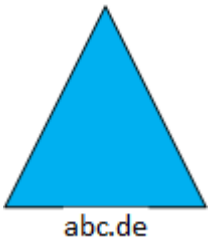
Table des matières

1 Au-delà du domaine !

Lors de l'introduction à Active Direcroty, nous avons essentiellement examiné ce qui se trouve à l'intérieur du domaine : le contrôleur de domaine (avec notamment NTDS.DIT présent dans le dossier *%systemroot%/NTDS*) et des objets de l'AD comme les groupes, les utilisateurs, les ordinateurs, les OU, etc. Mais lorsqu'un serveur est promu DC d'un nouveau domaine, il ne se crée pas seulement un domaine !



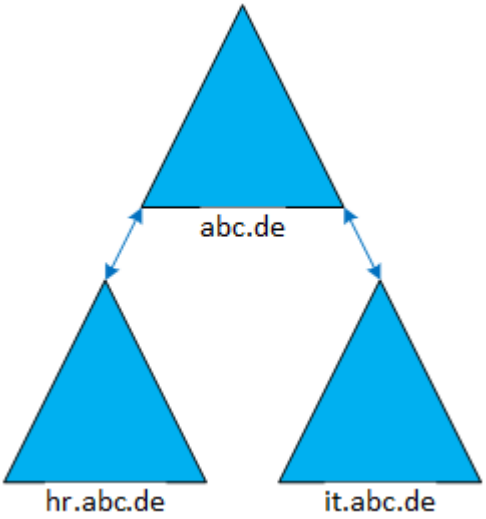
En créant le nouveau domaine abc.de, on crée également le premier arbre d'une forêt. Ce premier arbre est la racine (root tree).

Création d'abc.de = création 1 domaine | 1 arbre | 1 forêt !

Les termes anglais tree, forest et namespace sont souvent préférés aux mots français arbre, forêt et espace de nom (ou espace de nommage). La traduction n'est pourtant pas pire que pour d'autres termes du jardon…

2 Forêt à un arbre

Après avoir créé un domaine, il est parfois nécessaire de créer des sous-domaines. Les raisons de la création sont variables (organisation, taille de l'entreprise) mais il faut garder à l'esprit qu'un domaine est une limite administrative...



En faisant évoluer l'exemple, le domaine abc.de comporte à présent deux sous-domaines (child domain) : hr.abc.de et it.abc.de :

3 domaines | 1 arbre| 1 forêt

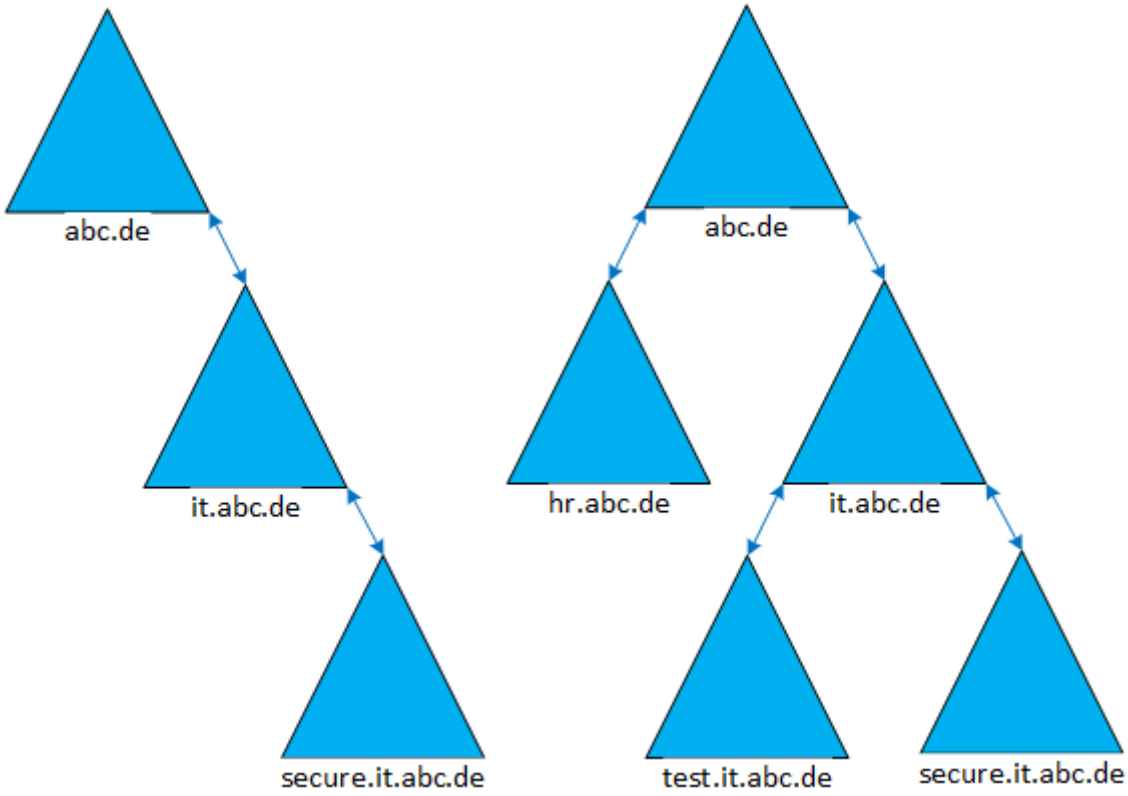
Pour hr.abc.de et it.abc.de, abc.de est le domaine parent (parent domain).

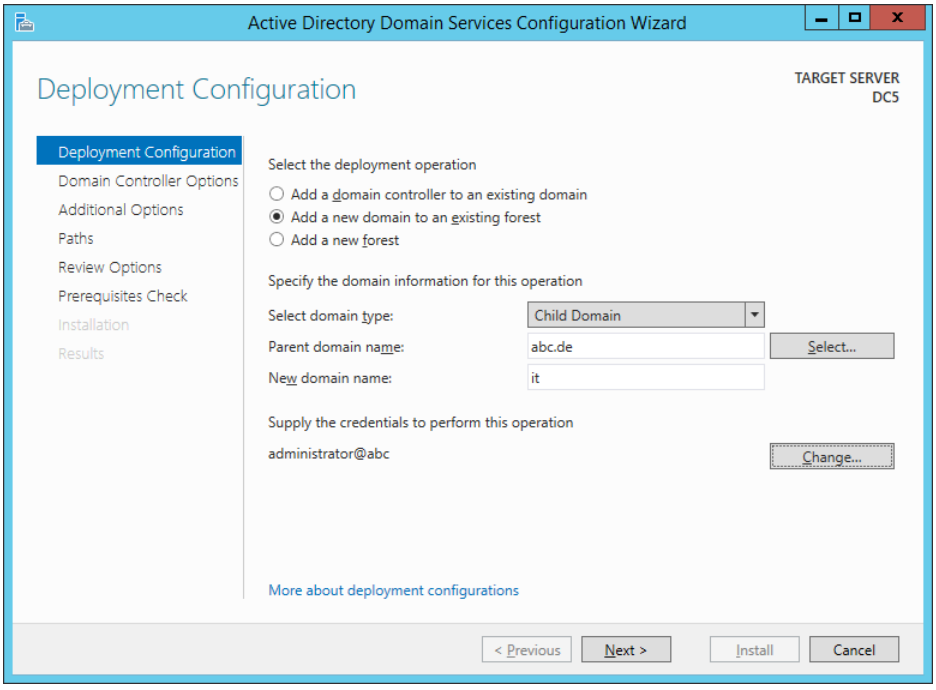
Un arbre est un ensemble de domaines partageant le même espace de nom (namespace) reliés entre eux par une relation de confiance bidirectionnelle et transitive. Ces relations de confiance sont appelées des Trusts. Elles sont générées automatiquement lors de la création des sous-domaines.

Un arbre peut évoluer de différentes manières comme le montrent les deux illustrations suivantes.

- A gauche, la structure change mais on conserve : 3 domaines | 1 arbre| 1 forêt.
- A droite, la structure évolue : 5 domaines | 1 arbre | 1 forêt.

Chaque domaine conserve son propre AD.





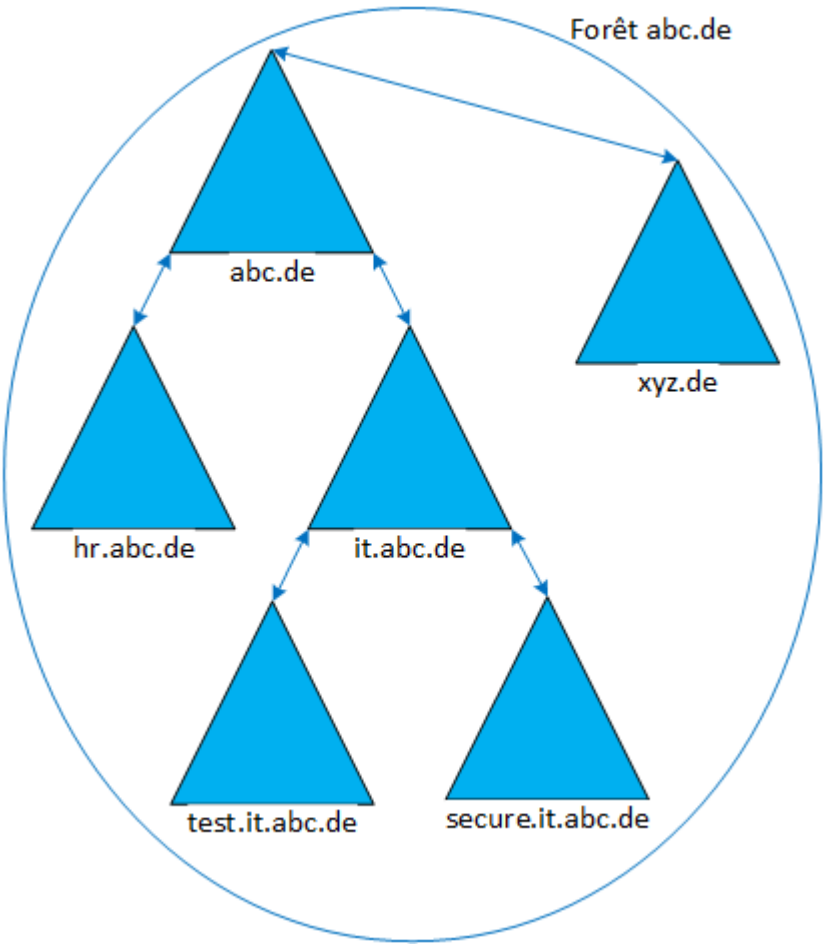
Cette capture issue de Windows 2012 R2 montre l'ajout du sous-domaine it dans le domaine abc.de.

