Chapitre 1
Introduction

Chapitre 2
Domaine Active Directory

Chapitre 3

Architecture distribuée d'accès aux ressources

Chapitre 4

Mise en place d'un système de messagerie

Chapitre 5

Mise en place des services réseaux d'entreprise

Chapitre 6

Déploiement des serveurs et postes de travail

Chapitre 7
Terminal Services

Chapitre 8
Accès distants

Chapitre 9

Application Internet

Chapitre 10

Limiter les possibilités d'attaque avec Server Core

Chapitre 11

Consolider vos serveurs

Chapitre 12

Sécuriser votre architecture

Chapitre 13

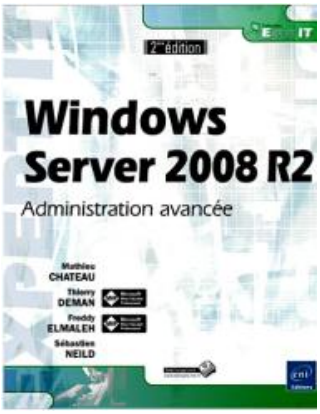
Cycle de vie de votre infrastructure

Chapitre 14
Se préparer pour le futur

Windows Server 2008 R2

Administration avancée [2ième édition]

Thierry DEMAN - Freddy ELMALEH - Mathieu CHATEAU - Sébastien NEILD



Résumé

Ce livre s'adresse aux **administrateurs et ingénieurs systèmes** désireux d'acquérir et de maîtriser des connaissances approfondies sur **Windows Server 2008 R2**.
Il répond aux besoins d'expertise du lecteur en traitant de façon approfondie, d'un point de vue théorique et pratique, des rôles incontournables comme **Active Directory, DFS, Hyper-V, la répartition de charge** ou encore le **VPN**.
Toutes les spécificités de Windows 2008 R2 sont également expliquées (comme la **corbeille Active Directory**, **Direct Access** etc..) afin de vous permettre d'utiliser pleinement le potentiel de cette version. Dans cet ouvrage mis à jour, les auteurs présentent les dernières innovations du Service Pack 1 (technologie **RemoteFX** du bureau à distance, **Mémoire Dynamique** sous Hyper-V, etc..).
Depuis le **déploiement** en passant par le **clustering** et jusqu'à la **virtualisation**, cet ouvrage est le compagnon idéal pour appréhender les moindres détails de cette version de Windows Server. Il apporte un haut niveau d'expertise et son ambition est de devenir un livre de référence.
Les auteurs mettent au service du lecteur **leur expertise Microsoft** (MVP, MCSE et/ou MCITP) et leur expérience très significative dans des **infrastructures conséquentes et complexes**, afin de fournir un livre de qualité respectant les meilleures pratiques du monde de l'entreprise.

Les chapitres du livre :
Introduction – Domaine Active Directory – Architecture distribuée d'accès aux ressources – Haute disponibilité – Mise en place des services réseaux d'entreprise – Déploiement des serveurs et postes de travail – Bureau à distance (Terminal Services) – Accès distant – Application Internet – Limiter les possibilités d'attaque avec Server Core – Consolider vos serveurs – Sécuriser votre architecture – Cycle de vie de votre infrastructure – Se préparer pour le futur

L'auteur

Thierry Deman est Architecte systèmes et maîtrise les technologies Microsoft depuis de nombreuses années au sein du Permis Informatique. Il est reconnu Microsoft MVP (Most Valuable Professional) sur Exchange depuis plusieurs années et est certifié MCITP Exchange 2007 et MCITP Enterprise Administrator sur Windows Server 2008.
Freddy Elmaleh est consultant freelance, architecte systèmes et chef de projet, expert Active Directory et Sécurité, fondateur de la société de services Active IT. Il intervient au sein de nombreuses grandes entreprises. Il est reconnu Microsoft MVP (Most Valuable Professional) sur Windows Server - Directory Services depuis plusieurs années et est certifié MCSE Securité/Messagerie et MCITP Enterprise Administrator sur Windows Server 2008.
Mathieu Chateau est Architecte freelance avec une triple compétence Microsoft, réseau et sécurité. Il apporte ainsi son expertise auprès des entreprises avec une vision globale de l'infrastructure.
Sébastien Neild est Ingénieur Systèmes et Réseaux dans une société de service. Il intervient en tant que responsable de projets Active Directory et Exchange et a participé à de nombreux projets de déploiement et migration d'infrastructures Windows Server. Il est certifié MCSE et MCITP Server Administrator sur Windows Server 2008.

Thierry Deman est reconnu **Microsoft MVP (Most Valuable Professionnal)** sur Exchange Server.
Freddy Elmaleh est reconnu **Microsoft MVP (Most Valuable Professionnal)** sur Windows Server - Directory Services.

Ce livre numérique a été conçu et est diffusé dans le respect des droits d'auteur. Toutes les marques citées ont été déposées par leur éditeur respectif. La loi du 11 Mars 1957 n'autorisant aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective", et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, "toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayant cause, est illicite" (alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal. Copyright Editions ENI

Ce livre numérique intègre plusieurs mesures de protection dont un marquage lié à votre identifiant visible sur les principales images.

Avant-propos

Ce livre s'adresse aux administrateurs et ingénieurs système désireux d'acquérir et de maîtriser des connaissances approfondies sur Windows Server 2008 R2.

Il répond aux besoins d'expertise du lecteur en traitant de façon approfondie des rôles incontournables comme **Active Directory**, **DFS**, **Hyper-V**, **la répartition de charge** ou encore le VPN.

L'ouvrage aborde ces différents sujets de façon théorique mais aussi pratique afin que le lecteur puisse avoir les éléments suffisants pour comprendre une technologie mais également les bienfaits de son utilisation au sein de son entreprise.

Toutes les nouveautés R2 de Windows Server 2008 sont également expliquées en détail (comme la **corbeille Active Directory**, **Direct Access**, etc.) afin de permettre au lecteur d'utiliser pleinement les spécificités de cette version. Dans cet ouvrage mis à jour, les auteurs présentent les dernières innovations du Service Pack 1 (technologie **RemoteFX**, **Mémoire Dynamique** sous Hyper-V, etc.).

Les évolutions majeures de cette version comme les **services du bureau à distance** ou bien la mise en quarantaine à l'aide de **NAP** présentent des avantages conséquents en entreprise et sont donc traitées de façon détaillée dans cet ouvrage.

Depuis le **déploiement** en passant par le **clustering** et jusqu'à la **virtualisation**, cet ouvrage est le compagnon idéal pour appréhender les moindres détails de cette version de Windows Server. Il apporte un haut niveau d'expertise et a une approche pragmatique.

Son ambition est de devenir un livre de référence, accessible par les administrateurs système aussi bien de PME que de grandes entreprises.

Les auteurs mettent au service du lecteur leur expertise Microsoft (MVP, MCSE et/ou MCITP) et leur expérience très significative dans des infrastructures conséquentes et complexes, afin de fournir un livre de qualité respectant les meilleures pratiques du monde de l'entreprise.

Ils mettent en avant les cas de figure les plus couramment rencontrés en entreprise, ainsi que les pièges à éviter pour permettre une intégration idéale de ce nouveau système d'exploitation au sein du Système d'Information en place.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce livre traite du dernier système d'exploitation de la gamme Windows Server de Microsoft.

Il s'agit bien entendu de Windows Server 2008 R2.

Windows Server 2008 R2 possède au moins les mêmes fonctionnalités et une interface quasi identique à Windows Server 2008. Néanmoins, dans un souci de clarté, nous ne nous intéresserons, dans cet ouvrage, qu'à la version 2008 R2.

Windows Server 2008 R2 a été pensé par Microsoft pour offrir une plate-forme souple et complète afin de répondre aux besoins sans cesse grandissant des entreprises. Vous pouvez ainsi profiter de nouvelles fonctionnalités à la fois utiles et judicieuses vous permettant de faire reposer l'ensemble de votre système d'information sur une solution Microsoft.

Le Service Pack 1 de Windows 2008 R2, paru en février 2011, intègre également quelques fonctionnalités intéressantes qui seront abordées dans cet ouvrage.

© ENI Editions - All rights reserved - adamo diarra

Les différentes éditions de Windows Server 2008 R2

Comme à l'accoutumée, Microsoft Windows Server 2008 R2 est disponible dans différentes éditions. Il n'existe pas moins de 9 versions différentes de ce système d'exploitation.

- Windows Server 2008 R2 Edition Standard avec ou sans Hyper-V
- Windows Server 2008 R2 Edition Enterprise avec ou sans Hyper-V
- Windows Server 2008 R2 Edition Datacenter avec ou sans Hyper-V
- Windows Server 2008 R2 Foundation
- Windows HPC Server 2008 R2
- Windows Web Server 2008 R2
- Windows Storage Server 2008 R2
- Windows Small Business Server 2008 R2 pour les PME
- Windows Essential Business Server 2008 R2 pour les PME
- Windows Server 2008 R2 pour Systèmes Itanium-based

Windows Server 2008 R2 n'est disponible qu'en version 64 bits.

Vous trouverez un descriptif détaillé de ces différentes versions sur le site suivant :

http://www.microsoft.com/windowsserver2008/en/us/editions.aspx (en anglais)

© ENI Editions - All rights reserved - adamo diarra

Les grands axes de Windows Server 2008 R2

Lors de l'étude des axes majeurs à suivre pour cette version de Windows Server, Microsoft a pris en considération la charge de travail et la pression sans cesse grandissante sur le service IT des entreprises. Il fallait donc que ce système d'exploitation réponde à trois exigences essentielles.

1. Un meilleur contrôle de l'information

Windows Server 2008 R2 propose un meilleur contrôle de l'information afin de garantir une meilleure efficacité d'administration et par conséquent une meilleure productivité.

Afin d'augmenter cette qualité d'administration, Windows Server 2008 R2 possède une capacité de script et d'automatisation de tâches accrues grâce au nouveau langage de script Microsoft **Windows Powershell**. L'automatisation des tâches courantes d'administration se voit ainsi grandement améliorée et plus flexible grâce à cette nouvelle fonctionnalité.

Le **service d'annuaire Active Directory** se voit également doté, depuis Windows Server 2008 R2, de fonctionnalités comme la corbeille Active Directory ou la gestion automatique des mots de passe des comptes de services qui raviront plus d'un administrateur.

L'installation basée sur les rôles et fonctionnalités grâce à la console unique **Gestionnaire de serveur** facilite l'administration. Les assistants disponibles permettent de limiter au maximum les erreurs de configuration grâce aux nombreuses explications qui viennent accompagner l'administration lors de l'installation d'un composant Windows.

Microsoft offre également la possibilité d'installer une version minimale de Windows Server 2008 R2, connue sous le nom de **Windows Server Core**. Cette version fonctionne alors sans interface graphique et tout doit donc être configuré en ligne de commande. L'avantage majeur de ce type d'installation réside dans le fait que la surface d'attaque est réduite par le fait que le strict minimum est installé sur le serveur. Les administrateurs viendront alors ajouter les rôles de leurs choix. Afin de ne pas trop exposer ces serveurs, le .NET Framework n'est pas installé et l'exécution de code comme PowerShell n'est donc pas possible.

Des nouvelles consoles comme le **moniteur de performance et de fiabilité** permettent également de détecter en amont des problèmes de configuration sur vos systèmes d'exploitation et d'en informer automatiquement le service informatique. Il offre également beaucoup d'informations précises sur l'utilisation des composants système de votre choix.

Une meilleure gestion de l'impression est désormais possible ! En effet, les imprimantes peuvent être automatiquement installées sur les ordinateurs des utilisateurs à l'aide de stratégies de groupe.

Une nouvelle console MMC vous permet de mieux gérer, contrôler et dépanner les imprimantes de votre domaine.

Enfin, dernière bonne nouvelle pour les administrateurs, les règles Applocker permettront un meilleur contrôle des applications autorisées à être utilisées avec Windows Server 2008 R2 et Windows 7.

2. Une meilleure protection du système d'information

Microsoft a totalement retravaillé les noyaux de Windows Server 2008 et 2008 R2 comparé au noyau de leurs prédécesseurs. Celui-ci présente de nombreuses similitudes avec celui de Windows Vista ou de Windows 7 puisque les deux systèmes d'exploitation se basent sur le nouveau noyau répondant au nom de NT6 (Windows 2000 et XP reposaient sur le noyau NT 5.x).

Ce noyau possède ainsi la nouvelle technologie **Patchguard** développée par Microsoft afin de protéger au maximum le système d'exploitation et ainsi de mettre un terme au rootkit ou autre attaque visant à modifier le noyau système.

La **protection de l'accès réseau (NAP)** devient également accessible et vous permet de mettre en place des conditions d'utilisation de votre réseau d'entreprise. Exit donc les personnes externes arrivant avec un ordinateur portable qui n'est pas à la norme de l'entreprise ou bien l'utilisateur n'ayant pas un antivirus à jour ! L'accès au réseau leur est refusé tant qu'ils ne remplissent pas les critères de conformité que vous aurez jugés nécessaires.

Les **contrôleurs de domaine en lecture seule (RODC)** renforcent la sécurité de vos domaines Active Directory dans la mesure où vous pouvez limiter la diffusion de certains mots de passe en cas de compromission de ces contrôleurs de domaine. Ces derniers trouveront par exemple leur place dans des petits réseaux d'agence où la sécurité physique du contrôleur de domaine ne pourra pas être garantie.

Les nouveaux services associés à l'Active Directory renforcent également la sécurité de votre informatique. Le rôle **AD CS** (*Active Directory Certificate Services*) permet la diffusion de certificats basés sur la cryptographie nouvelle génération (CNG). Le rôle **AD RMS** (*Active Directory Rights Management Services*) vous donne la possibilité de maîtriser la diffusion des documents de votre entreprise.

Le **pare-feu avancé** de Windows Server 2008 R2 permet de limiter la surface d'attaque de votre serveur en réalisant un filtrage des ports sur le trafic réseau entrant ou sortant. Le pare-feu analyse le flux au niveau applicatif et vous

© ENI Editions - All rights reserved - adamo diarra

pourrez donc n'autoriser un trafic que pour un service spécifique. De plus, la nouvelle console de gestion MMC pour le pare-feu avancé permet de configurer des flux **IPSec** afin d'assurer l'intégrité ou de chiffrer le flux entre ordinateurs. Cela est idéal pour définir un chiffrement entre des contrôleurs de domaine ou entre des postes d'administrateurs de domaine et des serveurs d'administration.

Le chiffrement du lecteur disque avec l'outil **Bitlocker** permet également d'empêcher l'accès aux données de votre disque dur depuis une installation parallèle d'un autre système d'exploitation.

Les fonctionnalités de sécurité présentes sous Windows Server 2008 permettent donc de limiter au maximum le risque d'attaque sur le serveur tout en garantissant une productivité et une flexibilité importante.

3. Une plate-forme évolutive

Windows Server 2008 est une plate-forme capable de s'adapter et de répondre ainsi au besoin d'évolution d'une société.

La technologie **hyperviseur (Hyper-V)** 64 bits répond au besoin grandissant des entreprises souhaitant virtualiser certains de leurs serveurs. Cette technologie répond ainsi de façon ultra-réactive aux charges de travail dynamiques. L'apport du support de la **mémoire dynamique** depuis le Service Pack 1 permet une meilleure gestion de la mémoire physique du serveur.

Les services **Terminal Server** apportent un lot d'innovations qui va beaucoup améliorer l'expérience utilisateur.

Un accès centralisé aux applications peut en effet être défini afin de décorréler petit à petit le poste de travail des applications qui sont nécessaires aux utilisateurs.

Il vous est ainsi possible de rendre disponibles des applications (publication d'applications) sans que celles-ci soient installées sur l'ordinateur de l'utilisateur. Le raccourci de l'application apparaît alors sur le bureau de l'utilisateur au côté des applications installées localement sur son ordinateur. L'utilisateur ne peut donc pas, à première vue, distinguer les applications locales de celles déportées ce qui vous fait également gagner du temps en terme de formation des utilisateurs. Couplée à la technologie **RemoteFX** apparue avec le Service Pack 1, l'expérience côté utilisateur s'en trouvera fortement améliorée.

Un service de **passerelle Terminal Services** (appelé aussi TS Gateway) ne vous oblige plus à multiplier les ports à ouvrir sur votre réseau ou à monter un réseau privé virtuel. Un unique point d'entrée, via un portail Web, vous permet d'accéder à votre réseau d'entreprise. Le trafic RDP est en effet encapsulé de façon transparente dans un flux SSL (HTTPS).

L'**accès Web aux services Terminal Server** (TS Web Access) est une interface Web permettant l'accès aux applications RemoteApp que vous avez choisi de publier. Ces applications sont ainsi accessibles depuis votre navigateur Internet. Cette solution s'appuie sur IIS et peut également être intégrée à un portail SharePoint.

Grâce à Windows Server 2008 R2, vous pouvez gérer les évolutions de la société et en particulier les applications ayant besoin de haute disponibilité.

Le **cluster de serveurs** a pour principe de contenir plusieurs serveurs ayant un rôle identique. Si un des serveurs (appelés nœud du cluster) devient indisponible, le système de cluster bascule automatiquement vers un autre nœud disponible. Cela se fait sans aucune intervention des administrateurs, ce qui limite la durée d'indisponibilité d'une application.

Le service de haute disponibilité se caractérise également par la possibilité de faire de l'**équilibrage de la charge réseau** (appelé également NLB pour *Network Load Balancing*). Cet équilibrage permet de répartir la charge réseau entre plusieurs serveurs présentant les mêmes informations. L'équilibrage de charge réseau peut ainsi répondre à un fort développement de l'activité d'un site Internet par exemple en choisissant de diriger les demandes de connexion au serveur Web vers le serveur IIS le moins occupé.

Enfin le cycle de vie de votre serveur devient plus simple à gérer avec un ensemble d'outils adaptés et performants.

Parmi ceux-ci nous pouvons citer la fonctionnalité de **sauvegarde** qui permet de gérer vos sauvegardes et restaurations à partir d'assistants très intuitifs. La technologie des clichés instantanés permet de sauvegarder vos fichiers en cours d'exécution de façon quasi immédiate.

Le serveur de patchs **WSUS3** permet de gérer l'ensemble des mises à jour (correctifs, patchs de sécurité) des systèmes d'exploitation et de certaines applications Microsoft au sein de votre réseau d'entreprise.

Ce livre a ainsi pour but de vous présenter les principales fonctionnalités de Windows Server 2008 R2.

Il sera parsemé d'avis et de conseils d'experts Microsoft et s'adresse ainsi à des personnes ayant déjà acquis une certaine expérience. Néanmoins, cet ouvrage s'est également attaché à expliquer les concepts de base afin d'être ainsi facilement accessible aux personnes n'ayant pas d'expérience notoire avec la technologie serveur de Microsoft.

Les nombreuses adresses Internet fournies dans ces pages sont reprises dans une webographie disponible sur le site de l'éditeur www.editions-eni.fr.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre est consacré à l'annuaire Microsoft Active Directory. Le service d'annuaire Microsoft est devenu indispensable dans la gestion de l'information au sein d'une entreprise.

Dans la première partie, une présentation du service d'annuaire sous Windows Server 2008 R2 sera abordée. Suivront alors des explications sur les principaux composants attachés au service d'annuaire comme les stratégies de groupes et des autres services attachés au service d'annuaire Microsoft.

© ENI Editions - All rights reserved - adamo diarra

Présentation du service d'annuaire Microsoft : Active Directory Domain Services

Vous connaissez sans doute le principe de fonctionnement de l'annuaire Active Directory. Cet ouvrage n'ayant pas pour but de réexpliquer ce que vous savez déjà, les grands principes d'un annuaire Active Directory (appelé désormais Active Directory Domain Services ou AD DS) seront traités de façon succincte pour ainsi pouvoir concentrer votre attention sur les spécificités apportées par Windows Server 2008 R2.

1. Définition d'un domaine Active Directory

Active Directory est un service d'annuaire permettant de référencer et d'organiser des objets comme des comptes utilisateurs, des noms de partages, des autorisations à l'aide de groupes de domaine, etc. Les informations peuvent ainsi être centralisées dans un annuaire de référence afin de faciliter l'administration du système d'information.

D'un point de vue logique, trois notions sont à retenir :

- Le domaine est l'unité de base chargée de regrouper les objets qui partagent un même espace de noms (un domaine doit en effet nécessairement reposer sur un système DNS supportant les mises à jour dynamiques et les enregistrements de type SRV).

- Une arborescence de domaines est le regroupement hiérarchique de plusieurs domaines partageant un même espace de nom (par exemple les domaines lyon.masociete.local et paris.masociete.local).

- Une forêt consiste à regrouper plusieurs arborescences de domaine qui ont en commun un catalogue global et qui ne partagent pas forcément un espace de nom commun.

D'un point de vue physique, trois principaux éléments sont à retenir :

- Les contrôleurs de domaine sont chargés de stocker l'ensemble des données et de gérer les interactions entre les utilisateurs et le domaine (ouverture de session, recherche dans l'annuaire, etc.). Contrairement aux anciens systèmes NT, une réplication multimaître a lieu sur un domaine ce qui permet ainsi à n'importe quel contrôleur de domaine de pouvoir initier une modification (ajout d'un compte utilisateur, changement d'un mot de passe utilisateur, etc.).

- Chaque contrôleur de domaine contient également des partitions. Microsoft a décidé de partager l'information en plusieurs partitions afin de pouvoir limiter l'étendue des données à répliquer. Chaque partition n'a donc pas la même étendue de réplication. Tous les contrôleurs de domaine d'une même forêt ont les partitions de **schéma** et de **configuration** en commun. Une modification sur une de ces partitions n'engendrera donc une réplication que vers certains contrôleurs de domaine.

  Tous les contrôleurs de domaine d'un même domaine partagent une partition de **domaine** commune.

  La quatrième partition (présente de façon facultative) est la partition d'**application**. Celle-ci stocke les données sur les applications utilisées dans Active Directory et se réplique sur les contrôleurs de domaine de votre choix faisant partie de la même forêt.

- Les sites Active Directory mettent en évidence le regroupement physique d'objets sur un domaine. Vous devez en outre attacher un (ou des) contrôleur(s) de domaine à un même site Active Directory si ces contrôleurs de domaine communiquent avec un lien réseau ayant un bon débit. En effet, les contrôleurs de domaine d'un même site dialoguent de façon beaucoup plus fréquente que des contrôleurs de domaine définis sur deux sites Active Directory distincts. Cela vous permettra ainsi de réduire de façon non négligeable le trafic réseau sur un lien distant séparant vos deux sites.

2. Fonctionnalités de l'Active Directory sous Windows Server 2008 R2

Windows Server 2008 R2 propose un grand nombre de fonctionnalités. Celles-ci raviront aussi bien les personnes n'ayant pas de connaissances préalables que celles désireuses d'en savoir davantage.

Il vous sera ainsi expliqué comment installer un contrôleur de domaine Active Directory avec Windows Server 2008 R2, comment utiliser les stratégies de mot de passe affinées, etc.

Ces fonctionnalités vous seront présentées par des travaux pratiques au travers de ce chapitre afin que vous puissiez constater par vous-même l'utilité de ces dernières.

© ENI Editions - All rights reserved - adamo diarra

a. Installation d'un annuaire Active Directory

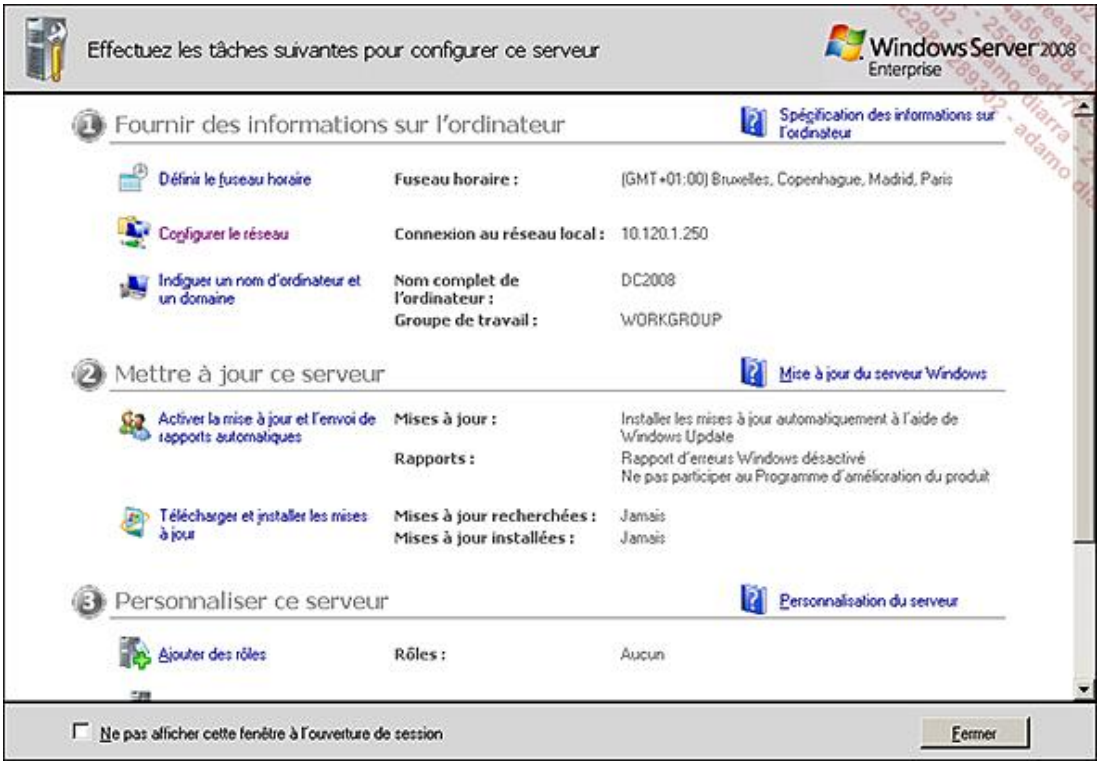
D'une façon générale, les assistants de configuration se sont beaucoup améliorés au fil des versions de Windows. Vous découvrirez rapidement que ces derniers sont très utiles et intuitifs. Par exemple, il vous est désormais possible de faire appel à la plupart des options avancées d'installation de l'annuaire Active Directory à partir de l'assistant créé à cet effet.

Windows 2008 R2 arrive avec deux nouvelles notions. Celles de Rôles et de Fonctionnalités. Elles sont configurables à partir de la console **Gestionnaire de serveur**. Vous utiliserez donc cette console afin d'ajouter le rôle **Service de domaine Active Directory** (connu aussi sous le nom AD DS pour *Active Directory Domain Services*).

L'ensemble de ces manipulations doit être effectué avec un compte utilisateur possédant les droits Administrateur sur le serveur.

- Assurez-vous dans un premier temps que vous avez correctement défini le nom NETBIOS de votre futur contrôleur de domaine, ainsi qu'une adresse IP fixe valide. Il est toujours conseillé de définir ces paramètres avant la promotion d'un serveur en tant que contrôleur de domaine.

Par défaut, l'assistant **Tâches de configuration initiales** se lance à chaque démarrage de Windows afin de vous permettre de configurer votre serveur une fois installé.



- Choisissez les options **Configurer le réseau** et **Indiquer un nom d'ordinateur et un domaine**. Vous pourrez ainsi définir une adresse IPv4 fixe, ainsi qu'un nom d'ordinateur évocateur pour votre serveur.

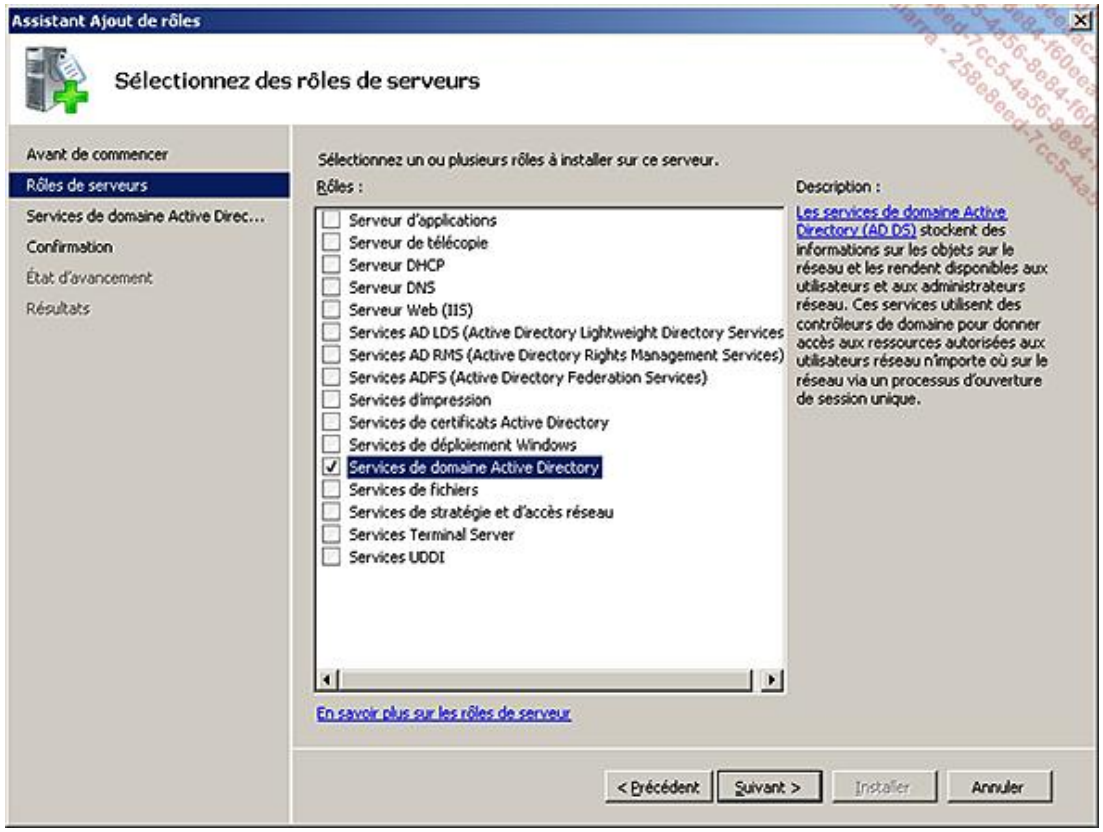
  Dans notre exemple, le nom d'ordinateur sera **DC2008** (DC pour *Domain Controller* ou Contrôleur de Domaine). Votre serveur devra alors être redémarré.

- Une fois le serveur redémarré, ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer - Outils d'administration** puis **Gestionnaire de serveur**.

- Au niveau de **Résumé des rôles**, cliquez sur **Ajouter des rôles**.

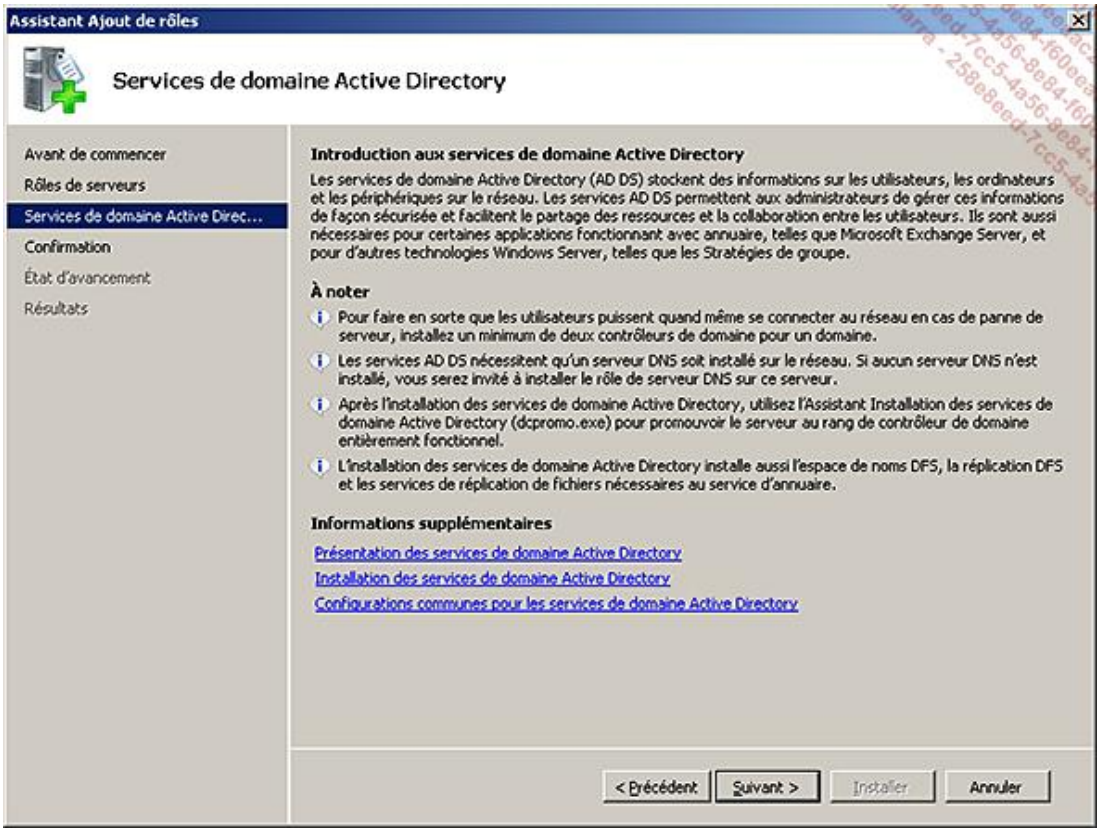
© ENI Editions - All rights reserved - adamo diarra

- L'**Assistant Ajout de rôles** s'ouvre alors. La première page est présente par défaut à chaque lancement de l'assistant. Celle-ci a pour but de vous faire vérifier un ensemble de bonnes pratiques avant de continuer à installer un rôle sur votre serveur (mot de passe fort, IP statique, correctifs de sécurité à jour). Cliquez sur **Suivant**. Choisissez alors de cocher le rôle que vous souhaitez installer. Comme vous souhaitez installer un contrôleur de domaine Active Directory, il vous faut choisir **Services de domaine Active Directory**. Sous Windows 2008 R2, l'assistant vous invitera à ajouter l'installation de la fonctionnalité requise, **.NET Framework 3.5.1**. Les étapes suivantes de l'assistant se mettent à jour de façon dynamique en fonction du rôle choisi. Cliquez alors sur **Suivant**.



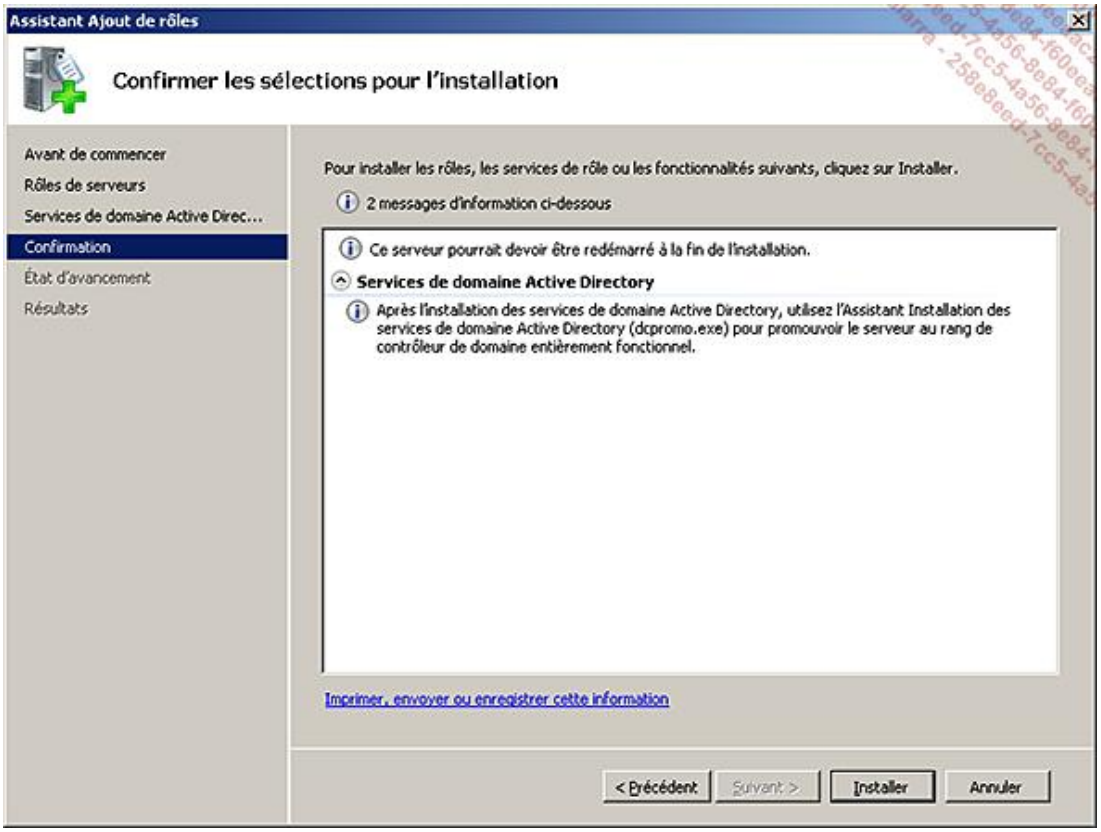
© ENI Editions - All rights reserved - adamo diarra

- L'assistant vous explique rapidement le rôle des services de domaine Active Directory et les principales informations à retenir. Il vous invite également à consulter des articles disponibles dans l'aide Windows pour plus de renseignements. Cliquez sur **Suivant**.



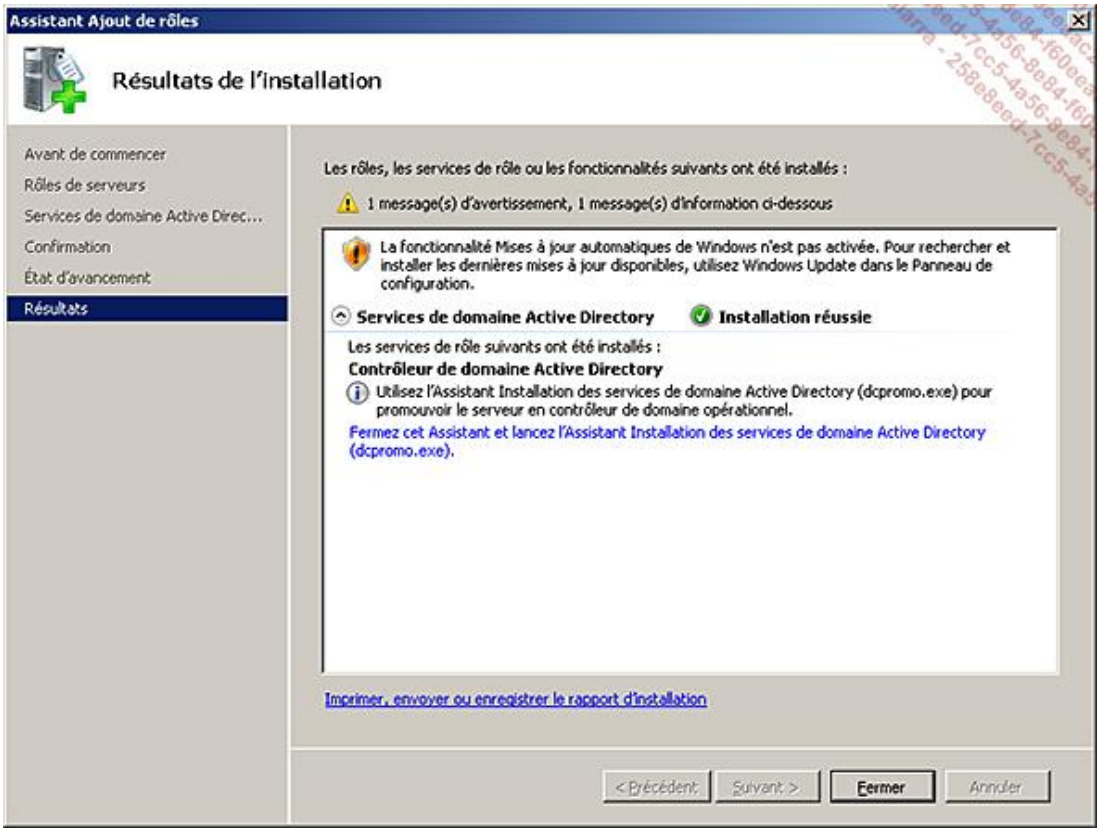
- La dernière étape consiste à confirmer l'installation du rôle en question. Les messages d'information vous mettent en garde car le serveur devra être redémarré à la fin de l'installation. Une étape supplémentaire consistera à exécuter la commande **dcpromo** pour compléter l'installation du contrôleur de domaine. Cliquez sur **Installer**. L'installation du rôle débute alors.

© ENI Editions - All rights reserved - adamo diarra



- Une fois l'installation terminée, vous vous rendrez rapidement compte de la puissance et de l'utilité des assistants de Windows Server 2008 R2. Ces derniers vérifient sans cesse si votre serveur répond aux critères de base en termes de sécurité et de configuration. Dans cet exemple, l'assistant alerte sur le fait que la fonctionnalité **Mises à jour automatiques de Windows** n'est pas activée (si vous ne l'aviez pas déjà activée bien entendu). Il vous indique également la suite à donner afin de mener à bien cette installation. Cliquez sur le lien **Fermez cet Assistant et lancez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe)**. Vous pourrez également choisir de lancer cette commande un peu plus tard en l'exécutant directement depuis le menu **Démarrer - Exécuter - Dcpromo.exe**.

© ENI Editions - All rights reserved - adamo diarra



Si le contrôleur de domaine que vous prévoyez d'installer rejoint une forêt et/ou un domaine existant ayant un niveau fonctionnel de schéma ou de domaine Windows 2000 ou 2003, il vous faudra impérativement étendre le schéma au moins à Windows Server 2008 puis mettre à jour le niveau fonctionnel de la forêt et du (ou des) domaine (s) impacté(s). Pour cela, insérez le DVD de Windows Server 2008 ou 2008 R2 (suivant le niveau de schéma désiré) dans votre contrôleur de domaine hébergeant le rôle de maître de schéma. Rendez-vous alors dans le dossier **sources\adprep** du DVD et lancez la commande `adprep /forestprep` s'il s'agit du premier contrôleur de domaine sous Windows Server 2008 ou 2008 R2 de votre forêt (avec un compte utilisateur membre des groupes d'administrateurs de l'entreprise, du schéma et du domaine). Une fois cette opération terminée, laissez le temps à la réplication d'opérer puis mettez à jour le niveau fonctionnel du domaine sur lequel sera installé votre nouveau contrôleur de domaine. Pour ce faire, insérez le DVD de Windows Server 2008 ou 2008 R2 (suivant les cas) dans un contrôleur de domaine du domaine impacté. Choisissez de préférence le contrôleur de domaine ayant le rôle de Maître d'infrastructure. Lancez alors la commande suivante `adprep /domainprep /gpprep`.

Si, au sein de votre domaine, vous n'avez que des contrôleurs de domaine sous Windows Server 2008 R2, vous pouvez augmenter le niveau de votre domaine en Windows Server 2008 R2 via la console **Domaine et approbation Active Directory** ou via le **centre d'administration Active Directory** (plus d'infos à l'adresse : http://technet.microsoft.com/fr-fr/library/cc753104(WS.10).aspx). Si au sein de votre forêt, tous vos contrôleurs de domaine sont des Windows Server 2008 R2, vous pourrez également augmenter le niveau fonctionnel de votre forêt, toujours via l'une de ces consoles (plus d'infos à l'adresse : http://technet.microsoft.com/fr-fr/library/cc730985 (WS.10).aspx).

Notez également que, à condition que la corbeille Active Directory que nous verrons ultérieurement n'ait pas été activée, il est possible de baisser le niveau fonctionnel d'un domaine ou d'une forêt de Windows Server 2008 R2 à Windows Server 2008 à l'aide des commandes PowerShell suivantes :

```
Import-Module Active Directory
Set-AdDomainMode -identity masociete.local -server dc2.enfant.masociete.local
-domainmode
Windows2008Domain

Set-AdForestMode -identity masociete.local -server dc2008R2..masociete.local
-forestmode
Windows2008Forest
```

- L'**Assistant Installation des services de domaine Active Directory** se lance alors. Choisissez d'**Utiliser l'installation en mode avancé**. Cliquez sur **Suivant**.

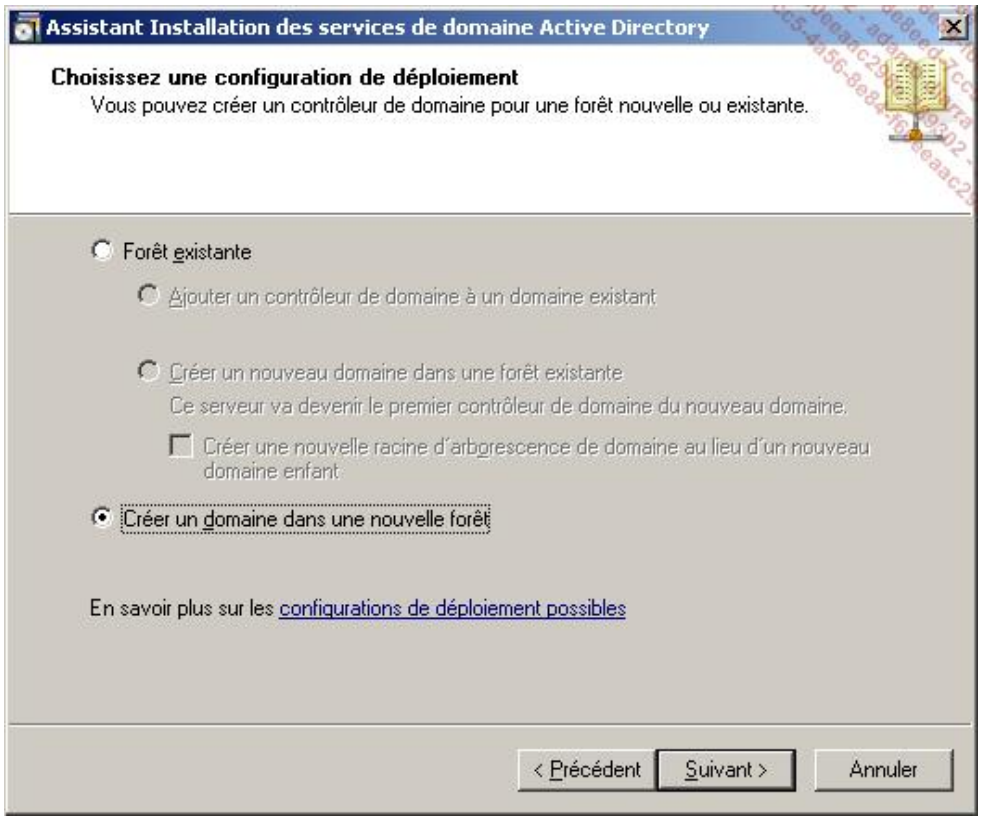
  Un message d'avertissement indique les problèmes que vous risquez de rencontrer du fait de l'amélioration de l'algorithme de chiffrement utilisé à l'établissement d'un canal de sécurité avec un client SMB. Par défaut, les anciens systèmes d'exploitation comme Windows NT 4.0 ne pourront pas, par exemple, accéder à des partages se

© ENI Editions - All rights reserved - adamo diarra

trouvant sur un serveur Windows Server 2008 et Windows Server 2008 R2.

- Cliquez sur **Suivant** (si aucun serveur DNS n'est défini dans les propriétés de votre serveur, un message vous demandera de configurer un serveur DNS ou d'installer automatiquement le service DNS sur le serveur).

- Choisissez une configuration de déploiement. Dans notre exemple, choisissez de **Créer un domaine dans une nouvelle forêt**. À noter que l'assistant vous indique un lien vers le fichier d'aide Windows traitant des différentes configurations de déploiement possibles.



Si vous avez choisi d'ajouter un contrôleur de domaine à un domaine existant, vous aurez la possibilité de définir l'installation du contrôleur de domaine à partir d'un média (une sauvegarde par exemple). C'est assez utile sur un site distant par exemple, afin d'éviter qu'un trafic réseau important ne vienne saturer la bande passante lors de la première synchronisation entre les contrôleurs de domaine. Vous pouvez sinon définir un contrôleur de domaine particulier pour la première synchronisation de l'annuaire Active Directory afin d'indiquer un contrôleur de domaine du même site et ainsi éviter que la synchronisation ne s'opère vers un site distant ayant une bande passante limitée.

- Nommez le domaine racine de la forêt. Dans notre exemple, le nom de domaine sera **masociete.local**.

  Il est toujours conseillé d'indiquer un nom de domaine à deux niveaux. Ne créez donc pas de domaine Active Directory ayant par exemple pour nom *Masociete*.

  Notez que l'assistant ne vous laissera pas la possibilité de créer un nom de domaine sur un seul niveau, que ce soit pour une nouvelle forêt ou un nouveau domaine dans une forêt existante. Il vous laissera par contre la possibilité d'ajouter un nouveau contrôleur exécuté sous 2008 R2 dans un domaine à un seul niveau déjà existant. La KB Microsoft suivante http://support.microsoft.com/kb/300684 traite de ce cas de figure.

  Évitez également de définir un nom de domaine public du type *masociete.com* ou *masociete.fr*. Cela entraînera en effet une gestion un peu plus complexe de votre zone DNS interne. Cliquez sur **Suivant**. L'assistant tentera alors de résoudre ce nom de domaine afin de contacter une éventuelle forêt existante.

Vous trouverez plus d'informations sur les différents types de zone DNS et sur la réplication dans le chapitre Mise en place des services réseaux d'entreprise - La mise en place des systèmes de résolution de nom.

© ENI Editions - All rights reserved - adamo diarra

- Laissez le nom de domaine NETBIOS par défaut et cliquez sur **Suivant**.

- Le niveau fonctionnel de la forêt devra alors être défini. Choisissez **Windows Server 2008 R2** (si tous vos contrôleurs de domaine dans la forêt exécutent Windows Server 2008 R2). La fonctionnalité de la Corbeille Active Directory sera alors disponible (comme expliqué plus loin dans ce chapitre au paragraphe La corbeille Active Directory). Cela vous permettra en effet d'éviter d'avoir à augmenter le niveau fonctionnel de domaine des éventuels futurs domaines de cette même forêt.

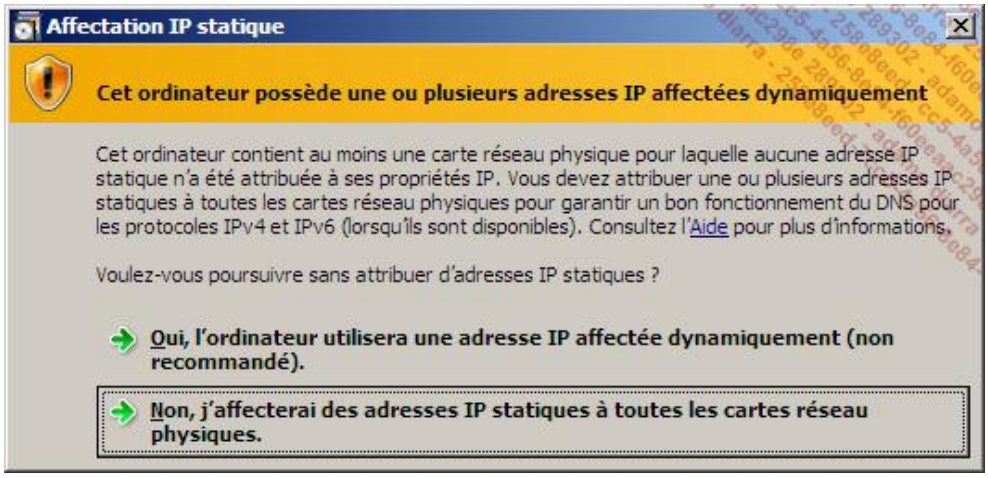
  Vous profiterez ainsi automatiquement des avantages liés au niveau fonctionnel de domaine Windows Server 2008 R2, comme les stratégies de mot de passe affinées (que vous verrez plus tard dans ce chapitre au paragraphe Stratégies de mot de passe et de verrouillage de compte granulaire).

  Il faut savoir que le niveau fonctionnel de la forêt ne peut pas être mis à jour vers un niveau fonctionnel inférieur (Windows 2000 ou Windows 2003). Comme indiqué par l'assistant, vous ne pourrez ajouter à cette forêt que des contrôleurs de domaine exécutant Windows Server 2008 R2 ou ultérieur.

  Cliquez sur **Suivant**.

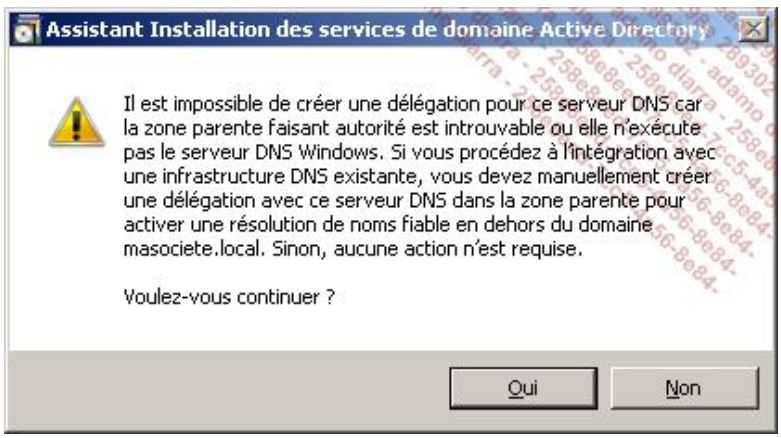
- Laissez la case **Serveur DNS** cochée afin d'installer ce rôle sur le futur contrôleur de domaine et cliquez sur **Suivant**. L'option **Catalogue Global** est forcément cochée dans notre exemple car aucun catalogue global n'existe encore sur le domaine puisque vous avez choisi de créer un nouveau domaine dans une nouvelle forêt.

Si vous n'avez pas défini d'adresse IP fixe à vos deux protocoles IPv4 et IPv6, le message suivant apparaîtra :



Si vous ne prévoyez pas d'utiliser le protocole IPv6, il est conseillé de désinstaller celui-ci.

Le système tente alors de contacter le serveur DNS défini au niveau des paramètres TCP/IP de la carte réseau du serveur. Si celui-ci ne répond pas au nom de domaine Active Directory défini, et si aucun serveur DNS n'est installé, l'assistant affichera le message suivant :



© ENI Editions - All rights reserved - adamo diarra

Noter également que si un serveur DNS est défini dans les propriétés TCP/IP du serveur, celui-ci sera automatiquement supprimé de ces propriétés de sorte que le futur contrôleur de domaine soit client de son propre DNS. L'ancien serveur DNS auparavant défini sera renseigné dans l'onglet **Redirecteurs des propriétés du service DNS**.

- Choisissez **Oui**.

- Comme vous vous trouvez dans un environnement de test, laissez le chemin par défaut pour la base de données, les fichiers journaux et SYSVOL. Dans un environnement de production, il est fortement conseillé de séparer la base de données et les fichiers journaux afin d'éviter la saturation des I/O (Entrées/Sorties). Cliquez sur **Suivant**.

- Définissez le mot de passe administrateur de restauration des services d'annuaire. Il vous sera utile en cas de restauration du serveur lors d'un démarrage en mode **Restauration des services d'annuaires** accessible via la touche [F8] au démarrage de votre système d'exploitation. Ce mot de passe devra répondre à la complexité requise par la stratégie de mot de passe.

Bien que cela soit tentant, ne définissez pas le même mot de passe que celui du compte Administrateur actuel pour des raisons de sécurité.

- Cliquez sur **Suivant**.

Un résumé affiche les différents choix que vous avez faits durant les étapes de l'assistant. Il vous est possible d'exporter ces paramètres afin de pouvoir les réutiliser dans un fichier de réponse.

Vous pourrez ainsi facilement déployer d'autres contrôleurs de domaine tout en minimisant le risque d'erreurs lors de la configuration de ce rôle. La commande à utiliser sera alors `dcpromo /answer:NomDuFichierCréé`.

Si vous exécutez directement la commande `dcpromo`, le rôle **Service de Domaine Active Directory** sera automatiquement installé.

- Cliquez sur **Suivant**. L'assistant lance l'installation du rôle Contrôleur de domaine sur Windows Server 2008 R2. Une fois son installation terminée, choisissez de redémarrer le serveur.

Lors du premier redémarrage du contrôleur de domaine, vous constaterez des messages d'avertissement liés aux rôles Serveur DNS et Services de domaine Active Directory. Ne vous inquiétez pas, ces messages peuvent être ignorés et disparaîtront rapidement d'eux-mêmes.

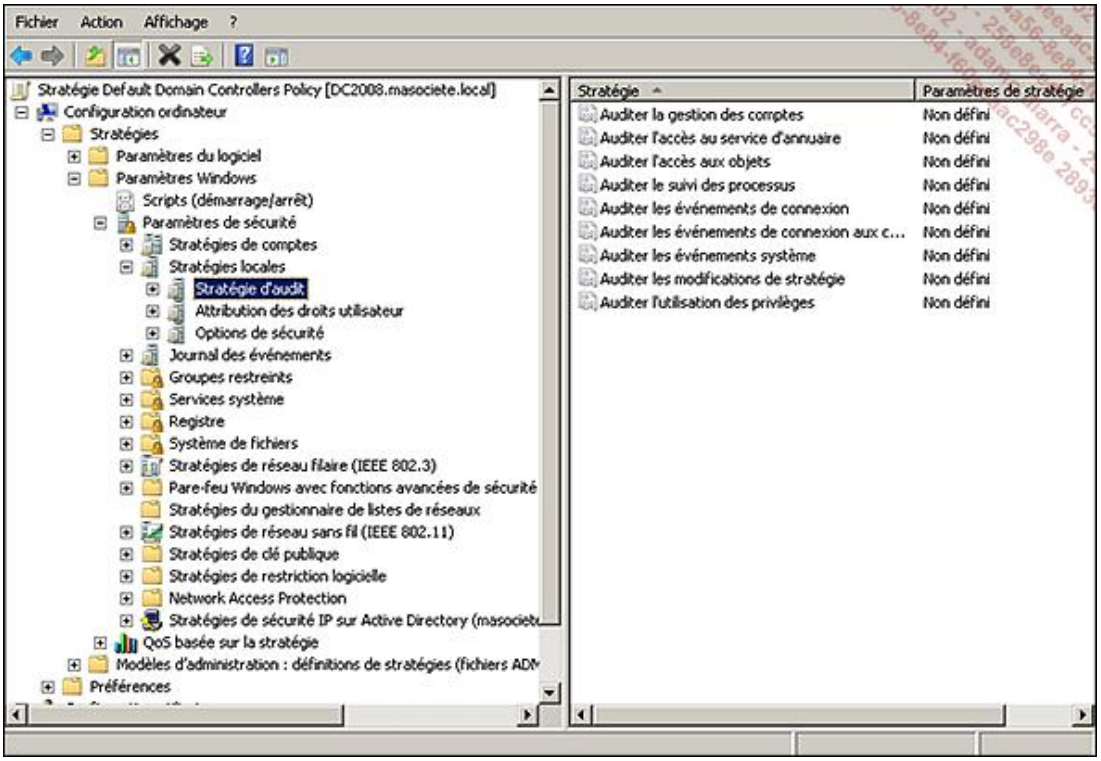
Félicitations ! Vous venez donc d'installer avec succès un contrôleur de domaine sous Windows Server 2008 R2.

b. Présentation de l'audit lié au service d'annuaire

Auditer ses serveurs consiste à recenser les évènements que l'on juge intéressants dans le journal des évènements. Cela vous aide alors à mettre en évidence certains problèmes de configuration ou bien encore à vérifier la sécurité de certains éléments critiques du système d'exploitation. Attention cependant à ne pas définir trop d'objets à auditer car les performances du serveur en pâtiront immédiatement !

Sous Windows Server 2008 R2, vous pourrez configurer les audits en éditant votre stratégie de groupe (depuis le menu **Démarrer** - **Outils d'administration** et **Gestion des stratégies de groupe**) au niveau de **Stratégie Default Domain Controllers Policy** (**Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Stratégies d'audit**).

© ENI Editions - All rights reserved - adamo diarra



Les informations affichées sont cependant trompeuses !

Les stratégies d'audit peuvent en effet être définies de façon beaucoup plus fine désormais et les paramètres affichés au niveau de la stratégie de groupe ne représentent que très grossièrement la configuration effective.

Sous Windows XP, seules 9 catégories d'évènements pouvaient être auditées. Depuis Windows Vista/Windows Server 2008, vous pouvez choisir d'auditer jusqu'à 53 catégories d'évènements différents.

L'affichage et la configuration de ces paramètres ne sont pas identiques si vous êtes sous Windows Server 2008 R2.

Sous Windows Server 2008 (ou Vista avec les outils d'administration RSAT), vous pourrez afficher et appliquer de façon plus fine les stratégies d'audit réellement possibles uniquement au travers de la ligne de commande **Auditpol.exe**.

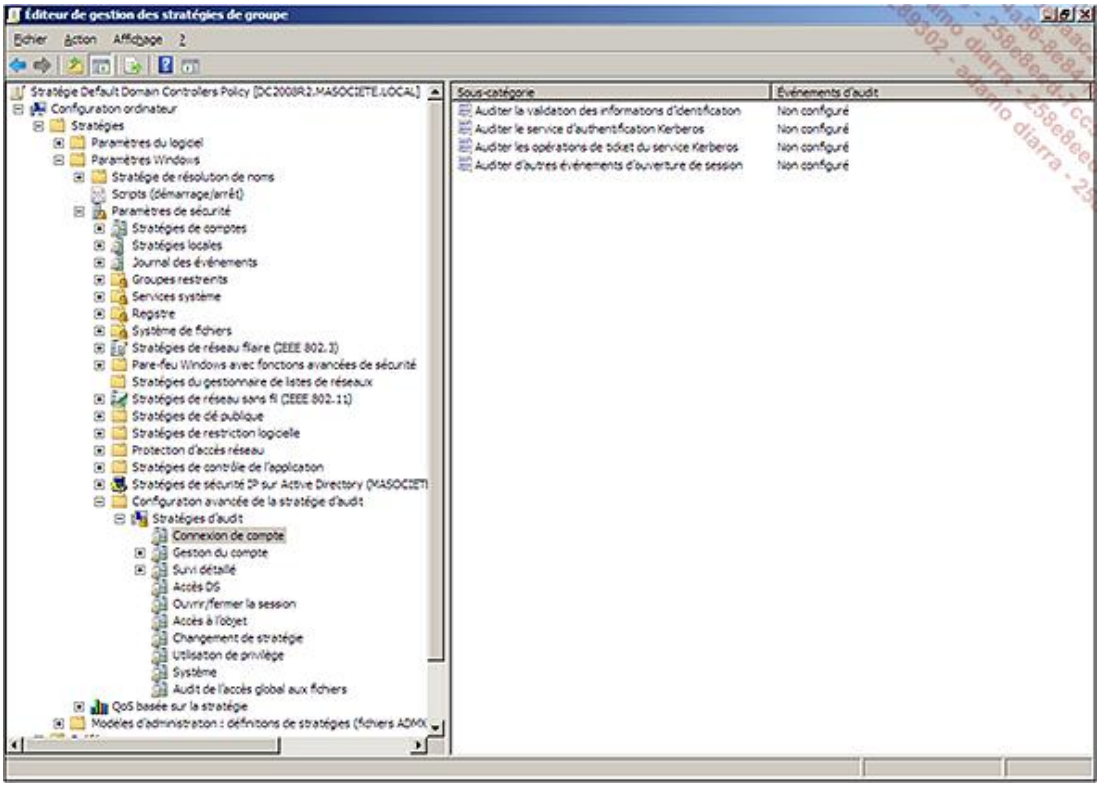
La commande suivante permet d'afficher les différentes catégories possibles pour l'audit :

```
Auditpol.exe /get /Category :*
```


© ENI Editions - All rights reserved - adamo diarra

Sous Windows Server 2008 R2 (ou Windows 7 avec les outils d'administration RSAT installés), il est possible de configurer, déployer et gérer l'audit détaillé depuis la console GPMC. La configuration de l'audit détaillé s'effectue au niveau de **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Configuration avancée de la stratégie d'audit - Stratégie d'audit**.

© ENI Editions - All rights reserved - adamo diarra



Ces stratégies peuvent être ainsi appliquées sur des OU spécifiques afin de maîtriser l'activité des comptes administrateurs, etc... Gardez cependant à l'esprit que ces paramètres définis via GPO ne seront exécutés que sur des ordinateurs Windows Server 2008 R2 ou Windows 7. Afin de déployer ces paramètres sous Windows Server 2008 ou Windows Vista, il faudra utiliser l'outil **auditpol.exe**. Un lien vers une KB expliquant la démarche est fournie dans ce chapitre quelques paragraphes plus loin.

Windows Server 2008 R2 et Windows 7 permettent également **d'auditer les accès aux objets globaux**. Vous aurez en effet la possibilité de définir une stratégie d'audit pour un utilisateur particulier sur une action précise et pour un ensemble de serveurs. Cela peut s'avérer très pratique si vous devez notamment justifier de l'audit et de la sécurité d'un serveur auprès d'auditeurs SOX.

Les évènements générés par les audits d'accès aux fichiers ou au registre seront d'ailleurs plus parlants si vous activez l'option **Auditer la manipulation du handle** car la "Raison de l'accès" sera alors affichée et vous permettra notamment de mettre en évidence des erreurs de configuration (comme par exemple un utilisateur qui a un accès en écriture au lieu de n'avoir qu'un accès en lecture).

Vous trouverez davantage d'informations sur les spécificités des stratégies de groupe sous Windows Server 2008 R2 à cette adresse : http://technet.microsoft.com/en-us/library/dd408940(WS.10).aspx.

Notez que Microsoft déconseille la configuration de l'audit simultanément au niveau de **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Stratégies d'audit** et de **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Configuration avancée de la stratégie d'audit - Stratégie d'audit**.

Vous remarquerez alors que les options d'audit sont beaucoup plus riches que sous les anciennes versions de Windows.

Les principales catégories ont été conservées et vous constaterez que beaucoup de sous-catégories viennent enrichir et rendre la collecte des évènements très précise.

Votre journal des évènements risquera donc d'être beaucoup moins pollué par des évènements inutiles.

Sachez toutefois que si vous utilisez la stratégie de groupe afin de définir les catégories principales d'audit, vous n'aurez pas la possibilité de définir de façon plus fine les paramètres des sous-catégories. Une stratégie d'audit configurée au niveau des stratégies de groupe active automatiquement les sous-catégories.

Pour configurer de façon plus fine l'audit sur les postes, il faudra donc utiliser la commande **auditpol** sur les postes ou serveurs choisis via un script ordinateur par exemple.

Si vous souhaitez toutefois pouvoir gérer la configuration des sous-catégories de vos postes Windows Vista/2008 de façon centralisée (et par conséquent sans avoir à passer par la commande `auditpol` sur chaque ordinateur), lisez l'excellente solution fournie dans l'article suivant de la KB Microsoft : http://support.microsoft.com/kb/921469.

© ENI Editions - All rights reserved - adamo diarra

Une de ces nouvelles sous-catégories d'audit a été spécialement créée pour répondre à un besoin fort des administrateurs de domaine Active Directory.

Cette nouvelle sous-catégorie se nomme **Directory Service Changes** (catégorie enfant de DS Access). Elle vous permettra d'enregistrer les anciennes et les nouvelles valeurs attribuées à un objet Active Directory et à ses attributs. Pour information, auparavant un contrôleur de domaine sous Windows 2000 ou 2003 indiquait simplement le nom de l'objet ou de l'attribut modifié mais pas les anciennes et nouvelles valeurs de celui-ci.

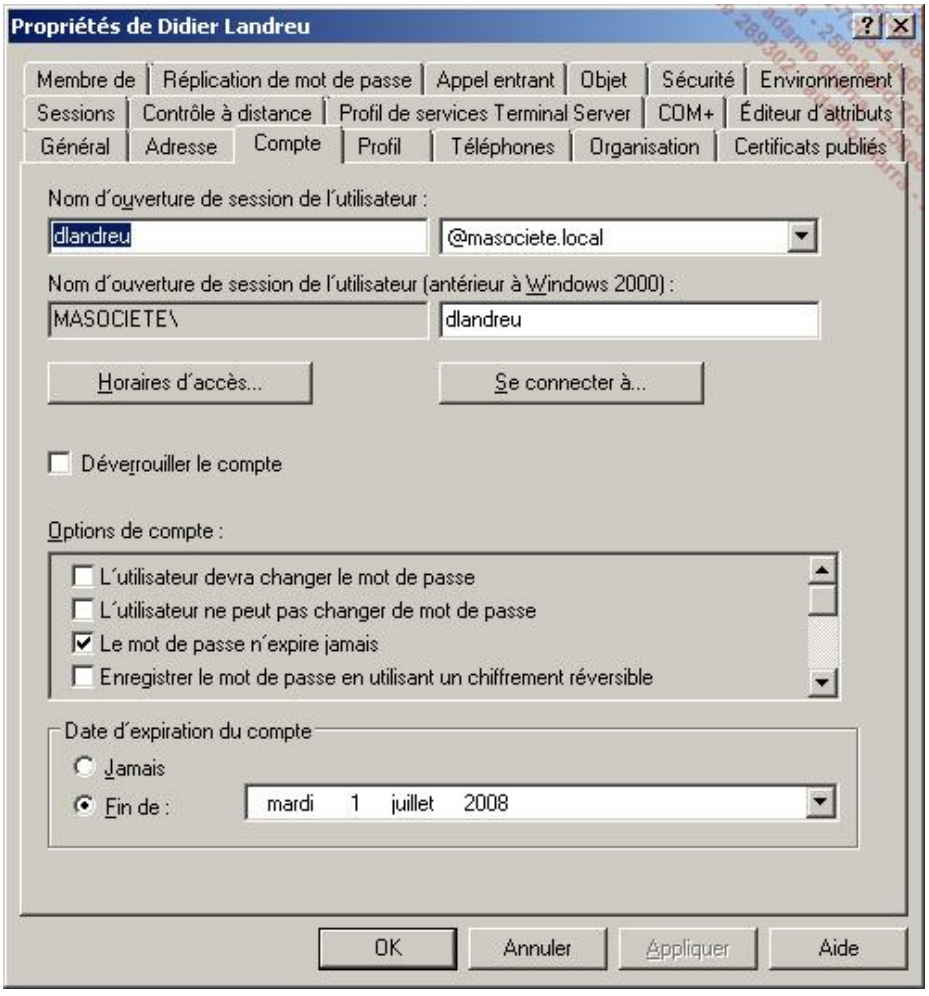
Une fois que l'audit de cette sous-catégorie aura été configuré, les évènements seront consignés dans le journal Sécurité. Le tableau suivant récapitule les quatre types d'évènements sur les objets Active Directory :

Numéro de l'évènement	Type de l'évènement
5136	Modification réussie d'un attribut de l'Active Directory.
5137	Création d'un nouvel objet de l'Active Directory.
5138	Restauration d'un objet de l'Active Directory.
5139	Déplacement d'un objet de l'Active Directory.

Si vous souhaitez par exemple activer l'audit pour toutes les sous-catégories concernant l'accès à l'annuaire Active Directory, suivez la procédure suivante :

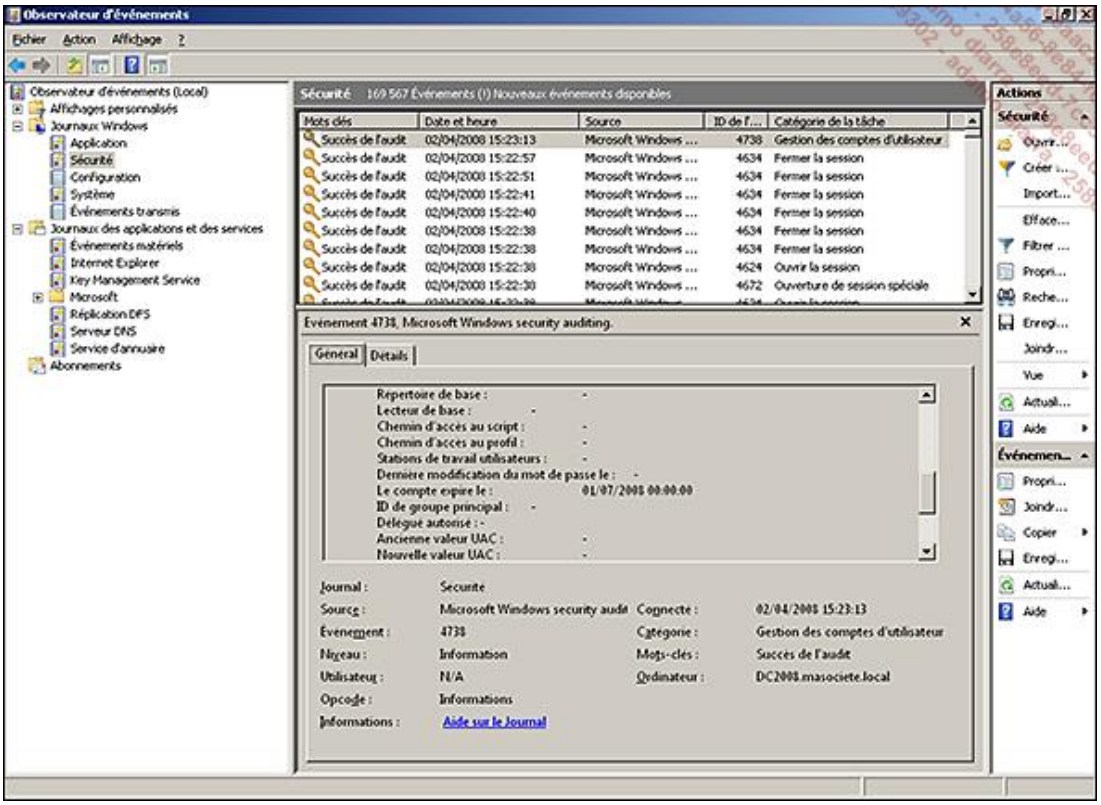
- La commande devra être exécutée sur le contrôleur de domaine : **Auditpol /set /category:"Accès DS" /success:enable**. Toutes les sous-catégories d'audit seront ainsi activées.

- Modifiez alors la date d'expiration d'un compte utilisateur de l'Active Directory via la console **Utilisateurs et ordinateurs Active Directory** (via **Démarrer - Exécuter - dsa.msc**).



© ENI Editions - All rights reserved - adamo diarra

- Ouvrez le journal des évènements de votre contrôleur de domaine (via **Démarrer - Exécuter - Eventvwr.msc**). Vous pouvez constater qu'un évènement 4738 est présent et qu'il précise la ou les valeurs qui viennent d'être modifiées ; dans notre exemple, la valeur **Le compte expire le :**.



c. Contrôleur de domaine en lecture seule

Windows Server 2008 R2 permet de créer des **contrôleurs de domaine en lecture seule** (appelés aussi **RODC** pour *Read Only Domain Controller*). Un contrôleur de domaine en lecture seule contient toutes les informations d'un contrôleur de domaine classique à l'exception du mot de passe des utilisateurs. Ces informations sont stockées en lecture seule uniquement et aucune modification au niveau du domaine ne peut donc être initiée depuis un RODC.

Sachez d'ailleurs que si vous ne souhaitez pas la réplication d'un attribut jugé sensible sur vos RODC il est possible de modifier les propriétés de celui-ci afin de limiter sa réplication uniquement à des contrôleurs de domaine inscriptibles. Pour cela, il vous faudra modifier la valeur **searchFlags** de l'attribut de votre choix au niveau de la partition de schéma. Le rôle maître de schéma devra d'ailleurs de préférence se trouver sur un contrôleur de domaine sous Windows Server 2008 R2. Vous trouverez plus d'informations à ce sujet sur le lien suivant : http://technet2.microsoft.com/windowsserver2008/en/library/f62c9720-a5c3-40c9-aa40-440026f585e91033.mspx?mfr=true (en anglais).

Microsoft a donc réfléchi à une solution adaptée aux besoins des sociétés possédant des sites distants avec quelques utilisateurs pour :

- augmenter la sécurité de ces sites ;
- améliorer l'authentification des utilisateurs d'un site distant sans forcément nécessiter un trafic WAN avec le contrôleur de domaine du site principal ;
- accéder aux ressources du réseau plus rapidement.

Augmenter la sécurité de ces sites

Auparavant, il était en effet nécessaire d'installer un contrôleur de domaine supplémentaire sur des sites distants si vous ne vouliez pas que certains utilisateurs se plaignent de lenteur d'authentification ou d'accès à des ressources du domaine. Le problème qui pouvait alors se poser était que ces sites n'avaient pas forcément les moyens ou le besoin d'avoir un administrateur à temps plein, ni d'investir dans un local protégé pour sécuriser leur serveur. En cas

© ENI Editions - All rights reserved - adamo diarra

de vol ou de corruption du contrôleur de domaine du site, l'attaquant pouvait potentiellement récupérer tous les noms d'utilisateurs et mots de passe des utilisateurs de la société.

Désormais, il est possible de limiter les conséquences d'une corruption d'un contrôleur de domaine sur ces sites car vous pouvez définir avec précision quels comptes ont leurs mots de passe stockés sur ce contrôleur de domaine en lecture seule. Cela se fait au travers de l'appartenance à deux groupes de sécurité appelés **Groupe de réplication dont le mot de passe RODC est autorisé** (mot de passe répliqué sur le RODC) et **Groupe de réplication dont le mot de passe RODC est refusé** (mot de passe non répliqué sur le RODC). Vous n'avez alors plus qu'à choisir les comptes de vos quelques utilisateurs et les ajouter au groupe de votre choix. En cas de conflit (si l'utilisateur appartient aux deux groupes précédents par exemple), le droit « Refusé » est prioritaire. Par défaut, deux condensés de mot de passe sont stockés sur un RODC. Celui du compte krbtgt_xxxx et celui du compte ordinateur. Le compte krbtgt_xxxx est propre à chaque RODC. Il permet de délivrer les tickets Kerberos aux clients en faisant la demande. En cas de vol du contrôleur de domaine d'un site, il vous suffit de réinitialiser les mots de passe de ces quelques comptes, comme vous le verrez plus loin.

Améliorer l'authentification des utilisateurs

Un RODC tente d'authentifier un compte par rapport aux mots de passe qu'il possède en cache. Si celui-ci ne se trouve pas dans son cache, il contactera un contrôleur de domaine inscriptible afin d'authentifier l'utilisateur. Dans le même temps, il regardera si la stratégie de réplication des mots de passe autorise le mot de passe de ce compte à être mis en cache sur le RODC ou non. Ainsi, si la stratégie le permet, les requêtes d'authentification seront directement traitées par le RODC.

Accéder aux ressources du réseau plus rapidement

Parmi les autres spécificités d'un contrôleur de domaine en lecture seule, sachez que ce dernier ne peut, par nature, que recevoir le trafic de réplication entrant (réplication unidirectionnelle). Il ne peut donc pas être défini comme serveur tête de pont d'une stratégie de réplication du domaine dans la mesure où il ne fait que subir les modifications sans pouvoir les initier.

Il est également possible d'installer le service DNS sur le RODC d'un site. Cela évite des temps de latence répétitifs lors de la tentative de résolution de nom par un utilisateur n'ayant pas de serveur DNS proche de lui. Ce service sera également en lecture seule sur un RODC et les ordinateurs n'auront pas la possibilité d'inscrire leurs enregistrements de façon dynamique sur ce DNS. Leurs requêtes d'inscription seront alors redirigées vers un DNS inscriptible.

Parmi les pré-requis à l'installation d'un RODC, sachez que :

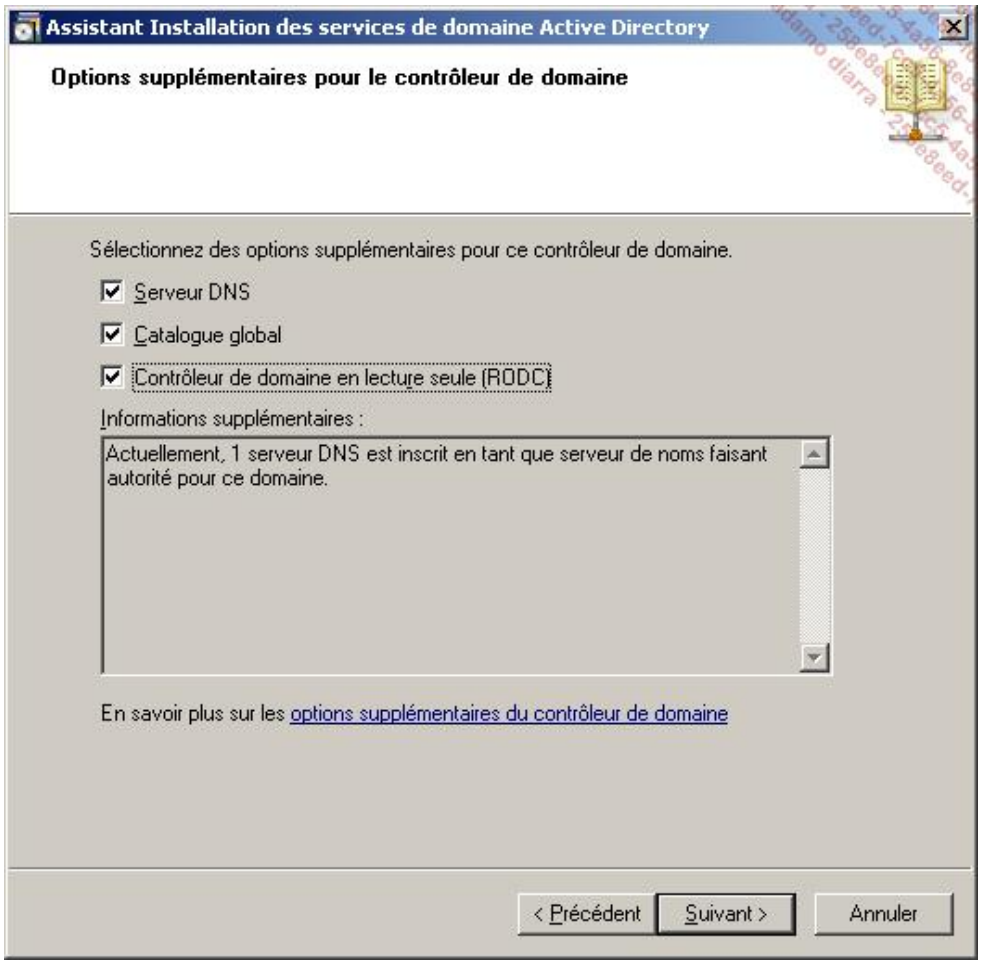
- Le contrôleur de domaine doit être capable de transférer les requêtes d'authentification vers un contrôleur de domaine sous Windows Server 2008 ou 2008 R2.
- Le niveau fonctionnel de la forêt et du domaine doivent être configurés en *Windows Server 2003 ou plus*.
- La commande `adprep /rodcprep` doit être lancée une seule fois sur la forêt. Elle permet de mettre à jour l'ensemble des domaines de la forêt afin de modifier les permissions sur la partition d'annuaire de l'application DNS.

Procédez comme suit si vous souhaitez installer un contrôleur de domaine en lecture seule :

- L'installation d'un RODC est quasiment identique à la procédure que vous avez utilisée lors de l'installation d'un contrôleur de domaine classique. Après avoir choisi le serveur qui servira de RODC, ouvrez la console **Gestionnaire de serveur** puis cliquez sur **Ajouter des rôles**. Choisissez **Services de domaine Active Directory**. Les étapes suivantes de l'assistant se mettent à jour en fonction du rôle choisi. Cliquez alors sur **Suivant** puis **Installer**.
- Une fois le rôle installé, choisissez **Fermez cet Assistant et lancez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe)**. Cochez alors la case **Utiliser l'installation en mode avancé** sans quoi un contrôleur de domaine inscriptible sera installé sans que vous ayez la possibilité d'indiquer que celui-ci est en lecture seule.
- Dans notre exemple, vous souhaitez installer un RODC, il vous faudra donc choisir d'installer un contrôleur de domaine **Dans une forêt existante** et **Ajoutez un contrôleur de domaine à un domaine existant**. Cliquez sur **Suivant**.
- Indiquez alors le nom du domaine existant sur lequel vous souhaitez ajouter un RODC puis cliquez sur **Définir** afin de spécifier le mot de passe d'un compte administrateur du domaine ou de l'entreprise. Cliquez alors sur **Suivant** (si une erreur apparaît, c'est que votre configuration DNS doit avoir un souci ou que des ports réseaux sont à autoriser car votre serveur RODC n'arrive pas à contacter votre domaine). Sélectionnez le domaine puis cliquez sur **Suivant**.
- Sélectionnez le site Active Directory puis cliquez sur **Suivant**.

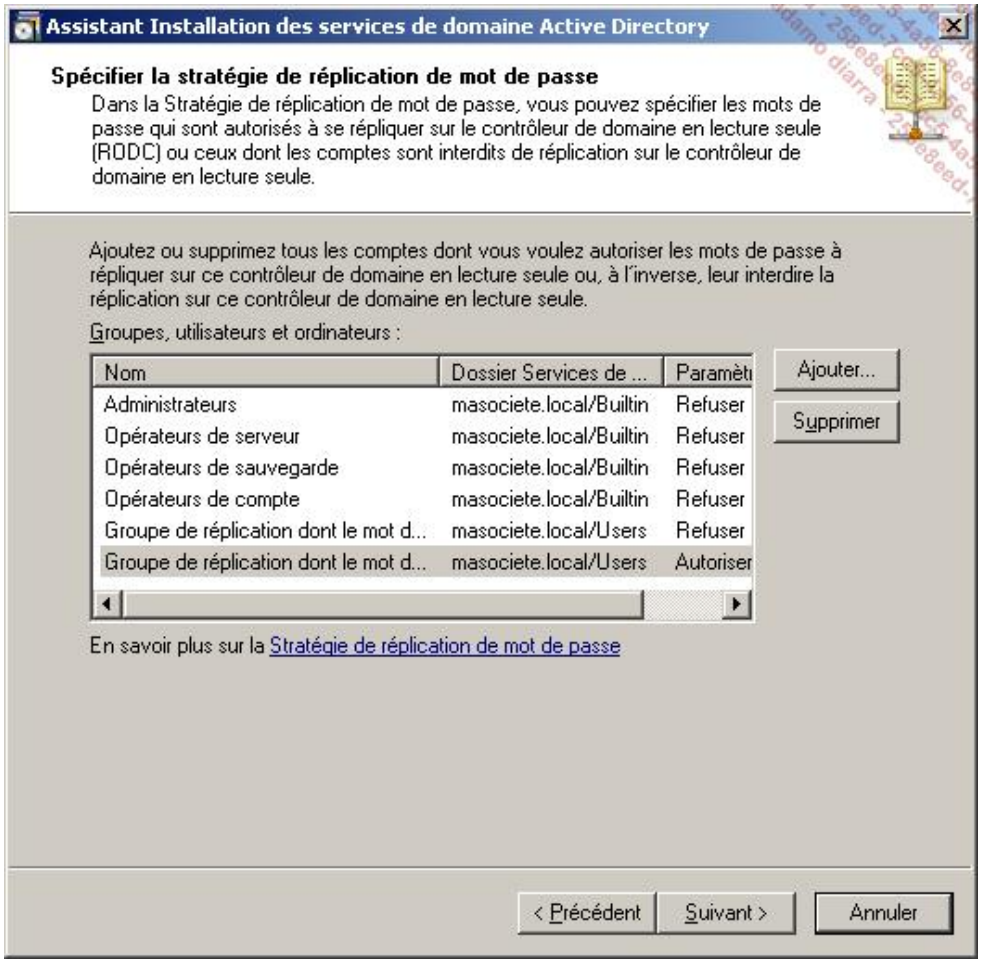
© ENI Editions - All rights reserved - adamo diarra

- À cette étape, cochez la case **Contrôleur de domaine en lecture seule (RODC)**. Si vous le souhaitez, vous pourrez attribuer le rôle de DNS et de catalogue global à ce futur contrôleur de domaine (en ayant toujours en tête les limitations énoncées précédemment). Cliquez sur **Suivant**.



- Spécifiez alors la **Stratégie de réplication de mot de passe** en ajoutant ou en supprimant les groupes et les comptes utilisateurs qui seront autorisés ou pas à répliquer leur mot de passe avec ce contrôleur de domaine en lecture seule. Une fois la réplication définie, cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- L'étape suivante permet de déléguer l'administration du RODC à l'utilisateur ou au groupe de votre choix. Dans la pratique, les membres de ce groupe se trouvent sur le site distant hébergeant ce contrôleur de domaine en lecture seule. Cliquez sur **Définir** pour ajouter le compte ou groupe de votre choix. Une fois l'ajout effectué, cliquez sur **Suivant**.

- Dans cette démonstration, vous choisirez **Répliquer les données sur le réseau à partir d'un contrôleur de domaine existant**. Cliquez sur **Suivant**.

- Si vous n'avez pas de contraintes particulières, laissez l'assistant choisir depuis quel contrôleur de domaine sera initiée la réplication. Cliquez sur **Suivant**.

- Choisissez un répertoire de destination pour les fichiers de l'Active Directory. Afin d'améliorer les performances, la base de données Active Directory et les fichiers journaux ne doivent pas se trouver sur les mêmes disques durs. Une fois les répertoires choisis, cliquez sur **Suivant**.

- Définissez alors le mot de passe du compte Administrateur qui sera utilisé lors du redémarrage du contrôleur de domaine en mode **Restauration des services d'annuaire**.

- Un résumé vous informe alors des différents choix que vous avez faits à la suite du lancement de l'assistant. Vous pouvez également sauvegarder cette configuration en cliquant sur **Exporter les paramètres**. Le fichier de réponse créé permettra l'installation d'un RODC en ligne de commande et sans intervention de l'utilisateur (à noter que le mot de passe de restauration du service d'annuaire ne sera pas automatiquement sauvegardé dans le fichier créé. Il faudra indiquer celui-ci avant d'utiliser le fichier d'installation sans quoi l'assistant vous demandera de saisir le mot de passe au moment voulu). Cliquez sur **Suivant** afin de lancer l'installation, puis sur **Terminer**. Redémarrez alors le serveur afin que les modifications puissent être prises en compte.

Le RODC est désormais installé. Vous devez maintenant configurer la **stratégie de réplication de mot de passe** depuis un contrôleur de domaine inscriptible. En effet, lorsqu'un RODC reçoit une demande d'authentification, il interroge la stratégie de réplication de mot de passe afin de déterminer s'il doit ou non garder en mémoire le mot de passe de l'utilisateur (ou de l'ordinateur) qui vient de s'authentifier. Par défaut, aucun mot de passe n'est gardé en mémoire. Suivant vos besoins, vous choisirez donc une stratégie de réplication de mot de passe plus ou moins sévère.

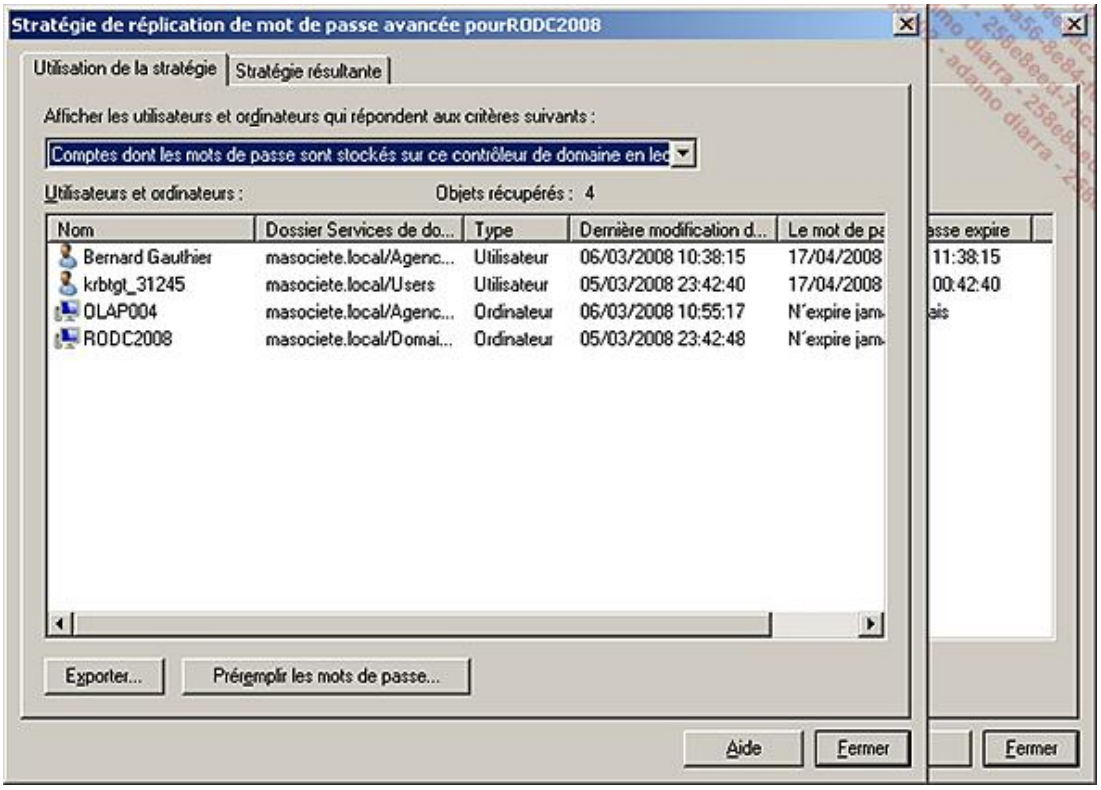
© ENI Editions - All rights reserved - adamo diarra

Afin de définir une stratégie de réplication de mot de passe, procédez comme suit depuis un contrôleur de domaine (non-RODC).

- Cliquez sur **Démarrer - Outils d'administration**, et ouvrez la console **Utilisateurs et ordinateurs Active Directory**. Rendez-vous au niveau de l'unité d'organisation **Domain Controllers** et cliquez avec le bouton droit de la souris sur le contrôleur de domaine en lecture seule puis sur **Propriétés**.

- Cliquez sur l'onglet **Stratégie de réplication de mot de passe**. Comme expliqué précédemment, un RODC ne stocke les mots de passe que des comptes utilisateurs ou groupes qui sont définis avec **Autoriser** (pour être autorisés à avoir leur mot de passe répliqué sur un RODC). Par défaut, la réplication du mot de passe est refusée pour les comptes d'administration comme Opérateurs de compte, Opérateurs de sauvegarde, Administrateurs, etc. **Ajouter** le compte de votre choix et choisissez si son mot de passe sera autorisé ou pas à être répliqué sur ce RODC puis cliquez sur **OK** afin de choisir le compte utilisateur ou groupe sur votre domaine. Validez en cliquant sur **OK** à nouveau.

- Si vous cliquez sur le bouton **Avancé** vous pourrez afficher le nom des **Comptes dont les mots de passe sont stockés sur ce contrôleur de domaine en lecture seule**.



- Vous pouvez également choisir dans la liste déroulante d'afficher les **Comptes authentifiés sur ce contrôleur de domaine en lecture seule**. Il est en effet intéressant de savoir qui s'est authentifié en passant par ce RODC et ainsi modifier la stratégie de réplication de mot de passe pour mettre en cache le mot de passe de cet utilisateur et ainsi éviter des requêtes inutiles vers un contrôleur de domaine inscriptible. Vous pourrez également choisir de **Préremplir les mots de passe** des comptes. Cela peut s'avérer très utile si vous installez votre RODC depuis votre site principal et que vous préremplissez les mots de passe des utilisateurs du site secondaire (sur lequel le RODC sera ensuite déplacé) à mettre en cache. Il faudra également préremplir les comptes d'ordinateur utilisés par les utilisateurs ajoutés. Cela évitera d'avoir la connexion WAN nécessairement active entre les deux sites lors de la première authentification des utilisateurs sur le site secondaire. Bien entendu, les comptes choisis devront au préalable être ajoutés à la stratégie de réplication de mot de passe, sans quoi le refus implicite interdira la mise en cache du mot de passe.

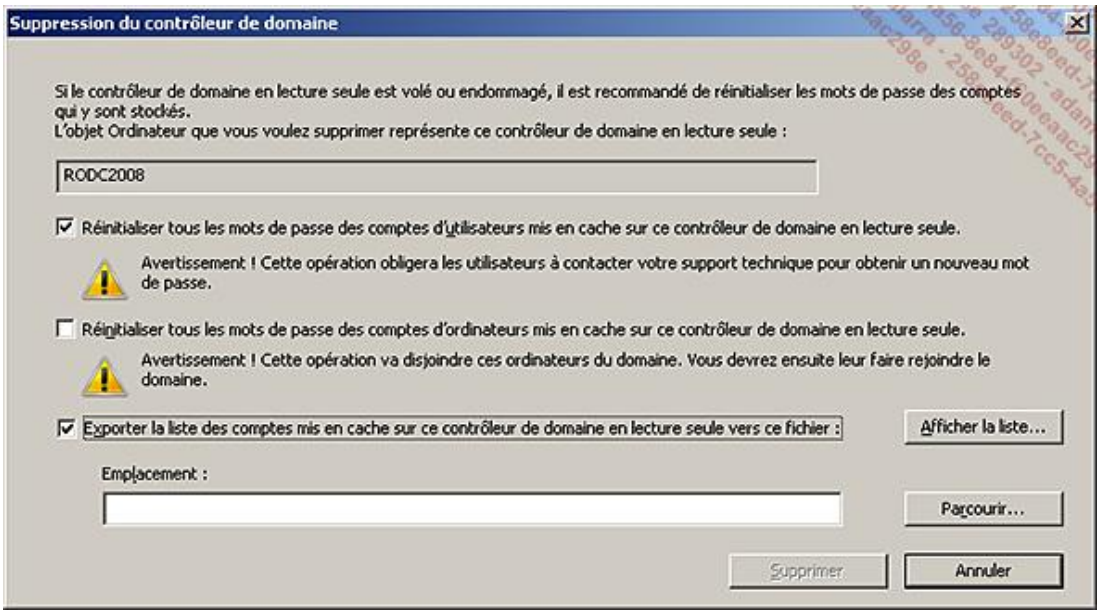
Sachez qu'il est possible de préremplir les mots de passe en utilisant la ligne de commande suivante : `repadmin /rodcpwdrepl [DSA_List] <Hub DC> <User1 Distinguished Name> [<Computer1 Distinguished Name> <User2 Distinguished Name> ...]`. Exemple : si on veut pré-peupler le mot de passe du compte utilisateur Freddy ELMALEH (et de son ordinateur portable LAP_FEL) sur un RODC nommé RODCSrv01 depuis un contrôleur de domaine inscriptible nommé DCSrv02, la commande utilisée sera : `Repadmin /rodcpwdrepl RODCSrv01 DCSrv02 "CN=FreddyELMALEH,OU=Utilisateurs_IT,DC=masociete,DC=local" "CN=LAP_FEL,OU=Ordinateurs_IT,DC=masociete, DC=local"`.

© ENI Editions - All rights reserved - adamo diarra

En cas de vol d'un RODC, vous pouvez très aisément contrôler les comptes impactés et ainsi limiter les risques de sécurité potentiels dûs au vol de ce serveur. En tant qu'administrateur, voici comment vous devrez réagir face à une telle situation :

- Depuis un contrôleur de domaine inscriptible, cliquez sur **Démarrer - Outils d'administration**, et ouvrez la console **Utilisateurs et ordinateurs Active Directory**. Rendez-vous au niveau de l'unité d'organisation **Domain Controllers** et cliquez avec le bouton droit de la souris sur le compte ordinateur du contrôleur de domaine en lecture seule puis choisissez **Supprimer**. Confirmez la suppression en cliquant sur **Oui**.

- Une fenêtre s'affiche alors vous permettant de forcer la réinitialisation du mot de passe pour vos comptes utilisateur et/ou ordinateur. Il vous est également possible d'exporter la liste des comptes qui étaient mis en cache. Une fois vos options choisies, cliquez sur **Supprimer**.



Votre contrôleur de domaine RODC est alors supprimé et même si un attaquant tente d'exploiter les mots de passe stockés sur celui-ci, ces derniers n'auront plus d'utilité car ils auront été aisément et rapidement modifiés.

d. Stratégies de mot de passe et de verrouillage de compte granulaire

Une des principales améliorations attendues par les professionnels de l'informatique utilisant l'annuaire Microsoft est sans aucun doute la possibilité de pouvoir définir des stratégies de mot de passe multiples sur un domaine Active Directory. Il n'était en effet pas possible de faire cela dans les versions précédentes d'Active Directory.

Windows Server 2008 R2 contient en effet une nouvelle classe d'objets nommée **msDS-PasswordSettings** qui rend possible la multiplication des stratégies de mot de passe au sein d'un même domaine. Sur un domaine Active Directory existant, il faudra mettre à jour le niveau fonctionnel du domaine au moins vers Windows Server 2008 (tous vos contrôleurs de domaine sur le domaine en question devront donc au moins être sous Windows Server 2008).

Il est ainsi possible de définir un objet paramètres de mot de passe (appelé aussi PSO pour *Password Settings Object*) différent entre les utilisateurs. Dans la pratique, vous pourrez ainsi avoir une durée de vie maximale des mots de passe de 30 jours pour les comptes administrateurs. Les comptes de services auront quand à eux une longueur minimale du mot de passe de 36 caractères et qui n'expire jamais.

Par défaut, seuls les membres du groupe **Administrateurs du domaine** ont la possibilité de définir des stratégies de mot de passe multiples.

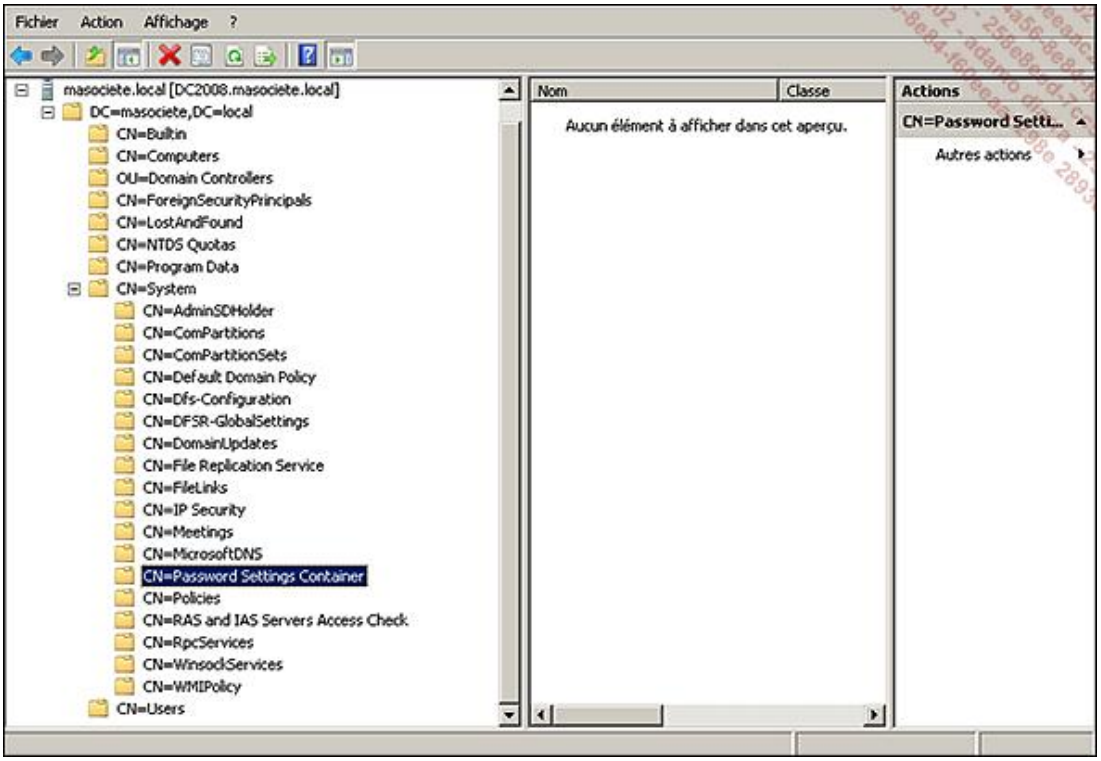
Prenons l'exemple de la définition d'une stratégie de mot de passe affinée pour les comptes utilisateurs utilisés pour l'administration du système d'information. Ces comptes utilisateurs font partis de groupes de sécurité leur octroyant beaucoup de droits sur le domaine et la compromission de leur mot de passe par un attaquant lui permettrait d'avoir un accès dangereux sur les serveurs. Il convient donc de sécuriser plus particulièrement ces comptes utilisateurs un peu spéciaux. Les paramètres de mot de passe seront les mêmes que ceux définis au niveau de la stratégie *Default Domain Policy*, à la différence de la durée de vie maximale du mot de passe qui sera de 30 jours au lieu de 42 jours. La longueur minimale du mot de passe passera également de 7 à 14 caractères. Le compte sera également verrouillé après 10 mauvaises tentatives. Ces principes limitent les risques de compromission du mot de passe des administrateurs. Afin de créer cette stratégie particulière, suivez les étapes suivantes :

- Ouvrez la console **adsiedit.msc** (depuis le menu **Démarrer - Exécuter** d'un Windows 2008 ou 2008 R2 de

© ENI Editions - All rights reserved - adamo diarra

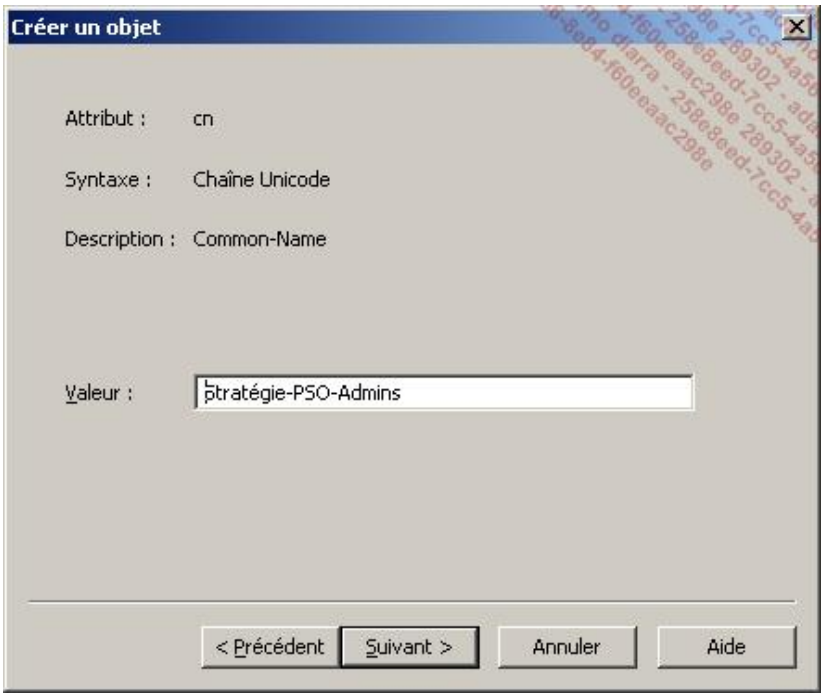
préférence) avec un compte utilisateur membre du groupe **Admins du domaine**. Faites un clic droit sur **Modification ADSI**, puis choisissez **Connexion**.

- Dans **Nom** : indiquez le nom FQDN du domaine s'il est différent du contexte d'attribution des noms par défaut (dans notre exemple **masociete.local**) puis cliquez sur **OK**. Naviguez alors dans l'arborescence sur la gauche de l'écran en cliquant sur ***Nom_FQDN_Du_Domaine*** **- CN=System - CN=Password Settings Container**. Faites un clic droit sur **CN=Password Settings Container** puis choisissez **Nouveau - Objet**.



- Dans **Créer un objet**, sélectionnez la classe **msDS-PasswordSettings** puis **Suivant**. Donnez un Common-Name à cet objet, comme *Stratégie-PSO-Admins* puis cliquez sur **Suivant**.

Cette stratégie sera appliquée à un groupe de sécurité nommé *PSO-Admins*. Ce groupe contiendra les utilisateurs pour lesquels vous souhaitez voir cette stratégie appliquée.



© ENI Editions - All rights reserved - adamo diarra

Vous devrez alors définir des valeurs pour un ensemble d'attributs.

- **msDS-PasswordSettingsPrecedence** correspond à une valeur de précédence. Elle doit avoir une valeur supérieure à 0 et permet l'arbitrage en cas de conflit lorsque deux objets PSO s'appliquent à un même utilisateur ou groupe. Deux règles sont à retenir si plusieurs paramètres s'appliquent à un même objet. L'objet PSO disposant de la valeur de précédence la plus faible sera appliqué et une stratégie appliquée au niveau Utilisateur sera prioritaire sur une stratégie appliquée au niveau Groupe.

Prévoyez d'espacer la numérotation de l'attribut **msDS-PasswordSettingsPrecedence** entre chaque stratégie PSO afin de vous permettre de jouer sur les priorités en cas de besoin futur.

- **msDS-PasswordReversibleEncryptionEnabled** est un booléen. Cet attribut correspond à l'option **Enregistrer les mots de passe en utilisant un chiffrement réversible**. Il est préférable d'indiquer la valeur **FALSE** sauf si vous avez des besoins particuliers.

- **msDS-PasswordHistoryLength** définit le nombre d'anciens mots de passe que l'utilisateur ne peut pas réutiliser. Il correspond au paramètre *Conserver l'historique des mots de passe*. Par défaut, sa valeur est de 24 sur le domaine.

- **msDS-PasswordComplexityEnabled** est un booléen qui définit si le mot de passe respecte des exigences de complexité ou non. **TRUE** est la valeur conseillée.

- **msDS-MinimumPasswordLength** est un entier qui définit *la longueur minimale du mot de passe*. La valeur par défaut est 7 sur le domaine. Dans notre exemple, il s'agit d'un PSO pour les comptes administrateurs. La valeur minimale sera donc indiquée à **14** caractères.

- **msDS-MinimumPasswordAge** est une durée qui indique *la durée de vie minimale du mot de passe* afin d'empêcher l'utilisateur de changer son mot de passe de façon successive jusqu'à ce qu'il dépasse la limite de l'historique des mots de passe afin de revenir sur son nouveau mot de passe. La valeur par défaut est de 1 jour. Son format s'inscrit alors ainsi **1:00:00:00**.

- **msDS-MaximumPasswordAge** est une durée qui indique *la durée de vie maximale du mot de passe*. Par défaut, le mot de passe doit être changé tous les 42 jours. Dans cet exemple, choisissez une durée de vie maximale de 30 jours soit **30:00:00:00**.

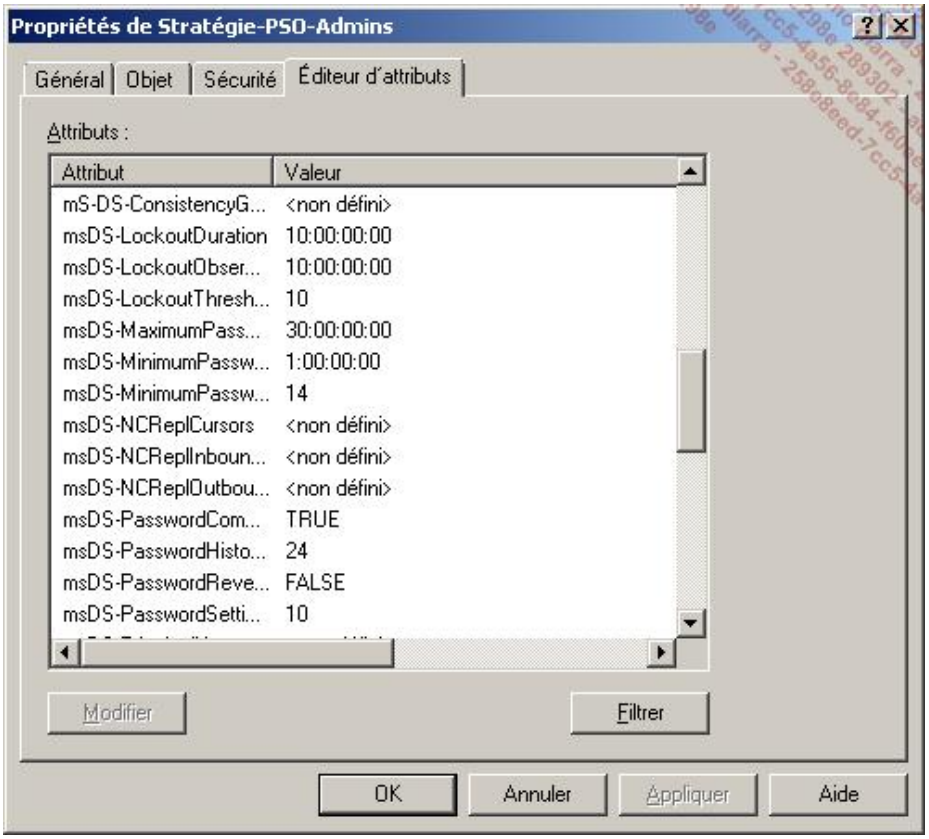
- **msDS-LockoutThreshold** définit le nombre de mots de passe erronés saisis avant que l'objet ne soit verrouillé. Il correspond au paramètre Seuil de verrouillage du compte qui est égal à 0 (ce qui indique que le compte n'est jamais verrouillé). Il est préférable d'indiquer un nombre de tentatives restreint pour éviter des attaques sur le mot de passe. Indiquez une valeur à **10** par exemple.

