Réseaux
Active Directory

Sommaire

- L'installation de Windows 2003 Serveur débute par l'installation du système d'exploitation lui-même ;
- Une fois le système installé, on peut procéder à l'installation du ou des services (DNS, DHCP, AD, …) ;
- Ces services peuvent être soit déjà présent au sein du système soit nécessiteront une installation de composants supplémentaire ;
- Après l'installation vient la configuration ;

- La configuration d'une machine en contrôleur de domaine est un exemple typique de ce genre de service.
- Elle requière l'installation de Active Directory et du service DNS si celui-ci n'est pas déjà implanté par ailleurs.

- Active Directory Service (ADS) est supporté par Windows 2003 Server et à pour but la gestion d'annuaires ;

- Il est utilisé pour toutes les tâches d'administration demandant une forte composante réseau, en particulier pour la création de domaines ;

- ADS n'est pas installé par défaut sous Windows 2003 ;

- Au cours de son installation, un domaine doit être défini.

- Contrôleur de domaine ;
- Contrôleur de domaine supplémentaire ;
- Domaine ;
- Domaine enfant ;
- Arborescence de domaine ;
- Forêt.

Dans une forêt Active Directory, un **contrôleur de domaine** est un serveur contenant une copie **inscriptible** de la base de données Active Directory et contrôlant l'accès aux ressources réseau.

Les administrateurs peuvent gérer les comptes d'utilisateurs, l'accès réseau, les ressources partagées et les autres objets d'annuaire à partir de n'importe quel contrôleur de domaine de la forêt.

Il s'agit d'un contrôleur de domaine qui reçoit une **copie en lecture seule** de la base de données de l'annuaire pour le domaine.

Cette dernière contient toutes les informations sur les comptes et les stratégies de sécurité du domaine.

Définition des notions employées: Domaine

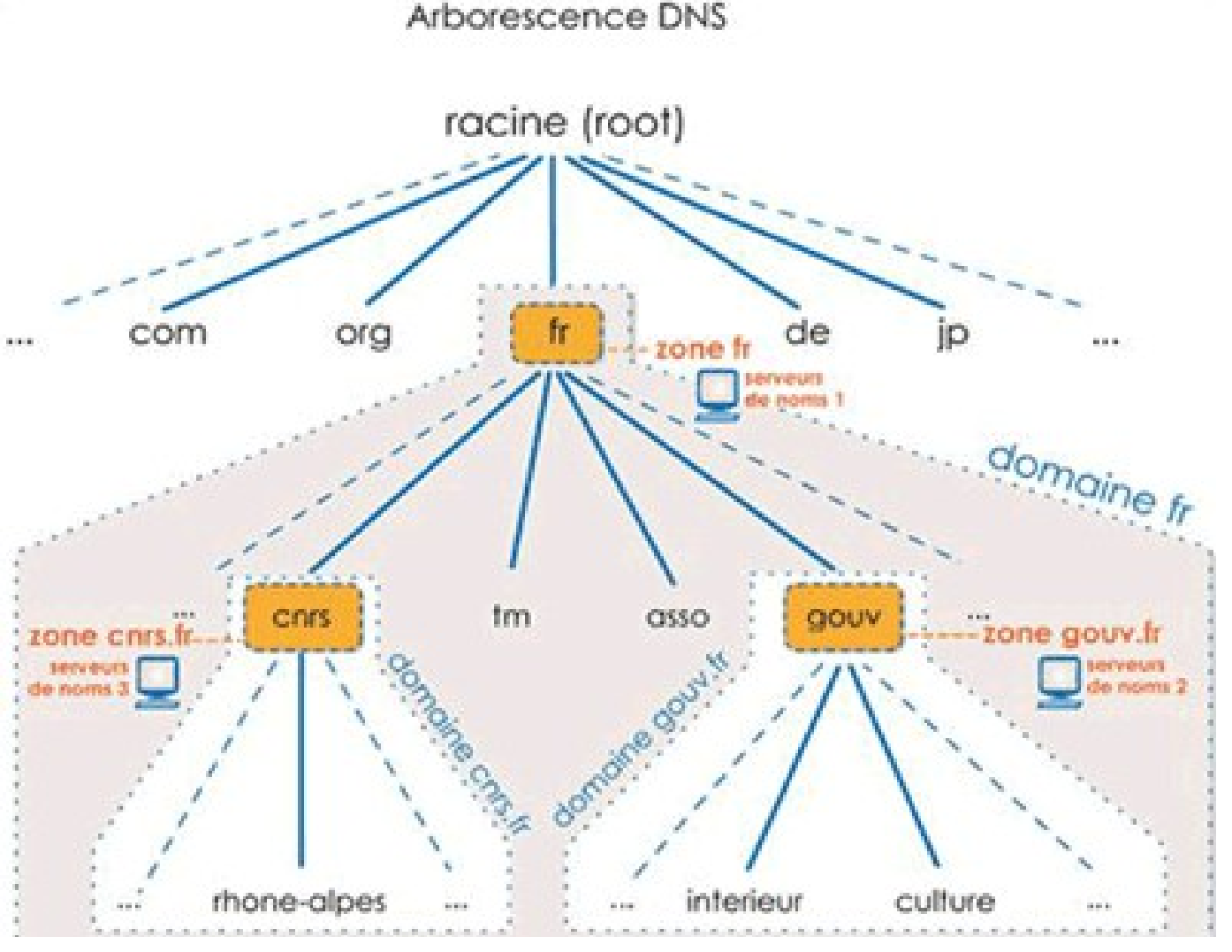
Dans Active Directory,un domaine est l’ensemble d'objets ordinateur, utilisateur et groupe défini par l'administrateur.
Ces objets partagent une base de données d'annuaire, des stratégies de sécurité et des relations de sécurité communes avec d'autres domaines.

Du point de vue du DNS, un domaine est toute arborescence ou sous-arborescence au sein d'un espace de nom.

Pour DNS et Active Directory, un domaine enfant est un domaine de l'arborescence de l'espace de noms situé immédiatement sous un autre nom de domaine (le domaine parent).

On parle aussi de sous-domaine

Dans DNS, l'arborescence de domaine est la structure de l'arborescence hiérarchique inversée qui est utilisée pour indéxer les noms de domaines.

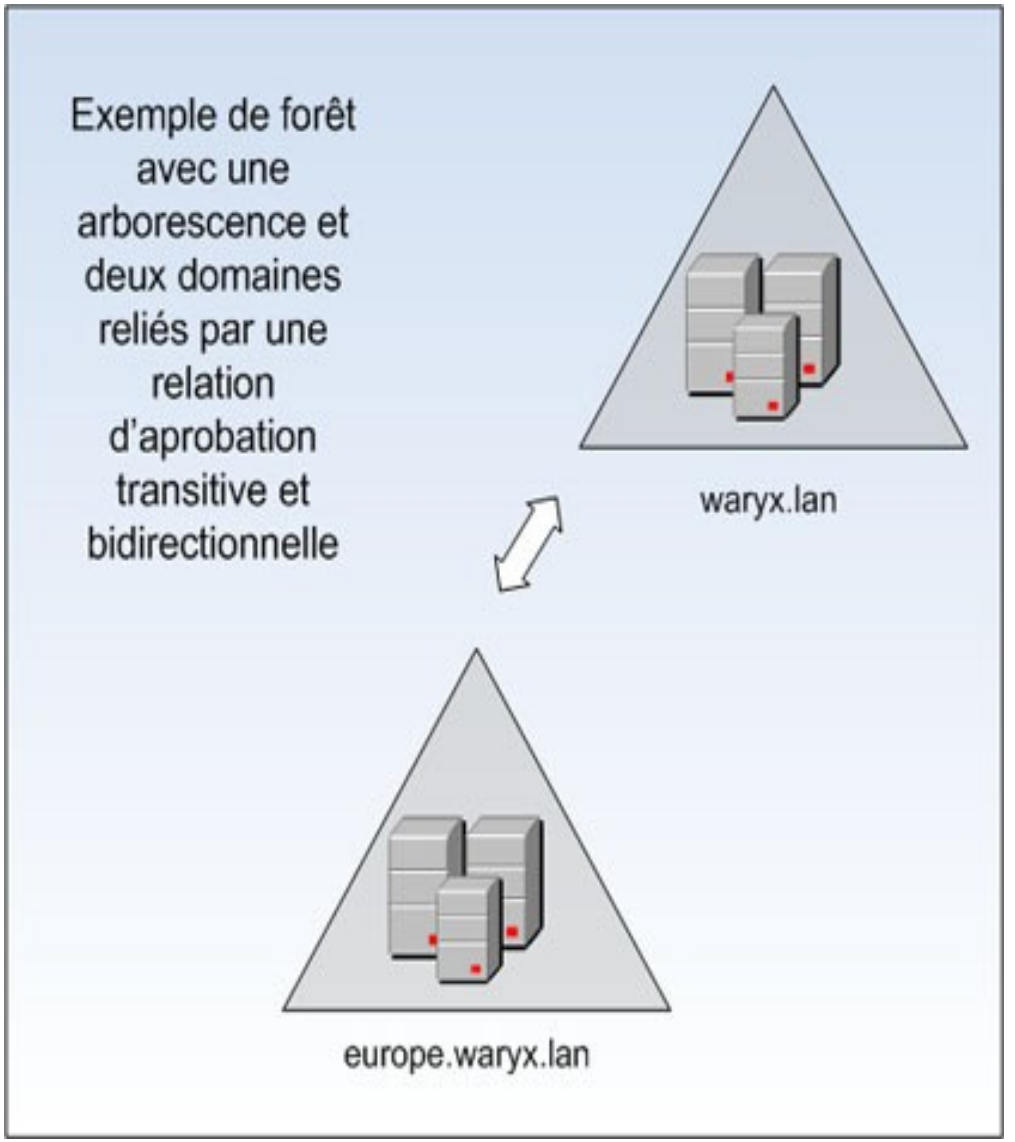


Dans Active Directory, l'arborescence de domaine correspond à la structure hiérarchique d'un ou plusieurs domaines liées par des relations d'approbations **bidirectionnelles et transitives** formants un **espace de nom contigu**.

Définition des notions employées: Forêt

Une fôret correspond à un ou plusieur domaines Active Directory partagant les mêmes définitions de schéma, les mêmes informations relatives à la configuration, et les mêmes fonctionnalités de recherche dans le catalogue global.

Les domaines d'une même fôret sont liés par des relations bidirectionnelles et transitives.



Deux méthodes sont disponibles pour installer Active Directory :

- Utiliser l'utilitaire "Gérer votre serveur"
  - Accessible dans Démarrer → Tous les programmes → Outils d'administration → Gérer votre serveur ;
  - Cet utilitaire simplifie l'installation sans poser les questions les plus pointues.
  - Il installe et configure AD, DNS et DHCP pour un nouveau domaine dans une nouvelle forêt..

- Utiliser l'assistant "dcpromo", lancé en ligne de commande, qui permet de contrôler tous les aspects de l'installation.

