

Notes provisoires

Présentation de la famille Windows Server

Matériel requis

Principes de base de Active Directory

Services d'annuaire Active Directory

Espace de nom

Objet

Classe

Attribut

Conteneur

Arborescence et sous-arborescence

Nom unique

Nom Principal

Schéma

Site

Catalogue global

Arborescence et forêt

Domaine et OU

Passage de Windows NT4 serveur à Windows 2003 Serveur

Présentation de la famille Windows Server

Windows Web Server

Windows Standard Server

Windows Enterprise Server

Windows Datacenter Server

Matériel requis

	STANDARD	ENTERPRISE	DATACENTER	WEB
<i>Fréquence recommandée</i>	550 MHz	733 MHz	733 MHz	550 MHz
<i>RAM recommandée</i>	128 Mo	128 Mo	512 Mo	128 Mo
<i>Nombre de processeurs</i>	1 ou 2	Jusqu'à 8	Minimum : 8 Maximum : 32	1 ou 2
<i>Espace disque nécessaire</i>	1.5 Go	1.5 Go (x86) 2.0 Go (Itanium)	1.5 Go (x86) 2.0 Go (Itanium)	1.5 Go

Principes de base de Active Directory

Active Directory est le service d'annuaire de Windows Server 2000 et 2003.

Active Directory stocke des informations sur les objets placés sur le réseau et facilite la recherche et l'utilisation de ces données pour les administrateurs et les utilisateurs. Active Directory fait appel à une banque de données structurée pour organiser les informations de l'annuaire de manière logique et hiérarchique.

Services d'annuaire Active Directory

Exemples d'annuaire : répertoire téléphonique, table des matières...

Espace de nom

La zone où on peut localiser un composant réseau. Active Directory offre un espace de noms qui permet d'accéder aux objets réseau à partir de leur nom.

Objet

C'est quelque chose de concret comme un utilisateur, une imprimante, un service... qui peut être stocké dans l'annuaire. Chaque objet de Active Directory est une instance d'une classe définie dans le schéma Active Directory.

Classe

Les classes, également appelées "classes d'objet", décrivent les objets d'annuaire qu'il est possible de créer. Chaque classe se compose d'un ensemble d'attributs. Lorsque vous créez un objet, les attributs stockent les informations qui définissent l'objet. La classe Utilisateur, par exemple, se compose de plusieurs attributs, notamment une adresse réseau et un répertoire de base. Chaque objet stocké dans Active Directory est une instance d'une classe d'objet.

Attribut

Les attributs se définissent de façon distincte des classes. Chaque attribut est défini une seule fois et peut être réutilisé dans plusieurs classes. Par exemple, l'attribut Description se retrouve dans plusieurs classes, mais n'est défini qu'une seule fois dans le schéma pour des raisons d'homogénéité.

Les attributs décrivent des objets. Chacun d'entre eux possède sa propre définition, qui décrit le type d'informations que vous pouvez spécifier pour l'attribut. Chaque attribut du schéma est spécifié dans la classe attribut-schéma, qui détermine les informations que chaque définition d'attribut doit contenir.

La liste des attributs applicables à un objet particulier dépend de la classe de laquelle l'objet est une instance et de toutes les superclasses de la classe de cet objet.

Conteneur

C'est une enveloppe qui contient des objets ou d'autres conteneurs.

Nom unique

Ou DN pour Distinguished Name LDAP.

Le DN est l'identifiant unique d'un objet et contient toutes les informations nécessaires pour retrouver l'objet dans l'annuaire. Ils sont complexes mais sans ambiguïté. Prenons l'exemple d'un utilisateur John Smith travaillant pour la section MSPress chez Microsoft. Son nom distingué est :

/O=Internet/DC=COM/DC=Microsoft/DC=MSPress/CN=Users/CN= John Smith. Le nom distingué identifie tous les conteneurs qui se trouvent entre le sommet de l'arbre et l'objet en question. Les conteneurs sont séparés par un slash et un identificateur.

Le nom distingué relatif est CN=John Smith : il identifie l'objet de façon unique dans son conteneur.

DC : Domain Controller

OU : Organizational Unit

CN : Common Name

Nom Principal

Exemple : smith@mspress.microsoft.com

Schéma

Schéma est un terme très fréquemment employé dans le contexte des bases de données.