Add a new domain to an existing forest permet au choix d'ajouter un *child domain* ou un *Tree domain* (voir plus loin).

3 Forêt avec plus d'un arbre

La forêt de notre exemple ne comporte qu'un seul arbre. A présent, un nouvel arbre xyz.de va étendre notre forêt.

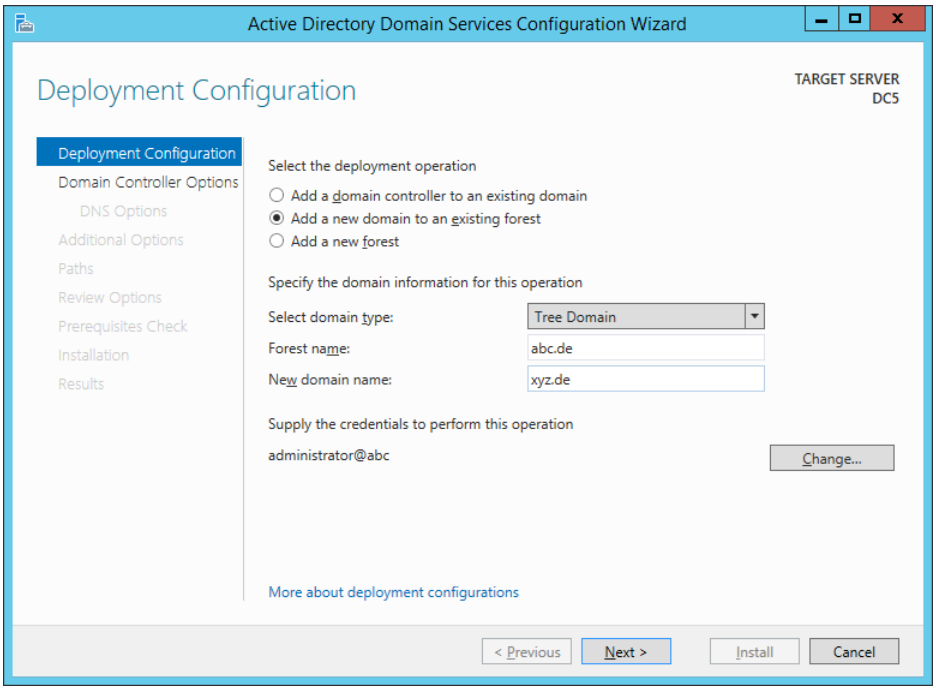
L'ajout de ce nouvel arbre ne change rien au nom de la forêt. Elle conserve le nom de forêt abc.de, c'est-à-dire le nom utilisé pour créer le premier domaine. Une relation de confiance bidirectionnelle et transitive est automatiquement crée entre abc.de et xyz.de.



A ce stade, la forêt abc.de comprend :

6 domaines | 2 arbres | 1 forêt

- La forêt utilise un seul et unique schéma.
- Il doit exister au moins un serveur Global Catalog par domaine.
- Chaque domaine conserver son autonomie.



La création d'un nouvel arbre utilise l'assistant habituel de promotion d'un DC.

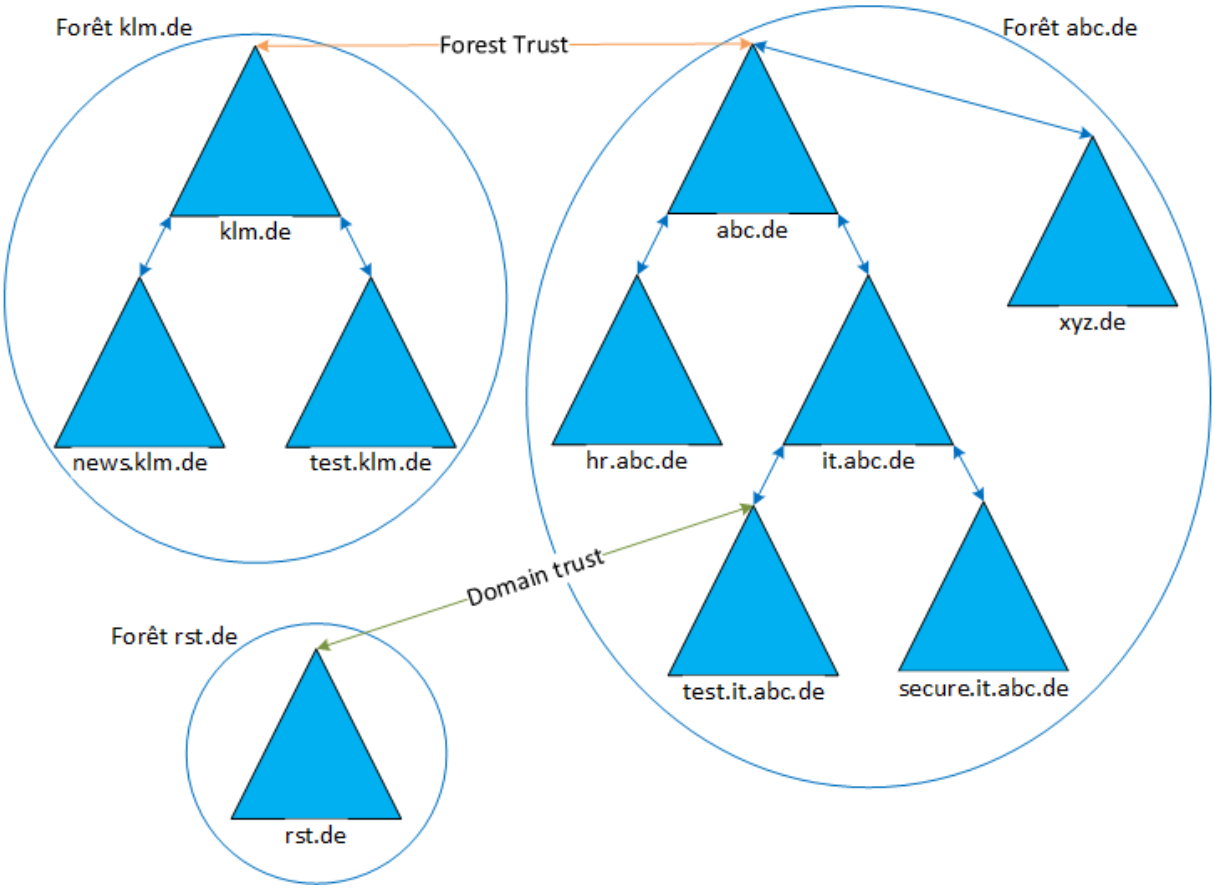
Cette fois, dans *Add a new domain to an existing forest,* c'est l'option *Tree Domain* qui est utilisée. Ce n'est plus le *parent name* qui est demandé mais le *Forest Name.*

4 Les relations d'approbation (Trusted relation)

Pour faciliter le partage de ressources, il peut être utile d'établir des relations privilégiées entre différents domaines ou forêts :

- Une entreprise rachète une autre entreprise
- Deux entreprises distinctes collaborent temporairement à un projet commun.

Deux notions interviennent dans les relations d'approbations : la direction et la transitivité.



Le Shortcut Trust n'est pas représenté, il permet de créer une relation par exemple entre test.it.abc.de et hr.abc.de dans le but d'optimiser les performances si ces deux domaines travaillent régulièrement ensemble.

4.1 Direction

Une relation d'approbation peut être à sens unique ou bidirectionnelle.

- La relation unidirectionnelle ne va logiquement que dans un sens. Le domaine A peut approuve le domaine B sans que le domaine B n'approuve le domaine A. Les utilisateurs du domaine A ont accès aux ressources du domaine B mais les utilisateurs du domaine B n'ont pas accès aux ressources du domaine A.
- La relation bidirectionnelle va dans les deux sens. Les utilisateurs de chaque domaine ont accès aux ressources de l'autre domaine.

4.2 Transitivité

Outre sa directivité, la relation d'approbation peut être transitive ou ne pas l'être. La transitivité peut être vue comme un héritage de l'approbation.

Si le domaine A approuve le domaine B et que le domaine B approuve le domaine C, alors A approuve C.

4.3 Prédéfinies ou externes

Les relations d'approbations se créent de deux manières différentes :

- Les relations prédéfinies résultent de la création d'un arbre ou d'une forêt et sont d'emblée définies au niveau de la direction et de la transitivité.
- Les relations externes doivent être crées manuellement d'un domaine vers un autre ou d'une forêt vers une autre. Elles sont unidirectionnelles et non transitives.

5 Le niveau fonctionnel

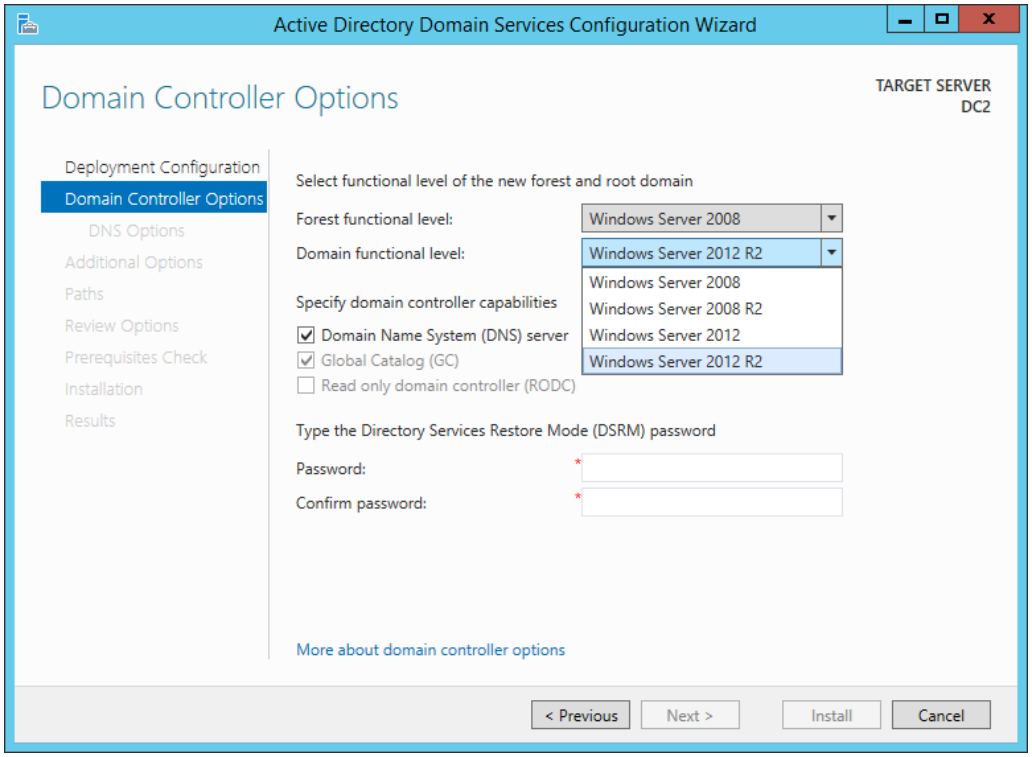
Une forêt est un regroupement d'arbres mais pour être en mesure de regrouper des arbres et avoir une communication au sein de la forêt, il faut un niveau fonctionnel commun. Le niveau fonctionnel s'affiche sous forme d'une version de Windows Server et indique que les fonctionnalités supportées par cette version de Windows Server sont disponible dans le domaine et/ou la forêt.

