MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI de TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du diplôme Master en Electronique

Option: Télécommunication et Réseau

Thème :

Migration d'une infrastructure réseau de Windows server 2003 ver windows server 2008 R2

Proposé et dirigé par :

Mr. OUALLOUCHE. F

Mr. KIBOUH.M

Présentée par :

M^{elle}. SADAOUI Kamilia

Année universitaire 2012/2013

Remerciements

Je remercie tout d'abord, DIEU tout puissant pour m'avoir donné la force et le courage pour terminer mes études et élaborer ce modeste travail.

Mes second remerciements vont à mes chères parents, que Dieu les protège et leurs procure une longue vie.

Je tiens à exprimer ma profonde gratitude et mes sincères remerciements à mon promoteur Mr. OUALLOUCHE.F et mon Co-promoteur Mr. KIBOUH.M pour tout le temps qu'ils m'ont consacré, leur directives précieuses, et pour la qualité de leur suivi durant toute la période de mon travail

Je tiens aussi à remercier vivement mon mari pour ces conseils et son encouragement pour finir ce travail.

Tous mes infinis remerciements vont à tous les enseignants qui ont collaboré à ma formation, pour le riche savoir qu'ils m'ont transmis avec rigueur et dévouement.

Mes sincères sentiments vont à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce projet. En particulier ma chère famille et mes amies.

Mon respect aux membres de jury, qui me feront l'honneur d'accepter et de juger ce modeste travail, et d'apporter leurs réflexions et leurs critiques scientifiques.

Dédicace

Je dédie avec ma profonde affection, ce travail.

A tous ceux qui me sont très chers,

- ✓ *A DIEU pour m'avoir protégé, béni et éclairé, je ne t'abandonnerai jamais,*
- ✓ *A ma très chère Mère qui m'a toujours prodigué de sages et précieux conseils et a mon cher Père qui a toujours fais en sorte a ce que j'ai le nécessaire pour ma réussite que DIEU vous protège*
- ✓ *A mon mari Hmimi qui ma soutenue et encourage pour finir ce travail et qui a crue en moi je pourrai jamais le remercier assez*
- ✓ *A mes frères Mohammed, Hocine et Nassim.*
- ✓ *A ma sœur Khadîdja et son mari Samir.*
- ✓ *A mon neveu Abdenour.*
- ✓ *A ma nièce Anaïs.*
- ✓ *A mes grands parents.*
- ✓ *A l'âme de ma grande mer.*
- ✓ *A tous mes cousines et cousins sans exception*
- ✓ *A tous mes oncles et tantes.*
- ✓ *A toute ma belle famille.*
- ✓ *A tous mes amies surtout Farida, Safia et Sabrina*
- ✓ *A tous ceux qui font partie de ma vie et qui sont chers (es)à mon cœur.*
- ✓ *A toute la promotion master ELN 2012/2013.*

Que dieu nous protège et nous préserve le bonheur et la santé.

Sommaire

Liste des figures

Introduction

Windows Server est aujourd'hui au cœur de l'informatique des entreprises. Déployé massivement dans les PME comme dans les grandes entreprises, Windows Server est le socle sur lequel s'appuie un grand nombre d'entreprises pour fournir à leurs utilisateurs une large palette de services d'infrastructure et de services applicatifs essentiels au bon fonctionnement du réseau.

Depuis 2010, Microsoft a basculé Windows Server 2003 et Windows Server 2003 R2 en mode extension de support. A partir de cette année, seule la fourniture de correctifs de sécurité est assurée, mais Microsoft ne produit plus de correctifs fonctionnels ou de correctifs de bogues. Or il est important de disposer de systèmes sous garantie afin de bénéficier de l'ensemble des services de support, tant d'un point de vue logiciel que matériel (ces versions de Windows tournent parfois sur des matériels pour lesquels le support est arrivé à échéance et pour lesquels même les pièces détachées ne sont plus fournies). Ces configurations à base de systèmes d'exploitation en voie d'obsolescence font peser un risque informatique sur l'entreprise et représentent un surcoût en frais de maintenance. La survie en production de ces vieilles versions est aussi un problème alors qu'arrive une nouvelle génération de serveurs basés sur de nouvelles architectures processeurs. Il est donc primordial pour les entreprises qui font encore fonctionner d'anciennes versions de Windows Server d'anticiper l'arrêt du support et de préparer la bascule vers une version plus moderne de Windows Server. Ces anciennes versions de Windows Server ne permettent pas de tirer partie des nouvelles capacités des serveurs modernes contrairement à Windows Server 2008 R2.

Dans ce contexte, l'utilisation de Windows Server 2008 R2 permettra pour les entreprises de profiter des avantages induits par les nouvelles technologies telles que la virtualisation (réduction du nombre de serveurs, économie de place, d'énergie), Direct Access (télétravail, connexion transparente et sécurisée des utilisateurs nomades), Branch Cache (optimisation des performances pour les sites distants). Tout en profitant d'un niveau de sécurité et de disponibilité inégalé pour l'infrastructure.

Pour continuer à bénéficier d'un support optimal, il est recommandé la migration vers Windows Server 2008 R2, qui permettra de continuer à profiter de l'étendue complète de services de support, tout en bénéficiant de considérables améliorations fonctionnelles comme le support de la virtualisation de serveurs, les nouvelles fonctions d'administration ou de virtualisation d'applications et de postes de travail, mais aussi de performances significativement en hausse.

Le travail décrit dans ce mémoire traite le problème de la migration d'un server équipé de Windows 2003 server vers Windows 2008 server. On a organisé notre mémoire en trois chapitres : Le premier consiste à définir l'Active Directory. Le deuxième a pour but de comparer les systèmes d'exploitation serveur et de définir la migration. Dans le dernier chapitre, nous allons migrer le server Windows 2003 vers le server 2008 R2.

Nous terminons notre mémoire par une conclusion ainsi que par des perspectives ouvertes.

Introduction

CHAPITRE I

Active Directory

1. Préambule

Active Directory est un annuaire d'entreprise qui existe depuis 1996 et est utilisable depuis Windows 2000 Server Edition sorti en 1999. Il s'agit donc d'un produit éprouvé par les années. Cet annuaire d'entreprise vient en remplacement des bases SAM (Security Account Manager) qui étaient exploitées avec NT4 et les groupes de travail.

Ces bases présentaient notamment des limitations d'administration. L'arrivée d'Active Directory a permis de passer des groupes de travail aux domaines Active Directory et ainsi de centraliser toute l'administration et la gestion des droits dans un annuaire de type LDAP. Tout logiciel utilisant LDAP sera capable de communiquer avec Active Directory : on peut, par exemple, gérer (partiellement) des postes Linux à partir d'un Active Directory.

2. Description d'un service d'annuaire

Un service d'annuaire est un service réseau qui identifie toutes les ressources d'un réseau et met ces informations à la disposition des utilisateurs ainsi que des applications. Les services d'annuaires sont importants, car ils fournissent un moyen cohérent de nommer, décrire, localiser, administrer et sécuriser les informations relatives à ces ressources et d'y accéder. Lorsqu'un utilisateur recherche un dossier partagé sur le réseau, le service d'annuaire identifie la ressource et fournit l'information à l'utilisateur.

2.1 Définition d'Active Directory

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'*Active Directory* est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. *Active Directory* répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées.

Active Directory stocke ses informations et paramètres dans une base de données centralisée. La taille d'une base Active Directory peut varier de quelques centaines d'objets

pour de petites installations à plusieurs millions d'objets pour des configurations volumineuses.

La sécurité est intégrée dans Active Directory à travers l'authentification de l'ouverture de session et le contrôle d'accès aux objets de l'annuaire. Avec une connexion réseau unique les administrateurs réseau peuvent gérer les données et l'organisation de l'annuaire à travers leur réseau, et les utilisateurs autorisés peuvent accéder aux ressources n'importe où sur le réseau. Une administration basée sur des stratégies facilite la gestion même du plus complexe des réseaux.

2.1.1 Les composants d'Active Directory

Il existe différents composants dans Active Directory. A partir de Windows 2008, des termes sont apparus pour les désigner.

- **ADDS :** Active Directory Domain Services. Il s'agit du composant principal qui va gérer les utilisateurs, ordinateurs, stratégies de groupe, etc.
- **ADCS:** Active Directory Certificate Services. Il s'agit du composant d'autorité de certification. Il va nous permettre de générer des certificats de sécurité pour nos utilisateurs et notre réseau.
- **ADFS:** Active Directory Federation Services. Il s'agit du composant permettant la fédération de services entre différents environnements Active Directory. Cela permet à une entreprise d'établir des relations de confiance avec des partenaires externes (fournisseurs, fabricants, etc.) afin de leur donner un accès à certains de nos services internes de manière contrôlée et sécurisée.
- **ADLDS:** Active Directory Lightweight Directory Services (anciennement ADAM). C'est ADDS mais allégé: seul l'annuaire est disponible. Cela est utile dans les cas où nous avons besoin d'un accès à des données de l'Active Directory sans avoir une autorisation de lecture totale dessus. C'est utilisé notamment dans la passerelle d'hygiène d'Exchange (Edge). ADLDS contiendra une copie partielle de notre Active Directory.
- **ADRMS:** Active Directory Rights Management Services. Ce composant permet de gérer les droits de manière pointue dans notre entreprise. Il ne s'agit pas des droits sur le fichier mais sur le contenu du fichier.

2.1.2 Les avantages d'Active Directory

Active Directory étend la fonctionnalité de base d'un service d'annuaire et fournit les avantages suivants :

✓ **Sécurité des informations**

La sécurité est entièrement intégrée dans Active Directory. Le contrôle d'accès peut être défini non seulement sur chaque objet de l'annuaire, mais aussi sur chaque propriété de chacun des objets. Active Directory fournit à la fois le magasin et l'étendue de l'application pour les stratégies de sécurité. Une stratégie de sécurité peut inclure des informations de compte, telles que des restrictions de mot de passe applicables sur l'ensemble du domaine ou des droits pour des ressources de domaine spécifiques. Les stratégies de sécurité sont mises en place par le biais des paramètres de Stratégie de groupe.

✓ **Administration basée sur les stratégies**

Le service de l'annuaire Active Directory comprend à la fois un magasin de données et une structure logique hiérarchique. Comme une structure logique, il fournit une hiérarchie des contextes pour l'application de la stratégie. En tant qu'annuaire, il stocke les stratégies (appelées objets Stratégie de groupe) affectées à un contexte précis. Un objet Stratégie de groupe représente un ensemble de règles commerciales contenant des paramètres qui, pour le contexte auquel l'objet est appliqué, peuvent déterminer come suivant

- L'accès aux objets de l'annuaire et aux ressources du domaine.
- Les ressources de domaine (telles que les applications) disponibles pour les utilisateurs.
- Le mode de configuration de ces ressources du domaine pour une utilisation.

Par exemple, un objet Stratégie de groupe peut définir les applications que les utilisateurs affichent sur leur écran lors d'une ouverture de session, le nombre d'utilisateurs pouvant se connecter à Microsoft SQL Server lors d'un démarrage sur un serveur et les documents ou services auxquels les utilisateurs peuvent accéder lorsqu'ils se déplacent vers d'autres services ou groupes. Les objets Stratégie de groupe nous permettant de gérer un petit nombre de stratégies au lieu de gérer un grand nombre d'utilisateurs et d'ordinateurs. Active Directory nous permet d'appliquer les paramètres Stratégie de groupe aux contextes adéquats, s'il s'agit de la totalité ou d'unités précises de notre organisation.

✓ **Extensibilité**

Active Directory est extensible, ce qui signifie que les administrateurs peuvent ajouter de nouvelles classes d'objets au schéma et de nouveaux attributs aux classes d'objets existantes. Par exemple, nous pouvons ajouter un attribut Autorisation d'achat à l'objet utilisateur, puis stocker la limite d'autorité d'achat de chaque utilisateur dans le compte de

l'utilisateur. Nous pouvons ajouter des objets et des attributs à l'annuaire en utilisant le schéma Active Directory ou en créant des scripts en fonction des interfaces ADSI ou des utilitaires de ligne de commande LDIFDE ou CSVDE.

- ✓ **Flexibilité**

Active Directory inclut un ou plusieurs domaines, chacun avec un ou plusieurs contrôleurs de domaine, qui permettent de faire évoluer l'annuaire en fonction des besoins de notre réseau. Nous pouvons combiner plusieurs domaines pour obtenir une arborescence de domaine et plusieurs arborescences de domaine pour obtenir une forêt. L'annuaire distribue ses informations sur le schéma et sur la configuration à tous les contrôleurs de domaine de l'annuaire. Ces informations sont stockées dans le contrôleur de domaine d'origine pour un domaine spécifique, puis elles sont répliquées sur tous les autres contrôleurs de domaine du domaine. Lorsque l'annuaire est configuré en tant que domaine unique, l'ajout de contrôleurs de domaine permet de faire évoluer l'annuaire sans la charge administrative liée aux domaines supplémentaires. L'ajout de domaines à l'annuaire nous permet de fractionner l'annuaire pour des contextes de stratégie différents et de faire évoluer l'annuaire afin d'accueillir un grand nombre de ressources et d'objets.

- ✓ **Réplication des informations**

La réplication garantit la disponibilité des informations, la tolérance de panne, l'équilibre de la charge et de meilleures performances pour l'annuaire. Active Directory utilise la réplication Multi-Master, qui nous permet de mettre à jour l'annuaire sur n'importe quel contrôleur de domaine, plutôt que sur un contrôleur principal de domaine unique. Le modèle Multi-Master offre l'avantage d'une meilleure tolérance de panne. En effet, lorsqu'il existe plusieurs contrôleurs de domaine, la réplication se poursuit même si l'un des contrôleurs de domaine est arrêté. Même si les utilisateurs ne s'en aperçoivent pas, grâce à la réplication Multi-Master, ils mettent à jour une seule copie de l'annuaire. Une fois que les informations de l'annuaire ont été créées ou modifiées sur un contrôleur de domaine, les nouvelles informations sont envoyées à tous les autres contrôleurs de domaine du domaine ; ainsi, leurs informations d'annuaire sont actualisées en permanence. Les contrôleurs de domaine nécessitent les dernières informations d'annuaire. Toutefois, pour pouvoir être efficaces, ils ne doivent effectuer les mises à jour que lorsque les informations de l'annuaire sont créées ou modifiées. Un échange arbitraire d'informations entre les contrôleurs de domaine pourrait saturer rapidement le réseau. Active Directory a été conçu pour répliquer uniquement des

informations d'annuaire modifiées. Avec la réplication Multi-Master, il existe toujours la possibilité que la même modification de l'annuaire soit effectuée sur plusieurs contrôleurs de domaine. Active Directory a également été conçu pour suivre et résoudre les modifications conflictuelles de l'annuaire. Les conflits sont automatiquement résolus dans presque tous les cas. Le déploiement de plusieurs contrôleurs de domaine dans un même domaine garantit la tolérance de panne et l'équilibre de la charge. Si un contrôleur de domaine ralentit, s'arrête ou tombe en panne, d'autres contrôleurs de domaine du même domaine peuvent garantir l'accès à l'annuaire, car ils contiennent exactement les mêmes données d'annuaire.

- ✓ **Intégration avec DNS**

Active Directory utilise le système de nom de domaine (DNS). DNS est un service standard Internet qui traduit les noms d'hôte facilement lisibles, par exemple monordinateur.microsoft.com, en adresses IP numériques. Ceci permet d'identifier et de se connecter aux processus en cours d'exécution sur les ordinateurs des réseaux TCP/IP. Les noms de domaine pour DNS sont basés sur la structure de nommage hiérarchique DNS, qui est une structure arborescente inversée : un domaine racine unique au-dessous duquel peuvent exister des domaines parents et des domaines enfants (branches et feuilles). Par exemple, un nom de domaine Windows 2000 tel que enfant.parent.microsoft.com identifie un domaine nommé « enfant », qui est un domaine enfant du domaine nommé « parent », qui est à son tour enfant du domaine racine microsoft.com. Chaque ordinateur d'un domaine DNS est identifié uniquement par son nom de domaine complet DNS. Le nom de domaine complet d'un ordinateur situé dans le domaine enfant.parent.microsoft.com serait nom_ordinateur.enfant.parent.microsoft.com

- ✓ **Interfonctionnement avec d'autres services d'annuaire**

Étant donné que Active Directory est basé sur des protocoles d'accès à l'annuaire standards, tels que les protocoles LDAP (Lightweight Directory Access Protocol) version 3 et NSPI (Name Service Provider Interface), il peut fonctionner simultanément avec d'autres services d'annuaire qui utilisent ces mêmes protocoles. LDAP est le protocole d'accès à l'annuaire utilisé pour demander et extraire des informations d'Active Directory. Comme il s'agit d'un protocole de service d'annuaire conforme aux normes industrielles, les programmes peuvent être développés en utilisant LDAP pour partager les informations d'Active Directory avec d'autres services d'annuaire qui prennent également en charge ce protocole. Le protocole

NSPI, utilisé par les clients Microsoft Exchange 4.0 et 5.x, est pris en charge par Active Directory pour garantir la compatibilité avec l'annuaire Exchange.

- ✓ **Souplesse des recherches**

Les utilisateurs et les administrateurs peuvent utiliser la commande ‹‹Rechercher›› du menu ‹‹Démarrer, Favoris réseau›› ou ‹‹utilisateurs et ordinateurs Active Directory›› pour rechercher rapidement un objet sur l'ensemble de réseau à l'aide des propriétés des objets. Par exemple, nous pouvons rechercher un utilisateur par le prénom, le nom, l'adresse de messagerie, l'emplacement du bureau ou toute autre propriété du compte d'utilisateur de cette personne. La recherche d'informations est optimisée par l'utilisation du catalogue global.

2.1.3. Fonctionnement d'Active Directory

Dans de grands réseaux, les ressources sont partagées par de nombreux utilisateurs et applications. Pour permettre aux utilisateurs et aux applications d'accéder à ces ressources et aux informations les concernant, une méthode cohérente est nécessaire pour nommer, décrire, localiser, accéder, gérer et sécuriser les informations concernant ces ressources. L'Active Directory remplit cette fonction. Active Directory est un référentiel d'informations structuré concernant les personnes et les ressources d'une organisation.

Active Directory dispose des fonctionnalités suivantes :

- ✓ **Accès pour les utilisateurs et les applications aux informations concernant des objets** : Ces informations sont stockées sous forme de valeurs d'attributs. On peut rechercher des objets selon leur classe d'objet, leurs attributs, leurs valeurs d'attributs et leur emplacement au sein de la structure Active Directory ou selon toute combinaison de ces valeurs.
- ✓ **Transparence des protocoles et de la topologie physique du réseau** : Un utilisateur sur un réseau peut accéder à toute ressource, une imprimante par exemple, sans savoir où celle-ci se trouve ou comment elle est connectée physiquement au réseau.
- ✓ **Possibilité de stockage d'un très grand nombre d'objets** : Comme il est organisé en partitions, Active Directory peut répondre aux besoins issus de la croissance d'une organisation. Par exemple, un annuaire peut ainsi passer d'un serveur unique contenant quelques centaines d'objets à des milliers de serveurs contenant des millions d'objets.
- ✓ **Possibilité d'exécution en tant que service indépendant du système d'exploitation** *:* AD/AM (Active Directory in Application Mode) permettant de résoudre certains scénarios de déploiement liés à des applications utilisant un annuaire. AD/AM s'exécute comme un service indépendant du système d'exploitation qui, en tant que tel, ne nécessite pas de déploiement sur un contrôleur de domaine. L'exécution en tant que service

indépendant du système d'exploitation signifie que plusieurs instances AD/AM peuvent s'exécuter simultanément sur un serveur unique, chaque instance étant configurable de manière indépendante.

3. Définition d'un schéma

Le schéma Active Directory contient les définitions de tous les objets, comme les utilisateurs, les ordinateurs et les imprimantes stockés dans Active Directory. Les contrôleurs de domaine exécutant Windows Server ne comportent qu'un seul schéma pour toute une forêt. Ainsi, tous les objets créés dans Active Directory se conforment aux mêmes règles.

Le schéma possède deux types de définitions : les classes d'objets et les attributs. Les classes d'objets comme utilisateur, ordinateur et imprimante décrivent les objets d'annuaire possibles qu'on peut créer. Chaque classe d'objet est un ensemble d'attributs.

Les attributs sont définis séparément des classes d'objets. Chaque attribut n'est défini qu'une seule fois et peut être utilisé dans plusieurs classes d'objets. Par exemple, l'attribut « Description » est utilisé dans de nombreuses classes d'objets, mais il n'est défini qu'une seule fois dans le schéma afin de préserver la cohérence.

4. Définition d'un catalogue global

Dans Active Directory, les ressources peuvent être partagées parmi des domaines et des forêts. Le catalogue global d'Active Directory permet de rechercher des ressources parmi des domaines et des forêts de manière transparente pour l'utilisateur. Par exemple, si on recherche toutes les imprimantes présentes dans une forêt, un serveur de catalogue global traite la requête dans le catalogue global, puis renvoie les résultats. En l'absence de serveur de catalogue global, cette requête exigerait une recherche dans chaque domaine de la forêt.

Le catalogue global est un référentiel d'informations qui contient un sous-ensemble des attributs de tous les objets d'Active Directory. Les membres du groupe Administrateurs du schéma peuvent modifier les attributs stockés dans le catalogue global, en fonction des impératifs d'une organisation. Le catalogue global contient :

- les attributs les plus fréquemment utilisés dans les requêtes, comme les nom et prénom d'un utilisateur, et son nom d'ouverture de session ;
- les informations requises pour déterminer l'emplacement de tout objet dans l'annuaire;
- un sous-ensemble d'attributs par défaut pour chaque type d'objet ;
- les autorisations d'accès pour chaque objet et attribut stocké dans le catalogue global.

Si on recherche un objet pour lequel on ne possède pas les autorisations de visualisation

requises, cet objet n'apparaîtra pas dans les résultats de la recherche. Les autorisations d'accès garantissent que les utilisateurs ne puissent trouver que les objets pour lesquels ils possèdent un droit d'accès.

Un serveur de catalogue global est un contrôleur de domaine qui traite efficacement les requêtes intraforêts dans le catalogue global. Le premier contrôleur de domaine qu'on crée dans Active Directory devient automatiquement un serveur de catalogue global. On peut configurer des serveurs de catalogue global supplémentaires pour équilibrer le trafic lié aux authentifications de connexion et aux requêtes.

Le catalogue global permet aux utilisateurs d'exécuter deux fonctions importantes :

- trouver les informations Active Directory en tout point de la forêt, indépendamment de l'emplacement des données ;
- utiliser les informations d'appartenance au groupe universel pour se connecter au réseau.

5. Structure logique d'Active Directory

Active Directory offre un stockage sécurisé pour les informations concernant les objets dans sa structure logique hiérarchique. Les *objets* Active Directory représentent des utilisateurs et des ressources, tels que des ordinateurs et des imprimantes. Certains objets en contiennent d'autres.

La structure logique d'Active Directory inclut les composants suivants :

5.1. Les objets

Il s'agit des composants les plus élémentaires de la structure logique. Les **classes** d'objets sont des modèles pour les types d'objets qu'on peut créer dans Active Directory. Chaque classe d'objet est définie par une liste d'attributs, qui définit les valeurs possibles qu'on peut associer à un objet. Chaque objet possède une combinaison unique de valeurs d'attributs.

5.2. Les unités d'organisation (OU, Organizational Unit)

Les unités d'organisation sont les conteneurs du service d'annuaire Active Directory qu'on utilise pour placer des utilisateurs, des groupes, des ordinateurs et d'autres unités d'organisation. On utilise ces objets conteneurs pour organiser d'autres objets de telle manière qu'ils prennent en compte nos objectifs administratifs. La disposition de ces objets par unité d'organisation simplifie la recherche et la gestion des objets. On peut également déléguer l'autorité de gestion d'une unité d'organisation. Les unités d'organisation peuvent être imbriquées les unes dans les autres, ce qui simplifie d'autant la gestion d'objets.

5.3. Les domaines

Unités fonctionnelles centrales dans la structure logique d'Active Directory, les domaines sont un ensemble d'objets définis administrativement qui partagent une base de données d'annuaire commune, des stratégies de sécurité et des relations d'approbation avec d'autres domaines. Les domaines disposent des trois fonctions suivantes :

• Une limite d'administration pour objets

• Une méthode de gestion de la sécurité pour les ressources partagées

• Une unité de réplication pour les objets

5.4. Les arborescences de domaines

Les domaines regroupés en structures hiérarchiques sont appelés arborescences de domaines. Lorsqu'on ajoute un second domaine à une arborescence, il devient *enfant* du domaine racine de l'arborescence. Le domaine auquel un domaine enfant est attaché est appelé *domaine parent*. Un domaine enfant peut à son tour avoir son propre domaine enfant. Le nom d'un domaine enfant est associé à celui de son domaine parent pour former son nom DNS (Domain Name System) unique, par exemple corp.nwtraders.msft. De cette manière, une arborescence a un **espace de noms contigu.**

5.5. Les forêts

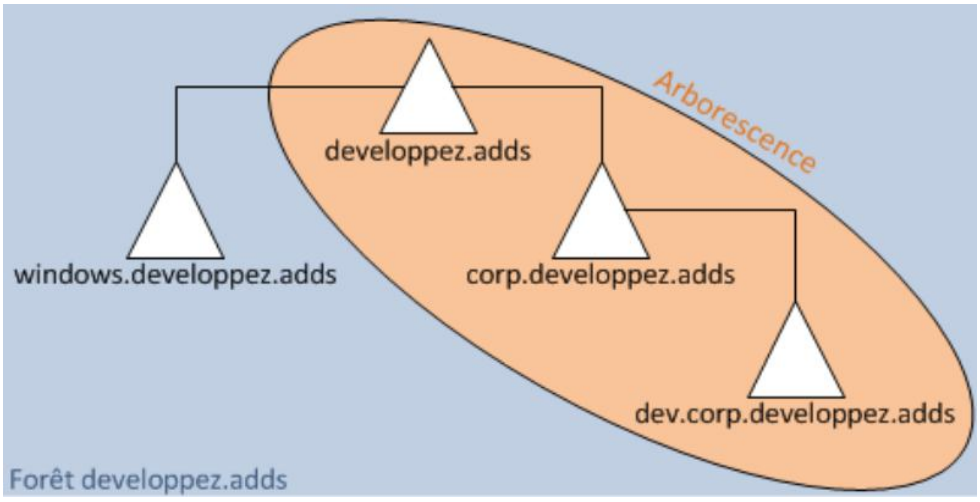


Fig I.1. Foret et arborescence

Une forêt est une instance complète d'Active Directory. Elle consiste en une ou plusieurs arborescences. Dans une arborescence unique à deux niveaux, qui est recommandée pour la plupart des organisations, tous les domaines enfants sont des enfants du domaine racine de la forêt afin de former une arborescence contiguë. Le premier domaine de la forêt est appelé le **domaine racine de la forêt**. Le nom de ce domaine fait référence à la forêt, par exemple nwtraders.msft. Par défaut, les informations dans Active Directory ne sont partagées

qu'à l'intérieur de la forêt. Ainsi, la forêt est une limite de sécurité pour les informations contenues dans l'instance d'Active Directory.

6. Structure physique d'Active Directory

Contrairement à la structure logique, qui modélise des exigences administratives, la structure physique d'Active Directory optimise le trafic réseau en déterminant où et quand se produit un trafic de connexions et de réplications. Pour optimiser l'utilisation par Active Directory de la bande passante du réseau, on doit en comprendre la structure physique. Les éléments de la structure physique d'Active Directory sont :

6.1. Les contrôleurs de domaine

Chaque contrôleur de domaine exécute des fonctions de stockage et de réplication. Un contrôleur de domaine ne peut gérer qu'un seul domaine. Pour assurer une disponibilité permanente d'Active Directory, chaque domaine doit disposer de plusieurs contrôleurs de domaine.

6.2. Les sites Active Directory

Ces sites sont des groupes d'ordinateurs connectés par des liaisons rapides. Lorsqu'on crée des sites, les contrôleurs de domaine au sein d'un même site communiquent fréquemment. Ces communications réduisent le délai de *latence de réplication* à l'intérieur du site ; autrement dit, le temps requis pour qu'une modification effectuée sur un contrôleur de domaine soit répliquée sur d'autres contrôleurs de domaine. On peut donc créer des sites pour optimiser l'utilisation de la bande passante entre des contrôleurs de domaines situés à des emplacements différents. Dans Active Directory, les sites facilitent la définition de la structure physique d'un réseau. Un ensemble de plages d'adresses de sous-réseaux TCP/IP définissent un site, qui à son tour définit un groupe de contrôleurs de domaine partageant les mêmes débits et coûts. Les sites sont composés d'objets serveurs, qui contiennent eux-mêmes les objets de connexion autorisant la réplication.

7. Comptes d'utilisateurs, de groupes et d'ordinateurs

7.1. Types de comptes

On peut créer trois types de comptes dans Active Directory : comptes d'utilisateurs, de groupes et d'ordinateurs. Les comptes d'utilisateurs et d'ordinateurs Active Directory représentent une entité physique, telle qu'un ordinateur ou une personne. On peut également utiliser les comptes d'utilisateurs comme comptes de services dédiés pour certaines applications.

a. Comptes d'utilisateurs

Un compte d'utilisateur est un objet stocké dans Active Directory qui permet une ouverture de session unique, autrement dit un utilisateur entre son mot de passe une seule fois lors de l'ouverture de session sur une station de travail pour obtenir un accès authentifié aux ressources réseau.

Il existe trois types de comptes d'utilisateurs, chacun ayant une fonction spécifique :

- ✓ Un compte d'utilisateur local : permet à un utilisateur d'ouvrir une session sur un ordinateur spécifique pour accéder aux ressources sur cet ordinateur.
- ✓ Un compte d'utilisateur de domaine : permet à un utilisateur de se connecter au domaine pour accéder aux ressources réseau, ou à un ordinateur individuel pour accéder aux ressources sur cet ordinateur.
- ✓ Un compte d'utilisateur intégré **:** permet à un utilisateur d'effectuer des tâches d'administration ou d'accéder temporairement aux ressources réseau.

b. Comptes d'ordinateurs

À l'image des comptes d'utilisateurs, les comptes d'ordinateurs permettent d'authentifier et d'auditer l'accès d'un ordinateur aux ressources réseau et du domaine. Chaque compte d'ordinateur doit être unique.

c. Comptes de groupes

Est un ensemble d'utilisateurs, d'ordinateurs ou de groupes. On peut utiliser des groupes pour gérer efficacement l'accès aux ressources du domaine, et ainsi simplifier l'administration. Lorsqu'on utilise des groupes, on affecte en une fois des autorisations pour des ressources partagées, telles que des dossiers et des imprimantes, à des utilisateurs individuels.

