Support de formation

Configuration Windows 2000 Server DNS – Active Directory

Nom du stagiaire :

Avertissement

Ce support n'est ni un manuel d'utilisation
(pour cela, consultez la documentation jointe à votre logiciel ou micro),
ni un outil d'auto-formation.

Ce support est un complément à vos notes personnelles
pour les formations sur la gestion et maintenance micro-informatique.

Modification et utilisation interdites sans l'accord de l'auteur de ce support.

L'auteur de ce support sur le web : **http://www.e-wsc.com**
Vous y trouverez des mises à jour, de nouveaux supports…

e-wsc.com

Sources diverses sur internet et l'ouvrage « Microsoft Windows 2000 Server au quotidien Expert » édition Microsoft Press

Sommaire

❑ Introduction

Ce support fait suite au support traitant de l'installation de Windows 2000 serveur.

❑ Active Directory

Dans un environnement Windows NT, l'utilisateur ouvre une session sur le domaine avec un nom (login) et un mot de passe. Cet utilisateur peut ouvrir le voisinage réseau, puis explorer les ressources partagées.
Ceci se déroule très bien tant que le réseau garde la même envergure.
Supposons que l'entreprise ajoute une messagerie électronique au réseau et que cet utilisateur soit doté d'une autre identité pour sa boite électronique. Les autres services, les bases de données et les outils d'administration, dont chacun identifie cet utilisateur d'une façon spécifique, doivent être accessibles par cet utilisateur.
Imaginons que cet utilisateur ne soit qu'un utilisateur parmi des centaines d'autres. Il y a là une source potentielle d'erreurs très difficiles à résoudre.
Lorsque le nombre d'objets du réseau atteint un certain seuil, il devient indispensable de disposer de services d'annuaire, c'est-à-dire d'un emplacement centralisé contenant toutes les données requises par l'administration de l'ensemble du système informatique.

Un service d'annuaire diffère d'un simple répertoire : il contient des données, des services permettant aux utilisateurs d'accéder à ces données.
Il est à la fois un outil d'administration et un outil pour l'utilisateur final. Il doit satisfaire aux besoins suivants :

- Accès à tous les serveurs, à toutes les applications et à toutes les ressources par le biais d'une ouverture de session unique.
- Réplication multi maître. Toutes les données sont distribuées sur l'ensemble du système informatique et répliquées sur plusieurs serveurs.
- Recherches de type « pages blanches ». Pour faire, par exemple, une recherche à partir d'un nom ou d'un type de fichier.
- Recherches de type « pages jaunes ». Pour faire, par exemple, une recherche de toutes les imprimantes du service administratif ou tous les serveurs du site de Tarbes.
- Suppression de la dépendance vis-à-vis des emplacements physiques, à des fins d'administration de l'annuaire, partiellement ou complètement.

Microsoft emploie parfois le terme « service d'annuaire » dans le contexte de Windows NT, mais Windows NT n'offre pas de véritables services d'annuaire hiérarchiques.
Sous Windows NT, les fonctionnalités d'annuaire sont assurées par plusieurs services :

- Le service DNS (Domain Name System) qui traduit les noms de machines en adresse IP.
- Le service WINS (Windows Internet Naming Service) qui sert à résoudre les noms NetBIOS.

Sous Windows 2000 serveur, Active Directory remplace les services éparpillés de Windows NT par un service unifié qui regroupe DNS, DHCP, LDAP (*) (Lightweigh Directory Access Protocol) et Kerberos.

(*) LDAP est le protocole d'annuaire standard et extensible sur TCP/IP.

L'interface ADSI (Active Directory Services Interface) permet aux développeurs de créer des applications pouvant accéder aux annuaires, donnant ainsi aux utilisateurs un point d'accès unique vers de multiples annuaires.

Active Directory permet d'administrer, depuis un même emplacement, toutes les ressources publiées comme les fichiers, périphériques, connexions d'hôte, bases de données, accès web, utilisateurs, services,…
Active Directory utilise le protocole DNS comme service de localisation et range les objets des domaines dans une hiérarchie d'unités organisationnelles. AD permet de regrouper plusieurs domaines au sein d'une arborescence.

1. Terminologie et concepts d'Active Directory

1.a Espace de noms et résolution de noms

Chaque annuaire est un espace de noms : une aire bien délimité permettant de résoudre un nom.
Ex : un programme de télévision, dans lequel le nom d'une chaîne est associé à un numéro de canal ; un système de fichiers d'un ordinateur, dans lequel le nom de fichier est associé au fichier lui-même ; un programme téléphonique, dans lequel le numéro de poste téléphonique est associé à l'emplacement dans l'auto-com.

Active Directory forme un espace de noms dans lequel le nom d'un objet de l'annuaire permet d'accéder à l'objet lui-même. La résolution de noms est le processus consistant à traduire un nom en un certain objet associé à ce nom.

1.b Attribut

Un attribut est un élément de données qui décrit un certain aspect d'un objet. Un attribut se compose d'un type et d'une ou plusieurs valeurs.
Ex : un numéro de téléphone ; type numérique ou alphanumérique, exemple de valeur 056200010203.

1.c Objet

Un objet est un ensemble particulier d'attributs qui représente quelque chose de concret, par exemple un utilisateur, une imprimante ou une application. Les attributs contiennent des données qui décrivent l'entité identifiée par l'objet de l'annuaire.
Les attributs d'un utilisateur sont, par exemple, le nom, le prénom, l'adresse de messagerie,…
La classification de l'objet indique quels sont les types d'attributs utilisés. Par exemple : les objets classifiés comme « utilisateur » permettent d'employer des types d'objet du genre « nom de famille », « numéro de téléphone » et « adresse de messagerie », alors que la classe d'objets « entreprise » permet d'employer des types du genre « nom de la société » et « secteur d'activité ». Un attribut peut prendre une ou plusieurs valeurs, selon son type.