Lors de la promotion d'un serveur en contrôleur de domaine, un domaine est créé mais aussi une forêt. La forêt et le domaine ont chacun leur niveau de fonctionnalité réglable de manière indépendante.

Au fil des versions, Windows Server évolue avec bien entendu de nouvelles fonctionnalités. Dans la politique de Microsoft, « qui peut le plus, peut le moins » ! Les versions plus récentes de Windows Server restent compatibles avec les plus anciennes. Certaines fonctions de l'Active Directory ne sont alors plus disponibles.

Il faut être vigilant lors de la sélection des niveaux de fonctionnalité ! En effet :

- Le niveau fonctionnel est choisi lors de la promotion du serveur en contrôleur de domaine.
- Le niveau des domaines est égal ou supérieur à celui de la forêt.
- Le niveau de fonctionnalité peut uniquement être augmenté !



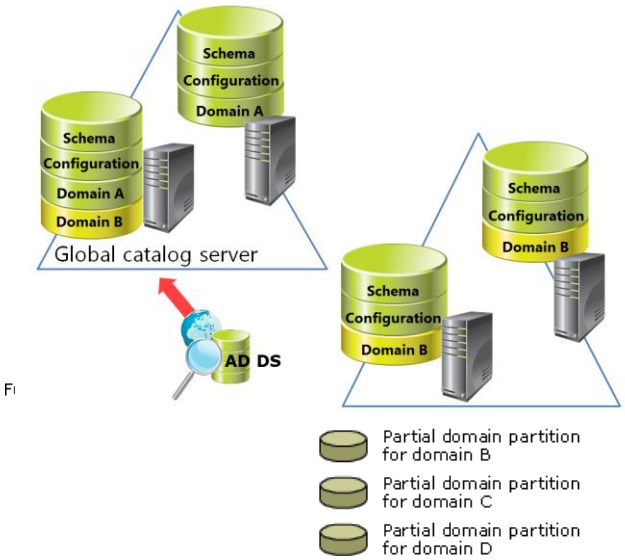
Le niveau fonctionnel assure la compatibilité mais des limites existent :

- Windows Server 2012 et 2012 R2 assurent la compatibilité avec Windows Server 2008 et Windows Server 2008 R2.
- Windows Server 2008 et 2008 R2 dont rétro compatibles jusqu'à Windows Server 2003 et Windows Server 2000.

Il n'est ainsi pas possible d'intégrer directement un domaine limité au niveau fonctionnel de Windows Server 2000 ou 2003 dans un enivrement Windows Server 2012 ou 2012 R2. Des migrations sont donc nécessaires…

6 Le catalogue global (et PAS)

Le catalogue global (en anglais : global catalogue, en version courte : CG ou GC) est un contrôleur de domaine spécifique qui contient une copie de tous les objets de son domaine (comme tout DC) ET en plus une copie en lecture seule des objets de tous les domaines de la forêt. Lors de la création d'un nouveau domaine, le serveur est promu contrôleur de domaine, une forêt est créée (on commence à le savoir) mais le serveur n'est pas simplement promu DC, il devient un DC GC. La capture précédente montre la casée cochée et grisée : Global Catalog (GC).



L'interrogation de l'AD sur un DC se fait via LDAP part le port 389 mais l'interrogation d'un DC GC passe par le port 3268.

Dans le cadre d'une forêt d'une grande entreprise établie dans plusieurs continents, interroger un DC GC dans le réseau local est bien plus rapide que l'interrogation d'un DC situé par exemple outre-Atlantique. Pour atteindre ce dernier, il faut passer par une connexion WAN moins rapide que le réseau local. En outre, le décalage horaire pourrait conduire à l'interrogation à un moment où il est fort chargé.

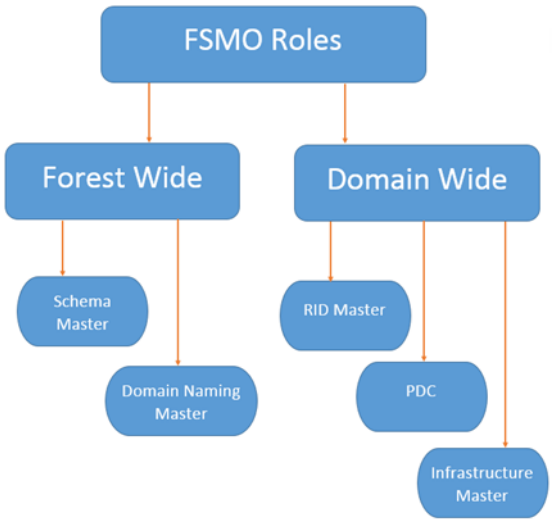
En pratique, afin de préserver la bande passante et éviter que le fichier NTDS.DIT ne devienne trop volumineux, le GC ne contient pas tous les attributs de l'AD des autres domaines de la forêt. Seul un jeu d'attribut « réduit » (mais largement suffisant) est présent dans le GC : le PAS pour Partial Attribute Set. Les attributs custom ne sont pas repris dans le PAS.

Parmi les attributs non repris, on peut citer : logonCount, accountExpires, lastLogoff, lastLogon, logonHours et pwdLastSet. Il n'y a guère de raisons de savoir quand des utilisateurs d'un autre domaine de la forêt ont changé leur mot de passe ou quand leur compte expire…

Si les besoins l'exigent, des attributs peuvent être ajoutés au PAS. Mais attention : il faut modifier le schéma de l'AD, ce qui ne peut absolument pas se faire à l'aveuglette.

7 Les rôles FSMO

Rappel : Les contrôleurs de domaine sont des serveurs particuliers qui stockent et répliquent les données relatives à l'AD (NTDS.DIT, LOGS et SYSVOL), permettent l'authentification des utilisateurs et appliquent les stratégies de groupes.



Vu sous un autre angle, tous les DC assurent un certain nombre de tâches communes… Il s'agit essentiellement des rôles de réplication. Ce système est appelé multi maitre (multi-master) car chaque DC peut modifier la base de données de l'AD et répliquer ces modifications aux autres DC afin que chaque DC dispose de la même base de données AD. Le model multi maitre présente l'avantage évident d'une redondance élevée (chaque DC a une copie de l'AD) mais peut être source de conflits de type « last writer wins ».

Certains rôles critiques ne peuvent soumis à aucun conflit et ne peuvent être dupliqués ! Il s'agit des cinq rôles appelés FSMO pour Flexible Single Master Operation. Le « Single Master » (ou maitre unique) de FSMO s'oppose naturellement à multi master : un et un seul DC assure le rôle pout le domaine ou pour la forêt.

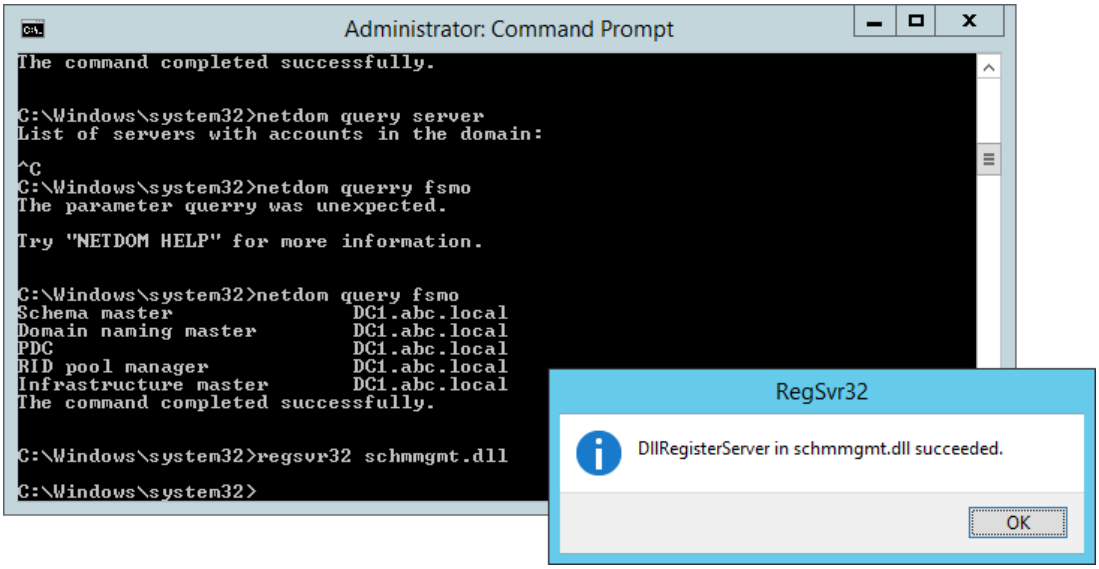
Lorsqu'un serveur est promu DC d'un nouveau domaine, il reçoit également les 5 rôles FSMO.

7.1 Schema Master

Le schéma master est le seul contrôleur de domaine d'une forêt qui peut apporter des changements au schéma de l'Active Directory. Le schéma de l'AD étant rarement modifié, le schéma master n'est

pas souvent sollicité. Le schéma master est par contre fortement sollicité lors de l'installation d'Outlook qui nécessite des modifications importantes du schéma en raison de l'ajout de nombreux attributs. Le schéma master est également actif en cas d'élévation du niveau fonctionnel. Lorsque les modifications du schéma sont terminées, elles sont répliquées du schéma master vers les autres DC. L'opération est à sens unique !

