Installation d'Active Directory sous Windows Server 2008 R2

par Michaël Todorovic (Autres articles) (Blog)

Date de publication : 3 mai 2010

Dernière mise à jour :

Cet article va vous permettre d'acquérir des bases d'Active Directory, notamment sur l'aspect du nommage et donc du DNS.

I - Introduction

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.

La conception de votre Active Directory est très importante. Toute erreur de conception pourra avoir des conséquences plus ou moins importantes selon l'évolution des besoins de votre entreprise. Par exemple, un mauvais choix de nom pour votre Active Directory peut amener jusqu'à une migration forcée. Je vais exposer les bases d'une conception pérenne.

Il est nécessaire d'avoir des connaissances dans les réseaux IP (adressage, masque, CIDR), de savoir ce qu'est un port TCP ou encore de connaitre de manière globale le principe du DNS.

II - Les bases

II-A - Les composants

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 vous permettre de générer des certificats de sécurité pour vos utilisateurs et votre réseau. J'ai écrit plusieurs articles sur ce sujet, le principal étant **Configuration d'une infrastructure à clés publiques à 2 niveaux sous Windows 2008 (R2)**.
- ADFS : Active Directory Federation Services. Il s'agit du composant permettant la fédération de services entre différents environnements Active Directory. Cela va vous permettre d'établir des relations de confiance avec des partenaires externes à votre entreprise (fournisseurs, fabricants, etc.) afin de leur donner un accès à certains de vos 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 vous avez 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 votre Active Directory. Attention, ADDS n'utilise pas ADLDS, c'est un composant à part entière.
- ADRMS : Active Directory Rights Management Services. Ce composant permet de gérer les droits de manière pointue dans votre entreprise. Il ne s'agit pas des droits sur le fichier mais sur le contenu du fichier. Vous pouvez dire sur un document Word qu'il ne peut pas être imprimé, transféré par e-mail, etc.

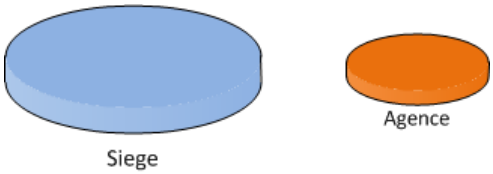
Ce tutoriel traite de l'installation d'ADDS.

II-B - Sites et domaines

Dans Active Directory, il existe un certain nombre de types d'objets et de concepts que je vais expliquer ici. Commençons par les sites et domaines.

Dans la conception d'Active Directory, Microsoft a tenté d'être le plus proche possible de la structure d'une entreprise. La structure d'une entreprise se compose en deux parties distinctes : physique et logique. Physique par son organisation géographique en différents sites et logique par sa hiérarchie. Il est important de garder cela à l'esprit.

Un site désigne la combinaison d'un ou plusieurs sous-réseaux IP. Bien souvent, on attribue un sous-réseau IP à un site physique d'une entreprise. Cela permet de distinguer les postes sur le réseau de l'entreprise. En créant des sites Active Directory, les ordinateurs sauront qu'ils font partie de tel ou tel site. Cela est très important dans une configuration multisites du même domaine Active Directory. Si un contrôleur de domaine fait partie du site Agence et qu'un ordinateur du site Agence a besoin d'un accès à Active Directory, alors il n'aura pas besoin de contacter le site Siege : il ira directement voir le serveur de l'agence. Si le serveur de l'agence est en panne alors il pourra aller voir le serveur du siège en utilisant des liens WAN. Les sites sont généralement symbolisés par des ovales ou des camemberts. Voici la représentation des sites mentionnés précédemment. Le lien WAN n'est pas représenté.



Représentation des sites

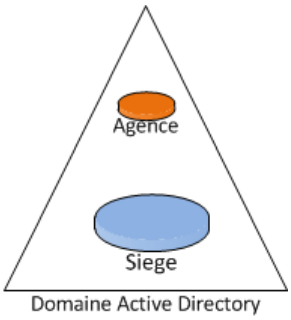
Un domaine, contrairement à un site, mappe la structure logique de l'organisation. C'est-à-dire bien souvent la hiérarchie. Le domaine n'a aucun lien avec le réseau IP : c'est un ensemble d'ordinateurs et d'utilisateurs partageant le même annuaire. Un domaine porte un nom : nous le verrons plus loin, il est très important de bien le choisir. L'espace de nommage est réalisé grâce au système DNS. Un domaine peut avoir plusieurs sous-domaines : on crée ainsi une arborescence. Le séparateur est le point. Si l'on souhaite créer un sous-domaine *corp* dans un domaine existant *developpez.adds*, alors le domaine se nommera corp.developpez.adds.

Chaque domaine doit être géré par au moins un serveur distinct. Cela veut dire qu'un serveur Active Directory ne peut pas gérer plusieurs domaines Active Directory. Si vous voulez un domaine et un sous-domaine, il vous faudra deux serveurs Active Directory distincts. Un domaine peut être géré par plusieurs serveurs Active Directory : cela permet de répartir les cinq rôles FSMO (Flexible Single Master Operation).

Bien qu'il soit possible de créer plusieurs domaines et sous-domaines, il est conseillé d'être le plus possible proche de la configuration idéale : une configuration mono-domaine. Il est très simple de créer des domaines à tour de bras. Cependant, créer des domaines multiplie la charge administrative par le nombre de domaines créés. La création d'un domaine supplémentaire doit être justifiée dans la mesure où elle va fortement impacter votre charge de travail. Voici des justifications possibles :

- la délégation de l'administration d'Active Directory ne convient pas dans votre organisation (pour des raisons principalement politiques) ;
- la sécurité des données de votre domaine, par exemple, lors de l'utilisation de serveurs BlackBerry ;
- etc.

Un domaine est généralement représenté par un triangle.



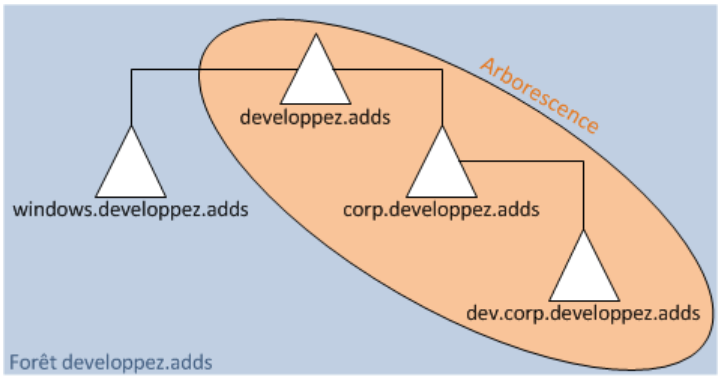
Représentation d'un domaine

Ce qu'il faut retenir, c'est qu'un domaine peut être sur plusieurs sites mais qu'un site (au sens Active Directory) ne peut pas avoir plusieurs domaines. Un site mappe la structure physique alors que le domaine mappe la structure logique de l'organisation.

II-C - Arborescences et forêts

Une arborescence est une notion qui découle du système DNS et des domaines Active Directory. Comme nous l'avons vu précédemment, il est possible de créer des domaines dans des domaines. Cette création se fait dans un espace de nommage contigu : le sous-domaine *corp* fait partie du domaine *developpez.adds* et portera donc le nom *corp.developpez.adds*. Cette notion d'arborescence est différente de celle de forêt. Une forêt peut comprendre plusieurs arborescences. La forêt developpez.adds présentée ci-dessous comporte quatre arborescences :

- de developpez.adds à windows.developpez.adds ;
- de developpez.adds à dev.corp.developpez.adds ;
- de developpez.adds à corp.developpez.adds ;
- de corp.developpez.com à dev.corp.developpez.adds.



Forêt et arborescence

Les arborescences d'une même forêt peuvent partager des ressources et des fonctions administratives. Comme pour les domaines, il est conseillé d'être, le plus possible dans la configuration idéale, c'est-à-dire en mono-forêt. La configuration idéale est donc un Active Directory mono-domaine mono-forêt.

II-D - Niveau fonctionnel de forêt et de domaine : différentes fonctionnalités

Active Directory est un produit en évolution depuis sa création. Afin de conserver des niveaux de compatibilité entre les différentes versions de Windows et des produits s'implantant dans Active Directory (Exchange, MOM, SCCM, etc.), il a été introduit la notion de niveau de forêt et de domaine. Il existe actuellement plusieurs niveaux de forêt et de domaine :

- Windows 2000 mixte ;
- Windows 2000 natif ;

- Windows 2003 ;
- Windows 2003 R2 ;
- Windows 2008 ;
- Windows 2008 R2.

Pour augmenter le niveau fonctionnel d'une forêt, il faut que tous les domaines soient au minimum de ce niveau fonctionnel. Un niveau fonctionnel impose que tous les contrôleurs de domaine soient capables de gérer ce niveau fonctionnel. Par exemple, pour avoir un niveau fonctionnel Windows 2008, il faut que tous les contrôleurs de domaine soient en Windows 2008. Il est possible d'avoir des contrôleurs de domaine de version supérieure dans un domaine de niveau inférieur : on peut avoir un niveau fonctionnel Windows 2003 avec des contrôleurs de domaine Windows 2003 et Windows 2008.

Je ne vais pas faire le comparatif des niveaux fonctionnels, je vous propose donc de consulter la page suivante : **Présentation des niveaux fonctionnels des services de domaine Active Directory**.

*Jusqu'en Windows 2008, il n'était pas possible de baisser le niveau fonctionnel d'un domaine ou d'une forêt. Depuis Windows Server 2008 R2, cela est possible. Je vous invite à consulter ceci : **Baisser le niveau fonctionnel d'une forêt sous 2008R2**. C'est maintenant possible mais je conseille d'éviter le plus possible d'utiliser cette fonctionnalité. En effet, cela peut avoir des effets de bord qui seront difficilement récupérables. Réfléchissez bien avant d'élever votre niveau fonctionnel, cela vous évitera une perte de temps considérable.*

II-E - Utilisateurs et ordinateurs

Chaque utilisateur dans Active Directory est associé à un objet. Cet objet contient plusieurs attributs qui décrivent l'utilisateur (nom, prénoms, login, adresse e-mail, téléphone, département, etc.). Ces attributs peuvent permettre de trouver des utilisateurs dans votre domaine. Ils peuvent par exemple être utilisés dans Exchange pour constituer des listes dynamiques de distribution d'e-mails. Ces utilisateurs peuvent se voir attribuer des autorisations sur d'autres objets de votre Active Directory. Lorsque vous commencerez à avoir plusieurs utilisateurs, vous pourrez les gérer par groupe.

Les ordinateurs disposent également de comptes spécifiques dans Active Directory. Ces comptes existent pour gérer la sécurité pour les accès à certaines ressources comme les stratégies de groupe, les logins, l'accès au réseau (avec **NAP** par exemple). Vous pourrez également gérer les ordinateurs par groupe.

II-F - Groupes

Il existe deux types de groupes. Le premier et le plus courant est le groupe de sécurité. Ce type permet de gérer la sécurité pour l'accès et l'utilisation des ressources de votre réseau. Le deuxième type est le groupe de distribution. Ce type permet simplement de gérer des listes de distribution d'e-mails dans un serveur de messagerie.

Pour ces groupes, il existe trois étendues :

- Domaine local : vous pourrez y ajouter des comptes de n'importe quel domaine et/ou des groupes "Domaine local" du même domaine et/ou des groupes universels/globaux de n'importe quel domaine. Les autorisations portent uniquement sur le domaine auquel le groupe appartient ;
- Globale : vous pourrez y ajouter des comptes du domaine d'appartenance et/ou des groupes globaux du domaine d'appartenance. Les autorisations peuvent être accordées dans n'importe quel domaine ;
- Universelle : vous pourrez y ajouter des comptes de n'importe quel domaine et/ou des groupes globaux et universels de n'importe quel domaine. Les autorisations pour cette étendue portent sur tout le contenu de la forêt.

II-G - 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 multisites. 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.

Je ne vais pas développer la configuration d'un RODC dans ce tutoriel. Je vous propose donc la page Technet **Read-Only Domain Controller Planning and Deployment Guide**.

II-H - DNS

Voici la partie la plus importante d'Active Directory. Le DNS est la base d'Active Directory : comme dans un château de cartes, retirez le DNS et votre architecture Active Directory s'écroule. C'est grâce au DNS que vos clients (postes utilisateurs ou serveurs membres du domaine) vont pouvoir trouver le ou les serveur(s) Active Directory.

Pour trouver le serveur Active Directory, les clients vont demander au DNS l'enregistrement de type SRV ayant pour nom _ldap._tcp.developpez.adds (où developpez.adds est votre nom de domaine). Cet enregistrement SRV contient le nom du serveur qui possède l'annuaire ainsi que le port TCP à utiliser pour accéder à ce serveur en LDAP. Par défaut, ce port est le 389 pour les communications non cryptées. Une requête DNS supplémentaire sera effectuée pour connaitre l'IP du serveur en question. Une fois que le client saura quel serveur contacter, il pourra avoir accès (à condition d'avoir des identifiants) aux différentes ressources proposées grâce à Active Directory : partage de fichiers et d'imprimantes, messagerie, etc. Il est dont vital pour votre architecture d'avoir un service DNS qui fonctionne correctement. Généralement, on va utiliser le serveur DNS fourni avec Windows Server et la plupart du temps, placer le serveur DNS sur le serveur Active Directory. Il est possible d'utiliser des serveurs différents du type Bind9 sous Linux. Cependant, cela requiert une certaine configuration, notamment pour la réplication des informations entre serveurs : celle-ci ne sera plus gérée par Active Directory mais par votre serveur DNS.

Avoir un service DNS fonctionnel est très important mais le choix du nom de votre forêt et domaine racine l'est encore plus. Voyons comment le choisir correctement.

III - Choisir correctement le nom de votre Active Directory

Pourquoi une partie dédiée au nommage de votre Active Directory ? *"Mais c'est pourtant simple, je prends n'importe quel nom DNS et ça va marcher !"*. C'est vrai qu'en prenant n'importe quel nom DNS non utilisé sur votre réseau, ça va marcher... jusqu'à une certaine limite. La limite n'est pas bien loin : dès que vous voudrez donner accès depuis Internet à un service de votre entreprise, ça risque de poser problème. Cela posera également problème aux postes Linux (uniquement ceux qui fonctionnent avec mDNS) et Apple.

Le service Bonjour peut être installé sur Windows par iTunes ou encore Acrobat Reader. Cependant, le service n'est pas utilisé comme client DNS principal : c'est celui de Windows qui est toujours utilisé. Sur Mac, le service Bonjour est utilisé comme client DNS principal d'où le problème.

Alors quelles sont les règles à respecter pour bien nommer votre domaine ?

Pour commencer, vous ne devez pas utiliser un **TLD** nommé .local. Ce TLD pose problème aux postes Apple à cause du service **Bonjour** et aux postes Linux fonctionnant avec Zeroconf ou mDNS. Ce service réserve le

TLD .local à la machine locale : tous les noms de domaine finissant par .local sont équivalent à localhost donc aucune requête à destination d'un domaine en .local ne sortira de la machine. Ainsi, un poste Apple ne pourra jamais contacter votre Active Directory.

Le nom de domaine choisi ne doit pas exister sur Internet : en effet, vos postes internes pourraient aller consulter les DNS d'Internet pour accéder à votre Active Directory. Ce n'est pas souhaitable. Vous pouvez acheter le nom de domaine pour être certain qu'il vous appartienne. Cependant, je vous déconseille d'utiliser un nom public mais il existe deux "écoles".

La première consiste à utiliser un nom de domaine public (mais que vous possédez !). Vous n'avez qu'une zone à gérer dans votre Active Directory pour l'accès interne de votre entreprise et une zone publique pour les services que vous pouvez proposer sur Internet comme un site web (commercial, webmail, etc.) ou d'autres services comme la messagerie électronique (SMTP principalement). Cette méthode est simple. Cependant, selon la dimension de votre réseau, votre zone interne sera plus ou moins remplie.

Si vous avez cinq postes et deux serveurs, la zone sera simple à gérer. Vous saurez quel enregistrement est publié pour vos collaborateurs : par exemple, vous saurez que l'enregistrement webmail pointe sur votre serveur de messagerie. Vous avez également créé cet enregistrement dans votre DNS externe pour que l'on puisse accéder au webmail depuis n'importe où. Bref, c'est assez simple de s'y retrouver. La situation est différente quand vous avez plus de postes. La zone devient difficile à gérer et vous ne retrouverez pas simplement les serveurs publiés. Personnellement, je n'aime pas cette méthode de nom public pour Active Directory. Je préfère la méthode suivante qui peut paraitre plus compliquée mais qui permet de bien différencier ce que l'on fait.

Cette deuxième méthode se nomme le split-dns (principe expliqué **ici**). Dans ce cas, on ne va pas utiliser un nom de domaine public mais un nom de domaine privé. Pour qu'il soit privé, il ne faut pas que le TLD choisi fasse partie de cette **liste**. Je déconseille d'utiliser des TLD courts (sur deux lettres) puisqu'ils risquent d'être ouverts un jour. Personnellement, j'utilise des TLD du genre ".adds" : cela n'est pas un mot, c'est assez long et relativement "insignifiant" pour qu'il soit ouvert au public un jour. Le nom de domaine doit être le plus passe-partout possible : aucune entreprise n'est à l'abri d'un rachat, d'une alliance avec une autre entreprise qui mènerait à un changement de nom ou simplement d'un changement de nom pour des raisons marketing. Vous pouvez tout à fait prendre le nom de votre entreprise comme nom de domaine mais en cas de changement de nom de l'entreprise, on pourra vous demander de supprimer toute référence à l'ancien nom (ça fait partie des aspects "corporate"). C'est une opération qui n'est pas faisable en trois minutes ou en deux clics. Cela se planifie et ça prend plusieurs mois. Renseignez-vous auprès des directions pour savoir si vous êtes susceptibles de changer de nom, si oui prévenez-les que ça prendra plusieurs mois s'il faut changer le nom de l'AD et essayez de savoir si un nom générique leur convient. Par nom générique, j'entends un nom qui ne pourra pas changer comme la ville où est implantée l'entreprise, la région, etc. C'est la situation idéale. Cependant, dans le cadre d'un rachat ou d'une fusion, les politiques dans les DSI peuvent différer et donc changer votre politique de nommage. Dans ce tutoriel, j'ai choisi le domaine racine de forêt todorovic.adds.