Le schéma Active Directory est l'ensemble des définitions qui régissent les types d'objets, ainsi que les types d'informations sur ces objets, qu'il est possible de stocker dans Active Directory. Ces définitions étant elles-mêmes stockées sous forme d'objets, Active Directory peut gérer les objets du schéma par le biais des mêmes procédures de gestion que pour le reste des objets figurant dans l'annuaire. Le schéma contient deux types de définitions : des attributs et des classes. Les attributs et les classes s'appellent également des "objets de schéma" ou des "métadonnées". En gros résumé, le schéma est la structure de la DB Active Directory. Le schéma est unique pour une forêt donnée et il est répliqué à travers la forêt.

Site

C'est un emplacement géographique. Les sites correspondent aux sous-réseaux IP logiques.

Un site est un ensemble de sous-réseaux IP connectés entre eux par des liaisons rapides et fiables. Ce qui permet aux applications de trouver le serveur le plus proche sur le réseau. Et de diminuer ainsi le trafic WAN.

Catalogue global

Un catalogue global est un **contrôleur de domaine** qui stocke une copie de tous les objets Active Directory présents dans une **forêt**. Un catalogue global concerne une forêt. Il stocke également les attributs de recherche les plus courants de chaque objet. Il contient aussi une copie complète de tous les objets de l'annuaire pour son domaine hôte et une copie partielle

de tous les objets pour tous les autres domaines de la forêt. Il permet ainsi d'effectuer efficacement des recherches sans avoir à faire inutilement référence aux contrôleurs de domaine.

Un catalogue global se crée automatiquement sur le contrôleur de domaine initial de la forêt. Vous pouvez en ajouter un à d'autres contrôleurs de domaine ou changer l'emplacement par défaut du catalogue global pour le placer sur un autre contrôleur de domaine.

Un catalogue global assure les rôles suivants dans l'annuaire :

- **Recherche d'objets** : un catalogue global permet aux utilisateurs de rechercher des données d'annuaire à travers tous les domaines d'une forêt, quel que soit l'endroit où ces données se trouvent. Les recherches effectuées au sein d'une forêt sont très rapides et n'engendrent qu'un trafic minimal sur le réseau.

Lorsque vous recherchez des utilisateurs ou des imprimantes à partir du menu Démarrer ou sélectionnez l'option Tout l'annuaire dans une requête, la recherche se fait en fait dans un catalogue global. Une fois les critères de recherche spécifiés, votre demande est acheminée vers le port 3268 de catalogue global par défaut et envoyée à un catalogue global pour résolution.

- **Authentification des noms d'utilisateur principaux** : un catalogue global résout les noms d'utilisateur principaux lorsque le contrôleur de domaine assurant l'authentification ne connaît pas le compte. Par exemple, si un compte d'utilisateur se trouve sur exemple1.microsoft.com et que l'utilisateur décide d'ouvrir une session sous le nom principal utilisateur1@exemple1.microsoft.com à partir d'un ordinateur situé sur exemple2.microsoft.com, le contrôleur de domaine de exemple2.microsoft.com n'est pas en mesure de trouver le compte de l'utilisateur. Il contacte alors le serveur de catalogues global pour terminer l'ouverture de session.
- **Fourniture des informations relatives à l'appartenance aux groupes universels dans un environnement à plusieurs domaines** : contrairement aux appartenances aux groupes globaux, qui sont stockées sur chaque domaine, les appartenances aux groupes universels résident uniquement dans un catalogue global. Par exemple, lorsqu'un utilisateur appartenant à un groupe universel ouvre une session sur un domaine défini sur le niveau de fonctionnalité de domaine Windows 2000 en mode natif ou version ultérieure, le catalogue global fournit les informations sur l'appartenance aux groupes universels pour le compte d'utilisateur.

Si aucun catalogue global n'est disponible lorsqu'un utilisateur ouvre une session sur un domaine Windows 2000 en mode natif ou version ultérieure, l'ordinateur utilise les informations d'identification figurant dans le cache pour connecter l'utilisateur, si ce dernier a déjà ouvert une session sur le domaine par le passé. Si l'utilisateur n'a jamais ouvert de session sur le domaine auparavant, il peut uniquement se connecter à l'ordinateur local.

Remarques :

- Les membres du groupe des administrateurs de domaine peuvent ouvrir une session sur le réseau même lorsque aucun catalogue global n'est disponible.
- Il n'y a pas d'outil pour examiner le CG.

