

# 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.

#### Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

I - Introduction	3
II - Les bases	3
II-A - Les composants	
II-B - Sites et domaines	3
II-C - Arborescences et forêts	5
II-D - Niveau fonctionnel de forêt et de domaine : différentes fonctionnalités	5
II-E - Utilisateurs et ordinateurs	6
II-F - Groupes	6
II-G - RODC	7
II-H - DNS	7
III - Choisir correctement le nom de votre Active Directory	7
IV - Installation d'Active Directory	9
IV-A - Installation du rôle	9
IV-B - Assistant Installation des services de domaine Active Directory (dcpromo.exe)	16
V - Configuration sommaire	26
V-A - Configuration du site	26
V-B - Suffixe UPN	29
V-C - Configuration DNS	29
V-C-1 - Zone de recherche inversée	29
V-C-2 - Zone de recherche directe publique à usage privé	34
V-C-3 - Redirecteurs	37
V-D - Réglage de l'heure via NTP	37
VI - Conclusion	37
VII - Remerciements	37

- 2 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/



#### 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.

- 3 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. 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.

- 4 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.





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 ;

- 5 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

- 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 : A 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

**Wana** 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.

- 6 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



## 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 ma **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 **Set IIISTE**. 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. Renseignezvous 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.todorovic.fr. Ce besoin de split-dns est encore plus fort lorsque vous êtes en situation de mobilité avec Outlook Anywhere ou Office Communicator.

- 8 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



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.

- 9 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Gestionnaire de serveur				IJ×
Fichier Action Affichage ?				
🗇 🔿   🔽   👔				
Gestionnaire de serveur (DC1)	Gestionnaire de serveur (	(DC1)		
	Obtenir une vue ajouter ou supp	e d'ensemble de l'état de ce serveur, ef rimer des rôles et des fonctionnalités a	ffectuer des tâches de gestion de haut niveau, e u serveur.	et
Aide	Résumé serveur		Aide récapitulative sur le serveur	
	Informations sur l Nom complet de l'ordinateur :	'ordinateur dc1	Modifier les propriétés système file Afficher les connexions réseau Configurer le Bureau à distance Configurer la gestion à distance du	
	Groupe de travail : Connexion au	WORKGROUP Non connecté	Gestionnaire de serveur	
	réseau local : Connexion réseau sans fil :	192.168.9.8, Compatible IPv6		
	Bureau à distance :	Désactivé		
	Gestion à distance du gestionnaire de serveur :	Désactivé		
	ID du produit :			-
	Dernière actualisation : A	ujourd'hui à 11:18 Configurer l'actuali	sation	

Ajout du rôle

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

- 10 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/

×

## Assistant Ajout de rôles

Sélectionnez des	rôles de serveurs	
Avant de commencer Rôles de serveurs Confirmation État d'avancement Résultats	Sélectionnez un ou plusieurs rôles à installer sur ce serveur. Rôles : Hyper-V Serveur d'applications Serveur de télécopie Serveur DHCP Serveur DNS Services AD LDS (Active Directory Lightweight Directory Services Services AD FS (Active Directory Rights Management Services) Services ADFS (Active Directory Federation Services) Services Bureau à distance Services de certificats Active Directory Services de déploiement Windows Services de déploiement Windows Services de documents et d'impression Services de fichiers Services de stratégie et d'accès réseau Services WSUS (Windows Server Update Services) Ten savoir plus sur les rôles de serveur	Description : Les services de domaine Active Directory (AD DS) stockent des informations sur les objets sur le réseau et les rendent disponibles aux utilisateurs et aux administrateurs réseau. Ces services utilisent des contrôleurs de domaine pour donner accès aux ressources autorisées aux utilisateurs réseau n'importe où sur le réseau via un processus d'ouverture de session unique.
	< Précédent Suivant	> Installer Annuler

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.