Pour modifier le schéma et donc faire travailler le Schema Master, il faut être membre du groupe schema administrator et avoir accès à la console de schéma (qui nécessite le passage par une ligne de commande). L'accès au schéma est bardé de garde-fous tant la modification du schéma est critique…



Le rôle du Schema Master est critique mais comme il est inutile 99,9999% du temps, sa présence n'est pas critique. Si le Schema Master n'est pas joignable, tous les services AD fonctionnent. Il serait juste impossible par exemple d'installer Outlook ou tout autre logiciel nécessitant une modification du schéma.

Le Schema Master travaille sur LDAP://cn=schema,cn=configuration,dc=<domain> (schema naming context).

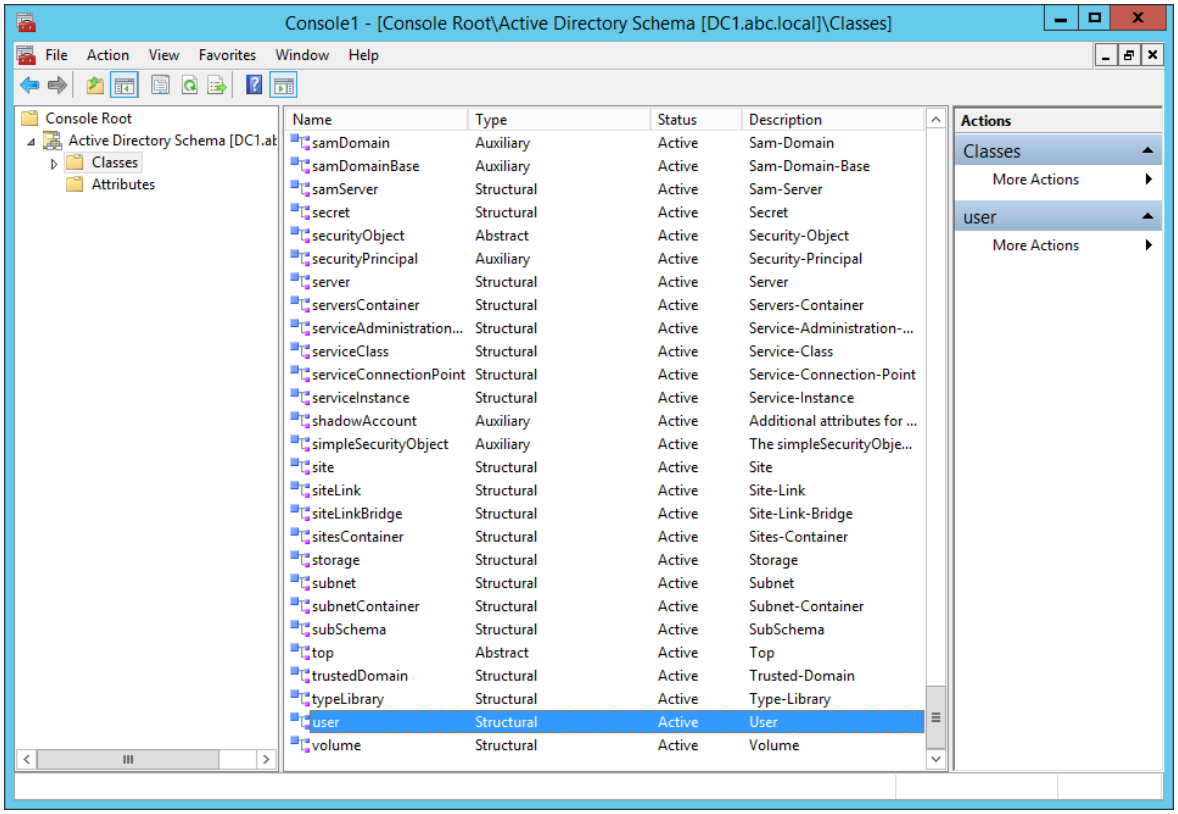
7.1.1 Accéder au schéma…

Accéder au schéma permet de visualiser des notions qui pourraient encore être abstraites…

- Sur un serveur promu DC d'un nouveau domaine, ouvrir une invite de commandes en mode administrateur et taper : `regsvr32 schmmgmt.dll` (voir la capture ci-dessus).
- Toujours dans l'invite de commandes ou en mode exécution (WIN + R), taper : `mmc`
- Dans la console MMC, via *File, Add/Remove Snap-in…*, ajouter *Active Directory Schema*. Puis cliquer sur OK.
- La console MMC affiche à présent le schéma de l'Active Directory (voir ci-dessous).

7.1.2 Les propriétés d'une classes

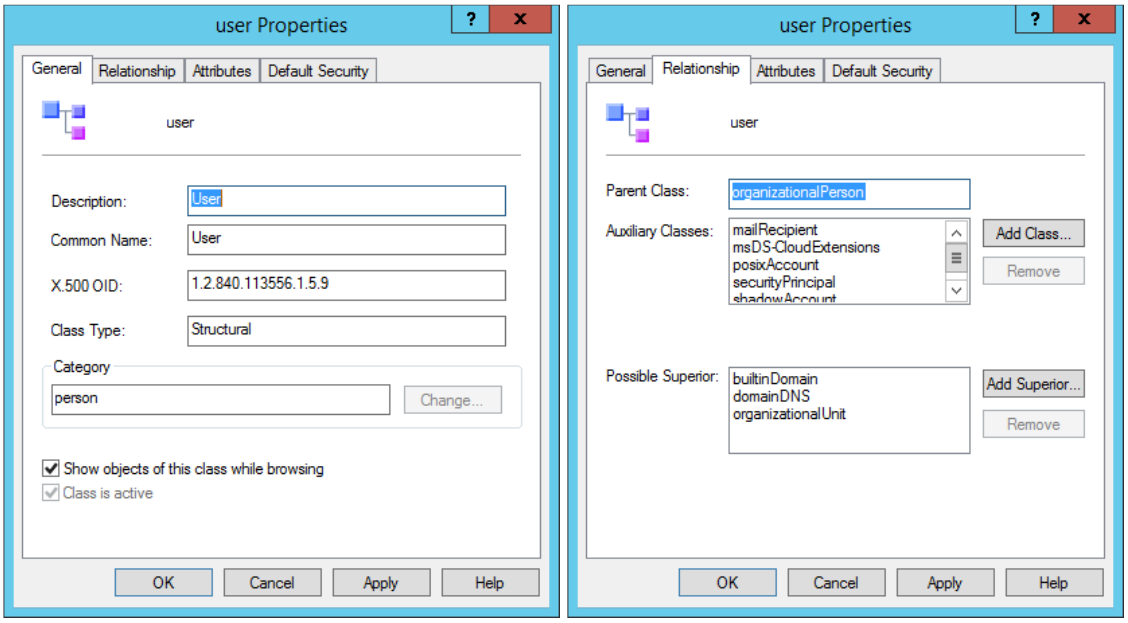
En sélectionnant *Classes* dans le volet de gauche, la console affiche toutes les classes d'objets existantes dans le schéma actuel. Certaines ont déjà été abordées comme : *computer, user, organizationalUnit*, etc.



Les propriétés de la classe utilisateur montrent

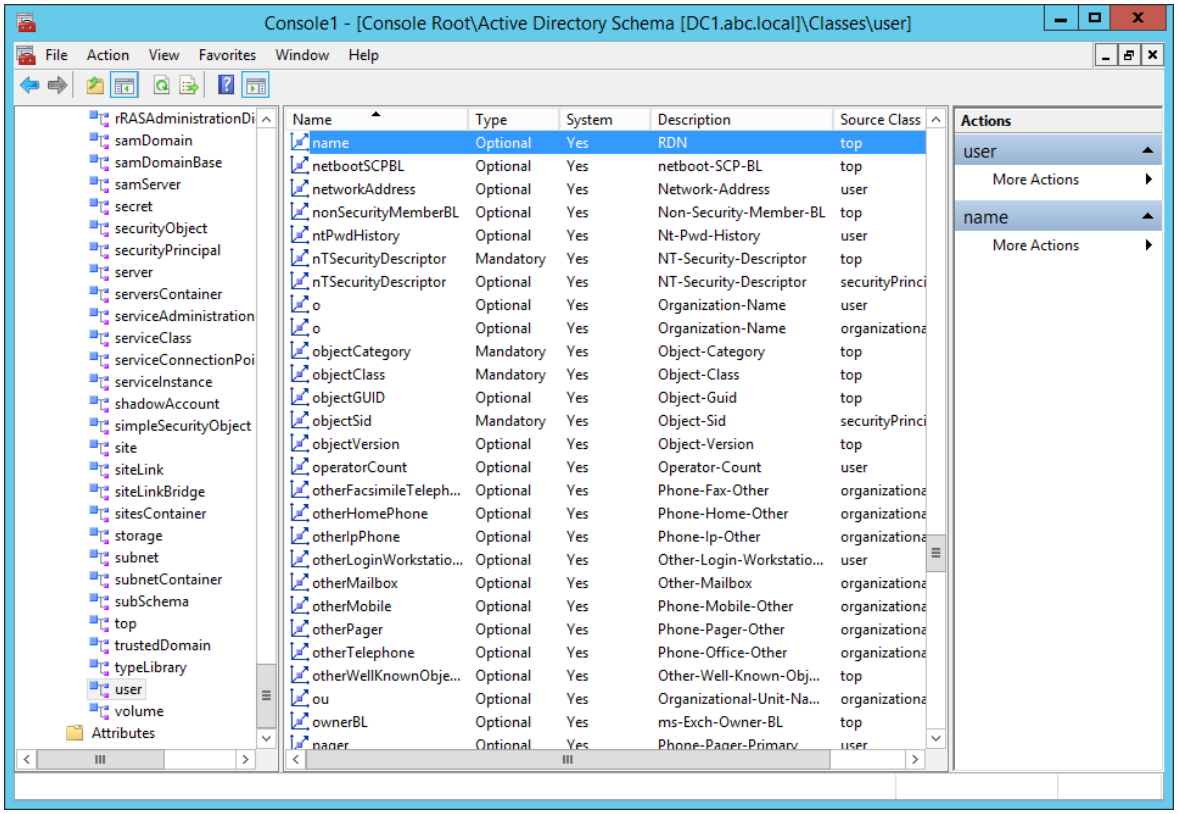
- Description : la description de la classe user
- Common Name (cn) : user, tout simplement le cn de la classe
- X.500 OID : identifiant unique au sein de LDAP

