Installation Windows 2000 Server

1. **Objectif**
   Ce document donne une démarche pour l'installation d'un serveur Windows 2000, d'un serveur DNS et d'un contrôleur de domaine (DC), en regard de certains éléments de sécurité. Les flèches (↳) indiquent les choix pour l'installation du premier DC dans un nouveau domaine

2. **Installation de Windows 2000 Server** Lors de l'installation, la machine doit être déconnectée du réseau. En effet, il est préférable de sécuriser la machine avant de la mettre en ligne. Par contre, elle sera connecter à un *hub* afin d'activer la couche Ethernet. Cela évite de devoir rebooter lors de changement d'adresses IP.

2.1. Formatage des HD
Tous les disques durs de la machine sont formatés en *NTFS* . En effet, le système *FAT* ne permet pas la gestion des autorisations d'accès aux ressources.
C: est le disque *système*.

2.2. Personnalisez votre logiciel
Nom : Entrez, par exemple le nom de votre établissement
Organisation : Education Nationale

2.3. Modes de licence

- ↳ Par serveur : Chaque connexion doit avoir sa propre licence d'accès. (possibilité de limiter le nombre de connexion)
- Par site : Chaque ordinateur doit avoir sa propre licence d'accès.

Voir :http://www.microsoft.com/France/licences/explication/utilisation/serveurs.asp

2.4. Nom de l'ordinateur et mot de passe Administrateur
Nom de l'ordinateur : Ce nom est utilisé pour reconnaître la machine sur le réseau. ex : DC1 (Domain Controler 1)
Mot de passe administrateur : Au minimum 8 caractères avec majuscules, minuscules et chiffres. ex : dWiht52Y

2.5. Composants Windows 2000
Afin de supprimer les services inutiles, désélectionner tous les composants sauf ***Accessoires et utilitaires – Accessoires***

2.6. Réglage de la date et de l'heure
Placer la machine dans le bon fuseau horaire afin d'éviter des problèmes avec Kerberos

2.7. Paramètres de gestion du réseau.
Choisir la configuration manuelle (***Paramètres personnalisé***)

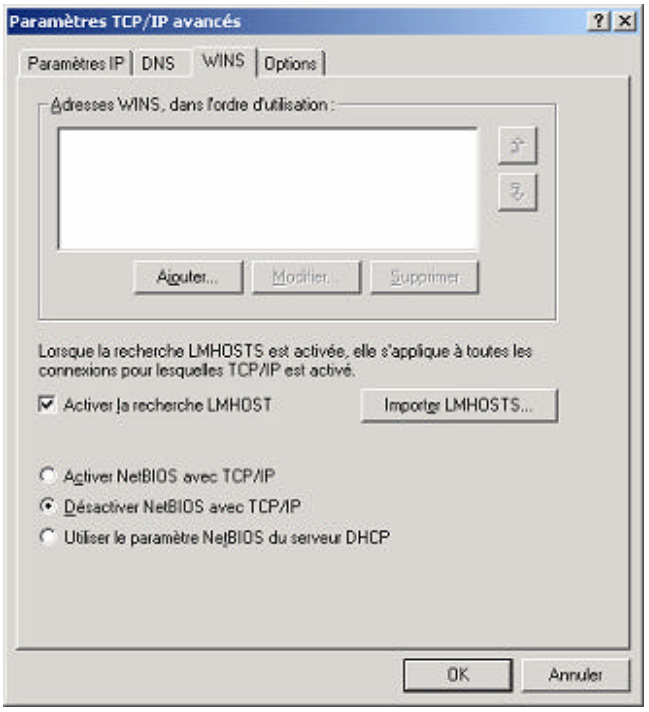
2.8. Composants de réseau
Désactiver **Partage de fichiers et d'imprimantes pour les réseaux Microsoft** si ce serveur ne

Philippe LOGEAN
Laboratoire de transmission de données
Ecole d'ingénieur de Genève
Hervé DEBRAY
Division Informatique
Rectorat de Créteil
15/12/2003

joue pas le rôle de Contrôleur de domaine ou de serveur de fichiers (port 445 tcp/udp).
Configurer les adresses IP. Exemple (adresses privées) :

- Adresse IP :172.16.0.2
- Masque de sous-réseau : 255.255.0.0
- Passerelle : 172.16.0.1
- Serveur DNS préféré : 172.16.0.2

Désactiver NetBIOS sur TCP/IP (ports TCP 139 et UDP 137,138). En effet, ce protocole génère beaucoup de trafic et permet d'obtenir des informations sur une machine, ce qui n'est pas acceptable au niveau de la sécurité.
Sur un réseau Windows 2000, ce protocole n'est pas utile. Pour le désactiver, sélectionnez ***Protocole Internet (TCP/IP) - Propriétés – Avancé… - WINS – Désactiver NetBIOS avec TCP/IP***



Attention, sans le protocole NetBIOS, il n'est plus possible d'accéder à une ressource sur une machine Windows NT 4.0 (ni avec le Voisinage Réseau, ni avec Exécuter…).