Domaine et OU

Domaines Windows 2000 et Windows Server 2003

Le modèle de domaine Windows NT 4 n'était pas très évolutif. Les approbations non transitives à sens unique du modèle de domaine Windows NT 4 impliquaient de lourdes charges administratives dans les implémentations de grandes entreprises. Le modèle de domaine Windows 2000 ou Windows Server 2003 ne présente plus cet inconvénient, grâce en grande partie à une nouvelle approche concernant les approbations, mais aussi à la redéfinition du concept de domaine dans son ensemble, conformément à des normes industrielles, telles que LDAP (Lightweight Directory Access Protocol) et DNS (Domain Name Service).

Domaines

Le domaine Windows 2000 ou Windows Server 2003 est une limite administrative. Les droits d'administration ne dépassent pas les limites d'un domaine ni ne sont automatiquement transférés sur l'ensemble d'une arborescence de domaine Windows 2000 ou Windows Server 2003. Par exemple, dans le cas d'une arborescence de domaine comprenant les domaines A, B et C, où A est le domaine parent de B et B celui de C, les utilisateurs disposant de droits d'administration sur le domaine A ne disposent pas des mêmes droits sur le domaine B, et ceux disposant de droits d'administration sur B ne disposent pas de ces droits sur C. Pour obtenir des droits d'administration sur un domaine donné, une autorité supérieure doit les accorder. Ceci ne signifie toutefois pas qu'un administrateur ne peut pas disposer de droits d'administration dans plusieurs domaines ; cela signifie simplement que tous les droits doivent être définis de manière explicite.

Hiérarchie du domaine

Dans les réseaux Windows 2000 et Windows Server 2003, les domaines sont organisés selon une hiérarchie. Cette nouvelle approche hiérarchique a donné naissance aux concepts de forêt et d'arborescence. Ceux-ci, combinés au concept des domaines, permettent aux organisations de gérer efficacement la structure de réseau Windows 2000 et Windows Server 2003.

Domaines

L'essence du modèle de domaine Windows 2000 et Windows Server 2003 n'a pas changé ; il s'agit toujours du domaine. Un domaine est une limite administrative qui, dans Windows 2000 et Windows Server 2003, représente un espace de noms correspondant à un domaine DNS.

Le premier domaine créé dans un déploiement Windows 2000 ou Windows Server 2003 s'appelle le domaine racine. Comme son nom l'indique, il constitue la racine de tous les autres domaines créés dans l'arborescence du domaine. Les structures de domaine Windows 2000 et Windows Server 2003 étant associées à des hiérarchies de domaine DNS, la structure des domaines Windows 2000 et Windows Server 2003 est semblable à celle des hiérarchies de

domaine DNS. Les domaines racine sont des domaines, tels que microsoft.com ; ils constituent les racines de leurs hiérarchies DNS et les racines de la structure de domaine Windows 2000 et Windows Server 2003.

Les domaines créés par la suite dans une hiérarchie de domaine Windows 2000 et Windows Server 2003 donnée deviennent les domaines enfants du domaine racine. Par exemple, si msdn est un domaine enfant de microsoft.com, le domaine msdn devient msdn.microsoft.com.

Comme vous pouvez le constater, Windows 2000 et Windows Server 2003 requièrent soit un domaine racine, soit un domaine enfant dans une hiérarchie de domaine. Les noms de domaine doivent être uniques au sein d'un même domaine parent sous Windows 2000 et Windows Server 2003 ; par exemple, deux domaines ne peuvent pas s'appeler msdn et être des domaines enfants directs du domaine racine microsoft.com. Vous pouvez toutefois avoir deux domaines qui s'appellent msdn dans la hiérarchie de domaine globale. Par exemple, deux domaines peuvent s'appeler msdn.microsoft.com et msdn.devprods.microsoft.com ; l'espace de noms microsoft.com possède un seul domaine enfant appelé msdn et l'espace de noms devprods.microsoft.com possède également un seul domaine enfant appelé msdn.

On appelle ce concept le "partitionnement logique". La plupart des grandes organisations qui nécessitent plus d'un domaine Windows 2000 ou Windows Server 2003 sont organisées selon une structure logique qui divise les responsabilités ou les tâches. Le fait de diviser une organisation en plusieurs unités (parfois appelées "divisions" dans le jargon d'entreprise) permet d'en simplifier la gestion. L'organisation est en effet partitionnée selon une structure plus logique, qui permet éventuellement de répartir le travail entre différentes sections. Ou, si vous préférez, lorsque des unités commerciales logiques (divisions) sont rassemblées sous l'égide d'une entité plus importante (une entreprise par exemple), ces divisions créent une entité plus importante. Bien que les tâches entre divisions puissent être très différentes, les divisions forment ensemble une entité plus grande et complète. Ce concept s'applique également à l'ensemble des domaines Windows 2000 et Windows Server 2003 qui forment une entité d'espace de noms plus grande et contiguë, appelée "arborescence".