1.d ID d'objet

Chaque objet dans Active Directory possède une identité qui lui est propre. Un objet peut être déplacé ou renommé, mais son identité reste inchangée.
L'identité d'un objet, qui sert à son référencement interne dans AD, s'appelle GUID (Globaly Unique IDentifier). Le GUID est assigné par le DSA (Directory System Agent) lors de la création de l'objet. L'attribut objectGUID ne peut être ni modifié, ni supprimé.

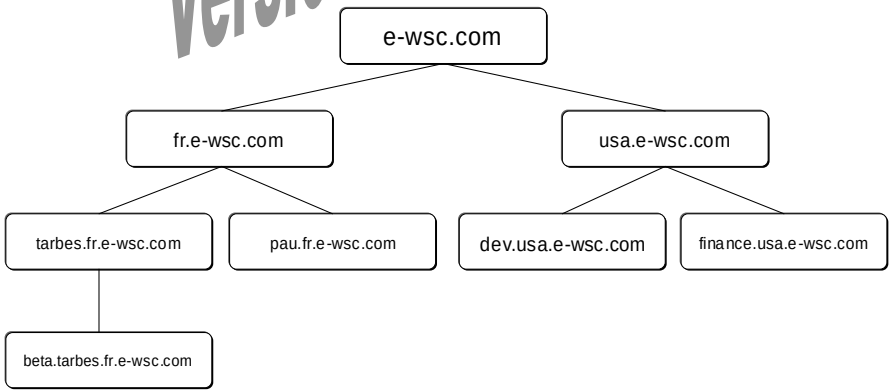
1.e Conteneur

Le conteneur ressemble à un objet en ce sens qu'il a des attributs et qu'il fait partie de l'espace de noms d'Active Directory. Toutefois, contrairement à un objet, il ne correspond à rien de concret : c'est juste une enveloppe qui renferme des objets et d'autres conteneurs.

1.f Arborescence et forêt

L'arborescence dans Active Directory est une hiérarchie d'objets et de conteneurs qui indique les relations entre les objets (chemins par lesquels on passe d'un objet à un autre).
Une arborescence est un espace de noms connexe dans lequel chaque nom est descendant direct d'un nom racine unique.

Exemple d'arborescence (arbre constitué de branches) :



Une forêt est constituée d'une ou plusieurs arborescences ne formant pas d'espace de noms contigu.

1.g Nom distingué

Dans Active Directory chaque objet a un nom distingué (différencié). Ce nom identifie le domaine contenant l'objet, ainsi que le chemin complet afin d'atteindre celui-ci à travers la hiérarchie des conteneurs.

Exemple :

CN= Jean BON, OU= Cuisine, DC=Spam, DC=COM
Ce nom indique que l'utilisateur « Jean BON » appartient à l'unité organisationnelle Cuisine qui elle-même appartient au domaine spam.com.
CN : Common Name
OU : Organizational Unit
DC : Domain Controller

1.h Schéma

Le terme schéma est fréquemment employé dans un contexte de bases de données. Dans Active Directory, le schéma est tout ce qui constitue l'annuaire Active Directory : les objets, les attributs, les conteneurs,…
Le schéma par défaut d'AD définit les classes d'objets les plus courantes : utilisateurs, groupes, ordinateurs, unités organisationnelles, stratégies de sécurité et domaines.
Ce schéma peut être modifié par des applications qui ajoutent de nouveaux attributs et de nouvelles classes.

2. Architecture d'Active Directory

2.a DSA (Directory System Agent)

DSA est le processus permettant d'accéder au magasin physique des données de l'annuaire situé sur le disque dur.

2.b Formats de noms

RFC 822 : format des utilisateurs de messagerie internet.
Ex : jeanBon@e-wsc.com.

URL HTTP : format des utilisateurs d'explorateurs web.
Ex : http://domaine/chemin_vers_page

LDAP : plus complexe que les noms internet mais généralement masqué dans les applications. Les noms LDAP emploient la convention de dénomination unique de X.500.
Exemple d'URL LDAP :
ldap://AServer.e-wsc.com/CN=jeanbon,OU=Cuisine,OU=Production,
O=Spam,C=FR

X.500 : Norme du CCITT répertoire des utilisateurs de systèmes X.400.
X.400 : Protocole standard du CCITT pour un système global d'échange de courrier Electronique (e-mail).
CCITT : Comité Consultatif International de Télégraphie et de Téléphonie. Ce groupement définit les normes de communications à l'échelle mondiale. La plupart de leurs recommandations concernent les modems et les fax de la série V (V.21, V.32, V.32bis ...)

UNC : Le format Universal Naming Convention, utilisé sur les réseaux Windows NT et 2000, permet de désigner des volumes, des imprimantes et des fichiers partagés.
Ex : \\e-wsc.com\production.cuisine.voume\DocsPublisher\recette001.pub

2.c Catalogue global

La catalogue global permet aux utilisateurs et aux applications de trouver un objet dans une arborescence de domaine Active Directory à partir d'un ou plusieurs attributs de cet objet.

3. En résumé

Active Directory est un outil extrêmement puissant et, comme tout outil très puissant, il peut faire des dégâts si l'on s'en sert mal.
AD est une base d'annuaire qui regroupe tous les objets réseaux.

❑ Serveur DNS et Windows 2000 Server

Windows 2000 serveur s'appuie sur le standard de résolution des noms DNS (Domain Name System) pour son espace de nom de domaine.
Votre domaine Windows 2000 pourra être du style e-wsc.com.
Il est donc indispensable d'utiliser le service DNS dans un réseau avec des domaines Windows 2000.
Avant la promotion d'un serveur membre ou autonome en contrôleur de domaine (installation d'Active Directory), vous devez obligatoirement disposer d'un serveur DNS.