Je reviens rapidement sur le split-dns. J'ai installé mon domaine Active Directory todorovic.adds et je possède le domaine todorovic.fr. Je veux mettre à disposition des services sur Internet. Je vais prendre l'exemple d'un webmail installé dans mes locaux sur un serveur nommé exchange. Ce serveur est disponible sur Internet grâce à une publication dans un reverse-proxy ou simplement un PAT (dangereux). Dans mon dns externe (disponible sur Internet), j'ai créé un enregistrement webmail. Je peux donc accéder à mon webmail via webmail.todorovic.fr. En interne, je souhaite accéder au webmail. Je peux donc y aller avec exchange.todorovic.adds ou si un alias a été créé avec webmail.todorovic.adds. J'arriverai directement sur le serveur de messagerie interne sans passer par Internet. C'est un comportement normal : il n'y a aucune raison d'aller sur Internet pour revenir en interne. Cela ajoute une charge sur le routeur/firewall de votre entreprise alors que c'est tout à fait inutile. Cependant, pour l'utilisateur, ça n'est pas très pratique : il faut retenir deux adresses et utiliser la bonne selon qu'il est à l'intérieur ou à l'extérieur de l'entreprise. On a donc créé une deuxième zone sur le dns interne nommée todorovic.fr. Dans cette zone, on a créé un enregistrement webmail pointant vers le serveur de messagerie interne. Ainsi, les utilisateurs, où qu'ils soient, accéderont au webmail via webmail.todorovic.fr. Ce besoin de split-dns est encore plus fort lorsque vous êtes en situation de mobilité avec Outlook Anywhere ou Office Communicator.

Maintenant que vous avez les éléments pour bien sélectionner votre nom de domaine, passons à l'installation d'Active Directory.

IV - Installation d'Active Directory

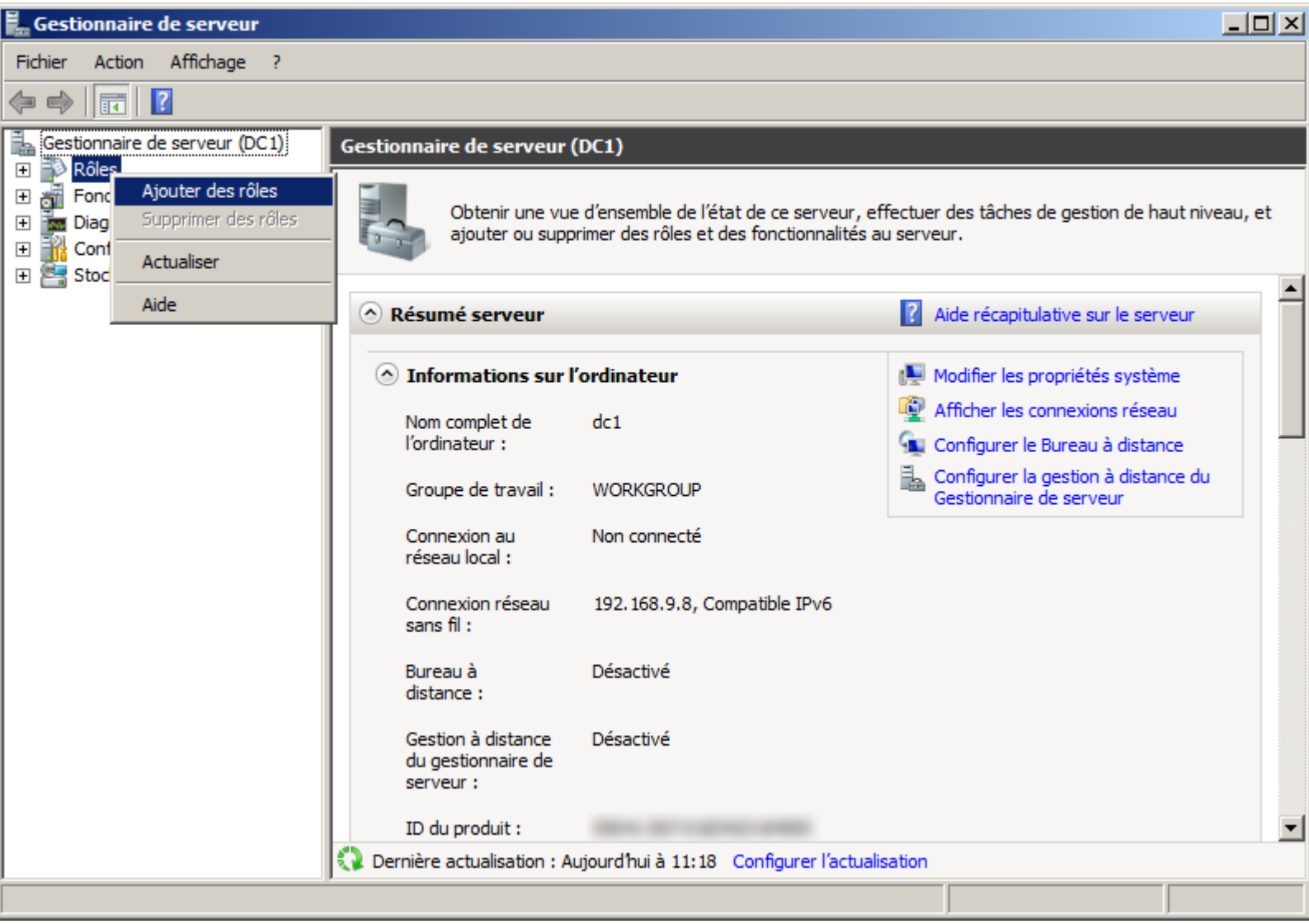
Je vais exposer l'installation d'une configuration Active Directory idéale (elle n'est pas pour autant irréaliste), c'est à dire un Active Directory mono-forêt et mono-domaine.

Vous aurez besoin d'une configuration IP fixe. Votre serveur devra porter un nom correct : le nom de serveur par défaut créé lors de l'installation de Windows n'est pas satisfaisant. Attention au nom de votre contrôleur de domaine (Domain Controller ou appelé fréquemment DC). Il ne doit pas être nommé "dc" : cela semble poser des problèmes dans ADCS et certainement dans d'autres produits.

IV-A - Installation du rôle

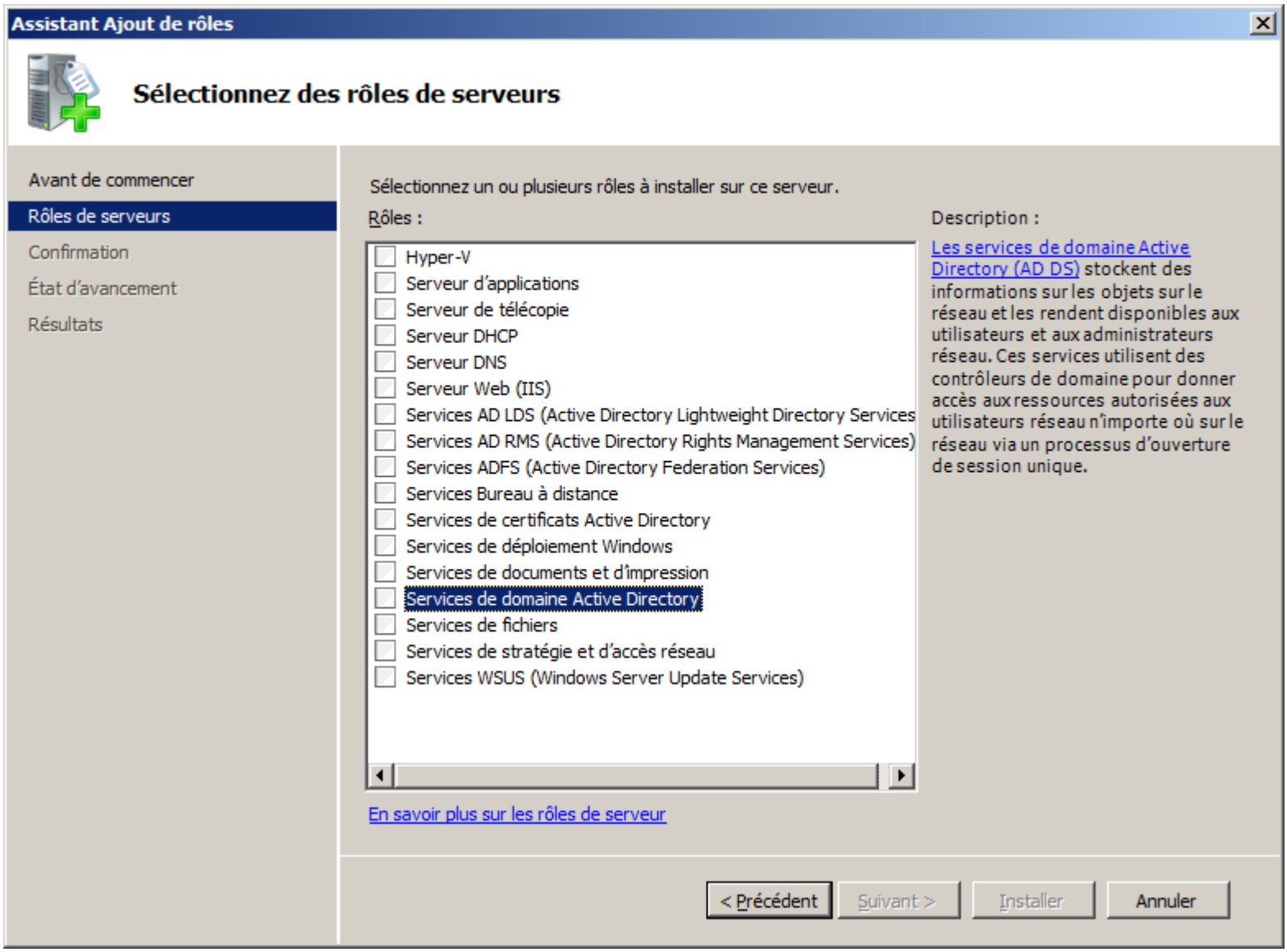
Sous Windows 2000 et 2003, il n'y avait pas d'installation des binaires d'Active Directory : ils étaient installés par défaut. Un serveur peut être utilisé pour autre chose qu'Active Directory donc Microsoft a décidé de ne plus installer ces binaires par défaut depuis Windows 2008.

Allez dans le gestionnaire de serveur puis faites un clic droit sur *Rôles, Ajouter des rôles*.



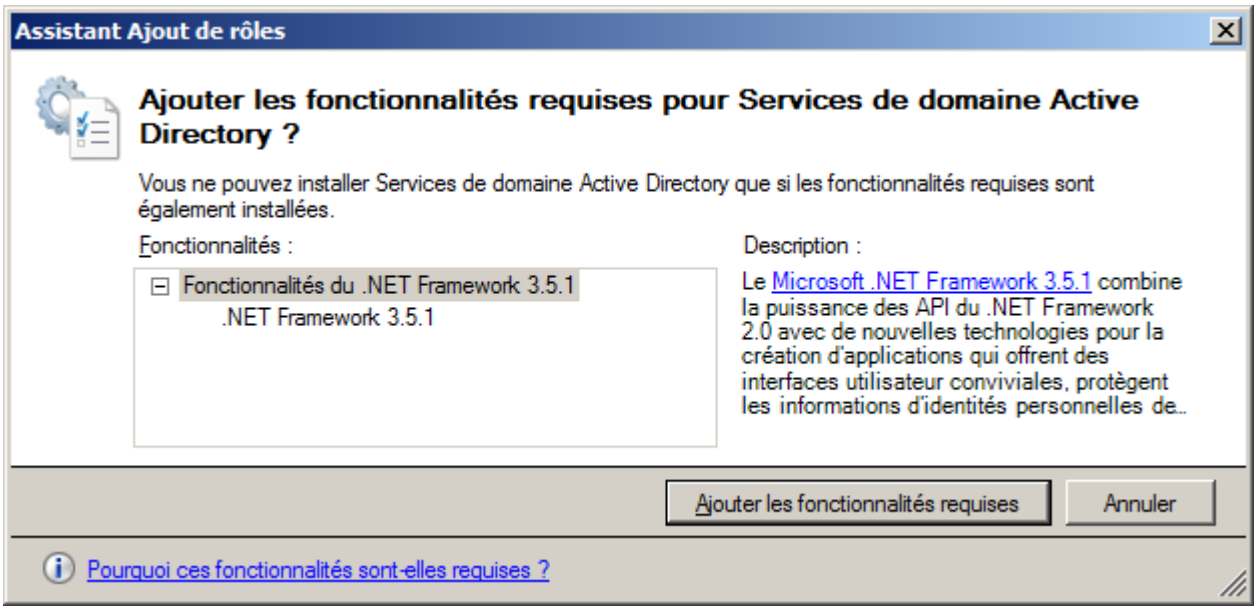
Ajout du rôle

Sélectionnez le rôle **Services de domaine Active Directory** et cliquez sur *Suivant*.



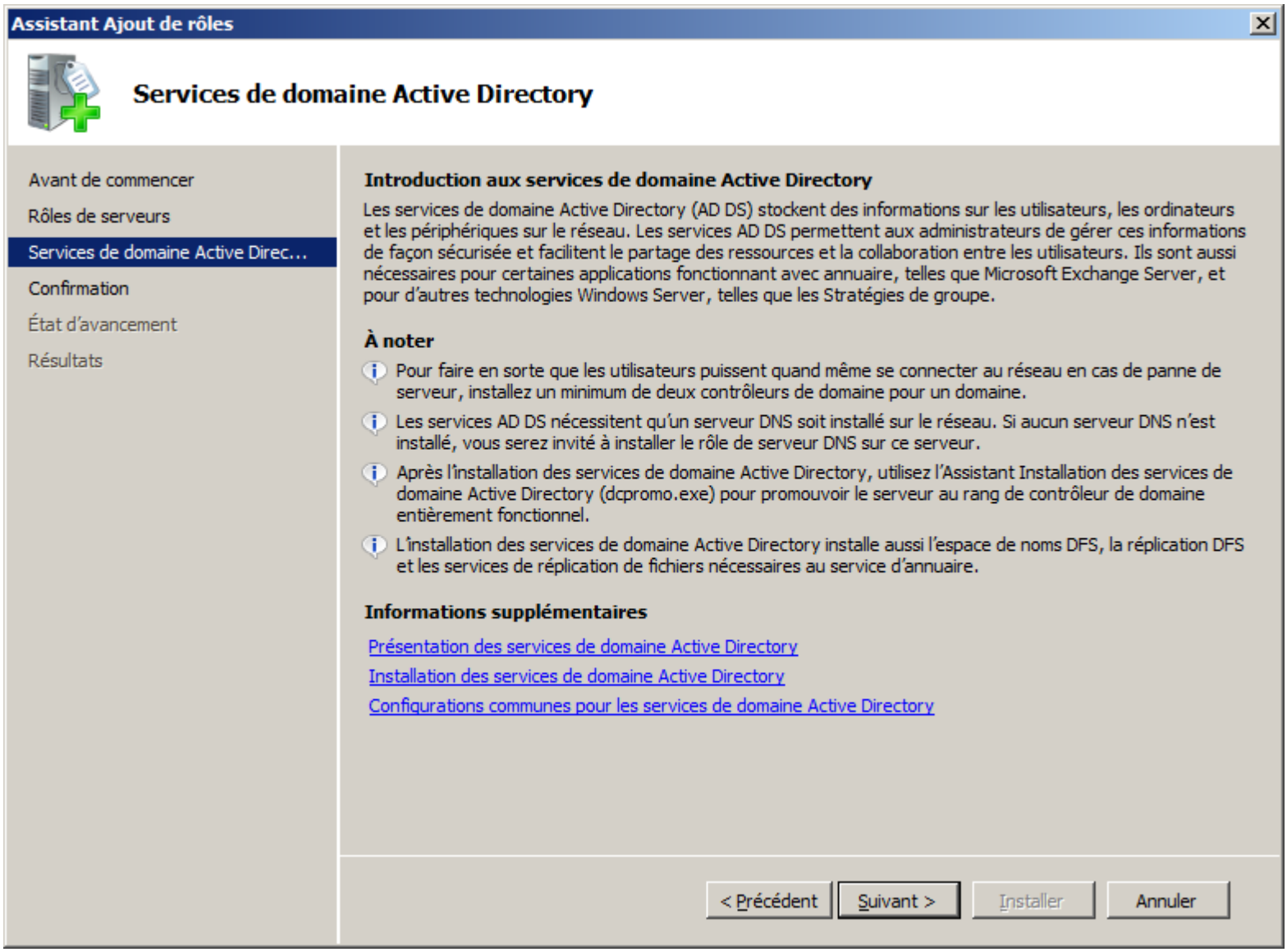
Sélection du rôle ADDS

Si vous n'avez rien installé précédemment sur votre serveur, vous devrez ajouter des fonctionnalités du framework .NET en cliquant sur *Ajouter les fonctionnalités requises*.



