

Active Directory

*Stage personnes ressources réseau en établissement
janvier 2004*

Formateur : Franck DUBOIS

SOMMAIRE

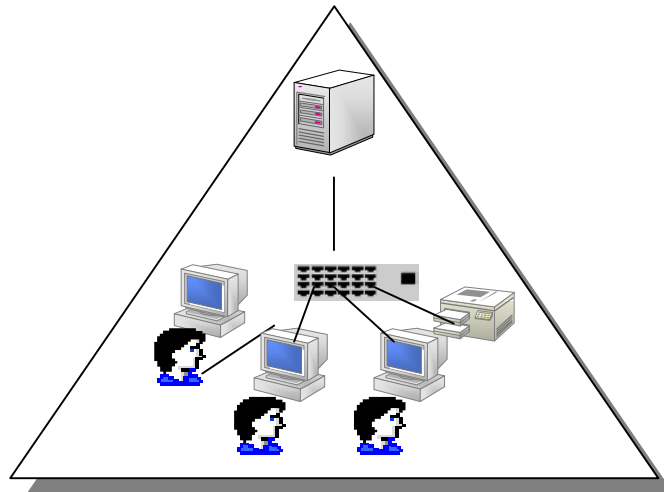
1	Le réseau administré.....	3
1.1	Le domaine	3
1.2	Les utilisateurs et leurs droits.....	3
2	Les domaines Windows 2000.....	4
2.1	Principes de base	4
2.2	Exemple de forêt.....	4
3	Qu'y a-t-il dans un domaine Active Directory ?	5
3.1	Des serveurs.....	5
3.2	Contrôleurs de domaine.....	5
3.3	Des "clients" : stations, imprimantes, etc.....	5
3.4	Des utilisateurs	5
3.5	Des groupes	5
3.6	Des stratégies de groupe.....	5
3.7	Des Unités d'organisation	5
4	Active Directory et DNS	6
5	Installation du Active Directory	6
5.1	Création d'une forêt qui ne contiendra qu'un arbre qui lui-même sera formé d'un seul domaine sans enfant.	6
5.2	Ajout d'un contrôleur de domaine supplémentaire.	10

1 Le réseau administré

Un réseau administré est obligatoirement de type client serveur.

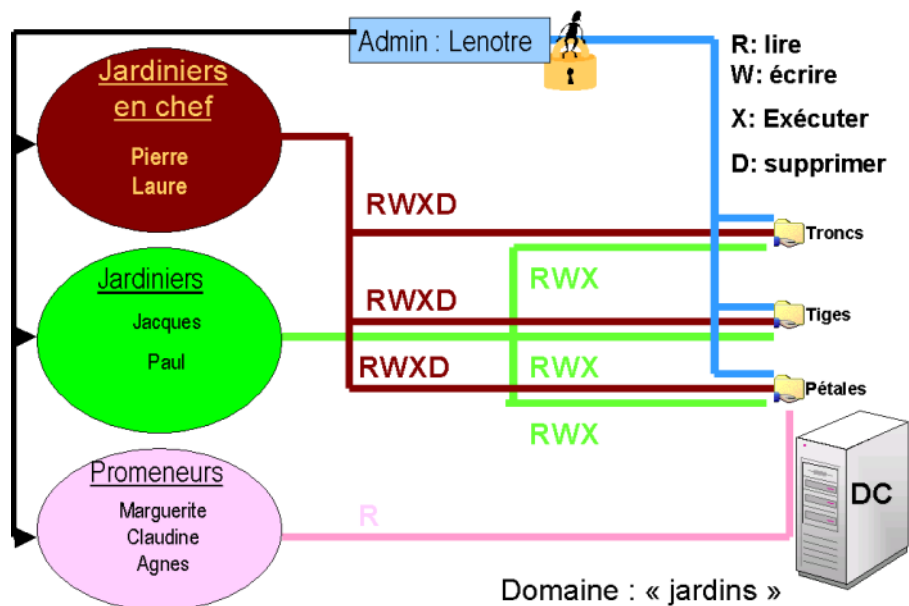
1.1 Le domaine

Un domaine regroupe des ordinateurs, des périphériques, des utilisateurs. C'est une sorte de zone sécurisée, sur laquelle on ne peut pénétrer que quand on a été authentifié par le Contrôleur de Domaine.