- 11 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Assistant	Ajout de rôles		×
¢₁=	Ajouter les fonctionnalités requises p Directory ?	oour Services de domaine Active	
	Vous ne pouvez installer Services de domaine Active Dir également installées.	rectory que si les fonctionnalités requises sont	
	Fonctionnalités :	Description :	
	Fonctionnalités du .NET Framework 3.5.1 .NET Framework 3.5.1	Le <u>Microsoft .NET Framework 3.5.1</u> combine la puissance des API du .NET Framework 2.0 avec de nouvelles technologies pour la création d'applications qui offrent des interfaces utilisateur conviviales, protègent les informations d'identités personnelles de	
	[	Ajouter les fonctionnalités requises Annuler	
(i) Pour	quoi ces fonctionnalités sont-elles 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.

- 12 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/

X

#### Assistant Ajout de rôles



## Services de domaine Active Directory

Avant de commencer Rôles de serveurs	Introduction aux services de domaine Active Directory Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations
Services de domaine Active Direc Confirmation	de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs. Ils sont aussi nécessaires pour certaines applications fonctionnant avec annuaire, telles que Microsoft Exchange Server, et pour d'autres technologies Windows Server, telles que les Stratégies de groupe.
État d'avancement Résultats	<ul> <li>pour d'autres technologies Windows Server, telles que les Stratégies de groupe.</li> <li>À noter <ul> <li>Pour faire en sorte que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine pour un domaine.</li> <li>Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS ur ce serveur.</li> <li>Après l'installation des services de domaine Active Directory, utilisez l'Assistant Installation des services de domaine Active Directory installe aussi l'espace de noms DFS, la réplication DFS et les services de réplication de fichiers nécessaires au service d'annuaire.</li> </ul> </li> <li>Informations supplémentaires Présentation des services de domaine Active Directory Installation des services de domaine Active Directory Configurations communes pour les services de domaine Active Directory Configurations communes pour les services de domaine Active Directory</li></ul>
	< Précédent Suivant > Installer Annuler

Informations à propos d'Active Directory

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

- 13 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/

## Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Assistant Ajout de rôles		×
Confirmer les sél	ections pour l'installation	
Avant de commencer Rôles de serveurs Services de domaine Active Direc Confirmation État d'avancement Résultats	Pour installer les rôles, les services de rôle ou les fonctionnalités suivants, diquez sur Installer. <ul> <li>2 messages d'information ci-dessous</li> </ul> <ul> <li>I est possible que ce serveur doive être redémarré à la fin de l'installation.</li> <li>Services de domaine Active Directory</li> <li>Après l'installation des services de domaine Active Directory, utilisez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe) pour promouvoir le serveur au rang de contrôleur de domaine entièrement fonctionnel.</li> <li>Fonctionnalités du .NET Framework 3.5.1</li> </ul> INET Framework 3.5.1   Interformation 3.5.1 Interformation 3.5.1 Interformation 3.5.1	
	< Précédent Suivant > Installer Annuler	

Résumé de ce qui va être fait

- 14 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Assistant Ajout de rôles	
Progression de l'	installation
Avant de commencer Rôles de serveurs Services de domaine Active Direc Confirmation État d'avancement Résultats	Les rôles, les services de rôle ou les fonctionnalités suivants sont en cours d'installation :         Services de domaine Active Directory         Fonctionnalités du .NET Framework 3.5.1
	Installation
	< <u>Précédent</u> <u>Suivant</u> > <u>Installer</u> Annuler

#### 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.

- 15 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

Assistant Ajout de rôles		×
Résultats de l'inst	allation	
Avant de commencer Rôles de serveurs Services de domaine Active Direc Confirmation État d'avancement Résultats	Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés : <ul> <li>① 1 message d'Information ci-dessous</li> </ul> <ul> <li>② Services de domaine Active Directory</li> <li>② Installation réussie</li> </ul> Les services de rôle suivants ont été installés : <li>Contrôleur de domaine Active Directory</li> <li>① Utilisez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe) pour promouvoir le serveur en contrôleur de domaine opérationnel.</li> <li>Ferrez cet Assistant et lancez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe).</li> <li>⑦ Onctionnalités du .NET Framework 3.5.1</li> <li>② Installation réussie</li> <li>Les fonctionnalités suivantes ont été installées :</li> <li>.NET Framework 3.5.1</li> Installation réussie Nettre renzevore 3.5.1	
	< <u>P</u> récédent <u>S</u> uivant > <u>E</u> ermer Annuler	

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.