1. Planification des zones DNS

Pour déterminer la structure de l'espace de noms il faut prendre en compte les points suivants :

- Doit-on déléguer la structure d'une partie de l'espace de noms de l'organisation à un autre emplacement de l'entreprise ?
- Doit-on diviser une zone afin de répartir le trafic ou créer une tolérance de panne ?
- Doit-on étendre l'espace de noms afin de prévoir l'ajout de site ou de département au sein de l'entreprise ?

Il existe deux zones de recherche :

- Directe.
- Inversée.

1.a Zone de recherche directe

A la configuration du serveur DNS, vous avez le choix entre trois types de zones :

- Principale standard : copie principale de la base de données de zone (c'est un fichier texte stocké sur %systemroot%\system32\dns).
- Secondaire standard : copie de la zone principale standard. Copie en lecture seule. Permet une tolérance de panne vis-à-vis de la zone principale.
- Intégrée à Active Directory : fichier de zone stocké dans la base d'annuaire Active Directory.

Il est possible à tout moment de changer le type de zone.

1.b Zone de recherche inversée

Cette zone permet d'effectuer la recherche inverse d'un ordinateur dont on dispose uniquement de son adresse IP et dont on veut obtenir son nom.
Ex : la commande *NSLOOKUP @ip* permet d'obtenir le nom de la machine qui possède comme adresse ip *@ip*.

1.c Mise à jour dynamique DNS

La mise à jour dynamique prise en charge par le service DNS de Windows 2000 server permet de renseigner automatiquement les fichiers de zones.
Ceci permet de réduire le travail de maintenance de l'administrateur.

❑ Rôle des contrôleurs de domaine

1. Maîtres d'opération

Dans un domaine Windows 2000, tous les contrôleurs de domaine sont « identiques ». La base d'annuaire est dupliquée et distribuée sur chaque contrôleur. On parlera de réplication multi maître.

Néanmoins certains contrôleurs de domaine jouent des rôles spécifiques de maître d'opération (FSMO Flexible Single Master Operation). Certains rôles sont critiques pour le réseau.

1.a Maître de schéma

Le maître de schéma supervise toutes les modifications apportées au schéma. Il ne peut y avoir qu'un seul maître de schéma dans toute la forêt.

Le premier contrôleur de domaine (le premier serveur installé) prend le rôle de maître de schéma.

Les modifications du schéma étant assez rare, une panne durable du maître de schéma ne gène pas les utilisateurs.

Pour transférer le rôle de maître de schéma d'un serveur à un autre :

- Outil d'administration, Schéma Active Directory
- Clic droit, Changer de contrôleur de domaine
- Sélectionnez le contrôleur qui prendra le rôle de maître de schéma. Vous accédez à sa base.
- Clic droit, Maître d'opération.
- Cliquez sur Modifier, puis Ok

Si le maître de schéma est HS et qu'il n'y a aucun espoir de le réparer, vous avez la possibilité de faire une capture du rôle de maître de schéma :

- Démarrer / Exécuter, tapez la commande NTDSUTIL
- A chaque invite, tapez les données suivantes (en police `courrier`) :
  - ntdsutil `roles`
  - fsmo maintenance `connections`
  - server connections `connect to server` `suivi_du_nom_domaine_complet(*) du serveur devant maître de schéma`
  - server connections `quit`
  - fsmo maintenance `seize schema master`
  - ntdsutil `quit`

(*) nom de domaine complet

Nom de domaine DNS qui a été déclaré sans ambiguïté afin d'indiquer une certitude absolue quant à son emplacement dans l'arborescence de l'espace de nom de domaine. Les noms de domaines pleinement qualifiés (FQDN, fully qualified domain name - nom de domaine pleinement qualifié) diffèrent des noms relatifs car ils sont indiqués avec un point en fin de chaîne (.), par exemple, « hôte.exemple.microsoft.com », pour indiquer leur position à la racine de l'espace de noms..

1.b Maître de dénomination de domaine

Le maître de dénomination de domaine est unique et est créé dans le premier domaine et y reste toujours. S'il vient à être indisponible, cela devient gênant lorsqu'on a besoin de créer un nouveau domaine. Ne transférer ce rôle uniquement si ce contrôleur doit être retiré définitivement du réseau.

Pour transférer le rôle de maître de dénomination de domaine d'un serveur à un autre :

- Outil d'administration, Domaines et approbation Active Directory.
- Clic droit, Se connecter au contrôleur de domaine.
- Sélectionnez le contrôleur qui doit devenir le maître de dénomination de domaine.
- Clic droit, Maître d'opération. La boîte de dialogue affiche le contrôleur qui deviendra maître de dénomination de domaine ainsi que le maître d'opération actuel.
- Cliquez sur modifier, puis ok

Si le maître de dénomination de domaine est HS et qu'il n'y a aucun espoir de le réparer, vous avez la possibilité de faire une capture du rôle de maître de dénomination de domaine :

- Démarrer / Exécuter, tapez la commande NTDSUTIL
- A chaque invite, tapez les données suivantes (en police `courrier`) :
  - ntdsutil `roles`
  - fsmo maintenance `connections`
  - server connections `connect to server` `suivi_du_nom_domaine_complet du serveur devant maître de dénomination`
  - server connections `quit`
  - fsmo maintenance `seize domain naming master`
  - ntdsutil `quit`

1.c Maître RID (Relative IDentifier)

Le maître RID alloue les ID relatifs à chaque contrôleur de domaine.

