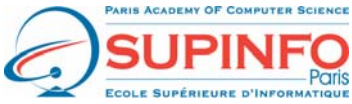
http://www.laboratoire-microsoft.org

Essentiel Windows 2003

Planification, implémentation et maintenance d'une infrastructure Active Directory Microsoft Windows Server 2003

Auteurs : Brahim NEDJIMI, Matthieu MARTINEAU & Loïc THOBOIS
Revu par : Nicolas MILBRAND & Camille BEFFARA
Version 0.95 – 01-03-2006



Ecole Supérieure d'Informatique de Paris
23. rue Château Landon 75010 – PARIS
www.supinfo.com

Table des matières

1. Introduction à l'infrastructure Active Directory

1.1. Présentation d'Active Directory

Active Directory permet de centraliser, de structurer, d'organiser et de contrôler les ressources réseau dans les environnements Windows 2000/2003. La structure Active Directory permet une délégation de l'administration très fine pouvant être définie par types d'objets.

1.1.1. Définition d'Active Directory

Active Directory est un annuaire des objets du réseau, il permet aux utilisateurs de localiser, de gérer et d'utiliser facilement les ressources.

Il permet de réaliser la gestion des objets sans liens avec la disposition réelle ou les protocoles réseaux employés. Active Directory organise l'annuaire en sections, ce qui permet de suivre le développement d'une société allant de quelques objets à des millions d'objets.

Combiné aux stratégies de groupes, Active directory permet une gestion des postes distants de façon complètement centralisée.

1.1.2. Objets Active Directory

Active Directory stocke des informations sur les objets du réseau. Il existe plusieurs types d'objets :

- serveurs
- domaines
- sites
- utilisateurs
- ordinateurs
- imprimantes
- …

Chaque objet possède un ensemble d'attributs regroupant diverses informations permettant par exemple d'effectuer des recherches précises dans l'annuaire (trouver l'emplacement physique d'une imprimante, le numéro de téléphone ou l'adresse d'un utilisateur, le système d'exploitation d'un serveur…).

1.1.3. Schéma Active Directory

Le schéma Active Directory stocke la définition de tous les objets d'Active Directory (ex : nom, prénom pour l'objet utilisateur).

Il n'y a qu'un seul schéma pour l'ensemble de la forêt, ce qui permet une homogénéité de l'ensemble des domaines.

Le schéma comprend deux types de définitions :

- **Les classes d'objets** : Décrit les objets d'Active Directory qu'il est possible de créer. Chaque classe est un regroupement d'attributs.
- **Les attributs** : Ils sont définis une seul fois et peuvent être utilisés dans plusieurs classes (ex : Description).

Le schéma est stocké dans la base de données d'Active Directory ce qui permet des modifications dynamiques exploitables instantanément.

1.1.4. Catalogue global

Le catalogue global contient une partie des attributs les plus utilisés de tous les objets Active Directory. Il contient aussi les informations nécessaires pour déterminer l'emplacement de tout objet de l'annuaire.

Le catalogue global permet aux utilisateurs d'effectuer 2 tâches importantes :

- Trouver des informations Active Directory sur toutes la forêt, quel que soit l'emplacement des ces données.
- Utiliser des informations d'appartenance à des groupes universels pour ouvrir une session sur le réseau.

Un serveur de catalogue global est un contrôleur de domaine qui conserve une copie du catalogue global et peut ainsi traiter les requêtes qui lui sont destinées. Le premier contrôleur de domaine installé au sein d'une forêt est automatiquement serveur de catalogue global. Il est possible de configurer d'autres contrôleurs de domaine en tant que serveur de catalogue global afin de réguler le trafic.

✍ L'authentification d'ouverture de session ne peut se faire que sur un contrôleur de domaine.

1.1.5. Protocole LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole du service d'annuaire utilisé pour interroger et mettre à jour Active Directory.

Chaque objet de l'annuaire est identifié par une série de composants qui constituent son chemin d'accès LDAP au sein d'Active Directory (CN=Loïc THOBOIS, OU=Direction, DC=labo-microsoft, DC=lan).

- **DC** : Composant de domaine (lan, com, labo-microsoft, …)
- **OU** : Unité d'organisation (contient des objets)
- **CN** : Nom usuel ou nom commun(Nom de l'objet)

Les chemins d'accès LDAP comprennent les éléments suivants :

- **Les noms uniques** : le nom unique identifie le domaine dans lequel est situé l'objet, ainsi que son chemin d'accès complet (ex : CN=Brahim NEDJIMI, OU=Direction, DC=labo-microsoft, DC=lan)
- **Les noms uniques relatifs** : partie du nom unique qui permet d'identifier l'objet dans son conteneur (ex : Brahim NEDJIMI).

1.2. Structure logique d'Active Directory

La structure logique d'Active Directory offre une méthode efficace pour concevoir une hiérarchie.

Les composants logiques de la structure d'Active Directory sont les suivants :

1.2.1. Les Domaines

Unité de base de la structure Active Directory, un domaine est un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données d'annuaire. Un domaine a un nom unique sur le réseau.

Dans un environnement Windows 2000/2003, le domaine sert de limite de sécurité. Le rôle d'une limite de sécurité est de restreindre les droits d'un administrateur ou de tout autre utilisateur avec pouvoir uniquement aux ressources de ce domaine et que seuls les utilisateurs explicitement promus puissent étendre leurs droits à d'autres domaines.

Dans un domaine Windows 2000/2003, tous les serveurs maintenant le domaine (contrôleurs de domaine) possèdent une copie de l'annuaire d'Active Directory. Chaque contrôleur de domaine est capable de recevoir ou de dupliquer les modifications de l'ensemble de ses homologues du domaine.

1.2.2. Les Unités d'organisation

Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein du domaine. Il peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation.

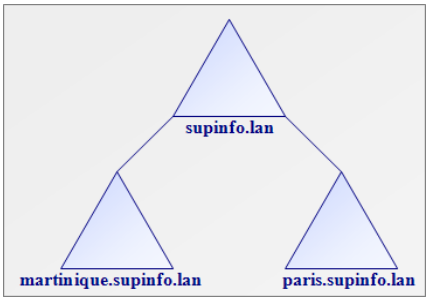
Les unités d'organisation permettent d'organiser de façon logique les objets de l'annuaire (ex : représentation physique des objets ou représentation logique).

Les unités d'organisation permettent aussi de faciliter la délégation de pouvoir selon l'organisation des objets et de contrôler l'environnement des utilisateurs et ordinateurs grâce à l'application de stratégies de groupe (GPO)

1.2.3. Les Arborescences

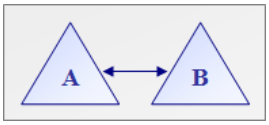
Le premier domaine installé est le domaine racine de la forêt. Au fur et à mesure que des domaines lui sont ajoutés, cela forme la structure de l'arborescence ou la structure de la forêt, selon les exigences pour les noms de domaine.

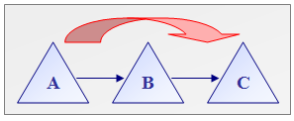
Une **arborescence** est un ensemble de domaines partageant un espace de nom contigu. Par exemple, *supinfo.lan* est le domaine parent du domaine *paris.supinfo.lan* et du domaine *martinique.supinfo.lan* (les deux domaines enfant et le domaine parent ont la chaîne de caractère supinfo.lan en commun).



La relation d'approbation entre un domaine enfant et son domaine parent est de type bidirectionnel transitif.

Une relation bidirectionnelle permet à deux domaines de s'approuver mutuellement. Ainsi le domaine A approuve le domaine B et le domaine B approuve le domaine A.

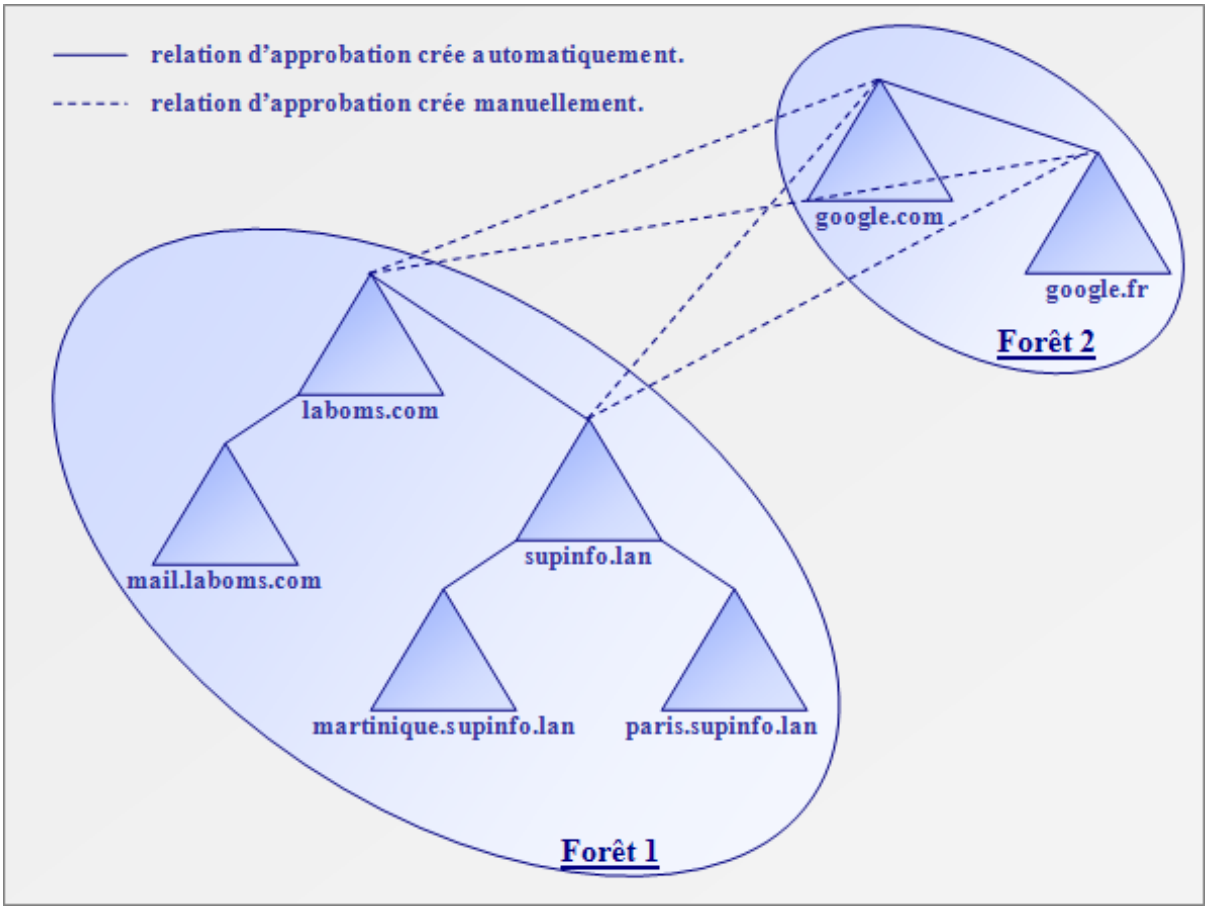




On dispose de trois domaines nommés A, B et C. A approuve B et B approuve C. La relation d'approbation transitive implique donc que A approuve C.

1.2.4. Les forêts

Une **forêt** est un ensemble de domaines (ou d'arborescences) n'ayant pas le même nom commun mais partageant un schéma et un catalogue global commun. Par exemple, une même forêt peut rassembler deux arborescences différentes comme laboms.com et supinfo.lan.



Par défaut, les relations entre les arborescences ou les domaines au sein d'une forêt sont des relations d'approbation bidirectionnelles transitives. Il est possible de créer manuellement des relations d'approbation entre deux domaines situés dans deux forêts différentes. De plus Windows Server 2003 propose un niveau fonctionnel permettant de définir des relations d'approbations entre différentes forêts.

1.2.5. Les rôles de maîtres d'opération

Avec Windows NT 4.0, les contrôleurs de domaine suivent un schéma maître/esclave. Ainsi on distingue les contrôleurs de domaine primaires ou PDC (Primary Domain Controler) accessibles en lecture/écriture et les contrôleurs de domaine secondaires ou BDC (Backup Domain Controler) uniquement accessibles en lecture.