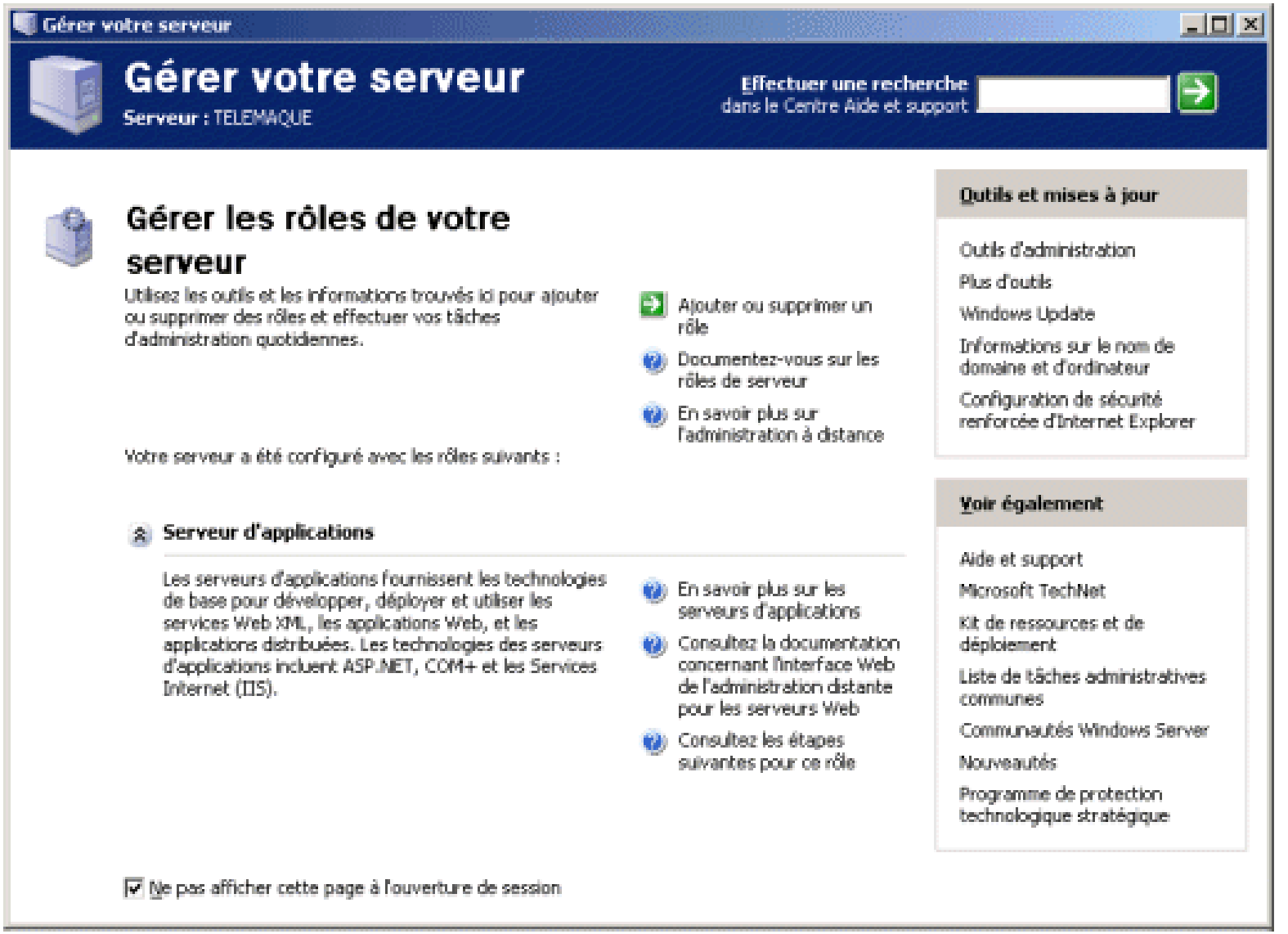
La machine d'installation pourra prendre différents rôles:

- premier contrôleur d'un nouveau domaine dans une nouvelle forêt ;
- premier contrôleur d'un domaine enfant (nécessite un domaine parent) ;
- premier contrôleur d'un nouveau domaine dans une forêt existante ;
- contrôleur supplémentaire au sein d'un domaine existant.

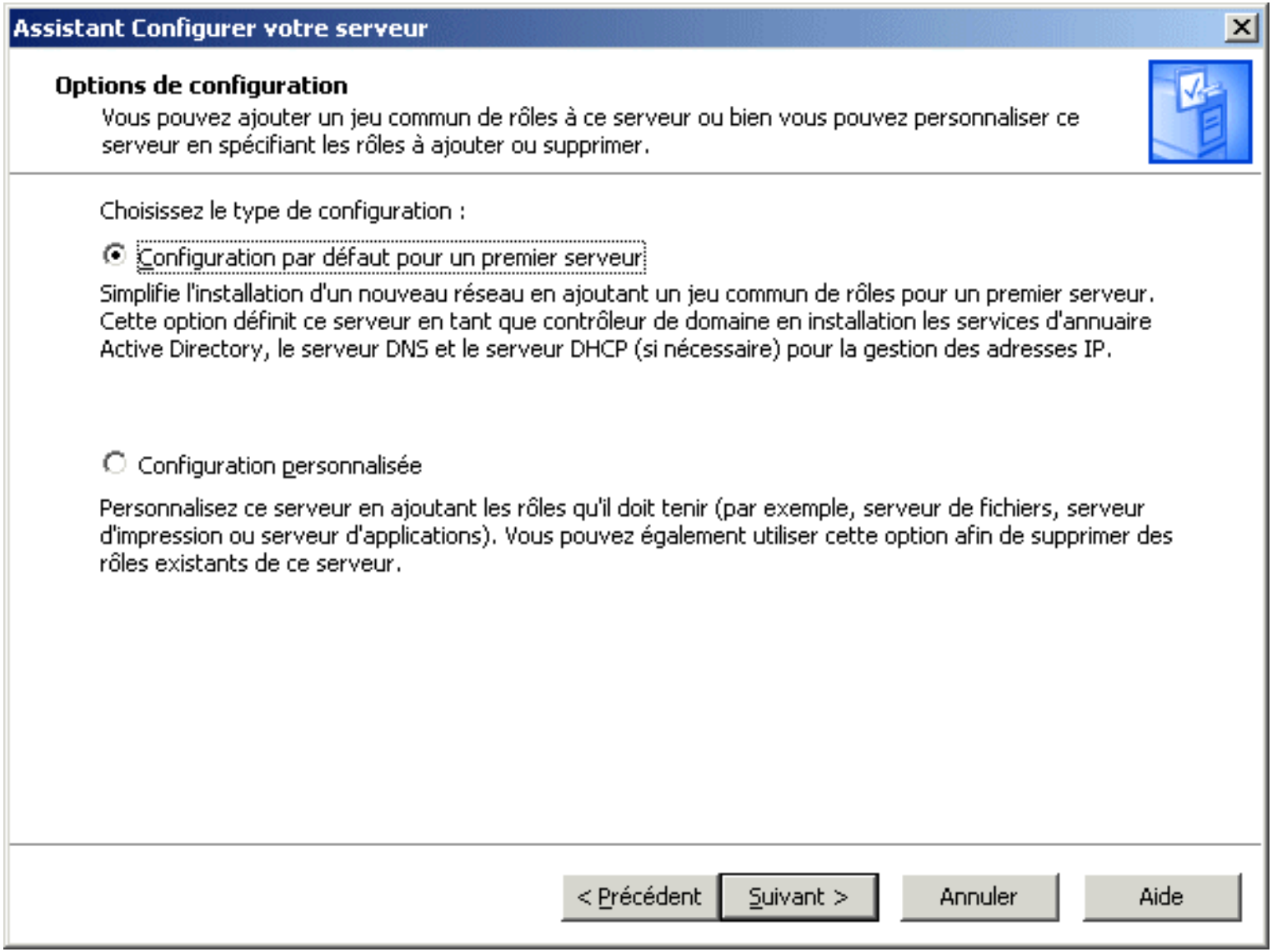
Les actions suivantes devront être effectuées:

- Ajout / suppression d'un rôle ;
- Choix de la configuration "par défaut", si l'option "personnaliser" est choisie, dcpromo démarre ;
- Choix du nom de domaine ;
- Choix du nom compatible NetBEUI ;
- Confirmation et démarrage de l'installation.

Installation du service d'annuaire: utilitaire "Gérer votre server"



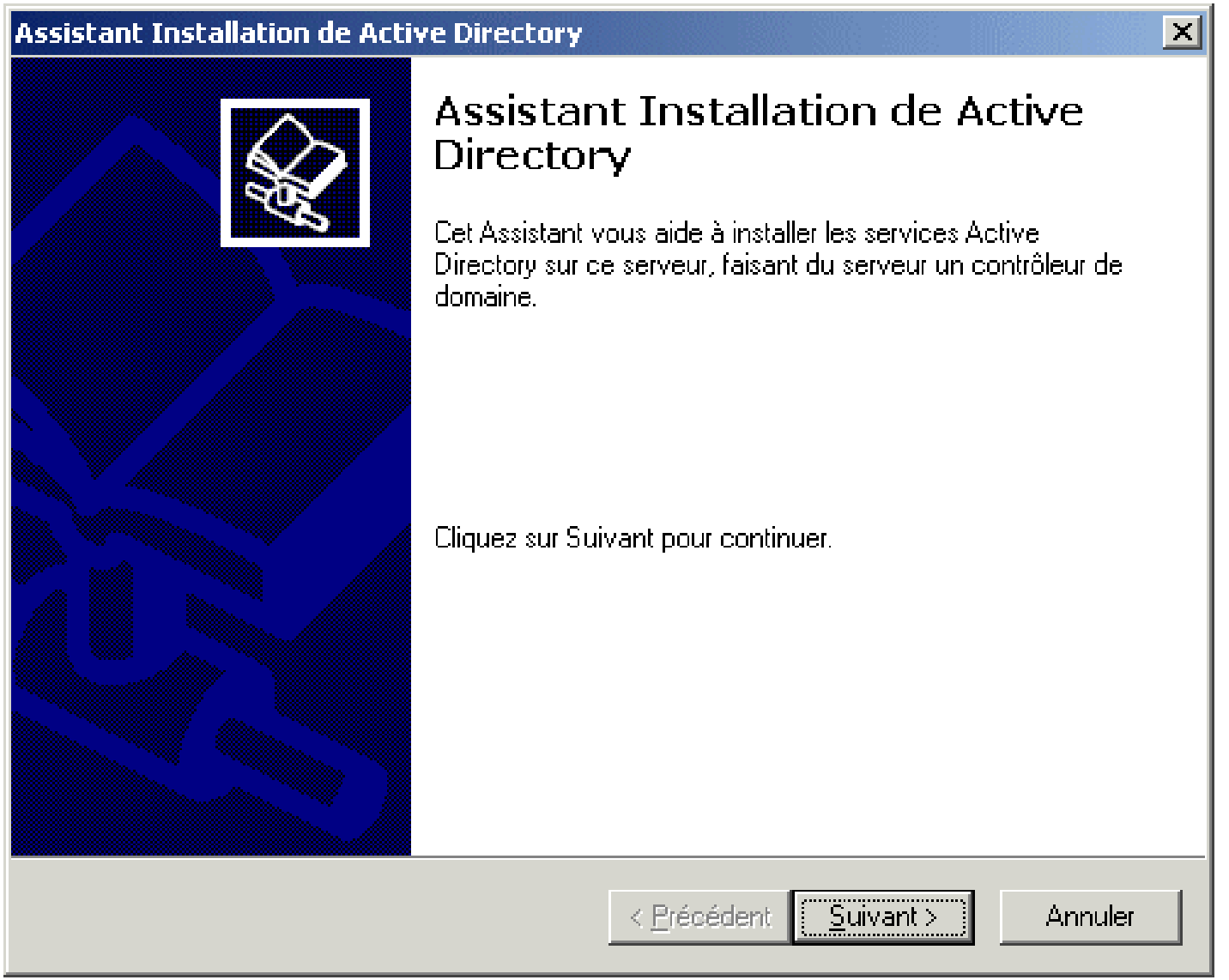
Installation du service d'annuaire: utilitaire "Gérer votre server"



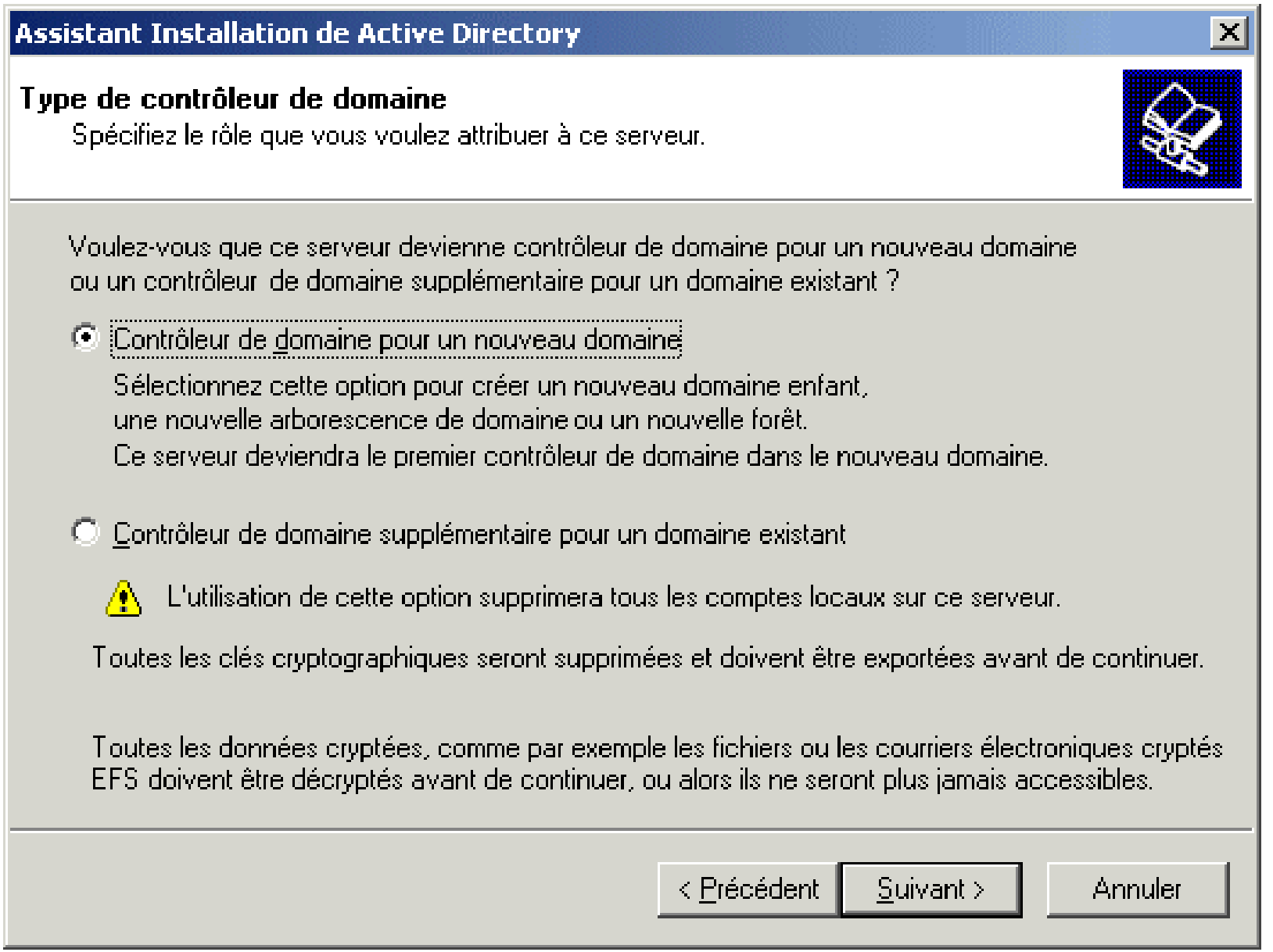
Les actions suivantes devront être effectuées:

- Choix du nom de domaine crée (nom complet) ;
- Choix du nom de domaine NetBIOS (compatibilité avec les version antérieur de Windows) ;
- Choix de l'emplacement de stockage des informations ADS ;
- Définition du mot de passe Administrateur pour le redémarrage en mode restauration ADS ;
- Installation.

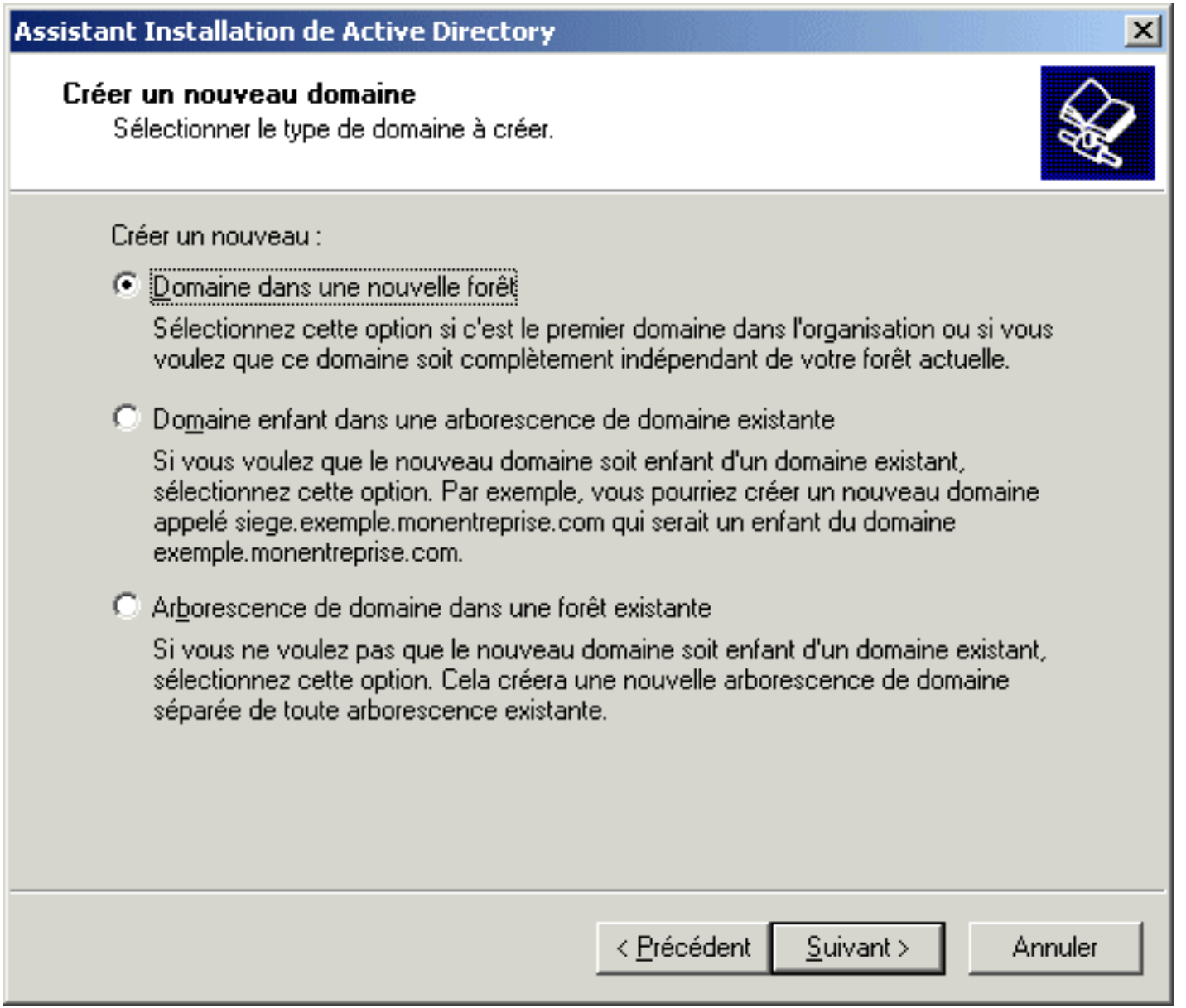
Installation du service d'annuaire: assistant dcpromo



Installation du service d'annuaire: assistant dcpromo



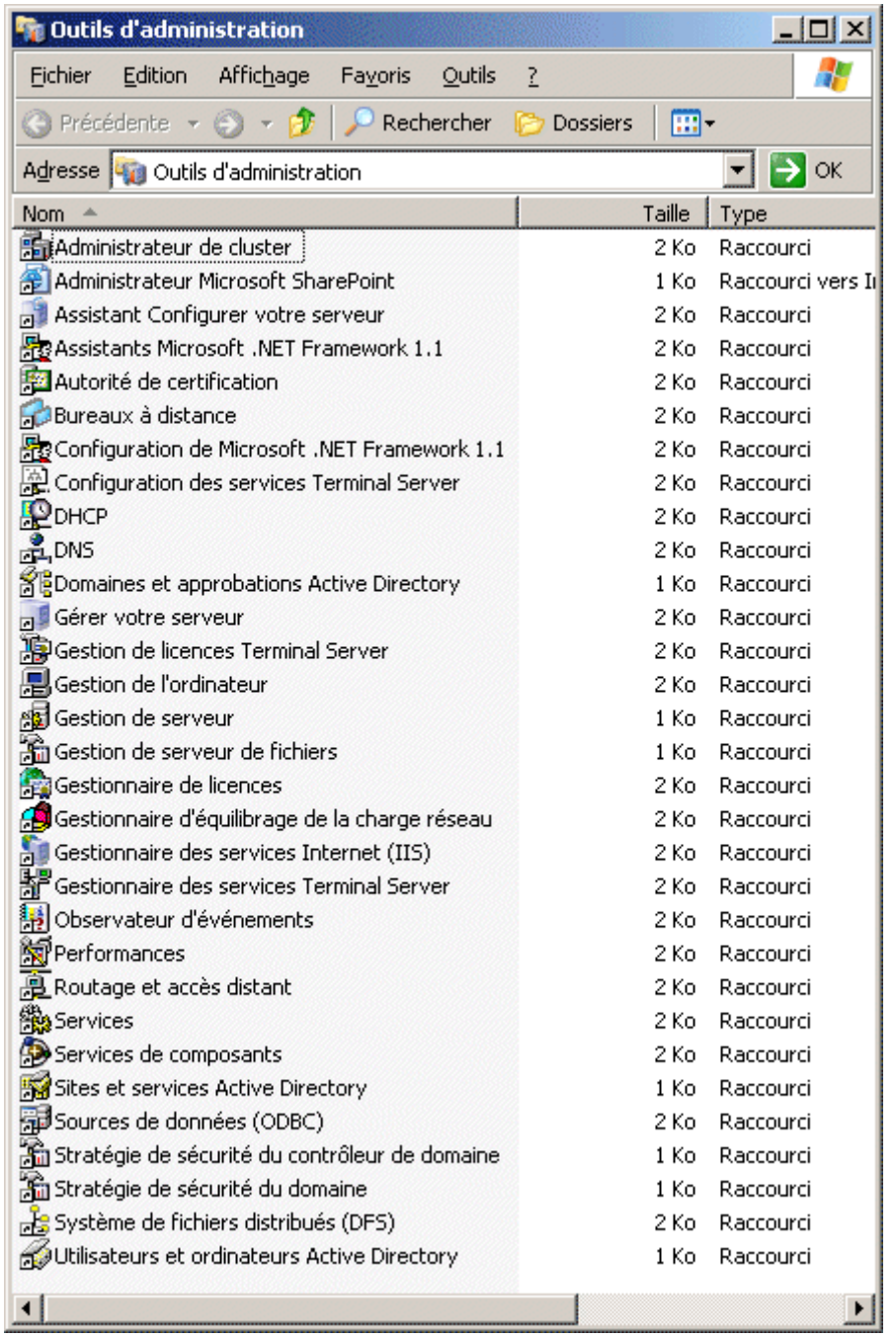
Installation du service d'annuaire: assistant dcpromo



Installation du service d'annuaire: fin de l'installation

- Après l'installation de ADS, un certain nombre d'outils d'administration sont disponible.
- Après redémarrage, ADS est en fonctionnement pour la gestion du (nouveau) domaine.
- Le service DNS est lui aussi en fonctionnement mais n'est pas configuré.

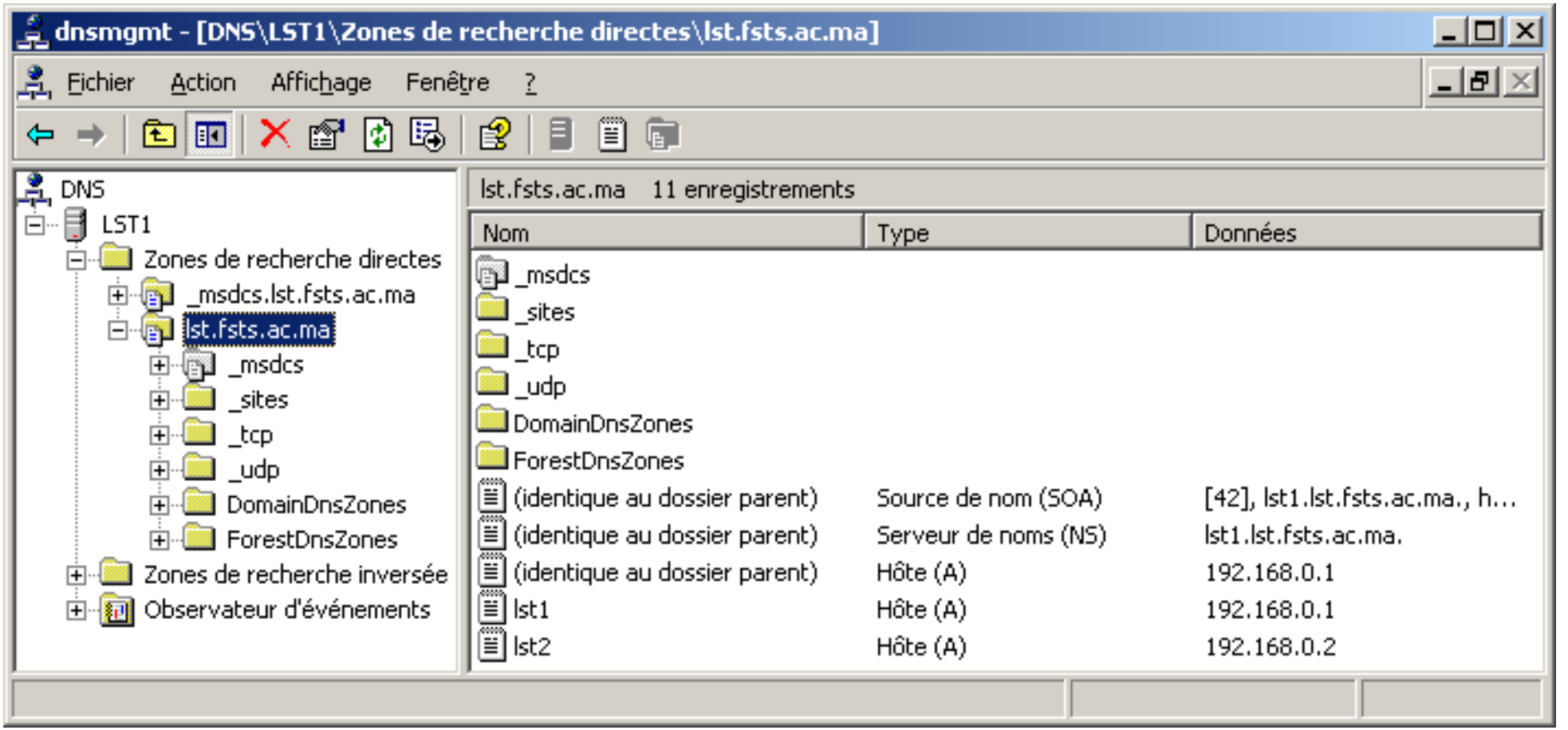
Installation du service d'annuaire: fin de l'installation