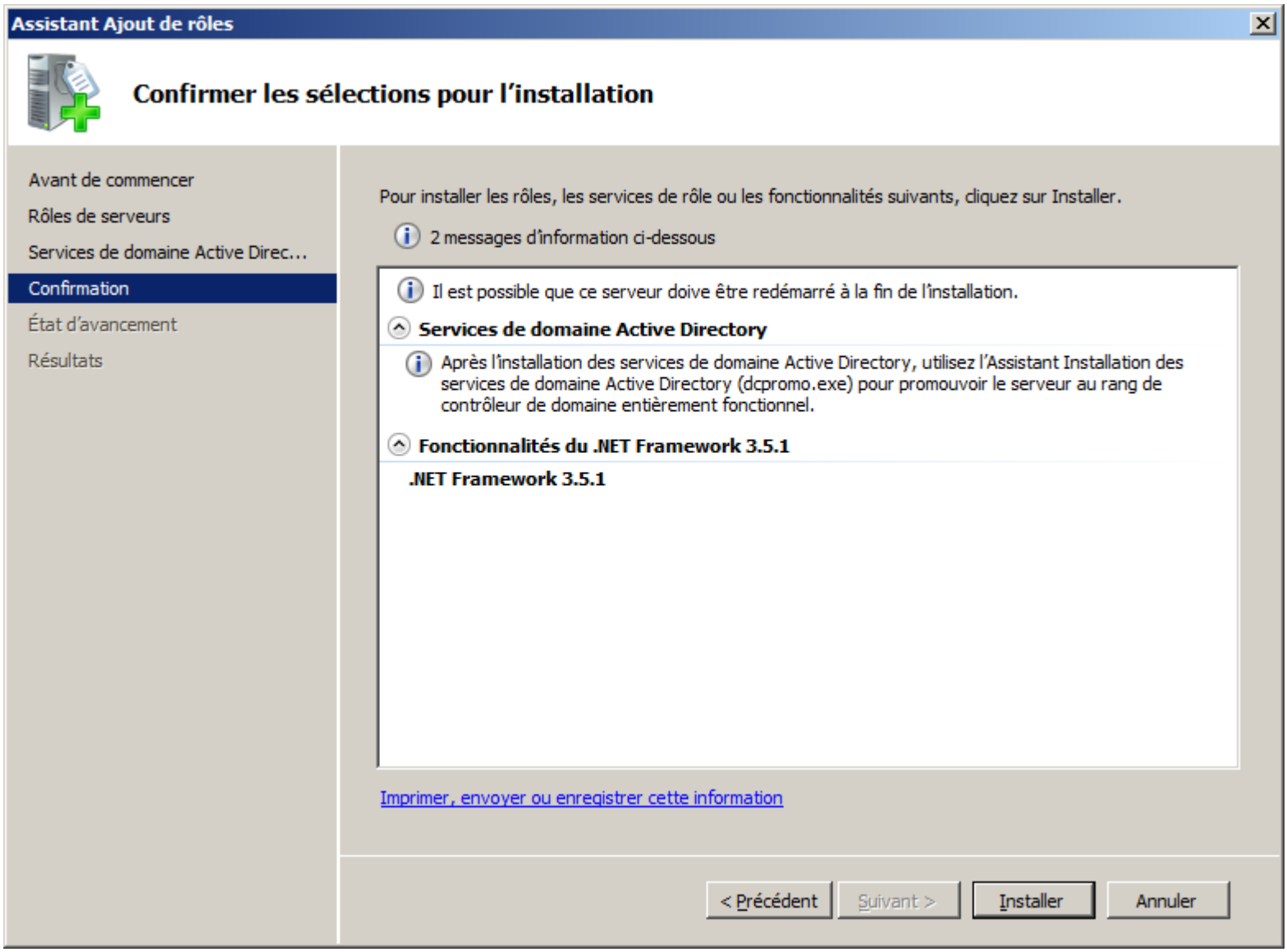
Ajout de fonctionnalité

Vous aurez ensuite quelques informations sur Active Directory et son fonctionnement. On retrouve la nécessité du système DNS. Il est également conseillé d'installer deux contrôleurs de domaine pour la haute disponibilité : je ne traite pas la haute disponibilité ici.

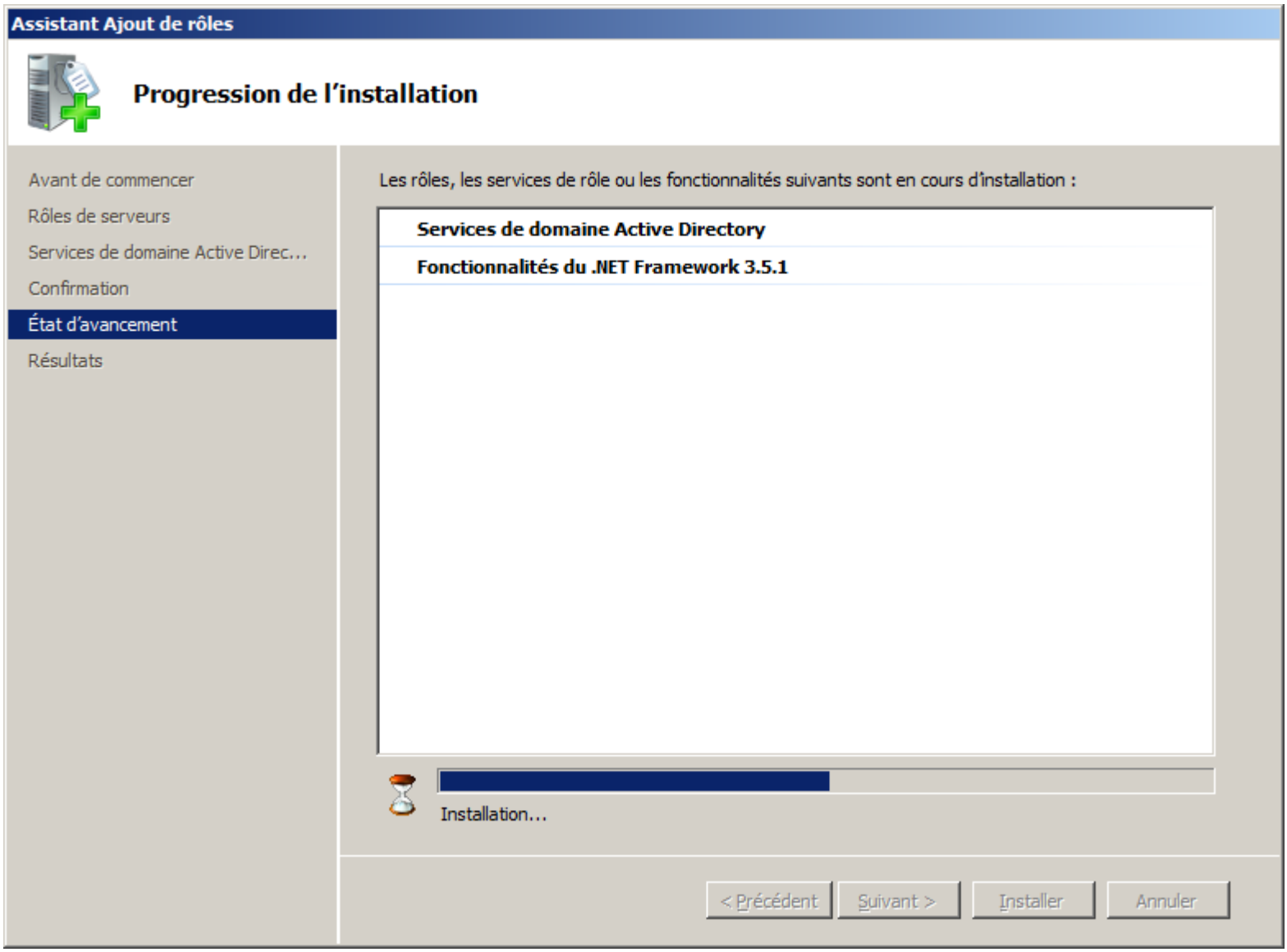


Informations à propos d'Active Directory

Vous aurez ensuite le résumé de l'installation qui va être faite.

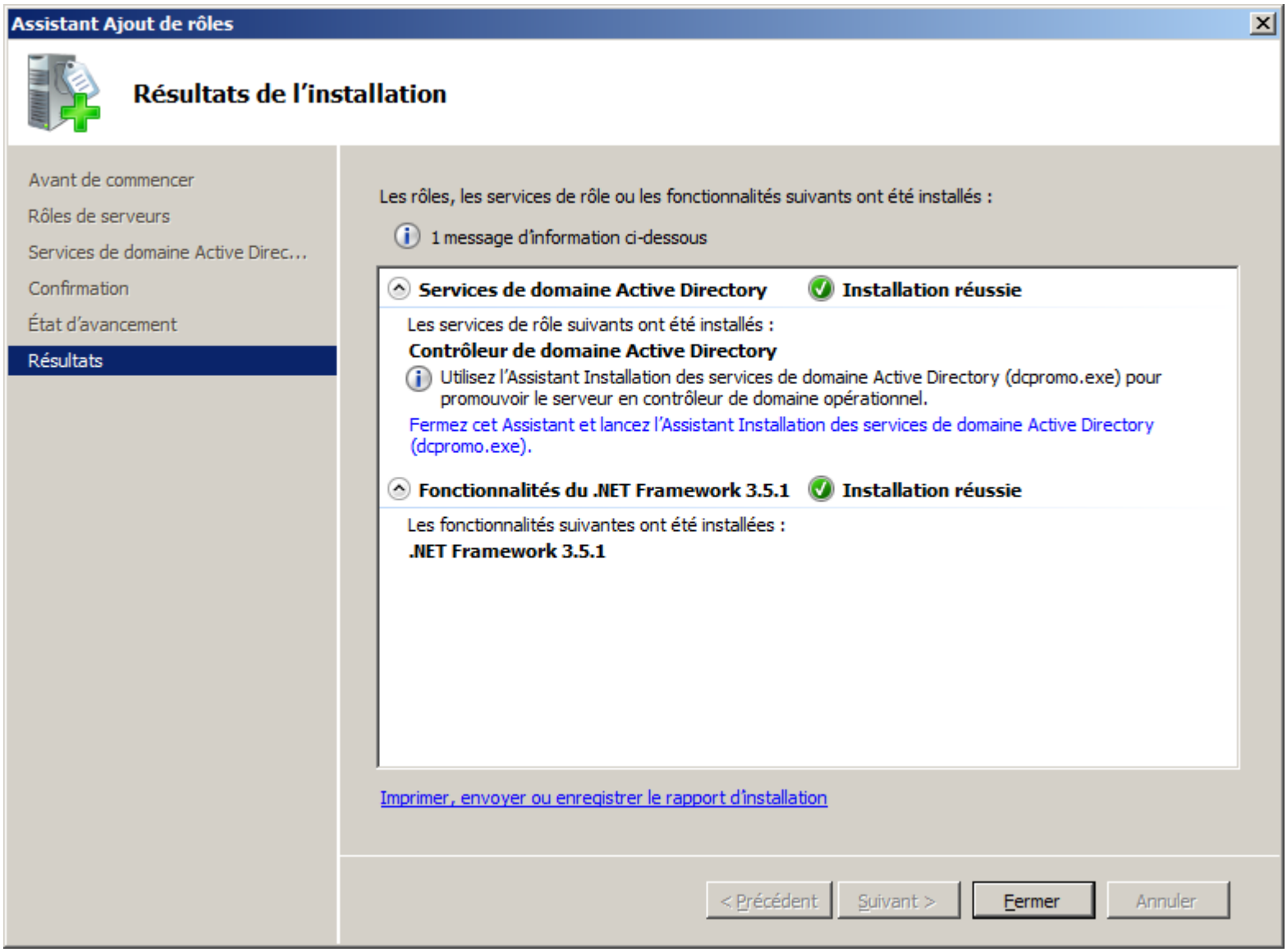


Résumé de ce qui va être fait



Installation en cours

L'installation des binaires ne doit poser aucun problème, sauf si vous manquez d'espace disque. Une fois l'installation finie, vous avez le résumé de l'installation.

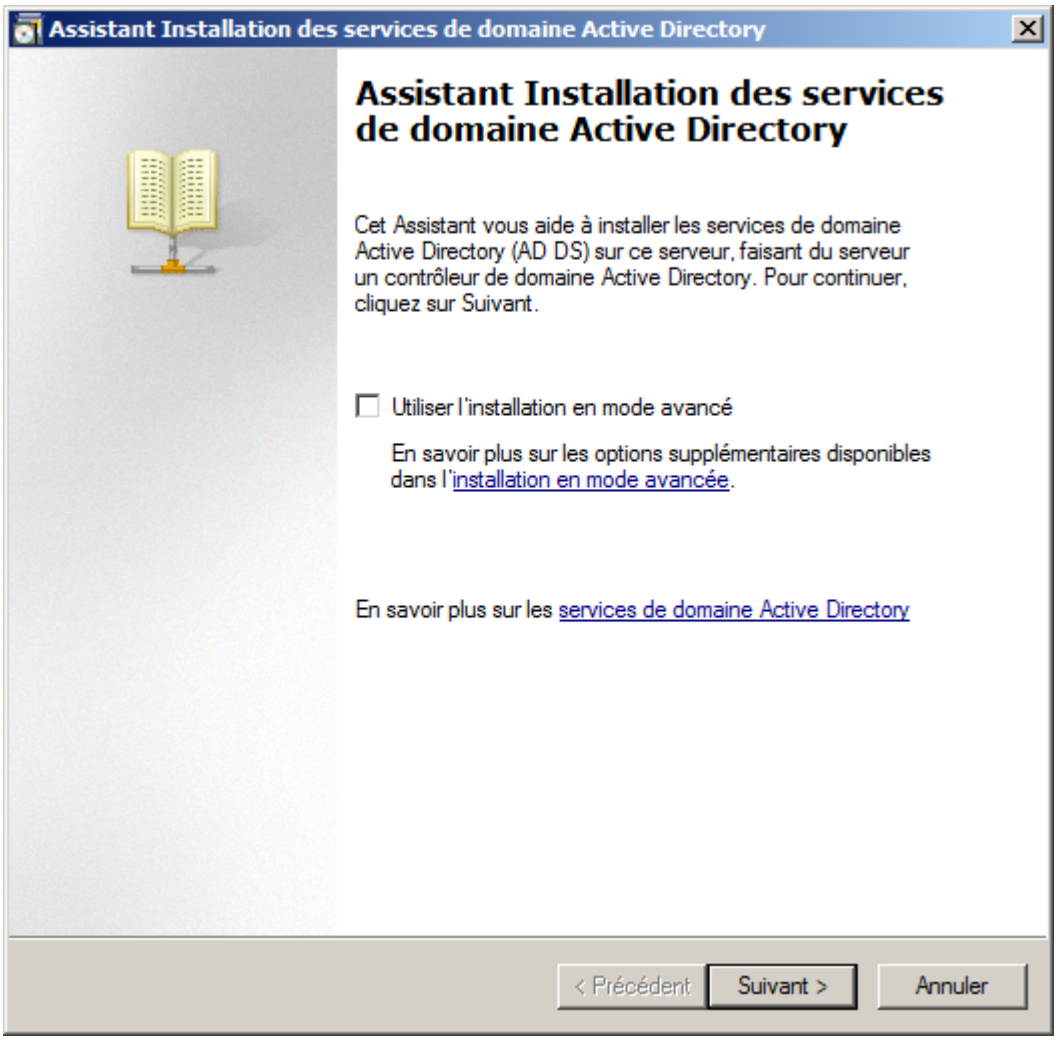


Installation finie !