Chaque **utilisateur** (ou **groupe d'utilisateurs**) est un objet, chaque objet a un **compte** géré par le **Contrôleur de Domaine** ou *Domain Controller* et enregistré dans une base de données, la **SAM** (*Security Account Management*) qui contient son **SID** (*Security Identifier*), un numéro d'identité qui lui est propre.

1.2 Les utilisateurs et leurs droits



2 Les domaines Windows 2000

2.1 Principes de base

Active Directory gère de manière hiérarchisée un certain nombre **d'objets** situés dans des **domaines** et organisés selon un **schéma**.

Ces objets peuvent être des serveurs, des stations, des périphériques, des dossiers partagés, des utilisateurs, des groupes d'objets (groupes locaux, groupes globaux), des **Unités d'Organisation** (conteneurs dans lesquels les administrateurs rangent différents objets).

Un **arbre** est un ensemble de domaines contigus.

Une **forêt** est un ensemble d'arbres.

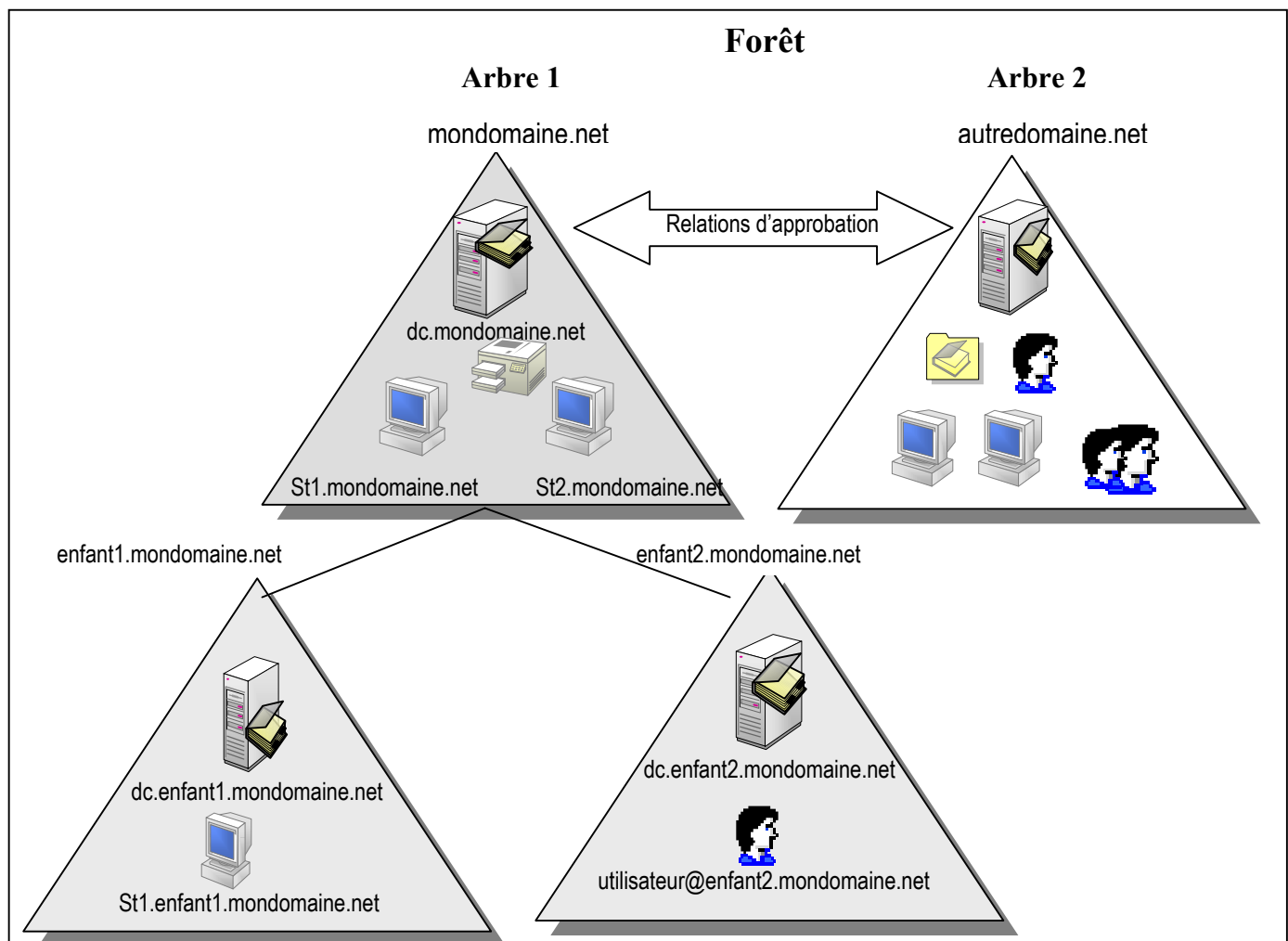
Un objet d'un domaine appartenant à un arbre ne peut pas communiquer avec un domaine d'un autre arbre sauf si des relations d'approbation ont été établies