La configuration du service DNS conprend les étapes suivantes:

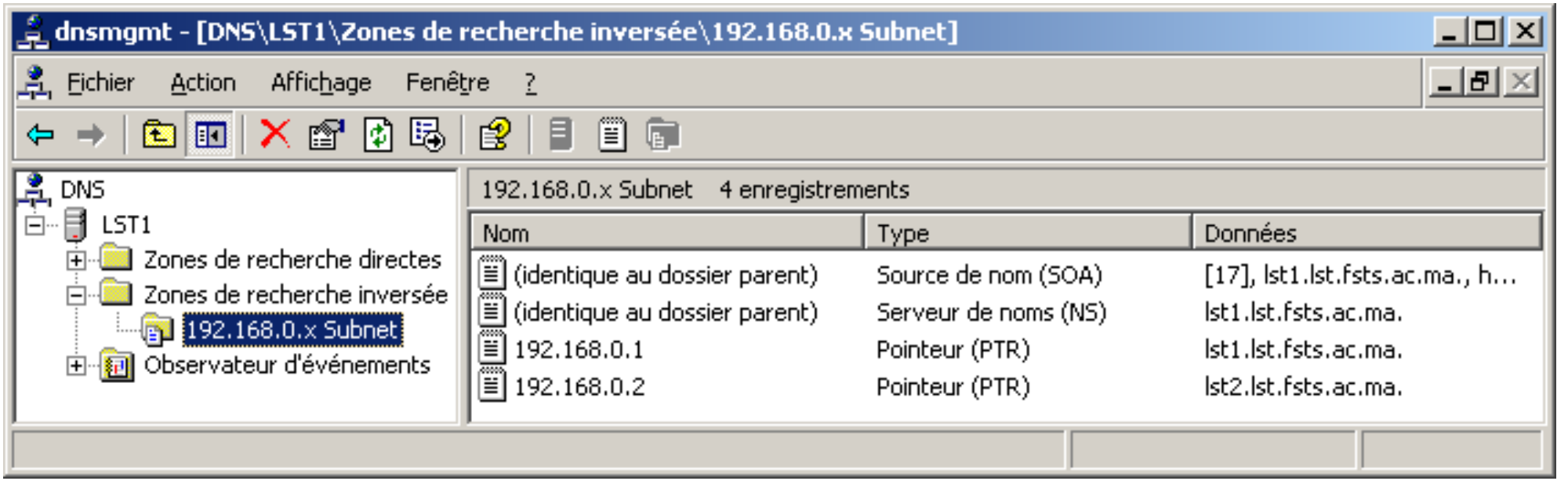
- Définition de zones de recherche directes pour les résolutions de nom en adresse IP ;
- Définition de zones de recherche inverse pour les résolutions d'adresse IP en nom.

Déclaration des nouvelles machines (hôtes) avec demande de création automatique du pointeur PTR associé.



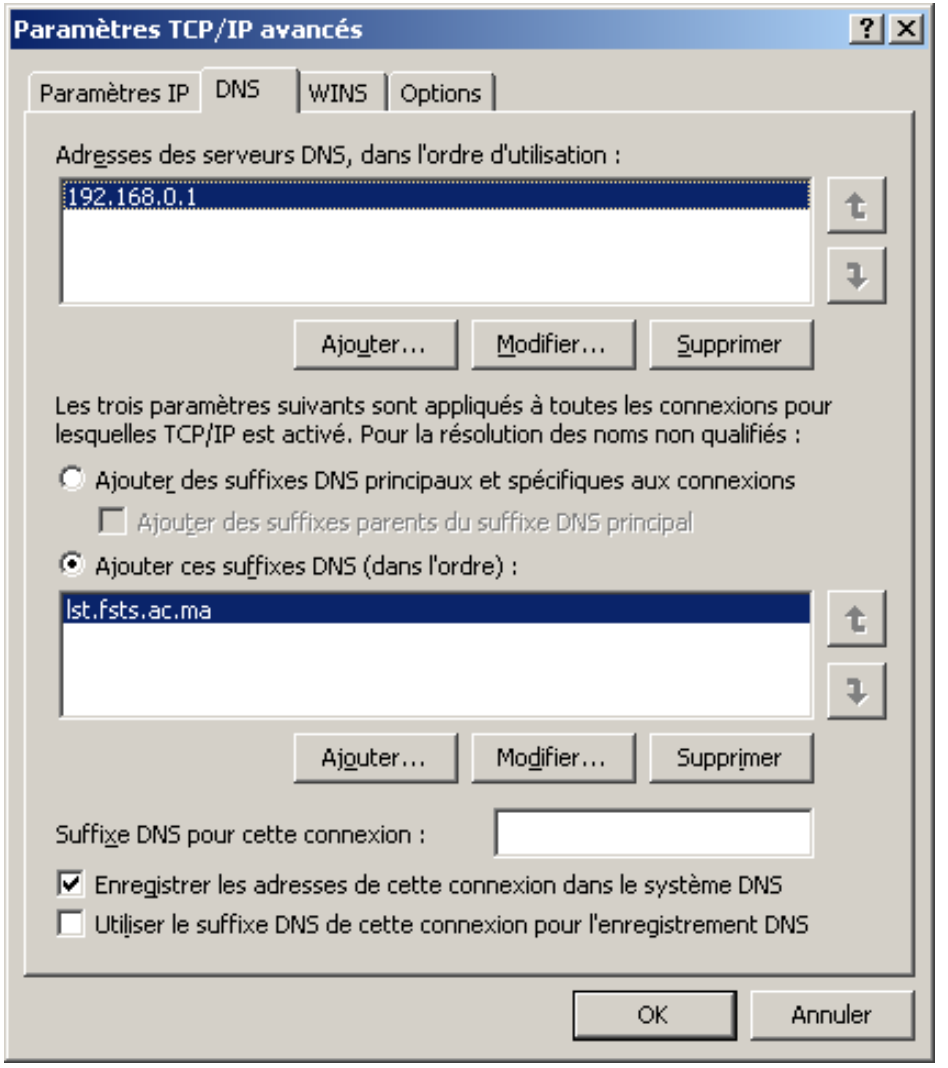
- Lancement de l'assistant de création de zone inverse ;
- Création d'une zône rincipale intégrée à AD ;
- Choix de l'étendue de réplication de cette zône ;
- Définition de l'ID réseau de cette zône ;
- Choix du mode de mise à jour dynamique ;
- Fin de l'assistant de création de zone inverse.

Configuration du service DNS: la zone inverse



Configuration du service DNS: paramètres TCP/IP

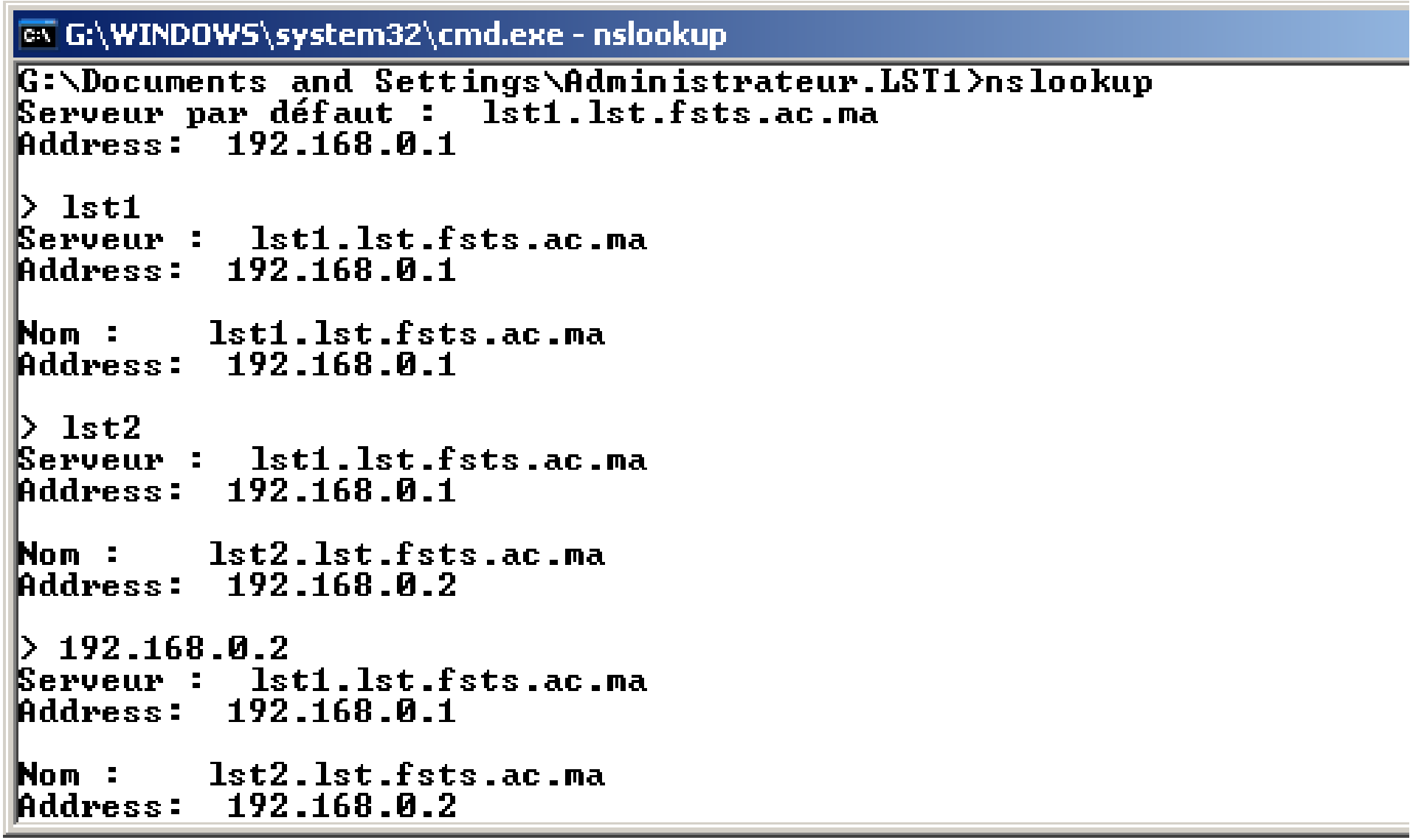
- Reconfiguration des paramètres TCP/IP pour prendre en compte le nouveau DNS ainsi que le suffixe DNS nouvellement créé.