Quand un contrôleur crée un objet de sécurité (utilisateur, groupe, compte d'ordinateur), le maître RID lui affecte un SID (Security IDentifier) unique. Le SID est composé de 2 parties : l'ID de sécurité du domaine (ID commun à tous les objets de sécurité du domaine) et l'ID relatif unique à chaque objet.

Si le maître RID vient à être indisponible, cela ne gène ni les utilisateurs, ni les administrateurs sauf s'ils créent des objets de sécurité et que le domaine est à cours d'ID relatifs (au domaine).

Ne transférer ce rôle uniquement si ce contrôleur doit être retiré définitivement du réseau.

Pour transférer le rôle de maître RID d'un serveur à un autre :

- Outil d'administration, Utilisateurs et ordinateurs Active Directory.
- Clic droit, Se connecter au contrôleur de domaine.
- Sélectionnez le contrôleur qui doit devenir le maître RID.
- Clic droit, Maître d'opération. L'onglet RID de la boîte de dialogue affiche le contrôleur qui deviendra maître RID ainsi que le maître d'opération actuel.
- Cliquez sur modifier, puis ok

Si le maître RID est HS et qu'il n'y a aucun espoir de le réparer, vous avez la possibilité de faire une capture du rôle de maître RID :

- Démarrer / Exécuter, tapez la commande NTDSUTIL
- A chaque invite, tapez les données suivantes (en police `courrier`) :
  - ntdsutil `roles`
  - fsmo maintenance `connections`
  - server connections `connect to server` `suivi_du_nom_domaine_complet du serveur devant maître RID`
  - server connections `quit`
  - fsmo maintenance `seize RID master`
  - ntdsutil `quit`

1.d Maître de l'infrastructure

Le maître d'infrastructure est chargé de suivre les modifications des appartenances aux groupes et de les ventiler vers les autres domaines. Il existe un seul maître d'infrastructure par domaine.

Si le maître d'infrastructure est indisponible, cela ne touche pas les utilisateurs. Les administrateurs ne remarqueront pas son absence tant que les autres contrôleurs de domaine ne reflèteront pas un certain nombre de modifications concernant les comptes utilisateurs.

Ne transférer ce rôle uniquement si ce contrôleur doit être retiré définitivement du réseau.

L'emplacement du maître d'infrastructure ne doit pas être le contrôleur qui héberge le catalogue global (*) sauf lorsque le domaine n'a qu'un seul contrôleur. En effet, le maître d'infrastructure consulte le catalogue global pour savoir s'il faut distribuer les modifications aux autres domaines, et s'actualise lui-même en utilisant le catalogue global. Si le contrôleur supportant le catalogue global est aussi maître d'infrastructure, il ne trouvera jamais de données non actualisées et donc ne répliquera rien vers les autres domaines.

(*) Catalogue global
Contrôleur de domaine qui contient un réplica partiel de chaque domaine dans Active Directory. Cela signifie qu'un catalogue global contient un réplica de chaque objet dans Active Directory, mais avec un nombre limité d'attributs pour chaque objet. Le catalogue global stocke les attributs les plus fréquemment utilisés dans les opérations de recherche (par exemple le nom et le prénom d'un utilisateur) et les attributs nécessaires à la recherche d'un réplica complet de l'objet.Le système de réplication Active Directory crée automatiquement le catalogue global. Les attributs répliqués dans le catalogue global comprennent un ensemble de base défini par Microsoft. Les administrateurs peuvent indiquer des propriétés supplémentaires pour répondre aux besoins de leur installation. Voir aussi réplication.

Pour transférer le rôle de maître d'infrastructure d'un serveur à un autre :

- Outil d'administration, Utilisateurs et ordinateurs Active Directory.
- Clic droit, Se connecter au contrôleur de domaine.
- Sélectionnez le contrôleur qui doit devenir le maître d'infrastructure.
- Clic droit, Maître d'opération. L'onglet Infrastructure de la boîte de dialogue affiche le contrôleur qui deviendra maître d'infrastructure ainsi que le maître d'opération actuel.
- Cliquez sur modifier, puis ok

Si le maître d'infrastructure est HS et qu'il n'y a aucun espoir de le réparer, vous avez la possibilité de faire une capture du rôle de maître d'infrastructure :

- Démarrer / Exécuter, tapez la commande NTDSUTIL
- A chaque invite, tapez les données suivantes (en police `courrier`) :
  - ntdsutil `roles`
  - fsmo maintenance `connections`
  - server connections `connect to server` `suivi_du_nom_domaine_complet du serveur devant maître d'infrastructure`
  - server connections `quit`
  - fsmo maintenance `seize infrastructure master`
  - ntdsutil `quit`

1.e Emulateur de PDC

L'émulateur PDC joue le rôle de contrôleur principal de domaine Windows NT. Ceci est indispensable lorsqu'il y a des contrôleurs secondaires Windows NT ou des clients dépourvus de logiciel client Windows 2000.
L'émulateur PDC gère les protocoles Kerberos (1) et NTLM (NT Lan Manager) permettant ainsi aux contrôleurs Windows NT de se synchroniser avec un réseau Windows 2000 fonctionnant en **mode mixte**.

(1) Kerberos
Kerberos est un service distribué d'authentification qui permet à un procédé (un client) à prouver son identité à un vérificateur (un serveur d'application, ou serveur simplement) sans envoyer des données à travers le réseau qui pourrait permettre à un agresseur à les imiter postérieurement.
Kerberos fournit intégrité et confidentialité pour des données envoyées entre le client et serveur.

Authentification NTLM

Dans Windows 2000, NTLM sert de protocole d'authentification pour les transactions entre deux ordinateurs d'un même domaine, où l'un des deux ordinateurs, ou les deux, exécutent Windows NT 4.0 ou une version précédente.