On voit également que la classe est active et que cette classe est affichée pour la création de nouveau objet. En décochant la case, il n'est plus possible de créer de nouveaux users via l'ADUC. Le second onglet montre les « possible superior » notamment organizationalUnit



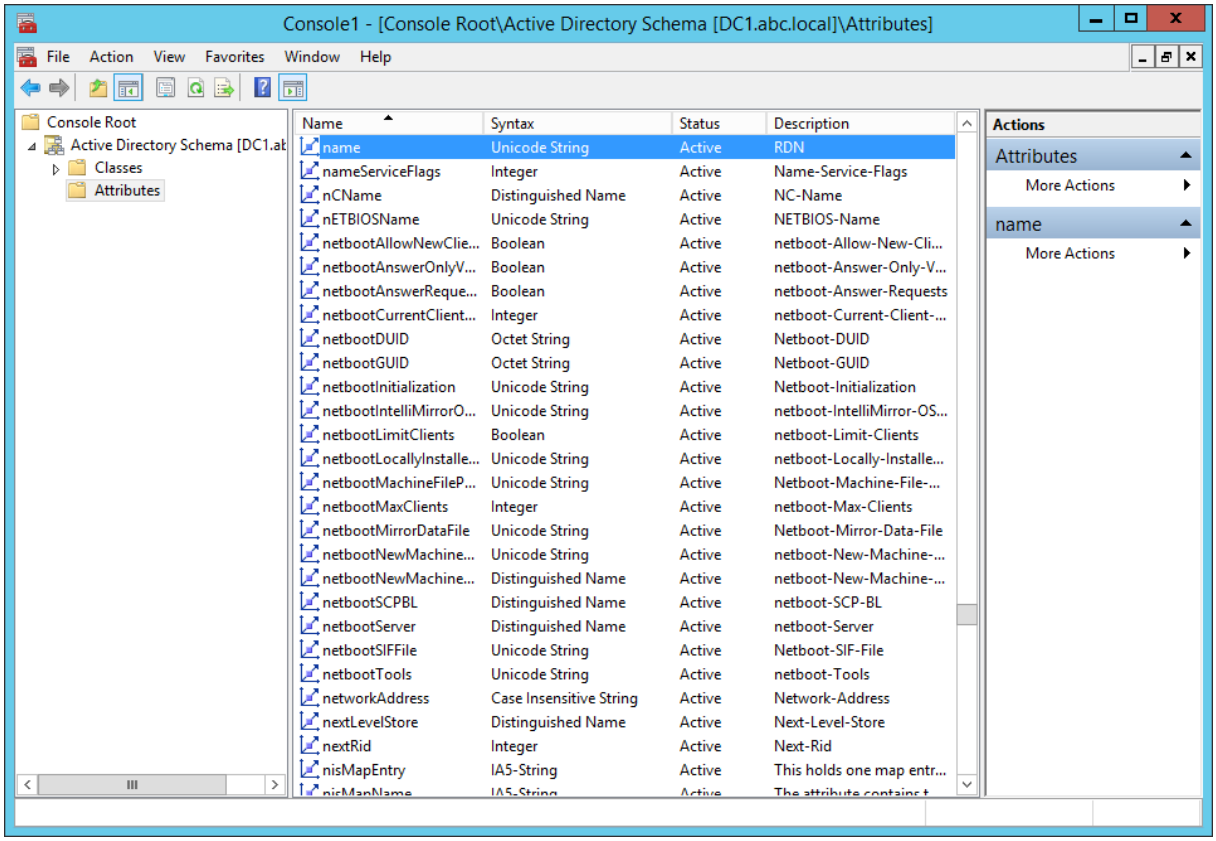
7.1.3 Les attributs d'une classe

En déployant à présent *Classes* dans le volet gauche, le volet central affiche à présent tous les attributs utilisé/utilisables de la classe sélectionnée. Dans le cas de *user*, on retrouve des attributs déjà évoqués dans le module précédent comme : *GivenName, Surname, SamAccountName, UserPrincipalName, Mail,* etc.



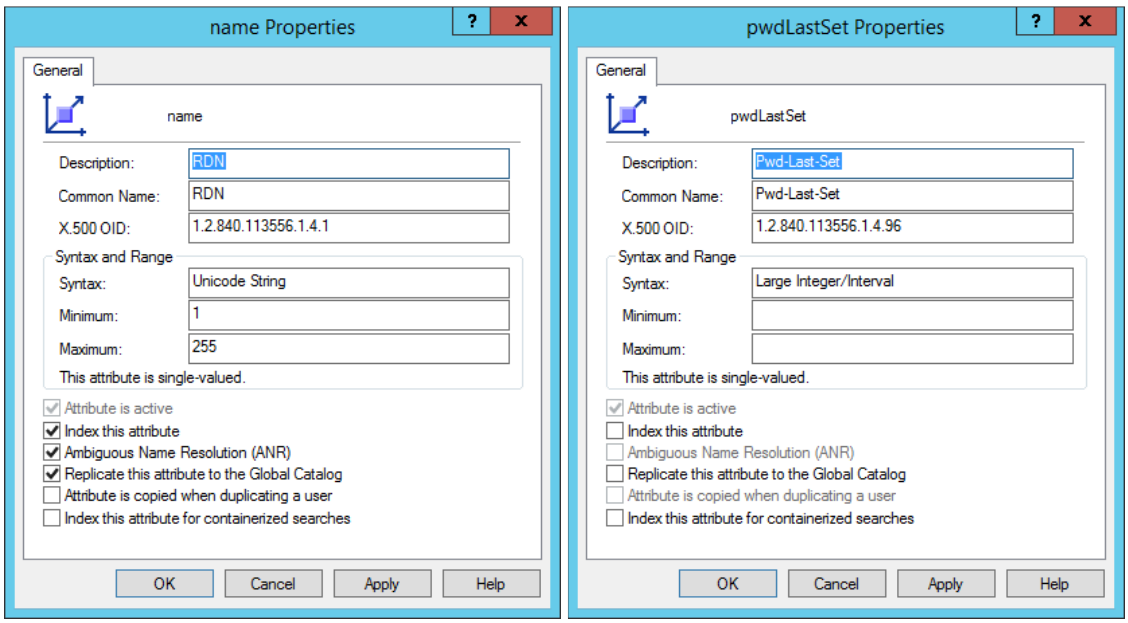
7.1.4 Les attributs

En sélectionnant *Attributes*, la liste complète des attributs disponibles dans l'AD s'affiche.



Examinons le cas de PwdLastSet et de Name :

- PwdLastSet : Il ne fait pas partie du catalogue global. Il n'est pas indexé.
- Name : Il fait partie du catalogue global. Il est indexé.



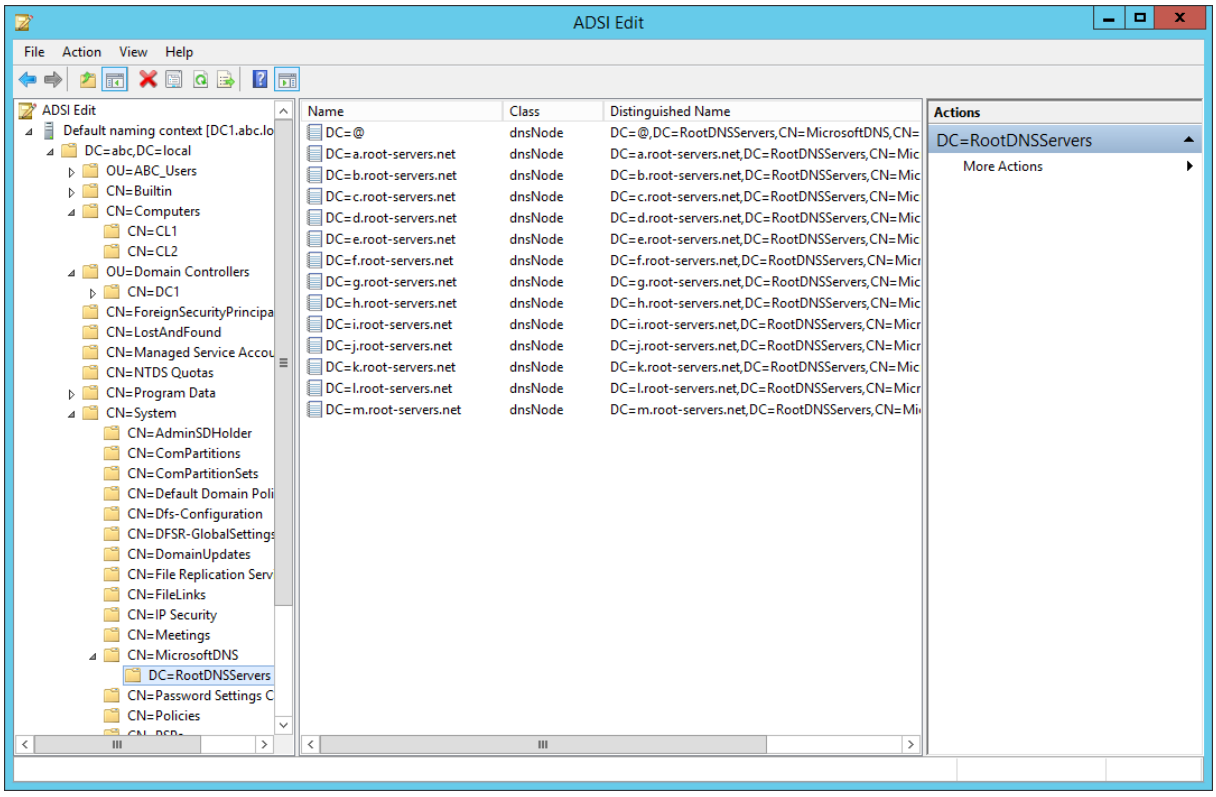
7.2 Domain Naming Master

Le Domain Naming Master est le seul DC à permettre l'ajout ou le retrait de domaines dans la forêt. L'ajout/suppression de domaine(s) engendre des changements au niveau des partitions dans NTDS.DIT, c'est le Domain Naming Master qui se charge des opérations. Certaines applications peuvent stocker des données dans l'AD qui dispose d'une partition prévue à cet effet. Quand le rôle DNS (un module lui est consacré) est installé, il stocke des informations dans le Naming Context.