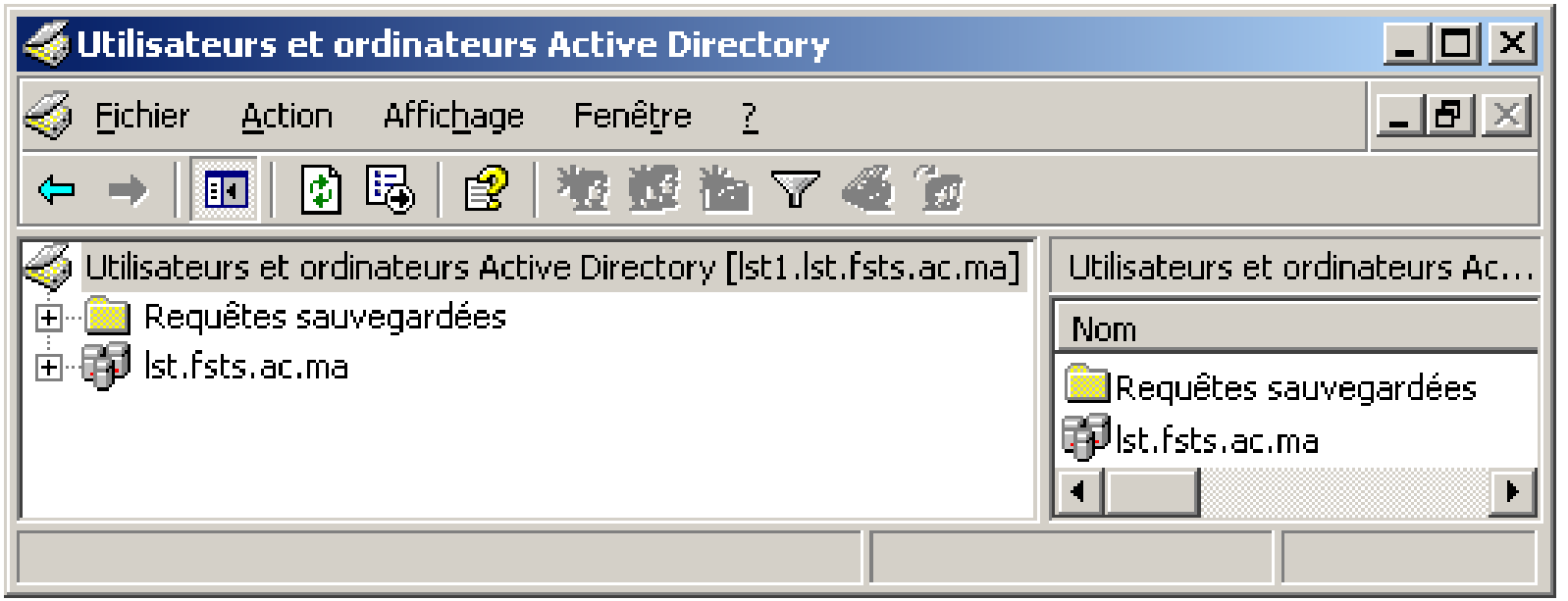
Exécution de la commande nslookup directement dans une invite de commande :

- Test de résolution nom DNS → adresse IP pour le nom de domaine ;
- Test de résolution nom DNS → adresse IP pour un nom quelconque
- Test de résolution adresse IP → nom DNS

Configuration du service DNS: test NSLOOKUP



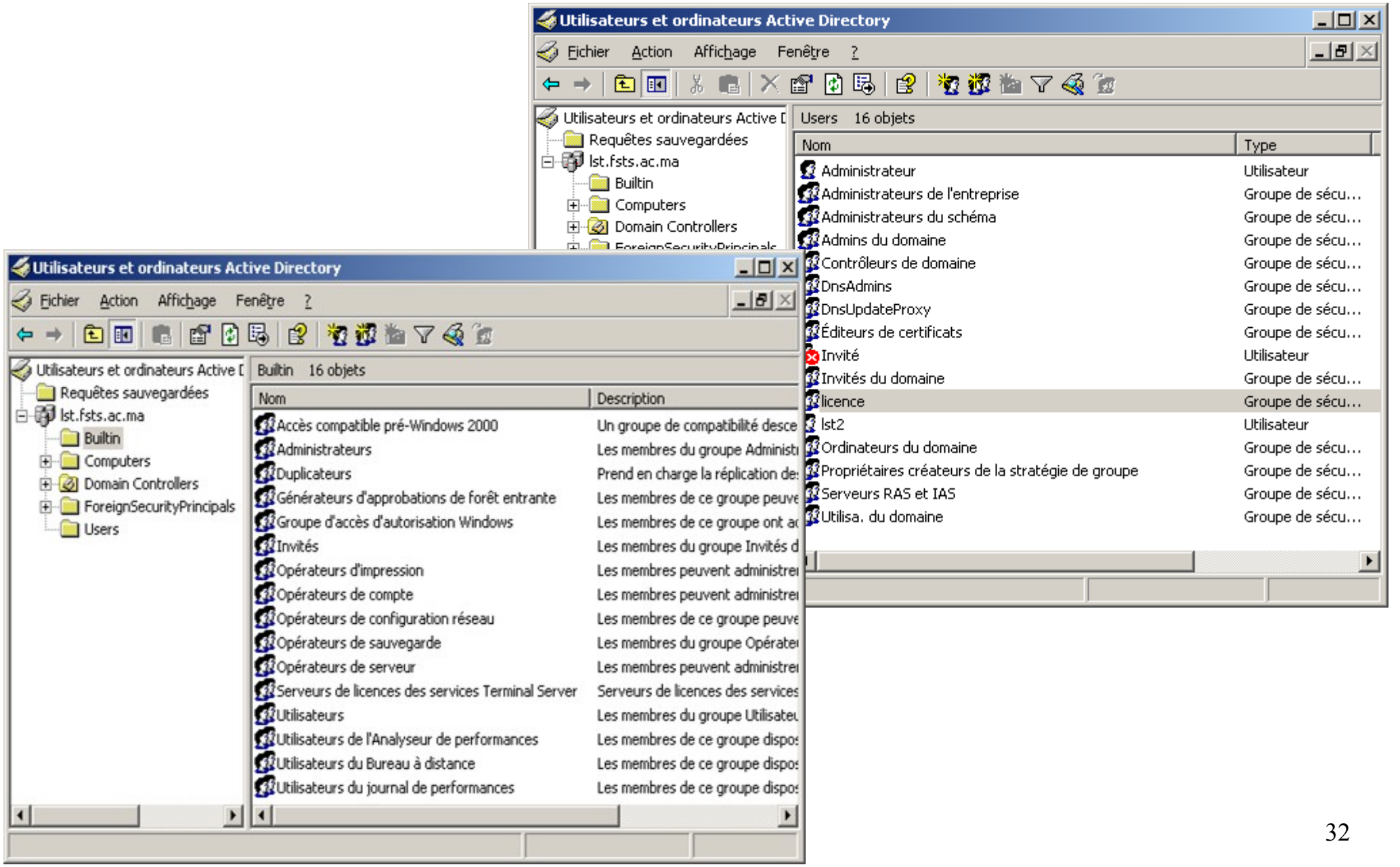
Pour effectuer la gestion du domaine, l'outil utilisateurs et ordianteurs Active Directory est utilisé:



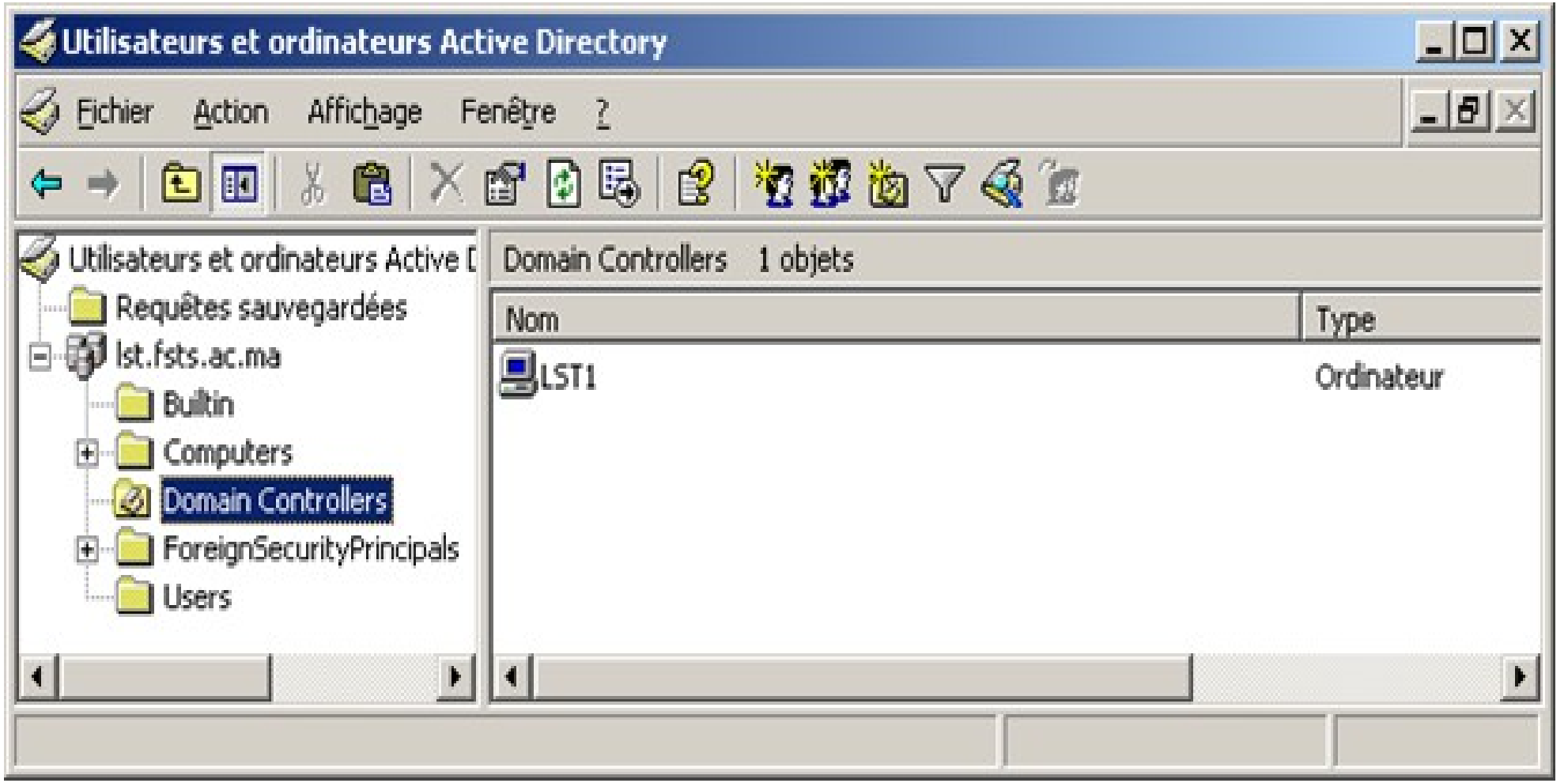
Cet outil réalise l'administration des utilisateurs, des groupes d'utilisateurs et des ordinateurs d'un domaine.

Il permet de créer un compte pour chacunes des entitées précédement citées.

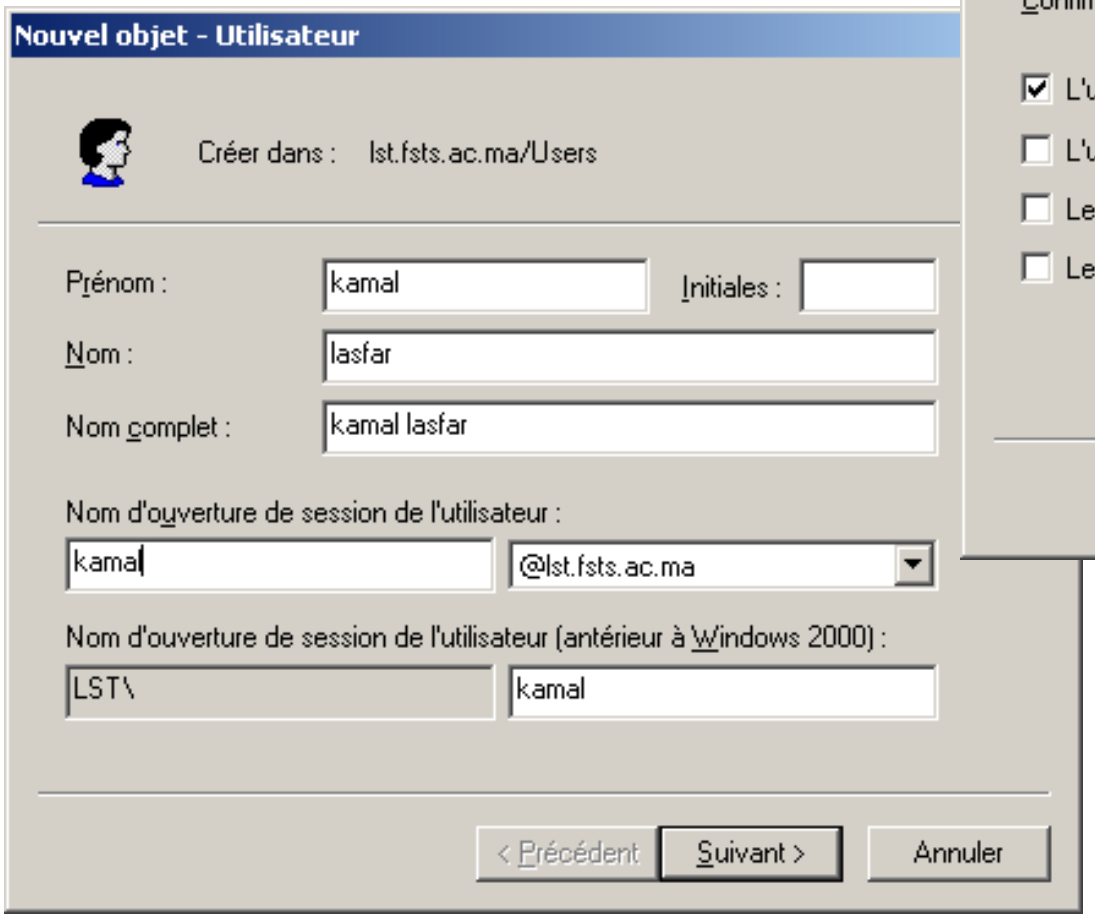
Gestion du domaine: utilisateurs, groupe et ordinateur

