

Réseaux Active Directory

1. Introduction
2. Définitions des notions employées
3. Installation du service d'annuaire
4. Configuration du service DNS
5. Gestion du domaine

- 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.

Dans Active Directory, un domaine est l'ensemble d'objets ordinateur, utilisateur et groupe défini par l'administrateur.

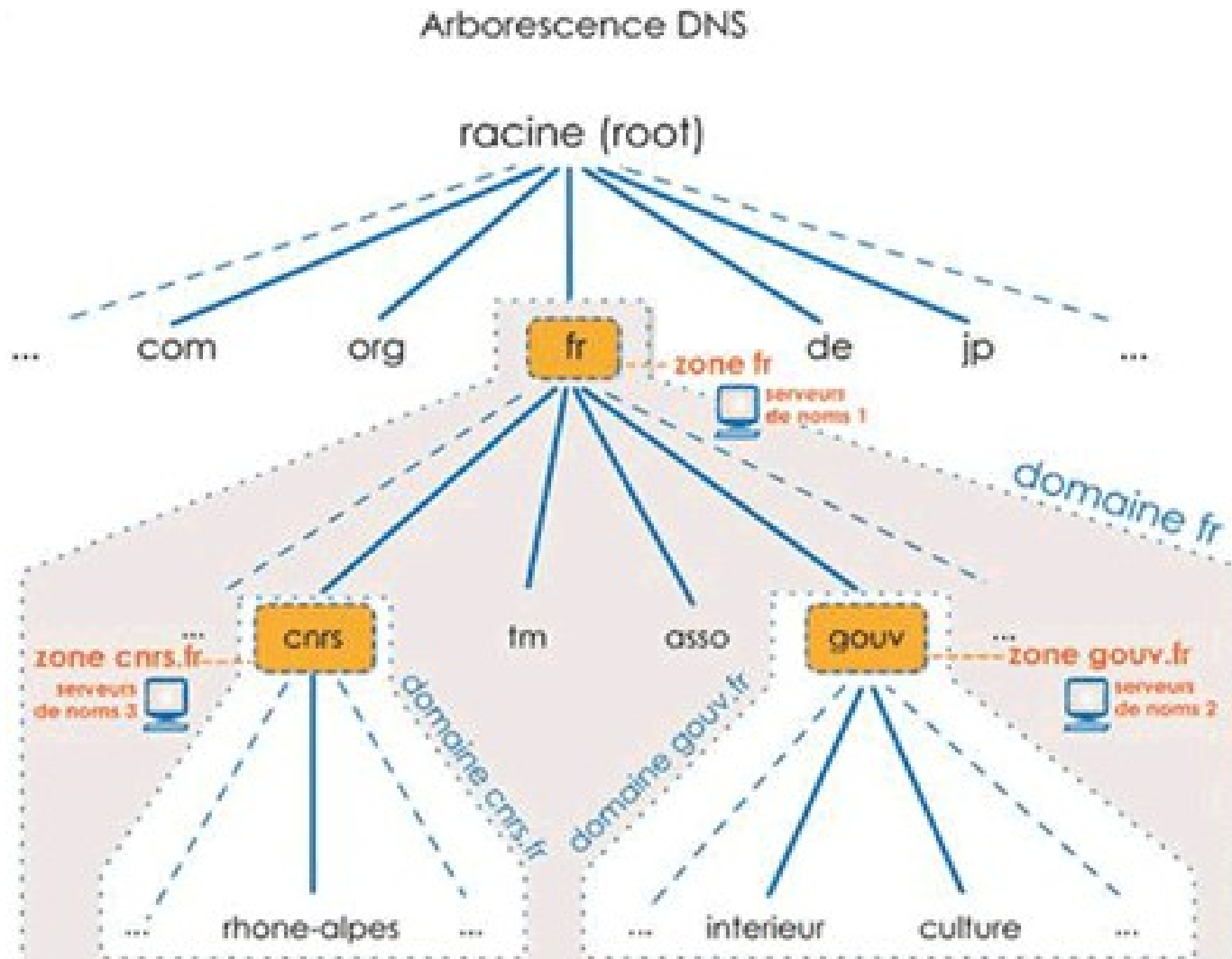
Ces objets partagent une base de données d'annuaire, des stratégies de sécurité et des relations de sécurité communes avec d'autres domaines.

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

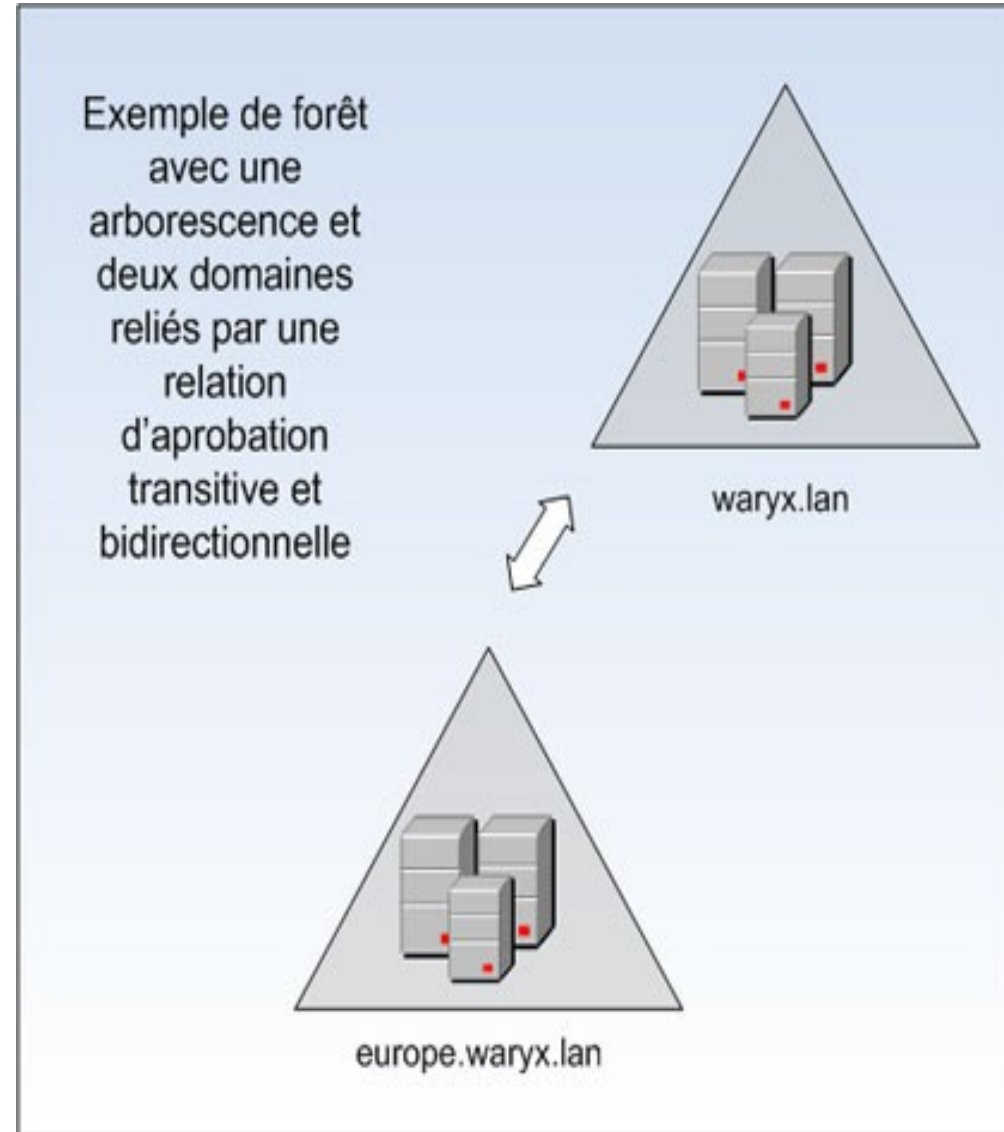
Dans DNS, l'arborescence de domaine est la structure de l'arborescence hiérarchique inversée qui est utilisée pour indexer les noms de domaines.



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**.

Une forêt correspond à un ou plusieurs domaines Active Directory partageant 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 forêt 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.

Gérer votre serveur
Serveur : TELEMAQUE

Effectuer une recherche dans le Centre Aide et support

Gérer les rôles de votre serveur

Utilisez les outils et les informations trouvés ici pour ajouter ou supprimer des rôles et effectuer vos tâches d'administration quotidiennes.

Votre serveur a été configuré avec les rôles suivants :

- Serveur d'applications**
Les serveurs d'applications fournissent les technologies de base pour développer, déployer et utiliser les services Web XML, les applications Web, et les applications distribuées. Les technologies des serveurs d'applications incluent ASP.NET, COM+ et les Services Internet (IIS).