Active directory s'appuyant sur **DNS**, le nommage des objets est du type **FQDN** (*Fully Qualified Domain Name* = nom de domaine pleinement qualifié, comme pour Internet).

Chaque domaine possède un ou plusieurs Contrôleur de Domaine (*Domain Controller*).

Remarque : dans la plupart des cas, le réseau d'un établissement scolaire sera limité à un seul domaine.

2.2 Exemple de forêt



3 Qu'y a-t-il dans un domaine Active Directory ?

Des **objets**, qui peuvent être...

3.1 Des serveurs.

Il y a plusieurs types de serveurs



Serveurs Membres : simples serveurs auxquels on attribue une tâche définie :

- serveurs de fichiers, destinés à stocker des documents,
- serveurs d'applications, sur lesquels sont installées les applications à exécuter à partir des stations
- serveurs d'impressions, qui gèrent les imprimantes

3.2 Contrôleurs de domaine



Ils sont les seuls habilités à authentifier les utilisateurs qui se connectent au domaine Ils remplissent plusieurs fonctions importantes.

Il est intéressant de disposer de plusieurs contrôleurs de domaines : répartition des services, réplication des données pour qu'un contrôleur en panne soit remplacé par un autre.

C'est l'installation d'Active Directory qui fait d'un serveur un Contrôleur de Domaine.

3.3 Des "clients" : stations, imprimantes, etc.



Seules les stations Windows 2000 et Windows XP bénéficient de toutes les fonctionnalités d'Active Directory. Un utilisateur (sous Win9x) peut ouvrir une session sur le domaine, mais la station n'est pas un objet du domaine.

3.4 Des utilisateurs



Chaque utilisateur a un certain nombre d'attributs et son propre UID (User Identity : Un numéro de code qui lui permet d'être identifié sur le domaine. Son UPN (User Principal Name) est du type utilisateur@mondomaine.local

3.5 Des groupes



Les groupes peuvent contenir des utilisateurs, des ordinateurs et d'autres groupes. Les groupes simplifient la gestion d'un grand nombre d'objets.

3.6 Des stratégies de groupe



Elles définissent le comportement du domaine pour tel ou tel utilisateur ou groupe d'utilisateurs ou ordinateurs.

Vous les utiliserez pour « gérer » les stations Windows 2000 ou XP, mais pas win9x

3.7 Des Unités d'organisation



Vous créez des unités d'organisation pour ranger des objets dans une hiérarchie logique et ordonnée.

Les différents OU ne contiennent pas des dossiers et des fichiers, mais des ordinateurs, des utilisateurs, des groupes d'utilisateurs, des imprimantes, etc. ...

Ce sont donc des conteneurs d'objets destinés à l'administration, pas des groupes d'utilisateurs !