Unités d'organisation

Les unités d'organisation (UO) permettent aux administrateurs de créer des limites administratives au sein d'un domaine. Grâce aux UO, les administrateurs peuvent déléguer des tâches administratives à d'autres administrateurs subordonnés sans leur accorder de privilèges administratifs étendus sur l'ensemble du domaine.

L'exemple suivant démontre l'utilité des unités d'organisation. Supposons que le service de vente de votre organisation dispose de ses propres administrateurs et ressources réseau telles que des imprimantes et des serveurs, et assure le financement de ces ressources au moyen d'un budget propre. Les administrateurs réseau du service souhaitent obtenir le contrôle des ressources du service, ainsi que des stratégies et d'autres éléments administratifs au sein de celui-ci. Toutefois, le service de vente fait partie du domaine d'entreprise.

Dans un réseau Windows NT 4, les administrateurs du service de vente devraient être ajoutés au groupe d'administrateurs du domaine pour disposer des droits d'administration dont ils ont besoin pour administrer l'unité de service de vente. L'appartenance à ce groupe d'administrateurs leur donnerait le contrôle administratif de l'ensemble du domaine

d'entreprise (et pas seulement de l'unité de service de vente). L'octroi de droits aussi étendus ne serait pas approprié, mais ce serait la seule manière d'accorder aux administrateurs du service de vente le contrôle des ressources et stratégies du service.

Ceci a été modifié dans Windows 2000 et Windows Server 2003, grâce à l'introduction d'unités d'organisation. Dans un réseau Windows 2000 ou Windows Server 2003, les superviseurs du réseau peuvent créer des UO, y compris une UO du service de vente, au sein même de la structure du domaine et établir ainsi de nouvelles limites administratives plus restreintes.

Par exemple, vous pourriez créer une unité d'organisation pour le service de vente et accorder aux administrateurs du service des droits d'administration complets uniquement pour cette UO et non pour les autres secteurs du domaine d'entreprise. Grâce à la création d'unités d'organisation, le groupe des administrateurs du domaine (qui accorde des droits d'administration sur l'ensemble du domaine, y compris ses UO) peut être limité aux administrateurs dont les responsabilités couvrent l'ensemble du domaine. Ceci permet d'obtenir une sécurité accrue et un réseau mieux géré.

Et si votre organisation a besoin d'unités d'organisation au sein d'unités d'organisation? Est-il possible d'imbriquer des UO ? La réponse à cette question est Oui, mais il existe certaines limites dues à la perte de performances. Vous pouvez imbriquer des UO, mais vous rencontrerez des problèmes de performances si vous les imbriquez sur plus de 15 niveaux. Il existe d'autres considérations pouvant affecter votre décision d'imbriquer ou non des UO (ou même d'utiliser ou non des UO).

Arborescence et sous-arborescence

Les arborescences, parfois appelées arborescences de domaine, sont des ensembles de domaines Windows 2000 et Windows Server 2003 qui forment un espace de noms contigu. Une arborescence de domaine est formée dès qu'un domaine enfant est créé et associé à un domaine racine donné. Sur le plan technique, une arborescence est une hiérarchie de nommage DNS contiguë ; sur le plan conceptuel, une arborescence de domaine ressemble à un arbre à l'envers : le domaine racine en haut, et les branches (les domaines enfants) en bas.

Une arborescence de domaine permet aux organisations de créer une structure logique de domaines qui respecte et reflète l'espace de noms DNS.

Forêt :

Certaines organisations peuvent avoir plusieurs domaines racines, par exemple microsoft.com et microsoft.com. Toutefois, l'organisation en elle-même est une entité indépendante. Dans de tels cas, les différentes arborescences de domaine forment un espace de noms non contigu appelé "forêt". Une forêt est constituée d'une ou plusieurs hiérarchies d'arborescence de domaine contiguës qui forment une organisation donnée. Par conséquent, une organisation qui ne possède qu'un seul domaine dans son arborescence de domaine est aussi considérée comme une forêt. La forêt est le conteneur le plus grand du schéma.