Tant qu'il n'y a pas de modifications à faire au niveau du Naming Context, le Domain Naming Master peut ne pas être joignable sans impact sur le fonctionnement du domaine.

Le Domain Naming Master travaille sur LDAP://CN=Partitions, CN=Configuration, DC=<domain> (Partitions\Configuration naming context).

Vue du *Default naming context* via ADSI Edit :



7.3 RID master

Rappel : Les objets de l'AD doivent être uniques. Pour ce faire, les objets ont un DistinguishedName et un GUID (Globally Unique Identifier).

Lors de la création d'objets comme des utilisateurs, des groupes, des ordinateurs, etc. un SID (Security IDentifier) est aussi généré.

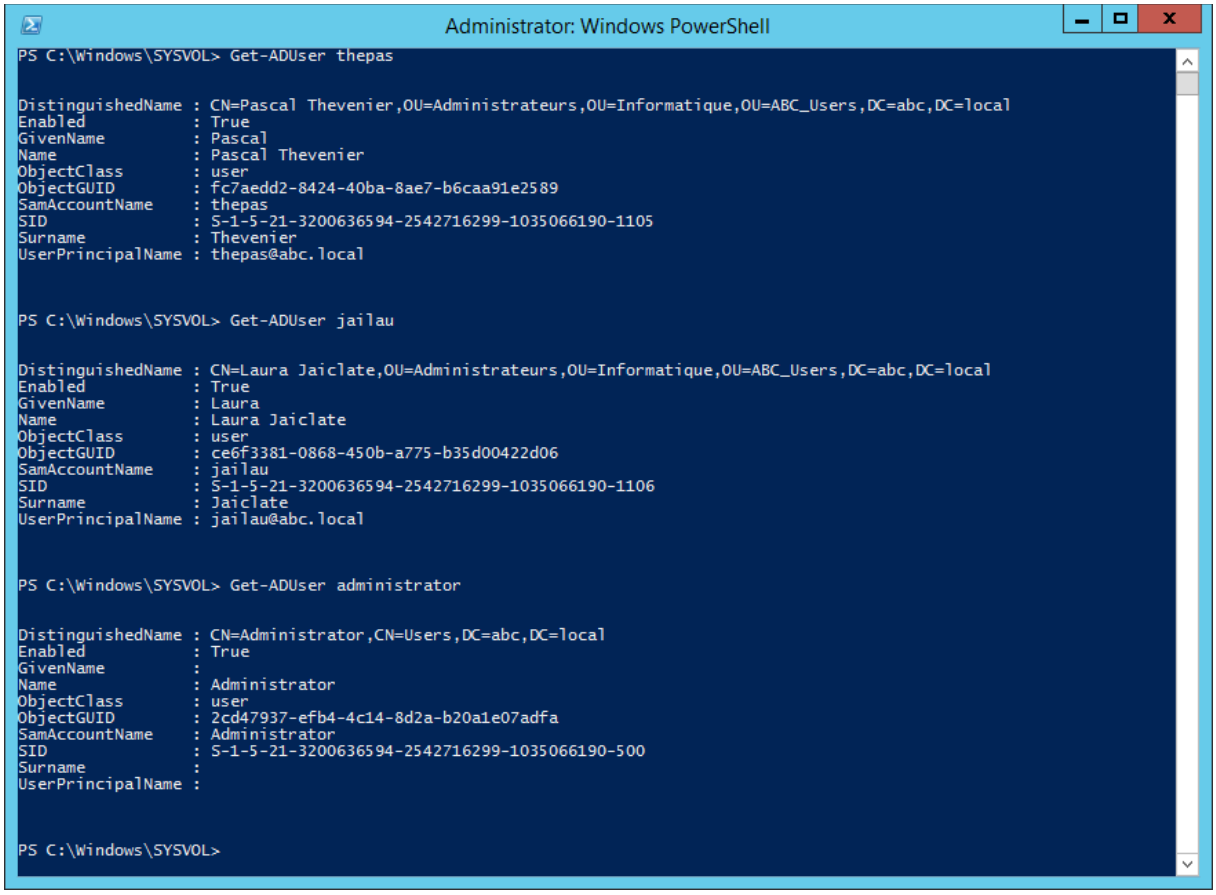
Le SID se compose de deux parties :

- Domain SID : commun à tous les objets du domaine.
- RID (Relative IDentifier) : unique pour chaque SID.

Exemple de SID : S-1-5-21-3200636594-2542716299-1035066190-1105

- Domain ID : S-1-5-21-3200636594-2542716299-1035066190
- RID : 1105

La capture suivante montre que les 3 utilisateurs ont bien le même Domain ID et un RID différent. Le compte Administrator a toujours 500 comme RID. La numérotation commence à 1000 pour les objets « non builtin ».



Le RID Master s'occupe de la gestion et de la distribution des RID dans le domaine ; il attribue une plage (un pool) de RID à chaque DC.

Si un DC a épuisé son quota de RID, il en demande un nouveau au RID Master. Tant que les DC ont des RID en disponibles, le RID Master n'est pas utile. Si un DC ne dispose plus de RID de réserver et que le RID Master n'est pas joignable, la création de nouveau objet n'est plus possible.

Le RID Master intervient également lors du déplacement d'un objet d'un domaine à un autre. C'est lui qui supprime l'objet dans le domaine de départ afin d'éviter la création d'un doublon.

Le nombre de RID par domaine est « limité à 1 million » (2^{30} = 1 073 741 824). Mais il ne faut pas perdre de vue qu'un pool alloué à un DC ne sera plus jamais disponible même si le DC est demote. Par défaut un DC demande des pools de 100 000 RID et fait une demande de 50 000 RID dès qu'il a consommé la moitié du pool.

7.4 PDC Emulator

Le PDC Emulator joue quatre rôles dans un domaine :

- Il assure la compatibilité avec les anciens systèmes Windows NT et clients.
- Il veille à la synchronisation horaire nécessaire au bon fonctionnement de Kerberos.
- Il gère le verrouillage des comptes et les changements de mot de passe.
- Il contrôle les modifications des stratégies de groupe (GPO) afin d'éviter les conflits.

7.5 Infrastructure Master

L'Infrastructure Master veille à la bonne gestion des liaisons inter domaines. Si dans le domaine A, on crée un groupe d'utilisateurs qui contient un utilisateur du domaine B (les deux domaines sont « trusted »), il faut être de l'identité de cet utilisateur et être en mesure de le manipuler correctement. C'est le rôle de l'Infrastructure Master.

L'Infrastructure Master sert dans des cas spécifiques en environnements multi domaines.

7.6 Trouver les serveurs FSMO

La commande `NetDom Query FSMO` affiche la liste des cinq serveurs ayant un rôle FSMO.

Pour les versions plus anciennes de Windows Server, il faut faire la recherche pour chaque rôle :

- Schema Master : `DSquery server –hasfsmo schema`
- Domain Naming Master : `DSquery server –hasfsmo name`
- RID Master : `DSquery server –hasfsmo rid`
- PDC Emulator : `DSquery server –hasfsmo PDC`
- Infrastructure Master : `DSquery server –hasfsmo infr`

8 Les sites

Un site est une combinaison de sous-réseaux IP reliés par une liaison fiable et rapide où se trouve au moins un DC. En général, un site a les mêmes limites qu'un réseau local. Les sites ne font pas partie de l'espace de nom d'Active Directory.

- Un site ne contient que des objets ordinateurs et des connexions.
- Un domaine peut s'étendre sur plusieurs sites.
- Un site peut contenir plusieurs domaines.

Les sites servent essentiellement à représenter une réalité physique où les vitesses de connexions seront encodées afin que les services de réplications opèrent au mieux.

9 Différentes façons de voir l'AD

Nous avons à présent vu tous les éléments importants liés à un environnement domanial utilisant les services Active Directory. Nous pouvons donc à présent facilement examiner l'ensemble sous les différents angles couramment utilisés dans la littérature Microsoft.

9.1 Vue logique

L'organisation des ressources dans AD se fait à travers une structure logique qui se veut le reflet du modèle organisationnel de votre environnement. Les domaines et sous domaines représentent par exemples la maison mère et des filiales, des départements, etc. Les OU peuvent représenter la structure hiérarchique de l'entreprise. Cette structure logique rend transparent pour les utilisateurs la structure physique du réseau : on ne voit pas les serveurs, les connexions, etc. La vue logique fait références aux forêts, arbres, domaines et unités organisationnelles.

La vue logiques est une vue de « l'immatériel »…

9.1.1 Forêt

Ensemble d'au moins une racine.

9.1.2 Arbre

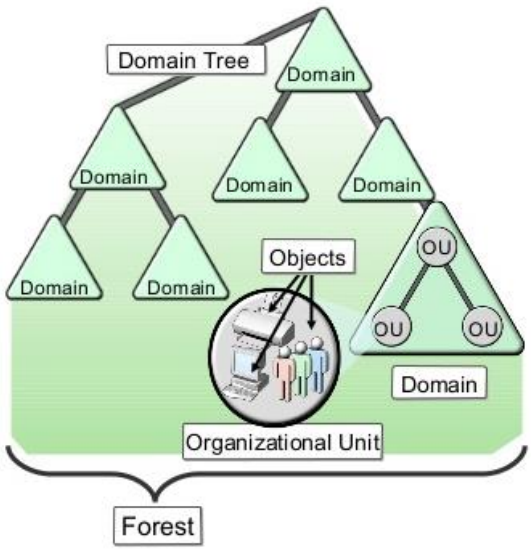
Racine avec éventuellement des branches.

9.1.3 Domaine

Limite administrative. A sa création, le domaine est une racine et une forêt. Brique de base.

9.1.4 OU

Container pour objets ou autres OU. Plus petit élément sur lequel il est possible d'attribuer des paramètres de stratégie de groupe ou déléguer une autorité administrative.



9.2 Vue physique

La vue physique est beaucoup plus concrète et fait référence à des objets biens réels : les sites, les liaisons entre sites et les contrôleurs de domaine. Elle illustre notamment une disposition géographique de la situation : le site A est à Arlon et le site B à Bruxelles ; ils sont reliés par une connexion 100 Mbps.