- Ajouter ou supprimer un rôle
- Documentez-vous sur les rôles de serveur
- En savoir plus sur l'administration à distance
- En savoir plus sur les serveurs d'applications
- Consultez la documentation concernant l'interface Web de l'administration distante pour les serveurs Web
- Consultez les étapes suivantes pour ce rôle

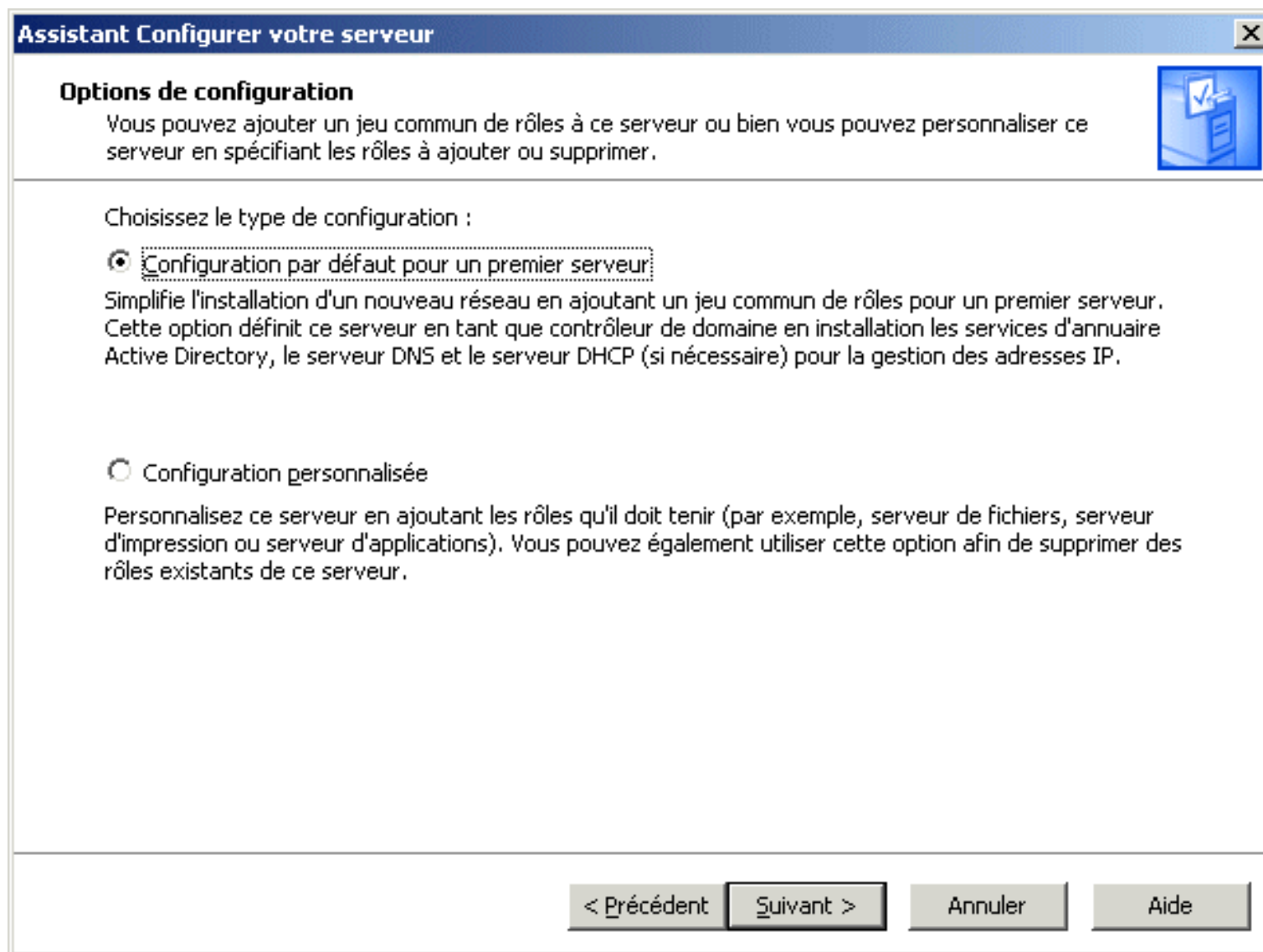
Outils et mises à jour

- Outils d'administration
- Plus d'outils
- Windows Update
- Informations sur le nom de domaine et d'ordinateur
- Configuration de sécurité renforcée d'Internet Explorer

Voir également

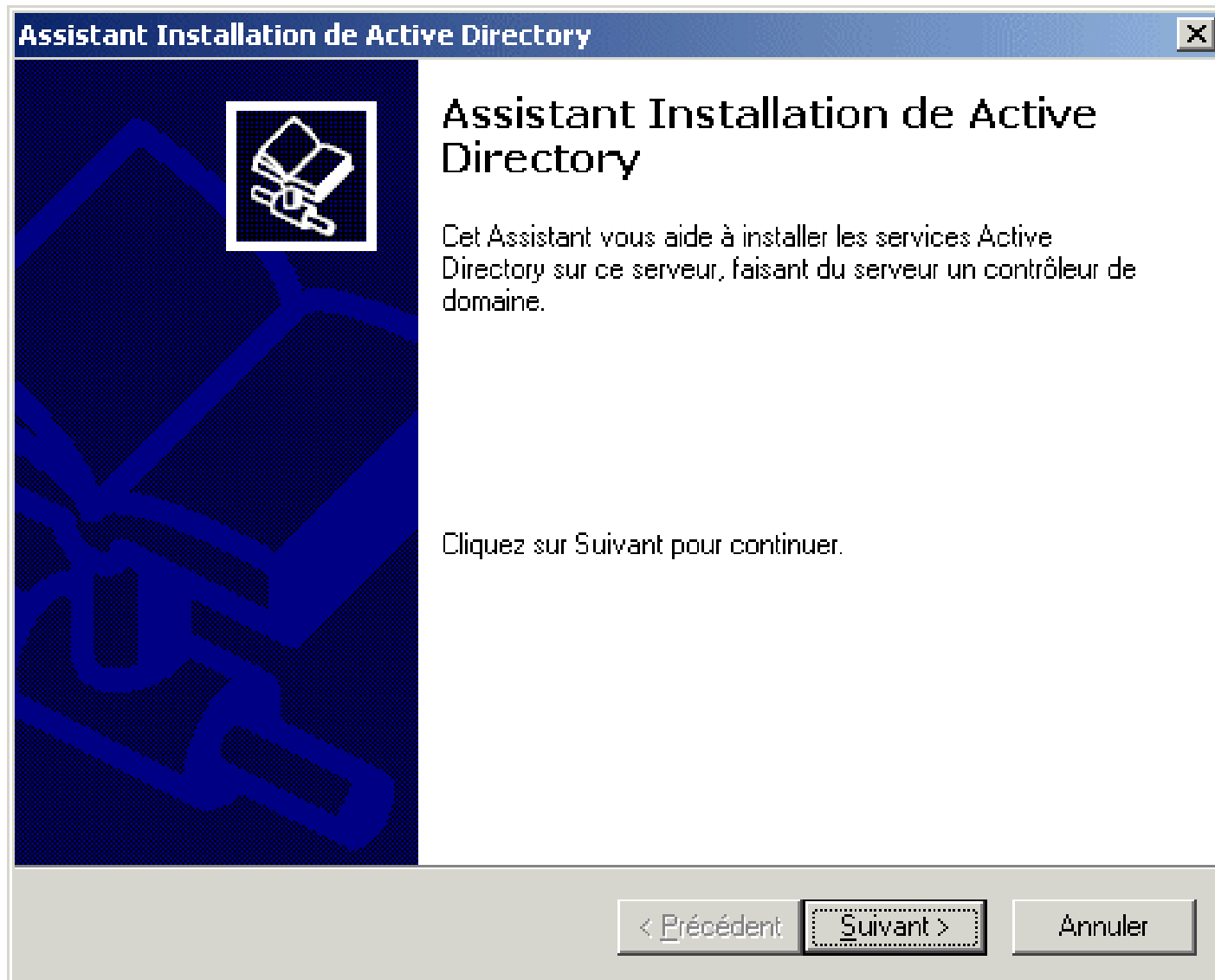
- Aide et support
- Microsoft TechNet
- Kit de ressources et de déploiement
- Liste de tâches administratives communes
- Communautés Windows Server
- Nouveautés
- Programme de protection technologique stratégique

Ne pas afficher cette page à l'ouverture de session



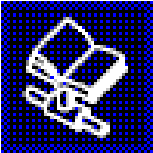
Les actions suivantes devront être effectuées:

- 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.



Assistant Installation de Active Directory ✕


Type de contrôleur de domaine
Spécifiez le rôle que vous voulez attribuer à ce serveur.



Voulez-vous que ce serveur devienne contrôleur de domaine pour un nouveau domaine ou un contrôleur de domaine supplémentaire pour un domaine existant ?

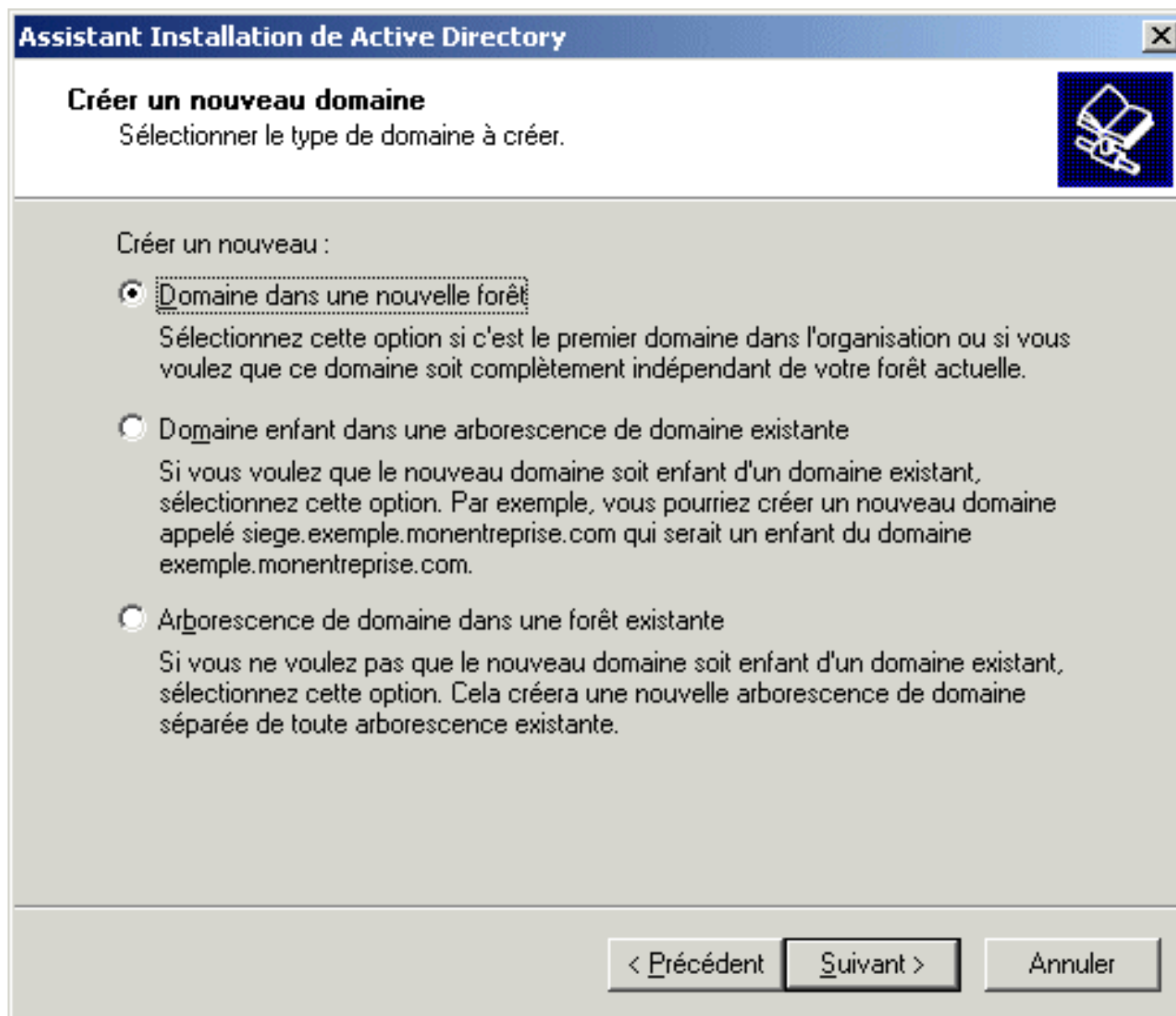
Contrôleur de domaine pour un nouveau domaine
Sélectionnez cette option pour créer un nouveau domaine enfant, une nouvelle arborescence de domaine ou un nouvelle forêt.
Ce serveur deviendra le premier contrôleur de domaine dans le nouveau domaine.