7.2. Types de groupes

Il existe deux types de groupes dans Active Directory, les groupes de distribution et les groupes de sécurité. Tous deux possèdent un attribut d'étendue, qui détermine qui peut être membre du groupe et à quel endroit on peut utiliser ce groupe dans un réseau. On peut convertir à tout moment un groupe de sécurité en un groupe de distribution et inversement, mais uniquement si le niveau fonctionnel de domaine est défini sur Windows 2000 natif ou ultérieur.

a. Groupes de distribution

On peut utiliser des groupes de distribution uniquement avec des applications de messagerie, telles que Microsoft Exchange, pour envoyer des messages à un ensemble

d'utilisateurs. La *sécurité* n'est pas activée sur les groupes de distribution, ce qui signifie qu'ils ne peuvent pas être répertoriés dans des listes de contrôle d'accès discrétionnaire (DACL, *Discretionary Access Control List*

b. Groupes de sécurité

On utilise des groupes de sécurité pour affecter des droits et des autorisations aux groupes d'utilisateurs et d'ordinateurs. Les droits déterminent les fonctions que les membres d'un groupe de sécurité peuvent effectuer dans un domaine ou une forêt. Les autorisations déterminent quelles ressources sont accessibles à un membre d'un groupe sur le réseau. Une méthode d'utilisation efficace des groupes de sécurité consiste à utiliser *l'imbrication*, c'est à dire, ajouter un groupe à un autre groupe. Le groupe imbriqué hérite des autorisations du groupe dont il est membre, ce qui simplifie l'affectation en une fois des autorisations à plusieurs groupes, et réduit le trafic que peut engendrer la réplication de l'appartenance à un groupe. Dans un domaine en mode mixte, on ne peut pas imbriquer des groupes possédant la même étendue de groupe.

Les groupes de distribution et de sécurité prennent en charge l'une des trois étendues de groupe suivantes : locale de domaine, globale ou universelle. Le niveau fonctionnel de domaine détermine le type de groupe qu'on peut créer. En mode Windows 2000 mixte, on ne peut pas créer de groupes de sécurité universels.

8. Définition des partitions d'annuaire

La base de données Active Directory est divisée de manière logique en plusieurs partitions : d'annuaire, du schéma, de la configuration, du domaine et d'application. Chaque partition est une unité de réplication et possède sa propre topologie de réplication. La réplication est exécutée entre les réplicas des partitions d'annuaire. Tous les contrôleurs de domaine de la même forêt ont au moins deux partitions d'annuaire en commun : celles du schéma et de la configuration. De plus, tous les contrôleurs de domaine partagent une partition de domaine commune.

8.1. Partition de schéma

Chaque forêt possède une seule partition de schéma. Cette partition de schéma est stockée dans tous les contrôleurs de domaine de la même forêt. Elle contient les définitions de tous les objets et attributs créés dans l'annuaire, ainsi que les règles qui permettent de les créer et de les manipuler. Les données du schéma sont répliquées dans tous les contrôleurs de domaine de la forêt. C'est pourquoi les objets doivent être conformes aux définitions d'objet et d'attribut du schéma.

8.2. Partition de configuration

Chaque forêt possède une seule partition de configuration. Stockée dans tous les contrôleurs de domaine de la même forêt, la partition de configuration contient les données sur la structure Active Directory de l'ensemble de la forêt, dont les domaines et les sites existants, les contrôleurs de domaine existants dans chaque forêt et les services disponibles. Les données de la configuration sont répliquées dans tous les contrôleurs de domaine de la forêt.

8.3. Partition de domaine

Chaque forêt peut comporter plusieurs partitions de domaine. Les partitions de domaine sont stockées dans chaque contrôleur de domaine d'un domaine donné.

Une partition de domaine contient les données sur tous les objets propres au domaine et créés dans ce domaine, dont les utilisateurs, les groupes, les ordinateurs et les unités d'organisation. La partition de domaine est répliquée dans tous les contrôleurs de domaine de ce domaine. Tous les objets de chaque partition de domaine d'une forêt sont stockés dans le catalogue global avec un seul sous-ensemble de leurs valeurs d'attribut.

8.4. Partition d'applications

Les partitions d'applications stockent les données sur les applications dans Active Directory. Chaque application détermine comment elle stocke, classe et utilise ses propres données. À la différence d'une partition de domaine, une partition d'applications ne peut pas stocker les principaux objets de sécurité, tels que les comptes d'utilisateurs. De plus, les données contenues dans une partition d'applications ne sont pas stockées dans le catalogue global.

Comme exemple de partition d'applications, si on utilise un système DNS qui est intégré à Active Directory, on a deux partitions d'applications pour les zones DNS : ForestDNSZones et DomainDNSZones.

- ForestDNSZones fait partie d'une forêt. Tous les contrôleurs de domaine et les serveurs DNS d'une forêt reçoivent un réplica de cette partition. Une partition d'applications d'une forêt entière stocke les données de la zone de la forêt.
- DomainDNSZones est unique pour chaque domaine. Tous les contrôleurs de domaine qui sont des serveurs DNS dans ce domaine reçoivent un réplica de cette partition. Les partitions d'applications stockent la zone DNS du domaine dans la DomainDNSZones <*nom_domaine*>.

9. Définition de la topologie de réplication

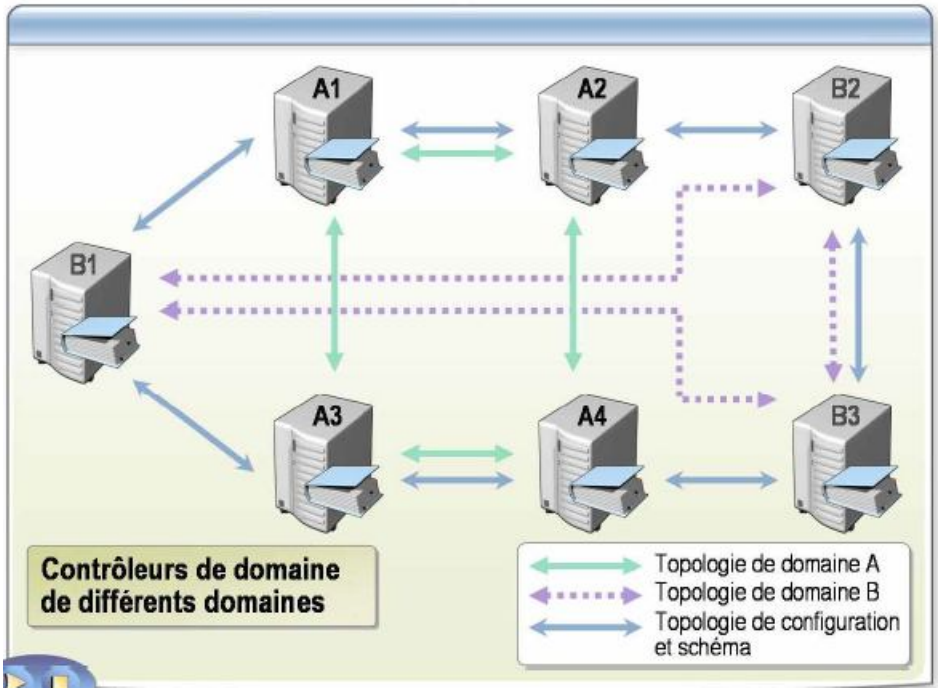


Fig .I.2 Réplication dans l'Active directory

La topologie de réplication est l'itinéraire suivi par les données de la réplication à travers un réseau. La réplication se produit entre deux contrôleurs de domaine à la fois. Avec le temps, la réplication synchronise les données dans Active Directory pour toute une forêt de contrôleurs de domaine. Pour créer une topologie de réplication, Active Directory doit déterminer quels contrôleurs de domaine répliquent les données avec les autres contrôleurs de domaine.

9.1. Réplication de partitions

Active Directory crée une topologie de réplication basée sur les données stockées dans Active Directory. La topologie de réplication peut différer pour les partitions de schéma, de configuration, de domaines et d'applications.

Tous les contrôleurs de domaine d'une même forêt partageant les partitions de schéma et de configuration, Active Directory réplique ces partitions de schéma et de configuration sur tous les contrôleurs de domaine. Les contrôleurs de domaine du même domaine répliquent également la partition du domaine.

De plus, les contrôleurs de domaine qui hébergent une partition d'applications répliquent la partition d'applications. Pour optimiser le trafic de la réplication, un contrôleur de domaine peut avoir plusieurs partenaires de réplication pour différentes partitions. Active

Directory réplique les mises à jour d'annuaire dans tous les contrôleurs de domaine qui contiennent la partition mise à jour dans la forêt.

9.2. Objets de connexion

Les contrôleurs de domaine qui sont liés par des objets de connexion sont appelés partenaires de réplication. Les liens qui relient les partenaires de réplication sont appelés objets de connexion. Les objets de connexion sont créés dans chaque contrôleur de domaine et pointent vers un autre contrôleur de domaine pour une source de données de réplication. Les objets de connexion représentent un chemin de réplication à sens unique entre deux objets serveur.

La topologie de réplication par défaut d'un site est un anneau bidirectionnel, composé de deux objets de connexion unidirectionnels complémentaires entre deux contrôleurs de domaine adjacents. Cette topologie améliore la tolérance de pannes lorsque l'un des contrôleurs de domaine est déconnecté.

Si nécessaire, Active Directory crée des objets de connexion supplémentaires pour limiter statistiquement à un maximum de trois le nombre de tronçons empruntés pour répliquer une mise à jour provenant de tous les réplicas d'une partition donnée dans un anneau.

9.3. Catalogue global et réplication de partitions

Un serveur de catalogue global est un contrôleur de domaine qui stocke deux partitions pour toute la forêt. Les partitions de schéma et de configuration. Plus une copie en lecture/écriture de la partition de son propre domaine et un réplica partiel de toutes les autres partitions de domaine dans la forêt. Ces réplicas partiels contiennent un sous-ensemble en lecture seule des données de chaque partition de domaine.

Lorsque nous ajoutons un nouveau domaine à une forêt, la partition de configuration stocke les données sur ce nouveau domaine. Active Directory réplique la partition de configuration sur tous les contrôleurs de domaine, y compris les serveurs de catalogue global, lors d'une réplication normale dans toute la forêt. Chaque serveur de catalogue global devient un réplica partiel du nouveau domaine en contactant un contrôleur de domaine pour ce domaine et en obtenant les données du réplica partiel. La partition de configuration fournit également aux contrôleurs de domaine la liste de tous les serveurs de catalogue global de la forêt.

Les serveurs de catalogue global enregistrent les enregistrements DNS spéciaux dans la zone DNS qui correspond au domaine racine de forêt. Ces enregistrements, écrits uniquement dans

la zone DNS racine de la forêt, aident les clients et les serveurs à localiser les serveurs de catalogue global à travers la forêt.

10. DHCP

Un serveur DHCP a pour but d'affecter des adresses IP à des ordinateurs. Plus concrètement, lorsqu'un ordinateur dépourvu d'adresse IPv4 est configuré pour en obtenir une automatiquement, cet ordinateur diffuse au démarrage des paquets de découverte DHCP sur le réseau. Ces messages de découverte DHCP sont alors transmet via les câbles, concentrateurs et commutateurs voisins

La négociation entre un client et DHCP s'effectue en quatre étapes (voir la figure suivante)

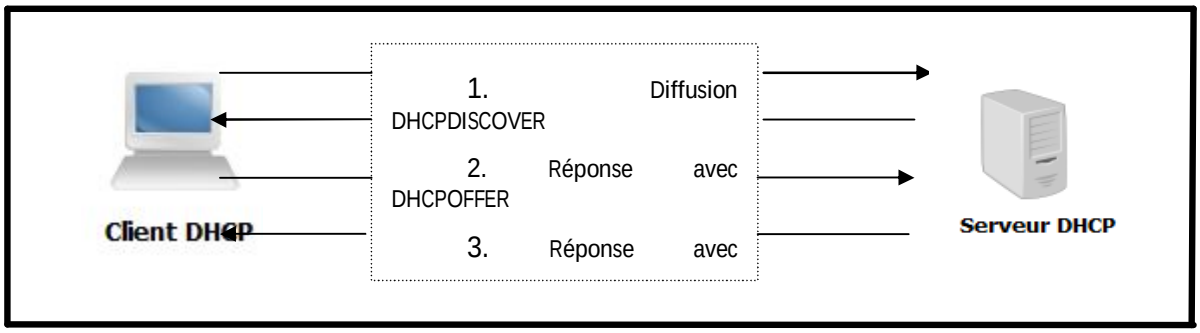


Fig I.3. Processus d'affectation d'adresse DHCP

- ✓ **Diffusion DHCP**

Lors de cette première étape, le client diffuse un message de découverte DHCP (DHCPDiscover) sur le réseau local pour identifier tous serveur DHCP disponible. Cette diffusion s'arrête au routeur le plus proche, à moins que ce dernier ne soit configuré pour la transmettre.

- ✓ **Réponse avec DHCP Offer**

Un serveur DHCP est connecté au réseau local et peut offrir au client DHCP une affectation d'adresse IP, il envoie un message mono diffusion d'offre DHCP (DHCP offer) au client DHCP

- ✓ **Réponse avec DHCP Request**

A la troisième étape de la négociation DHCP, le client répond au message DHCP Offer et demande l'adresse IP qui figure. Il peut toutefois demander l'adresse IP qui lui était précédemment affecté.

- ✓ **Confirmation avec DHCP ACK**

Si l'adresse IP demandée par le client DHCP est encore disponible, le serveur DHCP répond par un message d'accord DHCP A

11. RODC

Il s'agit d'une nouveauté apparue avec Windows 2008. RODC signifie Read-Only Domain Controller ou Contrôleur de domaine en lecture seule. Il s'agit d'un contrôleur de domaine spécialement prévu pour les architectures de type Branch Office ou réseau d'agences donc en architecture multi sites. Un contrôleur de domaine en lecture seule sera installé dans les agences : les seules modifications possibles seront faites par le biais du contrôleur de domaine responsable de la réplication. Ce contrôleur de domaine responsable de la réplication est nommé tête de pont.

L'avantage principal du RODC est qu'il ne nécessite quasiment aucune maintenance et est plus sécurisé qu'un contrôleur de domaine classique puisqu'il est en lecture seule. Ce type de contrôleur de domaine est parfait pour les agences où il n'y a pas d'administrateur système. Cependant, cela est problématique pour les applications ayant besoin d'un accès en écriture sur Active Directory comme Exchange par exemple.

12. Le répertoire SYSVOL

Sysvol est un répertoire présent sur tous les contrôleurs de domaine Active Directory. Il stocke entre autres tous les scripts utilisateurs ainsi que les objets de stratégie de groupe. Le contenu de ce répertoire est répliqué sur tous les contrôleurs de domaine de votre domaine. C’est le service NTFRS (Service de réplication de fichiers) qui s’occupe de la réplication de ce répertoire.

Sysvol contient deux partages créés automatiquement par le système :

* SYSVOL : ce partage est créé automatiquement par le système lorsque l’on démarre le service NTFRS (Service de réplication de fichiers)
* Netlogon : ce partage est créé automatiquement par le système lorsque l’on démarre le service NETLOGON (Ouverture de session réseau).

13. Les rôles FSMO

FSMO signifie Flexible Single Master Opération, nous y retrouvons 5 rôles au total:

FSMO	Emplacement	Rôle
Maître d'attribution des noms de domaine	Unique au sein d'une forêt	Inscription de domaines dans la forêt
Contrôleur de schéma	Unique au sein d'une forêt	Gère la modification du schéma Active Directory
Maître RID	Unique au sein d'un domaine	Distribue des plages RID pour les SIDs
Maître d'infrastructure	Unique au sein d'un domaine	Gère le déplacement des objets
Emulateur CPD	Unique au sein d'un domaine	Garantie une compatibilité avec les anciens systèmes

Tableau I.1. Les rôles FSMO.

13.1. Maître d'attribution des noms de domaine

Le maître d'opération est unique dans une forêt, il se charge de contrôler l'ajout ou la suppression de domaines dans la forêt. Il est le seul contrôleur de domaine capable d'ajouter un nouveau domaine. Si jamais ce serveur se retrouve injoignable alors il vous sera impossible d'ajouter ou de supprimer un domaine.

13.2. Contrôleur de schéma

Le contrôleur de schéma intervient lors d'une mise à jour, d'une modification d'un objet de l'Active Directory. Il est le seul contrôleur de domaine apte à modifier le schéma Active Directory. C'est donc pour cela qu'il est conseillé de ne mettre qu'un seul contrôleur de schéma, afin d'éviter les conflits de mise à jour simultanée du schéma.

Le contrôleur de schéma rempli 4 fonctions au sein d'une forêt Active Directory

-Il contrôle les mises à jour apportées au schéma.

-Il contient la liste des classes d'objets et des attributs utilisés pour la création d'objet dans Active Directory.

-Il réplique les mises à jour apportées au schéma sur tous les autres contrôleurs de domaine de la forêt via la partition de schéma.

-Il autorise uniquement les administrateurs du schéma à modifier le schéma

13.3. Maitre RID

Le contrôleur de domaine possédant le rôle de maître RID, ou maître des identificateurs relatifs se charge d'allouer des blocs d'identificateurs relatifs à chaque contrôleur de domaine du domaine. Nous retrouvons sur chaque contrôleur de domaine un pool RID unique à attribuer aux nouveaux objets créés. Lorsque le contrôleur épuise son pool RID, il fait une demande au contrôleur qui est maître RID afin que celui-ci lui alloue une nouvelle plage d'identificateurs. Si le maître RID est injoignable et que le pool est épuisé sur un contrôleur, alors il sera impossible de créer d'objet sur ce serveur contrôleur en question.

13.4 Maître d'infrastructure

Active Directory utilise des objets appelés « objets fantômes », afin de référencer les utilisateurs de domaines différents. Ces objets ne peuvent être observés par aucuns outils d'exploration LDAP. Ils sont identifiés par le nom unique, le SID, le GUID.

Lorsque l'on ajoute un membre d'un domaine différent dans un groupe, le contrôleur de domaine local qui contient le groupe crée cet objet fantôme pour l'utilisateur étranger.

Si le nom de cet utilisateur est modifié, ou bien supprimer, l'objet fantôme doit être mis à jour ou bien supprimé du groupe sur tous les contrôleurs de domaine du domaine contenant cette référence. C'est le rôle du maître d'infrastructure.

13.5 Emulateur CPD

Lors de l'installation d'un nouveau domaine, le premier contrôleur de domaine endosse le rôle d'émulateur PDC (Primary Domain Controller). Ce rôle est particulièrement important au bon fonctionnement de chaque domaine de la forêt.

Il ne peut exister qu'un seul émulateur PDC au sein d'un domaine.

Le maître émulateur PDC assure 4 fonctions au sein d'un domaine Active Directory :

-Il permet la compatibilité avec des contrôleurs de domaine du type Windows NT et réplique les mises à jour à destination des contrôleurs secondaire de domaine NT (*Backup DomainController*).

-La gestion du verrouillage des comptes utilisateurs et du changement des mots de passe.

-Les mécanismes de synchronisation horaire sur tous les contrôleurs de domaine du domaine

-Il est utilisé pour réaliser les modifications des stratégies de groupe du domaine (*Groupe Policy Object*) afin d'interdire toute possibilité d'écrasement et de conflit.

14. Kerberos

14.1 Définition de Kerberos

kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs. Créé au Massachusetts Institute of Technology, il porte le nom grec de Cerbère, gardien des Enfers (Κέρβερος). Kerberos a d'abord été mis en œuvre sur des systèmes Unix.

14.2. Fonctionnement

Dans un réseau simple utilisant Kerberos, on distingue plusieurs entités :

- le client (C), a sa propre clé secrète K_C
- le serveur (S), dispose aussi d'une clé secrète K_S
- le service d'émission de tickets (TGS pour *Ticket-Granting Service*), a une clé secrète K_{TGS} et connaît la clé secrète K_S du serveur
- le centre de distribution de clés (KDC pour *Key Distribution Center*), connaît les clés secrètes K_C et K_{TGS}

Le client C veut accéder à un service proposé par le serveur S.

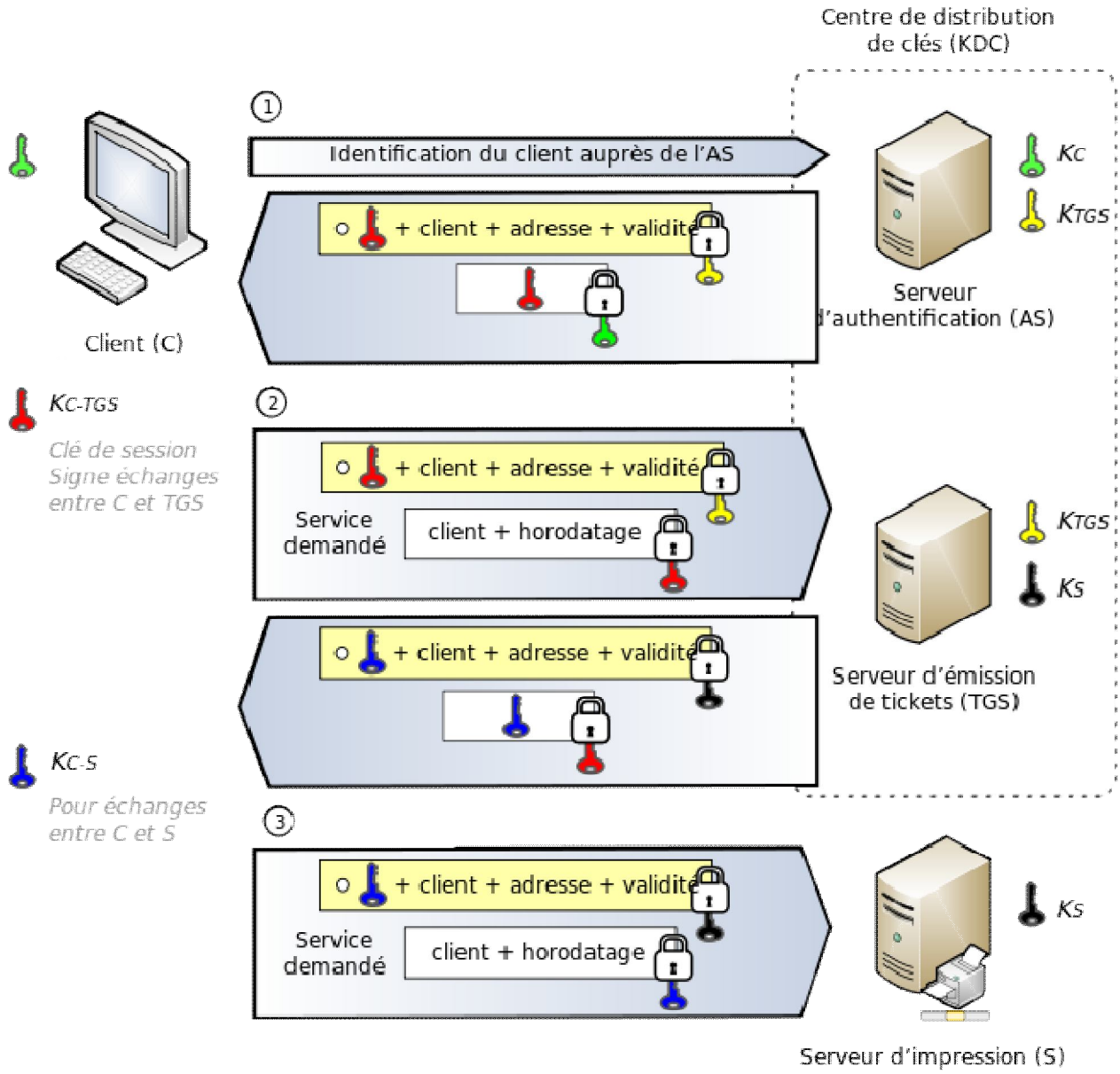


Fig.I.4. Les différentes étapes de fonctionnement de Kerberos.

La première étape pour le client consiste à s'identifier auprès du centre de distribution de clé (KDC). Le client a une clé secrète K_C, celle-ci est également connue par le serveur de distribution. Le client envoie son nom au serveur de distribution et lui indique le TGS qui l'intéresse. Après vérification sur l'identité du client (cette partie dépend des implémentations, certains serveurs utilisent des mots de passe à usage unique), le serveur de distribution lui envoie alors un ticket T_{TGS}. Ce ticket autorise le client à faire des requêtes auprès du TGS.

Ce ticket T_{TGS} est chiffré par le serveur de distribution avec la clé du TGS (K_{TGS}). Il contient notamment des informations sur le client mais également la clé utilisée pour établir la communication entre le client et le TGS. Cette clé de session, nous la noterons $K_{C,TGS}$. Le

client reçoit également cette clé de session $K_{C,TGS}$, elle a toutefois été chiffrée avec la clé secrète K_C du client.

À ce stade, le client possède un ticket T_{TGS} (qu'il ne peut pas déchiffrer) et une clé $K_{C,TGS}$

La deuxième étape est l'envoi par le client d'une demande de ticket auprès du TGS. Cette requête contient un identifiant (des informations sur le client ainsi que la date d'émission) chiffré avec la clé de session $K_{C,TGS}$ (qui est trouvée par le client en déchiffrant les informations reçues depuis le serveur de distribution avec sa clé secrète). Le client envoie aussi le ticket qui lui avait été transmis par le serveur de distribution.

Le TGS reçoit alors son ticket et il peut le déchiffrer avec sa clé secrète K_{TGS}. Il récupère le contenu du ticket (la clé de session) et peut ainsi déchiffrer l'identifiant que lui a envoyé le client et vérifier l'authenticité des requêtes. Le TGS peut alors émettre un ticket d'accès au serveur. Ce ticket est chiffré grâce à la clé secrète du serveur K_S. Le TGS envoie aussi ce ticket chiffré avec la clé secrète du serveur K_S et la clé de session $K_{C,S}$ chiffrée à l'aide de la clé $K_{C,TGS}$ au client pour les communications entre le serveur final et le client.

La troisième étape est le dialogue entre le client et le serveur. Le client reçoit le ticket pour accéder au serveur ainsi que l'information chiffrée contenant la clé de session entre lui et le serveur. Il déchiffre cette dernière grâce à la clé $K_{C,TGS}$. Il génère un nouvel identifiant qu'il chiffre avec $K_{C,S}$ et qu'il envoie au serveur accompagné du ticket.

Le serveur vérifie que le ticket est valide (il le déchiffre avec sa clé secrète K_S) et autorise l'accès au service si tout est correct.

14.3. Sécurité

Une fois qu'un client s'est identifié, celui-ci obtient un ticket (généralement, un fichier texte - mais son contenu peut aussi être stocké dans une zone de mémoire sécurisée). Le ticket joue le rôle d'une carte d'identité à péremption assez courte, huit heures généralement. Si nécessaire, celui-ci peut être annulé prématurément. Sous les systèmes Kerberos comme celui du MIT, ou de Heimdal, cette procédure est généralement appelée via la commande « *kdestroy* ».

La sécurité de Kerberos repose sur la sécurité des différentes machines qu'il utilise. Une attaque sur le serveur de clés serait dramatique car elle pourrait permettre à l'attaquant de s'emparer des clés privées des clients et donc de se faire passer pour eux. Un autre problème qui pourrait survenir sur la machine du client est le vol des tickets. Ils pourraient être utilisés

par une tierce personne pour accéder aux services offerts par les serveurs (si la clé entre le client et le serveur est connue).

L'expiration du ticket permet de limiter les problèmes liés au vol des tickets. De plus, un ticket peut contenir l'adresse IP du client et le ticket n'est alors valable que s'il est employé depuis cette IP (ce champ est toutefois optionnel dans Kerberos, qui peut tout à fait être utilisé sur un réseau attribuant dynamiquement les IP au travers de DHCP). Une attaque sur les identifiants échouera car Kerberos leur ajoute un élément. Cela évite les attaques par renvoi d'identifiants qui auraient été interceptés. Les serveurs conservent l'historique des communications précédentes et peuvent facilement détecter un envoi frauduleux.

L'avantage de Kerberos est de limiter le nombre d'identifiants et de pouvoir travailler sur un réseau non-sécurisé. Les identifications sont uniquement nécessaires pour l'obtention de nouveaux tickets d'accès au TGS.

Actuellement, deux implémentations de Kerberos version 5 existent pour OpenLDAP :

- MIT krb5
- Heimdal

15. Le protocole LDAP

Les ordinateurs clients utilisent le protocole LDAP pour rechercher et modifier des objets dans une base de données Active Directory. Le protocole LDAP est un sous-ensemble de la norme ISO X.500 relative aux services d'annuaire. Il utilise les informations portant sur la structure d'un annuaire pour trouver des objets individuels possédant chacun un nom unique.

Le protocole LDAP utilise un nom représentant un objet Active Directory par une série de composants concernant la structure logique. Cette représentation, appelée nom unique de l'objet, identifie le domaine dans lequel se trouve l'objet ainsi que le chemin complet permettant d'accéder à celui-ci. Un nom de ce type ne peut être qu'unique dans une forêt Active Directory.

Le nom unique relatif d'un objet identifie l'objet de manière unique dans son conteneur. Deux objets situés dans un même conteneur ne peuvent porter le même nom. Le nom unique relatif est toujours le premier composant du nom unique, mais il n'est pas toujours un nom usuel.

15. Conclusion

Dans ce chapitre nous avons vu c'est quoi l'Active Directory, son rôle et sa structure physique, ses avantages, ses composants, les contrôleurs de domaines, les différents types de comptes et de groupes, sa topologie et ses protocole

Active Directory est intégré dans le système Windows server pour cela une étude détaillée est présentée dans le chapitre suivant sur ces systèmes.

1. Préambule :

Dans ce chapitre nous allons définir le serveur en citant les types, en suite présenter et comparer les systèmes d'exploitation Windows puis on passera à la définition de la migration tout en donnant ces méthodes, les avantages et les inconvénients de chacune d'elles. Enfin, nous donnons les raisons de migrer les contrôleurs de domaine vers Windows server 2008 et vers Windows server 2008 R2.

2. Serveur

2.1 Définition d'un serveur

Le serveur est considéré comme le centre d'un réseau. C'est le cerveau du réseau.

Il est composé des mêmes sous-ensembles qu'un PC standard. Mais ces sous-ensembles sont beaucoup mieux optimisés:

- Il contient plus de mémoire vive
- Son contrôleur de disques est de très bonne qualité
- Disques durs de très grande capacité
- Microprocesseur(s) de dernière génération
- Capacités de gestion de réseau

2.2 Types de serveurs

Il existe 3 types de serveurs.

- **Serveur de fichier :** S'occupe de la gestion des fichiers. Il faut pour cela un très bon sous-système disque (contrôleur et disques), au moins 32 MB de RAM et une carte réseau très performante.

- **Serveur d'application :** Il contient les applications que les utilisateurs du réseau peuvent utiliser. Tous les traitements des logiciels se fait sur le serveur donc la rapidité du m P et la quantité de RAM (au moins 64MB) sont primordiaux.