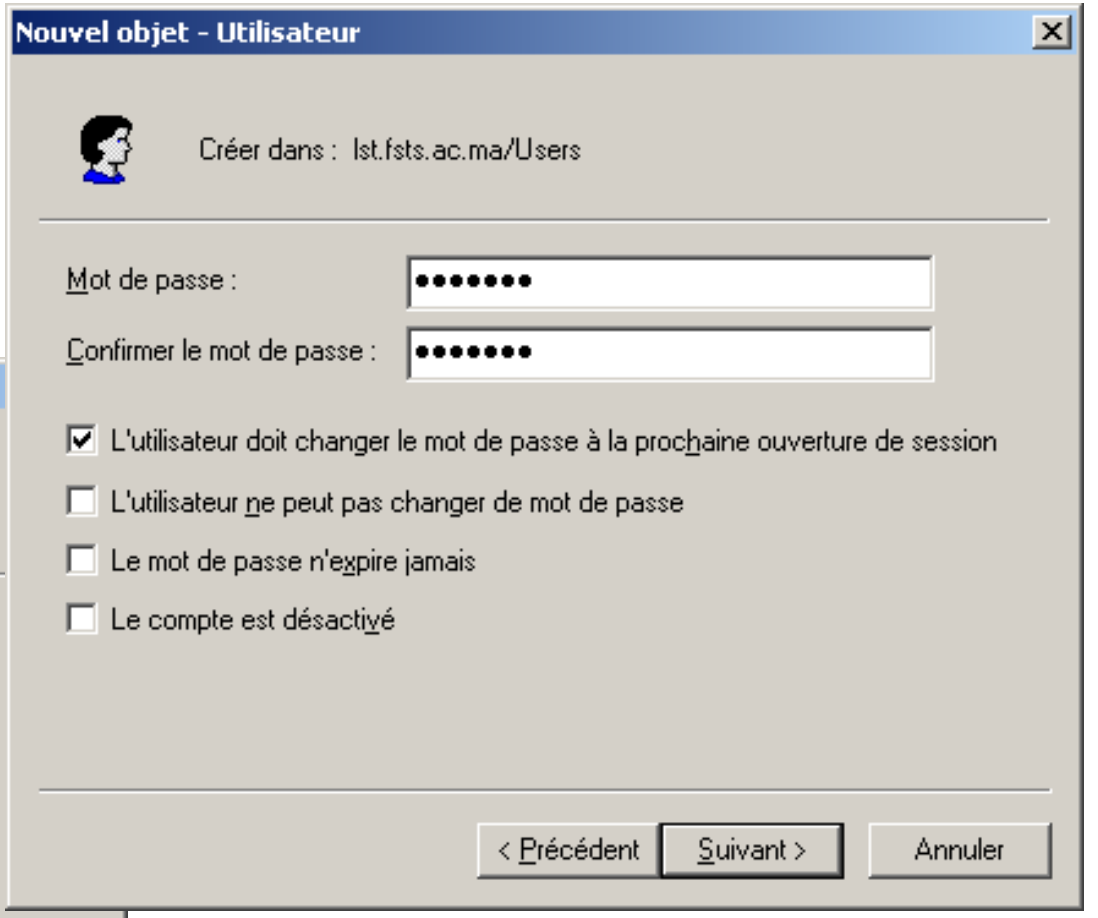


Contrôleur de domaine

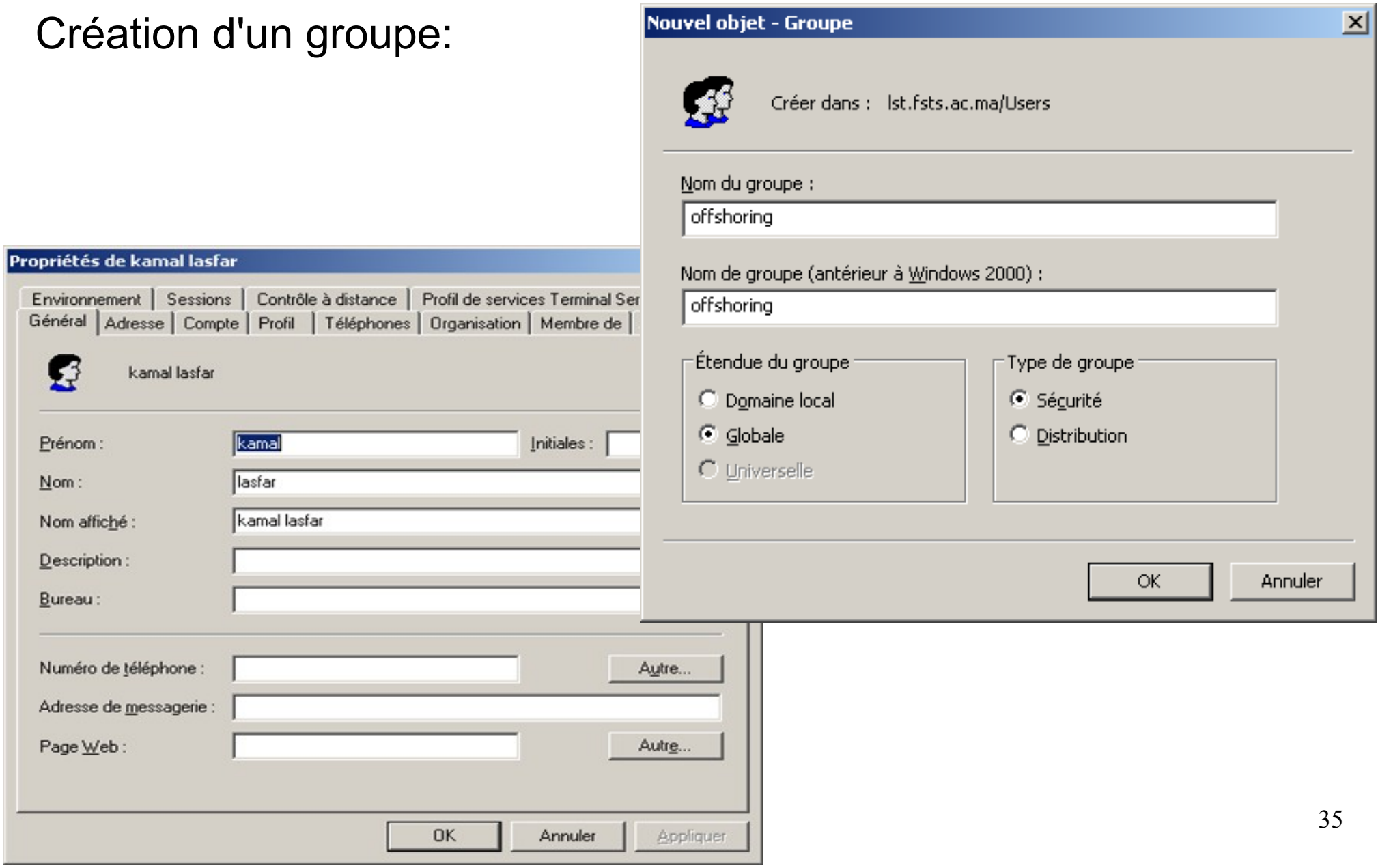


Création d'un utlisateur:

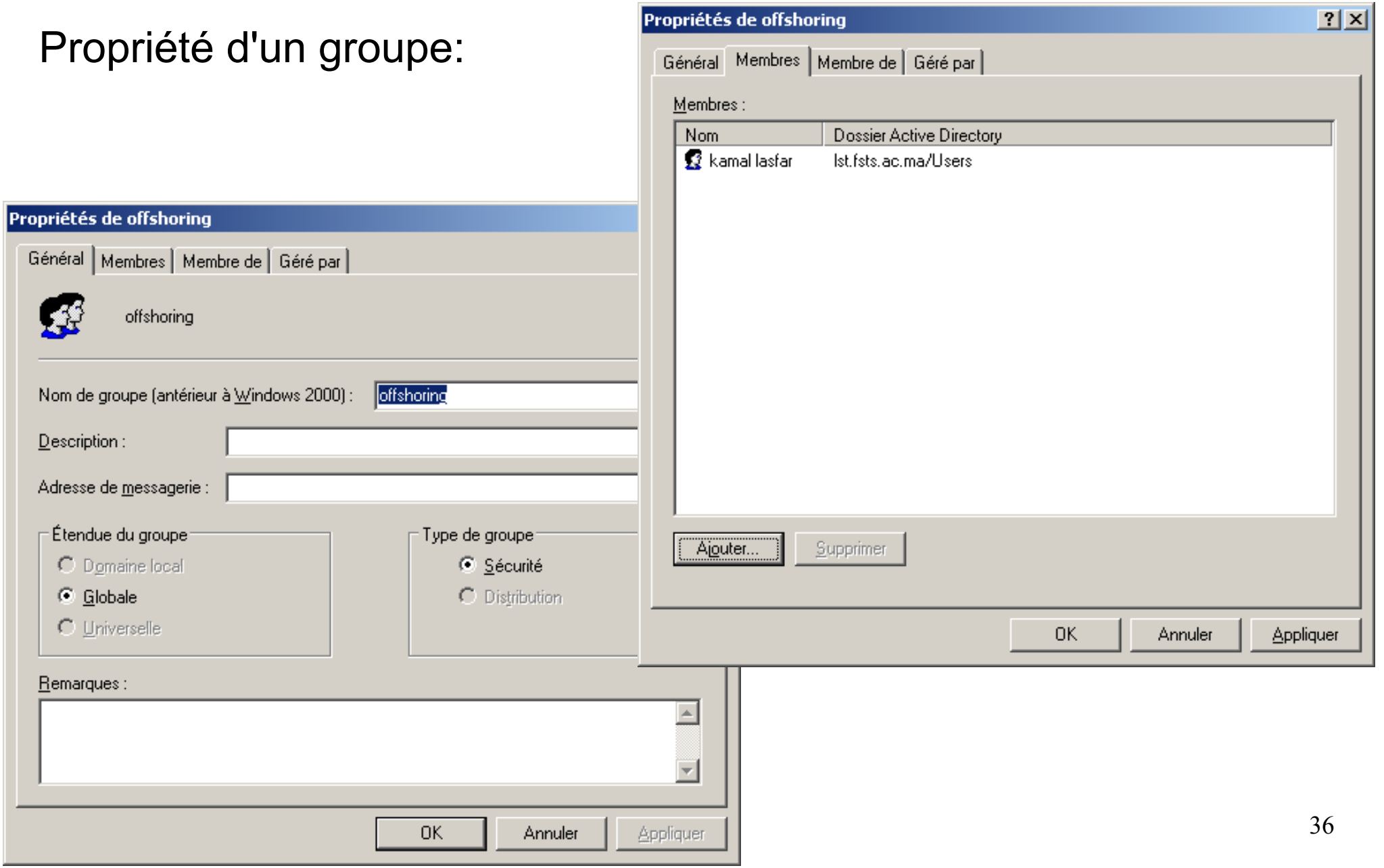




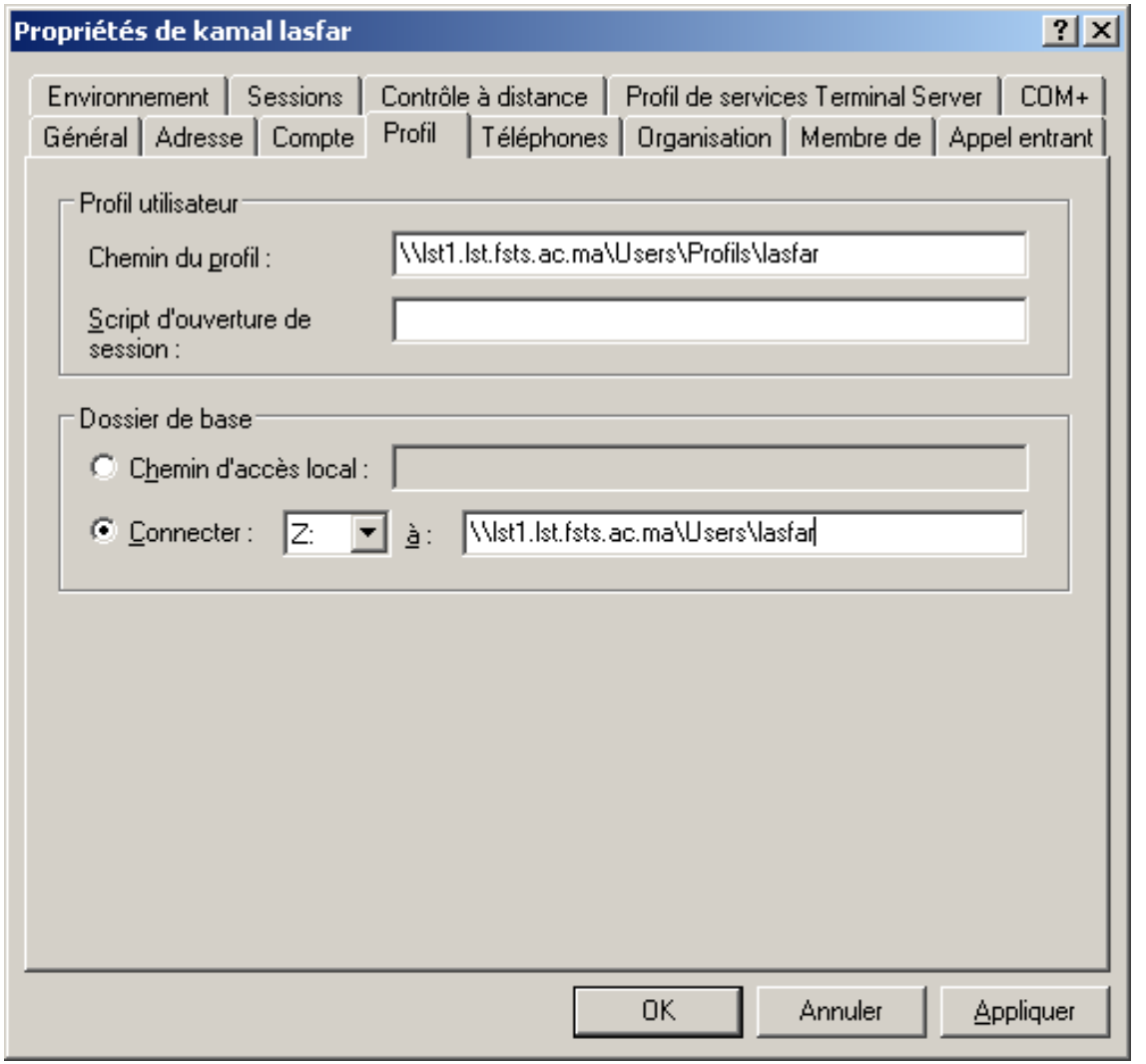
Création d'un groupe:



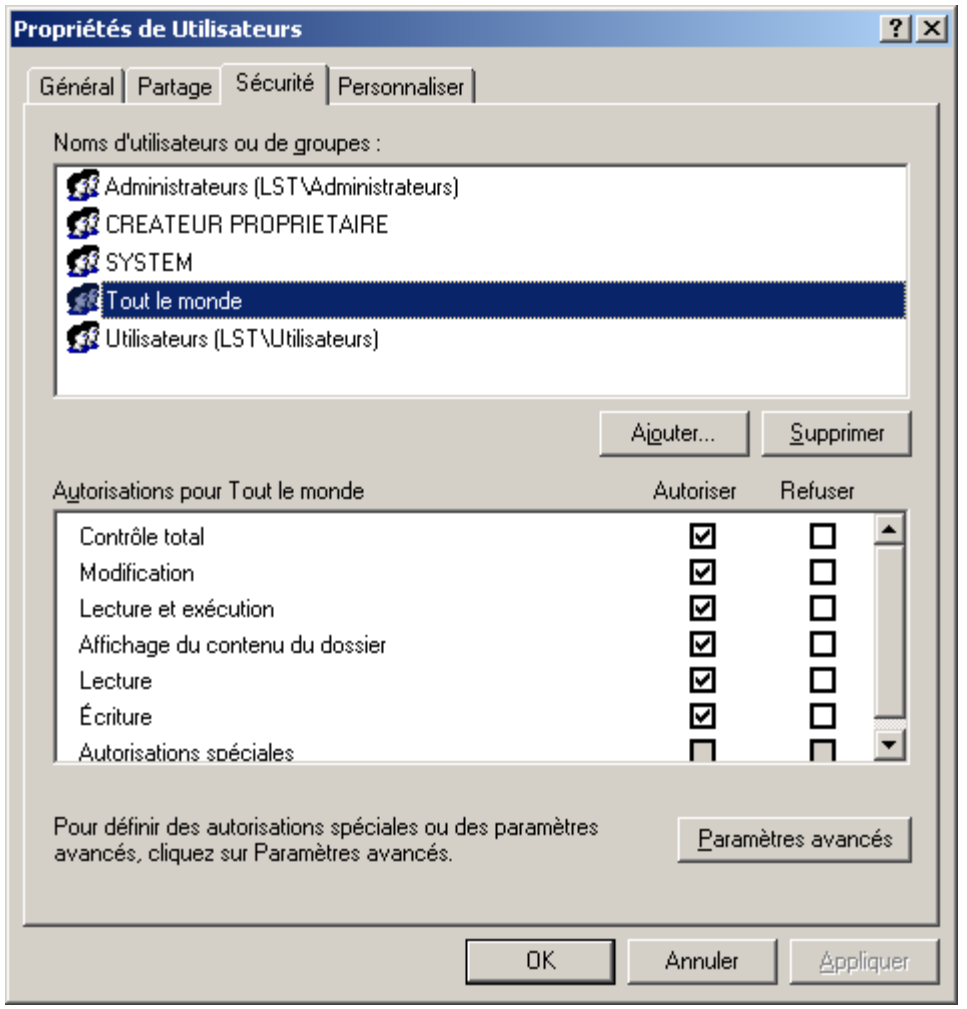
Propriété d'un groupe:

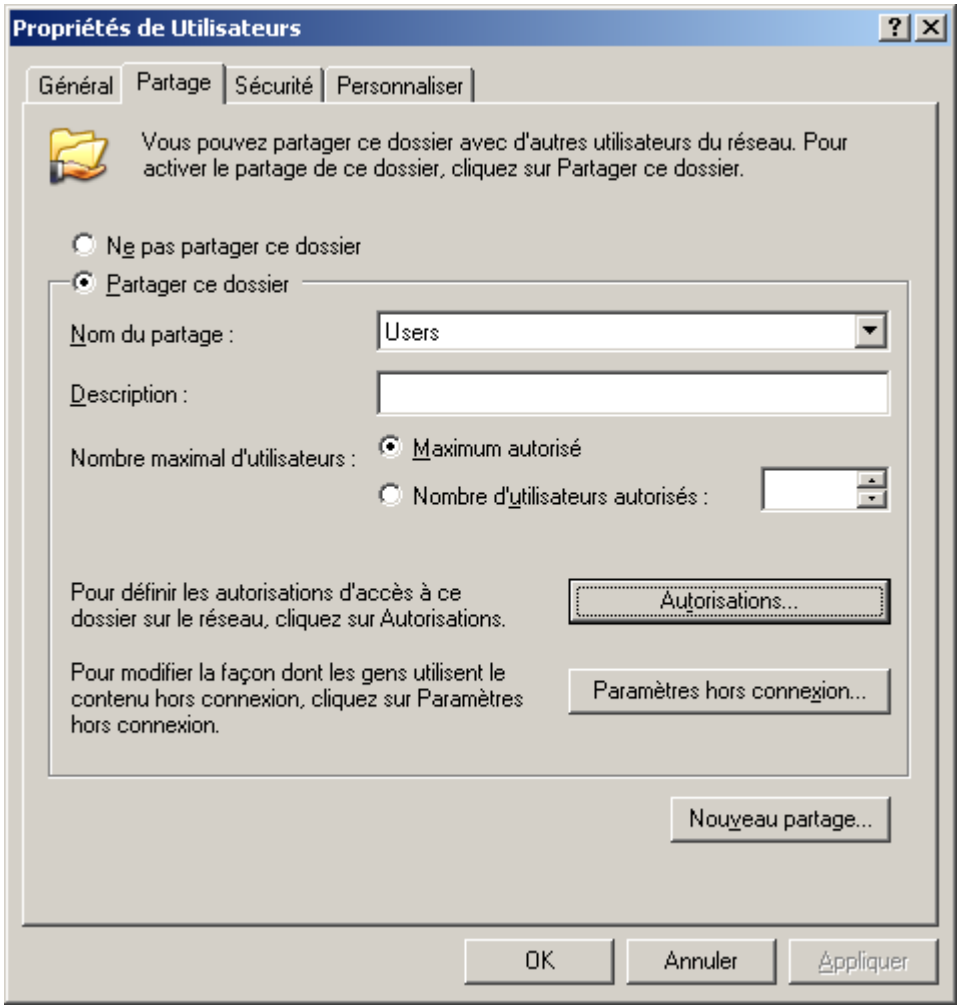


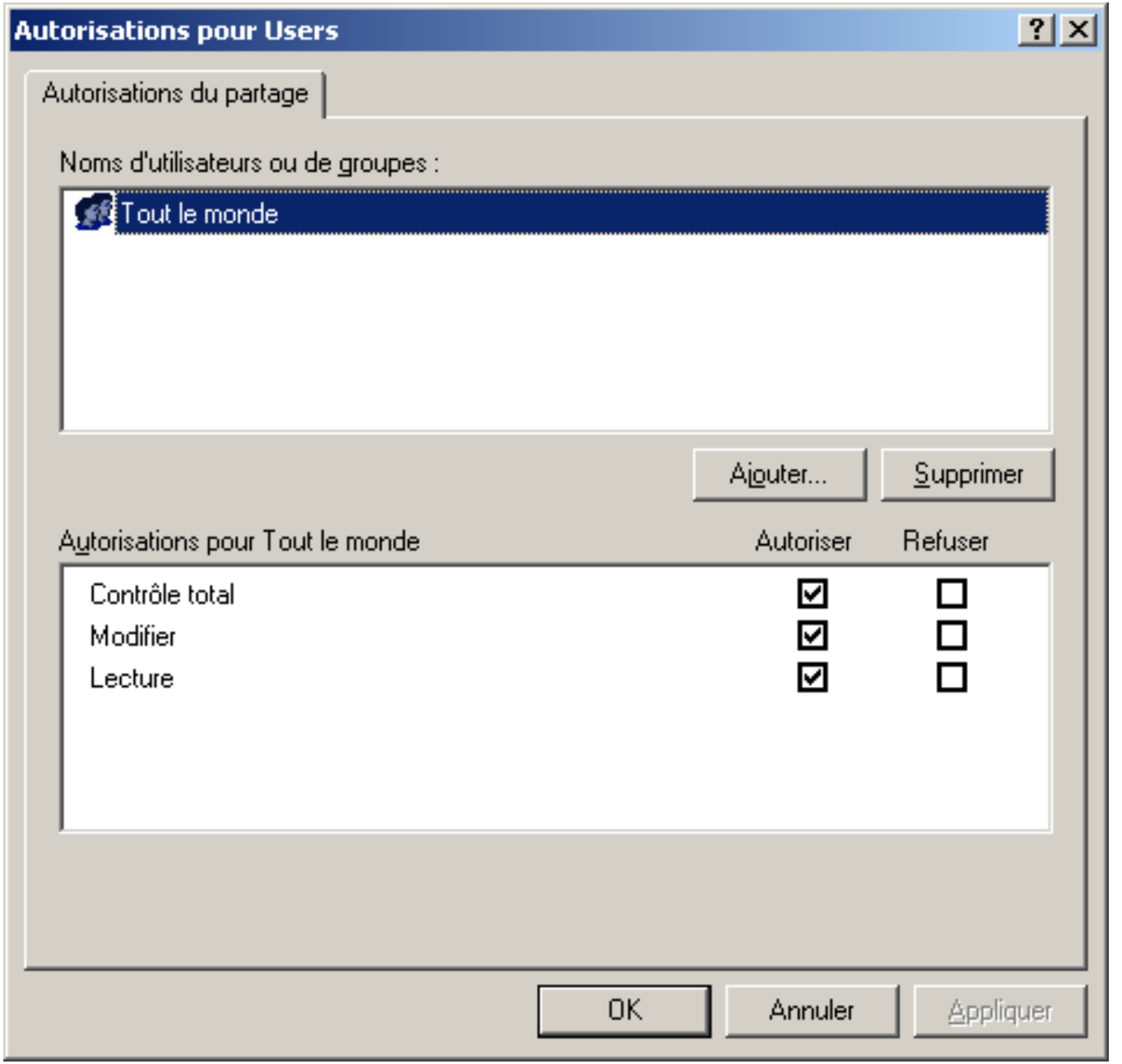
- Il est possible d'affecter un répertoire pour heberger les répertoires de base et les profils itinérant en allant dans le menu d'un utilisateur dans sa section 'Profils' ;