Le modèle de forêt permet aux organisations qui ne forment pas un espace de noms contigu de préserver la continuité de la structure de leur domaine agrégé dans toute l'organisation. Par exemple, si l'organisation Microsoft.com, pouvait dénicher suffisamment d'argent pour acheter une entreprise appelée Microsoftbis, qui possède déjà sa propre structure de

répertoire, les structures de domaine des deux entités pourraient être combinées dans une forêt. Le fait d'avoir une seule forêt présente les avantages suivants : tout d'abord, les relations d'approbation peuvent être gérées plus facilement (ce qui permet aux utilisateurs d'une arborescence de domaine d'accéder aux ressources dans l'autre arborescence) ; ensuite, le catalogue global incorpore les informations des objets pour la forêt tout entière, ce qui permet d'effectuer des recherches dans toute l'organisation ; finalement, le schéma Active Directory s'applique à toute la forêt. Même si une forêt peut comprendre plusieurs arborescences de domaine, elle représente une seule entreprise. La création de la forêt permet aux domaines membres de partager des informations (via le catalogue global).

Conception de l'Active Directory :

Il faut 4 planifications à réaliser :

Plan de forêt
Stratégie de domaine / DNS
Structure des Unités d'organisation
Topologie des sites

L'installation d'un domaine Active Directory s'effectue en trois étapes :

Installation d'un serveur Windows 200i.
Configuration du DNS en tant que client ou en tant que service sur ce serveur.
Lancement de l'assistant d'installation Active Directory : DCPRMO.exe.

Le premier domaine Active Directory installé devient le DC du domaine racine de la première forêt.

Windows 200i serveur s'installe toujours en tant que serveur membre sauf lors de la mise à jour d'un PDC NT4 !

Maîtres d'opérations/FSMO :

C'est une fonction particulière qui est prise en charge par certains DC.

Sous NT4, seul le PDC avait un droit en écriture sur la SAM.

Sous Windows 2003 (et 2000), tous les DCs sont égaux mais certains le sont plus que d'autres !!!

Il y a cinq rôles FSMO dans AD :

Contrôleur de schéma.

Maître d'attribution des noms de domaine.

Maître des ID relatifs (RID)

Maître de l'émulateur de PDC

Maître d'infrastructure

Il n'y a qu'un seul Contrôleur de schéma et qu'un seul Maître d'attribution des noms de domaine par forêt. Mais chaque domaine possède son propre Maître des ID relatifs, Maître de l'émulateur de PDC et Maître d'infrastructure.

Rôles FSMO (*Flexible Single Master Operations*)

Dans une forêt, au moins cinq rôles FSMO sont attribués à un ou plusieurs contrôleurs de domaine. Les cinq rôles FSMO sont les suivants :

- **Contrôleur de schéma.** Le contrôleur de domaine du schéma principal contrôle toutes les mises à jour et modifications apportées au schéma. Pour mettre à jour le schéma d'une forêt, vous devez avoir accès au contrôleur de schéma. Il ne peut y avoir qu'un seul contrôleur de schéma dans l'ensemble de la forêt.
- **Maître des noms de domaine.** Le contrôleur de domaine du maître des noms de domaine contrôle l'ajout ou la suppression de domaines dans la forêt. Il ne peut y avoir qu'un seul maître des noms de domaine dans l'ensemble de la forêt.
- **Maître d'infrastructure.** L'infrastructure est responsable de la mise à jour des références des objets de son domaine vers des objets dans d'autres domaines. À tout moment, il ne peut y avoir qu'un contrôleur de domaine qui joue le rôle de maître d'infrastructure dans chaque domaine.
- **Maître d'ID relatif (RID).** Le maître RID est responsable du traitement des requêtes du pool RID provenant de tous les contrôleurs de domaine d'un domaine particulier. À tout moment, il ne peut y avoir qu'un contrôleur de domaine qui joue le rôle de maître RID dans la forêt.

Émulateur PDC. L'émulateur PDC est un contrôleur de domaine qui s'annonce comme le PDC aux stations de travail, aux serveurs membres et aux contrôleurs de domaine qui exécutent des versions antérieures de Windows.

Passage de Windows NT4 serveur à Windows 2003 Serveur :

La migration d'un domaine NT4 vers un Active Directory 2003 est semblable à la migration vers un serveur 2000 sauf qu'il y a plus d'outils et de documentations.