- **Serveur d'impression :** C'est lui qui gère les queues d'impression. Ce type de serveur est souvent couplé avec un serveur de fichiers ou un serveur d'applications car il ne demande pas un sous-système très performant.

3. Les systèmes d'exploitation Windows

3.1. Le noyau de système d'exploitation :

Un noyau de système d'exploitation, ou simplement noyau, ou *kernel* (de l'anglais), est une des parties fondamentales de certains systèmes d'exploitation. Il gère les ressources de l'ordinateur et permet aux différents composants — matériels et logiciels — de communiquer entre eux.

En tant que partie du système d'exploitation, le noyau fournit des mécanismes d'abstraction du matériel, notamment de la mémoire, du (ou des) processeur(s), et des échanges d'informations entre logiciels et périphériques matériels. Le noyau autorise aussi diverses abstractions logicielles et facilite la communication entre les processus.

Le noyau d'un système d'exploitation est lui-même un logiciel, mais ne peut cependant utiliser tous les mécanismes d'abstraction qu'il fournit aux autres logiciels. Son rôle central impose par ailleurs des performances élevées. Cela fait du noyau la partie la plus critique d'un système d'exploitation et rend sa conception et sa programmation particulièrement délicates.

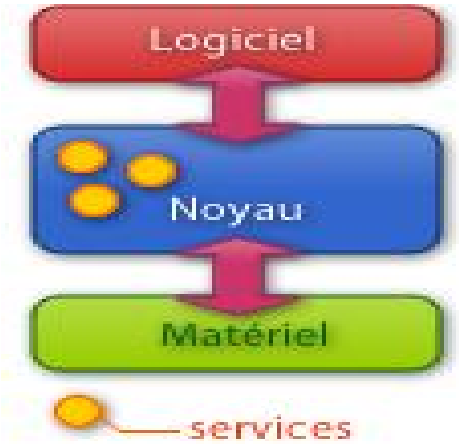


Fig. II.1. Le noyau de système d'exploitation :

3.2. Les différentes versions du système d'exploitation Windows server :

Windows est une gamme de système d'exploitation produite par Microsoft, principalement cette gamme est composée de plusieurs versions allant de Windows 1.0 à Windows 7 parmi ces versions on peut citer : Windows 2000, Windows 2003, Windows 2008, Windows 2008 R2, Windows XP, Windows vista et Windows 7.Nous présenterons les descriptions de ces différentes versions tout en les comparant en deux grand groupes : dans le premier groupe nous confronterons

Windows 2000, Windows 2003, Windows 2008 et Windows 2008 R2 dans le seconde Windows XP, Windows vista et Windows 7.

3.2.1. Présentation de Windows 2000 Server

Windows 2000 est un système d'exploitation 32bits développé et distribué par Microsoft. Windows 2000 est en fait le nom commercial de la version 5.0 de Windows NT. Elle est sortie le 17 février 2000 et a succédé à Windows NT 4.0, crée 4ans auparavant en avril 1996.

Très sommairement, on peut affirmer que Windows 2000 serveur offre la majorité des avantages de Windows NT serveur en plus de quelques fonctionnalités supplémentaires.

Parmi ces avantages on mentionne :

- ✓ Prise en charge de plusieurs protocoles ;
- ✓ Un annuaire évolué d'organisation et de gestion des objets réseau ;
- ✓ L'intégration d'un serveur web IIS et la simplification de l'utilisation interface administrateur ;
- ✓ L'ouverture de session à distance par Terminal Server ;
- ✓ Gestion centralisée de client multiple ;
- ✓ Processeur multiple et prise en charge d'une mémoire vive considérable ;
- ✓ Interface de gestion réseau pratique.

3.2.2. Présentation de Windows Server 2003 :

Microsoft Windows Server 2003 représente une nette évolution en termes de fiabilité, de disponibilité et de facilité de gestion. Il s'agit d'un système d'exploitation plus complet et plus souple que ces prédécesseurs.

Il est basé sur une gestion système et des concepts d'administration qui avaient été introduits par Windows 2000 Serveur, avec des dizaines d'autres fonctionnalités nouvelles. En voici quelques unes :

- ✓ Une nouvelle version améliorée d'Active Directory, avec une sécurité renforcée grâce au pare-feu intégré par défaut et à la désactivation de la plupart des services par défaut, une interface plus facile à utiliser et des meilleures performances.
- ✓ Une interface de gestion de système plus conviviale appelé fenêtre « Gérer votre Serveur », par ailleurs, Windows 2003 Serveur comprend un ensemble d'outils d'administration plus complet que celui de Windows 2000 Serveur comme :

- Configurer votre serveur **:** Ajoute, supprime et configure les services Windows pour le réseau.
- DHCP **:** Configure et gère le service DHCP (Dynamics Host Configuration Protocol).
- DNS **:** Gère le service DNS (Domain Name Service).
- Utilisateurs et ordinateurs Active Directory **:** Gère les utilisateurs, les groupes, les ordinateurs et autres objets d'Active Directory.
- Gestionnaire des services Internet **:** Gère les services Web, FTP et SMTP.

3.2.2.1. Les mises à jour :

Les fonctionnalités apportées par le Service Pack 1 de Windows Server 2003 incluent: l'Assistant de configuration de la Sécurité **;** Hot Patching permettant d'étendre la capacité de Windows Server 2003 à mettre à jour des fichiers DLL, des pilotes, et des améliorations réseaux concernant le support des Services de Fournisseurs Sans-fil (*Wireless Provisioning Services*); Pare-feu Windows ; des mises à jour de sécurité post-installation **;** Data Execution Prevention (DEP) permettant de prévenir les attaques de type *buffer overflow* qui sont souvent des vecteurs d'attaques de Windows Server ; Windows Media Player version 10 ; Internet Explorer 6 contenant Une liste complète des mises à jour contenues dans le Service Pack 1 est disponible dans la Base de connaissance Microsoft.

Le Service Pack 2 quant à lui contient la console de gestion Microsoft en version 3.0 (Microsoft Management Console 3.0), Windows Deployment Services, le support de WPA2, et des améliorations apportées à IPSec et MSConfig, le Pack d'Evolution Réseau à Windows Server 2003 (*Scalable Networking Pack* - SNP).

3.2.2.2. Les différentes versions :

La famille de système d'exploitation Windows 2003 Serveur se compose des plusieurs versions chacune a un objet précis :

A. Windows Server 2003, Standard Edition *:*

C'est la version de base de Windows 2003. Elle est conçue pour fournir des services et des ressources à d'autres systèmes du réseau. Cette version remplace directement Windows NT 4.0 Server et Windows 2000 Server. Elle propose une riche palette de fonctions et d'options de configuration.

Windows Server 2003 Standard Edition gère jusqu'à 4GO de mémoire (RAM) et jusqu'à 2 processeurs.

B. Windows Server 2003, Entreprise Edition :

Est conçu pour les réseaux de grandes taille ; elle se caractérise par des performances élevées ainsi qu'une grande fiabilité. Cette version prolonge les fonctionnalités de Windows Server 2003 Standard Edition pour permettre le service de cluster, les méta-annuaires et les services pour Macintosh.

Windows Server 2003 Entreprise Edition supporte des ordinateurs comportant jusqu'à 8 processeurs, 32 GO de mémoire (RAM).

C. Windows Server 2003, Datacenter Edition :

Est la version la plus puissante de Windows 2003 Server. Des avancés de gestion des erreurs et des tolérances en font un système de choix pour les applications les plus sophistiquées.

Elle prend en charge jusqu'à 64 GO de mémoire (RAM) et elle nécessite 8 processeurs au minimum et peut en gérer 32 au maximum.

D. Windows Server 2003, Web Edition :

Est conçu pour fournir des services web, déployer des sites web et des applications web.

Cette version prend en charge jusqu'à 2 GO de mémoire et 2 processeurs.

3.2.3. Windows Server 2003 R2

Windows Server 2003 R2 est distribué en 2 CD, dont un CD correspondant au CD d'installation de Windows Server 2003 SP1. Le second CD ajoute plusieurs fonctionnalités optionnelles et installables à Windows Server 2003. La mise à jour R2 est disponible pour les versions x86 et x64 mais pas pour les versions Itanium.

3.2.4. Présentation de Windows server 2008 :

Microsoft Windows Server 2008 est le système d'exploitation Windows Server de nouvelle génération qui aide les administrateurs système à optimiser leur contrôle sur l'infrastructure. Il offre une disponibilité et des fonctionnalités sans précédent. Les administrateurs bénéficient d'un environnement serveur davantage sécurisé, fiable et robuste. Par ailleurs, Windows Server 2008 propose aux organisations une nouvelle valeur ajoutée en garantissant à tous les utilisateurs l'accès à l'ensemble des services du réseau, où qu'ils se trouvent. Windows Server 2008 offre également une vue approfondie sur les fonctions du système d'exploitation et de diagnostic, permettant aux

administrateurs de consacrer davantage de temps à la valeur métier de l'entreprise. Windows Server 2008 s'appuie sur les points forts du système d'exploitation Windows Server 2003 et sur les innovations du Service Pack 1 et de Windows Server 2003 R2. Cependant, Windows Server 2008 est bien plus qu'une version perfectionnée des systèmes d'exploitation précédents. Il a été conçu pour offrir aux entreprises la plateforme la plus efficace pour prendre en charge des applications, des réseaux et des services Web, du groupe de travail jusqu'au centre de données. Pour cela, Windows Server 2008 est doté de nouvelles fonctionnalités très élaborées.

3.2.5. Présentation de Windows server 2008 R2

Windows Server 2008 R2 est conçu pour aider les organisations à réduire les coûts d'exploitation et à accroître l'efficacité, Windows Server 2008 R2 permet un meilleur contrôle des ressources dans toute l'entreprise. Il améliore les performances, réduit la consommation électrique et abaisse les coûts d'exploitation. Il permet aux agences et aux filiales de mieux travailler ; il propose de nouveaux moyens d'accès à distance, il simplifie l'administration des serveurs et étend la stratégie de virtualisation Microsoft à la fois aux postes clients et aux serveurs.

4. Migration d'Active Directory

La migration consiste a transféré les rôles FSMO d'un server à un autre server dans le même domaine AD avec des outils simple et facilement tout en garantissant la protection des donnes de l'entreprise et l'ensemble des paramètres et configurations actuels est conservé

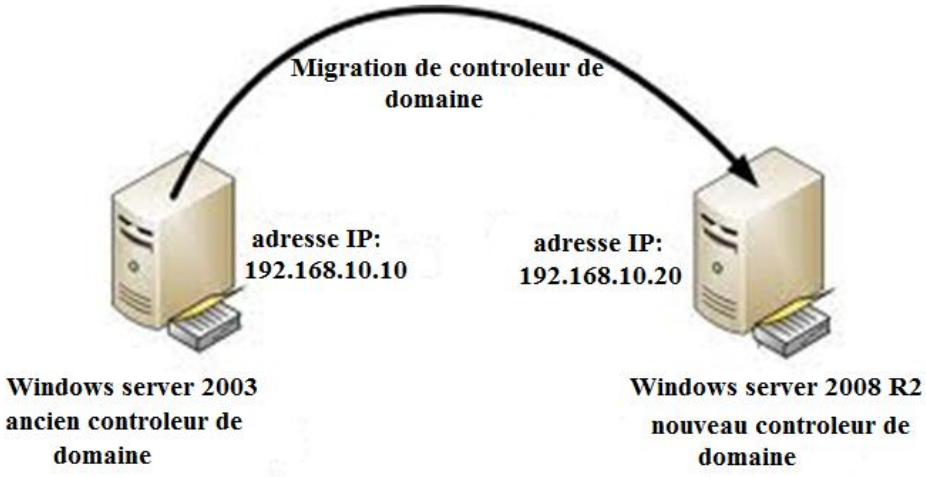


Fig II.2: La migration de contrôleur de domaine

4.1. Méthodes de migration

Nous pouvons distinguer trois méthodes :

- ✓ Mise à jour en lieu et place,
- ✓ Nouvelle installation
- ✓ Migration

4.1.1. Mise à jour en lieu et place

La mise à jour en lieu et place n'est possible qu'à partir des machines 64-bit avec des OS Windows 2003 SP2 ou 2003 R2 et Windows Server 2008.

A. Les avantages

Cette solution conserve l'ensemble des paramètres et configurations actuels de même que l'accès aux données.

B. Les inconvénients

- ✓ Tous les anciens objets AD et toutes les anciennes données, et par conséquent d'éventuelles erreurs, sont conservées sur le serveur mis à niveau.
- ✓ Les mises à niveau sur place nécessitent un temps d'arrêt plus long en raison du remplacement du système d'exploitation existant par le nouveau système d'exploitation.
- ✓ En cas d'échec de la mise à niveau, le rétablissement de l'état précédent est plus complexe

4.1.2. Nouvelle installation

A. Les avantages

- ✓ On crée un nouvel environnement adapté aux besoins actuels.
- ✓ On ne récupère pas les anciennes données inutiles.
- ✓ Ce processus n'intervient pas avec l'environnement de production.

B. Inconvénients

- ✓ On doit entièrement reconfigurer le nouvel ordinateur et l'environnement AD.
- ✓ Cette méthode peut être indiquée lorsqu'on veut restructurer son environnement AD. Par exemple, réduire le nombre de domaines, fusionner des forêts suite à un rachat d'une autre société, etc.

L'outil « ADMT » fourni par Microsoft peut nous aider à cloner ou à déplacer des objets AD à partir de domaines existants vers la nouvelle structure Windows Server 2008 R2.

4.1.3. Migration

A. Les avantages

- ✓ L'ensemble des paramètres et configurations actuels est conservé
- ✓ toutes les anciennes données et configurations inutiles sont supprimées du fait qu'on va précéder à une nouvelle installation 2008 R2.
- ✓ Étape de transition d'un environnement physique vers un environnement virtuel et d'une installation complète vers une installation minimale (Server Core).
- ✓ Un temps d'arrêt inférieur est requis car l'ancien Server reste opérationnel pendant la grande majorité du processus de migration.

B. Les inconvénients

Des opérations de planification et vérification supplémentaires sont nécessaires afin de s'assurer que la migration a réussi.

4.2. Les principaux raisons pour migrer vers Windows server 2008

- ➢ **Lancer un projet de virtualisation**

Hyper-V est la nouveauté la plus importante de Windows Server 2008 : il s'agit du premier hyperviseur de Microsoft apte à supporter la virtualisation de serveurs critiques, donc à concurrencer VMware. Pour une entreprise désirant lancer un projet de consolidation de serveurs tout en restant dans le monde Microsoft, l'adoption de Windows Server 2008 s'impose.

- ➢ **Déployer une infrastructure de clients légers**

On estime que Windows Server 2008 est, avec ses Terminal Services, la première solution permettant, sans la compléter par une offre tierce, de déployer une infrastructure de clients légers dédiée à des applications critiques ciblant un grand nombre d'utilisateurs. Des lacunes dans la version 2003 ont été comblées : équilibrage de charge, meilleure gestion des imprimantes, signature unique, portail Web dédié à l'accès distant et transparence accrue pour l'utilisateur (qui ne distingue plus applications locales et distantes).

- ➢ **Profiter des avantages d'Active Directory 2008**

Windows Server 2008 permet de déployer des contrôleurs de domaines en lecture seule(RODC). C'est intéressant pour équiper des agences distantes dont la sécurité physique ne peut être garantie. Egalement lié à AD 2008, Microsoft met en avant RMS (Right Management Server), la technologie de contrôle des droits numériques. RMS n'est pas nouveau. Dans Windows Server 2008, il est juste mieux intégré à l'Active Directory et n'impose plus une connexion à un service distant Microsoft, ce qui rebutait une entreprise sur deux.

- **Administration**

Tous les services sont désormais présentés sous forme de rôles ou de fonctionnalités. Désormais, lorsqu'on sélectionne un rôle, on voit l'ensemble des informations utiles pour l'administrer. De plus, des rôles existants et disparates ont été réorganisés.

Par exemple, l'annuaire Active Directory, le gestionnaire de certificats et le serveur de gestion des droits numériques ont été regroupés. L'administrateur a donc désormais une vision très claire de ce que fait chaque serveur, et n'a plus à superviser un par un des services participant à la même fonction.

- **Simplifier la tolérance aux pannes**

Le déploiement d'architectures en grappes serait beaucoup plus simple qu'avec Windows Server 2003, en particulier grâce à des assistants mieux conçus et à un meilleur contrôle de la cohérence entre nœuds.

- **Améliorer les performances**

La pile réseau TCP/IP et le protocole de transfert de fichiers ont été complètement réécrits, ce qui améliore les performances, à condition que les postes clients soient sous Vista SP1. Dans un autre registre, IIS 7.0, intégré à Windows Server 2008, offre de meilleures performances aux serveurs Web. II7 adopte en effet le principe de la modularité inhérente à Windows Server 2008. Seuls les modules nécessaires étant activés, les performances s'en trouvent améliorés. De plus, le clonage de serveurs Web physiques ou virtuels est simplifié

- **Contrôler la santé des postes clients**

Le support par Windows 2008 de NAP (Network Access Protection) est l'un des arguments avancés pour Microsoft pour migrer. Cette technologie permet de contrôler la santé des postes clients qui cherchent à se connecter aux serveurs

4.3. Principales raisons pour migrer vers Windows Server 2008 R2

- **Grande capacité de monter en charge**

Windows Server 2008 R2 a été conçu pour donner des résultats identiques ou supérieurs à Windows Server 2008 sur la même plateforme matérielle. De plus, R2 est le premier système d'exploitation Windows Server à travailler exclusivement sur une architecture 64 bits.

Windows Server 2008 R2 présente aussi plusieurs améliorations liées aux processeurs. En premier, cette version permet aux organisations de faire fonctionner jusqu'à 256 processeurs logiques. Pour les entreprises qui ont choisi Windows Server comme plateforme de virtualisation, R2 prend aussi en charge la traduction d'adresses de second niveau (SLAT). Cela permet à R2 d'exploiter la table des pages améliorée qui équipe les derniers processeurs AMD ainsi que la fonctionnalité similaire des tables de pages imbriquées des derniers processeurs Intel. Ainsi, les serveurs R2 peuvent fonctionner comme système virtuel avec une gestion améliorée de la mémoire du système.

Certains composants de Windows Server 2008 R2 exploitent mieux le matériel. Ainsi, dans Windows Server 2008 R2, Hyper-V peut maintenant accéder à 32 processeurs logiques sur les systèmes hôtes, deux fois le nombre initialement pris en compte par la première version d'Hyper-V. Cela permet de mieux exploiter la puissance des systèmes multi cœurs et d'obtenir un meilleur taux de consolidation des systèmes virtuels par hôte physique.

- **Consommation électrique réduite**

Windows Server 2008 R2 optimise la consommation électrique. Il surveille le niveau d'utilisation de chaque cœur de processeur sur le serveur et ajuste dynamiquement l'état des processeurs pour réduire la consommation électrique lorsque la charge baisse. Ce mécanisme, spécifique à Windows server 2008 R2, se nomme Core Parking (mise en veille des cœurs), et des stratégies de groupe permettent de l'optimiser.
Core Parking suit la charge en temps réel sur chaque cœur. Lorsqu'un cœur n'est pas ou peu utilisé, Core Parking le met en mode veille afin de réduire la consommation électrique. Ainsi, un serveur à 16 cœurs se réduit à un serveur à 4 cœurs lorsque l'activité est faible. Dès que l'activité remonte, les cœurs dormants sont réveillés en quelques millisecondes.

- **Hyper-V dans Windows Server 2008 R2**

Windows Server 2008 R2 est équipé d'une version améliorée de la technologie Hyper-V de virtualisation de Microsoft. Hyper-V version 2 améliore la gestion des systèmes virtuels et répond à certaines attentes spécifiques, notamment en ce qui concerne la migration de serveurs.

Hyper-V est la technologie qui permet à Windows Server 2008 R2 de proposer l'une de ses plus importantes innovations, la migration dynamique (Live Migration). Avec Hyper-V version 1.0, Windows Server 2008 pouvait effectuer une migration rapide, c'est-à-dire un déplacement de systèmes virtuels entre hôtes physiques en quelques secondes de temps d'arrêt. Malheureusement,

ces quelques secondes sont encore de trop dans certains scénarios, notamment lorsque des clients sont connectés à des serveurs virtuels. Avec la migration dynamique, le temps de déplacement d'un système virtuel se mesure en millisecondes. L'opération devient ainsi totalement transparente pour les utilisateurs.

La nouvelle version d'Hyper-V améliore les performances, sait prendre en charge jusqu'à 32 processeurs logiques sur l'hôte et bénéficie de la prise en charge de la traduction de deuxième niveau des adresses mémoire (SLAT). De plus, les systèmes virtuels peuvent ajouter ou retirer des disques virtuels (VHD) sans nécessiter de redémarrage et ils peuvent aussi démarrer à partir d'un disque virtuel.

- **Administration plus efficace des postes de travail**

Les solutions de virtualisation présentent un grand intérêt dans le monde des serveurs. Mais de grands progrès ont été réalisés dans la virtualisation de la présentation : le traitement s'effectue sur un serveur optimisé pour la capacité et la disponibilité, tandis que les graphiques, le clavier, la souris et d'autres fonctions d'entrées/sorties s'effectuent au niveau du poste de travail de l'utilisateur.

Windows Server 2008 R2 inclut une technologie VDI (intégration de poste de travail virtuel) améliorée, qui étend les fonctionnalités de Terminal Services afin de fournir certains programmes professionnels sur les postes de travail distants des employés. Avec VDI, les applications reçues par un ordinateur client via les services Bureau à distance apparaissent désormais dans le menu Démarrer, à côté des applications installées en local. Cette approche améliore la virtualisation du poste de travail et la virtualisation des applications.

La virtualisation du poste de travail bénéficiera d'une gestion améliorée de la personnalisation, d'une intégration quasi-transparente des applications et des bureaux virtualisés dans Windows 7, de meilleures performances audio et graphique, et d'un accès plus agréable par le Web, entre autres. VDI utilise mieux les ressources virtualisées et intègre mieux les périphériques locaux et les nouvelles puissantes fonctions d'administration des systèmes virtuels.

- **Administration serveur plus simple et plus efficace**

Bien que l'amélioration des capacités du système d'exploitation serveur soit toujours une bonne chose, elle est contrebalancée par une complexité croissante et une charge de travail importante dans la gestion quotidienne des systèmes. Windows Server 2008 R2 s'attaque à ce

problème en simplifiant de nombreuses tâches via de nouvelles consoles d'administration. Ces outils permettent :

- ✓ Une gestion améliorée du centre de données et une réduction de la consommation électrique.
- ✓ Une administration plus efficace à distance, incluant un Gestionnaire de serveur installable à distance.
- ✓ Des fonctions renforcées pour la gestion des identités via une mise à jour et une simplification des Services de domaines Active Directory (AD DS) et des Services fédérés Active Directory.

- ➢ **Faciliter l'accès à distance tout en simplifiant son administration**

L'informatique verte, le prix des trajets aériens, une économie au ralenti et l'obligation de pouvoir travailler n'importe où, tous ces éléments contribuent à développer l'informatique à distance et à rendre les tâches d'administration informatique plus importantes et plus complexes. Windows Server 2008 R2 propose une nouvelle fonctionnalité qui simplifie considérablement la gestion des connexions VPN et les rend aussi simples d'emploi qu'une connexion téléphonique.

DirectAccess (DA) est une solution complète d'accès à partir de n'importe quel endroit, qui permet aux organisations de fournir une connectivité sécurisée, toujours disponible, utilisable aussi bien par les utilisateurs sur site que par les utilisateurs à distance. Elle améliore la sécurité et réduit le coût total de possession. DA élimine le besoin de se connecter explicitement avec le réseau de l'entreprise lors des déplacements. DirectAccess représente la nouvelle génération de connectivité sécurisée, basée sur des stratégies. Pour les utilisateurs, le concept d'informatique à distance s'estompe car DirectAccess et Windows 7 se combinent pour leur présenter une connexion permanente à leur réseau d'entreprise, qu'ils soient dans l'entreprise, en déplacement ou sur un réseau public.

DA inclut des technologies déjà intégrées dans Windows Server 2008 comme IPSec et IPv6 mais les regroupe dans un assistant de configuration et d'administration simple à utiliser pour les administrateurs. Pour assurer la fiabilité et la sécurité, DA exploite aussi les innovations d'autres produits et services Microsoft, comme la protection d'accès réseau (NAP), l'isolation domaine et serveur, et Forefront™ Client Security. De plus Microsoft Forefront Intelligent Application Gateway (IAG) améliore le déploiement et la gestion.

- **Windows PowerShell 2.0**

Windows Server 2008 a introduit PowerShell, un puissant langage de script qui permet aux administrateurs d'automatiser des tâches d'administration répétitives en écrivant des scripts cmdlets. Plusieurs scripts (cmdlets) de base étaient préinstallés dans Windows Server 2008, accompagnés d'outils élémentaires permettant aux administrateurs d'écrire leurs propres cmdlets.

Windows Server 2008 R2 va plus loin en introduisant PowerShell 2.0, nette amélioration de la version précédente, avec plus de 240 nouvelles cmdlets et une nouvelle interface graphique qui ajoute des fonctionnalités professionnelles de développement. Cette interface exploite une syntaxe colorée, propose de nouvelles fonctionnalités de débogage et de nouveaux outils de tests.

PowerShell 2.0 prend aussi en charge Windows 7 et le rôle Server Core (qui dans la version précédente de Windows Server 2008 ne permettait pas le fonctionnement de PowerShell).

- **Accès à distance omniprésent**

Aujourd'hui, les employés sont de plus en plus mobiles et les demandes augmentent pour que les administrateurs autorisent des accès depuis l'extérieur aux ressources de l'entreprise. Toutefois, la gestion des ordinateurs à distance est un défi permanent, en raison de la faible bande passante des réseaux longue distance, des connexions fluctuantes et des reconnexions qui ralentissent les opérations d'administration des postes de travail, comme l'application de correctifs ou la modification des stratégies de groupe.
Windows Server 2008 R2 introduit un nouveau type de connectivité nommé DirectAccess. Ce mécanisme permet aux utilisateurs distants d'accéder facilement aux ressources de l'entreprise sans nécessiter de connexion ni de client VPN. En reprenant les technologies livrées dans Windows Server 2008, Microsoft a ajouté des assistants d'administration qui permettent de configurer DirectAccess entre la version R2 et les clients Windows 7 afin d'établir une connexion de base. Puis cette connexion est améliorée via d'autres outils de sécurité et de gestion propres à R2, comme NAP et des stratégies d'administration.

Avec DirectAccess, chaque utilisateur est considéré comme travaillant en permanence à distance. Les utilisateurs ne font plus la distinction entre une connexion locale et une connexion à distance. DirectAccess s'occupe de tout en arrière-plan. Les administrateurs conservent un contrôle précis sur les accès et la sécurité de périmètre. Ils résolvent plus facilement les problèmes de sécurité des postes de travail et d'administration aux deux extrémités de la connexion.

- **Amélioration de l'administration et des performances des agences**

Souvent dans les entreprises, les agences et les filiales ne disposent que d'une bande passante réduite entre elles et la maison mère. Les liaisons longue distance lentes réduisent l'efficacité des employés des agences en leur faisant perdre du temps lors de chaque accès à des fichiers de la maison mère. Le coût pour obtenir des liaisons à très haut débit est élevé. Pour résoudre ce problème, Windows Server 2008 R2 introduit une nouvelle fonctionnalité nommée BranchCache™ qui réduit la charge sur le réseau longue distance et améliore la réactivité des applications réseau pour les employés des agences.

Avec BranchCache, lorsqu'un employé accède à un fichier, la recherche de ce fichier s'effectue d'abord sur le réseau local de l'agence. Si le fichier est disponible localement dans l'agence, l'employé obtient immédiatement l'accès au fichier. Les fichiers peuvent être stockés sur un serveur local BranchCache ou simplement dans les autres PC de l'agence sous Windows 7.

- **Meilleure conformité avec les pratiques recommandées**

L'optimisation des serveurs d'une organisation afin d'atteindre un haut niveau de sécurité, de disponibilité, de performance et de souplesse d'administration, implique l'utilisation par les administrateurs des pratiques recommandées. Actuellement, dans beaucoup d'entreprises, l'utilisation des pratiques recommandées pour configurer un serveur, est un processus manuel. Fort du succès des Analyseurs de bonnes pratiques (BPA) Microsoft pour des plateformes comme Exchange Server 2007 et Microsoft SQL Server® 2008, Windows Server 2008 R2 intègre à son tour un analyseur de bonnes pratiques pour chaque rôle serveur de base.

En intégrant directement les informations de ces bonnes pratiques dans le Gestionnaire de serveur, Windows Server 2008 R2 simplifie la tâche d'optimisation des serveurs et réduit les coûts d'exploitation en permettant aux administrateurs de détecter rapidement des erreurs de configuration, avant qu'un problème ne se pose.

- **Le meilleur serveur d'applications et de services Web**

Windows Server 2008 R2 inclut de nombreuses améliorations qui font de Windows Server le meilleur serveur Windows pour des applications et des services Web, notamment avec Internet information Services (IIS) 7.5 et la fonctionnalité complète ASP.NET dans le rôle Server Core.

Le nouveau serveur Web facilite l'administration en complétant le Gestionnaire des services Internet par de nouveaux modules pour configurer le Filtrage des demandes, FastCGI et ASP.NET ; en incluant le nouveau fournisseur Windows PowerShell pour IIS et tout un ensemble de nouvelles

cmdlets ; et en intégrant de nouvelles fonctions de dépannage, comme un analyseur de pratiques recommandées dédié et une journalisation de la configuration. De plus, nous avons intégré de nombreuses extensions disponibles pour Windows Server 2008, y compris des versions à jour de Secure FTP et WebDAV.

- **Migration des systèmes virtuels sans irruption de service**

La migration rapide proposée par Windows Server 2008 est une fonctionnalité intéressante qui permet aux administrateurs de déplacer des systèmes virtuels entre des hôtes physiques, au prix d'un temps d'arrêt court. Le problème est que ce délai est malheureusement suffisamment long pour bloquer les applications ou les utilisateurs connectés, ce qui sature immédiatement d'appels le service d'assistance (help desk). Windows Server 2008 R2 résout ce problème avec la migration dynamique.

La migration dynamique exploite les services de cluster Windows et la technologie des volumes partagés en cluster pour déplacer des systèmes virtuels en quelques millisecondes. Ainsi, aucune connexion ne tombe en dépassement de délai. Cette fonctionnalité permet une gestion beaucoup plus dynamique des systèmes virtuels dans le centre de données. Nous avons aussi ajouté les fonctionnalités de migration dynamique à System Center Virtual Machine Manager, en incluant la possibilité d'effectuer des déplacements de systèmes virtuels selon des stratégies. Le monde virtuel se perfectionne.