2.9. Groupe de travail ou domaine d'ordinateurs

- Si ce serveur doit être le Contrôleur de domaine (DC) d'un nouveau domaine, sélectionner **Non, cet ordinateur ne se trouve pas…** . Le domaine sera créer lors de l'installation d'***Active Directory***.
- Si ce serveur doit faire partie d'un domaine existant, sélectionner ***Oui, faire de cet ordinateur un membre du domaine suivant :***
- Sinon, laisser **Non, cet ordinateur ne se trouve pas…**

Philippe LOGEAN
Laboratoire de transmission de données
Ecole d'ingénieur de Genève
Hervé DEBRAY
Division Informatique
Rectorat de Créteil
15/12/2003

2.10. Désactivation des partages administratifs

Les partages administratifs permettent à l'administrateur réseau d'accéder à distance aux disques durs de la machine. Mais ils peuvent aussi être utilisés par les *Hackers* pour pénétrer le système.
C'est pourquoi il faut les désactiver avec ***Regedit*** (*Démarrer – Exécuter… - regedit*), en ajoutant la clé de registre suivante :
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\
Mettre la valeur *AutoShareServer* à 0 (DWORD)

2.11. Services

Etudier les services actifs sur Windows 2000 afin désactiver ceux qui ne sont pas nécessaire.
http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp

3. Serveur DNS

3.1. Installation du serveur DNS

Pour installer le serveur DNS : ***Démarrer – Programmes – Outils d'administration – configurez votre serveur –Mise en réseau – DNS – Installer le service DNS***

3.2. Configurer le serveur DNS

Pour configurer le serveur DNS allez dans : ***Démarrer – Programmes – Outils d'administration – DNS***. Sélectionner le serveur DNS puis : ***Action – Configurer le serveur…***

3.3. *Serveur Racine*

- Si cette machine est le premier serveur DNS du réseau (*Root*), sélectionner ***Ceci est le premier serveur DNS sur le réseau***
- Sinon, entrer l'adresse IP du serveur DNS *Racine.*.

3.4. *Zone de recherche directe*

La *Zone de recherche directe* est utilisée par le serveur DNS pour traduire un Nom en adresse IP.

- Créer un *Zone de recherche directe* de type *Standard Principale*
- Donner un nom à cette zone : mon_etab.lan (domaine privé)
- Créer un nouveau *Fichier de Zone* (fichier qui contiendra la liste des Noms)

3.5. *Zone de recherche inversée*

La *Zone de recherche inversée* est utilisée par le serveur DNS pour traduire une adresse IP en Nom.

- Créer un *Zone de recherche inversée* de type *Standard Principale*
- Donner l'*ID* du sous réseau : 172.16 (pour le sous réseau 172.16.X.X)
- Créer un nouveau *Zone File* (fichier qui contiendra la liste des adresses IP)

3.6. Suppression de la zone *root*

Si le serveur DNS fait partie d'un domaine privé, il faut supprimer la zone *root*

3.7. Transfert de Zone

Le transfert de zone permet aux serveurs DNS de s'échanger leurs listes DNS. Par défaut, ce transfert de zone est autorisé avec tous les serveurs DNS. Cela est dangereux, car cette liste contient des informations sur toutes les machines du domaine. C'est pourquoi, si aucun autre serveur DNS ne doit être utilisé, il faut désactiver le transfert de zone (désactiver *Transfert de*

Philippe LOGEAN
Laboratoire de transmission de données
Ecole d'ingénieur de Genève
Hervé DEBRAY
Division Informatique
Rectorat de Créteil
15/12/2003

zone). Sinon, il faut limiter ce transfert au serveur DNS nécessaire.

3.8. Pollution du cache DNS

Du DNS « spoofing » est possible si les réponses aux *DNS query* ne sont pas sécurisées (Q241352). Cela peut engendrer une pollution du cache DNS et provoquer une résolution du nom vers un mauvais server. Pour éviter cela : ***Démarrer – Programmes – Outils d'administration – DNS***. Sélectionner le serveur DNS puis :***Propriétés – Avancé*** et sélectionner ***Sécuriser le cache contre la pollution***.

3.9. Remplir les zones de recherche d*irectes* et inversée

Zone de recherche direct: ***Action – Nouvel Hôte…*** , puis entrez les noms et les adresses IP des machines.
Zone *de recherche inversé* : ***Action – Nouveau Pointeur…*** , puis entrez les adresses IP et les noms des machines.