4 Active Directory et DNS

Le DNS est indispensable à la configuration de Active Directory. Devez-vous utiliser le serveur DNS de Microsoft pour prendre en charge Active Directory ? La réponse est non. Microsoft recommande (évidemment!!!) d'utiliser son DNS qui s'intègre à l'Active Directory. Active Directory est intégré au DNS de la façon suivante :

1. Active Directory et DNS ont la même structure hiérarchique.

Même s'ils sont séparés et implémentés différemment pour des raisons diverses, les espaces de noms d'une organisation pour DNS et pour Active Directory ont une structure identique. Par exemple, *mpg.local* est un domaine DNS et un domaine Active Directory.

2. Les zones DNS peuvent être stockées dans Active Directory.

Si vous utilisez le service DNS Windows 2000, vous pouvez stocker les fichiers de la zone principale dans Active Directory en vue d'une réplication sur d'autres contrôleurs de domaine Active Directory.

3. Les clients Active Directory utilisent DNS pour rechercher des contrôleurs de domaine.

Pour rechercher un contrôleur de domaine pour un domaine spécifique, les clients Active Directory interrogent leur serveur DNS configuré et lui demandent des enregistrements de ressources spécifiques ; ils interrogent les enregistrements SRV.

Les ordinateurs Windows 2000 peuvent enregistrer et mettre à jour dynamiquement les enregistrements avec un serveur DNS prenant en charge le protocole de mise à jour DNS dynamique. Qu'en est-il des clients de bas niveau (comme Windows 9x ou Windows NT) et les clients autres que Microsoft ne pouvant pas enregistrer dynamiquement leurs enregistrements de ressources ?

Nous pouvons, pour ces clients, utiliser la capacité du serveur DHCP Windows 2000 à enregistrer dynamiquement les enregistrements de ressources DNS.

5 Installation d' Active Directory

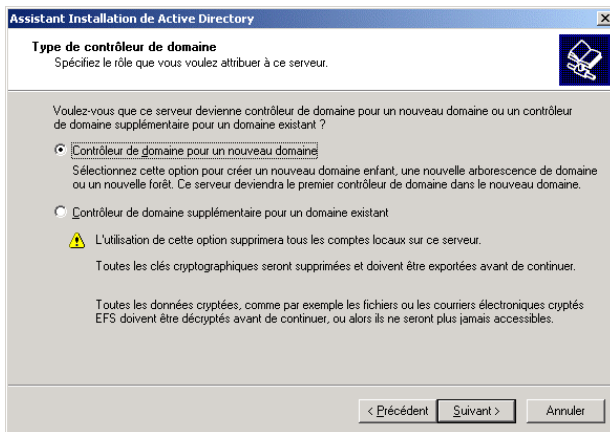
L'installation d'AD crée un contrôleur de domaine, une arborescence de domaine et une forêt d'arborescence de domaines.

5.1 Création d'une forêt qui ne contiendra qu'un arbre qui lui-même sera formé d'un seul domaine sans enfant.

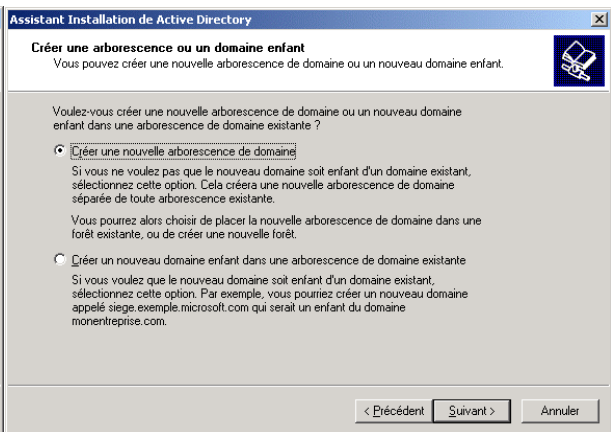
Menu Démarrer / Exécuter, taper dcpromo

L'**Assistant Installation de Active Directory** installe et configure les composants qui fournissent le service d'annuaire Active Directory aux utilisateurs et aux ordinateurs du réseau.