Par défaut, Windows 2000 est installé dans une configuration réseau en mode mixte. Ce type de configuration accepte toutes les associations entre Windows NT 4.0 et Windows 2000. Si vous n'avez pas un réseau en mode mixte, vous pouvez passer à un mode natif sur un contrôleur de domaine pour désactiver l'authentification NTLM.

Les exemples de configurations suivants utiliseraient NTLM comme mécanisme d'authentification :
* Un client Windows 2000 Professionnel s'authentifiant auprès d'un contrôleur de domaine Windows NT 4.0.
* Un client Windows NT 4.0 s'authentifiant auprès d'un contrôleur de domaine Windows 2000.
* Un client Windows NT 4.0 s'authentifiant auprès d'un contrôleur de domaine Windows NT 4.0.
* Les utilisateurs d'un domaine Windows NT 4.0 s'authentifiant auprès d'un domaine Windows 2000.

Par ailleurs, NTLM est le protocole d'authentification utilisé par les ordinateurs qui ne font pas partie d'un domaine, tels que les serveurs autonomes et les groupes de travail.

2. Serveur de catalogue global

Un serveur de catalogue global est un contrôleur de domaine possédant un catalogue dans lequel sont référencés les attributs les plus utilisés de tous les objets d'Active Directory.

La base de données d'AD est divisée en trois parties :

- Partition de schéma : ensemble des définitions des classes et attributs des objets de l'Active Directory.
- Partition de configuration : ensemble des objets de configuration de la forêt (les sites, les services, etc...).
- Partition de domaine : ensemble des utilisateurs, groupes, machines, etc., d'un domaine particulier.

Les partitions de configuration et de schéma sont créées à l'installation du premier contrôleur de domaine de la forêt. Elles sont copiées sur tous les autres contrôleurs de domaine installés par la suite. Les partitions de domaine sont spécifiques à chacun des domaines.
Le catalogue global, situé sur le premier contrôleur de domaine du domaine racine de la forêt, contient, en plus des partitions de configuration et de schéma, une copie en lecture de toutes les partitions de domaine de la forêt.
Comme les informations des objets d'un domaine ne sont pas dupliquées vers les autres domaines de la forêt, le serveur de catalogue global va être utilisé pour effectuer des recherches à l'échelle de la forêt.

Il est possible d'ajouter de nouveaux serveurs de catalogue global :

- Ouvrez la console Sites et services Active Directory
- Développez Sites, puis le nom du site dans lequel se situe le serveur que vous souhaitez faire devenir catalogue global. Par défaut un seul site existe et se nomme Premier-site-par-défaut.
- Développez ensuite le dossier Serveurs, puis le serveur en question. Effectuez ensuite un clic droit sur le connecteur NTDS Setting et cliquez sur Propriétés.
- Activez l'option Catalogue global.

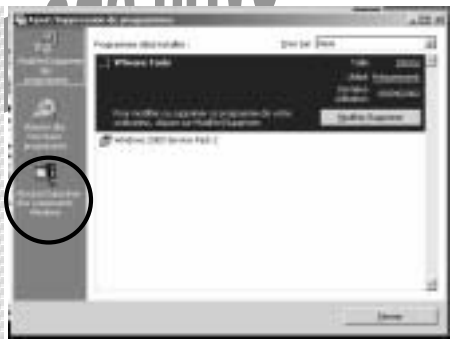
A l'ouverture de session d'un utilisateur, le contrôleur, ayant reçu cette demande, fera appel au serveur de catalogue global pour obtenir des informations comme l'appartenance à des groupes universels afin de créer un jeton d'accès. Si le serveur de catalogue global n'est pas disponible, l'utilisateur ne pourra qu'ouvrir une session localement. Seuls les membres du groupe administrateur ouvriront une session sur le domaine.

❑ Installation d'un serveur DNS sous Windows 2000

Nota : AD s'appuie sur un serveur DNS. Si vous ne possédez pas d'un serveur DNS, soit vous l'installez avant AD, soit lors de l'installation d'AD l'assistant vous propose d'installer un serveur DNS.

Ouvrez le panneau de configuration et cliquez sur « Ajout/suppression de programmes »

Dans « Ajout/suppression de programmes », cliquez sur « Ajouter/supprimer des composants Windows »



Sélectionnez le composant « Services de mise en réseau » et cliquez sur le bouton « Détails ».

Choisissez le service « Système de nom de domaine (DNS) » et validez par OK

Continuez l'installation en cliquant sur « Suivant ».

Le service DNS s'installe sur Windows 2000 Server.

Le service DNS est installé. Cliquez sur « Terminer ».

Une fois l'installation terminée, la première étape consiste à créer une zone DNS sur laquelle le serveur aura autorité.

Lancez l'utilitaire DNS depuis le groupe Outils d'administration.

La console de configuration du serveur DNS apparaît.

1. Configuration du serveur DNS par l'assistant

Lancez la configuration du serveur en faisant un clic droit sur l'icône représentant le serveur (ici SERVEUR).
Choisissez « Configurer le serveur ».

L'assistant de configuration vous aide pas à pas à configurer le serveur.

Comme c'est le premier serveur DNS du réseau, cliquez sur « Suivant ».

Choisissez la création d'une zone de recherche directe, cliquez sur « Suivant ».

AD n'étant pas encore installé, seule la zone principale standard (stockage dans un fichier) est disponible. Nous verrons plus loin comment intégrer la zone DNS dans AD.

Cliquez sur « Suivant ».

Choisissez la zone DNS qui devra être la même que le domaine 2000.
Pour un site local (non accessible sur internet), utilisez de préférence l'extension « local ».
Ex : domaine.local

Cliquez sur « Suivant ».

Le fichier contenant la zone DNS sera stocké dans le dossier %systemRoot%\system32\dns.
Cliquez sur « Suivant ».