- **msDS-LockoutObservationWindows** permet de *Réinitialiser le compteur de verrouillages du compte après la* durée de votre choix. Indiquez une valeur de 10 minutes par exemple sous la forme **10:00:00:00**.

- **msDS-LockoutDuration** indique la *durée de verrouillage des comptes* en cas de X mauvais mots de passe saisis à plusieurs reprises (X représentant la valeur de msDS-LockoutThreshold). Indiquez une valeur de 10 minutes par exemple sous la forme **10:00:00:00**.

- Cliquez alors sur **Attributs Supplémentaires** afin de lier cette stratégie à un utilisateur ou à un groupe. La liaison se fait au travers de l'attribut **msDS-PSOAppliesTo**, capable de contenir plusieurs valeurs (donc plusieurs utilisateurs et groupes). Choisissez ces paramètres : *Sélectionnez les propriétés à afficher* : **Les deux** et *Sélectionnez une propriété à afficher* : **msDS-PSOAppliesTo**. Dans modifier un attribut, indiquez le nom unique du groupe sous la forme **DN=PSO-Admins**, **OU=Admin-Groups**, **OU=Admins**, **OU=Paris**, **DC=masociete**, **DC=local**. Puis cliquez sur **Ajouter**. Vous pouvez ajouter autant de noms uniques que vous le souhaitez. Une fois l'opération terminée, cliquez sur **OK**.

© ENI Editions - All rights reserved - adamo diarra



L'objet paramètres de mot de passe sera également accessible depuis la Console Utilisateurs et Ordinateurs Active Directory sur laquelle vous aurez affiché les **Fonctionnalités avancées** dans le menu **Affichage de la console**. L'objet est alors visible et modifiable depuis le conteneur **System/Password Settings Container**.

Préférez appliquer une stratégie de mot de passe à un groupe plutôt qu'à un utilisateur afin de permettre une gestion bien plus simple et efficace. Si vous souhaitez connaître la stratégie appliquée à un utilisateur ou un groupe, affichez les propriétés du compte en question puis sélectionnez l'onglet **Éditeur d'attributs** puis **Filtrer - Afficher les attributs** : **Facultatif** et **Afficher les attributs en lecture seule : Construit**. L'attribut **msDS-ResultantPSO** sera alors visible et indiquera la stratégie PSO effective. Si l'attribut est nul alors la stratégie de mot de passe du domaine est appliquée pour le compte vérifié.

Vous pourrez utiliser des outils tiers gratuits afin de vous aider pour la configuration des stratégies PSO. Il existe un très bon outil en ligne de commande nommé PSOMgr.exe disponible sur http://www.joeware.net ou bien encore un outil graphique facile à prendre en main qui s'appelle SpecOps Password Policy Basic disponible sur http://www.specopssoft.com.

---

e. Active Directory en tant que service Windows

Il est possible d'arrêter et de démarrer l'annuaire Active Directory avec n'importe quel contrôleur de domaine sous Windows Server 2008 R2 car celui-ci est désormais considéré comme un service Windows.

Vous pouvez donc effectuer des opérations de maintenance comme la défragmentation hors-ligne de la base de données de l'annuaire Active Directory sans nécessairement redémarrer le serveur en mode Restauration du service d'annuaire.

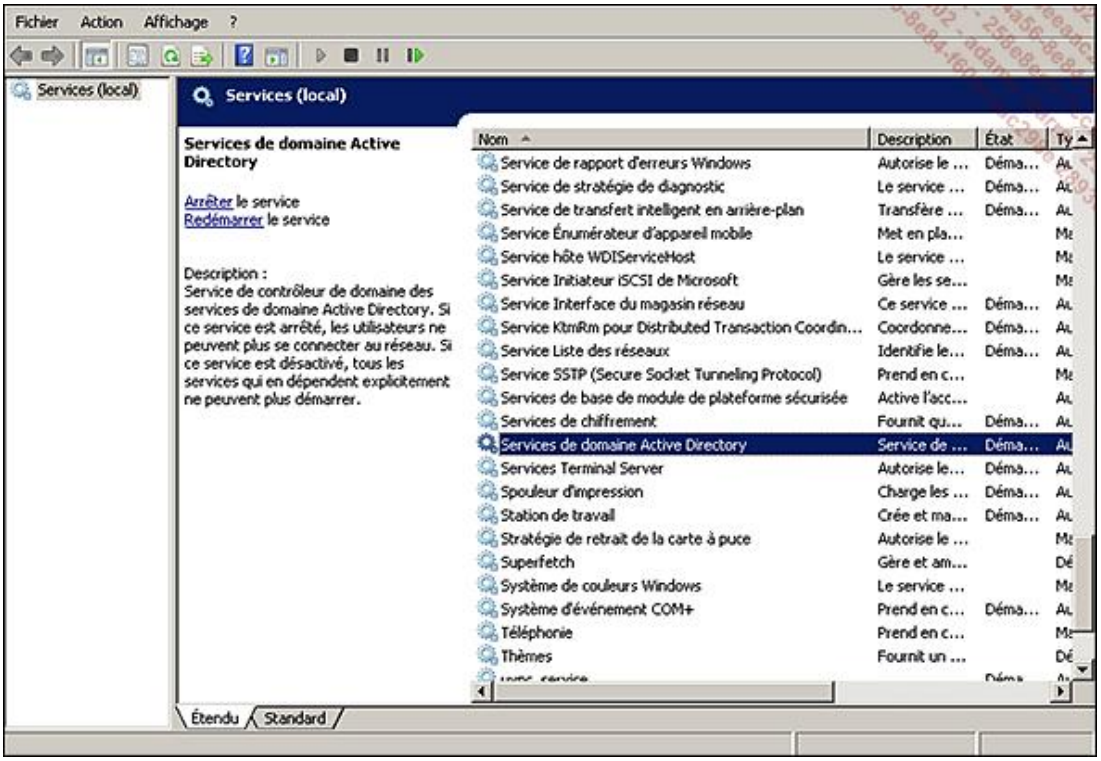
Les mises à jour Windows impactant le service d'annuaire ne nécessitent plus systématiquement le redémarrage complet du serveur. Un simple redémarrage du service Active Directory suffira.

Le principal avantage lié au fonctionnement d'Active Directory en tant que service est que les autres services installés sur le contrôleur de domaine ne seront plus inaccessibles lorsqu'une opération de maintenance sera nécessaire.

La défragmentation de la base de données de l'annuaire Active Directory ne rendra donc plus nécessairement le service DHCP (installé sur ce même serveur) inaccessible.

Vous pouvez configurer l'état du service au niveau de la console MMC services, disponible depuis les outils d'administration ou en tapant **services.msc** dans **Exécuter**.

© ENI Editions - All rights reserved - adamo diarra



Le service apparaît sous le nom complet **Services de domaine Active Directory**. Le nom du service est **NTDS**.

Lorsque le statut du service est défini sur **Arrêté**, le contrôleur de domaine est vu par les autres ordinateurs comme un serveur membre du domaine sur lequel des stratégies de groupe peuvent être appliquées. Le contrôleur de domaine se comporte également comme s'il était en mode **Restauration de service d'annuaire**. Son fichier **ntds.dit** est libéré et si aucun contrôleur de domaine n'est joignable pour vous authentifier lors de l'ouverture de session, il vous faudra utiliser le mot de passe du compte administrateur de restauration des services d'annuaire défini lors de la promotion du serveur en tant que contrôleur de domaine.

Il est important de garder à l'esprit que bien que le service NTDS puisse être arrêté, un minimum de précautions sont à prendre :

- Le service NTDS ne doit pas être arrêté pour une longue période. Comme, par exemple, le fait d'arrêter le service sur un contrôleur de domaine en se disant que l'annuaire sera remis à nouveau en ligne en cas de crash d'un contrôleur de domaine. En effet, suivant la durée d'arrêt du service NTDS, les enregistrements pourront être considérés comme trop anciens et ne seront pas répliqués.

- L'arrêt du service NTDS n'est pas suffisant pour permettre une restauration de l'Active Directory. Il faut toujours utiliser le mode DSRM (*Directory Services Restore Mode*) afin d'effectuer une restauration (autoritaire ou pas).

- Il n'est pas possible d'ouvrir une session avec le compte Administrateur DSRM (qui correspond en réalité au compte Administrateur local du DC) lorsque le service NTDS est arrêté et qu'il n'y a pas d'autres contrôleurs de domaine disponibles lors de la tentative d'authentification du compte. Il est possible de modifier ce comportement en éditant la clé **DSRMAdminLogonBehavior** sur votre contrôleur de domaine au niveau de la clé **HKLM\System\CurrentControlSet\Control\Lsa**.

Les valeurs possibles sont les suivantes :

Clé **DSRMAdminLogonBehavior**	
Valeur **0** (par défaut)	Ne permet pas d'ouvrir une session avec le compte administrateur DSRM. Pour ouvrir une session avec ce compte, il faudra qu'un autre contrôleur de domaine soit disponible au moment de l'authentification.
Valeur **1**	Le compte Administrateur DSRM peut être utilisé lorsque le service AD DS est arrêté. Cette valeur est notamment intéressante si vous n'avez qu'un seul contrôleur de domaine ou si la résolution de noms définie sur celui-ci pointe uniquement sur lui-même.

© ENI Editions - All rights reserved - adamo diarra

Valeur **2**	Le compte Administrateur DSRM peut être utilisé pour l'authentification dans n'importe quelle situation. Il faut cependant garder en tête que ce compte n'est soumis à aucune stratégie de mot de passe.

f. Cliché instantané de l'Active Directory

Windows Server 2008 R2 propose la création de clichés instantanés se reposant sur l'API VSS (*Volume Shadow Copy* ou Cliché Instantané de Volume). Pour vous aider dans vos recherches anglophones sur Internet, sachez que cette fonctionnalité s'appelle également Database Mounting Tool.

Le principal avantage est qu'une sauvegarde de ce type est possible même sur des fichiers verrouillés. Il n'est donc pas nécessaire d'arrêter le service Active Directory (et ainsi de libérer les fichiers attachés) pour pouvoir sauvegarder le fichier **ntds.dit** par exemple.

Vous pouvez coupler l'utilisation du cliché instantané avec l'utilisation de l'outil **dsamain.exe** afin de mettre en évidence n'importe quel changement effectué dans l'Active Directory.

Par défaut, seuls les utilisateurs membres du groupe Administrateurs du domaine et Administrateurs de l'entreprise sont autorisés à accéder aux clichés instantanés créés.

Afin d'utiliser au mieux les clichés instantanés pour l'Active Directory, trois outils sont indispensables.

- La commande `ntdsutil` pour créer, supprimer, lister, monter, démonter une sauvegarde (appelée pour l'occasion cliché instantané).
- La commande `dsamain` utilisée pour afficher le différentiel entre deux clichés instantanés par exemple.
- L'outil **ldp.exe** pour visualiser les données d'un cliché instantané de façon graphique.

L'utilisateur ne pourra accéder qu'aux données sauvegardées pour lesquelles les droits lui sont attribués. Les permissions sur les objets de la sauvegarde ne peuvent pas être modifiées car cette dernière est en lecture seule.

- Afin de créer un cliché instantané de l'annuaire Active Directory, vous allez utiliser la commande `ntdsutil`. Sachez toutefois que de nombreux autres logiciels du marché peuvent fonctionner à partir du moment où ces derniers utilisent la technologie des clichés instantanés.

  La commande à utiliser est :

  ```
  ntdsutil snapshot "activate instance ntds" create
  ```

- Vous pouvez planifier la sauvegarde de ces clichés via le Planificateur de tâches. La commande à définir sera alors légèrement différente car vous devrez sortir du prompt ntdsutil.

  ```
  ntdsutil snapshot "activate instance ntds" create quit quit
  ```

- Une fois le cliché terminé, vous pouvez choisir d'afficher tous les clichés déjà créés. Si vous êtes déjà au niveau de l'invite *instantané* : , tapez uniquement **List All** (sinon la commande complète est `ntdsutil snapshot "activate instance ntds" "List All"`).

- Il vous faudra alors monter le cliché de votre choix afin de pouvoir lire les données qui y avaient été sauvegardées :

  `mount` x (où x correspond au numéro du cliché instantané).

- Une fois le cliché monté, tapez **quit** deux fois de suite afin de revenir à une invite de commande classique.

© ENI Editions - All rights reserved - adamo diarra

Création d'un cliché instantané de l'annuaire Active Directory et montage d'une de ces sauvegardes.

- Maintenant il va falloir attacher cette sauvegarde à un serveur LDAP virtuel à l'aide de la commande `dsamain`.

  Pour cela, ouvrez une invite de commande avec un compte utilisateur membre du groupe Administrateurs du domaine ou Administrateurs de l'entreprise et tapez la commande suivante :

  ```
  dsamain /dbpath < Chemin de la base de donnée AD > /ldapport <numéro de
  port non utilisé>
  ```

Si le domaine depuis lequel avait été créé le cliché instantané n'existe plus, il vous faut ajouter l'argument /**allowNonAdminAccess**. Si votre pare-feu est activé, il faudra créer une exception pour l'exécutable dsamain.exe.

- Votre serveur LDAP virtuel est maintenant accessible tant que vous laisserez l'invite de commande ouverte. Connectez-vous via un client capable d'accéder aux données de ce serveur LDAP. Dans cet exemple, vous utiliserez l'outil **ldp.exe** disponible par défaut dans Windows.

- Depuis le menu **Démarrer - Exécuter**, tapez la commande `ldp.exe`. Cliquez alors sur **Connexion** et **Se connecter**. Dans l'adresse du serveur, tapez l'adresse IP du serveur et indiquez le port précédemment défini avec dsamain (ici 51389). Puis cliquez sur **OK**.

- Vérifiez le type de liaison via le menu **Connexion - Lier**. Assurez-vous de définir un compte utilisateur si celui qui est actuellement connecté ne possède pas les droits suffisants. Une fois configuré, cliquez sur **OK** afin de vous authentifier sur ce fichier d'annuaire.

- Cliquez alors sur **Affichage - Arborescence**, et définissez le nom unique de base correspondant à votre nom de domaine ; dans l'exemple, ce sera **DC=masociete, DC=local**.

Vous pouvez alors naviguer dans la sauvegarde de votre annuaire via cet outil.

Si vous trouvez que l'accès aux données n'est pas très digeste via l'outil **ldp.exe**, sachez que vous pouvez, si vos besoins sont plus limités, voir vos données directement depuis la console Utilisateurs et Ordinateurs Active Directory. Pour cela, faites un clic avec le bouton droit de la souris à la racine de la console puis choisissez

© ENI Editions - All rights reserved - adamo diarra

Changez de contrôleur de domaine. Cliquez sur le message **<Tapez ici un nom de serveur d'annuaire :[port]>** pour y indiquer le nom de votre contrôleur de domaine et le port défini précédemment. Vous accéderez alors à votre annuaire de façon plus pratique qu'avec l'outil **ldp.exe**. Afin d'être complet, il ne faut pas oublier de citer le très bon outil ADExplorer (http://technet.microsoft.com/en-us/sysinternals/66963907.aspx). Il vous permettra de comparer aisément deux clichés instantanés (créés via cet outil), ce qui peut s'avérer extrêmement utile.

- Une fois terminé, n'oubliez pas de fermer dsamain ([Ctrl] **C** à deux reprises) et de démonter l'annuaire avec la commande `ntdsutil snapshot "activate instance ntds" "unmount x"` où x est le numéro du cliché instantané.

g. Les comptes de service géré

Habituellement, lors de l'installation par défaut d'une application, l'administrateur peut configurer celle-ci afin de lancer son service associé en tant que Local System, Local Service ou Network Service.

Il est également possible d'indiquer un compte de domaine afin de lancer ce service mais ce compte de domaine doit généralement avoir un mot de passe qui n'expire jamais. De plus, la sécurité de ce compte laisse fortement à désirer car le mot de passe se trouvant dans le cache LSA, il devient assez facilement accessible.

Deux nouveaux types de comptes de service voient le jour avec Windows Server 2008 R2 (et Windows 7). Il s'agit des "comptes de service géré" (appelés aussi *Managed Service Accounts* ou MSA) et des comptes virtuels (*virtual accounts*).

Grâce à ces nouveaux types de comptes, vous allez vous affranchir de la gestion des mots de passe car ces derniers se renouvelleront automatiquement ! Il n'est ainsi plus nécessaire d'avoir à définir un compte de service avec un mot de passe qui n'expire jamais.

Les MSA sont des nouveaux types de comptes de domaine utilisés pour lancer des services. Ils sont utilisés afin que leur mot de passe soit changé automatiquement et afin de simplifier la gestion des SPN (*Service Principal Name*). Pour rappel, le SPN est nécessaire à l'authentification Kerberos.

Cela permet en outre d'accroître la sécurité du mot de passe du compte de domaine utilisé pour l'exécution d'applications comme SQL Server, IIS, Exchange, ou tout autre service, à condition que les comptes MSA soient supportés par l'éditeur de votre application associée.

Les comptes virtuels sont des comptes de service locaux qui ne nécessitent pas non plus de gestion de leur mot de passe. Les identifiants du compte ordinateur sont utilisés lorsque le service doit accéder à des ressources présentes sur le domaine. Ces comptes se définissent au niveau des propriétés du service depuis la console Services (services.msc), onglet **Connexion**, puis en indiquant le nom d'utilisateur **NT Service\NomDuCompte** et aucun mot de passe. Au redémarrage du service, celui-ci sera lancé avec un nom d'utilisateur portant le nom du service.

Nous allons nous concentrer ici plus particulièrement sur l'utilisation des comptes de service géré car ces derniers peuvent être très utiles dans des environnements de production complexes.

Principe général

Le compte de service géré utilise le même fonctionnement et la même fréquence de renouvellement de mot de passe que le compte ordinateur, soit tous les 30 jours. Il n'obéit à aucune règle de votre politique de mot de passe de domaine ou d'un PSO. Il ne peut pas non plus être verrouillé et il n'est pas possible d'ouvrir une session avec ce compte.

Le mot de passe auto-généré utilise une cryptographie sécurisée permettant de générer un mot de passe de 240 caractères aléatoires.

En termes de limitation de l'utilisation de ce compte, sachez que celui-ci ne peut pas être utilisé par tous les services Windows (vous risquez d'obtenir l'erreur 1297 au démarrage du service par exemple).

Un compte MSA ne peut être utilisé que sur un seul ordinateur à la fois (mais il peut lancer plusieurs services sur ce même ordinateur). Il ne sera ainsi pas possible d'utiliser un MSA pour des clusters ou du Network Load Balancing.

Le Service Pack 1 de Windows Server 2008 R2 permet également de définir un MSA associé à un service installé sur un serveur membre du domaine et qui se trouve sur un réseau périmètre (DMZ, extranet, etc.). Avant le SP1, cette opération échouait si le seul contrôleur de domaine présent sur le même réseau que le serveur exécutant le MSA était un RODC (contrôleur de domaine en lecture seule). Désormais les MSA fonctionneront car les RODC seront aptes à rediriger la requête du MSA vers un contrôleur de domaine inscriptible.

Pré-requis

Les pré-requis permettant d'utiliser les MSA sont les suivants :

- Un domaine Active Directory.
- Une mise à jour du schéma en version 2008 R2. Il n'est pas nécessaire d'avoir un niveau fonctionnel de

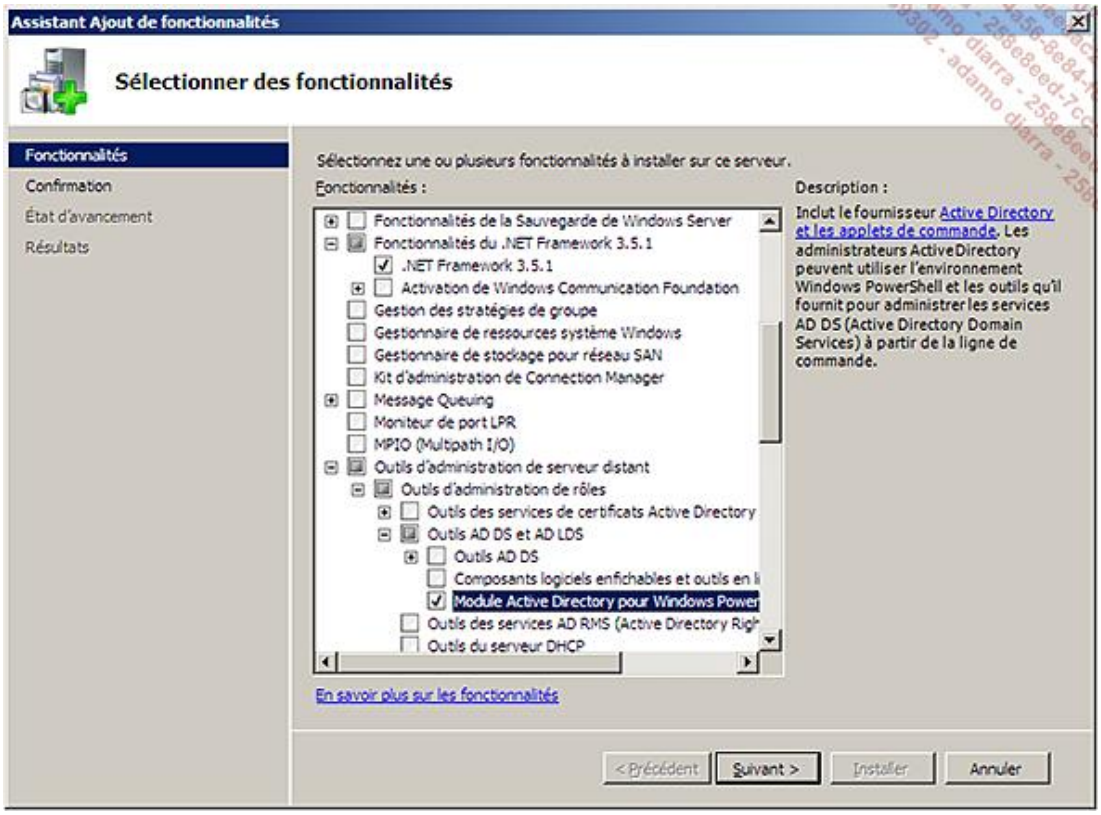
© ENI Editions - All rights reserved - adamo diarra

domaine ou de la forêt en 2008 R2 pour que le renouvellement automatique du mot de passe fonctionne. Par contre, si le niveau fonctionnel est 2003 ou 2008, l'administrateur devra continuer de définir manuellement le SPN de ces comptes MSA. En niveau fonctionnel 2008 R2, le SPN est automatiquement défini.

- Un ordinateur sous Windows Server 2008 ou Windows 7 hébergeant le service à configurer.

- Présence des fonctionnalités PowerShell, le module Active Directory pour PowerShell (disponible dans les outils d'administration RSAT pour Windows 7 à l'adresse suivante :

  http://www.microsoft.com/downloads/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d&displaylang=en) et le .NET Framework 3.5 installés sur les ordinateurs configurant les comptes MSA. Sous Windows Server 2008 R2, l'ajout de ces fonctionnalités se présente ainsi :



- Un service Windows supportant l'utilisation d'un compte MSA.

Installation et configuration

Lors de l'extension du schéma, une nouvelle classe d'objets est créée. Il s'agit de la classe nommée **msDS-ManagedServiceAccount**. Si vous souhaitez déléguer la création de ce compte, il faudra ainsi vérifier au préalable que l'utilisateur créant le compte MSA possède bien le droit Create/Delete msDS-ManagedServiceAccount.

Les pré-requis indiquant l'installation de PowerShell, vous avez sans doute déjà compris que la suite se déroulera sans interface graphique mais en ligne de commande !

Vous allez donc voir ici les étapes détaillées permettant de créer un compte MSA et de l'utiliser pour le lancement d'un service. Les principales sont :

- La création du compte MSA dans l'Active Directory.

- L'association du compte MSA à un ordinateur membre de l'Active Directory.

- L'installation du compte MSA sur l'ordinateur associé.

- La configuration du service afin que ce dernier utilise le compte MSA.

Tous les services Windows n'étant pas compatibles avec cette fonctionnalité, sachez que vous pourrez créer le

© ENI Editions - All rights reserved - adamo diarra

service de votre choix avec les outils **instsrv.exe** et **srvany.exe** du Ressource Kit de Windows Server 2003 (http://www.microsoft.com/Downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd).

- Afin de créer le compte MSA, tout d'abord connectez-vous à votre console d'administration sous Windows 7 ou depuis un serveur sous Windows 2008 respectant les pré-requis indiqués précédemment.

- Lancez la console PowerShell via le menu **Démarrer - Tous les programmes - Accessoires - Windows PowerShell**. La commande ci-dessous permet d'importer le module PowerShell Active Directory précédemment installé à l'aide de la commande puis de créer le compte MSA.

```
Import-Module ActiveDirectory
New-ADServiceAccount -Name <Nom du compte MSA> -Enabled $true
```

Pour éviter toute erreur lors de la saisie des commandes sous PowerShell, vous pouvez utiliser l'auto-complétion en appuyant sur la touche [Tab] après avoir écrit les premières lettres de la commande. Sachez également qu'une fois le compte MSA créé, celui-ci sera visible depuis la console **Utilisateurs et Ordinateurs Active Directory** au niveau du conteneur **Managed Service Accounts**. Vous pourrez ajouter ce compte MSA à un groupe de sécurité Active Directory. Pour cela, éditez le groupe désiré et choisissez d'ajouter un membre. Spécifiez alors le nom du compte MSA nouvellement créé. La cmdlet PowerShell **Add-ADGroupMember** permet également de le faire.

- Une fois le compte MSA créé, il vous faut l'associer à l'ordinateur cible membre de votre Active Directory. Lancez alors la commande PowerShell suivante :

```
Add-ADComputerServiceAccount -Identity <Le nom Netbios de l'ordinateur où sera
utilisé le MSA> -ServiceAccount <Nom du compte MSA crée à l'étape précédente>
```

- Ouvrez une session sur l'ordinateur qui hébergera le compte MSA et installez sur cet ordinateur également le module Active Directory pour PowerShell ainsi que le .NET Framework 3.5.

- Une fois ces composants installés sur l'ordinateur cible, ouvrez une session en tant qu'administrateur du domaine et lancez la console PowerShell pour importer le module Active Directory et installer le MSA.

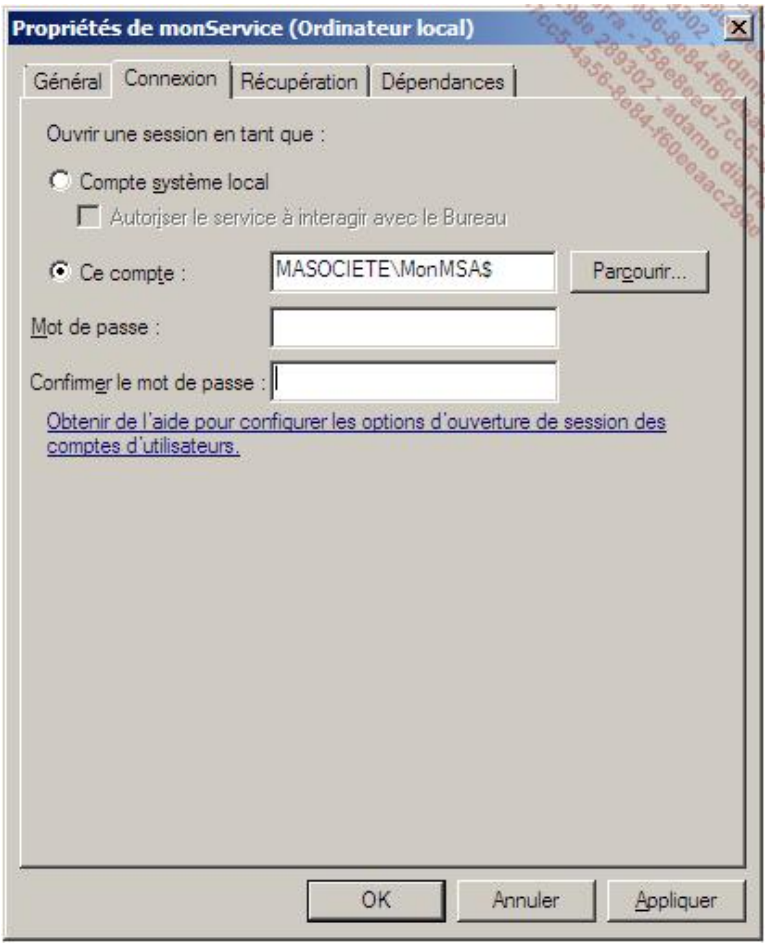
```
Import-Module ActiveDirectory
Install-ADServiceAccount -Identity <Nom du compte MSA créé à l'étape
précédente>
```

Si vous souhaitez déléguer cette étape sans donner les droits d'administrateur du domaine à votre utilisateur, il vous faudra déléguer les droits sur le MSA spécifique à l'aide du script suivant par exemple, à exécuter depuis une invite de commande :

```
dsacls "CN=<Nom du compte MSA créé à l'étape précédente>,CN=Managed Service
Accounts,DC=masociete,DC=local" /G "DOMAINE\<Utilisateur ou groupe>:
SDRCLCRPLOCA" "
DOMAINE\<Utilisateur ou groupe>:WP;Logon Information" " DOMAINE\<Utilisateur
ou groupe>:WP;Description" " DOMAINE\<Utilisateur ou groupe>:WP;DisplayName" "
DOMAINE\<Utilisateur ou groupe>:WP;Account Restrictions" " DOMAINE\<Utilisateur
ou groupe>:WS;Validated write to DNS host name" " DOMAINE\<Utilisateur ou
groupe>:WS;Validated write to service principal name"
```

- Le compte MSA peut alors être associé au service supporté via l'interface graphique en démarrant la console services.msc puis en spécifiant le nom d'utilisateur au niveau de l'onglet **Connexion - Ce compte**. Le compte à indiquer doit alors être **Domaine\NomDuMSA$** (n'oubliez pas le dollar) et n'indiquez aucun mot de passe.

© ENI Editions - All rights reserved - adamo diarra



À noter qu'il est également possible d'associer ce compte MSA à l'aide d'un script PowerShell comme celui-ci :

```
$MSA="domaine\NomduMSA$"
$ServiceName="'Nom_Du_Service'"
$Password=$null
$Service=Get-Wmiobject win32_service -filter "name=$ServiceName"
$InParams = $Service.psbase.getMethodParameters("Change")
$InParams["StartName"] = $MSA
$InParams["StartPassword"] = $Password
$Service.invokeMethod("Change",$InParams,$null)
```

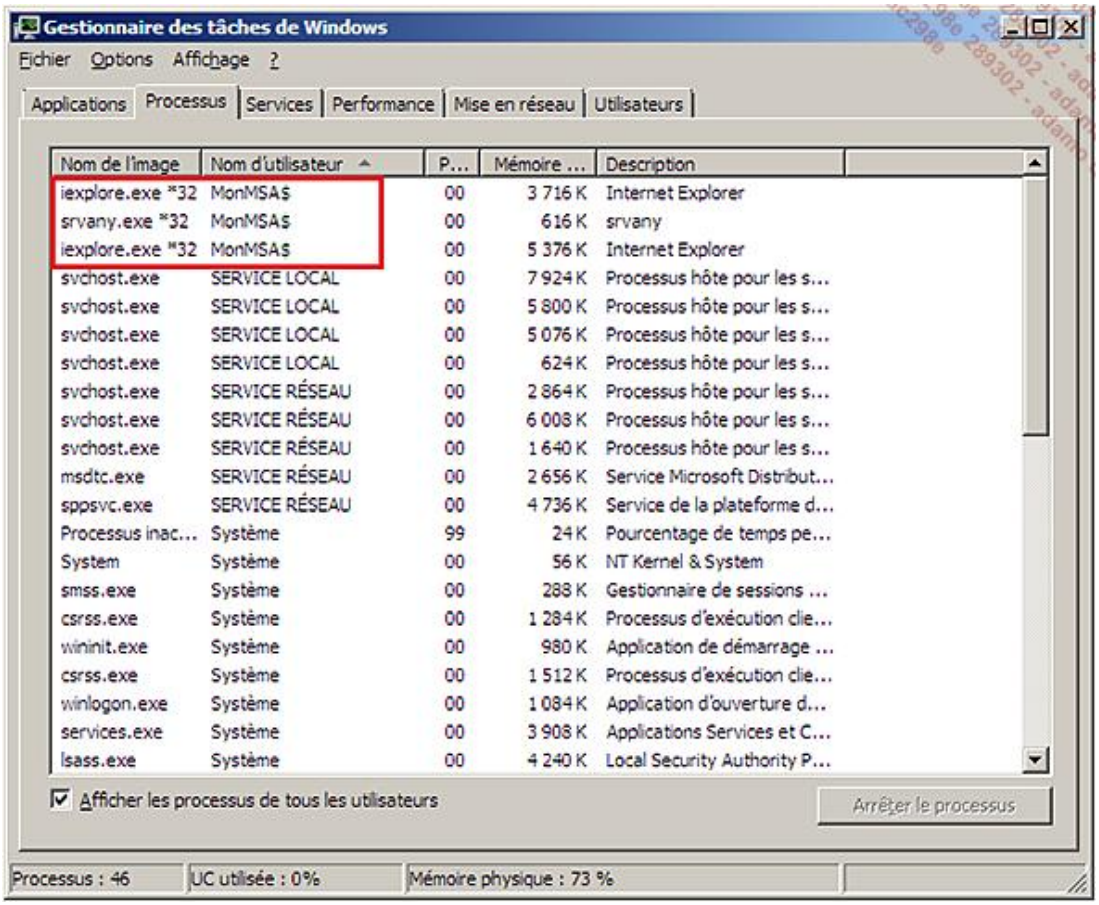
Éditez puis sauvegardez ce fichier à l'aide de notepad dans un fichier avec l'extension ps1.

Afin d'exécuter un script sous PowerShell, il faudra baisser la politique de sécurité par défaut à l'aide de la commande Set-ExecutionPolicy, lancer le script puis redéfinir la politique de sécurité par défaut.

```
Set-ExecutionPolicy remotesigned
Script.ps1
Set-ExecutionPolicy restricted
```

- Démarrez alors le service nouvellement configuré avec le compte MSA. Si tout s'est bien déroulé, le démarrage ne doit pas générer d'erreur et vous pourrez confirmer que ce service est lancé avec le compte MSA via le Gestionnaire des tâches.

© ENI Editions - All rights reserved - adamo diarra



Pour supprimer un compte MSA, il vous faut utiliser la commande PowerShell suivante :

```
Remove-ADServiceAccount -identity <Nom du compte MSA>
```

Vous pourrez également le supprimer de l'Active Directory soit via la console **Utilisateurs et Ordinateurs Active Directory**, soit via la commande suivante :

```
Remove-ADComputerServiceAccount -Identity <Le nom Netbios de l'ordinateur
qui utilisait le MSA>  -ServiceAccount <Nom du compte MSA>
```

Vous venez donc de configurer votre compte MSA pour l'ordinateur le nécessitant. Vous n'aurez ainsi plus à vous soucier de la gestion du mot de passe de ce serveur.

Vous obtiendrez davantage d'informations techniques sur la mise en place des MSA à cette adresse : http://technet.microsoft.com/en-us/library/dd548356(WS.10).aspx

h. La corbeille Active Directory

Windows Server 2008 R2 arrive avec une fonctionnalité qui ravira plus d'un administrateur. Il s'agit d'une corbeille pour les objets Active Directory !

En effet, il est désormais possible de restaurer un objet Active Directory effacé sans nécessairement faire appel à votre dernier jeu de sauvegarde, ni même recourir à un arrêt de service d'un de vos contrôleurs de domaine (en ayant à le redémarrer en mode DSRM puis en utilisant la commande NTDSUTIL). Il est désormais possible, grâce à cette fonctionnalité, de restaurer un objet créé **après** votre dernière sauvegarde disponible de l'Active Directory.

À noter que depuis Windows 2003 Server, il est possible d'utiliser la réanimation d'objets effacés (durant 180 jours par défaut). L'inconvénient majeur de cette solution est qu'elle ne restaure pas certains attributs à valeur liée et non liée.

Concrètement, cela signifie que la restauration d'un compte utilisateur par cette méthode, ne restaure pas ses appartenances aux groupes de sécurité et il faut donc connaître ces informations pour les ajouter dans un second temps.

La corbeille Active Directory vous simplifiera grandement la tâche !

Avant de voir plus en détails la façon dont elle peut être implémentée, concentrons-nous dans un premier temps sur son principe de fonctionnement.

© ENI Editions - All rights reserved - adamo diarra

Principe général

La fonctionnalité de corbeille Active Directory repose sur quatre attributs Active Directory.

isDeleted

Cet attribut existe depuis Windows 2000 Server. Il est présent sur tous les objets de l'annuaire. Il indique qu'un objet est effacé mais peut être restauré.

isRecycled

Cet attribut existe depuis Windows Server 2008 R2. Il est présent sur tous les objets supprimés une fois que la fonction de Corbeille AD est activée. Il indique qu'un objet peut être restauré via la fonction de Corbeille AD.

msDS-DeletedObjectLifetime

Cet attribut existe depuis Windows Server 2008 R2. Sa valeur détermine le temps (en jours) pendant lequel un objet effacé pourra être restauré. Par défaut sa valeur est égale à la valeur de l'attribut TombstoneLifetime.

TombstoneLifetime

Cet attribut existe depuis Windows 2000 Server. Depuis Windows Server 2003 SP1, sa valeur par défaut est de 180 jours. Ce nombre de jours sert à la propagation de l'information sur un objet effacé à tous les contrôleurs du domaine.

Voyons donc ce qui se passe lorsqu'un objet (un compte utilisateur par exemple) est supprimé de l'AD :

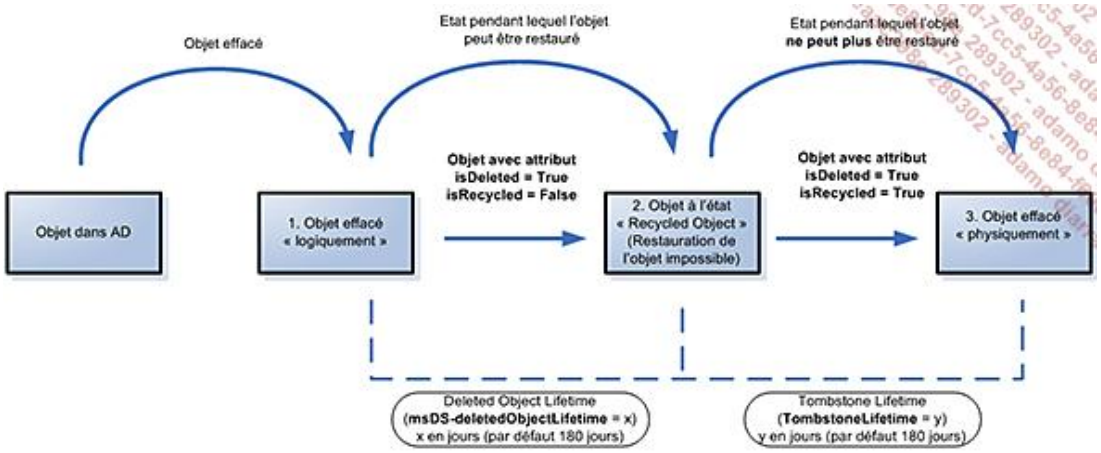
- Lorsqu'un objet est supprimé, celui-ci est déplacé dans le conteneur **CN=Deleted Objects,DC=masociete,DC=local** et l'attribut **isDeleted** prend la valeur **TRUE**. L'administrateur dispose alors du nombre de jours défini par l'attribut **msDS-deletedOjectLifetime** pour pouvoir restaurer l'objet à l'aide la fonctionnalité de la Corbeille AD. Par défaut, sa valeur est égale à la valeur de l'attribut TombstoneLifetime, soit 180 jours dans la plupart des situations. En clair, un objet peut être restauré par la corbeille Active Directory 180 jours après sa suppression par défaut.

- Une fois le nombre de jours défini pour l'attribut **msDS-DeletedObjectLifetime** dépassé, l'attribut **isRecycled** prend à son tour également la valeur **TRUE**. L'objet entre donc dans un nouvel état disponible depuis 2008 R2 nommé « Recycled object » (pardonnez le terme anglophone mais il n'y a pas de traduction française à l'heure où ces lignes sont écrites).

  À ce moment-là, l'objet ne peut plus du tout être restauré (ni via la corbeille AD, ni via une restauration autoritaire) et il perd certains de ses attributs à valeur liée et non liée. L'objet reste alors dans cet état durant la valeur définie pour l'attribut **TombstoneLifetime** soit à nouveau 180 jours. Le principal intérêt de cet état est de prévenir les autres contrôleurs de domaine qu'un objet a été supprimé.

- Une fois le nombre de jours défini pour l'attribut **TombstonedLifetime** dépassé (donc au final 180 + 180 soit 360 jours après la suppression de l'utilisateur), l'objet est « réellement » supprimé de l'Active Directory.

Voici un schéma récapitulatif :



Pré-requis

© ENI Editions - All rights reserved - adamo diarra

Les pré-requis nécessaires à l'utilisation de la corbeille Active Directory ne sont pas des moindres. En effet il faut nécessairement que tous les contrôleurs de domaine de la forêt soient sous Windows Server 2008 R2.

Il vous faudra alors étendre votre schéma à Windows Server 2008 R2 et augmenter le niveau fonctionnel de vos domaines et forêts en Windows Server 2008 R2 (nous avons traité de la façon de le faire au paragraphe Installation d'un annuaire Active Directory).

Sachez également qu'en activant la fonctionnalité de corbeille Active Directory, il ne sera plus possible d'abaisser le niveau fonctionnel du domaine et de la forêt.

Activation et utilisation

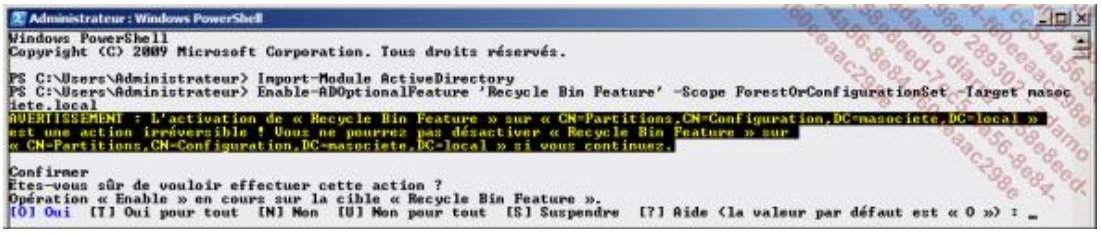
L'activation de la corbeille se fait via PowerShell.

- Ouvrez une session sur le contrôleur de domaine hébergeant le rôle de Maître d'attribution des noms de domaine. Lancez la console PowerShell avec un compte membre du groupe **Administrateurs de l'entreprise**.

- Installez la fonctionnalité **PowerShell** et le **module PowerShell pour Active Directory** si ces derniers ne sont pas présents.

- Lancez alors les commandes suivantes et indiquez "O" (Oui) pour valider la commande.

```
import-module ActiveDirectory

Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet
-Target <le nom de domaine de la racine de votre forêt>
```



Si vous ne savez pas si la corbeille Active Directory est déjà activée, utilisez la commande PowerShell suivante : `Get-ADOptionalFeature -filter *`.

Si **EnabledScopes** possède une valeur, cela signifie que la corbeille Active Directory est activée. S'il est vide {}, cela signifie que la corbeille Active Directory n'est pas activée.

Maintenant que la Corbeille Active Directory est activée, voyons comment l'utiliser en reproduisant différents scénarios possibles en production.

Restauration d'un objet spécifique

Prenons l'exemple d'un utilisateur Active Directory supprimé par mégarde. La réplication s'est faite sur tous les contrôleurs de domaine et vous n'auriez eu, en temps normal, plus d'autre choix que d'utiliser une sauvegarde de votre Active Directory.

Grâce à la corbeille AD, vous pourrez réaliser cette opération en quelques secondes et sans aucune coupure de service.

- Dans notre exemple, l'utilisateur effacé se nomme "Freddy Elmaleh" et son compte se trouvait dans l'unité d'organisation "Siège". Ce compte utilisateur était également membre de plusieurs groupes de sécurité.

- Utilisez PowerShell afin d'afficher les objets effacés pouvant être restaurés.

```
Get-ADObject -filter 'isdeleted -eq $true -and name -ne "Deleted Objects"' -
includeDeletedObjects -property * | Format-List
samAccountName,displayName,lastknownParent
```


© ENI Editions - All rights reserved - adamo diarra

L'option **| Format-List** permet d'interpréter le résultat de la commande **Get-Object** et d'afficher uniquement certains des attributs retournés dans un format facilement lisible. Si vous supprimez les arguments de la ligne de commande ci-dessus à partir du pipe (caractère "|"), PowerShell vous affichera tous les attributs qui seront restaurés pour les objets qui peuvent l'être.

Ceci peut être intéressant à titre informatif mais rapidement trop verbeux pour un environnement de production dans lequel vous aurez plusieurs dizaines d'objets potentiellement restaurables.

Notez qu'un objet ne peut être restauré que s'il a été effacé **après** l'activation de la corbeille Active Directory. Si un objet a été effacé avant, il ne pourra pas être restauré.

- Une fois l'objet identifié, vous pouvez le restaurer à l'aide de la commande PowerShell **Restore-ADObject** :

```
Get-ADObject -Filter 'samaccountname -eq "felmaleh"' -IncludeDeletedObjects |
Restore-ADObject
```

- Aucune confirmation n'apparaît mais si vous retournez dans votre console **Utilisateurs et Ordinateurs Active Directory**, vous verrez que votre compte utilisateur a bien été restauré ainsi que ses attributs comme l'appartenance à des groupes de sécurité.

Si vous n'êtes pas familier de PowerShell, sachez qu'il existe plusieurs outils permettant l'utilisation de la corbeille en mode graphique. PowerGUI est un excellent utilitaire très pratique pour effectuer les opérations normalement uniquement disponibles en PowerShell. Une fois le client PowerGUI installé, vous importez les modules de votre choix. Dans le cadre de la corbeille Active Directory, le module en question est disponible à cette adresse : http://powergui.org/entry.jspa?externalID=2461&categoryID=21.

Restauration d'une unité d'organisation

Prenons maintenant l'exemple de la suppression d'une unité d'organisation ainsi que de tous les objets contenus dans celle-ci (ce qui ne serait vraiment pas de chance si la protection contre la suppression accidentelle était activée sur cette OU !). Vous pouvez restaurer tous ces objets très facilement. Cela se déroule en deux étapes.

- Dans un premier temps il faut restaurer l'unité d'organisation à son endroit d'origine. Dans notre exemple, nous restaurons l'OU "Siège" se trouvant à la racine du domaine :

```
Get-ADObject -filter 'msds-lastKnownRdn -eq "Siège" -and lastKnownParent -eq
"DC=masociété,DC=local"' -includeDeletedObjects | Restore-ADObject
```

- Une fois l'unité d'organisation restaurée, vous pouvez lancer la restauration de tous les objets qu'elle contenait à l'aide de cette commande :

```
Get-ADObject -filter 'lastKnownParent -eq "OU=Siège,DC=masociété,DC=local"' -
includeDeletedObjects | Restore-ADObject
```

Tous les objets présents dans cette OU sont alors restaurés comme si de rien n'était !

Vous êtes désormais capable d'utiliser la corbeille Active Directory en cas de fausse manipulation de votre annuaire Active Directory.

Gardez cependant à l'esprit que cette fonctionnalité ne doit pas vous dispenser de faire des sauvegardes régulières de vos contrôleurs de domaine.

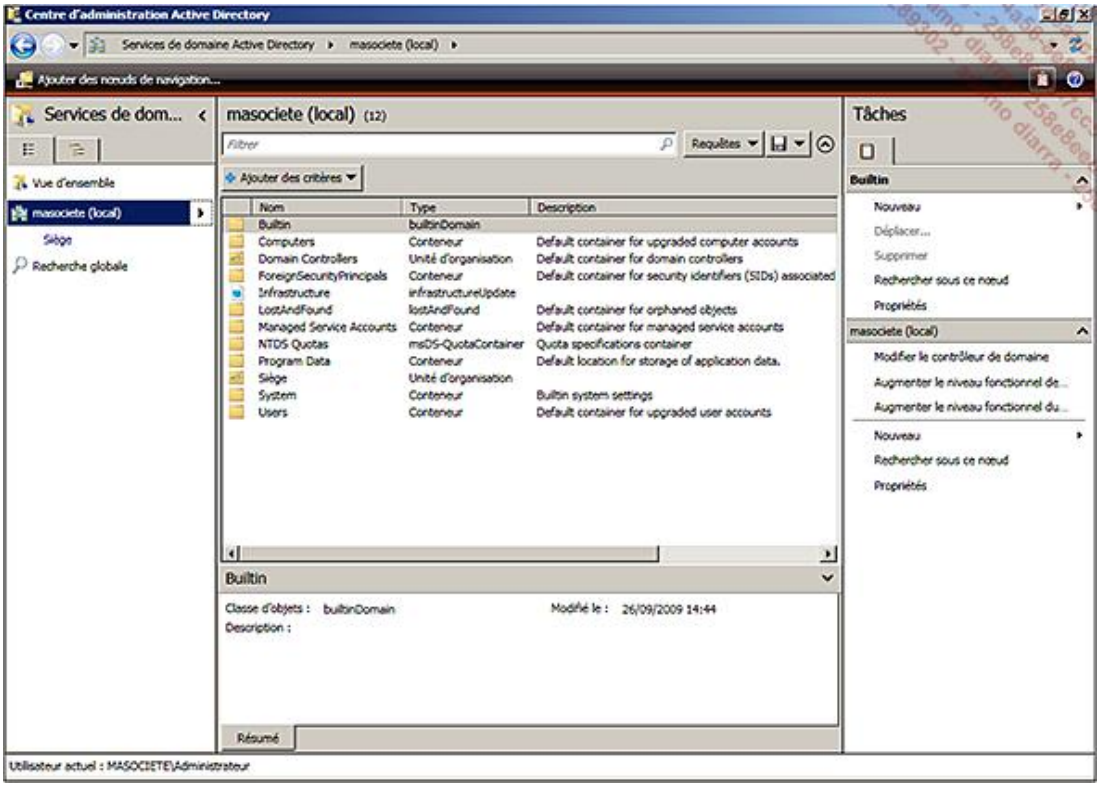
© ENI Editions - All rights reserved - adamo diarra

i. Autres spécificités de Windows Server 2008 R2

Windows Server 2008 R2 propose également certaines autres fonctionnalités très intéressantes concernant l'Active Directory. Parmi ces nouveautés, il y a :

- **Jonction au domaine en mode déconnecté (Offline domain join)** : la commande `djoin` permet de pré-provisionner un compte ordinateur sur un contrôleur de domaine et de créer le blob associé (*Binary Large OBject*). Ce blob pourra alors être déployé sur le poste client (via le registre ou le fichier VHD) permettant ainsi une jonction automatique du poste client au domaine (après redémarrage). Cette jonction sera possible même si l'ordinateur client ne se trouve pas sur le réseau d'entreprise lors de son redémarrage. Vous trouverez davantage d'informations sur cette solution dans le chapitre Déploiement des serveurs et postes de travail.

- **Centre d'administration Active Directory** : une nouvelle console de gestion de l'Active Directory voit le jour afin de remplacer la console ADUC. Cette console est une interface graphique pour PowerShell. Vous pouvez la lancer via les outils d'administration ou en appelant le fichier **dsac.exe**. Les recherches globales permettent notamment de lancer des requêtes LDAP prédéfinies comme la liste des utilisateurs dont le compte est désactivé ou dont le mot de passe a expiré.



Cette console est installée par défaut sur un contrôleur de domaine Windows Server 2008 R2. Elle nécessite la présence du module AD pour PowerShell ainsi que celle du service ADWS (Active Directory Web Service).

- **Service Active Directory Web Service (ADWS)**

  Ce service n'est disponible que sous Windows Server 2008 R2 et est installé par défaut lors de la promotion du serveur en tant que contrôleur de domaine.

  Lorsqu'un administrateur lance une recherche depuis sa console d'administration Active Directory (dsac.exe), celle-ci traduit la requête en commande PowerShell à l'aide des cmdlets du module Active Directory PowerShell installé.

  La commande PowerShell est alors transmise vers le service ADWS sur le port 9389/TCP au travers d'un protocole **WS-* (WS-Transfer, WS-Enumeration)**.

Notez qu'il existe un service équivalent pour les versions antérieures de Windows Server à partir de Windows Server 2003 SP2. Il faut pour cela télécharger et installer l'Active Directory Management Gateway Service (ADMGS) vous permettant ainsi d'interroger vos contrôleurs de domaine à l'aide de commandes PowerShell.

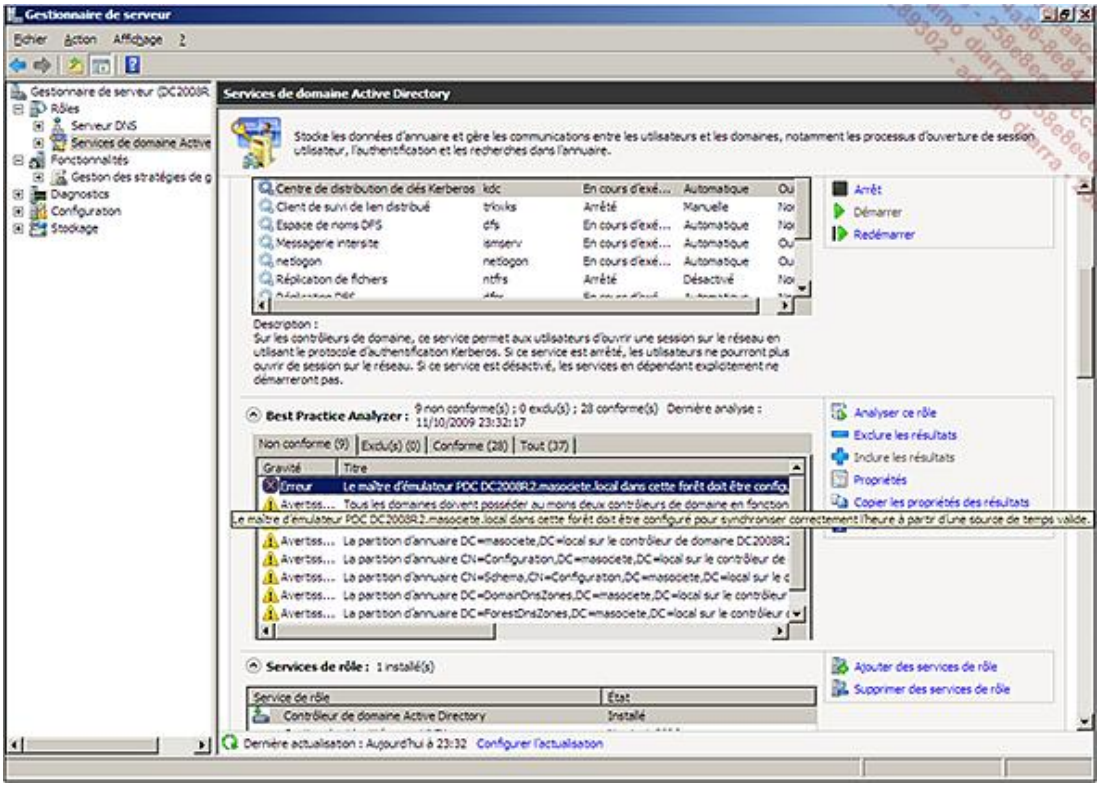
© ENI Editions - All rights reserved - adamo diarra

Les deux services sont équivalents à la différence prêt que l'ADMGS ne pourra pas utiliser une instance d'un cliché instantané de l'Active Directory.

- **Active Directory Best Practice Analyzer Tool**

  Lors de l'installation du rôle Active Directory, Windows Server 2008 R2 installe également le Best Practice Analyzer Tool. Cet outil permet de vérifier tout un ensemble de bonnes pratiques à suivre et de mettre en évidence les erreurs de configuration des contrôleurs de domaine de votre infrastructure, aussi bien des contrôleurs de domaine sous Windows Server 2008 R2 que les autres (2000/2003/2008).

Les tests s'exécutent depuis le Gestionnaire de serveur ou via PowerShell.



Via PowerShell, exécutez les commandes suivantes afin de lancer le scan :

```
Import-Module ServerManager
Import-Module BestPractices
Get-BpaModel
```

Cette commande permet de récupérer l'ID nécessaire pour la commande suivante. Choisissez l'ID correspondant au rôle pour lequel vous souhaitez lancer un scan.

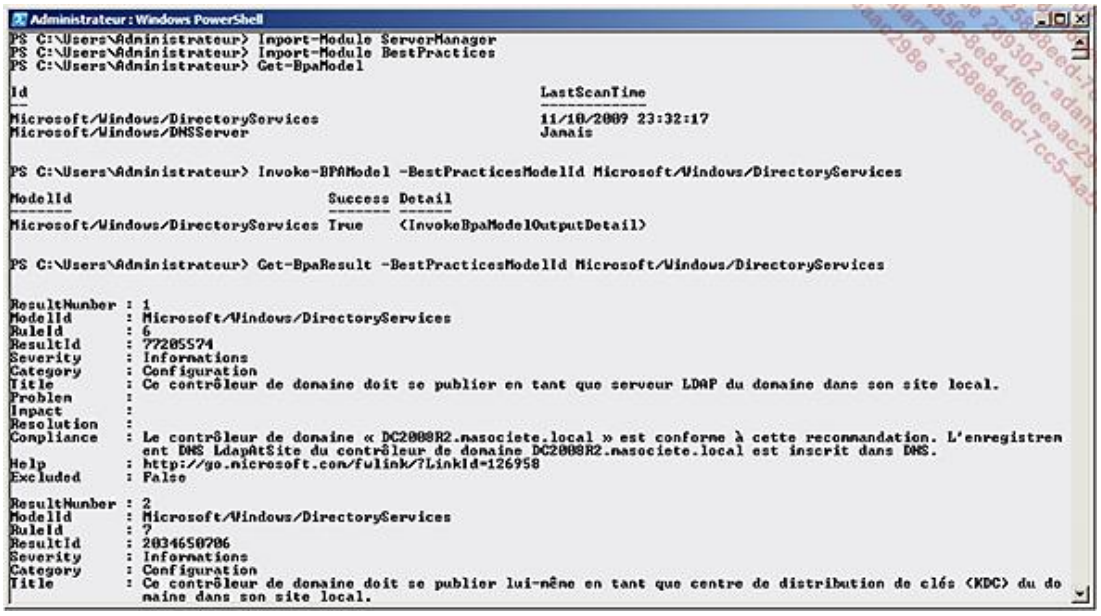
```
Invoke-BPAModel -BestPracticesModelId Microsoft/Windows/DirectoryServices
```

Cette commande permet de lancer l'outil de bonnes pratiques sur le rôle défini par son ID.

```
Get-BpaResult -BestPracticesModelId Microsoft/Windows/DirectoryServices
```

Cette commande permet d'afficher les résultats du scan précédent.

© ENI Editions - All rights reserved - adamo diarra



Sachez que cet outil est également disponible pour les rôles **Active Directory Certificate Services (AD CS), DNS** et **Terminal Server**.

- Support de l'authentification sur des réseaux à haute latence.

  Comme de plus en plus d'entreprises migrent vers "le nuage" (*cloud computing*), il pouvait arriver, avant le Service Pack 1 de Windows 2008 R2, qu'il y ait des échecs d'authentification NTLM (si celles-ci étaient effectuées par des ordinateurs clients sous Windows Vista/7/2008/2008 R2).

  Ces échecs s'expliquent lorsque le contrôleur de domaine se trouve sur un réseau à haute latence, entraînant alors un timeout des requêtes d'authentification.

  La valeur (DWORD) **MaxConcurrentAPI** à créer sur le contrôleur de domaine au niveau de HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters permet de définir le nombre maximum de connexions simultanées au travers d'un canal sécurisé. La valeur maximale est **150** (par défaut, la valeur est à 1 sur un DC et à 2 sur un ordinateur membre).

Maintenant que vous vous êtes familiarisé avec l'administration de l'annuaire Active Directory, découvrez une présentation approfondie des stratégies de groupe.

© ENI Editions - All rights reserved - adamo diarra

Les stratégies de groupe

Les stratégies de groupe sont utilisées au sein d'un domaine Active Directory afin de définir des paramètres communs à un ensemble d'ordinateurs.

Microsoft fournit des améliorations très utiles concernant la gestion des stratégies de groupe sous Windows Server 2008 R2. De nombreuses options supplémentaires ont vu le jour avec cette nouvelle version de Windows et paradoxalement la gestion de ces paramètres a été simplifiée, en comparaison avec les versions précédentes de Windows.

1. Détection des liens lents

La détection des liens lents permet de limiter l'application de certaines stratégies de groupe lorsque l'utilisateur se trouve connecté via un réseau bas débit.

Auparavant cette détection se faisait à l'aide du protocole ICMP avec toutes les contraintes associées. C'est pour cette raison que Microsoft a développé le service Connaissance des emplacements réseau (appelé aussi NLA pour *Network Location Awareness*) pour Windows Vista et Windows Server 2008. Grâce au service NLA, le rafraîchissement en tâche de fond de vos stratégies de groupe sera bien plus fiable car il ne repose plus sur le protocole ICMP mais sur RPC, connu pour sa fiabilité. Si votre ordinateur tente de rafraîchir ses stratégies de groupe (par défaut, cela se produit toutes les 90 minutes) alors que le contrôleur de domaine n'est pas accessible à ce moment là (si l'utilisateur n'est pas branché au réseau par exemple), le rafraîchissement ne se fera pas au prochain cycle (donc 90 minutes plus tard) mais dès que le contrôleur de domaine sera à nouveau accessible. Le service NLA permet en effet de détecter très rapidement la disponibilité du contrôleur de domaine dans ce cas de figure.

2. Le format ADMX

Un nouveau format de fichier a vu le jour avec Windows Vista et maintenant Windows Server 2008. Il s'agit des fichiers ADMX. Ces fichiers sont utilisés pour afficher les différentes options des stratégies de groupe.

Ils possèdent de nombreux avantages comparés au format de fichiers précédents (les fichiers ADM). Parmi les principaux avantages de ce nouveau format, il faut retenir :

- Le langage utilisé dans les fichiers AMDX est le XML. Ce format est censé devenir à terme un standard d'échanges d'informations entre applications, faciliter l'interopérabilité, etc.

- La centralisation du stockage des fichiers modèles ADMX dans le dossier SYSVOL alors qu'auparavant les fichiers ADM étaient stockés dans chaque stratégie de groupe de chaque contrôleur de domaine. Il suffit donc simplement de copier/coller les fichiers ADMX d'un poste client sous Windows Vista ou Windows Server 2008 (disponibles dans le dossier c:\Windows\PolicyDefinitions) vers le dossier PolicyDefinitions que vous aurez créé au niveau du partage \\<nom_de_domaine>\SYSVOL\<nom_de_domaine>\Policies. Les administrateurs souhaitant éditer une stratégie n'ont ainsi plus besoin de se soucier de savoir s'ils possèdent les bons fichiers modèles de stratégie puisque ces derniers seront automatiquement récupérés depuis le partage réseau.

- L'indépendance du fichier de langue contenant le texte de chacune des options des stratégies de groupe. Un fichier de langue ayant l'extension .ADML est attaché à chaque fichier ADMX. Il est modifiable à l'aide d'un simple éditeur de texte car il est aussi au format XML. Le détail des modifications engendrées sur le système par le choix d'une stratégie n'est pas contenu dans le fichier ADML mais dans le fichier ADMX associé.

Microsoft fournit par défaut 146 fichiers ADMX et autant de fichiers ADML correspondant à la langue du système d'exploitation. Si vous aviez créé vos propres fichiers modèles de stratégies au format ADM, il vous est possible de convertir ces derniers au format ADMX à l'aide de l'outil **ADMX Migrator** fourni par Microsoft à l'adresse suivante : http://www.microsoft.com/downloads/details.aspx?FamilyId=0F1EEC3D-10C4-4B5F-9625-97C2F731090C. Cet outil permet également de créer vos propres fichiers ADMX.

3. Journaux d'évènements

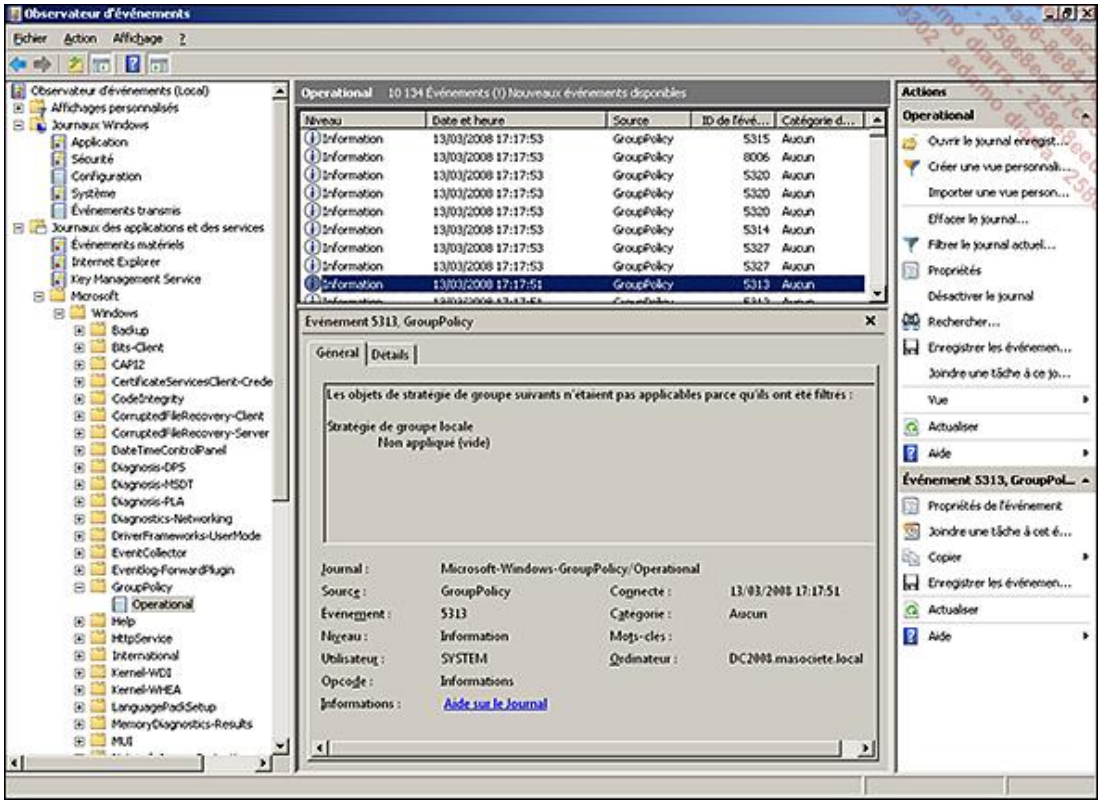
Dans les versions précédentes de Windows, les journaux d'évènements concernant les stratégies de groupe ont toujours été difficiles à appréhender car le format utilisé était peu parlant pour les administrateurs non-initiés.

Il est désormais possible d'afficher les évènements relatifs aux stratégies de groupe directement depuis le journal des évènements d'un poste sous Windows Vista ou Windows Server 2008.

© ENI Editions - All rights reserved - adamo diarra

- Pour cela, cliquez sur le menu **Démarrer** puis **Outils d'administration** et **Observateur d'événements**.

- Déroulez alors le menu **Journaux des applications et des services - Microsoft - Windows - GroupPolicy - Operational**.



L'outil **Group Policy Log View** vous permettra d'extraire le fichier journal des stratégies de groupe au format TXT ou HTML. Le logiciel est disponible à cette adresse : http://www.microsoft.com/downloads/details.aspx?FamilyID=BCFB1955-CA1D-4F00-9CFF-6F541BAD4563&displaylang=en

---

Vous pourrez ainsi récupérer beaucoup plus aisément un grand nombre d'informations concernant le fonctionnement des différents paramètres de stratégies de groupe appliqués.

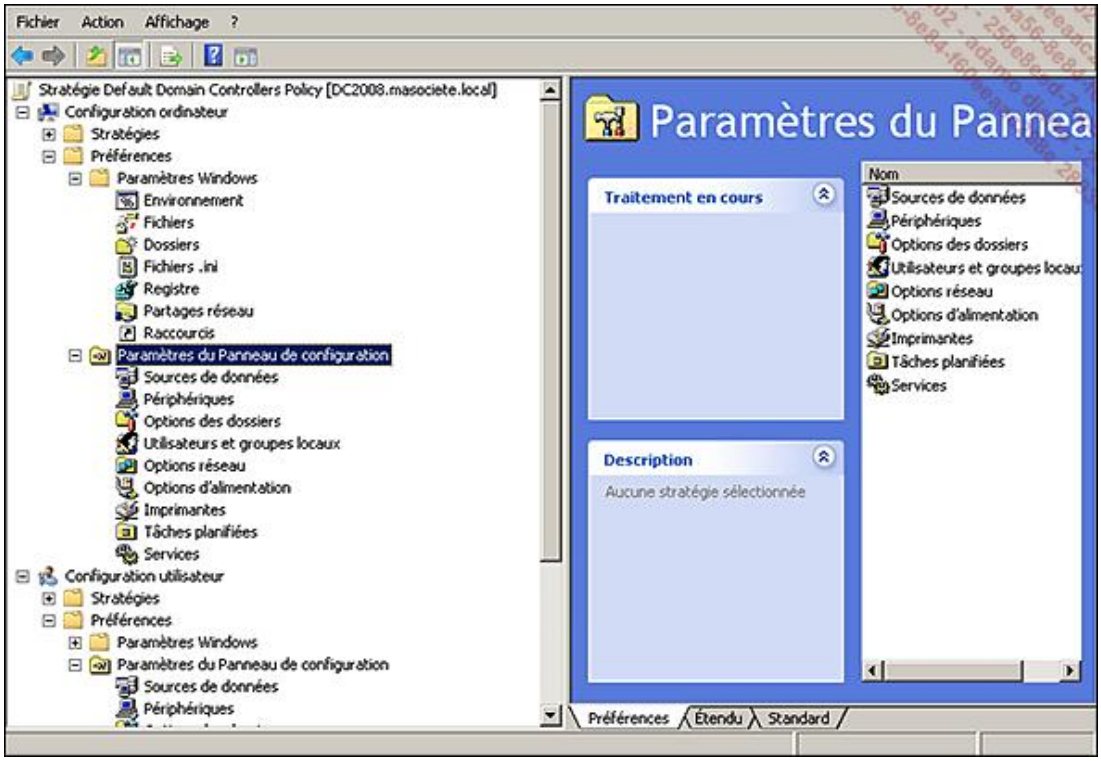
4. Des stratégies de groupe très utiles

De nouvelles catégories de stratégie de groupe très utiles ont vu le jour depuis Windows Server 2008 comme par exemple les *stratégies de groupe de préférences*.

Les *stratégies de groupe de préférences* offrent une alternative aux scripts très souvent utilisés pour la personnalisation de l'environnement utilisateur. Il est en effet possible d'utiliser les stratégies de groupe afin de configurer les lecteurs réseaux, les partages, les utilisateurs et groupes locaux, les options d'alimentation, les imprimantes à installer, les tâches planifiées, etc.

Ces paramètres sont visibles au niveau de **Configuration ordinateur (ou utilisateur) - Préférences - Paramètres du Panneau de configuration**.

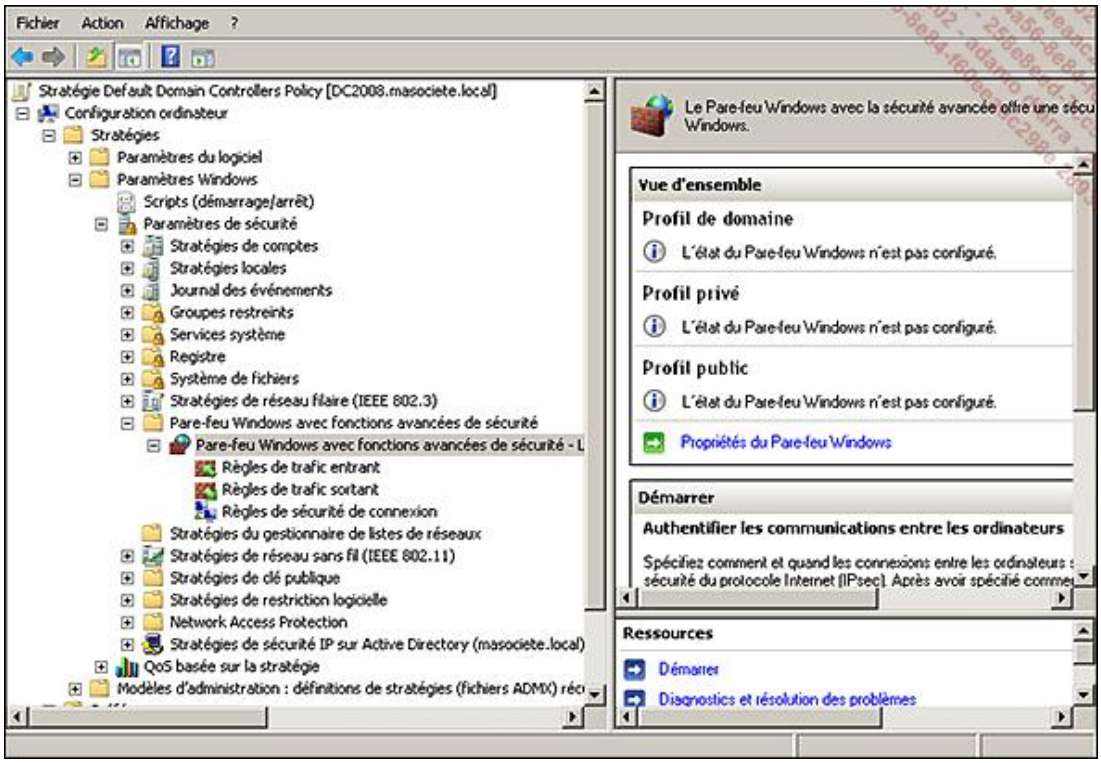
© ENI Editions - All rights reserved - adamo diarra



Les stratégies de groupe de préférences ont été améliorées sous Windows Server 2008 R2, notamment pour la prise en charge des postes clients Vista pour les options d'alimentation, les tâches planifiées, ainsi que les paramètres d'Internet Explorer 8.

Des options ont également été ajoutées au niveau des paramètres de sécurité comme les stratégies de réseau filaire (IEEE 802.3), les stratégies du gestionnaire de listes de réseaux, le Network Access Protection, etc.

Les paramètres de stratégies du pare-feu et d'IPSec ont été réunis dans une seule console MMC, accessible également depuis n'importe quelle stratégie de groupe. Il est alors possible de définir des règles de trafic entrant, de trafic sortant et de sécurité de connexion (utilisant le protocole IPSec) pour les clients sous Windows Vista et Windows Server 2008. Ces paramètres seront accessibles depuis **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Pare-feu Windows avec fonctions avancées de sécurité**.



Les paramètres de stratégies pour l'IPSec et le pare-feu des anciennes versions de Windows sont toujours accessibles en passant par l'ancien chemin **Configuration ordinateur - Stratégies - Modèles d'administration -**

© ENI Editions - All rights reserved - adamo diarra

5. La console Gestion des stratégies de groupe

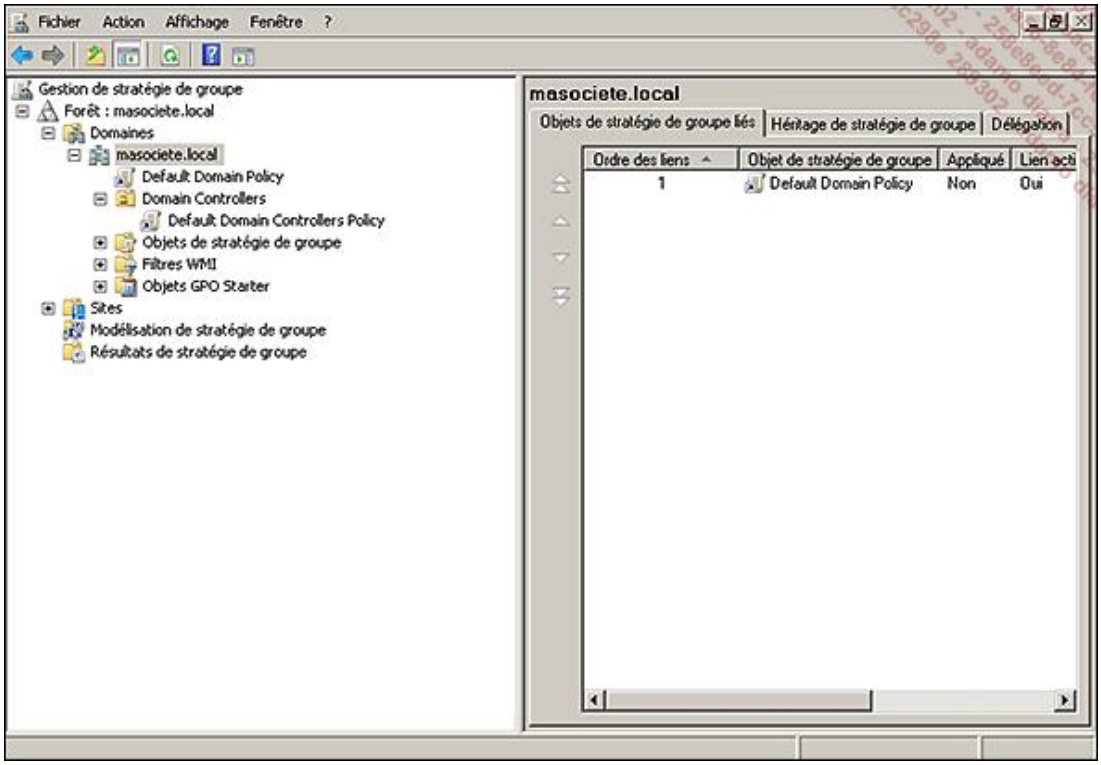
La console Gestion des stratégies de groupe (connue aussi sous le nom de GPMC pour *Group Policy Management Console*) est l'outil indispensable pour gérer les stratégies de groupe de votre domaine Active Directory.

Si l'ordinateur depuis lequel vous souhaitez éditer les stratégies de groupe ne possède pas la console GPMC, il vous faudra installer cette fonctionnalité depuis le **Gestionnaire de serveur - Ajouter des fonctionnalités** et cocher la case **Gestion des stratégies de groupe**.

L'outil RSAT (pour *Remote Server Administration Tools*) permet de déporter la configuration des stratégies de groupe (et d'une façon générale l'administration des rôles et fonctionnalités de votre serveur) depuis un ordinateur client. Cet outil est téléchargeable sur le site de Microsoft à l'adresse suivante : http://support.microsoft.com/kb/941314.

- Afin d'accéder à la console GPMC, cliquez sur le bouton **Démarrer** puis **Outils d'administration** et **Gestion des stratégies de groupe**.

La console vous présentera alors l'organisation du ou des domaines de la forêt de votre choix, leurs OU et sous-OU ainsi que les objets de stratégies de groupe définis.



Cette console vous permet donc de :

- Créer, modifier, supprimer ou lier vos stratégies de groupe au conteneur des sites, domaines ou unités d'organisation de la forêt de votre choix.
- Configurer le filtrage de l'application d'une stratégie (via filtre WMI ou via la sécurité de la stratégie).
- Gérer la délégation.
- Définir des résultats de stratégie de groupe afin de simuler l'application d'une statégie avant sa mise en production.
- Effectuer des sauvegardes/restaurations des stratégies de groupe.

© ENI Editions - All rights reserved - adamo diarra

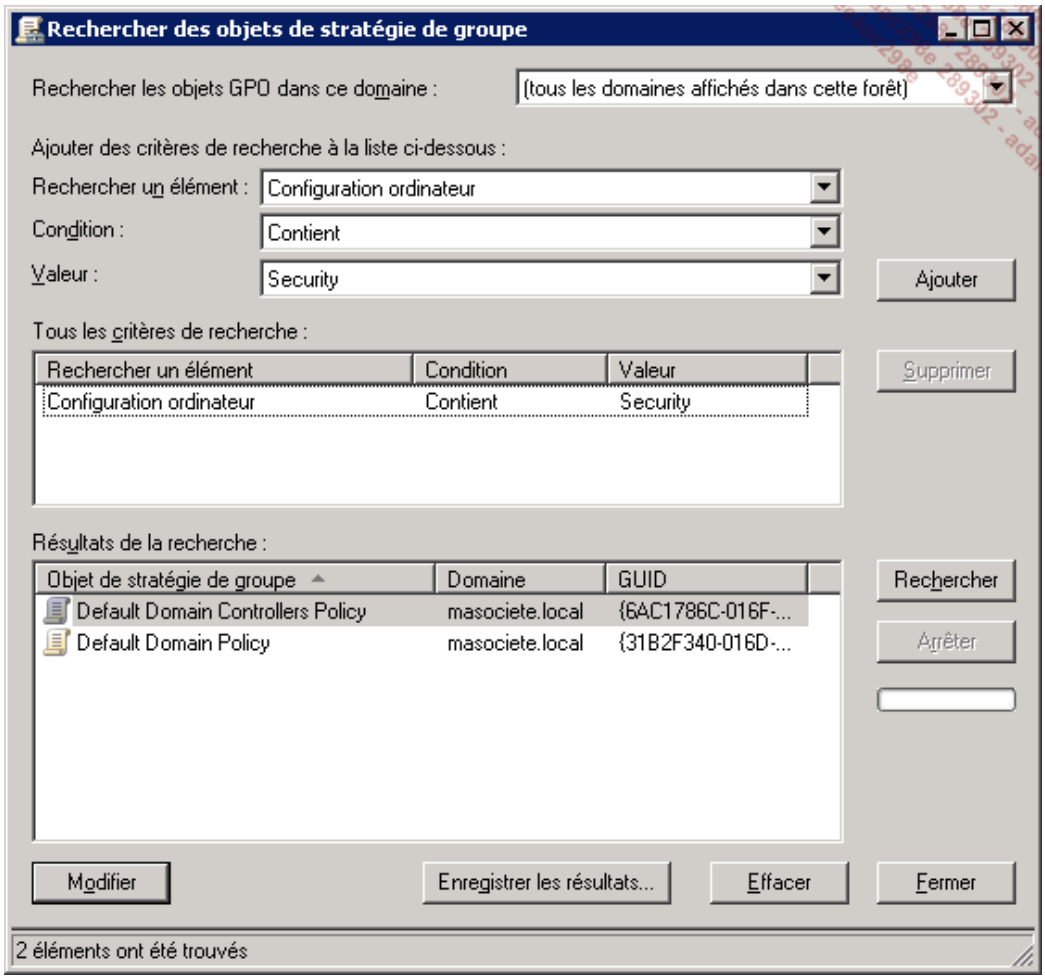
- etc.

Parmi ces nombreuses fonctionnalités, il ne faut pas oublier deux options qui ont fait leur apparition avec Windows Server 2008. Il s'agit de la possibilité d'effectuer des recherches et de définir des modèles de stratégies.

La fonction **Rechercher** est disponible à deux niveaux dans la console GPMC.

Pour les grosses sociétés gérant un grand nombre d'objets de stratégies de groupe, une fonction **Rechercher** est disponible en faisant un clic avec le bouton droit de la souris sur la forêt ou le domaine de votre choix. Il est alors possible d'afficher les objets de stratégies de groupe répondant à certains critères que vous aurez pris soin de définir.

Il est donc possible de choisir d'afficher les stratégies de groupe pour lesquelles des paramètres de sécurité sont définis.



L'autre fonction **Rechercher** disponible intéressera la plupart d'entre vous. Cette fonction est joignable depuis l'éditeur de gestion des stratégies de groupe. Elle vous permettra de filtrer l'affichage des nombreux paramètres de stratégies se trouvant sous le nœud **Modèles d'administration** en fonction de critères spécifiques.

Vous pouvez ainsi retrouver les paramètres de stratégies répondant à votre besoin sans avoir à naviguer parmi les milliers de paramètres possibles.

Pour utiliser cette option, procédez comme suit :

- Depuis votre console GPMC, faites un clic avec le bouton droit de la souris sur l'objet stratégie de groupe que vous souhaitez modifier ; choisissez alors l'option **Modifier** pour accéder à l'éditeur.

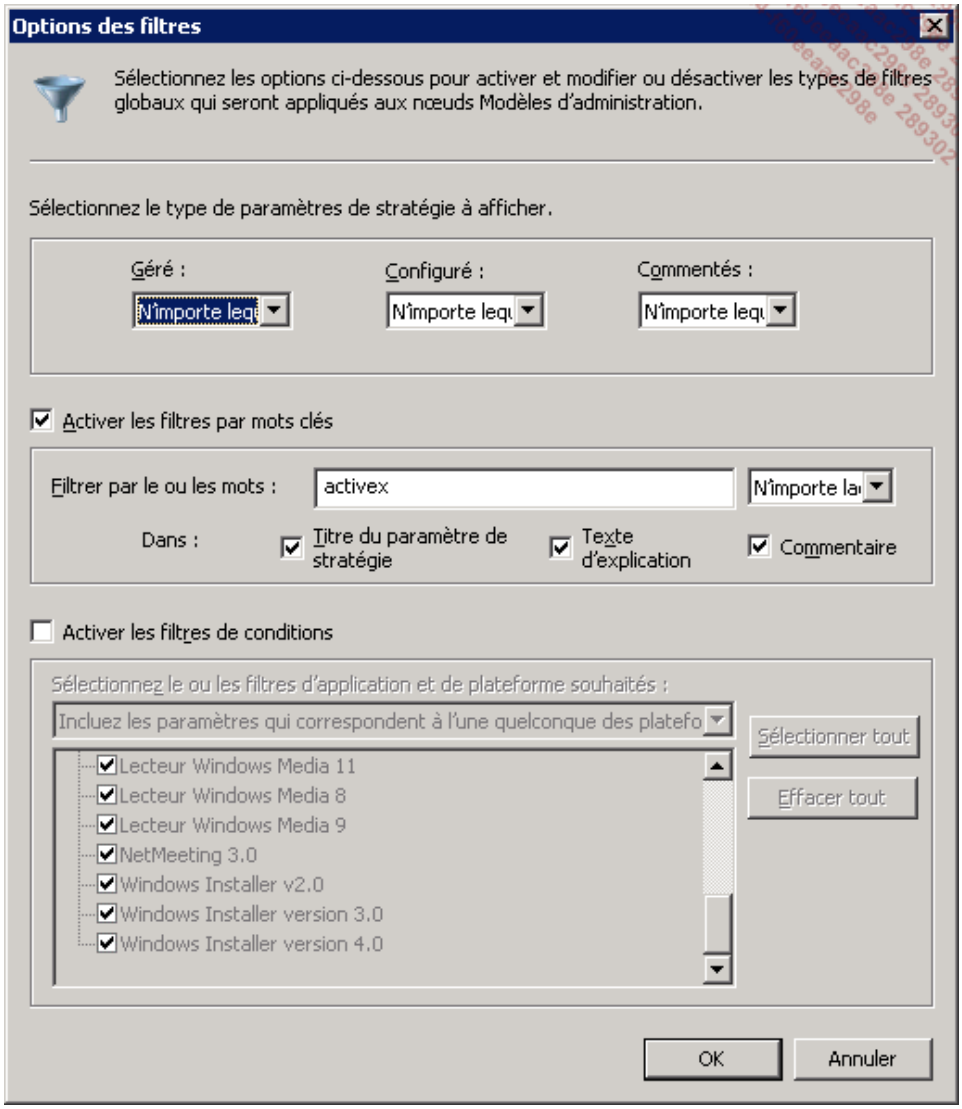
- L'éditeur de gestion des stratégies de groupe s'ouvre alors. Naviguez jusqu'au nœud **Modèles d'administration : définitions de stratégies...** via **Configuration ordinateur** (ou **Configuration utilisateur**) - **Stratégies**. Afin d'initier une recherche parmi tous ces paramètres, faites un clic avec le bouton droit de la souris sur ce nœud principal (ou l'un de ses sous-dossiers même si la recherche s'effectuera quoi qu'il arrive sur tous les paramètres de ce nœud) puis choisissez **Options des filtres**.

- Les options des filtres sont divisées en trois catégories vous permettant d'affiner votre recherche. Vous pouvez ainsi choisir d'afficher uniquement les paramètres de stratégie qui sont configurés. Il est également possible d'effectuer un filtrage par mots clés. Enfin, vous pouvez choisir d'afficher les paramètres en définissant des filtres de

© ENI Editions - All rights reserved - adamo diarra

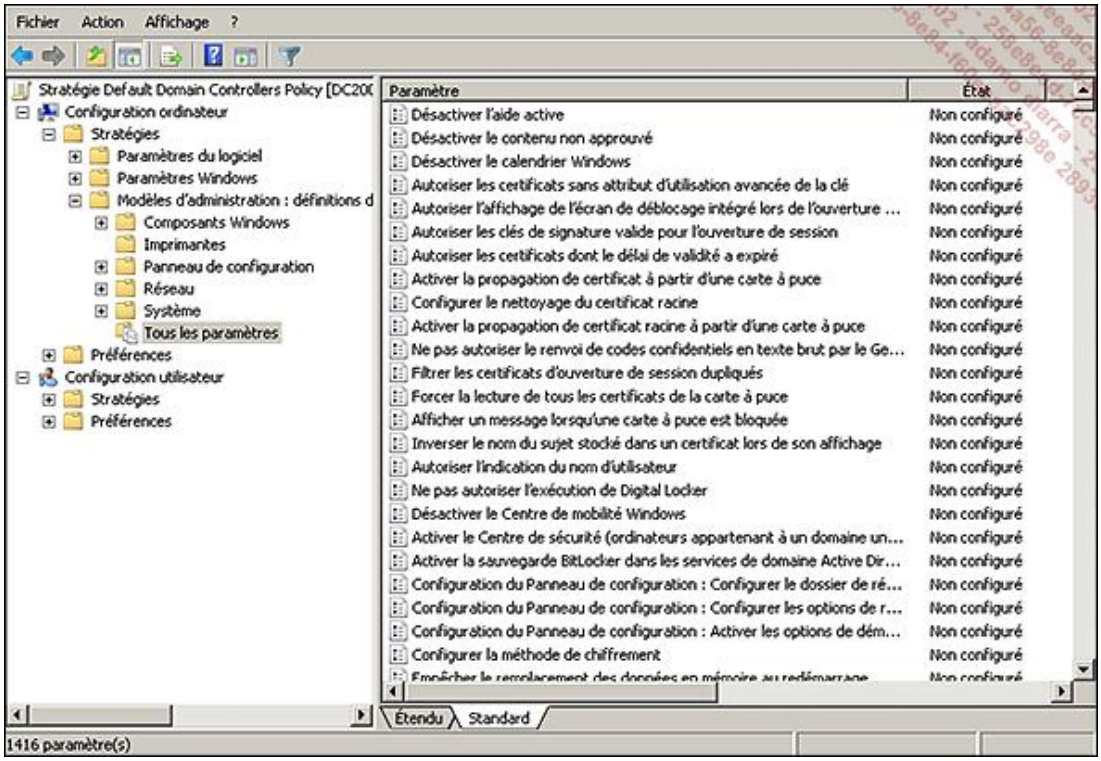
conditions afin d'afficher en quelques secondes les paramètres applicables à la famille Windows Vista par exemple.

L'exemple ci-dessous définit un filtre qui affichera tous les paramètres contenant le mot *activeX* dans le titre du paramètre de stratégie, le texte d'explication ou en commentaire (un onglet **commentaire** vous permet en effet d'ajouter le texte de votre choix à la création d'une stratégie de groupe ou à l'activation d'un paramètre). Cliquez alors sur **OK** pour valider le filtre.



Une fois le filtre validé, l'arborescence de l'éditeur de stratégie se met automatiquement à jour pour n'afficher que les paramètres correspondant au filtre défini. Ces paramètres sont également regroupés dans le nœud **Tous les paramètres**.

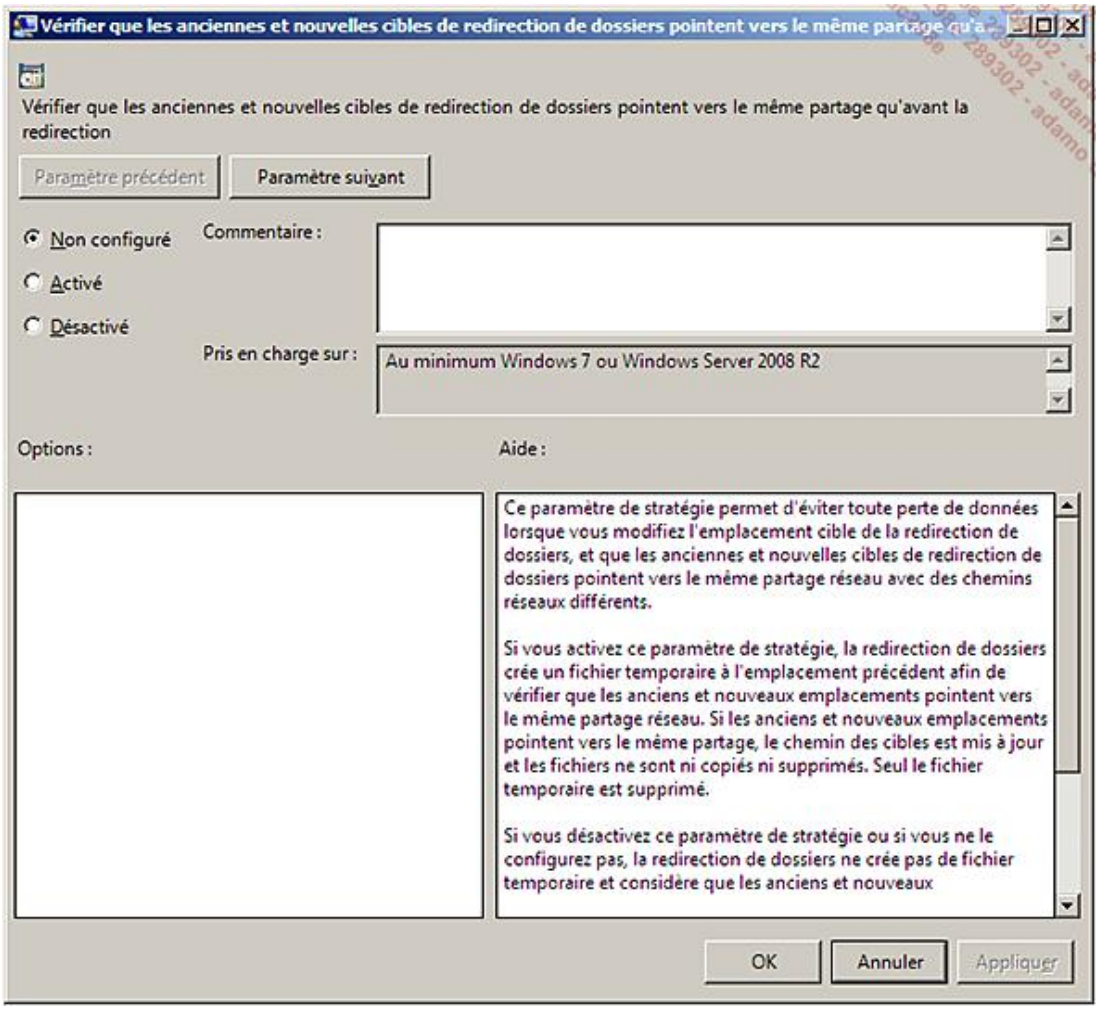
© ENI Editions - All rights reserved - adamo diarra



- Pour désactiver le filtre et retrouver un affichage complet, faites un clic avec le bouton droit de la souris sur un des dossiers de **Modèles d'administrations : définitions de stratégies** et enlevez la coche au niveau de **Filtre activé**.

Les stratégies éditées depuis Windows Server 2008 R2 ou Windows 7 avec les outils RSAT possèdent une interface utilisateur améliorée. En effet, les différents onglets qui étaient affichés lorsque vous éditiez une stratégie depuis Windows 2008 (ou versions antérieures) sont regroupés dans une seule et même fenêtre redimensionnable. Vous y gagnerez largement en clarté !

© ENI Editions - All rights reserved - adamo diarra



Depuis Windows Server 2008 R2, les paramètres de stratégies de groupe prennent en charge la valeur multi-chaîne (REG_MULTI_SZ) ainsi que les valeurs QWORD (pour des applications 64 bits).

Ces GPO de préférences peuvent être modifiées au travers de la cmdlet PowerShell **GPPrefRegistryValue** (ou **GPRegistryValue** pour des paramètres de GPO basés sur des modifications de registre). Il faudra pour cela importer le module via la commande **Import-Module GroupPolicy**.

Le filtrage est pour le moment limité aux paramètres définis dans les Modèles d'administration. Si vous souhaitez une liste plus complète (mais non exhaustive) des paramètres regroupant également les paramètres de sécurité, etc. récupérez le fichier Group Policy Settings Reference for Windows and Windows Server (valable pour Windows Server 2003 SP2/2008/2008 R2 et Windows Vista, Vista SP1 et 7) au format XLS ou XLSX : http://www.microsoft.com/downloads/details.aspx?familyid=18C90C80-8B0A-4906-A4F5-FF24CC2030FB&displaylang=en (disponible en anglais uniquement).

---

6. Les objets GPO Starter

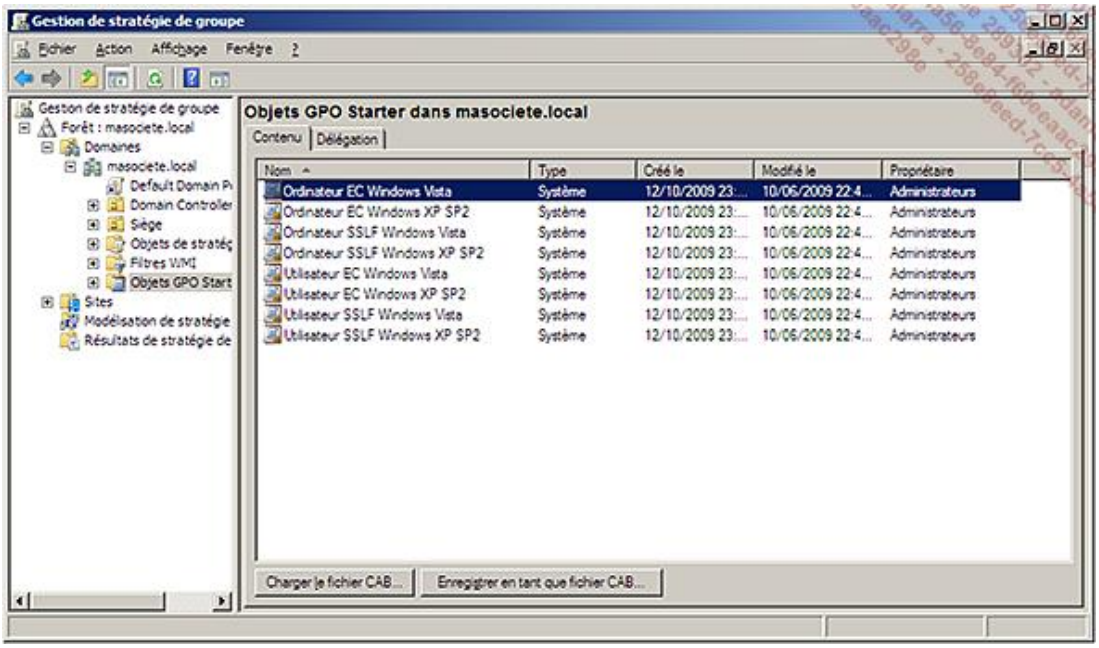
Si vous êtes un peu observateur, vous avez sans doute remarqué en éditant vos stratégies à l'aide de la console GPMC depuis un PC équipé de Windows Server 2008 ou Windows Vista SP1 qu'un nouveau paramètre avait fait son apparition. Il s'agit du conteneur **Objets GPO Starter**.

Cette option consiste à créer des modèles de stratégies de groupe se référant aux paramètres disponibles sous le nœud **Modèles d'administration** uniquement (coté Utilisateurs et Ordinateurs). Il est ainsi très facile de créer plusieurs objets de stratégies de groupe qui se baseront sur un ensemble de paramètres communs devant être définis dans vos stratégies de groupe.

Si vous éditez un objet GPO Starter depuis un poste sous Windows Server 2008 R2 ou un Windows 7 ayant les outils d'administration RSAT installés, vous obtiendrez directement les paramètres de stratégies de groupe recommandés pour les scénarios décrits dans les guides de Sécurité Vista et XP.

Pour information, sous Windows 2008, vous pourrez obtenir ces éléments après les avoir téléchargés à l'adresse suivante : http://www.microsoft.com/Downloads/details.aspx?familyid=AE3DDBA7-AF7A-4274-9D34-1AD96576E823&displaylang=en

© ENI Editions - All rights reserved - adamo diarra



Il est également possible d'exporter ces modèles de GPO dans un fichier CABinet (.CAB) pour alors les importer dans un environnement totalement différent comme par exemple votre environnement de préproduction.

Lors de la première activation des Objets GPO Starter, un dossier nommé StarterGPOs est créé dans le dossier SYSVOL du contrôleur de domaine. Un nouveau sous-dossier sera créé avec un GUID associé pour chaque nouvel objet GPO Starter.

Afin de planifier une sauvegarde de l'ensemble de vos stratégies, n'oubliez pas de choisir l'option **Sauvegarder tout** disponible depuis le conteneur Objets de Stratégie de Groupe **et** depuis le conteneur Objets GPO Starter.

© ENI Editions - All rights reserved - adamo diarra

Les autres composants Active Directory

Quatre autres principales fonctionnalités en rapport avec l'Active Directory sont disponibles sous Windows Server 2008 R2.

Il s'agit de AD LDS, AD FS, AD RMS et AD CS.

1. Active Directory Lightweight Directory Services (ou AD LDS)

Le rôle AD LDS disponible sous Windows Server 2008 R2 est le nouveau nom de l'ADAM qui avait fait son apparition avec Windows Server 2003 R2.

Il s'agit d'une version épurée de l'Active Directory Domain Services (AD DS) qui repose sur les mêmes fondamentaux (à savoir une réplication multimaîtres, un annuaire divisé en partitions, etc.) mais qui ne stocke aucun composant de sécurité de Windows (comme les comptes utilisateurs et ordinateurs du domaine), les stratégies de groupe, etc.

Le rôle AD LDS permet ainsi de répertorier des informations nécessaires aux applications dans un annuaire centralisé plutôt qu'individuellement dans chaque application. Les avantages à ne pas nécessairement intégrer les applications dans l'AD DS sont divers.

- Une application nécessitant pourra faire la mise à jour du schéma sur l'AD LDS plutôt que sur l'AD DS, ce qui évitera des risques inutiles de corruption du schéma.
- Une application accessible sur un extranet ou par VPN n'exposera pas l'ensemble du domaine AD DS si elle a pour annuaire de référence un annuaire AD LDS.

À noter qu'il est possible d'avoir plusieurs instances AD LDS sur un même serveur, de même qu'il est possible d'avoir le rôle AD LDS installé sur un Windows Server 2008 R2 possédant le rôle de AD DS. Le seul pré-requis est que les ports d'écoute des différentes instances doivent être différents.

2. Active Directory Federation Services (ou AD FS)

Le composant Active Directory Federation Services permet de mettre en place une solution d'accès sécurisée entre différentes plates-formes Windows ou non-Windows lors d'accès à des applications Web (sur un extranet par exemple).

L'utilité typique de la mise en place d'un AD FS au sein de votre société est de permettre à un client ayant récemment signé un contrat et se connectant depuis un autre réseau (cas d'un B2C), à une société partenaire (cas d'un B2B) ou à une fédération interentreprises (multiforêts) d'accéder aux ressources de votre réseau d'une façon simple et sans avoir à s'authentifier sur votre base de comptes utilisateurs.

Une relation d'approbation est en effet créée entre le réseau partenaire et le vôtre afin de projeter l'identité des utilisateurs et leurs droits d'accès depuis leur réseau vers les partenaires approuvés. L'utilisateur n'aura ainsi pas à entrer à nouveau ses identifiants (principe de l'authentification unique appelée aussi SSO pour *Single Sign On*).

Il faut savoir également que cette solution est limitée uniquement aux accès via des applications Web (en HTTPS) mais ces dernières étant de plus en plus puissantes, vos possibilités sont très larges. C'est le cas par exemple avec l'intégration de SharePoint Server 2007 ou de AD RMS que nous présenterons un peu plus tard.

Afin de pouvoir mettre en œuvre l'AD FS, un certain nombre de fonctionnalités et de services devront avoir été mis en place au préalable :

- Le Rôle AD DS ou AD LDS devra être installé sur au moins un des réseaux impliqués.
- Serveur de fédération de comptes/ressources.
- Serveur Web ADFS.
- Client.

Vous trouverez davantage d'informations sur le concept d'AD FS à cette adresse : http://technet.microsoft.com/fr-fr/library/bb821278.aspx

© ENI Editions - All rights reserved - adamo diarra

3. Active Directory Rights Management Services (ou AD RMS)

AD RMS (*Active Directory Right Management*) est un rôle permettant de limiter la diffusion et protéger des fichiers, courriers électroniques ou sites Web de votre société.

AD RMS fonctionne avec des applications compatibles RMS comme le système Microsoft Office 2003 Professionnel, Microsoft Office 2007, Internet Explorer 7.0, etc.

Le principe d'utilisation des fonctionnalités de l'AD RMS repose sur le principe qu'une licence de publication est délivrée à un fichier. L'utilisateur indique alors un ensemble de droits et de conditions spécifiques pour ce document. Ces propriétés le suivront alors afin de le protéger au cours de son cycle de diffusion. Vous serez ainsi capable de contrôler les actions possibles sur un fichier ou son contenu, de définir une durée de validité (pour un devis par exemple), etc.

Ainsi, lorsque le fichier diffusé est ouvert pour la première fois par une application compatible AD RMS, cette dernière contacte le serveur AD RMS ayant émis la licence de publication associée au fichier afin de demander l'autorisation d'accéder à son contenu.

Le serveur AD RMS vérifie alors si l'utilisateur est bien autorisé à visualiser le fichier, et si tel est le cas il envoie une licence d'utilisation au demandeur afin de lui permettre d'accéder au contenu du document. L'utilisateur peut alors ouvrir le fichier à l'aide de l'application compatible RMS.

4. Active Directory Certificate Services (ou AD CS)

Afin d'être complet, il est important d'évoquer le seul rôle que nous n'avons pas encore vu et qui est intimement lié à l'Active Directory. Il s'agit du service de certificats Active Directory (connu aussi sous le nom Active Directory Certificate Server ou AD CS).

Il vous permettra d'installer une autorité de certification sur votre réseau d'entreprise afin de pouvoir délivrer des certificats de façon aisée à vos utilisateurs et ordinateurs. Ces derniers pourront ainsi accéder à des sites Web via le protocole SSL sans nécessiter l'achat de certificats (souvent coûteux) auprès d'une autorité de certification publique.

L'avantage certain d'avoir une autorité de certification d'entreprise basée sur Windows Server 2008 tient au fait que le processus d'inscription et de renouvellement des certificats est grandement facilité par l'intégration de cette autorité dans l'Active Directory.

Il existe deux types d'autorité de certifications.

- **Autorité de certification d'entreprise** : nécessite que le serveur possédant le rôle AD CS soit intégré dans l'Active Directory et permet ainsi de profiter de nombreuses fonctionnalités supplémentaires (comme l'auto-enrôlement) et d'être administrée via les stratégies de groupe.

- **Autorité de certification autonome** : qui peut être installée aussi bien sur un serveur membre ou non mais qui ne profitera pas de fonctionnalités supplémentaires.

La mise en place de cette solution dépassant le cadre de ce livre, voici néanmoins quelques-unes des principales fonctionnalités désormais disponibles depuis Windows Server 2008 concernant ce rôle.

- L'inscription des certificats en passant par votre navigateur a été améliorée car elle repose sur un nouveau contrôle nommé CertEnroll.dll.

- Prise en charge du protocole NDES (*Network Device Enrollment Service*) afin de permettre aux périphériques réseaux (routeurs, commutateurs, etc.) d'obtenir des certificats X.509.

- Prise en charge du protocole OSCP (*Online Certificate Status Protocol*) afin d'améliorer la gestion des révocations des certificats.

- Le modèle de certificat en version 3 disponible dans les autorités de certificats d'entreprise prend désormais en charge la cryptographie nouvelle génération (CNG Suite-B).

- Une nouvelle console MMC nommée **PKIView** est désormais disponible afin d'administrer plus efficacement les certificats tout au long de leur cycle de vie.

Windows Server 2008 R2 apporte les fonctionnalités suivantes :

- L'auto-enrôlement est possible au travers d'une connexion HTTP (à condition d'avoir le niveau fonctionnel du

© ENI Editions - All rights reserved - adamo diarra

schéma Active Directory en 2008 R2).

L'un des avantages est notamment la possibilité de demander un certificat depuis une forêt différente de celle de l'autorité de certification. Il est même possible de publier le Web service correspondant sur un serveur en DMZ afin de délivrer des certificats à des utilisateurs Internet. Ce Web service sera le seul autorisé à dialoguer avec l'autorité de certifications se trouvant sur votre LAN. Notez cependant qu'une telle configuration n'est conseillée que pour renouveler des certifications déjà délivrées et non pour fournir des certificats aux clients connectés depuis Internet. Vous trouverez le Livre Blanc (en anglais) sur cette nouvelle fonctionnalité à cette adresse : http://download.microsoft.com/download/C/2/2/C229E624-36E4-4AD8-9D86-F564ED539A16/Windows%20Server%202008%20R2%20Certificate%20Enrollment%20Web%20Services.doc

Pré-requis : Autorité de certifications d'entreprise sous Windows Server 2003/2008 ou 2008 R2 et en version Entreprise ou Datacenter ; niveau fonctionnel de la forêt 2008 R2 et ordinateurs clients sous Windows 7.

- Consolidation des autorités de certifications au sein d'une entreprise possédant plusieurs forêts à relation bidirectionnelle.

  En effet, l'autorité de certification sous 2008 R2 supporte l'utilisation des "LDAP Referals" permettant de rediriger la requête vers le bon domaine de la bonne forêt.

  Pré-requis : Autorité de certifications d'entreprise sous Windows Server 2008 R2 Entreprise ou Datacenter ; niveau fonctionnel de la forêt 2003 et relations d'approbation inter-forêts bidirectionnelles

- Amélioration de l'autorité de certifications devant délivrer une grande quantité de certificats.

  Ceci est notamment valable pour les clients NAP reposant sur de l'IPSec. Les clients doivent en effet demander plusieurs certificats par jour.

  Si vous le souhaitez, vous pouvez donc ne pas sauvegarder l'enregistrement de ces certificats délivrés dans la base de l'autorité de certification. Cette étape de sauvegarde entraîne souvent une croissance exponentielle de la base de données entraînant un coût d'administration.

  Si vous choisissez de ne pas sauvegarder ces enregistrements de certificats dans la base, il ne vous sera pas possible de révoquer ces derniers. Ce risque est cependant acceptable dans la mesure où les certificats concernés ont une courte durée de vie.

  Pré-requis : Autorité de certifications d'entreprise sous Windows Server 2008 R2.

Vous venez de découvrir au travers de ce chapitre l'ensemble des solutions d'identité et d'accès proposées par Windows Server 2008 R2. Vous pouvez ainsi aborder au mieux les besoins en termes d'accès à des ressources aussi bien pour mettre en place une solution SSO (*Single Sign On* ou "identification unique") que pour contrôler la diffusion des fichiers de votre entreprise.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre aborde l'architecture distribuée (DFS) par la présentation de l'installation, de la configuration des racines, des liaisons, de la réplication DFS-R et des outils utilisables pour réaliser cela.

© ENI Editions - All rights reserved - adamo diarra

Description de DFS

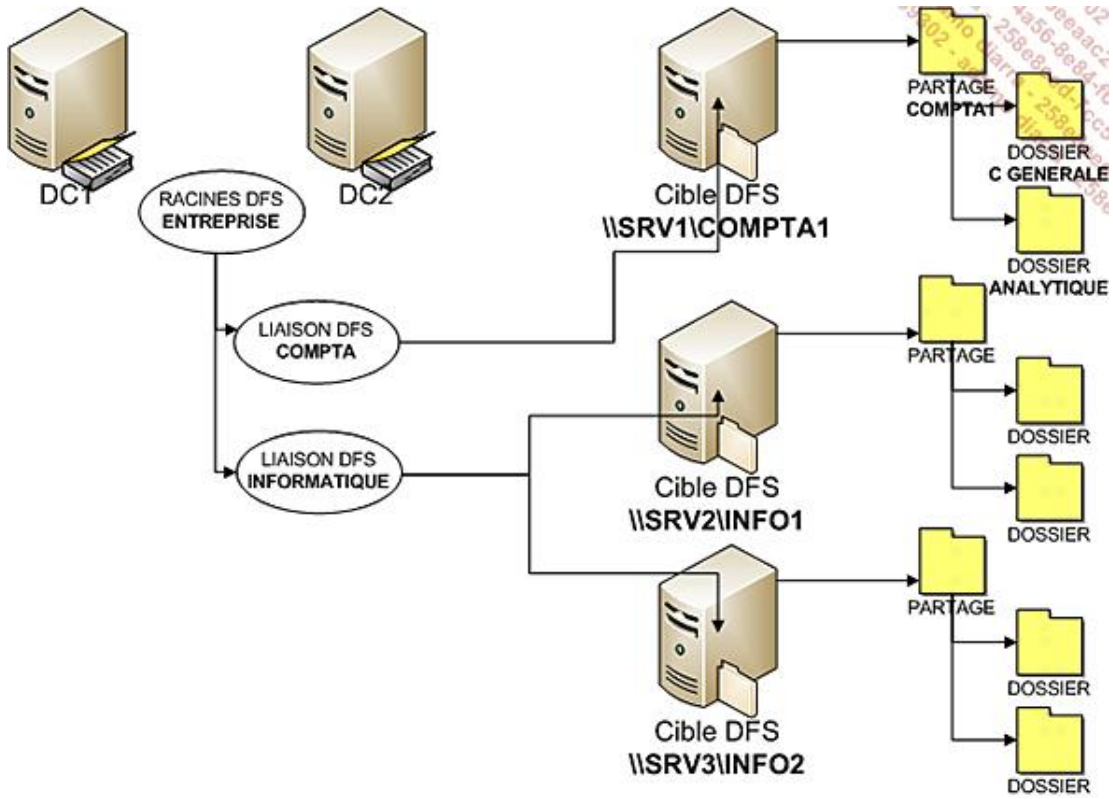
L'acronyme **DFS** signifie *Distributed File Systems*.