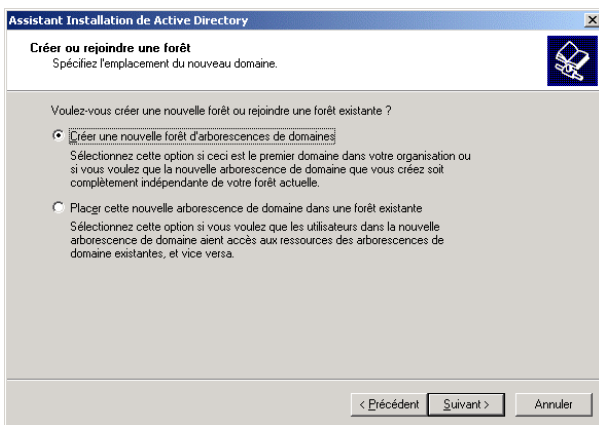




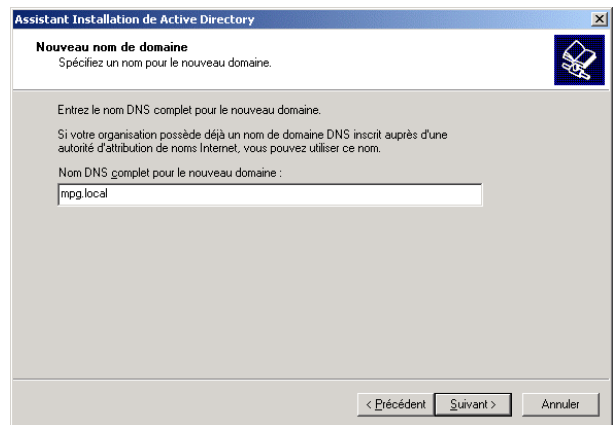
Nous désirons que ce serveur devienne contrôleur de Domaine pour un nouveau domaine



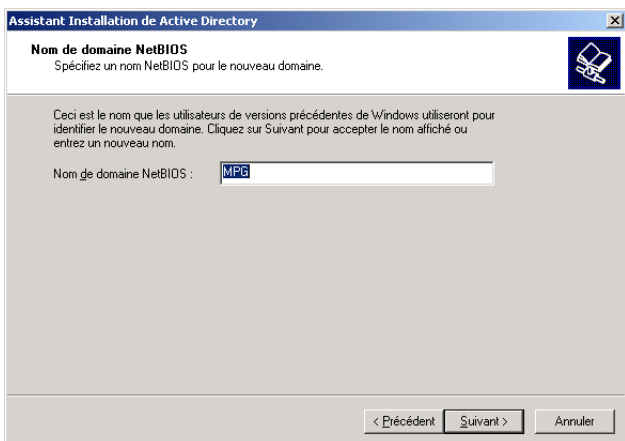
Votre serveur constitue le premier domaine (et le seul!!!) de votre organisation. Créez une nouvelle arborescence de domaine.



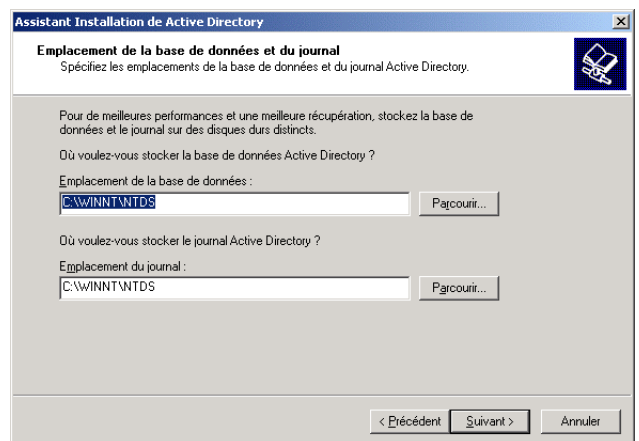
Vous allez créer évidemment une nouvelle forêt.