Création de la zone de recherche DNS inversée.
Validez la création de la zone et cliquez sur « Suivant ».

Tout comme la zone de recherche DNS directe, la zone de recherche DNS inversée ne peut pas être intégrée à AD.
Cliquez sur « Suivant ».

Le fichier de zone de recherche DNS inversée est établi à partir de l'adresse IP du réseau (ici 192.168.1.0 – donc saisie des 3 premiers octets).
Cliquez sur « Suivant ».

Le fichier de zone de recherche DNS inversée sera créé dans le même dossier que celui de la zone de recherche directe.
Il sera nommé 1.168.192.in-addr.arpa.dns.
Cliquez sur « Suivant ».

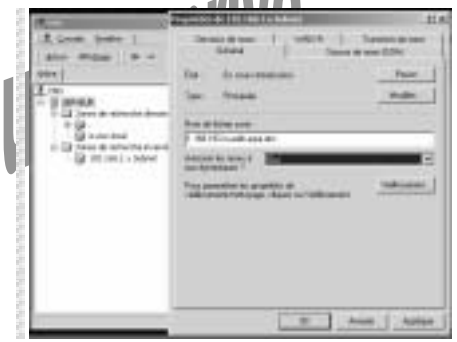
Ecran de récapitulation de configuration du serveur DNS.
Cliquez sur « Terminer » et le serveur DNS sera créé.

Le serveur DNS est configuré.

<u>Modification de l'enregistrement dynamique des clients dans le serveur DNS</u> :
Faites un clic droit sur le domaine de la zone de recherche directe, et choisissez « Propriétés ».

Choisissez « Oui » pour l'option « Autoriser les mises à jour dynamiques » et cliquez sur « OK ».

Faites de même pour la zone de recherche inversée.



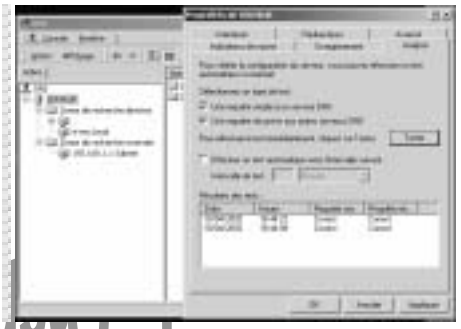
Le serveur fait appel à son propre serveur DNS. C'est pour cela que dans la configuration IP du serveur vous trouvez comme Serveur DNS l'adresse IP 127.0.0.1 (loopback).

Enregistrez le serveur dans les zones de recherche DNS :
Tapez la commande
`ipconfig /registerdns`

Regardez les zones de recherche pour voir si le serveur apparaît bien.
Vous pouvez utiliser la commande `nslookup` suivi soit du nom DNS de la machine (recherche directe), soit de l'adresse IP de la machine (recherche inverse).

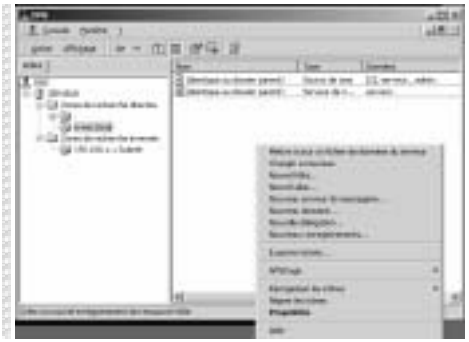
Il est aussi possible de valider le fonctionnement du serveur DNS en utilisant l'utilitaire d'analyse inclus dans la gestion DNS :

Faites un clic droit « Propriétés » sur le serveur.
Puis onglet « Analyse ».
Cocher les 2 tests de requête et cliquez sur « Tester ».



Si la machine n'apparaît pas encore dans le serveur DNS, vous pouvez l'ajouter manuellement :

Faites un clic droit dans la zone de recherche directe et « Nouvel hôte ».



Saisissez le nom de la machine, puis son adresse IP.
N'oubliez pas de cocher la création d'un point d'enregistrement PTR associé afin de créer la même relation dans la zone de recherche inversée.
Cliquez sur « Ajouter un hôte ».

Pointeur (PTR) : Utilisé pour mapper un nom de domaine DNS indirect basé sur l'adresse IP d'un ordinateur qui pointe vers le nom de domaine DNS direct de cet ordinateur.

Testez avec la commande `nslookup`

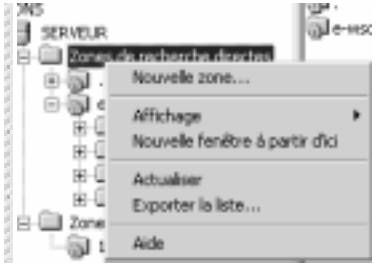
Le serveur DNS doit répondre correctement (voir exemple ci-contre).
Les valeurs Serveur et Address correspondent au serveur DNS.
Les valeurs Nom et Address correspondent à la machine testée.

Le serveur DNS de Windows 2000 est en place.

2. Configuration manuelle du serveur DNS

Cette configuration manuelle n'est pas plus compliquée que la précédente car elle s'appuie aussi sur des assistants.

Lancez la console de gestion DNS, puis faites un clic droit sur la zone de recherche directe et choisissez « Nouvelle Zone ».



L'assistant de création de zone DNS se lance.

Reportez-vous à la « configuration du serveur DNS par assistant ».

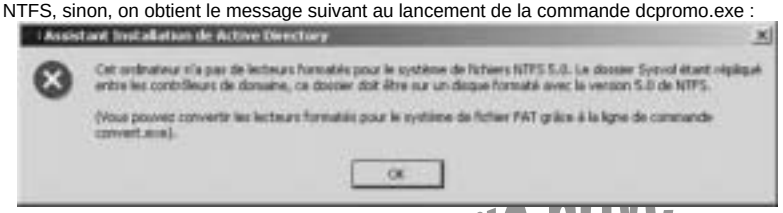
Faites de même pour la zone de recherche inversée.