Nous allons maintenant pouvoir commencer l'installation d'Active Directory. Habituellement, il fallait lancer manuellement le programme **dcpromo.exe**. Maintenant, nous avons un lien *Fermez cet assistant et lancez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe)*. Choisissez la méthode que vous souhaitez ;)

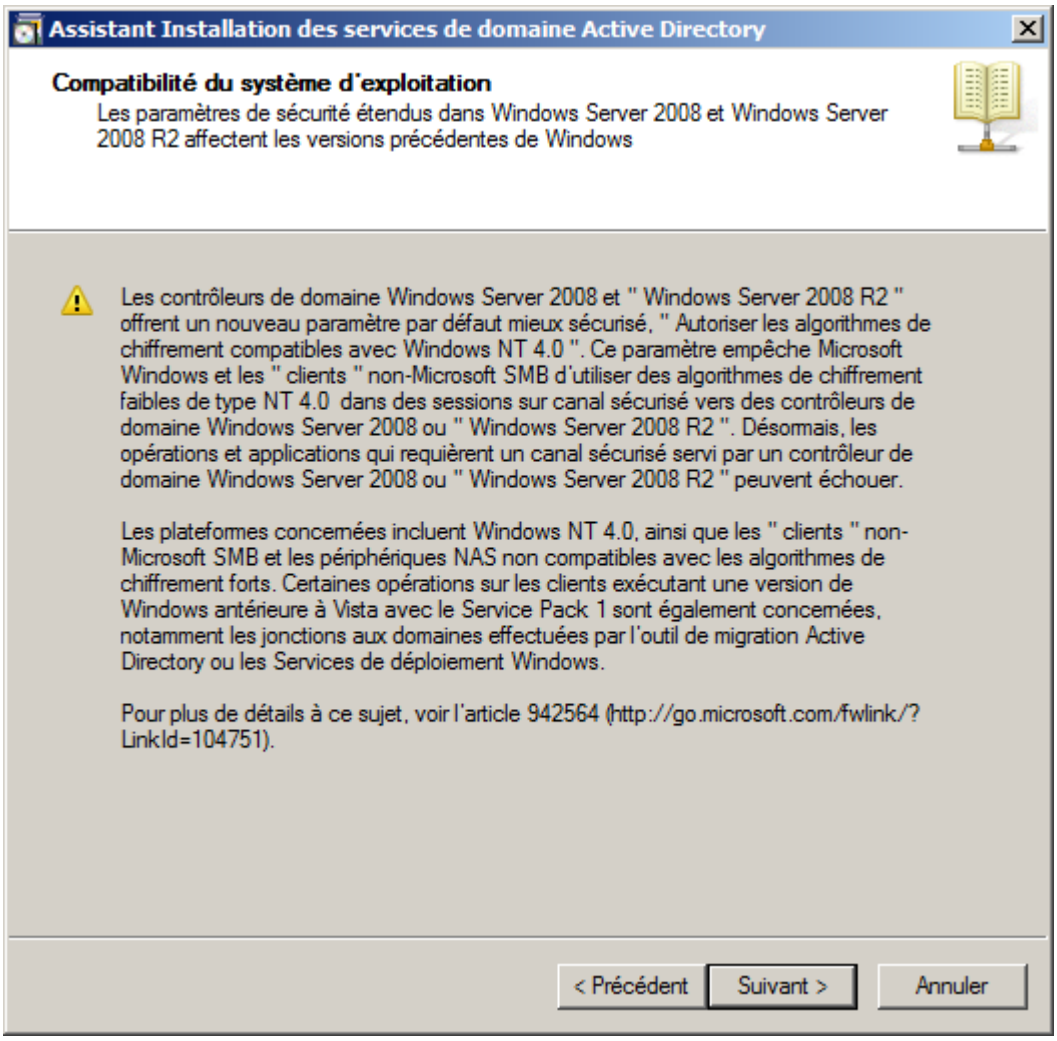
IV-B - Assistant Installation des services de domaine Active Directory (dcpromo.exe)

L'assistant commence par vous proposer l'installation en mode avancé. Ce mode avancé vous permet de fournir un fichier de réponses issu d'une autre installation ou encore de charger une sauvegarde de votre Active Directory. Pourquoi charger une sauvegarde ? Vous avez un Active Directory au siège de votre société et vous devez installer un autre contrôleur de domaine pour une agence. Si vous installez le DC de votre agence sans charger de sauvegarde alors le mécanisme de réplication va se mettre en route et cela va prendre du temps car tout le trafic passera par une connexion Internet. Au lieu de cela, vous pourrez envoyer une sauvegarde de votre Active Directory du siège pour la charger dans celui de l'agence. Cette sauvegarde faite à un moment M sera injectée dans votre nouveau serveur au moment M+1. La différence entre M et M+1 sera répliquée. Normalement, cela représente beaucoup moins de données donc une réplication moins longue.



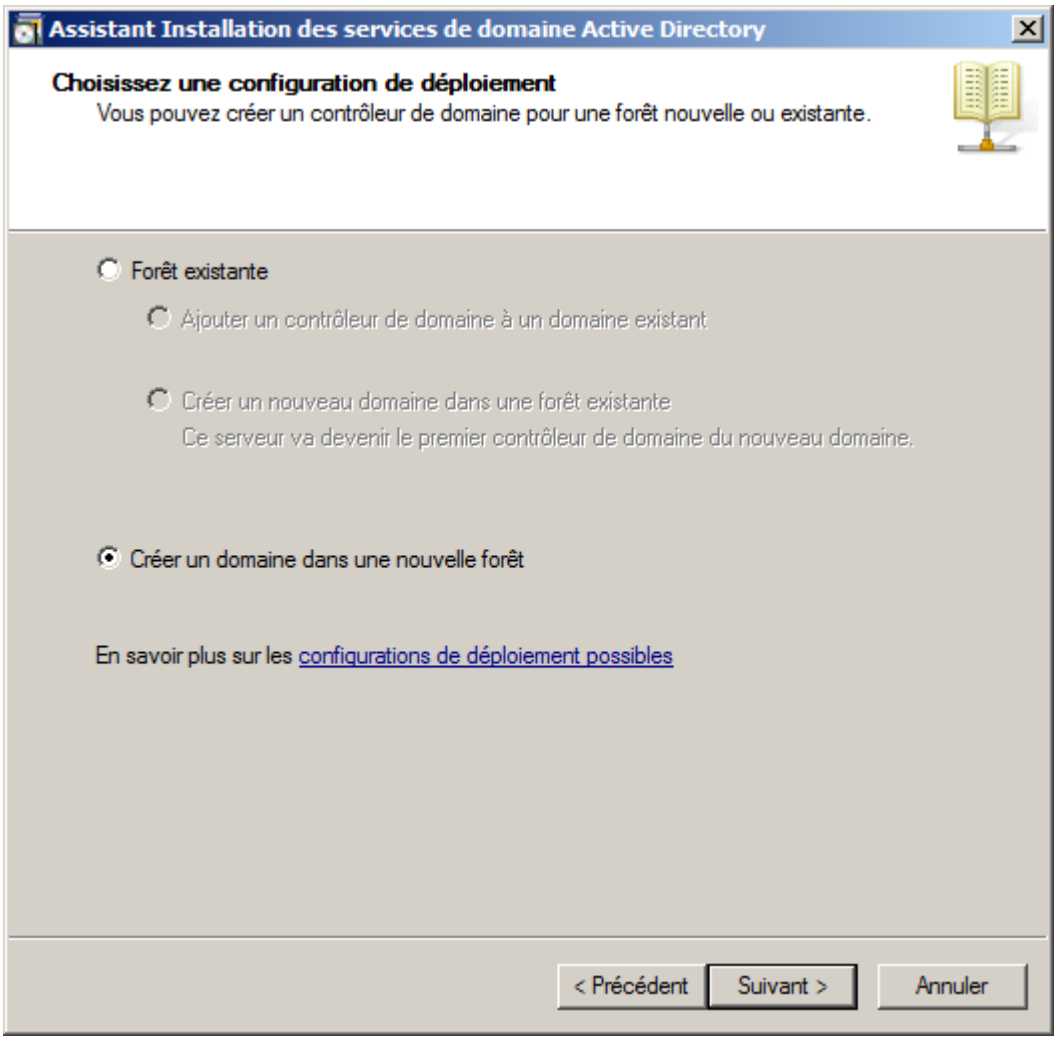
dcpromo.exe

Windows 2008 et 2008 R2 fonctionnent par défaut avec des algorithmes de chiffrement plus forts. Par conséquent, certains anciens clients sont incompatibles avec ce nouveau réglage. Il est possible d'abaisser cette sécurité par stratégie de groupe. Consultez le **kb 942564** pour plus d'informations.



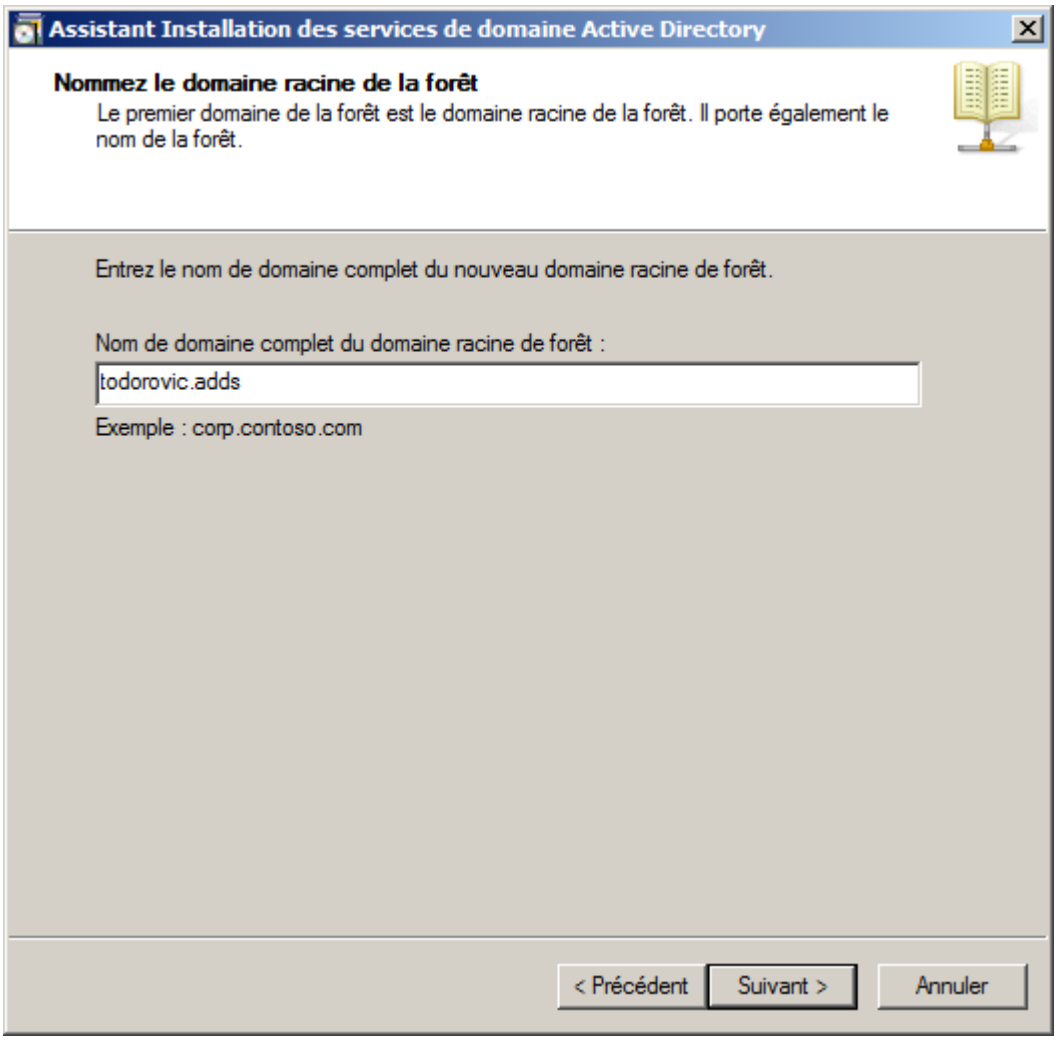
Avertissement sur un nouveau réglage par défaut

Nous allons maintenant commencer la création de votre Active Directory. Vous aurez le choix entre rejoindre une forêt existante ou créer un nouveau domaine dans une nouvelle forêt. Nous allons créer un nouveau domaine.



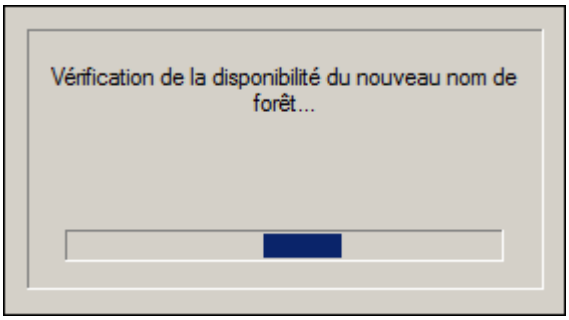
Créer ou rejoindre une forêt ?

Vous allez ensuite pouvoir indiquer le nom mûrement réfléchi de votre domaine racine de forêt.



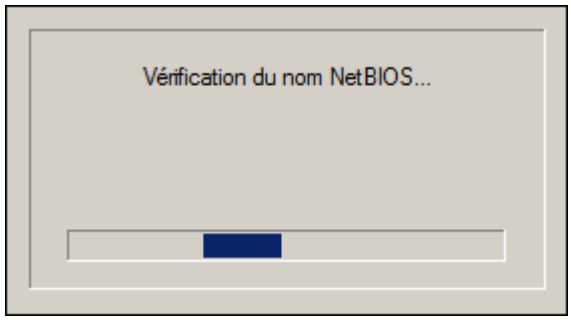
Nom du domaine racine de forêt

L'assistant va alors détecter si le domaine DNS est déjà utilisé ou non sur votre réseau.



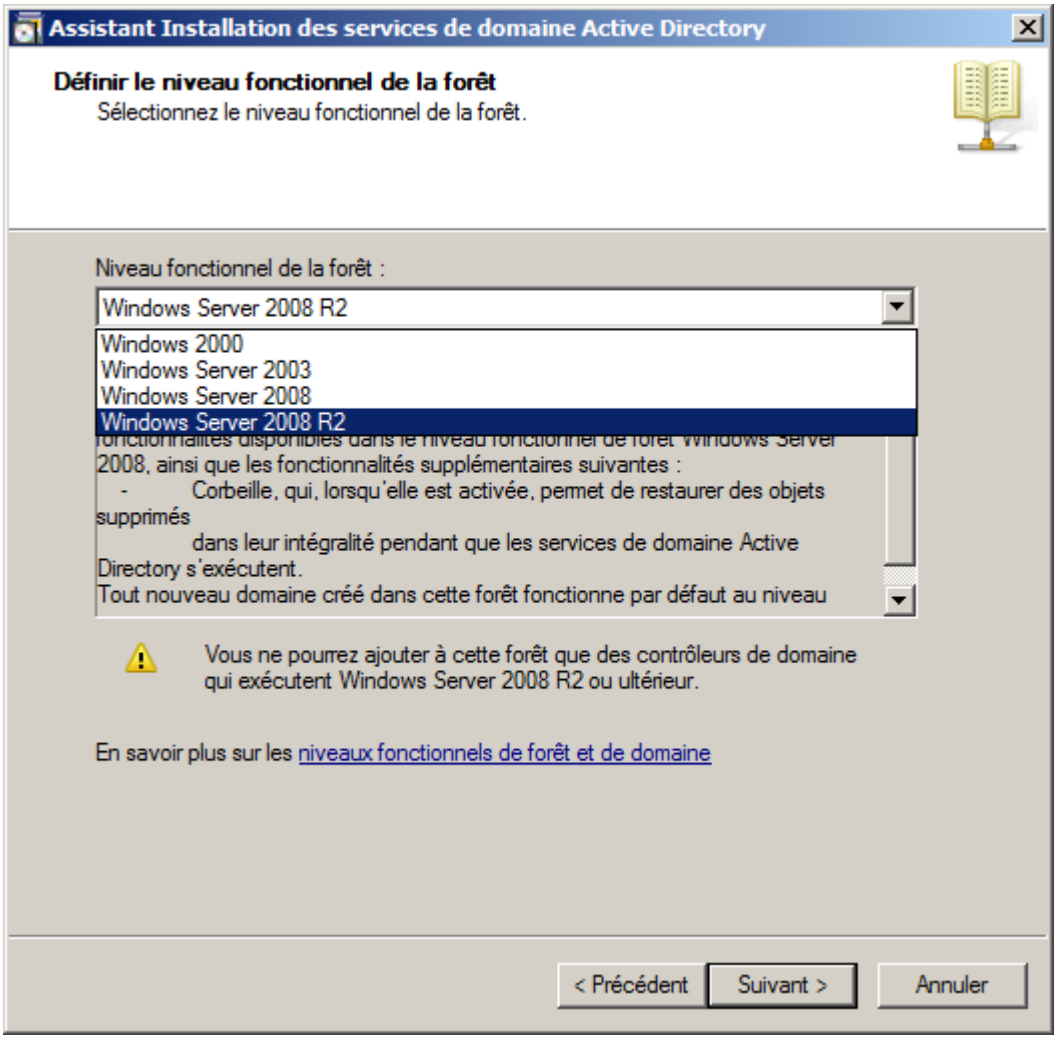
Détection de la disponibilité du domaine choisi

Voici quelque chose dont je n'ai pas parlé jusqu'à maintenant : le nom NetBIOS (**fr** ou **plus complet**) de votre domaine. Ce nom est également important : il prend la partie la plus à gauche de votre nom DNS. En mode avancé, vous pouvez sélectionner un nom NetBIOS différent. Pour le nom DNS todorovic.adds, le nom NetBIOS est TODOROVIC. Ce nom est repris dans les logins pre-Windows 2000 (TODOROVIC\utilisateur). Il est conseillé d'abandonner cette écriture pour la notation UPN (User Principal Name) de la forme utilisateur@todorovic.adds que nous verrons dans la partie suivante. Etant donné l'importance du nom NetBIOS, l'assistant doit contrôler la disponibilité de ce dernier.



Nom NetBIOS disponible ?