C'est un système de fichiers unique, logique, hiérarchisé, qui structure les fichiers partagés sur différents ordinateurs du réseau sous la forme d'une arborescence logique de ressources système. Le premier objectif de DFS est de référencer tous les partages que l'on veut rendre accessibles de manière uniforme et de centraliser tous les espaces disponibles sur les différents partages.

Ceci permet d'obtenir une vue uniforme et permanente des données qui ne seront plus liées aux serveurs physiques sur lesquels elles se trouvent. Outre l'économie d'unités réseaux, une seule lettre connectée permet d'atteindre tous les partages, les logiciels peuvent être configurés une fois pour toutes sur des chemins précis qui ne bougeront plus même si les données sont déplacées entre deux machines, notamment en cas d'évolution de la volumétrie nécessaire.

Une autre possibilité très intéressante consiste à pouvoir répliquer les données d'un même dossier sur plusieurs liens réseaux, c'est-à-dire sur plusieurs partages. Cette tolérance de pannes apporte une fonctionnalité assez proche d'un cluster de fichiers. Mais, il faut néanmoins bien étudier son mode opératoire pour éviter toute surprise.

Voici comment DFS organise les ressources résidantes sur différents composants d'un réseau :



L'arborescence DFS constituant un point unique de référence. Quel que soit leur emplacement, les utilisateurs peuvent accéder aisément aux ressources du réseau. Sur le réseau, les unités DFS sont vues comme des partages réseaux classiques et sont donc gérées par la fonction redirecteur de fichiers des clients réseaux classiques.

Un utilisateur naviguant dans un dossier partagé DFS n'a pas à connaître le nom ni la localisation du serveur sur lequel se trouve une ressource particulière. L'accès aux ressources réseau s'en trouve donc simplifié. Après s'être connecté à une racine DFS, il peut parcourir la structure et accéder à toutes les ressources situées sous cette racine. Un partage DFS utilise une structure d'arborescence contenant une racine et des liaisons DFS.

Pour démarrer l'utilisation de DFS, il faut tout d'abord créer une racine DFS. Depuis Windows 2003, il est possible de créer plusieurs racines. Chaque racine peut comporter plusieurs liaisons, chacune d'elle pointant vers un dossier partagé sur le réseau. Les liaisons DFS de la racine DFS représentent des dossiers partagés pouvant être physiquement localisés sur différents services de fichiers. Les avantages liés à DFS sont décrits ci-après :

Pour résumer, voici tous les avantages de cette solution :

- L'administration du réseau est simplifiée. En cas de défaillance d'un serveur, la liaison DFS peut être déplacée sur un autre serveur, en modifiant le dossier DFS pour indiquer le nouveau serveur d'hébergement des dossiers partagés. Le chemin reste le même pour les utilisateurs.

- L'espace de noms permet un accès à toutes les ressources par un nom unique, sans avoir à mapper de lettre

© ENI Editions - All rights reserved - adamo diarra

sur chaque ressource.

- DFS est intégré aux clients Windows et ne requiert pas d'agent ou de mémoire supplémentaire.

- Les serveurs de fichiers peuvent être remplacés sans affecter l'espace de noms utilisé par les clients.

- L'équilibrage et la tolérance de panne peuvent être obtenus sur les racines et sur les liaisons à protéger en indiquant plusieurs serveurs et partages sur chaque ressource. Différents cadres d'utilisation sont alors possibles.

- L'espace de noms peut être étendu dynamiquement pour inclure un espace disque complémentaire ou prendre en charge de nouveaux besoins.

- DFS utilise toutes les autorisations existantes. Aucune règle ou autorisation supplémentaire ne sont nécessaires pour les utilisateurs. Les listes de contrôle d'accès (ACL) situées sur des dossiers répliqués sont répliquées de la même manière que les données.

- Afin d'accélérer la recherche et le parcours de l'arborescence DFS, celle-ci est automatiquement mise en cache sur les clients lors de la première utilisation jusqu'à l'arrêt du client ou l'expiration du mot de passe.

© ENI Editions - All rights reserved - adamo diarra

L’installation

Contrairement aux anciennes versions, les modules DFS ne sont plus intégrés et démarrés automatiquement sur les serveurs Windows. La seule exception, mais de taille, se situe sur les contrôleurs de domaine qui utilisent la réplication DFS pour les dossiers de partages SYSVOL.

Le module `FS-DFS` est composé de deux sous-modules :

- `FS-DFS -namespace`
- `FS-DFS -Replication`

L’ensemble des modules peut être installé par script avec la commande suivante :

```
servermanagercmd -install FS-DFS
```

Les deux modules peuvent être utilisés séparément et répondre à des besoins différents. On peut très bien soit répliquer des dossiers, soit publier des espaces, mais l’idéal **consiste à utiliser les deux fonctions en même temps**.

1. Le module d’espace de noms

Comme dans Windows 2003, plusieurs espaces de nommages peuvent être créés. Ces espaces sont publiés dans Active Directory (AD).

L’installation du module d’espace de noms peut se faire par la commande :

```
servermanagercmd -install FS-DFS -namespace
```

2. Le module de réplication

Le module de réplication permet de créer des groupes de réplication de données. Une réplication doit contenir au moins deux partages provenant de deux serveurs différents.

L’installation du module de réplication peut se faire par la commande :

```
servermanagercmd -install FS-DFS-Replication
```

À noter que la réplication par les outils Microsoft n’est pas obligatoire. Il est possible d’utiliser les liaisons DFS pour pointer sur plusieurs partages. Mais, si l’on veut un contenu identique, celui-ci devra être placé de manière « explicite » par des outils ou des scripts adéquats.

3. La console d’administration

Si nécessaire, la console d’administration peut être installée séparément des deux autres modules dans les fonctionnalités.

La console d’administration se trouve dans la partie :

- Outils d’administration de serveur distants
- Outils d’administration des rôles
- Outils de services de fichiers
- Outils du système de fichiers DFS

L’installation peut aussi se faire par script :

© ENI Editions - All rights reserved - adamo diarra

```
Servermanagercmd -install RSAT-MGMT-DFS-con
```

Après lancement de la console, il suffira d'interroger AD pour obtenir la liste des racines DFS existantes.

4. Le cas des contrôleurs de domaine

Sur un contrôleur de domaine, les services d'espace de noms et de réplication sont installés automatiquement, mais AD gère directement ses propres dossiers partagés. Il n'est donc pas possible de voir ou de modifier à ce niveau la réplication utilisée par Active Directory pour répliquer le partage SYSVOL.

5. La cohabitation avec DFS 2003

Si l'on veut répliquer des données avec des racines DFS hébergées par Windows 2003 ou Windows 2000, il faudra installer un module spécifique de réplication basé sur l'ancien système de réplication de fichiers FRS. Ce module de réplication se trouve dans le rôle **services de fichiers** et sera installé par l'ajout du service de rôles **Service de réplication de fichiers**.

L'installation peut aussi se faire par script :

```
Servermanagercmd -install FS-Replication
```

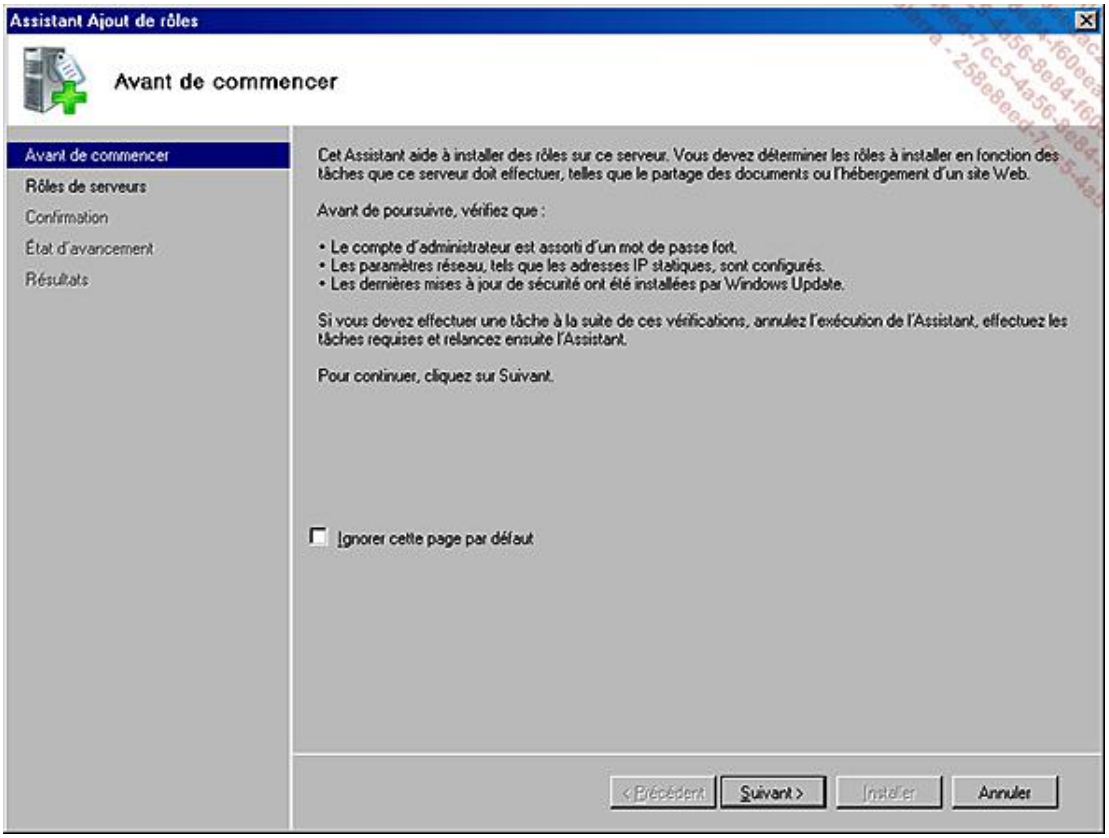
6. La procédure d'installation graphique

L'installation graphique permet d'ajouter tous les composants nécessaires en une seule opération. Celle-ci se fait à partir de l'outil **Gestionnaire de Serveur**, dans la ruche **Rôles**, en cliquant sur **Ajout des rôles**.

Voici les différentes étapes :

- Cliquez sur **Suivant**.

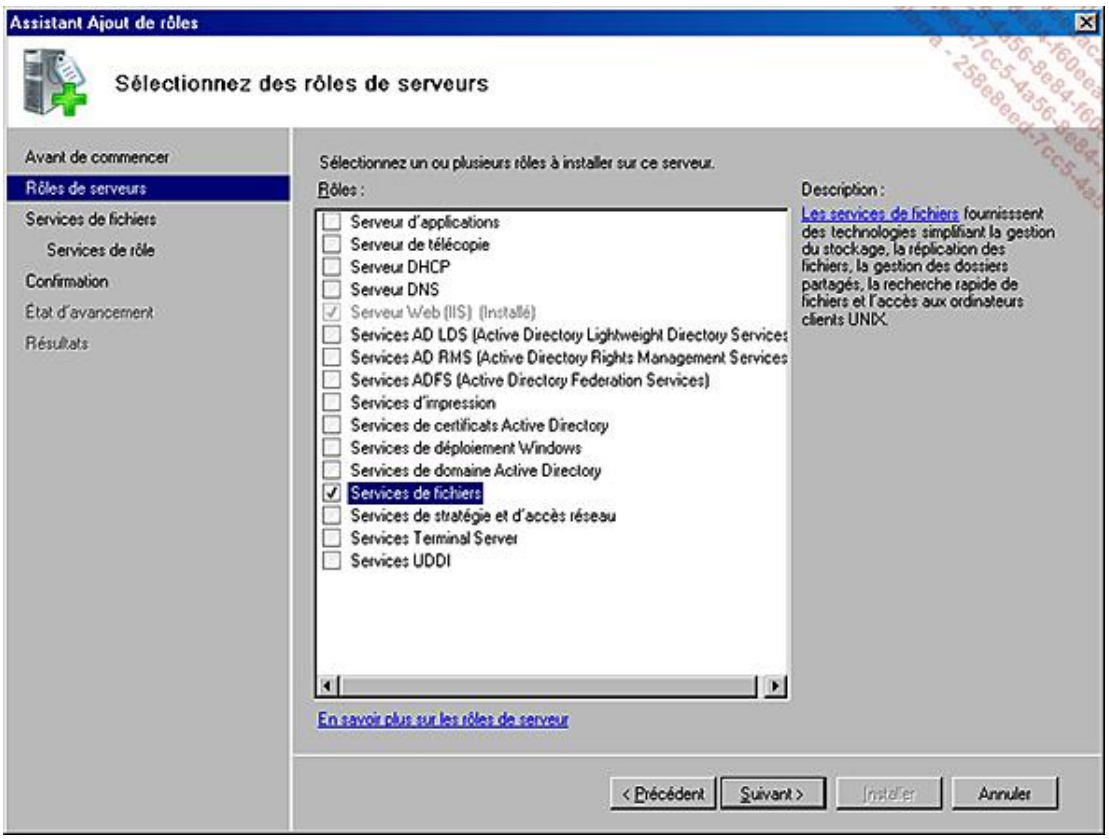
Cette étape peut ensuite être ignorée en cochant la case adéquate.



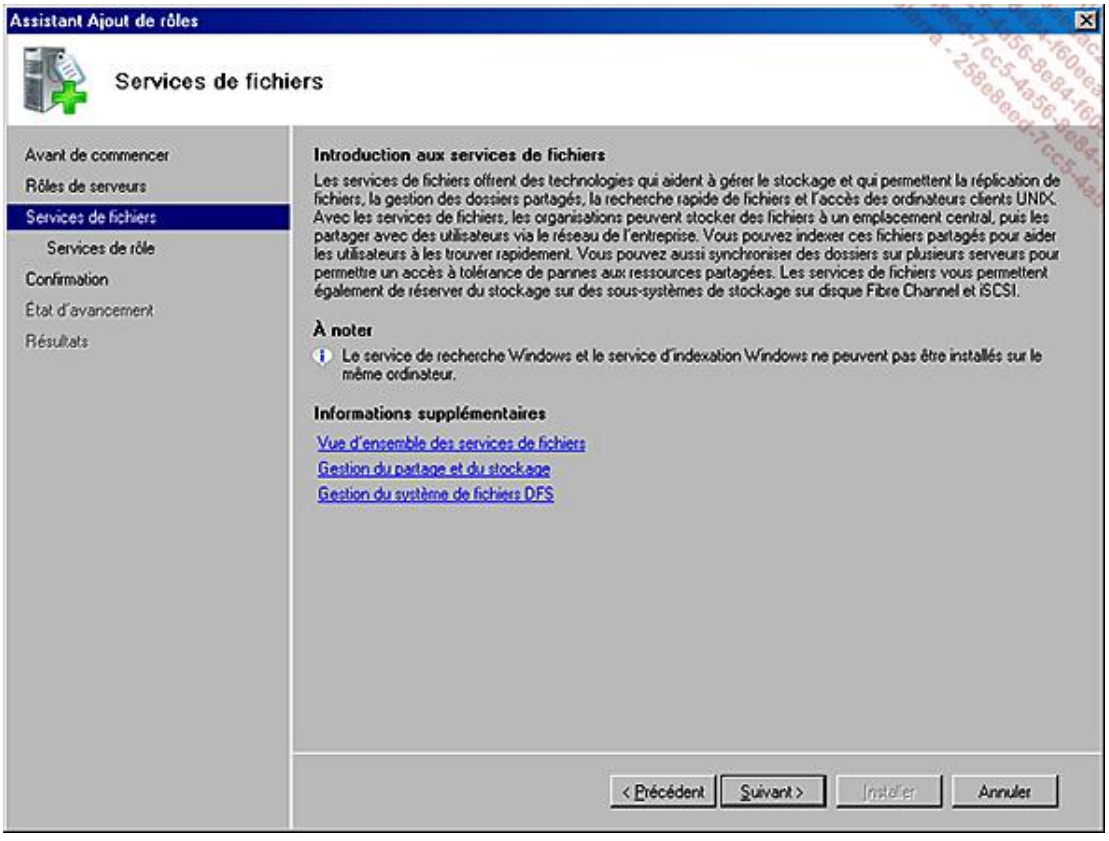
© ENI Editions - All rights reserved - adamo diarra

- Sélectionnez le rôle **Services de fichiers**.

  Les cases cochées et grisées indiquent les rôles qui sont déjà présents sur cette machine.



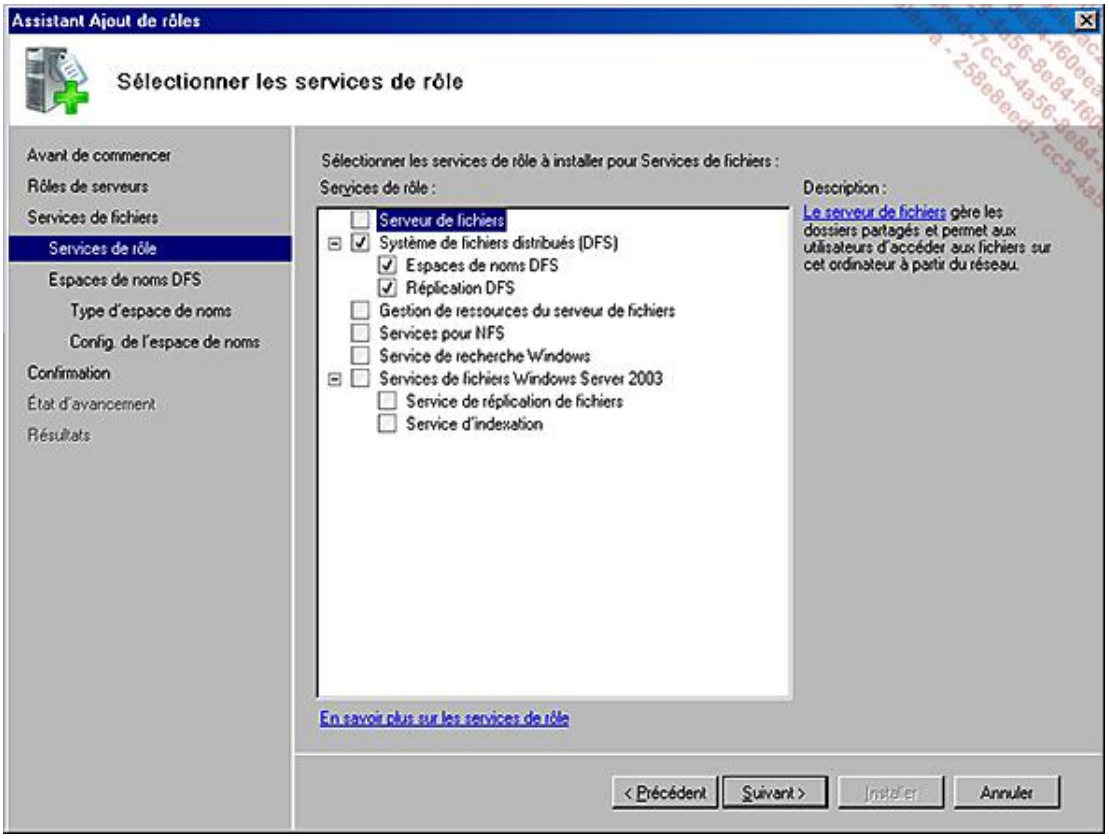
Cette page permet d'obtenir une aide précieuse lors des premières installations.



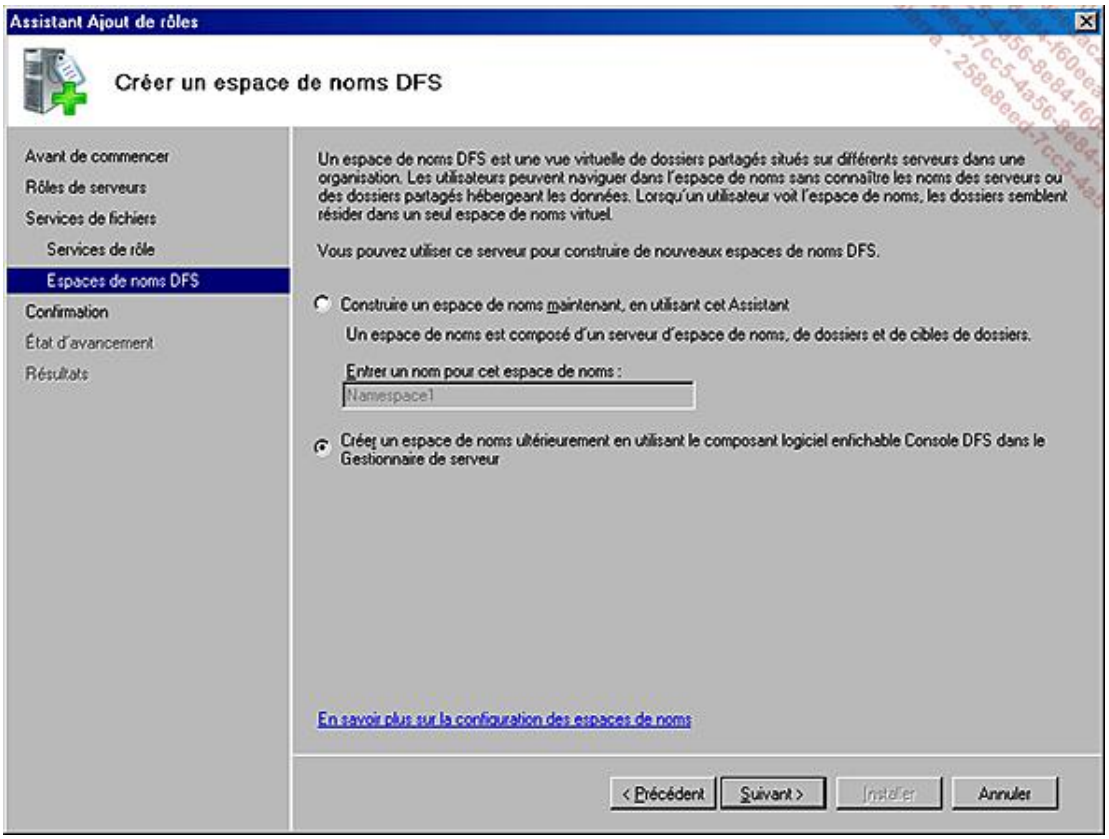
- Il suffit ensuite de sélectionner parmi les **Services de rôle** les composants souhaités.

© ENI Editions - All rights reserved - adamo diarra

À noter que le module **Service de réplication de fichiers** dans **Services de fichiers Windows Server 2003** devra être sélectionné s'il est nécessaire de répliquer vers des cibles DFS Windows 2003 ou 2000.

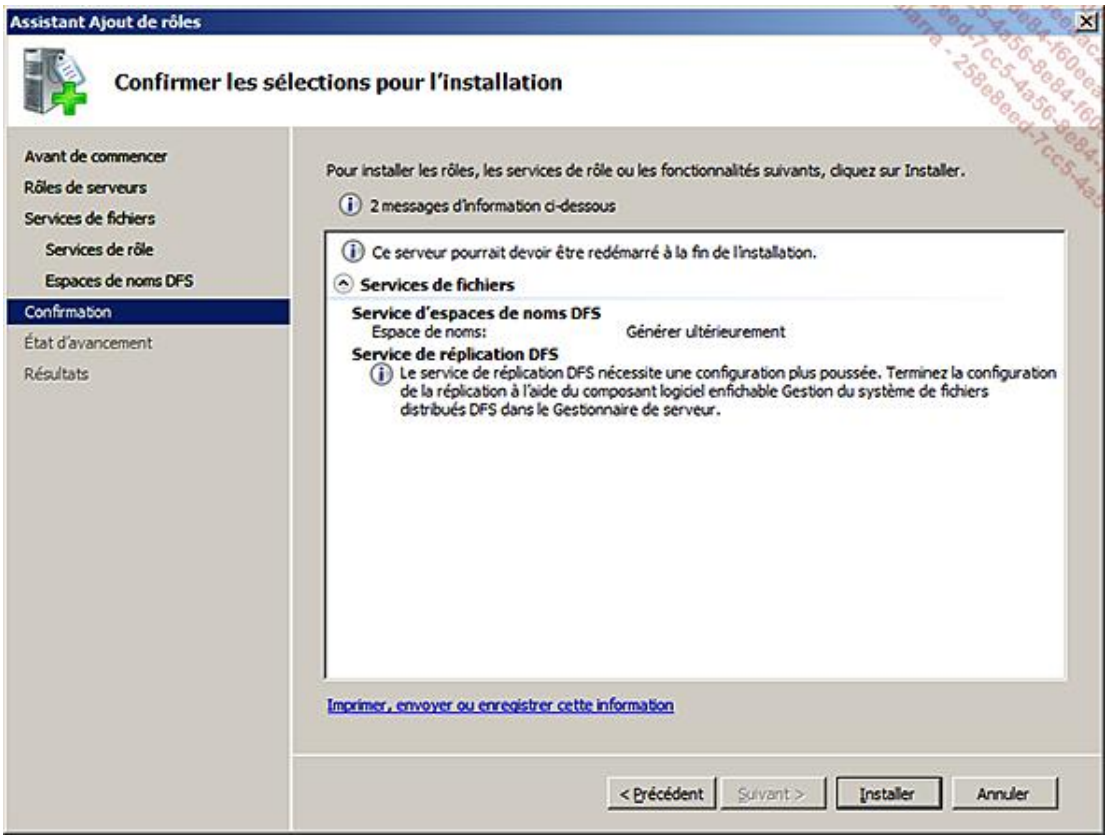


Il est possible de créer immédiatement un premier espace de noms, mais vous retrouverez cette opération plus tard.

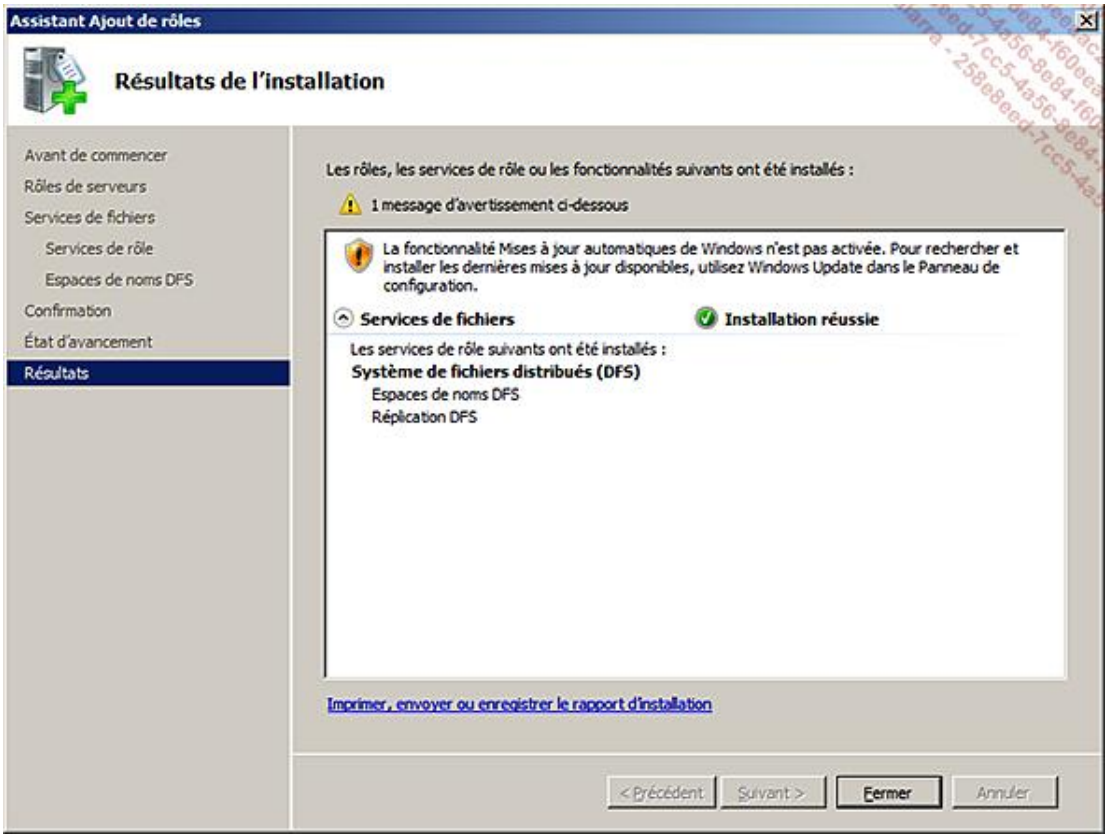


© ENI Editions - All rights reserved - adamo diarra

- Cliquez sur **Installer**.

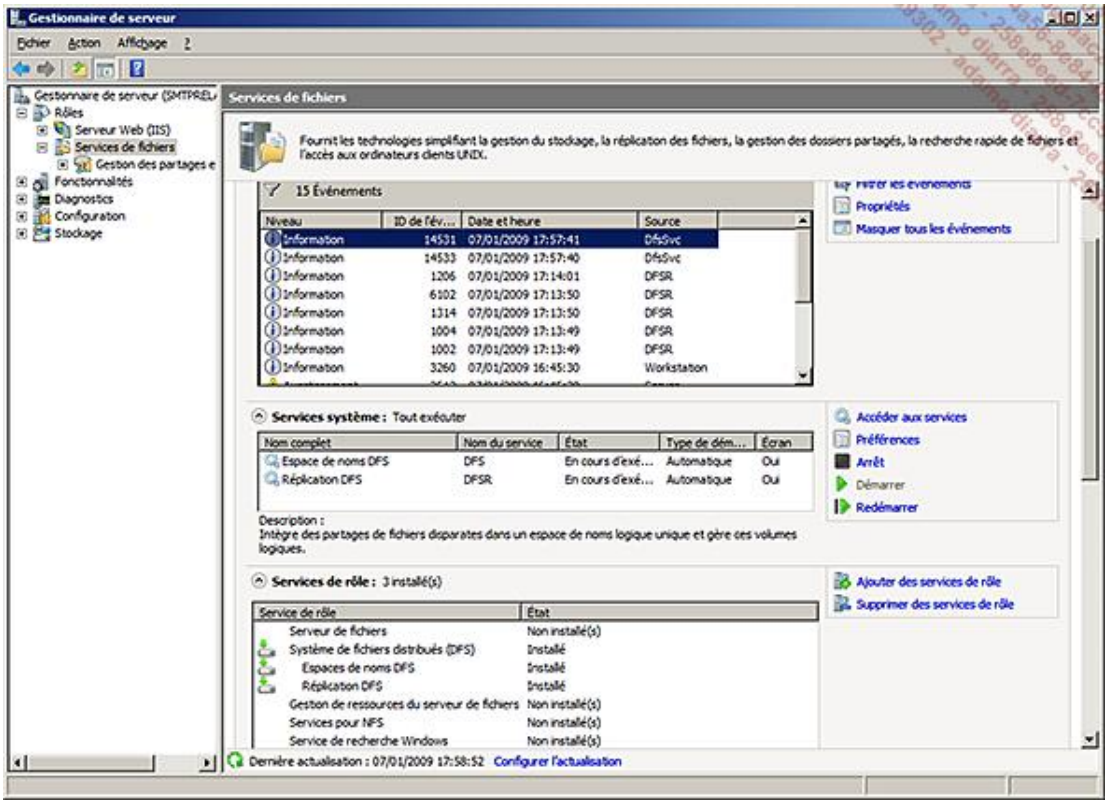


- Cliquez sur **Fermer**.



Après l'installation, les services sont démarrés automatiquement et apparaissent dans les services de rôles.

© ENI Editions - All rights reserved - adamo diarra



© ENI Editions - All rights reserved - adamo diarra

La configuration

1. Les différents types de racines distribuées

a. Les racines autonomes

Les racines autonomes permettent de créer des arborescences qui ne sont liées qu'à un serveur précis. Ces racines ne sont pas sécurisées, c'est-à-dire que la racine DFS ne sera plus ni accessible, ni utilisable si le serveur qui l'héberge ne fonctionne pas correctement. En revanche, les accès directs aux partages restent fonctionnels.

À noter que les dossiers (liens de partages) peuvent quand même être répliqués et synchronisés par un groupe de réplication spécifique.

Par ailleurs, si la racine autonome est configurée sur un cluster de fichiers, la racine DFS profitera de la même tolérance aux pannes que le partage de fichiers. Mais ceci ne sera possible que sur un cluster Windows 2008.

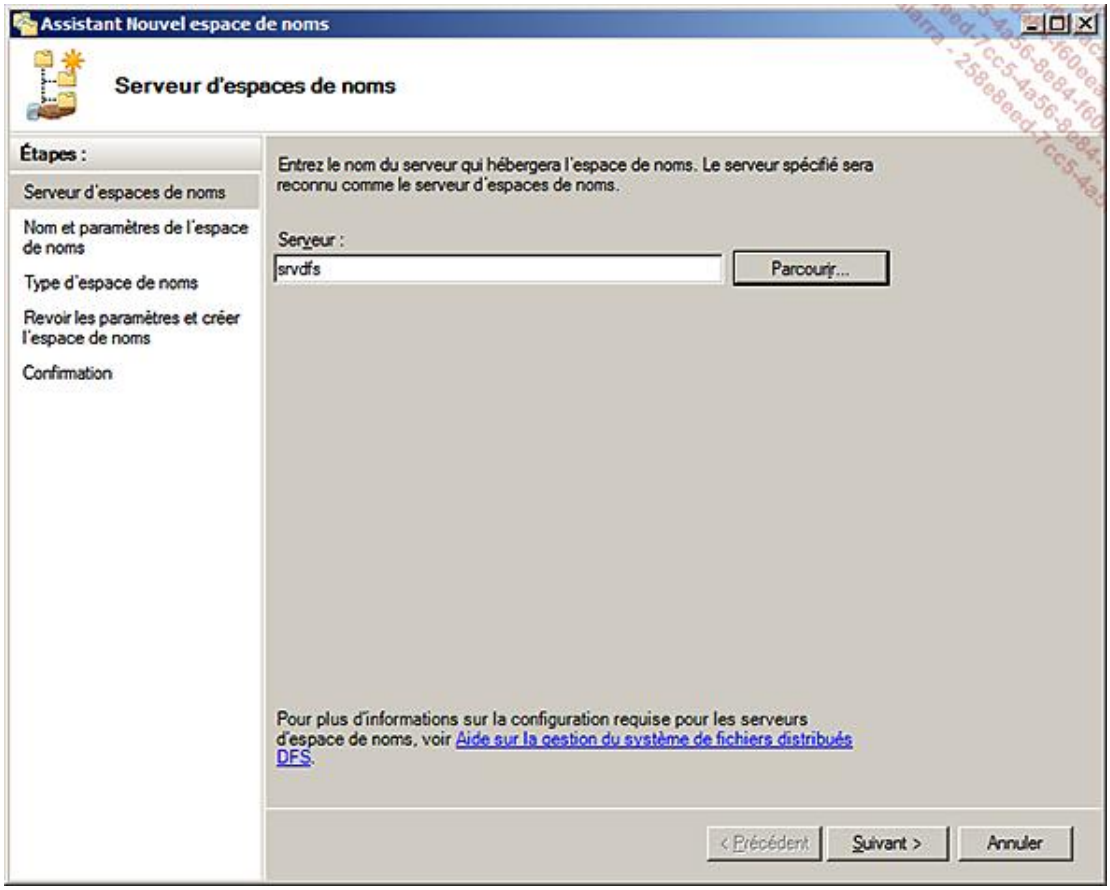
Voici la procédure de création d'une racine autonome.

En utilisant l'assistant de création d'un espace de nommage **Nouvel espace de noms**, ceci peut se mettre en place très rapidement.

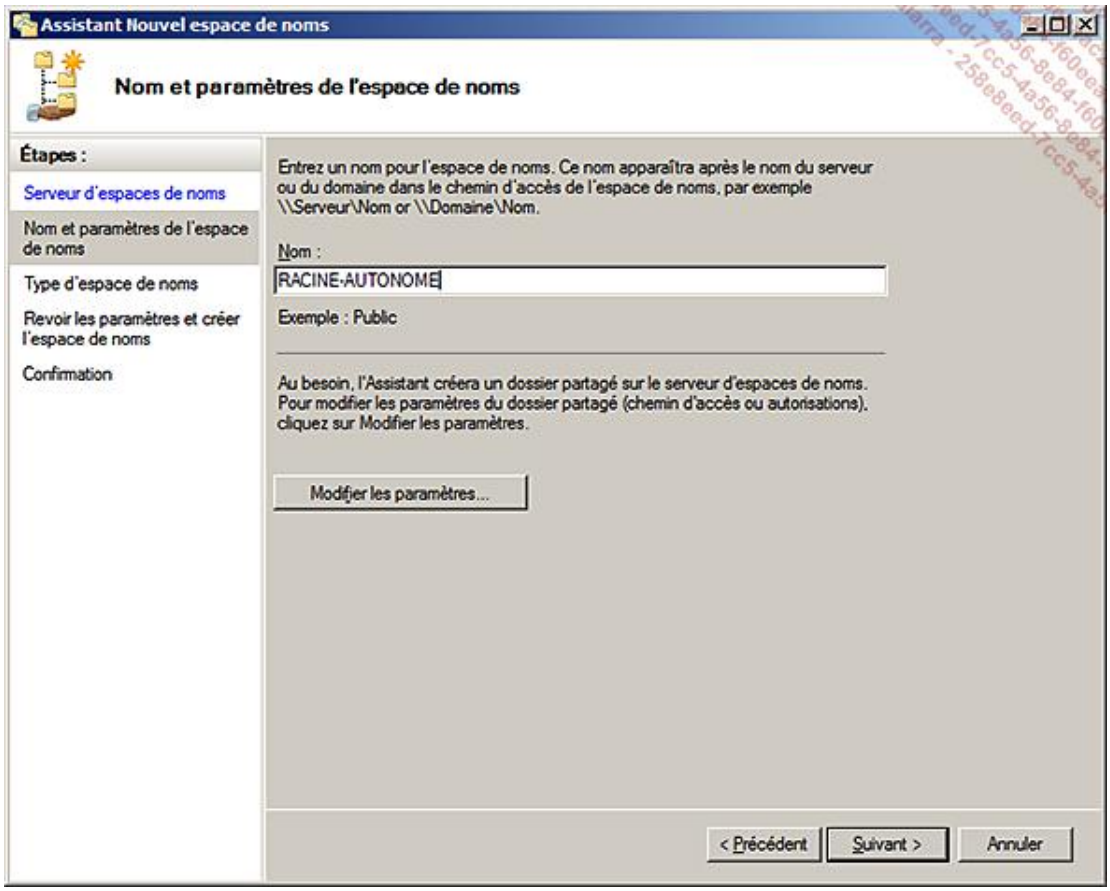
- Utilisez le bouton droit sur **Espaces de noms** pour faire apparaître le menu.

Les serveurs d'espaces de noms n'ont pas vocation à recevoir directement des données. Ils ne contiennent normalement que des dossiers **virtuels** qui eux, pointent sur des données réelles. Ce sont souvent des serveurs contrôleurs de domaine qui sont choisis pour suivre ce type d'information.

© ENI Editions - All rights reserved - adamo diarra

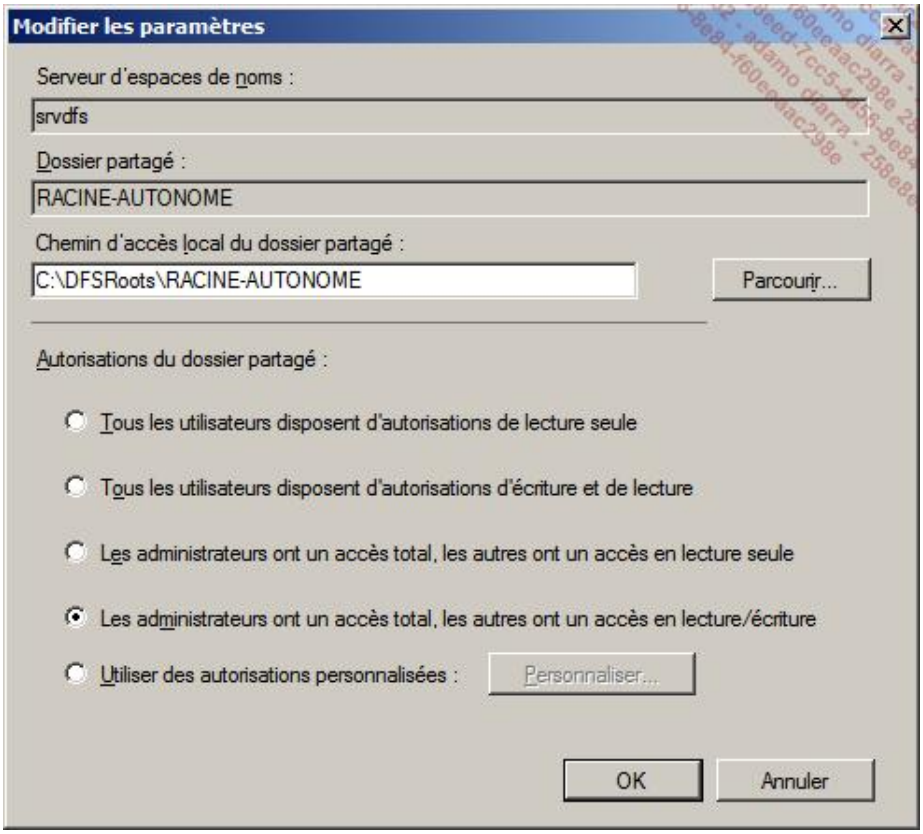


- Cliquez sur **Modifier les paramètres...** afin d'indiquer les permissions souhaitées sur la racine **RACINE-AUTONOME** qui sera vue comme un partage du serveur correspondant.

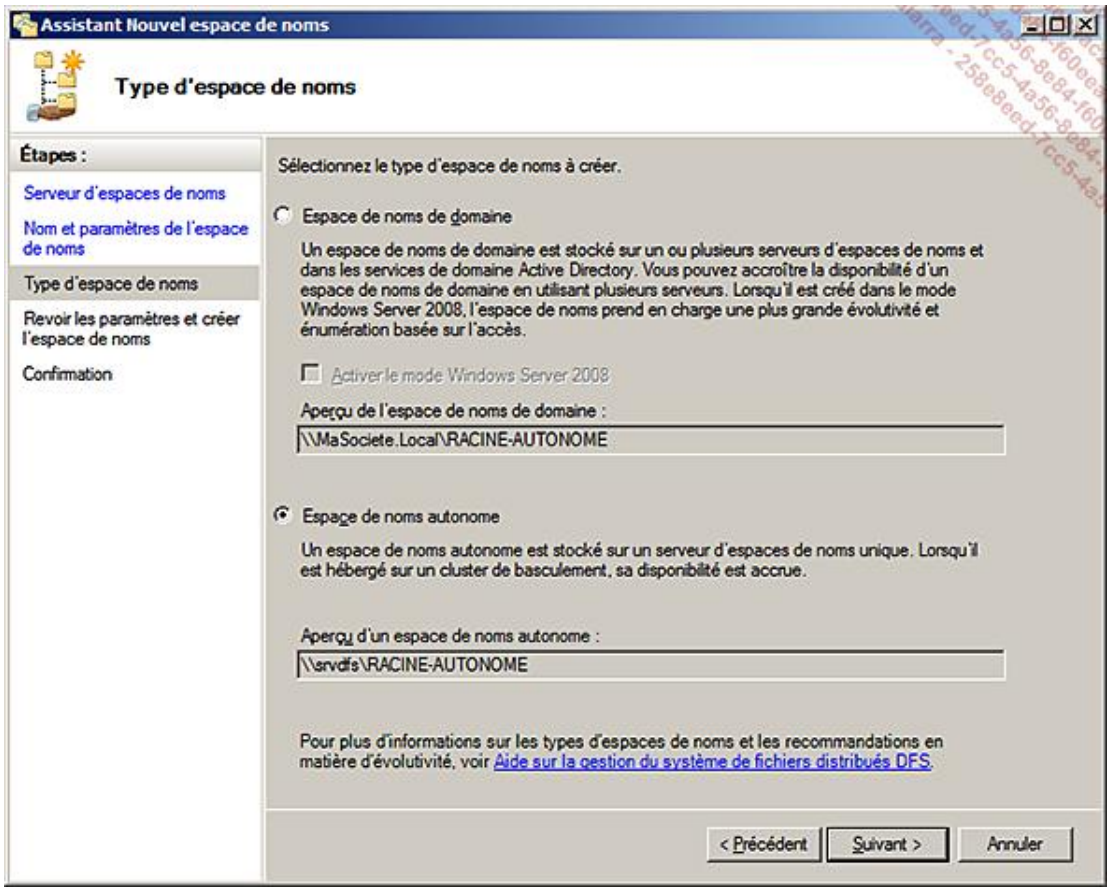


© ENI Editions - All rights reserved - adamo diarra

Il faut faire attention aux droits positionnés à ce niveau, car les éléments créés à la racine de ce partage se retrouveront effectivement dans le dossier local indiqué.



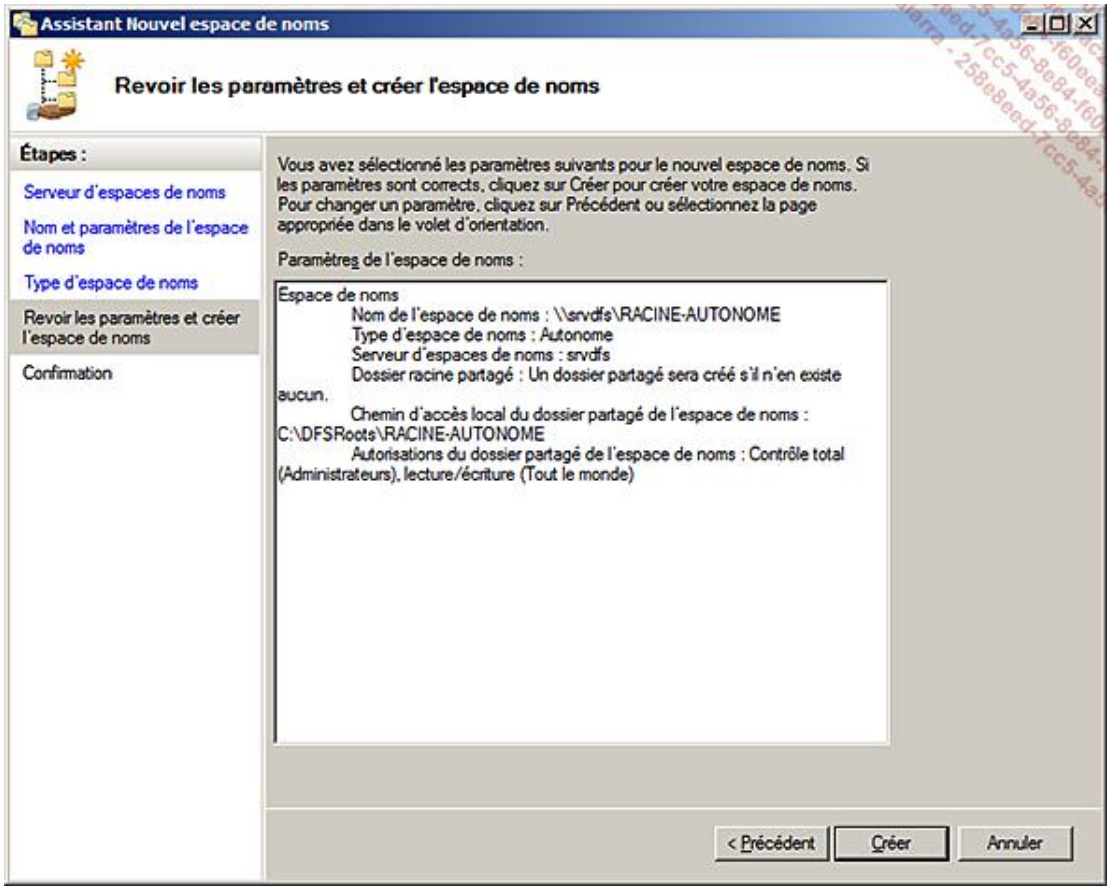
Le type d'espace correspond au choix crucial entre une racine qui sera spécifique à ce serveur, et une racine dite **de noms de domaine** qui pourra être vue et utilisée par toute la forêt. La racine **autonome** ne pourra être vue qu'à partir du serveur qui l'héberge.



© ENI Editions - All rights reserved - adamo diarra

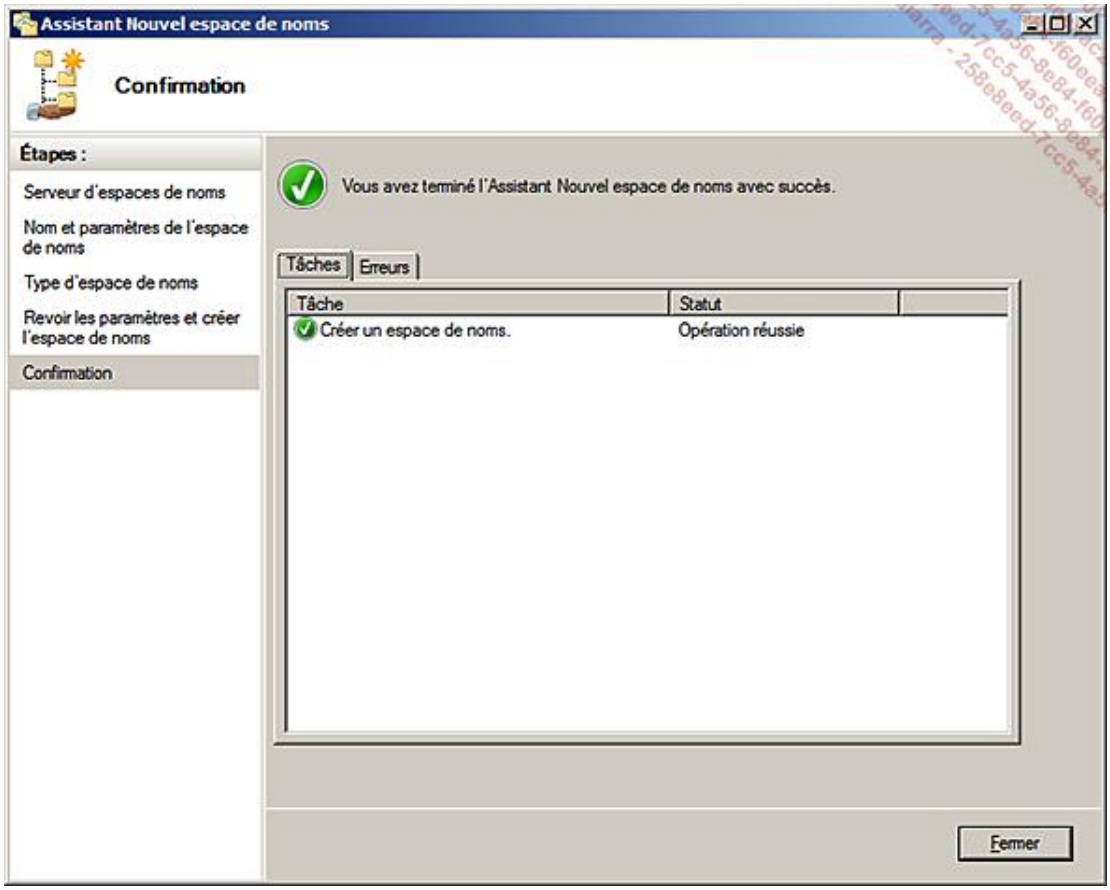
Cet écran reprend tous les choix réalisés.

- Cliquez sur le bouton **Créer**.



Cet écran confirme la création de la racine DFS. L'onglet **Erreurs** donne accès aux erreurs éventuelles. Les journaux d'évènements donneront des informations complémentaires.

© ENI Editions - All rights reserved - adamo diarra



b. Les racines de noms de domaine

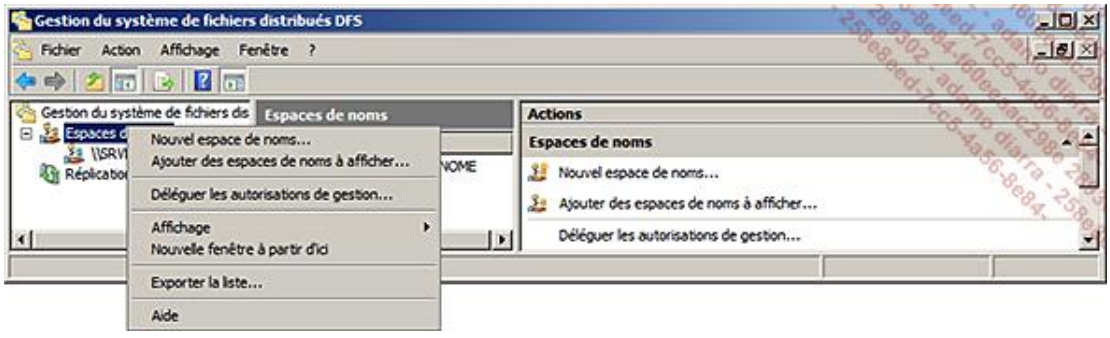
Les racines de noms de domaine sont basées sur la résolution DNS du domaine. L'avantage principal de cette solution réside dans la tolérance de panne qui peut être apportée à la racine par l'utilisation d'au moins deux serveurs liés au niveau de la même racine.

Les racines sont inscrites dans l'Active Directory, ce qui permet aux administrateurs et aux utilisateurs de toute la forêt d'accéder facilement aux unités DFS.

Voici la procédure de création d'une racine de noms de domaine.

Le début de la création est identique à la racine autonome.

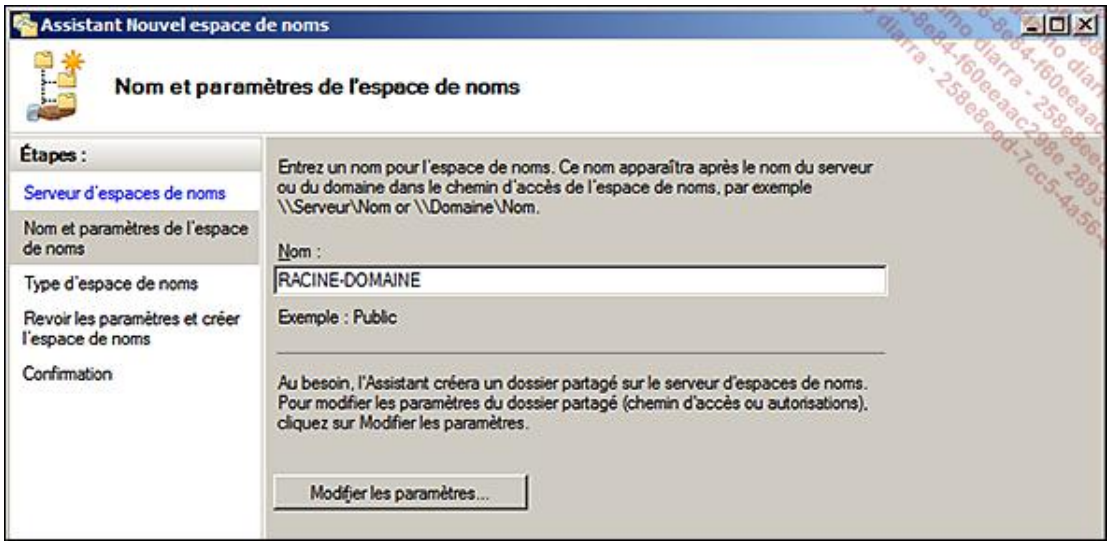
- Lancez l'assistant de création d'un **Nouvel espace de noms**.



- Indiquez le serveur qui gérera cette racine.

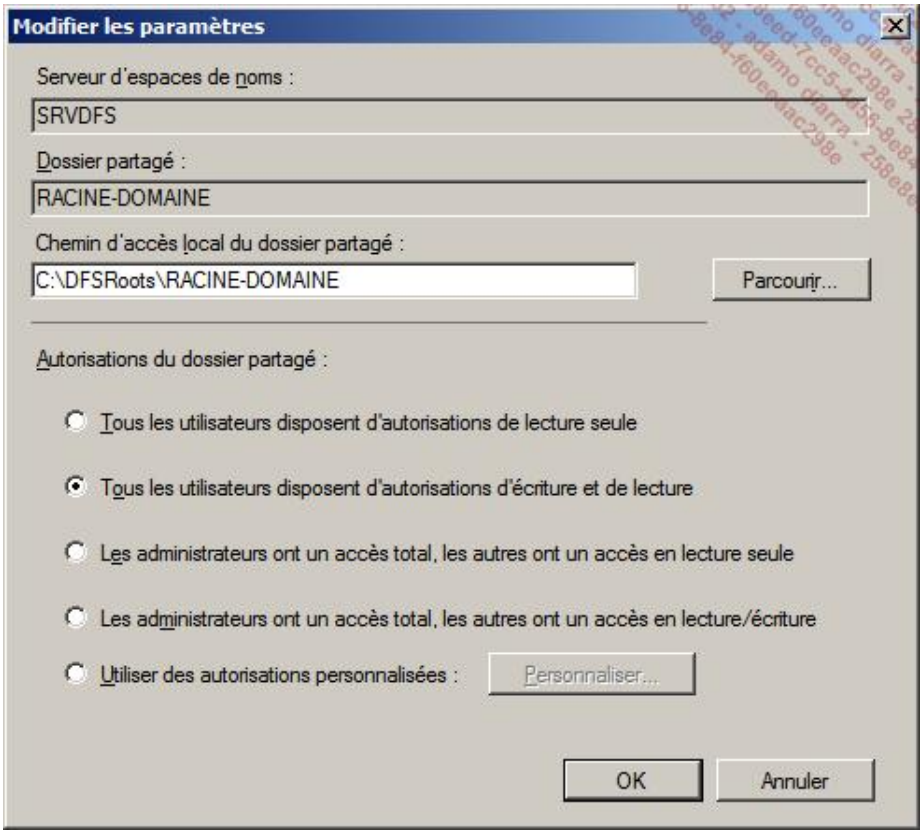
© ENI Editions - All rights reserved - adamo diarra

- Indiquez le **Nouvel espace de noms**, sachant que le nom devra être choisi judicieusement car il sera vu et utilisé par tous les utilisateurs de la forêt, voire plus.

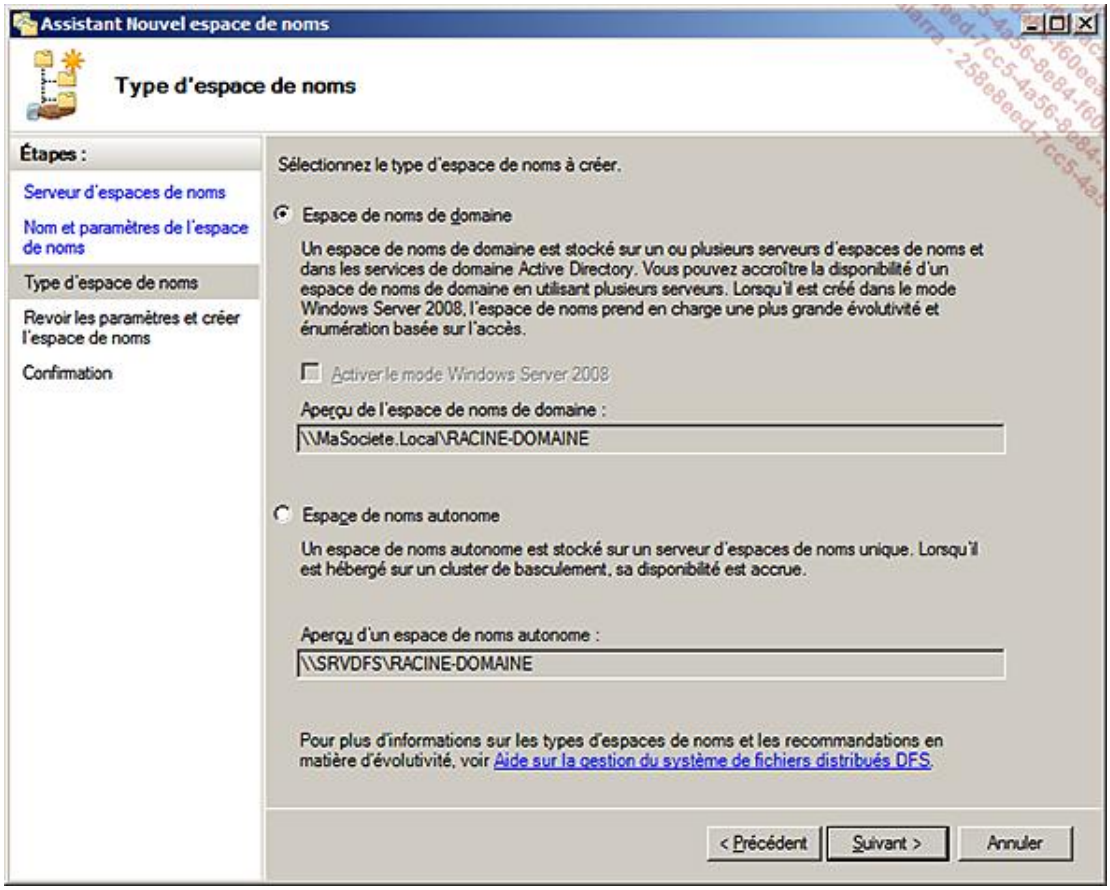


On retrouve le paramètrage des autorisations sur la racine.

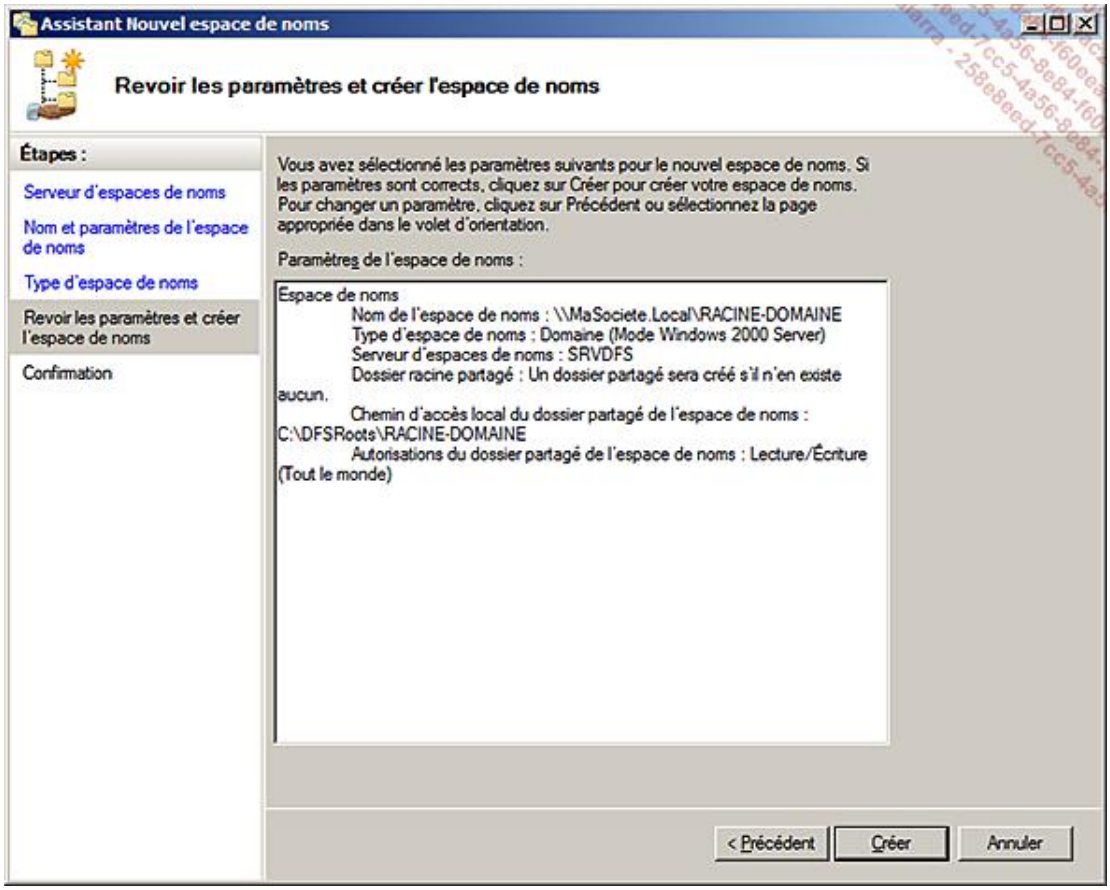
© ENI Editions - All rights reserved - adamo diarra



L'espace de noms de domaine permet de se baser sur la résolution du nom de domaine pour accéder à un espace partagé facile à trouver.



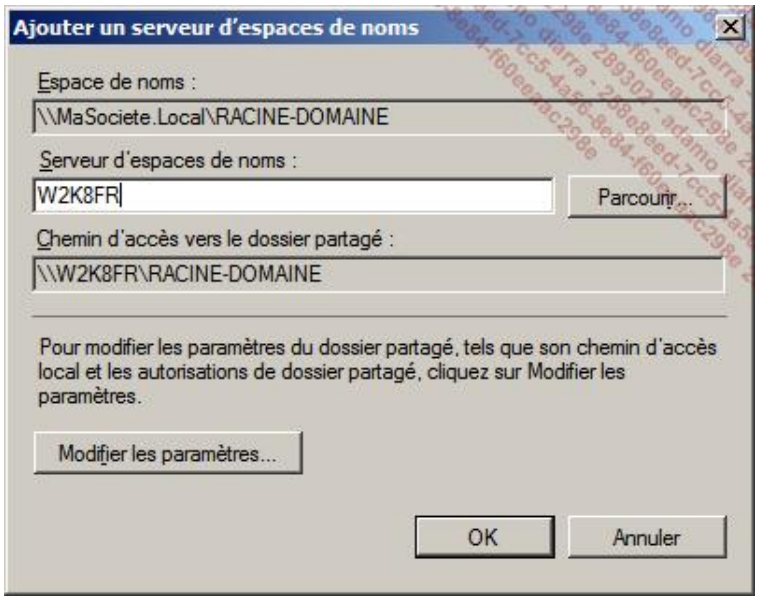
© ENI Editions - All rights reserved - adamo diarra



À noter que la création de la racine de domaine sera liée au mode de fonctionnement du domaine qui l'héberge.

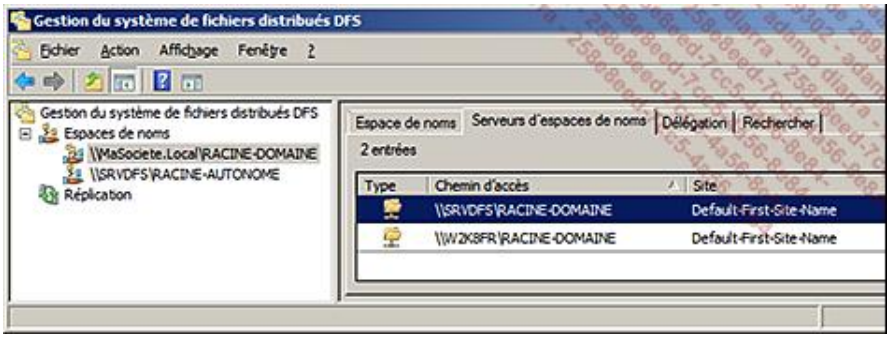
L'utilisation d'une racine de domaine suppose que l'on veut utiliser la tolérance aux pannes et l'équilibrage de charge sur la racine de DFS. Ceci est obtenu par l'ajout d'un serveur d'espace de noms supplémentaire.

Vous pouvez sélectionner ou saisir directement le nouveau nom du serveur à utiliser.



Bien entendu, il peut y avoir plus de deux serveurs contenant l'information sur les DFS.

© ENI Editions - All rights reserved - adamo diarra



2. La création des liaisons DFS et cibles DFS

Le nom d'une liaison correspond au nom de dossier qui apparaît dans l'espace de nom distribué. Une cible DFS correspond à un chemin réseau, c'est-à-dire un partage situé sur n'importe quel serveur (ou station du domaine) et que l'on associe à une liaison DFS.

Une liaison DFS peut être associée à plusieurs cibles, donc plusieurs partages différents. Il sera alors nécessaire de configurer la réplication de ces dossiers afin d'obtenir un contenu identique et synchronisé entre les différentes cibles.

Voici la procédure pour définir une cible sur les partages COMPTA1 et COMPTA2 définis sur deux serveurs différents :

- Sélectionnez l'espace de noms souhaité (Autonome ou de domaine), puis utilisez le clic droit pour afficher le menu.
- Utilisez l'option **Nouveau Dossier**.
- Saisissez le nom de la liaison DFS **COMPTA**.
- Cliquez sur **Ajouter** pour ajouter les cibles associées à cette liaison.
- Vous pouvez saisir directement le nom UNC d'accès à la ressource sous la forme \\SERVEUR\PARTAGE ou cliquer sur **Parcourir**.

  Dans le deuxième cas, l'astuce est d'indiquer le nom du serveur, puis de cliquer sur le bouton **Afficher les dossiers partagés**.
- Si plusieurs cibles sont précisées, l'assistant vous propose de créer un groupe de réplication. L'assistant de création d'un groupe de réplication est alors lancé automatiquement.

La procédure de mise en place d'une réplication est décrite dans la section suivante.

---

3. La réplication

La réplication est basée sur un moteur multimaître qui permet donc de prendre en compte les modifications simultanées de fichiers provenant de plusieurs points différents et de synchroniser l'ensemble. Cette réplication s'adapte aux liaisons lentes par l'utilisation d'une technologie de compression différentielle appelée **RDC**.

Chaque groupe de réplication (ensemble de serveurs) peut prendre en charge plusieurs dossiers répliqués.

Chaque dossier répliqué peut avoir ses propres paramètres, notamment des filtres de réplication permettant de limiter les types de fichiers et les sous-dossiers à inclure dans la réplication.

a. Les filtres de réplication

Par défaut, les filtres de fichiers excluent les fichiers temporaires commençant par le caractère ~ ainsi que les extensions .BAK et .TMP.

Par ailleurs, les fichiers suivants sont toujours exclus :

© ENI Editions - All rights reserved - adamo diarra

- les points de montages NTFS ;
- les fichiers chiffrés par EFS ;
- les fichiers définis comme temporaires.

Les dossiers comme les fichiers peuvent être exclus en fonction de leurs noms. Il est possible d'utiliser le caractère générique *.

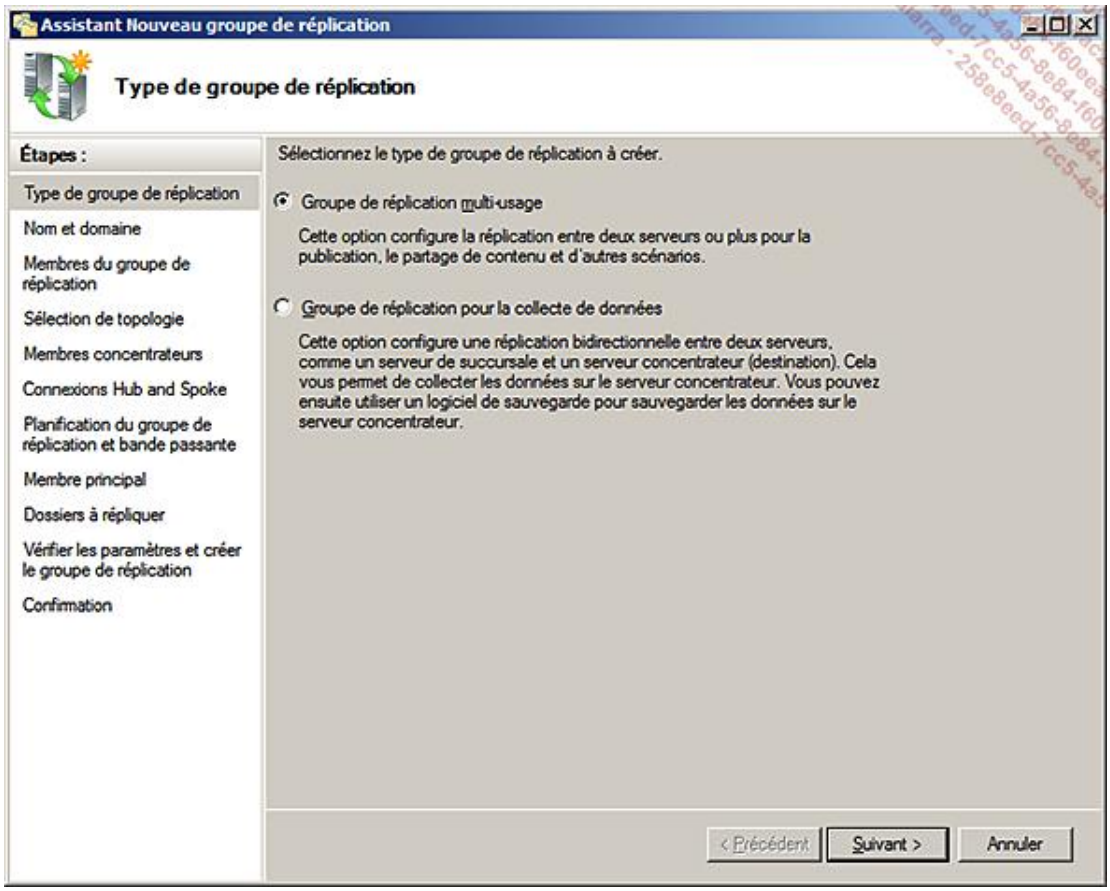
Les bases de données, les fichiers vidéo et les images de CD peuvent ainsi être exclus de cette réplication.

b. La mise en place graphique de la réplication

Voici la procédure graphique de mise en place d'une réplication.

Cette réplication se met en place de la même manière sur une racine autonome ou de domaine.

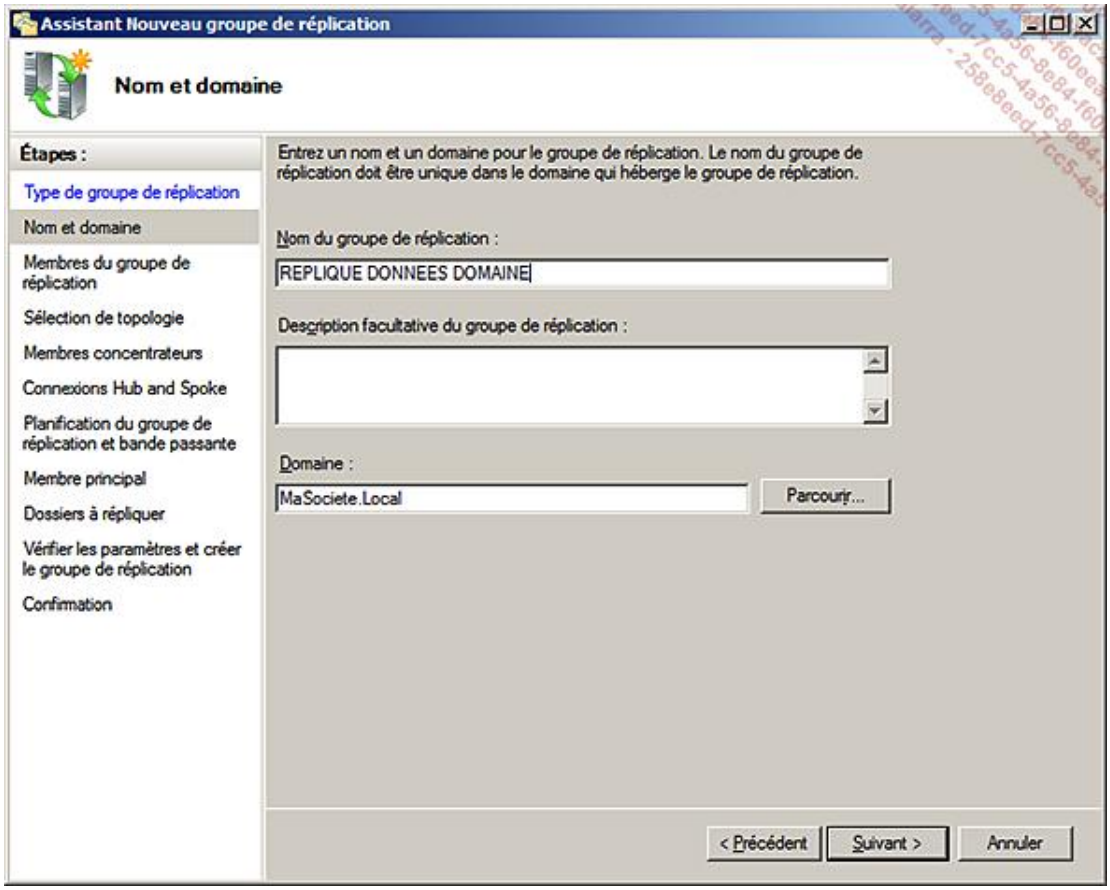
- Sélectionnez le module **Réplication**, puis cliquez avec le bouton droit pour faire apparaître le menu. Choisissez l'option **Nouveau groupe de réplication**.



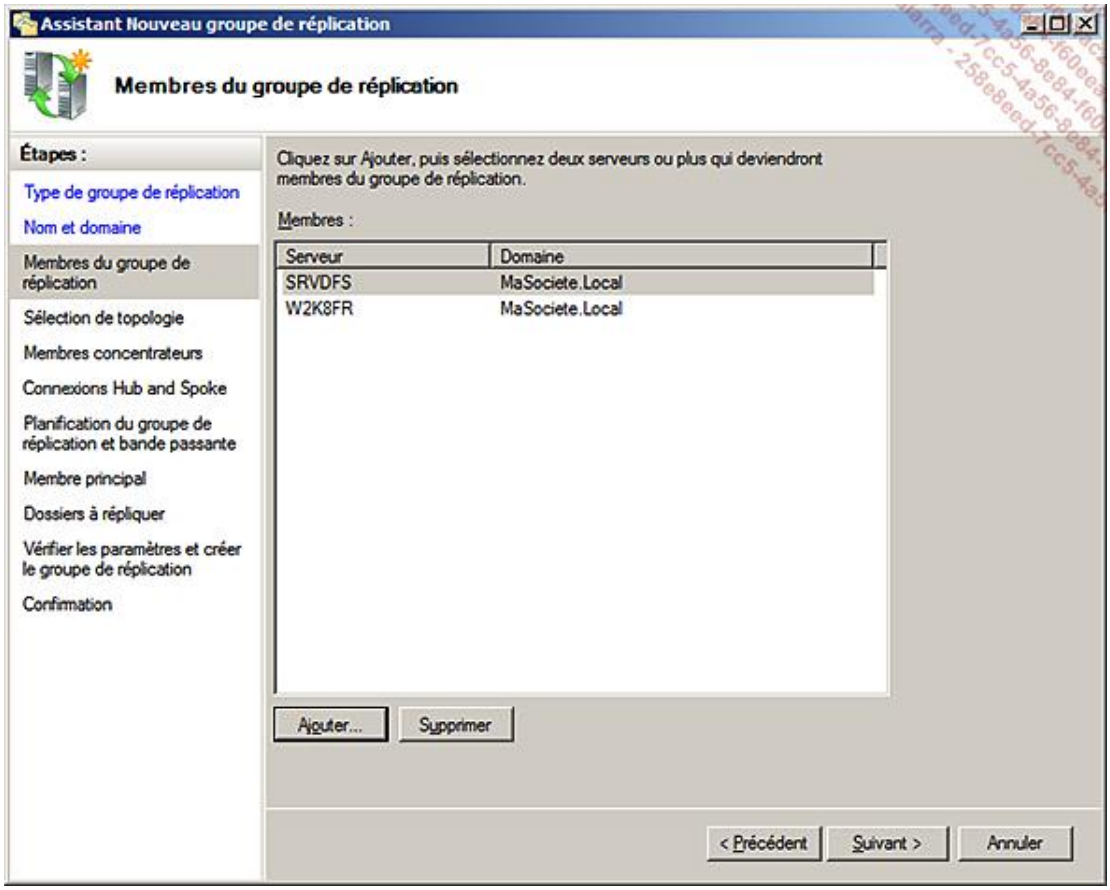
Ce choix permet principalement de définir si la réplication sera liée uniquement à deux serveurs, dont l'un contiendra les données principales.

- Nommez la réplication.

© ENI Editions - All rights reserved - adamo diarra

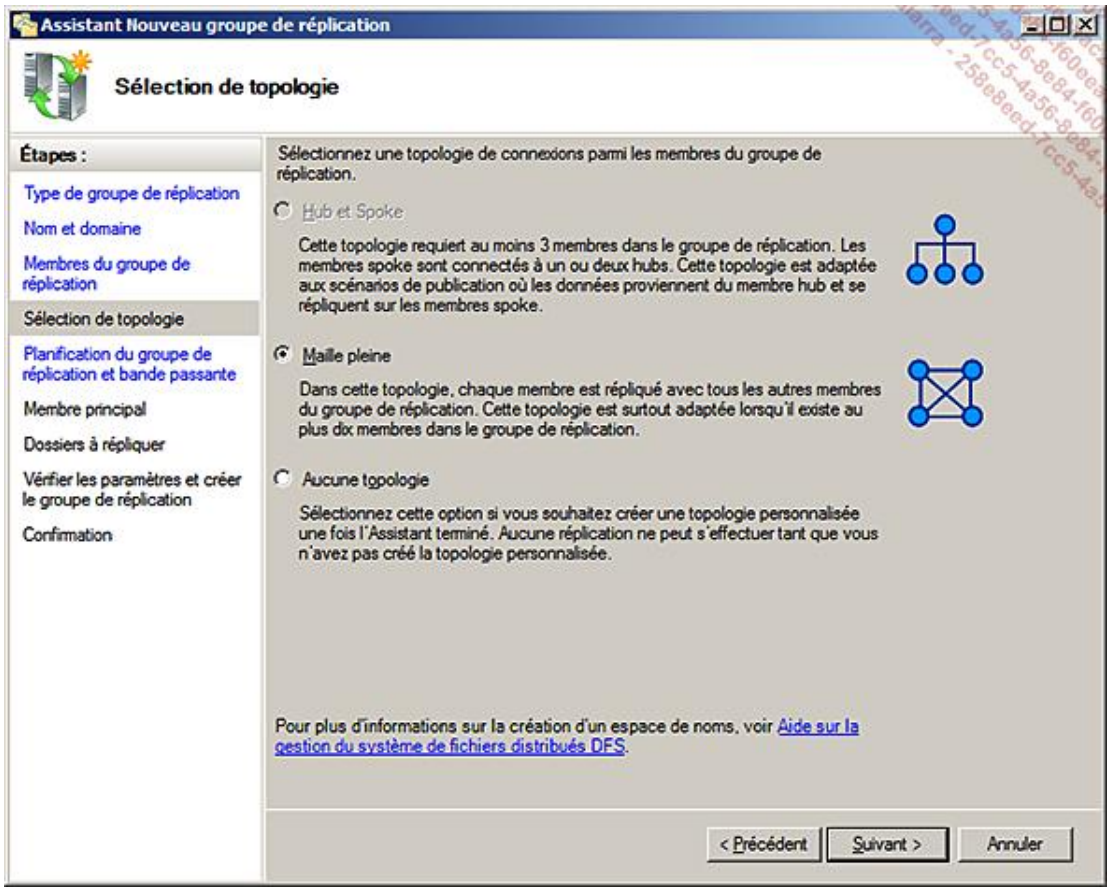


- Indiquez les serveurs membres.

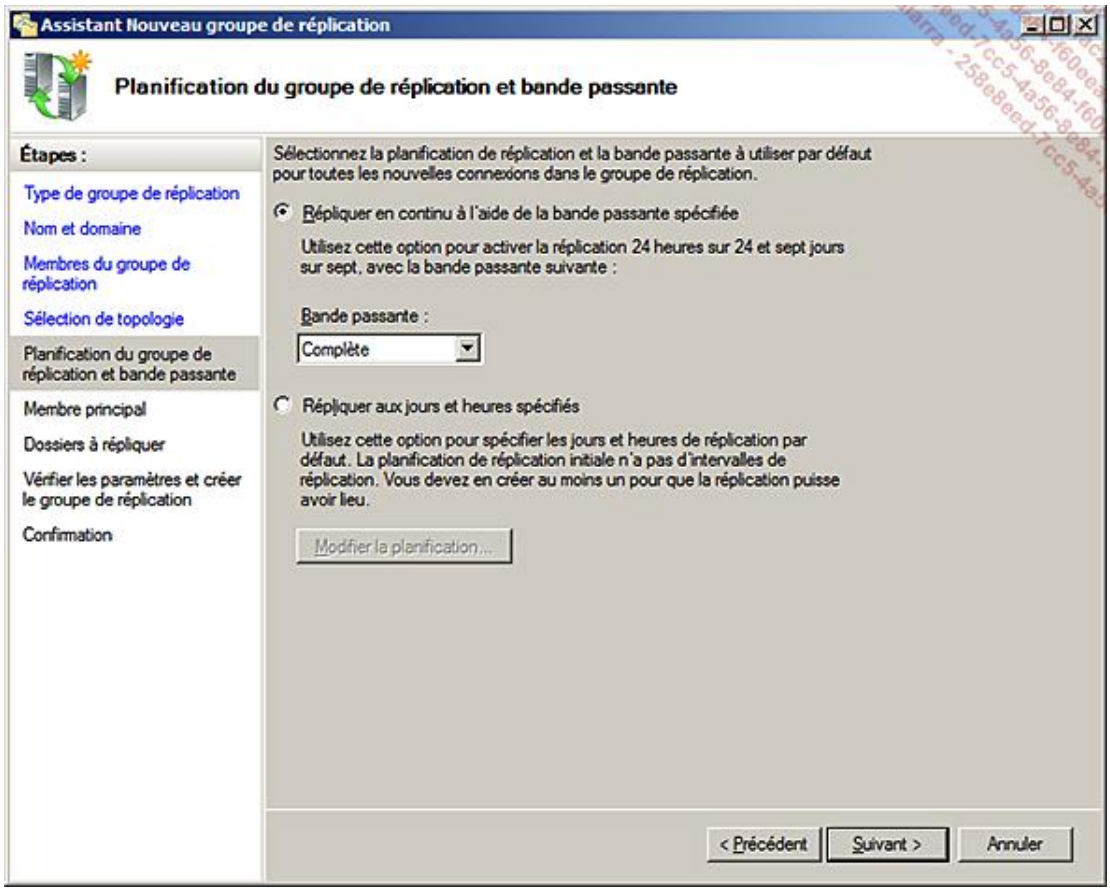


© ENI Editions - All rights reserved - adamo diarra

- Choisissez la topologie la plus adaptée à vos besoins. La topologie en maille pleine est adaptée aux modifications autorisées provenant de tous les serveurs membres.



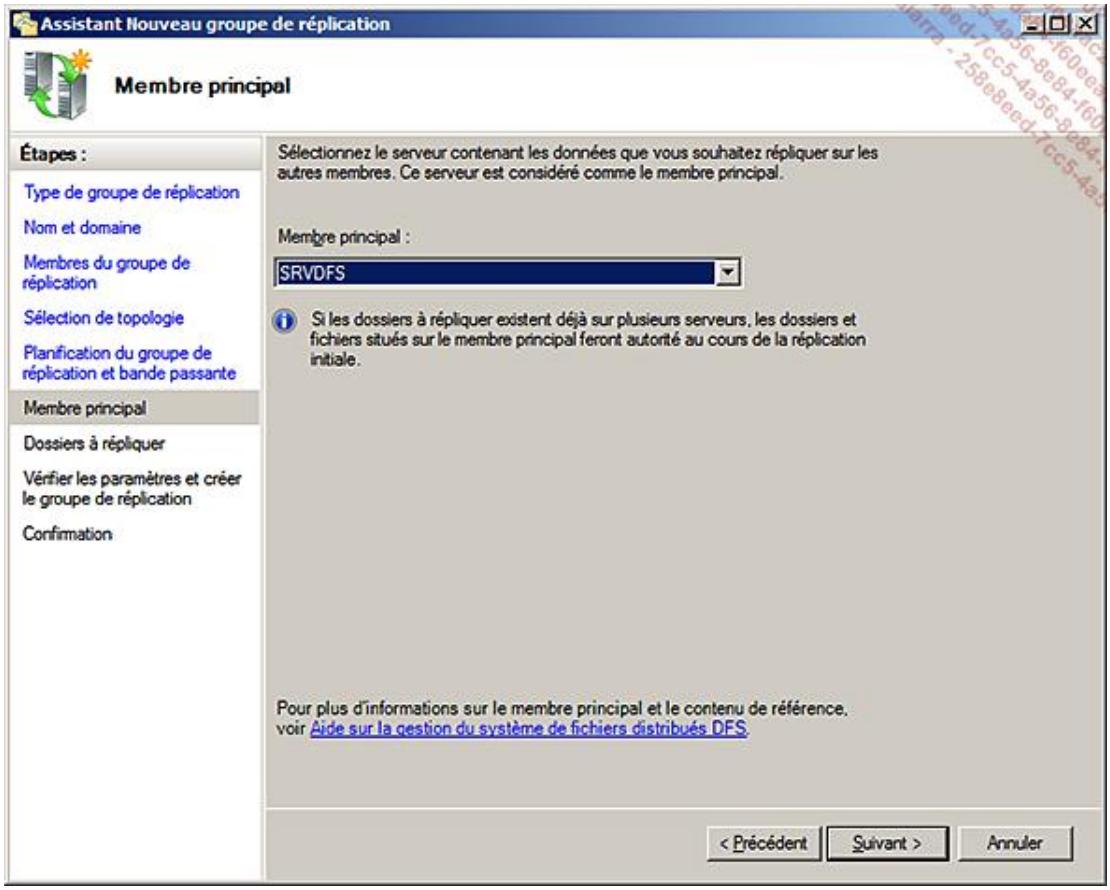
Selon les possibilités de votre réseau, il sera possible de moduler les horaires et le taux d'utilisation du réseau.



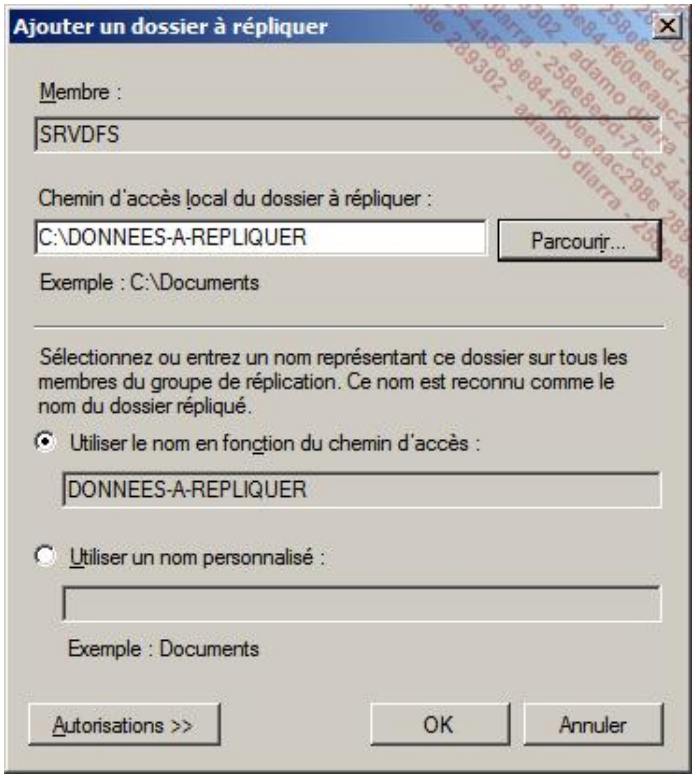
© ENI Editions - All rights reserved - adamo diarra

Vous pourrez modifier facilement les paramètres de réplication par la suite.

Il est préférable de démarrer les réplications sur des dossiers vides. Sinon, cette option permet de définir le serveur contenant les données initiales.

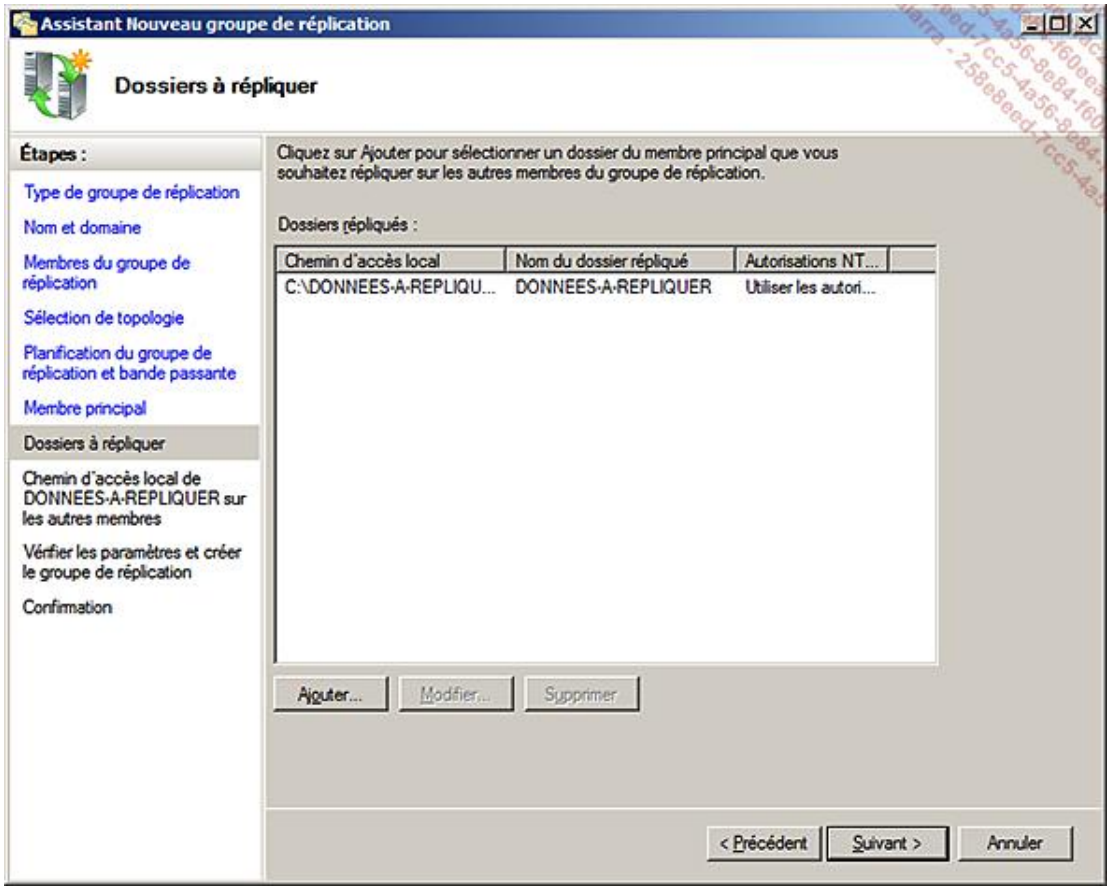


- Indiquez le nom exact du dossier racine à répliquer.



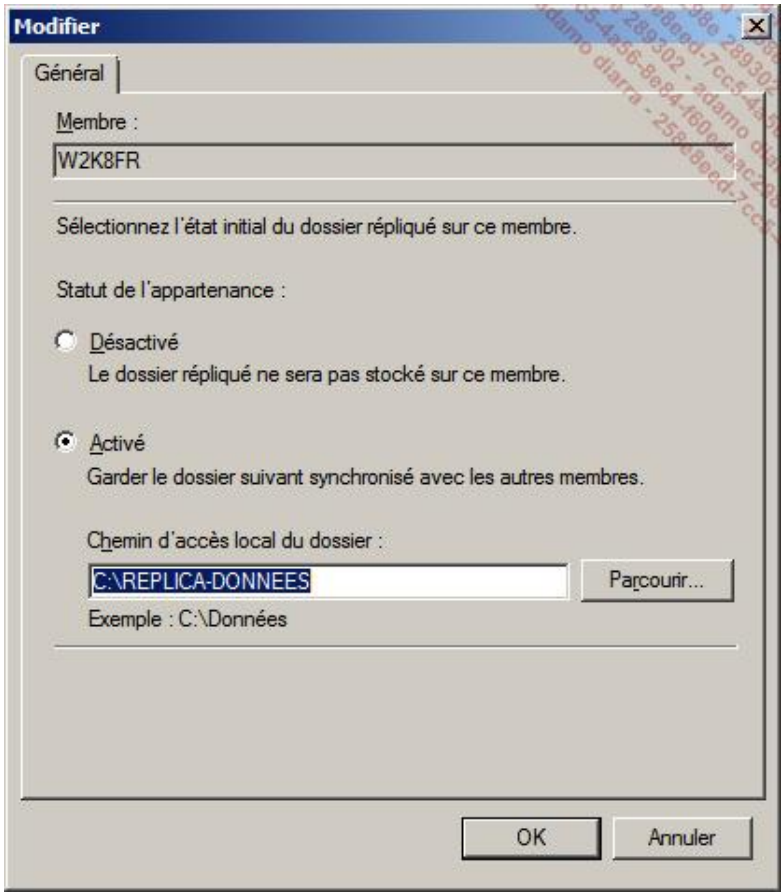
© ENI Editions - All rights reserved - adamo diarra

D’autres dossiers peuvent être ajoutés à ce groupe de réplication immédiatement ou par la suite !

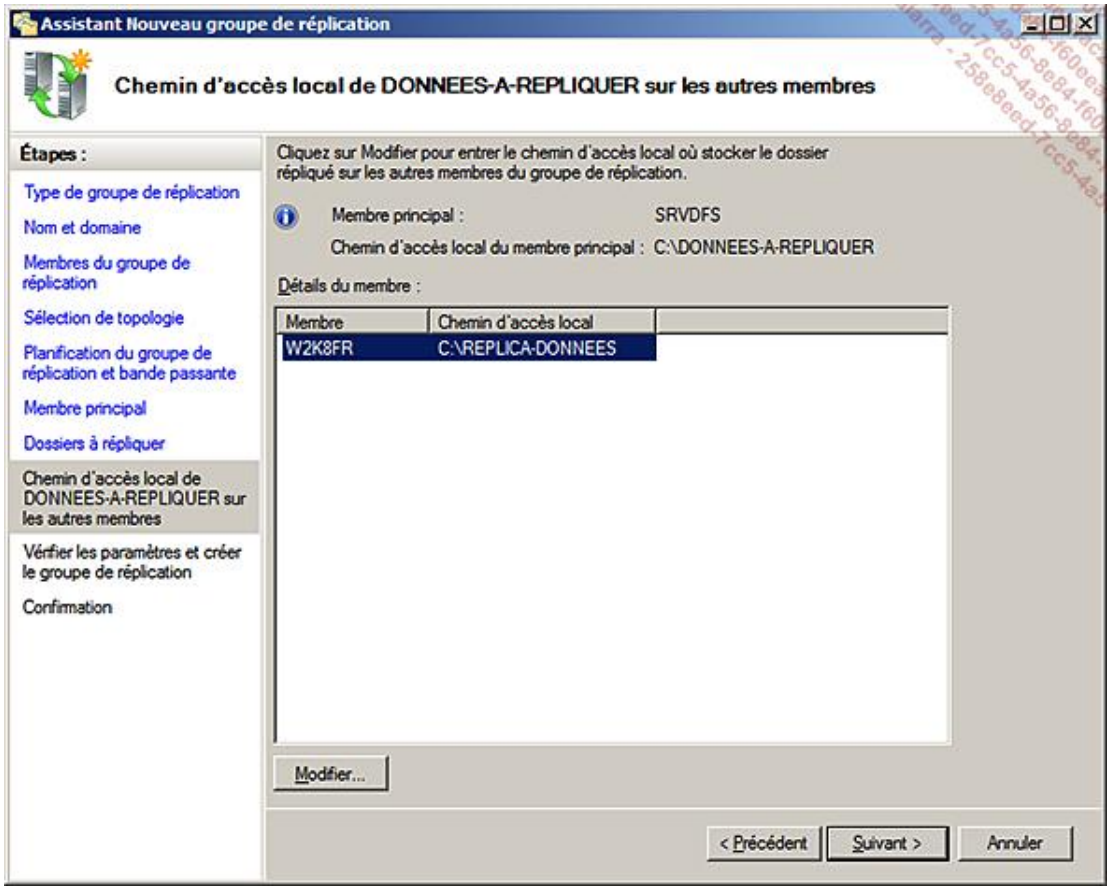


- Pour chaque serveur contenant un réplica des données, activez la réplication en indiquant un dossier de destination. Sélectionnez le serveur, puis cliquez sur **Modifier**.

© ENI Editions - All rights reserved - adamo diarra

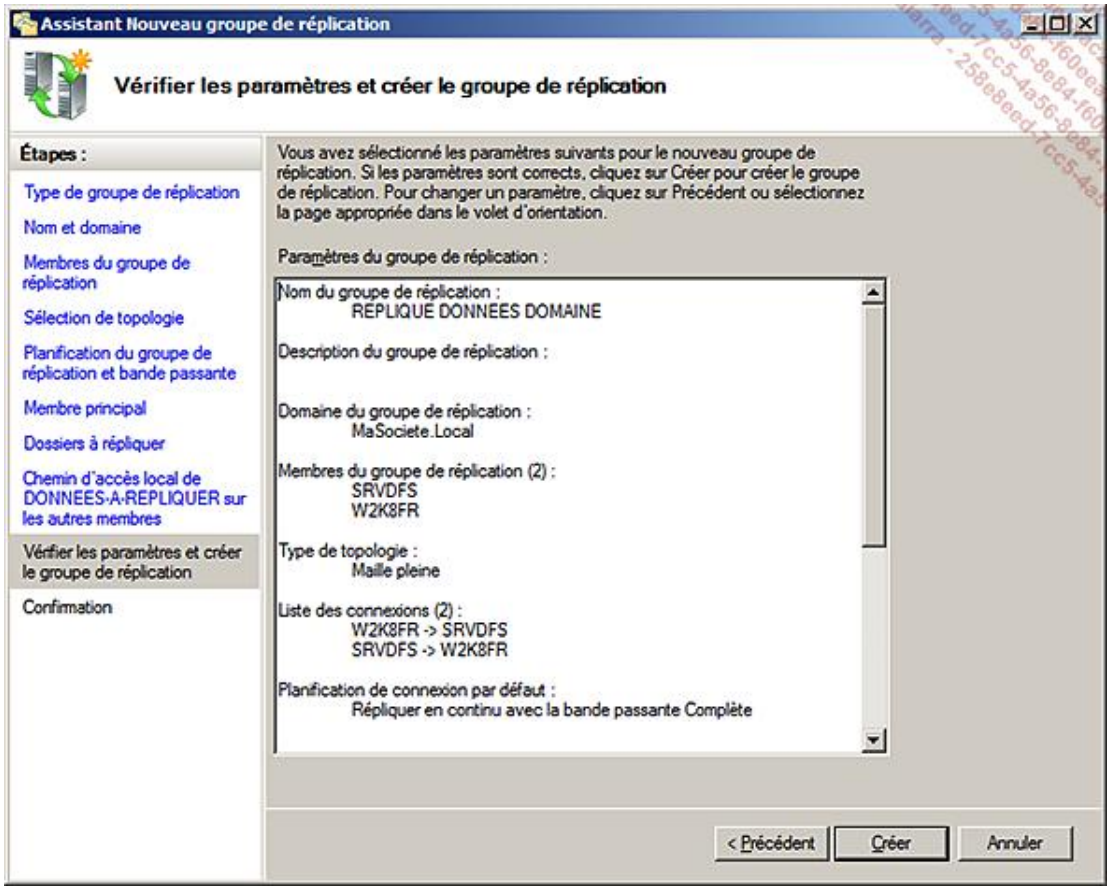


Cette option permet d'indiquer le nom du dossier principal et de le créer si nécessaire.

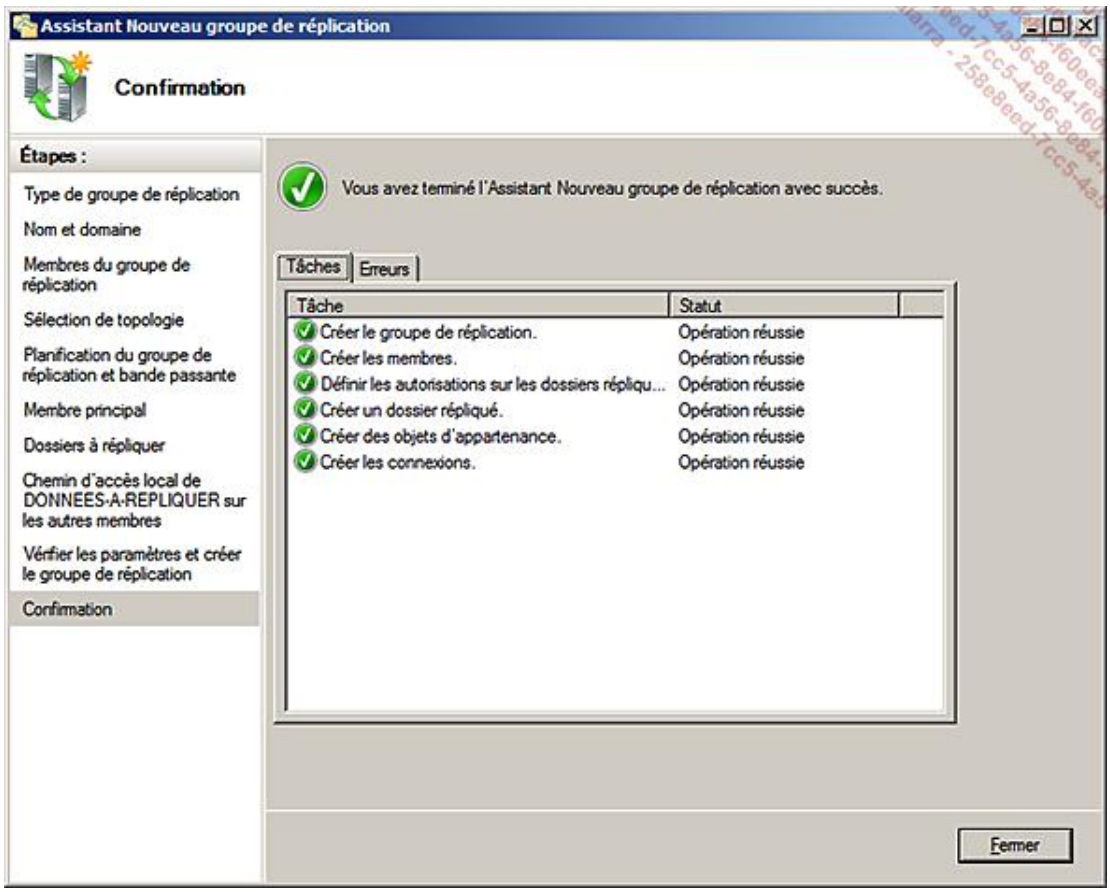


Cet écran résume les paramètres principaux de la réplication.

© ENI Editions - All rights reserved - adamo diarra



Voici le résultat de la mise en place de la réplication.



La mise en place effective dépendra du fonctionnement de l'Active Directory et des plannings de réplication mis en place entre les sites.

© ENI Editions - All rights reserved - adamo diarra

c. La topologie de réplication

Deux types de topologie sont proposés par défaut.

- Le mode **Hub & Spoke** dit **en étoile** nécessite trois membres au minimum. Ce mode est particulièrement utile lorsqu'il y a une source précise (le Hub) et la réplication vers de très nombreuses destinations.

- Le mode **maille pleine** autorise chaque serveur à répliquer avec les autres. Ce mode est conseillé pour les installations comportant une dizaine de membres au maximum.

La mise en place d'une nouvelle topologie dépend de la réplication Active Directory, et peut donc prendre du temps avant de se mettre en place sur chaque membre.

En revanche, la réplication locale des fichiers (de taille raisonnable) peut être très rapide, et généralement instantanée.

© ENI Editions - All rights reserved - adamo diarra

La configuration avancée

1. Les méthodes de classement

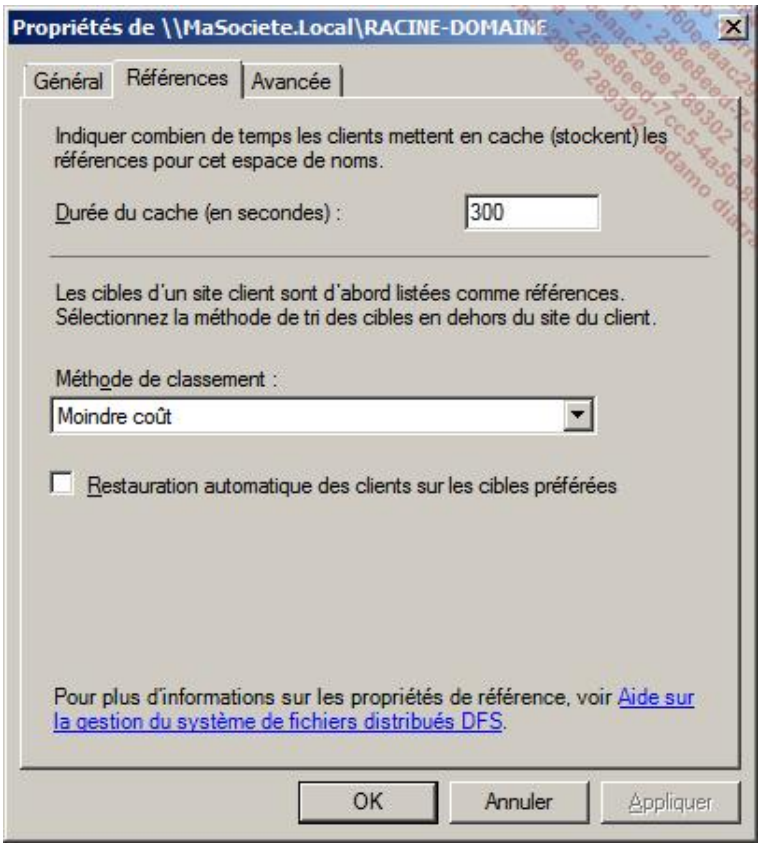
Les méthodes de classement sont très importantes à prendre en considération afin d'optimiser et d'éviter de nombreux désagréments.

En effet, lorsqu'un même dossier est accessible sur différents partages, situés sur différents serveurs, eux-mêmes situés sur des sites différents, l'optimisation logique serait d'utiliser le partage situé sur le serveur du site local. Même dans ce cas, il est parfois vital d'utiliser en priorité un serveur précis qui sert de référence. Dans d'autres cas, c'est un serveur distant qui sert de référence unique qu'il faut forcer afin d'éviter les modifications simultanées d'un document.

a. La configuration au niveau des racines DFS

L'onglet **Références** sur les propriétés des racines DFS permet de régler la valeur par défaut utilisée sur toutes les liaisons appartenant à cette racine.

- L'ordre aléatoire
- Moindre coût
- Exclusion de tous les sites distants



L'**Ordre aléatoire** consiste à proposer de manière aléatoire tous les serveurs situés sur le site du client, puis toujours de manière aléatoire tous les autres serveurs présents sur les autres sites sans tenir compte des différences de coûts.

Le **Moindre coût** présentera d'abord les serveurs situés sur le site du client de manière aléatoire. Ensuite, l'affichage des serveurs distants sera proposé du coût le moins élevé au plus élevé, mais les serveurs ayant un coût identique seront proposés aléatoirement.

Le dernier mode, **Exclure les cibles en dehors du site du client**, n'affichera que les serveurs présents sur le site du client. Vous verrez plus loin les exceptions à cette règle.

© ENI Editions - All rights reserved - adamo diarra

Si la restauration automatique des clients sur les cibles préférées est forcée à ce niveau, elle sera active sur toutes les liaisons et cibles qui dépendront de cette racine.

b. La configuration au niveau des liaisons DFS

Sur chaque dossier représentant une liaison vers une ou plusieurs cibles, il est possible d'indiquer une exclusion des sites distants, notamment si celle-ci n'a pas été indiquée précédemment. On peut aussi activer la restauration automatique des clients vers une cible préférée (si celle-ci n'avait pas déjà été configurée au niveau supérieur).

c. La configuration au niveau des cibles DFS

Sur chaque cible, dans l'onglet **Avancée**, il est possible de configurer un comportement particulier.

Il est possible de privilégier l'utilisation d'une cible en la définissant comme **Première de toutes les cibles** ou **Première parmi les cibles de même coût**.