Contrôleur de domaine supplémentaire pour un domaine existant

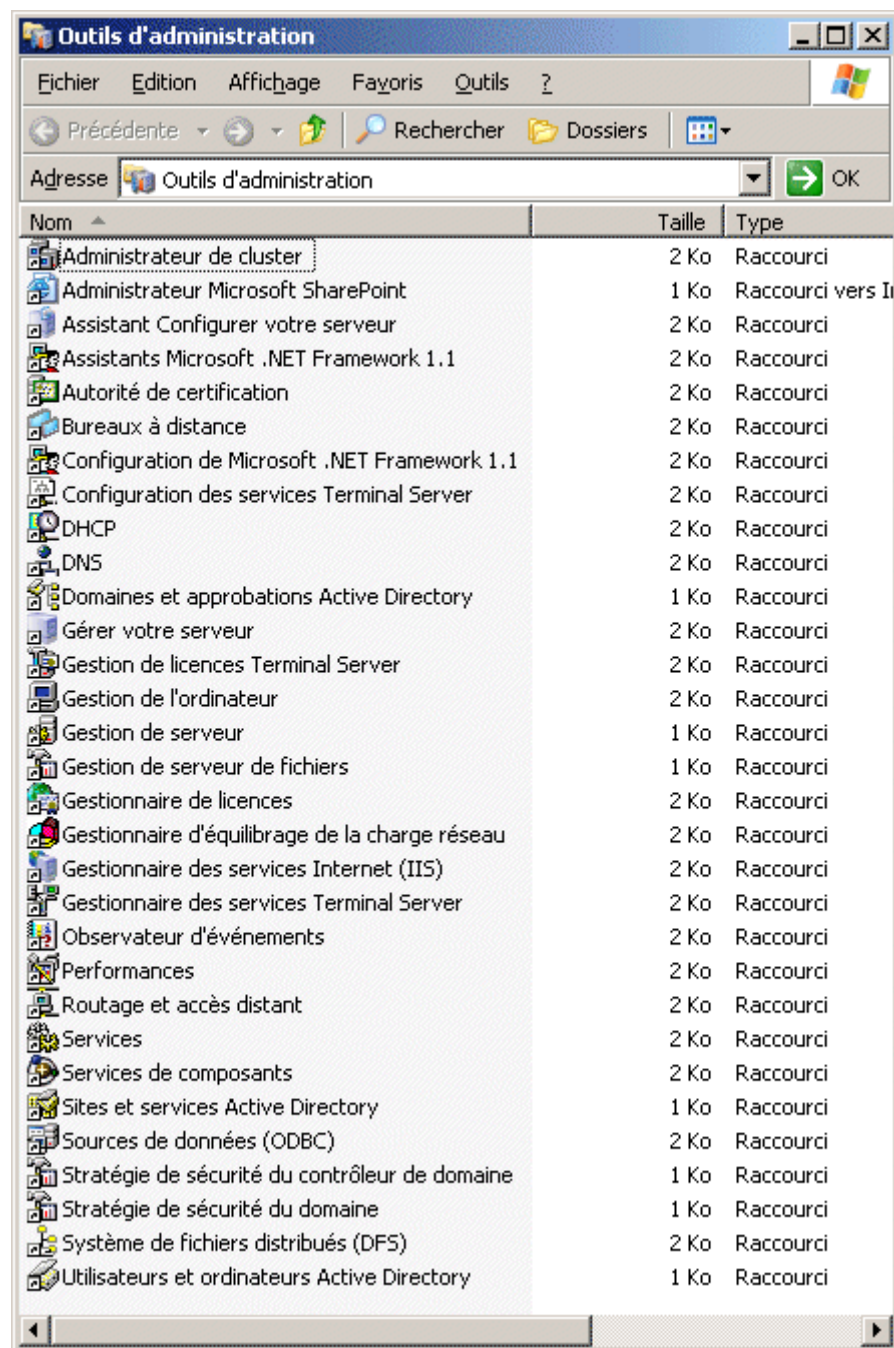
 L'utilisation de cette option supprimera tous les comptes locaux sur ce serveur.
Toutes les clés cryptographiques seront supprimées et doivent être exportées avant de continuer.

Toutes les données cryptées, comme par exemple les fichiers ou les courriers électroniques cryptés EFS doivent être décryptés avant de continuer, ou alors ils ne seront plus jamais accessibles.

< Précedent Suivant > Annuler



- 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.

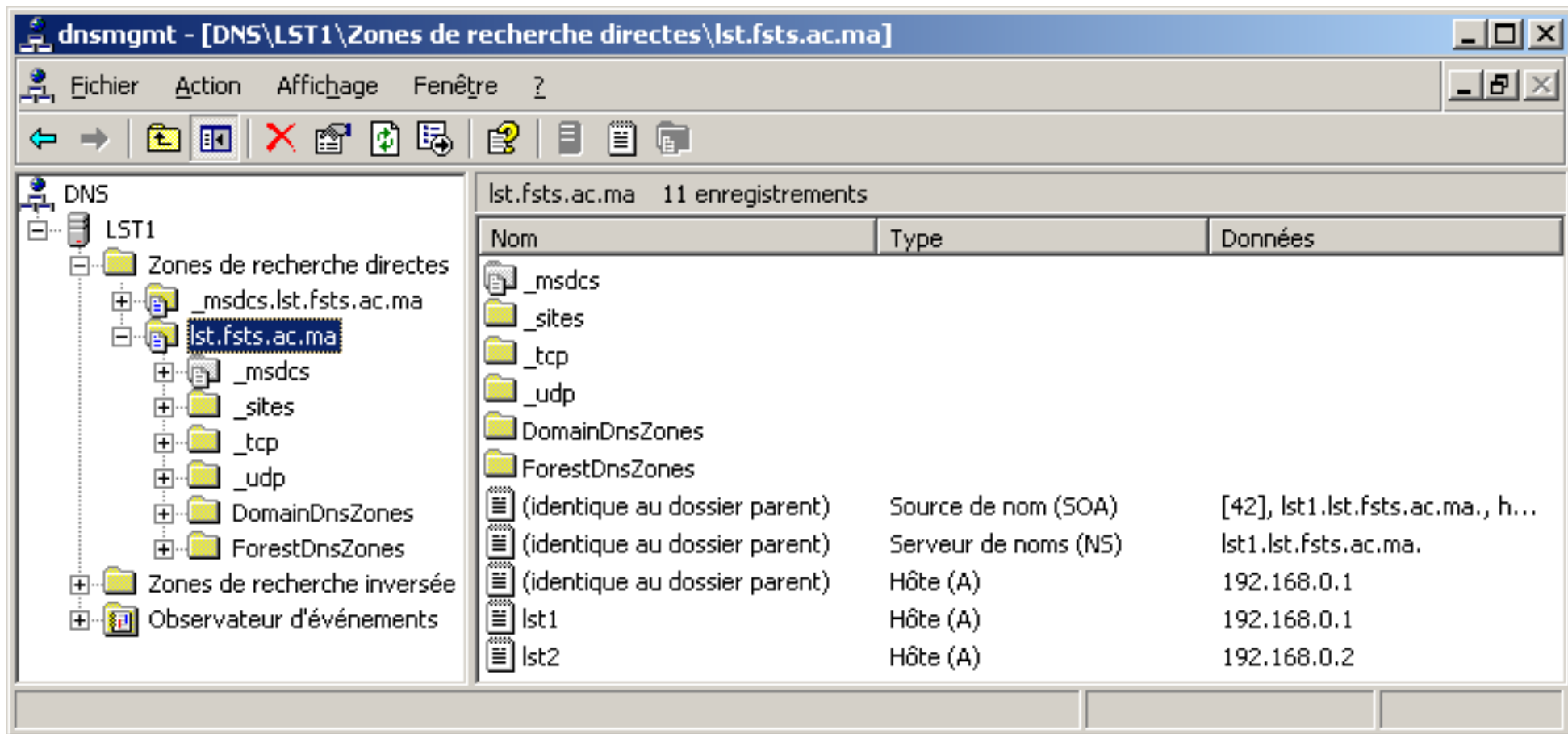


La configuration du service DNS comprend les étapes suivantes:

- 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.



The screenshot shows the DNS Management console window titled "dnsmgmt - [DNS\LST1\Zones de recherche directes\lst.fsts.ac.ma]". The left pane displays a tree view of the DNS hierarchy, with "lst.fsts.ac.ma" selected under "Zones de recherche directes". The right pane shows a table of 11 records for this zone.