- 16 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



assistant Installation de	s services de domaine Active Directory	×
	Assistant Installation des services de domaine Active Directory	
	Cet Assistant vous aide à installer les services de domaine Active Directory (AD DS) sur ce serveur, faisant du serveur un contrôleur de domaine Active Directory. Pour continuer, cliquez sur Suivant.	
	Utiliser l'installation en mode avancé En savoir plus sur les options supplémentaires disponibles dans l'installation en mode avancée.	
	En savoir plus sur les <u>services de domaine Active Directory</u>	
	< Précédent Suivant > Annule	r

#### 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.

- 17 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Assistant Installation des services de domaine Active Directory	×
Compatibilité du système d'exploitation Les paramètres de sécurité étendus dans Windows Server 2008 et Windows Server 2008 R2 affectent les versions précédentes de Windows	
▲ Les contrôleurs de domaine Windows Server 2008 et "Windows Server 2008 R2 " offrent un nouveau paramètre par défaut mieux sécurisé, "Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ". Ce paramètre empêche Microsoft Windows et les " clients " non-Microsoft SMB d'utiliser des algorithmes de chiffrement faibles de type NT 4.0 dans des sessions sur canal sécurisé vers des contrôleurs de domaine Windows Server 2008 ou " Windows Server 2008 R2". Désormais, les opérations et applications qui requièrent un canal sécurisé servi par un contrôleur de domaine Windows Server 2008 ou " Windows Server 2008 R2 " peuvent échouer. Les plateformes concernées incluent Windows NT 4.0, ainsi que les " clients " non- Microsoft SMB et les périphériques NAS non compatibles avec les algorithmes de chiffrement forts. Certaines opérations sur les clients exécutant une version de Windows antérieure à Vista avec le Service Pack 1 sont également concernées, notamment les jonctions aux domaines effectuées par l'outil de migration Active Directory ou les Services de déploiement Windows. Pour plus de détails à ce sujet, voir l'article 942564 (http://go.microsoft.com/fwlink/? LinkId=104751).	
< Précédent Suivant > An	nuler

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.

- 18 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Assistant Installation des services de domaine Active Directory	×
Choisissez une configuration de déploiement Vous pouvez créer un contrôleur de domaine pour une forêt nouvelle ou existante.	
O Forêt existante	
C Ajouter un contrôleur de domaine à un domaine existant	
C Créer un nouveau domaine dans une forêt existante	
Ce serveur va devenir le premier contrôleur de domaine du nouveau domaine.	
Créer un domaine dans une nouvelle forêt	
En savoir plus sur les <u>configurations de déploiement possibles</u>	
< Précédent Suivant > A	Innuler

Créer ou rejoindre une forêt ?

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

- 19 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

🗃 Assistant Installation des services de domaine Active Directory	×
Nommez le domaine racine de la forêt Le premier domaine de la forêt est le domaine racine de la forêt. Il porte également le nom de la forêt.	
Entrez le nom de domaine complet du nouveau domaine racine de forêt.	
Nom de domaine complet du domaine racine de forêt :	
todorovic.adds	
Exemple : corp.contoso.com	
( Bréaddant - Colomba	Annular 1
< Precedent Sulvant >	Annuler

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 ( If r 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.

- 20 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.





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.