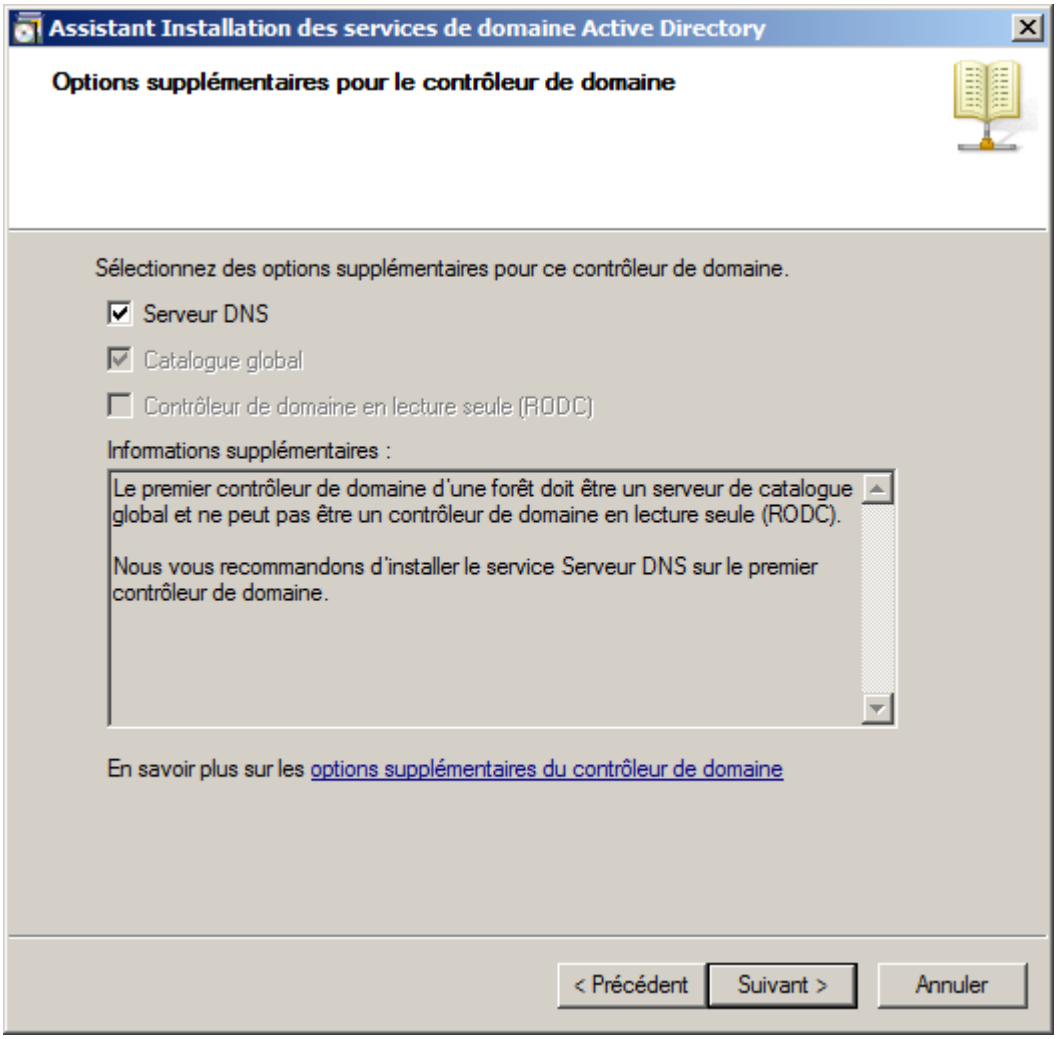
Si les noms DNS et NetBIOS ne sont pas déjà pris, vous pourrez sélectionner le niveau fonctionnel de votre forêt (pour rappel, ce choix ne doit pas être fait à la légère). Si vous ne savez pas quel niveau fonctionnel mettre, je vous conseille de mettre le niveau Windows 2003. Vous pourrez augmenter le niveau fonctionnel quand vous serez sûr de pouvoir le faire (compatibilité applicative au niveau des serveurs). Dans mon cas, je peux prendre le niveau 2008 R2 puisque ma future infrastructure (Exchange 2010) supporte ce niveau fonctionnel.



Sélection du niveau fonctionnel

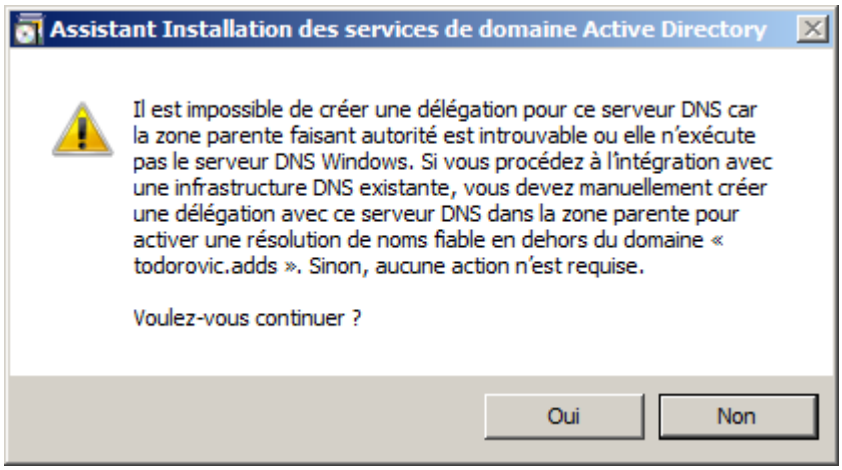
Si vous n'avez pas déjà installé un serveur DNS compatible avec les besoins d'Active Directory, vous devrez sélectionner l'installation du serveur DNS de Windows. Comme vous installez votre premier contrôleur de domaine, celui-ci sera obligatoirement catalogue global. Le catalogue global est utilisé dans la réplication : il contient un sous-ensemble des attributs de tous les objets de l'Active Directory. Ce sous-ensemble est créé par défaut et il est possible d'ajouter manuellement des attributs qui seraient fréquemment utilisés par des produits sur les autres sites de votre

architecture. Vous ne pouvez pas configurer ce premier contrôleur de domaine comme RODC (un RODC est un DC en lecture seule qui prend sa source sur le catalogue global).



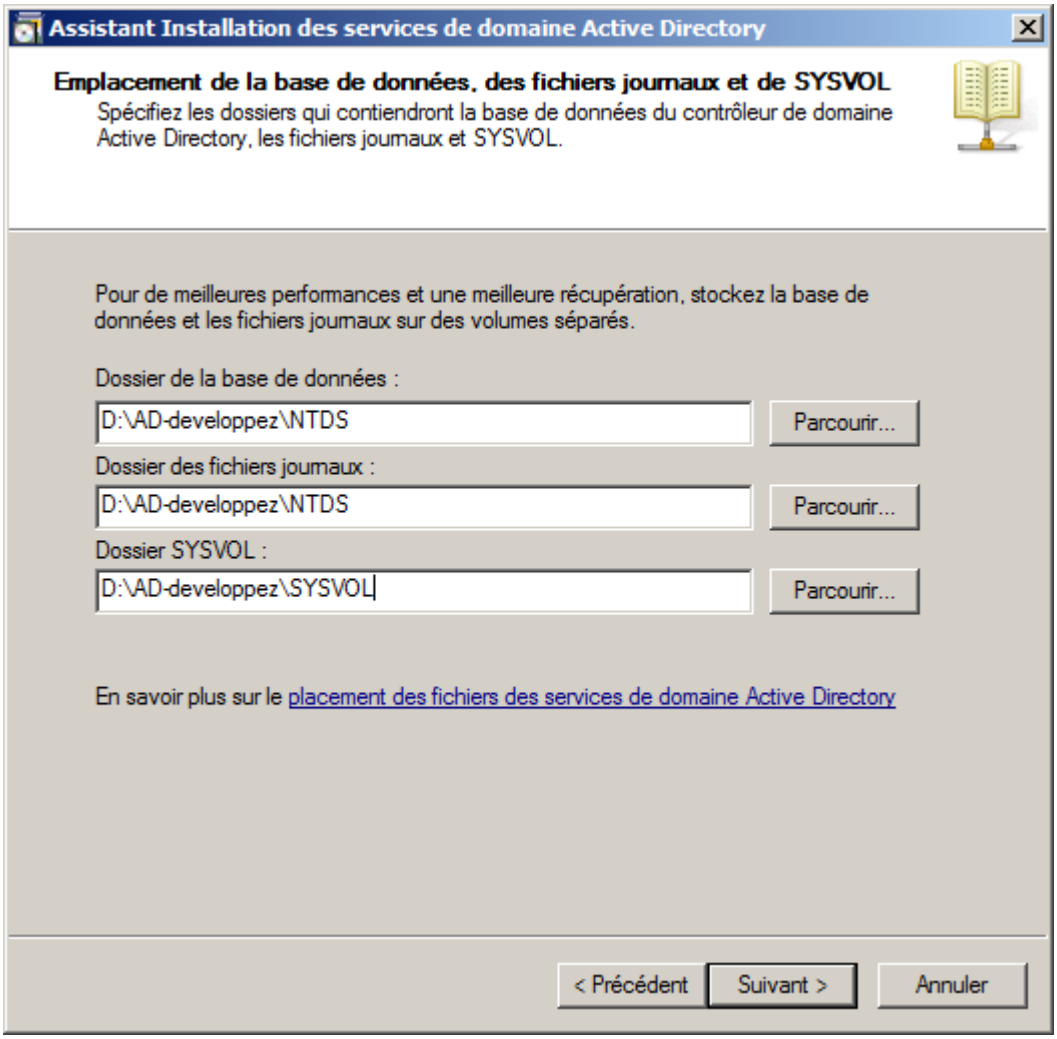
Options pour le contrôleur de domaine

Un message d'avertissement apparaît ensuite parce que le serveur n'arrive pas à contacter le DNS qui gère la zone parente. Dans mon cas, cette zone est nommée adds. Il n'existe pas de DNS gérant cette zone dans mon réseau et les serveurs indiqués dans les root hints (liste des adresses IP des serveurs DNS racines gérant notamment les zones correspondant aux TLD) ne gèrent pas cette zone. Le serveur ne trouvant pas de serveur DNS parent, il ne peut pas demander de délégation. Cet avertissement est donc normal. Cliquez sur *Oui* pour continuer l'installation du contrôleur de domaine.



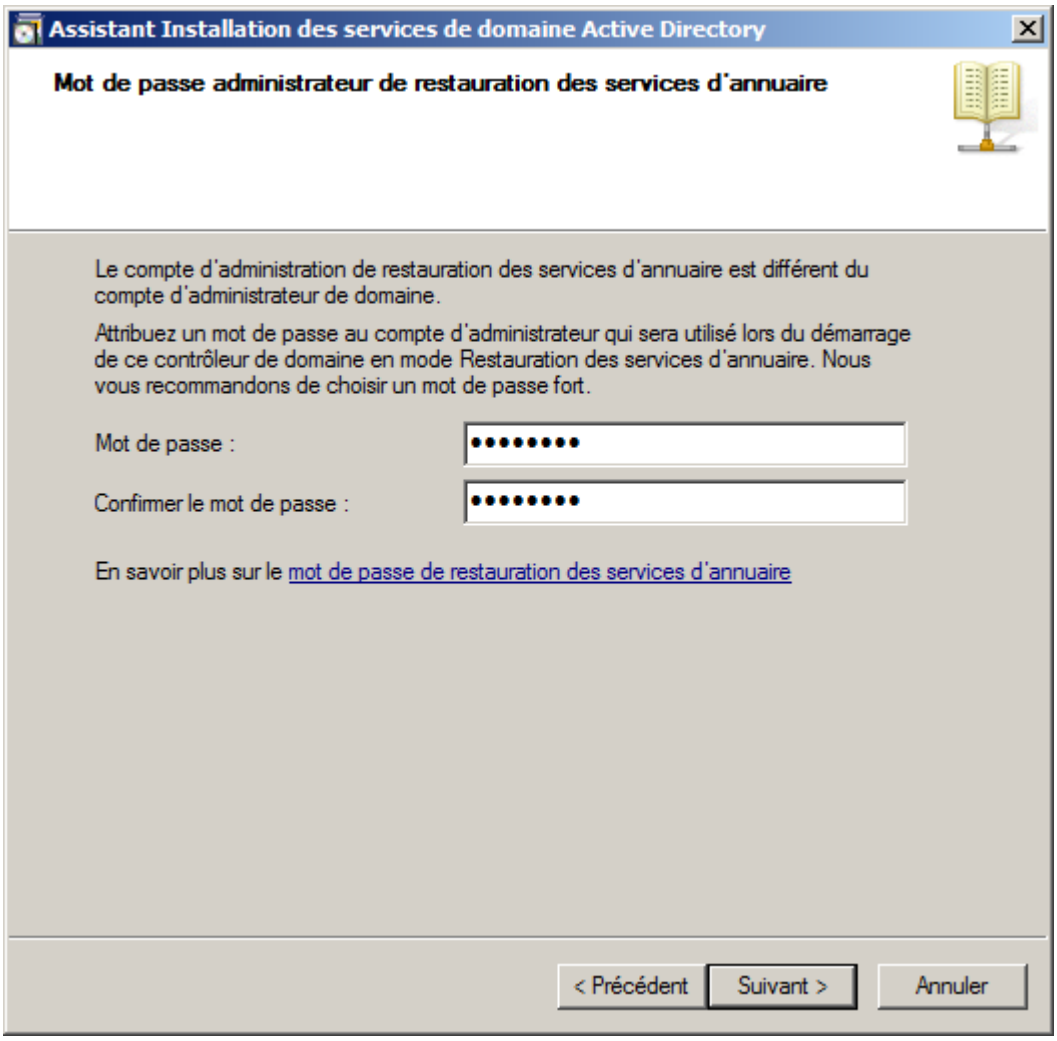
Impossible de créer une délégation DNS

Vous devrez ensuite indiquer le futur emplacement des fichiers servant à Active Directory. Il est recommandé de placer ces fichiers ailleurs que sur le disque système.



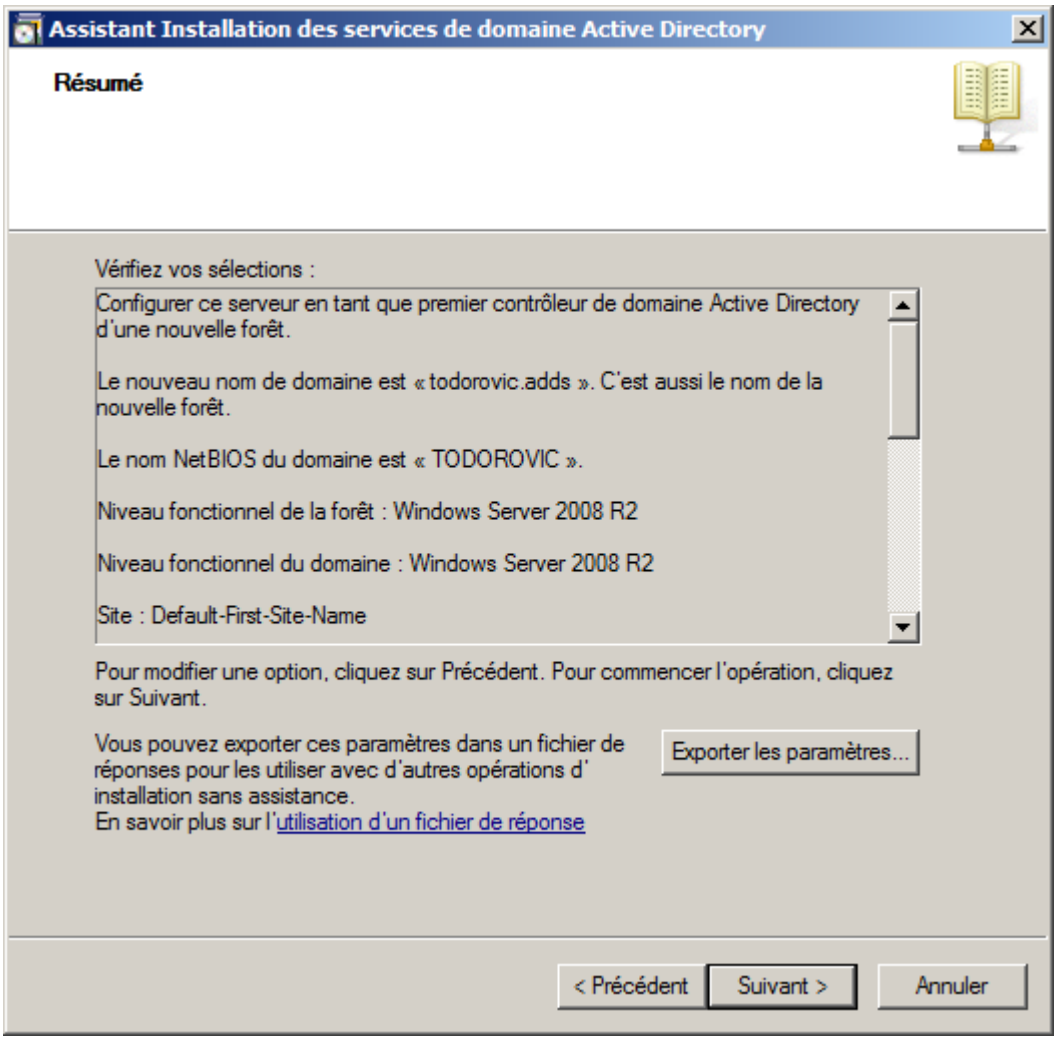
Emplacement des fichiers

Si votre Active Directory, pour une raison quelconque, venait à tomber en panne, vous pourrez le restaurer. Pour protéger votre serveur et ainsi éviter des restaurations non souhaitées, vous devrez donner un mot de passe fort différent du mot de passe administrateur. Vous pouvez mettre le même mais c'est déconseillé.