Vous devez entrer votre nom de domaine. On doit entrer le nom complet qui se trouve dans le DNS



Un nom de domaine NetBIOS vous sera proposé par défaut. Acceptez-le. Il représente la première partie de votre nom de domaine tel que défini au DNS. Le serveur WINS utilise également ce nom.

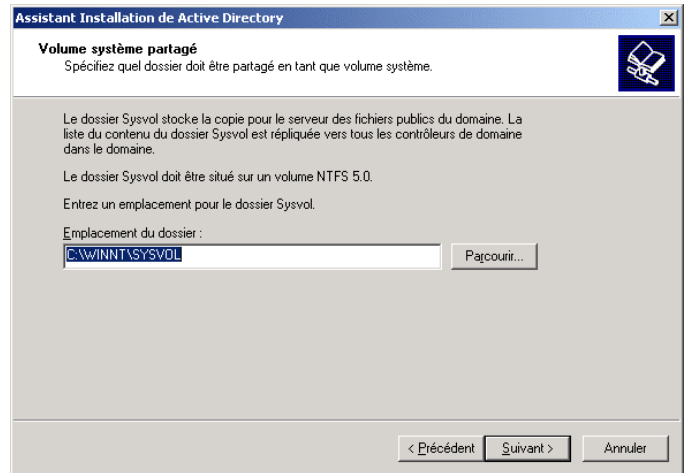


Il serait préférable de conserver ces fichiers sur un disque différent (au moins 300 Mo) afin d'améliorer la performance. Dans notre cas garder l'emplacement par défaut.

Vous avez maintenant la possibilité de modifier l'emplacement du répertoire partagé qui stocke la copie serveur des fichiers publics du domaine.

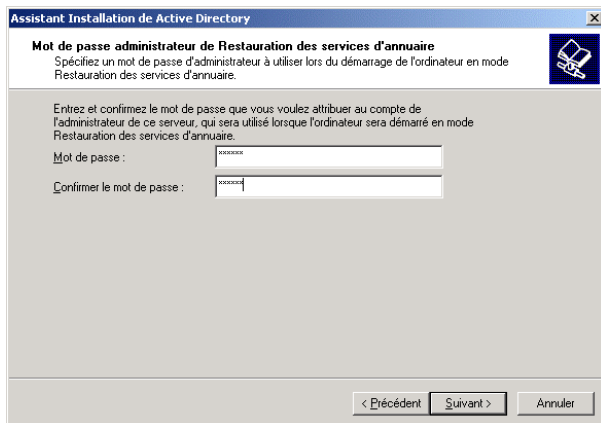
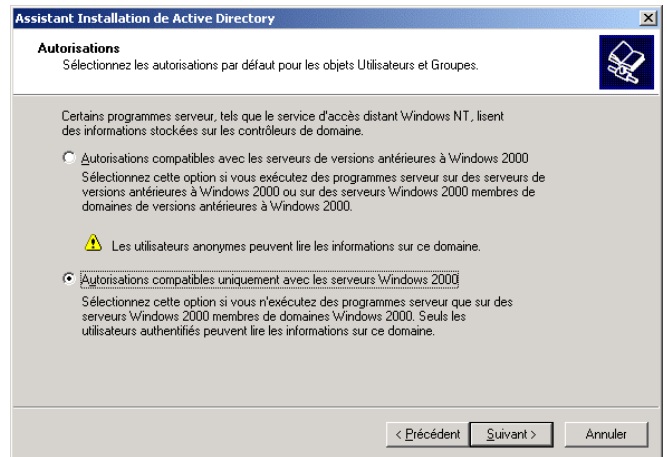
Ce dossier permet d'enregistrer les scripts qui font partie des objets Stratégie de groupe pour le domaine courant et le réseau de l'entreprise.