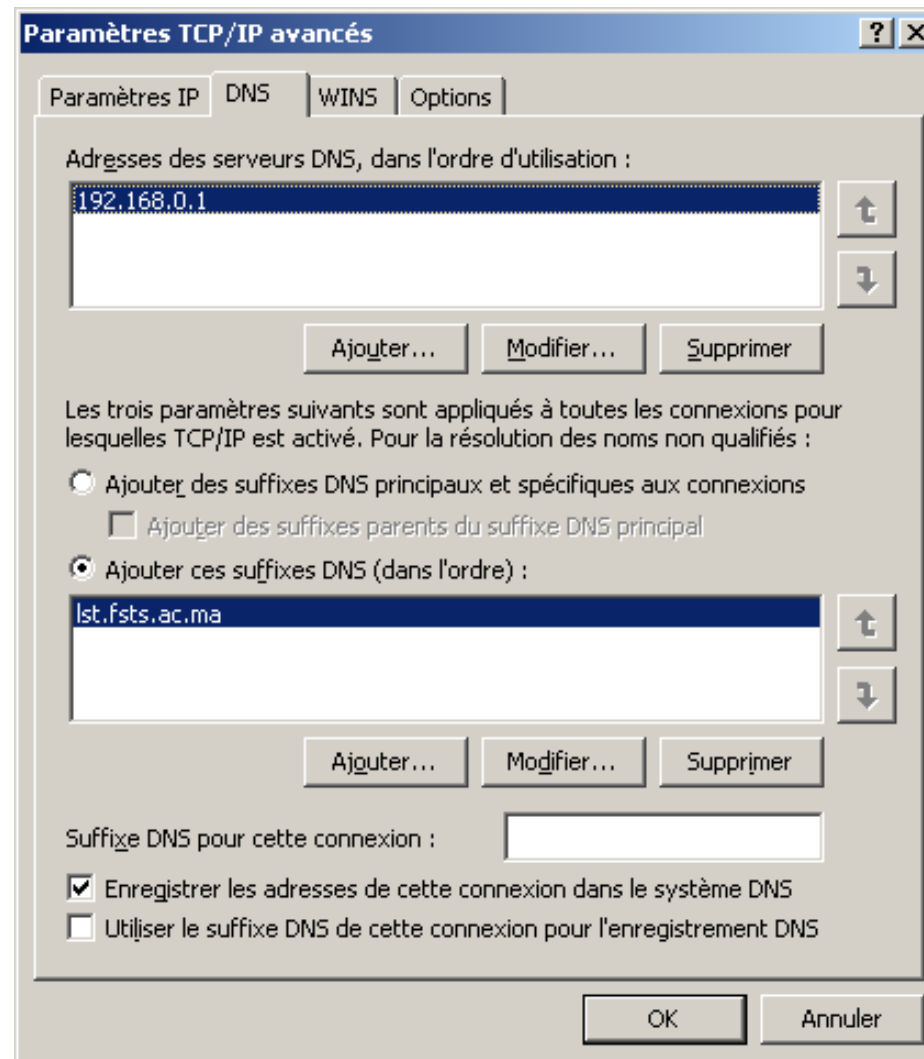
Nom	Type	Données
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(identique au dossier parent)	Source de nom (SOA)	[42], lst1.lst.fsts.ac.ma., h...
(identique au dossier parent)	Serveur de noms (NS)	lst1.lst.fsts.ac.ma.
(identique au dossier parent)	Hôte (A)	192.168.0.1
lst1	Hôte (A)	192.168.0.1
lst2	Hôte (A)	192.168.0.2

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

The screenshot shows the DNS Management console window titled "dnsmgmt - [DNS\LST1\Zones de recherche inversée\192.168.0.x Subnet]". The left pane shows the tree structure with "192.168.0.x Subnet" selected. The right pane displays a table of 4 records for this zone.

Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[17], lst1.lst.fsts.ac.ma., h...
(identique au dossier parent)	Serveur de noms (NS)	lst1.lst.fsts.ac.ma.
192.168.0.1	Pointeur (PTR)	lst1.lst.fsts.ac.ma.
192.168.0.2	Pointeur (PTR)	lst2.lst.fsts.ac.ma.

- 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

```
G:\WINDOWS\system32\cmd.exe - nslookup
```

```
G:\Documents and Settings\Administrateur.LST1>nslookup
```

```
Serveur par défaut : lst1.lst.fsts.ac.ma
```

```
Address: 192.168.0.1
```

```
> lst1
```

```
Serveur : lst1.lst.fsts.ac.ma
```

```
Address: 192.168.0.1
```

```
Nom : lst1.lst.fsts.ac.ma
```

```
Address: 192.168.0.1
```

```
> lst2
```

```
Serveur : lst1.lst.fsts.ac.ma
```

```
Address: 192.168.0.1
```

```
Nom : lst2.lst.fsts.ac.ma
```

```
Address: 192.168.0.2
```

```
> 192.168.0.2
```

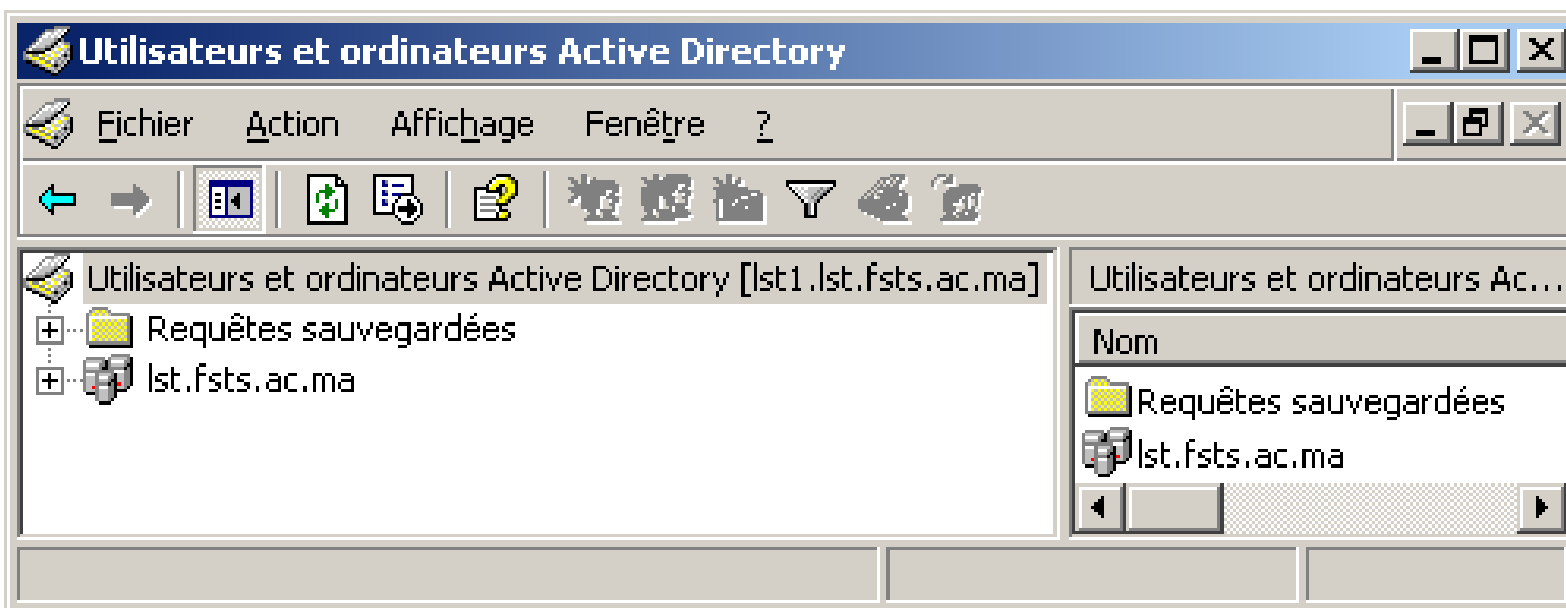
```
Serveur : lst1.lst.fsts.ac.ma
```

```
Address: 192.168.0.1
```

```
Nom : lst2.lst.fsts.ac.ma
```