5. Conclusion

Il n'est pas possible de faire une mise à jour en lieu et place de Windows Server 2003 à Windows Server 2008 R2. La solution consiste à installer un serveur 2008 R2 en tant que Contrôleur de domaine supplémentaire, à transférer vers lui tous les rôles FSMO et à supprimer le ou les DC 2003 dans le chapitre suivant on va voir les étapes de transfère.

CHAPITRE II

Comparaison entre les systèmes serveur

CHAPITRE III

Migration de Windows serveur 2003 vers Windows serveur 2008 R2

1. Préambule

Dans cette partie nous allons migrer un serveur 2003 avec les rôles Contrôleur de domaine et serveur DNS. Nous utiliserons la méthode « Migration » en remplaçant le serveur 2003 par un serveur 2008 R2 sans interruption du service et dans un laps de temps assez court.

2. La technologie RAID

L'utilisation de la technologie RAID qui signifie **« ensemble redondant de disques indépendants »** qui permet de constituer une unité de stockage à partir de plusieurs disques et d'y effectuer des sauvegardes régulières à partir de plusieurs disques durs. L'unité ainsi constituée (grappe) a donc une grande tolérance aux pannes ou une plus grande capacité et vitesse d'écriture. Une telle répartition de données sur plusieurs disques permet d'augmenter la sécurité et de fiabiliser les services associés donnes l'exemple RAID 0, RAID 1, RAID 5 et RAID 10.

- **RAID 0**

Le RAID 0, connu sous le nom d'« entrelacement de disques » (striping en anglais) est une configuration permettant d'augmenter significativement les performances de la grappe en faisant travailler les disques durs en parallèle (fonction de notre configuration matériel : 1 seul bus Sata avec 4 disque n'augmenterons pas le débit donc les performances, en revanche 4 bus Sata avec 1 disque par bus augmentera significativement les performances). Le RAID 0, augmente les performances mais n'apporte aucune protection des données. Si nous perdons un disque de la grappe, nous perdons les données.

- **RAID 1**

Egalement connu sous le nom volumes en miroir, c'est un volume à tolérance de panne qui garantit la redondance des données en utilisant deux copies, ou miroirs, du même volume. Toutes les données écrites sur le volume miroir sont écrites sur les deux volumes, qui sont situés sur des disques physiques distincts. Si un des disques physiques a un problème, les données du disque défaillant ne sont plus disponibles, mais le système continue à fonctionner en exploitant le disque non affecté.

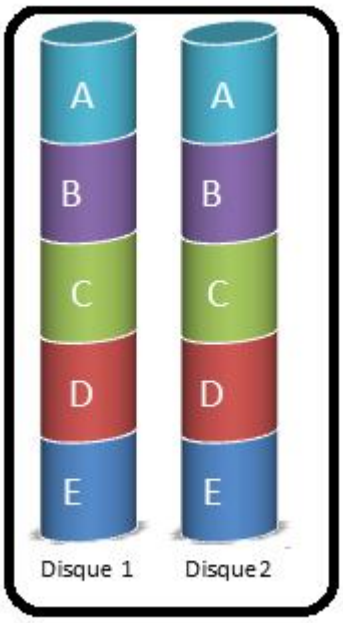


Fig III.1 : **Un volume RAID1 ou en miroir copie toutes les données sur un deuxième disque**

- **RAID 5**

Un volume RAID 5 est un volume tolérant aux pannes qui combine des zones d'espace libre d'un moins trois disques durs physiques en un seul volume logique. Les volumes RAID 5 agrègent les données par bondes avec des informations sur la parité (paire ou impaire) sur une baie de disques. Quand un disque est défaillant, Windows server 2008 se base sur ces informations parité pour recréer les données sur le disque défaillant. Les volumes RAID 5 peuvent accepter de perdre un seul disque dans la baie.

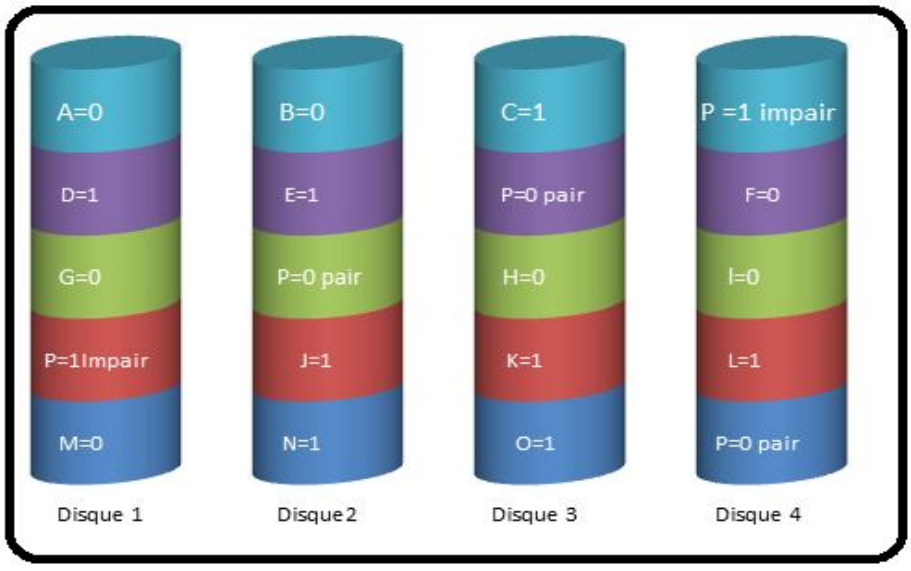


Fig III.2 Un volume RAID 5 calcule la parité (pair ou impair) pour la tolérance aux pannes

- **RAID 5+1 ou RAID 51**

C'est une construction des 2 grappes en RAID5 combinées avec un RAID1, disques minimum requis est 6 HDD en 2 grappes de 3 HDD capacité de la grappe : Efficience : 50% de la volumétrie est utile au stockage Tolérance de faute : très élevée, il faut perdre 4 HDD. Particularité : les HDD doivent avoir la même volumétrie et être identiques pour une solution optimale.
Le RAID 51 allie fiabilité et rapidité mais solution chère car on perd la moitié de la volumétrie totale pour stocker.

- **RAID 10**

Il permet d'obtenir un volume agrégé par bande fiable (puisqu'il est basé sur des grappes répliquées). Chaque grappe contenant au minimum 2 éléments et un minimum de 2 grappes étant nécessaire, il faut au minimum 4 unités de stockage pour créer un volume RAID10.

Sa fiabilité est assez grande puisqu'il faut que tous les éléments d'une grappe soient défectueux pour entraîner un défaut global. La reconstruction est assez performante puisqu'elle ne mobilise que les disques d'une seule grappe et non la totalité.

Remarque : Un volume agrégé par bandes, également connu sous le nom RAID 0, est un volume dynamique qui stocke des données dans des bandes sur deux disques physiques ou plus. Ce type de volume offre les meilleures performances par rapport à tous les autres volumes disponibles dans Windows, mais ne propose pas la tolérance de panne. Si un disque dans un volume agrégé par bandes est défaillant les données de tout le volume sont perdues. Solution proposé dans le cas de stockage de données temporaire.

3. Cahier de charge

Pour la réalisation de notre travail, on dispose des paramètres suivant :

- VMware : Ce logiciel est utilisé pour la virtualisation des deux environnements source et cible.
- Server Contrôleur de Domain Active Directory (Microsoft Windows 2003 server).

- Server Contrôleur de Domain Active Directory (Microsoft Windows 2008 R2).

4. Architecture source

Nous disposons d'un server contrôleur de domaine Windows server 2003 et quelques postes clients relié par un équipement d'interconnexion.

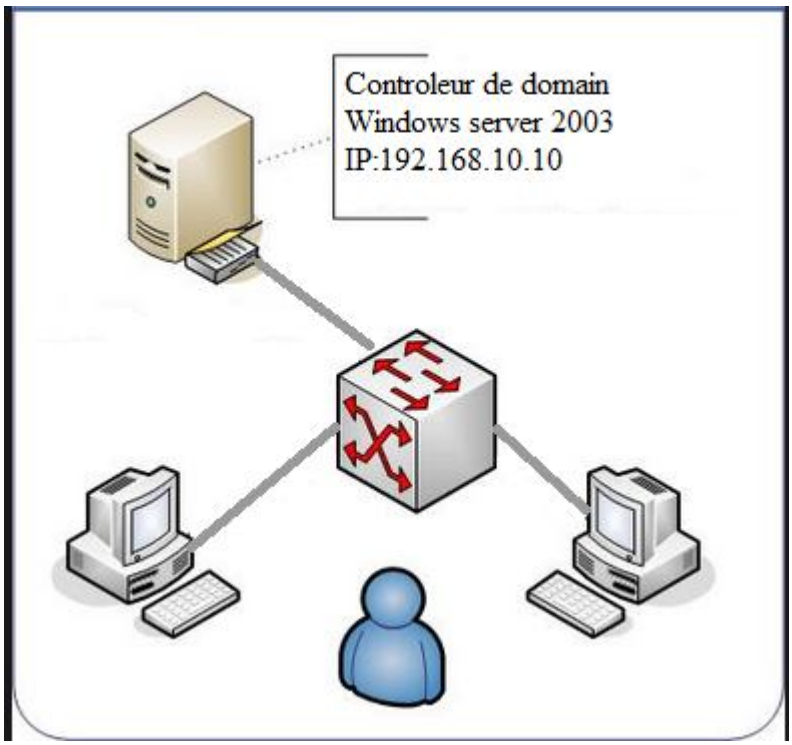


Fig.III.3 Architecture source

5. les problèmes lier a cette architecture

- La consommation d'électricité est considérable
- Faible bonde passante des réseaux longue distance
- L'absence de contrôleur de domaine en lecteur seul
- L'absence de hyper-V
- Système d'exploitation 32bits
- Sécurité limité

6. Architecture cible

Pour pallier aux inconvénients de Windows 2003 server, on effectue une migration vers Windows 2008 Server. L'architecture physique reste la même (Fig.III.3).

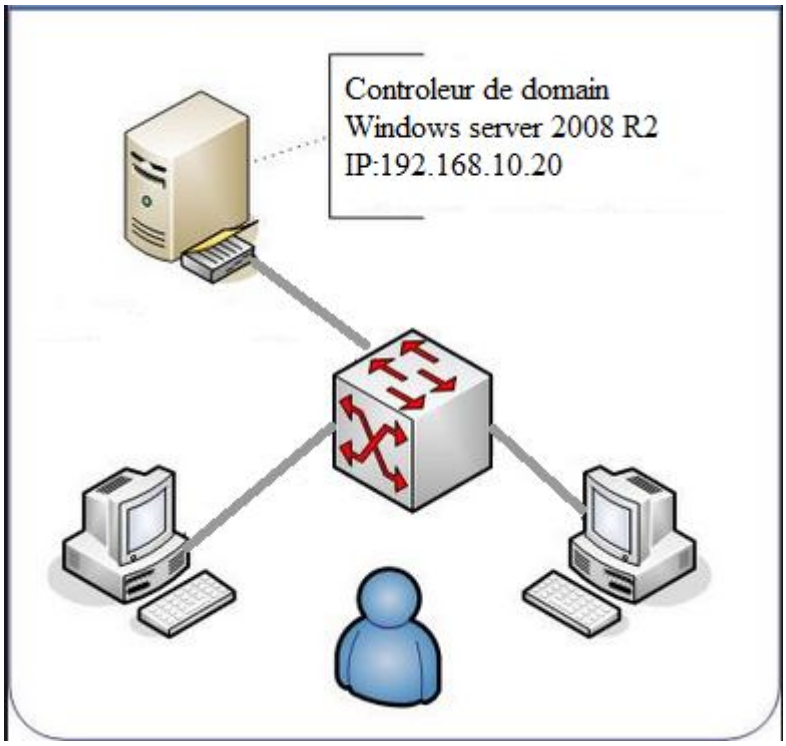
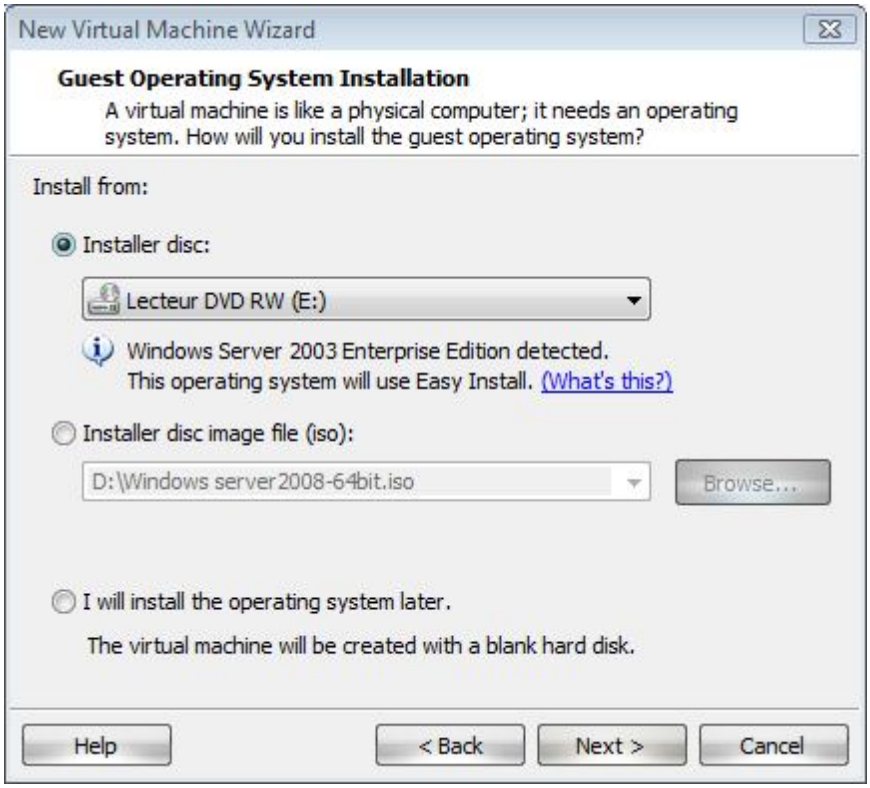


Fig III.4 Architecture cible

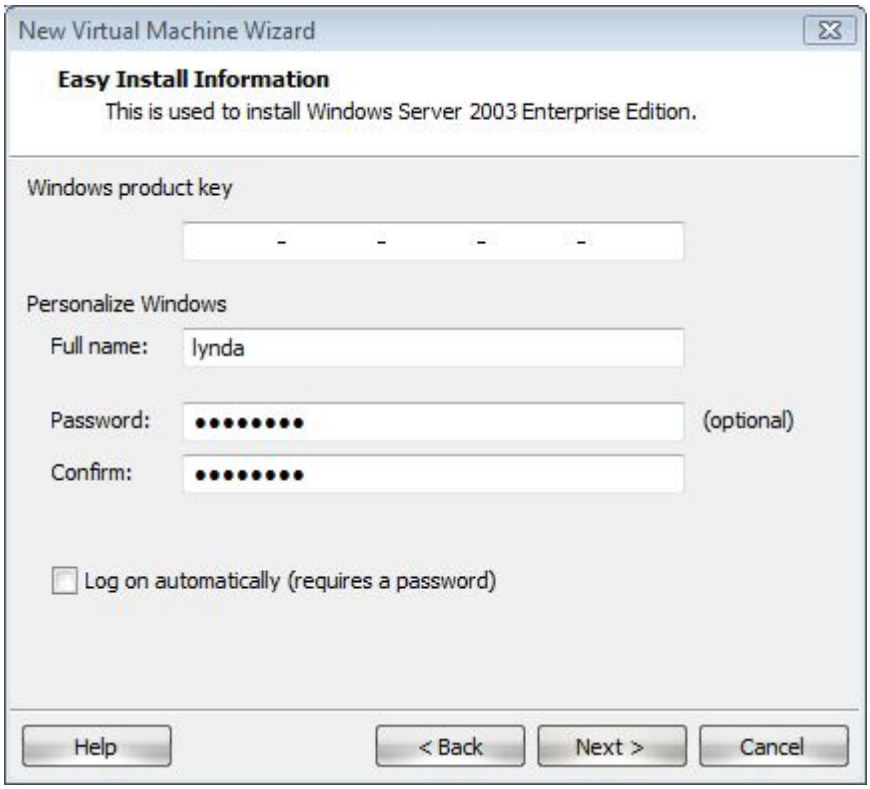
7. Installation de Windows server 2003

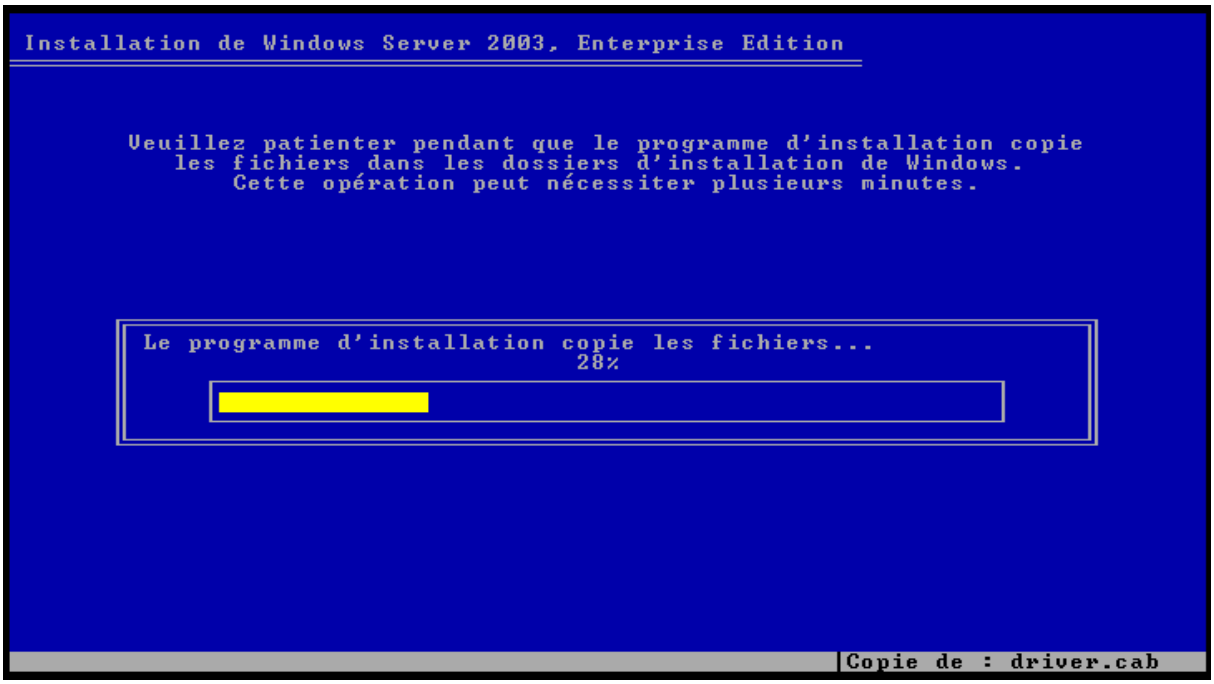
Crée une nouvelle machine Virtual, pour se faire on clic sur new virtuel machine une fenêtre s'ouvre et on clic sur Typical puis Next.

On insert le CD d'installation de Windows 2003 server et on choisit par disc puis next



Une fenêtre s'ouvre, on introduit la clé du produit, le nom de la machine et le mot de passe puis on clic sur Next

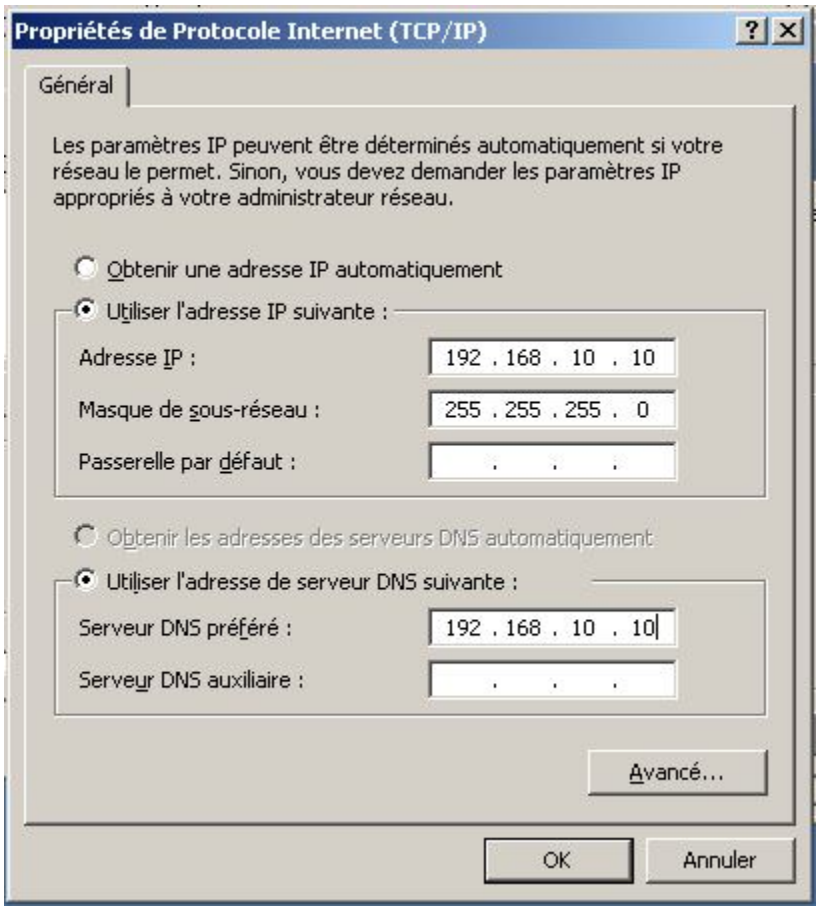




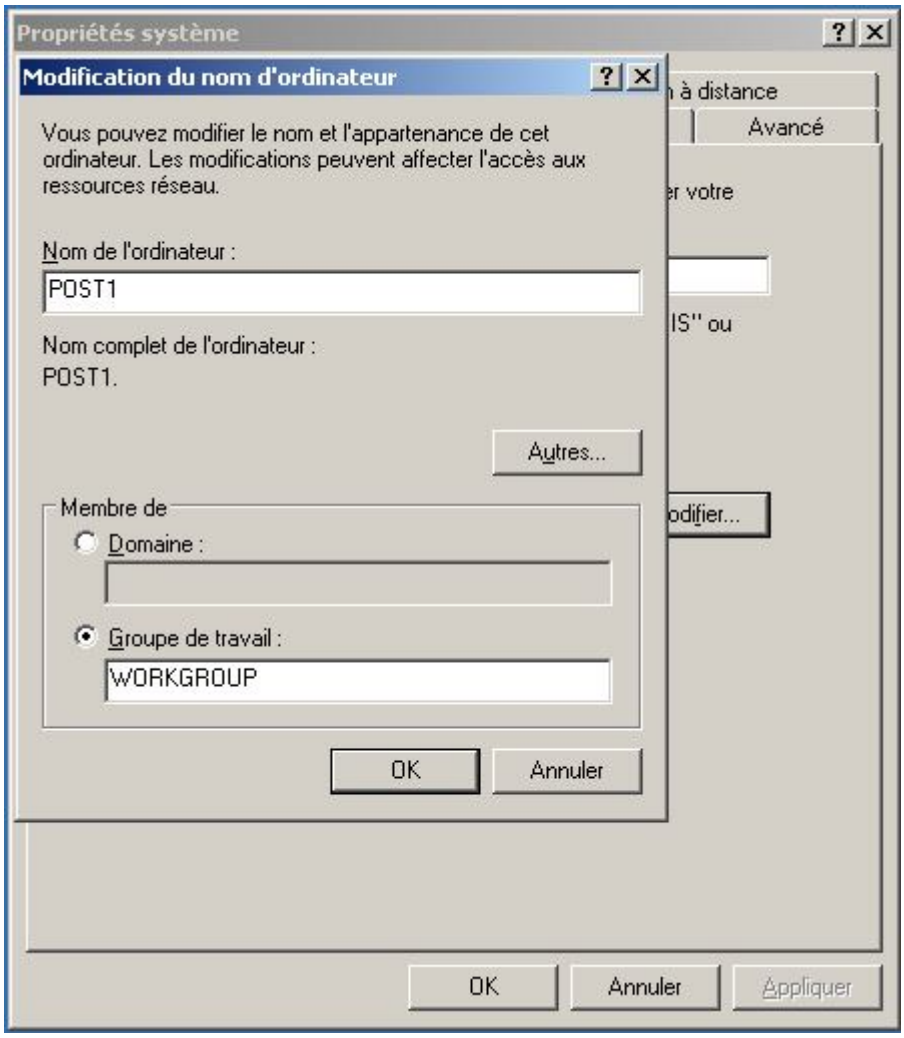
Le scénario d'installation va prendre un peu de temps pour copier les fichiers dans les dossiers d'installation de Windows 2003 Server.

Apres l'installation de Windows 2003 Server, on configure les adresses IP**.**

8. Configuration des adresses IP

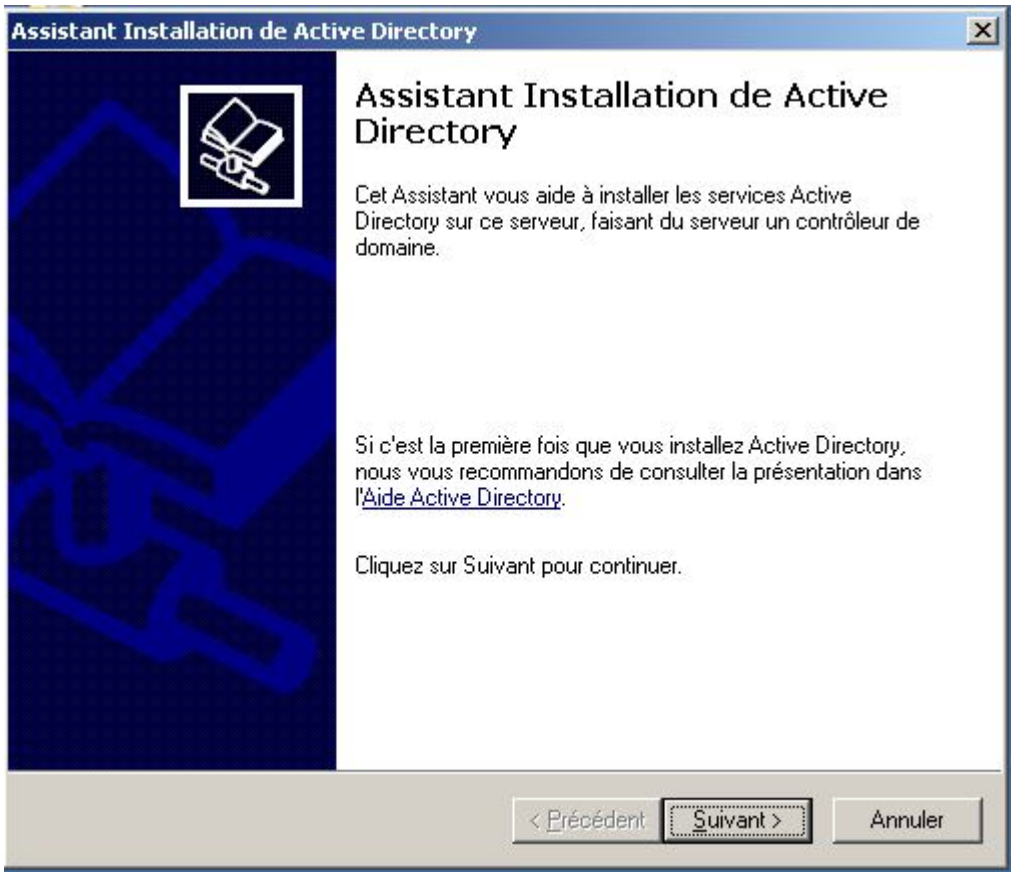


Puis on change le nom de la machine

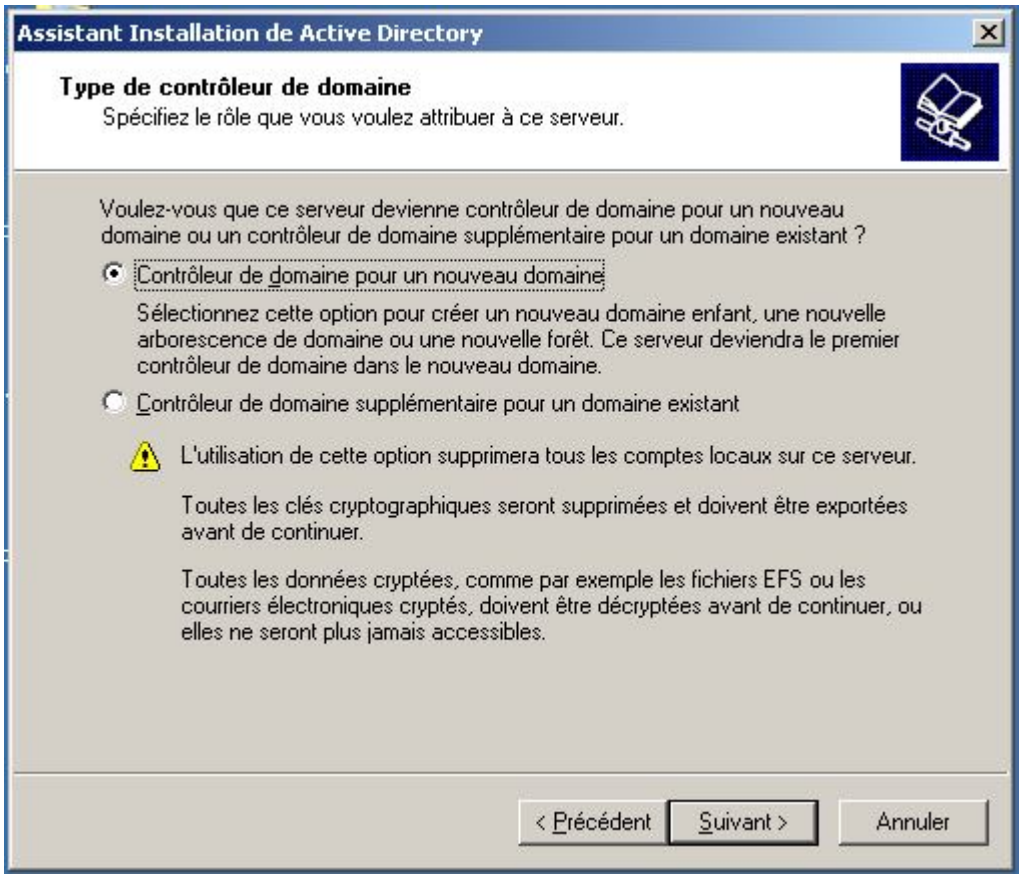


9. Installation d'Active Directory

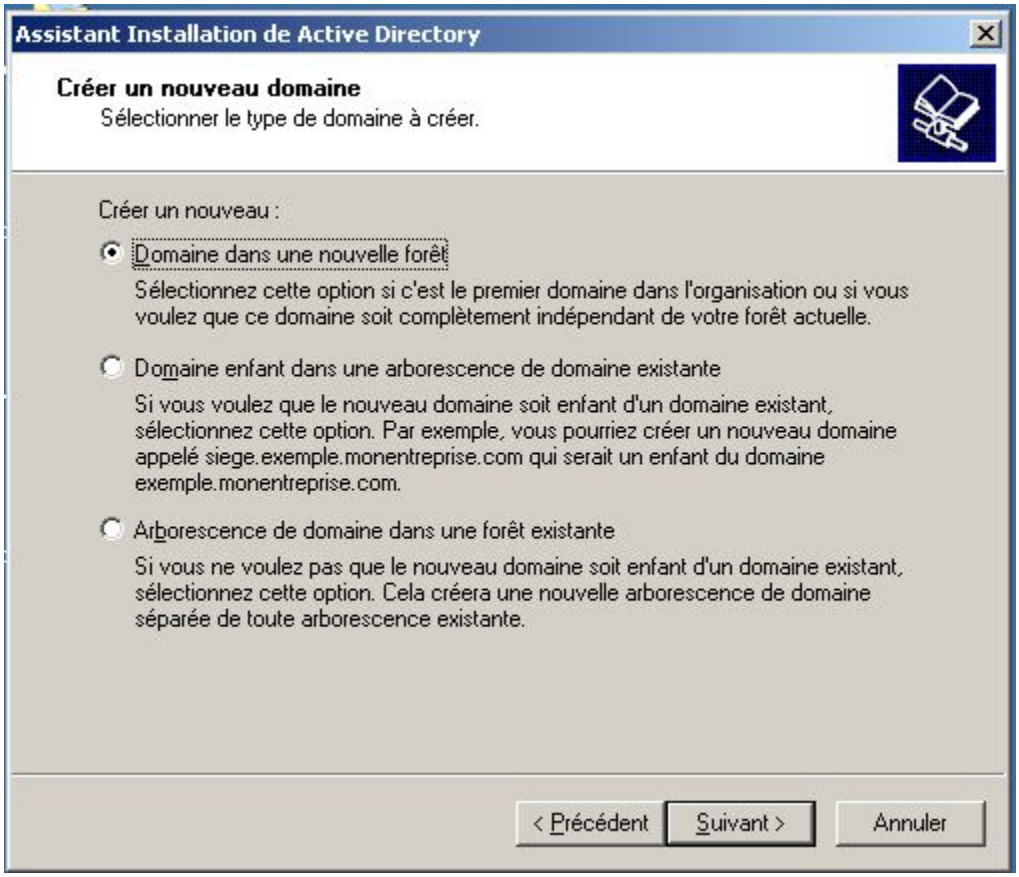
On installe l'Active Directory avec « DCPROMO »