Création d'un mot de passe de restauration

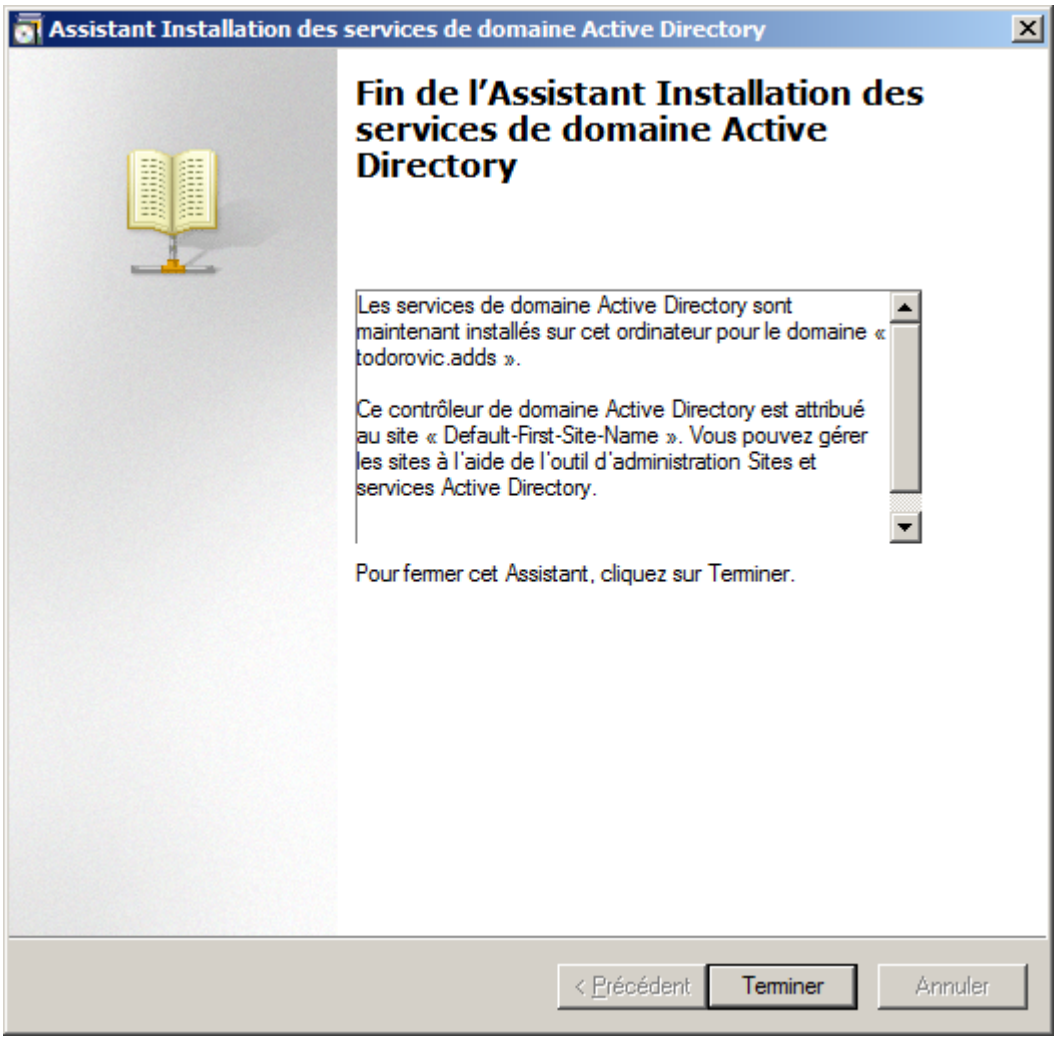
Vous arrivez ensuite sur le résumé de l'installation qui va être faite. Vous pourrez exporter les paramètres de cette installation afin de la reproduire ailleurs : il s'agit du fichier de réponses exploitable en mode avancé.



Résumé de l'installation

L'installation peut prendre quelques minutes et doit se passer sans problèmes.

Installation en cours



Installation terminée

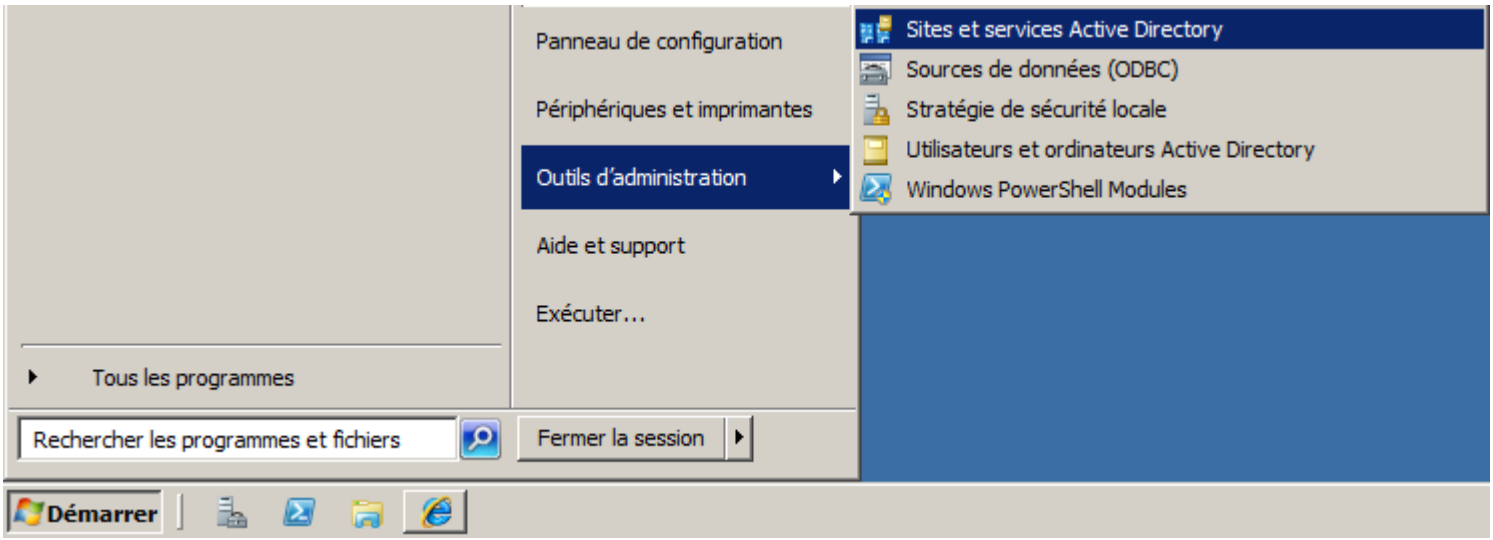
Vous serez invité à redémarrer votre serveur.

V - Configuration sommaire

Il existe certaines manipulations à effectuer. Elles ne sont pas obligatoires en tant que telles mais je les recommande, notamment si vous souhaitez par la suite configurer plusieurs sites ou un serveur de messagerie Microsoft Exchange.

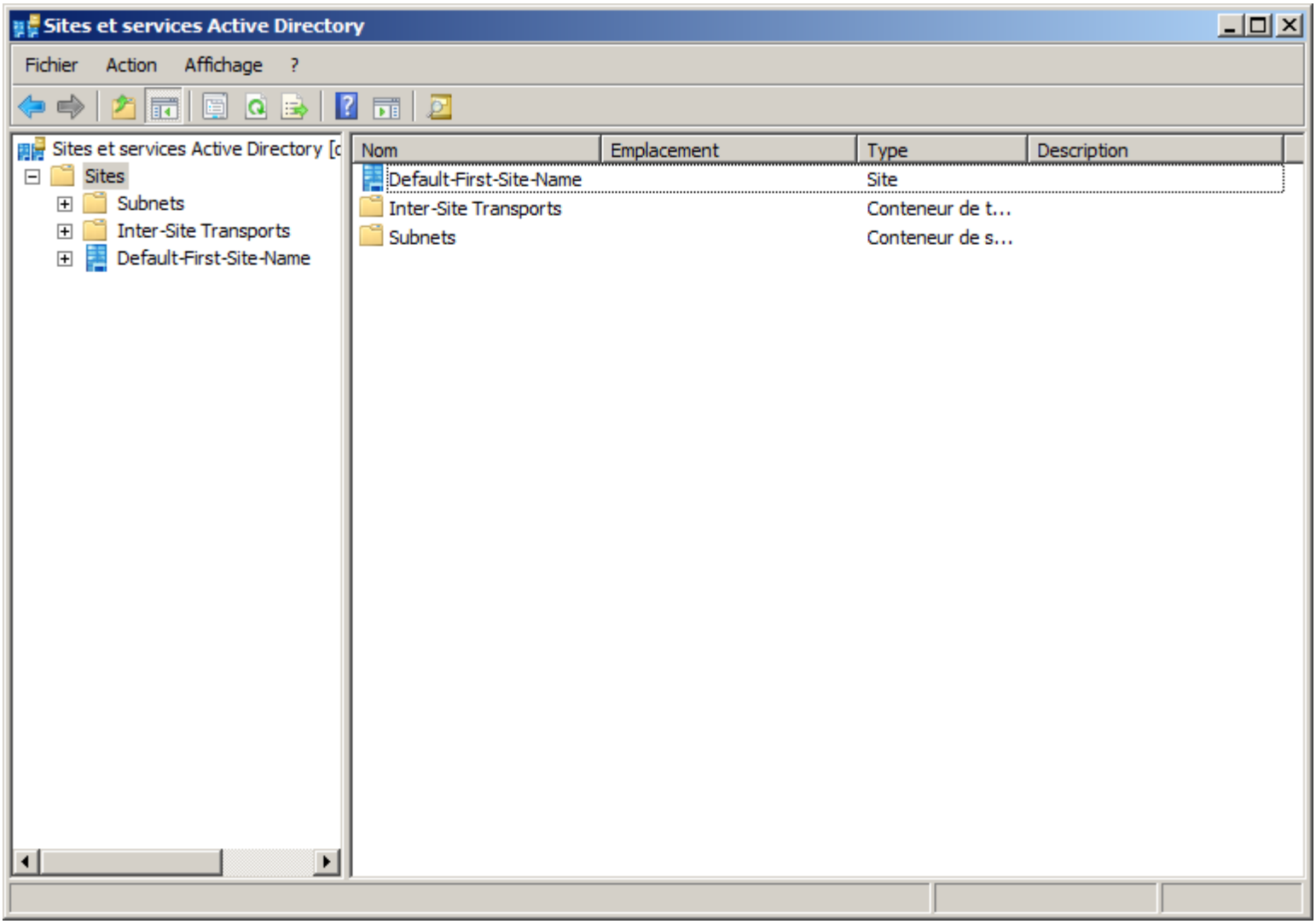
V-A - Configuration du site

La première étape consiste simplement à changer le nom du site courant et à créer le sous-réseau correspondant. Pour cela, allez dans *Menu démarrer, Outils d'administration, Sites et services Active Directory*.



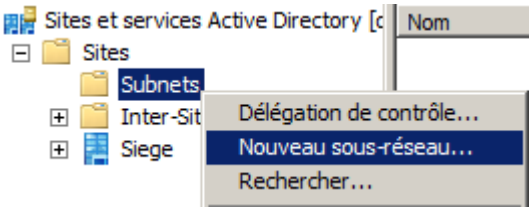
Sites et services Active Directory

Dans la fenêtre qui s'ouvrira, vous verrez le site **Default-First-Site-Name** ainsi qu'un dossier **Subnets** (sous-réseaux) et enfin un dossier Inter-Site Transports.



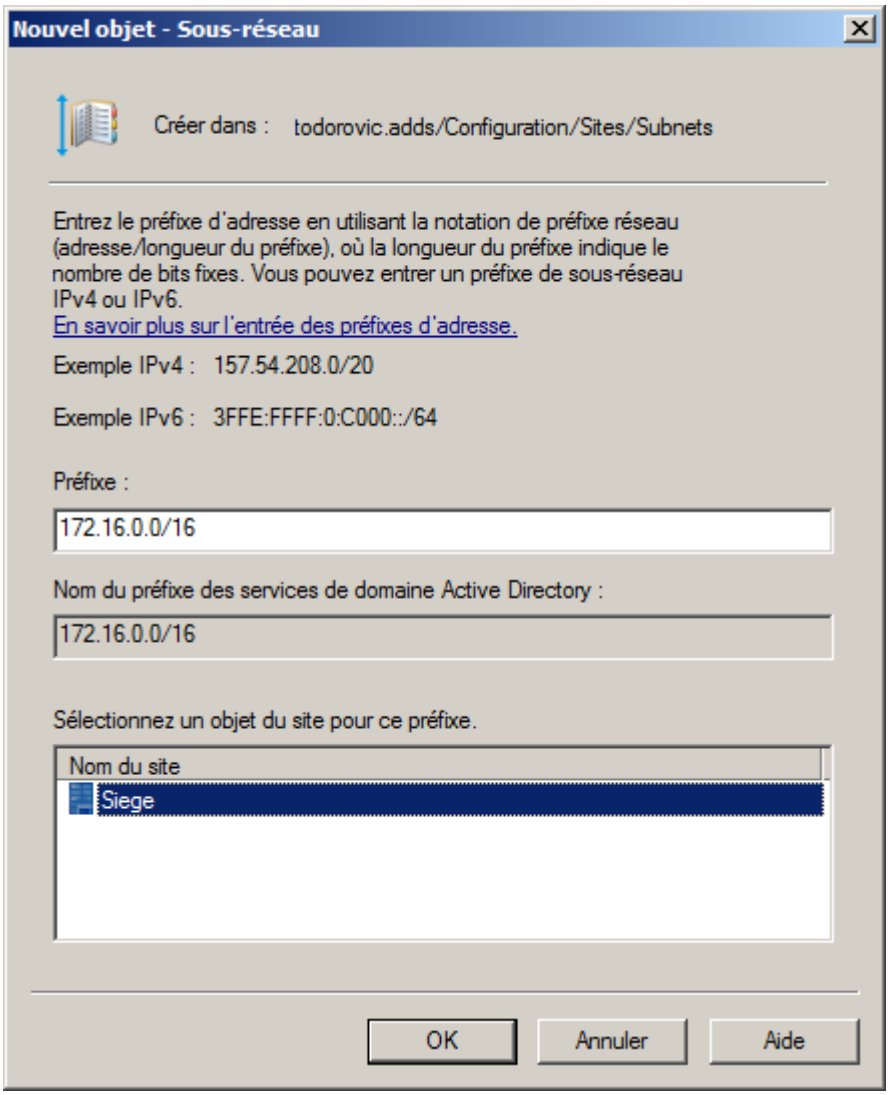
Renommez **Default-First-Site-Name** en quelque chose de plus explicite. Pour cela, double-cliquez dessus ou faites un clic droit *Renommer*.

Afin que les serveurs et les postes sachent sur quel site ils se trouvent, il faut créer un sous-réseau et l'associer à un site. Faites un clic droit sur *Subnet, Nouveau sous-réseau*.



Création du sous-réseau

Vous devrez entrer le sous-réseau sous la forme d'un CIDR dans le champ préfixe. Sélectionnez le site associé au sous-réseau.

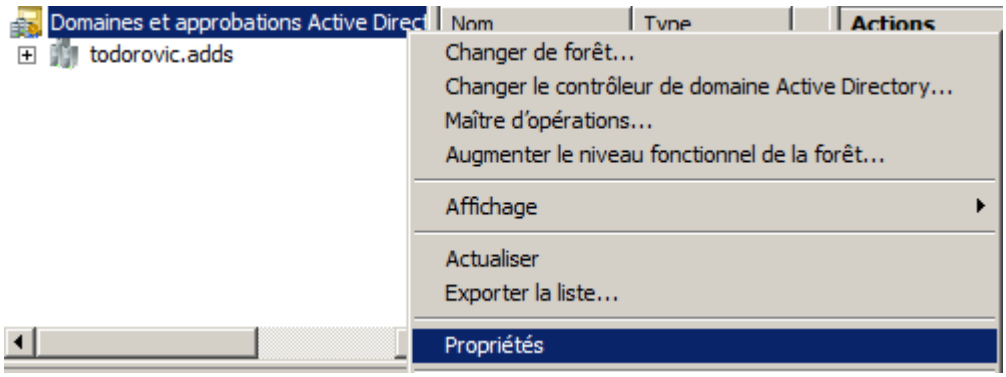


Association du sous-réseau au site

V-B - Suffixe UPN

Vous pouvez en profiter pour ajouter un suffixe UPN qui sera attribué à vos futurs utilisateurs. Grâce au suffixe UPN et à une politique de nommage adéquate, vos utilisateurs pourront se connecter avec leur adresse e-mail... ou du moins le croire puisque ce n'est pas l'attribut e-mail qui sera utilisé lors de la connexion mais l'UPN. Il est souhaitable de ne plus utiliser le login pre-Windows 2000 (domaine\utilisateur) et de lui préférer le login UPN.

Pour ajouter un suffixe UPN, ouvrez *Menu démarrer, Outils d'administration, Domaines et approbations Active Directory*. Dans la fenêtre qui s'ouvre, faites un clic droit sur *Domaines et approbations Active Directory, Propriétés*. N'ouvrez pas les propriétés de votre domaine, c'est une erreur fréquente.



Propriétés des domaines et approbations

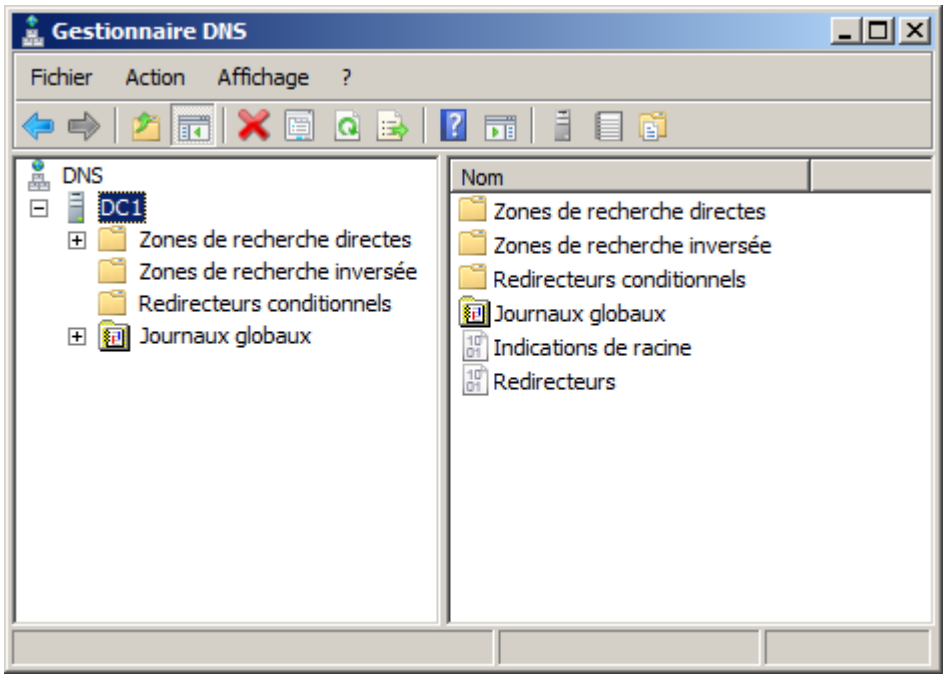
Vous pourrez ensuite ajouter votre nouveau suffixe UPN (idéalement votre nom de domaine public) et cliquer sur *Ajouter*. Lorsque vous ajouterez des utilisateurs, il faudra que le suffixe UPN corresponde à celui que vous souhaitez (domaine Active Directory ou domaine public).