Le répertoire par défaut est \SYSVOL

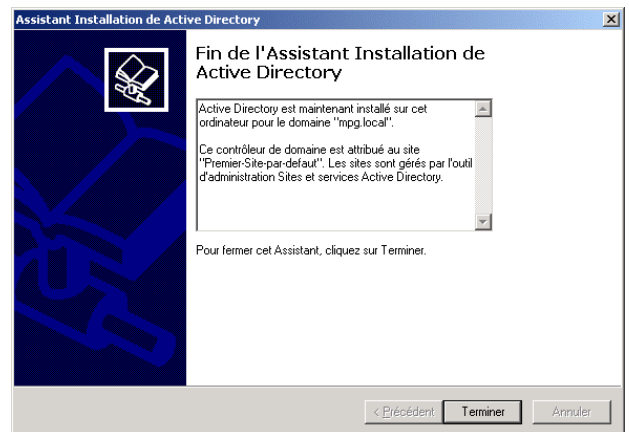


Windows 2000 Server assure une compatibilité avec les versions précédentes de Windows. L'assistant vous offre le choix entre une compatibilité avec ces anciennes versions ou une compatibilité uniquement avec les ordinateurs Windows 2000 (serveur et professionnel).

On parlera de **mode mixte** pour des environnements Windows 2000 et Windows NT qui coexistent. Dans un environnement qui ne contiendra que des ordinateurs Windows 2000 on parlera de **mode natif**. Choisissez le **mode natif**



Entrez et confirmez le mot de passe que vous voulez attribuer au compte de l'administrateur de ce serveur.



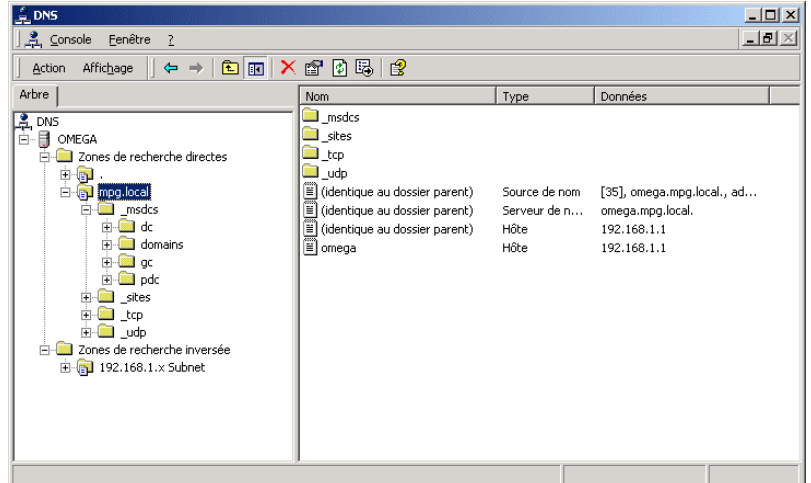
Vous avez installé votre premier Active Directory Windows 2000.

Vérifications

La console DNS apparaît maintenant comme ceci. Les 4 conteneurs supplémentaires correspondent à AD.

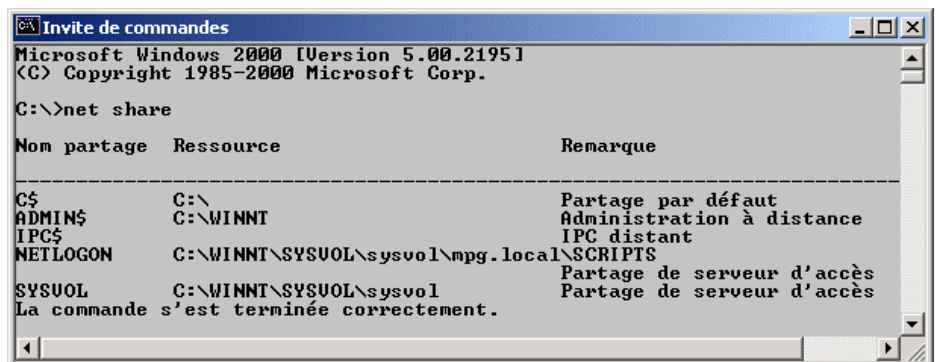
Mais vous pouvez vérifier que tous les éléments sont bien installés