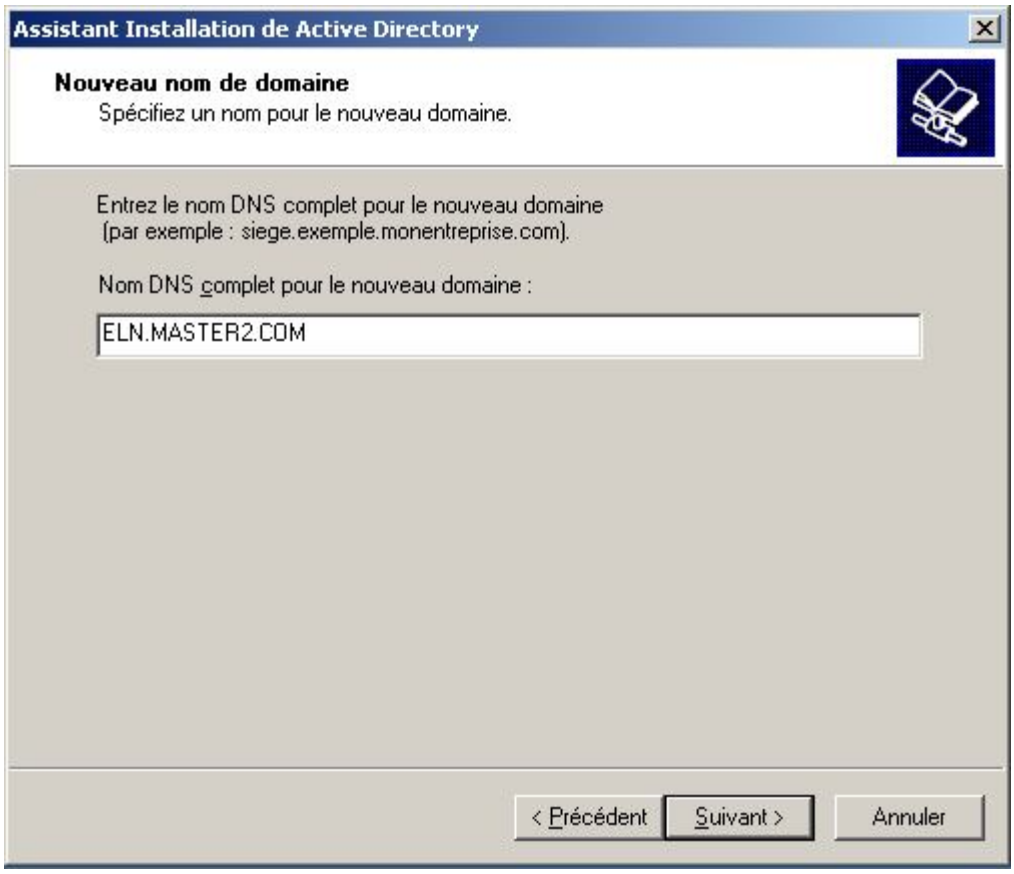
On crée un nouveau domaine



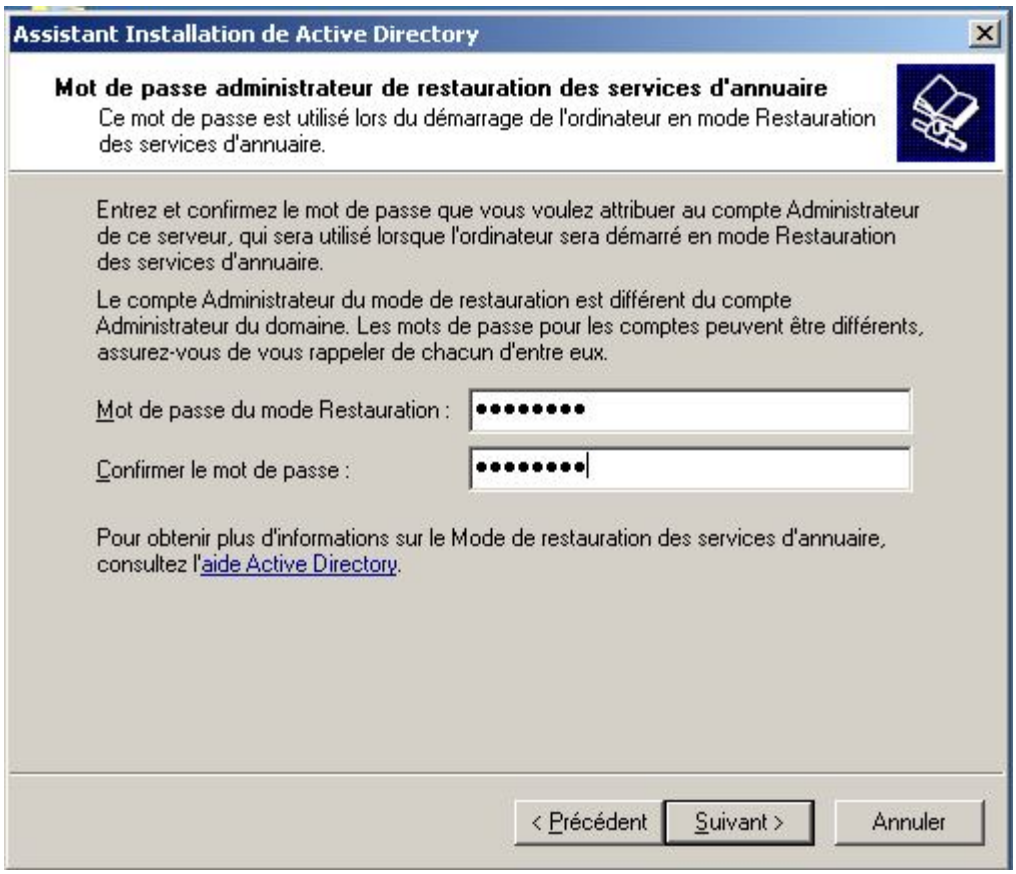
On sélection nouvelle foret puis suivant



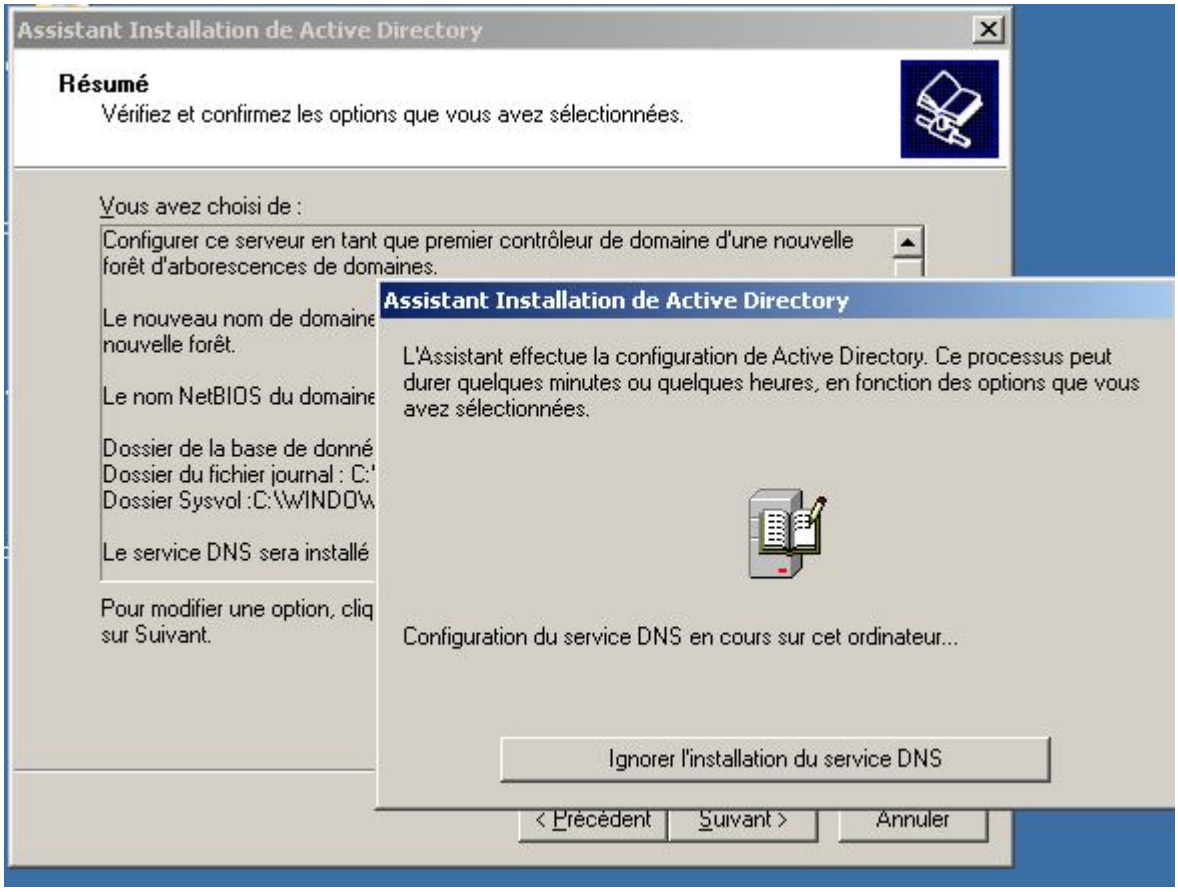
On donne le nom de domaine puis suivant



On introduit le mot de passe puis suivant



L'opération va durer quelque minute



10. Préparation de la migration :

Même si l'environnement AD source semble fonctionner correctement, il est important de s'assurer que certains paramétrages ou disfonctionnements ne présentent pas de problèmes de réplication, de lenteurs lors des ouvertures de session, de l'application des stratégies etc.

Voici quelques outils qui peuvent nous aider dans ces vérifications :

DCDIAG : Exécuter cet outil pour analyser l'AD et détecter d'éventuels problèmes. Inclus avec Windows Server 2003.

REPADMIN : Analyser la réplication AD. Inclus avec Windows Server 2003.

GPOTOOL : Cet outil permet de vérifier la cohérence des GPO (Group Policy Object) sur tous les DC.

Observateur d'événements : Confirmer qu'aucune erreur n'est signalée par les services AD, DNS, etc.

Vérifier les propriétés IP : Adresse IP, Passerelle par défaut et Serveur DNS.

Il s'agit du domaine «ELN.MASTER2.COM ».

Le domaine doit garder le même nom, le serveur DNS ne doit pas changer d'adresse, les stratégies continueront de s'appliquer et aucune manipulation sur les postes de travail ne doit être nécessaire.

On commence par quelques vérifications sur le server source.

Ensuite on procédera à une sauvegarde de l'état du système.

Après on mettra à jour le schéma vers 2008 R2

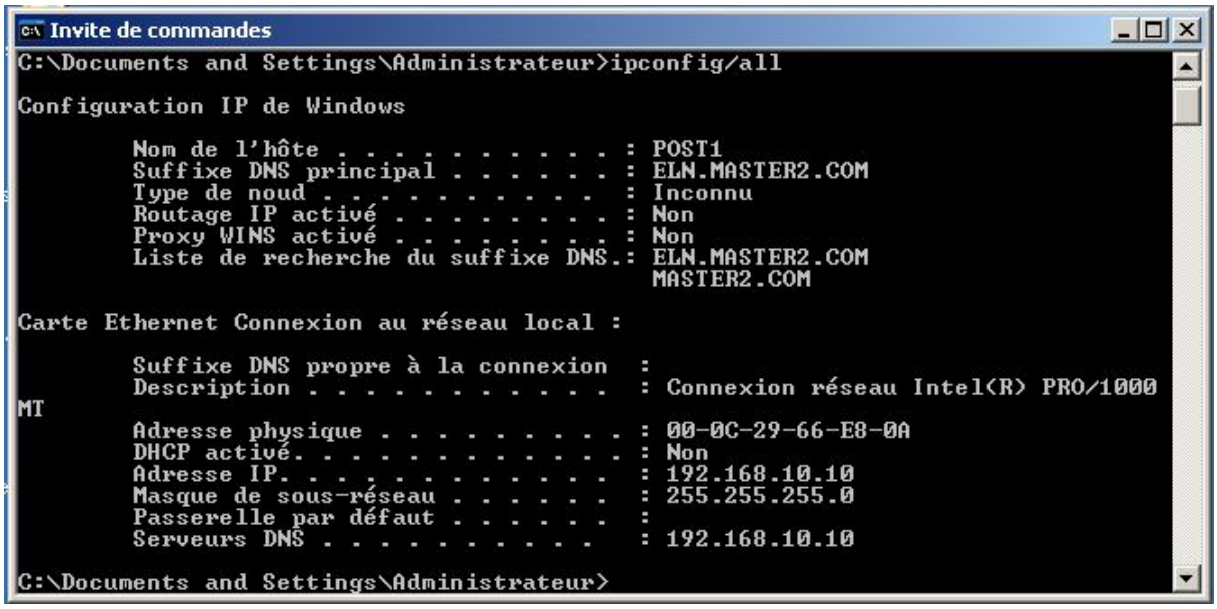
On procédera alors à la migration proprement dite

Et on finira avec les tâches de vérification post-migration

10.1 Préparer le serveur source :

Vérifier :

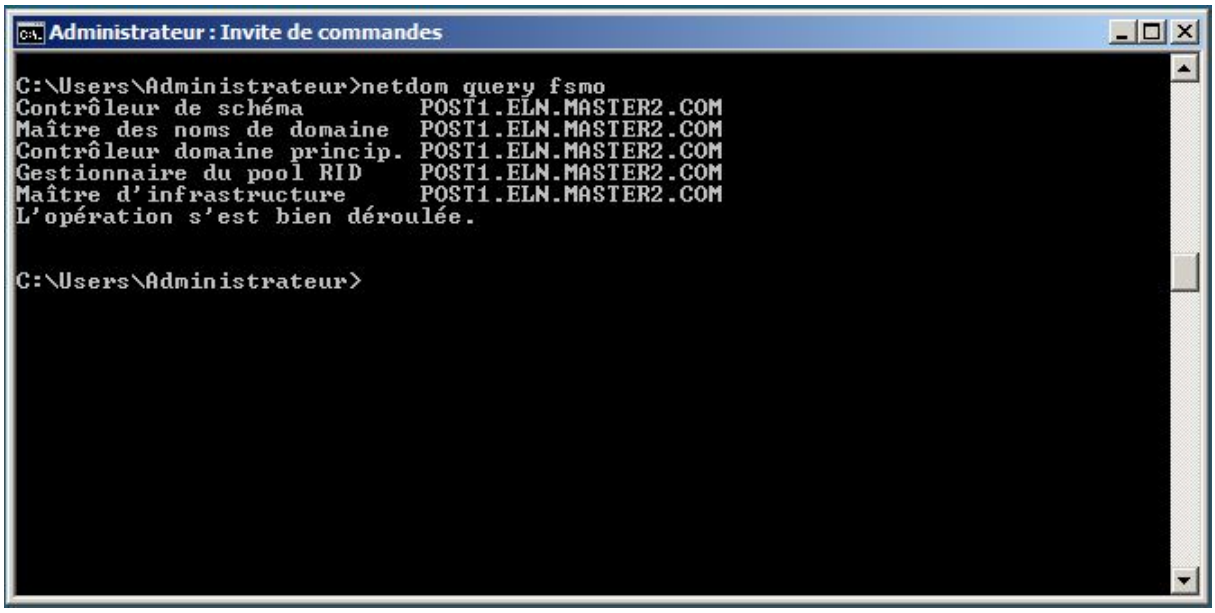
- le nom de serveur source : à l'invite de commande on tape «Hostname »
- Propriétés Tcp/Ip : A l'invite de commandes on tape : «Ipconfig /all »



- Rôles FSMO : Pour voir quel DC exécute les rôles FSMO :

Dans l'invite de commandes : « Démarrer > Exécuter > Cmd »

On tape la commande « Netdom Query FSMO »

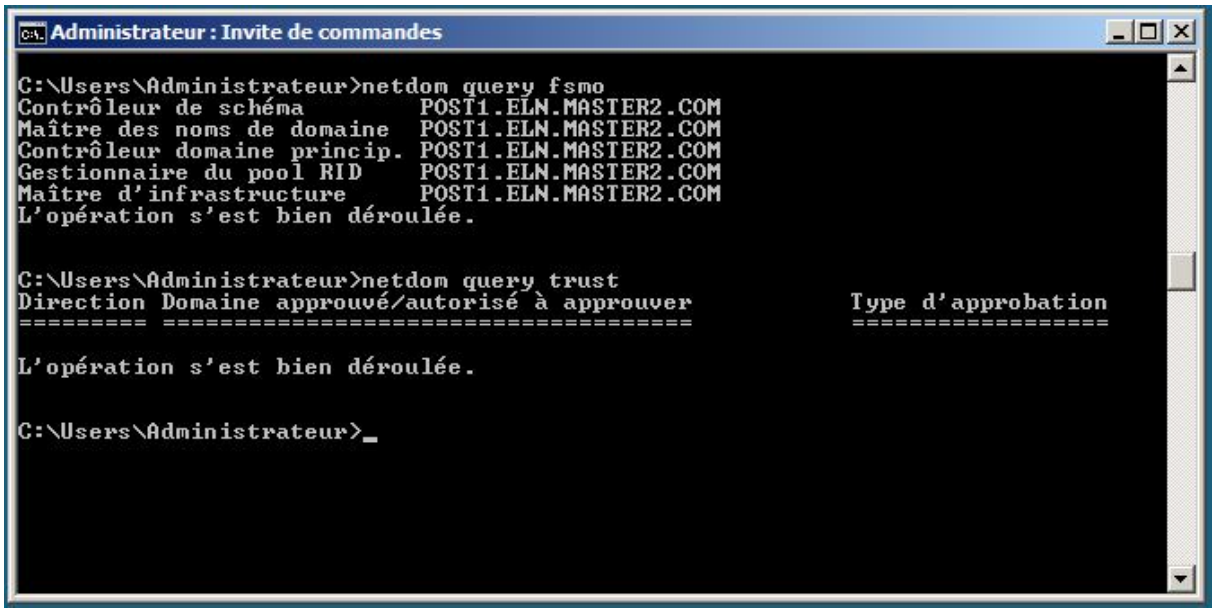


Donc les rôles FSMO sont héberge dons POST1

- On vérifie s'il ya des relations d'approbation Inter-domaines, Inter-Forêts

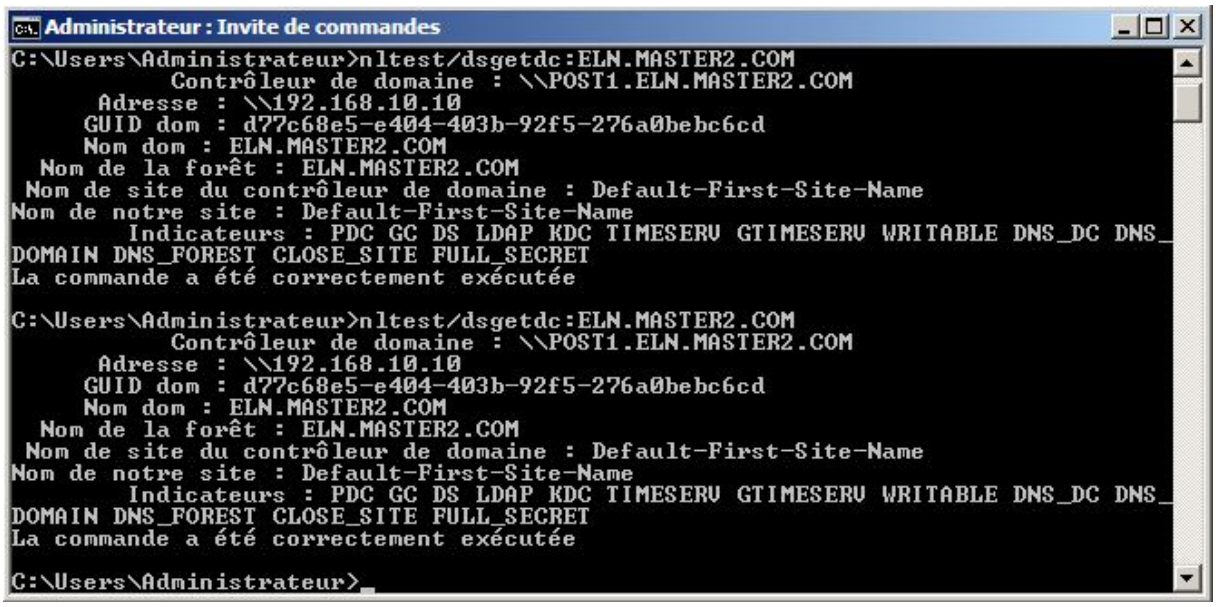
Dans l'invite de commandes : « Démarrer > Exécuter > Cmd »

Taper la commande : « Netdom query trust »



- On vérifie s'il est un Catalog Global et dans quel site il est

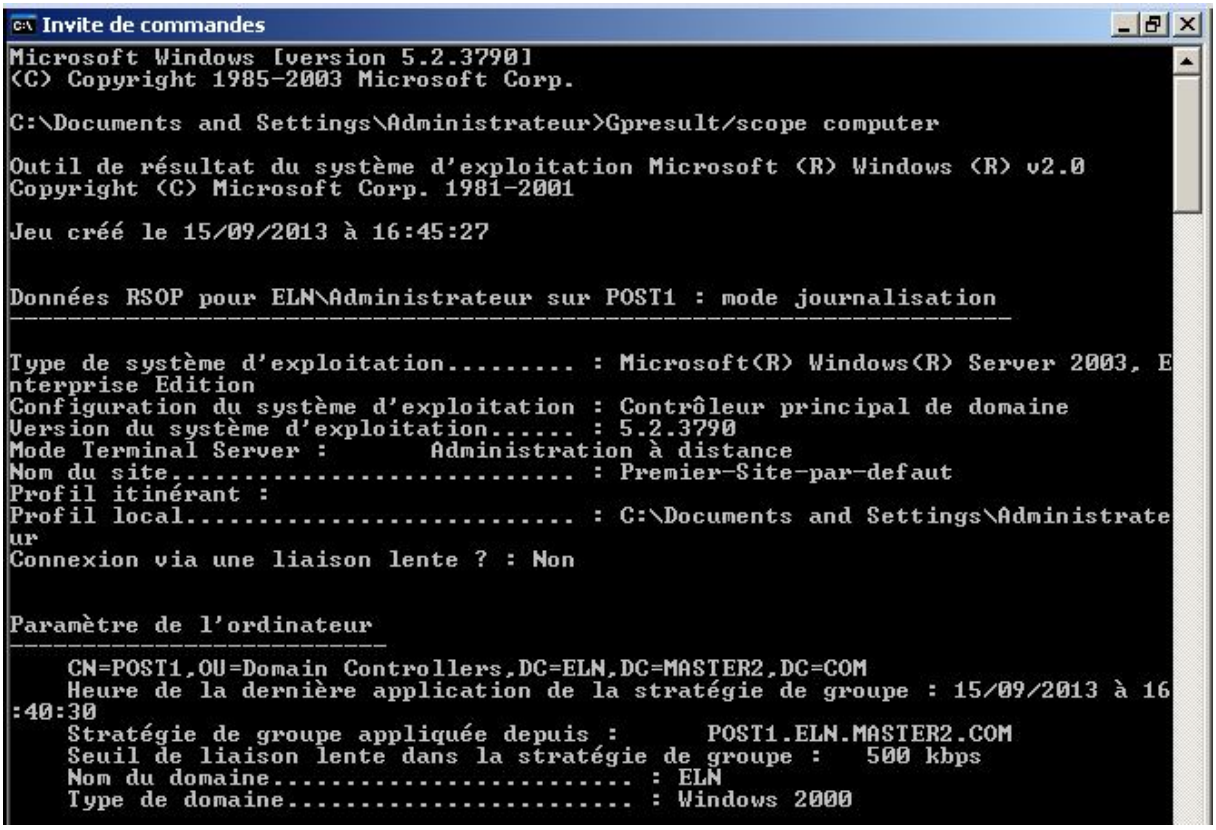
Démarrer > Exécuter > Cmd. on tape la commande:« Nltest /dsgetdc : ELN.MASTER2.COM».



- On vérifie quelles stratégies de groupe s'appliquent à ce DC

Se loguer en tant qu'Administrateur sur le DC à migrer.

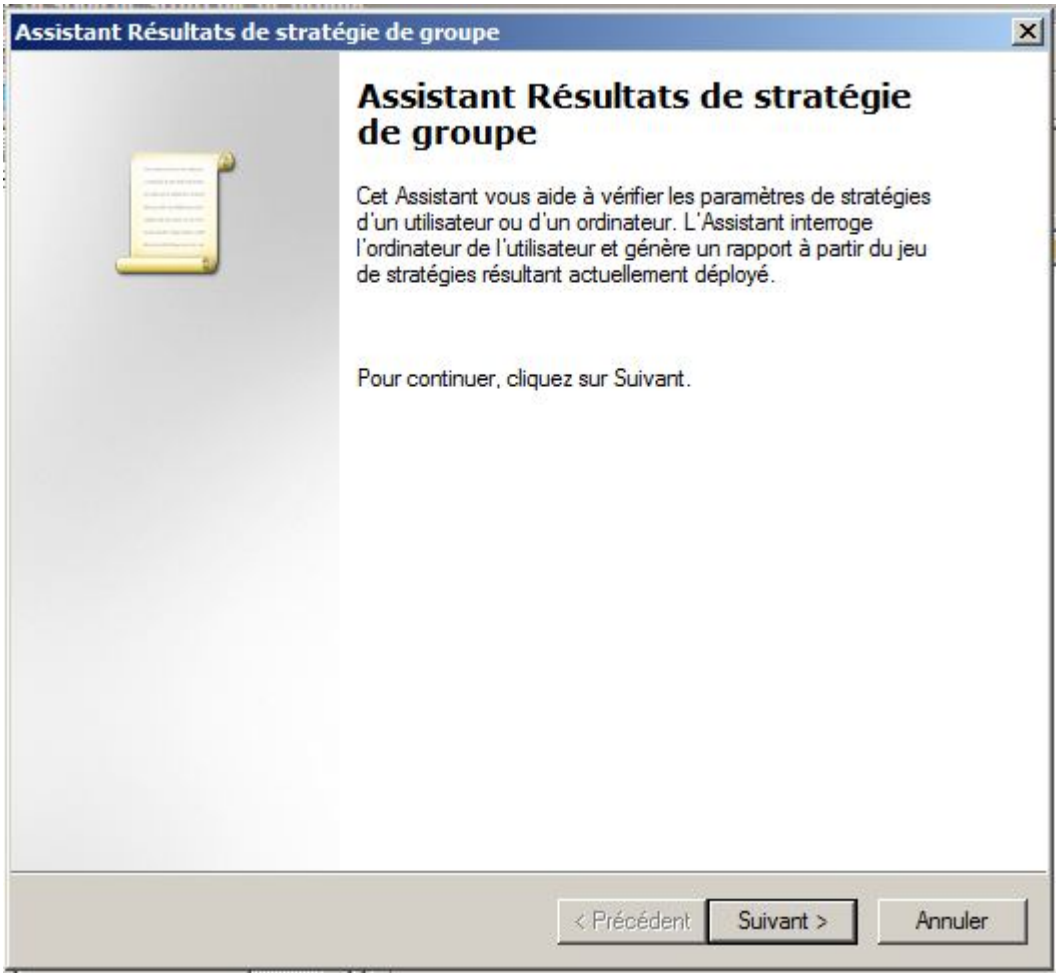
Démarrer > Exécuter > Cmd. Taper la commande : « Gpresult /scope computer /R ».