Dans un domaine Windows 2000/2003, cette notion n'existe plus, on parle de contrôleurs de domaine multi-maîtres. En effet, les modifications d'Active Directory peuvent être faîtes sur n'importe quel contrôleur de domaine. Cependant, il existe des exceptions pour lesquelles les modifications sont réalisées sur un contrôleur de domaine spécifiques. Ces exceptions sont nommées rôles de maître d'opération et sont au nombre de cinq :

- **Contrôleur de schéma** : C'est le seul contrôleur de domaine habilité à modifier et à mettre à jour le schéma.

- **Maître d'attribution des noms de domaine :** Il permet d'ajouter ou de supprimer un domaine dans une forêt.
- **Emulateur PDC** : Il ajoute la compatibilité avec les BDC sous Windows NT 4.0. Il gère également le processus de verrouillage des comptes utilisateurs, les changements de mots de passe et toutes les modifications faites sur des objets de stratégie de groupe.
- **Maître d'identificateur relatif ou maître RID** : Il distribue des plages d'identificateurs relatifs (RID) à tous les contrôleurs de domaine afin de générer les identificateurs de sécurité (SID)..
- **Maître d'infrastructure** : Il permet de mettre à jour les éventuelles références d'un objet dans les autres domaines lorsque cet objet est modifié (déplacement, suppression,…).

Les deux premiers rôles sont assignés au niveau de la forêt et les trois derniers au niveau du domaine. Ainsi pour chaque domaine crée dans une forêt, il faut définir le ou les contrôleurs de domaine qui auront les rôles émulateur PDC, maître RID et maître d'infrastructure.

Par défaut le premier contrôleur de domaine d'une nouvelle forêt cumule les cinq rôles.

1.3. Structure Physique d'Active Directory

Dans Active Directory, la structure logique et la structure physique sont distinctes. La structure physique permet d'optimiser les échanges d'informations entre les différents contrôleurs de domaine et ce en fonction des débits assurés par les réseaux qui les connectent.

1.3.1. Contrôleurs de domaine

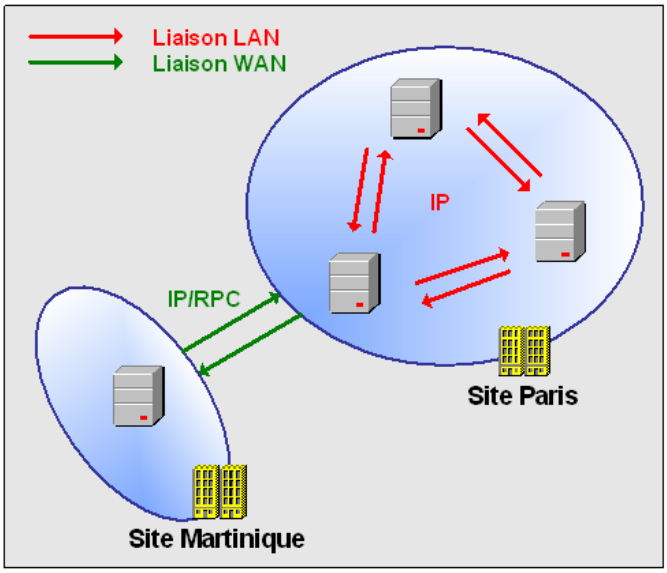
Un contrôleur de domaine est un ordinateur exécutant Windows 2000 Server ou Windows 2003 Server qui stocke un répliqua de l'annuaire. Il assure la propagation des modifications faites sur l'annuaire. Il assure l'authentification et l'ouverture des sessions des utilisateurs, ainsi que les recherches dans l'annuaire.

Un domaine peut posséder un ou plusieurs contrôleurs de domaine. Dans le cas d'une société constituée de plusieurs entités dispersées géographiquement, on aura besoin d'un contrôleur de domaine dans chacune de ses entités.

1.3.2. Sites et liens de sites

Un site est une combinaison d'un ou plusieurs sous réseaux connectés entre eux par une liaison à haut débit fiable (liaison LAN). Définir des sites permet à Active Directory d'optimiser la duplication et l'authentification afin d'exploiter au mieux les liaisons les plus rapides.

En effet, les différents sites d'une entreprise sont souvent reliés entres eux par des liaisons bas débit et dont la fiabilité est faible (liaisons WAN). La création de liens de sites permet de prendre en compte la topologie physique du réseau pour les opérations de réplication. Un lien de site avec des paramètres spécifiques. Ces paramètres peuvent prendre en compte le coût de la liaison, la planification ainsi que l'intervalle de temps entre deux réplications.



Dans l'exemple ci-contre, on dispose de deux sites : Paris et Martinique. Ces deux sites sont reliés par une liaison WAN proposant une bande passante de 128kb/s. A l'intérieur du site Paris, les contrôleurs de domaine sont interconnectés entre eux par le biais d'un commutateur gigabit (avec une bande passante de 1000 Mb/s).

En créant un lien de site, il est possible forcer la réplication entre les deux sites à s'effectuer toutes les 90 minutes uniquement entre 20 heures et 6 heures.

La réplication Active Directory peut utiliser deux protocoles différents :

- **RPC (Remote Procedure Call)** pour les liaisons intra-site et intersites (ce protocole est aussi appelé RPC sur IP)
- **SMTP (Simple Mail Transfer Protocol)** pour les liaisons inter site (selon certaines conditions énoncées ci-dessous)

Attention, SMTP ne peut pas être utilisé pour répliquer une partition de domaine ! Par contre on peut utiliser SMTP entre deux sites pour répliquer la partition de configuration, la partition de schéma et les partitions de domaines partielles stockées sur les serveurs de catalogue global.

Dans l'exemple ci-dessus, on ne peut pas utiliser le protocole SMTP entre le site PARIS et le site MARTINIQUE si les quatre contrôleurs de domaine hébergent le même domaine Active Directory. En effet la synchronisation de la partition de domaine entre le contrôleur de domaine de la Martinique et les contrôleurs de domaine de Paris est impossible avec SMTP.

En revanche si le contrôleur de domaine de la Martinique héberge le domaine martinique.lan et ceux de Paris le domaine paris.lan, on peut tout à fait utiliser SMTP pour la réplication intersites !

1.4. Méthodes d'administration d'un réseau Windows 2003

1.4.1. Utilisation d'Active Directory pour la gestion centralisée

Active Directory permet à un seul administrateur de centraliser la gestion et l'administration des ressources du réseau. Comme il contient des informations sur tous les objets et leurs attributs, la recherche d'informations se fait sur l'ensemble de la forêt.

Active Directory permet aussi d'organiser les objets de façon hiérarchique grâce aux conteneurs comme les unités organisationnelles, les domaines ou les sites. Il est ainsi possible d'appliquer certains paramètres à un ensemble d'ordinateurs et d'utilisateurs.

1.4.2. Les outils d'administration d'Active Directory

L'administration du service d'annuaire Active Directory se passe par le biais de différentes consoles MMC :

- **Utilisateurs et ordinateurs Active Directory** : C'est le composant le plus utilisé pour accéder à l'annuaire. Il permet de gérer les comptes d'utilisateurs, les comptes d'ordinateurs, les fichiers et les imprimantes partagés, les unités d'organisation …
- **Sites et Services Active Directory** : Ce composant permet de définir des sites, des liens de sites et de paramétrer la réplication Active Directory.
- **Domaines et approbations Active Directory** : Ce composant permet de mettre en place les relations d'approbations et les suffixes UPN. Il propose aussi d'augmenter le niveau fonctionnel d'un domaine ou d'une forêt.
- **Schéma Active Directory** : Ce composant permet de visualiser les classes et les attributs de l'annuaire. Pour pouvoir accéder à la console **Schéma Active Directory**, il faut dans un premier temps **enregistrer une DLL**. Pour cela, il vous faut ouvrir une invite de commande et taper la commande : **regsvr32 schmmgmt.dll**
- **Gestion des Stratégies de Groupe** : Ce composant permet de centraliser l'administration des stratégie de groupe d'une forêt, de vérifier le résultat d'une stratégie de groupe ou bien encore de comparer les paramètres de deux stratégies de groupe. Ce composant n'est pas disponible sur le CD-ROM de Windows 2003 Server, il doit être téléchargé sur le site de Microsoft.
- **ADSI Edit** : Ce composant permet de visualiser l'arborescence LDAP réelle du service d'annuaire. Elle peut s'avérer utile pour lire ou modifier certains attributs ou certains objets de l'annuaire. Elle permet aussi d'attribuer des permissions sur les objets de l'annuaire avec une granularité plus fine. En outre, elle se révèle quasi indispensable pour développoer une application accédant aux données contenues dans l'annuaire. Cette console doit être installée avec les outils de support situés sur le CD-ROM de Windows 2003 Server.

En complément des divers composants logiciels enfichables énumérés ci-dessus, divers outils sont mis à la disposition de l'administrateur pour gérer Active Directory :

- **Lpc.exe** : Cet outil permet d'envoyer manuellement des requêtes LDAP vers n'importe quel annuaire LDAP (Active Directory, NDS, Open LDAP,…). Il peut être utilisé pour vérifier la connectivité entre une machine et l'annuaire ou bien pour lister des informations bien spécifiques dans une partie de l'annuaire. LPC affiche l'intégralité des données échangées entre le poste client et le service d'annuaire. Il est disponible avec les outils de support situés sur le CD-ROM de Windows 2003 Server.
- **Dsadd, dsmod, dsrm, dsget, dsquery, dsmove** : Ces outils en ligne de commande permettent respectivement d'ajouter, de modifier, de supprimer, de lister ou de déplacer des objets dans l'annuaire. Ils sont utilisés dans des scripts afin d'automatiser certaines tâches administrativement lourdes.
- **Ldifde :** L'outil en ligne de commande LDIFDE (LDAP Data Interchange Format Directory Export) permet d'importer des données à partir d'un fichier texte vers Active Directory ou bien d'exporter des données à partir d'Active Directory vers un fichier texte.
- **Csvde** : L'outil en ligne de commande CSVDE est utilisé pour importer des comptes d'utilisateurs à partir d'un fichier texte vers Active Directory.
- **WSH** : WSH pour Windows Scripts Host est un environnement permettant d'exécuter des scripts en VBS ou en JScript.sur une plateforme Windows 9x ou NT.

1.4.3. Gestion de l'environnement utilisateur

A l'aide des stratégies de groupe de Windows 2000/2003, il est possible de restreindre les actions des utilisateurs directement à partir du serveur.

- Contrôle des actions que peuvent réaliser les utilisateurs.
- Centralisation de la gestion de l'installation des applications et des services.
- Configuration des données utilisateur pour suivre les utilisateurs.

1.4.4. Délégation du contrôle d'administration

La hiérarchie mise en place au sein d'Active Directory permet une délégation fine toujours basée sur les conteneurs permettant la délégation sur un ensemble défini de machines et d'utilisateurs.

2. Implémentation d'une structure de forêt et de domaine Active Directory

Un domaine désigne l'unité administrative de base d'un réseau Windows 2000/2003.

Le premier domaine d'une nouvelle forêt créé dans Active Directory représente le domaine racine de l'ensemble de la forêt.

La création d'un domaine d'effectue à l'aide de la commande dcpromo. L'assistant d'installation d'Active Directory vous guide alors dans la création d'un nouveau domaine ou dans la création d'un contrôleur de domaine supplémentaire dans un domaine Windows 2000/2003 existant.

2.1. Installation d'Active Directory

2.1.1. Les pré requis pour installer Active Directory

Voici la configuration requise pour pouvoir installer Active Directory :

- Un ordinateur exécutant Windows 2003 Standard Edition, Enterprise Edition ou Datacenter Edition. Attention, le service d'annuaire Active Directory ne peut pas être installé sur Windows 2003 Server Web Edition.
- 250 Mo d'espace libre sur une partition ou un volume NTFS
- Les paramètres TCP/IP configuré pour joindre un serveur DNS
- Un serveur DNS faisant autorité pour gérer les ressources SRV
- Des privilèges administratifs suffisants pour créer un domaine

Vous pouvez afficher les serveurs DNS faisant autorité pour un domaine donné en tapant la commande **nslookup -type=ns nom.du.domaine**.