Vérifiez que le dossier winnt\sysvol contient bien ceci



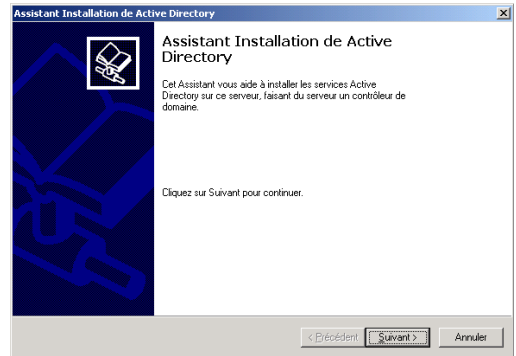
Dans une invite de commande tapez net share pour voir la liste des partages

Les partages NETLOGON et SYSVOL doivent y apparaître.

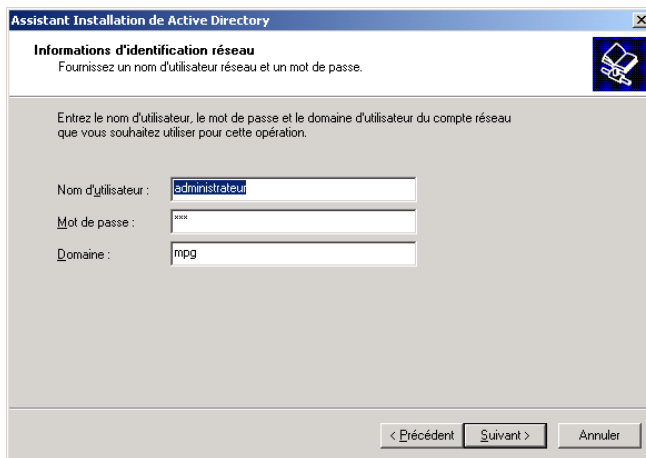
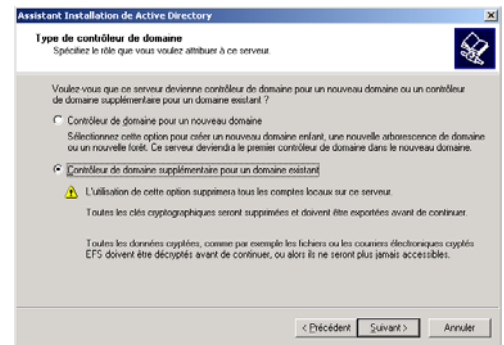


5.2 Ajout d'un contrôleur de domaine supplémentaire.

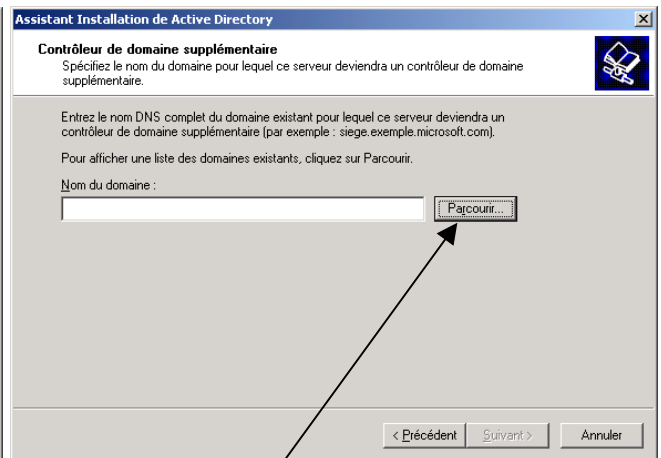
Menu Démarrer / Exécuter, taper dcpromo
L'Assistant Installation de Active Directory installe et configure les composants qui fournissent le service d'annuaire Active Directory aux utilisateurs et aux ordinateurs du réseau



Nous désirons que ce serveur devienne un contrôleur de Domaine supplémentaire pour un domaine existant.



Saisir le nom d'utilisateur et le mot de passe du Domaine existant.



Rechercher le domaine existant à l'aide de l'option Parcourir.

Pour la fin de l'ajout du domaine supplémentaire voir page 7/10.