On peut au contraire, définir la cible comme **Dernière de toutes les cibles** affichées lors de la sélection, ou **Dernière parmi les cibles de même coût**.

Attention, ces règles forcées (Première ou Dernière) provoquent l'affichage systématique des cibles correspondantes.

2. La délégation d'administration

Par défaut, seuls les administrateurs locaux ou du domaine peuvent gérer les groupes de réplication. Sur une racine du domaine, seul le groupe **administrateurs de l'entreprise** hérite automatiquement des droits d'administration. Sur une racine autonome, le groupe **administrateurs** local et le compte spécial **SYSTEM** ont les droits hérités.

Lorsqu'une racine est créée par un administrateur, celui-ci et le groupe **administrateurs du domaine** obtiennent des droits qui sont dit **explicites**. Ce qui veut dire que ces droits peuvent être supprimés.

Attention, les administrateurs qui ont reçu une délégation restent propriétaires des objets, même s'ils sont retirés par la suite des administrateurs.

© ENI Editions - All rights reserved - adamo diarra

Par ailleurs, tout administrateur d’une racine DFS peut déléguer l’autorisation de gestion.

© ENI Editions - All rights reserved - adamo diarra

Les apports de Windows 2008 R2

Attention, la plupart des fonctionnalités de Windows 2008 R2 ne sont utilisables que si les racines DFS sont gérées par des serveurs Windows 2008 dans un domaine possédant la fonctionnalité Windows 2008.

Le mode **Access-based enumeration** permet de ne montrer à l'utilisateur que les dossiers et documents sur lesquels il possède des droits. Si ce mode est bien actif par défaut sur les partages hébergés sur Windows 2008 R2, il est nécessaire de l'activer sur les racines qui remplissent les conditions indiquées.

Voici la commande utilisant DFSUTIL permettant d'activer ce mode.

```
dfsutil property abde enable \\<namespace_root>
```

Les autres fonctionnalités propres à Windows 2008 R2 sont :

- La recherche directe d'un dossier ou d'une cible DFS à partir de l'administration DFS.
- La création des racines autonomes DFS sur la machine virtuelle d'un cluster.
- La création de racines de domaine en mode **Windows Server 2008 mode domain-based namespaces** qui permet d'activer immédiatement les nouvelles fonctionnalités, sans avoir à convertir les anciennes racines dites en mode **domain-based namespace (Windows 2000 Server mode)**.
- La reprise accélérée de la réplication en cas de crash inattendu.
- Une sécurité particulière garantit la fraicheur du contenu en empêchant un vieux serveur de réécrire au dessus de données récentes.
- Un mécanisme de réplication amélioré aussi bien pour la réplication initiale que pour le différentiel, pour les petits et les gros fichiers.

© ENI Editions - All rights reserved - adamo diarra

Les outils

L'administration graphique classique permet de gérer les opérations normales et ponctuelles. Mais, de nombreuses raisons font qu'il est souvent nécessaire d'automatiser toutes ces opérations pour l'installation, la réparation ou la gestion d'environnements complexes et structurés.

Les outils en ligne de commande sont alors bien pratiques pour réaliser ce type d'opération.

Tous ces outils sont installés et utilisables directement sur tous les serveurs disposant du rôle DFS.

1. DFSCMD

La commande DFSCMD permet de gérer toute la partie **Espace de noms**, c'est-à-dire de créer et de configurer une arborescence DFS.

Il n'est pas utile de reprendre toute la documentation de cette commande qui est facilement accessible.

Voici un exemple de commande qui permet de créer un batch de **réinstallation** :

```
dfscmd /view \\MaSociete.local\racine-domaine /batchrestore
```

Exemple de résultat :

```
REM BATCH RESTORE SCRIPT
REM dfscmd /map "\\MASOCIETE\RACINE-DOMAINE" "\\SRVDFS\RACINE-DOMAINE" ""
/restore
REM dfscmd /add "\\MASOCIETE\RACINE-DOMAINE" "\\W2K8FR\RACINE-DOMAINE" /restore
dfscmd /map "\\MASOCIETE\RACINE-DOMAINE\COMPTA" "\\SRVDFS\COMPTA1" "" /restore
dfscmd /add "\\MASOCIETE\RACINE-DOMAINE\COMPTA" "\\W2K8FR\compta2" /restore
```

On y retrouve les commandes de bases qui permettent de créer une racine, puis d'y ajouter des liaisons DFS.

Pour gérer la partie réplication, il sera nécessaire d'utiliser la commande `DFSRADMIN`.

2. DFSRADMIN

L'outil permet de créer, supprimer et lister les éléments de la réplication DFS.

La commande suivante permet de générer un rapport de la réplication du dossier choisi :

```
DFSRADMIN PROPREP NEW /RgName :GroupeReplication
/RfName :DossierRépliqué /MemName :Domaine\Serveur
```

Comme la commande DFSCMD, elle permet d'automatiser la création d'ensembles de réplication à partir d'un fichier grâce à l'option **Bulk**.

3. DFSRDIAG

Cette commande permet de vérifier le bon fonctionnement, de diagnostiquer et de gérer l'activité de la réplication.

Il est possible de forcer une réplication sur une connexion précise, ou au contraire de l'arrêter immédiatement.

4. DFSUTIL

Cette commande permet de gérer les espaces de noms, les serveurs et les clients DFS.

5. DFSRMIG

Cet utilitaire ne sert pas dans l'utilisation normale de DFS. Il s'agit plutôt d'un outil d'optimisation de la réplication des

© ENI Editions - All rights reserved - adamo diarra

fichiers utilisés par AD.

La commande `DFSRMIG` permet en effet de migrer la réplication de SYSVOL du mode **NTFRS (Réplication 2003)** vers le mode **DFSR (Réplication 2008)**.

Elle permet aussi de vérifier le statut de cette migration sur les différents contrôleurs de domaine.

Certaines options particulières ne seront utiles que dans l'administration des contrôleurs de domaine en lecture uniquement (RODC) lors de leur migration en mode DFSR.

Vous trouverez plus d'informations sur les RODC dans le chapitre Domaine Active Directory de ce même ouvrage.

© ENI Editions - All rights reserved - adamo diarra

L’utilisation de DFS et les bons usages

L’utilisation de DFS ne nécessite aucune adaptation sur les postes clients.

En effet, du côté utilisateur (et des clients Windows), les partages DFS et les racines sont vus comme des partages classiques. C’est souvent dans le script de connexion que l’on réalise la connexion aux racines, en remplacement de toutes les anciennes connexions.

Par ailleurs, il est important de noter que les racines DFS de domaine sont disponibles pour tous les utilisateurs de la forêt. Mais, toutes les permissions affectées aux partages et aux dossiers NTFS restent totalement actives comme s’il s’agissait d’un accès direct.

En revanche, l’utilisation de DFS permet de simplifier le nombre d’unités disques et de partages utilisés. Ceci permet de fédérer l’ensemble des espaces disponibles.

Les applications peuvent être configurées sur un chemin unique qu’il sera possible de maintenir durant toute la vie de la forêt.

DFS dans la configuration **Hub & Spoke** est préconisé pour la réplication sur de nombreux sites d’informations bougeant peu ou n’ayant qu’un seul point de modification. Les procédures validées, notices, comptes-rendus et informations générales sont les documents entrant dans ce type de configuration.

DFS peut aussi être utilisé pour sauvegarder les données utilisateurs ou les profils itinérants. Une configuration particulière doit alors être réalisée au niveau des cibles DFS afin que ce soit toujours le même partage et le même serveur qui sont utilisés. C’est-à-dire qu’il faut toujours proposer la cible principale en premier, et de ne proposer la copie (sauvegarde) qu’en dernière cible.

Lorsque DFS est utilisé pour la bureautique, avec de nombreux documents de type Word ou Excel mis à jour sur différents site, il est important de bien gérer le versionning des documents afin d’éviter toute modification « simultanée » d’un même document. En effet, seule la dernière version écrite sera conservée. Dans certains cas, il sera préférable de forcer l’utilisation d’une cible précise qui servira de référence pour les modifications de ce genre, même si le site de l’utilisateur comporte la réplication locale de cette cible.

Donc, DFS n’est pas la solution universelle, mais elle peut rendre de nombreux services qu’il faut comparer aux autres solutions, par exemple de gestion documentaire.

© ENI Editions - All rights reserved - adamo diarra

Les améliorations de DFS avec Windows Server 2008 R2

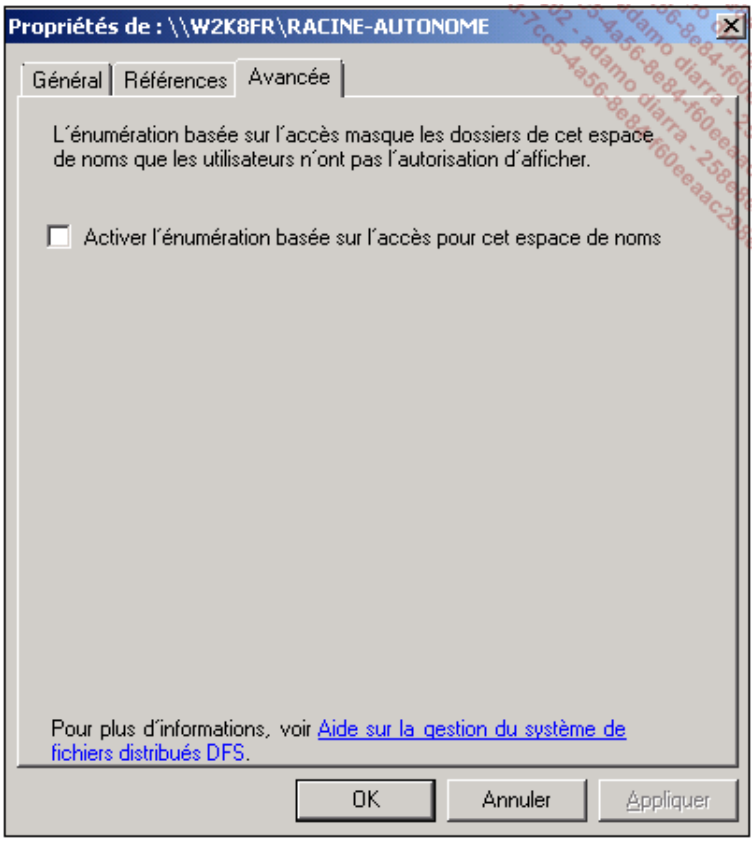
1. Le mode ABE

Le mode **ABE** (c'est-à-dire l'Accès Basé sur l'Enumération) activé sur les partages a pour fonction de masquer automatiquement tous les dossiers et fichiers sur lesquels un utilisateur n'a pas au moins un accès en lecture. Sauf dans le cas de très gros dossiers, ce mode diminue le trafic réseau et sécurise l'information en ne laissant apparaître à l'utilisateur que les données utiles et autorisées.

Chaque partage Windows peut être configuré individuellement pour utiliser ce mode et les racines Windows Server 2008, vues comme des partages, peuvent maintenant en profiter avantageusement.

L'activation peut se faire par l'interface graphique ou par la ligne de commande.

Pour les racines hébergées sur Windows Server 2008 R2, la configuration se trouve dans les propriétés de la racine, au niveau de l'onglet **Avancée**.



Pour les racines de domaine, le mode ABE n'est activable que pour celles créées après le passage du domaine en fonctionnalité 2008. Il sera nécessaire de supprimer et de recréer les anciennes racines en suivant cette procédure : http://technet.microsoft.com/en-us/library/cc753875.aspx.

Pour information, pour les serveurs Windows Server 2008 non R2, la ligne de commande est indispensable :

```
DFSUTIL PROPERTY ABE ENABLE \\MaSociete.local\RACINE-DOMAINE.
```

Le filtrage ABE n'a réellement de sens que si chaque partage (cible) est lui-même configuré dans ce mode.

2. Le mode « lecture uniquement » de la réplication DFS sur Windows 2008 R2

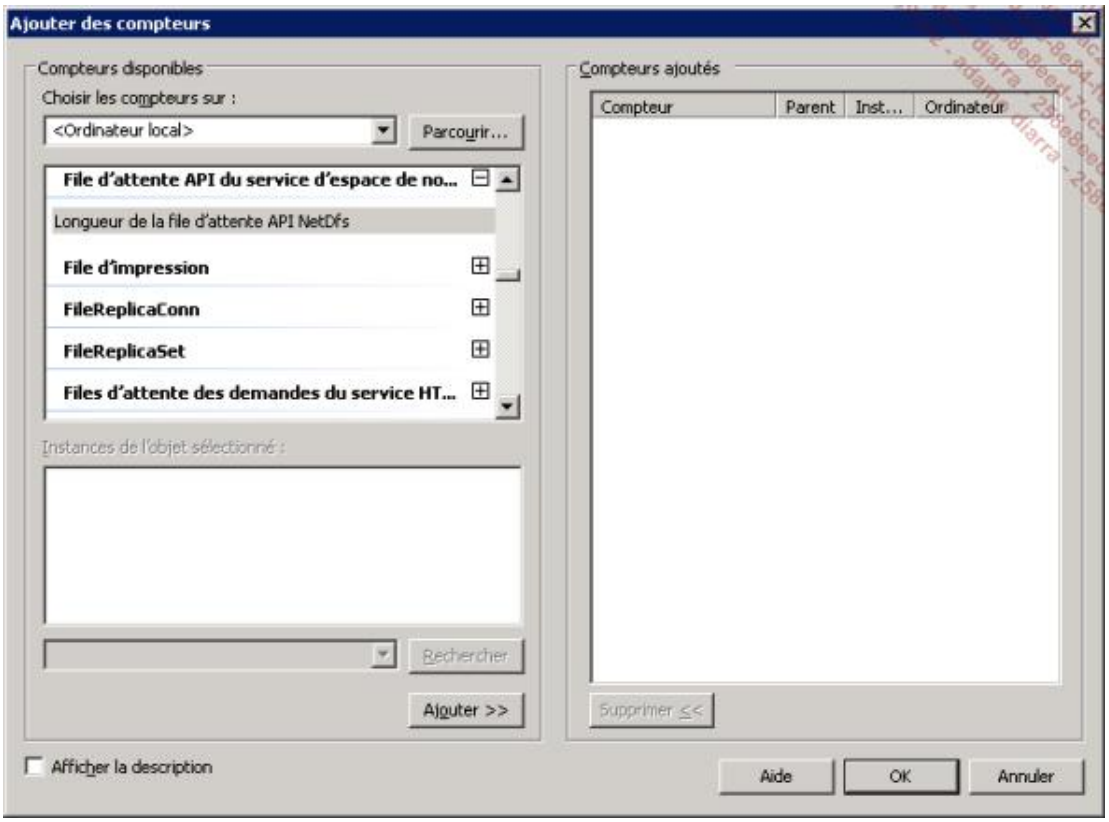
Les partages hébergés par des clusters de fichiers peuvent maintenant être intégrés à DFS et utilisés dans les groupes de réplication.

Certains réplicas peuvent être configurés en **Lecture Uniquement**, cette possibilité étant directement utilisée par les partages SYSVOL sur les contrôleurs de domaine en mode RODC.

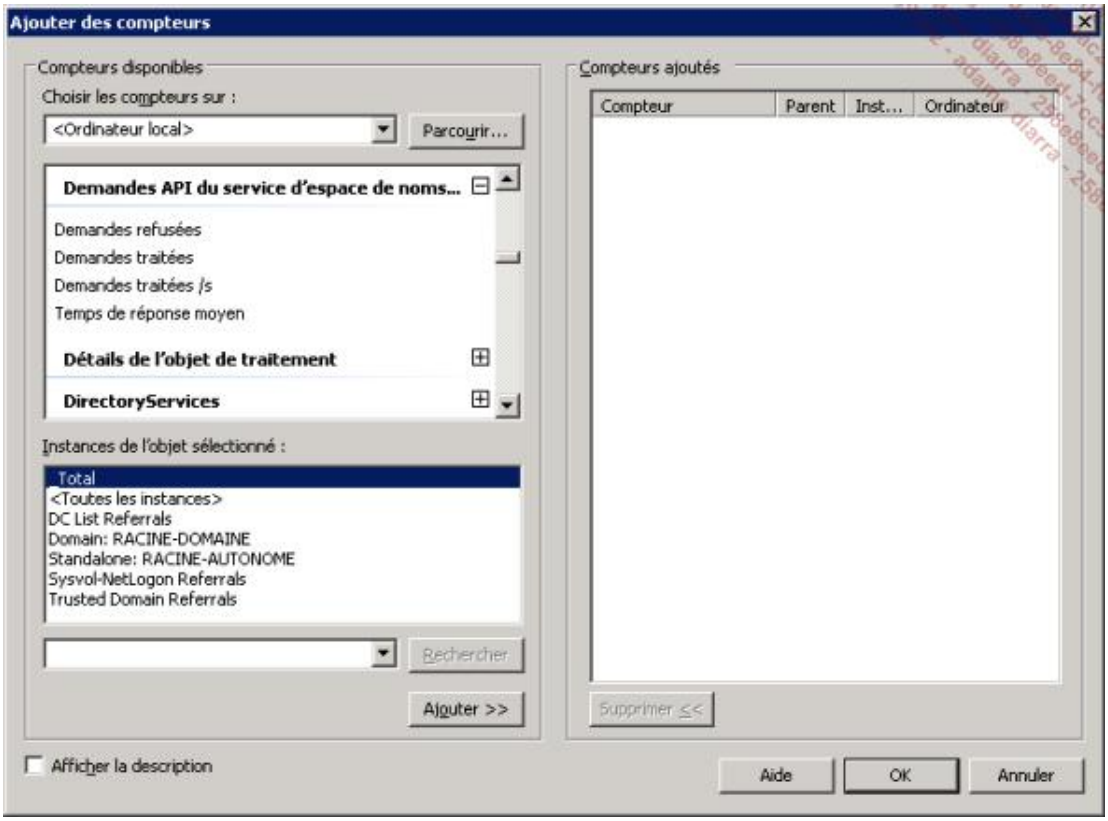
© ENI Editions - All rights reserved - adamo diarra

3. Des compteurs de performances spécifiques pour DFS sur Windows 2008 R2

Ces nouveaux compteurs permettent de mieux prendre en compte l'activité spécifique de DFS par rapport aux accès classiques aux partages.

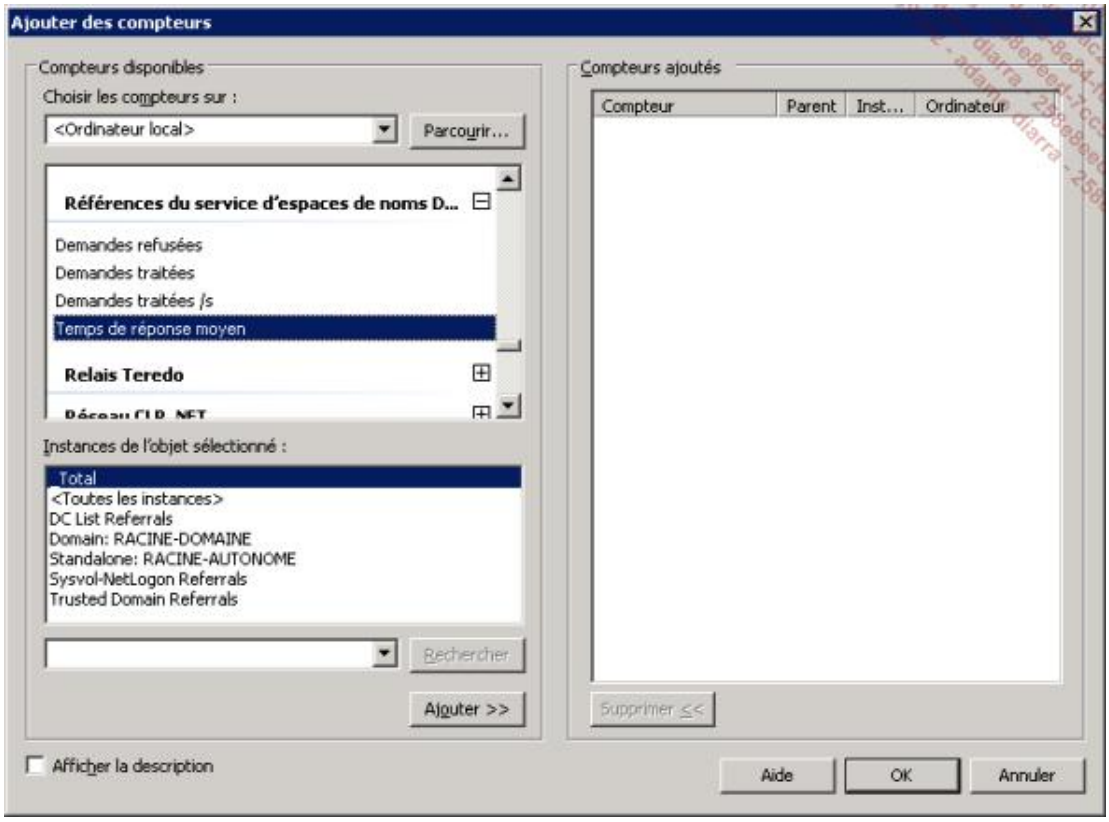


- Le compteur **File d'attente API du service d'espace de noms** indique la longueur de la file d'attente API.



© ENI Editions - All rights reserved - adamo diarra

- Les **Demandes API du service d'espace de noms DFS** donnent des informations sur les performances des requêtes.



- Les **références du service d'espaces de noms** donnent des informations sur les performances des requêtes de type référentiel.

4. Les performances améliorées pour les grosses infrastructures DFS

Les performances sont fortement améliorées au démarrage et à l'utilisation pour les racines comportant plus de 5 000 liens DFS et l'on constate une légère amélioration pour 300 000 liens et plus.

5. De nouvelles options pour DFSFRDIAG

DFSFRDIAG dispose de nouvelles options : replstate, idRecord et FileHash.

L'option replstate permet notamment d'obtenir un résumé sur les réplications en cours.

Les options idRecord et FileHash servent à identifier et comparer chaque document intégré à DFS.

© ENI Editions - All rights reserved - adamo diarra

Les éléments ajoutés à la gestion des imprimantes sur Windows 2008 R2

Le principal ajout consiste en une console appelée **Gestion de la numérisation** qui est maintenant dédiée à l'administration des scanneurs sous la forme d'un service de rôle appelé **serveur de numérisation distribuée** qu'il faut sélectionner lors de l'installation du rôle **Services de documents et Impressions**. Certaines améliorations sont à noter dans la délégation, le CSR (*Client Side Rendering*) et XPS (*Xml Paper Specifications*).

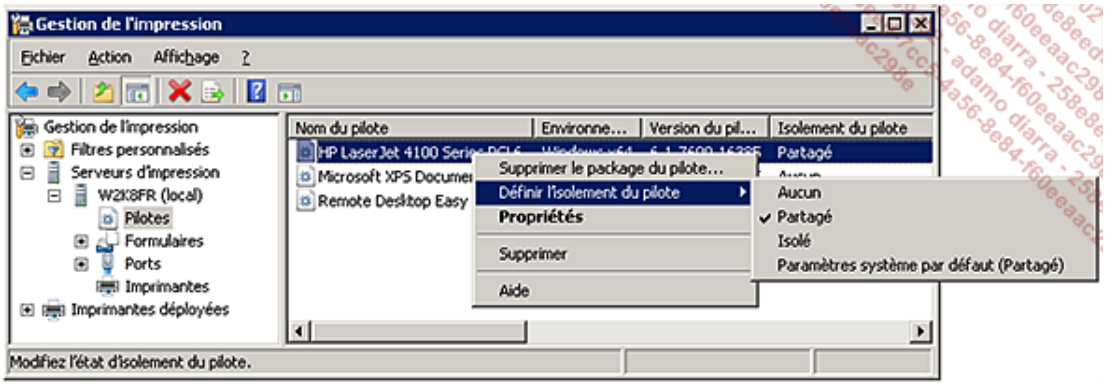
1. L'amélioration de l'assistant de migration

L'outil **PrintMig** est remplacé par **PrintBrm**. L'assistant permet de sauvegarder spécifiquement les **processeurs d'impressions** et les **moniteurs de langage d'impression**. Les caractéristiques des queues et des serveurs d'impression peuvent maintenant être restaurées à partir d'une sauvegarde. L'exécutable en ligne de commande se trouve dans le dossier C:\windows\system32\spool\tools.

2. L'isolement des pilotes d'impression

L'isolement d'un pilote d'impression lui affecte un processus différent de la tâche spooler. En cas de pilotes défectueux, l'activité du spooler d'impression n'est ni perturbée ni bloquée. Cet isolement est conseillé pour les pilotes notablement connus pour leur manque de fiabilité ou pour les nouveaux pilotes à valider.

Après l'installation d'un pilote, ses propriétés accessibles par un clic droit permettent de basculer du mode **Partagé** au mode **Isolé**.



3. Location-aware printing (impression dépendante du site)

Cette option permet à l'utilisateur de définir une imprimante par défaut différente sur chaque réseau détecté et nommé. Pour les utilisateurs nomades se déplaçant avec leurs machines, l'imprimante par défaut de chaque site sera ainsi conservée dans les registres de son profil Windows.

4. Le serveur de numérisation distribuée

Le **serveur de numérisation distribuée** gère la centralisation de la communication entre les scanneurs du réseau et les serveurs qui canalisent l'information en créant des processus de scan spécifiques.

Attention, seuls les scanneurs compatibles **WSD** (*Web Services Distributed*) peuvent être gérés par ce service. En particulier, ces scanneurs doivent disposer des fonctions de recherches LDAP, d'envoi de messages par SMTP... Ce serveur de numérisation évite généralement l'installation des multiples outils différents fournis par les constructeurs et permet une administration centralisée et uniforme.

Sur le serveur de numérisation sont définis les processus qui précisent comment un document est scanné, où il est placé, à qui il est envoyé ainsi que les utilisateurs et groupes autorisés à utiliser cette règle. Sur les appareils compatibles WDS, l'utilisateur choisit le processus de scan sur le panneau de configuration au moment du scan.

Le processus de scan précise la résolution de l'image, le codage des couleurs et le type de fichier. Ces éléments font partie des règles du processus. L'utilisateur peut être autorisé à modifier certains éléments de la configuration du processus au moment du scan. La destination du document scanné peut être une combinaison des éléments

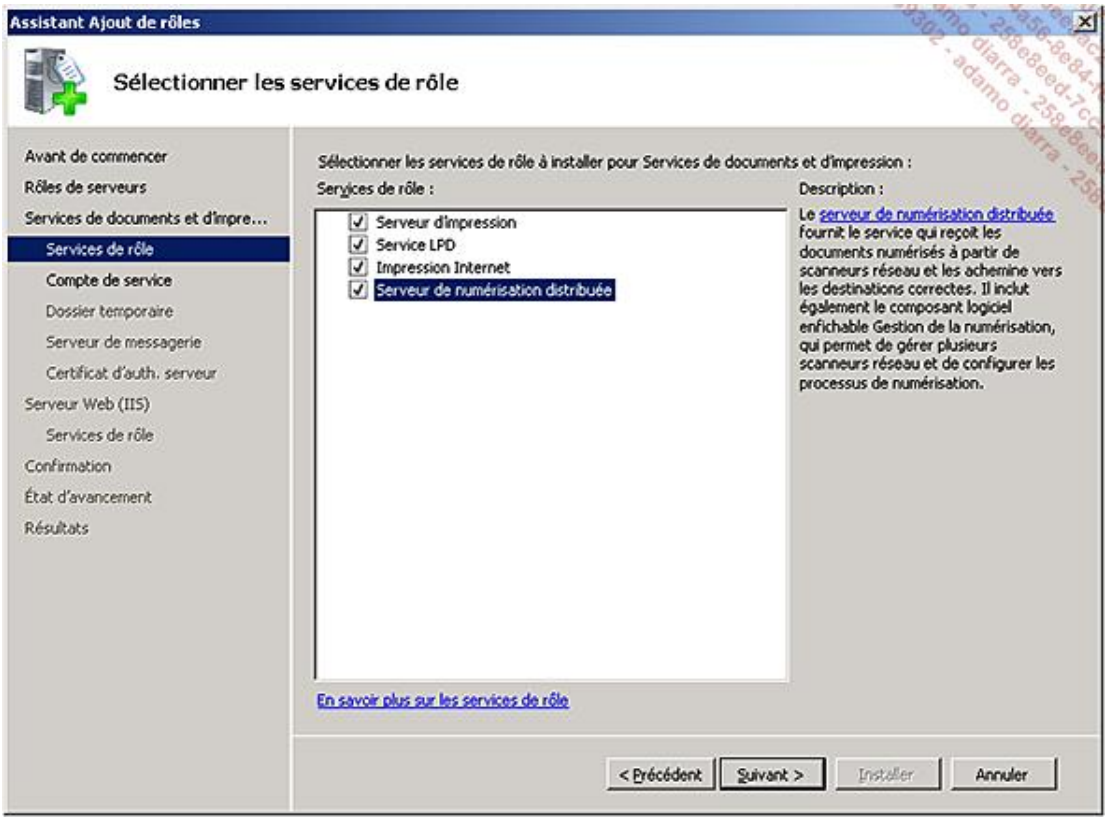
© ENI Editions - All rights reserved - adamo diarra

suivants : un dossier partagé, un site SharePoint ou des destinataires de messagerie.

a. L'installation du service de rôle Serveur de numérisation distribuée

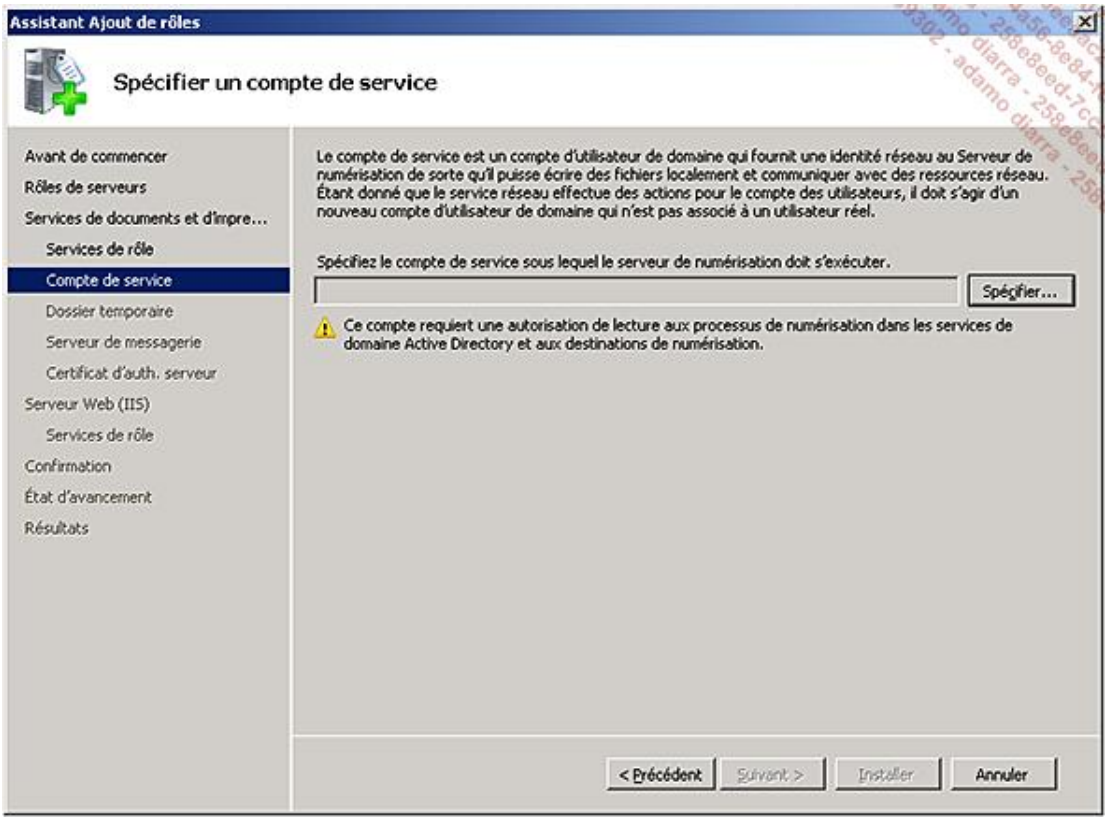
Attention, l'installation de ce service de rôle nécessite un certificat et un redémarrage du serveur. Le certificat peut être généré automatiquement, mais il est préférable de l'obtenir par une autorité interne.

- Lors de l'installation du rôle **Services de documents et d'impressions**, sélectionnez le service de rôle correspondant.

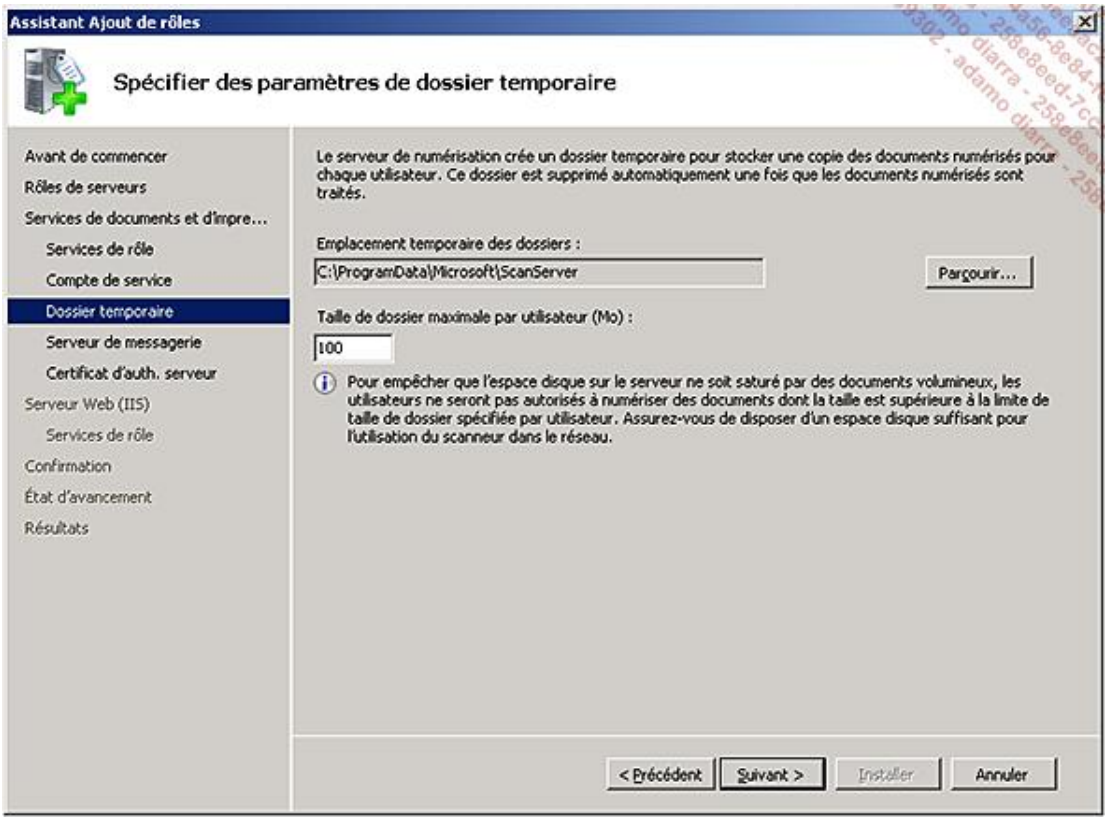


Un compte de service doit être défini afin de pouvoir écrire localement les documents de travail, mais aussi communiquer avec les ressources du réseau (scanneurs, partages...).

© ENI Editions - All rights reserved - adamo diarra

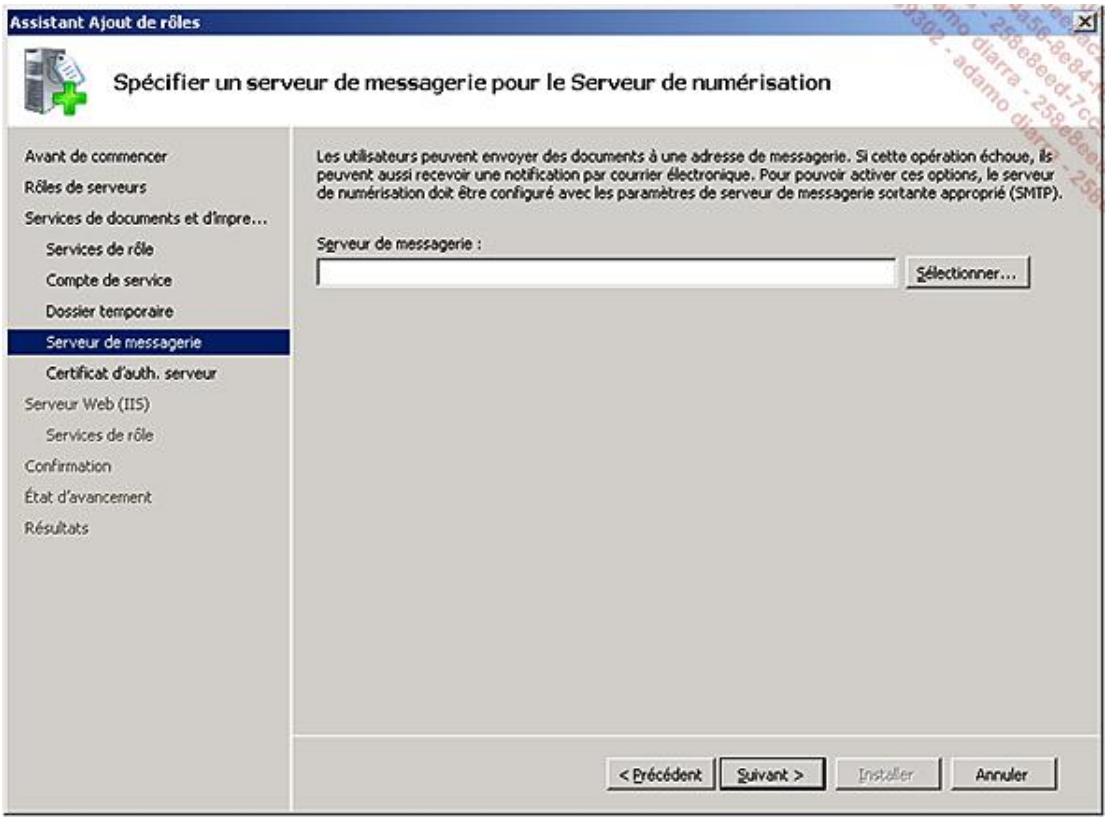


Définissez un emplacement de stockage suffisant pour l'ensemble des numérisations à réaliser simultanément, ainsi que la taille maximale autorisée pour chaque numérisation.

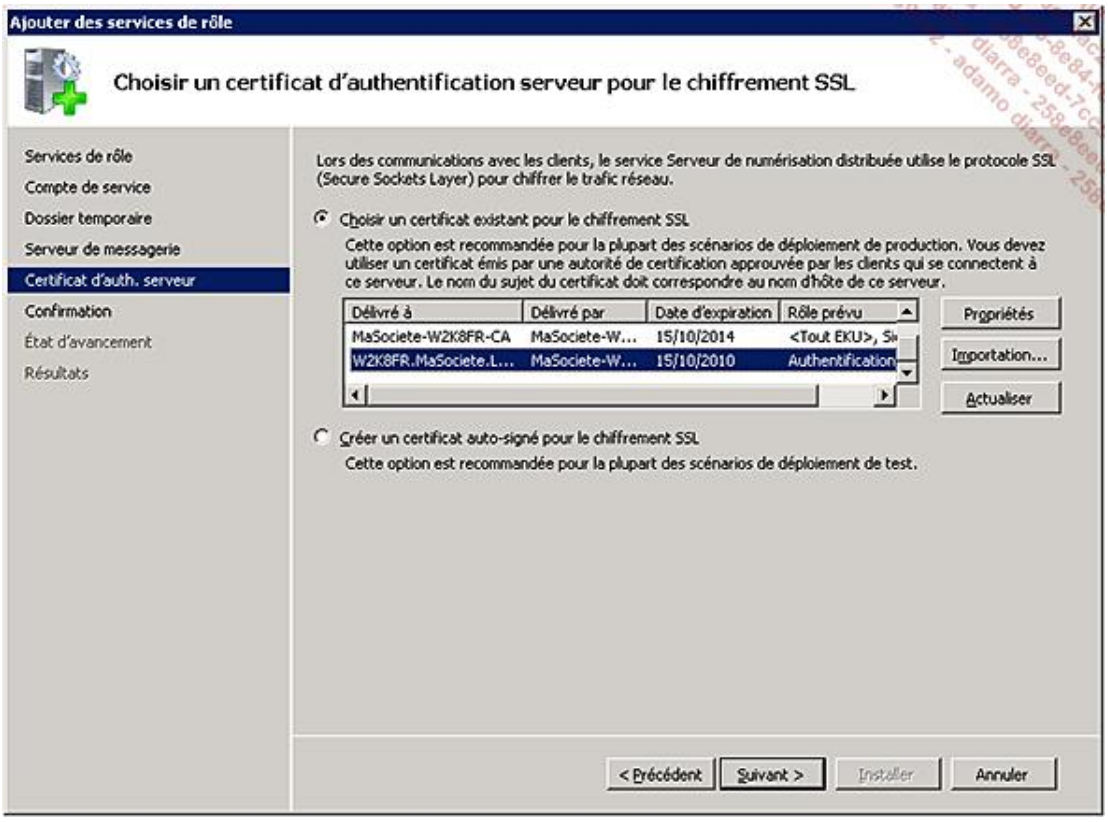


Si un serveur de messagerie disposant d'un connecteur SMTP est spécifié, les processus de scan pourront inclure l'envoi et la distribution de la numérisation par ce biais.

© ENI Editions - All rights reserved - adamo diarra

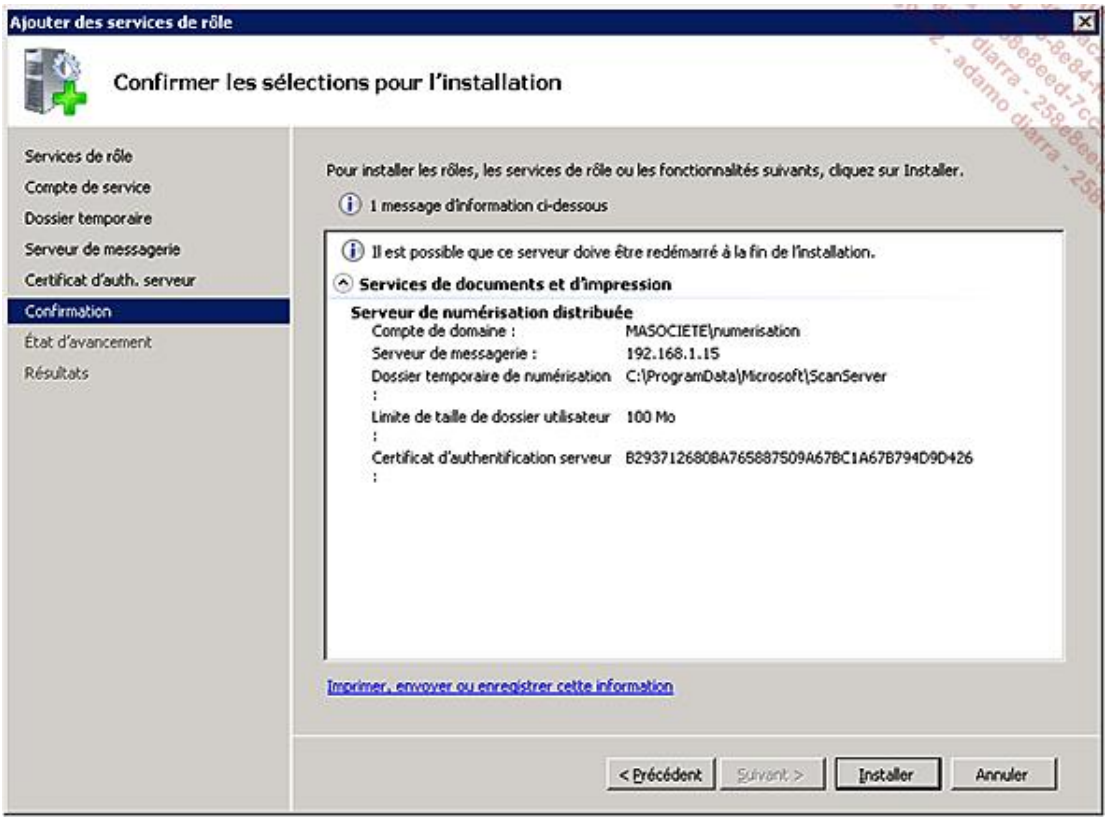


Le certificat servira à sécuriser les communications et les documents transmis entre les clients et le serveur de numérisation. Si le certificat est émis par une autorité de certification interne ou reconnue, les clients accepteront automatiquement ce certificat.



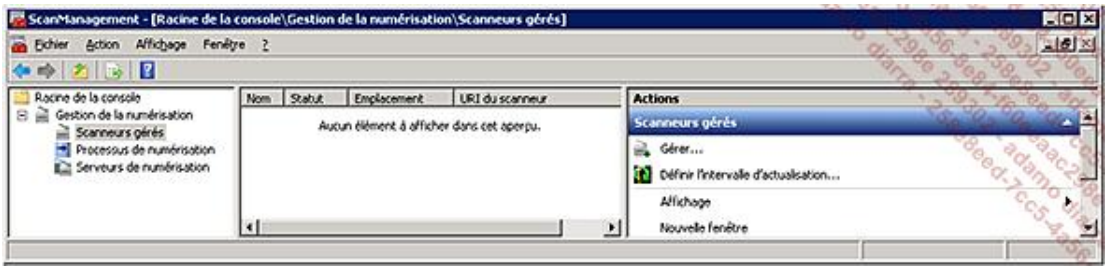
Cet écran résume les choix réalisés et le redémarrage est proposé en fin d'installation.

© ENI Editions - All rights reserved - adamo diarra



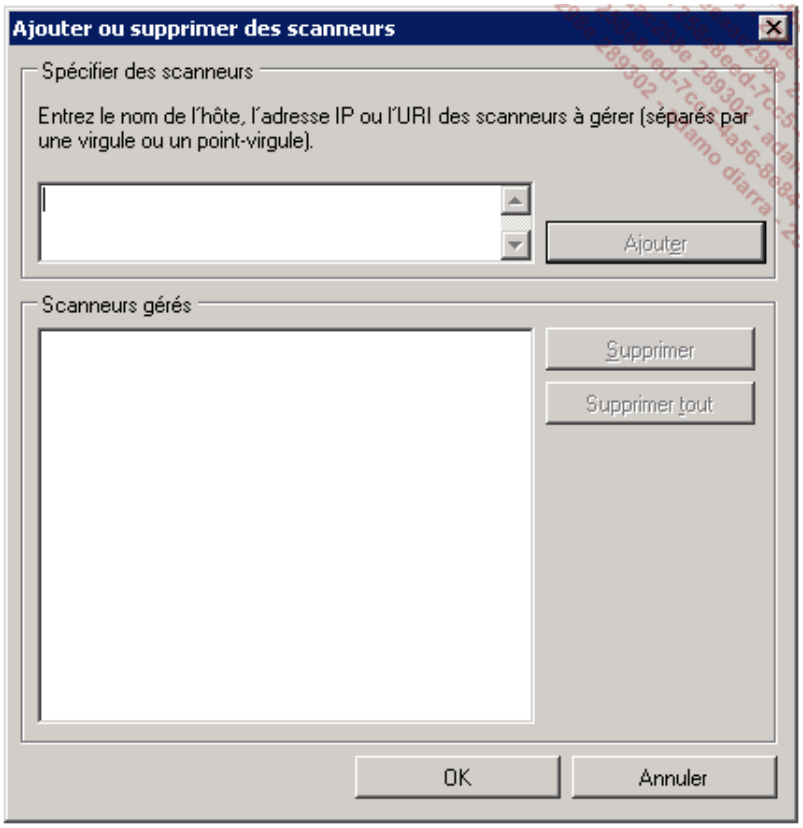
b. La définition d'un processus de numérisation

La console **Gestion de la numérisation** permet de définir les scanneurs gérés, les processus de numérisation prédéfinis et les différents serveurs de numérisation existants.



La première étape consiste à intégrer les scanneurs compatibles dans l'administration des serveurs de numérisation.

© ENI Editions - All rights reserved - adamo diarra



Les scanneurs peuvent être indiqués par leur nom ou leur adresse IP.

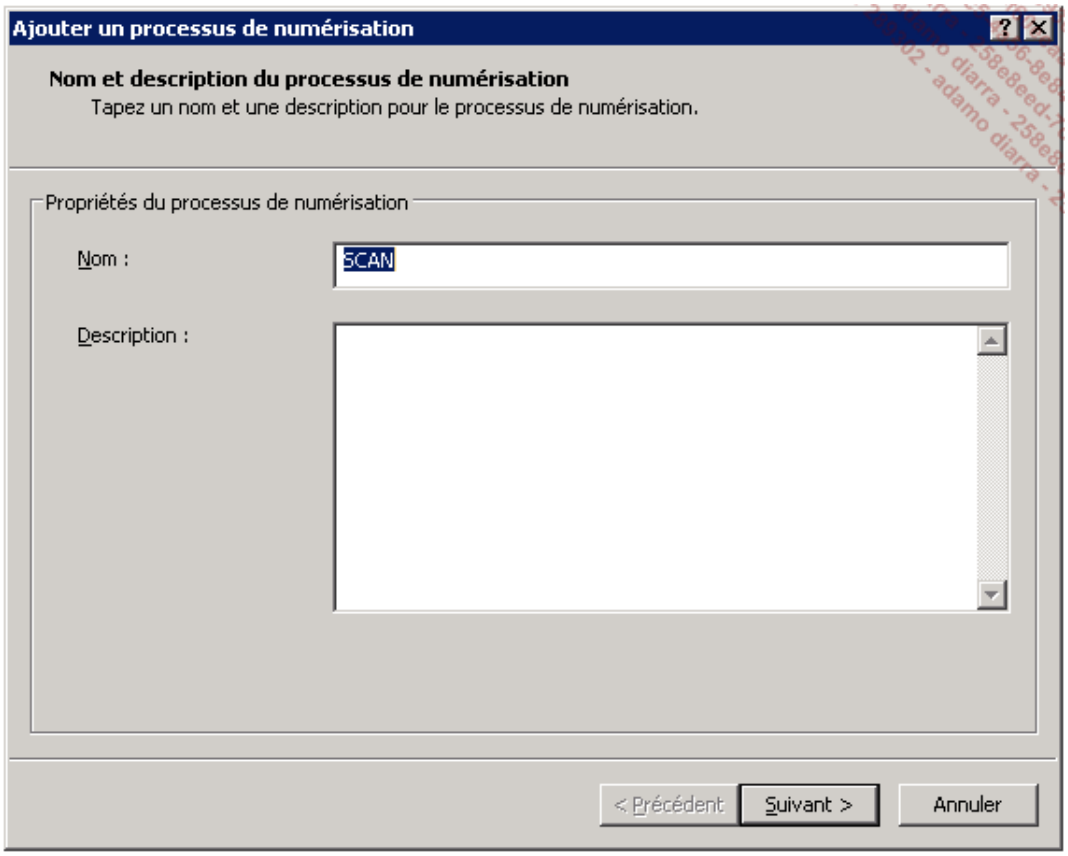
Les serveurs de numérisation sont intégrés de la même manière. Il est parfois nécessaire de posséder un certificat de type client pour accéder aux scanneurs ou aux serveurs de numérisation.

Différents paramètres constituent le processus de numérisation.

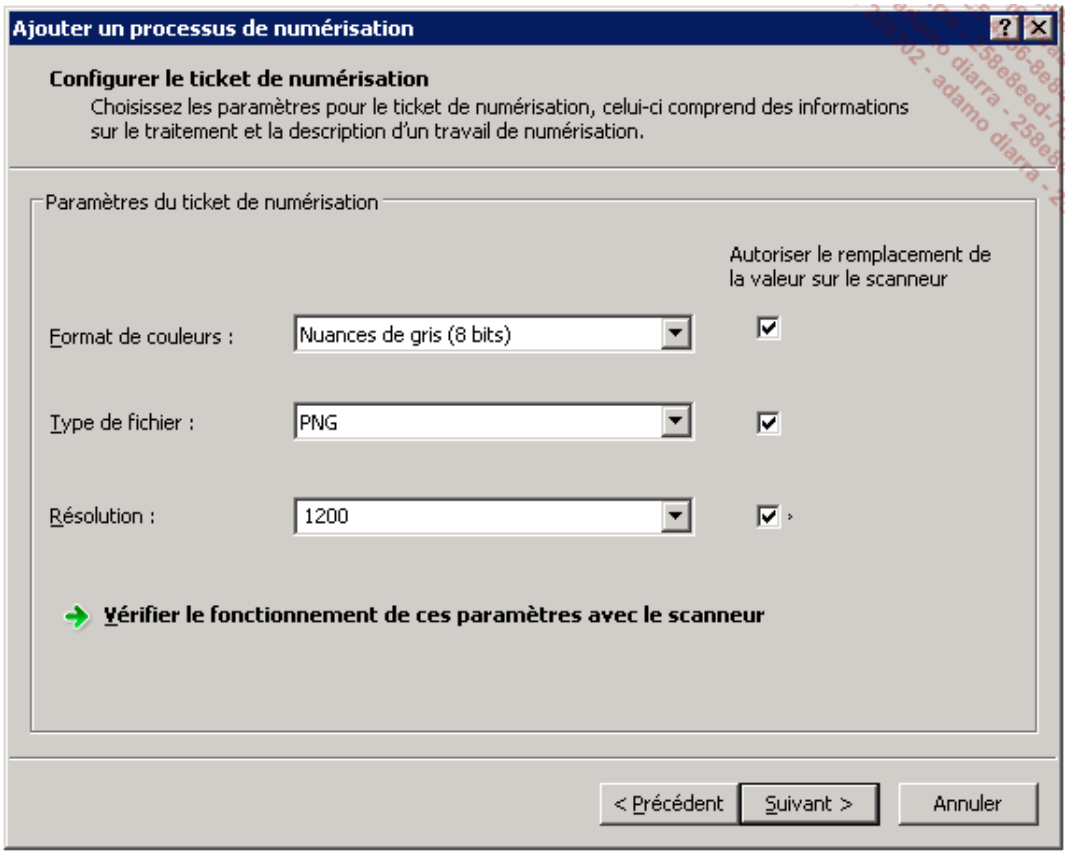
Chaque processus de numérisation décrit ensuite les opérations à réaliser et si l'utilisateur est autorisé à modifier les valeurs prédéfinies.

Le nom qui est défini est celui qui apparaîtra sur le panneau de configuration du scanneur.

© ENI Editions - All rights reserved - adamo diarra

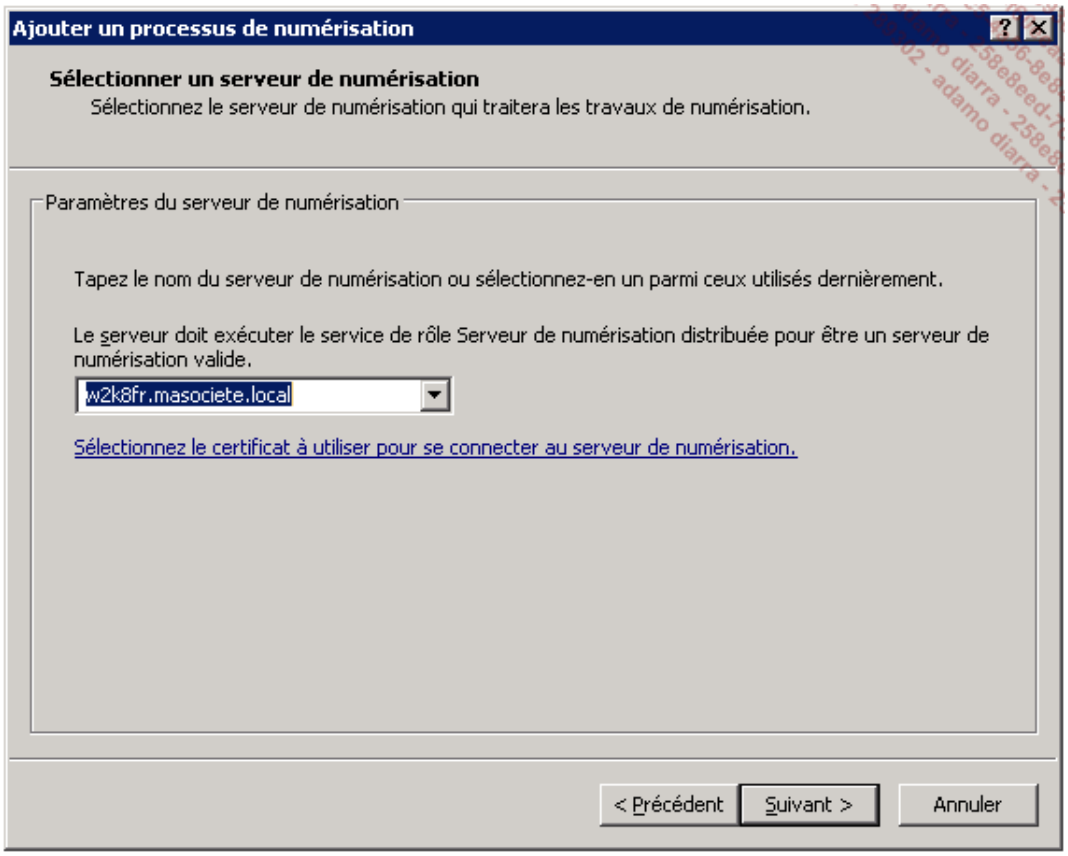


Voici un exemple d'opérations définies permettant de proposer les valeurs par défaut, l'utilisateur étant autorisé à modifier les choix sur la console du scanneur :



Choisissez ensuite le serveur de numérisation associé à ce processus.

© ENI Editions - All rights reserved - adamo diarra



© ENI Editions - All rights reserved - adamo diarra

Le BranchCache

Cette fonctionnalité qui apparaît dans Windows 2008 R2 permet d'optimiser l'accès aux ressources partagées hébergées sur des partages de fichiers ou des serveurs Web internes de type documentaire tels que SharePoint pour les sites distants.

La logique de fonctionnement correspond beaucoup à celle des Proxy Internet. C'est-à-dire que lors de la première récupération d'un document (fichier ou exécutable), celui-ci ne passe qu'une seule fois par la liaison lente. Pour tous les autres clients de ce document sur ce site, après une vérification des droits et de la non-modification du document, celui-ci est transmis directement par l'ordinateur présent sur le site qui dispose de la copie de ce document. L'économie est réalisée non seulement sur la bande passante de la liaison, mais aussi sur les temps d'accès aux documents et applications distantes qui deviennent très proches d'un accès local.

Cette option est aussi disponible sur les clients Windows 7 sous la forme d'un cache réparti entre les différentes machines.

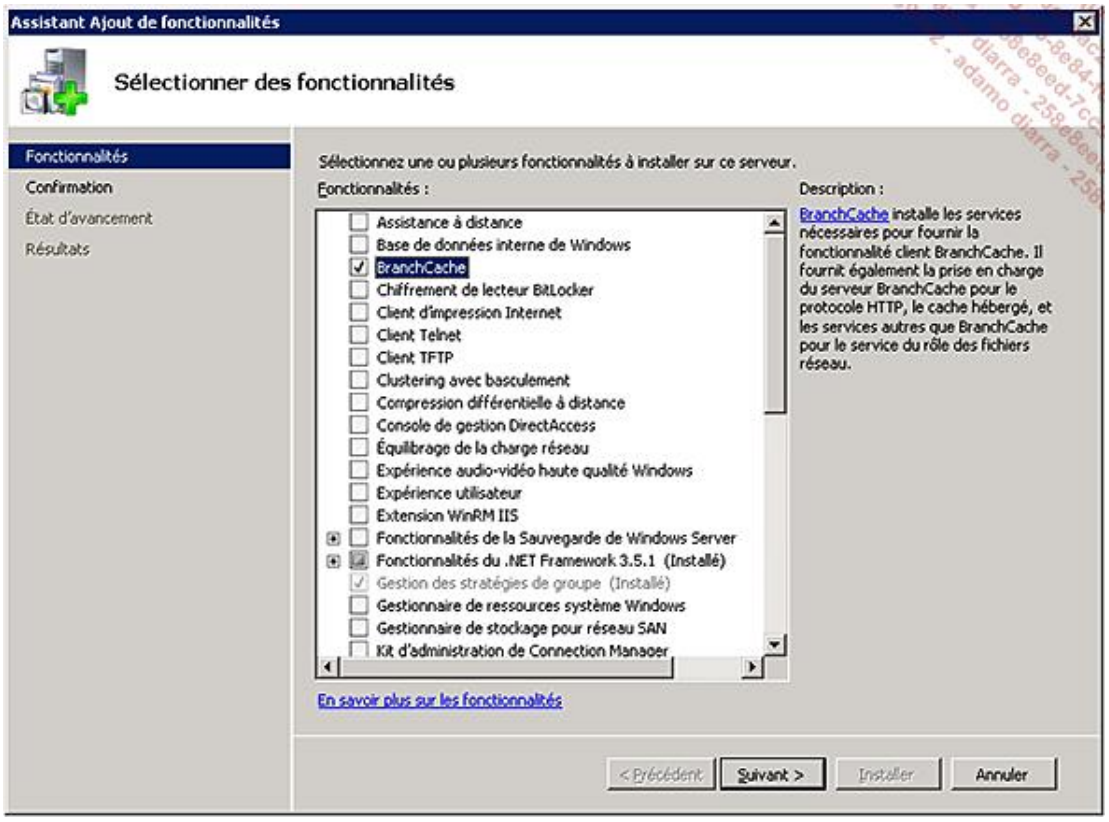
À noter que seuls Windows 7 et Windows Server 2008 R2 peuvent tirer parti du Branch Cache.

Attention, sur les serveurs de fichiers où l'on veut activer des partages utilisant le BranchCache, un service de rôle **BranchCache pour les fichiers réseaux** doit être ajouté.

---

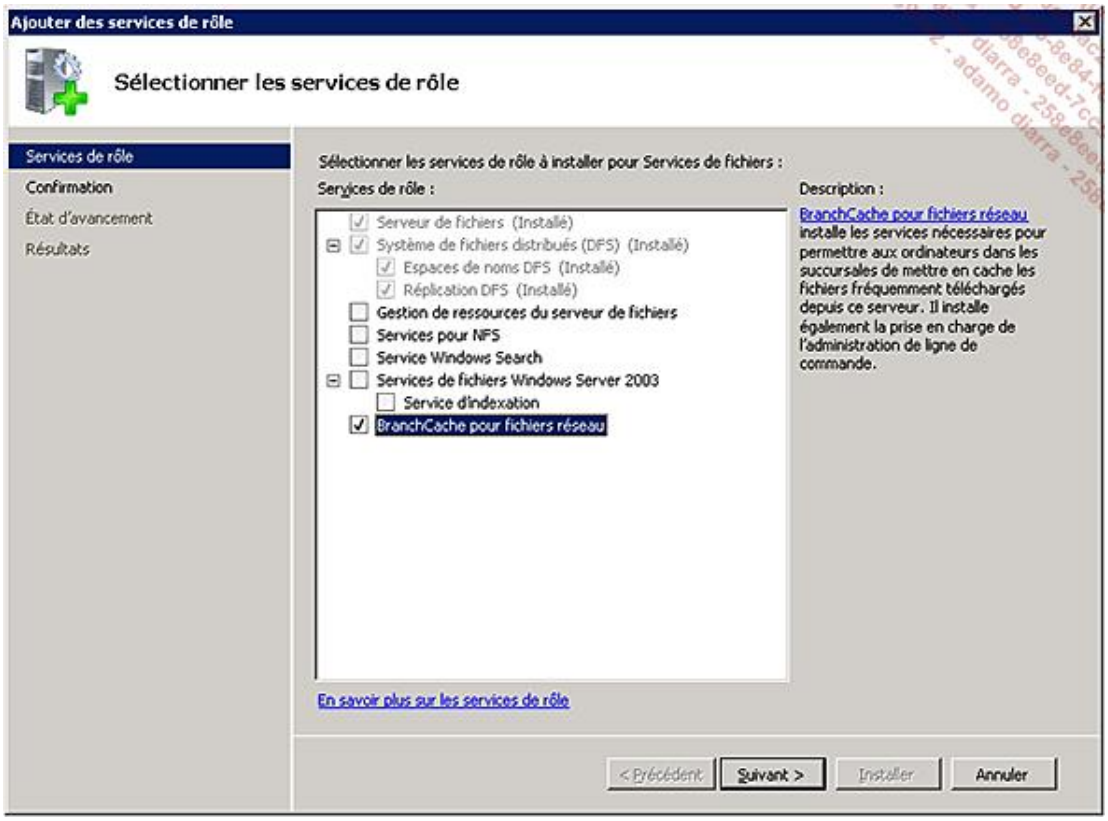
1. L'installation

La première étape consiste à installer la fonctionnalité sur chaque serveur partageant des ressources.

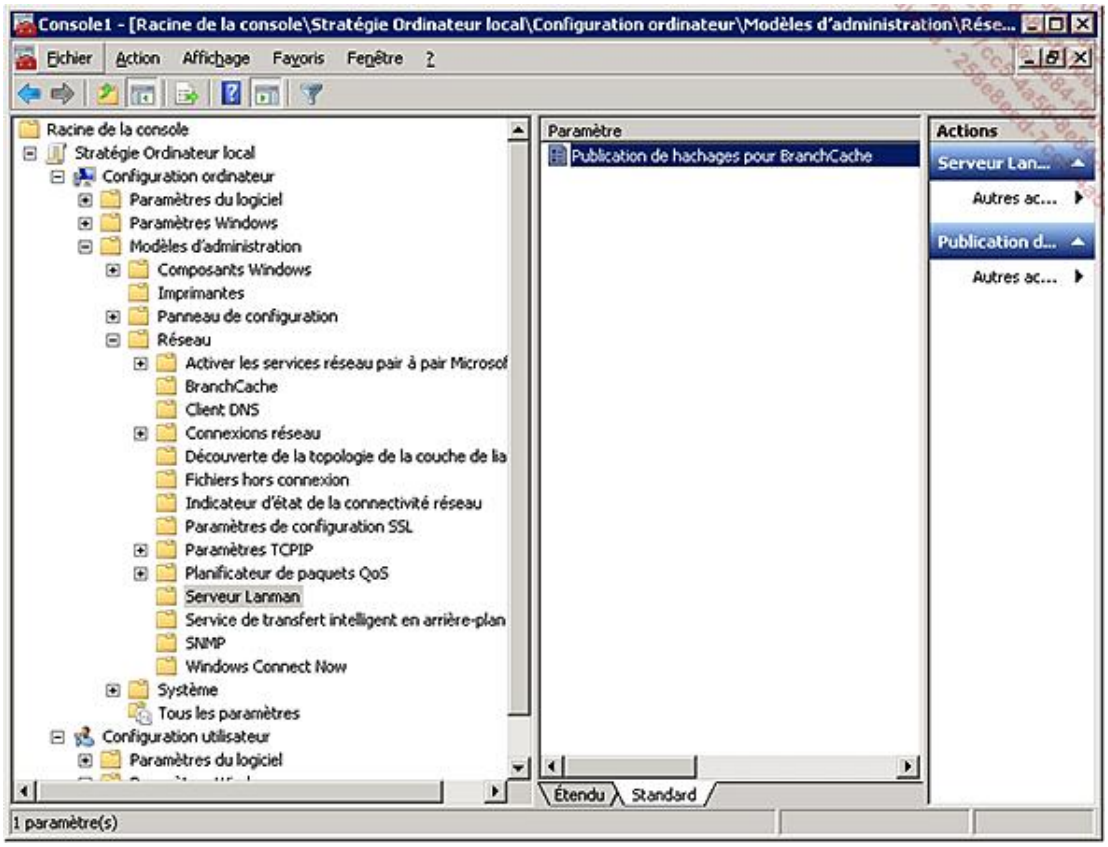


Le serveur est alors actif en tant que client et serveur du BranchCache pour les sites Web et client uniquement pour les serveurs de partages de fichiers. Il faut une étape supplémentaire pour que le cache sur les fichiers partagés puisse être activé.

© ENI Editions - All rights reserved - adamo diarra



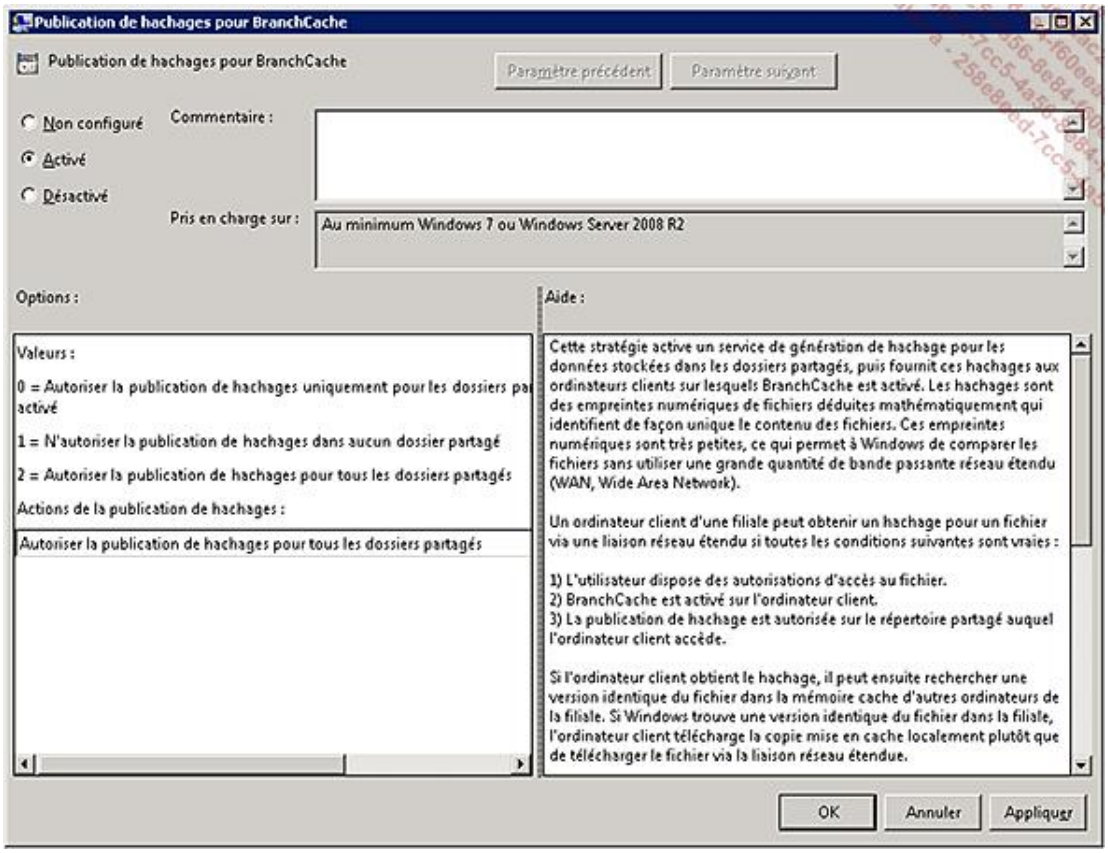
Le serveur est alors aussi actif en tant que serveur de BranchCache pour les fichiers.



Il faut ensuite activer une stratégie de groupe permettant au serveur d'utiliser des fonctions de codage de type Hash coding. Cette fonction permettra d'identifier chaque document de manière unique et de détecter ses modifications en se basant sur le hash unique généré pour chaque fichier.

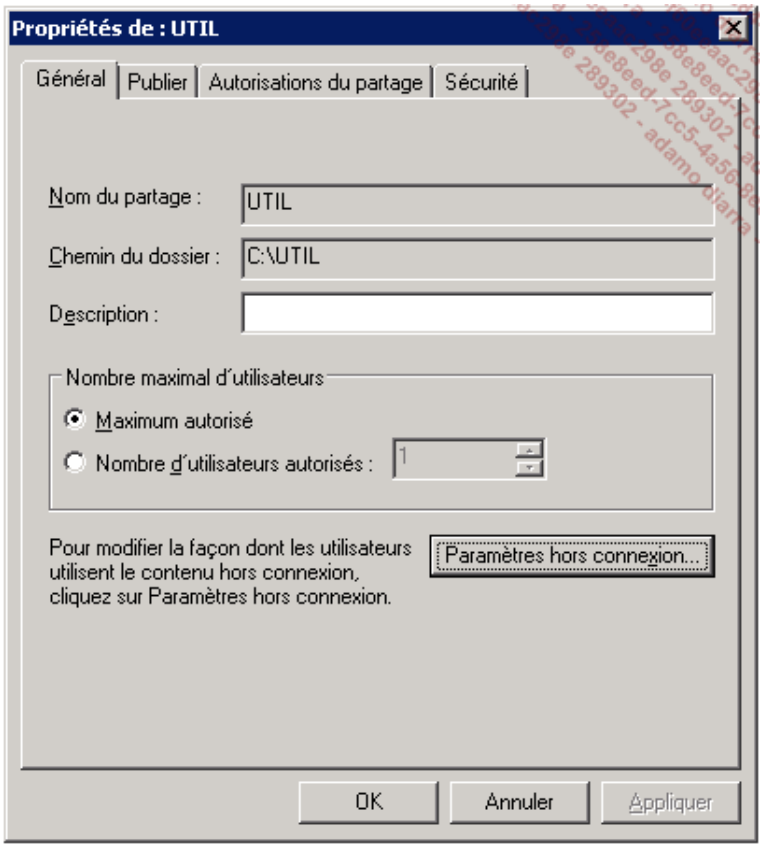
Cette option autorise l'activation du cache sur tous les partages. N'oubliez pas de forcer l'application de la stratégie.

© ENI Editions - All rights reserved - adamo diarra



2. La configuration des partages

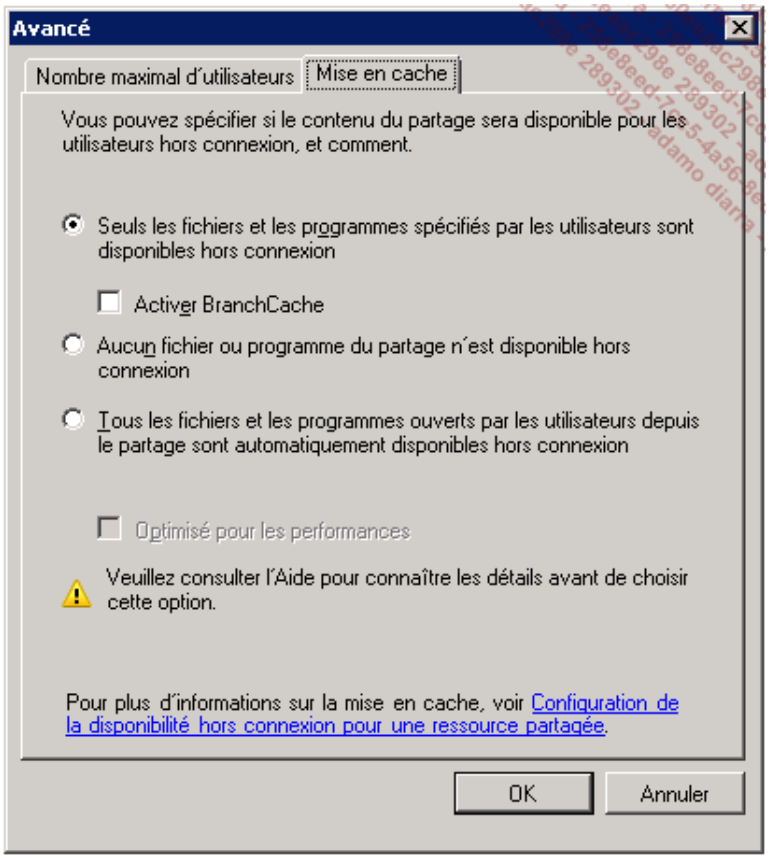
Sur chaque partage, l'option de cache est accessible à partir du bouton **Paramètres hors connexion**.



La configuration des partages peut se faire à partir de la console **Gestion de l'ordinateur - Dossiers partagés -**

© ENI Editions - All rights reserved - adamo diarra

Gestion des partages et du stockage ou tout simplement à partir du dossier lui-même, par l'onglet **Partage - partages avancés**, puis le bouton **Mise en cache**.

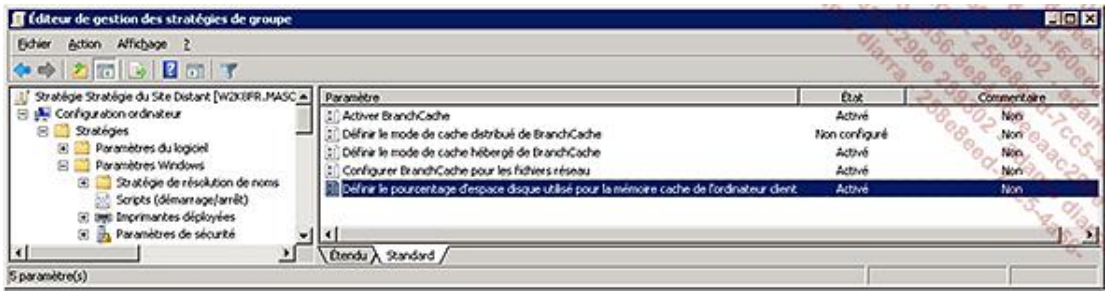


Attention, contrairement au mode **Hors Connexion classique**, les documents ou exécutables ne seront accessibles que si le partage et le document distant sont effectivement accessibles. En effet, avant de transmettre le document à l'utilisateur à partir du cache, il est nécessaire de vérifier que le fichier n'a pas été modifié et que les permissions autorisent toujours l'utilisateur à y accéder.

3. La configuration des clients

Le service **BranchCache** est installé par défaut sur les stations Windows 7, mais celui-ci devra être démarré pour que la stratégie soit efficace.

Voici la stratégie à définir pour configurer les clients :



- Le premier paramètre de la stratégie BranchCache permet d'activer l'utilisation du cache, mais ceci ne provoque pas le démarrage du service **BranchCache** qui sera donc placé en démarrage automatique sur les stations.

Son activation sera réalisée par stratégie, car deux modes sont proposés :

- Le mode **distribué** est utilisé quand aucun serveur n'est disponible sur le site.

  Dans ce mode, toutes les stations du site activées pour le BranchCache se partagent le cache et vérifient

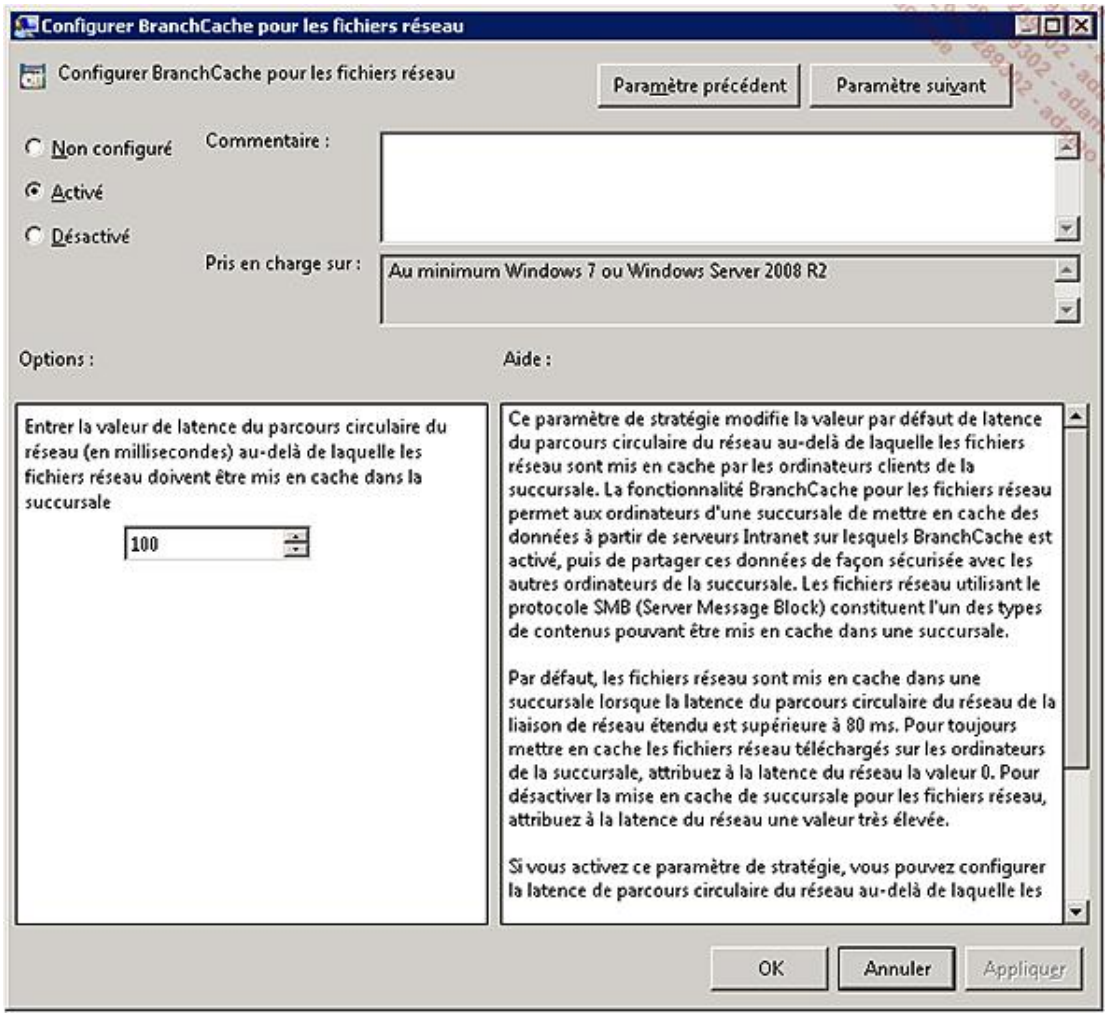
© ENI Editions - All rights reserved - adamo diarra

localement la présence du document recherché dans un des caches avant d'aller chercher le fichier sur le serveur du site central.

- Le mode **hébergé** est souvent préférable quand un serveur Windows 2008 R2 est présent sur le site distant.

  Dans ce mode, toutes les stations du site activées pour le BranchCache utilisent le serveur pour vérifier la présence du document et y mettre le document en cache si nécessaire.

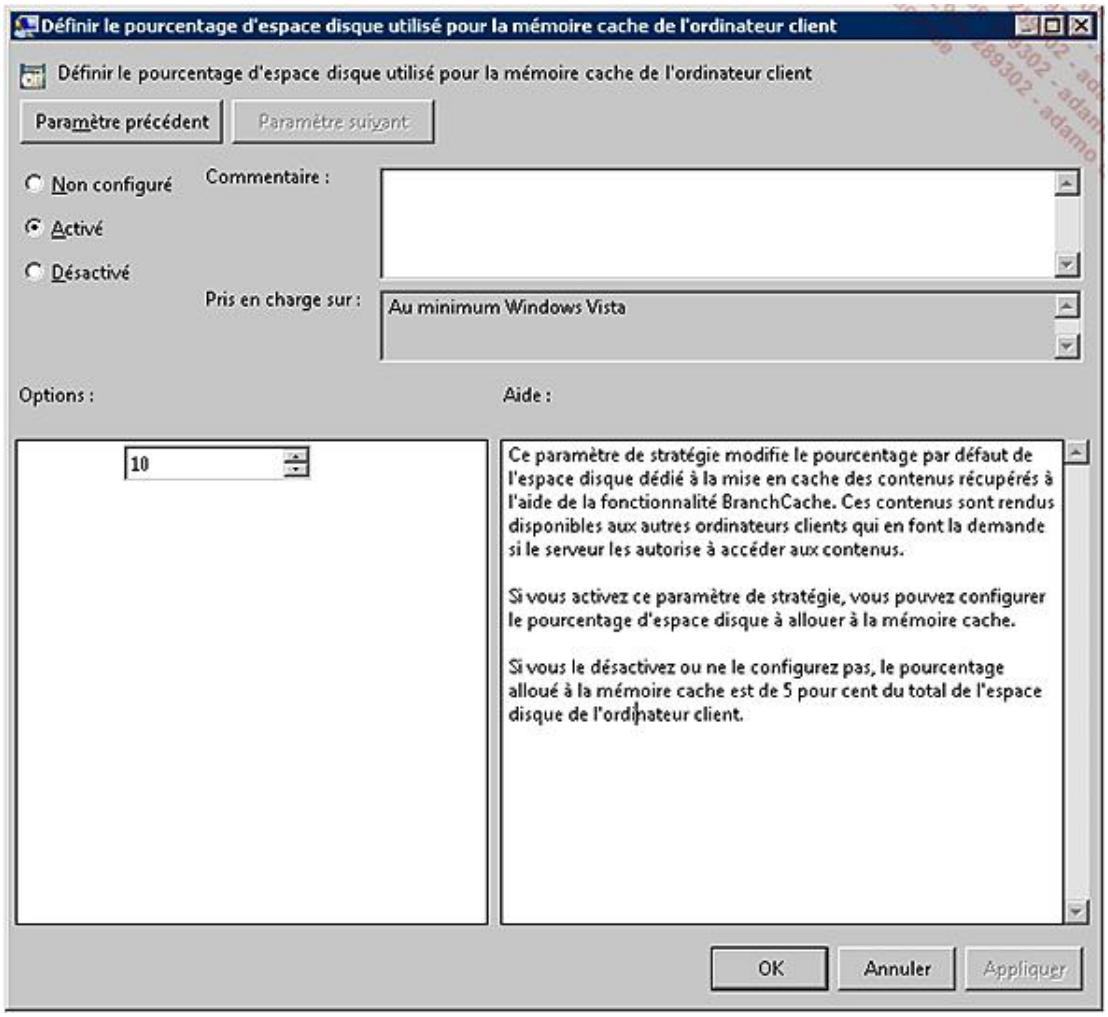
- L'activation du mode **BranchCache pour les fichiers réseaux** permet d'indiquer le délai au-delà duquel le fichier sera effectivement mis en cache.



La valeur 0 provoque la mise en cache de tous les fichiers.

Le dernier paramètre de la stratégie définit le pourcentage d'espace disque autorisé pour le cache sur les stations ou les serveurs définis pour le stockage des fichiers.

© ENI Editions - All rights reserved - adamo diarra



La valeur par défaut est de 5%.

Cette logique signifie qu'une stratégie spécifique sera préparée pour chaque site distant contenant soit un serveur, soit un cache réparti entre les différentes stations. À noter que le démarrage automatique du service peut être ajouté dans la même stratégie.

En conclusion, l'optimisation des sites distants reste une préoccupation importante pour Microsoft qui prévoit encore d'améliorer cette fonctionnalité dans la prochaine version de Windows. En effet, ce type de fonctionnalité permet d'envisager une centralisation beaucoup plus importante des ressources de type partages de fichiers et bases documentaires, tout en limitant le nombre de serveurs nécessaires pour maintenir l'ensemble et faciliter l'administration et la sauvegarde de l'ensemble des informations.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre est dédié à la haute disponibilité. L'objectif est de parcourir les possibilités offertes en terme de haute disponibilité par Windows Server 2008 R2. Augmenter la disponibilité des services offerts est un challenge permanent pour toutes les DSI.

Un ensemble de facteurs favorise cela :

- Homogénéiser les serveurs en passant par une installation et des paramètres identiques (voir le chapitre Déploiement des serveurs et postes de travail).
- Centraliser la configuration par GPO (voir le chapitre Domaine Active Directory).
- Sauvegarder et maintenir à jour les serveurs (voir le chapitre Cycle de vie de votre infrastructure).
- Répliquer les fichiers bureautiques (voir le chapitre Architecture distribuée d'accès aux ressources).
- Doubler les services d'infrastructure réseau (contrôleurs de domaines, serveurs DNS, DHCP...).
- Utiliser la version Core de Windows Server 2008 R2 pour limiter les temps d'arrêt dus à l'installation des mises à jour de sécurité.
- Virtualiser le service et héberger la machine virtuelle sur un cluster Hyper-V.

Une fois tous ces facteurs en œuvre, certains services critiques sont toujours dépendants d'un serveur unique qui tombera forcément en panne tôt ou tard, ou qu'il faudra redémarrer suite au Microsoft Patch Day. C'est là que la haute disponibilité entre en jeu, permettant de passer d'un service fortement disponible à un service hautement disponible. Elle vient bien en complément des facteurs ci-dessus.

Les serveurs participant à la haute disponibilité sont désignés comme nœuds du cluster, ce dernier désignant en retour l'ensemble des serveurs. Le cluster est prévu pour répondre à des besoins forts de disponibilité et ne doit pas être pris à la légère. Avant de décider si une solution de type cluster répond à ce besoin, certaines questions doivent être posées :

- Quel est le taux de disponibilité de la solution actuelle ?
- Quel est le taux de disponibilité souhaité/demandé ?
- Combien coûte le manque de disponibilité actuel ?
- En cas de panne, combien de temps faut-il pour restaurer le serveur ?
- Est-ce que la solution qui fournit le service est bien prévue pour fonctionner en cluster ?
- Est-ce qu'un seul serveur fournit toutes les ressources matérielles nécessaires, ou faut-il plusieurs serveurs actifs en même temps ?

© ENI Editions - All rights reserved - adamo diarra

Les choix d'architecture

1. Les différentes architectures

Derrière les termes de haute disponibilité se cachent deux types de solutions distinctes :

- La solution de type actif/passif.
- La solution de type actif/actif.

La première augmente la disponibilité en basculant les ressources d'un serveur à un autre en cas de problème (solution hautement disponible). La deuxième solution permet d'avoir plusieurs serveurs qui répondent aux demandes en même temps (répartition de charge) et qui peuvent tolérer la perte d'un membre (solution hautement disponible).

Les solutions de type actif/actif peuvent sembler de prime abord plus intéressantes, mais elles sont également encore plus complexes et doivent être envisagées pour répondre d'abord à un problème de répartition de charge. Dans un environnement Microsoft, les solutions sont les suivantes :

- Solution actif/passif : cluster à basculement (MSCS).
- Solution actif/actif : cluster NLB (*Network Load Balancing*).

Une application destinée aux utilisateurs doit être compatible avec une solution de haute disponibilité. En dehors des « grands » éditeurs de logiciels, il est courant qu'un éditeur n'ait jamais testé son application en environnement hautement disponible et ne puisse donc s'engager sur son bon fonctionnement. Au minimum, les points suivants sont à analyser :

- Est-ce que l'ensemble des données peut résider sur des volumes partagés et donc autres que C:\ ?
- Est-ce que certaines clés de registre doivent être répliquées entre les serveurs ?
- L'application utilise-t-elle un dongle ou une connexion physique qui ne peut pas être doublée ou connectée sur deux machines ?
- Est-ce que les clients peuvent utiliser un nom NetBIOS/DNS et une adresse IP différents de ceux de la machine physique (nom/IP virtuels) ?
- Quels sont les mécanismes pour détecter une panne de l'application et décider de basculer ?

Dans la solution actif/passif

Un seul serveur héberge une même ressource à un moment donné. Il n'a pas besoin de synchroniser les données métiers avec les autres serveurs (16 au maximum, 8 en édition itanium). S'il tombe en panne, un autre serveur démarrera l'application, qui aura accès aux mêmes volumes disque que le serveur précédent, devant juste gérer l'interruption brutale du service (journaux de transactions pour une base de données par exemple). Le stockage peut être un point de faille unique dans certains cas. Le stockage d'entreprise (SAN, ...) coûte cher et il est donc mutualisé entre les plates-formes. En échange, tous les éléments sont doublés, notamment les contrôleurs. Bien que tout soit mis en œuvre pour qu'une panne n'arrive jamais, cela reste possible. Un autre problème est la corruption du volume (LUN) hébergeant les données. Si une vérification de la partition s'impose (chkdsk), il faut prendre en compte l'indisponibilité pendant la durée de celle-ci (qui dépend du nombre de fichiers et non du volume).

Dans la solution actif/actif

N serveurs (32 au maximum) répondent aux requêtes simultanément. Les serveurs doivent pouvoir répondre à toutes les requêtes et donc avoir accès à l'ensemble des données permettant d'y répondre. L'utilisation la plus répandue concerne les fermes de serveurs Web. Tous les serveurs ont une copie des sites Web et les données sont stockées dans une base de données qui est hébergée en dehors de la ferme. La complexité concerne la session de l'utilisateur. Il peut avoir un panier (site commercial) et/ou être authentifié sur le site. Si le serveur qui a répondu à ses requêtes tombe en panne, un autre serveur doit pouvoir prendre la relève, de préférence sans renvoyer l'utilisateur sur la page d'accueil. La session de l'utilisateur doit donc être conservée à l'extérieur du serveur, par exemple dans une base de données. Cela implique que le site Web ait prévu ce type d'architecture et stocke bien la

© ENI Editions - All rights reserved - adamo diarra

session en dehors du serveur. Sur un site marchand très fréquenté, cette gestion de sessions a un impact important sur la consommation de ressources. Il est possible de faire fonctionner un cluster NLB en mode actif/passif, mais ce mode de fonctionnement est un usage atypique par rapport à la philosophie du produit.

Voici un tableau synthétisant les différences importantes entre les deux solutions :

	Avantages	**Inconvénients**
Cluster à basculement	Pas de synchronisation entre les serveurs. Conscience de l'état de l'application et des ressources.	Stockage externe mutualisé. Un seul serveur doit pouvoir gérer la charge (actif/passif par groupe de ressource).
Cluster NLB	Répartition de charge (actif/passif). Pas de stockage mutualisé.	Travaille seulement au niveau IP. Pascde conscience de l'état de l'application.

Notez que ces deux technologies ne sont pas supportées sur le même serveur, cf. l'article 235305 (Interoperability between MSCS and NLB) de la base de connaissances Microsoft.

2. La haute disponibilité, nirvana de votre infrastructure ?

Les promesses de la haute disponibilité ne seront tenues que si les équipes et les processus sont en cohérence avec le besoin auquel répond cette promesse. Alors que le coût de la solution est certain, il ne sera amorti que si elle permet effectivement de parer à des coupures de services. Le coût de la solution porte au moins sur les éléments suivants :

- Les investissements matériels (par exemple deux serveurs au lieu d'un).
- Encombrement, consommations électrique et climatique complémentaires.
- Le socle logiciel « infrastructure » (2 licences édition Entreprise pour le cluster à basculement, les agents de sauvegardes...).
- Certains éditeurs font payer deux fois le prix de la licence applicative, même en actif/passif.
- Complexification de la supervision et de la sauvegarde.
- Nécessité d'un stockage partagé externe là où des disques internes suffisaient.
- Charge en jour-homme pour appréhender cette technologie.
- Charge en jour-homme pour mettre en œuvre et surtout maintenir la solution.

Ces coûts s'entendent par environnement et doivent donc être reportés sur chaque environnement impacté (préproduction, qualification...). Le coût d'indisponibilité doit donc être supérieur à ces exemples de coûts.

Le danger consiste à considérer un cluster comme un serveur classique « amélioré ». Cette approche était souvent fatale dans les versions antérieures de Windows. Il suffisait qu'un administrateur supprime un partage de fichiers depuis l'explorateur au lieu de le faire par la console d'administration du cluster pour faire échouer cette ressource cluster et générer par défaut une bascule du cluster. Microsoft a fortement revu l'intégration de la couche cluster dans le système d'exploitation. Cette même erreur sur Windows Server 2008 R2 est gérée, le système supprimant en fait la ressource cluster directement sans générer d'incident. Il en résulte une forte diminution des incidents provoqués par des erreurs humaines dues à la méconnaissance des spécificités et une réduction de celles-ci.

La politique des éditeurs concernant les licences évolue, même si un décalage persiste. Par exemple, il n'est plus nécessaire d'acheter la version Entreprise de Microsoft SQL Server pour l'implémenter en cluster depuis la version 2005. En revanche, le même produit est toujours nécessaire en version Entreprise pour constituer une ferme cluster NLB de serveurs SSRS (*SQL Server Reporting Services*).

Un cluster NLB présente aussi des points à ne pas négliger. C'est un répartiteur de charge de niveau 3 (IP), qui n'a

© ENI Editions - All rights reserved - adamo diarra

donc pas conscience de l'état des applications pour lesquelles il répartit la charge. S'il s'agit de sites Web par exemple, l'arrêt de IIS ne fera pas sortir la machine du cluster. Vous aurez ainsi une partie des utilisateurs qui n'accèderont plus au site, notamment si l'affinité est active. Il vous incombe de mettre en place un mécanisme de vérification de l'applicatif, afin de sortir de la ferme un nœud défaillant. Le seul cas géré par cluster NLB est un problème de niveau 3 et inférieur. Par exemple, si le serveur perd l'accès au réseau, il sera automatiquement sorti de la ferme et les utilisateurs répartis sur les nœuds restants (convergence). Une exception est constituée par exemple par Microsoft ISA, qui pilote le cluster NLB et sort du cluster en cas de problème.

La technologie NLB propose plusieurs solutions pour créer l'adresse IP virtuelle, toutes ont des avantages et inconvénients. Certains commutateurs réseaux (Cisco, Enterasys...) nécessitent un paramétrage spécifique avant que cela fonctionne.

Un cluster NLB est constitué le plus souvent avec deux serveurs. Contrairement au mode actif/passif, on peut se retrouver dans une situation où l'absence d'un nœud n'est plus possible pour tenir la charge. L'aspect haute disponibilité n'est donc plus couvert, car la perte d'un nœud engendre une interruption de service ou du moins une trop grande dégradation. Il faut donc être très vigilant sur la charge que doit absorber la ferme afin de tolérer la perte d'un nœud. Ce phénomène est aussi possible avec un cluster à basculement, si les deux nœuds sont actifs en même temps sur des ressources différentes (actif/actif en mode croisé). Cette configuration n'est pas recommandée par Microsoft, qui propose plutôt un cluster à trois nœuds dans ce cas (actif/actif/passif). Le nœud passif est alors mutualisé pour les deux actifs.

© ENI Editions - All rights reserved - adamo diarra

La répartition de charge (Cluster NLB)

La répartition de charge devient indispensable quand un seul serveur ne suffit plus pour tenir la charge ou maintenir un temps de réponse acceptable. Si le besoin de disponibilité supplémentaire n'est pas un critère, il est conseillé d'ajouter d'abord des ressources matérielles au premier serveur avant d'envisager plusieurs serveurs.

La répartition de charge n'induit pas une capacité de charge linéaire. Si un serveur peut traiter 200 utilisateurs, deux serveurs ne permettront pas forcément de traiter 400 utilisateurs. Tout va dépendre de la nature de la charge et du comportement des sessions TCP générées. La notion d'affinité permet de conserver un utilisateur sur le même nœud tant que celui-ci fonctionne. De cette façon, on minimise le chargement des sessions utilisateurs sur les serveurs. Pour cela la ferme calcule un hash à partir de l'adresse IP du client et sa destination. Si tous les clients se présentent avec la même adresse IP (par exemple derrière un pare-feu avec du NAT), ils seront tous dirigés vers le même serveur, annulant ainsi la répartition de charge.

La répartition n'est pas faite en fonction de la charge des serveurs. Si quelques utilisateurs saturent à eux seuls un des nœuds, il recevra pour autant le même nombre d'utilisateurs que les autres nœuds. Si la charge entre vos nœuds n'est pas du tout uniforme, vous devrez développer une routine qui draine les nœuds au-delà d'une certaine charge.

1. Créer une ferme NLB

La création d'une ferme NLB est techniquement rapide. Il faut cependant décider de certains points au préalable :

- Le mode d'opération du cluster :
  - Monodiffusion (même adresse MAC sur tous les nœuds).
  - Multidiffusion (adresse MAC unique par nœud).
  - Multidiffusion IGMP (adresse MAC unique par nœud et inscription d'adresse IGMP).
- Le mode de filtrage :
  - Hôte multiple (répartition de charge).
  - Hôte unique (actif/passif).
  - Aucun (bloquer le trafic correspondant à la règle).
- Le mode d'affinité (hôte multiple uniquement) :
  - Aucune (envoi sur un nœud aléatoire).
  - Unique (maintien sur le même nœud par adresse IP cliente).
  - Réseau (maintien sur le même nœud par sous réseau entier).

Le choix du mode d'opération doit se faire en concertation avec les responsables du réseau :

- Le mode monodiffusion assigne la même adresse MAC sur tous les nœuds du cluster. Cela va à l'encontre des switches, qui mémorisent les adresses Mac par port, et pour lesquels enregistrer deux fois la même adresse MAC n'est pas possible. NLB mitige ce point en activant la clé « MaskSourceMAC ». Le paquet arrive avec comme adresse MAC de destination celle du cluster, mais le nœud répond avec la sienne. Le switch ne peut donc pas assigner l'adresse MAC au nœud qui répond et continue à envoyer les paquets sur tout le réseau (inondation). Ce comportement est « by design ». Si ce mode est impératif (il l'était avec Microsoft ISA au départ), plusieurs contournements existent. Il est possible de mettre un hub entre les serveurs du cluster et le switch. De cette façon, le switch ne voit l'adresse MAC du cluster que depuis un seul port (pas de « MaskSourceMac »), ce qui arrête l'inondation. Cela ne fait cependant pas parti des « meilleures pratiques ». L'utilisation d'un commutateur de niveau 3 (routeur) n'est pas possible car tous les nœuds partagent la même adresse IP et le routeur envoie les paquets en fonction de l'adresse IP. Les serveurs ne peuvent pas communiquer entre eux, car ils ont la même adresse MAC. Les paquets sont renvoyés au serveur sans même quitter la carte réseau.

© ENI Editions - All rights reserved - adamo diarra

- Le mode multidiffusion règle le problème de l'adresse MAC en ajoutant une adresse MAC de type multidiffusion et en empêchant les équipements réseaux de mémoriser l'adresse MAC du cluster. Le switch envoie les paquets à l'ensemble des ports, dont ceux des nœuds du cluster. On se trouve toujours avec une inondation du trafic sur tous les ports du réseau. Certains équipements (Cisco notamment) nécessitent de transformer partiellement le switch en hub par configuration, en lui indiquant de transférer systématiquement les paquets pour l'adresse MAC du cluster aux ports de tous les nœuds. Il est possible de limiter ce problème en isolant les serveurs derrière un routeur, sur un vlan dédié.

- Le mode multidiffusion IGMP se comporte comme le précédent, mais les nœuds s'enregistrent également sur une adresse IP IGMP de classe D (de 224.0.0.0 à 239.255.255.255). Cela impose que les équipements réseaux supportent la multidiffusion IGMP, mais permet de régler le plus élégamment possible les différents problèmes. Chaque nœud a sa propre adresse MAC, l'adresse IP de multidiffusion et seulement les nœuds reçoivent le trafic réseau du cluster.

Voici quelques articles en fonction des fabricants :

Cisco :
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a0080a07203.shtml.

Enterasys : http://www.enterasys.com/partners/microsoft/sa-nlb-tb.pdf.

Le mode de filtrage le plus intéressant est **hôte multiple**. Le mode **hôte unique** est de type actif/passif, avec le nœud qui a le plus petit ID actif. Le mode de filtrage **Aucun** permet quant à lui de bloquer le trafic sur certains ports, notamment pour protéger les nœuds.

En mode **hôte multiple**, trois choix d'affinité sont possibles :

- **Aucun** : à chaque connexion TCP d'un même client, celui-ci sera dirigé vers le nœud ayant le moins de clients. Ce mode assure la meilleure répartition possible, surtout lorsqu'il n'y a pas de spécificité cliente à maintenir (panier, session...).

- **Unique** : permet de maintenir un client (son adresse IP) sur le même nœud tant que la topologie de la ferme n'est pas modifiée (ajout/suppression de nœud). Chaque client doit avoir une adresse IP unique afin d'avoir une répartition efficace (pas de Nat, de proxy...).

- **Réseau** : se comporte comme le filtrage précédent, mais au lieu d'utiliser directement l'adresse IP du client, il calcule l'adresse du réseau. Si par exemple un client se connecte avec l'adresse IP 192.168.1.1, NLB le transformera en 192.168.1.0. Tous les clients appartenant à cette classe C iront sur le même nœud. Ce filtrage est pertinent lorsqu'il faut maintenir un ensemble de clients venant d'un même réseau sur un même nœud.

En complément, sur Windows Server 2008 R2, l'affinité unique peut survivre à un changement de topologie (convergence), contrairement aux versions précédentes où le client était redirigé sur un autre nœud. Si un client X est connecté sur un nœud A et qu'un nœud est ajouté ou supprimé du cluster, le cluster retiendra l'affinité et maintiendra cette affinité pendant X minutes. Le délai d'expiration, exprimé en minutes, commence dès que le client est inactif.

Si nécessaire, le cluster peut très bien avoir plusieurs adresses IP virtuelles. Cela est notamment nécessaire si vous hébergez plusieurs sites Web avec des certificats SSL. À moins d'avoir un certificat de type wildcards (*.masociete.local), chaque site devra avoir une IP dédiée pour les connexions SSL. Contrairement au protocole HTTP qui autorise les hôtes virtuels, le protocole SSL commence par négocier la sécurité avant toute chose, et cela passe par une validation de l'URL demandée par le client.

2. Configurer la ferme

La mise en œuvre consiste à :

- Installer la fonctionnalité équilibrage de charge.

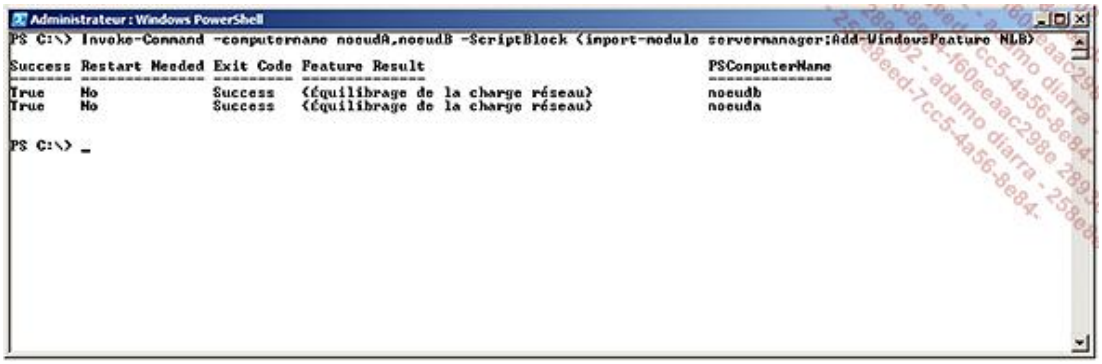
- Créer la ferme avec un nom et au moins une adresse IP sur au moins un nœud.

- Configurer les règles pour déterminer le trafic à équilibrer.

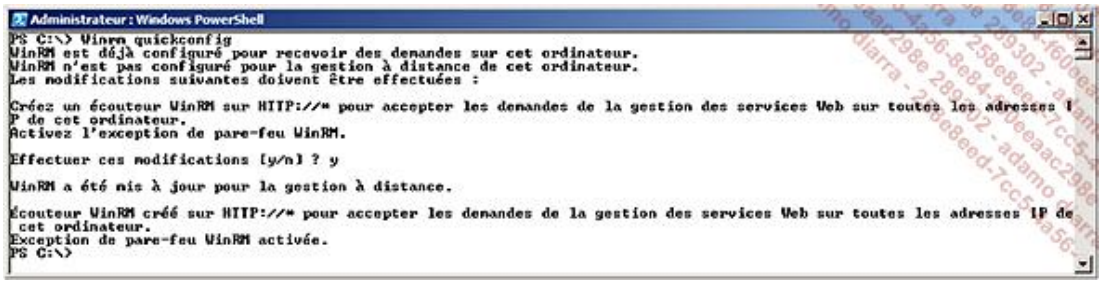
L'installation peut se faire par le **Gestionnaire de serveur** mais également via PowerShell. Windows Server 2008 R2 est fourni avec la version 2 de PowerShell, ce qui permet d'installer la fonctionnalité sur plusieurs nœuds en une commande :

© ENI Editions - All rights reserved - adamo diarra

```
Invoke-Command -computername noeudA,noeudB -ScriptBlock {import-module
servermanager;Add-WindowsFeature NLB}
```



WinRM doit être configuré au préalable avec la commande **winRM quickconfig** sur chaque nœud.



Vous pouvez créer la ferme NLB de deux façons :

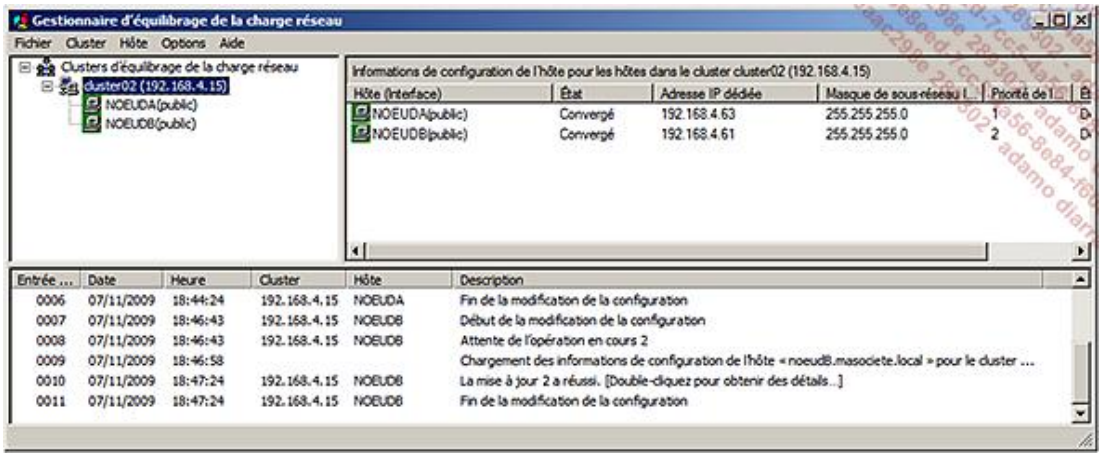
- Avec l'interface classique NLB.
- Avec PowerShell.

Windows Server 2008 R2 est la dernière version à proposer la console NLB telle qu'on la connaît. Suivant le schéma directeur de Microsoft, il faudra utiliser PowerShell dès la version suivante de Windows pour scripter la gestion de NLB et de la couche cluster. Comme pour d'autres produits (Exchange, SCVMM...), la console graphique servira juste à construire les commandes PowerShell à exécuter.

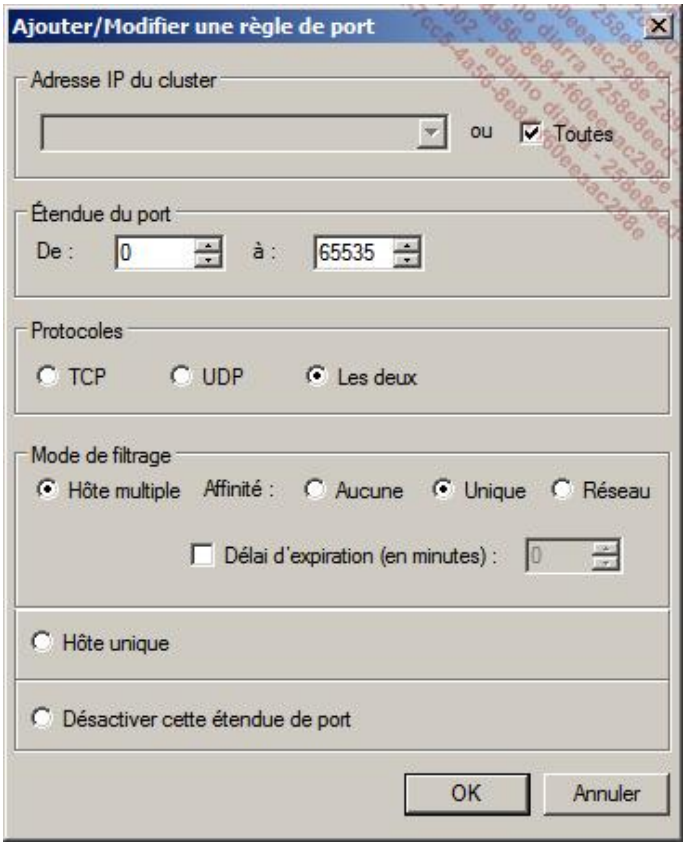
- Pour configurer la ferme avec l'interface graphique, cliquez sur **Démarrer**, puis **Outils d'administration**, puis sur le **Gestionnaire d'équilibrage de la charge réseau**.
- Cliquez ensuite sur **Cluster** et **Nouveau**.
- Choisissez un premier nœud à configurer, ainsi qu'une interface. Définissez sa priorité, son interface de gestion et son statut par défaut.
- Ajoutez ensuite au moins une adresse IP utilisée par la ferme.
- Déterminez l'adresse IP principale du cluster ainsi que le nom du cluster.
- Étape critique, choisissez le mode d'opération du cluster (monodiffusion, multidiffusion avec ou sans IGMP). Par défaut, tous les ports sont en équilibrage de charge, avec une affinité de type unique.