2.1.2. Le processus d'installation d'Active Directory

L'assistant d'installation réalise diverses tâches successives :

- Démarrage du protocole de sécurité et définition de la sécurité
- Création des partitions Active Directory, de la base de données et des fichiers journaux
- Création du domaine racine de la forêt
- Création du dossier SYSVOL
- Configuration de l'appartenance au site du contrôleur de domaine
- Activation de la sécurité sur le service d'annuaire et sur les dossiers de réplication de fichiers.
- Activation du mot de passe pour le mode de restauration

2.1.3. Les étapes post installation

Une fois que l'installation d'Active Directory terminée, il faut vérifier la présence et le bon fonctionnement du service d'annuaire. Cela passe par plusieurs étapes :

- Contrôler la création du dossier SYSVOL et de ses partages
- Vérifier la présence de la base de données d'annuaire et des fichiers journaux
- Contrôler la structure Active Directory par défaut
- Analyser les journaux d'évènements

2.2. Implémentation du système DNS pour la prise en charge d'Active Directory

Les infrastructures Windows 2000/2003 intègrent le système DNS (Domain Name Service) et le service d'annuaire Active Directory.

Ces deux éléments sont liés: En effet, le système DNS est un pré requis pour installer Active Directory. Ces deux composants utilisent la même structure de noms hiérarchique afin de représenter les domaines et les ordinateurs sous forme d'objets Active Directory ou bien sous forme de domaines DNS et d'enregistrement de ressources.

2.2.1. Le rôle du Système DNS dans Active Directory

Le système DNS fournit les principales fonctions ci-dessous sur un réseau exécutant Active Directory :

- **Résolution de noms :** le système DNS résout les noms d'hôtes en adresses IP. Par exemple, un ordinateur nommé labo-1 désirant se connecter à un autre ordinateur nommé labo-2 enverra une requête au serveur DNS qui lui renverra l'adresse IP de labo-2. Le système DNS peut aussi effectuer une résolution de nom inversée, c'est-à-dire fournir le nom d'hôte à partir de l'adresse IP qui lui est communiquée.
- **Convention de dénomination :** Active Directory emploie les conventions de dénomination du système DNS. Ainsi, microsoft.supinfo.com peut être un nom de domaine DNS et/ou un nom de domaine Windows 2000.
- **Localisation des composants physiques d'Active Directory :** Le système DNS identifie les contrôleurs de domaine par rapport aux services spécifiques qu'ils proposent comme l'authentification d'une connexion ou la recherche d'informations dans Active Directory. Lors de l'ouverture d'une session, une machine cliente doit s'adresser à un contrôleur de domaine, seul capable de l'authentifier. Le système DNS pourra lui fournir l'emplacement de l'un de ces contrôleurs de domaine.

2.2.2. Les zones DNS intégrées à Active Directory

Contrairement aux zones DNS classiques qui stockent les enregistrements de ressources dans des fichiers, les zones DNS intégrées à Active Directory stockent les enregistrements de ressources directement dans le service d'annuaire Active Directory.

Seules les zones primaires et les zones de stub peuvent être intégrées à Active Directory. De plus, seuls les contrôleurs de domaine jouant aussi le rôle de serveur DNS peuvent héberger des zones intégrées à Active Directory.

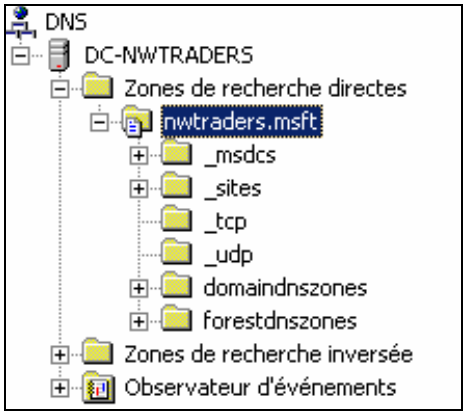
Les zones DNS intégrées à Active Directory sont intéressantes puisqu'elles permettent de renforcer la sécurité du processus de résolution de noms de diverses manières :

- Les zones intégrées à Active Directory peuvent être dupliquées sur tous les contrôleurs de domaine.
- Cela permet d'assurer la tolérance de panne, puisque si un contrôleur de domaine connaît une défaillance, alors la résolution de noms sera toujours assurée.
- L'intégration à Active Directory sécurise les transactions entres les serveurs DNS. En effet, les zones DNS intégrées au service d'annuaire utilisent le mécanisme de réplication Active Directory qui s'avère plus sécurisé que les échanges AXFR et IXFR réalisés entre des serveurs DNS utilisant des zones standard.

- Les zones intégrées à Active Directory permettent de sécuriser les mises à jour automatiques des ordinateurs clients (seuls les ordinateurs clients équipés de Windows 2000/XP/2003 peuvent faire des mises à jour automatiques). En effet, si les mises à jour automatiques sont activées, seuls les ordinateurs clients membres du domaine peuvent mettre à jour automatiquement leurs enregistrements A et PTR.

2.2.3. Les enregistrements de ressources crées lors de l'installation d'Active Directory

Lors de l'installation d'Active Directory, la structure de la zone DNS de recherche directe est modifiée. Un certain nombre de sous domaines et d'enregistrements de ressources sont ajoutés. Il convient de vérifier la présence de ces enregistrements à la fin du processus d'installation d'Active Directory.



Les sous domaine **_tcp**, **_udp** et **_sites** contiennent les enregistrements SRV faisant références à tous les contrôleurs de domaine de la forêt.

Ce sont ces enregistrements qui permettent aux ordinateurs clients de connaître l'emplacement des contrôleurs de domaine. De plus ces enregistrements sont aussi utilisés par le processus de réplications.

Le sous domaine **_msdcs** permet notamment de trouver les contrôleurs de domaine ayant un rôle de maître d'opération (exemple : émulateur PDC).

2.3. Les différents niveaux fonctionnels

Le niveau fonctionnel d'un domaine ou d'une forêt définit l'ensemble des fonctionnalités supportées par le service d'annuaire Active Directory dans ce domaine ou dans cette forêt.

2.3.1. Les niveaux fonctionnels de domaine

Le niveau fonctionnel par défaut d'un domaine est Windows 2000 mixte. Il existe deux autres niveaux fonctionnels disponibles sous Windows 2003 Server. Voici leurs caractéristiques :

- **Windows 2000 mixte :** supporte la prise en charge des contrôleurs secondaires de domaine Windows NT 4.0 (BDC)
- **Windows 2000 natif :** supporte les groupes universels, les imbrications de groupes et l'historique SID
- **Windows Server 2003 :** supporte le changement du nom d'un contrôleur de domaine, la mise à jour du cachet d'ouverture de session, le numéro de version des clés Kerberos KDC et un mot de passe utilisateur sur l'objet InetOrgPerson.

2.3.2. L'augmentation d'un niveau fonctionnel de domaine

Il est possible d'augmenter le niveau fonctionnel d'un domaine. Cette opération se réalise dans la console Domaines et approbations Active Directory (accessible en tapant domain.msc dans la boite de dialogue exécuter) ou bien dans la console Utilisateurs et ordinateurs Active Directory (accessible en tapant dsa.msc dans la boite de dialogue exécuter). Pour réaliser cette opération, vous devez être membre du groupe admins du domaine ou administrateurs de l'entreprise.

Avant d'augmenter le niveau fonctionnel d'un domaine, il est nécessaire de vérifier que les contrôleurs de domaines exécutent le système d'exploitation requis. En effet, une fois le niveau fonctionnel

augmenté, il est impossible de revenir en arrière sans désinstaller le service d'annuaire sur l'ensemble des contrôleurs de domaine du domaine. Voici les la liste des systèmes d'exploitation utilisables pour chaque niveau fonctionnel :

- **Windows 2000 mixte :** contrôleurs de domaine exécutant Windows NT 4.0, 2000 Server ou 2003 Server.
- **Windows 2000 natif :** contrôleurs de domaine exécutant Windows 2000 Server ou 2003 Server.
- **Windows Server 2003 :** contrôleurs de domaine exécutant Windows 2003 Server uniquement.
- **Windows 2003 server version préliminaire :** contrôleurs de domaine exécutant NT 4.0 et des contrôleurs de domaine sous Windows 2003 server. Ce niveau fonctionnel est uniquement utilisé dans le cadre d'une migration de Windows NT4 vers Windows Server 2003 (ou vers Windows Server 2003 R2).

Ainsi, pour augmenter le niveau fonctionnel d'un domaine vers le niveau Windows Server 2000 natif, il faudra impérativement effectuer une mise à jour du système d'exploitation de tous contrôleurs de domaine du domaine ou de la forêt fonctionnant avec Windows NT 4.0 ou une version antérieure.

De plus, une fois le niveau fonctionnel du domaine augmenté, les contrôleurs de domaine exécutant des versions antérieures du système d'exploitation ne peuvent pas être introduits dans le domaine. Par exemple, si vous augmentez le niveau fonctionnel du domaine à Windows Server 2003, les contrôleurs de domaine exécutant Windows 2000 Server ne peuvent pas être ajoutés à ce domaine.

2.3.3. Les niveaux fonctionnels de forêt

Le niveau fonctionnel d'une forêt active des fonctionnalités spécifiques dans tous les domaines de cette forêt. Voici les trois niveaux fonctionnels disponibles pour une forêt ainsi que la liste des systèmes d'exploitation utilisables pour chaque niveau :

- **Windows 2000 (niveau par défaut):** contrôleurs de domaine exécutant Windows NT 4.0, 2000 Server ou 2003 Server.
- **Windows Server 2003 provisoire :** contrôleurs de domaine exécutant Windows NT 4.0 ou 2003 Server.
- **Windows Server 2003 :** contrôleurs de domaine exécutant Windows 2003 Server uniquement.

Les niveaux Windows 2000 et Mode forêt provisoire Windows Server 2003 ne proposent aucunes fonctions spéciales au niveau de la forêt. En revanche, le niveau Windows Server 2003 met en place les avantages suivants :

- Catalogue global de réglage de la réplication
- Objets schéma défunts
- Approbation de forêt
- Réplication de valeur liée
- Changement du nom de domaine
- Algorithmes de réplication avancés
- Classes auxiliaires dynamiques
- Modification de la classe de l'objet InetOrgPerson
- Fréquence de réplication intrasite de 15 secondes pour les contrôleurs de domaine Windows Server 2003 mis à niveau à partir de Windows 2000

2.3.4. L'augmentation d'un niveau fonctionnel de forêt

Lorsque tous les domaines d'une forêt ont le même niveau fonctionnel, il est possible d'augmenter le niveau fonctionnel de la forêt. Seul un membre du groupe administrateurs de l'entreprise peut réaliser cette opération.

Une fois le niveau fonctionnel de la forêt augmenté, les contrôleurs de domaine exécutant des versions antérieures du système d'exploitation ne peuvent pas être introduits dans la forêt. Par exemple, si vous augmentez le niveau fonctionnel de la forêt à Windows Server 2003, les contrôleurs de domaine exécutant Windows 2000 Server ne peuvent pas être ajoutés à cette forêt.

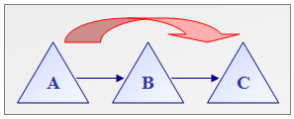
Dans le cadre de la migration vers Windows 2003 Server d'un domaine exclusivement composé de machines sous Windows NT 4.0, il est possible d'utiliser le niveau Windows 2003 Server provisoire. Ce niveau ne prend pas en charge les contrôleurs de domaine sous Windows 2000 Server.

2.4. Les relations d'approbation

Les relations d'approbations permettent à un utilisateur d'un domaine donné d'accéder aux ressources de son domaine, mais aussi d'autres domaines (les domaines approuvés). Les relations d'approbations se différencient de par leur type (transitif ou non transitif) et de par leur direction (unidirectionnel entrant, unidirectionnel sortant, bidirectionnel).

2.4.1. Transitivité de l'approbation

Soient trois domaines distincts reliés entres eux par les deux relations suivantes :



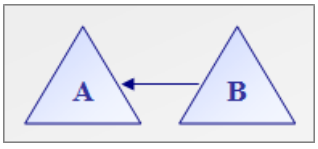
- Le domaine A approuve directement le domaine B. Ainsi un utilisateur du domaine A peut accéder à toutes les ressources du domaine A et du domaine B.
- Le domaine B approuve directement le domaine C. Ainsi un utilisateur du domaine B peut accéder à toutes les ressources du domaine B et du domaine C.

Si les deux relations d'approbations de A à B et de B à C sont transitives, alors le domaine A approuve indirectement le domaine C. Dans ce cas de figure un utilisateur du domaine A peut accéder à toutes les ressources du domaine A, du domaine B et du domaine C.

Si les deux relations d'approbations de A à B et de B à C ne sont pas transitives, alors le domaine A n'approuve pas le domaine C. Dans ce cas de figure, un utilisateur du domaine A ne peut pas accéder aux ressources du domaine C.