4. Contrôleur de domaine

4.1. Installation d'*Active Directory*

Pour installer le contrôleur de domaine : ***Démarrer – Programmes – Outils d'administration – Configurer votre serveur – Active Directory – Démarrer l'assistant Active Directory***

4.2. *Type de Contrôleur de Domaine*

- ↳*Contrôleur de Domaine pour un nouveau domaine* : Option pour créer soit un nouveau domaine enfant, soit un nouvel arbre de domaine, soit une nouvelle forêt.
- *Contrôleur de domaine supplémentaire pour un domaine existant* : **Ajoute** un contrôleur de domaine dans un domaine déjà existant.

4.3. Créer une arborescence ou un domaine enfant.

- ↳*Créer une nouvelle arborescence* : Crée un nouvel arbre de domaine ou une nouvelle forêt. Il est aussi possible de placer un nouvel arbre de domaine dans une forêt existante.
- *Créer un nouveau domaine enfant* : Le nouveau domaine est un enfant d'un domaine existant. Par exemple, on peut créer un nouveau domaine appelé *pedago.mon_etab.lan* comme un enfant de mon_etab.lan.

4.4. *Créer ou rejoindre une forêt*

- ↳*Créer une nouvelle forêt d'arborescence de domaine* : Il faut choisir cette option soit si c'est le premier domaine de la hiérarchie, soit pour créer un arbre de domaine indépendant dans une forêt.
- *Placer cette nouvelle arborescence de domaine dans une forêt existante* : L'arbre de domaine est placé dans une forêt existante. Un *Login* et un *mot de passe* sont demandés pour rejoindre le domaine.

4.5. *Nouveau nom de domaine*

Il faut choisir un nom de domaine. **Attention**, ce nom ne peut plus être changé ultérieurement.

- Pour un **domaine public**, il faut utiliser un nom respectant la structure DNS d'Internet (ex : ac-creteil.fr).
- ↳Pour un **domaine privé**, choisir un simple nom permettant d'identifier le domaine (ex : mon_etab.lan)

Philippe LOGEAN
Laboratoire de transmission de données
Ecole d'ingénieur de Genève
Hervé DEBRAY
Division Informatique
Rectorat de Créteil
15/12/2003

4.6. ***Nom de domain NetBIOS***

Le nom de domaine NetBIOS permet aux utilisateurs d'anciennes versions de Windows d'identifier le nouveau domaine. C'est souvent un « raccourci » du nom DNS. Par exemple, le nom NetBIOS qu'on pourrait choisir pour mon_etab.lan serait mon_etabTD.
Attention, ce nom NetBIOS **n'a plus vraiment son utilité** car Windows 2000 travaille avec le **protocole DNS**.

4.7. ***Emplacement de la base de données et du journal***

Ces deux répertoires représentent l'endroit sur le disque dur où sont stockés la copie locale de la base de données d'*Active Directory* et les fichiers de *logs*.
Par défaut, c'est le répertoire C:\WINNT\NTDS qui est utilisé.
Microsoft recommande de stocker la base de donnée et les fichiers de *logs* sur deux partitions séparées pour des questions de performance.

4.8. ***Volume système partagé***

Ce répertoire contient une copie des fichiers publics du domaine. Ce répertoire doit se trouver sur une partition NTFS.
Par défaut, ce répertoire correspond à C:\WINNT\SYSVOL

4.9. ***Configurer le serveur DNS***

- *Yes, install and configure DNS on this computer (recommended).*
- *No, I will install and configure DNS myself.*

Le contrôleur de domaine a besoin d'un serveur DNS dynamique pour fonctionner correctement. Si pendant l'installation d'Active Directory, aucun serveur DNS est trouvé, Windows 2000 recommande son installation sur le contrôleur de domaine.

4.10. ***Autorisation***

Certains programmes serveurs utilisent les informations stockées sur le contrôleur de domaine.

- *Autorisations compatibles avec les serveurs de version antérieures à Windows 2000* : Cette option est utilisée si l'on possède des programmes serveurs s'exécutant sur un pre-Windows 2000 serveur ou si l'on désire ajouter le serveur Windows 2000 dans un domaine pre-Windows 2000. **Des utilisateurs anonymes peuvent accéder aux informations sur le domaine**.
  Microsoft considère Windows NT 4, Windows 9x et Windows ME comme des *pre-Windows 2000*.
- *Autorisations compatibles uniquement avec les serveurs Windows 2000* : Les programmes serveurs peuvent seulement s'exécuter sur des serveurs Windows 2000 qui sont membres d'un domaine Windows2000. **Seuls les utilisateurs authentifiés peuvent lire les informations sur le domaine**.

4.11. ***Mot de passe administrateur de restauration des services d'annuaire***

Ce mot de passe est utilisé par l'administrateur s'il doit restaurer Active Directory (au minimum 8 caractères avec majuscules, minuscules et chiffres. ex : dWiht52Y). Il est préférable que ce mot de passe soit différent de celui du point 2.4.