À ce stade, la ferme est créée avec un seul serveur comme membre. L'ajout du second nœud se fait depuis le menu **Cluster - Ajouter un hôte** :

© ENI Editions - All rights reserved - adamo diarra



L'interface de gestion des règles permet de choisir l'adresse IP du cluster où elle s'applique, un port ou une plage de ports, la nature (TCP, UDP) et le mode de filtrage :



Voici l'équivalent en PowerShell :

```
#Création du cluster sur le premier noeud
New-NlbCluster -InterfaceName public -ClusterName cluster02 -ClusterPrimaryIP
192.168.4.15 -
SubnetMask 255.255.255.0

#Ajout du second noeud
Get-NlbCluster | Add-NlbClusterNode -NewNodeName noeudB -NewNodeInterface
public
```

3. Exemple : ferme Web IIS

Une ferme de serveurs Web constitue l'usage type de NLB. IIS 7 a introduit la notion de configuration partagée, qui facilite la gestion de la ferme en centralisant la configuration IIS de tous les serveurs Web sur un partage de fichiers UNC. L'article TechNet suivant décrit sa mise en œuvre : http://technet.microsoft.com/en-us/library/cc771871

© ENI Editions - All rights reserved - adamo diarra

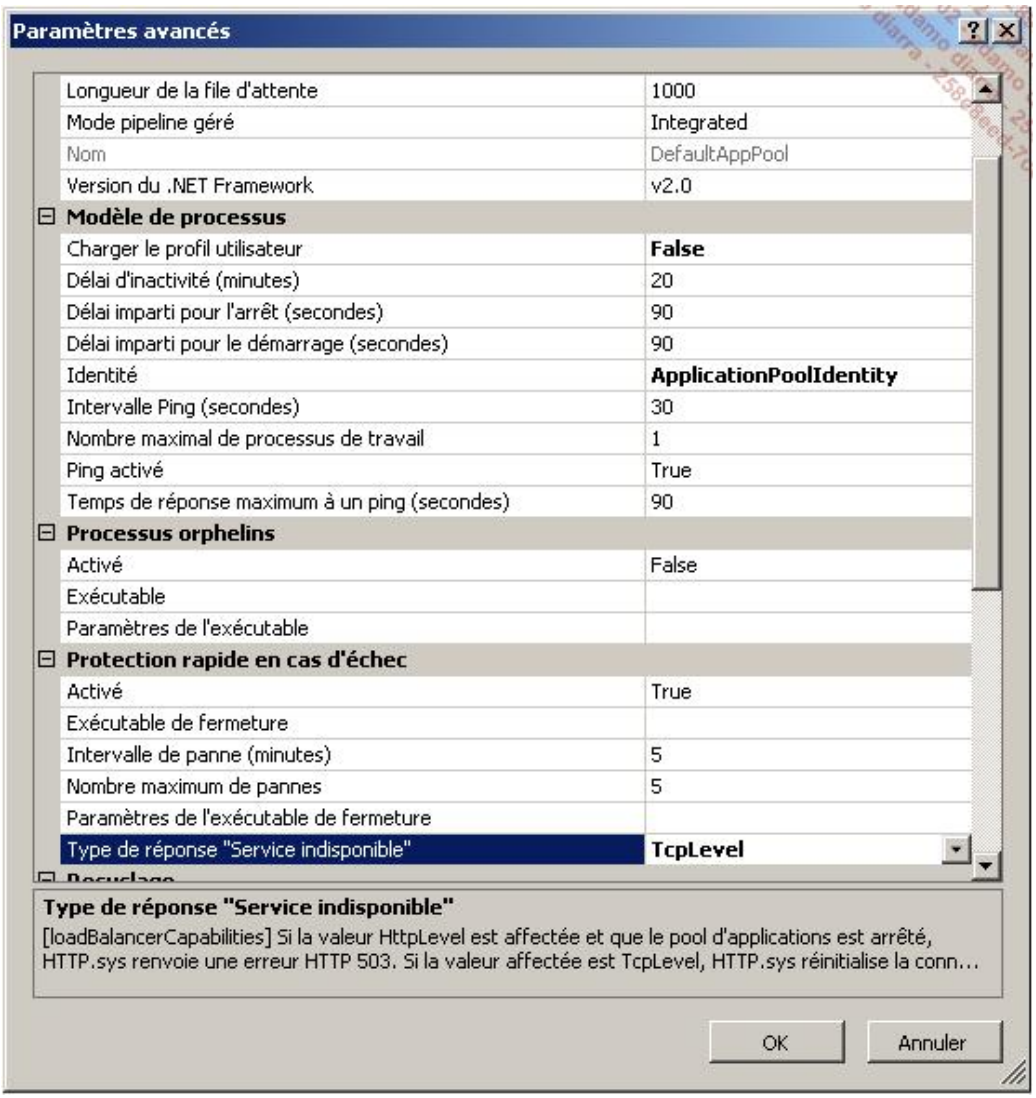
(WS.10).aspx.

Les étapes sont les suivantes :

- Installer le rôle Serveur Web (Web-Server).
- Créer au moins un cluster NLB avec deux nœuds.
- Modifier la règle par défaut, afin d'équilibrer uniquement les ports TCP 80 (**HTTP**) et 443 (**HTTPS**).

À ce stade, vous avez une ferme constituée de 2 serveurs Web avec une affinité unique. Vous savez déjà que NLB n'a pas conscience de l'état de l'application qui est répartie. En revanche, vous pouvez modifier le comportement de IIS afin qu'il prenne en compte NLB et modifie son comportement en cas de problème. Par défaut, IIS renvoie un code HTTP 503 en cas de défaillance du pool d'application. Dans le cas d'une ferme de serveurs, il est fort probable que seul ce serveur a ce problème. En indiquant au pool d'applications de faire une réponse de niveau TCP, il va fermer la connexion du client, qui sera alors redirigé vers un autre nœud de la ferme.

Pour modifier ce comportement, il faut aller dans les paramètres avancés du pool de l'application :



© ENI Editions - All rights reserved - adamo diarra

Le cluster à basculement

La technologie de cluster à basculement a une approche très différente de NLB. L'objectif est de maintenir des ressources en ligne en permanence. Chaque ressource est instanciée sur un seul serveur à la fois, mais plusieurs serveurs peuvent être actifs en même temps sur des ressources différentes. Afin de garantir le bon fonctionnement, la couche cluster vérifie un ensemble de points :

- Est-ce que l'adresse IP et le nom virtuel fonctionnent ?
- Est-ce que l'accès au stockage fonctionne ?
- Est-ce que le nœud peut communiquer avec les autres nœuds (pas d'isolation) ?
- Est-ce que les services à maintenir en ligne sont fonctionnels ?

Si un incident est détecté sur un de ces points, le cluster bascule l'ensemble des ressources nécessaires au(x) service (s) sur un autre nœud.

Au minimum, un cluster possède au moins un groupe (le « groupe cluster ») qui contient :

- Une adresse IP virtuelle.
- Un nom virtuel.
- Potentiellement un volume faisant office de quorum, ou un partage de fichiers témoin.

En cas de problème réseau, le cluster doit déterminer quels nœuds sont en état de fonctionner et quels nœuds doivent être retirés du cluster (et les ressources qu'ils hébergent basculées). Les nœuds qui sont majoritaires restent en ligne. Quatre modes de fonctionnement sont proposés afin de déterminer cela :

- **Nœud majoritaire** : le nœud qui communique avec le plus grand nombre d'autres nœuds gagne. Ce mode ne fonctionne qu'avec un nombre impair de nœuds.
- **Nœud et disque majoritaire** : chaque nœud a une voix, ainsi que le disque quorum. Le nœud qui a le plus grand nombre de voix gagne. Non recommandé pour une configuration multisite (stockage répliqué).
- **Nœud et partage de fichiers** : identique au précédent mais utilise un partage de fichiers externe au cluster au lieu du disque quorum.
- **Disque uniquement** : un seul nœud peut posséder ce volume à un instant donné et récupère l'ensemble des ressources. Cette solution correspond au fonctionnement d'un cluster Windows Server 2000/2003. Ce n'est plus le mode recommandé, surtout dans le cas des clusters multisites (stockage répliqué). Ne tolère pas la perte du disque quorum (point de faille unique).

Chaque ressource mise en cluster (instance SQL, partage de fichiers, Exchange...) a un ou plusieurs groupes contenant un ensemble de ressources dédiées à son fonctionnement.

Afin de définir un service ou une application, les choix suivants sont possibles :

- Application générique
- Service Windows
- DTC (*Distributed Transaction Coordinator*)
- Ordinateur virtuel (machine virtuelle Hyper-V)
- Message Queuing
- Serveur d'espace de nom DFS

© ENI Editions - All rights reserved - adamo diarra

- Serveur d'impression
- Serveur de fichiers
- Serveur DHCP
- Serveur iSNS (*Internet Server Name Service*)
- Serveur WINS
- Autre serveur
- Service Broker pour les services Bureau à distance
- Un script générique. Ce dernier vous permet d'utiliser un script afin de faire des vérifications spécifiques pour déterminer l'état de la ressource et décider ou non de basculer le cluster.

Une fois le groupe créé, les ressources suivantes peuvent être ajoutées :

- Application générique
- Point d'accès client (un nom et une adresse IP virtuelle)
- Script générique
- Service générique
- Adresse de tunnel IPv6
- Adresse IP (IPv4 ou IPv6)
- Coordinateur de transactions distribuées
- Partage NFS
- Service DHCP, WINS
- Spouleur d'impression
- Un dossier partagé

En fonction du type de ressource, certains paramètres sont ou non disponibles. Les paramètres suivants sont communs à toutes les ressources :

- **Dépendances** : quelles sont les autres ressources nécessaires qui doivent être opérationnelles pour que cette ressource fonctionne ? Cela permet également de déterminer dans quel ordre les ressources doivent être démarrées. Si une dépendance devient défaillante, les ressources qui en dépendent seront arrêtées. Il est possible d'utiliser les opérateurs logiques « ET » et « OU ». Ce dernier permet d'assouplir les dépendances, quand deux ressources remplissent le même rôle. C'est notamment le cas avec un cluster ayant des nœuds sur deux sous-réseaux différents. Deux ressources de type adresse IP existent (une pour chaque réseau), mais une seule est en ligne à un instant T. L'opérateur logique « OU » permet de ne satisfaire qu'une des deux dépendances.

- **Affecter le groupe** : ce paramètre est actif par défaut. Si une ressource au sein du groupe échoue, tout le groupe bascule sur un autre nœud. Si cette ressource n'est pas indispensable immédiatement au fonctionnement, il peut être judicieux de ne pas affecter le groupe. Les solutions de sauvegardes créent généralement une ressource dans le cluster. Si un problème se produit (crash ou mauvaise action dans la

© ENI Editions - All rights reserved - adamo diarra

solution de sauvegarde), tout le groupe va basculer. Une solution de supervision adéquate permet d'alerter sur l'échec de cette ressource et de laisser le temps de réparer avant que la plage de sauvegarde commence. Vous évitez ainsi de perturber la disponibilité du cluster de façon imprévue et non indispensable.

- **Intervalle de vérifications** : intervalle entre deux vérifications sur la santé de la ressource. Il peut être nécessaire d'augmenter le temps par défaut sur des serveurs très occupés.

Dans les versions antérieures de Windows Server, il était nécessaire d'avoir un réseau privé, dédié à la communication inter-nœuds, appelé « heartbeat ». Windows Server 2008 R2 offre une plus grande souplesse et n'impose plus cela. Le principal est de n'avoir aucun point de faille unique et donc au moins deux chemins réseaux entre les nœuds. Si vous utilisez du iSCSI, les cartes réseaux doivent y être dédiées et la communication inter-nœuds bloquée. Si vous utilisez un réseau dédié à la sauvegarde, c'est également une bonne idée de l'interdire au cluster. Le blocage se gère depuis les propriétés des réseaux, sur le **gestionnaire du cluster de basculement**.

Il est assez courant qu'une application stocke certains paramètres en base de registre. Si nécessaire, le cluster peut répliquer une arborescence de la base de registre, du moment qu'elle se situe sous HKEY_LOCAL_MACHINE. Ce paramétrage peut être rattaché soit à un service Windows soit à une application.

1. Migration de Windows Server 2003 à 2008 R2

Bien que ce livre soit orienté sur Windows Server 2008 R2, il y a quelques considérations à prendre en compte si vous souhaitez migrer un cluster depuis une édition antérieure vers Windows Server 2008 R2 (ou Windows 2008) :

- 2008 R2 existe uniquement en 64 bits. Cela implique que le matériel et toutes les applications du cluster doivent fonctionner en 64 bits ou au moins avec l'émulation 32 bits WoW64 (*Windows On Windows*).

- La fonctionnalité **Partager les sous-dossiers** n'est plus disponible. Il faudra créer chaque partage. Cela avait été mis en place à cause d'une limite technique à 900 partages. Dans la mesure où ce n'est plus le cas, cette fonctionnalité a été supprimée.

- DFS et FRS ne sont pas supportés sur 2008 R2 (à l'exception des contrôleurs de domaine). Vous devez migrer sur DFSR au préalable. Cela implique que les autres nœuds DFS soient au moins en Windows Server 2003 R2.

- Est-ce que vous utilisez bien des noms virtuels et des adresses IP autres que ceux du groupe cluster pour vos ressources ? Si ce n'est pas le cas, la migration impliquera une coupure plus longue, car les deux clusters (l'ancien et le nouveau) doivent cohabiter pendant la migration.

Deux approches de migration sont possibles :

- Conserver le même matériel.

- Migrer le cluster vers un nouveau cluster physique.

La première approche consiste à :

- Sortir un nœud du cluster (voir l'article de connaissance Microsoft 935197).

- Le mettre à jour en Windows Server 2008 R2 ou installer de nouveau tout le système d'exploitation.

- Créer un nouveau cluster sur ce serveur.

- Utiliser l'**assistant de migration d'un cluster**.

- Mettre en ligne les ressources migrées.

- Sortir le nœud 2003 de l'ancien cluster et le mettre à jour.

La deuxième approche est souvent utilisée, car le changement de système d'exploitation va souvent de pair avec un changement de génération de matériel. Le plan est très similaire, si ce n'est que l'ancien cluster n'est pas dégradé (en nombre de nœuds) pendant la migration :

© ENI Editions - All rights reserved - adamo diarra

- Installer un cluster Windows Server 2008 R2 sur au moins deux nœuds (nouveau cluster).
- Utiliser l'**assistant de migration d'un cluster**.
- Vous pouvez choisir d'utiliser le même stockage ou pas.
- Mettre en ligne les ressources migrées.
- Supprimer l'ancien cluster.

2. Validation de votre cluster

Dans les versions précédentes de Windows Server, le matériel devait être certifié pour fonctionner avec le cluster Microsoft. Le cas échéant, le support Microsoft ne pouvait pas être engagé. Depuis Windows Server 2008, ce processus est maintenant très simple. Pour être dans une configuration supportée par Microsoft, il suffit que :

- Le matériel porte le logo « certifié pour Windows Server 2008 R2 ».
- L'installation soit validée par l'**assistant Validation d'une configuration**.

L'assistant effectue un ensemble de vérifications portant sur les domaines suivants :

- Configuration du cluster
- Configuration du système
- Inventaire
- Réseau
- Stockage

Deux exceptions existent concernant l'assistant de validation. Les configurations suivantes n'ont pas à passer le test concernant le stockage :

- Exchange en mode CCR (*Cluster Continuous Replication*). Le cluster n'a pas de stockage partagé, car il est répliqué par CCR. Le test ne peut donc être concluant (http://technet.microsoft.com/en-us/library/bb676379.aspx).
- Les clusters utilisant un stockage répliqué. Les deux nœuds ont accès à l'ensemble des volumes, y compris le quorum (http://technet.microsoft.com/en-us/library/cc732035(WS.10).aspx#BKMK_multi_site).

Le test sur le stockage est le seul qui pourrait interrompre la disponibilité. Une fois le cluster en production, vous pouvez utiliser une LUN temporaire pour passer les tests sur le stockage dans certains cas, au lieu d'un test complet.

Cet assistant a pour objectif de valider un cluster avant sa mise en production, mais aussi après chaque changement significatif apporté au cluster, comme :

- La mise à jour de firmware ou des pilotes.
- L'ajout ou la suppression d'un nœud dans le cluster.
- Le changement de matériel sur le stockage.

À l'adresse ci-après sont référencés les tests à rejouer en fonction des modifications apportées au cluster : http://technet.microsoft.com/en-us/library/cc732035(WS.10).aspx#BKMK_validation_scenarios.

© ENI Editions - All rights reserved - adamo diarra

3. Mise en œuvre du cluster

La mise en œuvre d'un cluster comprend plusieurs étapes :

- Installer la fonctionnalité cluster à basculement.
- Configurer le cluster :
    - Interface réseau
    - Déterminer la majorité (quorum, partage témoin...)
- En fonction de son objectif, installer le rôle sur tous les nœuds (serveur de fichiers...).
- Créer l'application dans le cluster.
- Basculer sur chacun des nœuds pour valider le bon fonctionnement.
- Passer encore une fois l'assistant de validation d'un cluster.

L'installation de la fonctionnalité cluster peut se faire de plusieurs façons :

- Depuis le **Gestionnaire de serveur**.
- En ligne de commande : `servermanagercmd -i Failover-Clustering`
- Depuis PowerShell :

```
import-module servermanager
Add-WindowsFeature Failover-Clustering
```

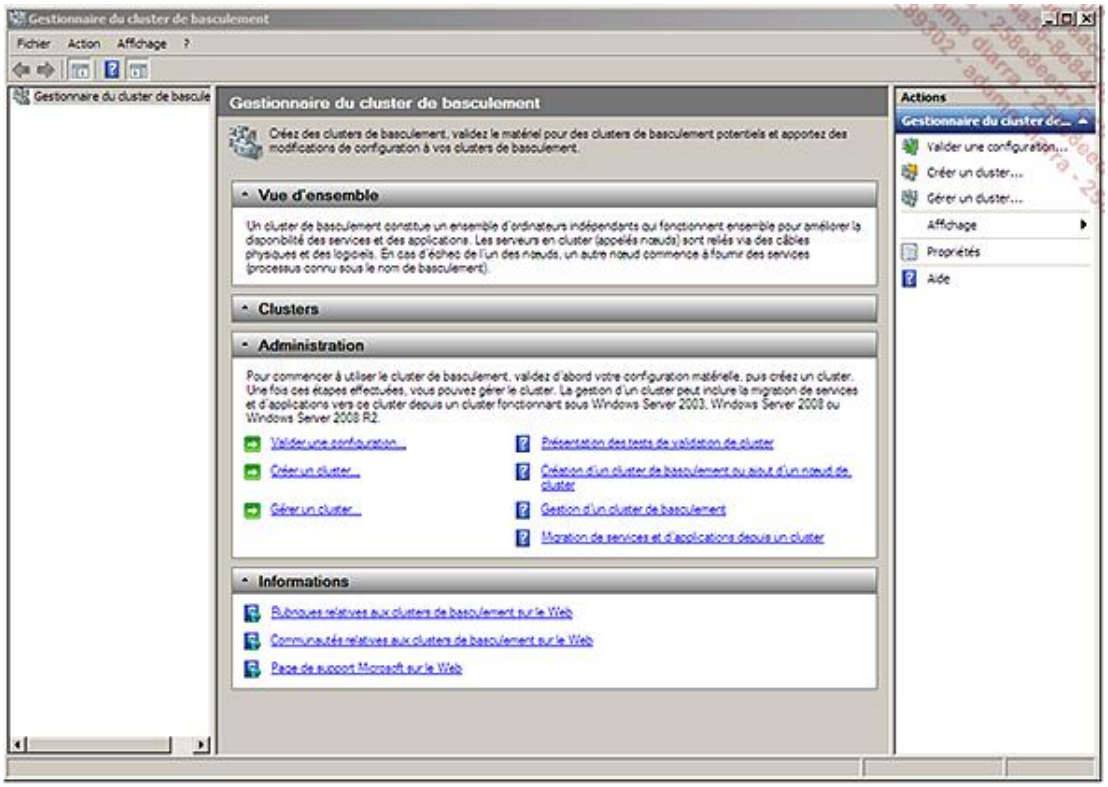
La configuration peut se faire également par plusieurs moyens :

- L'interface graphique : **Gestionnaire du cluster de basculement**.
- Depuis la ligne de commande : **cluster.exe**. Investir sur cette méthode est déconseillé car Windows Server 2008 R2 est la dernière version qui le propose.
- Depuis PowerShell.

Dans cet ouvrage, nous allons couvrir la première et la dernière méthode pour la configuration d'un cluster. Voici les étapes de configuration avec l'interface graphique.

- Lancez le **Gestionnaire du cluster de basculement**.

© ENI Editions - All rights reserved - adamo diarra



- Cliquez sur **Valider une configuration** dans le panneau **Actions**.

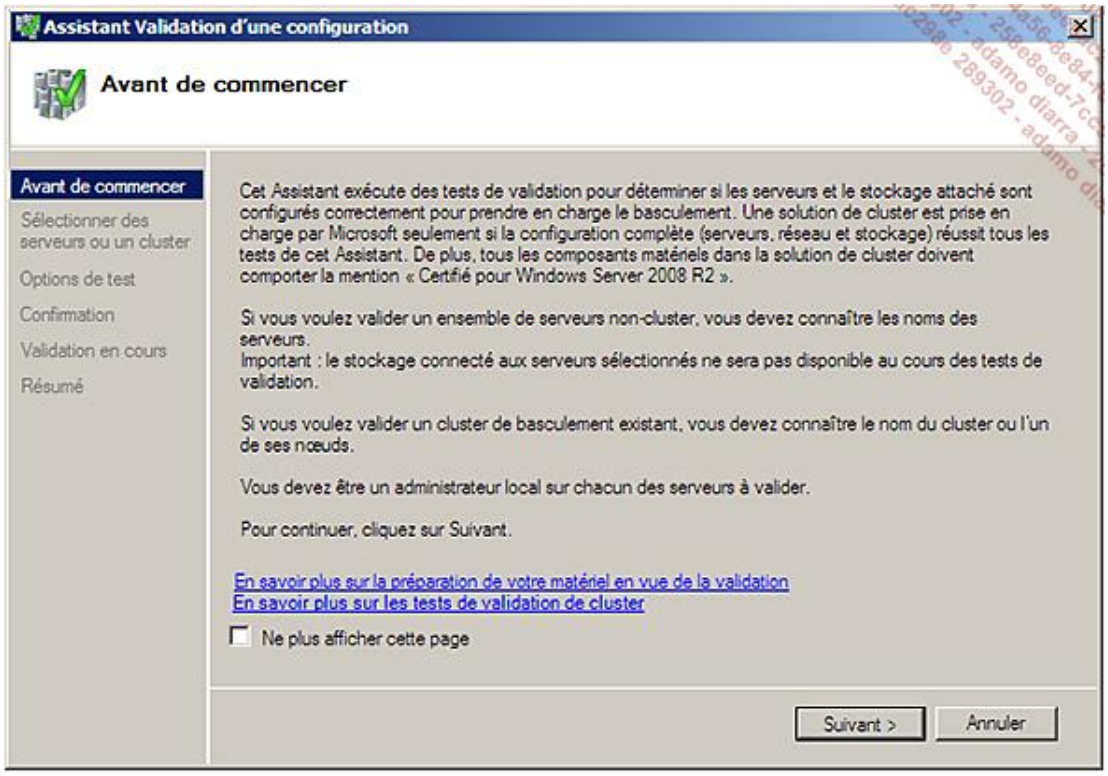
- Le message d'accueil qui suit vous rappelle trois éléments importants :

  - Même si votre installation passe la validation, il faut tout de même que le matériel porte la mention « pour Windows Server 2008 R2 ».

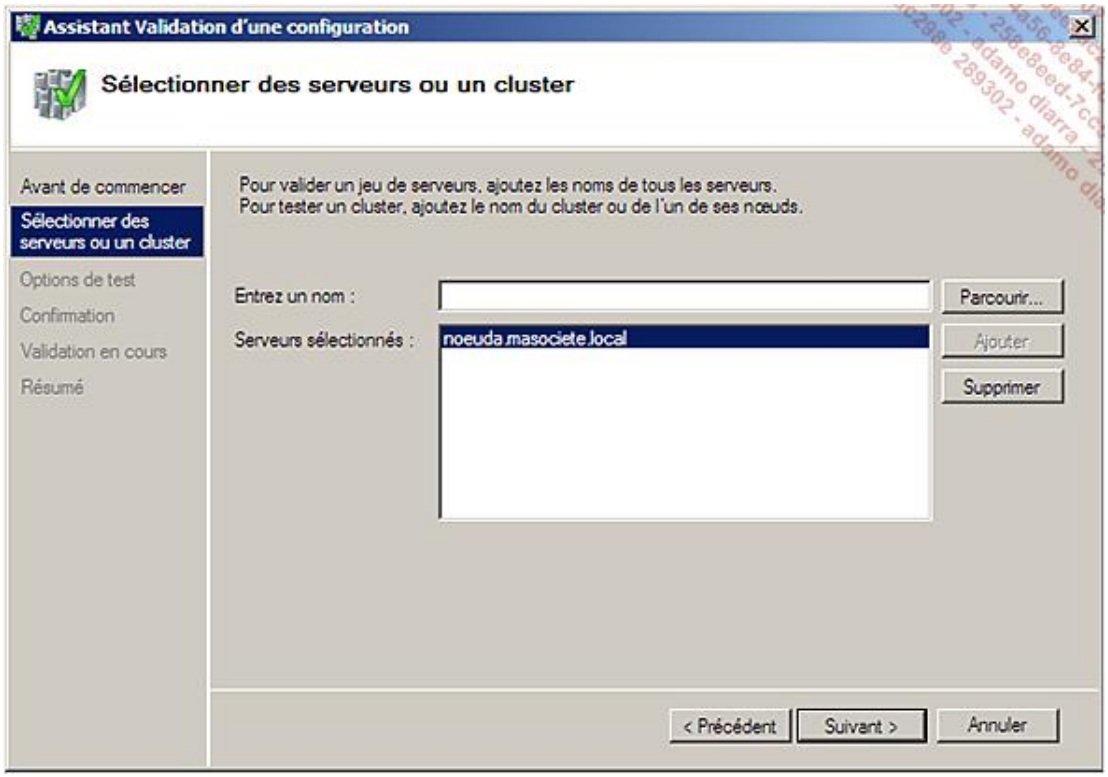
  - Il faut être au moins administrateur local de chacun des nœuds.

  - La validation est disruptive si vous faites soit tous les tests (qui incluent le stockage), soit un test personnalisé en sélectionnant le stockage.

© ENI Editions - All rights reserved - adamo diarra

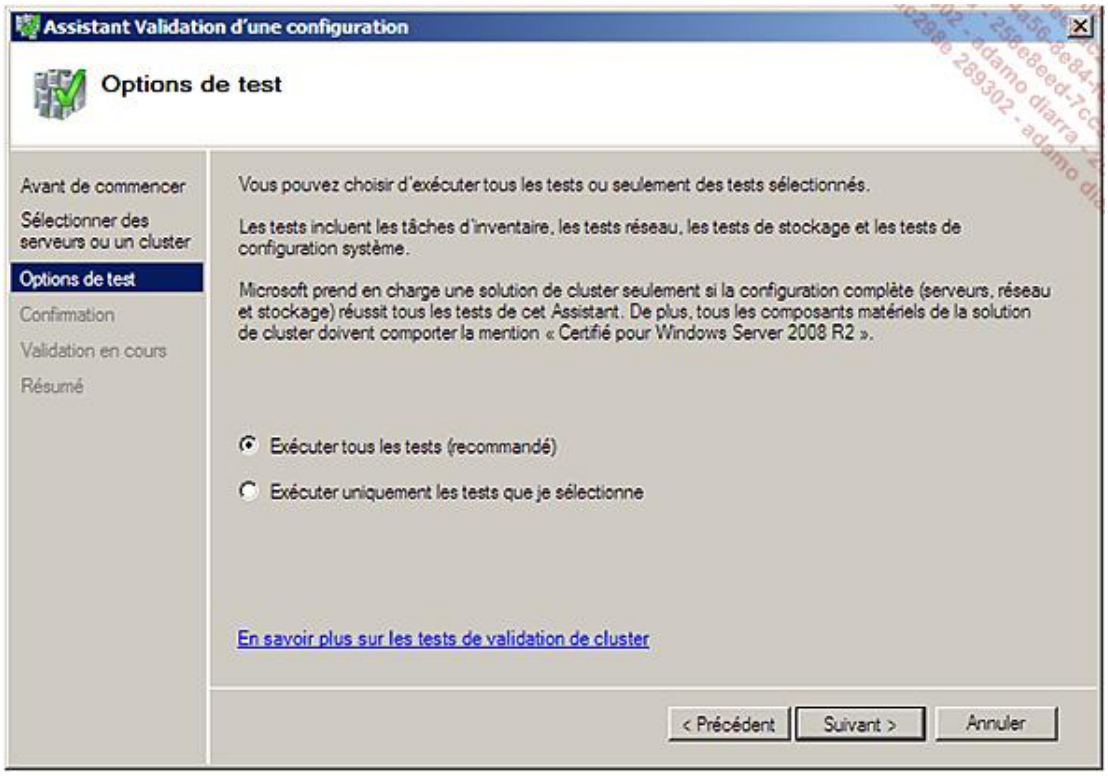


- Cliquez sur **Suivant**.

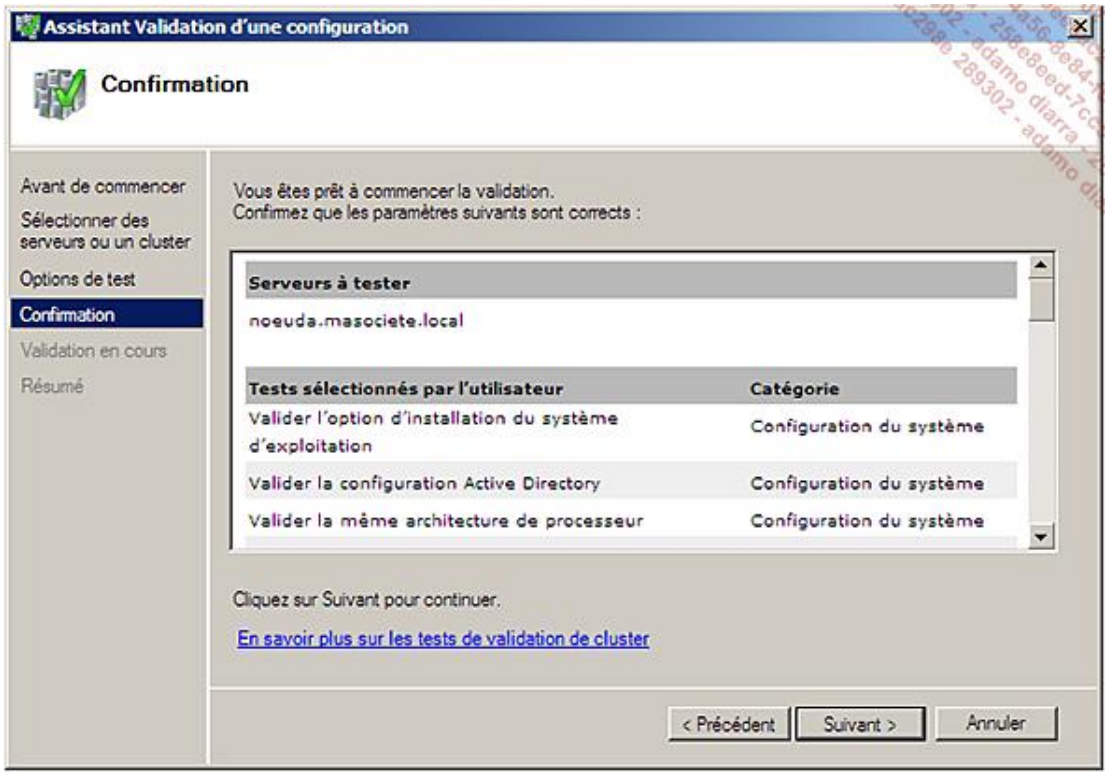


- Ajoutez tous les nœuds qui vont participer au cluster.

© ENI Editions - All rights reserved - adamo diarra



- Choisissez d'**Exécuter tous les tests** sauf si vous êtes sur une exception, comme un cluster Exchange CCR ou un cluster multisite. Cliquez sur **Suivant**.



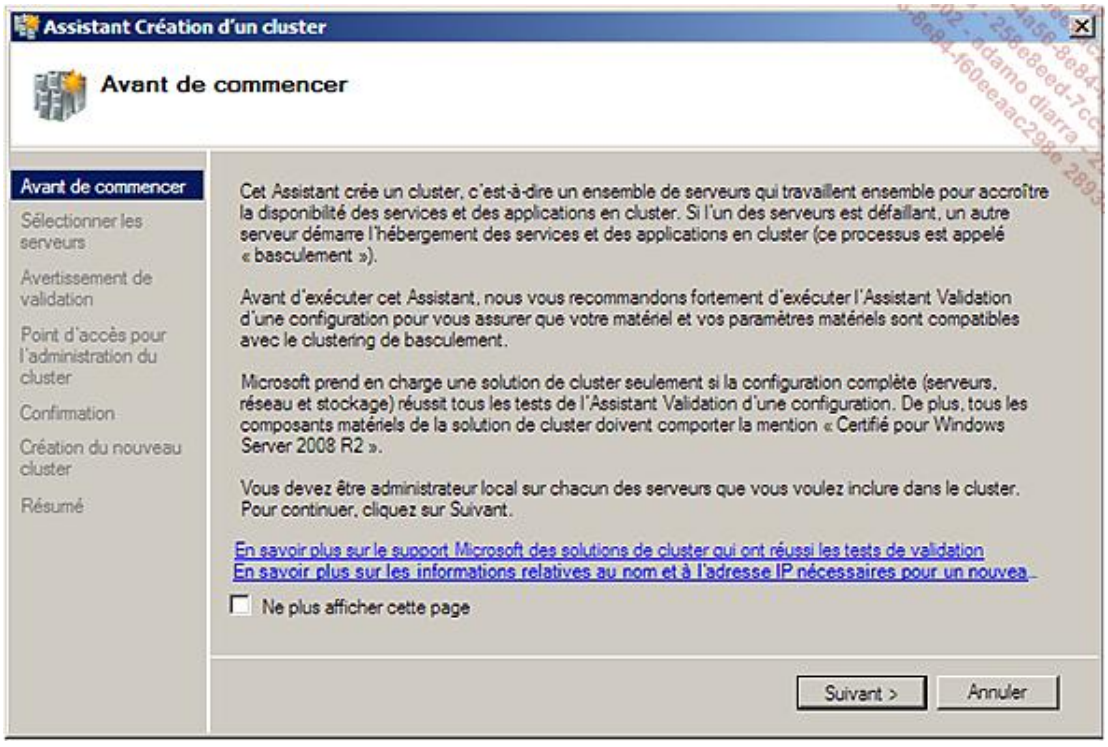
- L'assistant affiche un résumé des choix précédents. Cliquez sur **Suivant**.

- Une fois les tests effectués, leurs résultats s'affichent. La phrase tout en haut permet de savoir tout de suite si l'ensemble des tests est concluant. Si des problèmes ont été détectés, vous pouvez les consulter dans le rapport.

© ENI Editions - All rights reserved - adamo diarra

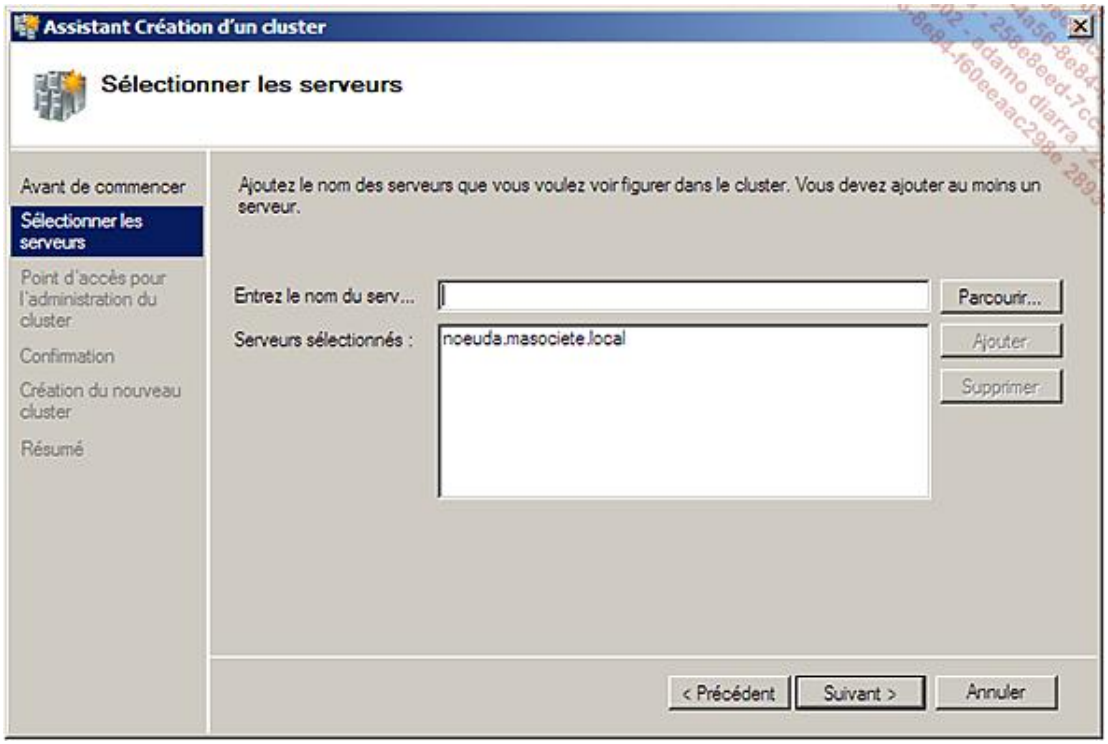
Votre installation étant maintenant validée pour fonctionner en cluster à basculement, il est temps de créer le cluster.

- Cliquez maintenant sur **Créer un cluster** depuis le panneau **Actions** :

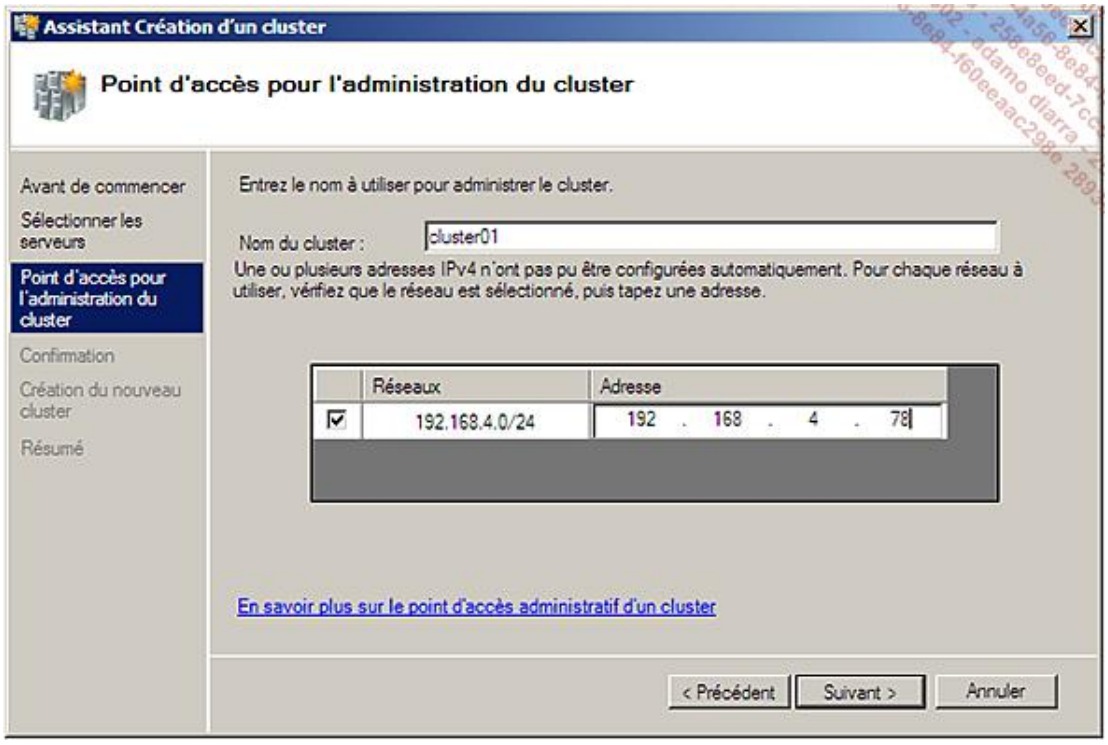


- Cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra

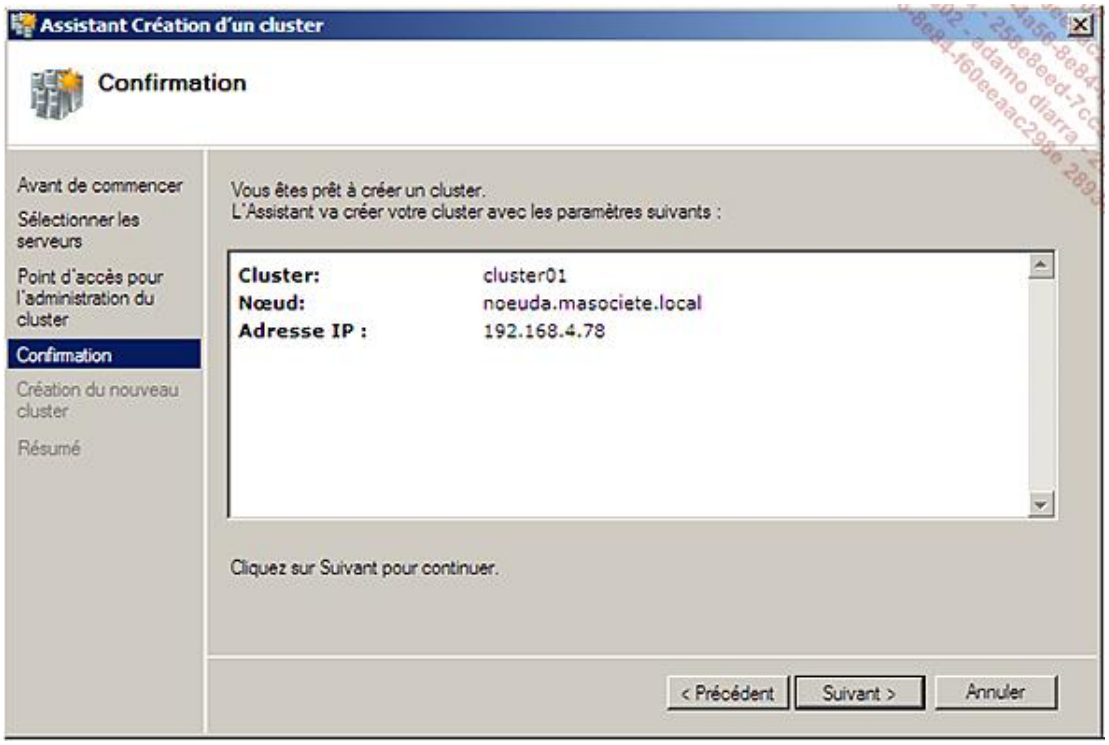


- Ajoutez les nœuds qui vont participer au cluster (uniquement un nœud dans notre exemple). Cliquez sur **Suivant**.



- Le cluster doit avoir au moins un nom (virtuel) et une adresse IP. Ces deux ressources seront dédiées au fonctionnement du cluster et ne devront pas être utilisées pour autre chose. Cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- L'assistant résume la configuration à appliquer avant de le faire réellement. Cliquez sur **Suivant**.

À ce stade, nous avons un cluster opérationnel mais qui n'héberge pas encore de services.

Nous aurions pu arriver au même résultat avec les commandes PowerShell suivantes :

```
import-module FailoverClusters
Test-Cluster -Node noeudA,noeudB
New-Cluster -Name cluster01 -Node noeudA,noeudB -StaticAddress 192.168.4.78
```

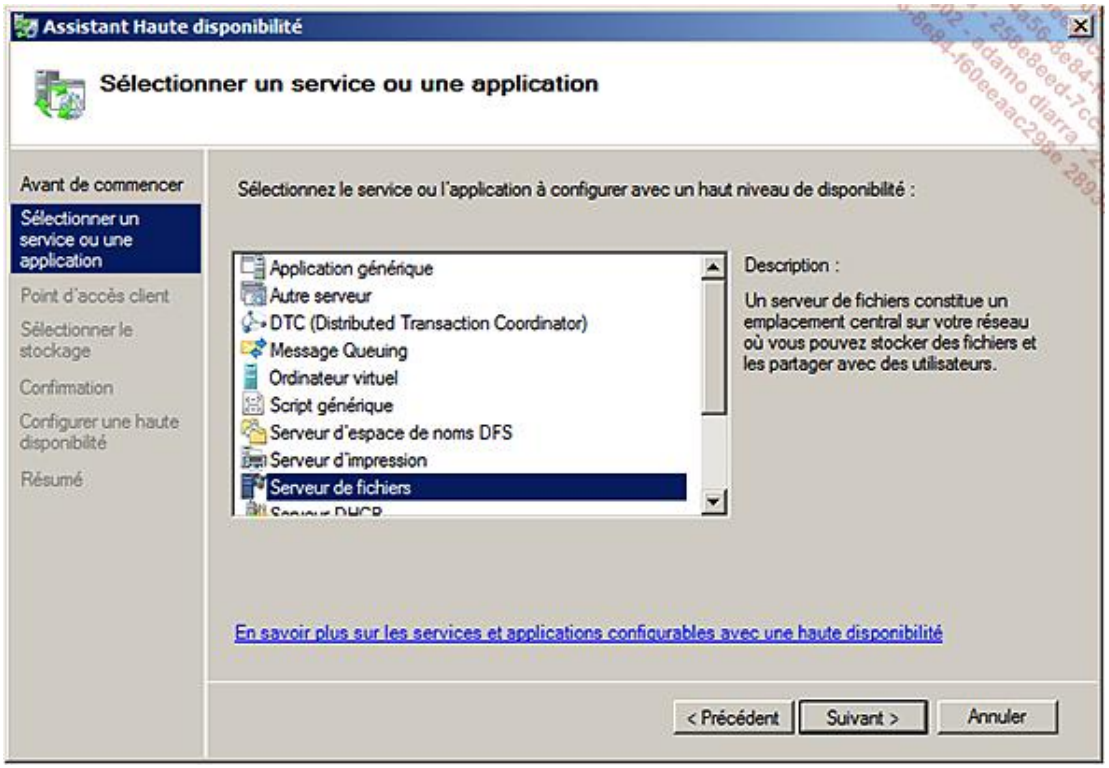
Vous pouvez récupérer la liste des commandes de gestion des clusters avec : `get-command -module FailoverClusters`.

Dans le sous-chapitre NLB, nous avons configuré WinRM. Nous allons l'utiliser de nouveau pour installer le rôle serveur de fichiers sur les nœuds :

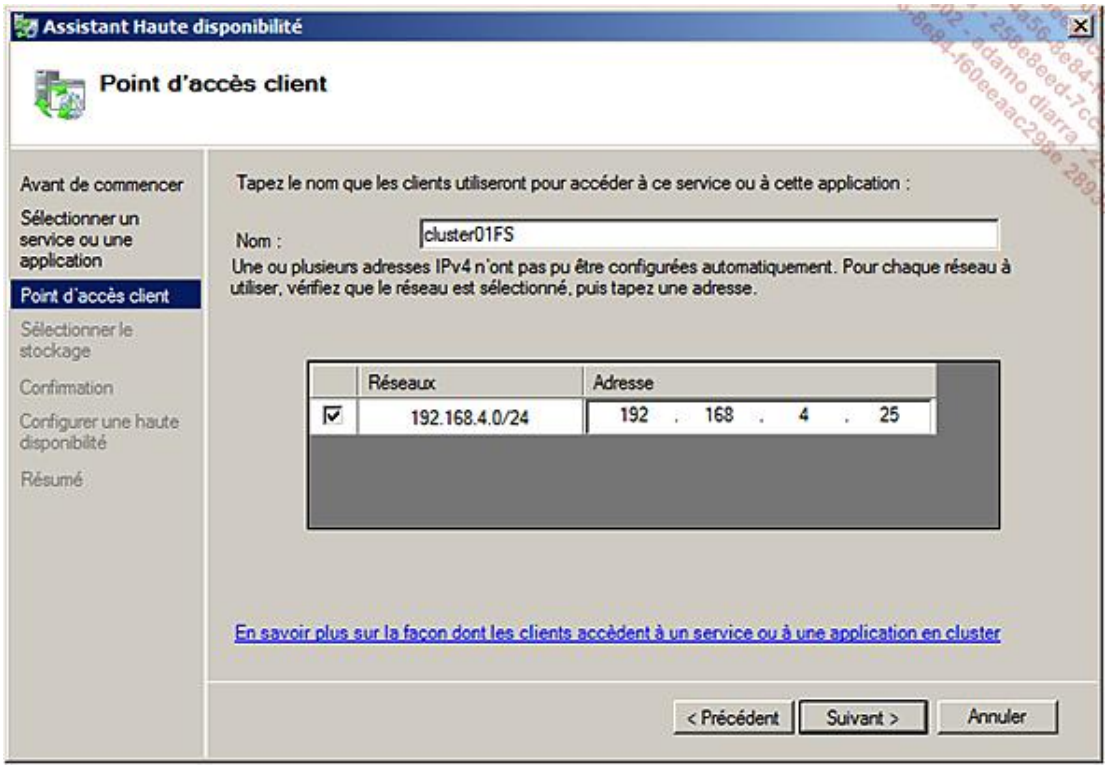
```
Invoke-Command -computername noeudA,noeudB -ScriptBlock {import-module
servermanager;Add-WindowsFeature File-Services}
```

- Nous allons utiliser l'interface graphique pour ajouter un groupe serveur de fichiers à notre cluster :

© ENI Editions - All rights reserved - adamo diarra

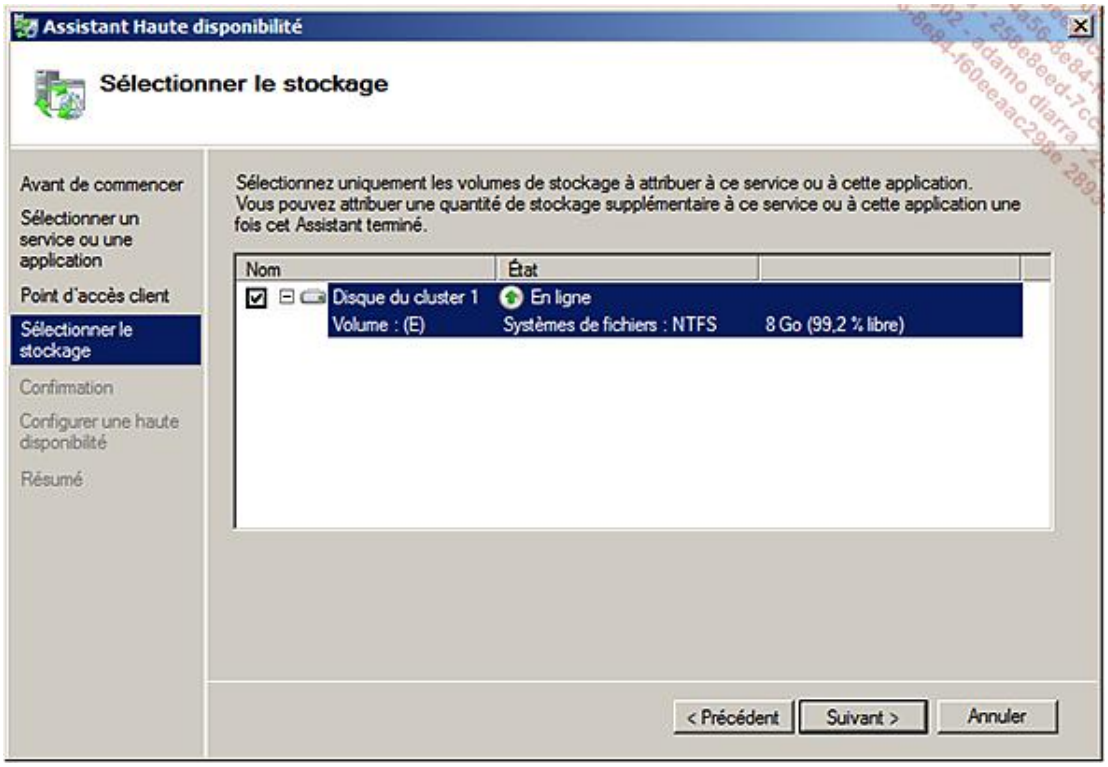


- Cliquez sur **Suivant**.

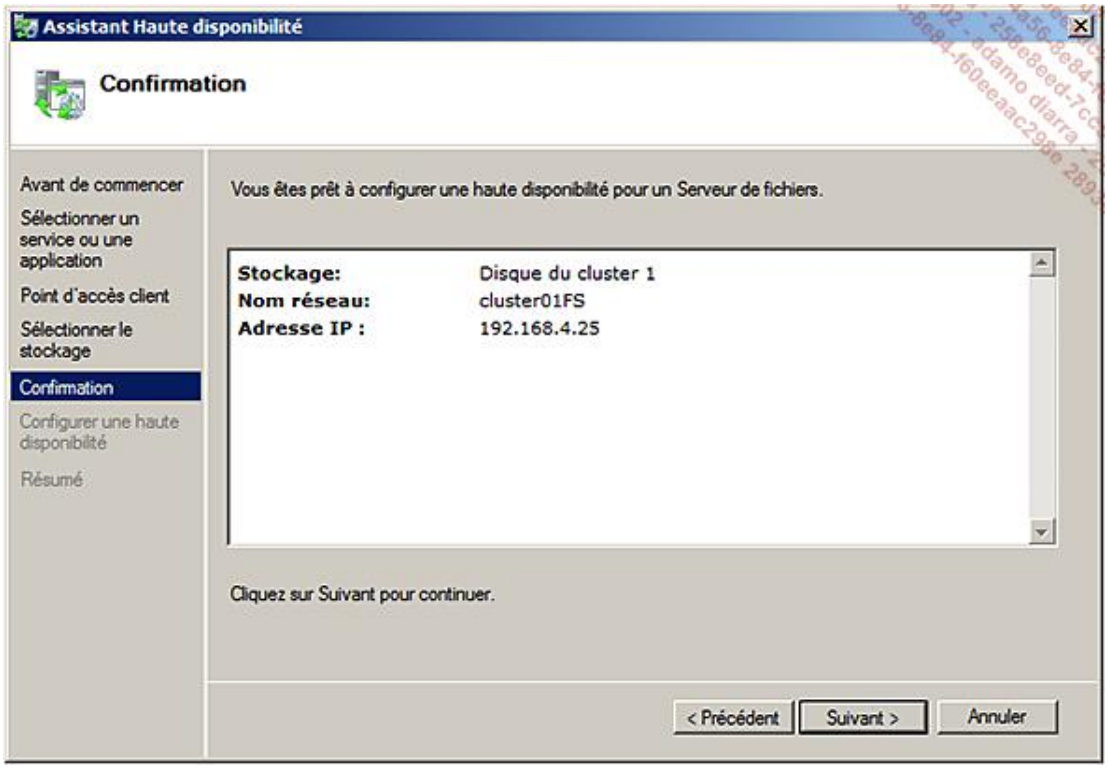


- Il faut maintenant indiquer le nom virtuel du cluster pour ce groupe, ainsi qu'une adresse IP virtuelle.

© ENI Editions - All rights reserved - adamo diarra



- Choisissez le ou les volumes qui hébergeront les données.

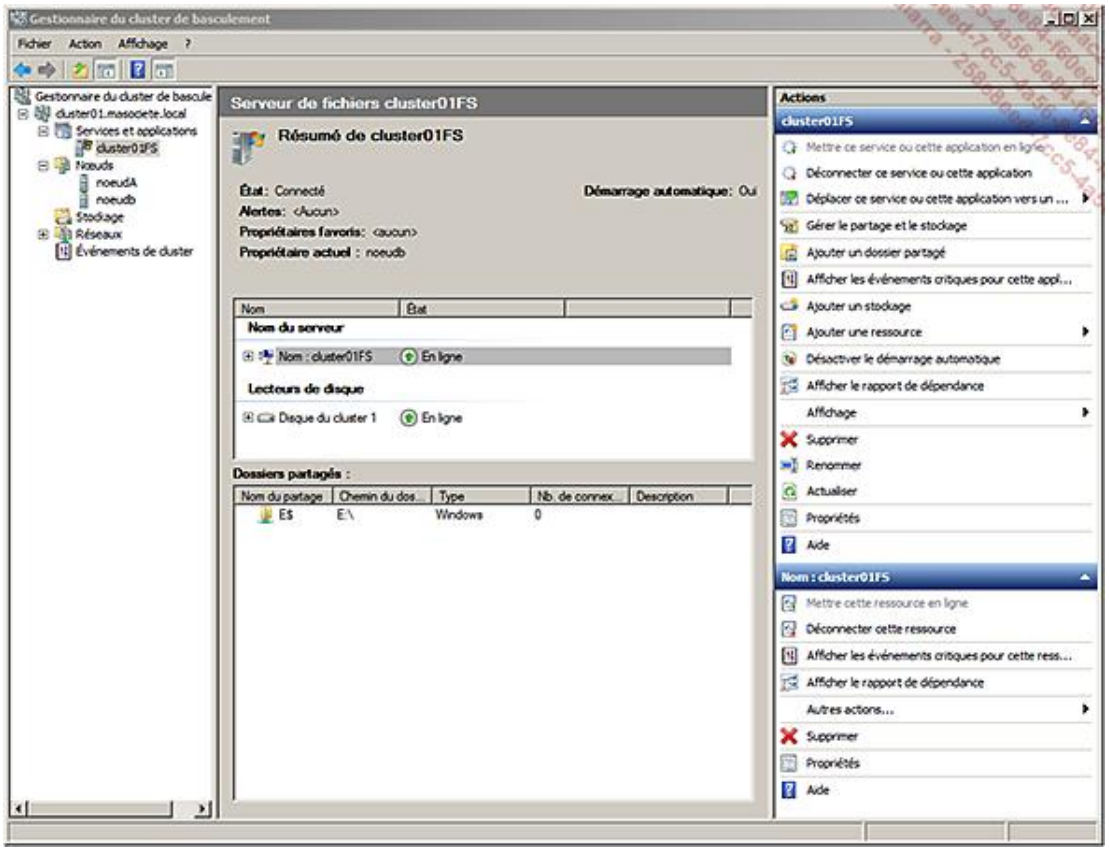


- L'assistant affiche le résumé de la configuration qui va être appliquée. Cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra

- L'assistant affiche le rapport de création.

Le groupe ainsi créé apparaît sous l'arborescence **Services et applications** :



Il ne reste plus qu'à créer des partages.

Cette procédure est la même pour tous les rôles Windows à mettre en cluster.

Il faut savoir que pour la mise en cluster d'une application Microsoft SQL Server par exemple, il faut :

© ENI Editions - All rights reserved - adamo diarra

- installer le cluster,
- installer MSDTC en temps qu'application cluster (si nécessaire),
- installer Microsoft Framework 3.5 SP1,
- installer Windows Installer 4.5,
- créer un groupe cluster vide (un par instance à installer),
- assigner des volumes de stockage dans ce groupe,
- lancer le setup d'installation de SQL Server (avec au minimum, le Service Pack 3 pour SQL Server 2005 et le Service Pack 1 pour SQL Server 2008).

Privilégiez des versions incorporant déjà les Services Pack mentionnés, notamment afin d'éviter certains problèmes décrits dans les articles de connaissance 955725 et 973993.

Concernant Exchange 2007, il faut au moins le Service Pack 1. Au moment de la rédaction de cet ouvrage, il n'est pas supporté sur Windows Server 2008 R2. L'équipe Produit souhaitait uniquement supporter Exchange 2010 sur Windows Server 2008 R2, mais face aux retours des clients, elle va fournir des mises à jour afin qu'Exchange 2007 puisse fonctionner sur Windows Server 2008 R2, mais la date de sortie n'est pas encore officielle.

L'une des principales nouveautés à propos d'Hyper-V et des clusters concerne le stockage des machines virtuelles. Le CSV (*Cluster Shared Volume*), nouveauté de Windows Server 2008 R2, permet de ne plus avoir un volume par machine virtuelle. Un ensemble de machines virtuelles est alors hébergé sur le même volume. Un des nœuds porte le rôle de coordinateur, il est le seul à pouvoir créer des fichiers. C'est lui qui gère l'accès en écriture aux fichiers par les serveurs, afin qu'il n'y ait pas deux serveurs qui modifient le même fichier. Les avantages sont nombreux :

- L'espace libre est commun à toutes les VM. Cet espace peut être consommé par des VM dont le stockage est de type extensible ou par l'ajout de nouvelles VM. La suppression d'une VM rend son espace disponible immédiatement aux autres VM.
- Le nombre de volumes est considérablement réduit. Il y aura d'autant moins d'interventions sur le stockage central et donc moins de risques inhérents.
- La taille du volume peut être importante, le temps d'analyse par un chkdsk est lié au nombre de fichiers et non à la volumétrie.

Le mode CSV est exclusivement supporté et réservé pour stocker des machines virtuelles Hyper-V. Il ne doit jamais être utilisé pour stocker autre chose.

L'ajout de volumes en mode CSV se fait depuis le **Gestionnaire du cluster de basculement** ou depuis PowerShell :

```
$cluster = Get-Cluster cluster01
$cluster.EnableSharedVolume="Enabled"
```

Vous connaissez maintenant les avantages et les contraintes d'une solution de haute disponibilité et ou de répartition de charge. Vous avez les cartes en main pour préparer votre solution et la gérer une fois en production. Comme pour beaucoup de solutions, vous ne devez pas attendre d'avoir besoin de cette technologie (au moment d'un plantage par exemple) pour valider son bon fonctionnement. Vous devez planifier des tests aussi régulièrement que possible, afin que la bascule fonctionne le jour J. Contrairement à la plupart des projets, c'est parce que l'utilisateur ne se rendra compte de rien que le projet sera un succès et rentabilisé.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre est consacré à la définition et la configuration des composants nécessaires au bon fonctionnement d'un réseau d'entreprise basé sur Windows 2008 R2.

Les composants IP, DNS, DHCP, WINS, ainsi que la mise en place de la quarantaine réseau sur DHCP, IPSEC et 802.1x seront abordés.

© ENI Editions - All rights reserved - adamo diarra

L'implémentation d'un système d'adressage IP

La mise en place de toute architecture réseau passe par l'analyse des réseaux existants. Il est souvent difficile de modifier l'ensemble en une seule fois. La migration se fait donc souvent en implémentant un nouvel adressage réseau et une cohabitation avec les réseaux existants. La modification de l'adressage IP est souvent vue comme coûteuse, n'apportant que peu d'avantages supplémentaires.

Le changement d'un domaine DNS est encore plus compliqué, surtout lorsque ce domaine DNS sert de support à un domaine Active Directory. Dans ce cas, une migration représente une étude particulière qui sort du cadre de cette présentation.

1. Le choix de l'architecture réseaux

Deux point précis sont à étudier à ce niveau :

- le choix de la zone DNS ;
- le choix de la classe réseau.

a. La zone DNS

Deux aspects sont importants lors du choix de la zone DNS.

Le nom choisi pour la zone DNS doit correspondre à l'intégralité de l'entité (entreprise, groupe, etc.) que l'on souhaite gérer. Ce nom doit pourvoir être accepté par toutes les entités dépendantes qui vont se retrouver dans cette zone. Le problème est beaucoup plus politique que technique !

Si une entité n'entre pas dans ce cadre, cela veut dire qu'une zone DNS spécifique devra lui être affectée.

Si la zone DNS doit être utilisée sur Internet, le domaine DNS sera forcément public et enregistré, c'est-à-dire utilisant une extension reconnue de type .fr, .com, .info... !

En revanche, pour un réseau interne, le domaine peut être public ou privé. Le choix le plus courant est alors d'utiliser un domaine DNS local avec une extension inconnue sur Internet. L'extension **.local** est très souvent utilisée sous la forme **MaSociete.local**. Le découpage entre ce qui est interne ou externe est plus facile à réaliser. En revanche, l'utilisation d'un même nom suppose une double administration, plus complexe, donc des serveurs DNS différents pour ne rendre visible sur Internet que ce qu'il est souhaitable de montrer.

b. La classe réseau

Pour tous les réseaux internes, le choix se portera évidemment toujours sur les classes réseaux privées. Si l'on ne peut pas toujours modifier l'intégralité des réseaux existants pour des raisons souvent historiques, on peut au moins créer tous les nouveaux réseaux en suivant cette règle.

La classe du réseau se choisit en fonction du nombre de machines présentes sur le réseau, du nombre de sites, etc. Un réseau de classe C (192.168.0.X) représente souvent un bon choix initial. Il est toujours possible de changer de classe, de réseau ou même surtout d'utiliser plusieurs réseaux en fonction des besoins.

L'usage de TCPIP v6 n'est pas encore bien développé mais deviendra nécessaire dans les 2 ou 3 années qui suivent, principalement sur Internet. Sur le réseau local, il reste encore de nombreux logiciels qui ne sont pas compatibles, mais ceci devrait évoluer très rapidement !

2. L'installation d'un serveur DHCP

Si le service DHCP permet de mettre en place rapidement le réseau choisi, il permet aussi de modifier rapidement et globalement une série de paramètres. Il reste encore quelques irréductibles qui n'utilisent pas ce service, mais c'est maintenant rarissime.

Parmi les nombreux composants de Windows 2008 R2, le service DHCP est un rôle.

a. Définition

Le protocole DHCP (*Dynamic Host Configuration Protocol*) a pour but de fournir une adresse IP et un masque à tout

© ENI Editions - All rights reserved - adamo diarra

périphérique réseau (station, serveur ou autre) qui en fait la demande. Selon la configuration, d'autres paramètres tous aussi importants seront transmis en même temps : les adresses IP de la route par défaut, des serveurs DNS à utiliser, des serveurs WINS et le suffixe de domaine pour ne citer que les principaux.

DHCP est souvent réservé aux stations, aux imprimantes et ne devrait servir qu'exceptionnellement aux serveurs.

b. L'installation

Comme pour tous les composants Windows, l'installation peut se faire graphiquement ou en mode ligne de commande sans avoir besoin d'insérer le moindre média.

```
servermanagercmd -install DHCP
```

Attention, le service devra être mis en démarrage automatique !

```
sc \\%COMPUTERNAME% config DHCPServer start= auto
```

Le service peut ensuite être démarré de manière classique :

```
NET START DHCPSERVER
```

Le démarrage du service permet de le rendre accessible et configurable.

Pour que le service DHCP commence à distribuer des adresses, il est indispensable de configurer et d'activer une étendue.

Attention, si le serveur qui héberge DHCP fait partie d'une forêt Active Directory, il doit en plus avoir été autorisé par des administrateurs membres du groupe « Administrateurs de l'entreprise » ou ayant reçu les droits d'administration DHCP.

Le service DHCP, comme les autres services réseaux de références (DNS, WINS), devrait toujours être installé sur des serveurs disposant d'adresses IP fixes.

c. La configuration

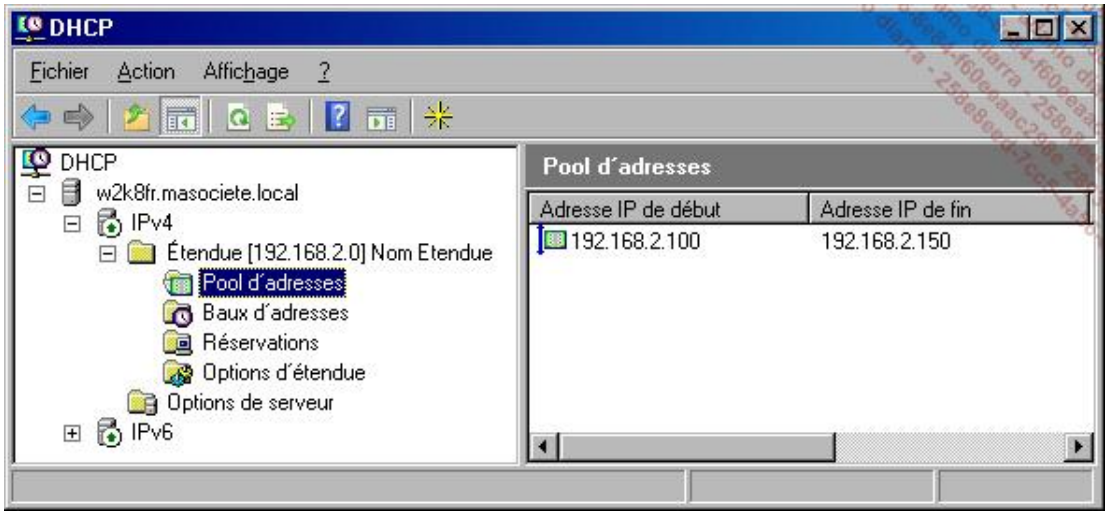
La console d'administration DHCP est automatiquement installée en même temps que le service, mais peut aussi être lancée à partir de toute autre machine la possédant.

Y compris sur le serveur lui-même, sélectionnez le serveur DHCP (ou les serveurs) que vous souhaitez gérer. La liste des serveurs déjà autorisés s'affiche automatiquement.

Pour autoriser un serveur DHCP, utilisez l'option **Gérer les serveurs autorisés**, puis cliquez sur le bouton **Autoriser**, et saisissez le nom ou l'adresse IP.

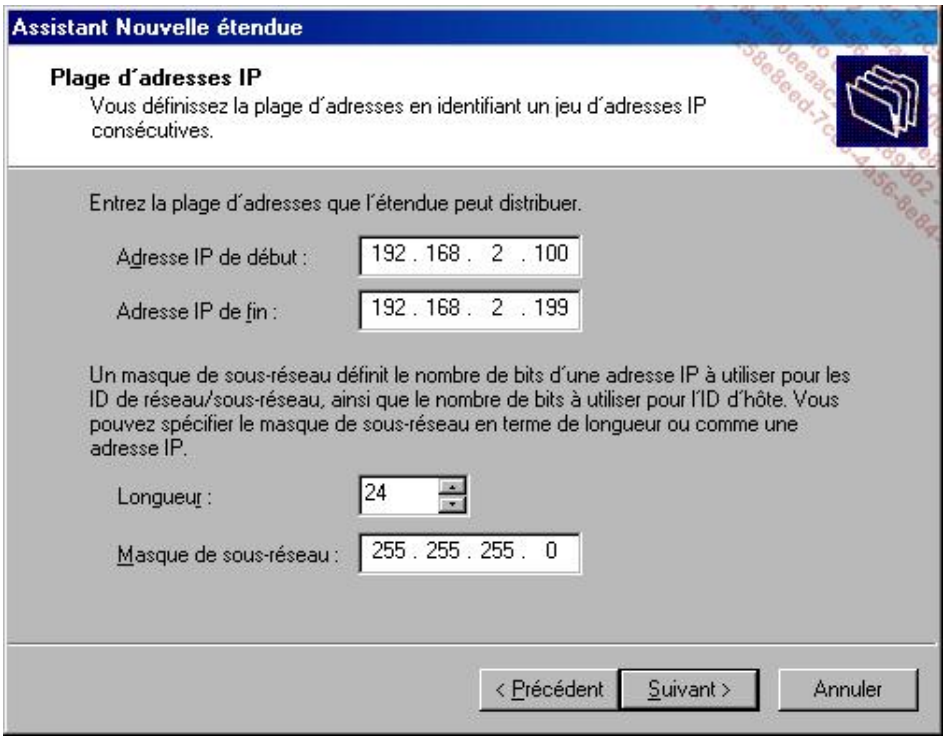
Les serveurs autorisés apparaissent avec une flèche verte.

© ENI Editions - All rights reserved - adamo diarra



Chaque serveur DHCP peut servir de nombreuses étendues, mais une seule pour chaque réseau IP.

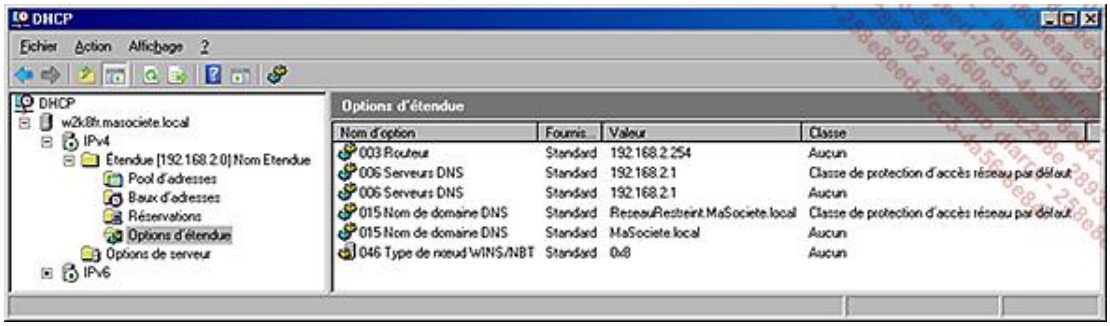
Voici une étendue classique pour un réseau 192.168.2.X de classe C utilisant le masque standard 255.255.255.0 !



La plage utilisée ne doit pas forcément utiliser la totalité de la classe réseau afin de laisser de la place pour les serveurs ou les adresses IP réservées pour les imprimantes.

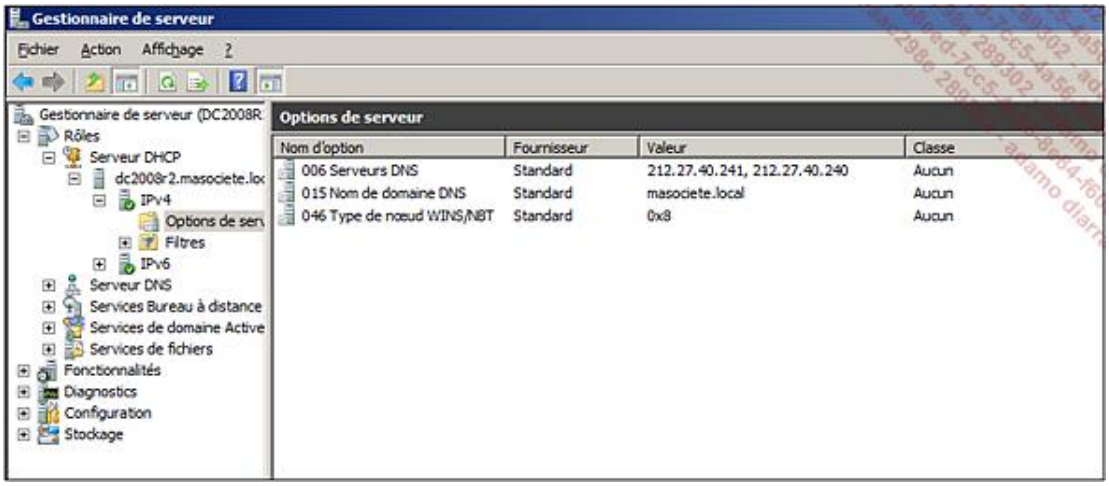
La route par défaut fait partie des paramètres habituels liés à l'étendue.

Les options au niveau du serveur contiennent les paramètres qui sont valables globalement sur toutes les étendues.



© ENI Editions - All rights reserved - adamo diarra

Les options de serveur (005,006,015,046) servent de valeurs par défaut, mais sont remplacées par les options de l'étendue qui ont priorité.

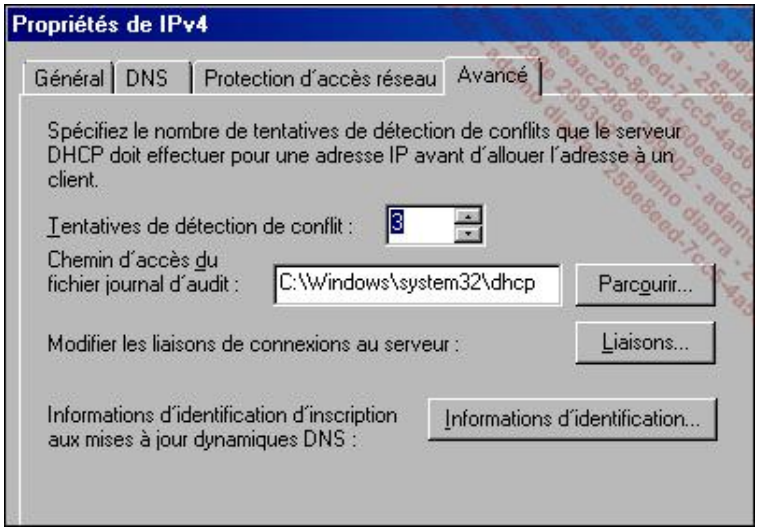


- La zone **Nom de domaine DNS** ne permet pas de spécifier plusieurs suffixes de recherche DNS. Si nécessaire, les stratégies proposent d'ajouter des suffixes de recherche.

- Le **Type de nœud** avec la valeur 0x8 configure le mode de résolution hybride. C'est-à-dire qu'une interrogation des serveurs DNS/WINS sera effectuée en premier, avec bascule en mode Broadcast en cas d'échec.

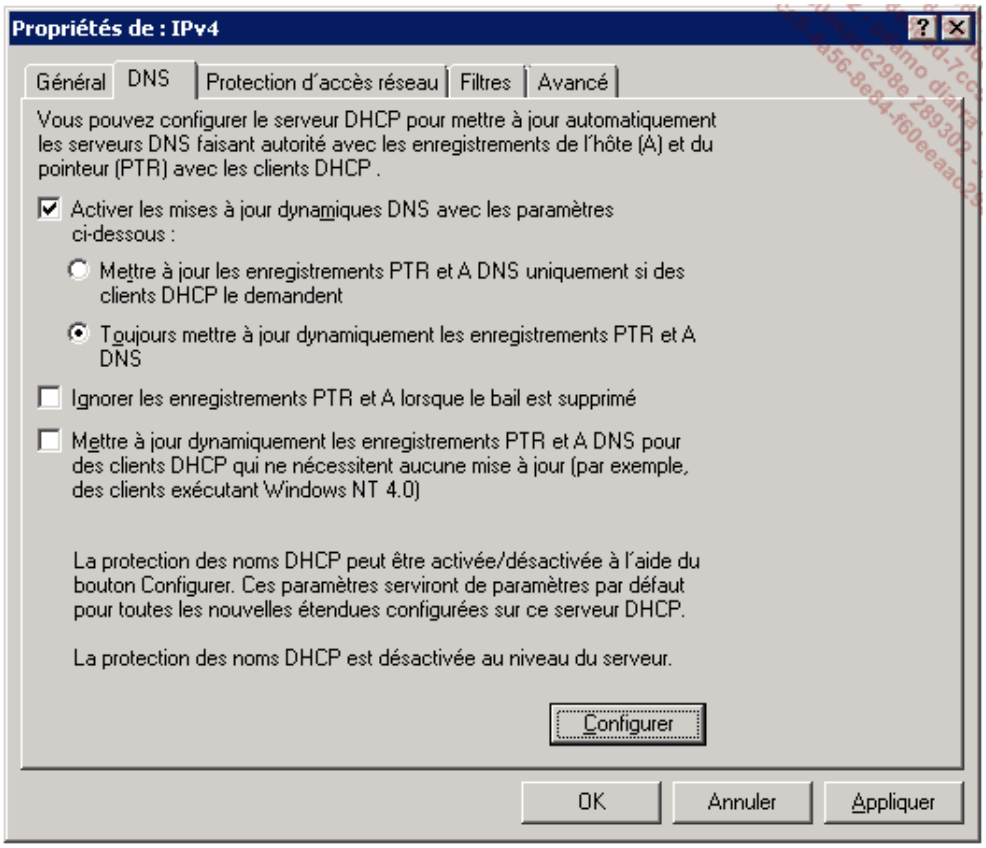
Certaines propriétés avancées du serveur DHCP peuvent être très intéressantes à configurer.

Par exemple, lorsque la zone **Tentatives de détection de conflit** est configurée avec une valeur supérieure à zéro, DHCP utilisera l'instruction **ping** pour déterminer l'existence éventuelle d'une machine sur cette adresse.



La mise à jour dynamique des DNS est un élément particulièrement important à gérer.

© ENI Editions - All rights reserved - adamo diarra



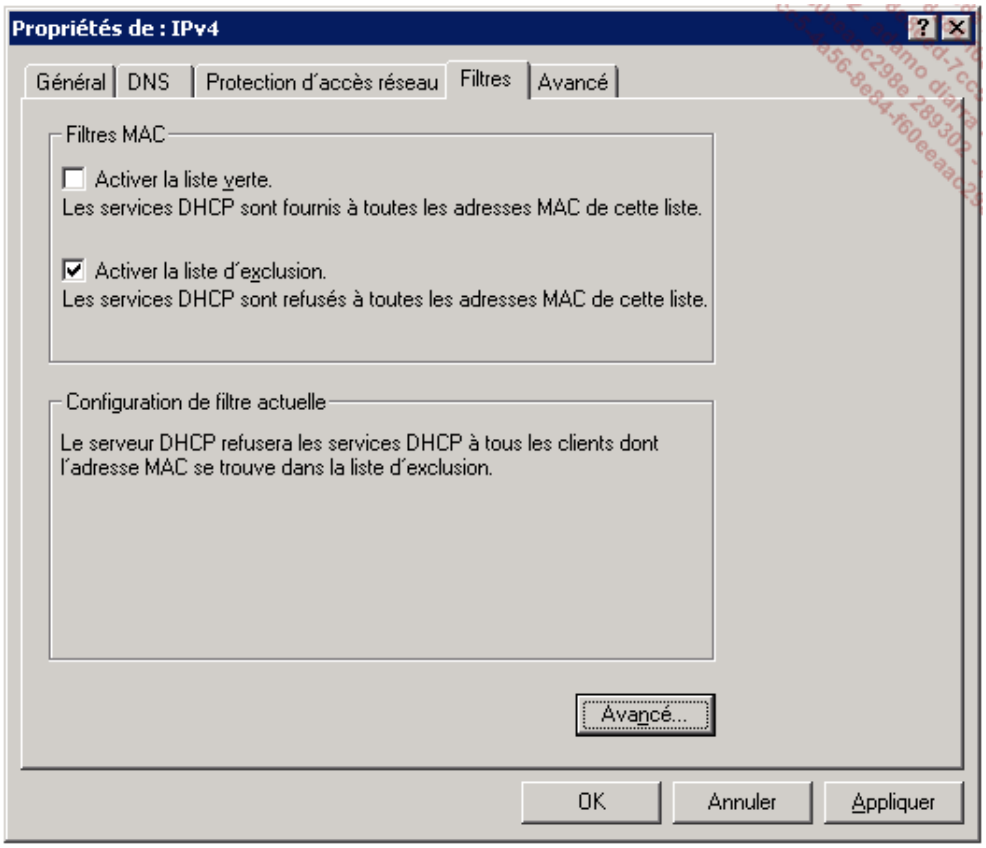
Le bouton **Configurer** permet d'activer la protection des noms lors de l'inscription, les mises à jour et la suppression des enregistrements de type A et PTR. Cette protection n'est effective que si le mode Mise à jour dynamique sécurisé est actif.

Lorsque les zones de recherche inverses (Reverse ARP) sont créées et utilisées, il est important de mettre à jour les enregistrements PTR et de ne pas les ignorer lorsque le bail est supprimé.

La durée du bail sera d'autant plus longue que le nombre d'adresses IP disponibles est important et que le risque de conflit est limité.

L'onglet **Filtres** vise à limiter la distribution des adresses DHCP, soit en n'autorisant que certains types de matériels réseaux, soit en excluant certains types. Ces types incluent notamment Token Ring, X25, ATM, Ethernet, Localtalk, Frame Relay, Fibre channel, HDLC, LocalNet et Ethernet IEE 802.

© ENI Editions - All rights reserved - adamo diarra



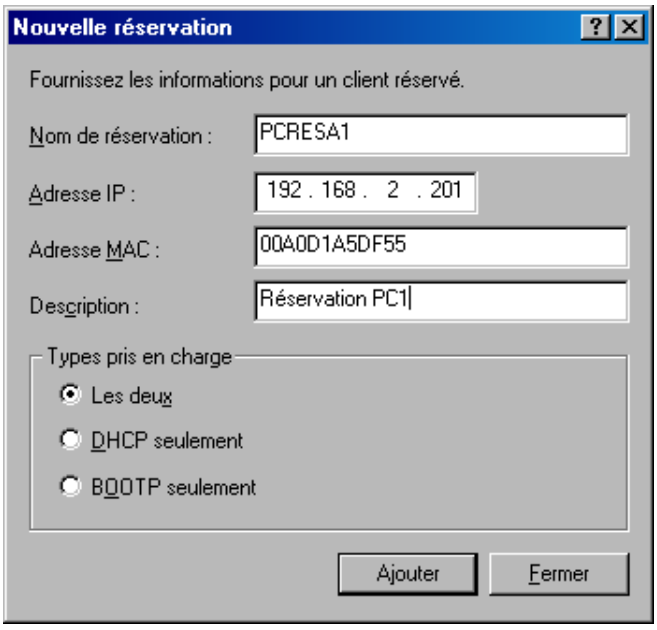
d. Les réservations

Même pour les administrateurs qui souhaitent gérer toutes les machines avec un adressage IP fixe, DHCP peut être très utile. En effet, certains gèrent ainsi la totalité du parc avec une réservation pour chaque adresse IP, même si ceci représente une sécurité plus que fictive.

Sans aller jusqu'à gérer tout le réseau, les réservations sont très utiles pour les imprimantes en réseau, les périphériques administrables (switch...) et parfois pour certaines machines dont l'adresse IP a été autorisée et utilisée dans la configuration d'un logiciel.

Chaque carte réseau disposant d'une adresse physique unique appelée **MAC Address**, il est possible d'identifier la demande provenant de cette adresse, et de lui fournir toujours la même adresse IP et la même configuration.

Voici un exemple de définition de réservation :



© ENI Editions - All rights reserved - adamo diarra

À noter que les réservations doivent faire partie du réseau mais pas de l'étendue DHCP ce qui peut parfois être très pratique. Si plusieurs serveurs DHCP sont utilisés pour un même réseau (avec les restrictions d'usages), les réservations doivent être configurées sur tous ces serveurs.

Certains outils provenant des kits de ressources comme DHCPCMD.EXE, ou la librairie DHCPOBJS.DLL permettent de développer des scripts pour automatiser la création et la configuration des étendues. La commande `NETSH` permet aussi de réaliser certaines opérations de configuration, d'import et d'export.

Pour exporter ainsi une configuration existante, il faut utiliser la commande `NETSH` :

```
NETSTH DHCP SERVER DUMP  >DHCPCONFIG.CMD
```

Adaptez ensuite le fichier DHCPCONFIG.CMD en fonction des besoins en supprimant les lignes inutiles et en modifiant les autres.

© ENI Editions - All rights reserved - adamo diarra

La mise en place des systèmes de résolutions de nom

1. La résolution DNS

DNS est devenu la pierre de base du fonctionnement d'un réseau Windows basé sur Active Directory, mais pas seulement.

La plupart des activités actuelles (Messagerie, Internet) sont basées sur le bon fonctionnement du réseau et en particulier du module DNS.

Il n'est donc maintenant plus possible de se passer de ce système qui héberge de plus en plus d'informations vitales au bon fonctionnement de l'ensemble du réseau.

a. Définition

DNS (*Domain Name Server*) correspond tout d'abord à un protocole permettant à des clients (du réseau) d'interroger une base de données contenant des informations sur les machines et les services hébergés par ces machines.

DNS est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.

b. L'installation

L'installation du service DNS sur un réseau Windows se fait souvent dans le cadre de l'installation du premier contrôleur de domaine Active Directory. Sa configuration initiale est alors automatiquement prise en charge par l'assistant DCPROMO. Par défaut, la zone DNS utilisée par Active Directory est alors intégrée et gérée par Active Directory.

Si l'on doit automatiser ou ajouter un service DNS, voici l'instruction à utiliser :

```
servermanagercmd -install DNS
```

Si le service DNS est ajouté sur un contrôleur de domaine, alors toutes les zones intégrées à Active Directory sont connues et utilisées par le service DNS pour sa résolution.

Dans tous les autres cas, le service DNS devra être géré comme un serveur DNS classique. Il pourra alors héberger des zones et servir de cache ou de renvoi vers d'autres systèmes DNS.

c. Les différents types de zones

La zone de type principale

Bien entendu, ce type de zone sera surtout utilisé pour gérer des zones non liées à AD. Les zones DNS publiques, contenant les serveurs Web de l'entreprise et les serveurs de messagerie, sont les exemples les plus courants d'utilisation.

Chaque zone est sauvegardée dans un fichier texte spécifique au format tout à fait standard avec l'extension .DNS. Ce type de fichier est compatible avec les autres systèmes DNS très connus comme BIND. Ceci autorise l'importation ou l'exportation de zones DNS entre différents serveurs.

Le serveur qui héberge la zone principale est le seul à autoriser et valider les mises à jour de sa zone. C'est la principale différence avec les zones intégrées à AD qui autorisent elles les modifications sur chaque contrôleur.

La zone de type secondaire

Une zone secondaire peut être établie à partir d'un serveur de zone principale, d'une zone intégrée à Active Directory ou même d'un autre serveur de zone secondaire. La zone secondaire n'est qu'une réplique exacte de la zone dont elle dépend. En revanche, la réplication doit avoir été autorisée sur le serveur servant de référence.

Dans le monde Windows, la zone de type secondaire sert très souvent à répliquer les informations d'un autre domaine AD afin de réaliser une approbation entre deux domaines. Les zones secondaires sont souvent configurées sur des serveurs BIND (Unix ou Linux) pour obtenir une résolution indirecte des domaines DNS gérés par AD.

Comme la zone principale, les informations sont sauvegardées dans un fichier texte utilisant l'extension .DNS.

© ENI Editions - All rights reserved - adamo diarra

En cas de perte du serveur principal, un serveur de zone secondaire peut devenir un nouveau serveur principal.

Les zones secondaires présentent souvent des problèmes de réplication, de délais de mise à jour, de notification et de sécurité à configurer, qu'il vaut mieux éviter.

La zone intégrée à Active Directory

La zone intégrée à Active Directory consiste, comme le nom l'indique, à utiliser la base de données Active Directory comme réceptacle de l'information. Du coup, elle bénéficie de toutes les options de sécurité de AD, ainsi que de la réplication incrémentale entre tous les contrôleurs de domaine.

Tous les domaines DNS peuvent être intégrés à AD, et pas seulement ceux utilisés par AD.

À moins que votre serveur DNS ne se trouve pas sur votre contrôleur de domaine, toutes les zones DNS ont intérêt à être intégrées à AD.

d. Les différents types de réplications

Ceux-ci ne s'appliquent qu'aux zones intégrées à AD en accédant aux propriétés du domaine choisi.

La réplication sur tous les serveurs DNS de la forêt

Cette réplication est à préconiser pour les domaines qui ont intérêt à être connus (et résolus) rapidement sur tous les domaines de la forêt sans avoir à transférer les requêtes vers ce que l'on appelle les **redirecteurs** (Forwarders). Ce choix s'applique particulièrement au domaine racine de la forêt.

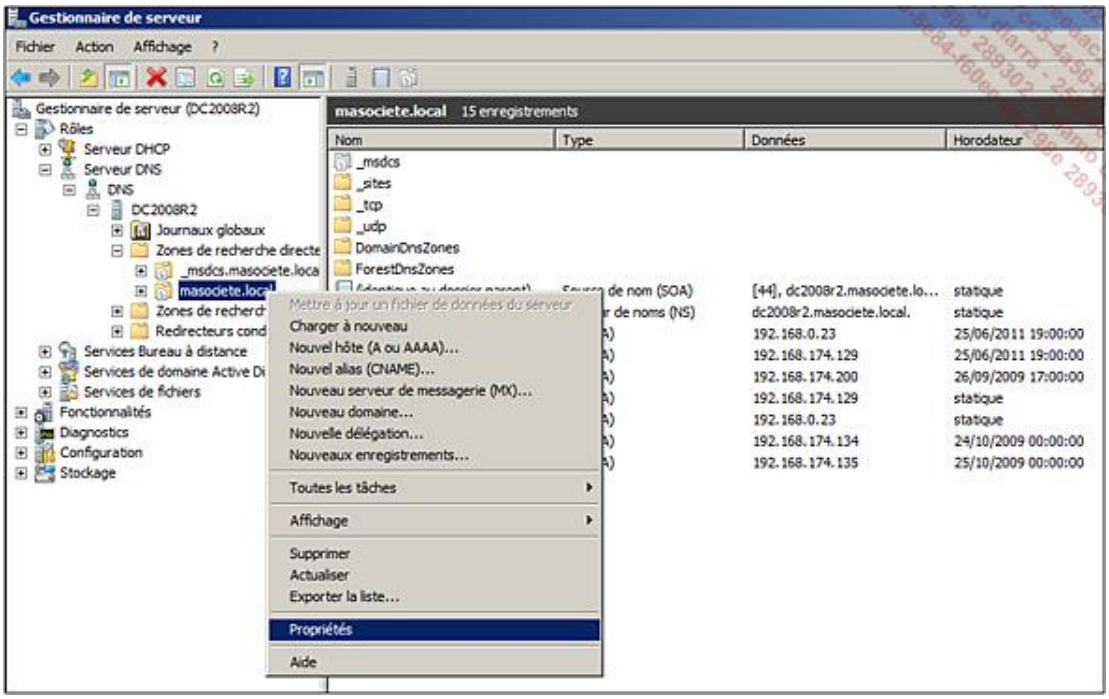
La réplication sur tous les contrôleurs du domaine

La réplication sur tous les contrôleurs du domaine est le mode compatible avec ce qui se faisait sur Windows 2000. C'est le choix logique lorsque les contrôleurs de domaine sont utilisés seuls comme serveurs DNS de référence. En effet, comme les contrôleurs de domaine répliquent déjà les données DNS au même titre que les autres données de l'annuaire, il suffit d'installer le service DNS pour qu'ils assurent cette fonction.

La réplication sur tous les serveurs DNS du domaine

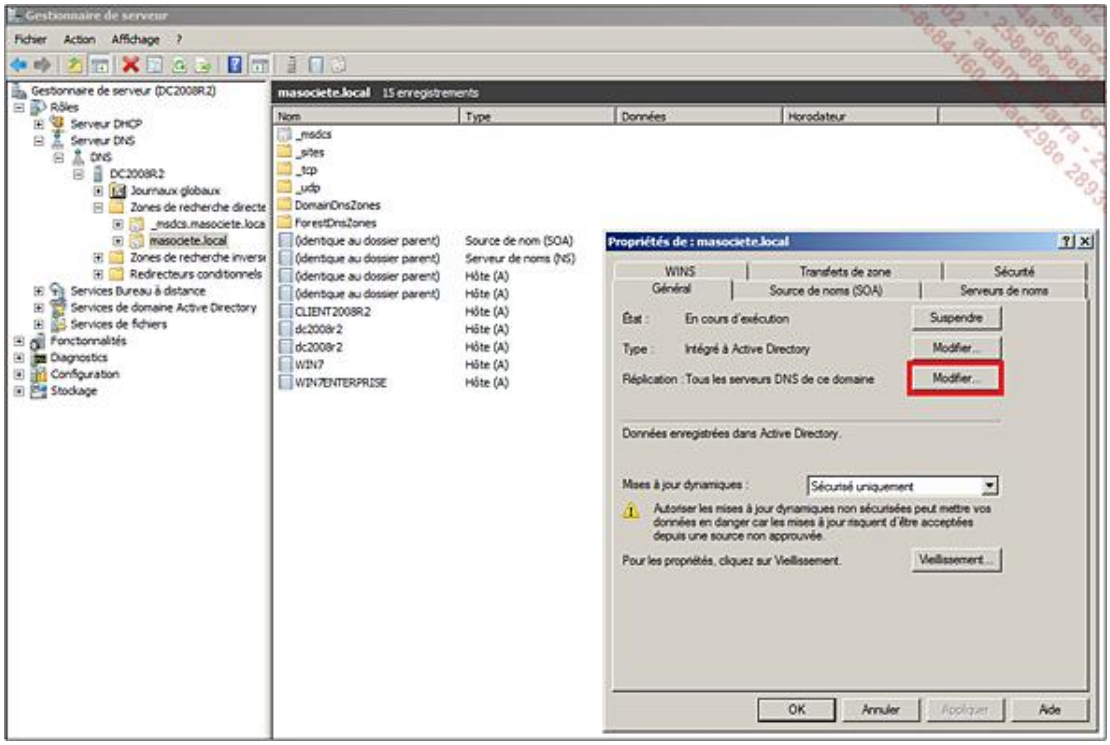
Ce choix est rarement utilisé et permet à des serveurs DNS qui ne sont pas contrôleurs de domaine de recevoir aussi la réplication d'une zone précise.

- Sélectionnez la zone DNS, puis cliquez avec le bouton droit de la souris et sélectionnez **Propriétés** dans le menu.



- Cliquez sur le bouton **Modifier** en face de **Réplication**.

© ENI Editions - All rights reserved - adamo diarra



Les différents types de réplications apparaissent.

La réplication liée à une partition souvent dite applicative

Par défaut, dans une forêt AD, il existe déjà deux partitions applicatives particulières de ce type et qui sont déjà proposées pour la réplication :

- la ForestDnsZones ;
- la DomainDnsZones.

Si une autre partition applicative a été créée, celle-ci peut être utilisée pour répliquer des informations DNS (ou autres) sur des groupes de machines personnalisés.

À noter qu'en cliquant droit sur le serveur DNS, l'option **Créer des partitions de l'annuaire d'applications par défaut** peut s'avérer utile pour recréer l'une ou l'autre des partitions.

e. Les zones de recherche inversée

Les zones de recherche inversée ARP recherchent le nom d'une machine à partir de l'adresse IP. Le classement est donc fait en fonction de l'adressage réseau IP.

Ce mode de recherche n'est pas nécessaire et n'est pas utilisé pour le fonctionnement normal d'une forêt Active Directory. C'est pour cette raison que Microsoft ne crée pas automatiquement de zones de recherche inversée.

En revanche, le client DNS Microsoft sait bien entendu les utiliser si elles sont définies. Certains logiciels comme la sauvegarde **TINA** (*Time Navigator de ATEMPO*) ont un besoin impératif de ce type de zone pour fonctionner correctement.

Lors de la résolution d'un problème réseau et de l'utilisation de l'outil NsLookup, il est indispensable d'avoir créé les zones de recherche inversée pour le bon fonctionnement de cet outil et la bonne interprétation des résultats.

Comme les zones classiques dites de **recherches directes**, il est possible de créer des zones principales (intégrées ou non à AD) ou des zones secondaires.

Dès que ces zones sont créées, il est important de configurer DHCP pour gérer les mises à jour des enregistrements **PTR**, c'est-à-dire du nom d'hôte associé à chaque adresse IP. L'intégration de ces zones à AD concernera surtout les réseaux IP qui contiennent majoritairement des machines Windows.

Lors de la création d'une zone de recherche inverse, le nom de la zone est basé sur l'adressage IP donc chaque valeur est prise à l'envers.

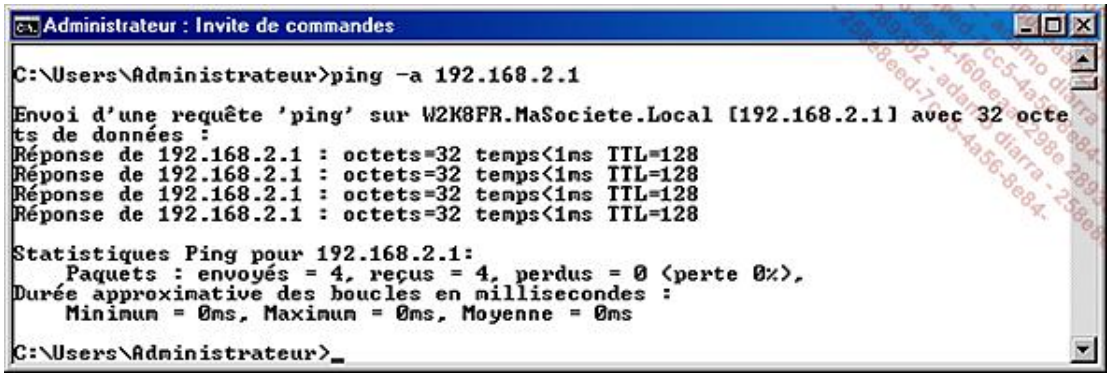
© ENI Editions - All rights reserved - adamo diarra

f. Les tests et vérifications

Différents outils sont utilisables pour vérifier le bon fonctionnement de la résolution sur les différents domaines.

L'outil **ping** est le premier à utiliser pour les tests de résolution. Attention, le résultat des tests peut être perturbé par le filtrage existant sur les pare-feu intermédiaires ou sur les systèmes eux-mêmes. Utilisez **ping** avec le nom court, le nom complet (nom suivi du domaine DNS complet) et l'adresse IP. Si une réponse est obtenue sur chacun de ces tests, tout est pour le mieux. Dans le cas de l'adresse IP, l'argument `-a` permet aussi de vérifier la résolution inverse.

Si le nom complet **W2K8FR.MaSociete.Local** apparaît, c'est que la résolution inverse fonctionne bien, même dans le cas où il n'y a pas de réponse au ping.



L'outil **NsLookup** permet d'interroger les serveurs DNS sur tous les différents champs et enregistrements des zones DNS accessibles.

Les deux commandes `Tracert` et `PathPing` sont un équivalent du ping, mais qui indiquent toutes les étapes, les adresses traversées et les durées de chaque étape.

Bien entendu, d'autres outils comme **netsh**, **dnscmd** et **dcdiag** augmentent énormément les possibilités.

Vous trouverez également des informations complémentaires sur l'implémentation de l'Active Directory dans le chapitre Domaine Active Directory.

g. Les différents types d'enregistrement

SOA : l'enregistrement de type SOA correspond à la source de l'autorité de la zone concernée. Toutes les modifications dans la zone incrémentent un numéro de version associé à cette zone.

NS : l'enregistrement NS contient tous les serveurs de noms de serveurs autorisés à répondre pour ce domaine.

Contrairement aux autres enregistrements, les enregistrements SOA et NS sont uniques dans chaque zone.

A : l'enregistrement A définit l'adresse IP associée à un nom de machine bien précis (appelée hôte ou Host en anglais).

CNAME : l'enregistrement CNAME crée un nom (appelé Alias) dans une zone, qui pourra être associé à un enregistrement de type A dans la même zone ou dans une autre zone DNS.

MX : chaque enregistrement MX doit pointer sur un enregistrement de type A donc une machine possédant un service SMTP actif. Cet enregistrement est totalement inutile pour la messagerie interne basée sur Exchange. Lorsque plusieurs enregistrements de type MX existent, le poids (priorité) le plus faible affecté à chacun d'eux indique le serveur de messagerie à utiliser en priorité.

SRV : l'enregistrement SRV a pour fonction d'indiquer un service particulier qui sera rendu sur le port spécifié. Les services LDAP, Catalogue Global, Kerberos, SIP et bien d'autres sont basés sur ce type d'enregistrement.

PTR : ce type d'enregistrement est le pendant du type A. Il n'existe que dans les zones de recherches inversées.

D'autres types existent comme le champ TXT qui sont plus rarement utilisés et peu utiles dans le fonctionnement de Windows.

h. Les bons usages

Dans le cadre de forêts Active Directory, les bonnes pratiques visent à éviter les réplications inutiles d'informations, et donc à éviter l'usage des zones secondaires à l'origine de nombreux problèmes.

Les deux solutions à utiliser sont les stubs zones ou les redirections conditionnelles.

© ENI Editions - All rights reserved - adamo diarra

Pour les forêts et réseaux complexes, la simplification passe par l'utilisation de redirecteurs au niveau de chaque sous-domaine vers le domaine racine de chaque forêt.

Au niveau de chaque domaine racine de chaque forêt, l'utilisation d'une redirection conditionnelle vers chaque forêt suffira pour résoudre toute la forêt correspondante.

i. DNSSEC

Windows 2008 R2 propose maintenant d'augmenter la fiabilité des informations données et reçues par le service DNS. La condition principale pour utiliser DNSSEC est de disposer d'un serveur Windows 2008 R2 avec le rôle DNS installé. Le serveur n'est pas nécessairement intégré à Active Directory. En revanche, si la zone DNS que l'on veut signer est intégrée à AD, alors tous les serveurs DNS du domaine ou de la forêt gérant cette zone DNS doivent être installés en version Windows 2008 R2.

DNSSEC permet d'authentifier l'information DNS. Les zones peuvent être signées numériquement. Ces signatures sont envoyées aux clients sous la forme d'enregistrements de ressources depuis les serveurs gérant ces zones. Le client peut alors valider l'information comme authentique auprès des serveurs DNS « signés ». DNSSEC empêche ainsi des attaques de type **Man in the Middle** visant entre autres à corrompre les enregistrements en cache d'un serveur DNS afin de rediriger les utilisateurs vers des adresses IP contrôlées par un attaquant.

L'ancienne norme DNSSEC de Windows 2008 était très limitée et basée sur trois types d'enregistrements :

- **KEY** : cet enregistrement contient la clé publique indiquée dans la zone DNS du domaine.

  Cette clé peut correspondre à un serveur, la zone ou une autre entité. Les enregistrements KEY sont authentifiés par les enregistrements de type **SIG**.

- **NXT** : cet enregistrement permet d'indiquer le prochain enregistrement signé s'il existe.

- **SIG** : cet enregistrement contient la signature numérique d'une zone ou partie de zone afin d'authentifier une ressource d'un type particulier.

L'implémentation DNSSEC de Windows 2008 ne permettait ni de gérer ni de vérifier l'information transmise.

La norme utilisée par DNSSEC sous Windows 2008 R2 consiste en quatre nouveaux enregistrements de ressources :

- **DNSKEY** : enregistrement d'une clé DNSSEC.

- **RRSIG** : signature des RR existants avec DNSSEC.

- **NSEC** : Next SEC, signature des RR inexistants avec DNSSEC.

- **DS** : signature des délégations de zone dans DNSSEC.

Windows 2008 R2 peut non seulement gérer des zones signées, mais aussi recevoir des informations signées, les valider et les transmettre aux clients.

Voici les différentes étapes pour l'implémentation de DNSSEC :

- Bien vérifier les conditions d'emploi de DNSSEC dans **les points importants** indiqués à la fin de la procédure.

  Dans cet exemple, une zone simple appelée **MaSociete.FR** statique et publique contenant deux enregistrements MonSiteWeb (Type A) et WWW (Type CNAME) sera sécurisée.

- La première étape consiste à autoriser DNSSEC sur le serveur DNS.

```
DnsCmd  /config /EnableDnsSec 1
```

- Obtenir ensuite un fichier DNS contenant la zone DNS à sécuriser.

  Pour les zones DNS intégrées à AD, la commande suivante permet de générer ce fichier :

© ENI Editions - All rights reserved - adamo diarra

```
DNSCMD /ZONEEXPORT MaSociete.FR MaSocieteFR.DNS
```

Le fichier se trouve dans le dossier C:\windows\system32\dns.

Pour les autres zones, le fichier peut être récupéré directement sur le serveur DNS hébergeant la zone primaire dans le dossier cité précédemment.

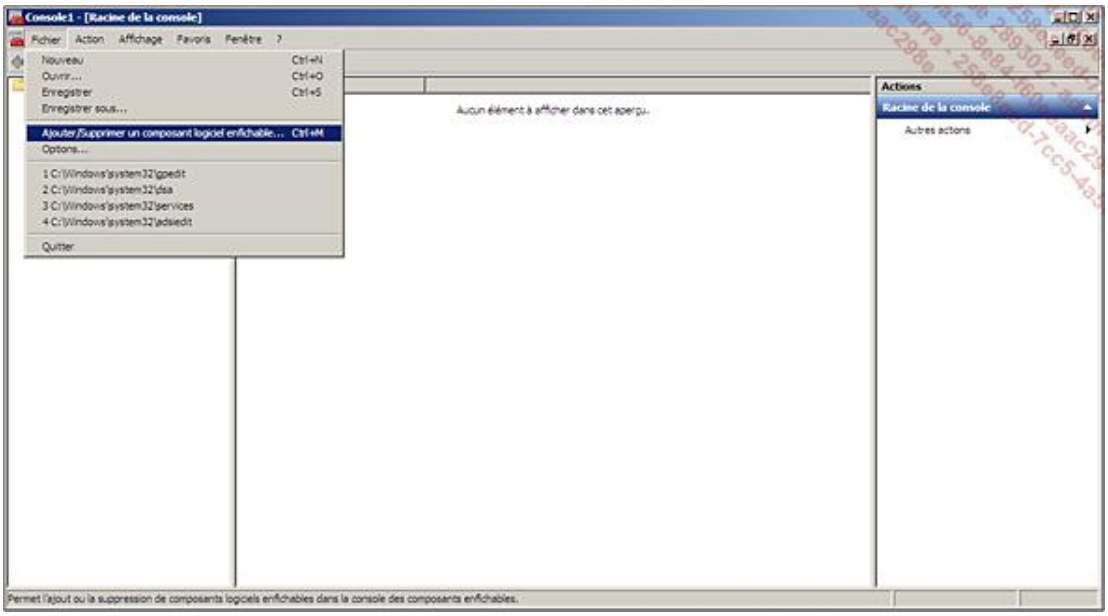
- Générer les clés de cryptage : ZSK et KSK.

ZSK (*Zone Signing Key*) : cette clé sert au cryptage de chaque élément inclus dans la zone DNS.

KSK (*Key Signing Key*) : cette clé sert à valider l'ensemble de la zone elle-même auprès des zones parentes et enfants.

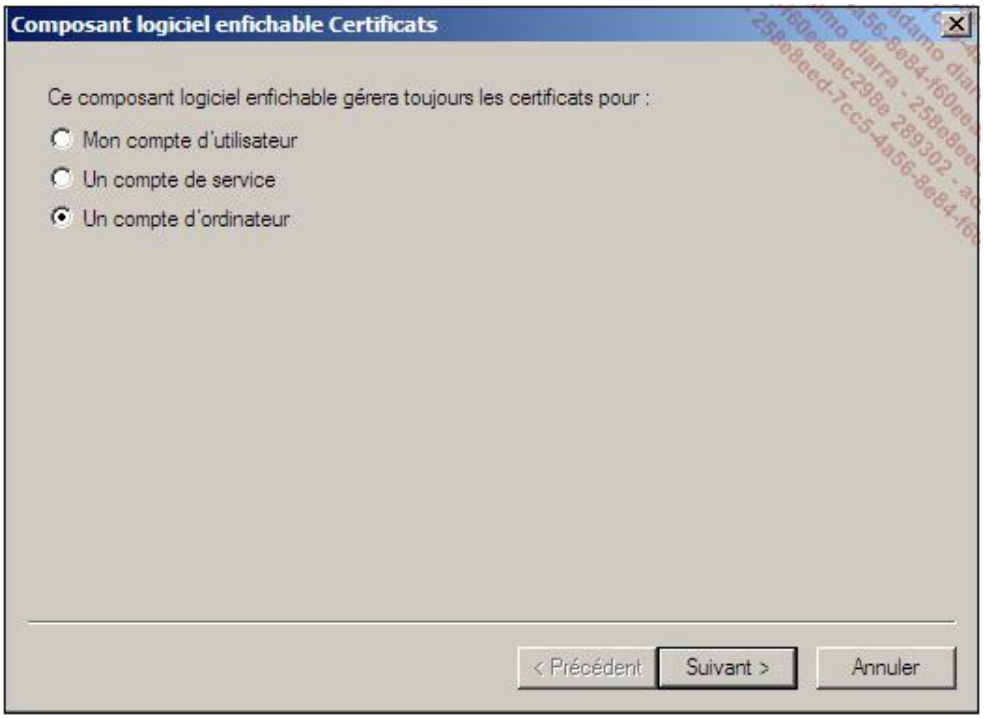
```
DnsCmd /OfflineSign /GenKey /Alg rsasha1 /Flags KSK /Length 1024
/Zone Masociete.Fr /SSCert /FriendlyName KSK-MaSociete.Fr

DnsCmd /OfflineSign /GenKey /Alg rsasha1 /Length 1024 /Zone Masociete.
/SSCert /FriendlyName ZSK-MaSociete.Fr
```

- Vérifier les clés et les sauvegardes.
    - Lancer le programme MMC.exe et cliquer sur **Fichier** puis **Ajouter/Supprimer un composant logiciel enfichable**.