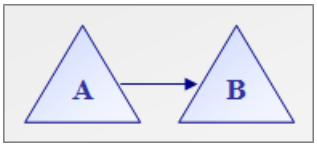
2.4.2. Direction de l'approbation

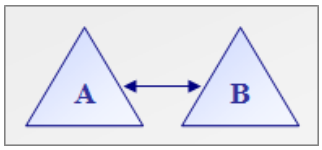
Lors de la création d'une relation d'approbation manuelle sous Windows Server 2003, trois directions d'approbation différentes sont utilisables.



Si vous avez configuré une relation d'approbation unidirectionnelle entrante entre le domaine A et le domaine B, alors les utilisateurs du domaine A peuvent être authentifiés dans le domaine B.

Si vous avez configuré une relation d'approbation unidirectionnelle sortante entre le domaine A et le domaine B, alors les utilisateurs du domaine B peuvent être authentifiés dans le domaine A.





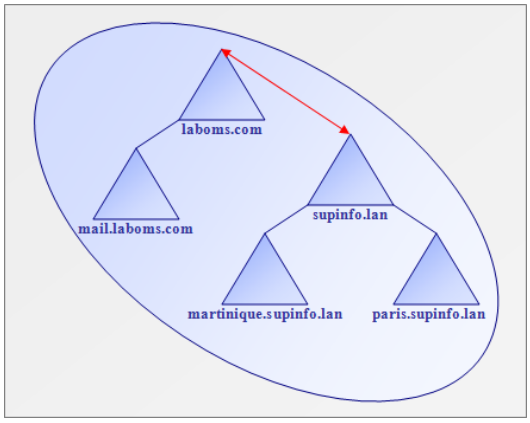
Si vous avez configuré une relation d'approbation bidirectionnelle entre le domaine A et le domaine B, alors les utilisateurs de chaque domaine peuvent être authentifiés dans les deux domaines.

2.4.3. Les relations d'approbations

Approbation racine/arborescence

Lorsqu'une nouvelle arborescence est crée au sein d'une forêt, une relation d'approbation bidirectionnelle transitive lie automatiquement cette nouvelle arborescence au domaine racine de la forêt.

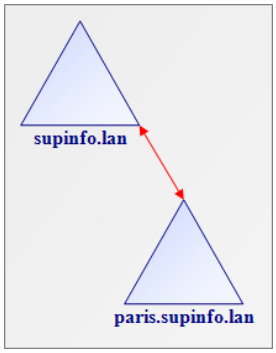
Dans exemple ci-contre, l'arborescence supinfo.lan est liée à laboms.lan, le domaine racine de la forêt, par le biais d'une relation racine/arborescence.



Approbation parent-enfant

Une approbation parent-enfant est une relation d'approbation bidirectionnelle transitive. Elle est automatiquement créée lorsqu'un nouveau domaine est ajouté à une arborescence.

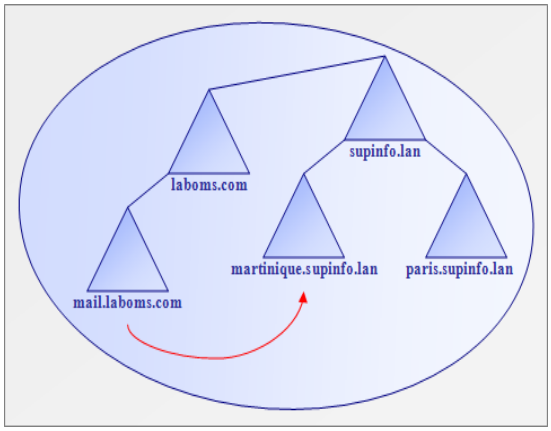
Dans l'exemple ci-contre, on ajoute le sous domaine paris.supinfo.lan à l'intérieur du domaine supinfo.lan. Les deux domaines sont automatiquement reliés par une relation parent-enfant. Ainsi les utilisateurs du domaine supinfo.lan peuvent être authentifiés dans le domaine paris.supinfo.lan et vice-versa.



Approbation raccourcie

Une approbation raccourcie est une relation d'approbation partiellement transitive. Elle doit être définie manuellement ainsi que sa direction. Les relations d'approbation raccourcie permettent de réduire les sauts de l'authentification Kerberos.

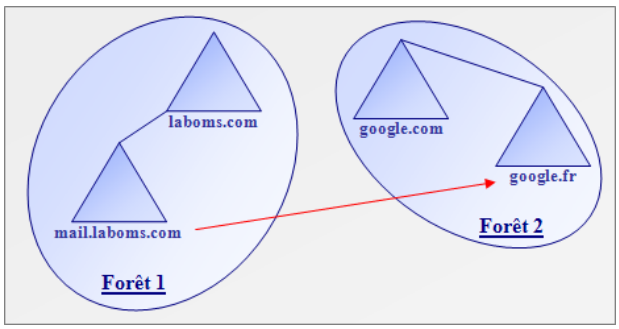
En effet, si un utilisateur du domaine martinique.supinfo.lan souhaite s'authentifier dans le domaine mail.laboms.lan, il doit passer par deux approbations parent/enfant et par une approbation racine/arborescence. L'approbation raccourcie permet donc d'accélérer l'authentification inter-domaine.



Approbation externe

Une approbation externe est une relation d'approbation non transitive. Elle doit être créée manuellement et peut avoir une direction unidirectionnelle ou bidirectionnelle.

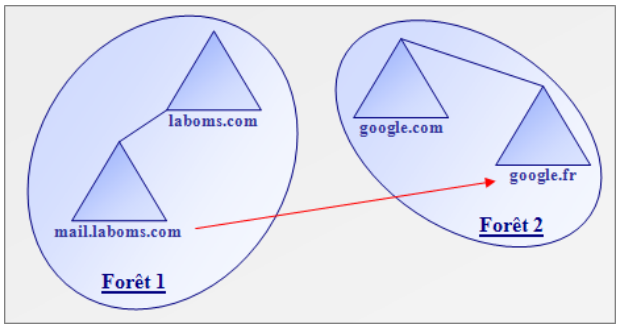
L'approbation externe permet de relier des domaines appartenant à deux forêts distinctes.



Approbation de domaine

Une approbation de domaine est une relation d'approbation dont la transitivité et la direction doivent être paramétrées par l'administrateur.

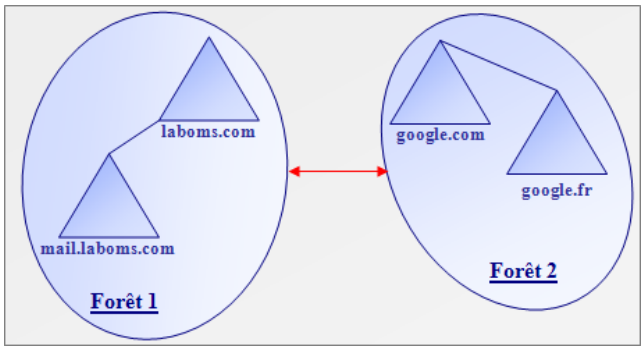
L'approbation de domaine permet de relier un domaine sous Active Directory avec un domaine Kerberos non Microsoft.



Approbation de forêt

Une approbation de forêt permet de relier l'intégralité des domaines de deux forêts.

Les approbations de forêt sont non transitives et leurs directions doivent être définies manuellement. Les deux forêts doivent impérativement utiliser le niveau fonctionnel de forêt Windows Server 2003. Il n'y a pas de transitivité entre les forêts.



3. Implémentation d'une structure d'unité d'organisation

3.1. Création et gestion d'unités d'organisation

3.1.1. Présentation de la gestion des unités d'organisation

La création et la gestion d'unités d'organisation passent par quatre phases très importantes :

- **La planification :** C'est la phase la plus importante car c'est à ce moment que vous allez déterminer le système hiérarchique des objets les uns par rapport aux autres. Ce système hiérarchique sera l'épine dorsale de votre système administratif. Vous devez prévoir aussi la nomenclature de nom des UO à ce niveau.

- **Le déploiement :** C'est la phase de création des unités d'organisation sur le serveur, elle comprend aussi la phase de déplacement des objets dans les unités d'organisation.

- **La maintenance :** C'est la phase d'exploitation des unités d'organisation une fois qu'elles sont en production. Cela comprend toutes les modifications liées aux modifications courantes d'organisation de l'entreprise.

- **La suppression :** Tous les objets dans Active Directory occupent un certain espace sur le disque ainsi que sur le réseau lors des réplications.

3.1.2. Méthodes de création et de gestion des unités d'organisation

Afin de pouvoir créer vos unités d'organisation, quatre méthodes sont à votre disposition :

- **L'outil Utilisateurs et ordinateurs Active Directory :** Cet outil graphique est le moyen le plus rapide pour créer une unité d'organisation. Il atteint rapidement ces limites lorsque l'on désire créer plus d'une cinquantaine de compte.

- **Les outils en ligne de commande (dsadd, dsmod, drrm) :** Ces outils permettent via ligne de commande ou via script batch de créer des unités d'organisation.
  Exemple :
  dsadd ou "ou= SUPINFO Training Center, dc=supinfo, dc=lan" -u Administrateur -p *

- **L'outil LDIFDE :** Cet outil permet de faire de l'import et de la modification en masse à partir d'un fichier texte. La plupart des moteurs LDAP permettent d'exporter vers ce format.
  Exemple :
  dn: OU=Labo-Cisco,DC=supinfo, DC=lan
  changetype: delete

  dn: OU=Labo-Microsoft, DC=supinfo, DC=lan
  changetype: add
  objectClass: organizationalUnit

- **Les scripts VBS :** Ces scripts permettent de faire de l'import d'unités d'organisation en ajoutant des conditions pour la création de ces UO.
  Exemple :
  Set objDom = GetObject("LDAP://dc=supinfo,dc=lan")

```
Set objOU = objDom.Create("OrganizationalUnit", "ou=Salle A")
objOU.SetInfo
```

3.2. Délégation du contrôle administratif des unités d'organisation

Active Directory est un système intégrant la sécurisé : seuls les comptes ayant reçu les permissions adéquates peuvent effectuer des opérations sur ces objets (ajout, modification, …).
Les administrateurs, en charge de cette affectation de permissions peuvent aussi déléguer des tâches d'administration à des utilisateurs ou des groupes d'utilisateurs.

3.2.1. Sécurité des objets

Dans Active Directory, chaque objet est sécurisé, ce qui signifie que l'accès a chacun d'eux est cautionné par l'existence de permissions en ce sens.

A chaque objet est associé un descripteur de sécurité unique qui définit les autorisations d'accès nécessaires pour lire ou modifier les propriétés de cet objet.
En ce qui concerne la restriction d'accès aux objets ou à leurs propriétés, le descripteur contient la DACL (Discretionary Access Control List) et en ce qui concerne l'audit, le descripteur contient la SACL (System Access Control List).

Le contrôle d'accès dans Active Directory repose non seulement sur les descripteurs de sécurité des objets, mais aussi sur les entités de sécurité (par exemple un compte d'utilisateur ou un compte de machine), et les identificateurs de sécurité (SID, dont le fonctionnement est globalement identique à celui sous NT 4.0 et Windows 2000).

Active Directory étant organisé hiérarchiquement, il est possible de définir des permissions sur un conteneur et de voir ces permissions héritées à ses sous conteneurs et à ses objets enfants (si on le souhaite). Grâce à cela, l'administrateur n'aura pas à appliquer les mêmes permissions objet par objet, limitant ainsi la charge de travail, et le taux d'erreurs.

Dans le cas où l'on définirait des permissions spécifiques pour un objet et que ces dernières entrent en conflit avec des permissions héritées, ce seront les permissions héritées qui seront appliquées.
Dans certains cas, on ne souhaite pas que des permissions soient héritées, il est alors possible de bloquer cet héritage. Par défaut, lors de la création d'un objet, l'héritage est activé. Par conséquent, une DACL correspondant aux permissions du conteneur parent est créée pour cet objet. Lors du blocage de l'héritage, on définit une nouvelle DACL qui sera soit copiée depuis la DACL du parent, soit vierge.

3.2.2. Délégation de contrôle

Il est possible de déléguer un certain niveau d'administration d'objets Active Directory à n'importe quel utilisateur, groupe.
Ainsi, vous pourrez par exemple déléguer certains droits administratifs d'une unité organisationnelle (ex : création d'objets dans cette UO) à un utilisateur.

