers partagés accessibles = 500 Jetons)
- Performances surtout liées au réseau

Au cœur de AD

- Journalisation (résiste aux coupures secteurs)
- La base de données reste toujours à jour
- La base de données de Active Directory est stockée dans c:\winnt\ntds\Ntds.dit
- Les journaux sont dans les .log (format propriétaire)
- Principe de la journalisation
  - Ecriture du fichier log
  - Ecriture en mémoire
  - Confirmation de la transaction
  - Ecriture de Ntds.dit