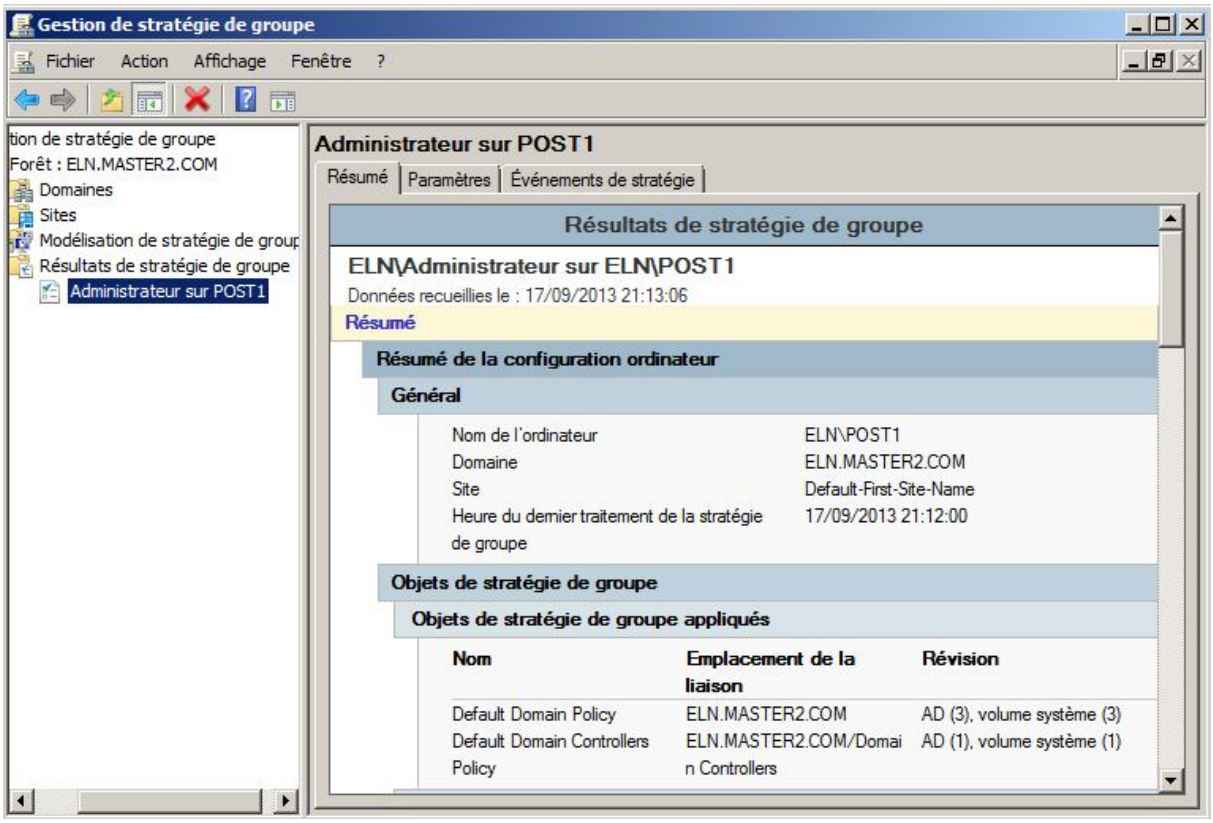
Si la GPMC (Groupe policy management Console) est installée, on peut voir plus aisément les paramètres de stratégie qui s'appliquent à l'ordinateur avec RSOP.

Se loguer en tant qu'Administrateur sur le DC à migrer.

Démarrer > Outils d'administration > Gestion des stratégies de groupe > Ouvrir : «Forêt ELN.MASTER2.com » > Sélectionner : « Résultats de stratégie de groupe » > Clic droit > Assistant Résultats Stratégie de groupe > Suivant > Cet ordinateur > Suivant > Utilisateur actuel > Suivant > Suivant > Terminer.

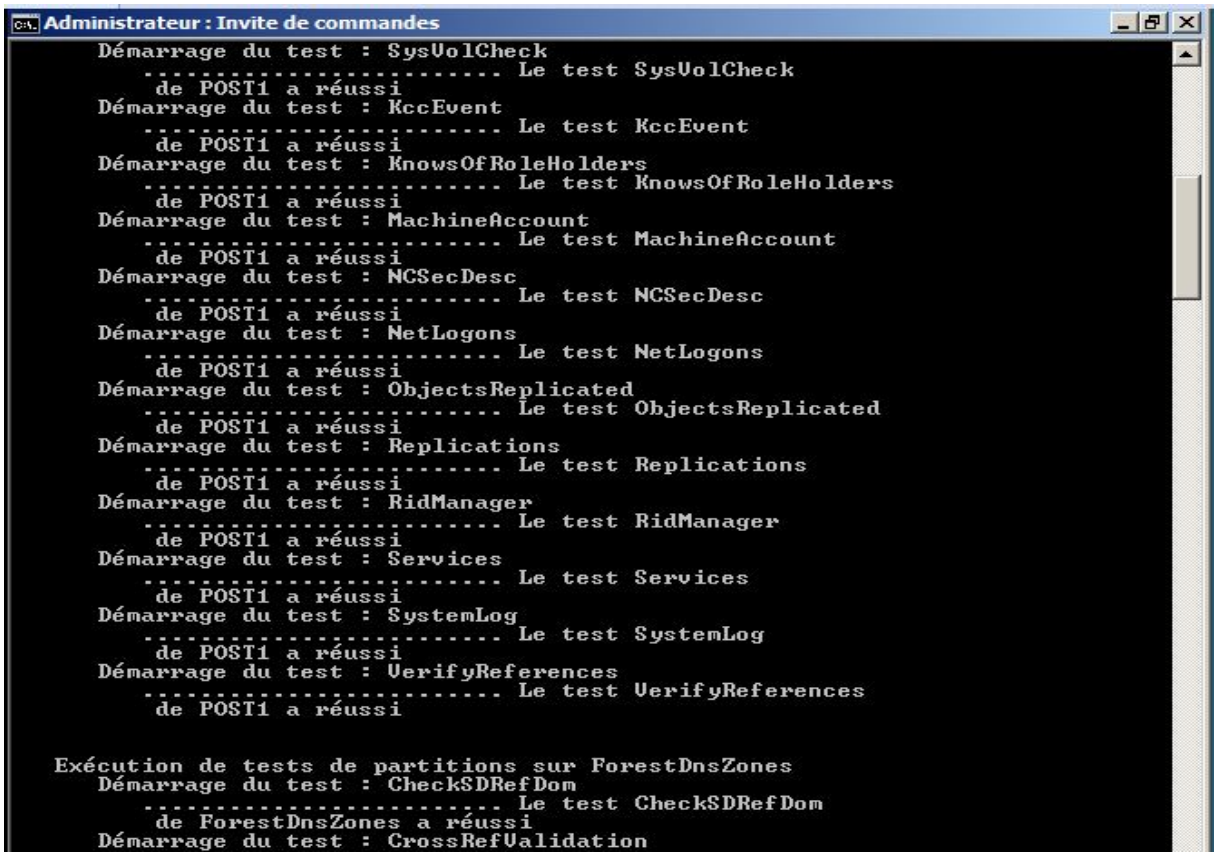


Après création du rapport, dans l'onglet « Résumé » voir quels sont les GPO qui s'appliquent et dans l'onglet « Paramètres » voir en détail quels sont les paramètres appliqués et par quel GPO.

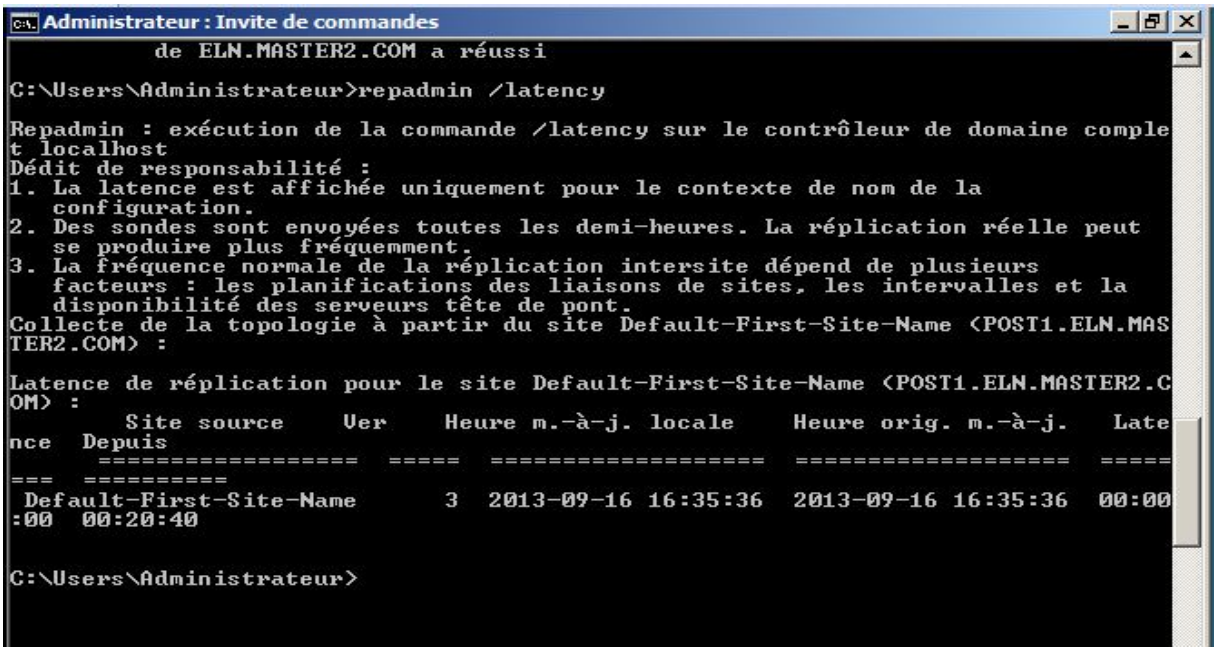


- Analyser l'AD avec « DCDIAG »

On peut voir toutes les options avec : « Dcdiag / ? »



- Analyser l'AD avec « REPADMIN ». Ex : Vérifier la latence de réplication



- Vérifier la cohérence de la réplication des stratégies avec GPOTOOL. Installer le Ressource Kit 2003 si ce n'est pas fait déjà.

Lancer la commande GPOTOOL.

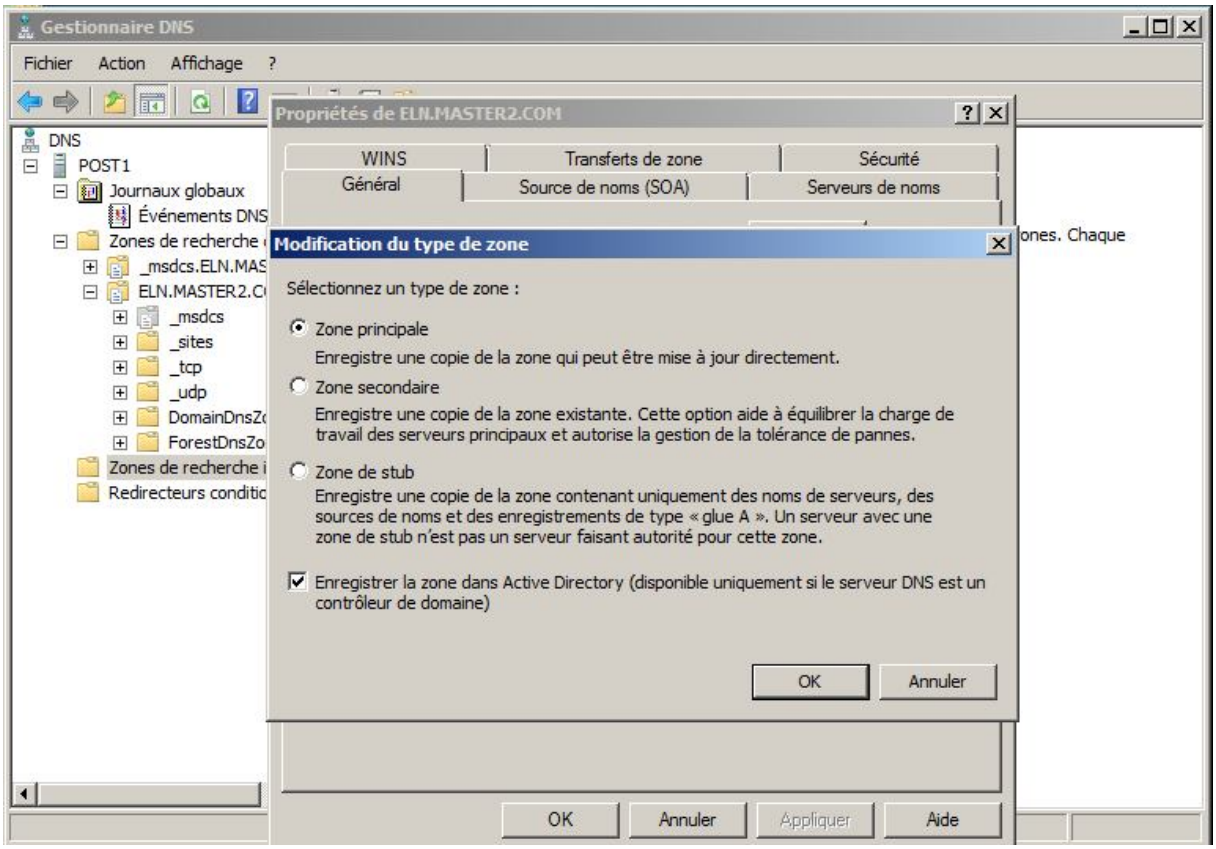
Lors de l'installation des Ressource Kit il ne crée pas de raccourcis ni de « Path » pour les utilitaires installés. La solution la plus simple consiste à aller sur le menu : « Démarrer > Tous les programmes > Windows Resource Kit Tools > Windows Resource Kit Tools Help »

Puis on exécute la commande Gpotool à partir de la fenêtre d'aide

- Modifier la Zone DNS en zone DNS intégrée:

Si la zone DNS n'est pas une zone intégrée on pourrait précéder à son intégration pour qu'elle soit répliquée vers les autres serveurs DC- DNS.

Démarrer > Outils d'administration > DNS > Clic droit sur le nom de la zone > Propriétés > Cocher la case « Enregistrer la zone dans Active Directory »

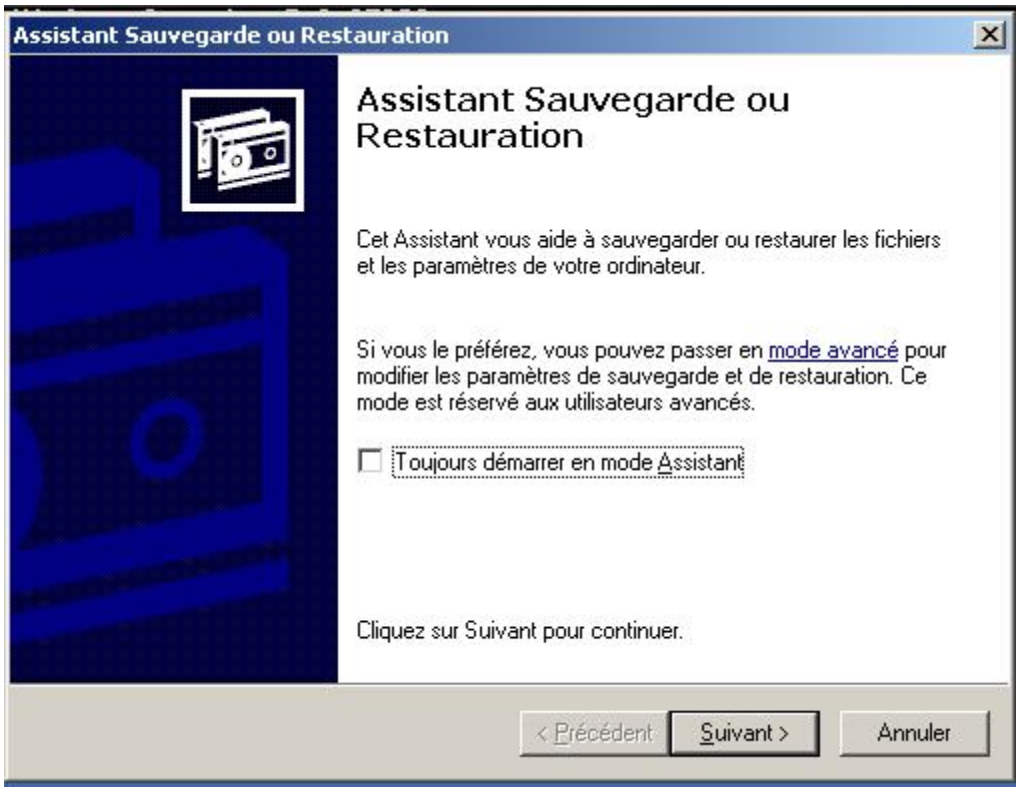


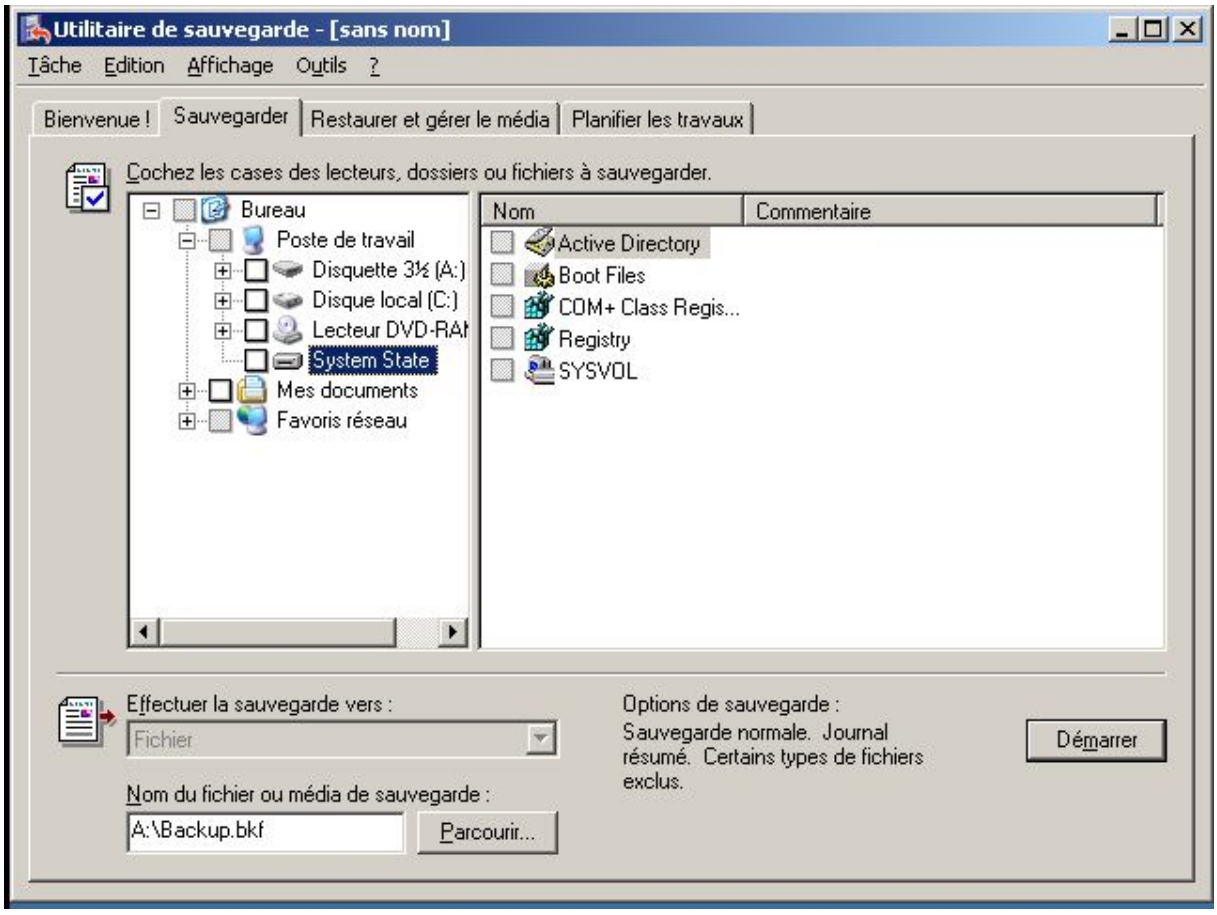
- Faire une sauvegarde de l'Etat du système du DC à migrer.

S'assurer que cette sauvegarde est saine et permet une restauration en cas de besoin. Pour cela on peut faire un test de restauration sur une machine hors réseau.

Pour exécuter cette sauvegarde on pourra utiliser soit une application tierce, soit Ntbackup.

Pour une sauvegarde avec Ntbackup : Menu Démarrer > Exécuter. On tape Ntbackup > Désélectionner la case « Toujours démarrer en mode assistant » > Annuler. Lancer à nouveau Ntbackup


Assistant Sauvegarde ou Restauration
Assistant Sauvegarde ou Restauration
Cet Assistant vous aide à sauvegarder ou restaurer les fichiers et les paramètres de votre ordinateur.
Si vous le préférez, vous pouvez passer en mode avancé pour modifier les paramètres de sauvegarde et de restauration. Ce mode est réservé aux utilisateurs avancés.
Toujours démarrer en mode Assistant
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler


Utilitaire de sauvegarde - [sans nom]
Tâche Edition Affichage Outils ?
Bienvenue ! Sauvegarder Restaurer et gérer le média Planifier les travaux
Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder.
Bureau
Poste de travail
Disquette 3½ (A:)
Disque local (C:)
Lecteur DVD-RAM
System State
Mes documents
Favoris réseau
Nom
Commentaire
Active Directory
Boot Files
COM+ Class Regis...
Registry
SYSVOL
Effectuer la sauvegarde vers :
Fichier
Nom du fichier ou média de sauvegarde :
A:\Backup.bkf
Parcourir...
Options de sauvegarde :
Sauvegarde normale. Journal résumé. Certains types de fichiers exclus.
Démarrer

Dans l'onglet « Sauvegarder »on sélectionne « System state ». On choisir un emplacement puis on lance la sauvegarde.

- Préparer le Schéma en vue de l'installation d'un serveur 2008 R2.

On récupére l'outil « ADPREP » sur le DVD avec les sources 2008 R2. (\Support\Adprep)

Dans le DC 2003 avec le rôle FSMO « Schema Master » on exécute la commande : « Adprep /ForestPrep »

Dans le DC 2003 avec le rôle FSMO « Infrastructure Master » on exécute la commande : «Adprep /domainPrep »

Dans le DC 2003 avec le rôle FSMO « Infrastructure Master » on exécute la commande : « Adprep /domainPrep /Gpprep» Si on souhaite installer ultérieurement un Contrôleur de domaine en lecture seule il faut aussi modifier le « Schéma » : avec la commande : « Adprep /RODC Prep» dans le DC avec le rôle FSMO « Schema Master ».

Avant de commencer l'intégration des serveurs 2008, on doit s'assurer que les modifications du Schéma ont été répliquées sur tous les DC de la forêt. Ceci est très important à fin d'éviter une éventuelle corruption de l'AD.

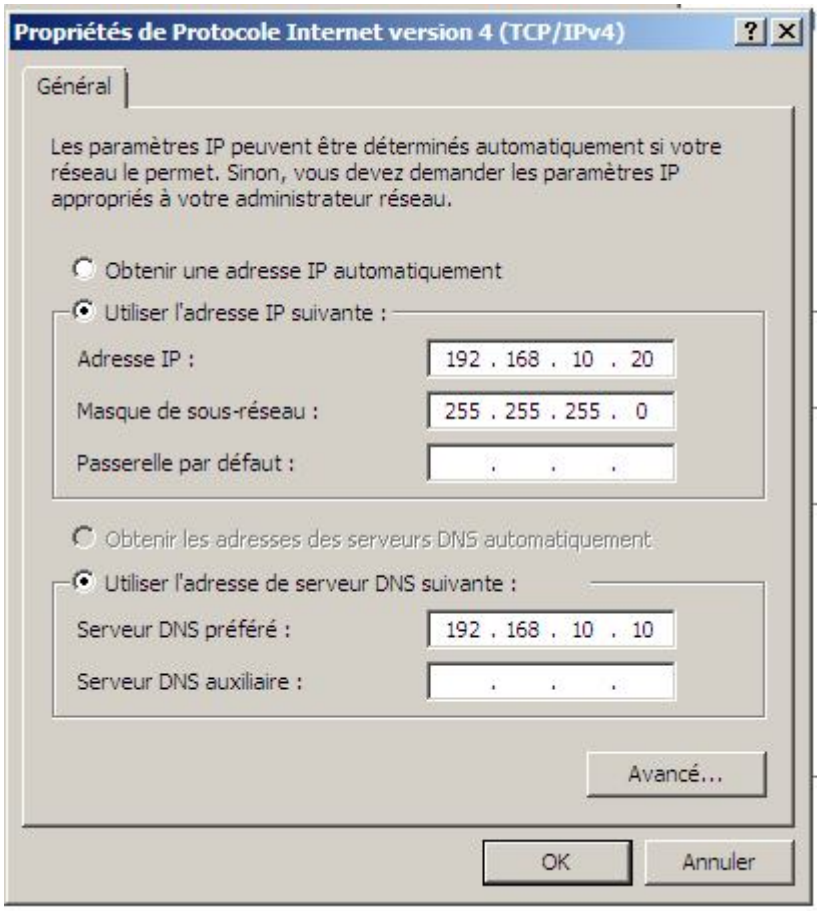
10.2 Préparer le nouveau serveur

- Installation de Windows server 2008 R2 : cela se fait en suivant les mêmes étapes que l'installation du Windows server 2003

Apres l'installation de Windows 2008 Server, on configure les adresses IP

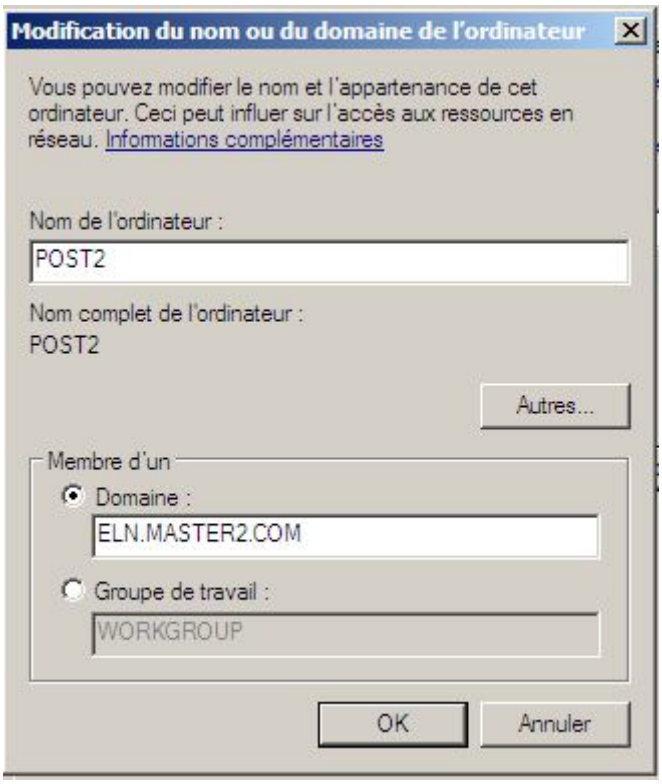
- Vérifier les propriétés des connexions Tcp/Ip.

Il faut une adresse IP fixe. La machine doit être cliente d'un serveur DNS capable de résoudre l'adresse du ou des contrôleurs de domaine où on va l'ajouter.



- On ajoute la machine en tant que serveur membre du domaine.

En mode graphique : Menu démarrer > on clic droit sur « Ordinateur » > Propriétés > Paramètres Système avancés > Nom de l'ordinateur > Modifier.



En ligne de commande : on tape

« Netdom Join « POST2 » /Domain:« ELN.MASTER2.COM » /UserD:Administrateur

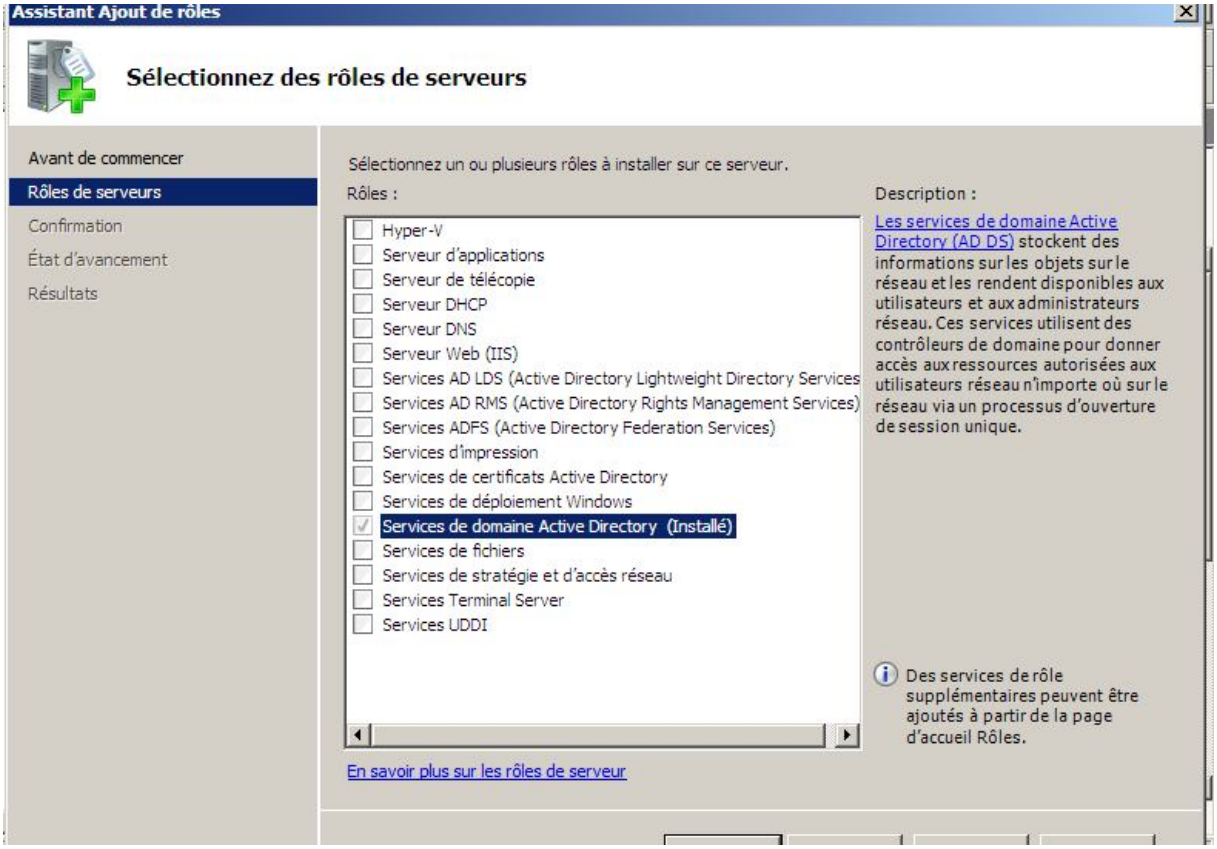
/PasswordD:Le mot de passe administrateur du domaine.