Première étape : inventaire de votre réseau physique : les sous-réseaux, le nombre et le type de serveurs... Et grand nettoyage de printemps.

Deuxième étape :

Installer un serveur Windows 2003 pour l'étudier. (se faire la main sur les serveurs d'impression, les serveurs de fichiers).

Troisième étape :

Il faut donc avant d'aborder la procédure avoir mis sur papier :

- Le type de forêt
- Le nombre de domaines
- La présence ou non de sites physiques
- La disposition des Contrôleurs de domaines et catalogues globaux
- L'arborescence des OU

Quatrième étape :

Choisir entre la mise à jour du domaine NT4 et la création d'un nouvel Active Directory 2003 (2000) avec migration des utilisateurs.

Stratégie 1 – Upgrade d'un domaine existant :

0. Backup des serveurs NT4 PDC et BDC.

1. Monter un nouveau NT4 BDC sur le domaine.
2. Promouvoir cette machine en PDC (NT4)
3. Mettre hors circuit un serveur NT4 BDC (comme sauvegarde)
4. Upgrade le nouveau serveur NT4 PDC en Win200x
5. Monter d'autres serveurs Win200x Domaine Contrôleurs si nécessaire
6. Upgrade les autres NT4 BDC si nécessaire

PROS: Pas de changement pour les clients.

CONS: Le domaine NT4 (qui fonctionne) va être mis en jeu.
Les serveurs n'auront pas une nouvelle installation propre.

UNDO: En cas de difficulté, retirer le DC 2000 et repartir sur le BDC mis de côté pour sauvegarde,
Et le promouvoir en PDC.

Stratégie 1bis – Upgrade d'un domaine existant avec nouvelle installation:

0. Backup des serveurs NT4 PDC et BDC.
1. Monter un nouveau NT4 BDC sur le domaine.
2. Promouvoir cette machine en PDC (NT4)
3. Mettre hors circuit un serveur NT4 BDC (comme sauvegarde)
4. Upgrade le nouveau serveur NT4 PDC en Win200x
5. Monter un nouveau serveur 200x en Domain Contrôleur
6. Transférer les FSMO rôles du "PDC" à ce nouveau DC
7. Mettre le premier DC hors circuit
8. Monter d'autres serveurs Win200x DomaineContrôleurs si nécessaire

PROS: Pas de changement pour les clients.
Installation propre sur tous les serveurs.

CONS: Le domaine NT4 (qui fonctionne) va être mis en jeu.
Plus gourmand en temps et en ressources.

UNDO:

En cas de difficulté, retirer le DC 2000 et repartir sur le BDC mis de côté pour sauvegarde,
Et le promouvoir en PDC.

STRATEGIE #2 – Construire un nouveau domaine ACTIVE DIRECTORY

0. Backup des serveurs NT4 PDC et BDC.
1. Construire un nouveau serveur 200X et mettre en place l'Active Directory
2. . Monter d'autres serveurs Win200x DomaineContrôleurs
3. Etablir un Trust entre les domaines NT4 et Win200x
4. Migrer les utilisateurs et les machines dans le nouveau domaine
5. Finir la migration, enlever le trusts, et éliminer NT4

PROS: L'ancien domaine reste accessible.
Moins éprouvant pour les administrateurs.

CONS: Requièrre plus de temps et de hardware. D e plus, vous ne pouvez pas utiliser le même nom NetBIOS pour le nouveau domaine AD que celui du domaine NT4 (qui existe toujours).

UNDO: Tant que le domaine NT4 existe, on peut revenir en arrière.

Cette méthode est basée sur l'historique des SIDs.

Elle utilise l'outil ADMT (Active Directory Migration Tool). l'outil de migration Active Directory (ADMT) pour mettre les utilisateurs, les serveurs, les imprimantes, etc., à niveau vers le nouveau domaine Active Directory

Remarques :

Pour faire la mise à niveau, il faut :
Une partition NTFS.

Etre en service pack 6.
Opérer sur le PDC en premier.

Références et lectures :

Microsoft Knowledge Base Article – 326209
« Mettre à niveau un contrôleur principal de domaine Windows NT 4.0 vers
Windows Server 2003 »

Microsoft Knowledge Base Article – 325851
Configurer l'outil de migration Active Directory pour une migration de Windows NT 4.0 vers
Windows Server 2003

Microsoft Knowledge Base Article – 816106
Vérifier une installation Active Directory sous Windows Server 2003