L'un des principaux avantages qu'offre cette fonctionnalité de délégation de contrôle est qu'il n'est plus nécessaire d'attribuer des droits d'administration étendus à un utilisateur lorsqu'il est nécessaire de permettre à un utilisateur d'effectuer certaines tâches.

Sous NT4, si l'on souhaitait qu'un utilisateur dans un domaine gère les comptes d'utilisateurs pour son groupe, il fallait le mettre dans le groupe des Opérateurs de comptes, qui lui permet de gérer tous les comptes du domaine.

Avec Active Directory, il suffira de cliquez avec le bouton droit sur l'UO dans laquelle on souhaite lui déléguer l'administration d'une tâche et de sélectionner Déléguer le contrôle.
On pourra définir quelques paramètres comme les comptes concernés par cette délégation et le type de délégation, dans notre cas, « Créer, supprimer et gérer des comptes d'utilisateur » (On peut affiner en déléguant des tâches personnalisées comme par exemple uniquement le droit de réinitialiser les mots de passe sur les objets de compte d'utilisateur de l'UO, …).

4. Implémentation de comptes d'utilisateurs, de groupes et d'ordinateurs

Le service d'annuaire Active Directory distingue trois types de comptes :

- **Le compte d'utilisateur** permet à un utilisateur physique d'ouvrir une session unique sur le domaine et d'accéder aux ressources partagées.
- **Le compte d'ordinateur** permet d'identifier un ordinateur physique par le biais d'un mécanisme d'authentification. Il est possible d'activer l'audit de l'accès d'un compte d'ordinateur aux ressources du domaine.
- **Le compte de groupe** permet de simplifier l'administration en regroupant des comptes d'utilisateurs, d'ordinateurs ou bien d'autres comptes de groupes.

4.1. Implémentation de comptes d'utilisateurs

4.1.1. Présentation du nom d'utilisateur principal

Un nom d'utilisateur principal ou UPN (User Principal Name) est un nom d'ouverture de session. Il doit être unique au sein de la forêt. Il se décompose en deux parties séparées par le caractère @ :

- Le préfixe UPN
- Le suffixe UPN

Par exemple l'utilisateur Loïc Thobois situé dans le domaine supinfo.com ouvre sa session en utilisant le nom d'utilisateur principal suivant : thoboi_l@supinfo.com où thobois_l représente le préfixe UPN et supinfo.com le suffixe UPN.

Le nom d'utilisateur principal n'est pas modifié lors du déplacement du compte d'utilisateur vers un autre domaine car ce nom est unique dans la forêt. De plus Il peut être utilisé en tant qu'adresse électronique car il a le même format qu'une adresse de messagerie standard.

Un utilisateur peut toujours ouvrir une session à l'aide du nom d'ouverture de session d'utilisateur pré-windows 2000 (dans notre exemple SUPINFO\thoboi_l). En outre, Windows 2003 Server autorise l'assignation de suffixes UPN supplémentaires à un compte d'utilisateur.

4.1.2. Le Routage des suffixes UPN

Il est possible d'ajouter ou de supprimer des suffixes UPN dans la forêt grâce à la console Domaines et approbations (accessible en tapant domain.msc dans la boite de dialogue exécuter) ou bien par le biais d'un script. Seul un membre du groupe administrateurs de l'entreprise est autorisé à modifier les suffixes UPN.

La console Domaines et approbations permet aussi d'activer le routage des suffixes UPN. Le routage des suffixes UPN est un mécanisme fournissant une résolution de noms UPN inter forêts. Ainsi il est possible de définir quels suffixes UPN les utilisateurs de la forêt 1 pourront utiliser pour s'authentifier dans la forêt 2. Bien entendu, les relations d'approbations appropriées (approbation de forêt) doivent être définies pour permettre le routage des suffixes UPN.

4.2. Implémentation de comptes de groupe

Les groupes permettent de simplifier la gestion de l'accès des utilisateurs aux ressources du réseau. Les groupes permettent d'affecter en une seule action une ressource à un ensemble d'utilisateurs au

lieu de répéter l'action pour chaque utilisateur. Un utilisateur peut être membre de plusieurs groupes. Les groupes se différencient de par leur type et de par leur étendue.

4.2.1. Le type de groupe

Il existe deux types de groupes dans Active Directory :

- **Les groupes de sécurité** : permettent d'affecter des utilisateurs et des ordinateurs à des ressources.
- **Les groupes de distribution** : exploitables entre autres via un logiciel de messagerie.

4.2.2. L'Etendue de groupe

Les deux types de groupes gèrent chacun trois niveaux d'étendue. Les fonctionnalités des étendues de groupe peuvent varier selon le niveau fonctionnel du domaine.

Les groupes globaux :

	Mode mixte	**Mode natif**
Membres	Comptes d'utilisateurs du même domaine	Comptes d'utilisateurs et groupes globaux du même domaine
Membres de	Groupes locaux du même domaine	Groupes locaux de domaines, groupes globaux et groupes universels
Etendue	Visibles dans leur domaine et dans tous les domaines approuvés	
Autorisations pour	Tous les domaines de la forêt	

Les groupes locaux de domaine (ou groupes de domaine local) :

	Mode mixte	**Mode natif**
Membres	Comptes d'utilisateurs et groupes globaux de tout domaine	Comptes d'utilisateurs, groupes globaux et groupes universels d'un domaine quelconque de la forêt, et groupes locaux de domaine du même domaine
Membres de	Membres d'aucun groupe	Groupes locaux de domaine du même domaine
Etendue	Visibles dans leur propre domaine	
Autorisations pour	Le domaine dans lequel le groupe local de domaine existe	

Les groupes universels :

	Mode mixte	**Mode natif**
Membres	Non utilisables	Comptes d'utilisateurs, groupes globaux et autres groupes universels d'un domaine quelconque de la forêt.
Membres de	Non utilisables	Groupes locaux de domaine et universels de tout domaine.
Etendue	Visibles dans tous les domaines de la forêt	
Autorisations pour	Tous les domaines de la forêt	

4.2.3. Stratégie d'utilisation de groupe dans un domaine

Diverses stratégies sont recommandées afin d'attribuer les autorisations sur les ressources du réseau (fichiers/dossiers/imprimantes partagées). La stratégie privilégiée au sein d'un domaine est la stratégie C G DL A :

Rassemblez des **comptes d'utilisateur** (C) dans des groupes globaux.
Ajoutez les groupes globaux à un **groupe local de domaine** (DL).
Affectez les **autorisations** (A) sur les ressources du domaine sur le groupe local de domaine.

> ✍ . Cette stratégie est aussi appelée A G DL P (pour **A**ccounts **G**lobal group **D**omain **L**ocal group **P**ermissions)

Il existe une évolution de cette stratégie qui permet à utilisateurs situés dans plusieurs domaines différents d'accéder à une ressource donnée. Cette stratégie fait intervenir les groupes d'étendue universelle et est nommée C G U DL A.

4.3. Outils d'administration et tâches administratives

4.3.1. Les outils d'administration

Divers outils sont mis à disposition de l'administrateur afin de lui faciliter la gestion des comptes d'utilisateurs, d'ordinateurs et de groupes :

- **Utilisateurs et ordinateurs Active Directory** : Console permettant d'ajouter, modifier et supprimer des comptes d'utilisateurs, d'ordinateurs et de groupe en mode graphique.
- **Dsadd, dsmod, dsrm,… :** Commandes permettant respectivement de créer, de modifier ou de supprimer des objets dans Active Directory.
- **csvde** : Outil en ligne de commande permettant de créer des objets à partir d'un fichier au format csv (champs délimités par des virgules).
- **ldifde** : Outil en ligne de commande permettant de créer, modifier, supprimer des objets à partir d'un fichier au format ldif (champs délimités par des sauts de ligne).
- **WSH** : Environnement permettant d'exécuter des scripts en VBS ou en JScript.

5. Implémentation d'une stratégie de groupe

5.1. Création et configuration d'objets Stratégie de groupe

5.1.1. Présentation d'une stratégie de groupe

Une stratégie de groupes est un objet Active Directory qui va contenir un ensemble de paramètres.

Ces paramètres vont permettre d'agir sur l'environnement d'un utilisateur ou d'un ordinateur :

- Les paramètres de stratégies de groupe pour les **ordinateurs** définissent le comportement du système d'exploitation et d'une partie du bureau, la configuration de la sécurité.
- Les paramètres de stratégies de groupe pour les **utilisateurs** définissent les options d'applications affectées et publiées, la configuration des applications.

☞ Une stratégie de groupe peut aussi être appelée GPO (Group Policy Object)

Cet objet de stratégie de groupe va ensuite être lié à un conteneur **site**, **domaine** ou **unité d'organisation**. Cela va permettre d'appliquer les paramètres de stratégie de groupe aux objets contenu dans ces conteneurs.

5.1.2. Composants d'un objet Stratégie de groupe

Un objet de stratégie de groupe se décompose en deux parties :

- Une partie qui sera stockée dans la base **Active Directory**. Cet objet va ensuite être lié à des objets de sites, domaines ou unités d'organisation.
  Cet objet permet aussi de gérer les versions permettant une réplication optimisée.

- Une partie qui sera stockée dans le répertoire **SYSVOL** sous la forme d'un répertoire ayant pour nom le SID de l'objet dans la base Active Directory. Ce répertoire contient l'ensemble des fichiers de scripts, de configuration, etc.
  Le dossier SYSVOL est répliqué automatiquement entre tous les contrôleurs de domaine.

5.1.3. Gestion des Stratégies de groupe par un contrôleur de domaine

La modification des paramètres de stratégie de groupe peut se faire sur n'importe quel contrôleur de domaine, mais pour éviter les conflits un contrôleur de domaine s'occupe de centraliser l'ensemble des modifications.

Ce contrôleur est par défaut celui ayant le rôle de maître d'opérations **Emulateur PDC**, mais il est bien évidemment possible de le changer avec les options suivantes :

- Le contrôleur de domaine avec le jeton de maître d'opérations pour l'émulateur PDC.
- Tout contrôleur de domaine disponible.
- Tout contrôleur de domaine exécutant Windows Server 2003 ou version ultérieure.
- Ce contrôleur de domaine.

5.1.4. Définition des filtres WMI

Pour appliquer une stratégie de groupe, un fois celle-ci liée à un conteneur, vous avez la possibilité de créer un script pour définir des conditions d'applications.

Exemple :
Vous souhaitez déployer une application sur vos postes clients et cette application occupe 1 Go sur le disque dur, avec un script WMI vous avez la possibilité de filtrer l'application de cette stratégie en testant l'espace disque libre sur les stations de travail.

5.2. Configuration des fréquences d'actualisation et des paramètres de stratégie de groupe

5.2.1. Planification de l'application des stratégies de groupe

Lorsque l'ordinateur démarre :

- Les paramètres de la stratégie de groupe dont l'objet ordinateur dépend sont appliqués.
- Les scripts de ces stratégies sont lancés de façons synchrones (les uns après les autres).

L'utilisateur ouvre une session :

- Les paramètres de la stratégie de groupe dont l'objet utilisateur dépend sont appliqués.
- Les scripts de ces stratégies sont lancés de façons asynchrones (tous en même temps).

5.2.2. Fréquence d'actualisation des paramètres de stratégie de groupe

Les stratégies sont ensuite rafraîchies toutes les cinq minutes sur les contrôleurs de domaine et toutes les 90 minutes (plus une valeur aléatoire en 0 et 30 minutes) pour tout les ordinateurs membres du domaine.

5.2.3. Application des stratégies de groupe lors de connexions réseau lentes

Lors de la détection d'une connexion réseau lente (500kb/s par défaut, modifiable par une GPO), l'ordinateur détermine s'il est nécessaire ou non de mettre à jour les stratégies de groupe. Le comportement en mode connexion lente peut être défini à l'aide d'une GPO.

5.3. Gestion des objets Stratégie de groupe

En standard, Windows 2003 Server n'offre que très peu de fonction pour la gestion avancée des stratégies de groupe, pour combler cela, Microsoft a développé un outil gratuit d'administration dédié à la gestion des GPO.

Vous pouvez trouver cet outil à l'adresse suivante :
http://www.microsoft.com/downloads/details.aspx?FamilyID=f39e9d60-7e41-4947-82f5-3330f37adfeb&displaylang=fr

5.3.1. Copie d'une stratégie de groupe

A l'aide de la console de gestion de stratégie de groupe, il est possible de dupliquer une GPO.

Elle conservera tous ces paramètres mais ne sera lié à aucun objet (sites, domaines, unités d'organisations).