Assistant Installation des services de domaine Active Directory	×
Définir le niveau fonctionnel de la forêt Sélectionnez le niveau fonctionnel de la forêt.	
Niveau fonctionnel de la forêt :	
Windows Server 2008 R2	
Windows 2000 Windows Server 2003 Windows Server 2008	
Windows Server 2008 R2 Torretionmalites disponibles dans le niveau fonctionnel de foret windows Server 2008, ainsi que les fonctionnalités supplémentaires suivantes : - Corbeille, qui, lorsqu'elle est activée, permet de restaurer des objets supprimés dans leur intégralité pendant que les services de domaine Active Directory s'exécutent. Tout nouveau domaine créé dans cette forêt fonctionne par défaut au niveau	
Vous ne pourrez ajouter à cette forêt que des contrôleurs de domaine qui exécutent Windows Server 2008 R2 ou ultérieur.	
En savoir plus sur les <u>niveaux fonctionnels de forêt et de domaine</u>	
< Précédent Suivant > A	Annuler

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 sousensemble 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

- 21 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



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).

Assistant Installation des services de domaine Active Directory	×
Options supplémentaires pour le contrôleur de domaine	
Sélectionnez des options supplémentaires pour ce contrôleur de domaine.	
Serveur DNS	
🔽 Catalogue global	
Contrôleur de domaine en lecture seule (RODC)	
Informations supplémentaires :	
Nous vous recommandons d'installer le service Serveur DNS sur le premier contrôleur de domaine.	
En savoir plus sur les <u>options supplémentaires du contrôleur de domaine</u>	
< Précédent Suivant > A	nnuler

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.

🖥 Assistant Installation des services de domaine Active Directory		
Emplacement de la base de données, des fichiers journaux et de SYSVOL Spécifiez les dossiers qui contiendront la base de données du contrôleur de domaine Active Directory, les fichiers journaux et SYSVOL.		
Pour de meilleures performances et une meilleure récupération, stockez données et les fichiers journaux sur des volumes séparés. Dossier de la base de données :	: la base de	
D:\AD-developpez\NTDS	Parcourir	
Dossier des fichiers journaux :		
D:\AD-developpez\NTDS	Parcourir	
Dossier SYSVOL :		
D:\AD-developpez\SYSVOL	Parcourir	
En savoir plus sur le <u>placement des fichiers des services de domaine A</u>	<u>ctive Directory</u>	
< Précédent Su	ivant > Ar	nuler

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.

- 23 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



assistant Installation des services de domaine Active Directory	×
Mot de passe administrateur de restauration des services d'annuaire	
Le compte d'administration de restauration des services d'annuaire est différent du compte d'administrateur de domaine.	
Attribuez un mot de passe au compte d'administrateur qui sera utilisé lors du démarrage de ce contrôleur de domaine en mode Restauration des services d'annuaire. Nous vous recommandons de choisir un mot de passe fort.	
Mot de passe :	
Confirmer le mot de passe :	
En savoir plus sur le <u>mot de passe de restauration des services d'annuaire</u>	
< Précédent Suivant >	Annuler

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.

- 24 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



Assistant Installation des services de domaine Active Directory Résumé	
Vérifiez vos sélections :	
Configurer ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.	
Le nouveau nom de domaine est « todorovic.adds ». C'est aussi le nom de la nouvelle forêt.	
Le nom NetBIOS du domaine est « TODOROVIC ».	
Niveau fonctionnel de la forêt : Windows Server 2008 R2	
Niveau fonctionnel du domaine : Windows Server 2008 R2	
Site : Default-First-Site-Name	
Pour modifier une option, cliquez sur Précédent. Pour commencer l'opération, cliquez sur Suivant.	
Vous pouvez exporter ces paramètres dans un fichier de réponses pour les utiliser avec d'autres opérations d' installation sans assistance. En savoir plus sur l' <u>utilisation d'un fichier de réponse</u>	
< Précédent Suivant > An	nuler

Résumé de l'installation

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

Assistant Installation des services de domaine Active Directory
L'Assistant effectue la configuration des services de domaine Active Directory. Ce processus peut durer de quelques minutes à quelques heures, en fonction de votre environnement et des options que vous avez sélectionnées.
En attente de la fin de l'installation du service DNS
Annular
I Redemarrer a la fin de l'operation

Installation en cours

- 25 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/





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*.

Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



	Panneau de configuration Périphériques et imprimantes Outils d'administration Aide et support Exécuter	Sites et services Active Directory Sources de données (ODBC) Stratégie de sécurité locale Utilisateurs et ordinateurs Active Directory Windows PowerShell Modules
Tous les programmes		
Rechercher les programmes et fichiers       Image: Construction of the second seco		

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.

📲 Sites et services Active Director	γ				
Fichier Action Affichage ?					
🗢 🔿 🙍 📊 🗐 🙆 🛃	1 🖬 🛛 🗾				
Sites et services Active Directory [c Sites Subnets Subnets Default-First-Site-Name	Nom Default-First-Site-Name Inter-Site Transports Subnets	Emplacement	Type Site Conteneur de t Conteneur de s	Description	

- 27 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/

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.

Nouvel objet - Sous-réseau	×
Créer dans : todorovic.adds/Configuration/Sites/Subnets	
Entrez le préfixe d'adresse en utilisant la notation de préfixe réseau (adresse/longueur du préfixe), où la longueur du préfixe indique le nombre de bits fixes. Vous pouvez entrer un préfixe de sous-réseau IPv4 ou IPv6. En savoir plus sur l'entrée des préfixes d'adresse.	
Exemple IPv4 : 157.54.208.0/20	
Exemple IPv6 : 3FFE:FFFF:0:C000::/64	
Préfixe :	
172.16.0.0/16	
Nom du préfixe des services de domaine Active Directory :	
172.16.0.0/16	
Sélectionnez un objet du site pour ce préfixe.	
Nom du site	1
Siege	
OK Annuler Aide	

Association du sous-réseau au site

- 28 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



## 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.

😹 Domaines et approbations Active Dire	C Nom	Type	Actions
∎	Changer de forêt Changer le contrôleur de domaine Active Directory Maître d'opérations Augmenter le niveau fonctionnel de la forêt		
	Affichage		•
	Actualiser Exporter la li	ste	
	Propriétés		

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 peutêtre 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.

- 29 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.





Console de gestion DNS

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

🛔 Gestionnaire DNS		
Gestionnaire DNS         Fichier       Action       Affichage ?         Image: Construction of the second secon	Nom Zones de recherche directes Zones de recherche inversée Redirecteurs conditionnels Nouvelle zone	
	Aide	
Crée une 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.

- 30 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

## 

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Assistant Nouvelle zone	×
Type de zone         Le serveur DNS prend en charge différents types de zones et de stockages.	
Sélectionnez le type de zone que vous voulez créer :	
Zone principale Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.	
<ul> <li>Zone secondaire</li> <li>Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.</li> <li>Zone de stub</li> <li>Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone</li> </ul>	
Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)	
< Précédent Suivant > Annuler	

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.

Assistant Nouvelle zone	×
Étendue de la zone de réplication de Active Directory Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.	
Choisissez la façon dont les données de la zone doivent être répliquées :	
O Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : todorovic.adds	
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : todorovic.adds	
Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : todorovic.adds	
Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :	T
< Précédent Suivant > Ar	nnuler

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

- 31 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



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.

Assistant Nouvelle zone	×
Nom de la zone de recherche inversée Une zone de recherche inversée traduit les adresses IP en noms DNS.	
Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresse ou les adresses IPv6.	s IPv4
Zone de recherche inversée IPv4	
C Zone de recherche inversée IPv6	
	. 1
< Précédent Suivant > An	nuler

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.

Assistant Nouvelle zone		×
Nom de la zone de recherche inversée Une zone de recherche inversée traduit les	adresses IP en noms DNS.	
<ul> <li>Pour identifier la zone de recherche inversée</li> <li>ID réseau :</li> <li>I72 .16 .1</li> <li>L'ID réseau est la partie des adresses IP réseau dans son ordre normal (non inver Si vous utilisez un zéro dans l'ID réseau, exemple, l'ID réseau 10 crée la zone 10. 0.10.in-addr.arpa.</li> <li>Nom de la zone de recherche inversée :</li> <li>1.16.172.in-addr.arpa</li> </ul>	e, entrez l'ID réseau ou le nom qui appartient à cette zone. I rsé). il va apparaître dans le nom d in-addr.arpa, l'ID réseau 10.0	n de la zone. Entrez l'ID le la zone. Par l crée la zone
	< Précédent Suivant >	Annuler

#### Inscription de l'identifiant de réseau

- 32 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



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.