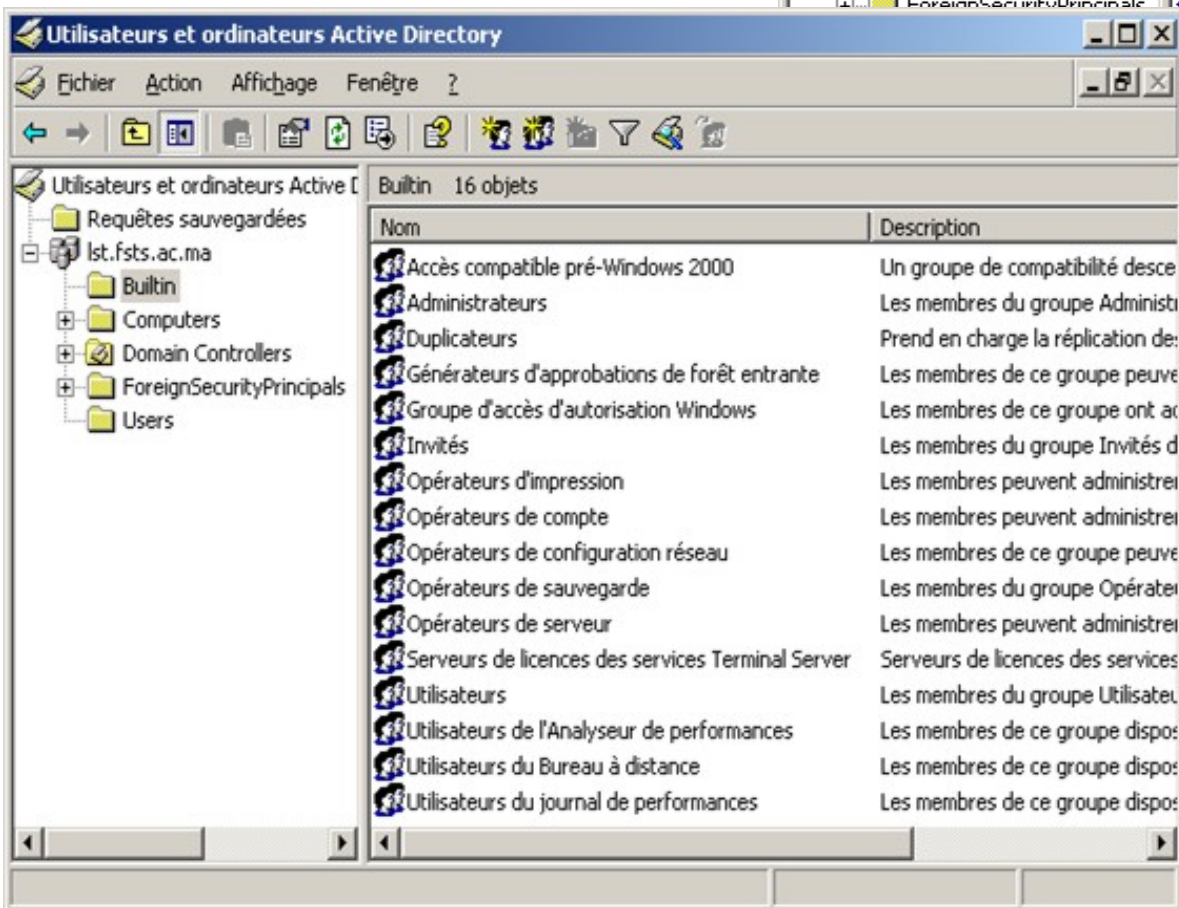
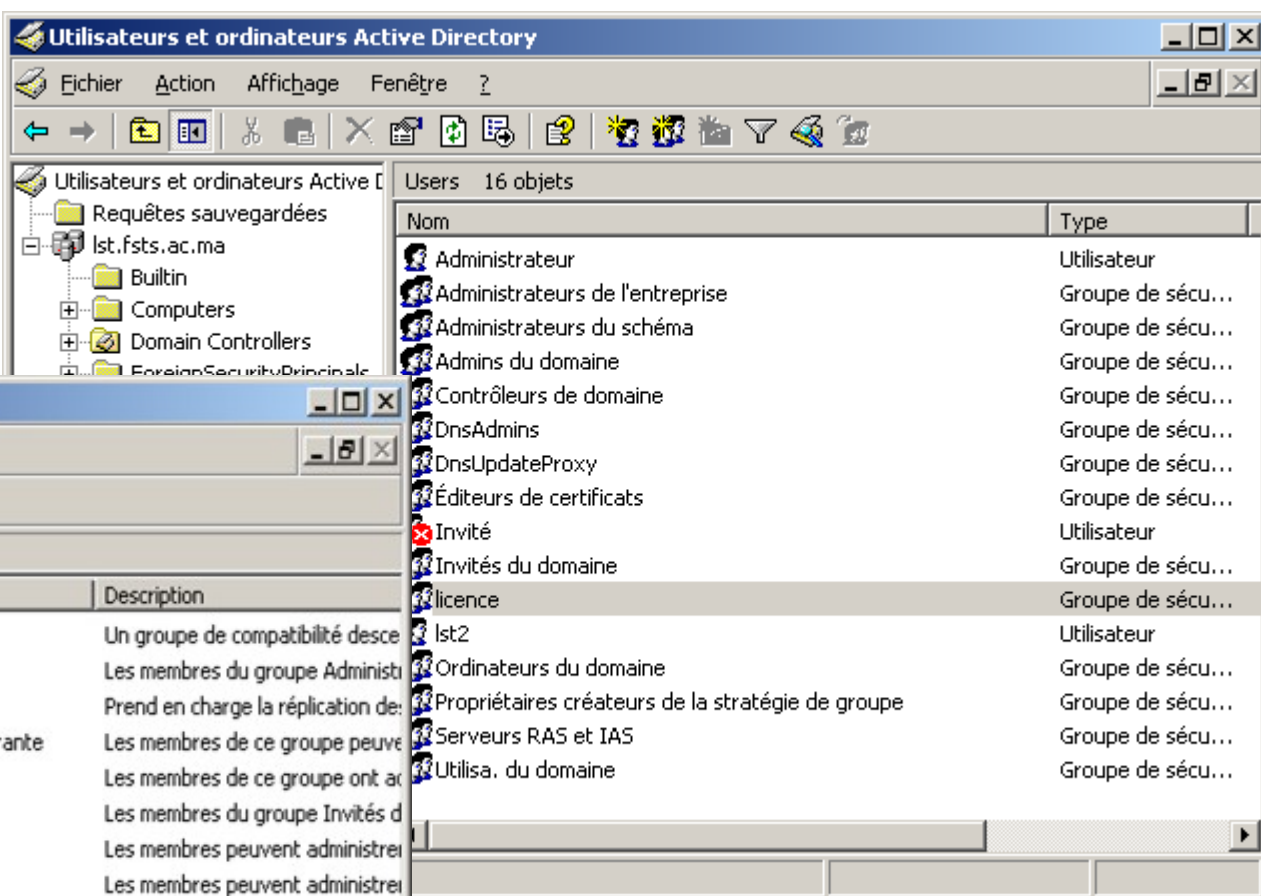
```
Address: 192.168.0.2
```

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

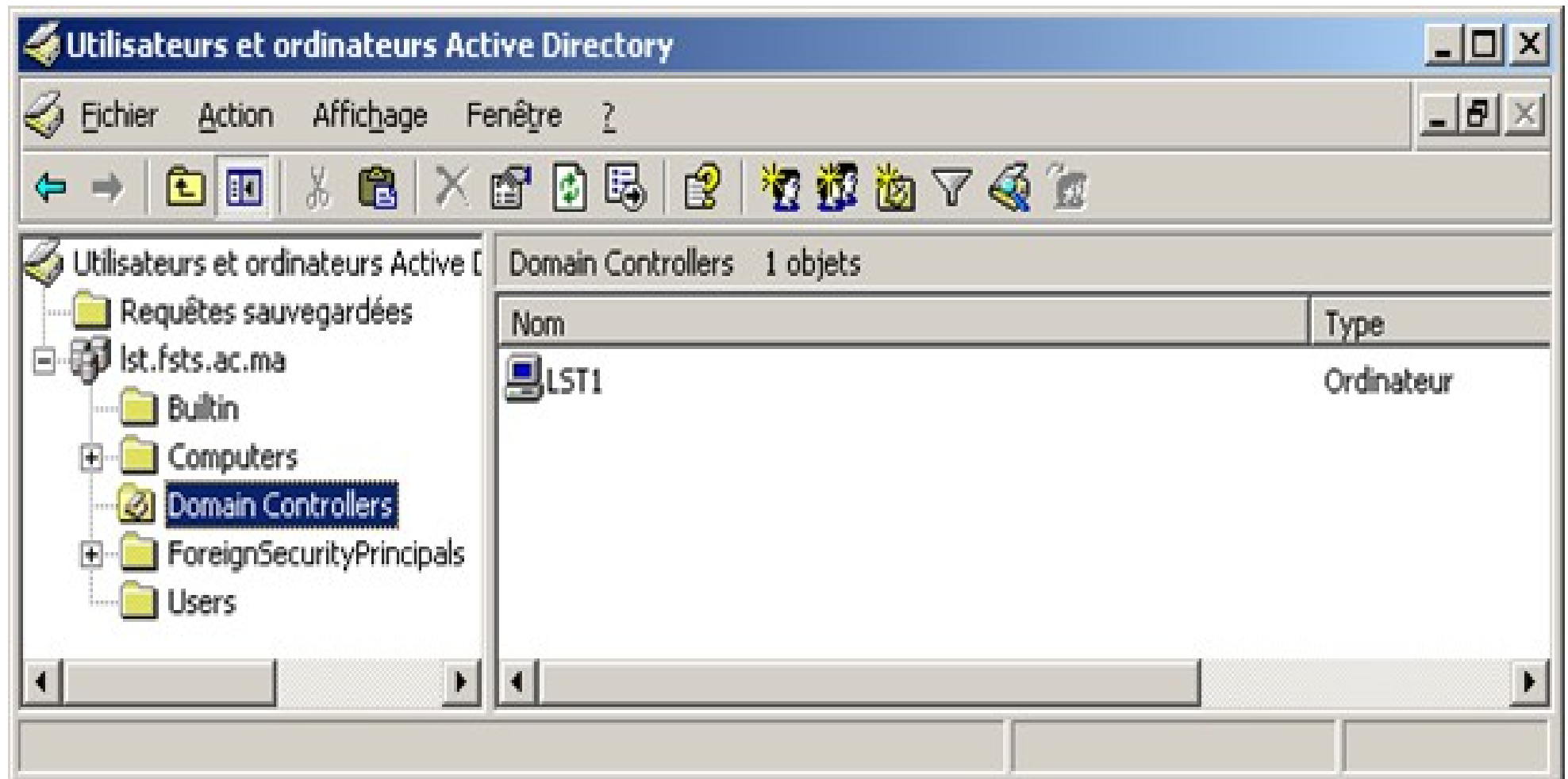


Cet outil réalise l'administration des utilisateurs, des groupes d'utilisateurs et des ordinateurs d'un domaine.

Il permet de créer un compte pour chacune des entités précédemment citées.