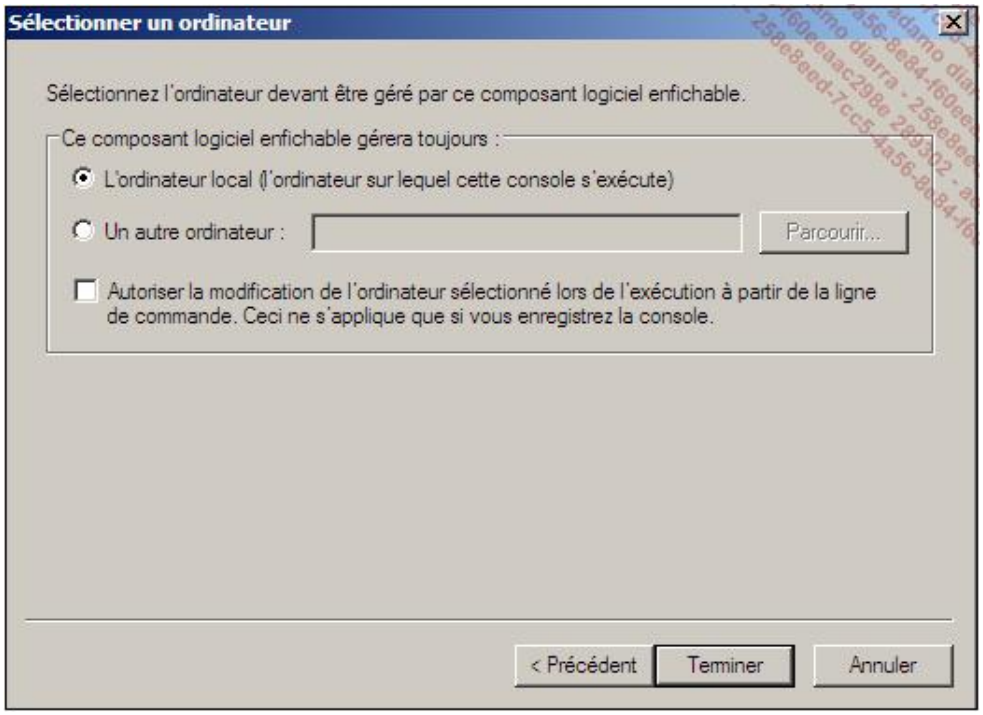


    - Ajouter le composant **Certificats**.
    - Choisir **Un compte d'ordinateur**.

© ENI Editions - All rights reserved - adamo diarra



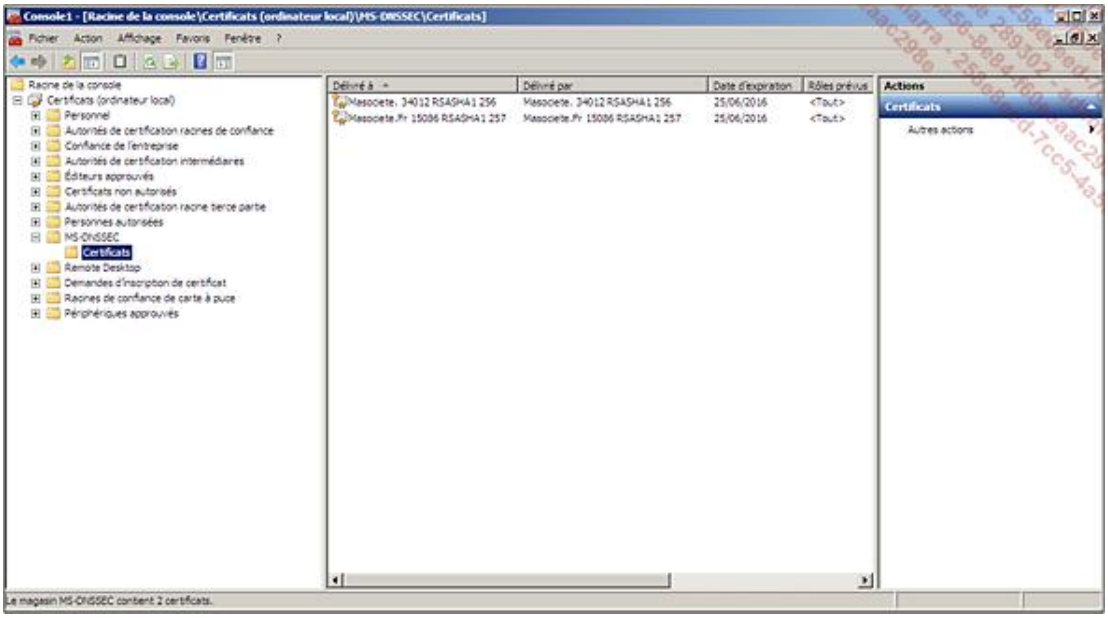
- Puis sélectionner **L'ordinateur local (...)**.



- Et cliquer sur **Terminer** et **OK**.

- Rechercher le conteneur **MS-DNSSEC**. Les deux certificats peuvent alors être exportés si nécessaire, puis placés sur un autre serveur.

© ENI Editions - All rights reserved - adamo diarra



- Signer la zone.

```
DnsCmd /OfflineSign /SignZone /input c:\windows\system32\dns\
MaSocieteFR.DNS /output
c:\temp\MaSocieteFR.DNS.SIG.TXT /zone MaSociete.FR /signkey /cert
/friendlyname ksk-MaSociete.FR
```

Cette opération crée un nouveau fichier contenant la zone et tous les enregistrements signés par les clés.

- Recharger la zone signée.

La zone DNS protégée peut maintenant être rechargée, mais ceci nécessite la suppression de l'ancienne version de la zone.

- Copier le nouveau fichier de zone dans le dossier C:\windows\system32\dns.
- Supprimer l'ancienne zone non signée.

```
DnsCmd /ZoneDelete MaSociete.Fr /DSDEL
```

Attention, l'option /DsDel n'est à ajouter que pour les zones intégrées à Active Directory.

- Charger le fichier correspondant à la nouvelle zone signée.

```
DnsCmd /ZoneAdd MaSociete.Fr /Primary /file MaSocieteFR.DNS
```

Si la zone à protéger est une zone intégrée à Active Directory, il faut lancer la commande suivante :

```
DnsCmd /ZoneResetType maSociete.local /DsPrimary
```

Pour le moment, seul le serveur DNS primaire, qui est l'autorité pour la zone signée, dispose des éléments nécessaires pour valider les enregistrements signés. Tous les autres serveurs DNS gérant la zone doivent être configurés en tant que **Trust Anchors** (**Points de validation**).

- Configurer et distribuer les points de validation de DNSSEC.

```
DnsCmd /TrustAnchorAdd MaSociete.Fr DNSKEY Flag   3   5  Binaire64
```


© ENI Editions - All rights reserved - adamo diarra

flag correspond à la valeur numérique **257** (de type compteur incrémental) trouvée dans le fichier signé de la zone.

Binaire64 correspond à la longue chaîne de chiffres et de lettres.

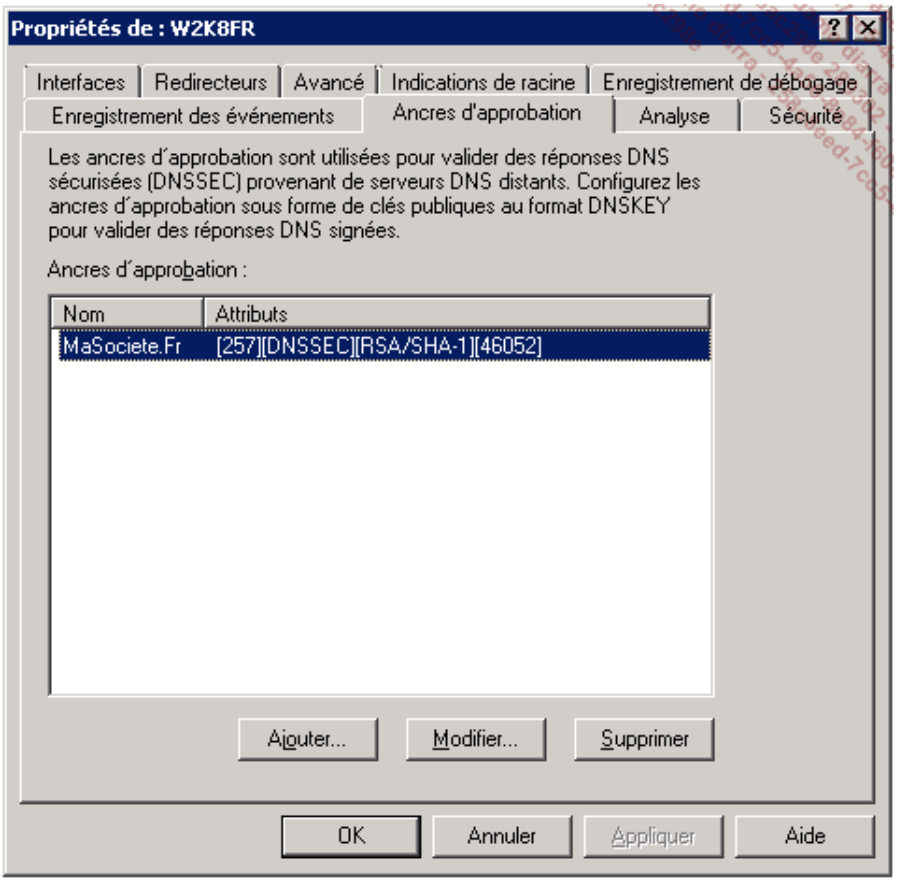
Extrait du fichier généré :

```
3600 DNSKEY 257    3    5  (
     AwEAAcBh1QEC1f7kDUGSgo7zi/72PF/r678w
     GORADrXk11rypsHlBaXc9GlyxJFiLHP1JTBY
     hnIg2kZBXhHxpEOEEdyg0dO7Gz3XtamJwhSw
     BNhuwRZmycj8olJsVzEuDXZdNdZCHem27Tag
     9Vd7H+jyMSspXutZnaMslxCsdu0Xs8Zj
     ) ; key tag = 46052
```

Attention, cette configuration ne doit pas être réalisée sur le serveur **primaire**, mais uniquement sur les autres serveurs DNS recevant les requêtes pour cette zone.

Si la zone est intégrée et que le serveur DNS est contrôleur de domaine, cette opération ne doit être réalisée qu'une seule fois pour toute la forêt.

Les ancres d'approbation sont visibles et gérables dans les propriétés du serveur DNS sur l'onglet correspondant.



Configuration des serveurs DNS intégrés à Active Directory

Idéalement, si les serveurs DNS sont contrôleurs du domaine, les stratégies sont appliquées directement sur le conteneur des contrôleurs de domaine. De même, une unité d'organisation peut être utilisée pour tous les serveurs DNS membres.

Les certificats utilisés par les serveurs DNS intégrés à AD peuvent aussi être délivrés automatiquement par une autorité de certification interne en utilisant le modèle « Directory Service Email Replication » pour créer un nouveau template incluant l'identifiant d'objet **1.3.6.1.4.1.311.64.1.1**.

Une configuration particulière est appliquée en cas d'utilisation de IPSEC afin que le protocole DNS puisse arriver de manière anonyme et authentifiée afin de provoquer la vérification des certificats.

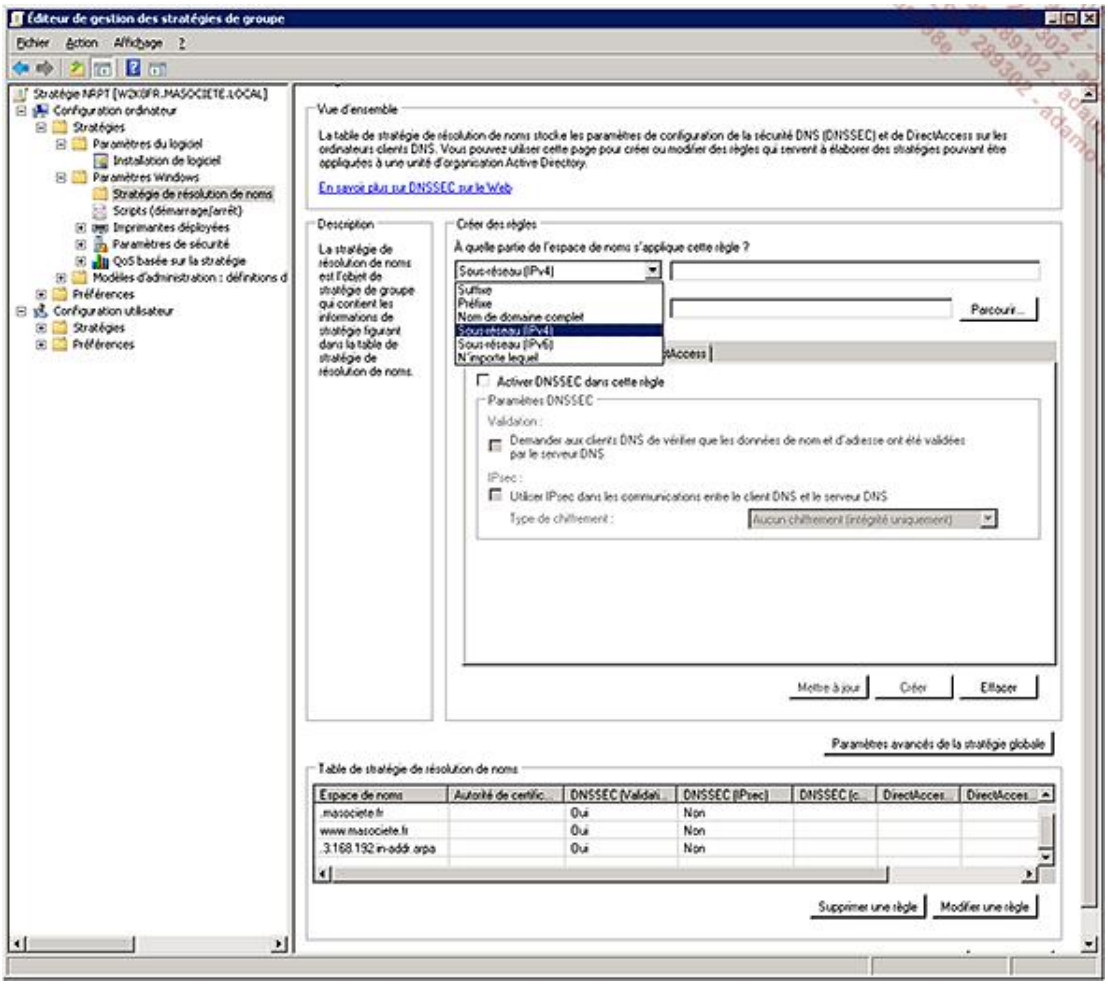
Configuration des clients de DNSSEC

Les stations ou serveurs membres prévus pour utiliser DNSSEC doivent être configurés pour utiliser une NRPT (*Name Resolution Policy Table*), c'est-à-dire un tableau reprenant une stratégie de résolution des noms.

© ENI Editions - All rights reserved - adamo diarra

Une stratégie peut être créée pour les machines membres. Les autres sont configurées directement dans les clés de registre.

La stratégie consiste en un ensemble de règles qui ne s'appliquent qu'à tout ou partie de la zone correspondante. Celle-ci se trouve dans **Configuration Ordinateur - Stratégies - Paramètres Windows - Stratégie de résolution de noms**.



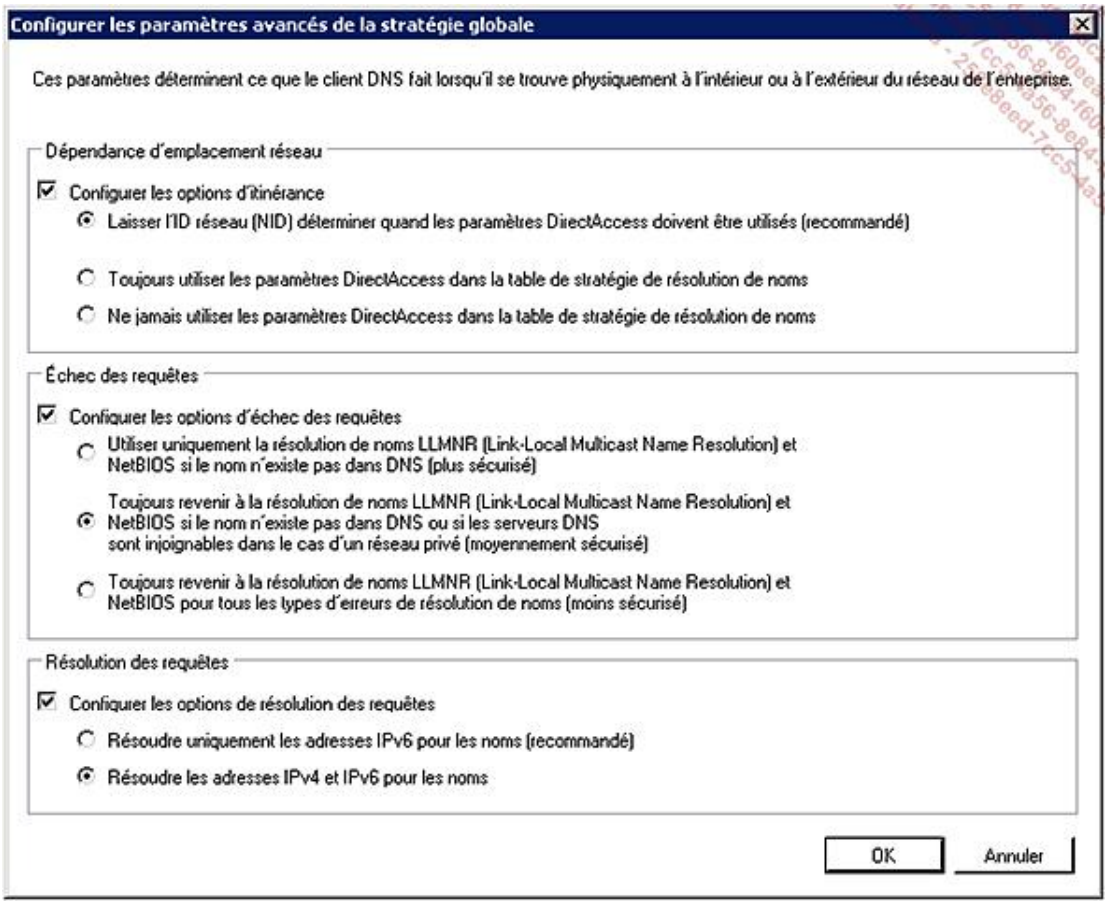
Voici les différentes règles qui peuvent être activées par cette stratégie :

- Le suffixe correspond au nom de la machine : MonSiteWeb.
- Le préfixe correspond au nom du domaine : MaSociete.fr.
- Le nom complet est la somme du préfixe et du suffixe : www.MaSociete.fr.
- Le sous-réseau (IPv4) saisi sous la forme 192.168.3.1/24 permet de sécuriser la recherche à partir de l'adresse IP pour la zone de recherche inversée : .3.168.192.in-addr.arpa.
- Le sous-réseau (IPv6) réalise la même opération pour IPv6.

Les boutons **Mettre à jour**, **Créer**, **Effacer**, mais aussi **Supprimer une règle**, **Modifier une règle** permettent d'ajouter, modifier ou supprimer l'ensemble des règles de la liste attachée à la stratégie.

Le bouton **Paramètres avancés de la stratégie globale** accède à des options complémentaires indiquant comment doit fonctionner la résolution DNS selon l'emplacement réseau, l'échec des requêtes et la résolution des requêtes.

© ENI Editions - All rights reserved - adamo diarra



Pour les machines qui n'appartiennent pas au domaine, la configuration de la table NRPT peut être réalisée manuellement dans la stratégie locale. Si l'on souhaite réaliser un script pour appliquer cette stratégie, il suffit d'exporter la clé **HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig** dans un fichier **NRPT.REG** avec l'outil REGEDIT, puis de l'appliquer avec l'instruction **REGEDIT /S NRPT.REG**.

Plusieurs points importants sont à prendre en compte lors de l'utilisation de DNSSEC :

- Attention, ce choix implique que la zone n'accepte plus les mises à jour dynamiques ! La zone devient automatiquement statique.

  Ce type de zone sera donc utilisée le plus souvent pour les racines de forêt ou pour les zones accédées depuis Internet.

- Le renouvellement des clés.

  L'utilisation de clés sécurisées par des certificats suppose de prévoir le mécanisme de renouvellement régulier des clés.

- L'ajout et la suppression d'enregistrements se réalisent hors-ligne et provoquent la nécessité de signer à nouveau la zone. En revanche, de nouveaux certificats ne sont pas nécessaires.

- La sécurité fournie par DNSSEC ne fonctionne qu'avec les systèmes possédant un client DNS compatible et sur les ordinateurs Windows 7 ou Windows 2008 R2.

2. La résolution WINS

En théorie, cette résolution ne devrait plus être utilisée sauf pour intégrer d'anciens domaines NT4. En pratique, il arrive que celle-ci soit nécessaire (voire très pratique) pour certaines vieilles applications de Microsoft ou non, mais aussi pour des applications très récentes comme Exchange 2007 (dans des cas très particuliers).

Lors d'une migration ou lorsqu'il y a un doute pour le fonctionnement de certaines applications, il est courant de garder un ou deux serveurs WINS sur le site central. Les stations et serveurs utilisant ce type d'application

© ENI Editions - All rights reserved - adamo diarra

pointeront directement sur ce serveur WINS. Il est ainsi inutile de maintenir et de répliquer les serveurs WINS à travers tout le réseau.

a. Définition

WINS (*Windows Internet Naming Service*) est un service basé sur une base de données Jet permettant de retrouver l'adresse IP d'un nom Netbios, et réciproquement.

Contrairement à DNS, WINS maintient des informations sur les groupes de machines, mais aussi sur les utilisateurs connectés aux machines.

b. L'installation

L'installation de WINS se fait par l'ajout de la fonctionnalité correspondante :

```
servermanagercmd -install WINS-Server
```

c. La configuration

Sauf dans de rare cas où il faut entrer manuellement un nom (dit statique) et une adresse IP, il n'est pas nécessaire de configurer un serveur WINS qui reçoit dynamiquement toute l'information nécessaire par le serveur et les clients qui s'inscrivent automatiquement dans la base.

Le seul élément particulier de la réplication consiste à répliquer la base entre deux serveurs WINS, voire plus dans certains cas.

d. La réplication entre serveurs WINS

La réplication WINS est basée sur deux opérations : l'émission et la collecte.

Pour qu'une réplication WINS fonctionne dans un sens, un serveur WINS doit être configuré pour émettre les modifications qu'il reçoit vers un autre serveur WINS, mais il faut aussi que l'autre serveur WINS soit configuré pour collecter les informations en provenance du serveur émetteur en question.

Pour une réplication fonctionnant dans les deux sens entre deux serveurs WINS, il faut et il suffit que chaque serveur soit configuré en mode **Emission/Collecte** pour le serveur distant.

e. Quand et pourquoi utiliser WINS ?

Attention, il ne faut plus voir WINS comme une solution à part entière. Car DNS est maintenant indispensable.

WINS est simplement une solution pour résoudre des problèmes marginaux de fonctionnement d'applicatifs ou d'accès qu'il serait trop complexe de résoudre autrement.

Le cas le plus concret, comme pour Exchange dans certaines parties, est le logiciel qui n'a prévu que des noms de serveurs **simples** et relativement **courts**.

L'installation d'un service WINS unique, centralisé qui ne serait utilisé que par les quelques stations ou serveurs qui en ont vraiment besoin répond très bien à ce type de problème.

© ENI Editions - All rights reserved - adamo diarra

La mise en place de la quarantaine réseau

La quarantaine réseau n'est pas une véritable solution de sécurité, mais c'est un élément dont l'objectif est de maintenir en bonne santé les éléments présents sur le réseau.

1. La préparation de l'environnement commun aux différents types de quarantaine

L'utilisation du client NAP (*Network Access Protection*) est basée sur l'utilisation d'un NPS (*Network Policy Server*), c'est-à-dire un serveur de stratégies réseau, qui permet de définir des restrictions souhaitées.

Il est donc nécessaire d'installer et de configurer ce rôle :

```
servermanagercmd -install NPAS-Policy-Server
```

Après l'installation, différents points sont à définir pour des stratégies fonctionnelles :

- Un système de validation (SHV), c'est-à-dire de tests à réaliser pour vérifier un système.

  Windows 2008 R2 autorise maintenant plusieurs configurations différentes du système de validation. Lors de la configuration de la stratégie de santé de l'intégrité du système, il est possible de sélectionner l'une de ces configurations. Chaque stratégie réseau peut être configurée pour utiliser une ou plusieurs stratégies de santé.

- Un groupe de serveurs de **remediation** : ce sont les serveurs vus et autorisés par les stations non conformes afin de se mettre en conformité avec la politique de sécurité décidée.

- Des stratégies de **santé**, qui définissent comment les SHVs sont interprétés.

- Des stratégies de réseau.

Le kit d'intégration **ForeFront for NAP** (gratuit) doit être téléchargé afin de disposer d'un système de validation complémentaire. Différents modules doivent être chargés sur les machines en fonction du type de processeurs (32 ou 64 bits), le module SHV sur les serveurs NPS, le module SHA sur les clients à valider.

La première étape consiste à définir les tests que l'on souhaite réaliser sur les machines disposant du client NAP, c'est-à-dire Windows XP SP3, Windows Vista ou Windows 7.

- Dans l'administration du serveur NPS, **Protection d'accès réseau**, sélectionnez le conteneur **Programmes de validation d'intégrité système**.

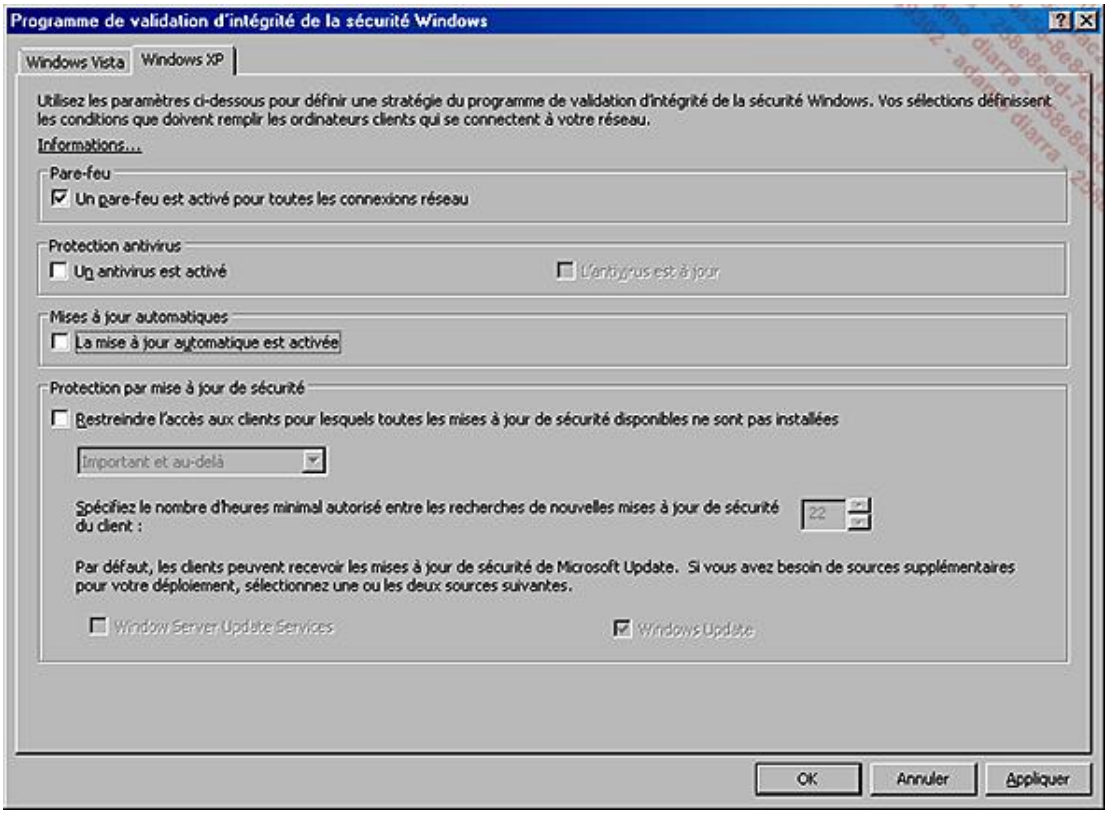
- Configurez ensuite le système de validation fourni par défaut appelé **Validateur d'intégrité de la sécurité Windows**.

- Dans les paramètres principaux, on considère que si les programmes de validation d'intégrité ne répondent pas ou ne peuvent pas répondre, le client sera réputé **Non Conforme**. Mais pour chaque situation, l'adaptation du statut est modifiable.

- Cliquez sur le bouton **Configurer** pour accéder aux propriétés à tester. À noter qu'il y a un onglet pour Windows XP et un autre pour Windows Vista et Windows 7.

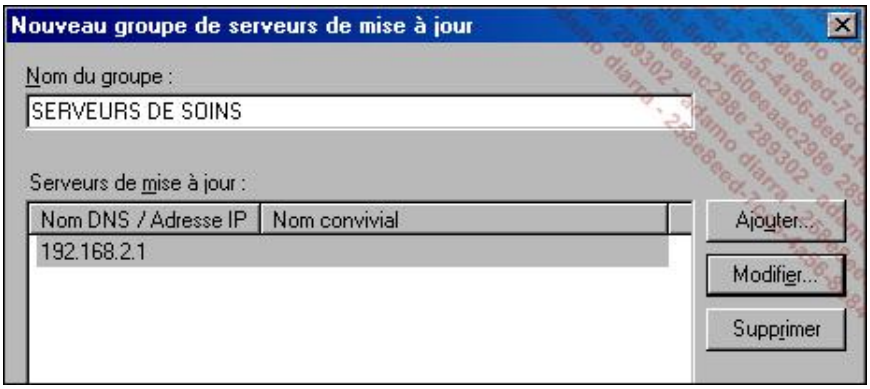
Dans le cadre de cette mise en place de test, une configuration simplifiée basée sur la présence du pare-feu sera utilisée.

© ENI Editions - All rights reserved - adamo diarra



Windows 2008 R2 ajoute la possibilité de vérifier si l'antivirus est non seulement actif, mais aussi à jour.

La deuxième étape consiste à définir un groupe contenant les serveurs autorisés pour réaliser la remise aux normes demandées dans les groupes de serveurs de mise à jour.



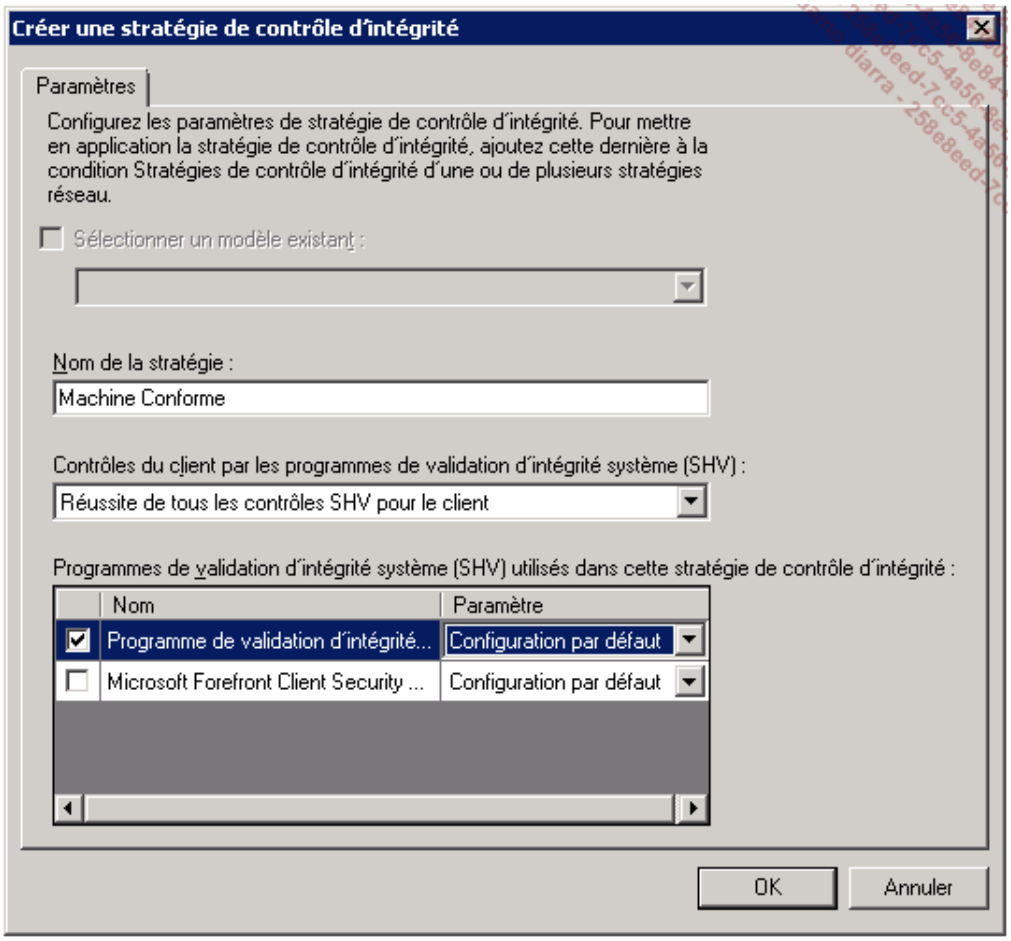
Les machines non conformes pourront se connecter aux serveurs indiqués si la **mise à jour automatique** (Remediation) est autorisée dans la stratégie réseau.

La troisième étape consiste à créer au moins deux stratégies de santé différentes dans les stratégies de contrôle d'intégrité.

a) Une pour les machines conformes :

Seuls les validateurs activés entrent dans la règle de conformité !

© ENI Editions - All rights reserved - adamo diarra



Windows 2008 R2 ajoute la possibilité de sélectionner une configuration spécifique parmi celles proposées et configurées précédemment.

b) Une pour les machines non conformes :

Sélectionnez le même validateur que pour une machine conforme, mais définissez la règle sur **Echec d'un ou de plusieurs contrôles SHV pour le client**.

La quatrième étape est la création des stratégies réseau.

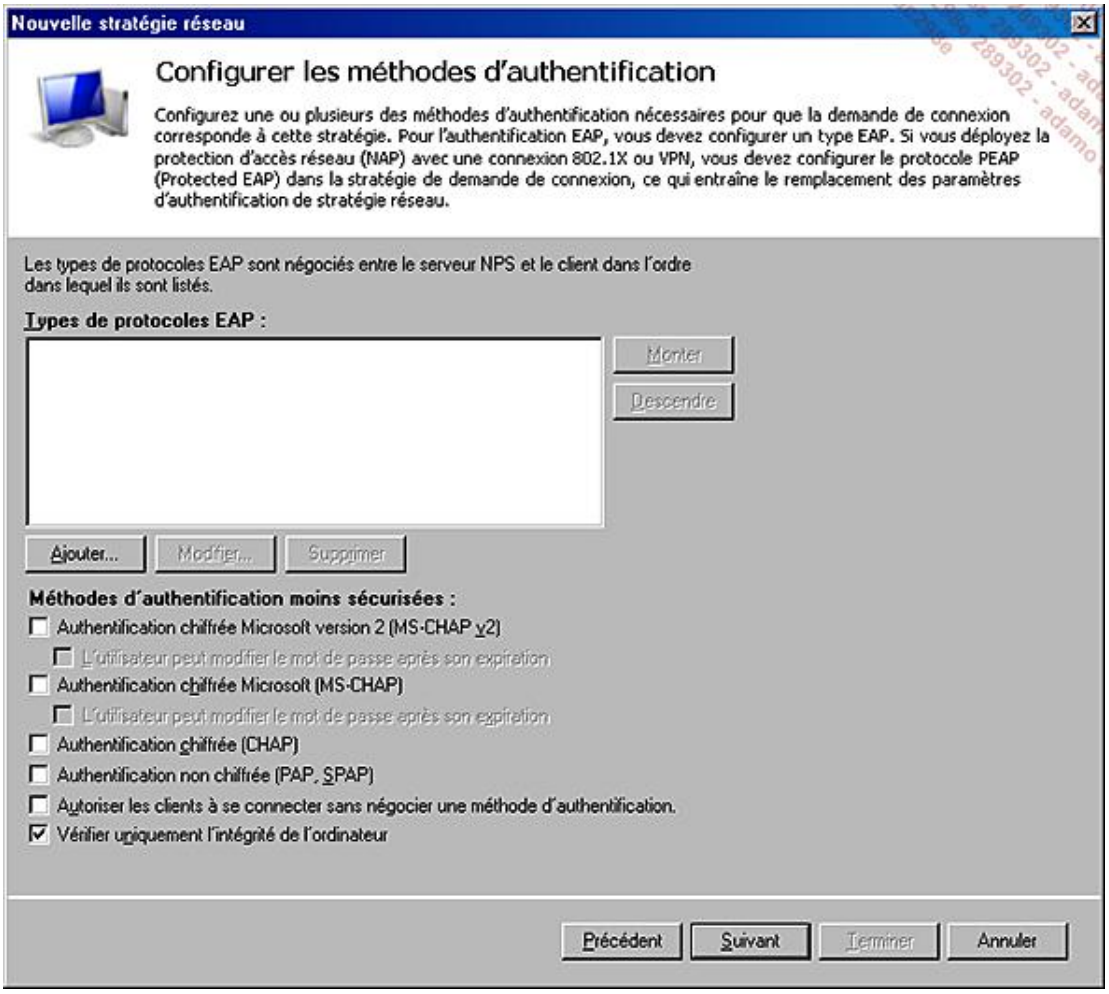
a) Création de la stratégie réseau pour les machines conformes :

- Cliquez avec le bouton droit sur **Stratégies Réseau**. Puis choisissez **Nouveau** dans le menu.
- Nommez la stratégie **Accès complet pour les machines conformes**, laissez le type de réseau sur **Non spécifié**.

Non spécifié signifie que la stratégie sera appliquée quel que soit le type d'accès réseau utilisé.

- Sur l'écran **Spécifier les conditions**, il est impératif de préciser à qui s'applique cette stratégie, cliquez sur **Ajouter**.
- De nombreuses conditions complexes peuvent être appliquées, sélectionnez **Stratégies de contrôle d'intégrité**.
- Choisissez dans la liste proposée la stratégie **Machine Conforme**, puis passez à l'écran suivant.
- Spécifiez **Accès accordé**, ce qui est logique pour des machines conformes !
- Aucune authentification n'est requise pour ce type de quarantaine, sélectionnez donc **Vérifier uniquement l'intégrité de l'ordinateur**.

© ENI Editions - All rights reserved - adamo diarra



- Sur l'écran **Configurer des contraintes**, aucune valeur n'est à modifier.

- Sur l'écran **Configurer les paramètres**, il s'agit d'appliquer une configuration (modification) du client réseau. Ici, dans la section **Protection d'accès réseau**, on va **Autoriser un accès réseau complet**.

- Cliquez sur **Terminer** sur l'écran final qui résume l'ensemble de la stratégie.

b) Création de la stratégie réseau pour les machines non conformes :

- Cliquez avec le bouton droit sur **Stratégies Réseau** puis choisissez **Nouveau** dans le menu.

- Nommez la stratégie **Accès complet pour les machines non conformes**, laissez le type de réseau sur **Non spécifié** comme pour les machines conformes.

- Sur l'écran **Spécifier les conditions**, il est impératif de préciser à qui s'applique cette stratégie, cliquez sur **Ajouter**.

- De nombreuses conditions complexes peuvent être appliquées, sélectionnez **Stratégies de contrôle d'intégrité**, puis choisissez dans la liste proposée la stratégie **Machine non Conforme**, puis passez à l'écran suivant.

- Spécifiez **Accès accordé**. En effet, même pour des machines non conformes, il s'agit d'une règle qui va aussi autoriser un accès mais seulement aux éléments autorisés !

- Aucune authentification n'est requise pour ce type de quarantaine, sélectionnez donc **Vérifier uniquement l'intégrité de l'ordinateur** comme pour les machines conformes.

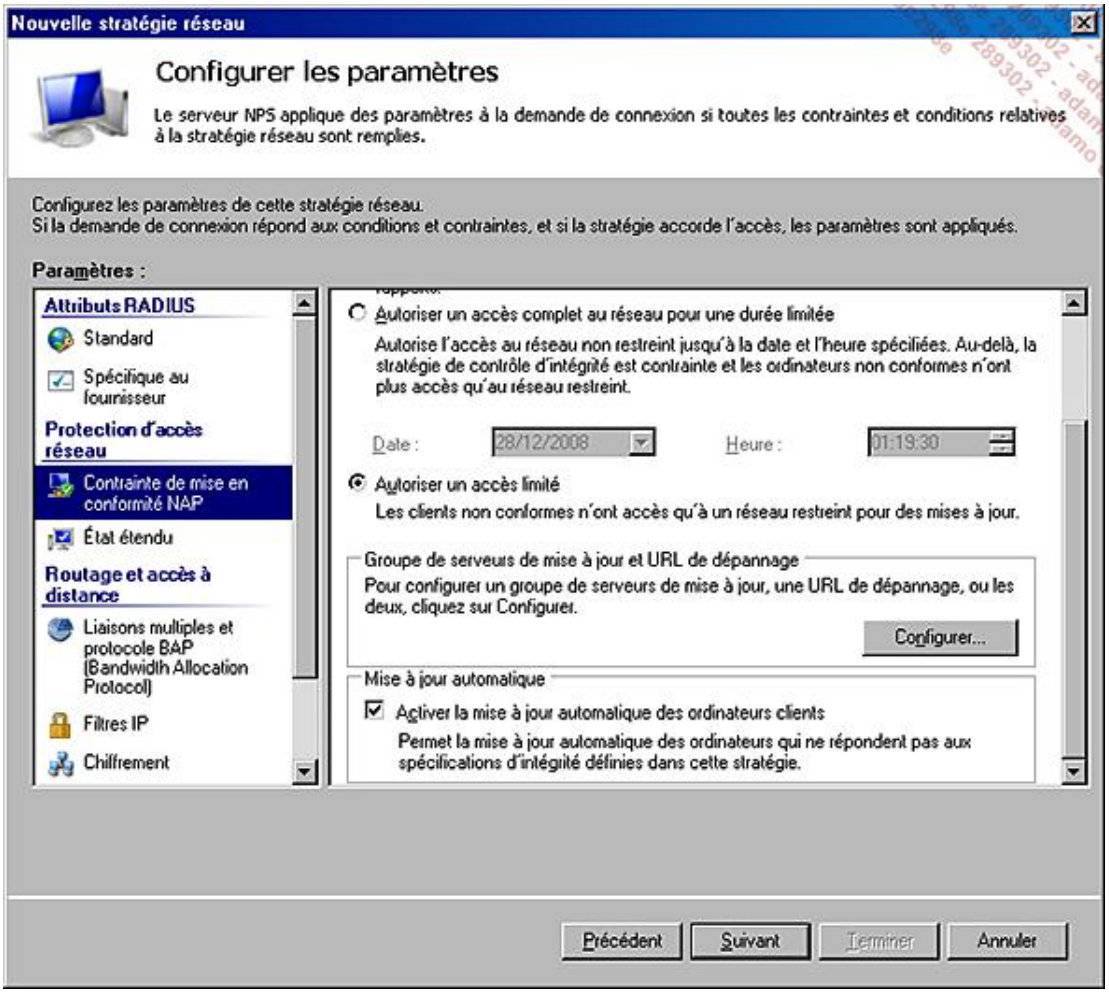
- Sur l'écran **Configurer des contraintes**, aucune valeur n'est à modifier.

© ENI Editions - All rights reserved - adamo diarra

- Sur l'écran **Configurer les paramètres**, il s'agit d'appliquer une configuration (modification) du client réseau. Ici, dans la section **Protection d'accès réseau**, on va **Autoriser un accès limité**.

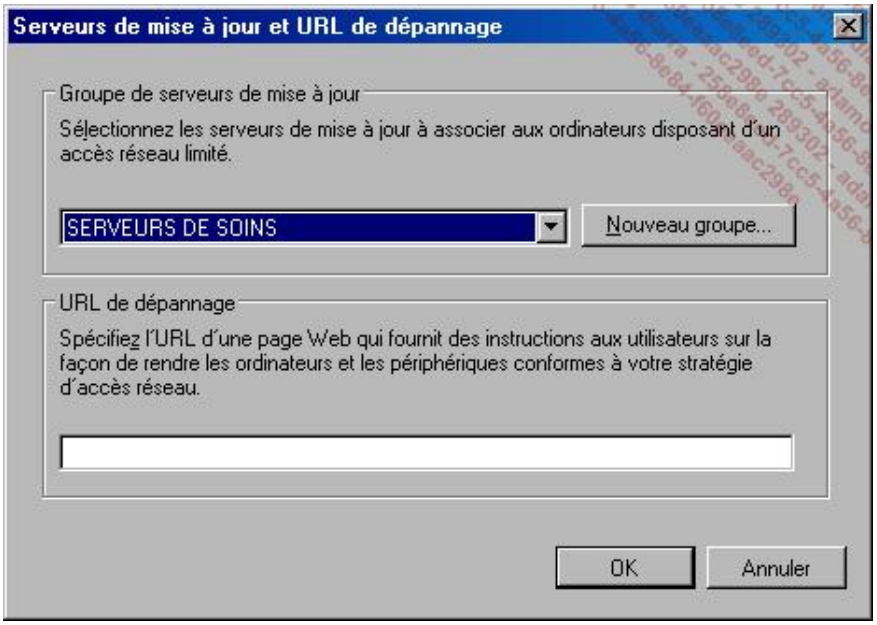
Le choix d'**autoriser un accès limité** ne doit être effectué que si l'on est sûr des effets de sa stratégie. Il est souvent préférable d'autoriser d'abord un accès complet, d'utiliser le mode rapport pour avoir une idée de l'étendue des machines qui seraient impactées.

- Si l'on veut autoriser la remise à niveau automatique (et donc autoriser les serveurs de remediation), il faut cocher la case **Activer la mise à jour automatique des ordinateurs clients**.



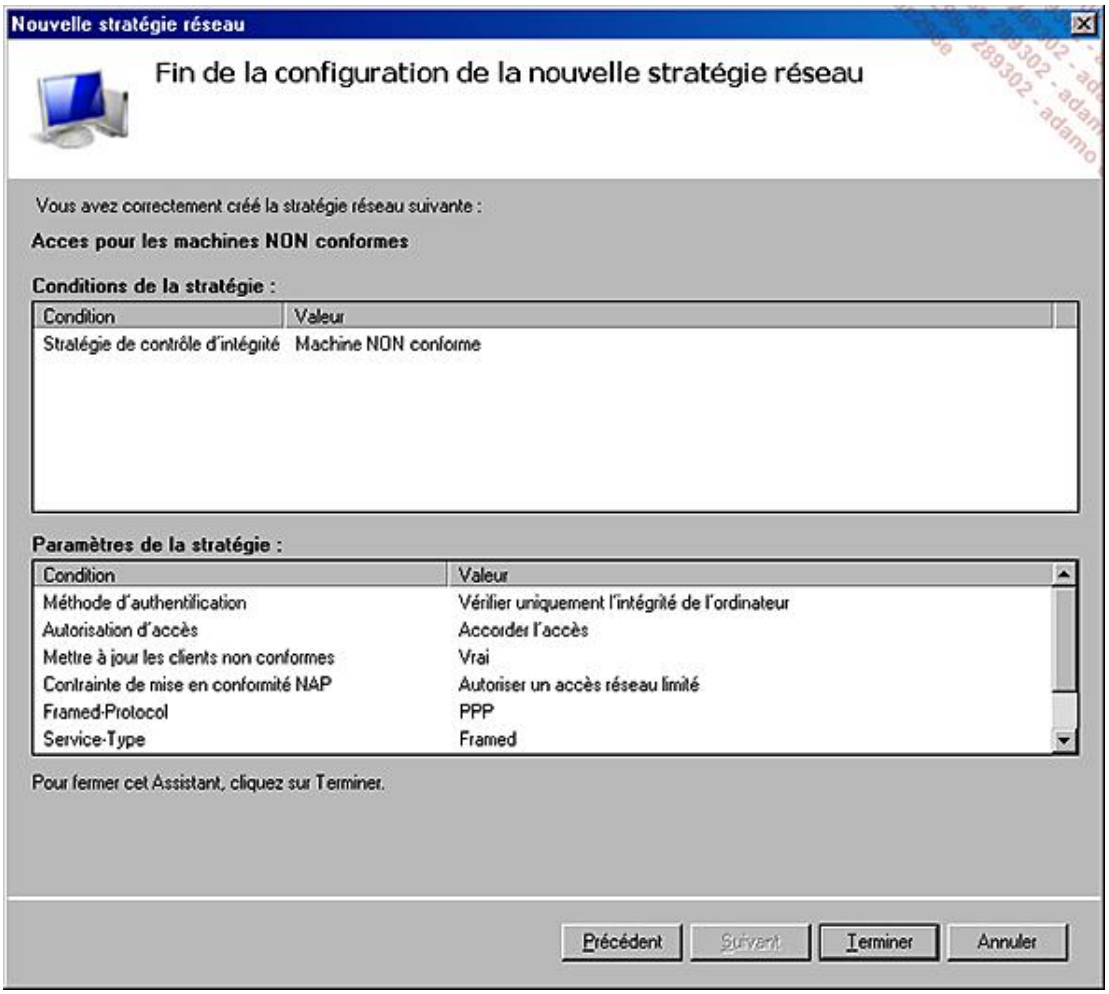
- Cliquez sur **Configurer** pour spécifier un **Groupe de serveurs de mise à jour** ainsi que l'adresse d'une page Web optionnelle d'explication pour les utilisateurs.

© ENI Editions - All rights reserved - adamo diarra



Sur les clients restreints, chaque serveur indiqué dans ce groupe dispose de sa propre route avec un masque à 255.255.255.255. Assez logiquement, les autres serveurs ne sont pas accessibles.

- Cliquez sur **Terminer** sur l'écran final qui résume l'ensemble de la stratégie.



À noter que, selon la répartition des rôles sur les différents serveurs autorisés, la réparation automatique (remediation) peut parfois nécessiter un accès complet.

Le client **Agent de protection d'accès réseau** doit être actif sur les postes clients, c'est-à-dire que le service doit être en démarrage automatique.

© ENI Editions - All rights reserved - adamo diarra

Le Centre de sécurité doit être activé, ce qui peut être forcé par une stratégie.

La console du client NAP (`NAPCLCFG.MSC`) permet de vérifier les contraintes mises en place.

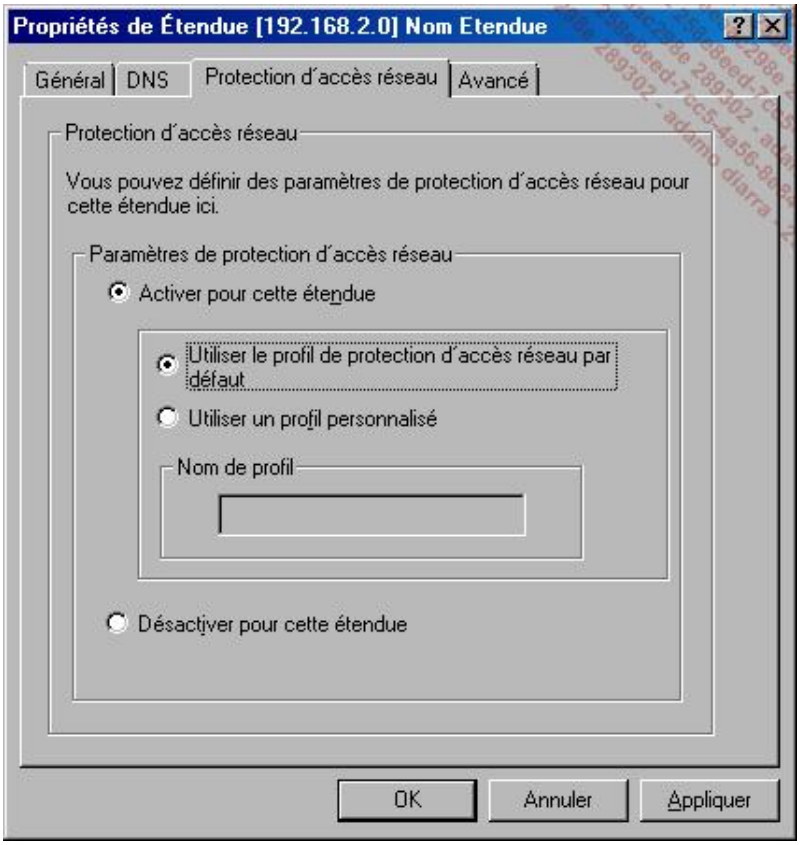
La commande `Napstat` permet de vérifier la conformité par rapports aux règles établies.

2. La mise en place de NAP via DHCP

Lorsque les préparations initiales décrites plus haut ont été réalisées, il ne reste que peu d'étapes à ajouter pour que NAP sur DHCP fonctionne.

L'étendue DHCP doit tout d'abord être activée pour utiliser la sécurité basée sur NAP.

Dans les propriétés de l'étendue, vous trouverez l'onglet **Protection d'accès réseau**.



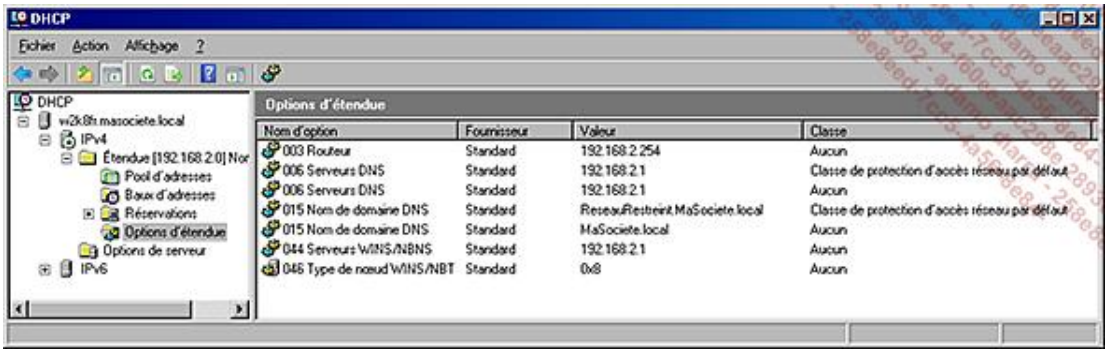
Les machines qui sont conformes aux pré-requis utilisent les options que vous avez configurées dans les **options standard DHCP** (Classe du fournisseur), pour la **Classe utilisateur par défaut**.

Le **profil de protection d'accès réseau par défaut** correspond à la classe d'utilisateur **Classe de protection d'accès réseau par défaut** qui est accessible dans les paramètres avancés des propriétés de l'étendue. Les machines non conformes utiliseront les options définies au niveau de cette classe.

Seules les options souhaitables sont à définir, donc par exemple :

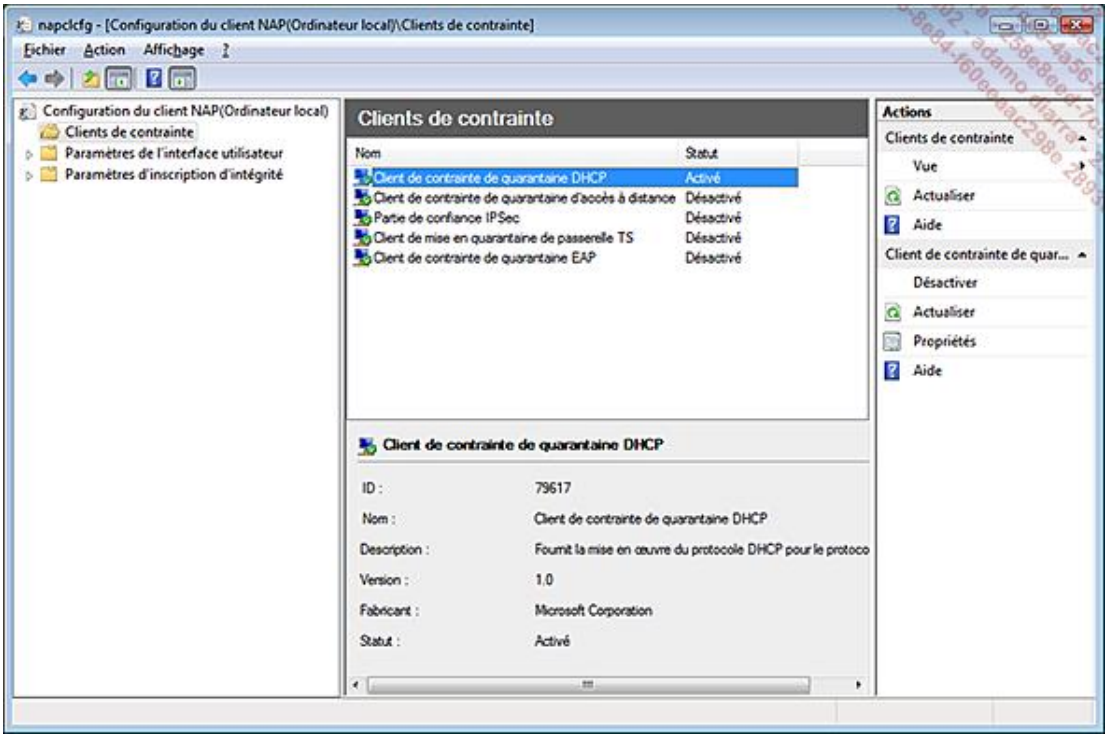
- un serveur DNS spécifique ou non permettant d'atteindre ou de résoudre certains noms ;
- une zone DNS fictive ou non mais spécifique pour identifier rapidement les machines non conformes ;
- pas de routeur pour empêcher la machine d'accéder à des parties de réseau à protéger.

© ENI Editions - All rights reserved - adamo diarra



Les options particulières apparaissent avec une classe réseau spécifique.

La stratégie de quarantaine DHCP peut maintenant être activée sur DHCP, soit par une stratégie, soit directement dans l'**outil de configuration du client NAP** que l'on peut lancer par la commande `NAPCLCFG.MSC`.



En cas d'arrêt du service **Pare-Feu Windows**, la station ne sera plus conforme. Si la mise à jour automatique a été autorisée et que les serveurs de dépannages sont accessibles, les réparations sont effectuées immédiatement. Dans notre cas, le redémarrage immédiat du service Pare-Feu remet la station en conformité et fonctionnelle.

Utilisez la commande `napstat.exe` pour vérifier le statut de conformité des stations par rapport aux stratégies mises en place. Une icône vient se placer dans la zone de notification et reste en place tant que l'on ne ferme pas l'outil.

La quarantaine réseau basée sur DHCP est la plus faible des protections possibles, qui est facilement contournée par tout utilisateur disposant des droits d'administrateur local de son poste.

3. La mise en place de NAP via IPSec

a. Installation du service Autorité HRA

Cette sécurité nécessite l'installation du service **Autorité HRA** (*Health Registration Authority*).

```
servermanagercmd -install NPAS-Health
```

L'installation d'une autorité de certification de type Entreprise est nécessaire si aucun autre système de distribution de clé (PKI) n'est en place. L'utilisation du rôle Microsoft correspondant simplifie énormément la tache. Il est fortement conseillé d'utiliser l'interface graphique pour passer par l'assistant de création du certificat racine.

© ENI Editions - All rights reserved - adamo diarra

Afin de limiter l'application de la quarantaine basée sur IPSec, il est prudent de créer des groupes d'ordinateurs pour chaque catégorie.

- Les ordinateurs clients de NAP IPSec : c'est-à-dire toutes les stations qui doivent se conformer aux règles de sécurité.

- Les serveurs dits de frontière (**Boundary**) qui reçoivent automatiquement un certificat de **santé** et qui servent à l'authentification des clients. Les contrôleurs de domaine, les serveurs DNS et les serveurs de **réparation** (Remediation) doivent faire partie de ce groupe.

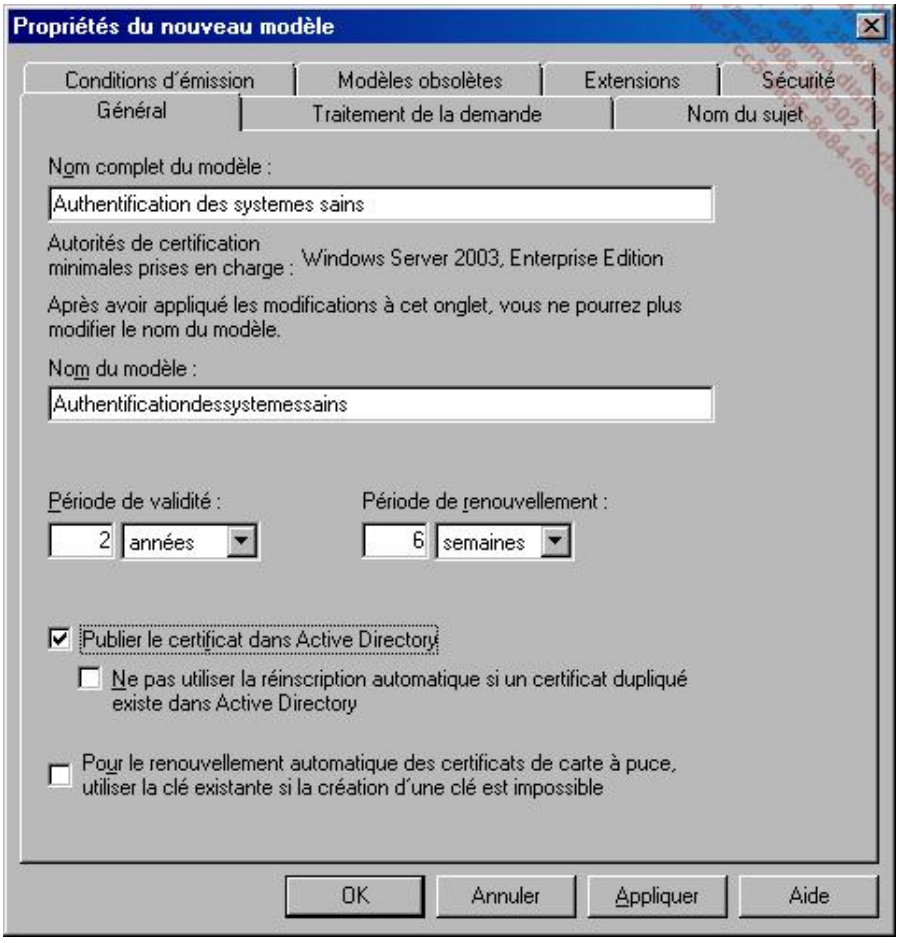
- Les ordinateurs protégés par NAP IPSec : ceux-ci reçoivent aussi automatiquement un certificat et n'autoriseront la connexion que depuis des machines authentifiées.

Chaque machine (stations ou serveurs) doit pouvoir recevoir un certificat. Or, le certificat transmis par défaut aux stations ne contient pas la stratégie d'authentification adéquate.

- Créez un nouveau certificat **Authentification de station de travail** en dupliquant le modèle existant à partir de la **console des Modèles de Certificats** que l'on peut obtenir directement par la commande `certtmpl.msc`.

- Lors de la duplication, choisissez la compatibilité Windows 2003 ou Windows 2008. Dans tous les cas, une version Enterprise est nécessaire pour que la distribution des certificats soit automatique.

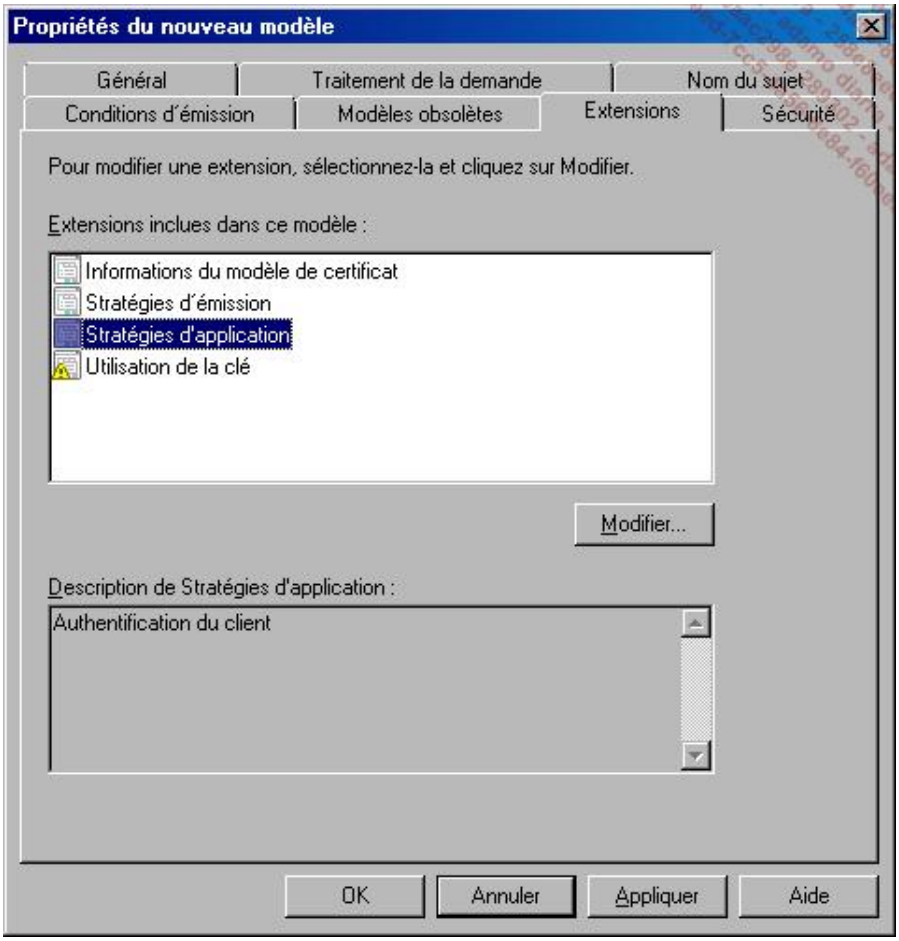
- Nommez le certificat, modifiez la période de validité et publiez le certificat dans Active Directory.



Les serveurs impliqués dans la validation ont effectivement un certificat validé pour deux ans. En revanche, les ordinateurs qui demanderont la validation n'obtiendront qu'un certificat d'une durée de vie de quatre heures.

- Dans l'onglet **Extensions**, sélectionnez **Stratégies d'application**, et ajoutez la stratégie **Authentification** de l'Agent SHA (*System Health*).

© ENI Editions - All rights reserved - adamo diarra



- Au niveau de l'onglet **Sécurité**, ajoutez les groupes des serveurs de type frontière et des serveurs Protégés, et donnez les droits **Inscrire** et **Inscription automatique**.

- Dans la console **Autorité de Certification**, sur le conteneur des modèles de certificats, utilisez le bouton droit et choisissez **Modèle de certificats à délivrer**, puis le modèle **Authentification des systèmes sains**.

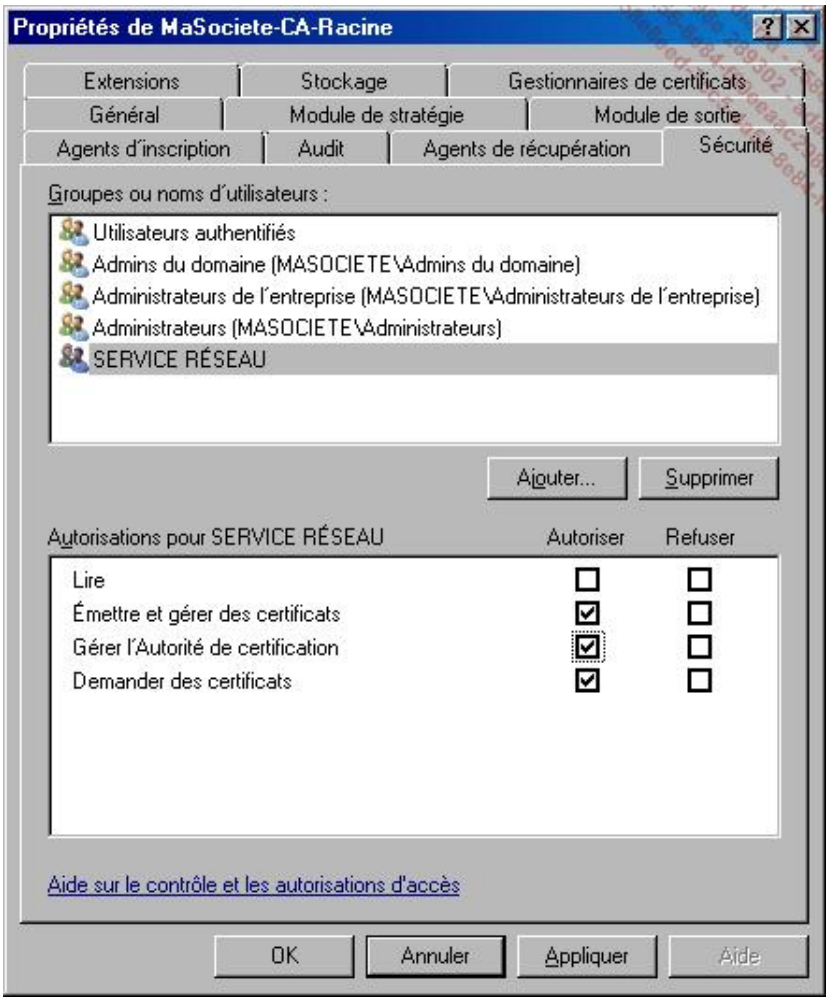
- Comme la validation des clients nécessitera régulièrement des certificats de **bonne santé**, il est important de vérifier que le module de stratégie (sur le certificat de la racine) soit configuré sur **Emettre automatiquement le certificat**.

- Les clients doivent être configurés pour demander automatiquement les certificats. Dans l'outil GPMC (Gestion de Stratégie de Groupe), configurez la **demande automatique de certificats dans la Default Domain Policy**. Ceci se trouve dans **Paramètres Windows - Paramètres de sécurité - Stratégies de clé publique**.

- Utilisez le bouton droit dans **Configuration ordinateurs** - **Paramètres Windows** - **Paramètres de sécurité** - **Stratégie de clé publique** - **Paramètres de demande automatique de certificats** - sur la stratégie **Client des services de certificats - Inscription automatique**.

© ENI Editions - All rights reserved - adamo diarra

Le compte **SERVICE RÉSEAU** (si le CA et le HRA sont sur la même machine) ou l'ordinateur sur lequel est installé le système de validation (HRA) doit obtenir les droits suivants :



© ENI Editions - All rights reserved - adamo diarra

La commande suivante permet au système validateur de demander des certificats avec une durée de vie différente de la validité de deux ans définie et imposée dans le modèle.

```
certutil -setreg policy\editflags +EditF_attributeEndDate
```

b. Configuration du système de validation (HRA)

- Créez une console MMC et ajoutez le composant **Autorité HRA (Health Registration Autority)**.
- Ajoutez l'autorité de certification à partir de AD.
- Modifiez les propriétés de l'autorité de certification, notamment pour valider l'autorité de certification de l'entreprise, et les modèles de certificats à utiliser.

Dans l'outil d'administration NPS, la réparation automatique doit être désactivée.

Sur le poste client, pour activer IPSec sur XP SP3, il est nécessaire de passer par la ligne de commande suivante :

```
netsh nap client set enforcement ID =79619
```

Chaque contrainte (Enforcement) dispose d'un identifiant spécifique :

- DHCP = 79617
- RAS = 79618
- IPSec = 79619
- TS Gateway = 79621
- EAP = 79623

À noter que si l'ordinateur n'est plus conforme, le certificat reçu sera invalidé immédiatement sans attendre les quatre heures.

© ENI Editions - All rights reserved - adamo diarra

Pour le moment, aucune restriction n'est apportée sauf le fait de disposer d'un certificat. Ces restrictions sont apportées par trois stratégies basées sur les groupes de sécurité créés au départ.

c. Définition des règles de sécurité de connexion

Ces stratégies peuvent être définies à la racine du domaine puisqu'un filtrage basé sur les groupes de sécurité sera mis en place.

Les serveurs de frontière doivent demander, mais ne pas imposer, des certificats de santé. Les serveurs protégés et les postes clients doivent imposer des certificats, néanmoins des stratégies différentes sont préférables afin d'ajouter des configurations spécifiques pour les clients (URL de configuration HRA).

Voici la stratégie à mettre en place sur les serveurs de frontière (Boundary) :

- Dans **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Pare-feu Windows avec fonctions avancées de sécurité - Pare-feu Windows avec fonctions avancées de sécurité - LDAP...** créez une nouvelle règle de sécurité dans **Règles de sécurité de connexion**, choisissez **Isolation** puis **Demander l'authentification des connexions entrantes et sortantes**, puis l'authentification par **Certificat d'ordinateur**.
- Indiquez votre autorité de certification du domaine, et cochez la case **N'accepter que les certificats d'intégrité**.
- Laissez cochés tous les profils qui s'appliquent **Domaine**, **Privée**, **Publiques**.
- Nommez cette règle **REGLE NAP IPSEC Frontière**.
- Sur l'onglet **Etendue de la stratégie**, ajoutez un filtrage de sécurité pour le groupe **Serveurs IPSEC de Frontière**.

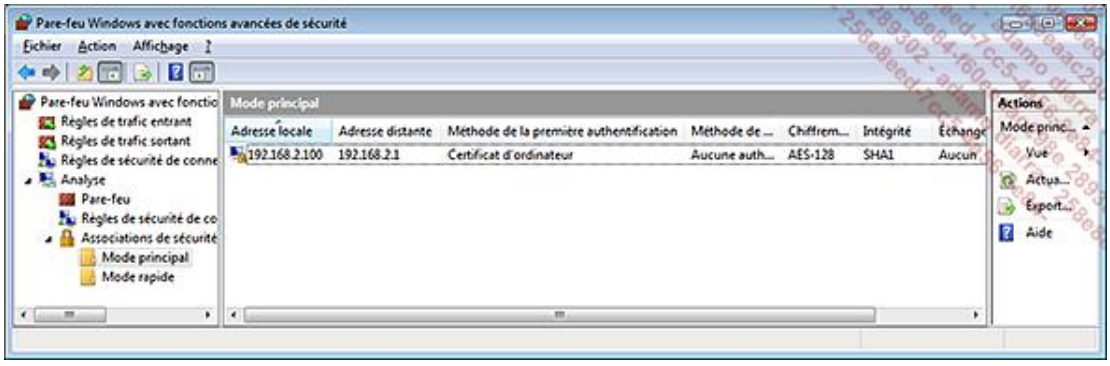
Voici la nouvelle stratégie à mettre en place sur les clients :

- Dans **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Pare-feu Windows avec fonctions avancées de sécurité - Pare-feu Windows avec fonctions avancées de sécurité - LDAP...** créez une **nouvelle règle** de sécurité dans **Règles de sécurité de connexion**, choisissez **Isolation**, puis **Imposer l'authentification des connexions entrantes et demander l'authentification des connexions sortantes**, puis l'authentification par **Certificat d'ordinateur**.
- Indiquez votre autorité de certification du domaine, et cochez la case **N'accepter que les certificats d'intégrité**.
- Laissez cochés tous les profils qui s'appliquent **Domaine**, **Privée**, **Publiques**.
- Nommez cette règle **REGLE NAP IPSEC Client**.
- Sur l'onglet **Etendue** de la stratégie, ajoutez un filtrage de sécurité pour le groupe **Clients IPSEC**.

Une stratégie identique sera créée pour les serveurs à protéger.

En utilisant l'instruction `ping -t` vers un serveur de frontière ou un serveur protégé, il sera possible de vérifier l'utilisation de l'authentification par certificat avec l'outil **Pare-feu Windows avec fonctions avancées de sécurité**.

Une association de sécurité basée sur les certificats sera utilisée pour la communication.



© ENI Editions - All rights reserved - adamo diarra

Bien sûr, ceci n'est qu'une possibilité de mise en place de la sécurité basée sur la quarantaine par IPSec ! Il est fort prudent de maquetter l'ensemble du réseau avant de la mettre en place sur le réseau de production.

4. La mise en place de NAP sur 802.1x

802.1X était jusqu'à présent principalement réservée aux points d'accès sans fil.

Maintenant, NAP permet aussi d'utiliser plus facilement cette authentification directement sur le réseau local. Cette mise en place suppose l'utilisation de RADIUS pour relayer la demande, et l'affectation d'un VLAN spécifique grâce à un switch acceptant les VLAN.

Trois éléments sont nécessaires :

- un serveur d'authentification ;
- un agent authentificateur (Switch ou Point d'accès sans fil) ;
- le demandeur.

Le client demandeur utilise le protocole EAP (EAP over Lan) pour envoyer la demande à l'agent d'authentification (Pass-Through). L'agent Pass-Through peut alors interroger un serveur RADIUS pour valider ou non la connexion.

Le serveur NPS remplace la technologie IAS mais continue à utiliser le protocole RADIUS pour communiquer. Si les clients ne sont pas conformes avec la sécurité demandée, un réseau restreint utilisant un VLAN spécifique ou un filtrage IP leur est affecté.

a) La configuration du switch (ou point d'accès) :

Voici la configuration des différents VLAN à réaliser sur le switch (ou point d'accès) :

- VLAN ID 1 est le VLAN par défaut ;
- VLAN ID 2 pour les machines non conformes ;
- VLAN ID 3 pour les machines conformes.

Le routage inter VLAN doit être désactivé entre le VLAN 2 et le VLAN 3.

Les ports utilisés pour connecter le serveur NPS et les contrôleurs de domaine doivent être configurés pour ne pas imposer l'authentification 802.1X. Toutes les demandes d'authentification et d'autorisation du switch doivent être redirigées vers le serveur NPS.

b) Dans la forêt Active Directory, une autorité racine de certification de type Entreprise est aussi nécessaire. Le serveur NPS doit avoir reçu un certificat d'ordinateur et le certificat racine devrait être ajouté parmi les autorités principales de confiance sur toutes les machines.

Un groupe de sécurité spécifique appelé **Clients NAP 802.1X** pour les clients NAP 802.1X peut être créé afin de restreindre l'application des stratégies aux machines ajoutées à ce groupe.

La plupart des éléments (Contrôleur de domaine, Serveur NPS, Autorité de certification, Gestion de stratégies de groupes) peuvent être installés sur une même machine, ce qui simplifiera la configuration de test. Si les systèmes précédents de quarantaine ont été testés, tous les éléments nécessaires sont déjà en place. En revanche, il sera préférable, dans un premier temps, de supprimer ou désactiver les stratégies de groupe et les stratégies réseau déjà configurées.

c) Configurez le serveur NPS en tant que serveur de stratégie de **santé** (Health Policy Server) :

Le plus simple est d'utiliser l'assistant de configuration de NAP.

À partir de la racine (NPS Local) :

- Cliquez sur **Configurer la protection d'accès réseau (NAP)** dans la partie **Configuration standard**.
- Dans **Méthode de connexion réseau**, sélectionnez **IEE 802.1X (câblé)**.
- Dans les **Clients RADIUS**, ajoutez l'adresse IP du ou des switch RADIUS, ainsi que la phrase secrète qui sera utilisée par le client.

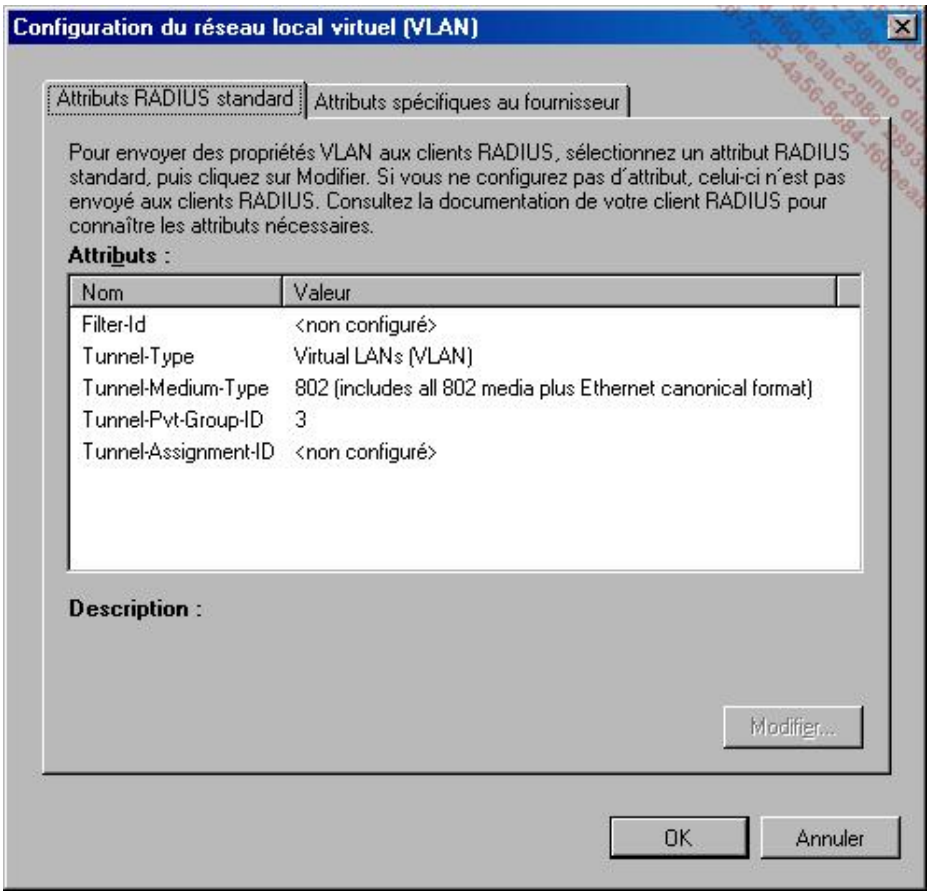
© ENI Editions - All rights reserved - adamo diarra

- Sur l'écran **Groupes d'ordinateurs et d'utilisateurs**, ne rien indiquer.

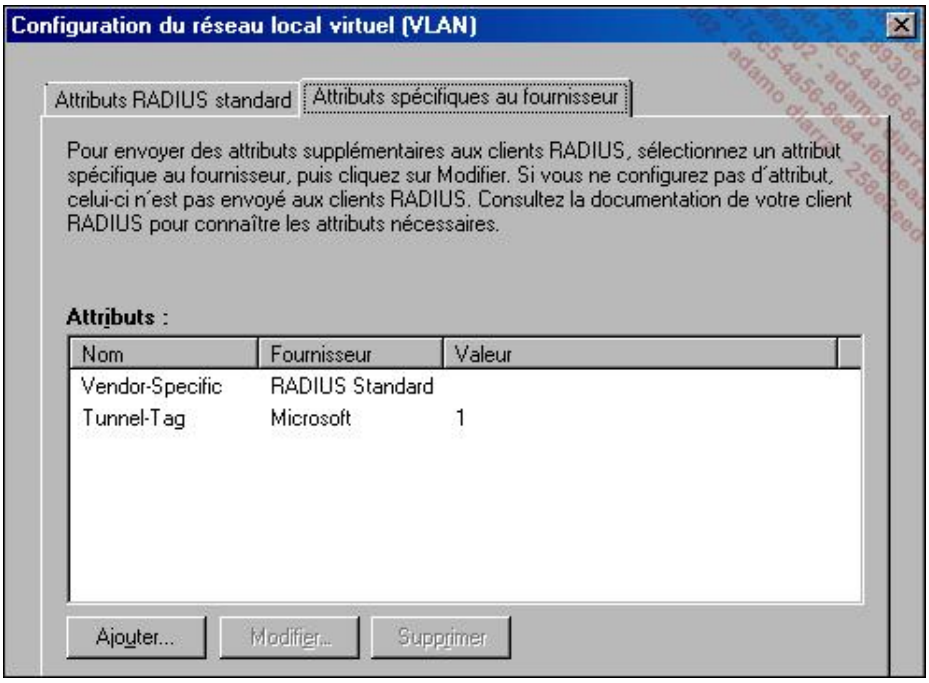
- Pour la méthode d'authentification, cliquez sur **Choisir**, sélectionnez le certificat (valide) émis pour le serveur hébergeant NPS et validez le mode **PEAP-MS-CHAP v2**.

Il faut ensuite configurer les deux réseaux locaux virtuels (VLAN) de la manière suivante en cliquant sur **Configurer** :

d) Le VLAN du réseau de l'organisation à obtenir en modifiant chaque attribut standard :

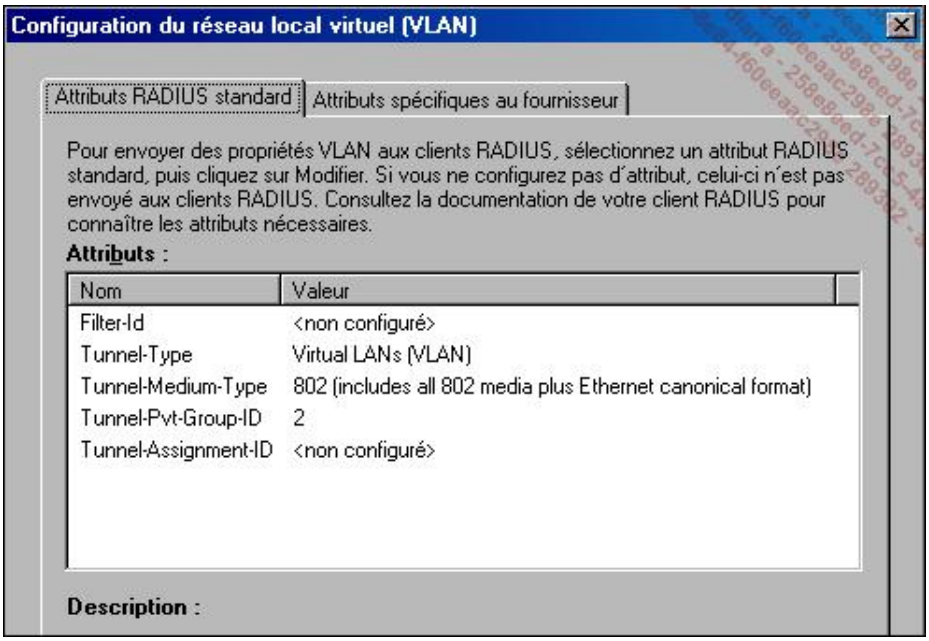


Un attribut (tag) spécifique à Microsoft doit être ajouté :



© ENI Editions - All rights reserved - adamo diarra

Le VLAN du réseau restreint :



L'attribut spécifique **Tunnel-Tag** de Microsoft doit aussi être positionné sur **1**.

- Dans **Définir la stratégie de contrôle d'intégrité NAP**, sélectionnez le système de validation souhaité, c'est-à-dire le **Validateur d'intégrité de la sécurité Windows**, dans notre cas.
- Par défaut, l'accès réseau complet n'est pas accordé aux clients non conformes.
- Toutes les stratégies sont créées sur l'écran final en cliquant sur **Terminer**.

e) Après configuration par l'assistant, il est intéressant de revérifier chaque paramètre.

- Pour la réalisation des tests, le validateur d'intégrité de la sécurité Windows est configuré pour ne vérifier que le démarrage du service pare-feu.
- Les stratégies de contrôles d'intégrité (définir les validateurs à utiliser).
- Les stratégies de demande de connexion (vérifiez l'ordre d'exécution, notez que la stratégie NAP 802.1X ne s'applique qu'aux connexions de type **ETHERNET**).
- Les stratégies réseau, et en particulier la stratégie **NAP 802.1X (câblé) Non Compatible NAP**.

En effet, lors de la mise en place de stratégies sur le réseau, il est primordial de traiter l'existence des machines Unix, Linux, Mac ou autres qui ne seraient pas compatibles NAP. Ces machines doivent continuer à fonctionner et communiquer sur le réseau, soit par des exclusions, soit par des règles spécifiques.

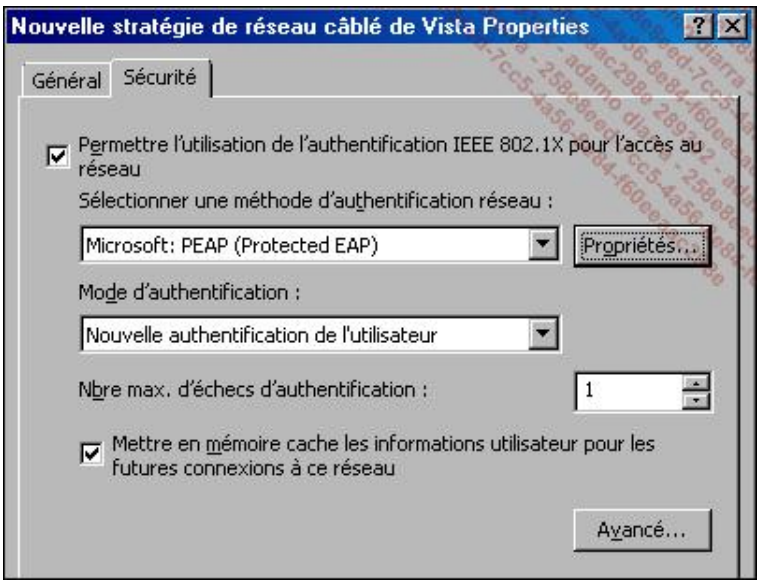
f) Pour que les clients NAP soient déclarés **conformes**, il est nécessaire que les clients aient la configuration adaptée. Pour les machines intégrées au domaine, il est logique d'utiliser les stratégies de groupes pour forcer la bonne configuration.

Voici les points importants de cette stratégie :

- Démarrez automatiquement le service **Agent de protection d'accès réseau**.
- Démarrez automatiquement le service **Configuration automatique de réseau câblé**.
- Activez le **Client de contrainte de quarantaine EAP** dans la section **Paramètres Windows - Paramètres de sécurité - Network Access Protection - Configuration du client NAP - Clients de contrainte**.
- Activez le **Centre de sécurité (Ordinateurs appartenant à un domaine)**.

© ENI Editions - All rights reserved - adamo diarra

- Dans **Stratégies de réseau filaire (IEEE 802.3)**, créez une stratégie de réseau câblé ayant les paramètres suivants :



- Cliquez sur **Propriétés** et laissez la case **Valider le certificat du serveur** cochée, ainsi que la méthode d'authentification **EAP-MSCHAP v2** par défaut.

- Décochez la case **Activer la reconnexion rapide**.

- Cochez la case **Activer les tests de quarantaine**.

- Si l'on veut restreindre cette stratégie à un groupe d'ordinateurs précis, retirez le groupe **Utilisateurs authentifiés** dans la partie **Filtrage de sécurité** et ajoutez le groupe **Clients NAP 802.1X** créé en début de procédure.

Attention, n'oubliez pas d'intégrer les clients dans ce groupe !

À noter que les paramètres peuvent aussi être configurés manuellement sur la station, à condition de démarrer manuellement tous les services indiqués dans la stratégie.

5. Conclusion

Voici les résultats obtenus avec ces différents types de quarantaine.

Règles	Client correct	Client incorrect
DHCP	Adresse IP complète et accès complet.	Des routes restreintes.
802.1X	Accès complet.	Accès au VLAN restreint ou aux ports autorisés.
IPSec	Communication avec tout pair de confiance.	Les pairs de confiance rejettent les connexions des systèmes non sûrs.

La meilleure sécurité sera obtenue par 802.1X, suivi de près par IPSec, DHCP pouvant être facilement contourné. Dans tous les cas, la quarantaine n'est pas une sécurité absolue mais améliore fortement la sécurité globale en favorisant la remise à niveau de l'ensemble du réseau.

D'autres types de quarantaine existent, mais ne s'appliquent pas à la totalité du réseau : il s'agit de la quarantaine VPN, Accès Distant et TS.

Une des seules contraintes liées à l'utilisation de la quarantaine consiste à utiliser Windows XP SP3, Windows Vista ou Windows 7, et à démarrer les services de protection réseau nécessaires. Néanmoins, il est important de noter que de nombreux fournisseurs proposent des produits compatibles NAP et notamment qu'il existe des clients NAP pour

© ENI Editions - All rights reserved - adamo diarra

Linux et Mac.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre est dédié au déploiement des serveurs et postes de travail. Posséder un socle d'installation automatisé est un gain de productivité et de qualité notable. L'installation de serveurs a peu de valeur ajoutée mais doit toujours être faite de la même façon, avec les mêmes versions de composants, afin d'avoir une cohérence entre tous les systèmes. Un déploiement comprend au minimum le système d'exploitation, mais aussi généralement l'ensemble des pilotes, utilitaires systèmes, voir même l'ensemble des applications nécessaires.

L'automatisation de ce processus prend encore plus de sens avec la virtualisation, et les environnements « à la demande ». La préparation de ce déploiement a une part très importante dans la réussite de votre projet. La technique n'étant pas une difficulté ici, il n'y a aucune raison de s'en priver !

© ENI Editions - All rights reserved - adamo diarra

Préparer son déploiement en choisissant bien sa stratégie

La préparation est la phase critique du projet. Afin de ne rien oublier tout en accélérant votre déploiement, Microsoft propose différents outils adaptés à votre contexte. À la fin de cette partie, vous aurez déterminé le périmètre, le type de licence et d'édition de Windows, le vecteur de déploiement ainsi que l'infrastructure à mettre en œuvre pour y parvenir.

1. Définir le périmètre

Comme pour tout projet, le périmètre est ici un élément clé. Vous devriez définir ce qui est « obligatoire » et ce qui est « facultatif/optionnel ». Afin d'alimenter votre réflexion, voici une liste d'éléments pouvant être intégrés dans votre projet :

- Seulement les serveurs ou aussi les postes clients ?
- Quelles versions et éditions de Windows sont à inclure ?
- Est-ce que vos applications fonctionnent et sont supportées sur un serveur 64 bits ? Windows Server 2008 R2 n'existe qu'en version 64 bits, contrairement à Windows Server 2008 qui existe aussi en 32 bits. Les applications 32 bits passent par Wow64 qui émule un système 32 bits. Attention, cette compatibilité n'est pas installée par défaut sur l'édition Core de Windows Server 2008 R2.
- Faut-il gérer plusieurs langues ?
- Quelle nomenclature adopter pour les systèmes ainsi déployés ?
- Qui va déployer ces images ? La mise en œuvre doit-elle être entièrement automatisée ?
- Quels matériels (et donc pilotes) sont à inclure ?
- Est-ce que des mises à jour Windows doivent/peuvent déjà être présentes post déploiement ?
- Quels outils ou applications font partis du tronc commun et peuvent donc être présents post déploiement ? Pouvez-vous faire une installation générique et automatisée de ces applications ?
- Faut-il créer plusieurs images de déploiement avec différentes options ou une seule image suffit-elle ? Faut-il une image spécifique pour vos environnements virtuels ?
- Est-ce que toutes les machines à déployer sont sur le réseau local et dans le domaine ? Faut-il pouvoir installer une image depuis un DVD ?
- Utilisez-vous déjà SCCM 2007 (*System Center Configuration Manager 2007*) ?
- Comment allez-vous gérer les licences associées à vos systèmes d'exploitation ? Utilisez-vous des licences en volume ?

La réponse à l'ensemble de ces questions couvre déjà une grande partie du périmètre. Les choix qui impactent le plus un projet de déploiement sont :

- l'utilisation de SCCM 2007, qui permet un déploiement « zero touch » ;
- l'intégration d'applications dans l'image ;
- le choix du mode de transport pour le déploiement (réseau ou autre).

Le fait d'inclure plus ou moins de types de matériels n'a qu'un impact sur le temps nécessaire afin d'inclure les pilotes adéquats. Vous aurez remarqué l'emploi du terme « image » pour désigner la méthode de déploiement. Il s'agit en

© ENI Editions - All rights reserved - adamo diarra

effet de construire un modèle de serveur que l'on va par exemple capturer sous forme d'image et rendre générique. Cela rend l'intégration d'applications dans le déploiement très simple, du moment que leur installation est générique. Cette image peut ensuite être déployée par divers moyens, tel que le réseau ou un DVD.

2. Gestion des licences

Contrairement aux versions précédentes de Windows, Windows Server 2008 R2 et Windows Vista/7 introduisent un service de gestion des licences en volume : KMS (*Key Management Service*). Il s'agit d'un service d'infrastructure à mettre en place sur votre réseau afin de gérer les licences de vos serveurs et stations de travail. Si vous ne mettez pas en place ce service, chaque machine devra se connecter individuellement à Microsoft via Internet pour être activée. L'activation via le service KMS permet de ne pas avoir à contacter Microsoft pour activer Windows, et cette activation est valable 6 mois. Passée cette période, le système doit être de nouveau activé pour une période de 6 mois en se connectant à votre réseau. KMS peut être implémenté dès que vous avez au moins 25 licences Windows Vista/7 ou 5 Windows Server 2008 R2.

Afin de simplifier le choix du type de licence à acheter, Microsoft a créé des groupes de produits qui couvrent différentes versions et éditions. Les groupes sont hiérarchiques. Un groupe donne droit à lui-même ainsi qu'à tous les groupes de niveaux inférieurs. Les groupes sont les suivants :

- Groupe Serveur C, qui couvre :
    - Windows Server 2008 R2 Datacenter.
    - Windows Server 2008 pour Itanium.
- Groupe Serveur B, qui couvre :
    - Windows Server 2008 R2 Standard.
    - Windows Server 2008 R2 Enterprise.
- Groupe Serveur A, qui couvre :
    - Windows Web Server 2008 R2.
    - Windows Server 2008 R2 HPC Edition.
    - Windows HPC Server 2008 R2.
- Groupe « Licence cliente en volume », qui couvre :
    - Windows Vista Business.
    - Windows Vista Entreprise.
    - Windows 7 Professionnel.
    - Windows 7 Enterprise.

Le groupe A couvre lui-même et les licences clientes en volumes. Le groupe B couvre lui-même, le groupe A et les licences clientes. Le groupe C couvre lui-même et tous les autres groupes.

L'installation de KMS est aussi simple que d'entrer la clé KMS, car le service Windows associé est déjà installé et actif par défaut (il s'agit du service **Licence du logiciel**) :

```
cscript C:\windows\system32\slmgr.vbs /ipk cléKMS
```

Le serveur doit ensuite valider cette clé auprès de Microsoft. Ce processus n'a lieu qu'une fois par ajout de clés. Si le serveur a un accès à Internet :

© ENI Editions - All rights reserved - adamo diarra

```
cscript C:\windows\system32\slmgr.vbs /ato
```

Dans le cas contraire, vous pouvez réaliser l'activation par téléphone en exécutant la commande `slui.exe 4`.