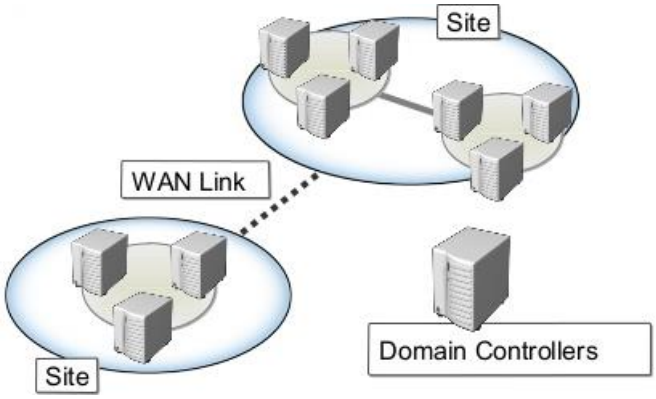
La vue physique montre tout ce qui peut être touché ou pris en main.

9.2.1 Domain controllers

Serveur qui stocke et réplique les données de l'AD (permet l'authentification des utilisateurs et applique les stratégies de groupes).

9.2.2 Sites

Ensemble de sous-réseaux reliés à haut débit.



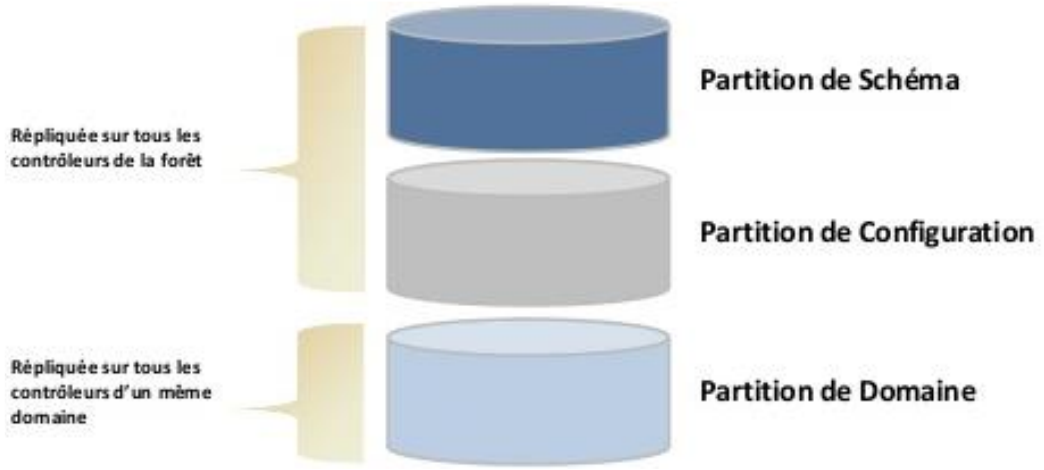
9.2.3 WAN links

Liens entre les sites. Ils servent à matérialiser dans l'AD les liaisons entre sites en tenant compte du coût (proportionnel aux performances).

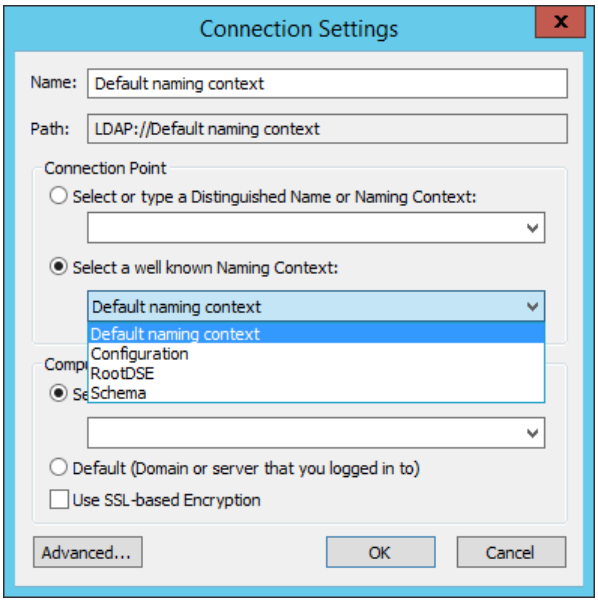
9.3 Vue partitions

Le fichier NTDS.DIT est agencé en naming contexts (contexte de nommage). Les naming contexts sont caractérisé par ce qu'ils contiennent ainsi que la façon dont ils sont répliqués. Il existe bien entendu une corrélation entre ces partitions, les rôles FSMO et la structure de l'AD.

- Schema : contient les classes d'objets et leurs attributs qui peuvent être contenus dans l'AD.
- Configuration : contient la structure logique de la forêt et la topologique physique.
- Domain : contient les objets du domaine (users, computers, groupes).



Ces partitions sont visibles en utilisant l'utilitaire ADSI Edit. Lors de la création d'une nouvelle connexion, l'application propose de se connecter à un « well know Naming context » :

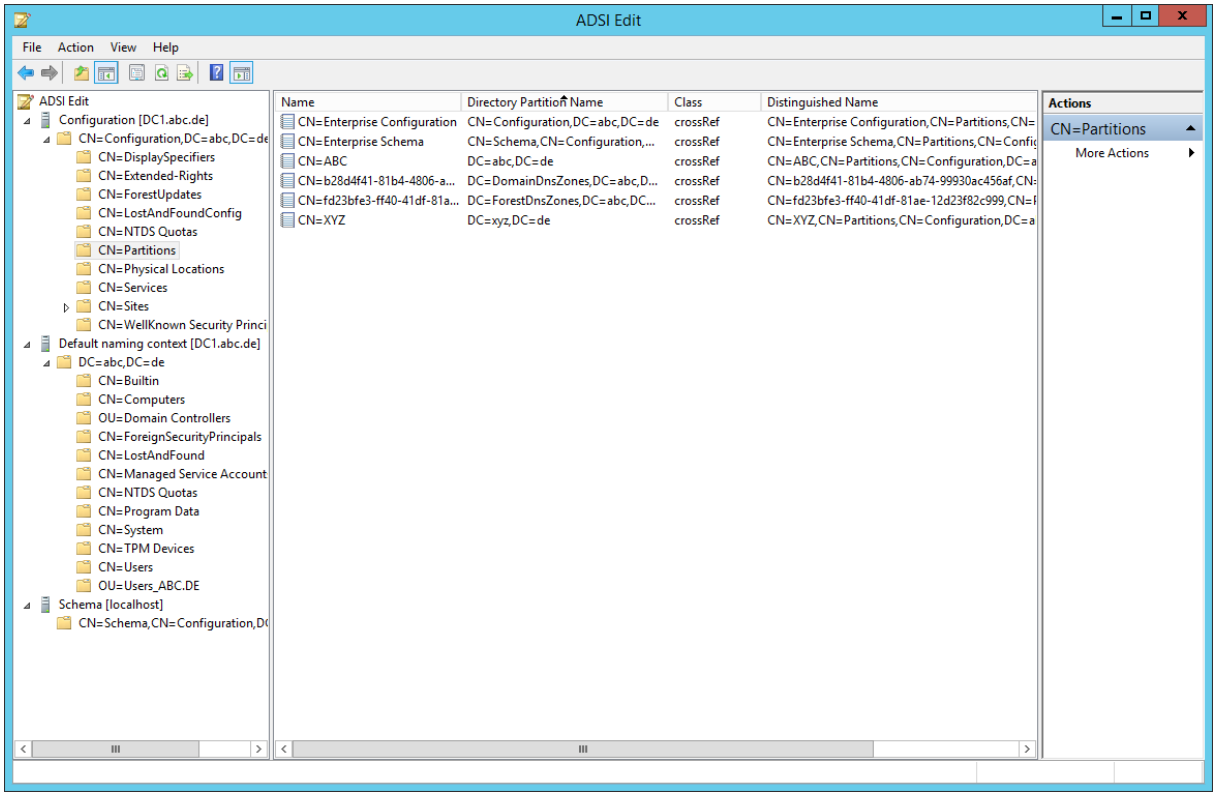


- Configuration
- Schema
- Default naming context (Domain)

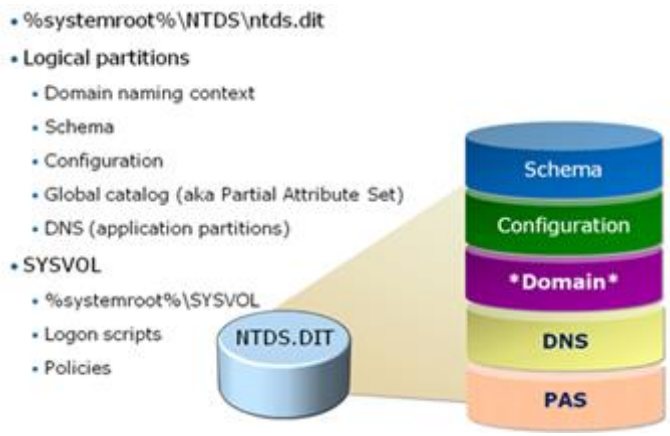
Pour bien comprendre l'agencement des partitions, il suffit de se connecter à la configuration et examiner les partitions telles quelles sont intégrées dans la base de données de l'Active Directory.

Comme le montre sans surprise la capture suivante, les trois partitions sont bien visibles :

- CN=Enterprise Configuration
- CN=Enterprise Schema
- CN=ABC (le domaine)



Les trois partitions « de base » sont présentes sur les contrôleurs de domaine mais elles sont souvent accompagnées d'autres partitions en fonctions des rôles installés sur le DC. Lors de la promotion d'un DS, le système propose d'installer les rôles DNS et GG.



Quand le DNS est intégré à l'AD, il stocke ses informations dans une partition appelée application. Cette partition application n'est pas réservée au seul DNS (comme pourrait le laisser penser l'illustration). D'autres applications comme Exchange vont stocker des informations dans cette partition.

Pour être précis, la partie DNS se compose d'une partie DNS Domain et d'une partie DNS Forest. Cette séparation est visible sur la capture d'ADSI Edit.

Un GG stocke également le PAS des autres domaines. Elles prennent place dans une partition appelée PAS ou GG.