- Il faut ensuite partager ce répertoire sous le nom 'Users' et configurer les autorisations sur le répertoire ainsi que sur le partage ;

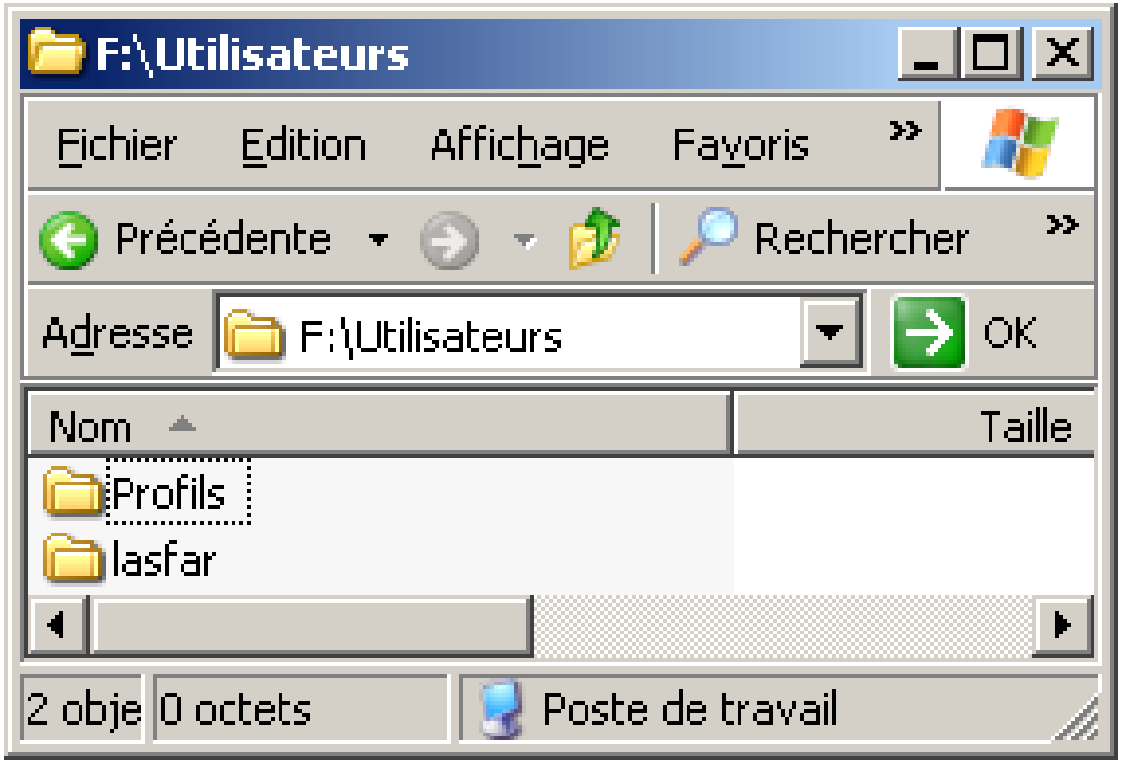





Autorisations pour Users
Autorisations du partage
Noms d'utilisateurs ou de groupes :
Tout le monde
Ajouter...
Supprimer
Autorisations pour Tout le monde
Autoriser
Refuser
Contrôle total
Modifier
Lecture
OK
Annuler
Appliquer

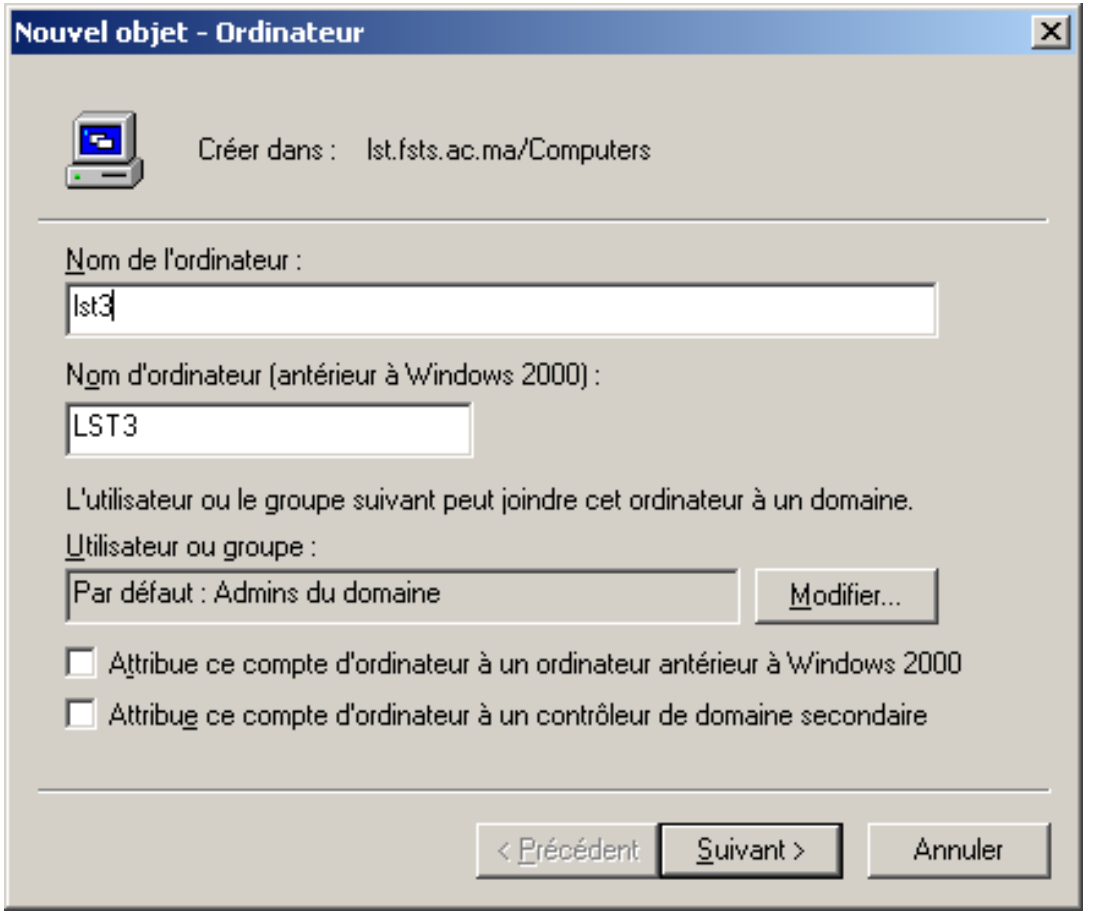
- Le gestionnaire des utilisateurs crée lui-même le répertoire de base et lui affecte les permissions en limitant l'accès au seul administrateur et à l'utilisateur ;

- Le montage du répertoire de base est automatique au niveau du client.



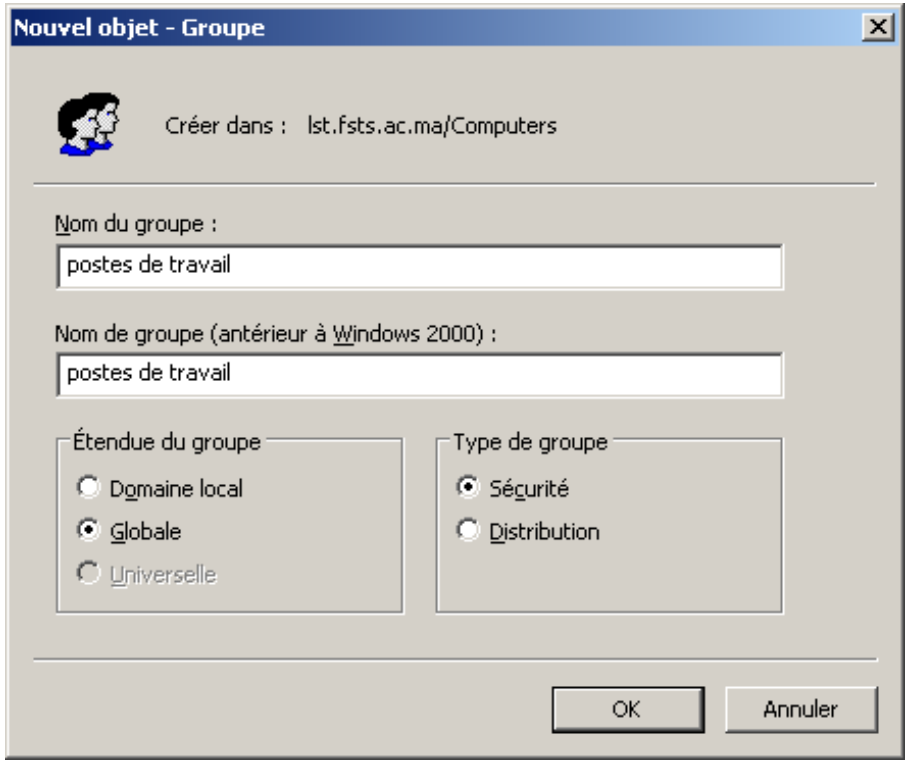
La création d'un ordianteur passe par les étapes suivantes:

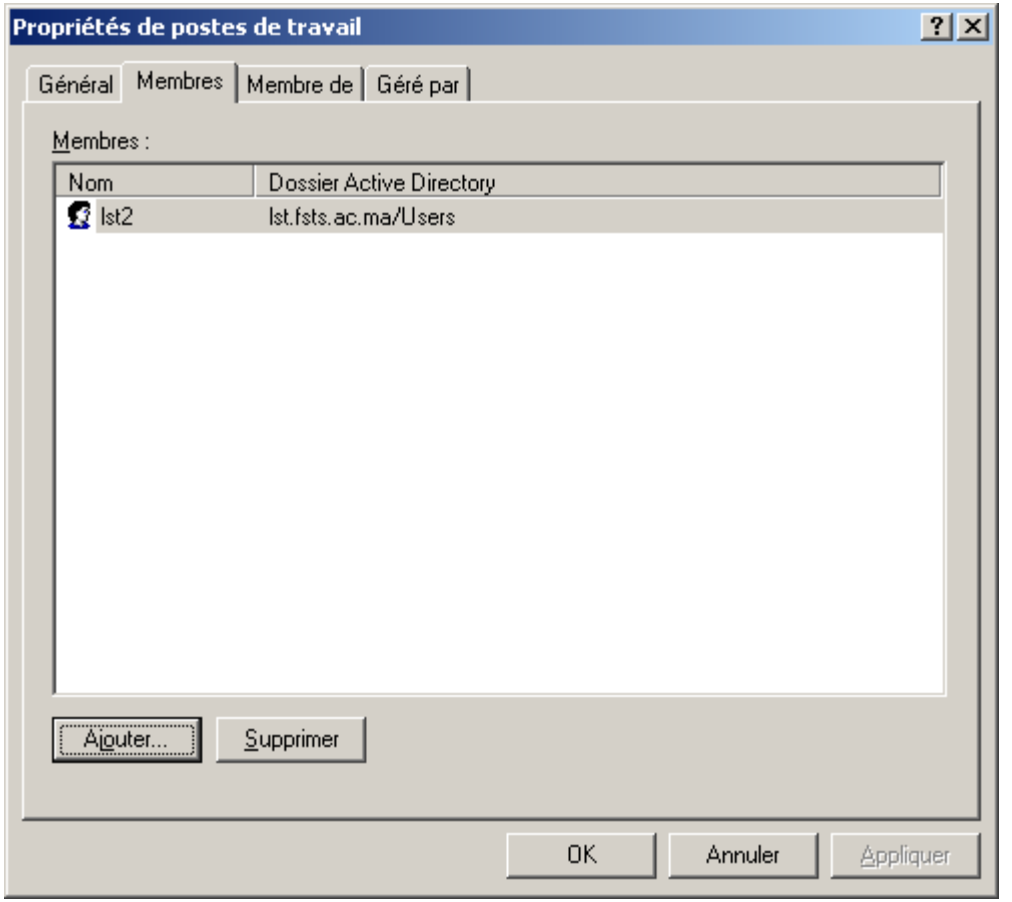
- Définition d'un nom unique ;
- Déclaration en tant que membre simple ou contrôleur de domaine supplémentaire.



La création d'un groupe passe par les étapes suivantes:

- Définition d'un nom unique ;
- Ajout des ordinateur / utilisateurs au groupe.





- Installation de AD;
- Configuration du DNS ;
- Test du DNS ;
- Création des utilisateurs / groupes / ordianteurs ;
- Test d'authentification en se logant sur un poste client.