Pour détecter le serveur KMS, Windows utilise le DNS, une ressource SRV en particulier. Si les mises à jour DNS dynamiques sont autorisées, le service crée automatiquement les enregistrements DNS adéquats. Si votre environnement ne les autorise pas, vous pouvez configurer KMS pour qu'il n'essaie plus de créer la ressource SRV en exécutant :

```
cscript %systemroot%\system32\slmgr.vbs /cdns
```

La ressource SRV peut alors être créée manuellement avec les paramètres suivants :

- Service : _VLMCS
- Protocole : _TCP
- Port : 1688
- Hôte offrant le service : FQDN de l'hôte

Si le service DNS n'est pas disponible depuis un client, vous pouvez spécifier manuellement l'adresse IP du serveur KMS à utiliser avec la commande :

```
cscript %systemroot%\system32\slmgr.vbs /skms X.X.X.X:1688
```

Si un firewall est en place entre les machines à activer et le serveur KMS, le port TCP 1688 (par défaut) doit être ouvert (à l'initiative du client seulement). Si vous souhaitez changer le port TCP, il faut modifier la clé suivante à la fois sur le serveur KMS et sur les clients :

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL
```

Nom : `KeyManagementServicePort`

Type : `REG_SZ`

Valeur : XXXX (valeur représentant le nouveau port TCP en écoute).

Pour les environnements de test, les maquettes, ou temporaires, vous pouvez profiter de la période de grâce de Windows qui peut être réinitialisée si besoin. La durée de la période de grâce et le nombre de réinitialisations dépendent de la version et de l'édition de Windows :

- Windows Vista/7 : 30 jours de grâce, 3 réinitialisations
- Windows Vista Entreprise/7 : 30 jours de grâce, 5 réinitialisations
- Windows Server 2008/2008 R2 : 60 jours de grâce, 3 réinitialisations

Si ces environnements sont respectivement reconstruits plus souvent que les 90, 150 et 180 jours, vous n'avez pas besoin d'activer Windows. À l'installation, ni Windows Vista/7 ni Windows Server 2008/2008 R2 ne demandent de numéro de licence, ce qui permet d'être en période de grâce sans fournir de numéro de licence. Si le service KMS est hébergé sur une machine virtuelle, cette dernière ne doit pas être déplacée sur un autre serveur physique. Ce type de changement est en effet détecté par KMS, qui requiert alors de nouveau une activation auprès de Microsoft avant de pouvoir fournir de nouvelles licences.

Pour connaître le nombre de licences actuellement utilisé sur votre KMS, vous pouvez exécuter la commande suivante :

```
cscript %systemroot%\system32\slmgr.vbs /dli
```

Si vous ne souhaitez pas utiliser KMS mais tout de même activer en masse vos systèmes Windows, vous pouvez utiliser VAMT (*Volume Activation Management Tool*). Il est téléchargeable directement depuis MDT 2010, dans le nœud **Components**.

© ENI Editions - All rights reserved - adamo diarra

3. Choix de l'édition et du type d'installation

Au-delà de l'impact sur la gestion des licences, chaque paire édition/type d'installation (complète ou minimale) va nécessiter une nouvelle image de déploiement. Le choix de l'édition dépend de plusieurs critères :

- les rôles nécessaires ;
- les fonctionnalités nécessaires ;
- les ressources matérielles à utiliser ;
- l'homogénéité de vos systèmes dans votre infrastructure afin d'avoir une édition couvrant le maximum de vos besoins ;
- une installation de type Core constitue une image séparée. Le chapitre Consolider vos serveurs couvre en détail ce type d'installation.

Microsoft met à disposition plusieurs tableaux permettant de voir les différences entre les éditions serveurs.

Les différences sur les rôles sont disponibles à cette adresse :

http://www.microsoft.com/windowsserver2008/en/us/r2-compare-roles.aspx

Pour une installation Core :

http://www.microsoft.com/windowsserver2008/en/us/r2-compare-core-installation.aspx

Les différences sur les fonctionnalités sont disponibles à cette adresse :

http://www.microsoft.com/windowsserver2008/en/us/r2-compare-features.aspx

Les différences sur le matériel sont disponibles à cette adresse :

http://www.microsoft.com/windowsserver2008/en/us/r2-compare-specs.aspx

Pour les différences entre les éditions de Windows 7 :

http://windows.microsoft.com/fr-FR/windows7/products/compare

© ENI Editions - All rights reserved - adamo diarra

Créer et déployer

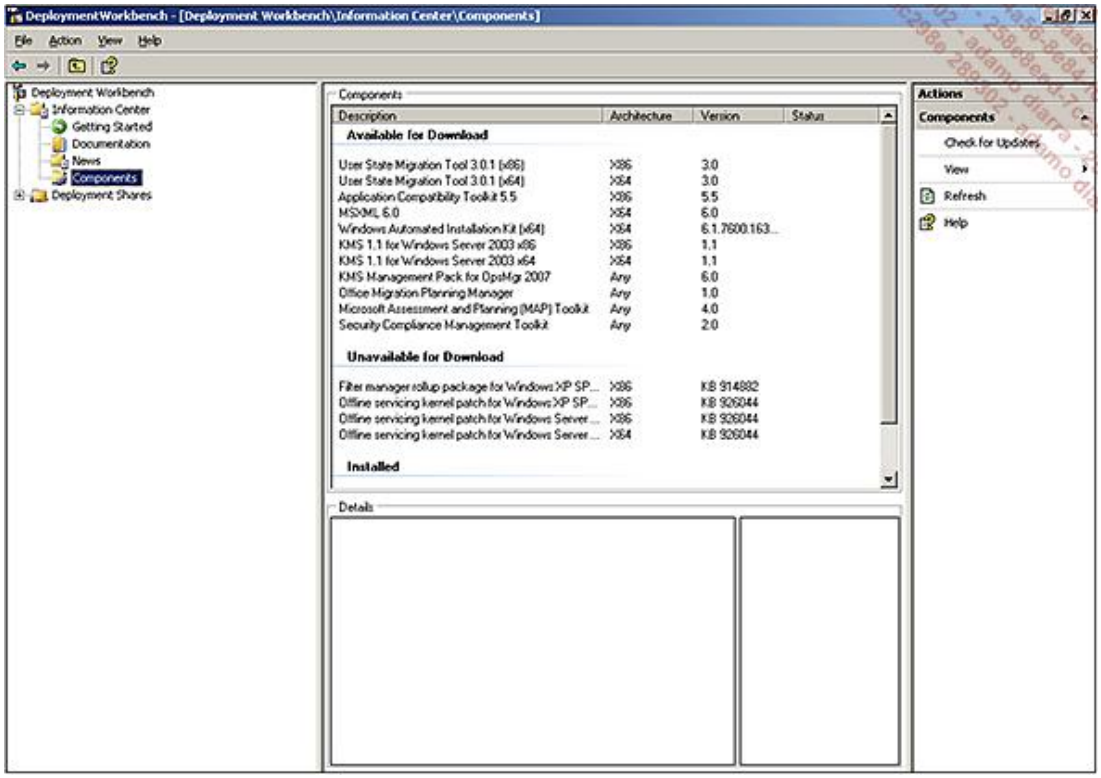
Cette section couvre la création et le déploiement des systèmes d'exploitation, à la fois clients et serveurs. Microsoft Deployment Toolkit est l'outil central, qui enrichit les outils natifs à travers une interface conviviale et un emplacement unique pour toutes les données nécessaires aux déploiements. Deux méthodes sont proposées : Lite Touch et Zero Touch.

MDT utilise plusieurs composants, dont WAIK (*Windows Automated Installation Kit*), Windows PE, et ImageX. Ces deux derniers sont fournis dans WAIK.

1. Microsoft Deployment Toolkit (MDT 2010)

Microsoft met gratuitement à votre disposition un outil afin d'accélérer votre projet de déploiement, MDT 2010. Il est disponible en téléchargement à cette adresse : http://www.microsoft.com/downloads/details.aspx?familyid=3bd8561f-77ac-4400-a0c1-fe871c461a89&displaylang=en&tm.

Une fois installé, l'interface de gestion se trouve dans **Démarrer - Tous les programmes - Microsoft Deployment Toolkit - Deployment Workbench**. Les composants complémentaires sont proposés en téléchargement depuis l'onglet **Components** dans la console :

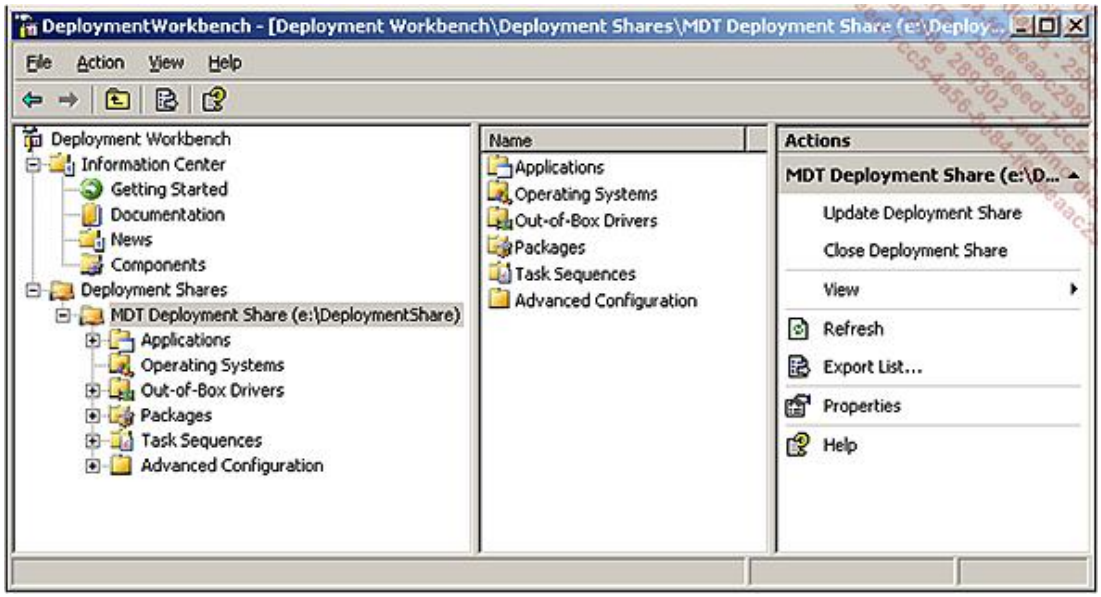


Il faut au moins télécharger le composant **Windows Automated Installation Kit** (appelé aussi **WAIK**), en 32 ou 64 bits suivant votre environnement. MDT n'étant disponible qu'en anglais, il téléchargera ce composant en anglais. Pour télécharger la version française, il suffit de se rendre à cette page : http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34.

Tant que ce composant n'est pas présent, aucune des fonctions de l'arbre **Deployment Share** ne fonctionne. MDT pilote WAIK afin de vous assister dans sa mise en œuvre et ne peut donc pas fonctionner sans celui-ci. En le téléchargeant, vous obtenez aussi Windows PE.

Une fois WAIK installé, l'arbre **Deployment Share** permet de créer un espace de travail. Pour cela, il suffit de faire un clic droit dessus, de choisir **New Deployment Share**. L'emplacement choisi doit avoir suffisamment de place pour contenir les sources et les images générées.

© ENI Editions - All rights reserved - adamo diarra



Nous pouvons maintenant alimenter chaque module de cet espace de travail :

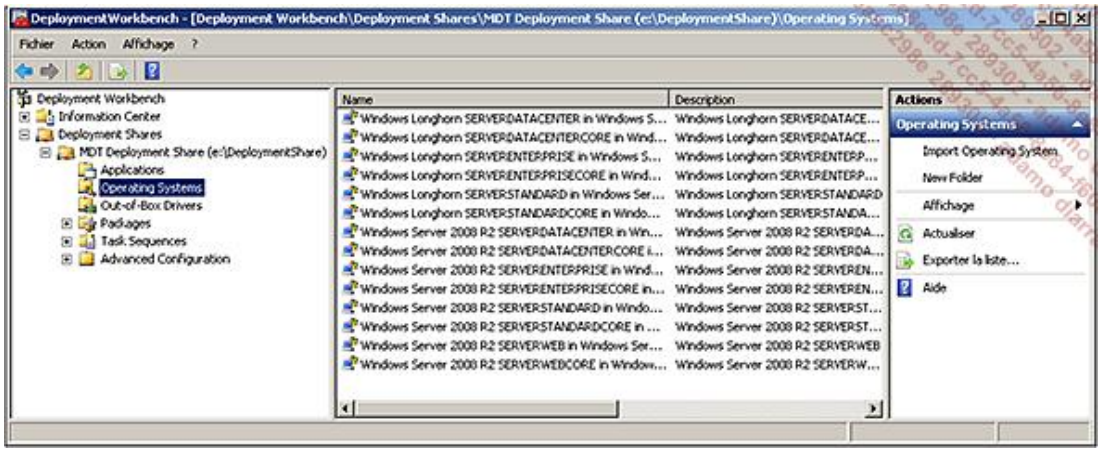
- **Applications** : contiendra les applications ajoutées dans le déploiement.
- **Operating Systems** : contient les sources des systèmes d'exploitation.
- **Out-of-Box Drivers** : contiendra les pilotes supplémentaires nécessaires.
- **Packages** : contiendra les mises à jour Windows à intégrer.
- **Task Sequences** : permet de créer un scénario à partir des éléments des modules.
- **Advanced configuration** : permet de créer un média (DVD...), de garder une trace des déploiements dans une base SQL ou de gérer des réplicas du point de distribution.

Les étapes suivantes sont :

- Ajouter des systèmes d'exploitation (depuis leur DVD...).
- Ajouter des applications (installation silencieuse...)
- Ajouter des mises à jour Windows.
- Ajouter des pilotes.
- Créer une séquence d'actions à effectuer.
- Créer une base de données pour inventorier les machines déployées.

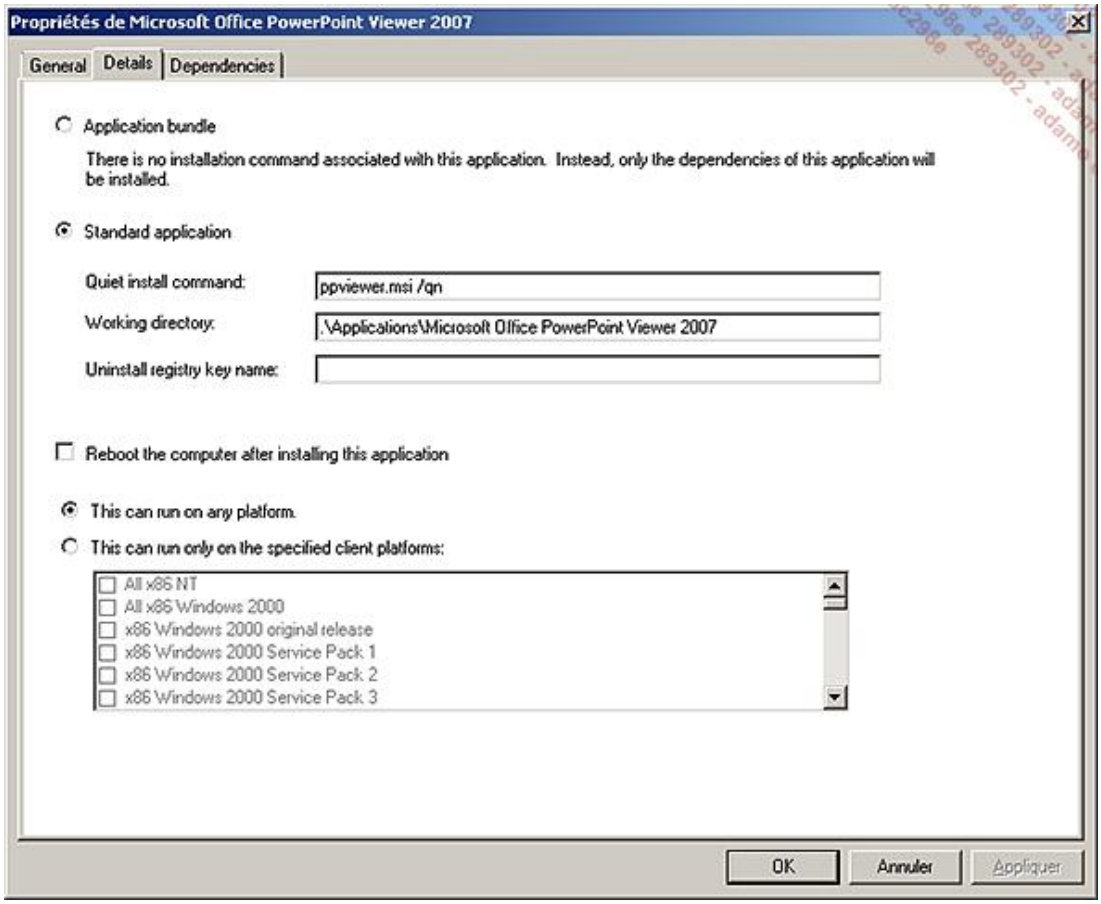
L'ajout de systèmes d'exploitation est très simple. Une fois les DVD ou CD importés, ils apparaissent comme ceci :

© ENI Editions - All rights reserved - adamo diarra



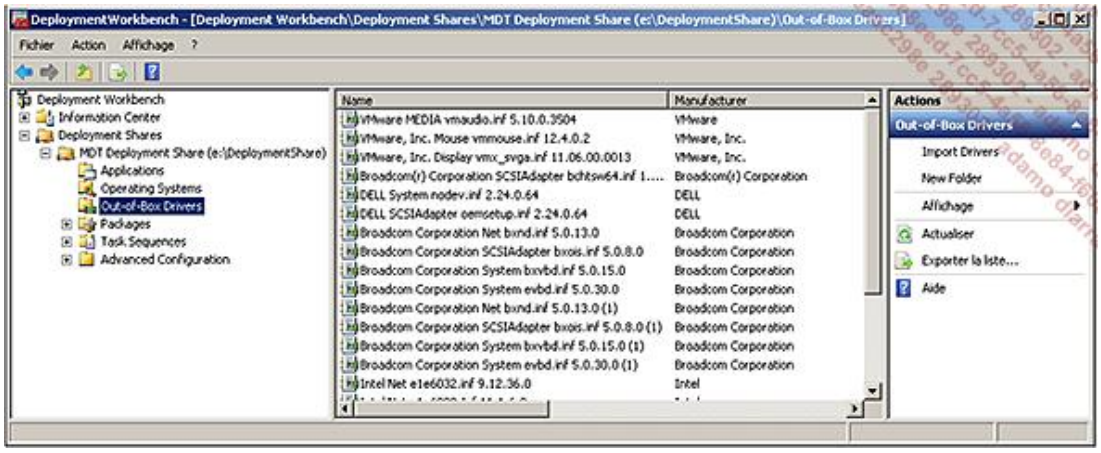
Remarquez que la liste comprend à la fois Windows Server 2008 et Windows Server 2008 R2. MDT permet de déployer également Windows Vista, 7 et même Windows XP.

L'ajout d'application à travers le nœud **Applications** permet d'installer des applications post déploiement. Il s'agit d'installations silencieuses, de fichiers MSI, etc. Vous pouvez ensuite les intégrer dans les séquences d'installations. Les propriétés suivantes sont disponibles :



Le choix **Application bundle** permet de grouper des applications. L'ajout de mises à jour Windows se fait via le nœud **Packages**. C'est aussi simple que de fournir le dossier qui les contient (fichiers .cab et .msu). Par défaut, elles appartiennent au groupe **All Packages**. Vous pouvez ajouter des groupes personnalisés afin de filtrer les mises à jour à appliquer dans les séquences d'installation. Le nœud **Out-of-Box Drivers** contiendra tous vos pilotes. Il suffit de fournir le dossier les contenant (fichiers .inf). Vous pouvez classer les éléments de chaque nœud dans des dossiers et sous-dossiers.

© ENI Editions - All rights reserved - adamo diarra

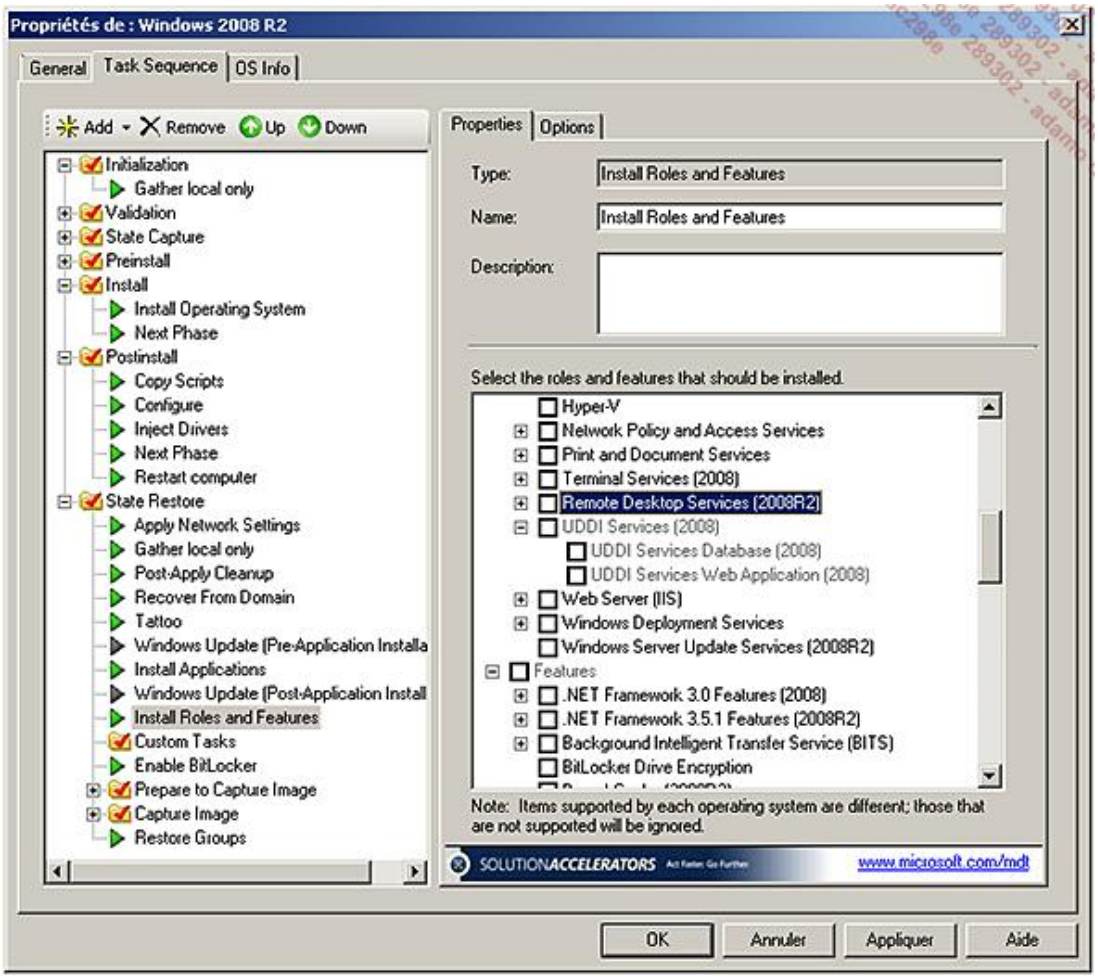


Le nœud **Task Sequences** est la clé de voûte du logiciel. Il permet de rassembler toutes les briques précédentes afin d'en tirer des scénarios d'installation. Lors de la création d'une séquence, seules les options courantes sont proposées :

- Un identifiant unique, un titre, une description.
- Un masque de séquence.
- Un système d'exploitation parmi la liste du nœud **Operating Systems**.
- Indiquer ou non un numéro de série (période d'essai le cas échéant).
- Le nom, la page par défaut d'Internet Explorer.
- Le mot de passe Administrateur local (ou à demander au premier lancement).

Une fois créée, il faut ouvrir les propriétés de la séquence, dans l'onglet **Task Sequence**, pour découvrir toutes les capacités des séquences :

© ENI Editions - All rights reserved - adamo diarra



Les ajouts possibles sont regroupés par thèmes :

- Général
    - Exécuter une ligne de commande.
    - Positionner une variable.
    - Exécuter une commande en tant que.
    - Redémarrer.
    - Collecter des informations.
    - Installer des mises à jour au premier lancement.
    - Valider.
    - Installer une ou des applications présentes dans le nœud **Applications**.
- Disques
    - Partitionner et formater un disque.
    - Activer BitLocker.
- Images

© ENI Editions - All rights reserved - adamo diarra

        - Installer un système d'exploitation.

- Paramètres

        - Appliquer un paramétrage réseau (IP, DNS, WINS).

        - Capturer le paramétrage réseau existant.

- Rôles

        - Installer et configurer des rôles et fonctionnalités. Les possibilités varient suivant le système d'exploitation à installer.

        - Configurer le serveur DHCP, DNS, Active Directory, et enfin autoriser le DHCP.

Les scénarios possibles sont très larges lors du déploiement :

- Sauvegarde ou non des profils utilisateurs locaux sur un partage réseau (avec restauration).

- Capture des paramètres réseaux avant la réinstallation, puis restauration de ceux-ci.

- Installation et configuration des rôles communs Windows Server 2008 R2.

- Gestion de BitLocker avec paramétrage :

        - Moyen de stockage (TPM, USB, les deux).

        - Création d'une clé de recouvrement dans l'Active Directory.

        - Attendre la fin de l'encryption avant de continuer.

- Injections de pilotes et mises à jour Windows.

Il reste ensuite à définir un point de déploiement dans le nœud **Deploy - Deployment Points**. Les possibilités sont :

- le partage local à la machine où s'exécute MDT 2010 ;

- un partage local ou distant ne contenant qu'un jeu de la configuration ;

- un média de stockage amovible (DVD, USB) ;

- une intégration à SMS 2003.

Les séquences sont stockées dans le sous-dossier **Control du partage** créé précédemment, avec l'arborescence suivante :

- À la racine :

        - **Bootstrap.ini** : fichier de configuration quand la machine à déployer ne peut pas se connecter au point de déploiement.

        - **CustomSettings.ini** : fichier de configuration commun à toutes les séquences.

- {Numéro de séquence}

        - **TS.xml** : contient des métadonnées sur la séquence.

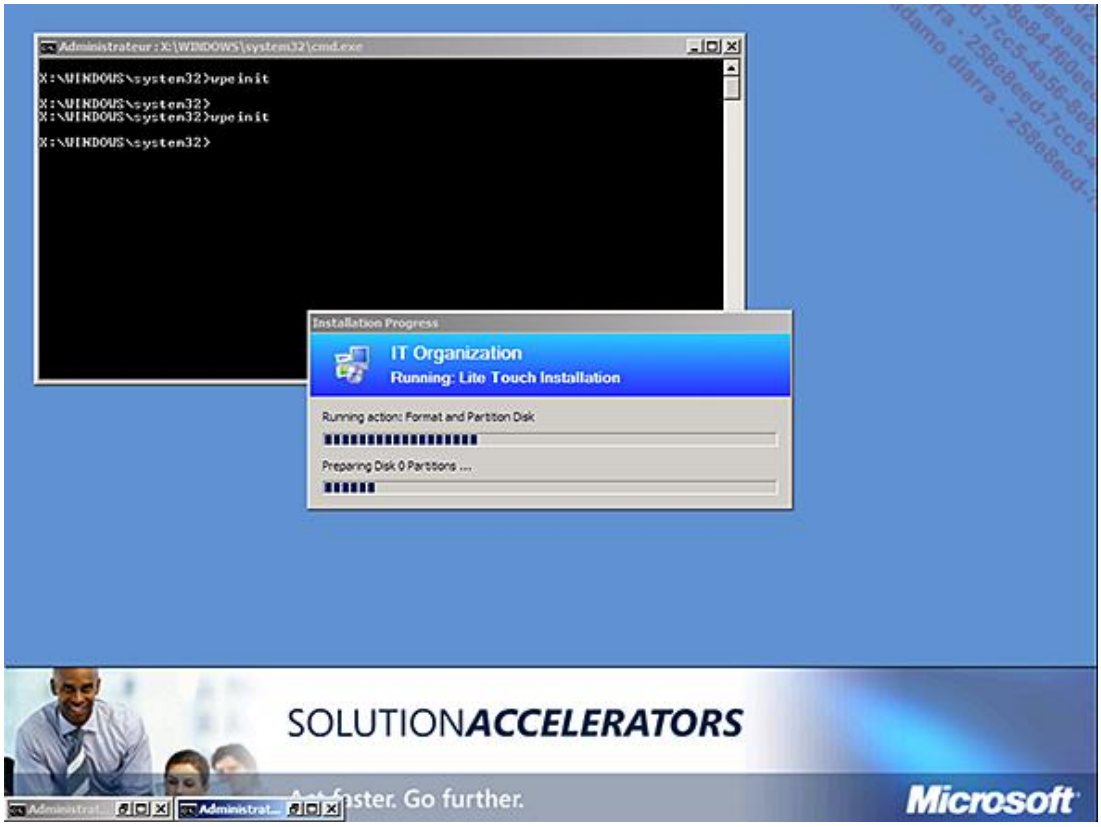
© ENI Editions - All rights reserved - adamo diarra

- **Unattend.xml** : contient les valeurs pour le sysprep.

Le déploiement via un média amovible est le plus basique, mais il est très efficace quand la connectivité réseau est limitée. Dans le dossier de destination, vous trouverez une image ISO bootable, LiteTouchPE_x86.iso ou LiteTouchPE_x64.iso suivant votre environnement.

Window PE est l'environnement de préinstallation de Windows. Il s'agit d'un système Windows très léger permettant d'exécuter un ensemble d'outils pour déployer un système d'exécution Windows. L'image WIM générée par MDT utilise Windows PE. Dans ce type d'environnement, le moteur vbscript est notamment disponible. Les écrans graphiques MDT sont des vbscript et HTA (*HTML Applications*). Windows PE ayant ses fichiers en mémoire, il est possible de partitionner et de formater tout le stockage disponible, notamment la partition système. Certains outils, comme USMT et ImageX, fonctionnent dans ce type d'environnement, ce qui permet de sauvegarder les données de la machine avant sa réinstallation par exemple. La version actuelle est la 3.0, qui correspond à Windows 7 et Windows Server 2008 R2.

Voici par exemple l'environnement fourni par MDT :



2. Lite Touch

La solution Lite Touch permet d'industrialiser votre déploiement sans pour autant disposer de l'infrastructure de gestion Microsoft, System Center Configuration Manager 2007. La solution reste simple à mettre en œuvre tout en étant très efficace, car elle utilise le moteur de séquence de ce dernier en version autonome. Le déploiement doit être initié manuellement, mais vous êtes guidé à travers des écrans graphiques pour effectuer celui-ci.

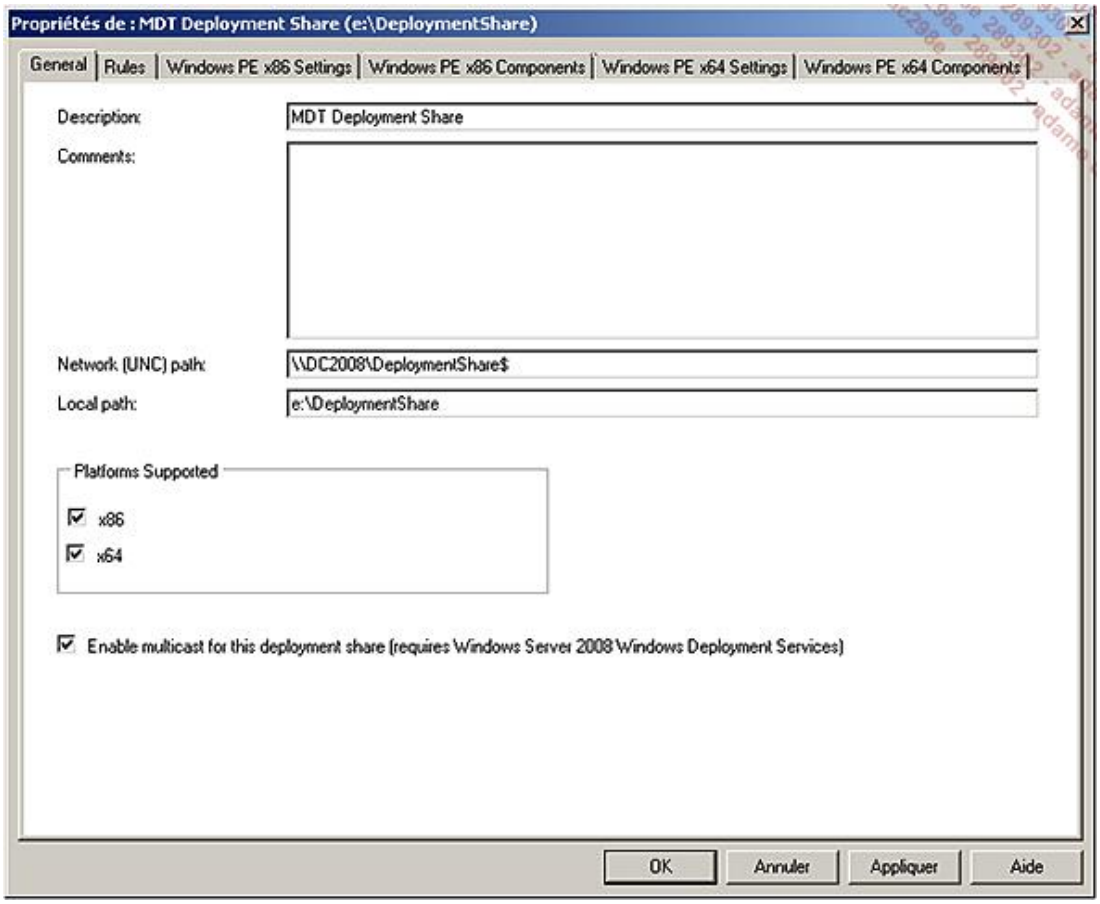
Au-delà d'une image ISO comme vu précédemment, le déploiement via le réseau est possible en utilisant WDS (dont l'installation est couverte plus loin). Vous devez ensuite spécifier dans **CustomSettings.ini** la variable `DeployRoot=\\%WDSServer%\DeploymentShare$`, sous la section [Default].

Il faut remplacer `DeploymentShare$` par le nom de votre partage si vous n'avez pas laissé le nom par défaut. Il faut ensuite mettre à jour le point de distribution, en effectuant un clic droit dessus, puis choisir **Update Deployment Share**. Il suffit ensuite :

- d'importer ces deux images WIM dans WDS ;
- de démarrer une machine via PXE.

L'utilisation du multicast pour le déploiement est même disponible :

© ENI Editions - All rights reserved - adamo diarra



Avant de déployer une image, certaines questions seront posées via des interfaces graphiques. Il est possible d'augmenter l'automatisation en les évitant. Vous devrez fournir les réponses à ces questions dans le fichier **CustomSettings.ini**. Voici les étapes pouvant être évitées si les variables suivantes sont positionnées à **YES** (en majuscules) dans le fichier **CustomSettings.ini**, section [Default]. À chaque écran correspond une variable pour l'éviter, ainsi qu'une ou plusieurs variables afin de renseigner les informations demandées par cet écran :

`SkipAdminPassword` : ne demande pas de mot de passe administrateur local.

- Automatiser par `AdminPassword`=monmotdepasseadmin. Le mot de passe sera stocké en clair dans le fichier, vous devez donc changer ce mot de passe ultérieurement. Il est même conseillé de le changer régulièrement de façon automatisée sur l'ensemble de vos machines.

`SkipApplications` : ne propose pas d'installer des applications.

- Automatiser par `Applications001={GUID de l'application trouvée dans control\Applications.xml}`

`SkipAppsOnUpgrade` : ne propose pas d'installer des applications si c'est une mise à jour.

`SkipBDDWelcome` : évite la fenêtre d'accueil.

`SkipBitLocker` : ne propose pas BitLocker.

`SkipBitLockerDetails` : ne demande pas la configuration de BitLocker.

`SkipTaskSequence` : ne propose pas le choix de la séquence.

- Automatiser par `TaskSequenceID={Identifiant de séquence}`

`SkipCapture` : ne propose pas l'utilisation de capture.

- Automatiser par `DoCapture=NO|YES|PREPARE`

`SkipComputerBackup` : ne propose pas la sauvegarde de l'ordinateur.

- Automatiser par `ComputerBackupLocation=NETWORK|AUTO|NONE`

© ENI Editions - All rights reserved - adamo diarra

- NETWORK fait une sauvegarde sur le réseau.
- AUTO fait une sauvegarde locale s'il y a suffisamment d'espace disque, sinon sur le réseau.
- NONE ne fait aucune sauvegarde.

Si vous souhaitez faire une sauvegarde sur le réseau, il faut aussi utiliser ces deux variables :

- BackupShare=\\DC2008\Backup$
- BackupDir=%ComputerName%

Pour que la sauvegarde fonctionne, les permissions doivent être les suivantes sur le partage utilisé :

- Objet ordinateurs et utilisateurs du domaine en création de dossiers et ajouts de données.
- Créateur propriétaire en contrôle total.

SkipComputerName : ne demande pas le nom de l'ordinateur.

- Automatiser par ComputerName=%SerialNumber% par exemple.

SkipDeploymentType : ne demande pas le type de déploiement.

- Automatiser par DeploymentType=NEWCOMPUTER. Il peut prendre les valeurs NEWCOMPUTER, REFRESH, REPLACE, UPGRADE

SkipDomainMembership : ne propose pas de joindre un domaine.

- Automatiser par JoinDomain=MASOCIETE. Les variables additionnelles sont :
  - MachineObjectOU=OU=Mes_Serveurs,DC=masociete,DC=local
  - DomainAdmin=Administrateur
  - DomainAdminDomain=MASOCIETE
  - DomainAdminPassword=motdepassecomplexe

Le mot de passe étant stocké en clair, vous devriez utiliser un compte qui n'a que le droit de joindre les machines au domaine.

SkipFinalSummary : ne montre pas la fenêtre finale de résumé de la séquence.

SkipLocaleSelection : ne propose pas de choisir les paramètres régionaux.

- Automatiser par :

KeyboardLocale=fr-FR (mettre également cette variable dans bootstrap.ini pour avoir le clavier en français pendant l'installation).

UserLocale=fr-FR et UILanguage=fr-FR

SkipPackageDisplay : ne propose pas de package complémentaire.

SkipProductKey : ne demande de numéro de série.

SkipSummary : ne montre pas le résumé.

SkipTimeZone : ne demande pas le fuseau horaire.

© ENI Editions - All rights reserved - adamo diarra

- Automatiser par `TimeZoneName=''TimeZoneName=Romance StandardTime''`.

`SkipUserData` : ne demande pas s'il faut sauvegarder les profils utilisateurs.

- Automatiser par `UserDataLocation=NETWORK|AUTO|NONE`.
    - `NETWORK` fait une sauvegarde sur le réseau.
    - `AUTO` fait une sauvegarde locale si il y a suffisamment d'espace, sinon sur le réseau.
    - `NONE` ne fait aucune sauvegarde.

Si vous souhaitez faire une sauvegarde sur le réseau, il faut aussi utiliser ces deux variables :

- `UDShare=\\DC2008\Profiles$`
- `UDDir=%ComputerName%`

Et enfin, pour renseigner le compte à utiliser pour accéder au partage contenant les ressources MDT :

```
USERID=Administrateur
UserPassword=motdepassecomplexe
UserDomain=MASOCIETE
```

Votre fichier **CustomSettings.ini** pourrait donc ressembler à ceci :

```
[Settings]
Priority=Default
Properties=MyCustomProperty

[Default]
OSInstall=Y
SkipBDDWelcome= YES
SkipCapture=YES
SkipAppsOnUpgrade=YES
SkipFinalSummary=YES
SkipPackageDisplay= YES
SkipProductKey=YES
SkipSummary=YES
USERID=Administrateur
UserPassword= motdepassecomplexe
UserDomain=MASOCIETE

SkipComputerBackup=YES
ComputerBackupLocation= NONE

SkipAdminPassword=YES
AdminPassword=monmotdepasseadminlocal

SkipApplications=YES
Applications001={73823faf-bb78-4491-a053-b47afb5553c4}

SkipTaskSequence=YES
TaskSequenceID= 001

SkipComputerName=YES
ComputerName=%SerialNumber%

SkipDeploymentType=YES
DeploymentType=NEWCOMPUTER

SkipDomainMembership=YES
JoinDomain=MASOCIETE
MachineObjectOU=OU=Mes_Serveurs,DC=masociete,DC=local
```


© ENI Editions - All rights reserved - adamo diarra

```
DomainAdmin= Administrateur
DomainAdminDomain=MASOCIETE
DomainAdminPassword= motdepassecomplexe

SkipLocaleSelection=YES
KeyboardLocale=fr-FR
UserLocale=fr-FR
UILanguage=fr-FR

SkipTimeZone=YES
TimeZoneName=Romance Standard Time"

SkipUserData=YES
UserDataLocation=NONE
DeployRoot=\\DC2008\DeploymentShare$
```

L'intégration avec WSUS est prévue dans MDT. Si le système d'exploitation à déployer est antérieur à Windows Server 2008 ou Windows Vista, le client Windows Update doit être mis à jour. Il est téléchargeable ici :

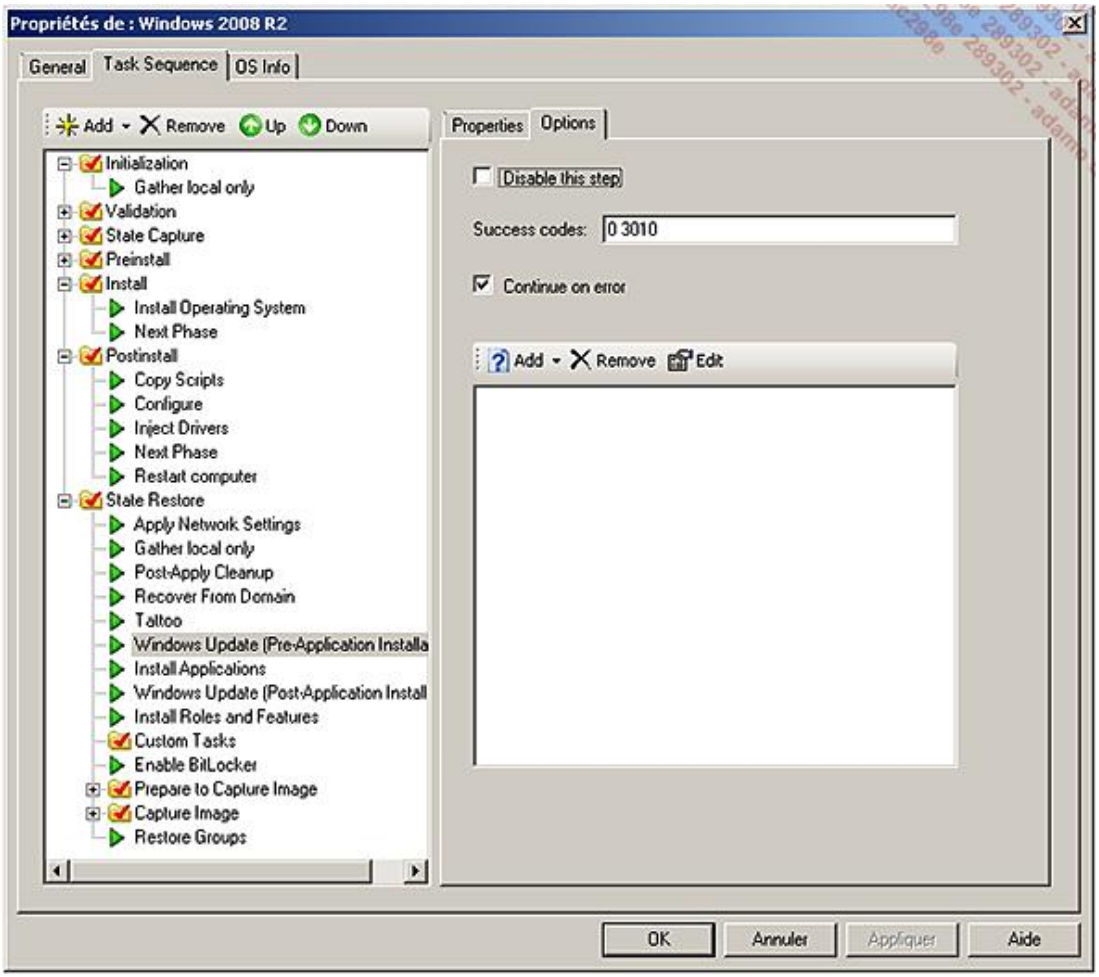
Version x86 : http://go.microsoft.com/fwlink/?LinkID=100334.

Version x64 : http://go.microsoft.com/fwlink/?LinkID=100335.

MDT peut les déployer automatiquement si ces exécutables sont copiés dans le sous-dossier Tools\x86 et Tools\x64 respectivement. Si vous déployez Windows XP Service Pack 2 ou 3, ou Windows Server 2003 Service Pack 2, une alerte de sécurité bloquera cette installation car il est installé depuis le partage réseau. Pour contourner ce problème, il faudra alors installer l'agent comme une application standard depuis MDT avec la commande : `WindowsUpdateAgent30-[platforme].exe /quiet /norestart /wuforce`.

Par défaut, la machine essaiera de se connecter aux serveurs Microsoft Windows Update sur Internet. Si vous avez un serveur WSUS, vous pouvez l'indiquer à MDT en ajoutant la variable `WSUSServer=http://monserveur` dans le fichier **CustomSettings.ini.** Si vous spécifiez un serveur WSUS mais que le client n'est pas à jour, MDT essaiera de le télécharger depuis Internet.

Il ne reste plus qu'à activer les deux étapes Windows Update dans la séquence (Pre et Post), car elles sont désactivées par défaut :



© ENI Editions - All rights reserved - adamo diarra

Une autre approche est de déployer complètement une machine, de la configurer entièrement en installant les applications et les mises à jour par exemple, puis de la capturer à travers Lite Touch. Cela deviendra votre image de référence, qu'il vous suffira de déployer en faisant un sysprep. Sysprep permet de rendre unique une machine, en ce qui concerne son nom et son SID (*Security IDentifier*). C'est pour cette raison que vous ne pouvez pas joindre un domaine AD pendant une phase de capture. La phase de sysprep est automatiquement incluse par MDT (phase *Copy sysprep files*). Un point nécessitant votre attention lors d'une capture effectuée par Lite Touch reste l'utilisation d'antivirus, qui peut poser des problèmes.

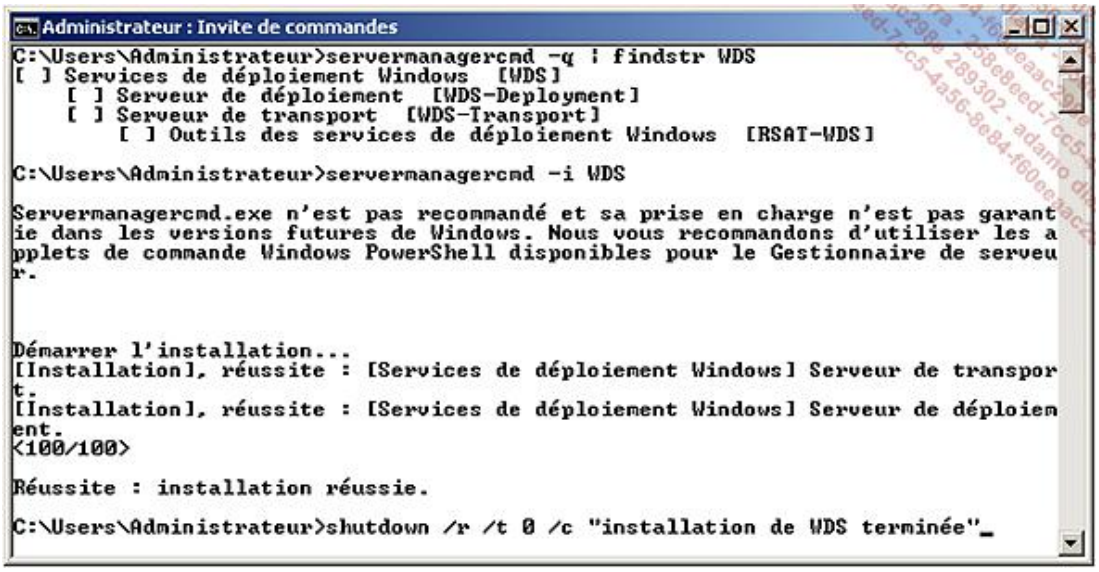
La migration des profils utilisateur est faite via le composant USMT (*User State Migration Tool*). Il n'est pas nécessaire de l'installer sur le serveur de déploiement. Tout comme pour le client Windows Update, il faut télécharger les installeurs 32 et 64 bits et les copier dans les sous-dossiers Tools\x86 et Tools\x64. Ils sont disponibles en téléchargement ici : http://www.microsoft.com/downloads/details.aspx?FamilyID=799ab28c-691b-4b36-b7ad-6c604be4c595&displaylang=en#filelist

MDT offre la possibilité d'inventorier toutes les machines déployées dans une base de données SQL Server. Si vous le souhaitez, vous pouvez utiliser une base SQL Express. Cette version de SQL Server est gratuite et suffit à ce besoin. Elle est téléchargeable chez Microsoft :

http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=7522a683-4cb2-454e-b908-e805e9bd4e28

3. WDS

L'installation du rôle WDS est très simple, mais nécessite un redémarrage du serveur. Les pré-requis sont un domaine Active Directory, les services DNS et DHCP sur le réseau, ainsi qu'une partition NTFS pour le stockage. Afin d'installer le rôle depuis une ligne de commande, exécutez la commande `servermanagercmd -i WDS` :



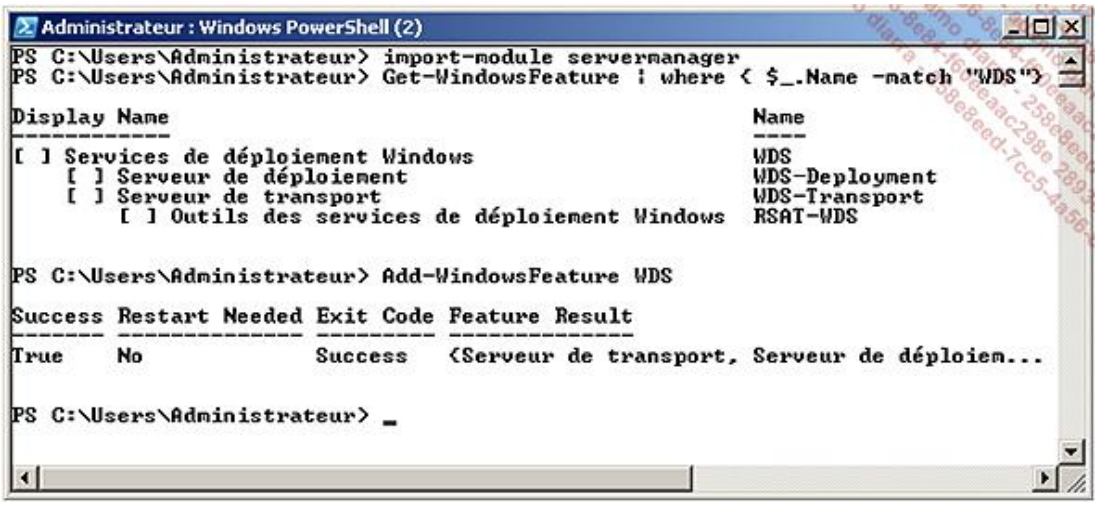
Trois composants ont été installés :

- **Serveur de déploiement** : il s'agit du composant principal.
- **Serveur de transport** : ce composant peut être installé tout seul en environnement restreint (sans Active Directory, DHCP, DNS...). Il est aussi utilisé par le composant principal.
- **Outils des services de déploiement Windows** : composants d'administrations.

Le message d'avertissement pour **servermanagercmd** ci-dessus n'apparaît que sur Windows Server 2008 R2. **Servermanagercmd** a été introduit avec Windows Server 2008. Mais depuis Windows Server 2008 R2, il est remplacé par des commandes PowerShell. L'objectif est notamment d'uniformiser les commandes entre les versions classiques et Core. La version Core inclut le Framework .NET sous 2008 R2 et donc PowerShell. L'équivalent en PowerShell est le suivant :

```
Import-module servermanager
Get-WindowsFeature | where { $_.Name -match "WDS"}
Add-WindowsFeature WDS
```


© ENI Editions - All rights reserved - adamo diarra

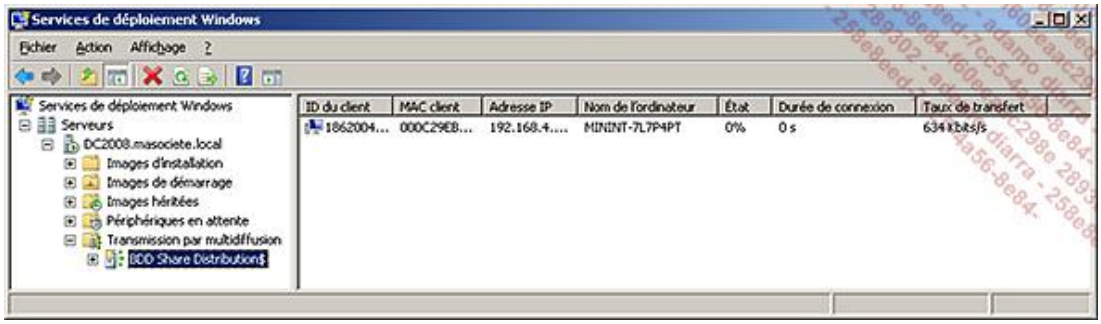


Une fois le rôle installé, l'interface de gestion se trouve dans **Démarrer - Outils d'administration - Services de déploiement Windows**. Étendez les nœuds jusqu'au nom de votre serveur et sélectionnez **Configurer le serveur**. Choisissez ensuite un dossier pour le stockage des images (**%systemdrive%\RemoteInstall** par défaut). La volumétrie de ce dossier pouvant être importante, une alerte est émise si la partition système est utilisée. Si nécessaire, il est possible de réduire à chaud les volumes depuis le gestionnaire de disques, afin de disposer d'un lecteur dédié à ce stockage.

WDS peut être restreint afin de répondre uniquement aux clients connus. Pour qu'un client soit connu, il faut qu'il ait déjà joint l'Active Directory antérieurement, ou qu'un objet ordinateur ait été créé manuellement dans Active Directory avec le bon identifiant. L'identifiant utilisé est affiché au démarrage de la machine cliente, au moment de la recherche de PXE (GUID). Un mode d'approbation est aussi possible, l'administrateur visualisant les demandes de clients inconnus en attente.

Pour un déploiement massif, le mode multicast est très adapté. Il permet de ne pas inonder le réseau en envoyant tous les octets individuellement à chaque machine. À la place, les machines s'inscrivent à l'adresse multicast, WDS n'envoyant alors qu'une fois les données à cette adresse pour toutes les machines. S'agissant de multicast IGMP, il faut que vos équipements réseaux le supportent. Si ce n'est pas le cas, le switch les traitera comme des diffusions, et inondera alors tout le réseau.

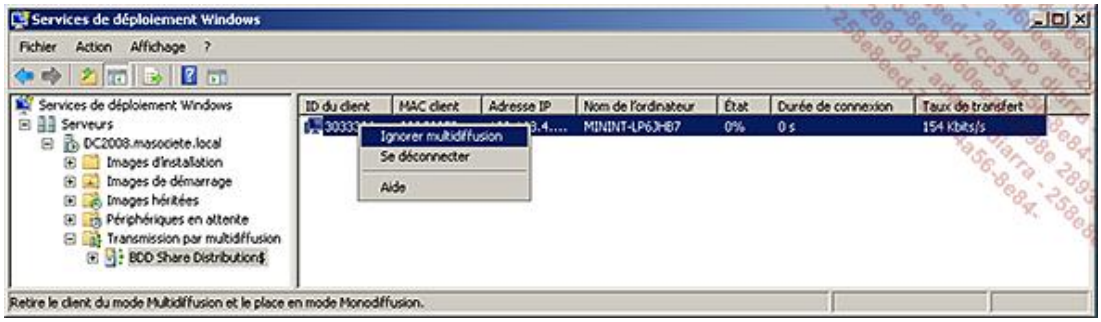
Si des machines arrivent pendant le déploiement, elles récupèrent les données envoyés jusqu'à la fin, puis WDS enverra les données manquantes à ces machines, qui sont donc capables de recevoir les données dans le désordre. Outre le gain réseau, le serveur est capable de déployer plus de machine à la fois car il ne lit qu'une fois les données à déployer. Cela réduit donc très fortement les accès au stockage disque. La liste des machines en cours de déploiement, ainsi que leur débit réseau est affichée depuis la console WDS :



Sous Windows 2008 (et non 2008 R2), la vitesse de déploiement de l'ensemble des machines est égale à la vitesse de déploiement de la machine la plus lente. S'il n'y a, par exemple, que des machines rapides sauf une, celle-ci empêchera les autres de se déployer plus vite. Le serveur n'émettant les paquets réseaux qu'une fois, il doit attendre qu'elles soient toutes prêtes à recevoir le prochain paquet. Dans la fenêtre ci-dessus, la colonne **Taux de transfert** permet de déterminer la vitesse de chaque machine pendant le déploiement. Si une machine est clairement plus lente que les autres, vous pouvez changer son mode de déploiement en partage de fichier, afin qu'elle ne ralentisse plus les autres.

Il suffit pour cela de faire un clic droit sur la machine et de choisir **Ignorer multidiffusion** :

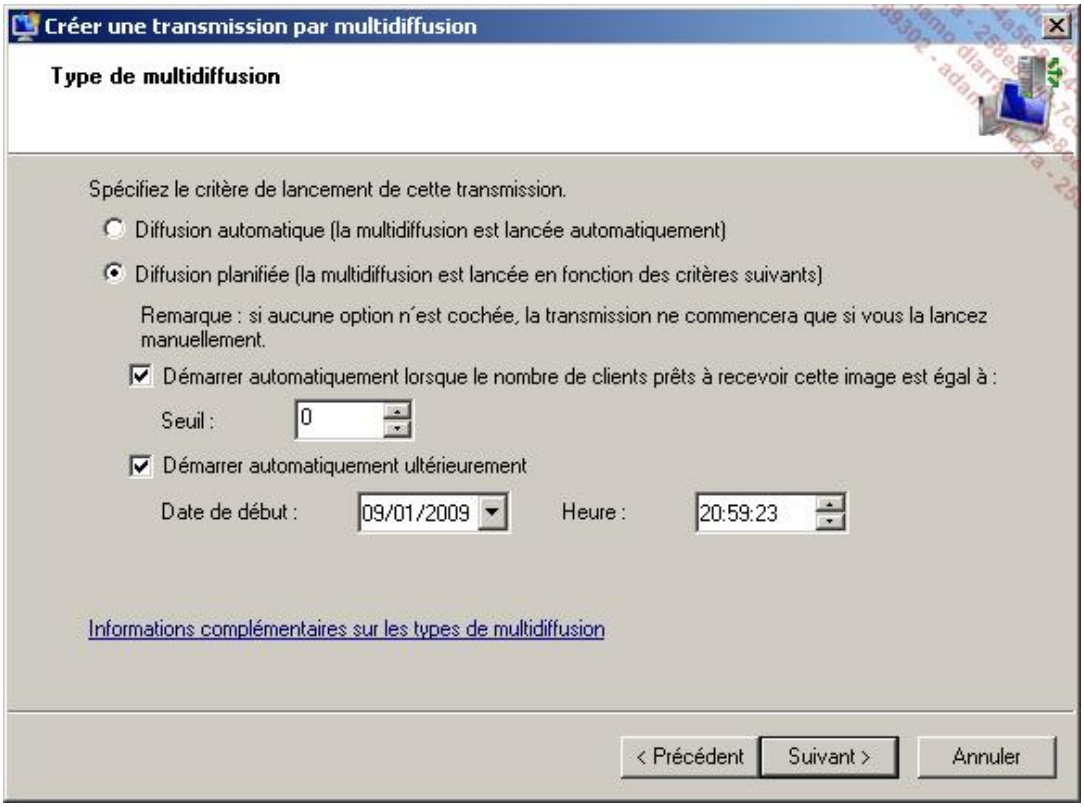
© ENI Editions - All rights reserved - adamo diarra



En revanche, Windows Server 2008 R2 propose de classer automatiquement en deux ou trois catégories les machines (rapide, moyenne, lente). Le serveur devra au final envoyer 2 ou 3 fois les données, mais cela permet de déployer les machines plus rapidement.

La transmission par multidiffusion, créée par défaut par MDT 2010, est de type automatique. C'est-à-dire que le déploiement commence dès qu'un client demande une multidiffusion. WDS propose cependant aussi une multidiffusion planifiée. Cette planification peut se faire sur deux critères :

- le nombre de clients en attente de déploiement ;
- une date et une heure où déclencher le déploiement.



Les deux critères peuvent être utilisés en même temps. Si aucun des deux n'est sélectionné, il faudra démarrer manuellement la multidiffusion. Même s'il s'agit d'un déploiement planifié, un démarrage manuel est toujours possible par ailleurs.

Hors cadre d'utilisation par MDT, WDS sur Windows Server 2008 R2 permet :

- De gérer les pilotes pour des images Windows 7 et Windows Server 2008 R2.
- De démarrer directement sur des images VHD.

© ENI Editions - All rights reserved - adamo diarra

Aller plus loin

Le déploiement de vos serveurs constitue le premier socle technique. Il reste maintenant à automatiser l'installation de vos applications, ce qui peut s'avérer long et difficile. La virtualisation crée un nouveau besoin : le déploiement à la demande d'environnement. Il n'est plus question de faire du paramétrage manuel dans ce contexte.

1. Microsoft Application Compatibility Toolkit

Cet outil vous aide à résoudre les incompatibilités applicatives avec Windows Vista. Les incompatibilités portent généralement sur :

- l'élévation de privilège (UAC) ;
- les tentatives d'écritures dans %ProgramFiles%.

Pour le télécharger gratuitement, il suffit de se rendre ici : http://www.microsoft.com/downloads/details.aspx?FamilyId=24DA89E9-B581-47B0-B45E-492DD6DA2971&displaylang=en

Si vous ne pouvez pas modifier l'application, il vous est possible d'implémenter des *shims*, afin de modifier à la volée les appels posant problèmes pendant l'exécution. Le mot shim désigne une bibliothèque qui convertit l'appel d'une API en un autre. Le programme **Compatibility Administrator** permet de visualiser les shims utilisés par Microsoft pour rendre compatible 5649 applications. Pour y parvenir, 340 shims sont disponibles.

En ajoutant l'argument **-x** au programme ci-dessus, 772 shims sont disponibles. Ils sont masqués par défaut car rarement nécessaires. Il est ainsi possible de « faire croire » à votre application que le système d'exploitation est Windows XP, ou qu'Internet Explorer 6 est présent. Les développeurs ont tendance à faire ces vérifications bloquantes pour être certains qu'il n'y ait pas de problème, alors que la plupart du temps il n'y a pas d'incompatibilité avérée. Une fois l'application rendue compatible avec Windows 7 ou Windows Server 2008 R2, il faudra installer la base de données sur les machines l'utilisant.

Afin de faciliter le diagnostic, le programme **Standard User Analyzer Wizard** guide étape par étape :

- la préparation avant l'exécution.
- l'exécution de l'application, en réalisant toutes les actions posant problèmes.
- l'analyse et la proposition de shims.

2. Environnement à la demande

Le déploiement de machines virtuelles peut devenir très consommateur en temps, surtout s'il s'agit d'environnements à la demande pour du développement. System Center Virtual Machine Manager 2008 R2 offre notamment un portail d'environnement à la demande.

Vous pouvez créer une séquence pour vos environnements virtuels afin d'installer automatiquement les outils additionnels. Hyper-V étant compatible avec le démarrage PXE, vous pouvez installer vos machines virtuelles directement via le réseau avec WDS. Vous n'avez ainsi qu'un point central qui contient toutes vos images et applications pendant le déploiement, au lieu d'avoir une image à part pour la génération de machines virtuelles.

3. ImageX

ImageX est un outil en ligne de commande permettant de gérer et modifier les images WIM. Le format WIM a notamment une propriété intéressante, il est basé sur les fichiers et non les clusters, comme pour les formats ISO. Cela permet notamment de ne stocker dans l'image qu'un seul exemplaire de chaque fichier, même s'il est présent plusieurs fois d'un point de vue logique (*Single Instance Storage*).

L'outil accepte les arguments suivants :

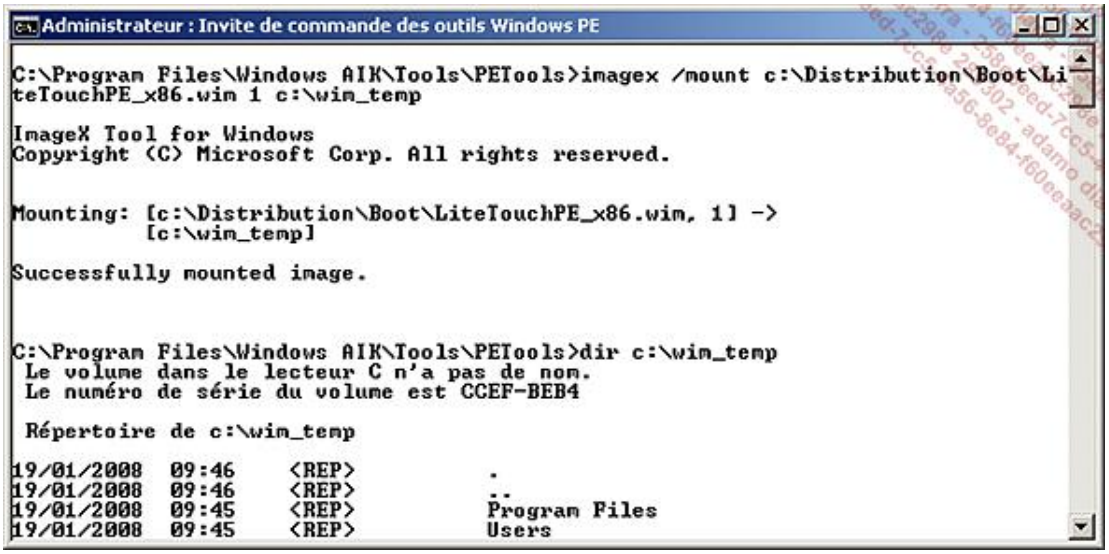
- **APPEND** : combine deux images ensembles.
- **APPLY** : applique une image à un dossier.

© ENI Editions - All rights reserved - adamo diarra

- **CAPTURE** : capture une partition dans une image wim.
- **DELETE** : efface un volume au sein d'un fichier wim.
- **DIR** : liste les fichiers contenus dans un fichier wim.
- **EXPORT** : copie un volume d'un fichier wim dans un autre fichier wim.
- **INFO** : affiche la description XML d'un fichier wim.
- **SPLIT** : sépare un fichier wim en deux fichiers wim.
- **MOUNT** : monte en lecture seule un fichier wim dans un répertoire.
- **MOUNTRW** : monte en lecture et écriture un fichier wim dans un répertoire.
- **UNMOUNT** : démonte un fichier wim d'un répertoire.

Cet outil est utile si vous souhaitez modifier l'image générée par MDT.

Par exemple, pour monter l'image WIM LiteTouch dans un dossier, il faut exécuter : `imagex /mount c:\Distribution\Boot\LiteTouchPE_x86.wim 1 c:\wim_temp`.



L'exécutable ImageX se trouve à différents endroits :

- dans le sous-dossier **Tools\PeTools** du répertoire d'installation de Windows AIK ;
- dans **X:\Deploy\Tools\x86 ou X:\Deploy\Tools\x64** depuis l'environnement de démarrage Windows PE construit par MDT.

4. DISM (Deployment Image Servicing and Management)

Cet outil, fourni avec Windows PE 3.0, combine les fonctions auparavant réparties :

- Montage des fichiers WIM.
- Personnalisation des images de démarrage Windows PE.
- Injection/suppression de pilotes.

© ENI Editions - All rights reserved - adamo diarra

- Activation/Désactivation de composants Windows.

- Configuration des paramètres régionaux.

Il est complémentaire à ImageX, permettant d'en configurer l'image. Leur seul point commun est de pouvoir monter des images WIM.

5. Zero touch avec SCCM 2007 SP2

Utiliser System Center Configuration Manager 2007 permet d'automatiser entièrement le déploiement des machines. Depuis la console SCCM, vous pouvez directement programmer et effectuer des déploiements sur des machines existantes, sans devoir vous déplacer devant la machine pour démarrer en PXE et choisir la séquence.

6. Joindre le domaine sans réseau

Il est possible de joindre une machine à un domaine AD sans que celle-ci n'ait à joindre un contrôleur de domaine pendant toute la procédure. Cela ouvre de nouvelles perspectives :

- Déployer des machines virtuelles ou non en quantité : cela supprime un redémarrage.

- Joindre une machine au domaine alors qu'elle n'a pas accès au réseau à ce moment-là.

- Simplifier la procédure lorsque le contrôleur de domaine est un RODC.

- Limiter les perturbations et diagnostics lorsqu'il y a une erreur ou un incident réseau pendant un déploiement.

La procédure se déroule en deux temps :

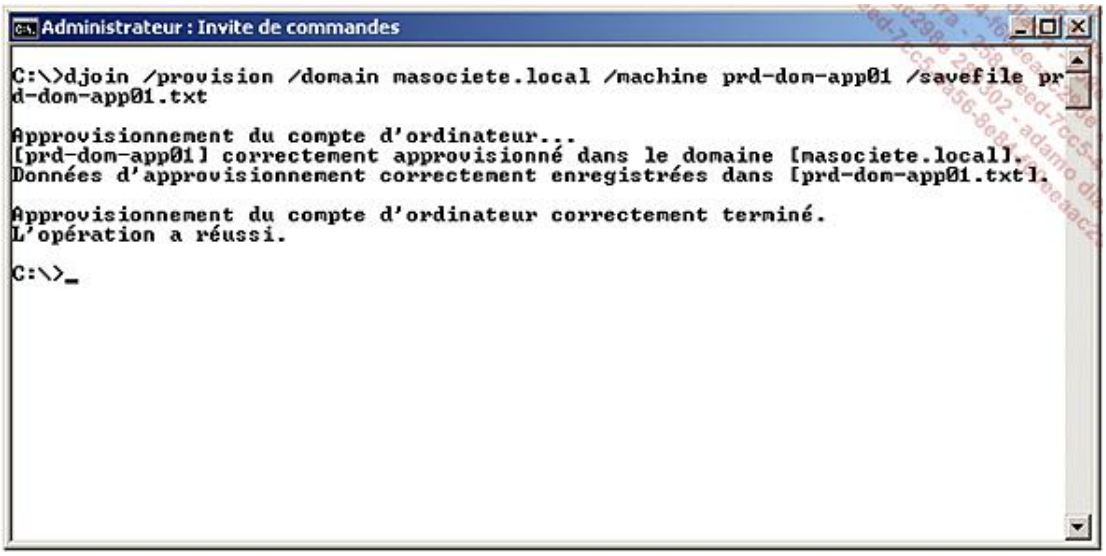
- Préparer l'AD en initialisant l'objet ordinateur avec la commande **djoin**. Il en résulte un fichier texte à conserver (jeton).

- Injecter le fichier ci-dessus dans la machine cible avec **djoin**. Le fichier peut être positionné pendant que la machine est arrêtée. Au démarrage, elle sera membre du domaine sans redémarrage nécessaire.

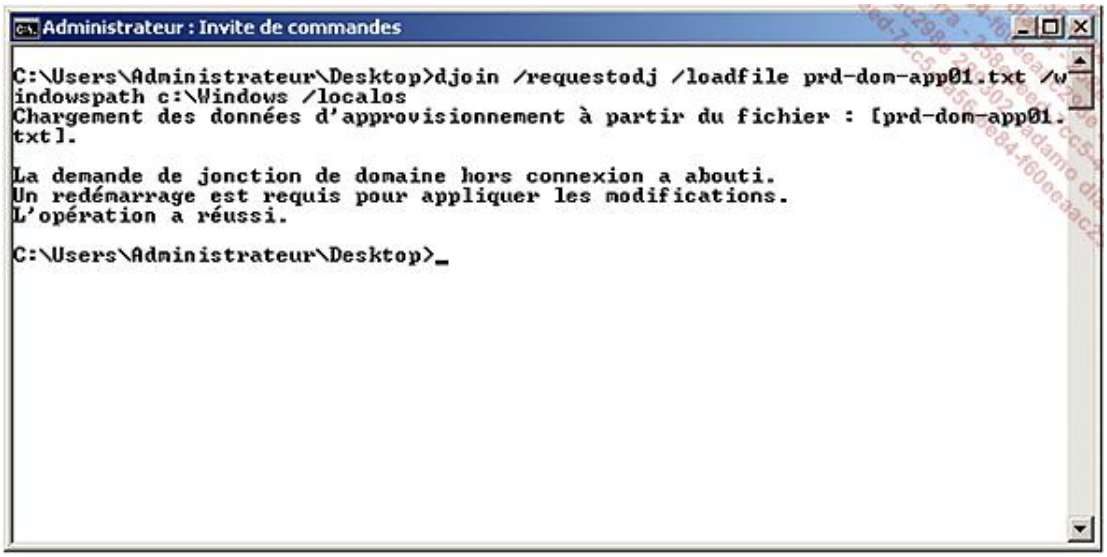
La commande à utiliser est **djoin**. Elle nécessite Windows 7 ou Windows Server 2008 R2 sur l'ordinateur qui prépare l'AD et sur la machine à joindre hors réseau. Le contrôleur de domaine peut être dans une version antérieure à Windows Server 2008 R2 (argument **/downlevel** de **djoin**).

Voici la commande pour préparer la machine prd-dom-app01 :

© ENI Editions - All rights reserved - adamo diarra



Voici la commande pour joindre la machine au domaine :



7. En cas de problème

L'informatique est pleine de surprises qui pimentent notre quotidien. Quand un déploiement ne se passe pas comme prévu, voici certaines traces pertinentes :

- Un problème de jonction au domaine : %WINDIR%\Debug\netsetup.log
- Un problème de pilote : %WINDIR%\inf\Setupapi.dev.log
- Un problème d'installation : %WINDIR%\panther\Setupact.log et Setuperr.log

Message d'erreur "Multiple connections to a server or shared resource by the same user" :

Ce message apparaît lorsqu'une séquence utilise un compte pour se connecter au partage MDT différent de celui défini dans **customsettings.ini**. L'équipe produit MDT fournit les modifications à apporter sur leur blog (**ztiutility.vbs**) :

http://blogs.technet.com/msdeployment/archive/2009/09/18/fix-for-multiple-connections-to-a-server-or-shared-resource-by-the-same-user-using-more-than-one-user-name-are-not-allowed-problem-with-mdt-2010.aspx

Vous êtes maintenant prêt à déployer vos serveurs et postes de travail. D'un point de vue technique, cela n'a jamais été aussi simple et souple, notamment avec MDT 2010. Continuer à faire les installations à la main serait vraiment une perte de temps et de qualité !

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre sera consacré au rôle Services Bureau à distance (Terminal Services) dans Windows Server 2008 R2. Vous pratiquez certainement un usage intensif de ce service pour administrer votre parc de serveurs au quotidien. Après avoir couvert cet usage simple mais néanmoins critique, la puissance du rôle RDP sera mise au jour. Cela couvre notamment la publication d'applications et non plus juste d'un bureau, ainsi que l'accès à ces applications à travers une passerelle Web.

Mais avant de commencer, un éclairage s'impose sur la nomenclature. Le nom des services a changé entre les différentes versionsde Windows Server. Voici donc un récapitulatif des termes utilisés avec Windows Server 2008 R2 afin de vous permettre d'aborder avec sérénité ce chapitre :

Windows Server 2008	Windows Server 2008 R2
Terminal Services	Remote Desktop Services (RDS)
Terminal Server	Hôte de session Bureau à distance
Gestionnaire de licences TS	Gestionnaire de licences Bureau à distance
Service Broker TS	Service Broker pour les connexions Bureau à distance
Accès Web TS	Accès Bureau à distance par le Web
Passerelle TS	Passerelle Bureau à distance

Comme vous le constatez, le changement principal est « Terminal Services », remplacé par « Bureau à Distance ».

À part les nouvelles fonctions, les fonctions qui existaient déjà sous Windows Server 2008 sont inchangées. Windows Server 2008 R2 introduit aussi un nouveau service : Hôte de virtualisation des services Bureau à distance.

Cet ouvrage étant tourné vers Windows Server 2008 R2 en priorité, nous allons utiliser les nouveaux noms dans le reste du chapitre. Les fonctionnalités qui n'existent que dans une version seront cependant mises en évidence. La dénomination « Bureau à distance » sera souvent remplacée par l'acronyme anglais RDS (*Remote Desktop Services*) afin d'alléger la lecture.

© ENI Editions - All rights reserved - adamo diarra

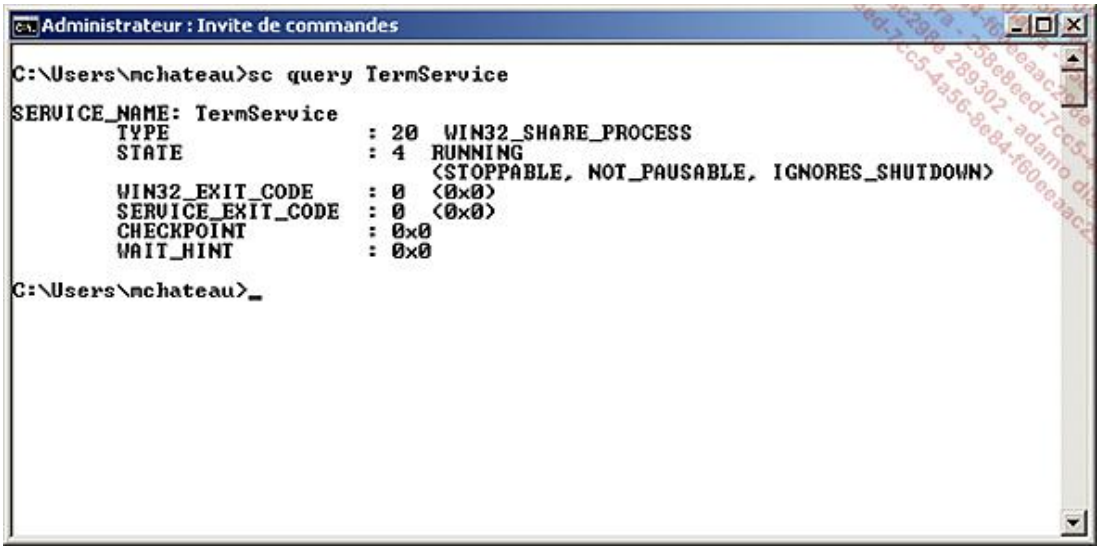
Mise en œuvre des Services Bureau à distance

D'un point de vue technique, le service Bureau à distance est déjà installé par défaut avec Windows Server 2008 R2. Contrairement aux versions précédentes de Windows, il tourne désormais avec le compte « Service Réseau » au lieu du compte système local. La sécurité du système est améliorée, car une faille dans le service a moins d'impact qu'auparavant. Comme expliqué dans la base de connaissance Microsoft (KB946399), le compte « Service Réseau » a besoin de trois privilèges pour lancer le service TSE :

- Ajuster les quotas de mémoire pour un processus (SeIncreaseQuotaPrivilege).
- Générer des audits de sécurité (SeAuditPrivilege).
- Remplacer un jeton de niveau processus (SeAssignPrimaryTokenPrivilege).

Ces trois privilèges ne doivent pas être retirés au compte (par GPO...), sous peine de ne plus pouvoir exécuter le service. Depuis Windows 2008 Server, il est cependant possible d'arrêter le service TSE, ce qui n'était pas le cas avant. Vous pouvez vérifier l'état actuel du service ainsi que les états acceptés par le service en utilisant la ligne de commande suivante (le nom court du service n'a pas été modifié entre les deux versions de Windows Server 2008) :

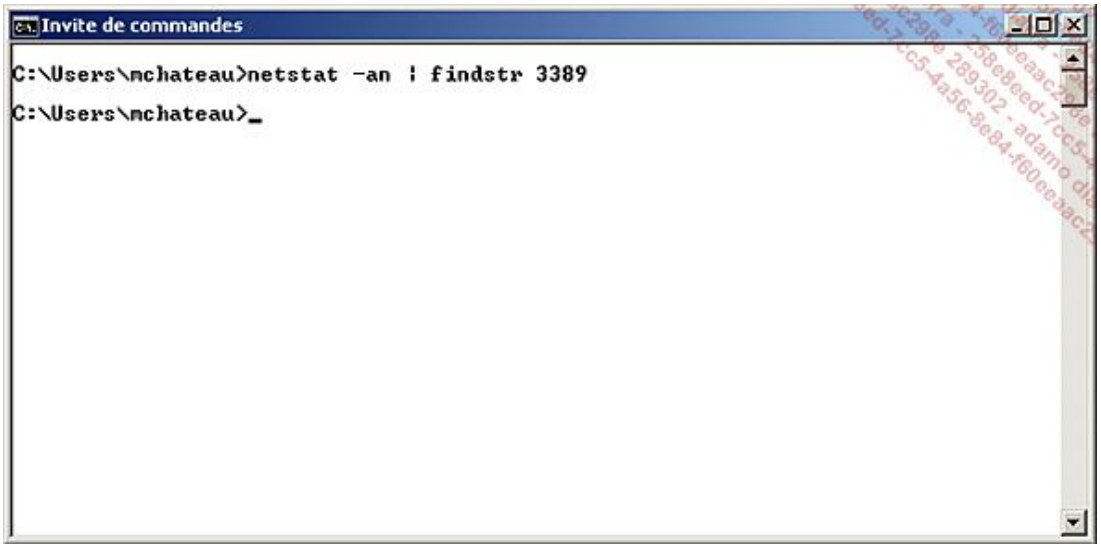
```
sc query TermService
```



Le service RD utilise par défaut le port TCP 3389. Tant que l'accès à distance n'est pas autorisé explicitement, le service n'écoute pas le port TCP afin de ne pas exposer le service sur le réseau. La ligne de commande suivante permet de vérifier que le port TCP 3389 n'est pas écouté sur le serveur pour l'instant :

```
stat -an | findstr 3389
```

© ENI Editions - All rights reserved - adamo diarra



Pour bénéficier de l'ensemble des fonctionnalités offertes par Windows Server 2008 R2, le client RDP version 6.1 est nécessaire. Il est déjà inclus dans Windows 7, Windows Vista Service Pack 1 et Windows XP Service Pack 3. Si vous êtes sous Windows XP Service Pack 2, il est téléchargeable gratuitement à cette adresse : http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=6e1ec93d-bdbd-4983-92f7-479e088570ad

Les services de rôles qui composent le rôle sont :

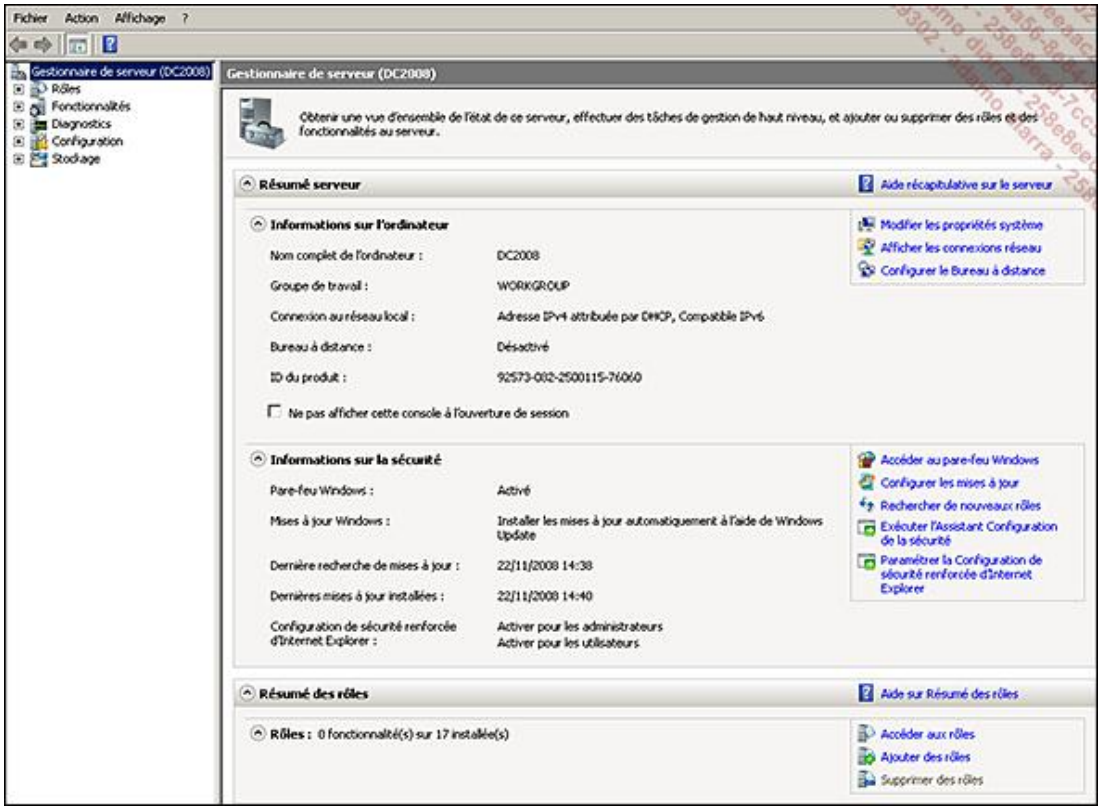
- **Hôte de session** : permet à un serveur d'héberger des applications ou le bureau complet de Windows. Les utilisateurs peuvent s'y connecter, et non plus seulement les administrateurs. La limitation à deux sessions concomitantes est levée.
- **Gestionnaire de licences** : gère l'attribution des licences CAL par périphérique ou utilisateur afin de se connecter à un serveur RD.
- **Session Broker** : permet la répartition des sessions TS dans une ferme de serveurs, ainsi que la reconnexion à une session existante dans une ferme.
- **Passerelle** : permet aux utilisateurs habilités de consommer des ressources depuis Internet du moment que le périphérique exécute le client RDC. Elle n'a pas vocation à remplacer un VPN, mais permet de s'en affranchir pour les accès aux ressources offertes par les services Bureau à distance.
- **Accès Web** : permet aux utilisateurs d'accéder à des applications RemoteApp et au bureau à distance à travers un simple site Web. Un accès Web étant le minimum autorisé en général, cela permet de maximiser les possibilités d'accès par les utilisateurs, notamment depuis les hôtels ou d'autres entreprises.

1. Administration à distance

Bien que le service Windows soit déjà installé et démarré, vous ne pouvez pas l'utiliser pour administrer à distance vos serveurs pour l'instant. Il faut autoriser explicitement l'accès à distance via le **Gestionnaire de serveur**.

- Ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer - Outils d'administration** puis **Gestionnaire de serveur**.
- Au niveau de **Résumé serveur**, cliquez sur **Configurer le Bureau à distance**.

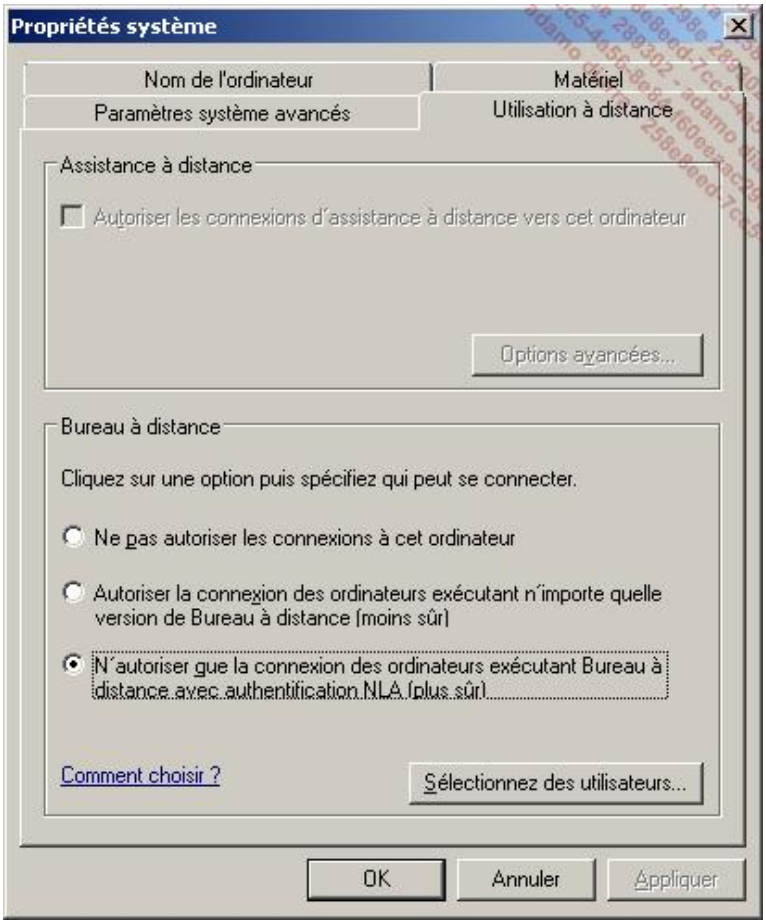
© ENI Editions - All rights reserved - adamo diarra



- La fenêtre suivante s'affiche, permettant d'activer le bureau à distance, avec ou sans NLA. Choisissez **N'autoriser que la connexion des ordinateurs exécutant Bureau à distance avec authentification NLA (plus sûr)**.

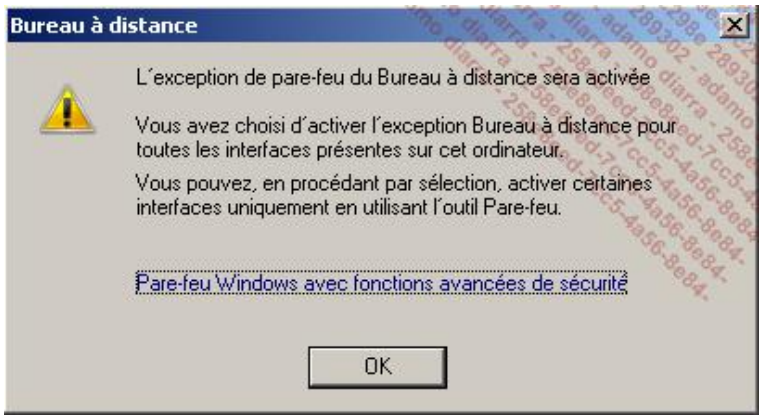
NLA signifie *Network Level Authentication*. L'objectif est de lutter contre les attaques dites de l'homme du milieu (man in the middle) en authentifiant le serveur RD avant que l'utilisateur ne s'y connecte. Il peut utiliser différents protocoles pour arriver à cet objectif : kerberos, TLS/SSL, NTLM. Techniquement, il s'appuie sur le fournisseur CredSSP qui utilise lui-même SSPI (*Security Service Provider Interface*). Après la phase d'authentification mutuelle, le client fournit les identifiants de l'utilisateur qui sont encryptés deux fois avec les clés de sessions SPNEGO et TLS.

© ENI Editions - All rights reserved - adamo diarra



Cette interface modifie en fait deux clés de registre : **fDenyTSConnections** et **UserAuthentication**, situées sous **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server**. La première bloque toute connexion TS et la deuxième exige l'authentification NLA quand elles sont positionnées à 1.

- Le message d'information suivant apparaît, cliquez sur le bouton **OK**.



La gestion du pare-feu Windows est décrite dans le chapitre Sécuriser votre architecture.

- Cliquez sur le bouton **OK** pour fermer la fenêtre des propriétés système.

Maintenant que l'accès au bureau à distance est ouvert, le service TSE écoute le port TCP (une ligne pour IP version 4 et une ligne pour IP version 6) :

© ENI Editions - All rights reserved - adamo diarra

Pour la petite histoire, IPV5 existe bien, mais il s'agit d'une version de test (RFC 1819).

Vous pouvez maintenant utiliser le bureau à distance pour administrer votre serveur. Cette fonctionnalité n'a pas nécessité l'installation du rôle Bureau à distance. L'administration à distance est jugée indispensable pour tous les serveurs, quel que soit leur usage, et ne caractérise donc pas un rôle à ce stade.

L'administration à distance est très utile, mais ne constitue pas une avancée notable. Il est donc temps d'exploiter tout le potentiel du rôle ! Pour cela, après avoir installé les composants du rôle, ils seront configurés dans le cadre d'un exemple concret.

2. Le rôle Hôte de session

a. Installation

Afin de ne pas s'installer dans la routine des assistants, installez le rôle et ses services associés avec PowerShell, en ligne de commande :

```
Import-module servermanager
Add-WindowsFeature RDS-RD-Server,RDS-Licensing,RDS-Connection-Broker,
RDS-Gateway,RDS-Web-Access
```

En effet, depuis Windows Server 2008 R2, l'outil **servermanagercmd** est déprécié au profit de PowerShell. L'utilisation de cet outil génèrera une alerte indiquant qu'il ne sera peut-être plus présent dans les futures versions. Une autre différence est l'utilisation de la virgule comme séparateur.

Pour information, voici la ligne de commande équivalente basée sur **servermanagercmd** :

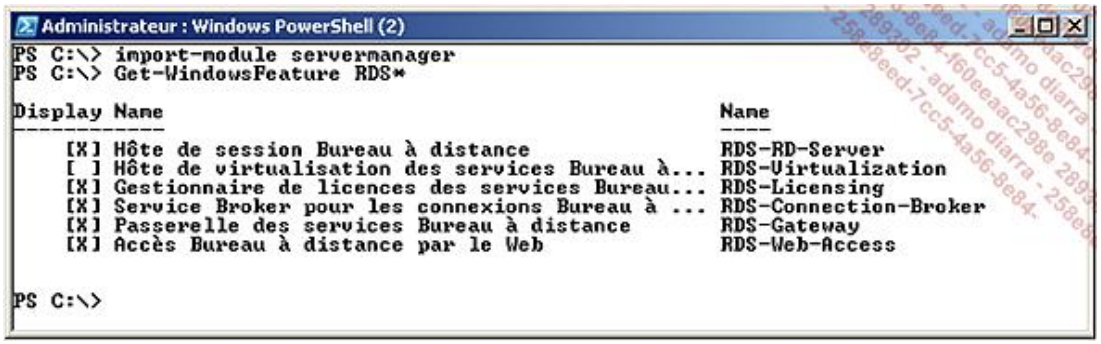
```
servermanagercmd -i TS-Terminal-Server TS-Licensing TS-
Session-Broker TS-Gateway TS-Web-Access
```

Un message d'avertissement vous indiquera qu'un redémarrage est nécessaire pour prendre en compte l'installation du rôle. Si vous réalisez l'installation depuis le **gestionnaire de serveur**, et que le serveur a aussi le rôle contrôleur de domaine, une alerte vous indiquera que ce n'est pas recommandé. Installer le rôle Bureau à distance sur un contrôleur de domaine comporte de vrais risques que vous devez évaluer au préalable.

Redémarrez le serveur pour finaliser l'installation de ce rôle. Une icône dans la barre des tâches vous alertera sur l'absence de licences. Faute d'avoir un serveur de licences, un délai de grâce de 120 jours sera mis en œuvre. Vérifiez que les services de rôles sont bien installés, depuis la ligne de commande avec :

```
Import-module servermanager
Get-WindowsFeature RDS*
```

© ENI Editions - All rights reserved - adamo diarra



L'équivalent avec **servermanagercmd** :

```
servermanagercmd -q | findstr TS
```

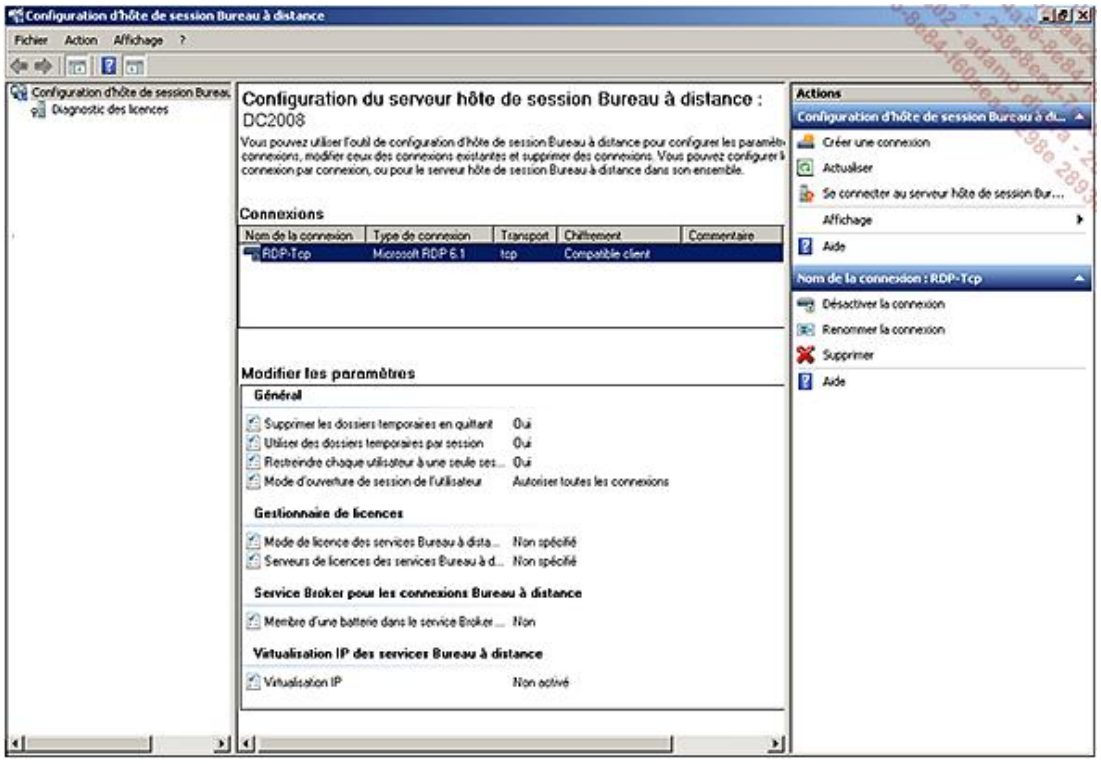
Dans cet exemple, l'ensemble des rôles est sur un serveur unique. Cependant, dans votre architecture, il peut être pertinent d'installer par exemple le **Gestionnaire de Licences** sur le serveur exécutant KMS (*Key Management System*). Si ce service de rôle est en particulier installé sur un contrôleur de domaine, tous les serveurs RDS du domaine seront capables de le trouver automatiquement. Le rôle Hôte de virtualisation n'est pas installé car il nécessite une infrastructure Hyper-V et SCVMM.

---

b. Configuration

La configuration se fait via la console **tsconfig.msc**. Vous pouvez la lancer depuis le menu **démarrer** :

- Ouvrez la console **Configuration des services Terminal Server** en cliquant sur le bouton **Démarrer - Outils d'administration**, puis **Services Bureau à distance** et enfin **Configuration d'hôte de session Bureau à distance**.



- Cliquez deux fois sur la connexion **RDP-Tcp**.

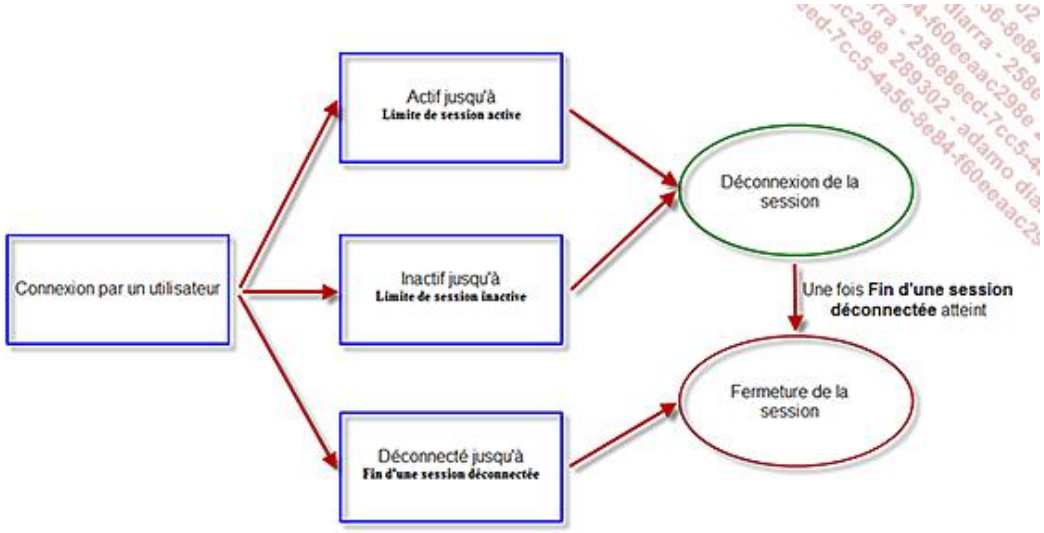
Depuis l'onglet **Sessions**, vous pouvez définir la durée de vie des sessions inactives, ainsi que le comportement à adopter quand le temps imparti est atteint. Pourquoi gérer ces aspects ? Si un utilisateur ne fait que se déconnecter, toute sa session ainsi que les programmes en mémoire restent sur le serveur. La consommation en ressource système étant maintenue, le serveur ne peut pas accueillir d'autres utilisateurs à la place. Voici une explication et

© ENI Editions - All rights reserved - adamo diarra

une recommandation pour les paramètres :

- **Fin d'une session déconnectée** : ferme de façon arbitraire toute session déconnectée. Valeur suggérée : 2 heures.
- **Limite de session active** : oblige l'utilisateur à fermer sa session même s'il est actif. Cela permet de lutter contre les fuites mémoires dans les applications, et d'éviter qu'un utilisateur ne ferme jamais sa session. Valeur suggérée : 12 heures.
- **Limite de session inactive** : ferme de façon arbitraire toute session maintenue par un client mais qui n'envoie pas d'évènements clavier/souris. Valeur suggérée : 4 heures.
- **Lorsqu'une limite de session est atteinte ou la connexion est interrompue** : action à appliquer quand un des deux évènements est atteint. Choix suggéré : **Déconnexion de la session**.

L'enchaînement est donc le suivant :



Le temps maximum avant la fermeture d'une session est donc égal à :

Limite de session active + **Fin d'une session déconnectée** = 14 heures.

Vous avez remarqué que l'utilisateur a encore 2 heures potentielles pour se reconnecter sans pour autant perdre sa session.

Avant de sauvegarder un serveur TS le soir, il est recommandé de fermer toutes les sessions TS du serveur de façon arbitraire. Cela évite les erreurs sur les fichiers ouverts en mode exclusif, et permet de sauvegarder les profils TSE (recopiés à la fermeture de session sur leur répertoire).

---

c. Configuration de l'accès Web

L'usage de RDS s'est étendu bien au-delà d'un simple bureau à distance. Windows Server 2008 R2 offre donc un moyen pour centraliser les ressources publiées sur un portail Web. Du point de vue du client, deux critères restent nécessaires :

- Pouvoir accéder au site Web fourni par l'accès Web depuis un navigateur, avec ou sans proxy.
- Avoir le client RDC 6.1 installé. Il est déjà intégré à Windows depuis Windows Vista Service Pack 1 et Windows XP Service Pack 3.

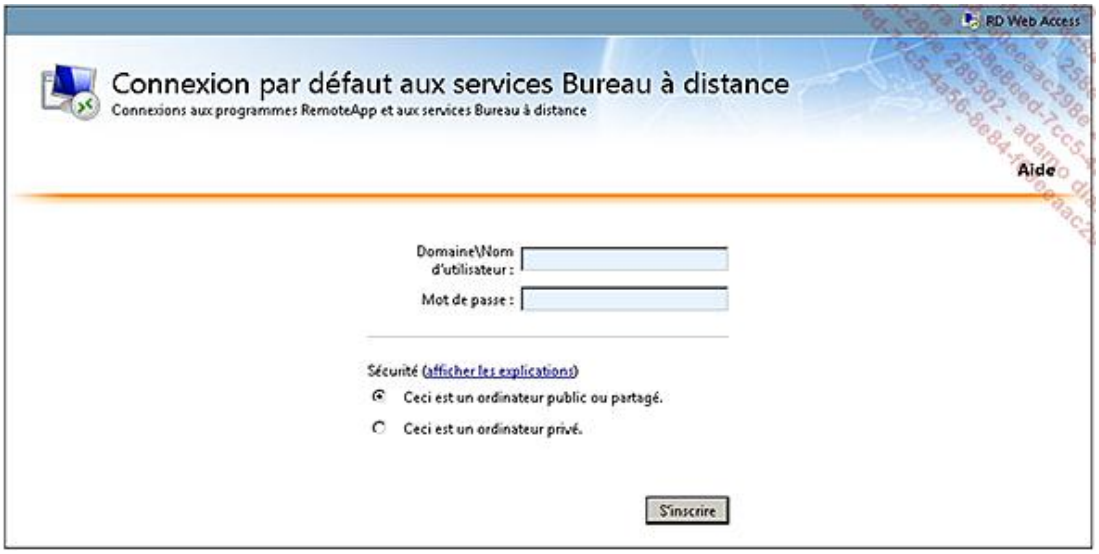
Ce service de rôle peut être installé sur un serveur qui n'a pas le service Terminal Server. Il nécessite toutefois au moins IIS 7 pour fonctionner et une relation de confiance avec les serveurs hôtes de sessions pour pouvoir lister les applications RemoteApp.

Pour accéder au service, ouvrez un navigateur Web à cette adresse, en remplaçant *MonServeurWebRDS* par le nom

© ENI Editions - All rights reserved - adamo diarra

du serveur ayant le service de rôle : http://MonServeurWebRDS/RDWeb/

Par défaut, l'authentification se fait via un portail (formulaire) :



Une fois authentifié, la page suivante d'affiche :

Deux onglets sont présents. L'onglet **Programmes RemoteApp** est peuplé dynamiquement par les applications auxquelles vous avez droit si la fonctionnalité RemoteApp a été configurée. L'onglet **Bureau à distance** permet d'avoir une session RDP complète via le site Web.

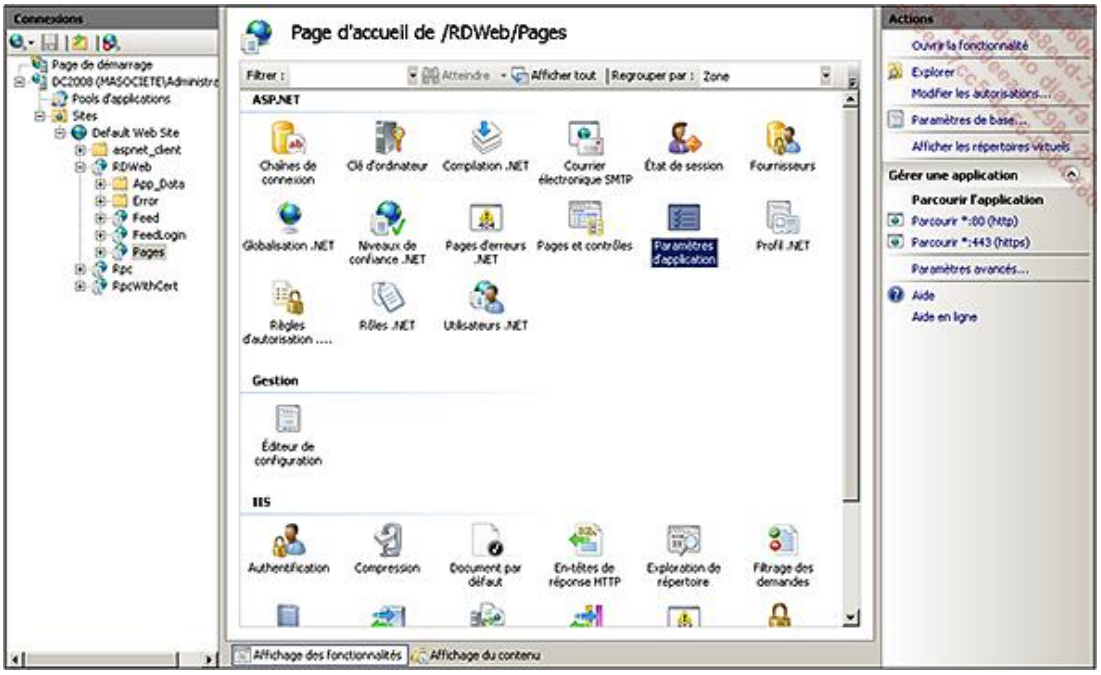
L'onglet **Bureau à distance** offre quelques options, mais ne permet pas de choisir le serveur sur lequel ouvrir une connexion. Pour configurer le service, vous avez deux options possibles :

- passer par la MMC IIS7 ;
- éditer le fichier de configuration XML, *web.config*, présent par défaut dans C:\Windows\Web\RDWeb\Pages.

Configuration via IIS :

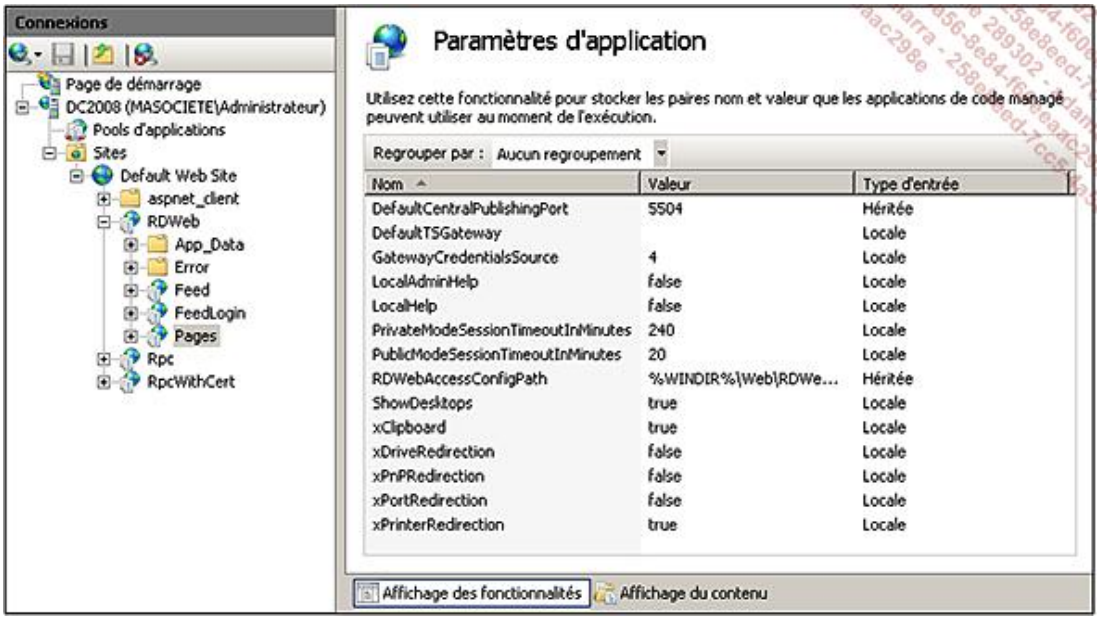
- Ouvrez la console **Gestionnaire des services Internet (IIS)** en cliquant sur le bouton **Démarrer** - **Outils d'administration** puis **Gestionnaire des services Internet (IIS)**.
- Dans l'onglet **Connexions**, dépliez le nom de votre serveur, puis **Sites - Default Web Site - RDWeb** et enfin le dossier virtuel **Pages**.
- Cliquez deux fois sur l'icône **Paramètres d'application** au centre de l'écran :

© ENI Editions - All rights reserved - adamo diarra



Le site d'accès Web TS peut être incorporé dans un site SharePoint, car il s'agit d'un Web part. Cette partie n'est pas couverte dans cet ouvrage, car SharePoint est hors périmètre.

Les paramètres configurables sont les suivants :



DefaultTSGateway : permet de spécifier la passerelle par défaut à utiliser pour les connexions. Par défaut, aucune passerelle n'est positionnée. Une fois l'application RemoteApp ou le bureau à distance choisi, une connexion RDP classique sur le port TCP 3389 sera effectuée.

GatewayCredentialsSource : peut prendre les valeurs 0, 1 ou 4. La valeur par défaut est 4, ce qui correspond à « me demander plus tard ».

ShowDesktops : positionné à *true* par défaut. Cette variable contrôle le fait d'afficher ou non l'onglet **Bureau à distance** sur le site Web.

xClipboard : positionné à *true* par défaut. Bloque l'utilisation du presse papier Windows s'il est positionné à *false*.

xDriveRedirection : positionné à *false* par défaut. Autorise la redirection des lecteurs locaux s'il est positionné à *true*.

xPnPRedirection : positionné à *false* par défaut. Autorise la redirection de périphériques dit plug & play s'il est positionné à *true*. Cela concerne uniquement les périphériques multimédia prenant en charge le *Media Transfer Protocol*, le *Picture Transfer Protocol* ou *Microsoft Point of Service (POS) for .NET 1.11*.

© ENI Editions - All rights reserved - adamo diarra

xPortRedirection : positionné à *false* par défaut. Autorise la redirection de port COM et LPT s'il est positionné à *true*.

xPrinterRedirection : positionné à *true* par défaut. Bloque la redirection des imprimantes s'il est positionné à *false*.

Passer par le fichier XML *web.config* a l'avantage d'avoir accàs aux commentaires qui expliquent les différentes valeurs, par exemple pour GatewayCredentialsSource :