❑ Installation d'Active Directory : mise en place du premier contrôleur de domaine 2000

Si sous Windows NT 4 Server le choix du statut du serveur se fait à l'installation, sous Windows 2000 Server vous pouvez à tout moment choisir le type de serveur à l'aide de la commande DCPROMO.

Windows 2000 est livré avec un utilitaire, DCPROMO.EXE, qui sert à promouvoir un serveur membre/stand-alone au rang de Contrôleur de Domaine, et vice-versa.

Pour pouvoir passer de serveur membre à Domain contrôleur, il faut absolument que la partition système soit en NTFS, sinon, on obtient le message suivant au lancement de la commande dcpromo.exe :



La conversion d'une partition FAT en NTFS se fait à l'aide de la commande CONVERT (voir support sur NT4 : `CONVERT C: /FS:NTFS` si la partition à convertir est C)

Si aucun serveur DNS n'est installé, l'assistant vous proposera de l'installer.

1. Promotion du premier serveur

Lancez l'utilitaire DCPROMO à partir de « Démarrer / Exécuter ».

Démarrage de l'assistant d'installation d'Active Directory.
Cliquez sur « Suivant ».

C'est le premier contrôleur du domaine !
Cliquez sur « Suivant ».

Aucune arborescence n'existe.
Le domaine créé ne sera pas un domaine enfant (ex : enfant.e-wsc.local) mais la racine d'une nouvelle arborescence.
Cliquez sur « Suivant ».

De même, ce domaine n'est pas rattaché à un autre (notion de forêt).
Ce domaine sera donc à l'origine d'une nouvelle forêt (cette forêt sera donc composée d'un seul arbre qui comportera une seule branche / une feuille ! avec un nid et des oiseaux dedans).
Cliquez sur « Suivant ».

Saisissez votre nom de domaine (le même que pour le serveur DNS bien évidemment !).
Ex : e-wsc.local (local pour les mêmes raisons que pour le DNS).
Cliquez sur « Suivant ».

Le nom Netbios du domaine sera utile pour les clients antérieurs à Windows 2000.
Normalement il correspond au début du nom DNS (ex : e-wsc pour e-wsc.local ou enfant pour enfant.e-wsc.local)
Cliquez sur « Suivant ».

Spécifiez l'emplacement de la base de données et du journal AD.
Cliquez sur « Suivant ».

Ce dossier comporte la définition des stratégies de groupes, les scripts et des informations de réplication.
Cliquez sur « Suivant ».

Le mode « Compatible » de Windows 2000 Server permet d'intégrer ce serveur dans un domaine NT4. Il prendra le rôle de CPD (émulateur CPD).
Le mode « Compatible » supprime certaines fonctionnalités de Windows 2000 Server dans l'administration notamment.
Nous verrons comment passer d'un serveur 2000 en mode « Compatible » à un serveur 2000 « Natif ».
Cliquez sur « Suivant ».

Un mot de passe est demandé afin de protéger l'accès au service de restauration d'ADC.
Ce mot de passe n'est pas lié à celui de l'administrateur.
Cliquez sur « Suivant ».

Récapitulatif des éléments avant la mise en place d'AD.
Cliquez sur « Suivant ».

Active Directory se met en place…
Patientez le temps que l'arbre pousse.

C'est fini !
N'oubliez pas l'arrosage : redémarrez Windows !

Active Directory est installé.

Votre serveur prend donc les rôles suivants :

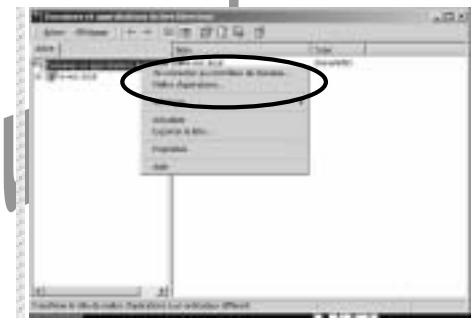
- Maître d'opération :
  - Maître de schéma (rôle unique dans la forêt)
  - Maître de dénomination de domaine (rôle unique dans la forêt)
  - Maître RID (rôle unique dans le domaine)
  - Maître d'infrastructure (rôle unique dans le domaine)
  - Emulateur PDC (rôle unique dans le domaine)
- Serveur de catalogue global (au moins un dans le domaine)

2. Pratique : Identification des rôles des serveurs

2.a Maître de dénomination de domaine

Ouvrez la console « Domaines et approbations Active Directory ».

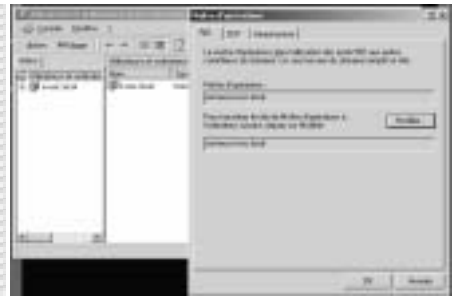
Faites un clic droit sur « Domaines et approbations Active Directory », puis sélectionnez « Maître d'opérations ».



Pour modifier le serveur jouant ce rôle, effectuez cette opération sur le contrôleur de domaine qui deviendra le nouveau maître de dénomination de domaine et cliquez sur le bouton « Modifier ».

2.b Maître RID – Emulateur PDC – Maître d'infrastructure

Lancez l'outil « Utilisateurs et ordinateurs Active Directory » et faites un clic droit sur « Utilisateurs et ordinateurs Active Directory ».
Cliquez ensuite sur Maître d'opérations.