V-C - Configuration DNS

V-C-1 - Zone de recherche inversée

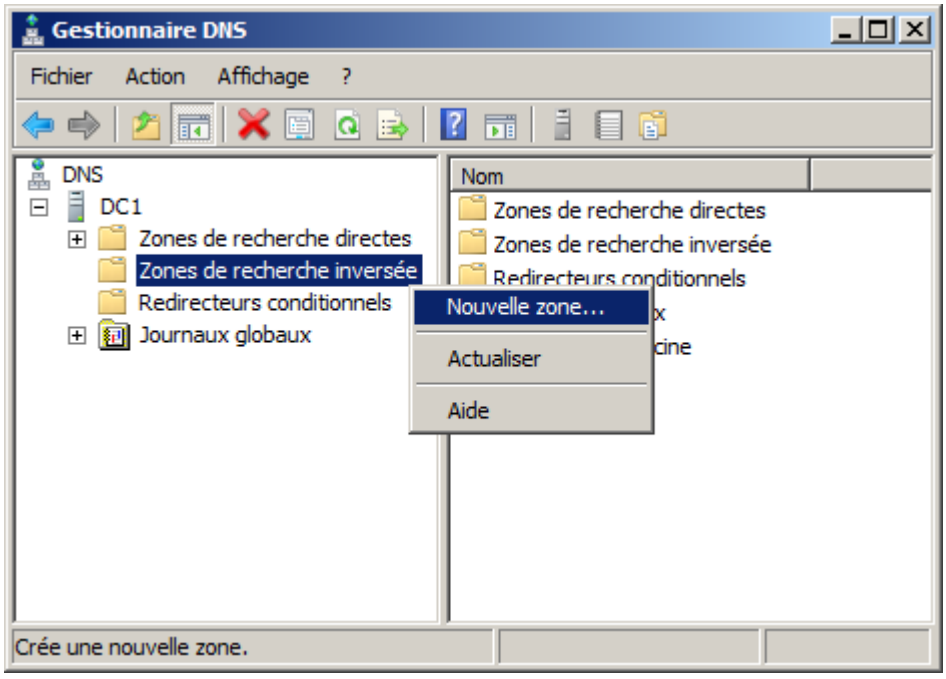
La zone de recherche inversée peut vous permettre de retrouver un nom d'hôte à partir de son adresse IP. Cela peut-être utile dans certains cas. Cette zone peut être utilisée par les services d'antispam afin de contrôler si l'expéditeur des e-mails est bien le serveur nommé dans les en-têtes e-mail.

Dans le cas d'un Active Directory, cela ne servira pas aux moteurs d'antispam. La création de cette zone est simple. Ouvrez la console de gestion DNS dans le gestionnaire de serveur (ou par Menu démarrer, Outils d'administration, DNS). Vous verrez alors les zones de recherche directe et inversée, les redirecteurs conditionnels et les journaux concernant le DNS.



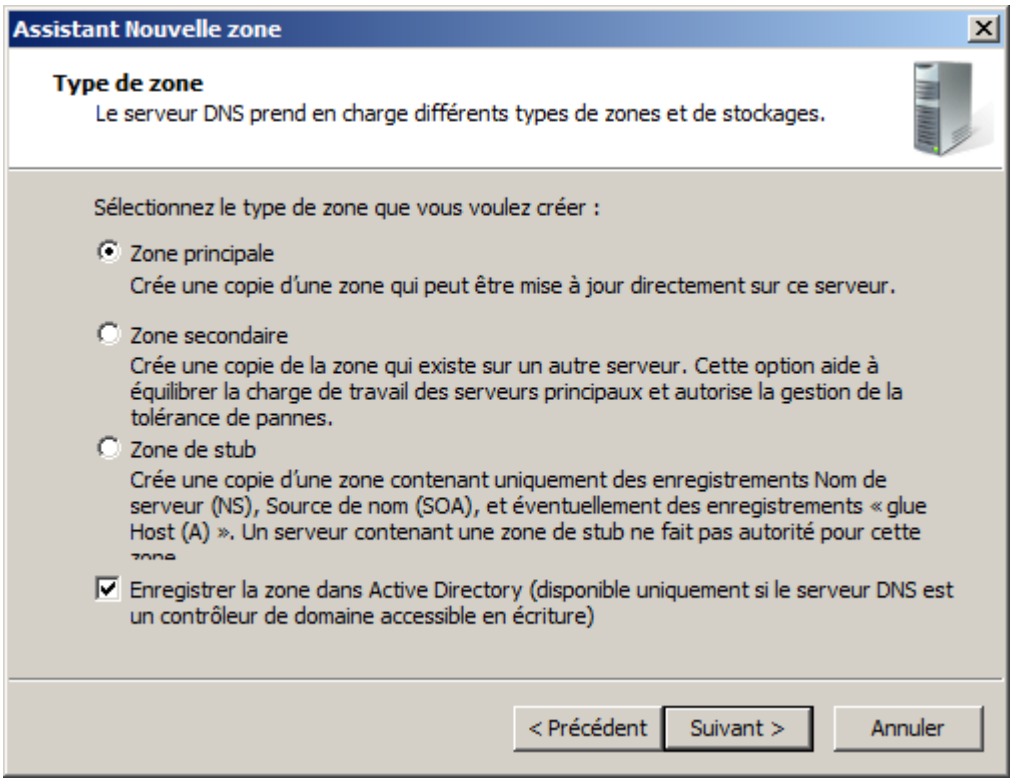
Console de gestion DNS

Pour ajouter une nouvelle zone inversée DNS, faites un clic droit sur *Zone de recherche inversée, Nouvelle zone*.



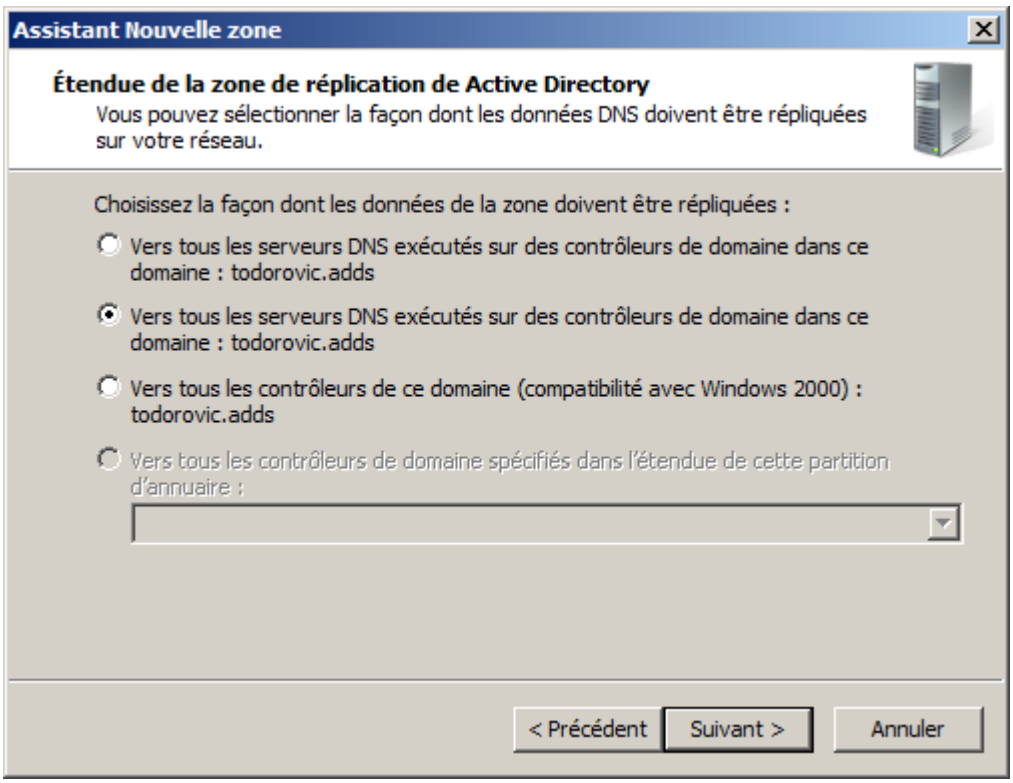
Nouvelle zone de recherche inversée

Nous avons besoin d'une zone principale de préférence stockée dans l'AD pour la réplication intersites si vous en avez ou comptez en avoir.



Sélection du type de zone

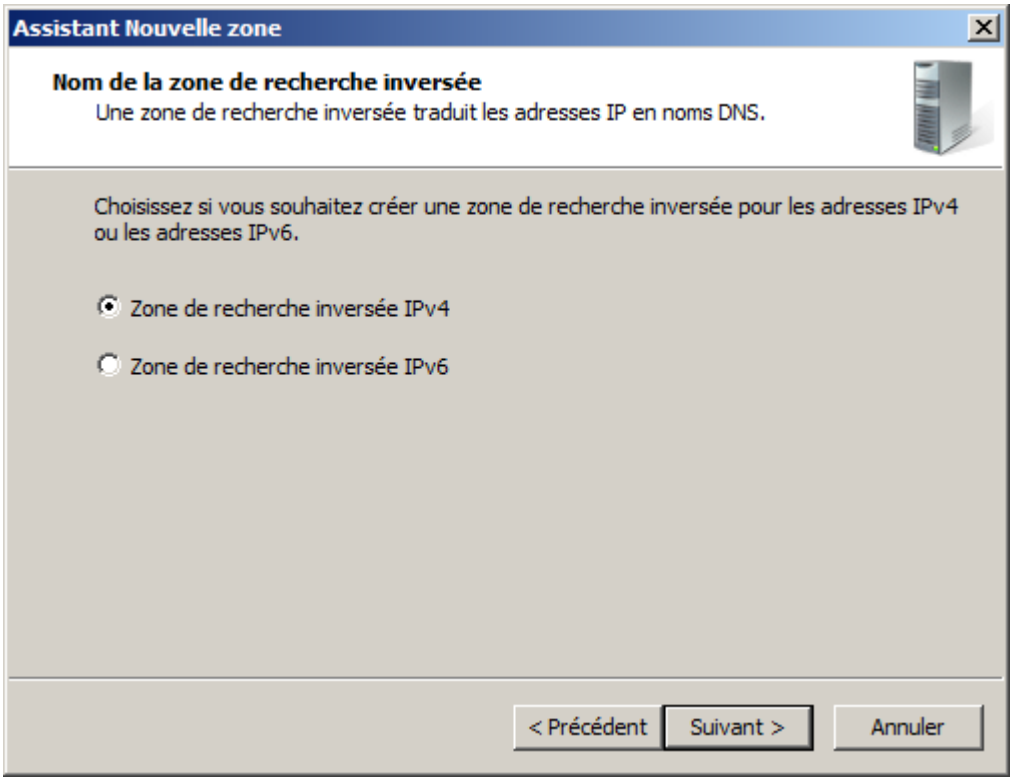
Si vous enregistrez la zone dans Active Directory, vous aurez alors le choix pour la réplication de cette zone. Il existe un bug sur cette partie : les deux premiers choix semblent identiques. Le choix par défaut est généralement le bon.



Sélection de la réplication

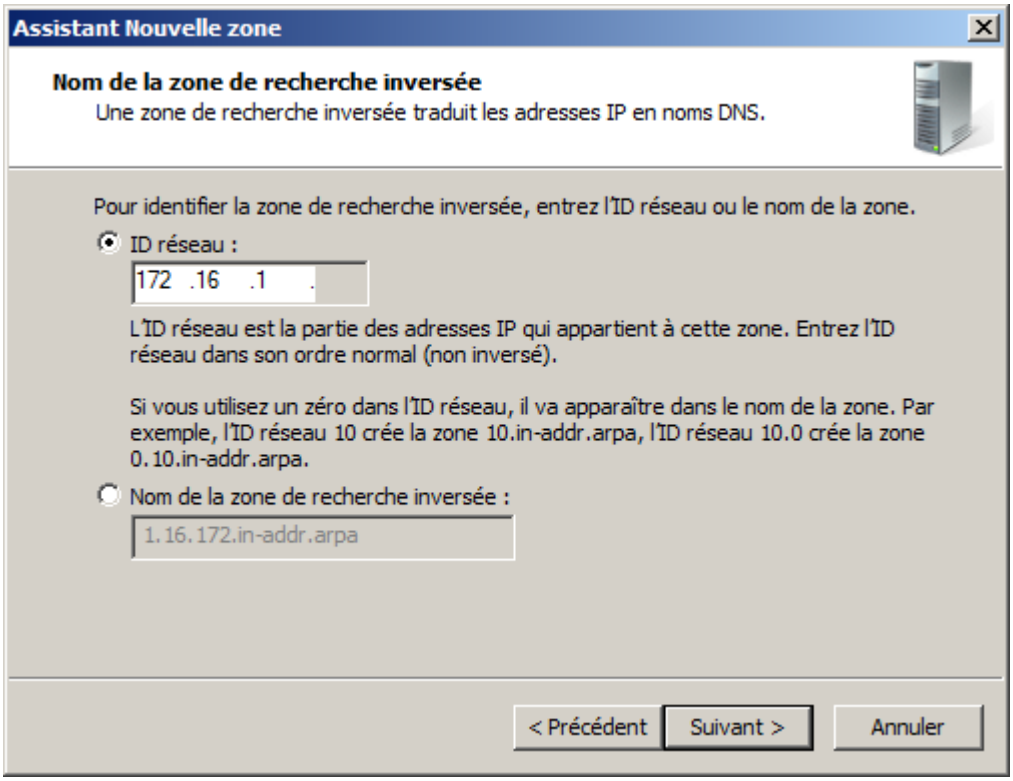
Un grand changement est intervenu dans la couche réseau à partir de Windows 2008. En effet, Windows 2008 (R2) est natif IPv6. Cela signifie qu'il utilise IPv6 par défaut. IPv4 est bien heureusement utilisable. Lors de la création de

la zone inversée, vous devrez choisir le type d'IP (v4 ou v6) qui constituera la zone. A moins que votre réseau soit déjà en IPv6, sélectionnez la zone IPv4.



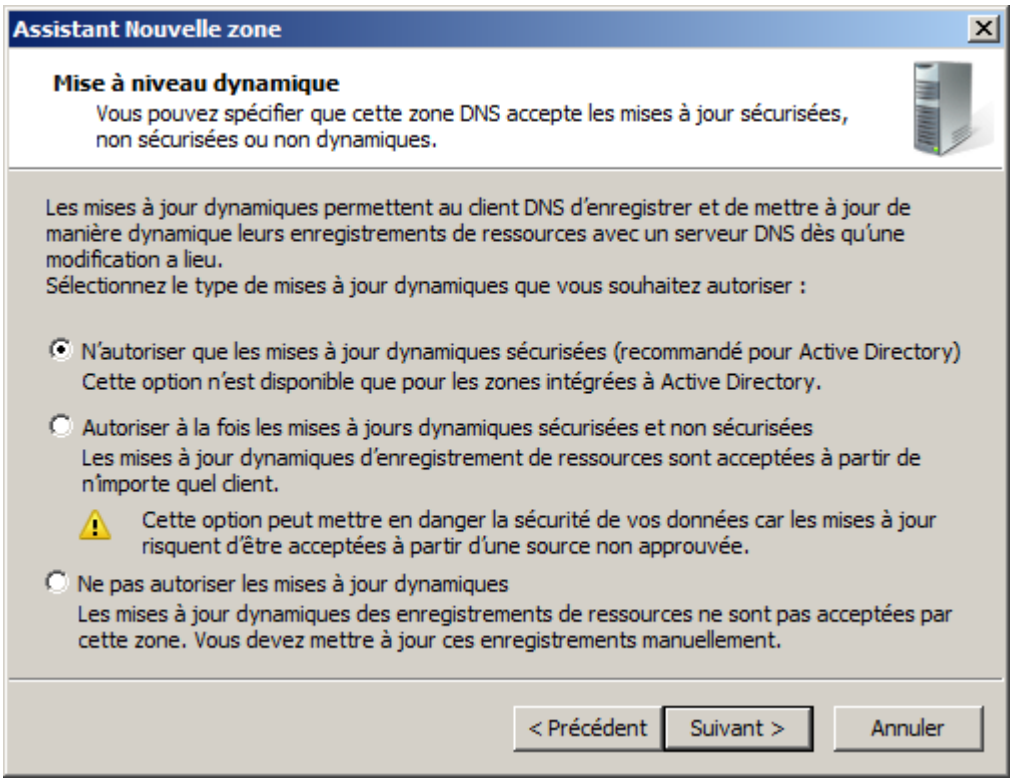
Type d'adresses IP

Vous devrez ensuite entrer l'ID de votre réseau. Mon réseau IP est 172.16.0.0/16. J'utilise notamment les IP 172.16.1.x donc mon ID de réseau sera 172.16.1.