La possibilité de copier une stratégie est aussi possible entre différents domaines

5.3.2. Sauvegarde et restauration d'une stratégie de groupe

Une option de sauvegarde des stratégies de groupe est disponible dans l'outil de gestion des stratégies de groupe.
Cette option va vous permettre de sauvegarder sous un fichier GPT (Group Policy Template).

Vous aurez ensuite la possibilité de restaurer cette stratégie de groupe quand vous le souhaitez.

5.3.3. Importation d'une stratégie de groupe

Le principe de l'importation est très proche de la copie de stratégie de groupe avec pour fonctionnalité supplémentaire de modifier via une table de migration les paramètres (Exemple : Mettre à jour les chemins réseaux des paramètres de la GPO).

5.4. Délégation du contrôle administratif de la stratégie de groupe

5.4.1. Délégation d'administration des stratégies de groupe

Il y a trois aspects à la délégation d'une stratégie de groupe :
- Gestion des liaisons à un conteneur (Site, Domaine, Unité d'organisation)
- Création d'objets GPO
- Modification d'objets GPO

A l'aide de l'assistant délégation de contrôle, il est possible de déléguer la gestion des liaisons à n'importe quelle personne sur un conteneur.

Par défaut, pour pouvoir créer une GPO, il faut être membre du groupe :
- Admins de domaine
- Administrateur de l'entreprise
- Propriétaires créateurs de la stratégie de groupe

Pour pouvoir modifier une GPO, il faut avoir l'accès en lecture/écriture, puis être soit le propriétaire de la GPO, soit membre des groupes :
- Admins de domaine
- Administrateur de l'entreprise

5.4.2. Délégation d'administration de filtres WMI

Vous pouvez déléguer la gestion des scripts WMI.

Les Scripts WMI sont stockés dans le conteneur nommé WMIScript dans Active Directory.
La délégation d'administration sur les scripts WMI est déterminée par les autorisations sur ce répertoire.

6. Déploiement et gestion des logiciels à l'aide d'une stratégie de groupe

6.1. Présentation de la gestion du déploiement de logiciels

1. **Préparation** : Les fichiers d'installation au format Windows Installer doivent être copiés dans un partage sur un serveur de fichiers sur lequel les utilisateurs concernés auront les droits de lecture. Ce partage est nommé point de distribution.
2. **Déploiement** : Une GPO doit être créée afin que les logiciels s'installent automatiquement lors du démarrage de l'ordinateur, à l'ouverture de session ou suite à une action manuelle de l'utilisateur (publication).
3. **Maintenance** : Le logiciel qui a été déployé peut être mis à jour via le même procédé et un Service Pack peut être automatiquement déployé sur l'ensemble des postes sur lesquels le logiciel a été installé.
4. **Suppression** : Lorsque vous voulez désinstaller un logiciel à distance, il suffit de supprimer la GPO permettant le déploiement du logiciel et automatiquement le logiciel sera supprimé des machines.

6.2. Présentation de Windows Installer

- **Service Windows Installer** : service s'exécutant sur le client et permettant de réaliser les installations à distance de façon complètement automatisée. Il est capable de modifier ou de réparer automatiquement les logiciels défectueux.
- **Package Windows Installer** : fichier de type .msi contenant toutes les informations nécessaires à l'installation du logiciel.

6.3. Déploiement de logiciels

6.3.1. Affectation de logiciels :

L'affectation permet de garantir la présence d'un logiciel pour un utilisateur ou une machine.

Dans le cas d'une affectation à un utilisateur, un raccourci de l'application va apparaître dans son menu Démarrer et les types de fichier de l'application seront directement enregistrés. Des que l'utilisateur va cliquer sur le raccourci ou sur un fichier de l'application (ex : un fichier .doc dans le cas de Word), le logiciel va s'installer automatiquement.

Dans le cas d'une affectation à un ordinateur, l'application va s'installer dès le démarrage de la machine. Le logiciel sera alors disponible pour tous les utilisateurs de la machine.

☞ L'affectation d'une application à un contrôleur de domaine ne fonctionne pas.

6.3.2. Publication de logiciels :

La publication d'un logiciel laisse le choix à l'utilisateur d'installer ou non l'application sur sa machine.

Elle ne peut être mise en œuvre que pour un utilisateur et pas pour un ordinateur.

L'application apparaît dans le panneau de configuration Ajout/Suppression de programmes dans une liste regroupant toutes les applications pouvant être installées.

Une autre méthode permet d'installer le logiciel en utilisant l'appel de documents. Lorsqu'une application est publiée dans l'Active Directory les types de fichiers qu'elle prend en charge sont enregistrés et lorsqu'un fichier reconnu fait l'objet d'une tentative d'ouverture par un utilisateur ayant l'application correspondante publiée, le programme est installé.

6.3.3. Utilisation des modifications de logiciel

Dans certains cas il n'est pas nécessaire de déployer une application dans son intégralité, mais une version personnalisée de l'application. Dans ce cas il est possible de modifier le script d'installation pour réaliser une installation spécifique à l'aide des fichiers de modification (fichiers de type .mst).

6.3.4. Création de catégories de logiciels

Afin de simplifier l'installation des applications publiées il est possible de créer des catégories qui vont éviter de chercher l'application dans une longue liste.

6.3.5. Association d'extensions de noms de fichiers à des applications

Active Directory maintient une liste des extensions de fichiers et des applications associées. Il n'est pas possible de d'agir sur cette liste mais il est possible de modifier la priorité des applications pour chaque extension (ex : Word 2000 ou Word XP pour l'extension .doc)

6.3.6. Mise à niveau de logiciels déployés

Il existe deux types de mises à niveau des logiciels déployés :

- **Mise à niveau obligatoire** : Le logiciel est remplacé automatiquement au prochain démarrage ou à la prochaine ouverture de session.
- **Mise à jour facultative** : L'utilisateur est libre de faire la mise à jour au moment où il le souhaite.

6.3.7. Redéploiement de logiciels

Le redéploiement de logiciels permet d'appliquer un Service Pack ou un correctif sur un logiciel déjà déployé. Une fois que le logiciel est marqué pour être redéployé, il y a trois scénarios possibles.

- **L'application est affectée à un utilisateur** : Les raccourcis et les éléments du Registre sont mis à jour à la prochaine ouverture de session de l'utilisateur.
- **L'application est affectée à un ordinateur** : Le Service Pack ou le correctif est installé au prochain démarrage de l'ordinateur.
- **L'application est publiée et installée** : Les raccourcis et les éléments du Registre sont mis à jour à la prochaine ouverture de session. Le correctif ou le Service Pack sera automatiquement installé à la prochaine utilisation du logiciel.

6.3.8. Suppression de logiciels déployés

Lors de la suppression d'un logiciel dans l'Active Directory, une boite de dialogue s'ouvre et deux options de suppression vous sont proposées :

- **Désinstallation immédiate** : Le logiciel est désinstallé au prochain démarrage de la machine ou à la prochaine ouverture de session de l'utilisateur.

- **Autoriser l'utilisateur à continuer à utiliser le logiciel** : Les logiciels ne sont pas désinstallés mais ils n'apparaîtront plus dans la liste du panneau de configuration Ajout/Suppression de programmes.

7. Implémentation de sites pour gérer la réplication Active Directory

7.1. Fonctionnement de la réplication

Dans un domaine Windows 2003, un ou plusieurs contrôleurs de domaine hébergent la base de données Active Directory.

La réplication répercute les modifications apportées a la base de données Active Directory depuis un contrôleur de domaine sur tous les autres contrôleurs de domaine du domaine et ce, de façon transparente pour les administrateurs et les utilisateurs.
Cette réplication est qualifiée de multi maîtres car plusieurs contrôleurs de domaine (appelés maîtres ou répliquas) ont la capacité de gérer ou modifier les mêmes informations d'Active Directory.

La réplication peut se produire à différents moments.
Par exemple, lors de l'ajout d'objets sur un contrôleur de domaine, on peut dire que la copie de la base de données Active Directory qu'il contient a subit une mise à jour d'origine.
Lorsque cette mise à jour est répliquée sur un autre répliqua du domaine, on dira alors que ce dernier a effectué une mise à jour dupliquée.
La mise à jour effectuée sur le second contrôleur peut aussi être répliquée sur un troisième contrôleur de domaine.

> ✍ Le processus de réplication n'intervient qu'entre deux contrôleurs de domaine à la fois.

Apres avoir apporté une modification sur un contrôleur de domaine, un temps de latence (par défaut 15 secondes) est observé avant d'envoyer un message de notification au premier partenaire de réplication. Chaque partenaire direct supplémentaire est informé 3 secondes (valeur par défaut) après la réception de la notification. Lorsqu'un partenaire de réplication est informé d'une modification apportée à la base, il récupère celle ci depuis le contrôleur de domaine ayant émis la notification.
Dans certains cas, la notification de changement est immédiate, ainsi que la réplication. C'est le cas lors de la modification d'attributs d'objets considérés comme critiques du point de vue sécurité (par exemple, la désactivation d'un compte). On parle alors de réplication urgente.

> ✍ Toutes les heures (valeur par défaut paramétrable), si aucune modification n'a été apportée à la base Active Directory, un processus de réplication est lancé. Ceci, pour s'assurer que la copie de la base de données Active Directory est identique sur tous les contrôleurs de domaine.

7.2. Résolution des conflits de réplication

La réplication D'Active Directory étant multi maître, des conflits peuvent survenir lors des mises à jour.

Pour minimiser les conflits, les contrôleurs de domaines se basent sur les modifications apportées aux attributs des objets plutôt que les objets eux même. Ainsi, si deux attributs distincts d'un même objet sont modifiés simultanément par deux contrôleurs de domaine, il n'y aura pas de conflit.

Pour résoudre certains conflits, Active Directory emploie un cachet unique global qui est envoyé avec les mises à jour d'origine (et uniquement celles-ci). Ce cachet contient les composants suivants (du plus important au moins important):

- **Le numéro de version :** la numérotation commence à 1. Il est incrémenté de 1 à chaque mise à jour d'origine.

- **Dateur :** il s'agit de la date et de l'heure du début de la mise a jour, issue de l'horloge système du contrôleur de domaine sur lequel a eu lieu la mise a jour d'origine.
- **Serveur GUID (Globally Unique IDentifier – Identificateur universel unique) :** il est défini par le DSA (Directory System Agent) d'origine qui identifie le contrôleur de domaine sur lequel a eu lieu la mise à jour d'origine.

> ✍ Pour que les dateurs soient justes, il est impératif que toutes les horloges des contrôleurs de domaine soient synchronisées. Dans le cas contraire il y a un risque de perte de données dans l'annuaire ou que ce dernier soit endommagé.

On dénombre trois types de conflits potentiels :

- **Conflit d'attribut :** il survient lorsque l'attribut d'un objet est modifié sur différents contrôleurs avec des valeurs différentes. On résout le conflit en gardant l'attribut modifié ayant la plus grande valeur de cachet.
- **Conflit de conteneur supprimé :** ce conflit intervient lorsqu'un objet est ajouté dans un conteneur (par exemple un utilisateur dans l'UO ventes) alors que ce conteneur a été supprimé sur un autre contrôleur de domaine. La réplication n'ayant pas eu lieu, cette suppression n'a pas encore été prise en compte par tous les contrôleurs de domaine. Le conflit est résolu par la récupération des objets orphelins dans le conteneur LostAndFound.
- **Conflit RDN (Relative Distinguish Name) :** ce conflit se produit lorsqu'un répliqua tente de déplacer un objet dans un conteneur dans lequel un autre répliqua a placé un objet portant le même nom. Ce conflit est résolu par le changement de nom de l'objet ayant le cachet le moins important.

7.3. Optimisation de la réplication

Lors de la réplication, un contrôleur de domaine peut recevoir plusieurs fois la même mise à jour, car cette dernière peut emprunter différents chemins. Active Directory emploie le blocage de propagation pour réduire la quantité de données inutiles qui vont transiter d'un contrôleur de domaine à un autre. Ainsi, chaque contrôleur de domaine va gérer une table de vecteurs contenant entre autre des USN (Update Sequence Number). Les USN servant à déterminer ce qu'il est nécessaire de mettre a jour dans un répliqua. Lorsqu'un objet est mis à jour, le contrôleur de domaine affecte l'USN modifié.

> ✍ Il existe un USN pour chaque attribut et un USN pour chaque objet.