Schema	**Réplication dans la forêt**
Configuration	**Réplication dans la forêt**

Domain	**Réplication dans le domaine**
Applications	**Réplication domaine ou forêt selon l'application**
DNS Forest	**Réplication dans la forêt**
DNS Domain	**Réplication dans le domaine**
Exchange	
Global Catalog (PAS)	**Réplication dans la forêt**
GG Domain a	
GG Domain b	
…	

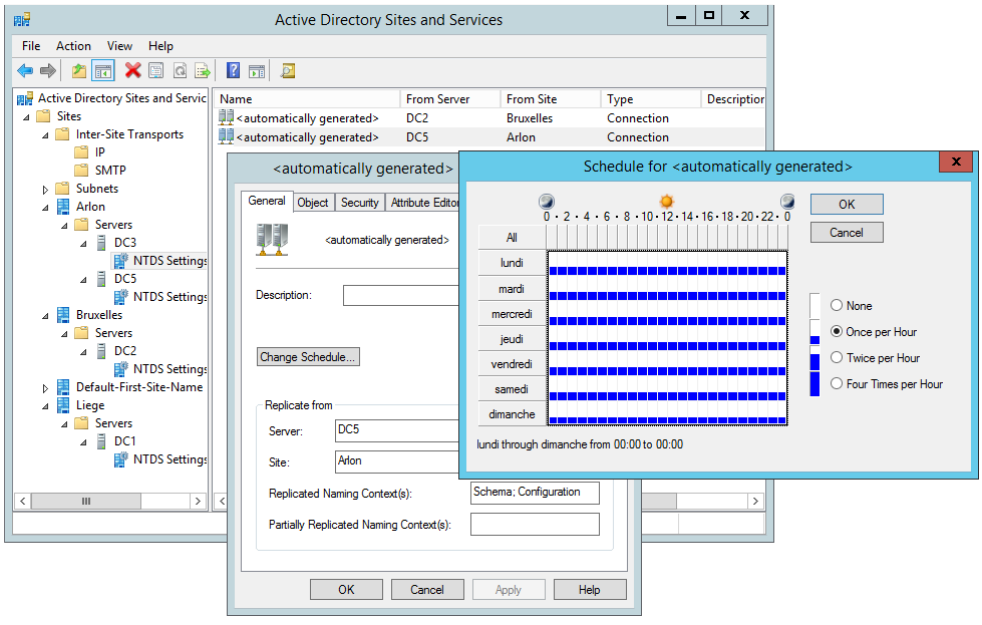
10 Réplication

Les contrôleurs de domaine répliquent la base de données Active Directory dans un but d'offrir de la redondance afin d'assurer une disponibilité maximale. Chaque DC contient donc un relplica de l'AD. Depuis l'examen de la vue partitions, nous savons même ce qui est répliqué. Il reste à savoir comment se fait cette réplication ou plus exactement comment se font les réplications dans un environnement multi maitres où des modifications de l'AD peuvent être apportées au même moment sur différents DC.

Dans les cas des OS du siècle dernier, le PDC (Primary Domain Controller) et le BDC (Backup Domain Controller) étaient les seul à disposer d'un accès en lecture/écriture sur l'AD. A présent, tous les DC accèdent en lecture/écriture sur l'AD (sauf les RODC).

Planification

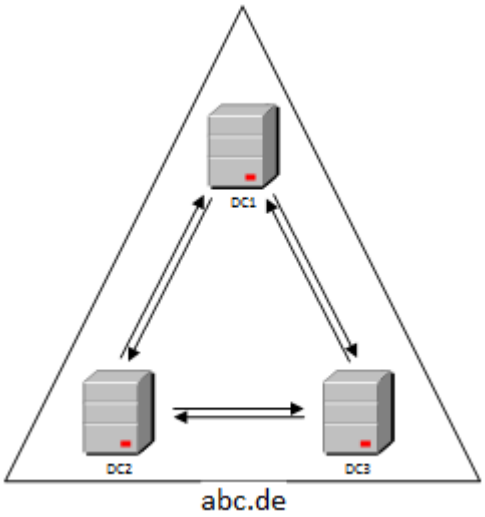
Dans un environnement mono domaine, les DC se concertent une fois par heure et une réplication se produit. Cette option est réglable dans Site and Services au niveau des propriétés d'une connexion généré automatiquement ainsi que dans les propriétés du NTDS Site Settings de Default-First-Site-Name.



Certaines actions au niveau de l'AD comme la désactivation d'un compte sur un DC engendrent directement une notification immédiate aux autres DC et une mise à jour. Il est effectivement primordial qu'un utilisateur dont le compte a été désactivé ne puisse immédiatement plus se connecter.

Topologie

Dès qu'un serveur est promu DC, il est automatiquement ajouté dans Default-First-Site-Name (sauf si des sites ont été configurés). La topologie de réplication est créée et gérée automatiquement par le KCC (Knowledge Constency Checker). Dans l'exemple, le KCC génère les connexions de manière à ce que chaque DC se réplique sur les deux autres.

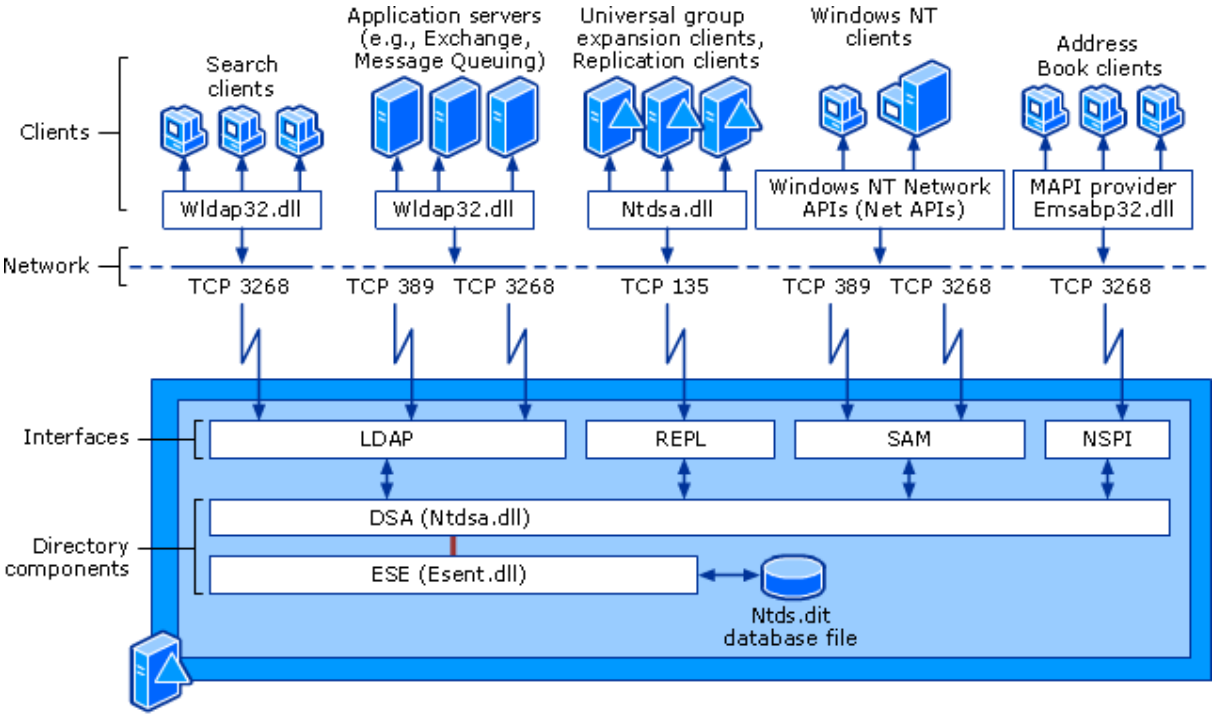


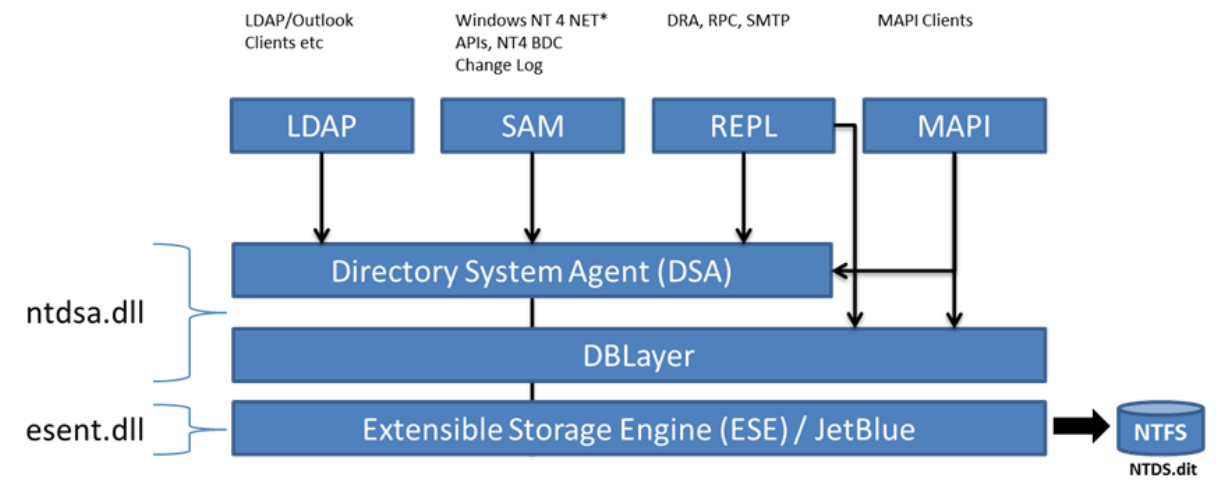
11 NTDS.DIT en détail.

L'AD est une base de données qui centralise les données en provenance de nombreuses sources ; les clients sur l'illustration. Elle évolue donc continuellement. L'AD doit également répondre à des demandes diverses. Si les données proviennent *in fine* toutes du réseau, en fonction du type de données et leur « provider », le cheminement varie (processus est similaire dans l'autres sens). Il passe par une des quatre interfaces :

- LDAP : interface standard principale d'accès l'AD en lecture et écriture. LDAP fonctionne directement sur TCP/IP (port 389 lecture/écriture, port 3268 pout le catalogue global).
- REPL : interface de réplication de l'AD entre les contrôleurs de domaines ainsi que du catalogue global.
- NSPI : Name Service Provider Interface utilisée pour l'accès à l'AD par les clients Messaging API (MAPI).
- SAM : interface propriétaire utilisée pour l'accès au DSA par Windows NT 4.

Le Directory System Agen (DSA) est l'intermédiaire entre les interfaces et le moteur de gestion de base de données ESE capable de lire et écrire dans le fichier NTDS.DIT.





Microsoft http://slideplayer.fr/slide/1650096/