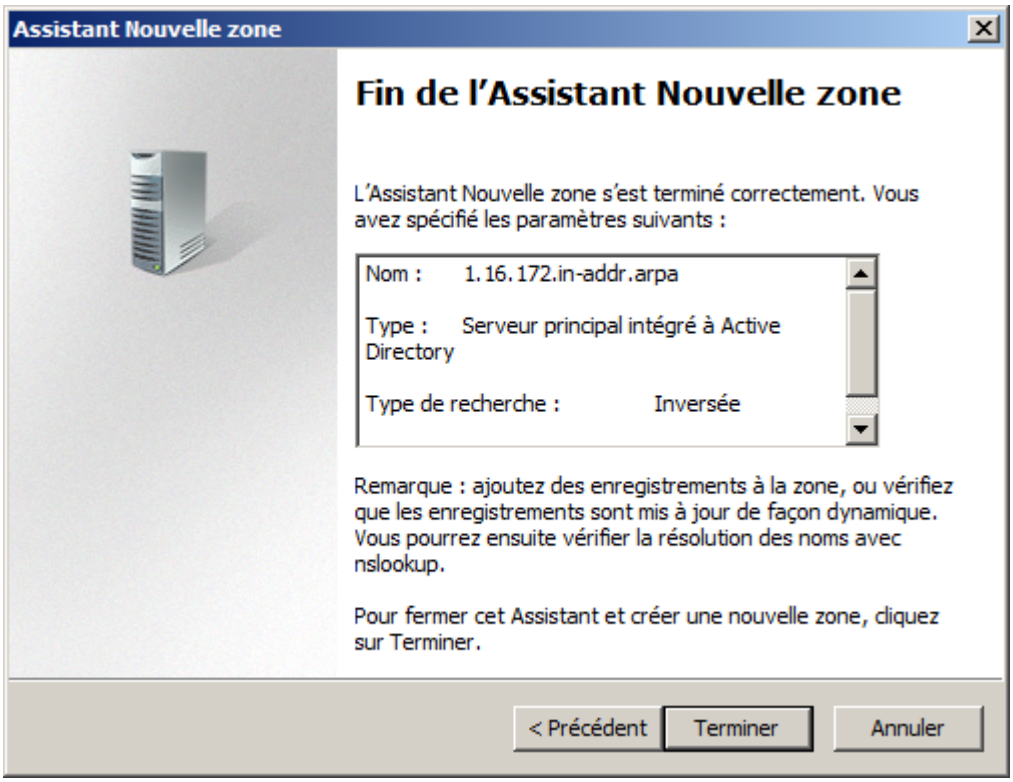
Inscription de l'identifiant de réseau

La dernière étape de configuration consiste à préciser comment la zone pourra être mise à jour. Votre choix dépendra du type de zone (intégrée à Active Directory ou non). Vous pourrez aussi choisir d'interdire les mises à jour dynamiques de la zone : elles seront alors manuelles. Je conseille ces mises à jour dynamiques automatiques : en mode manuel, cela induit une charge de travail très conséquente si vous souhaitez avoir des configurations IP attribuées par DHCP.



Sélection du type de mise à jour

Enfin, un résumé s'affiche. La zone sera créée lorsque vous terminerez l'assistant de création.

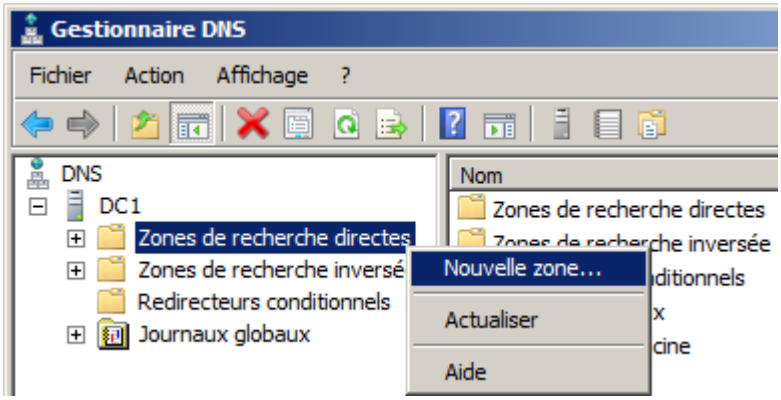


Résumé de la création de zone inversée

V-C-2 - Zone de recherche directe publique à usage privé

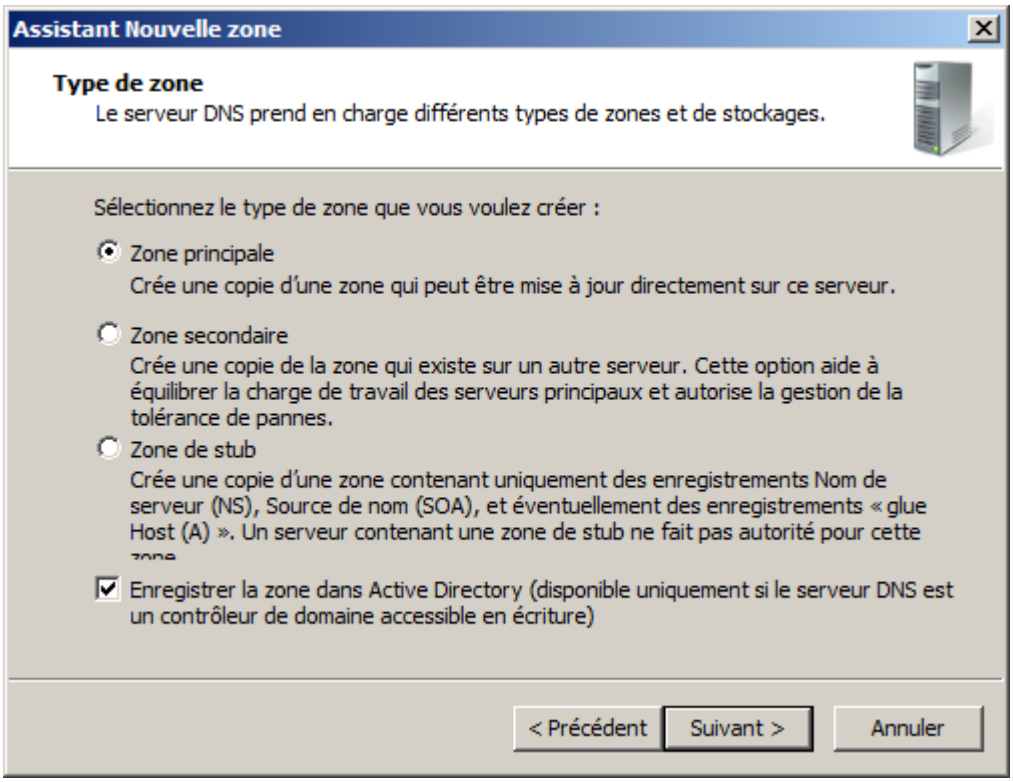
C'est ici que vous allez mettre en place le split-dns si vous avez choisi cette méthode. Cela consiste simplement à créer une zone portant le nom de votre domaine public. Cela va court-circuiter les requêtes de vos clients internes à destination de ce domaine : pour cette zone, ils vont rester en local puisqu'ils interrogent uniquement votre DNS normalement. Ce dernier possédant votre zone publique, il ne va pas interroger les serveurs DNS racines pour obtenir votre vraie zone publique.

Nous allons commencer par créer la zone de recherche directe. Dans la console de gestion du DNS, faites un clic droit sur *Zones de recherche directes, Nouvelle zone*.



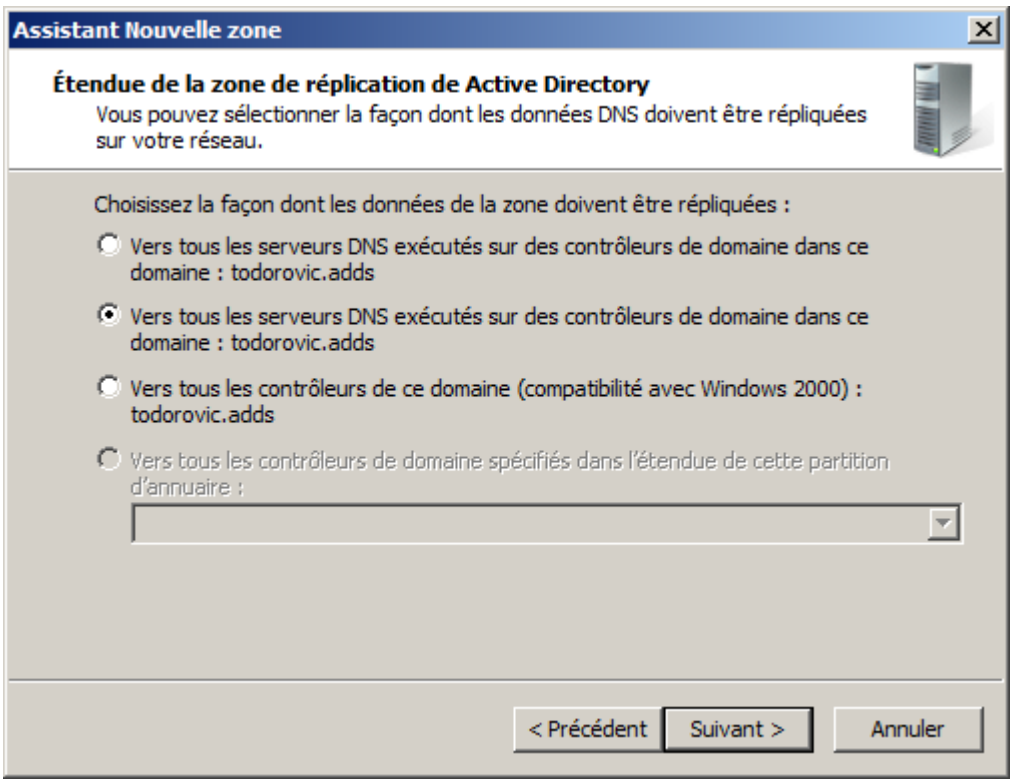
Création d'une nouvelle zone

Vous devrez ensuite sélectionner le type de zone. Nous avons besoin d'une zone principale stockée dans Active Directory.



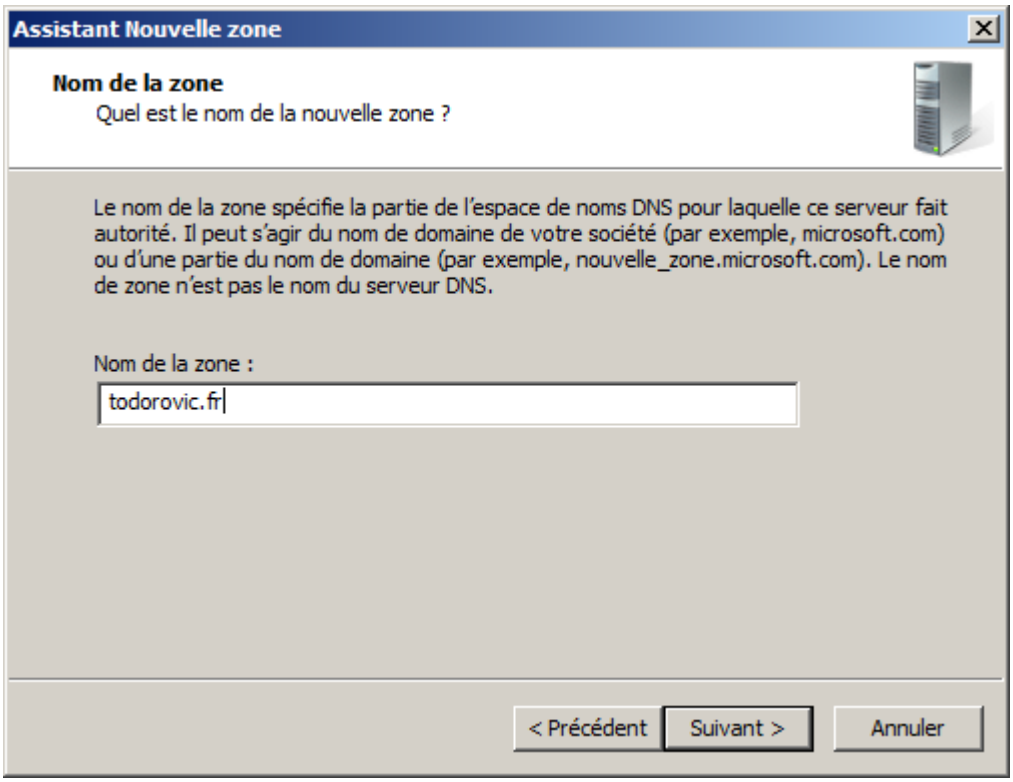
Création d'une nouvelle zone

La zone étant stockée dans Active Directory, on pourra sélectionner le fonctionnement de la réplication pour la zone DNS. Le choix par défaut est correct.



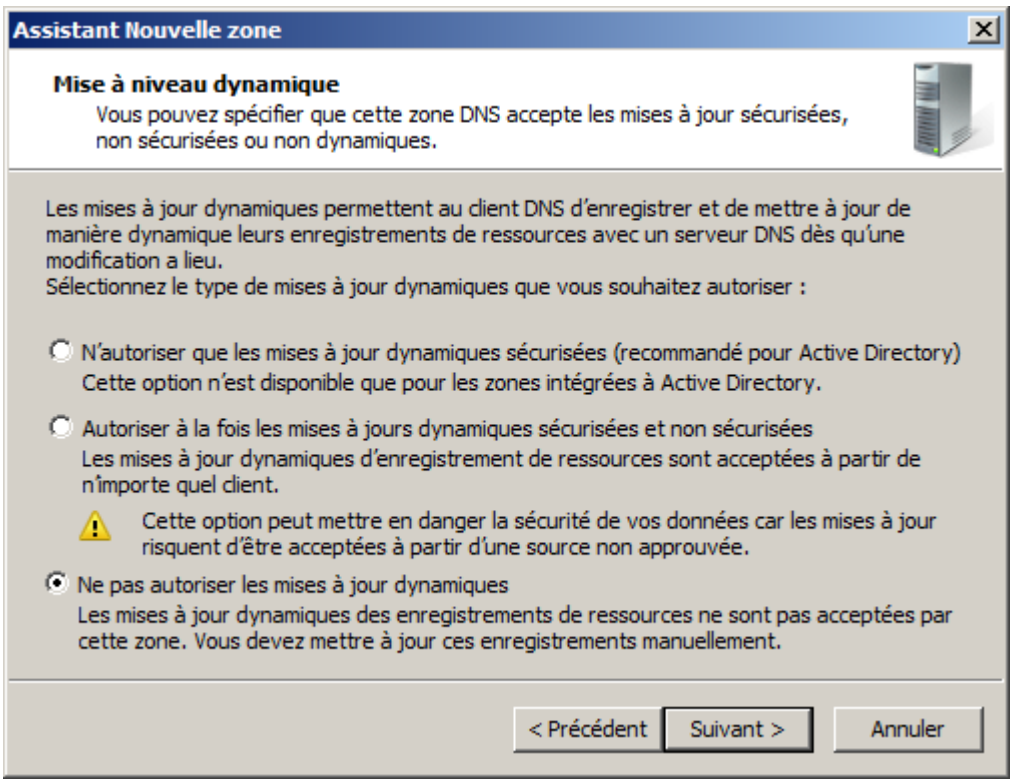
Réplication de la zone

Vous pourrez ensuite indiquer le nom de votre zone.



Nom de la zone

Normalement, vous n'aurez pas besoin des mises à jour dynamiques pour cette zone : il ne devrait y avoir que des enregistrements relatifs à vos serveurs. Afin d'éviter tout problème, désactivez les mises à jour dynamiques.



Interdiction des mises à jour dynamiques

Enfin, l'assistant affiche un résumé de la création à effectuer. Cliquez sur *Terminer* pour créer la zone. Vous pourrez ensuite créer (manuellement) des enregistrements pour vos serveurs.

V-C-3 - Redirecteurs

Un petit point sur les redirecteurs du DNS... Il n'y a pas besoin de renseigner ces redirecteurs. En effet, votre serveur DNS possède des indicateurs de racine. Lorsque votre DNS n'a pas de réponse à fournir, il va soit interroger les serveurs stockés dans les redirecteurs, soit interroger les serveurs DNS racines. S'il interroge les serveurs racines, il va constituer son propre cache et les réponses seront normalement fiables. Si vous interrogez les serveurs de votre FAI, vous aurez des réponses qui peuvent être anciennes : ces serveurs vont aller piocher dans leur cache. En faisant cela, vos réponses seront mises à jour toutes les 48h, ce qui peut être très long. Ne touchez pas aux redirecteurs, c'est inutile et peut vous poser plus de problèmes qu'autre chose. En revanche, les redirecteurs conditionnels sont différents et sont utilisés dans des cas où il faut interroger un serveur DNS particulier au lieu d'aller interroger les serveurs racines.

V-D - Réglage de l'heure via NTP

NTP (Network Time Protocol) est un protocole qui permet de régler l'heure d'une machine à partir d'un serveur de référence. Il existe différents niveaux de serveurs NTP (0 à 3, le plus faible étant le meilleur). En France, il n'existe que quelques serveurs de niveau 2 :

- ntp.obspm.fr
- ntp.univ.lyon1.fr
- ntp.via.ecp.fr

Nous allons définir ces trois serveurs comme serveur de temps sur votre Active Directory. Par défaut,

VI - Conclusion

Votre Active Directory est maintenant installé et fonctionnel. Il n'est pas encore totalement configuré : il vous reste la délégation de l'administration à effectuer, la mise en place de la sauvegarde, etc. Vous pourrez ajouter des ordinateurs et des utilisateurs dans votre Active Directory et ajouter des services comme le partage de fichier, le bureau à distance, etc. Il s'agit vraiment de la base de beaucoup d'applications réseaux, en tout cas dans le monde Microsoft.

VII - Remerciements

Je tiens à remercier **jacques_jean** pour sa relecture attentive.