7.4. Topologie de réplication

7.4.1. Partitions d'annuaire

La base de données Active Directory se compose logiquement de plusieurs partitions d'annuaire : la partition de schéma, la partition de configuration et les partitions de domaine. Une partition est une unité de réplication indépendante des autres utilisant une procédure de réplication propre.

7.4.1.1. Partition de schéma

Elle contient la définition de tous les objets et attributs pouvant être créés dans l'annuaire, ainsi que les règles de création et de gestion de ces objets. Ces informations sont répliquées sur tous les contrôleurs de domaine de la forêt car il ne peut y avoir qu'un seul schéma pour une forêt.

7.4.1.2. Partition de configuration

Elle contient toutes les informations liées à la structure d'Active Directory, avec entre autres les domaines, domaines enfants, sites, etc…

Ces informations sont, elles aussi, répliquées sur tous les contrôleurs de domaine afin de maintenir l'unicité dans la forêt.

7.4.1.3. Partitions de domaine

Une partition de domaine contient les informations liées aux objets d'un domaine Active Directory. Ces informations sont répliquées sur l'ensemble des DCs du domaine. Par conséquent, il peut exister plusieurs partitions de domaine dans une même forêt.

7.4.2. Topologie de réplication

La topologie de réplication est le chemin que va emprunter le processus de réplication pour mettre à jour les données sur les contrôleurs de domaine.

Deux contrôleurs de domaine impliqués dans la duplication d'Active directory sont liés par des objets de connections, qui sont des chemins de réplication unidirectionnels. On parle aussi de partenaires de réplication.
Les objets de connexion peuvent être créés manuellement par un administrateur où automatiquement, via le KCC.
La gestion des objets de connexion se fait par l'intermédiaire de la console Sites et Services Active Directory.

Lorsque les partenaires de réplications sont directement liés par des objets de connexion, on parle de partenaires de réplication directs.
Si l'on a trois contrôleurs de domaine A,B et C et qu'il existe des objets de connexion entre A-B et B-C, alors A et C sont partenaires de réplication transitifs.
L'utilitaire Réplication Monitor Active Directory (replmon.exe) permet de visualiser les partenaires de réplication transitifs.

7.4.3. Génération de topologie de réplication automatique

Lorsque l'on ajoute un contrôleur de domaine à un site, Active Directory est capable de lier automatiquement ce contrôleur à d'autres via des paires d'objets de connexion. Ceci afin de prendre en compte ce contrôleur dans la réplication.

C'est le KCC (Knowledge Consistency Checker – vérificateur de cohérence des connaissances) s'exécutant sur chaque contrôleur de domaine qui est en charge de cela. C'est donc lui qui génère la topologie de réplication pour la forêt.
Il utilise entre autre les informations sur les différents sites (sous-réseau, type de lien et coût de transmission intersites,…) pour calculer le meilleur chemin entre les contrôleurs de domaine de la forêt.

Au sein d'un même site, la topologie par défaut générée est un anneau à communication bidirectionnelle (deux objet de connexion unidirectionnels en sens opposés entre toutes les paires de contrôleurs de domaines). Des liens supplémentaires sont établis lorsque le nombre de sauts nécessaire pour qu'une mise à jour d'origine atteigne un répliqua est supérieur à trois.

> ☞ Si un problème de communication intersite intervient, le KCC tentera d'établir automatiquement un nouveau chemin de duplication.

7.5. Utilisation des sites pour optimiser la réplication

7.5.1. Présentation des sites

Un site est représenté par un ou plusieurs sous réseaux. Par conséquent, les sites s'appuient sur la structure physique d'un réseau, notamment au niveau des interconnexions de réseaux locaux et étendus.
Un site est automatiquement mis en place lorsque l'on installe le premier contrôleur de domaine dans un domaine. Il est nommé Premier-Site-par-défaut.
Ainsi, même si l'on a un réseau non segmenté en sous réseaux, on aura quand même un site.
Dans le cas d'une entreprise ayant son siège dans une ville et une succursale dans une autre ville, si elle dispose de un ou plusieurs sous réseaux par ville, elle pourra créer un site regroupant les sous réseaux de la première ville et un autre pour les sous réseaux de l'autre ville.

Un site est constitué d'objets serveurs qui correspondent à des contrôleurs de domaine. Les objets serveurs sont créés lorsqu'un serveur sous Windows 2000/2003 est promu en tant que contrôleur de domaine. Ils contiennent entre autres des objets connexion nécessaire à la réplication.

☞ Un site peut contenir des contrôleurs de domaine de n'importe quel domaine d'une forêt.

Pour créer un site, il faut utiliser l'outil d'administration Sites et services Active Directory située dans les outils d'administration. On peut y définir des sous réseaux (représentés par des objets sous-réseau) en précisant l'adresse du sous réseau, le masque de sous réseau ainsi que le site correspondant.

La mise en place de sites permet :

- L'optimisation du trafic de réplication entre les sites.
- La localisant les ressources du réseau (ex : un utilisateur qui ouvre une session le feras sur un contrôleur de domaine situé sur le même site que lui).

En somme l'intérêt des sites dans un réseau peut être de contrôler le volume de données liés au fonctionnement d'Active Directory (trafic de réplication et de connexion). Ceci permet de limiter l'engorgement des liens entre les sous réseaux, en général, une ligne spécialisée, voir même un simple modem 56K.

7.5.2. Réplication intrasite

Elle se produit entre les contrôleurs de domaine situés sur un même site. Les données liées à ce type de réplication ne sont pas compressées par défaut car on considère que les connexions réseau des machines d'un même site sont rapides et fiables. Cela limite le temps processeur utilisé par les contrôleurs de domaine pour la compression.

7.5.3. Réplication intersite

Elle permet à différents sites de récupérer les modifications apportées à Active Directory depuis un contrôleur de domaine situé sur un site, et ce, en empruntant des chemins considérés comme non fiables et avec une faible bande passante.

If faudra créer des liens de site pour lesquels il faudra définir manuellement un certain nombre de paramètres pour déterminer le moment auquel la réplication intervient et la fréquence à laquelle les contrôleurs de domaine vérifieront si des modifications ont été apportées à Active Directory.
Le trafic lié à la réplication intersite est compressé avec un ratio d'environ 15% pour transiter efficacement par des liaisons à faible débit. L'inconvénient est la charge CPU supplémentaire sur les contrôleurs de domaine.

☞ La duplication intersite étant programmée manuellement, le système de notification des modifications n'est employé que pour le trafic intrasite.

7.5.4. Notion de coût

Lors de la mise en place des liens de sites, on peut définir un certain nombre de propriétés, et notamment le coût.
Le coût d'un lien de site est un nombre qui représente l'efficacité, la vitesse, la fiabilité (relatifs) d'un chemin, un peu à l'image des routeurs.
Le trafic de duplication empruntera toujours le chemin (un chemin peut être composé d'un ou plusieurs liens de sites) dont le coût total sera le plus faible.
Par exemple, si nous avons trois sites A, B, C et qu'il existe des liens intersites A-B (coût 100), B-C (coût 10), C-A (coût 10), le trafic de duplication entre A et B empruntera le chemin AC puis CB, pour un coût total de 20 au lieu de A-B pour un coût de 100.

> ✍ Le coût par défaut d'un lien intersite est de 100.

7.5.5. Serveur tête de pont

Dans la duplication intersites, un ou plusieurs serveurs sur chaque site peuvent servir de « ponts » entre les sites par lesquels le trafic de duplication va se propager. On les nomme les serveurs têtes de pont.
Par conséquent, les duplications intersites passent uniquement par des têtes de ponts.
Dans chaque site, un contrôleur de domaine est automatiquement désigné comme serveur tête de pont par l'ISTG (InterSite Topology Generator ou générateur de topologie inter-site), chargé de mettre en œuvre la réplication intersite (c'est un contrôleur de domaine de la forêt).
Lorsqu'un serveur tête de pont reçoit une mise à jour depuis un autre site, il la communiquera aux contrôleurs de domaine de son site suivant la procédure classique de duplication intrasite.
Il est possible de définir manuellement des serveurs têtes de pont plutôt que de laisser l'ISTG choisir.

Le serveur tête de pont peut être déterminé en allant dans l'outil d'administration Sites et services Active Directory situé dans les outils d'administration.

7.6. Protocoles de réplication

Les ordinateurs emploient des protocoles de réplication pour transmettre leurs mises à jour d'Active Directory.
Le protocole RPC (encore appelé RPC sur IP) est employé lors de la duplication intrasite. Ce dernier assure une connexion fiable et à grande vitesse.
Dans le cas de la duplication intersites, il est possible de paramétrer le protocole employé, à savoir RPC ou SMTP (Simple Mail Transfer Protocol).
En général, on utilisera RPC pour la réplication intersite.

> ✍ Le protocole SMTP ne peut être utilisé qu'avec des contrôleurs de domaine se trouvant dans des domaines et des sites différents, il ne prend pas en charge la réplication de la partition de domaine. De plus il nécessite une autorité de certification pour signer les messages SMTP.

8. Implémentation du placement des contrôleurs de domaine

8.1. Le rôle du serveur de catalogue global

8.1.1. Définition du serveur de catalogue global

Le catalogue global ou GC (Global Catalogue) permet aux utilisateurs d'effectuer 2 tâches importantes :

Trouver des informations Active Directory sur toutes la forêt, quel que soit l'emplacement des ces données.
Utiliser des informations d'appartenance à des groupes universels pour ouvrir une session sur le réseau.

Un serveur de catalogue global est un contrôleur de domaine qui conserve une copie du catalogue global et peut ainsi traiter les requêtes qui lui sont destinées. Le premier contrôleur de domaine est automatiquement le serveur de catalogue global. Il est possible de configurer d'autres contrôleurs de domaine en serveur de catalogue global afin de réguler le trafic.

8.1.2. L'importance du catalogue global dans le processus d'authentification

Voici les étapes importantes qui sont réalisées lorsqu'un utilisateur s'authentifie sur le domaine :

1. **L'utilisateur entre des informations d'identification** (son identifiant, son mot de passe ainsi que le domaine sur lequel il souhaite ouvrir une session) sur un ordinateur membre du domaine afin d'ouvrir une session.

2. Ces informations d'identification sont **cryptées par le centre de distribution de clefs** ou KDC (pour Key distribution Center), puis **envoyées à l'un des contrôleurs de domaine** du domaine de l'ordinateur client.

3. **Le contrôleur de domaine compare les informations** d'identification cryptées du client avec celles se trouvant sur Active Directory (les informations stockées dans le service d'annuaire Active Directory qui sont cryptées nativement). Si les informations concordent alors le processus continue, sinon il est interrompu.

4. Le contrôleur de domaine **crée ensuite la liste de tous les groupes dont l'utilisateur est membre**. Pour cela, le contrôleur de domaine interroge un serveur de catalogue global.

5. Le contrôleur de domaine fournit ensuite au client **un ticket d'accord ou TGT (Ticket Granting Ticket)**. Le TGT contient les identificateurs de sécurité ou SID (Security Identifier) des groupes dont l'utilisateur est membre (Un TGT expire au bout de 8 heures ou bien quand l'utilisateur ferme sa session).

6. Une fois que l'ordinateur client a reçu le TGT, **l'utilisateur est authentifié** et peut tenter de charger son profil et d'accéder aux ressources du réseau.

> Si le serveur de catalogue global n'est pas joignable, le processus d'authentification est mis en échec. En effet, le contrôleur de domaine ne peut pas obtenir les SID des groupes dont l'utilisateur

est membre lorsque le serveur de catalogue global est indisponible. Dans ce cas le contrôleur de domaine n'émet pas de TGT et l'utilisateur ne peut pas ouvrir sa session.

8.1.3. L'importance du catalogue global dans le processus d'autorisation

Voici les étapes importantes qui sont réalisées lorsqu'un utilisateur authentifié essaye d'accéder à une ressource sur le domaine :

1. **Le client essaye d'accéder à une ressource** située le réseau (ex. : serveur de fichier).

2. **Le client utilise le TGT** qui lui a été remis lors du processus d'authentification pour accéder au service d'accord de ticket ou TGS (Ticket Granting Service) situé sur le contrôleur de domaine.

3. **Le TGS émet un ticket de session** pour le serveur sur lequel se trouve la ressource qu'il envoie au client. Le ticket de session contient les identificateurs SID des groupes auxquels l'utilisateur appartient.

4. **Le client envoie son Ticket de session au serveur de fichier.**

5. **L'autorité de sécurité locale ou LSA** (pour Local Security Authority) du serveur de fichier utilise les informations du ticket de session pour **créer un jeton d'accès**.