Apres on redémarre la machine.

- On ajoute le rôle serveur DNS

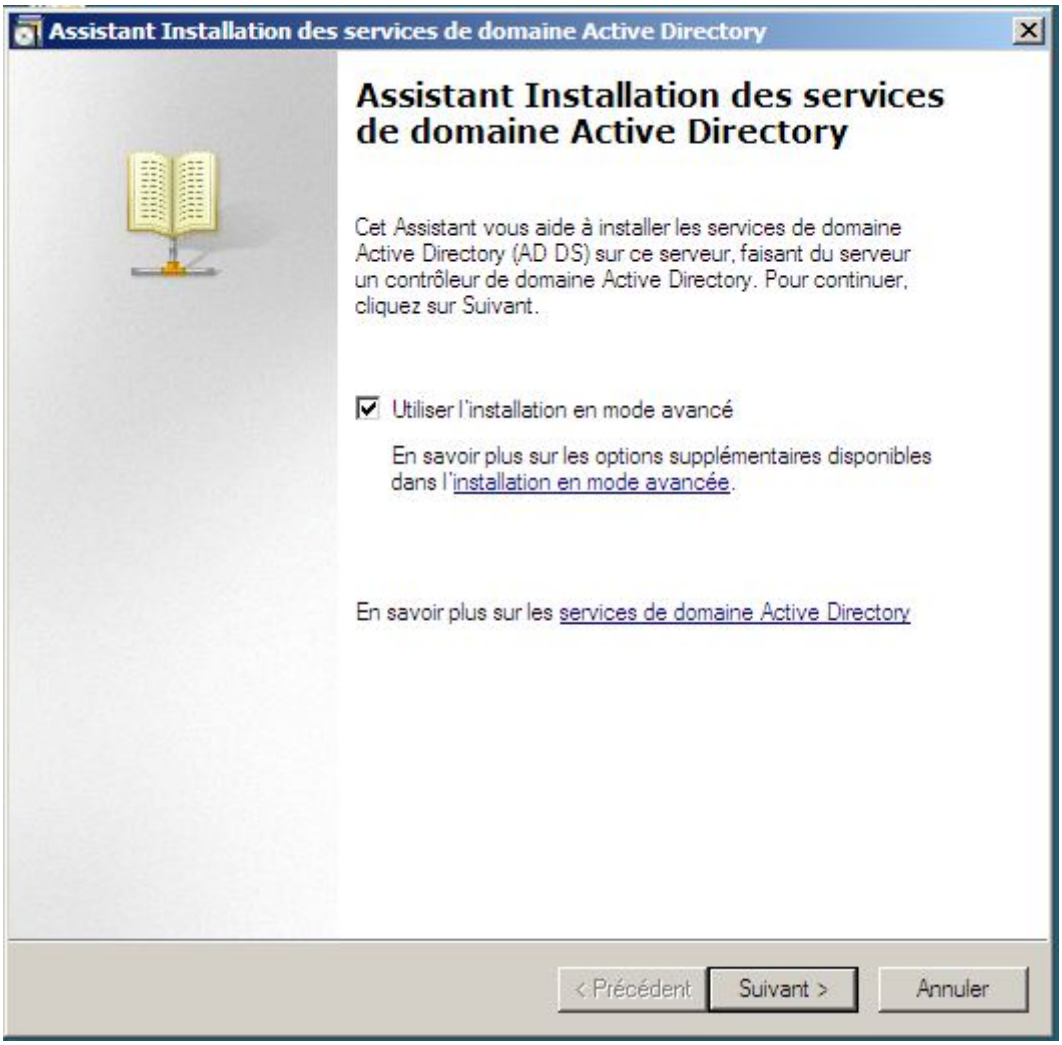
Démarrer > Outils d'administration > Gestionnaire de serveur > Rôles > on ajoute un rôle.

Note : Les rôles DNS et AD doivent être ajoutés séparément

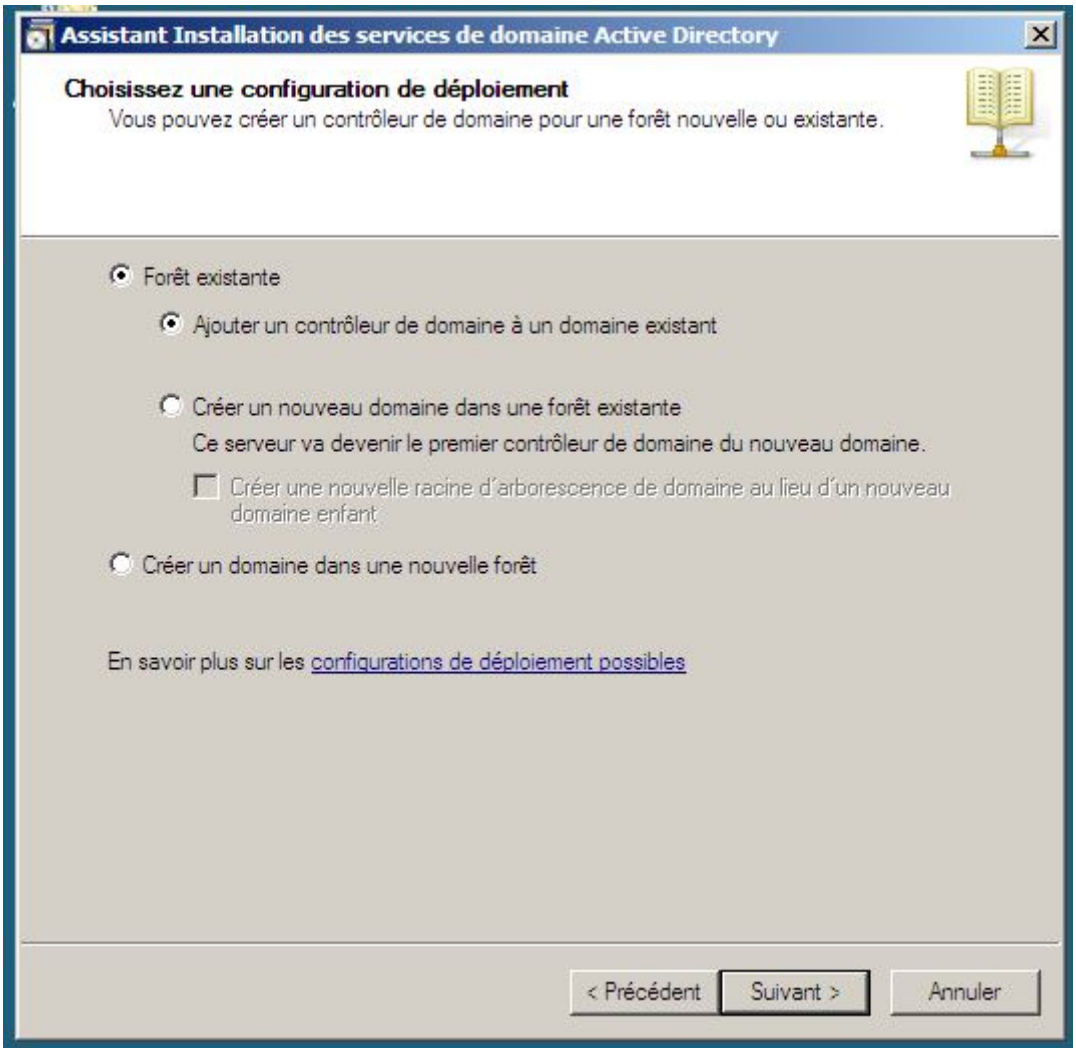


- On ajoute le rôle « Services de domaine Active Directory »
- On installe l'Active Directory avec « DCPROMO »

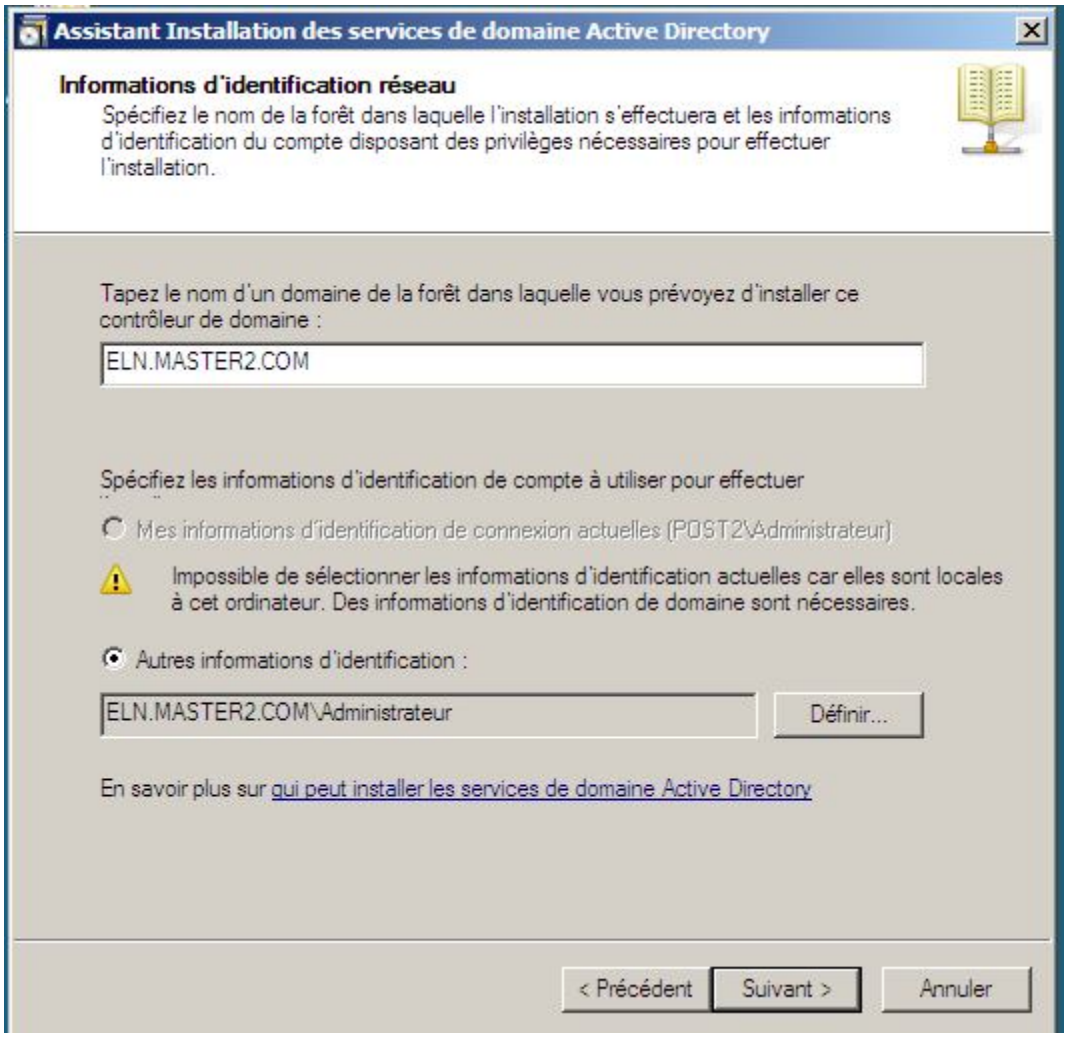
On peut choisir « Utiliser l'installation en mode avancé » pour spécifier certaines options.



On ajoute ce contrôleur de domaine à une forêt existante



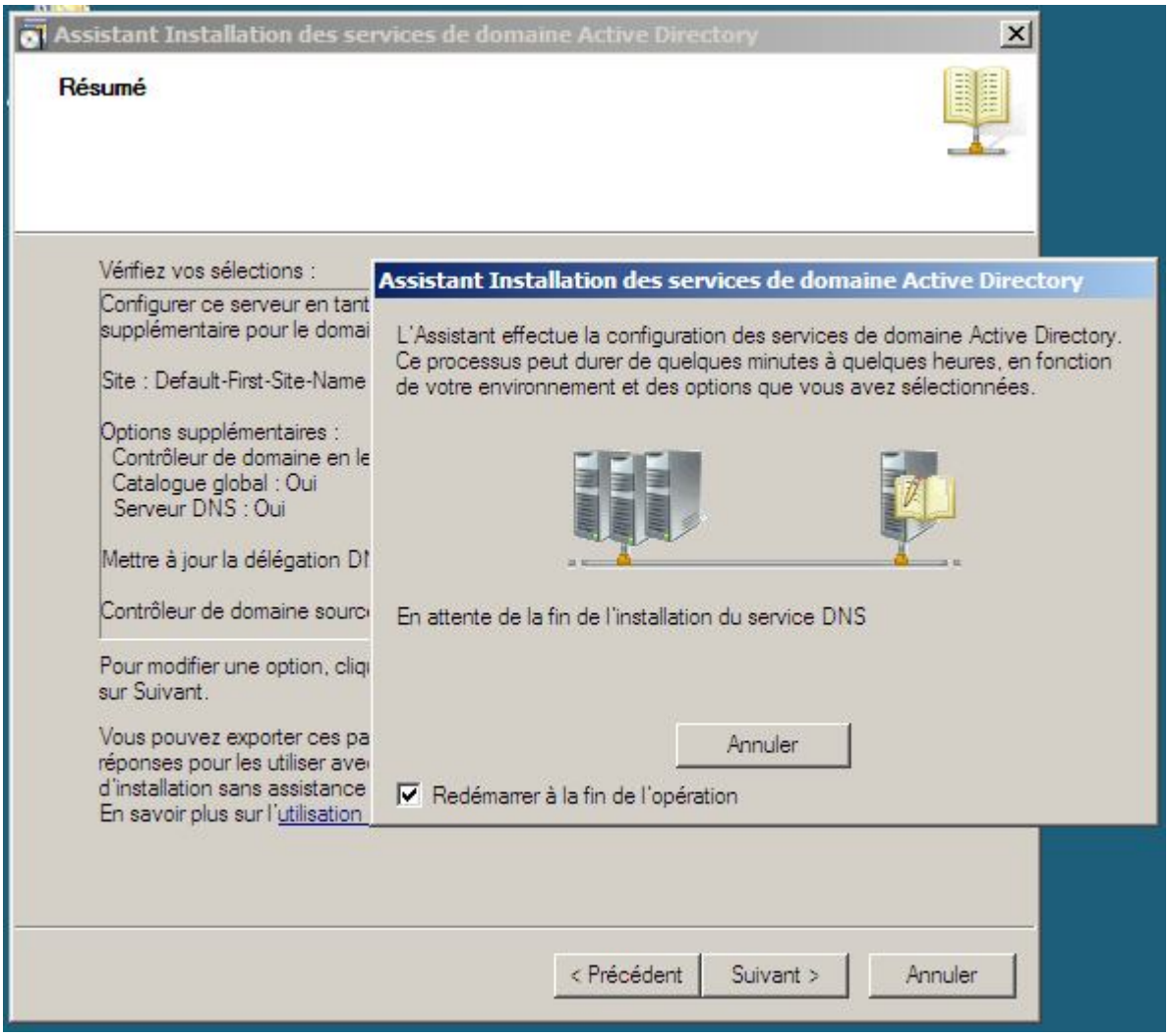
Dans la fenêtre « Informations d'identification réseau », on confirme que le nom du domaine proposé, correspond bien à celui où on veut intégrer le DC. On fournir le nom et le mot de passe d'un compte membre du groupe « Administrateurs du domaine » en cliquant sur le bouton « Définir ».



On accepte les options par défaut dans les pages qui suivent.

Fournir le mot de passe pour le démarrage en mode « Restauration Active Directory»

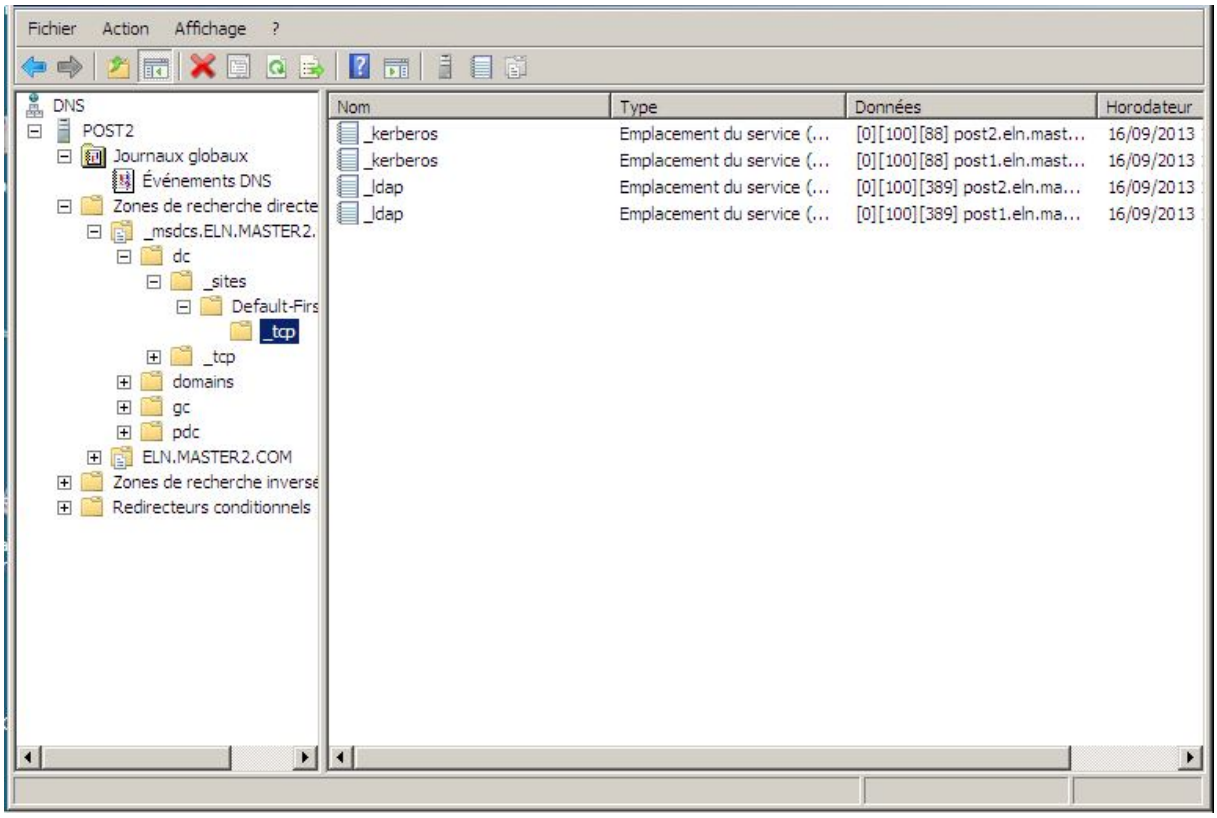
- On termine et redémarre la machine.



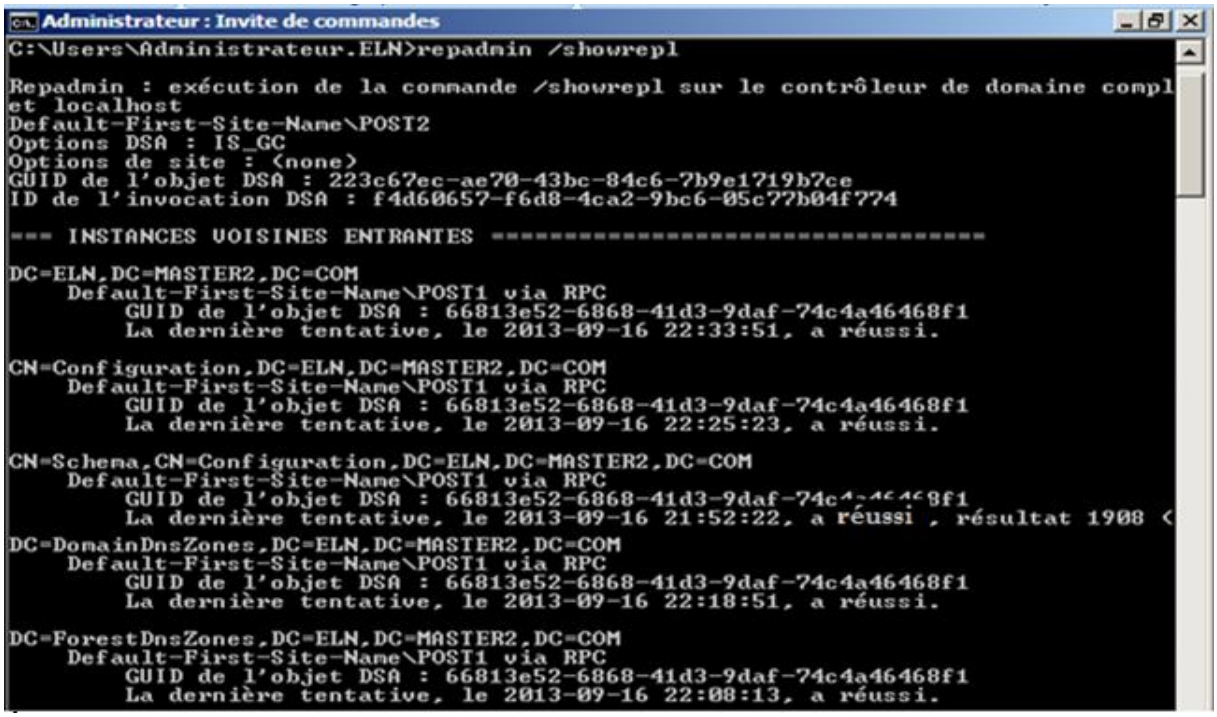
Le nouveau DC est maintenant installé et opérationnel.

11. Tâches «Post migration »

- On vérifie sur le serveur DNS que le nouveau DC a mis à jour ses enregistrements « SRV ».

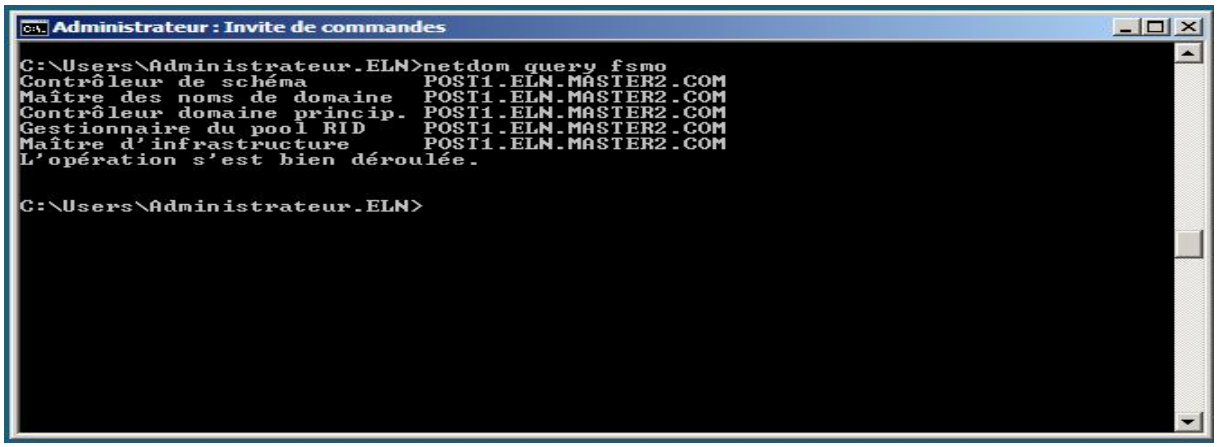


- On confirme que la réplication se déroule bien avec « Repadmin /showrepl



- On transfère les rôles FSMO vers le nouveau DC.

Tout d'abord on doit vérifier quelle est la machine qui héberge les rôles FSMO avec la commande : « Démarrer > Cmd > Netdom query FSMO »



On déplace les rôles FSMO vers le nouveau DC.

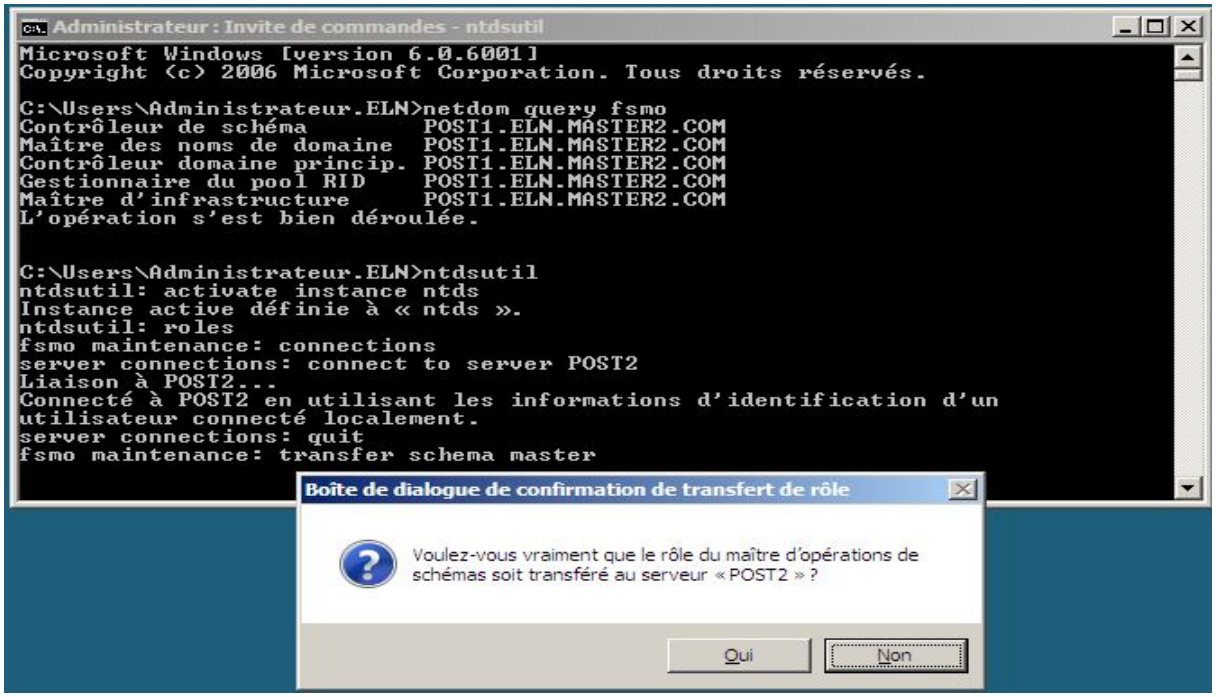
On se positionne dans l'Invite de commandes du nouveau DC.

Menu Démarrer > Exécuter > CMD > on tape la commande Ntdsutil

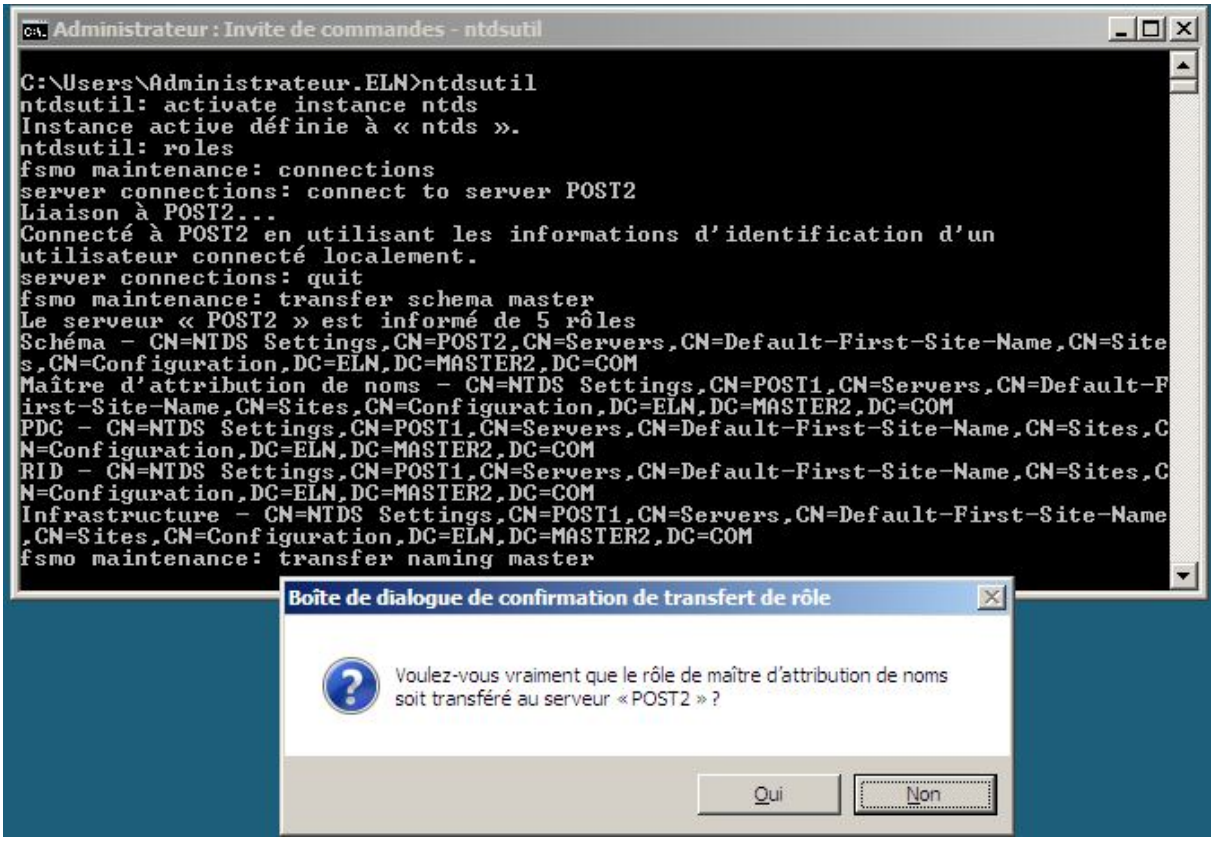
Dans le contexte Ntdsutil on sélectionne l'instance NTDS : avec la commande « Activate instance NTDS »

Ensuite il faut préciser le serveur auquel on veut se connecter : « Connections », dans le contexte « Connections », on tape « Connect to server POST2». Une fois « connecté » on tape « Quit ».