Contrôleur de domaine



Création d'un utilisateur:

Nouvel objet - Utilisateur

Créer dans : Ist.fsts.ac.ma/Users

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :
 @Ist.fsts.ac.ma

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : Ist.fsts.ac.ma/Users

Mot de passe :

Confirmer le mot de passe :

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais


Le compte est désactivé

< Précédent Suivant > Annuler

Création d'un groupe:

Propriétés de kamal lasfar

Environnement | Sessions | Contrôle à distance | Profil de services Terminal Ser
Général | Adresse | Compte | Profil | Téléphones | Organisation | Membre de

 kamal lasfar

Prénom : Initiales :

Nom :

Nom affiché :

Description :


Bureau :

Numéro de téléphone :

Adresse de messagerie :

Page Web :

Nouvel objet - Groupe

 Créer dans : lst.fsts.ac.ma/Users

Nom du groupe :

Nom de groupe (antérieur à Windows 2000) :

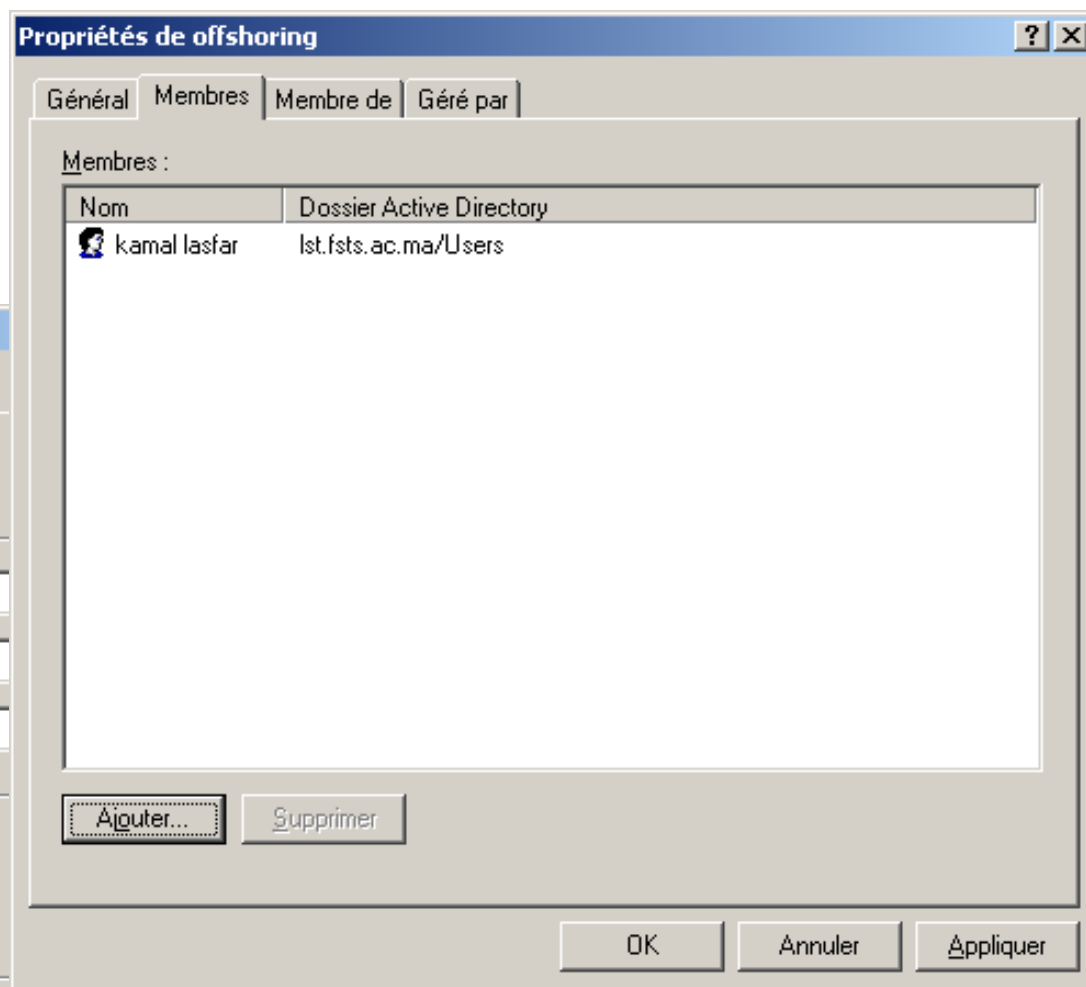
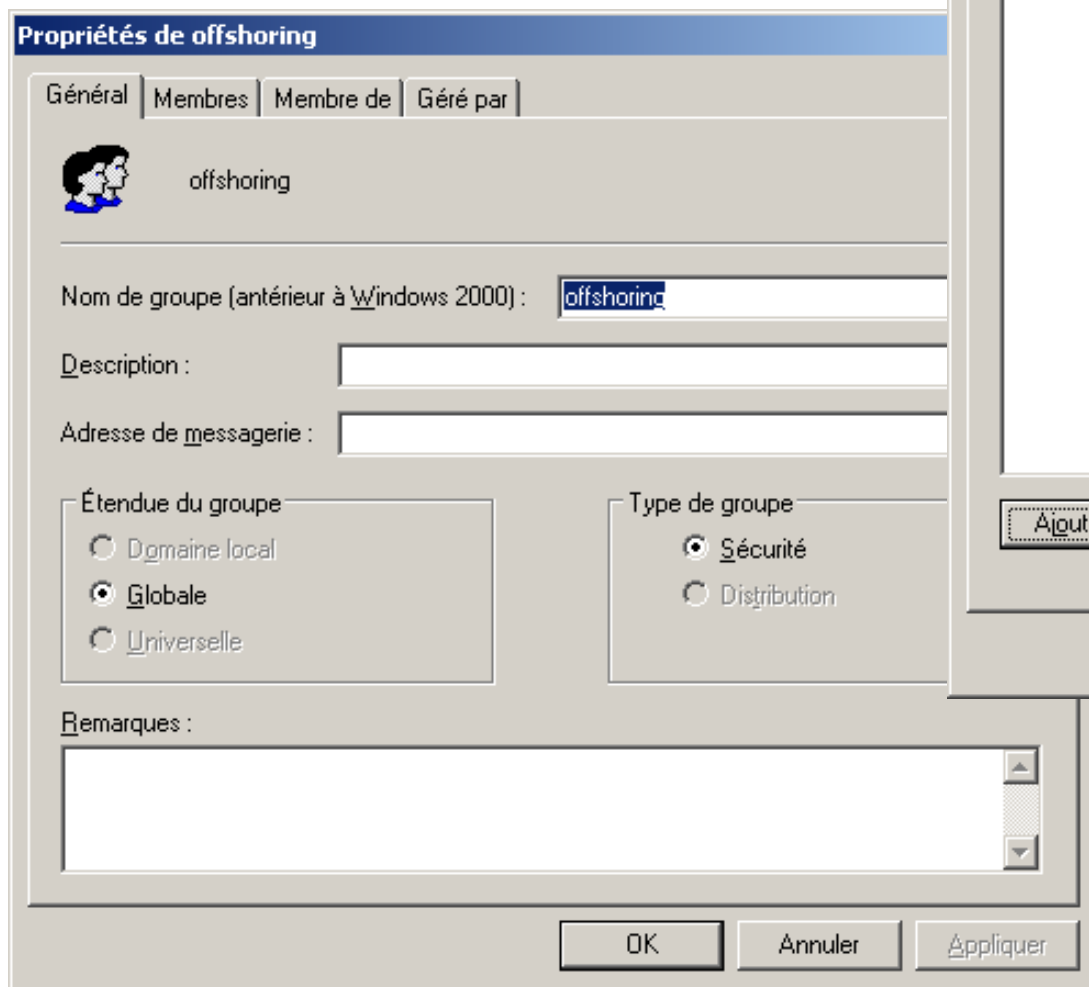
Étendue du groupe