6. L'autorité **LSA contacte ensuite le contrôleur de domaine** et lui envoie les SIDs de tous les groupes figurant dans la liste DACL (Discretionary ACcess List) de la ressource. Le contrôleur de domaine doit ensuite joindre **un serveur de catalogue global** afin de connaître les identificateurs de sécurité (ou SIDs) des groupes de la liste DACL dont l'utilisateur est membre.

7. Enfin, l'autorité LSA compare les identificateurs SID du jeton d'accès avec les SID des groupes dont l'utilisateur est membre et qui figurent dans la liste DACL. Si les groupes auxquels l'utilisateur appartient sont autorisés à accéder à la ressource alors l'utilisateur peut accéder à la ressource sinon, l'accès est refusé.

☞ Si le serveur de catalogue global est indisponible, alors le processus d'autorisation ne peut pas se poursuivre et l'utilisateur ne peut pas accéder à la ressource.

8.1.4. La mise en cache de l'appartenance au groupe universel

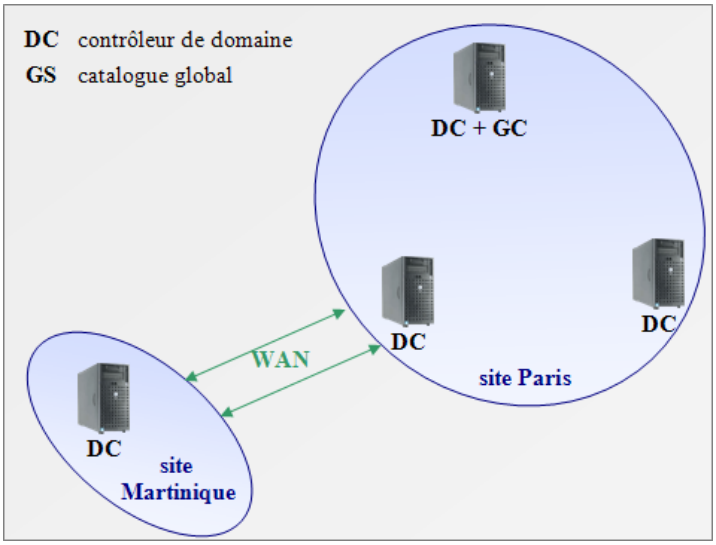
La fonction de mise en cache de l'appartenance au groupe universel est disponible uniquement sur les contrôleurs de domaine exécutant Windows 2003 server. La mise en cache de l'appartenance au groupe universel consiste à stocker sur un contrôleur de domaine les résultats des requêtes effectuées auprès d'un serveur de catalogue global.

La mise en cache de l'appartenance au groupe universel est principalement utilisée lorsque deux sites sont reliés entre eux par une liaison WAN (Wide Area Network) possédant une faible bande passante (par exemple une connexion RNIS à 128Kb/s). En effet, dans ce cas de figure la connexion WAN impose diverses restrictions au niveau de l'implémentation du réseau :

Il est obligatoire de placer un contrôleur de domaine dans le site distant sinon la connexion ralentira les ouvertures de session.
Il n'est pas possible d'héberger le catalogue global sur le site distant car la réplication entre les serveurs de catalogue global entraîne un trafic réseau trop important.

Malgré le fait qu'un contrôleur de domaine soit disponible en local dans le site distant, le trafic entre les deux sites reste élevé puisque pour chaque ouverture de session ou bien chaque accès à une ressource partagée, le contrôleur de domaine accède à un serveur de catalogue global situé dans la maison mère. Une solution à ce problème est donc l'implémentation de la mise en cache de l'appartenance au groupe universel.

Le schéma ci-dessous illustre l'utilisation classique de la mise en cache de l'appartenance au groupe universel :



Lorsqu'un utilisateur du site Martinique tente d'ouvrir sa session pour la première fois, il contacte le contrôleur de domaine qui va lui-même contacter le serveur de catalogue global (GS sur le schéma) afin de récupérer les SIDs des groupes dont l'utilisateur est membre. Le contrôleur de domaine va ensuite mettre en cache les informations qu'il a reçues du serveur de catalogue global pendant une durée de 8 heures (durée par défaut). La même opération (mise en cache) est effectuée lors du premier accès de l'utilisateur à une ressource partagée.

Si l'utilisateur se « logue » de manière récurrente sur le domaine ou bien si il accède régulièrement à des partages réseaux, le contrôleur de domaine du site Martinique utilise les informations situées dans son cache. Cela offre trois grands avantages :

Les authentifications des utilisateurs et les accès aux ressources du réseau sont moins dépendantes de la liaison WAN.
Le trafic d'authentification et d'autorisation au niveau de la liaison WAN utilise peu de bande passante.
La résolution de l'appartenance au groupe universel est plus rapide puisque le contrôleur de domaine possède les informations nécessaires en local.

9. Gestion des maîtres d'opérations

9.1. Présentation des maîtres d'opérations

Les modifications d'Active Directory peuvent être faites sur n'importe quel contrôleur de domaine. Il y a toutefois 5 exceptions pour lesquelles les modifications sont faites sur un et un seul contrôleur de domaine particulier : les 5 rôles des maîtres d'opérations.

Voici les cinq rôles des maîtres d'opérations :

- Contrôleur de schéma
- Maître d'attribution des noms de domaine
- Emulateur CPD
- Maître d'identificateur relatif
- Maître d'infrastructure.

Les deux premiers sont assignés au niveau de la forêt, les trois derniers au niveau du domaine. Ce qui implique s'il y a plusieurs domaines dans une forêt, autant de maîtres d'opérations pour les trois derniers rôles, que de domaines.

Par défaut le premier contrôleur de domaine d'une nouvelle forêt contient les cinq rôles.

9.1.1. Rôle du contrôleur de schéma

Il est le seul dans une forêt à pouvoir modifier le schéma. Il duplique les modifications aux autres contrôleurs de domaine dans la forêt lorsqu'il y a eut une modification du schéma. Le fait d'avoir un seul ordinateur qui gère le schéma évite tout risque de conflits.

Un seul groupe peut faire des modifications sur le schéma : le groupe « administrateurs du schéma ».

9.1.2. Maître d'attribution de nom de domaine

Seul le contrôleur de domaine ayant ce rôle, est habilité à ajouter un domaine dans une forêt. Si le maître d'opération d'attribution de nom de domaine n'est pas disponible, il est impossible d'ajouter ou de supprimer un domaine à la forêt.

Du fait de son rôle, le maître d'attribution de nom de domaine est aussi un serveur de catalogue global. En effet pour éviter tous problèmes, celui-ci doit connaître tous les noms des objets présents dans la forêt.

9.1.3. Emulateur CPD (PDC)

Ce rôle a été créé principalement dans un souci de permettre une compatibilité avec les versions antérieures de Windows 2000.

Rôle propre aux versions antérieures à Windows 2000 :

- Il permet la prise en charge des BDC Windows NT4.
- Il a la gestion des modifications des mots de passes pour des clients antérieurs à Windows 2000.

Autres Rôles :

- Authentification de secours: Lorsque vous avez modifié votre mot de passe sur votre ordinateur, et que vous vous connectez peu de temps après sur une autre machine, il se peut que la réplication du changement de votre mot de passe n'ait pas encore été effectuée. Dans ce

cas, le DC qui vérifie votre mot de passe va demander à l'émulateur CPD si votre mot de passe n'a pas été changé avant de vous refuser l'accès.
- Synchroniser l'heure de tous les DC en fonction de son horloge.
- Elimine les risques d'écrasement d'objets GPO : par défaut la modification de GPO se fait sur ce DC.

9.1.4. Maître RID

Un SID est composé de deux blocs : un identificateur de domaine et un RID (Identificateur unique dans le domaine).

Pour qu'il ne puisse y avoir deux DC qui assignent le même SID à deux objets différents, le maître RID distribue une plage de RID à chacun des DC. Lorsque la plage de RID a été utilisée, le DC demande une nouvelle plage de RID au maître RID.

Le maître RID à aussi la charge des déplacements inter-domaines, pour éviter la duplication de l'objet.

9.1.5. Maître d'infrastructure

Le maître d'infrastructure sert à mettre à jour, dans son domaine, les références à des objets situés dans d'autres domaines. Si des modifications d'un objet du domaine surviennent (déplacement intra et extra domaine), alors si cet objet est lié à un ou plusieurs objets d'autres domaines, le maître d'infrastructure est responsable de la mise à jour vers les autres domaines. La mise à jour se fait par le biais d'une réplication.
Un Maître d'infrastructure ne peut être aussi un serveur de catalogue global.

9.2. Transfert et prise de rôles de maîtres d'opérations

Si le serveur défaillant sera rapidement remis en marche, ne transférez pas le rôle de maître d'opération.
On ne transfère le rôle de maître d'opération que lorsque le serveur ne pourra pas être remis en marche ou dans des délais longs. (La limite en temps est vague car elle dépend de l'environnement de votre réseau, cela peut être une journée comme une semaine).

9.2.1. La défaillance de l'Emulateur de CPD

La défaillance est la plus handicapante :
- Les ordinateurs clients exécutant une version antérieure à Windows 2000 ne pourront plus s'authentifier.
- Perte de la diminution de latence pour la mise à jour des mots de passe.
- Eventuelle perte de synchronisation horaire entre les contrôleurs.

9.2.2. Défaillance du maître d'infrastructure

Limite le déplacement des objets dans Active Directory

9.2.3. Défaillance des autres maîtres d'opérations

Ces défaillances sont les moins gênantes. Il est préférable de restaurer une sauvegarde de ces maîtres d'opérations plutôt que de les transférer, le transfert de ces maîtres d'opérations peut entraîner des erreurs dans les données.

La prise du rôle de ces maîtres d'opérations ne doit être envisagée qu'en dernier recours.

10.Maintenance d'Active Directory

10.1. Entretien de la base de données Active Directory

La sauvegarde d'Active Directory doit être effectuée régulièrement. La sauvegarde de l'Etat du Système sur un DC sauvegarde la base de données AD (ainsi que le dossier sysvol, le Registre, les fichiers de démarrage du système, l'inscription des classes et les certificats).

La défragmentation d'Active Directory doit être effectuée de temps en temps, pour éviter que la base de données AD ne prenne trop d'espace disque. (L'utilitaire NTDSUTIL permet de défragmenter la base de données).
Lors de la défragmentation la base de données AD est déplacée, l'original peut être conservé en tant que backup.
Le déplacement de la base de données AD peut être nécessaire lors d'un manque d'espace disque.

10.1.1. Fichiers d'Active Directory

- **Ntds.dit** : Base de données contenant les objets d'Active Directory.
- **Edb*.log** : Journal des modifications sur la base de données
- **Edb.chk** : Fichier de contrôle, permet de ne pas perdre d'informations ou de corrompre la base de données lors d'un sinistre.
- **Res*.log** : ces fichiers ne sont là que pour réserver de l'espace disque pour le fichier de journal.

☞ Le moteur de la base de données Active Directory est nommé ESE (Extensive Storage Engine)

10.1.2. Nettoyage de la mémoire

Un processus s'exécute toutes les douze heures pour supprimer les objets obsolètes d'Active Directory et défragmenter la mémoire utilisée par Active Directory. Lors de la suppression d'un objet Active Directory, il est placé dans le conteneur Deleted Objects et lorsqu'il aura dépassé sa durée de vie désactivée (par défaut 60 jours), le processus de nettoyage de la mémoire le supprimera.

10.1.3. Restauration d'Active Directory

Il existe trois types de restauration :

- Forcée (authoritative)
- Normale ou Non Forcée (non authoritative)
- Principale

Une restauration forcée est utile dans le cas ou vous avez effacé des objets dans Active Directory par erreur, et que la réplication a été effectuée entre les différents contrôleurs de domaines. Les objets effacés vont être restaurés et répliqués aux autres DC.

Une restauration non forcée, est une restauration dite 'normale' toutes les modifications faites depuis la sauvegarde vont être récupérées lors de la prochaine réplication entre les DCs.

La restauration principale doit être utilisée uniquement lorsque **les données contenues dans tous les contrôleurs de domaine du domaine sont perdues**. Une restauration principale reconstruit le premier contrôleur de domaine à partir de la version sauvegardée. Utilisez ensuite la restauration normale sur les autres contrôleurs de domaine. Ce mode doit être utilisé lorsqu'il n'existe aucune autre

manière de reconstruire le domaine. En effet, toutes les modifications postérieures à la sauvegarde sont perdues.