4.12. **Configurer le serveur DNS pour le Contrôleur de Domaine**

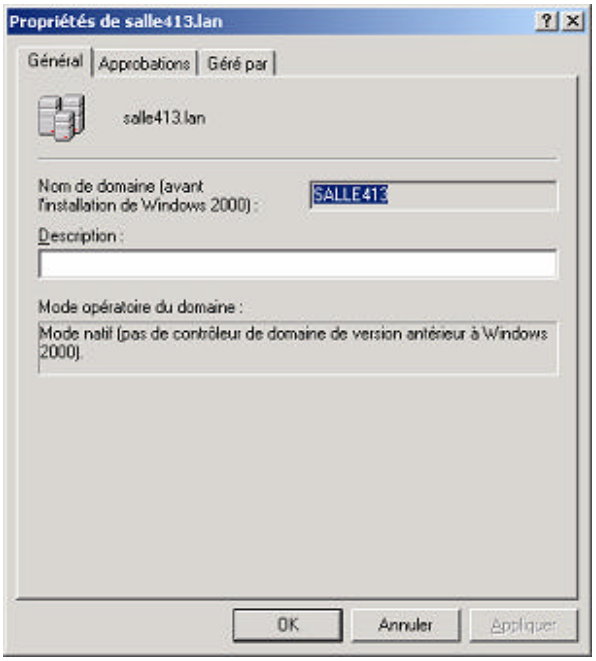
Dans ***Démarrer – Programmes – Outils d'administration – DNS*** changer le type de *zone de recherche Directe* de *Standard principale* à *Active Directory-integrated*. Pour cela, sélectionner la zone puis ***Propriétés –*** onglet ***Général – Modifier… - Intégré à Active Directory***. Activer le serveur DNS dynamique : toujours dans l'onglet ***Général***, ***Autoriser les mises à jour***

Philippe LOGEAN
Laboratoire de transmission de données
Ecole d'ingénieur de Genève
Hervé DEBRAY
Division Informatique
Rectorat de Créteil
15/12/2003

dynamiques – Uniquement les mises à jour sécurisées (voir RFC 2136 et RFC 2137)
Effectuer les mêmes opérations pour la zone *Reverse*.

4.13. Mettre le contrôleur de domaine en mode natif

Par défaut, le contrôleur de domaine se trouve dans le mode mixte. C'est-à-dire qu'il supporte aussi bien les contrôleurs de domaine pre-Windows 2000 que les contrôleurs de domaine Windows 2000.
Pour changer de mode, il faut exécuter ***Démarrer – Programmes – Outils d'administration – Domaines et approbations active directory*** et afficher les propriétés du domaine.



En cliquant sur *changer de mode*, le mode devient natif. Seuls les contrôleurs de domaine fonctionnant sous Windows 2000 peuvent être utilisés. **Attention, le processus n'est pas réversible**.
Avantages du mode natif :

- Le mode natif supporte des nouvelles étendues des groupes comme les groupes **locaux de domaines** et les **groupes universels**.
- La possibilité de mettre des groupes globaux **à l'intérieur** d'autres groupes globaux.
- La notion de domaine primaire et secondaire disparaît.

5. Installation des *Services Pack*

Installer ***Windows 2000 Service Pack 4*** qui règle certains problèmes de sécurité.
Copier le répertoire I386 de la distribution Windows 2000 sur une unité du serveur et le patcher (Slipstreaming).

6. Antivirus

Il est important d'installer un antivirus sur la machine afin d'éviter que les données stockées sur le poste soient exposées à des virus, qui sont transmis soit par disquette, soit par le réseau et qui

peuvent endommager les données.
Il est important de garder la liste des virus à jour. Configurer une mise à jour automatique de cette liste.

7. Mise en exploitation du serveur

A présent, le serveur est près à être connecté sur le réseau. Effectuer des tests pour vérifier le bon fonctionnement des services (DNS, DC, …).

8. Garder le serveur à jour

Il est important de garder un serveur à jour. En effet, de nouvelles mises à jour, réglant des bugs et des failles de sécurité, sont régulièrement disponibles sur le site http://www.microsoft.com/ms.htm.
Type de mise à jour :

- Hot fixe : *Patch* non testé mit à disposition rapidement pour contrer une faille de sécurité.
- Rollup : *Package* rassemblant tous les *patchs* disponibles et les installant dans le bon ordre.
- Service Pack : Mise à jour du système d'exploitation (nouvelle fonctionnalité, correction de bugs, patchs de sécurité).

Philippe LOGEAN
Laboratoire de transmission de données
Ecole d'ingénieur de Genève
Hervé DEBRAY
Division Informatique
Rectorat de Créteil
15/12/2003