- Domaine local
- Globale
- Universelle

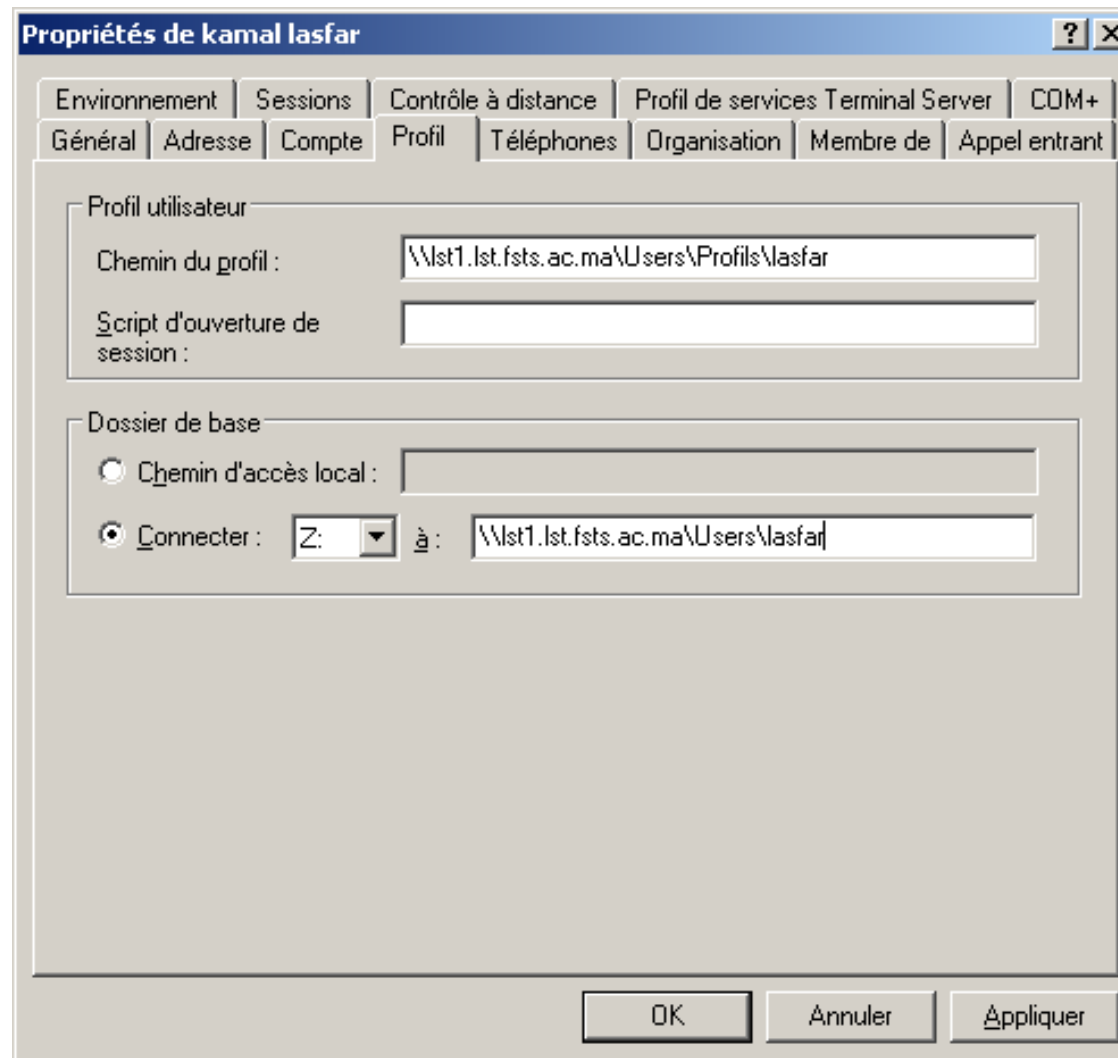
Type de groupe

- Sécurité
- Distribution

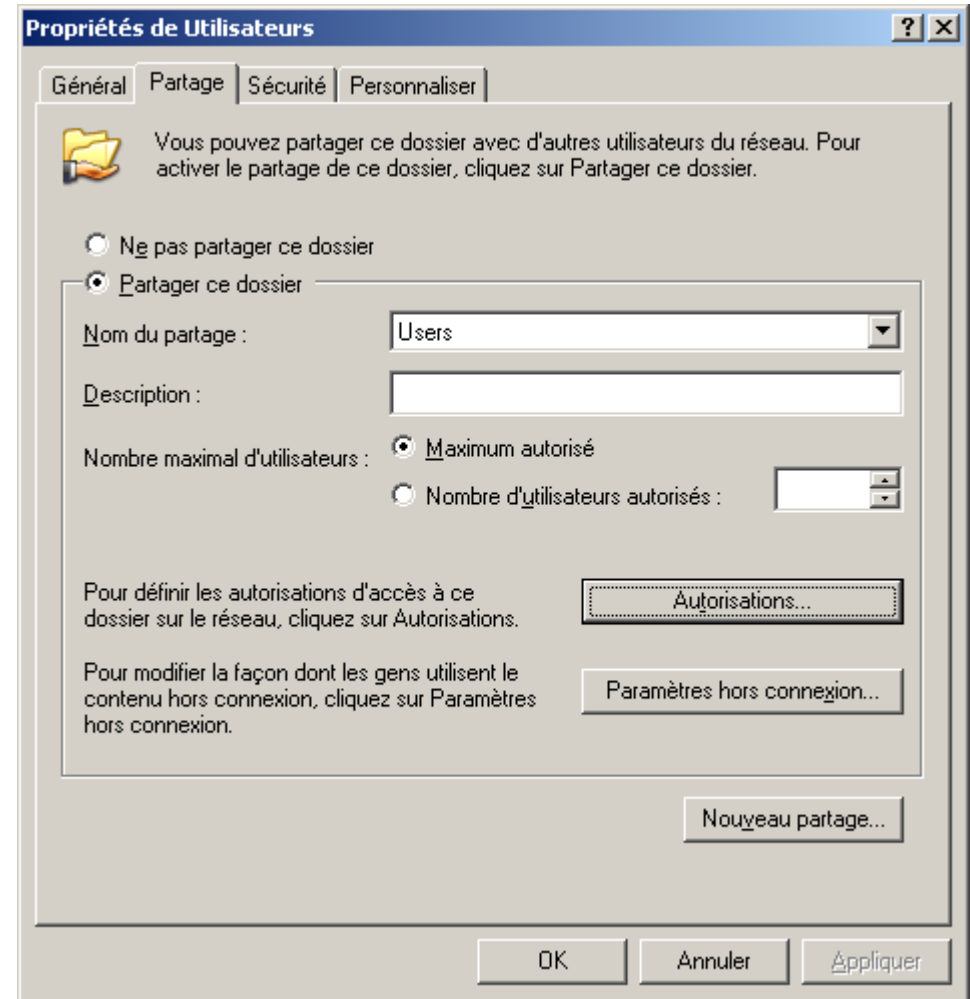
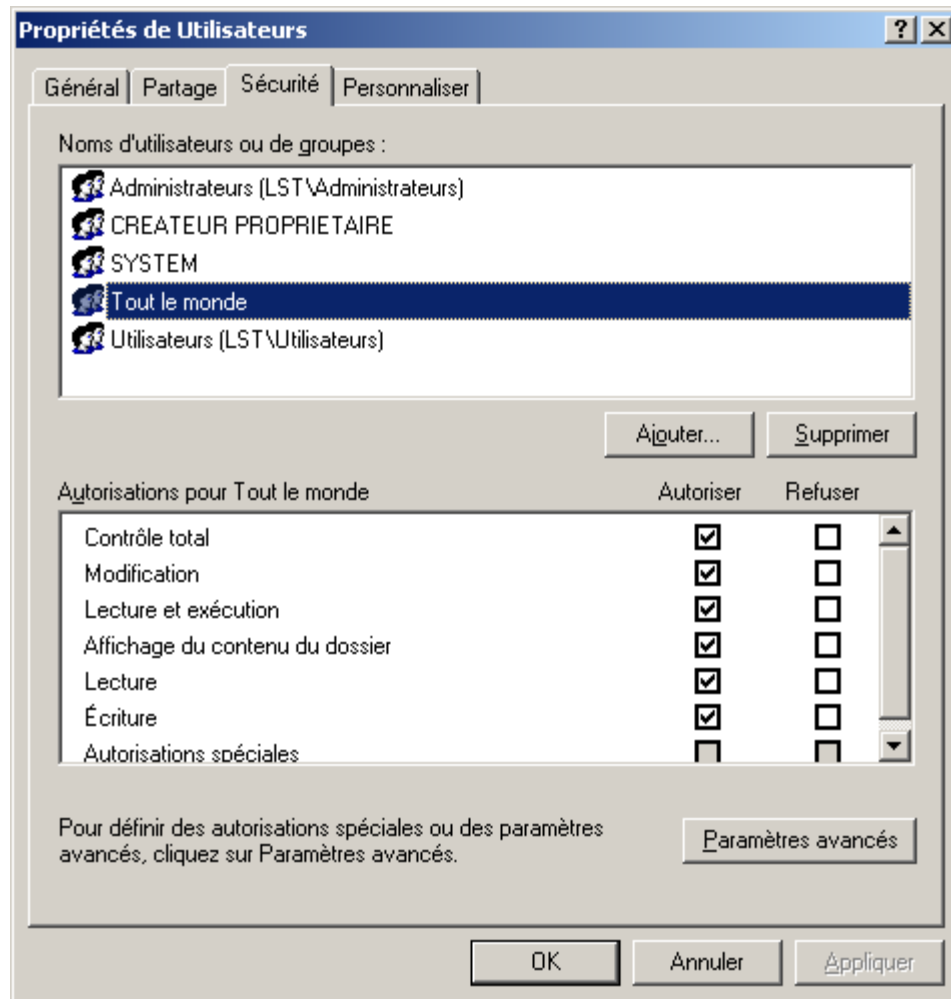
Propriété d'un groupe:

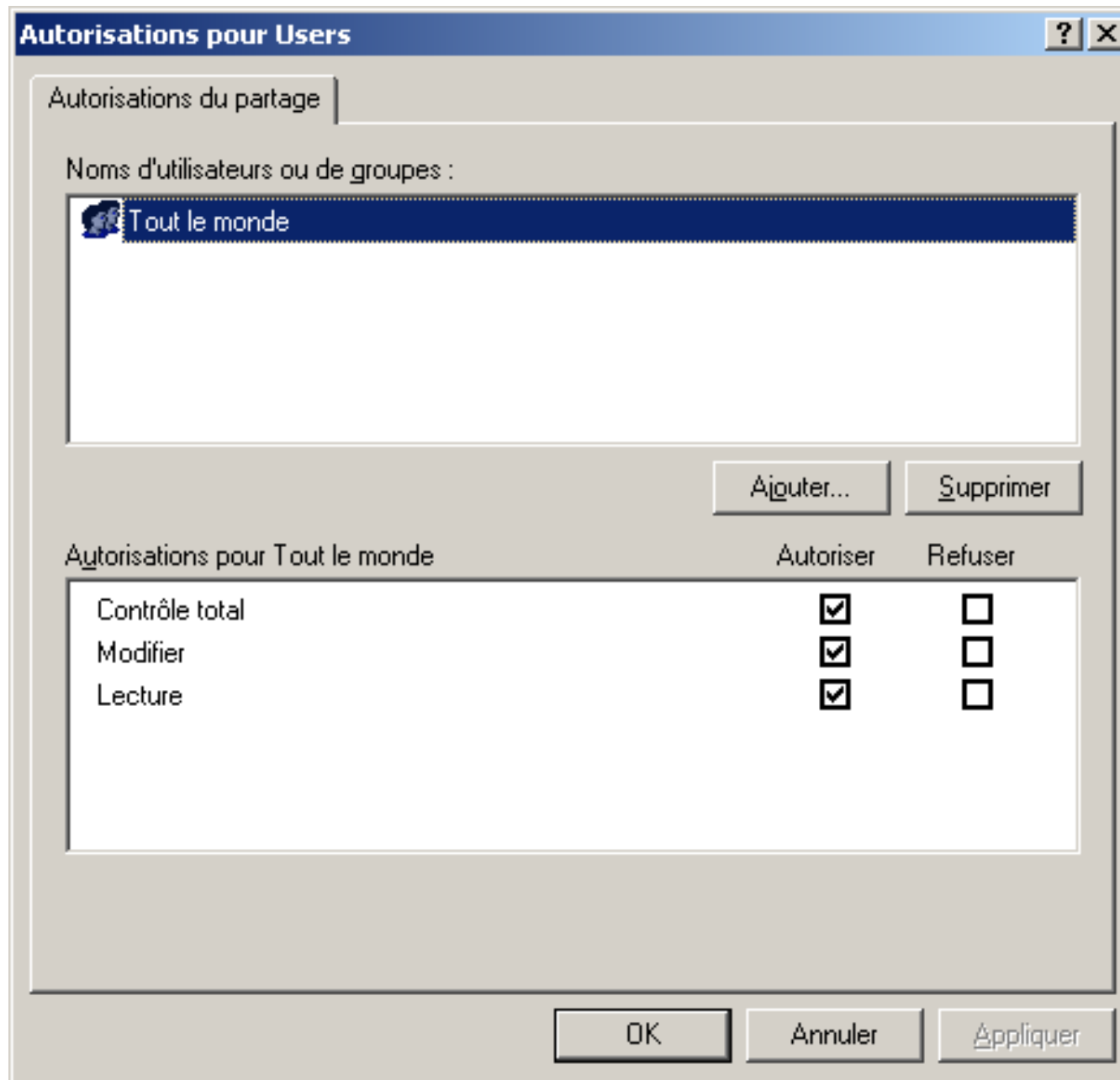


- Il est possible d'affecter un répertoire pour héberger les répertoires de base et les profils itinérant en allant dans le menu d'un utilisateur dans sa section 'Profils' ;