Assistant Nouvelle zone	×
Mise à niveau dynamique Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.	
Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'u modification a lieu. Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :	de ne
N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Di Cette option n'est disponible que pour les zones intégrées à Active Directory.	rectory)
Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à parti n'importe quel client.	r de
Cette option peut mettre en danger la sécurité de vos données car les mises risquent d'être acceptées à partir d'une source non approuvée.	à jour
Ne pas autoriser les mises à jour dynamiques Les mises à jour dynamiques des enregistrements de ressources ne sont pas accept cette zone. Vous devez mettre à jour ces enregistrements manuellement.	ées par
< Précédent Suivant > A	nnuler

Sélection du type de mise à jour

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

## 

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)



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*.

🛔 Gestionnaire DNS		
Fichier Action Affichage ?		
🗢 🔿 🖄 🖬 🗶 🖬 🧕	🛛 🖬   🗄 🔲 (	<b>j</b>
<ul> <li>BNS</li> <li>□ □ □ DC1</li> <li>□ □ Zones de recherche directes</li> <li>□ □ Zones de recherche inversé</li> <li>□ □ Zones de recherche inversé</li> <li>□ □ Redirecteurs conditionnels</li> <li>□ □ Journaux globaux</li> </ul>	Nom Zones de recher Nouvelle zone Actualiser Aide	rche directes che inversée iditionnels x cine

Création d'une nouvelle zone

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

- 34 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Assistant Nouvelle zone	×
<b>Type de zone</b> Le serveur DNS prend en charge différents types de zones et de stockages.	
Sélectionnez le type de zone que vous voulez créer :	
Zone principale Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.	
<ul> <li>Zone secondaire</li> <li>Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.</li> <li>Zone de stub</li> <li>Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone</li> </ul>	
Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS e un contrôleur de domaine accessible en écriture)	est
< Précédent Suivant > Annule	er

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.

Assistant Nouvelle zone	X
Étendue de la zone de réplication de Active Directory Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.	
Choisissez la façon dont les données de la zone doivent être répliquées :	
O Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : todorovic.adds	
<ul> <li>Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : todorovic.adds</li> </ul>	
O Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : todorovic.adds	
<ul> <li>Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire ;</li> </ul>	
	7
< Précédent Suivant > An	nuler

Réplication de la zone

Vous pourrez ensuite indiquer le nom de votre zone.

- 35 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC. http://mtodorovic.developpez.com/tutoriels/windows/installation-active-directory-sous-windows-server-2008-r2/

Installation d'Active Directory sous Windows Server 2008 R2 par Michaël Todorovic (Autres articles) (Blog)

Assistant Nouvelle zone	×
Nom de la zone Quel est le nom de la nouvelle zone ?	1
Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveu autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft. ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le de zone n'est pas le nom du serveur DNS.	r fait com) : nom
Nom de la zone :	
todorovic.fr	
< Précédent Suivant > An	nuler

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.

Assistant Nouvelle zone	×
Mise à niveau dynamique Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.	
Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'u modification a lieu. Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :	r de ine
O N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active D Cette option n'est disponible que pour les zones intégrées à Active Directory.	irectory)
C Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à part n'importe quel client.	ir de
Cette option peut mettre en danger la sécurité de vos données car les mises risquent d'être acceptées à partir d'une source non approuvée.	à jour
Ne pas autoriser les mises à jour dynamiques Les mises à jour dynamiques des enregistrements de ressources ne sont pas accept cette zone. Vous devez mettre à jour ces enregistrements manuellement.	tées par
< Précédent Suivant >	Annuler

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.

- 36 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.



## 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.

- 37 -Copyright 2010 - Michaël Todorovic. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts. Droits de diffusion permanents accordés à developpez LLC.