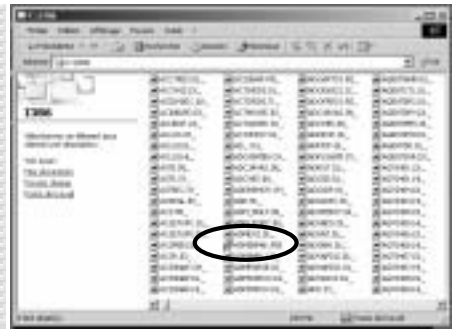
Les trois onglets permettent de voir ou de modifier les trois rôles de maître d'opération.

2.c Maître de schéma

Par défaut vous n'avez aucun outil pour visualiser ce rôle.

2.c.1 Installation des outils d'administration supplémentaires de Windows 2000

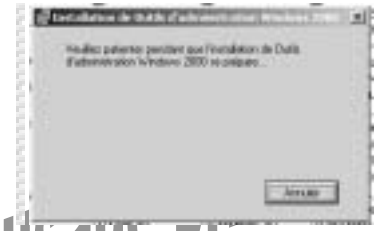
Identifiez le fichier « adminpack.msi » sur le CDRom d'installation de Windows 2000 (ou dans le dossier i386 du disque dur si vous avez copié les fichiers d'installation sur le disque).



Faites un clic droit et installer.

Si vous lancez l'installation à partir du CDRom, vous aurez sans doute un message d'erreur. Pour contrer ce bug, copiez adminpak.msi sur le disque dur, et relancez l'installation.

L'assistant d'installation d'outils d'administration de Windows 2000 démarre…



Cliquez sur « Suivant ».

Choisissez « installer touts les outils d'administration » et cliquez sur « Suivant ».

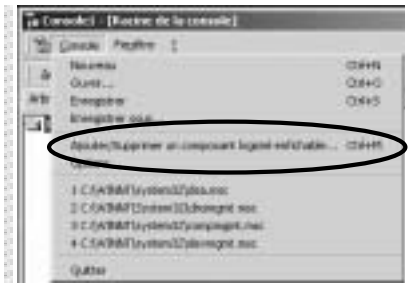
Installation en cours…

Fin de l'installation.
Vous pouvez réinstaller le SP2 de Windows 2000.

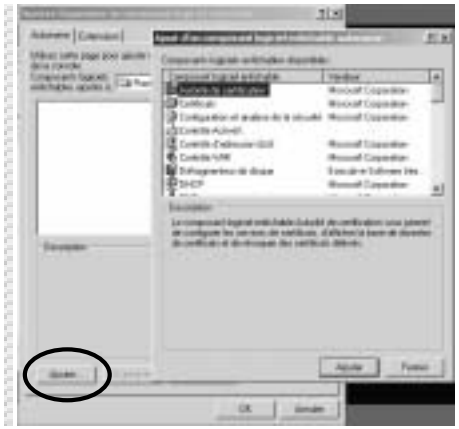
2.c.2 Création d'une nouvelle console de management (MMC)

Lancez l'utilitaire Microsoft Management Console (MMC).
Démarrer / Exécuter / MMC ↵

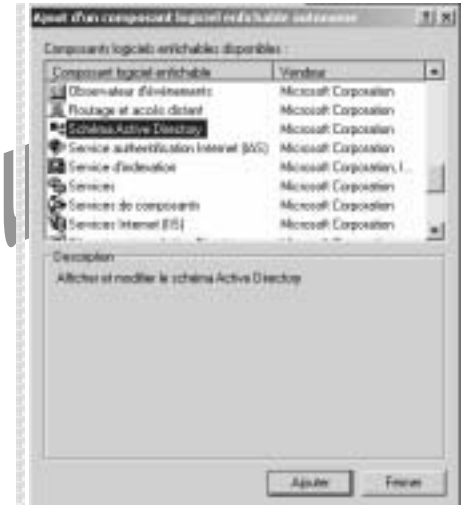
Ajoutez le composant enfichable « Schéma Active Directory » :
Menu Console, Ajouter/supprimer un composant logiciel enfichable…



Cliquez sur le bouton « Ajouter » pour afficher la boite de dialogue « Ajout d'un composant logiciel enfichable autonome ».



Choisissez « Schéma Active Directory » et cliquez sur « Ajouter », puis « Fermer ».



Validez par « OK ».

La nouvelle console est créé, enregistrez la dans le menu Démarrer / outils d'administration.

2.c.3 Connaître quel serveur joue le rôle de maître de schéma

Ouvrez la nouvelle console « Schéma Active Directory ».
Faites un clic droit sur « Schéma Active Directory », cliquez sur « Maître d'opérations ».

2.d Serveur de catalogue global

Lancez la console « Sites et services Active Directory ».
Développez « Sites », puis le nom du site dans lequel se situe le serveur, enfin le serveur (ici « SERVEUR »).

Faites un clic droit sur le connecteur NTDS Settings » puis « Propriétés ».

Par défaut, seul le premier serveur de la forêt, sur lequel Active Directory a été installé, prend ce rôle. Mais vous pouvez ajouter d'autres serveurs de catalogue global.

Entre domaines, les seules informations sur les objets qui sont distribuées sont celles contenues dans le catalogue global. Il est donc intéressant de disposer d'au moins un serveur de catalogue global par domaine.

❑ Désinstallation d'Active Directory

Lancez l'utilitaire DCPROMO et suivez l'assistant pas à pas.

❑ Quelques liens internet

http://www.tutorials-online.com/tutorials/ls/w2k/ad.htm

http://herve-pc.cnrs-orleans.fr/Security/Win2k/ActiveDirectory/ActiveDirectory1.htm

http://microsoft.supinfo.com/articles/ad/

http://www.gmg.ch/zoomout/windows2000/1560/module15.htm

Fin du support