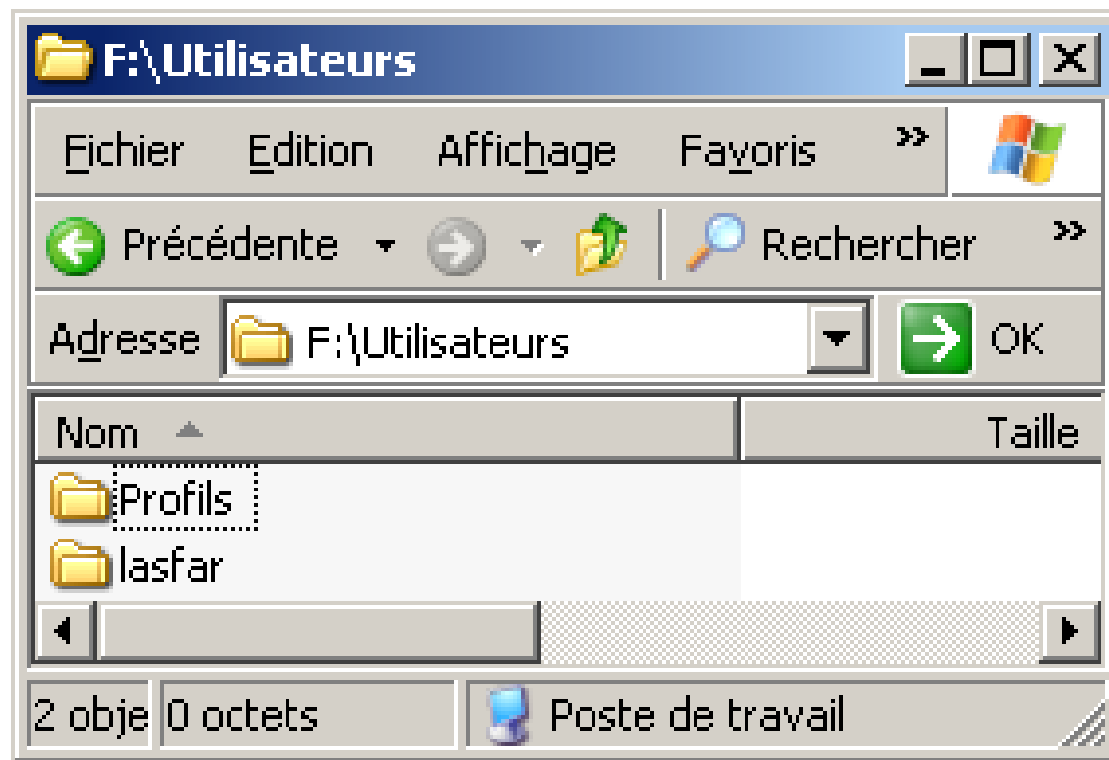


- Il faut ensuite partager ce répertoire sous le nom 'Users' et configurer les autorisations sur le répertoire ainsi que sur le partage ;





- 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 ordinateur passe par les étapes suivantes:

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

Nouvel objet - Ordinateur

Créer dans : Ist.fsts.ac.ma/Computers

Nom de l'ordinateur :
Ist3

Nom d'ordinateur (antérieur à Windows 2000) :
LST3

L'utilisateur ou le groupe suivant peut joindre cet ordinateur à un domaine.
Utilisateur ou groupe :
Par défaut : Admins du domaine [Modifier...]

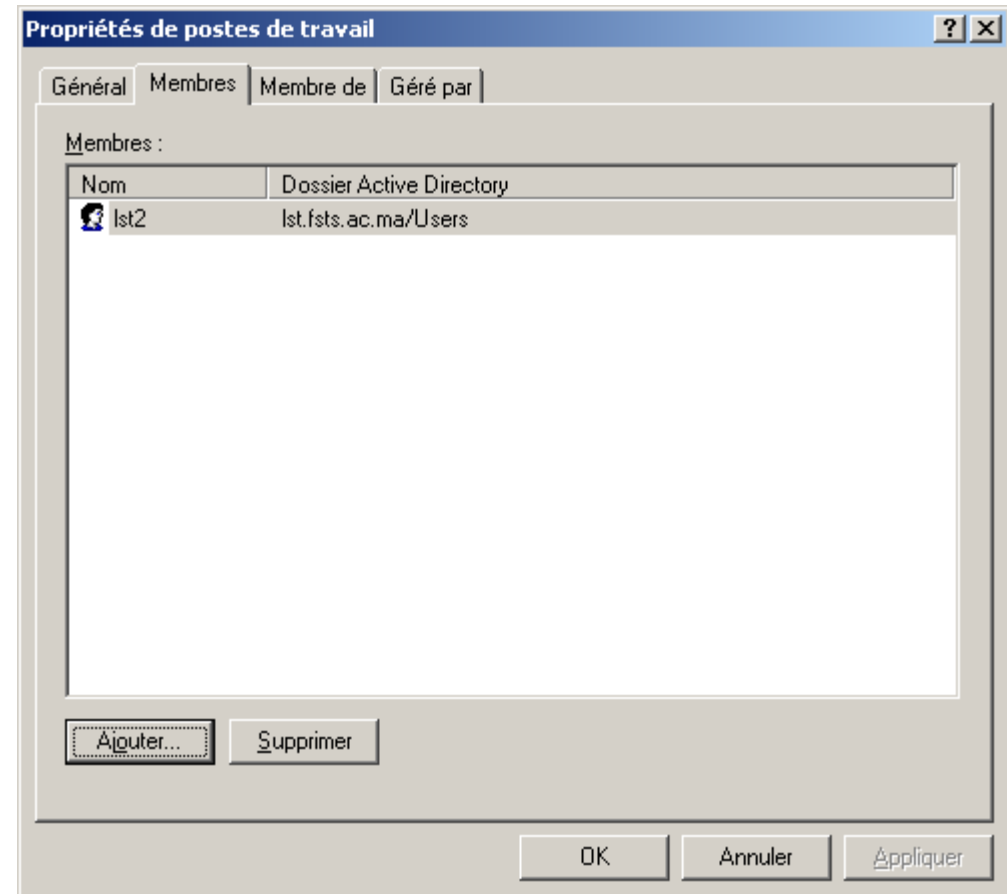
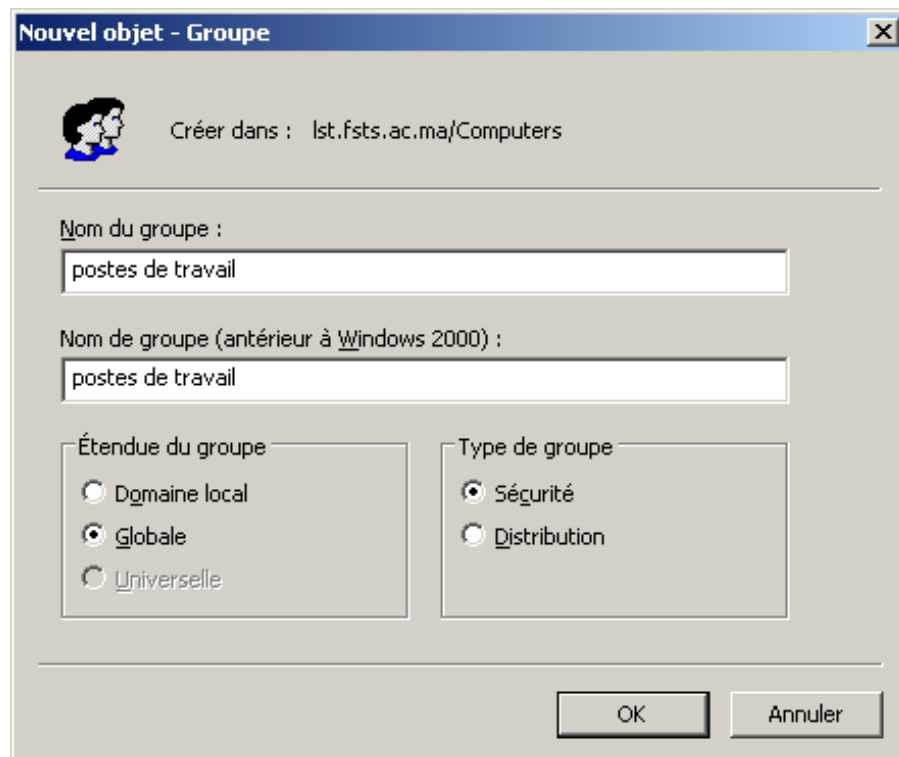
Attribue ce compte d'ordinateur à un ordinateur antérieur à Windows 2000

Attribue ce compte d'ordinateur à un contrôleur de domaine secondaire

< Précédent Suivant > Annuler

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

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



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