Puis on tape la commande « Transfer Schema Master ». On répète cette opération pour tous les autres rôles FSMO à transférer. (Eventuellement : Naming Master, PDC, RID Master, Infrastructure Master)



On confirme le transfère



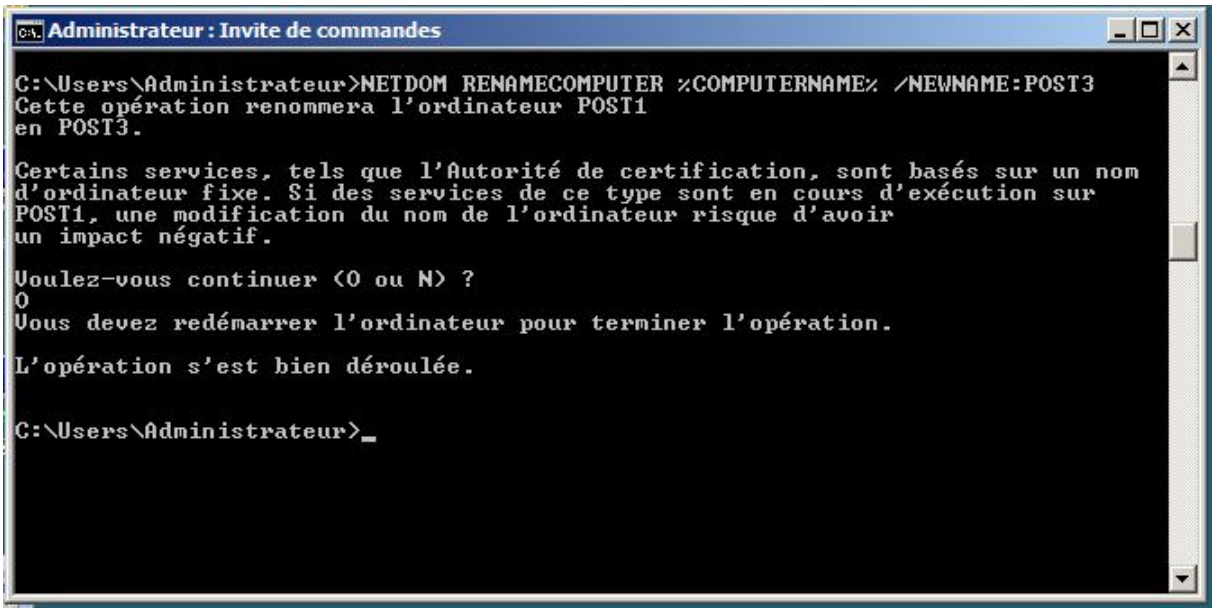
- Confirmer la convergence des serveurs DNS avec le script «DNSconvergeCheck.cmd».

L'exécuter sur le server cible. Se placer avec l'invite de commandes sur le dossier où il a été décompressé. Lancer la commande : « DNSconvergeCheck.cmd (adresse IP du DC source) (adresse IP du DC cible) (Nom du serveur)». Dans notre cas : DNSconvergeCheck.cmd 192.168.10.10 192.168.10.20dc=ELN,dc=MASTER2,dc=com.

- Renommer le nouveau DC avec le nom de l'ancien DC et remplacer son adresse IP.

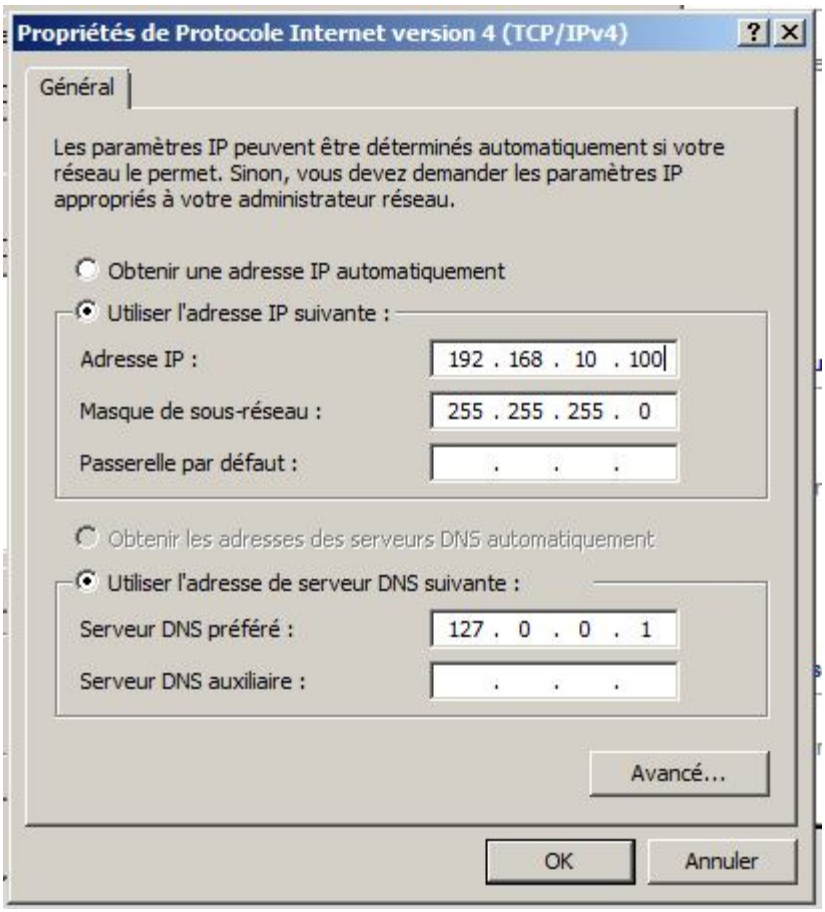
D'abord on doit renommer l'ancien DC :

A l'invite de commandes on tape : Netdom renamecomputer %computername% /Newname:POST3.

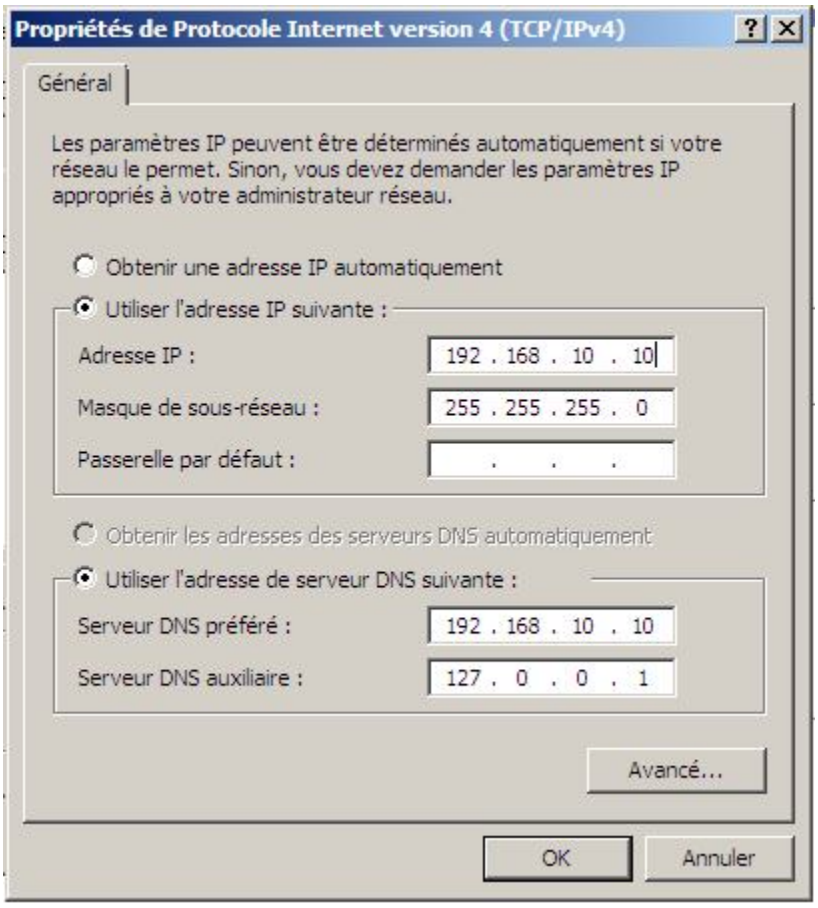


Puis on redémarre le serveur

Changer son adresse IP en 192.168.10.100



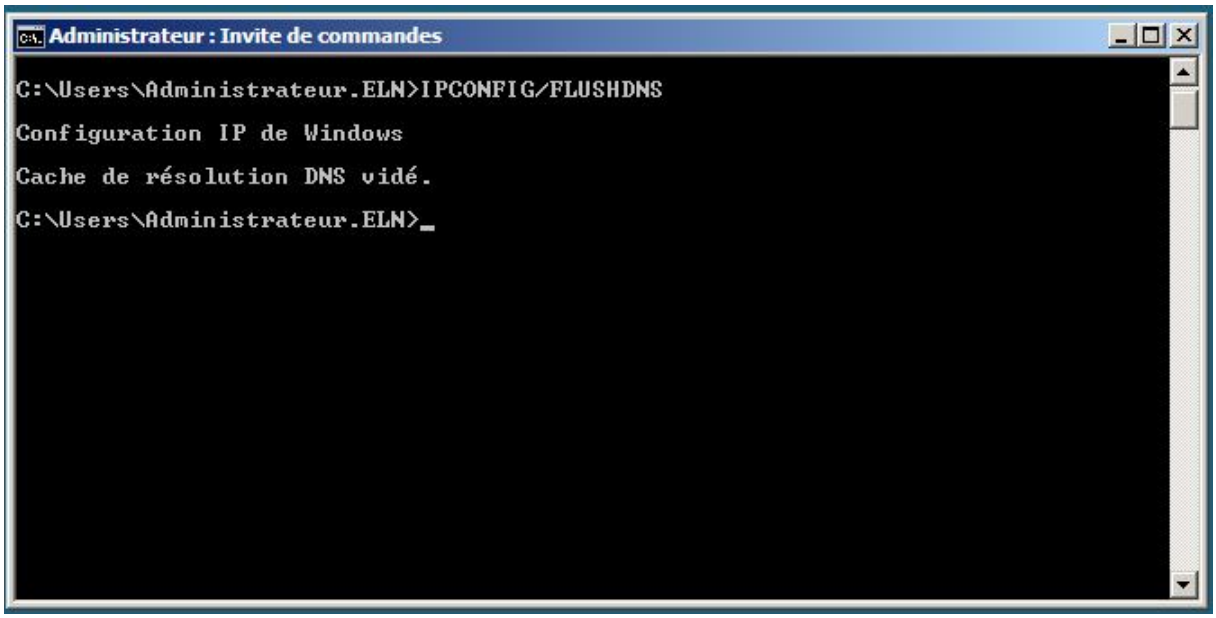
Changer l'adresse IP sur le nouveau DC en192.168.10.10 (l'adresse de l'ancien DC)

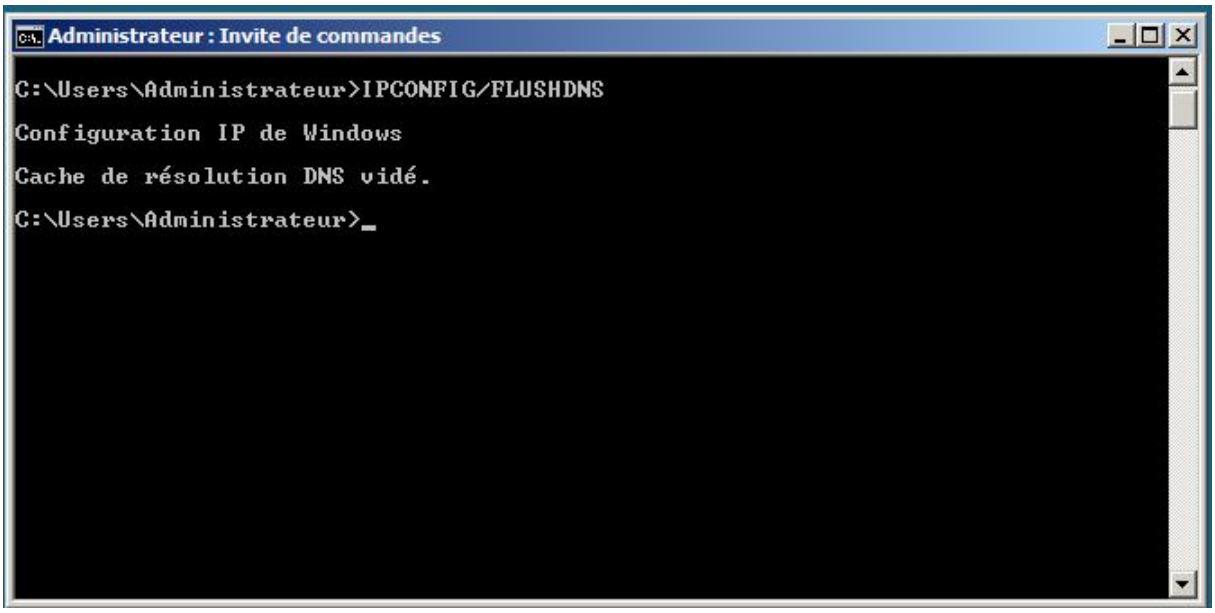


On vérifie que ses adresses ont été enregistrées dans le DNS.

Puis on vide les cache DNS des deux serveurs avec pour que les nouvelles adresses soient mises à jour :

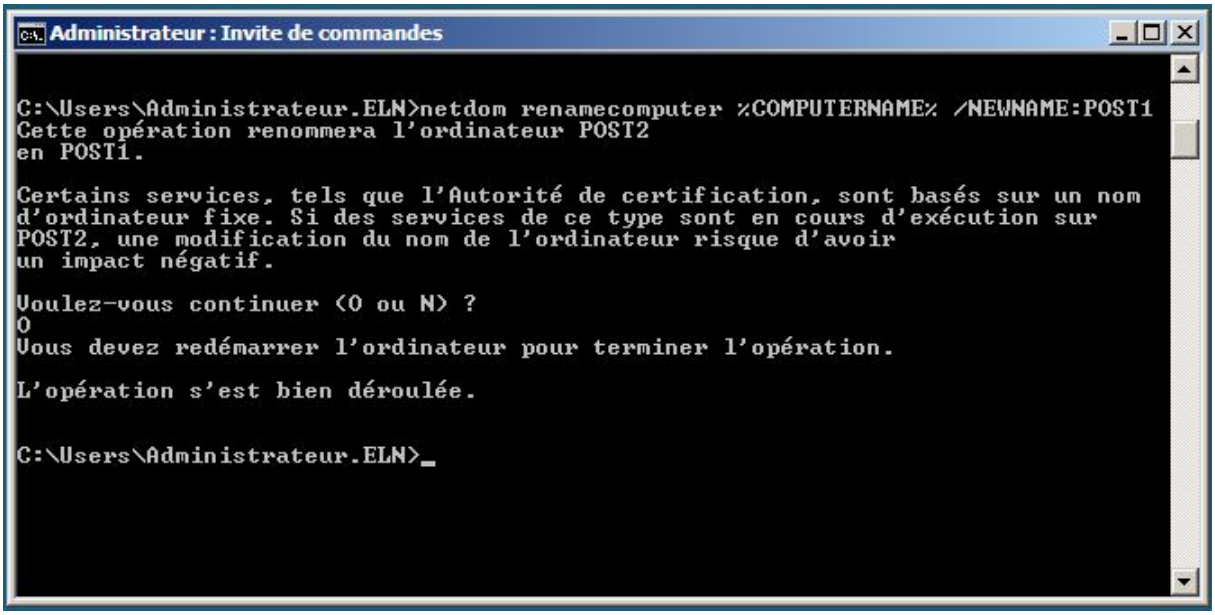
Démarrer > Invite de commandes > Ipconfig /flushdns.





On passe alors à renommer le nouveau DC :

A l'invite de commandes on tape : Netdom renamecomputer %computername%/Newname:POST1 (nom de l'ancien DC).

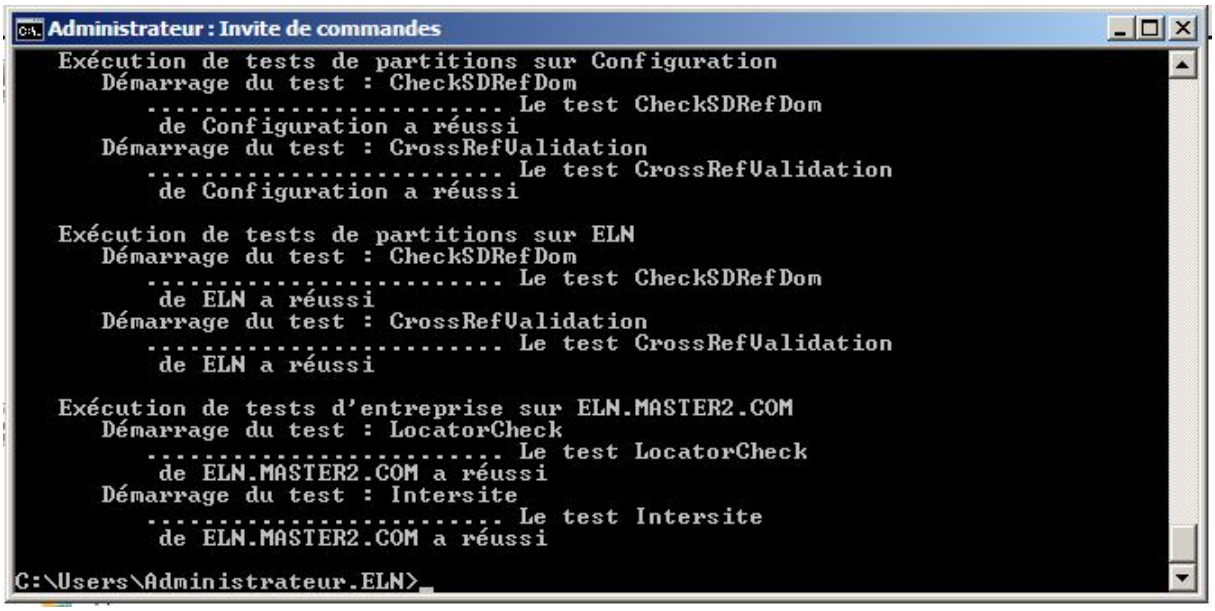


On redémarre le serveur.

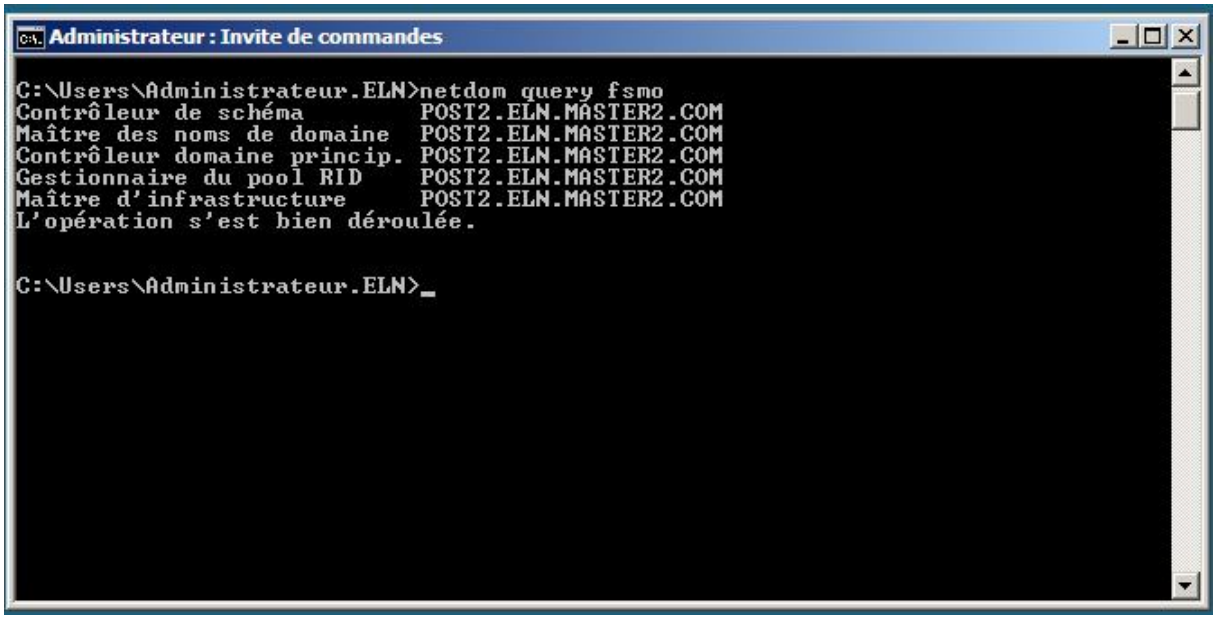
12. Vérifications Post-migration

En utilisant les outils vus plus haut s'assurer qu'il n'y a pas d'erreurs au niveau de l'AD : Dcdiag, Repadmin, Netdom, Ipconfig, etc.

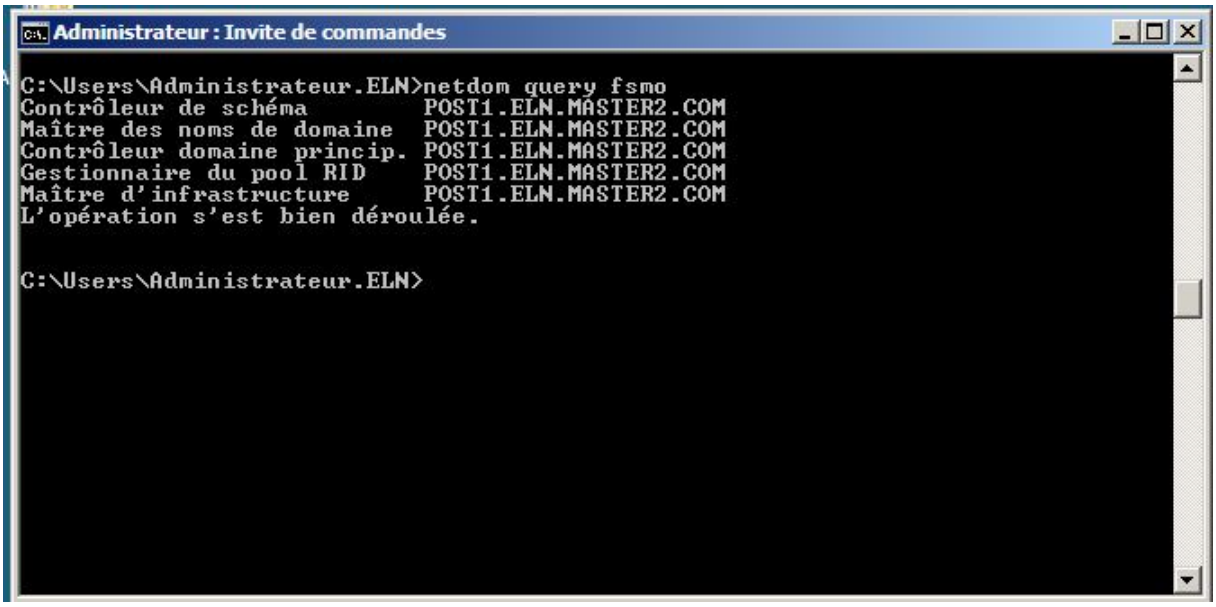
DCDIAG :



Netdom query FSMO avant de chance le nom de server



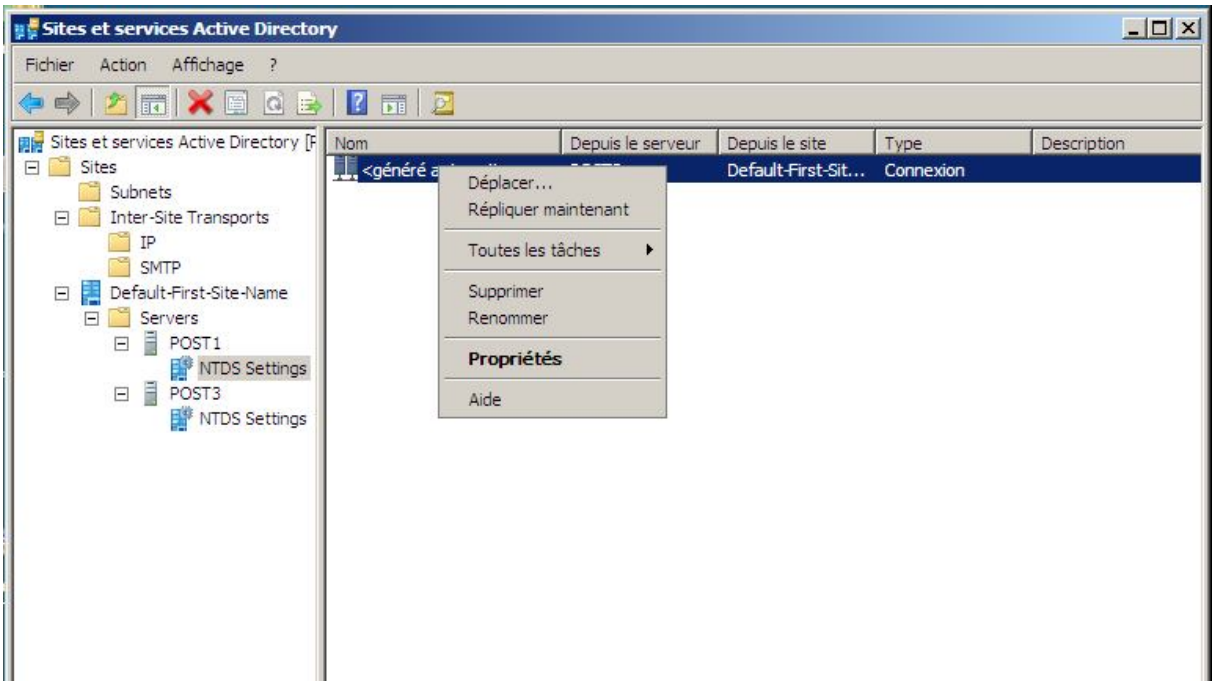
Netdom query FSMO après de chance le nom de server



Ipconfig :

Procéder à une analyse avec le composant « Sites et services » :

Démarrer > Sites et services > Vérifier que les DC se trouvent dans leurs sites respectifs et qu'ils peuvent se répliquer.



13. Supprimer l'ancien DC

On démarre l'ancien DC et on faire un DCPROMO pour le supprimer de l'Active Directory.

14. Conclusion

Le remplacement d'un serveur Windows 2003 par le server Windows 2008 R2 est une opération simple et rapide mais aussi très importante pour profite des nouvelles fonctionnalités et support de Windows server 2008 R2.

La migration d'une version précédente vers Windows Server 2008 R2 ne présente pas des difficultés majeures dés lors que nous avons respecté les principales étapes, à savoir : Faire une analyse très approfondie de son environnement actuel. Analyser aussi en détail, quels sont les réels besoins de l'entreprise qui justifient le passage à la version 2008 R2.En procédant ainsi, on pourra mettre en adéquation, les besoins de l'entreprise et les réponses qui pourront être apportées par cette nouvelle version.

Ensuite, il faut procéder avec minutie, à la préparation de l'environnement source de telle sorte qu'on récupère un environnement sain, nettoyé de tous les objets inutiles. Il est aussi très important de s'assurer de la qualité de ses sauvegardes et de l'entière réplication du Schéma avant de démarrer la migration. Il est préférable de procéder à une restructuration en partant sur un environnement propre et peut être mieux adapté aux besoins actuels de l'entreprise.

Ce projet m'a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il m'a initié au monde de la recherche sur les réseaux. Il m'a également permis de découvrir les nouvelles technologies de Microsoft.

Comme perspective, il est important de faire une étude sur la migration de serveurs de Windows server vers Linux version server.

Conclusion

Mémoires :

[1] M^{elle} YADDADENE Farida et TOUMI Nedjma, Mise en Œuvre d'une infrastructure réseau sécurisée par ISA Server, UMMTO, 2012

[2] M^{elle} YESGUER Fatima, Implémentation d'une politique de sécurité pour une infrastructure réseau d'entreprise, UMMTO, 2013

Site :

[1] http://technet.microsoft.com

[2] http://support.microsoft.com

[3] http : //www.system.it.net

[4] http://mtodorovic.developpez.com/tutorieels/windows/installation-active-directory-server-2008-R2

[5] http : //blogs.technet.com

[6] http : //sociel.technet.microsoft.com

[7] http://fr.wikipedia.org

Livre :

[1] Don HOLME, Nelson RUEST et Danielle RUEST, MCTS 70-640 Configuration d'une infrastructure Active Directory avec Windows Server 2008; Dunod ; 2008

[2] Michael todorovic, installation d'Active Directory sous Windows server 2008 R2; mai 2010.

BIBLIOGRAPHIE

Glossaire

A

AD Active Directory

ADDS Active Directory Domain Service

ADCS Active Directory Certificate Service

ADFS Active Directory Federation Service

ADLDS Active Directory Lightweight Directory Service

ADRMS Active Directory Rights management Service

B

BPA Analyseurs de Bonnes Pratique

D

DACL Discretionary Access Control List

DEP Data Execution Prevention

DFS Replication Distributed File System

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

F

FTP File Transport Protocol

FSMO Flexible Single Operation

G

GPO Group Policies Object

I

IAG Intelligent Application Gateway

IP Internet Protocol

IIS Internet Information Services

K

KDC Key Distribution Center (Centre de Distribution de clés)

L

LAN Local Area Network

LDAP Light weight Directory Access Protocol

N

NAP Network Access Protection

NTFRS New Technology File Service Replication

NT New Technology

Glossaire

NIDS Network Based Intrusion Detection System

NSPI Name Service Provider Interface

O

OU Organization Unit

P

PDC Primary Domain Controller

R

RODC Read Only Domain Controller

RMS Right Management Server

S

SNP Scalable Networking Pack

T

TCP Transfer Control Protocol

V

VPN Les réseaux privés virtuels

GLOSSAIRE

Résumé :

Windows Server est aujourd'hui au cœur de l'informatique des entreprises. Déployé massivement dans les PME comme dans les grandes entreprises

Pour continuer à bénéficier d'un support optimal, il est recommandé la migration vers Windows Server 2008 R2, qui permettra de continuer à profiter de l'étendue complète de services de support, tout en bénéficiant de considérables améliorations fonctionnelles comme le support de la virtualisation de serveurs, les nouvelles fonctions d'administration ou de virtualisation d'applications et de postes de travail, mais aussi de performances significativement en hausse.

La migration d'une version précédente vers Windows Server 2008 R2 ne présente pas des difficultés majeures dés lors que nous avons respecté les principales étapes, à savoir : Faire une analyse très approfondie de son environnement actuel. Analyser aussi en détail, quels sont les réels besoins de l'entreprise qui justifient le passage à la version 2008 R2.En procédant ainsi, on pourra mettre en adéquation, les besoins de l'entreprise et les réponses qui pourront être apportées par cette nouvelle version.

Ensuite, il faut procéder avec minutie, à la préparation de l'environnement source de telle sorte qu'on récupère un environnement sain, nettoyé de tous les objets inutiles. Il est aussi très important de s'assurer de la qualité de ses sauvegardes et de l'entière réplication du Schéma avant de démarrer la migration. Il est préférable de procéder à une restructuration en partant sur un environnement propre et peut être mieux adapté aux besoins actuels de l'entreprise.

Mots clés : La migration, Windows Server, la virtualisation, Active Directory ,service d'annuaire, la version