```
<!-- GatewayCredentialsSource: TS Gateway Authentication Type.
          Admins can preset this.
          0 = User Password
          1 = Smartcard
          4 = "Ask me later"
-->
```

Les modifications sont traitées à chaud et ne nécessitent aucun redémarrage. Il suffit de rafraîchir la page Web pour voir les changements.

Si l'accès Web est installé sur un serveur qui est aussi Hôte de session, il utilisera le serveur où il est installé pour détecter les applications publiées via RemoteApp. En revanche, s'il est installé seul, l'onglet supplémentaire **Configuration** permettra de choisir le serveur RDS à partir duquel afficher les applications publiées. Le groupe Windows *Ordinateurs Accès Web TS* devra contenir le compte ordinateur du serveur d'accès Web, afin qu'il puisse interroger la liste des programmes.

Dans notre cas, tous les services de rôles sont sur le même serveur. Mais ajouter le serveur à ce groupe est recommandé afin d'être conforme aux bonnes pratiques. Comme il s'agit d'un contrôleur de domaine, il faut éditer le groupe *Ordinateurs Accès Web TS* via le composant *DSA* : **Démarrer - Exécuter - dsa.msc**. La seule particularité est qu'il faut ajouter les objets ordinateurs dans les filtres.

Par défaut, les applications RemoteApp sont activées pour l'Accès Web. Cette autorisation peut se gérer par application, depuis la console **Gestionnaire RemoteApp**.

d. Configuration de la passerelle Bureau à distance

L'usage de RDS s'est répandu au-delà des frontières de l'entreprise. Une fois en dehors de l'entreprise, on ne maîtrise plus l'infrastructure en place, ainsi que ses restrictions. L'ouverture d'une connexion sur le port TCP 3389 depuis une autre société, un hôtel ou autre est parfois bloquée par des firewalls, ce qui en limite la pertinence. Windows Server 2008 R2 offre donc un moyen de transport adapté à ce contexte pour accéder aux ressources : HTTPS.

Le premier pré-requis sera d'avoir un certificat SSL valide, que ce soit via un tiers de confiance, soit via votre propre infrastructure de PKI. Windows Server 2008 R2 vous permet de générer un certificat auto-signé, mais cela implique de pouvoir ajouter ce certificat racine sur les ordinateurs utilisés pour se connecter. Cette solution est peu onéreuse, mais l'expérience utilisateur n'est pas optimale, et va être problématique pour la connection depuis un ordinateur en libre service dans un hôtel, par exemple. Le principal est que le poste client considère votre certificat comme digne de confiance.

Les attributs du certificat doivent respecter certaines règles que voici :

- Le certificat doit être de type ordinateur.
- L'objet du certificat est l'authentification du serveur. L'attribut EKU est de type Server Authentication (1.3.6.1.5.5.7.3.1).
- Le certificat ne doit pas avoir expiré.
- Un OID de 2.5.29.15 n'est pas requis, mais si vous souhaitez l'utiliser il doit aussi avoir un de ces usages :

  CERT_KEY_ENCIPHERMENT_KEY_USAGE, CERT_KEY_AGREEMENT_KEY_USAGE, et CERT_DATA_ENCIPHERMENT_KEY_USAGE.

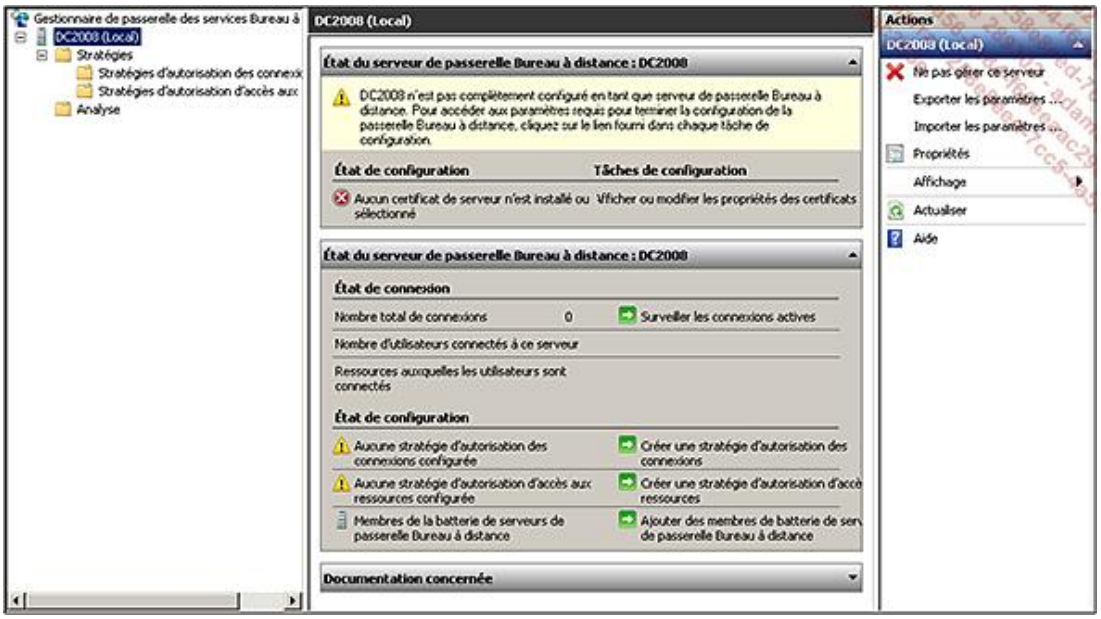
- Le nom du certificat (CN) doit correspondre au nom DNS utilisé par le client pour se connecter à la passerelle.

Pour créer un certificat :

- Ouvrez la console **Gestionnaire de passerelle Bureau à distance** en cliquant sur le bouton **Démarrer - Outils**

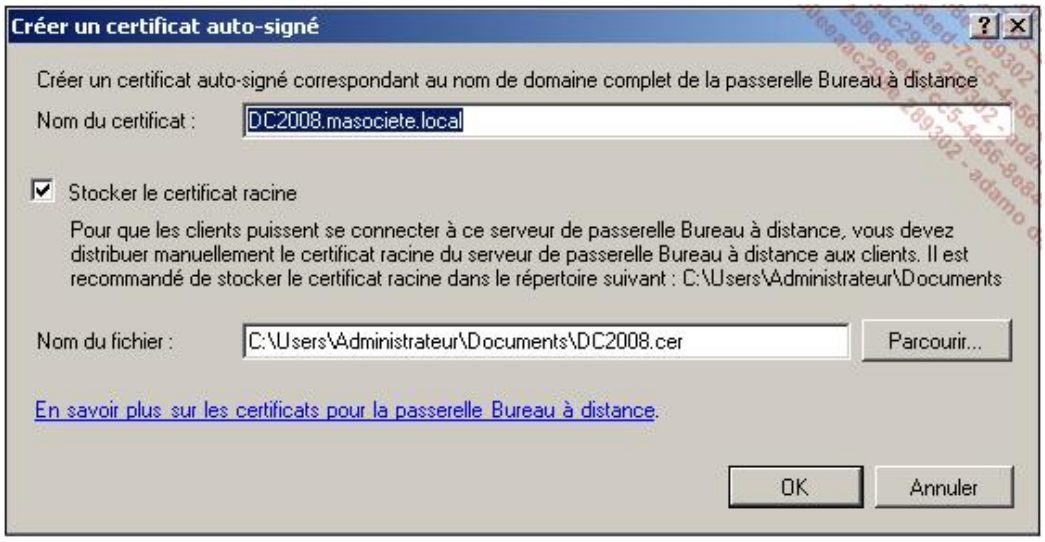
© ENI Editions - All rights reserved - adamo diarra

d'administration - Services Bureau à distance puis **Gestionnaire de passerelle Bureau à distance**.



- Dans le panneau gauche, faites un clic avec le bouton droit sur le nom de votre serveur, puis cliquez sur **Propriétés**.

- Dans l'onglet **Certificat SSL**, cliquez sur **Créer un certificat**. L'écran suivant apparaît :

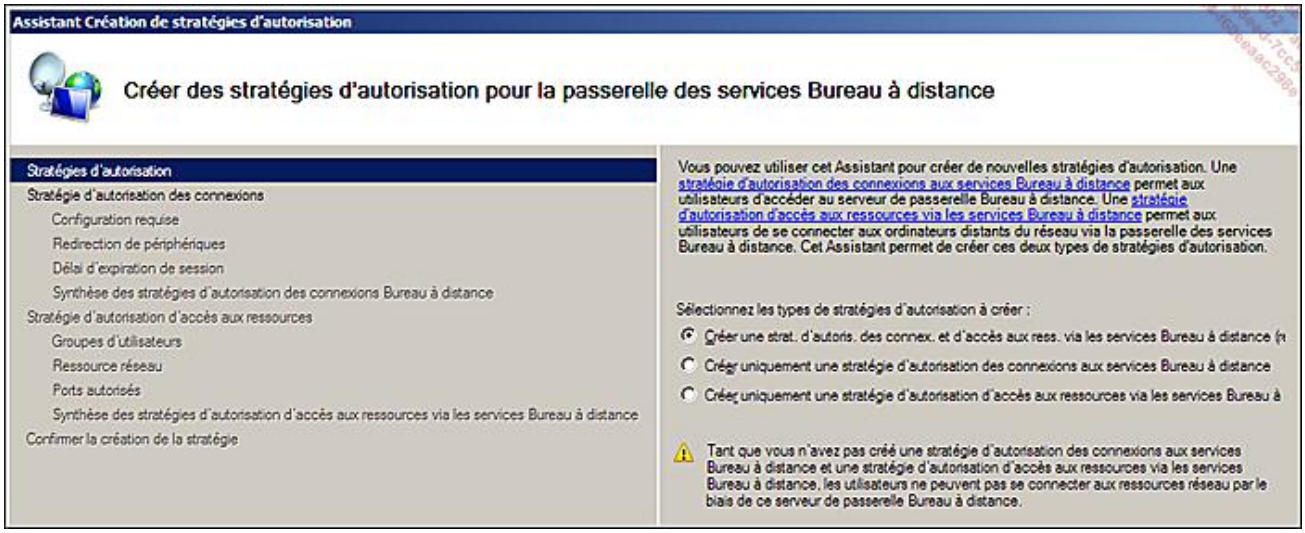


Il faudra ajouter le certificat racine généré à tous les clients utilisant la passerelle. Cela permet à la passerelle TS de fonctionner sans message d'avertissement, immédiatement mais cela n'est pas souhaitable en production. C'est toutefois suffisant dans le cadre de cet ouvrage.

- Validez le message d'information, et revenez à la fenêtre principale du Gestionnaire de passerelle TS.

- Dépliez le dossier **Stratégies**, puis cliquez sur **Créer des stratégies d'autorisation** dans le panneau **Actions**.

© ENI Editions - All rights reserved - adamo diarra

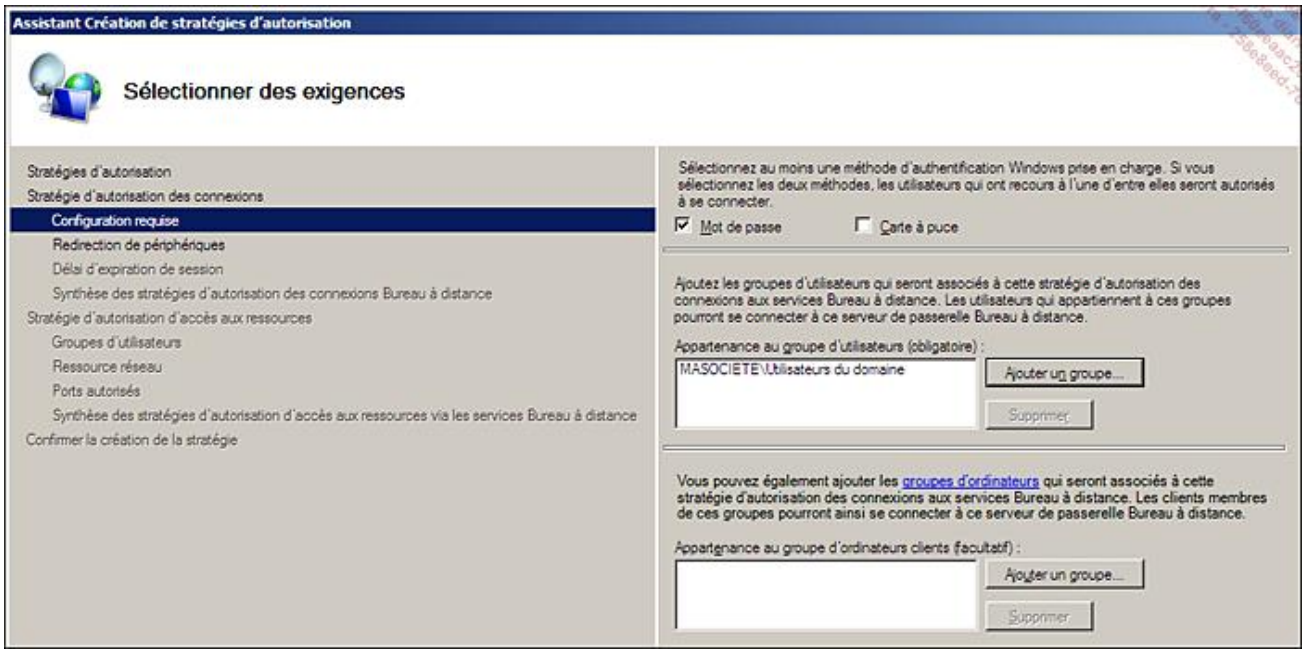


- Choisissez **Créer une strat. d'autoris. des connex. et d'accès aux ress. via les services Bureau à distance** puis cliquez sur **Suivant**.

- Choisissez un nom à donner à la stratégie, *Stratégie des connexions de masociete* par exemple.

- L'écran suivant vous permet de définir les méthodes d'authentification acceptées (mot de passe, carte à puce ou les deux). Vous devez ensuite spécifier les groupes d'utilisateurs et d'ordinateurs autorisés à utiliser la passerelle.

- Ajoutez le groupe *Utilisateurs du domaine* pour **Appartenance au groupe d'utilisateurs** puis cliquez sur **Suivant**.



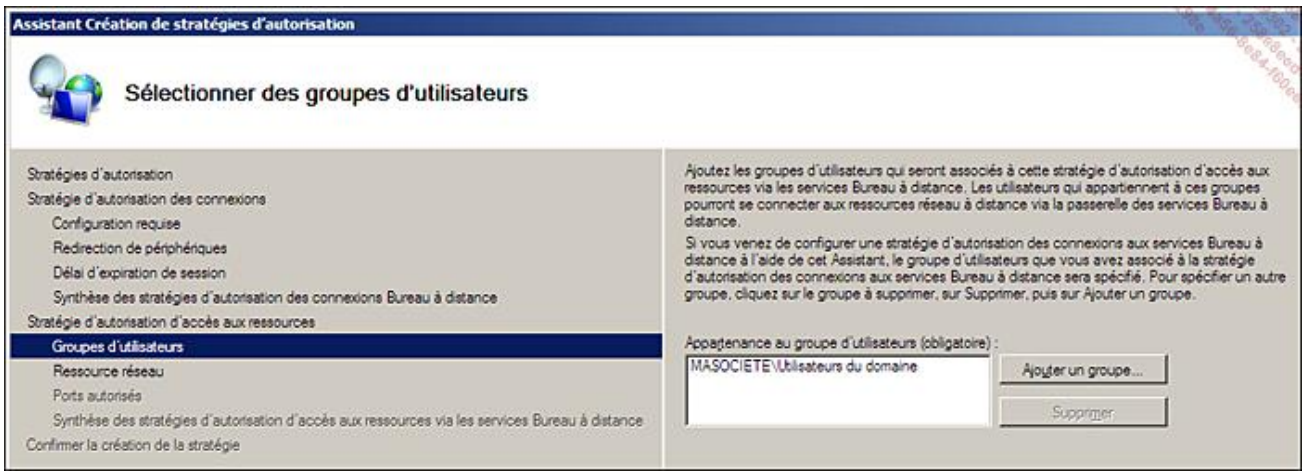
- Par défaut, l'ensemble des redirections sont actives via la passerelle. Vous avez la possibilité de restreindre les redirections disponibles et le délai d'expiration. Cliquez sur **Suivant**.

- La synthèse de la stratégie est affichée, cliquez sur **Suivant**.

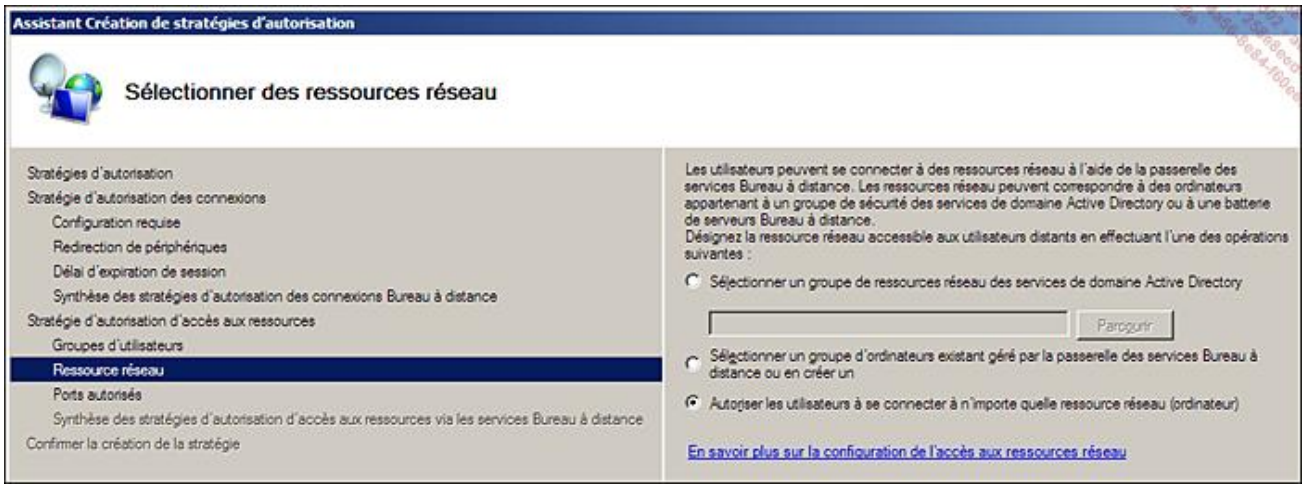
- L'assistant permet maintenant de créer une **Stratégie d'autorisation d'accès aux ressources**. Entrez *Stratégie d'accès aux ressources de masociete* comme nom et cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra

- Le groupe d'utilisateurs autorisé à accéder aux ressources est déjà prérempli avec le groupe déclaré pour la première stratégie. Cliquez sur **Suivant**.

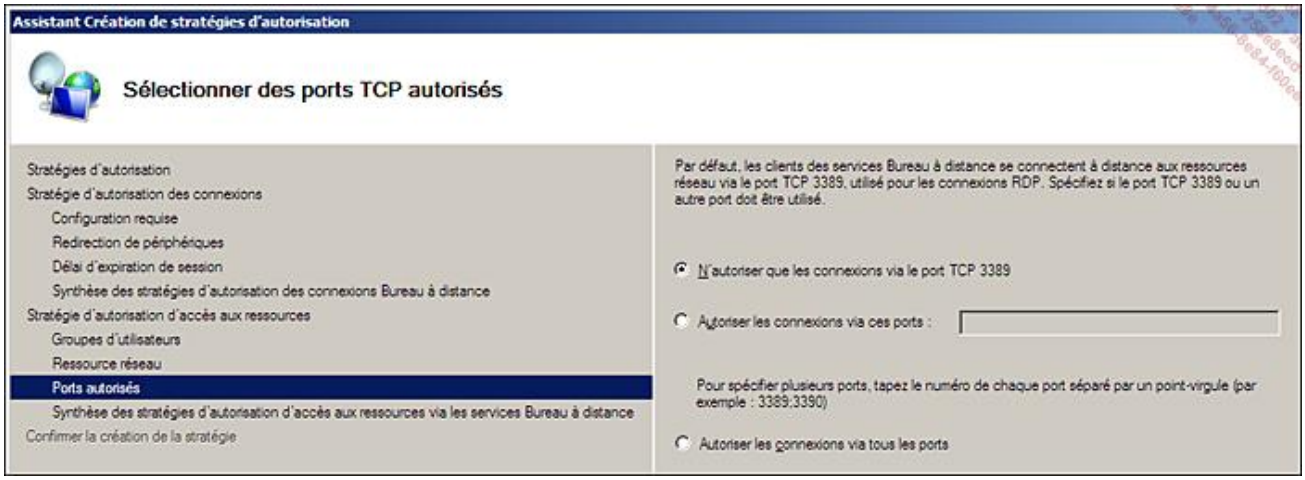


- Il est important de définir les ordinateurs auxquels les utilisateurs pourront accéder à travers la passerelle. Il est possible de spécifier un groupe Active Directory, un groupe géré par la passerelle TS ou bien tous les ordinateurs. En production, vous devrez être le plus restrictif possible dans l'ouverture des accès. Choisissez **Autoriser les utilisateurs à se connecter à n'importe quelle ressource réseau (ordinateur)** et cliquez sur **Suivant**.

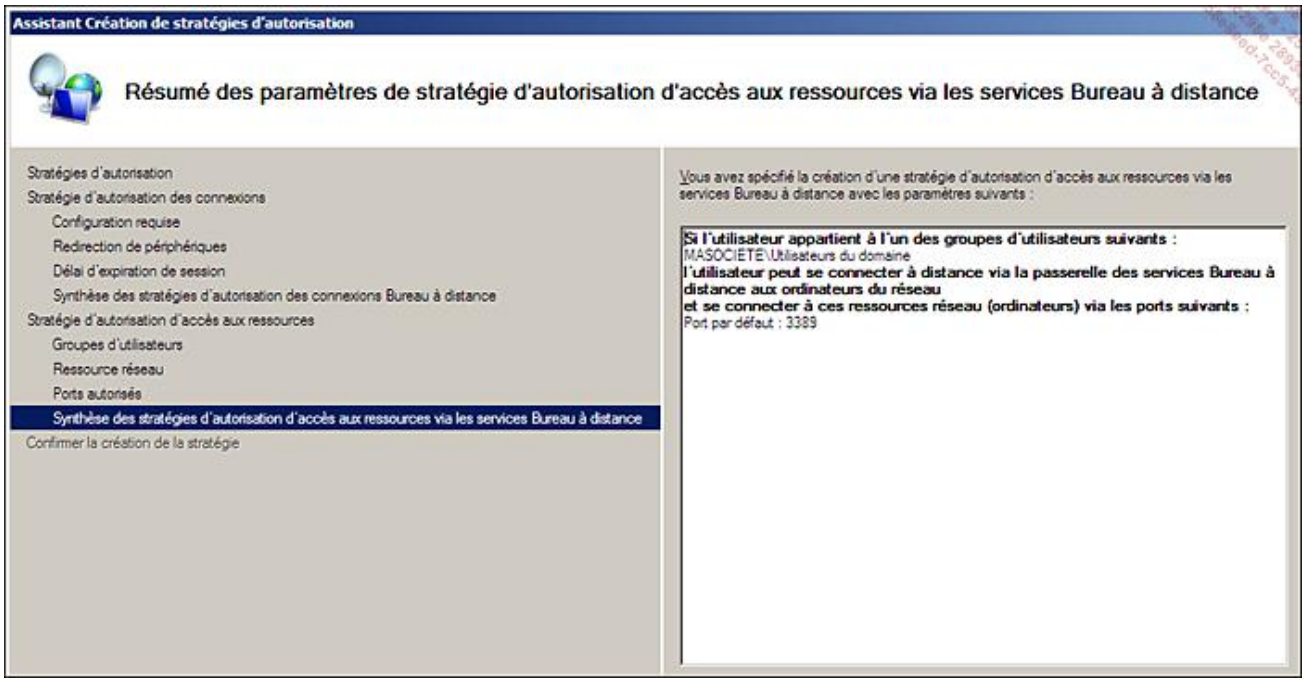


- L'écran suivant permet de définir les ports réseaux autorisés. Par défaut, seul le port TCP 3389, qui est le port RDP par défaut est autorisé. Cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- La synthèse de la stratégie s'affiche, cliquez sur **Terminer** puis sur **Fermer**.



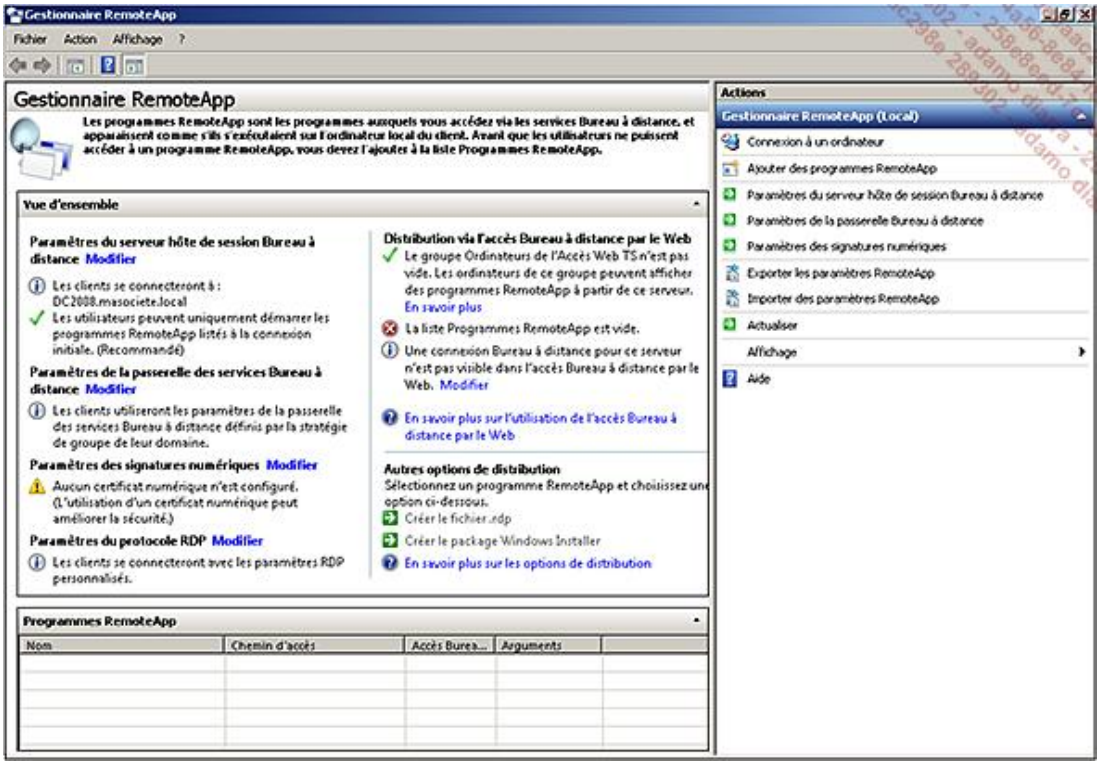
La passerelle RDS est maintenant opérationnelle. Elle possède un certificat SSL auto généré et deux stratégies ont été définies. Tous les utilisateurs du domaine peuvent utiliser la passerelle pour accéder à n'importe quel ordinateur du réseau.

e. Configuration du RemoteApp

Ce service de rôle rend RDS très attrayant. Il permet de publier des applications au lieu d'un bureau complet. Pour le configurer :

- Ouvrez la console **Gestionnaire RemoteApp** en cliquant sur le bouton **Démarrer - Outils d'administration** puis **Services Bureau à distance** et **Gestionnaire RemoteApp**.

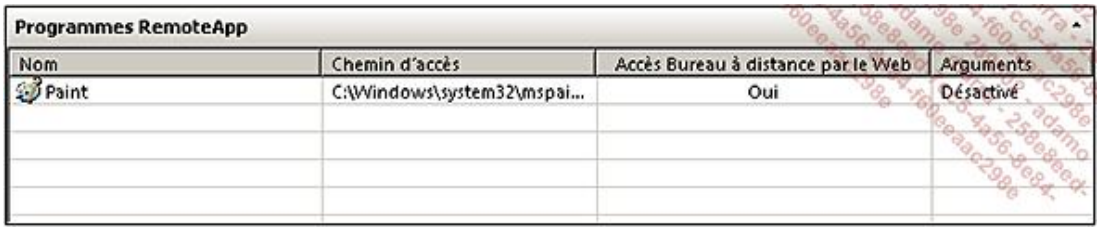
© ENI Editions - All rights reserved - adamo diarra



Par défaut, l'accès bureau à distance n'apparaît pas pour notre serveur sur l'accès Web configuré précédemment. Les utilisateurs peuvent toujours aller dans l'onglet **Bureau à distance** et renseigner le nom du serveur, mais ce n'est pas très ergonomique. Pour ajouter explicitement une icône bureau à distance dans les RemoteApp, cliquez sur un des liens hypertextes **Modifier**. Allez dans l'onglet **Serveur hôte de session Bureau à distance** et cochez la case **Afficher une connexion Bureau à distance sur ce serveur hôte de session Bureau à distance dans l'accès Bureau à distance par le Web**.

- Pour publier un programme via RemoteApp, dans le panneau **Actions**, cliquez sur **Ajouter des programmes RemoteApp**. Cliquez sur **Suivant**, puis choisissez **Paint** et cliquez sur **Suivant** et **Terminer**.

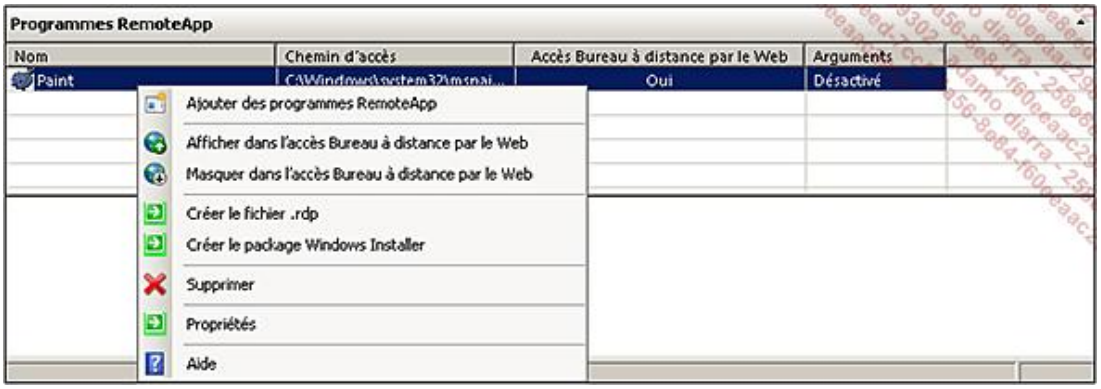
L'application Paint apparaît maintenant dans la liste des programmes RemoteApp :



Depuis l'Accès Web, l'application apparaît immédiatement en rafraîchissant l'écran :

RemoteApp permet aussi de créer un fichier rdp ou un package Windows Installer afin que les utilisateurs puissent accéder à l'application :

© ENI Editions - All rights reserved - adamo diarra



- Le fichier rdp est très simple à déployer et peut être envoyé par mail aux utilisateurs.

- L'installation via un package MSI complique l'installation, mais permet un inventaire sur les postes de travail, une industrialisation du déploiement, ainsi que l'association des extensions de fichiers. Par exemple, si Microsoft Visio est uniquement disponible via Terminal Service, le package peut associer l'extension .vsd à cette application publiée. Ainsi, lorsqu'un utilisateur double clique sur un fichier .vsd, Microsoft Visio est automatiquement lancé en tant que RemoteApp et ouvre le fichier demandé. L'opération est donc transparente pour l'utilisateur.

f. Configuration du gestionnaire de licences Bureau à distance

Les licences d'accès clients Windows Server 2008 R2 sont compatibles avec celles de Windows Server 2008. Toutes les fonctionnalités amenées par l'un seront accessibles par les licences de l'autre. L'installation de CAL RDS Windows Server 2008 R2 sur un Windows Server 2008 non R2 nécessite tout de même l'installation d'un hotfix (KB 968074). Les licences d'accès clients incluent l'utilisation de APP-V dans le cadre des publications d'applications sur RDS. Vous trouverez plus de détails à l'adresse : http://www.microsoft.com/systemcenter/appv/terminalsvcs.mspx

La technologie APP-V est issue du rachat de Softgrid par Microsoft. Elle permet de virtualiser les applications, ce qui permet de les isoler entres elles et de les consommer sous la forme de stream.

Les licences RDS sont proposées sous deux types :

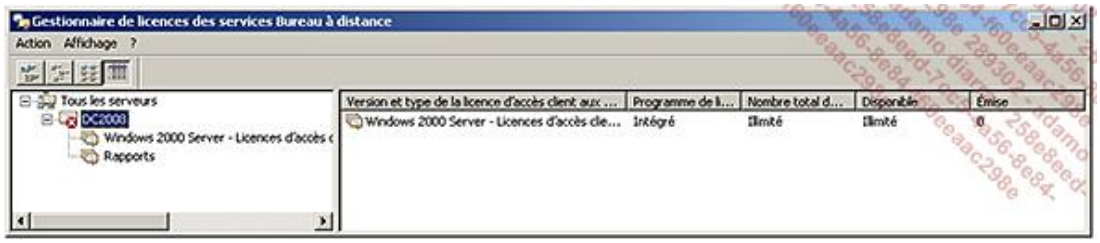
- par périphérique, quel que soit le nombre d'utilisateurs utilisant ce périphérique pour accéder à des ressources RDS ;

- par utilisateur, quel que soit le périphérique utilisé pour accéder à des ressources RDS.

Il est recommandé d'installer ce service de rôle sur un contrôleur de domaine, car tous les serveurs RDS du domaine trouveront automatiquement le serveur de licence.

Pour configurer le service de licences, lancez la console de gestion :

- Ouvrez la console **Gestionnaire de licences des services Bureau à distance** en cliquant sur le bouton **Démarrer - Outils d'administration**, puis **Services Bureau à distance** et **Gestionnaire de licences des services Bureau à distance**.



La première étape va consister à activer le serveur auprès de Microsoft. Trois méthodes sont possibles :

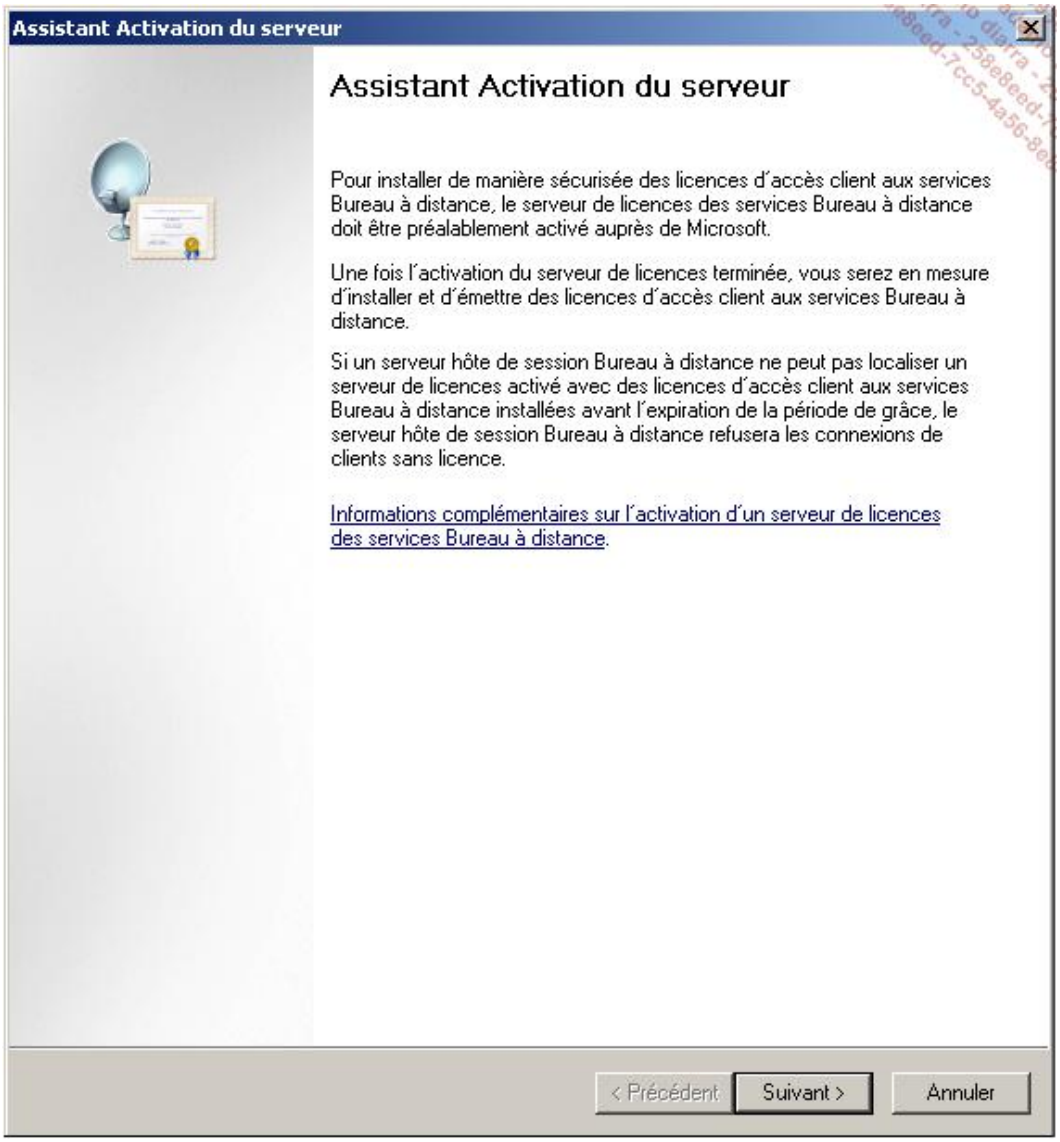
- **Connexion automatique**. Le serveur doit pouvoir établir une connexion au serveur Microsoft via le protocole HTTPS.

© ENI Editions - All rights reserved - adamo diarra

- **Navigateur Web**. Utilisez un autre ordinateur qui lui a accès à Internet pour effecuter la procédure d'activation.

- **Par téléphone**. Vous allez échanger des numéros de série avec Microsoft par téléphone.

- Pour cela, faites un clic avec le bouton droit sur le nom du serveur et cliquez sur **Activer le serveur**. Une fois l'activation effectuée, vous obtenez cet écran :



Cela ne constitue que la première étape, enregistrer votre serveur auprès de Microsoft. Maintenant il est possible d'ajouter des licences TS, en choisissant le programme de licences. Une fois que vous aurez fourni les numéros nécessaires, les licences TS seront affichées dans le **Gestionnaire de licences**.

- Ce service de rôle consomme très peu de ressources, mais doit être mis sur un serveur stable. Les licences ne pourront pas être transférées sur un autre serveur facilement, et l'absence de ce rôle passe l'ensemble des serveurs TS en période de grâce de 120 jours.

- Par défaut, une base de données des licences est créée sur le serveur dans ce répertoire : %systemroot% \system32\lserver.

- Lors de l'installation, le service de licence a créé un groupe, *Terminal Server Computers*. Ce groupe est local, sauf s'il est installé sur un contrôleur de domaine, auquel cas il devient un groupe Active Directory. Si la GPO *Configuration ordinateur\Modèles d'administration\Composants Windows\Services Bureau à distance\Gestionnaire de licences des services Bureau à distance\Groupe de sécurité du serveur de licences* est activée, seuls les ordinateurs membres du groupe pourront interroger le service de licence.

© ENI Editions - All rights reserved - adamo diarra

- Le gestionnaire de Licences permet de suivre la consommation des licences en mode utilisateur, et de générer des rapports. Pour utiliser cette fonctionnalité, l'objet ordinateur du serveur doit être membre du groupe AD **Serveurs de licences des services Terminal Server**. Si le serveur est aussi un contrôleur de domaine, le compte Service Réseau doit aussi être membre de ce groupe.

- S'il n'est pas installé sur un contrôleur de domaine, vous pouvez spécifier manuellement le nom du serveur de licences TS sur les serveurs TS via la base de registre. Il faut créer la clé DefaultLicenseServer de type REG_SZ avec le nom du serveur dans :

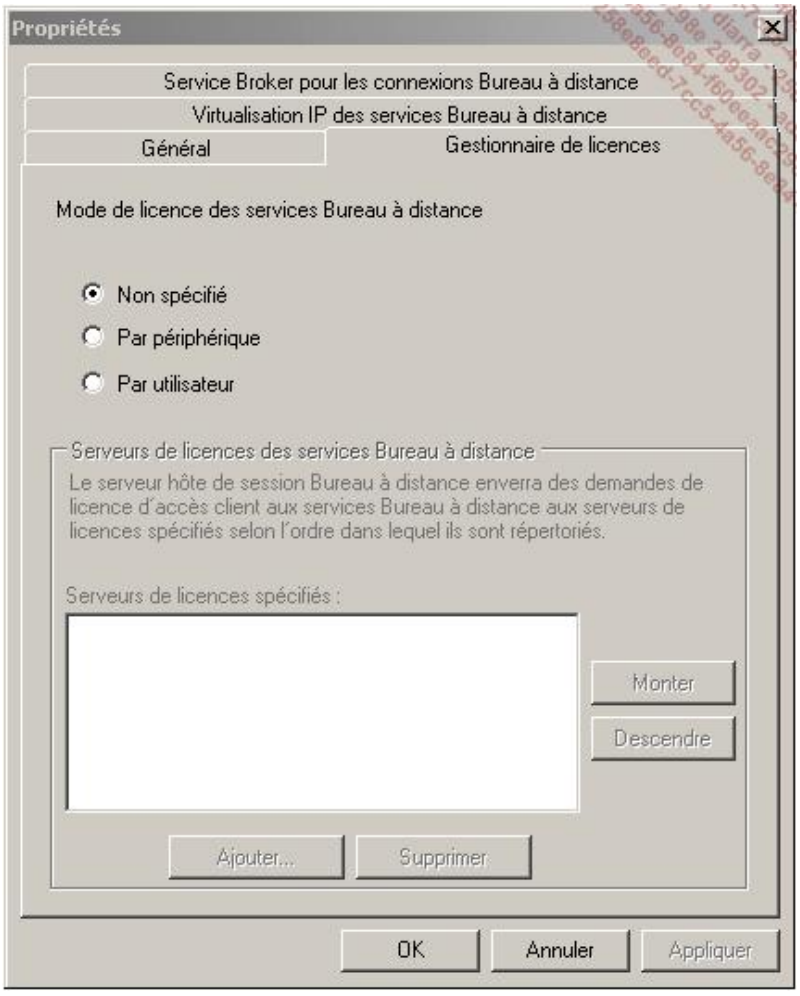
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters.

- Sur les serveurs RDS, vous devez choisir le mode de licence à appliquer (par périphérique ou par utilisateur). Vous pouvez le faire de façon graphique et individuelle ou par GPO.

  Pour spécifier le mode de licence et le nom du serveur de licence de façon graphique :

  - Ouvrez la console **Configuration d'hôte de session Bureau à distance** en cliquant sur le bouton **Démarrer - Outils d'administration**, puis **Services Bureau à distance** et enfin **Configuration des services Terminal Server**.

  - Dans le panneau **Configuration d'hôte de session Bureau à distance**, double cliquez sur **Mode de licence des services Bureau à distance**.



Si le service de rôle de gestion des licences TS n'est pas sur un contrôleur de domaine, vous avez la possibilité d'indiquer le ou les noms des serveurs de licences TS.

Pour appliquer le paramétrage via GPO, il faut aller dans : **Configuration ordinateur - Modèles d'administration - Composants Windows - Service Bureau à distance - Hôte de la session Bureau à**

© ENI Editions - All rights reserved - adamo diarra

distance - Gestionnaire de licences :

- Utiliser les serveurs de licences des services Terminal Server indiqués.
- Définir le mode de concession de licences des services Terminal Server.

Vous avez maintenant un serveur de licences TS configuré et fonctionnel.

g. Installer un logiciel sur un serveur RDS

Lorsque vous installez un logiciel sur un serveur RDS, vous devez lui indiquer qu'une installation va avoir lieu. Pour ce faire, vous pouvez utiliser la commande :

```
change user /install
```

Une fois l'installation terminée, vous pouvez revenir en mode standard :

```
change user /execute
```

Si l'installeur utilise la technologie MSI, cette commande n'est pas nécessaire, vous pouvez l'exécuter directement.

Windows Server 2008 R2 existe uniquement en 64 bits. Wow64 permet de faire fonctionner les applications 32 bits par émulation. Cela rajoute toutefois une charge complémentaire et ne permet pas de tirer le meilleur de la plate-forme. Vérifiez systématiquement si une version 64 bits existe avant d'installer le composant ou l'application en question.

© ENI Editions - All rights reserved - adamo diarra

Configurations avancées

1. Configuration du Session Broker

Ce service de rôle permet de gérer l'ensemble des sessions utilisateurs sur plusieurs serveurs RDS. Cela améliore également l'expérience utilisateur, en agrégeant les publications RemoteApp, bureau à distance et bureaux virtuels dans une vue unique. Pour ce faire, il stocke l'état de toutes les sessions de tous les serveurs, informations envoyées par les serveurs RDS. Quand un utilisateur se connecte pour la première fois sur un serveur, le Session Broker mémorise cette connexion. Si l'utilisateur perd sa connexion réseau, sa session TS reste active sur le serveur, mais en état déconnecté. Quand il disposera à nouveau d'une connexion réseau et qu'il se connectera, le Session Broker détectera qu'il y a déjà une session existante et l'enverra sur le serveur RDS concerné. Ainsi il retrouvera sa précédente session au lieu d'en créer potentiellement une nouvelle.

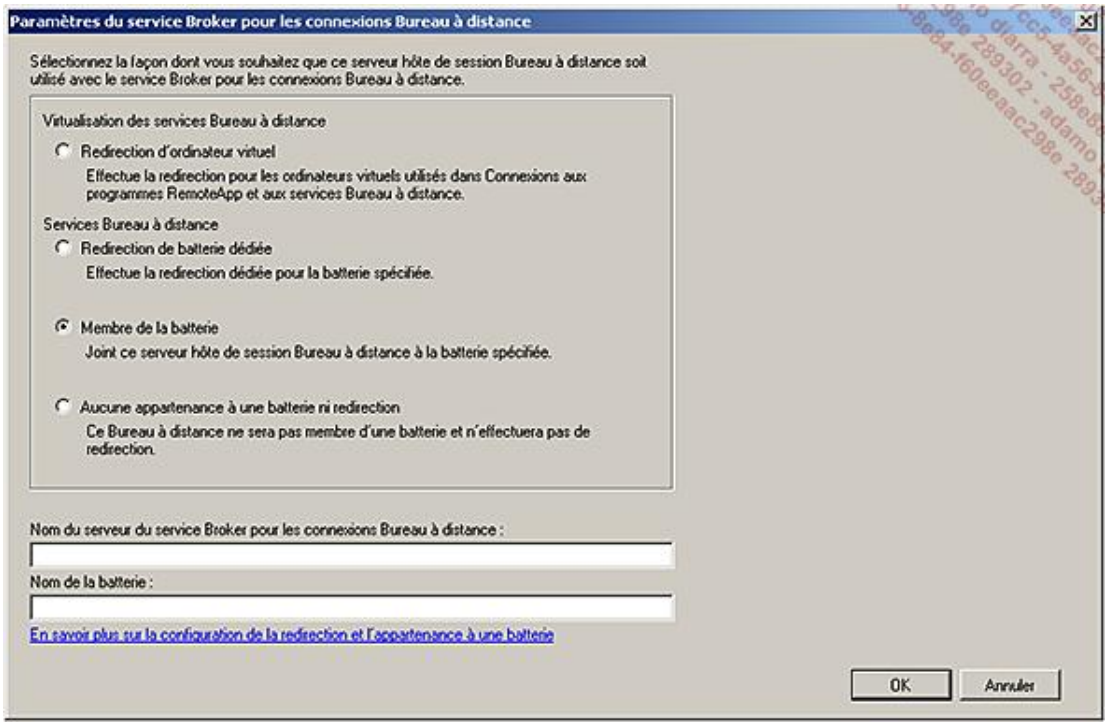
L'activation du Session Broker peut être réalisée via cinq GPO, qui se trouvent sous : **Configuration ordinateur - Modèles d'administration - Composants Windows - Service Bureau à distance - Hôte de la session Bureau à distance - Service Broker pour les connexions Bureau à distance**.

- **Joindre le service Broker pour les connexions Bureau à distance** : doit être activé pour former une ferme de serveurs RDS.
- **Configurez le nom de la batterie de serveurs du service Broker pour les connexions Bureau à distance** : doit contenir un nom unique par ferme de serveurs à créer.
- **Utiliser la redirection d'adresse IP** : si activée, tout utilisateur ayant déjà une session ouverte sera redirigé sur l'adresse IP du serveur qui possède la session. Le client doit donc pouvoir joindre directement l'adresse IP de chaque serveur RDS. Si désactivée, un jeton est fourni au client, qui permet au système d'équilibrage de charge de l'aiguiller sur le bon serveur RDS tout en se connectant sur l'adresse IP virtuelle.
- **Configurer le nom du serveur du service Broker pour les connexions Bureau à distance** : tous les serveurs RDS d'une même ferme doivent utiliser le même Session Broker. Il est possible d'indiquer soit le nom netbios, l'adresse IP ou le nom complet (FQDN).
- **Utiliser l'équilibrage de charge du service Broker pour les connexions Bureau à distance** : si activée, redirige les nouveaux utilisateurs sur le serveur RDS le moins chargé. Si désactivée, le premier serveur contacté sera utilisé.

La redirection d'adresses IP est obligatoire avec les technologies suivantes de répartition de charges : NLB, à résolution de noms d'hôtes tourniquet (round robin), et tout répartiteur de charge ne prenant pas en charge le jeton de routage Service Broker. L'activation peut aussi se faire depuis l'interface graphique.

- Ouvrez la console **Configuration d'hôte de session Bureau à distance** en cliquant sur le bouton **Démarrer - Outils d'administration**, puis **Services Bureau à distance** et enfin **Configuration d'hôte de session Bureau à distance**.
- Dans le panneau **Configuration d'hôte de session Bureau à distance**, double cliquez sur **Membre d'une batterie dans le service Session Broker**.

© ENI Editions - All rights reserved - adamo diarra



Le session broker est désormais configuré.

2. Gestion des impressions

La gestion des impressions, et en particulier des pilotes d'imprimantes, a toujours été un sujet important en environnement Terminal Services. Windows Server 2008 R2 introduit la fonctionnalité ***Easyprint*** pour pallier les différents problèmes. Elle est implémentée dans tsprint.dll, en 32 et 64 bits, tant du côté client que du côté serveur. Les pré-requis côté client sont les suivants :

- le client RDC 6.1 (presque tous les rôles de service TS en dépendent) ;
- le Framework .NET 3.0 Service Pack 1.

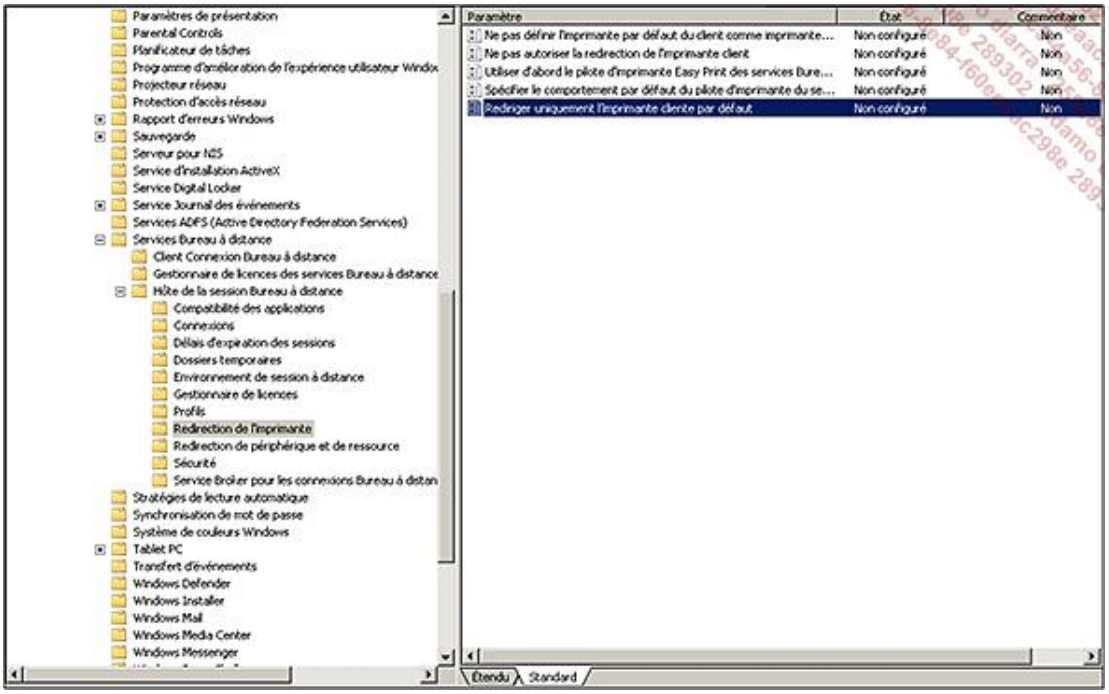
Il est à noter que si le client ne répond pas à ces pré-requis, il faudra installer les pilotes d'imprimantes sur le serveur.

Easyprint permet d'afficher depuis le serveur RDS l'ensemble des propriétés de l'imprimante sans avoir à installer le pilote sur le serveur. Pour cela, il se comporte comme un proxy et redirige tous les appels d'interfaces sur le pilote côté client. Il va convertir l'impression du format GDI au format XPS (si le format n'est pas déjà XPS) sur le serveur, et l'envoyer au client dans la session RDP, via un canal virtuel (XPS over RDP). Une fois sur le poste client, si le pilote d'imprimante est compatible XPS, le document est imprimé directement, sinon il est converti de nouveau du format XPS au format GDI et imprimé.

Il est maintenant possible de restreindre le nombre d'imprimantes à contacter depuis le poste client via GPO. L'ouverture de session est accélérée, et l'imprimante par défaut du poste client suffit la plupart du temps.

Pour appliquer cette restriction par GPO, il faut activer le paramètre : **Configuration ordinateur - Modèles d'administration - Composants Windows - Service Bureau à distance - Hôte de la session Bureau à distance - Redirection de l'imprimante**.

© ENI Editions - All rights reserved - adamo diarra



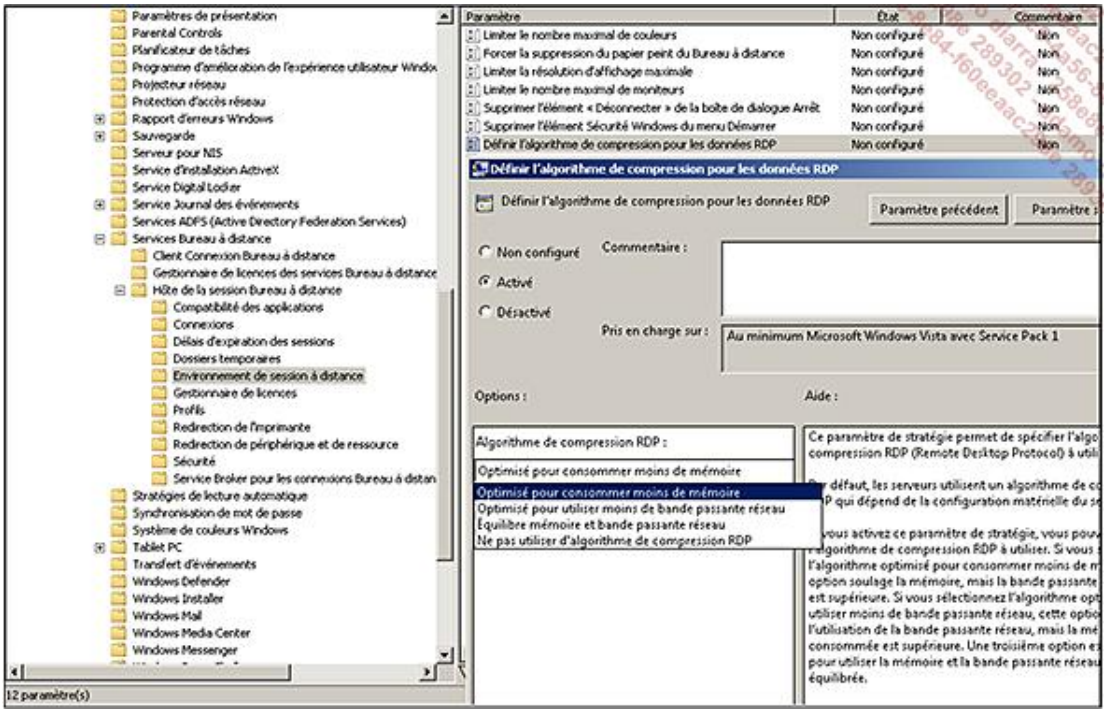
3. Optimiser la bande passante

Des modifications peuvent être apportées afin d'optimiser la consommation réseau générée par les clients :

- Configurer Terminal Services pour utiliser un algorithme de compression plus efficace.
- Configurer l'affichage pour utiliser le mode 32 bit, qui consomme moins que le mode 16 bit (le mode 24 bit n'existe plus).
- Désactiver l'utilisation de Clear Type (attention à l'aspect).
- Activer et augmenter le cache RDP persistant sur le client.

Vous pouvez choisir un algorithme plus économique en bande passante et le positionner par stratégie de groupe :

© ENI Editions - All rights reserved - adamo diarra



Les tailles des caches standard et persistant peuvent être configurées en base de registre globalement ou à l'intérieur d'un fichier RDP. Les valeurs sont à positionner sous cette clé : **HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client**

- BitmapCacheSize : a une valeur de 1500 par défaut, avec un maximum de 32000. L'unité de valeur est le Ko. Ce cache est situé en mémoire vive.
- BitmapPersistCacheSize : a une valeur de 10 par défaut. L'unité de valeur est le Ko. Ce cache est situé sur le disque dur.

4. Maintenances

Contrairement à un serveurs Web par exemple, passer un serveur Terminal Services en maintenance est plus compliqué vis-à-vis des utilisateurs. Ils peuvent avoir des documents ouverts non sauvegardés, des mails en cours, etc. Heureusement, des outils adaptés sont disponibles, afin de couper le service dans les règles de l'art.

Pour commencer, vous pouvez autoriser ou non les ouvertures de sessions utilisateurs avec la commande `change logon`. Cette commande accepte plusieurs arguments :

- **/QUERY** : affiche le mode d'ouverture de session actuelle.
- **/ENABLE** : autorise les ouvertures de sessions utilisateurs.
- **/DISABLE** : interdit les ouvertures de sessions utilisateurs.
- **/DRAIN** : interdit les nouvelles ouvertures de sessions utilisateurs, mais autorise les reconnexions aux sessions existantes.
- **/DRAINUNTILRESTART** : interdit les nouvelles ouvertures de sessions utilisateurs jusqu'a ce que le serveur ait redémarré, mais autorise les reconnexions aux sessions existantes.

Pour fermer toutes les sessions à la fois, vous pouvez utiliser le script suivant :

```
for /f "skip=2 tokens=2," %i in ('query session') do logoff %i
```

La commande `query session` permet de lister toutes les sessions utilisateurs du serveur.

Une fois la liste des sessions affichée, notez le numéro de session pour lequel vous souhaitez réaliser une action.

© ENI Editions - All rights reserved - adamo diarra

Vous pouvez ensuite :

- Fermer la session : `logoff XXX`
- Déconnecter l'utilisateur : `tsdicon XXX`
- Supprimer de force une session : `session reset XXX`
- Vous connecter à cette session : `tsconn XXX`
- Envoyer un message à l'utilisateur : `msg XXX « Veuillez fermer votre session »`

© ENI Editions - All rights reserved - adamo diarra

Améliorations avec Windows Server 2008 R2

1. Remote Desktop Client 7.0

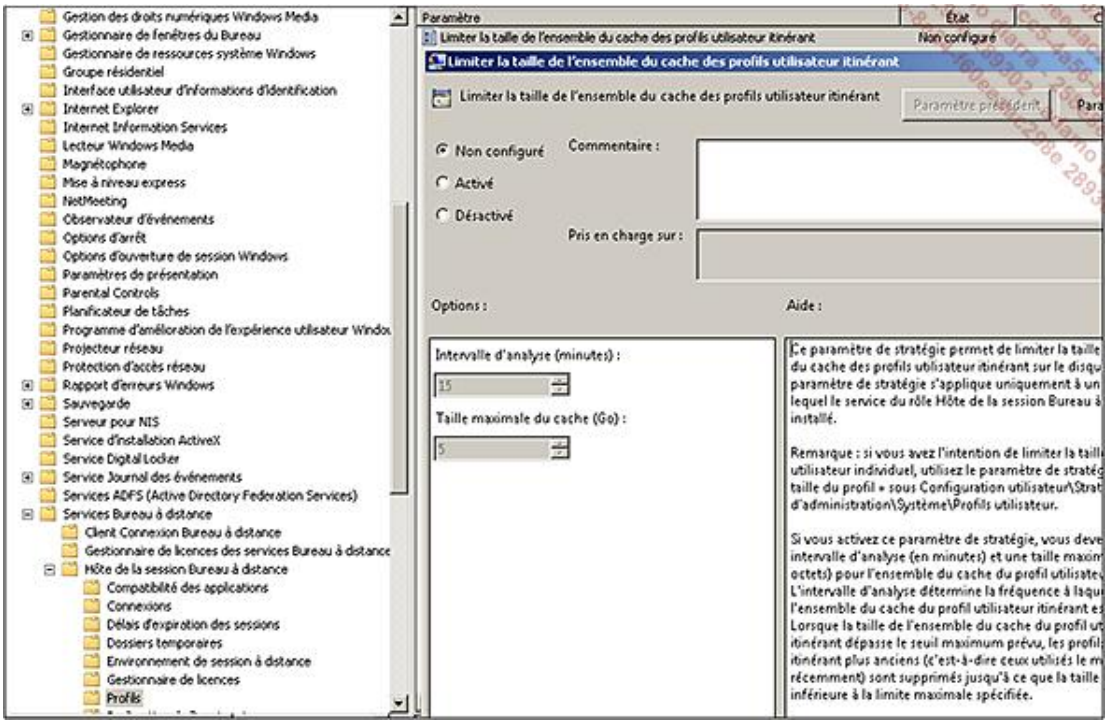
Windows 7 et Windows Server 2008 R2 sont les premiers systèmes d'exploitation livrés avec le Remote Desktop Client (RDC) en version 7.0. L'objectif est d'améliorer l'expérience utilisateur en fournissant :

- Un véritable support multi-écran (au lieu de l'extension habituelle).
- La redirection de flux Media player (flux décodé sur le poste client). Cela est possible à la fois pour des flux vidéos classiques mais aussi ceux incorporés dans une page Web.
- La gestion de l'état des connexions Bureau à distance depuis la barre des tâches.
- La souscription à la liste des applications publiées. Elles sont alors automatiquement listées dans le menu **Démarrer**. La liste est gérée automatiquement (ajouts et suppressions).
- La transmission bidirectionnelle du son (enregistrement depuis le client envoyé au serveur).
- Le support de Aero Glass.
- L'accélération bitmap améliorée pour les applications graphiques intensives (PowerPoint...).
- La barre de langues intégrée. Cela permet de gérer la langue des applications publiées par RemoteApp directement.
- Web SSO : l'utilisateur s'authentifie une seule fois pour accéder à toutes les applications publiées dans RemoteApp.
- La gestion et la vérification des clients accédant aux ressources publiées.

2. Gérer les profils itinérants

Un nouveau mécanisme de cache pour les profils utilisateurs évite de supprimer les profils itinérants à la fermeture de session. Un quota est alloué et seuls les profils les plus anciens seront automatiquement purgés une fois le quota atteint. Le paramétrage se fait via GPO : **Configuration ordinateur - Modèles d'administration - Composants Windows - Service Bureau à distance - Hôte de la session Bureau à distance - Profils - Limiter la taille de l'ensemble du cache des profils utilisateur itinérant**.

© ENI Editions - All rights reserved - adamo diarra



3. Intégration VDI/Hyper-V

Le Bureau à distance et VDI (*Virtual Desktop Infrastructure*) deviennent une solution intégrée. Hyper-V supporte les bureaux virtuels, notamment à travers un broker unique et éventuellement SCVMM (le gestionnaire de machines Virtuelles). L'objectif est d'être complémentaire à un serveur de Bureau à distance classique. Il s'agit de fournir un bureau à distance sur un Windows Client (Windows 7 par exemple) à un utilisateur. Cette assignation peut être temporaire (pool de VM) ou permanente (bureau personnel). Cette souplesse permet de couvrir des besoins plus spécifiques :

- Certaines applications ne fonctionnent ou ne sont supportées que sur un OS client, ou le modèle de licence est plus avantageux avec des OS de type client.
- Certains utilisateurs doivent avoir le privilège « administrateur » sur la machine (développeur à distance...). De cette façon, ils ne sont pas administrateurs sur tout un serveur RDS.
- Dans le cas de recettes d'applications, dès que la recette est finalisée, la VM revient automatiquement à son état initial (disque de rollback).

Ce type d'architecture est orienté multiserveur :

- Un serveur joue le rôle de broker afin de dispatcher les connexions des utilisateurs (RDS-Connection-Broker).
- Un ou plusieurs serveurs Hyper-V hébergent des machines virtuelles. Ces machines doivent être strictement identiques (mêmes programmes installés).

Comme souvent, une solution amène également des contraintes :

- Si les données des utilisateurs doivent être persistantes, elles doivent être stockées dans le profil utilisateur (itinérant) ou en dehors de la VM. Si une application stocke des informations dans un chemin local, les données seront perdues. Ce type de problème peut être contourné de plusieurs façons. Le chapitre consacré au Déploiement explique l'intérêt des shims (qui représentent une solution adaptée si le nombre d'applications à traiter est faible). Une méthode plus industrielle est d'utiliser Microsoft APP-V.
- Sur un parc significatif, SCVMM s'impose rapidement en tant que complément indispensable.
    - Ce type d'environnement « à la demande » peut être surchargé si des VM persistent alors qu'elles ne sont plus utiles. La bibliothèque de SCVMM permet de piloter facilement les VM instanciées.

© ENI Editions - All rights reserved - adamo diarra

- La création de VM est basée sur une VM « modèle ».

- Les serveurs Hyper-V participant au pool de VM doivent avoir le service **Hôte de virtualisation des services Bureau à distance** (RDS-Virtualization) installé. Ce service n'est pas disponible sur l'édition Core. Il faut utiliser l'édition complète, qui est soumise à un nombre de patches plus important et donc prévoir une gestion d'indisponibilité.

Décrire l'installation étape par étape nécessiterait un chapitre à part entière, mais la difficulté ne réside pas dans cette phase. L'enjeu va être de préparer une image d'un poste de travail aussi complète que possible, afin de limiter au maximum les VM dites permanentes. APP-V est une offre intéressante, permettant de pallier beaucoup de problèmes, mais elle doit être considérée comme un projet à part entière, sous peine de s'enliser dans la gestion de l'ensemble. Vous devez faire un choix pertinent entre le Bureau à distance classique et le VDI, en adaptant la réponse en fonction des besoins avérés.

4. RemoteFX

Le Service Pack 1 de Windows Server 2008 R2 apporte une fonctionnalité de taille aux connexions bureau à distance, il s'agit de RemoteFX.

RemoteFX est une fonctionnalité qui permet d'améliorer de façon significative l'expérience utilisateur en permettant d'afficher un rendu 3D de bonne qualité au travers d'une connexion établie via une prise en main "Bureau à distance" depuis un poste avec un client RDP 7.1. De plus, la technologie apporte le support d'Aéro, des animations Flash ou Silverlight avec un très bon rendu (si le débit réseau est suffisamment correct, bien entendu). Avec l'arrivée du HTML5 et la multiplication des entreprises faisant le choix d'utiliser des clients légers pour se connecter à leur infrastructure, il ne fait pas de doute que RemoteFX a un bel avenir devant lui.

À noter que RemoteFX permet également d'élargir les possibilités de redirection des périphériques USB.

Deux architectures de connexion sont possibles afin de profiter de la technologie RemoteFX. Soit via une infrastructure virtualisée VDI sous Hyper-V, soit au travers d'une connexion à un serveur possédant le rôle Hôte de session sous Windows Server 2008 R2 SP1.

a. RemoteFX pour un hôte de virtualisation des services Bureau à distance

RemoteFX peut être utilisé au travers d'une infrastructure virtualisée hébergée sous Hyper-V au travers du rôle de virtualisation des services Bureau à distance.

Les postes clients virtuels accédés sur cette infrastructure profitent de l'accélération graphique de la carte physique du serveur Hyper-V, permettant ainsi de profiter des avantages de RemoteFX. La carte graphique est en effet virtualisée et est ainsi accessible à toutes les machines virtuelles hébergées.

Les pré-requis pour permettre la mise en place de cette infrastructures sont nombreux :

- Le processeur doit être compatible SLAT (*Second Level Address Translation*). Cette fonctionnalité est appelée EPT (*Extended Page Tables*) sur les processeurs Intel et NPT (*Nested Page Tables*) sur les processeurs AMD. Les processeurs Intel Nehalem comme les Xeon X5540, Xeon E5530, Intel i5 ou Intel i7 et les processeurs AMD Opteron 2356 font partie des modèles compatibles.

- Une carte graphique (GPU) est nécessaire sur le serveur hébergeant RemoteFX. Le driver doit supporter DirectX 9.0c et DirectX 10.0 et disposer d'au moins 1 Go de mémoire dédiée à la vidéo. Les modèles ATI FirePro v5800, v7800 et v8800 ou bien encore les cartes graphiques NVidia Quadro FX 3800, 4800, 5800 et Quadroplex S4 sont compatibles avec RemoteFX.

À noter que le nombre de machines virtuelles permettant de profiter de la fonctionnalité RemoteFX dépendra directement de la capacité mémoire de la carte graphique ; chaque machine virtuelle nécessitant environ 200 Mo de mémoire (suivant la résolution de l'écran et le nombre de moniteurs utilisés).

- La carte GPU installée sur le serveur ne doit posséder qu'un seul processeur graphique. Si une carte graphique est embarquée sur le serveur, il faudra la désactiver afin que la carte GPU soit la seule utilisée.

- La fonctionnalité Hyper-Threading doit être activée sur le serveur.

© ENI Editions - All rights reserved - adamo diarra

- La machine virtuelle accédée doit exécuter Windows 7 Entreprise ou Intégrale avec le Service Pack 1 installé. S'il s'agit d'une version x86, la quantité de mémoire allouée doit être de 1024 Mo minimum. Pour un système d'exploitation en version 64 bits, il faudra allouer 2048 Mo de mémoire au minimum.

- Les pré-requis matériels du rôle Hyper-V doivent être supportés sur le serveur comme nous l'avons vu plus haut.

- Le rôle "Hôte de virtualisation des services Bureau à distance" (ainsi que le rôle Hyper-V, bien sûr) doivent être installés sur le serveur hébergeant les machines virtuelles, sous Windows Server 2008 R2 SP1.

- Le client RDP utilisé pour accéder à la machine virtuelle doit être en version 7.1 (disponible pour l'instant sous Windows 7 SP1 et 2008 R2 SP1 uniquement) afin de gérer logiciellement la compression/décompression/encodage/décodage des flux audio et vidéo au niveau du protocole RDP 7.1. Ces actions peuvent autrement s'effectuer au travers d'un composant matériel dédié (ASIC) qui sera présent côté poste et serveur.

À noter que les cartes de supervision à distance (carte ILO, iDrac, IMM, KVM sur IP, etc .), qui servent habituellement à prendre la main sur un serveur pour y configurer son BIOS ou accéder à la console, peuvent poser des problèmes de compatibilité.

RemoteFX utilise en effet des pilotes WDDM lorsqu'une carte GPU est installée, tandis que les cartes de supervision utilisent pour la plupart le pilote XPDM. Ces deux pilotes ne pouvant fonctionner simultanément, si un utilisateur tente de se connecter au travers de la carte de supervision alors que le pilote RemoteFX est chargé, la console du serveur ne sera pas visible lors d'une prise en main à distance d'un système d'exploitation démarré.

La solution est alors de désactiver la carte de supervision depuis le BIOS ou d'utiliser le pilote "cap" de RemoteFX. Vous trouverez davantage d'information sur l'installation du pilote "cap" à cette adresse : http://technet.microsoft.com/fr-fr/library/gg607270(WS.10).aspx.

La mise en place de RemoteFX passe par ces principales étapes :

- Installation de RemoteFX sur le serveur Hyper-V (ouvrir le gestionnaire de serveur puis **Ajouter des rôles - Services Bureau à distance - RemoteFX**).

- Configuration de la prise en charge de RemoteFX dans la machine virtuelle (dans les paramètres de la machine virtuelle, ajoutez le matériel carte vidéo 3D RemoteFX) puis redémarrer la machine virtuelle.

- Utilisation du client RDP 7.1 (depuis un poste Windows 7 SP1 ou 2008 R2 SP1 donc, car le client n'est disponible que pour ces versions des systèmes d'exploitation pour l'instant). Le client RDP 7.1 doit être configuré pour utiliser une connexion d'accès à distance en "LAN" et avec couleurs 32 bits. Un évènement avec l'ID 2 est alors généré sur la machine virtuelle dans le journal Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Admin, confirmant ainsi que vous êtes bien connecté sur la machine en utilisant RemoteFX. Vous pourrez ainsi profiter des effets 3D, Aéro, etc. pour vous en convaincre.

Pour bénéficier d'une meilleure expérience utilisateur, vous pouvez également suivre cette étape facultative en configurant le paramètre **Définir l'indice de performance lors de l'utilisation de RemoteFX** avec un taux de capture d'écran ajusté à **Le plus élevé (qualité optimale)** au niveau de **Configuration ordinateur - Modèles d'administration - Composants Windows - Services Bureau à distance - Hôte de la session bureau à distance - Environnement de session à distance**. Après un redémarrage pour confirmer la bonne prise en compte sur l'ordinateur accédé (et à condition que la connexion réseau ait un bon débit), vous apprécierez encore un meilleur rendu des animations déportées.

Vous trouverez le guide pas-à-pas du déploiement de RemoteFX pour un hôte de virtualisation des services Bureau à distance à cette adresse : http://go.microsoft.com/fwlink/?LinkId=177903.

b. RemoteFX pour un hôte de session bureau à distance

Les pré-requis à l'installation de RemoteFX sur un serveur hébergeant le rôle d'hôte de session bureau à distance sont un peu moins nombreux que dans le cas d'une infrastructure VDI.

Il faudra en effet respecter les conditions suivantes :

- Le processeur doit supporter SSE2 (Streaming SIMD Extensions 2).

© ENI Editions - All rights reserved - adamo diarra

- Le rôle "Hôte de session bureau à distance" doit être installé sur un serveur sous Windows Server 2008 R2 SP1.

- Le client RDP utilisé pour accéder à la machine virtuelle doit être en version 7.1 (disponible pour l'instant sous Windows 7 SP1 et 2008 R2 SP1 uniquement) afin de gérer logiciellement la compression/décompression/encodage/décodage des flux audio et vidéo au niveau du protocole RDP 7.1. Ces actions peuvent autrement s'effectuer au travers d'un composant matériel dédié (ASIC) qui sera présent côté poste et serveur.

La mise en place de RemoteFX passe par ces principales étapes :

- Installation du rôle "Hôte de session bureau à distance" sur votre serveur Windows Server 2008 R2 SP1.

- Configuration de la prise en charge de RemoteFX sur le serveur accédé. Il faut ainsi **limiter le nombre maximal de couleurs** à 32 bits par pixel, soit au niveau des propriétés de la connexion RDP, soit via une stratégie de groupe au niveau de **Configuration Ordinateur - Modèles d'administration - Composants Windows - Services bureau à distance - Hôte de la session Bureau à distance - Environnement de session à distance**. L'autre paramètre à activer se trouve à ce même endroit et se nomme **Configurer RemoteFX**.

- Utilisation du client RDP 7.1 (depuis un poste Windows 7 SP1 ou 2008 R2 SP1donc). Le client RDP 7.1 doit être configuré pour utiliser une connexion d'accès à distance en LAN et avec couleurs 32 bits. Un évènement avec l'ID 1000 est alors généré sur la machine virtuelle dans le journal Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Admin, confirmant ainsi que vous êtes bien connecté sur la machine en utilisant RemoteFX. Vous pourrez ainsi profiter des effets 3D, Aéro, etc. pour vous en convaincre.

Pour bénéficier d'une meilleure expérience utilisateur, vous pouvez également suivre cette étape facultative en configurant le paramètre **Définir l'indice de performance lors de l'utilisation de RemoteFX** avec un taux de capture d'écran ajusté à **Le plus élevé (qualité optimale)** au niveau de **Configuration ordinateur - Modèles d'administration - Composants Windows - Services Bureau à distance - Hôte de la session bureau à distance - Environnement de session à distance**. Après un redémarrage pour confirmer la bonne prise en compte sur l'ordinateur accédé (et à condition que la connexion réseau ait un bon débit), vous apprécierez encore un meilleur rendu des animations déportées.

Vous trouverez le guide pas-à-pas du déploiement de RemoteFX pour un hôte de session bureau à distance à cette adresse : http://go.microsoft.com/fwlink/?LinkId=192436.

c. RemoteFX utilisé pour la redirection USB

Si vous le souhaitez, vous pouvez également profiter de la redirection des périphériques USB afin de rediriger tout type de périphériques USB vers votre bureau à distance hébergé sur une machine virtuelle sous Windows 7 SP1. Les périphériques pris en charge sont alors nombreux (scanner, imprimante multifonctions, webcam, etc.) Si vous avez donc physiquement une webcam branchée à votre ordinateur client, vous pourrez déporter son utilisation sur la machine virtuelle distante accédée au travers du bureau à distance.

À noter que la redirection USB ne fonctionne pas si RemoteFX est hébergé sur un hôte de session bureau à distance. La redirection ne sera effective qu'à condition que RemoteFX soit installé sur un hôte de virtualisation des services Bureau à distance.

Vous pourrez utiliser cette fonctionnalité sur un ordinateur virtuel sous Windows 7 SP1 via une connexion de bureau à distance, via un accès Web TS, ou bien encore une RemoteApp.

Pour activer la redirection des ports USB, voici les principales étapes à suivre :

- Activer la fonctionnalité de redirection USB via RemoteFX au niveau de **Configuration ordinateur - Modèles d'administration - Composants Windows - Services Bureau à distance - Client Connexion Bureau à distance - Redirection de péripherique USB RemoteFX**. Le paramètre **Autoriser la redirection de protocole RDP des autres périphériques USB RemoteFX pris en charge à partir de cet ordinateur** doit être **Activé** avec des **Droits d'accès de la redirection USB RemoteFX** définis pour **Administrateurs et utilisateurs**. Redémarrez alors le poste en question.

- Configurer le client RDP 7.1 afin de rediriger le périphérique voulu. Le périphérique devra être branché avant que la connexion bureau à distance soit initiée. Au niveau de la connexion d'accès distant (mstsc.exe) dans les **Options - Ressources Locales - Autres**, cochez le périphérique USB à rediriger. À la connexion via le bureau à distance, le périphérique sera alors disponible sur l'ordinateur distant.

© ENI Editions - All rights reserved - adamo diarra

Vous trouverez le guide pas-à-pas pour la configuration de la redirection USB à cette adresse : http://go.microsoft.com/fwlink/?LinkId=192432.

Vous savez maintenant mettre en œuvre le rôle Bureau à distance avec l'ensemble de ses composants. Vous pouvez mettre en place différentes méthodes d'accès, adaptées à chaque contexte (depuis le réseau local, Internet, vers un serveur ou du VDL) sans réduire la sécurité du système d'information. Il serait dommage de priver ses utilisateurs, donc clients, d'une technologie aussi efficace et rapide.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre sera consacré aux moyens d'accéder aux services de votre société lorsque vous vous trouvez en dehors de celle-ci.

La première partie abordera les différents moyens permettant cet accès distant. Viendront ensuite les différents services offerts par Windows Server 2008 R2 pour répondre à un besoin de mobilité grandissant.

© ENI Editions - All rights reserved - adamo diarra

Principe de l'accès distant

De nos jours, les utilisateurs nomades sont de plus en plus exigeants et ont besoin d'avoir accès à toutes leurs données en tout temps (mails, fichiers, etc.) de la même façon que s'ils étaient dans les locaux de leur société. Pour pouvoir les satisfaire vous serez certainement amenés à configurer des solutions d'accès distant.

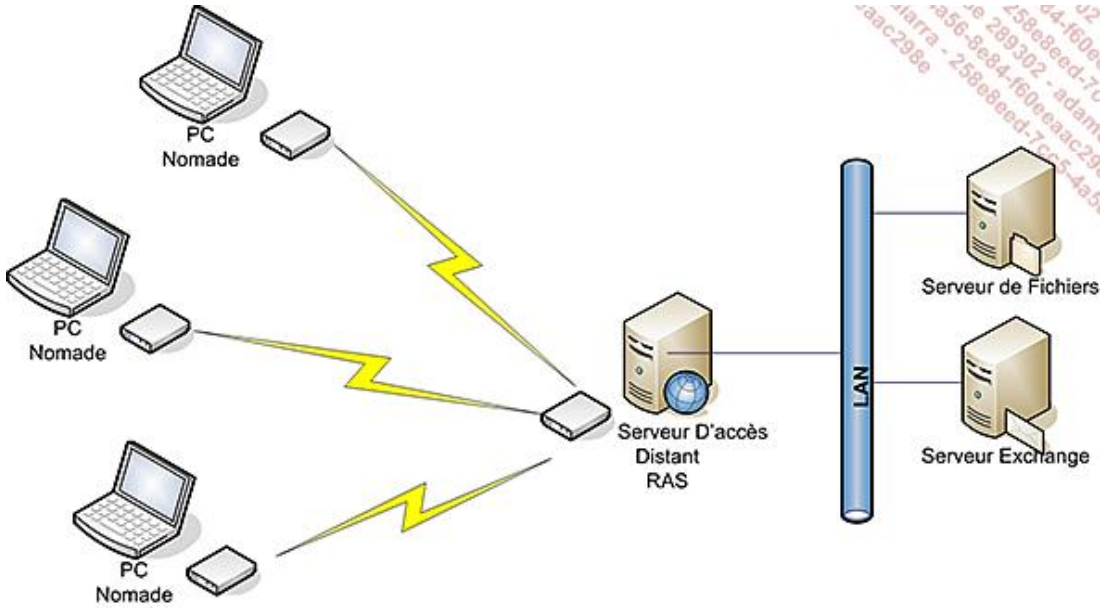
Cet accès distant peut se réaliser au travers de deux types de liaisons. Soit par une liaison de type **Numérotation à la demande** (fréquemment appelée Dial-up), soit par l'établissement d'un **réseau virtuel sécurisé** (VPN : *Virtual Private Network*).

1. Accès par téléphone

a. Généralités sur les connexions Dial-Up

Utiliser une connexion de type Dial-up permet d'accéder au réseau de l'entreprise au moyen d'une simple ligne téléphonique depuis n'importe quel endroit. Contrepartie de cette facilité d'accès, il s'agit d'une technologie déjà ancienne et qui n'offre que des performances très limitées du fait des bas débits proposés.

En pratique, il faut qu'à la fois le serveur et le PC de l'utilisateur soient munis d'un modem. L'utilisateur configure une connexion de numérotation à la demande dans laquelle un simple numéro de téléphone est spécifié. À l'initiation de la connexion, un nom d'utilisateur et un mot de passe sont requis. Le serveur gérant l'accès distant (appelé aussi RAS pour *Remote Access Server*) va être contacté tout simplement au travers de la ligne téléphonique auquel il est raccordé par le modem.



b. Avantages et inconvénients des connexions Dial-Up

Avantages

- Pas besoin d'abonnement Internet : une simple ligne téléphonique classique suffit.
- Confidentialité des données : les informations ne transitant pas au travers d'Internet, elles ne sont pas la cible de toutes les attaques que l'on trouve communément à travers le réseau de communication mondial. La sécurité est donc maximale car le réseau local n'a pas besoin d'être ouvert sur l'extérieur.

Inconvénients

- Faible bande passante. Basée sur la technologie téléphonique, les débits sont très limités. En effet, le réseau téléphonique a été conçu pour pouvoir reproduire les voix humaines et rien d'autre. Les fréquences pouvant transiter par ce biais devaient donc êtes peu élevées.

© ENI Editions - All rights reserved - adamo diarra

- Pour augmenter le débit que l'on trouve le plus couramment (56K), il existe des lignes Numeris (128K). Cependant celles-ci représentent un investissement bien plus important.

- Coût élevé. Les communications téléphoniques ont un coût non négligeable ; récupérer un simple fichier de 10 Mo devient un investissement en considérant le temps qu'il va falloir mettre pour le télécharger (environ une quarantaine de minutes à une vitesse moyenne de 4 ko/s).

- De plus, fournir des connexions distantes multiples nécessitera autant de lignes téléphoniques que d'utilisateurs nomades pouvant se connecter simultanément.

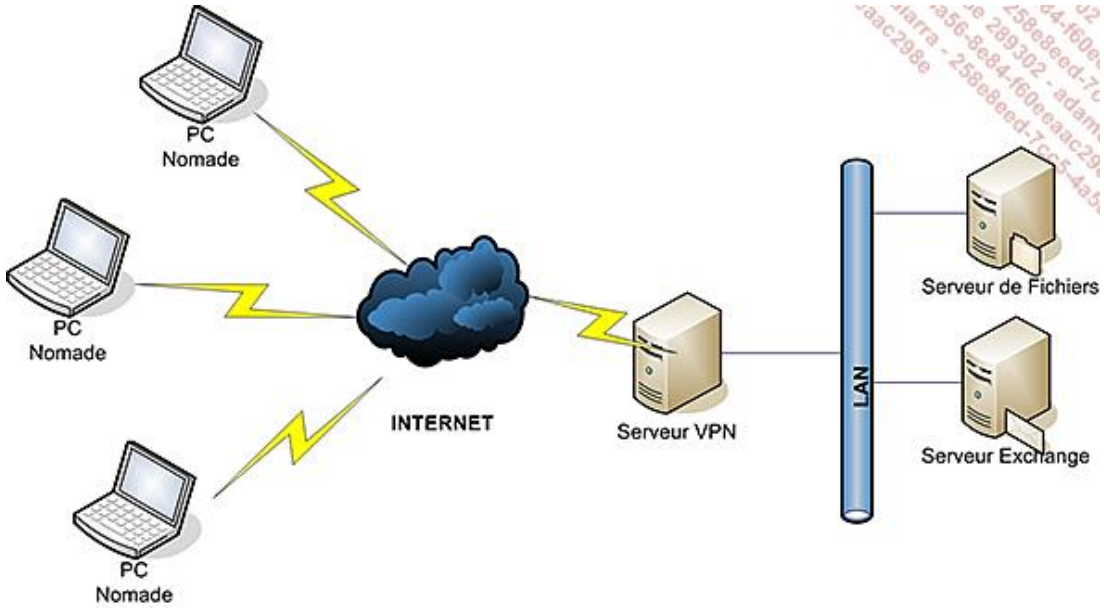
Bien que le coût très élevé de cette technologie soit un repoussoir notable, elle peut être utilisée dans certains cas très précis. S'il n'est pas rare d'avoir des problèmes de connexion à Internet, il est beaucoup plus rare d'avoir des pannes téléphoniques. Il peut être ainsi intéressant de bénéficier de ce type d'accès pour certaines sociétés dans un but d'administration. En effet, un administrateur pourra continuer à gérer des serveurs à distance et ce même s'ils sont injoignables au travers d'Internet.

---

2. Accès via Internet

a. Généralités sur les VPN

La seconde technologie permettant l'accès à distance utilise le réseau Internet et non plus le réseau téléphonique. Contrairement aux connexions à la demande qui vous connectent directement au réseau de la société, il est ici nécessaire de passer « au travers » du réseau Internet. La technologie employée est appelée VPN (*Virtual Private Network* ou Réseau Privé Virtuel en français). Ici la communication s'établit directement au niveau IP.

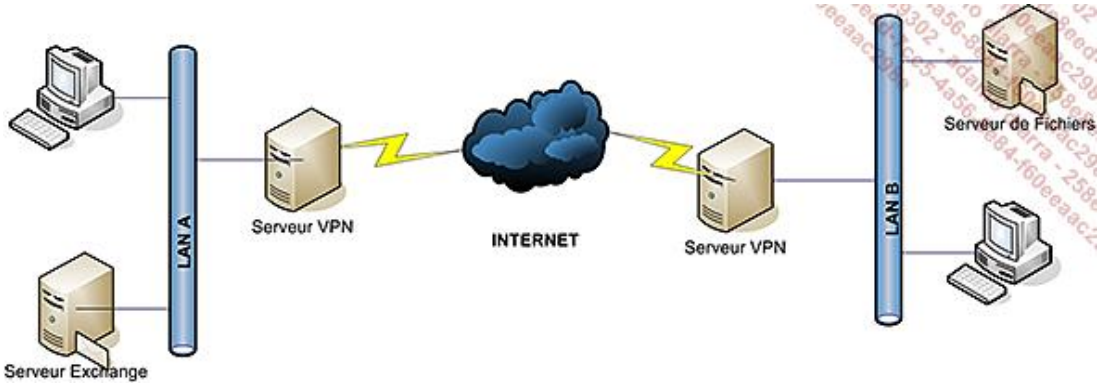


Quelques explications concernant la terminologie **Réseau Privé Virtuel** :

La connexion est virtuelle car quand l'ordinateur va établir la connexion VPN à travers Internet, il va agir comme s'il était directement connecté au réseau local, tout comme s'il avait un câble réseau qui y était relié. L'utilisateur va ainsi pouvoir accéder aux mêmes ressources que s'il était physiquement relié au réseau. Cette connexion reste cependant considérée comme virtuelle, justement parce qu'il n'y a pas de liaison Ethernet avec le réseau de destination. Elle est privée car une connexion point à point entre la source et la destination va être émulée. Les données échangées vont y être chiffrées. De cette façon, si ces données venaient à être interceptées, elles ne pourraient pas être déchiffrées sans la clé privée de la transaction.

Les VPN sont couramment utilisés pour relier des sites distants. On parle alors de VPN site à site. Le but de ce type de connexions est de pouvoir relier logiquement des réseaux distants sans pour autant avoir de liaison réseau directe (Ethernet, Wi-Fi, etc.).

© ENI Editions - All rights reserved - adamo diarra



b. Les différents types de VPN proposés sous Windows Server 2008 R2

Windows Server 2008 R2 comme ses prédécesseurs supporte les types de VPN suivants :

- PPTP (*Point Point Tunneling Protocol*) :

  PPTP est la méthode la plus simple à mettre en œuvre et à utiliser. Le chiffrement des données intervient après le processus d'authentification via le protocole PPP. Préférez une authentification utilisant RS-CHAPv2 à une authentification se basant sur du PAP (*Password Authentication Protocol*) ou CHAP (*Challenge Handshake Authentication Protocol*) afin de ne pas laisser le mot de passe transiter en clair.

- L2TP/IPSec (*Layer 2 Tunneling Protocol*) :

  Plus sécurisé que PPTP, L2TP/IPSec est issu d'un développement conjoint entre Microsoft et Cisco.

  À la différence de PPTP, le chiffrement inclut la phase d'identification puisque la session IPSec est établie juste avant.

  De plus, l'authentification mutuelle des machines (aussi appelée *handshake* ou poignée de main en français) empêche toute machine non reconnue de se connecter. Cela évite donc notamment les attaques de type Man-In-Middle dont souffrent les VPN reposant sur du PPTP.

  Attention cependant, il faut théoriquement éviter le NAT avec de l'IPSec car il modifie le contenu des paquets. Cette modification est incompatible avec les mécanismes de protection de l'intégrité des données IPSec. Si des impératifs vous obligent toutefois à utiliser du L2TP sur un réseau "natté", tournez-vous vers la norme NAT-T (*NAT Traversal*).

Windows Server 2008 R2 apporte aussi des nouveautés :

- SSTP (*Secure Socket Tunneling Protocol*) :

  SSTP est une nouvelle forme de tunnel VPN. Il facilite l'établissement d'une connexion VPN via un pare-feu ou via un périphérique effectuant de la traduction d'adresses réseaux (NAT).

  Cela est rendu possible par l'encapsulation de paquets PPP (*Protocole Point à Point*) dans de l'HTTPS. L'établissement des connexions VPN via un proxy HTTP est aussi rendu possible.

  Disponible avec Windows Server 2008/2008 R2 et Windows Vista SP1, SSTP utilise des connexions HTTP cryptées avec SSL pour établir des connexions vers les passerelles VPN.

  De la même façon qu'avec L2TP/IPSec, celui-ci ne transmet les informations d'identification qu'une fois la session SSL établie avec la passerelle VPN.

  Aussi appelé PPP/SSL, ce nouveau protocole permet l'utilisation de PPP et EAP pour l'authentification afin de rendre la connexion plus sécurisée encore.

Uniquement disponible avec le couple Windows Server 2008 R2/Windows 7, la technologie VPN Reconnect permet une reconnexion transparente de la liaison VPN. En cas de coupure Internet par exemple, le système va se charger de relancer la connexion VPN sans aucune intervention de l'utilisateur et en à peine quelques secondes.

© ENI Editions - All rights reserved - adamo diarra

c. Avantages et inconvénients du VPN

Avantages

- **Coûts réduits** : toutes les sociétés ainsi que les utilisateurs sont généralement déjà équipés d'une connexion Internet. Le coût de l'implémentation est donc minime puisqu'il suffit de rajouter un serveur pour jouer le rôle de serveur VPN. De plus, une seule connexion Internet peut servir à plusieurs connexions distantes simultanées sans devoir faire l'acquisition d'une ligne supplémentaire.

- **Débits élevés** : la technologie VPN s'appuie directement sur l'IP et donc également sur l'infrastructure Internet. Avec la banalisation de l'ADSL et l'explosion des débits associés, cette technologie est donc bien plus rapide que les connexions de type Dial-Up.

- **VPN Anywhere** : petite analogie avec la technologie employée sur Exchange (RPC over HTTPS) où l'on encapsule le trafic d'Outlook au travers du trafic Web sécurisé (HTTPS). Comme expliqué précédemment ici c'est du trafic VPN qui est encapsulé dans de l'HTTPS. La sécurité des réseaux étant souvent une priorité, il est très courant de bloquer tout trafic sortant ne correspondant pas aux besoins de l'entreprise. Il est par contre rare de voir le trafic HTTPS sortant bloqué. De cette façon, grâce au SSTP, l'utilisateur doit pouvoir se connecter depuis n'importe quel réseau d'entreprise ou point d'accès Internet.

Inconvénients

- **Dépendant du réseau** : a contrario des connexions à la demande, les performances de l'abonnement Internet de l'une ou l'autre des deux parties (société ou nomade) ont un impact non négligeable sur la qualité des transmissions. Tout problème chez le fournisseur d'accès de l'un ou de l'autre peut provoquer une incapacité totale à communiquer.

- **Confidentialité des données** : bien qu'utilisant des systèmes de chiffrement il n'en reste pas moins que les données transitent au travers d'Internet. Elles sont du coup potentiellement visibles de tous et ce bien qu'elles soient chiffrées.

d. Direct Access, le "VPN-Killer"

Spécificité de Windows Server 2008 R2, la technologie Direct Access est surnommée le « VPN-Killer » par de nombreux professionnels de l'informatique. Ce surnom provient du fait qu'a contrario des VPN habituels (PPTP, L2TP, etc.), Direct Access permet l'établissement d'une connexion au réseau de l'entreprise avant même d'avoir ouvert une session sur la machine cliente.

L'objectif visé côté client est d'améliorer le ressenti de l'utilisateur nomade en lui fournissant des conditions de travail totalement identiques à celles qu'il a au sein de la structure de l'entreprise.

Les administrateurs systèmes tireront également partie de cette technologie. Ils pourront désormais gérer intégralement les ordinateurs situés en dehors de l'entreprise : déploiement de mises à jour logicielles, mise en conformité de l'antivirus, applications de stratégies de groupe, etc.

Par défaut, et contrairement aux technologies VPN habituelles, seul le trafic à destination de l'entreprise passera au travers de Direct Access, de façon à ne pas ralentir le trafic Internet. Il reste néanmoins possible de faire transiter la totalité du trafic par Direct Access en vue de maîtriser de bout en bout la sécurité des accès.

Direct Access repose sur l'utilisation d'IPSec et d'IPv6 et au besoin du protocole IP-HTTPS.

Sa capacité à gérer la haute disponibilité a été améliorée avec l'arrivée du Service Pack 1 de Windows Server 2008 R2 puisqu'il ajoute le support de l'adressage 6to4 et ISATAP lors de l'utilisation de DirectAccess via un cluster NLB (*Network Load Balancing*).

Voici les étapes du processus de connexion au réseau de l'entreprise grâce à Direct Access :

- Le client détecte s'il est connecté à un réseau.

- Il tente d'établir une session sur un site Intranet SSL afin de déterminer s'il se trouve au sein du réseau d'entreprise ou à l'extérieur.

- Le client se connecte au serveur Direct Access au moyen d'IPSec et IPv6. Si une connexion native en IPv6

© ENI Editions - All rights reserved - adamo diarra

n’est pas disponible (c’est généralement le cas si la machine cliente est connectée à Internet), le client va établir un tunnel IPv6 sur IPv4 au moyen de 6To4 ou de Teredo (pour plus d’informations sur Teredo rendez-vous à la page : http://technet.microsoft.com/en-us/network/cc917486.aspx).

- Si le client ne parvient pas à établir la connexion à cause d’un pare-feu ou d’un proxy, il essaiera automatiquement de se connecter grâce au protocole HTTPS.

- La machine cliente et le serveur Direct Access vont s’authentifier mutuellement grâce aux certificats d’ordinateurs. Ce processus fait partie intégrante des mécanismes IPSec.

- Le serveur Direct Access va vérifier dans ses règles si la machine cliente est autorisée (ou fait partie d’un groupe autorisé) à établir une connexion Direct Access.

- Le serveur Direct Access va faire suivre le trafic de la machine cliente vers les serveurs Intranet sur lesquels l’accès de l’utilisateur est autorisé.

© ENI Editions - All rights reserved - adamo diarra

Mettre en place un accès sécurisé à travers Internet

Dans cette partie vous verrez comment configurer votre serveur en tant que serveur d'accès distant. Dans un premier temps, les méthodes pour configurer les différents types de VPN offerts par Windows Server 2008 R2 (PPTP, L2TP, SSTP) seront décrites. Puis les aspects concernant la sécurisation seront abordés. La configuration d'un serveur RAS avec modem ne sera pas évoquée, la technologie n'étant quasiment plus utilisée.

1. Mise en place d'une liaison VPN

Pré-requis matériel : le serveur doit être muni de deux cartes réseaux. L'une connectée à Internet et l'autre connectée au réseau local (LAN). La première se charge d'accepter les connexions VPN entrantes et nécessite une IP fixe (dans notre exemple configurée en 192.168.250.123). La seconde interface réseau fait suivre le trafic entre les connexions VPN et les ressources réseaux du LAN.

Il est techniquement possible dans le cas d'un VPN PPTP ou L2TP de n'avoir qu'une seule carte réseau. Cela sort par contre du cadre des bonnes pratiques préconisées par Microsoft et les performances peuvent s'en ressentir.

Pré-requis logiciel : pour configurer les VPN **L2TP/IPSec** et **SSTP** vous devez avoir installé un certificat d'ordinateur sur le serveur.

Un certificat auto-signé peut néanmoins être généré à la fin de la procédure d'installation du service. Attention cependant, ces certificats ne sont pas reconnus par des autorités publiques et vont générer des alertes de sécurité. Ils ne doivent être utilisés qu'à des fins de tests.

Il faut donc leur préférer une autorité de certificat interne (appelé aussi PKI pour *Public Key Infrastructure*) ou mieux encore un certificat signé par une autorité publique. L'avantage d'un certificat signé par une autorité publique est que ce certificat ne nécessite pas le déploiement du certificat de l'autorité de certificats sur les postes clients contrairement à l'utilisation d'un certificat généré par une PKI.

Ci-après un lien vers le TechNet de Microsoft traitant de la mise en place d'une PKI Microsoft : http://technet.microsoft.com/en-us/library/cc872789.aspx

---

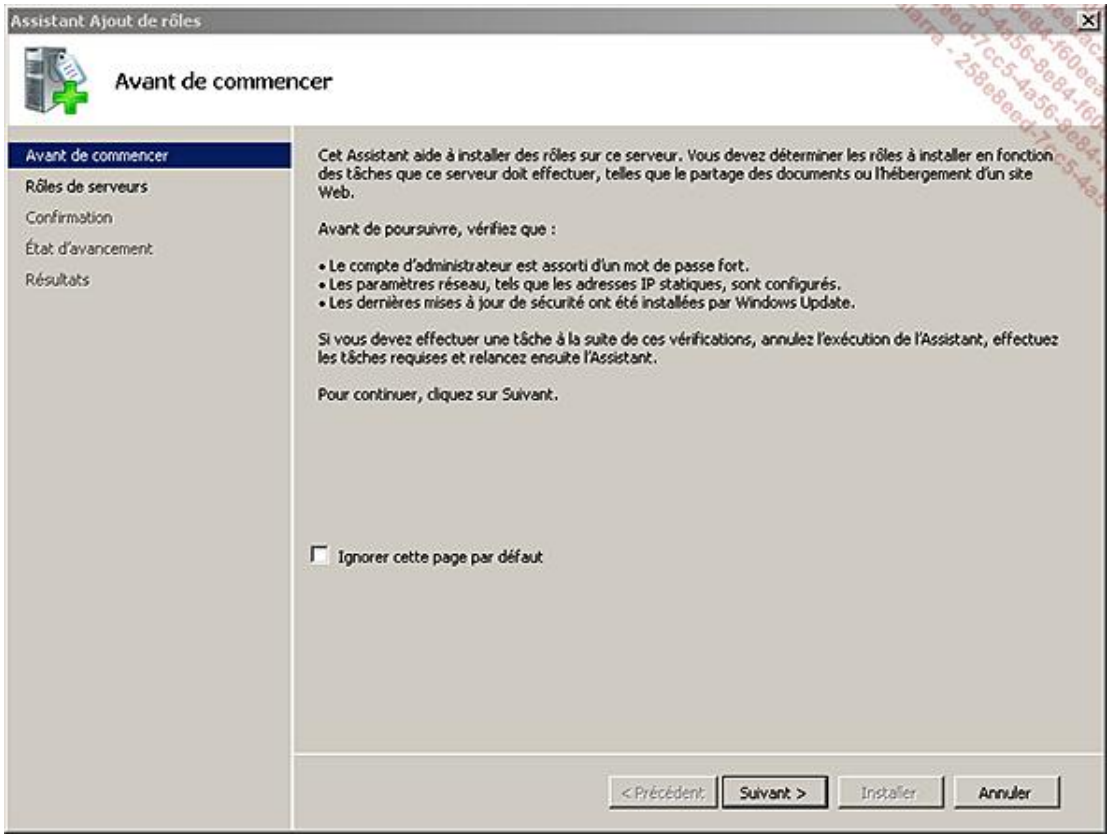
a. Installation du rôle Services de stratégie et d'accès réseau

L'installation du rôle se fait depuis la console **Gestionnaire de serveur**, dans le sous-dossier **Rôles**, en cliquant sur **Ajouter des rôles**.

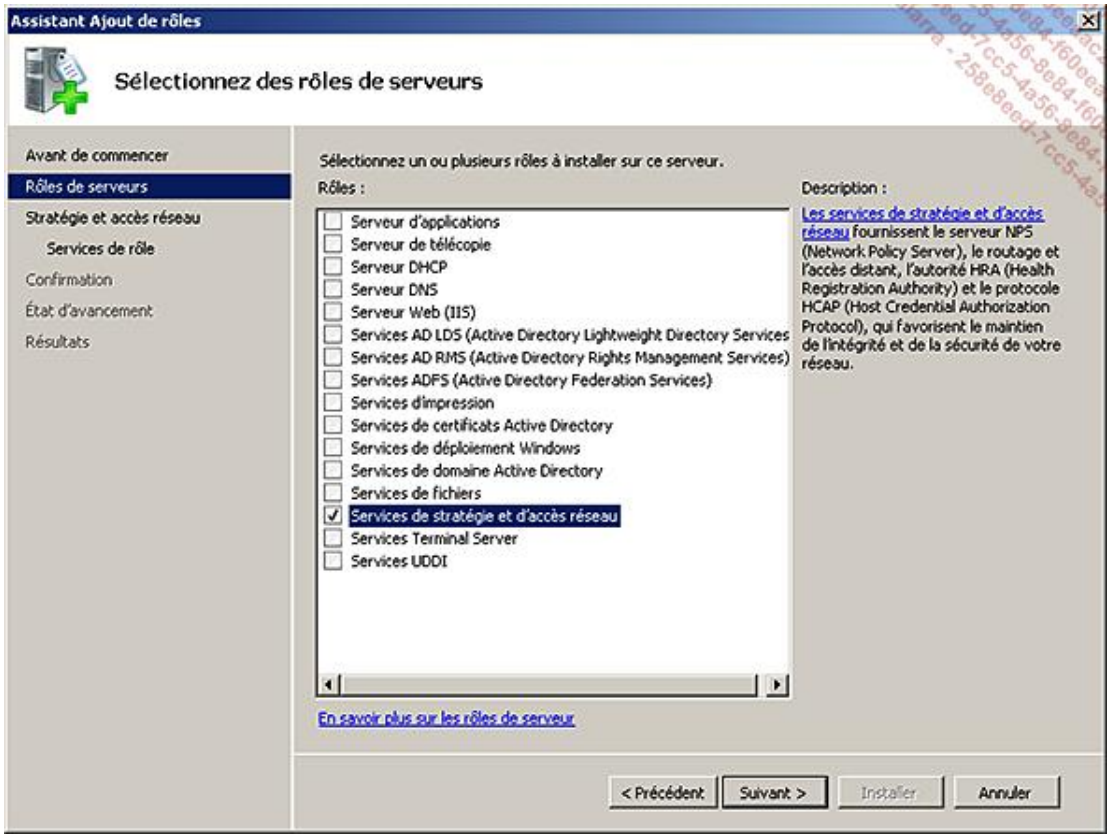
Voici les différentes étapes :

- Ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer** - **Outils d'administration** puis **Gestionnaire de serveur**.

© ENI Editions - All rights reserved - adamo diarra

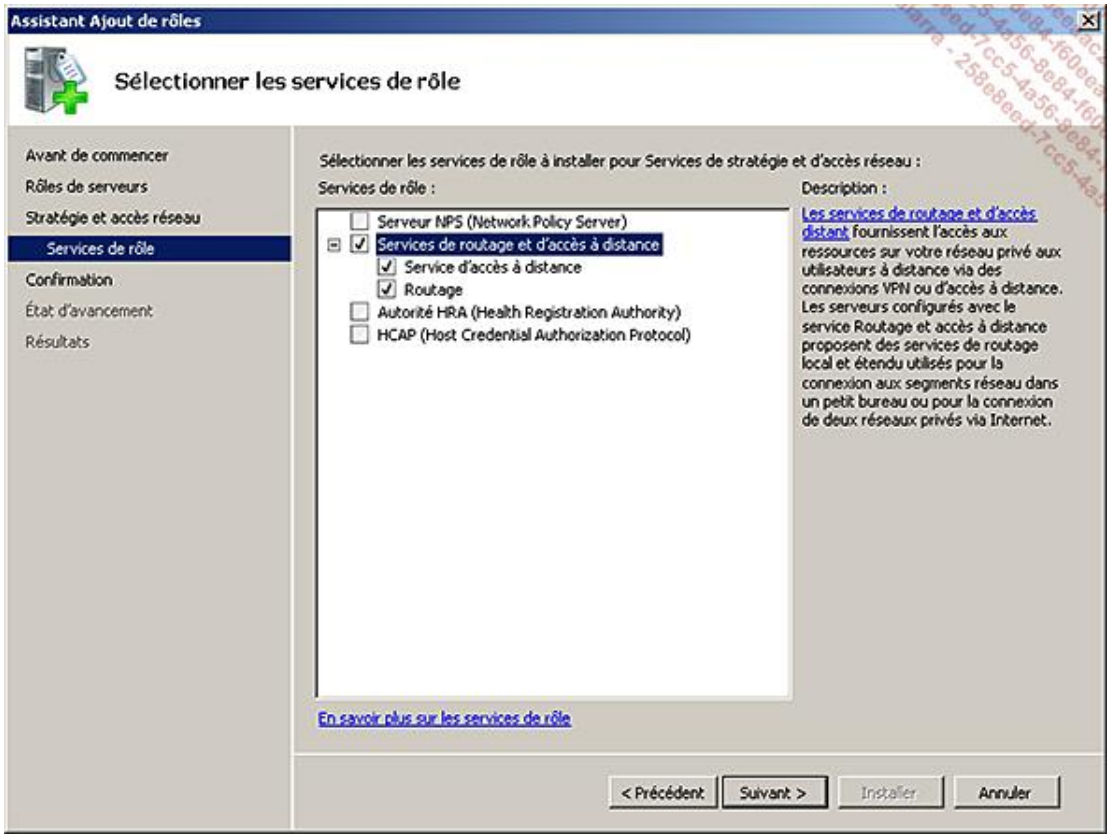


- Cliquez sur **Suivant**.
- Au niveau de **Résumé des rôles**, cliquez sur **Ajouter des rôles**.
- Sélectionnez le rôle : **Services de stratégie et d'accès réseau**.



© ENI Editions - All rights reserved - adamo diarra

- Sur la page d'**Introduction au service de stratégie et d'accès réseau**, cliquez sur **Suivant**.
- Cochez les cases **Service d'accès à distance** et **Routage** comme illustré sur l'écran ci-dessous :



- À la page de confirmation, cliquez sur **Installer**.
- Sur la page de **Résultats**, vérifiez que l'installation s'est bien déroulée et cliquez sur **Fermer**.

Pour créer un certificat auto signé pour L2TP/IPSec ou SSTP, ouvrez la console IIS et dans le volet de droite double cliquez sur **Certificats de serveur**. Dans le panneau d'outils à droite cliquez sur **Créer un certificat auto-signé** puis saisissez un nom convivial.

---

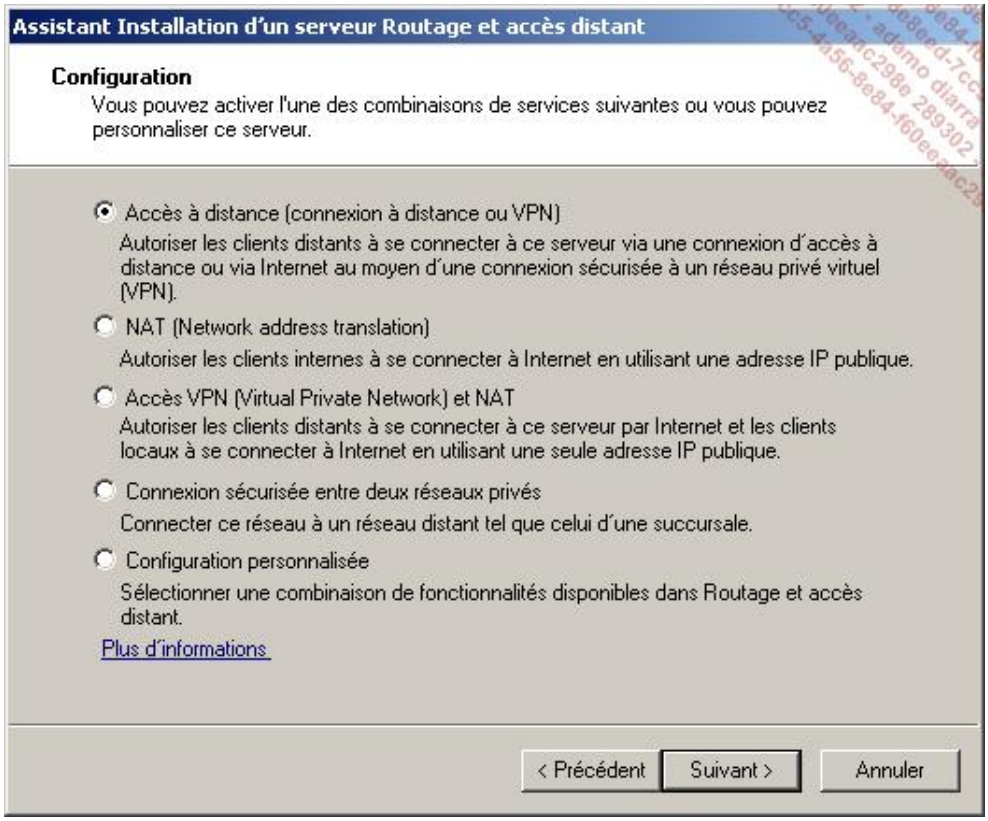
b. Configuration des fonctionnalités VPN

Maintenant que vous avez installé le rôle de serveur d'accès distant, vous allez configurer les paramètres associés.

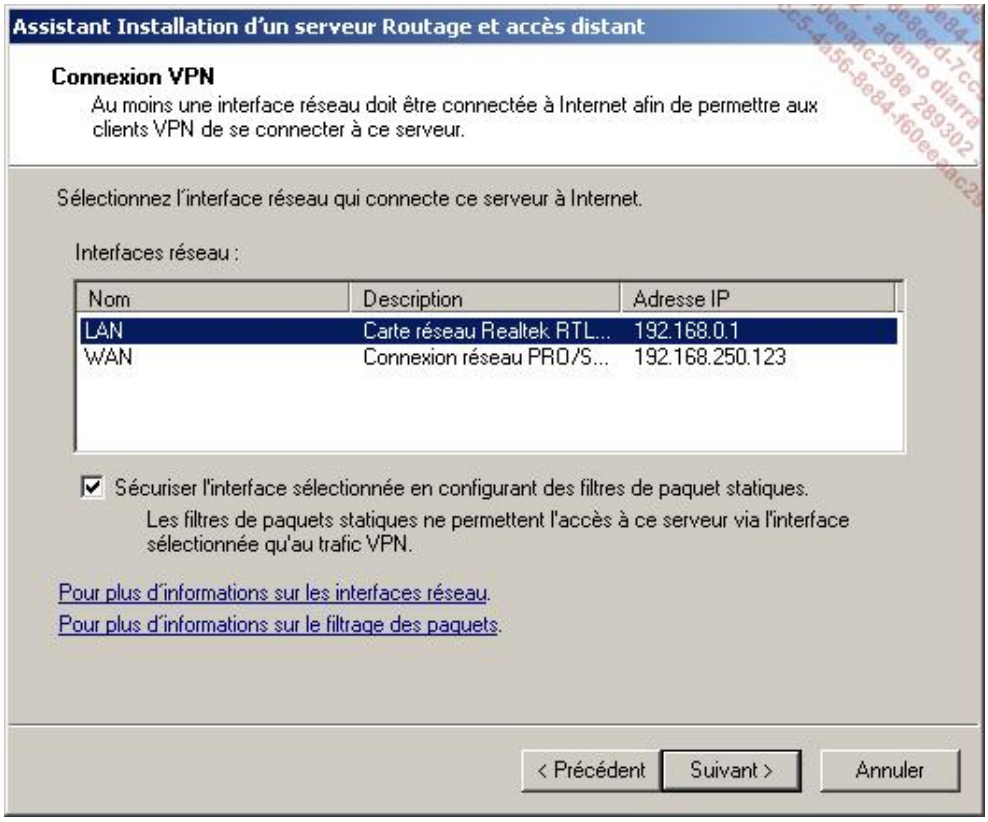
La procédure de configuration pour les trois technologies VPN est identique. Cependant pour pouvoir utiliser SSTP il faut au préalable avoir satisfait le pré-requis suivant : **Installation du rôle de serveur WEB IIS** abordée dans le chapitre Application Internet - Mettre en place un serveur Intranet/Internet.

- Dans la console **Gestionnaire de serveur**, développez l'arborescence : **Rôles - Services de stratégie et d'accès réseau**.
- Faites un clic droit sur **Routage et accès distant** puis cliquez sur **Configurer et activer le routage et l'accès à distance**.
- L'assistant d'Installation se lance, cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- Sélectionnez **Accès à distance** et cliquez sur **Suivant**.
- Sélectionnez **VPN** et cliquez sur **Suivant**.
- Sélectionnez votre interface publique (ici pour plus de simplicité les connexions ont été renommées en fonction de leur utilisation).



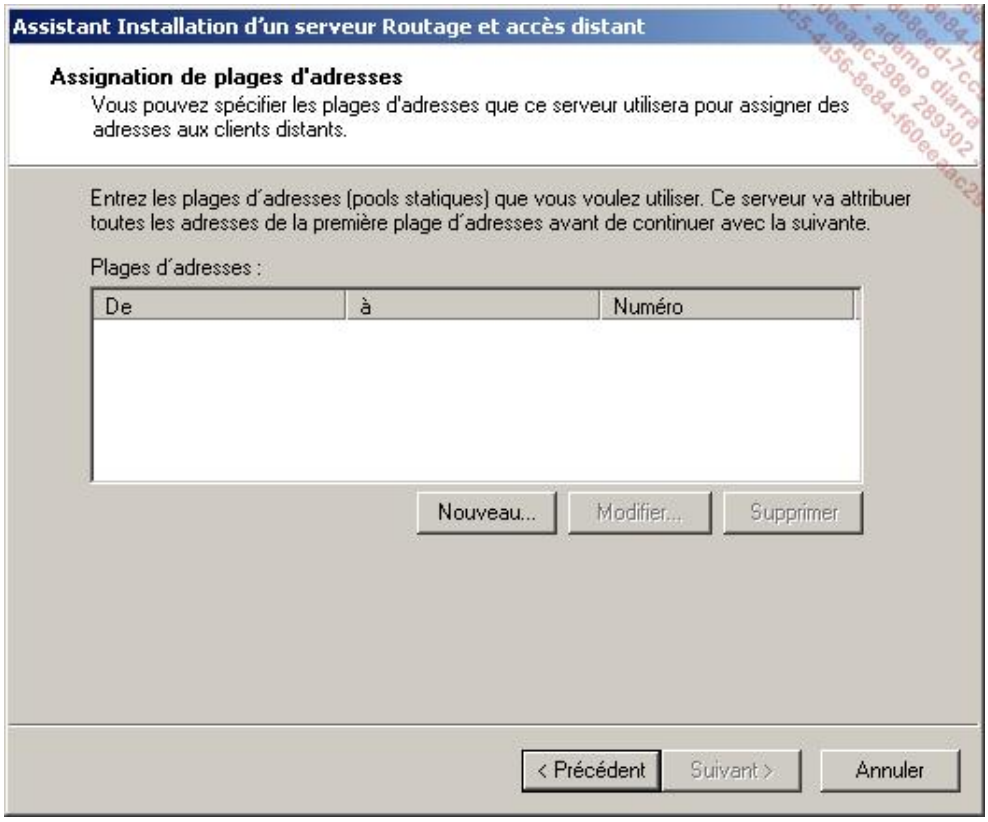
© ENI Editions - All rights reserved - adamo diarra

- Cliquez sur **Suivant**.

- Dans la page **Attribution d'adresses IP**, sélectionnez **Automatiquement** si vous disposez d'un serveur DHCP. Autrement, sélectionnez **A partir d'une plage d'adresses spécifiée**.

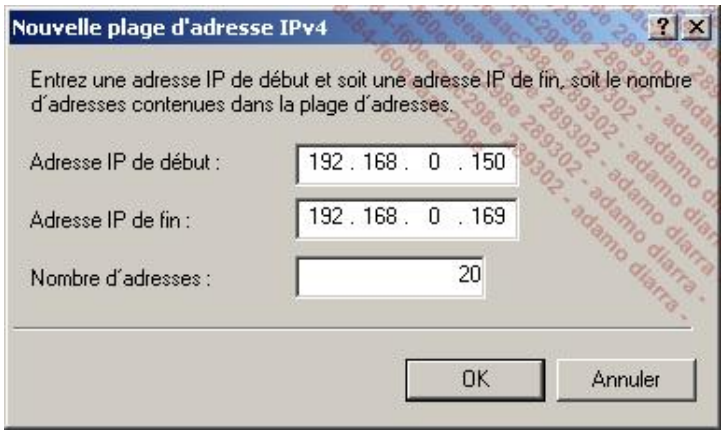
- Cliquez sur **Suivant**.

- Si vous choisissez de faire attribuer les adresses par le serveur VPN vous obtiendrez la page suivante :



- Cliquez sur **Nouveau** puis spécifiez une plage contenant suffisamment d'adresses réseaux. Validez puis cliquez sur **Suivant**.

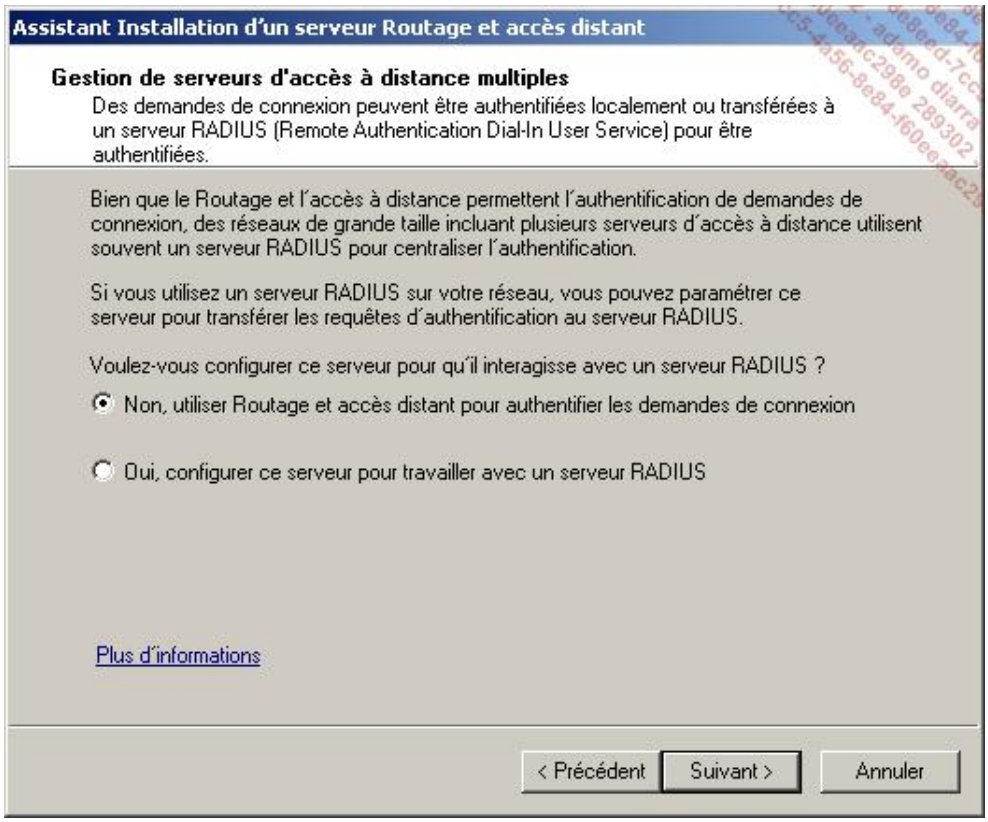
  Attention à bien spécifier une plage correspondant à votre réseau local. Sans cela la communication ne peut pas fonctionner.



- À la page **Gestion de serveurs d'accès à distance multiples**, si vous disposez d'un serveur RADIUS cochez **Oui**, sinon cochez **Non**.

© ENI Editions - All rights reserved - adamo diarra

Ici vous allez cocher **Non** car la sécurité avec RADIUS est abordée plus tard dans ce chapitre.



- Cliquez sur **Suivant**.

- À la page **Résumé**, vérifiez que les informations de configuration sont bien celles désirées puis cliquez sur **Terminer** puis **OK**.

Une fois cet assistant terminé, Windows Server 2008 R2 crée automatiquement 128 ports pour chacune des trois technologies de VPN qu'il connaît. Chaque connexion requiert un port unique. Pour plus de sécurité il convient d'ailleurs de désactiver les ports inutiles.

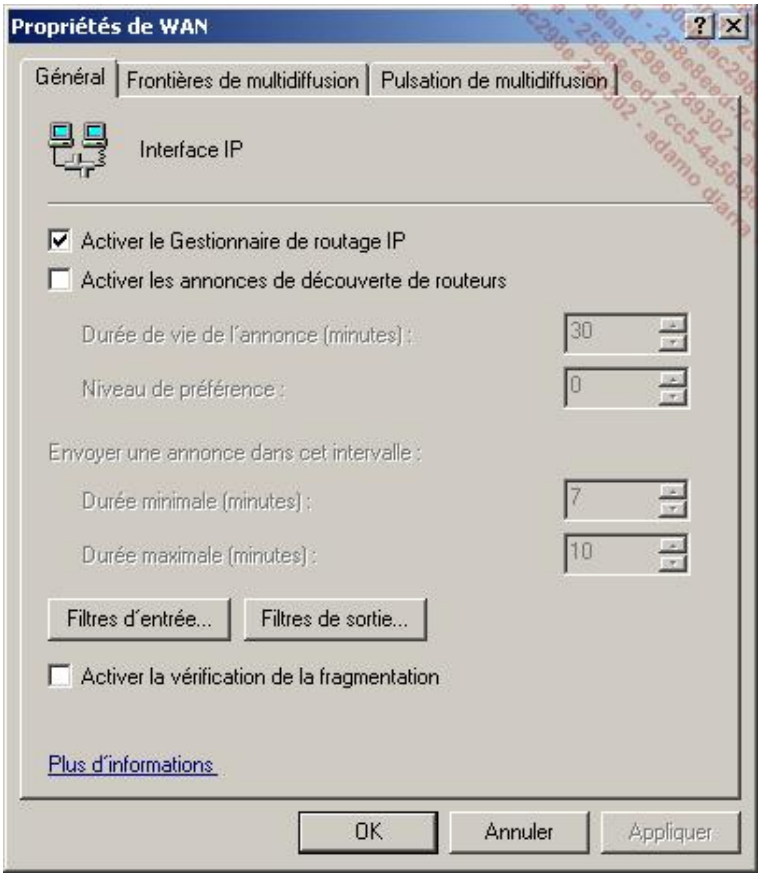
Une fois configuré pour accepter les connexions VPN entrantes, Windows Server 2008 R2 va automatiquement bloquer tout le trafic entrant sur l'interface publique qui ne correspondrait pas au trafic VPN.

Pour modifier les paquets autorisés (ex : pour pouvoir prendre la main sur le serveur en bureau distant) :

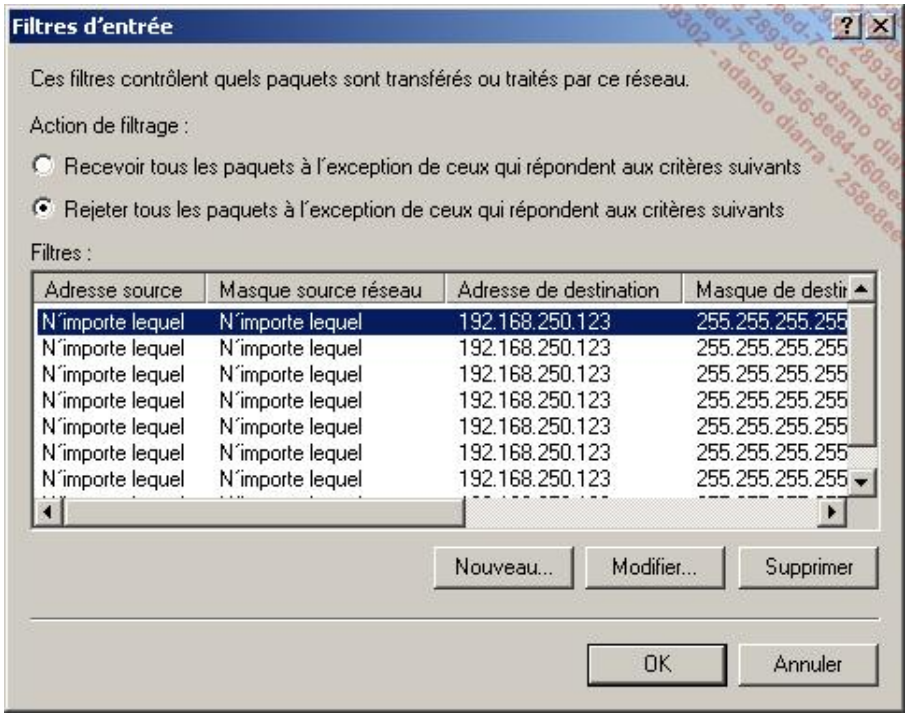
- Depuis la console **Gestionnaire de serveur**, développez **Services de stratégie et d'accès réseau - Routage et accès distant - IPV4** (ou **IPV6** selon votre utilisation) - **Général**.

- Faites un clic droit sur votre interface publique puis sélectionnez **Propriétés**.

© ENI Editions - All rights reserved - adamo diarra



- Cliquez sur **Filtres d'entrée...**.



- Il ne vous reste ensuite plus qu'à autoriser le trafic voulu (3389 en TCP par exemple pour le bureau à distance).

2. Gestion de la sécurité des accès

Maintenant que vous savez configurer Windows Server 2008 R2 en tant que serveur d'accès distant, vous voudrez

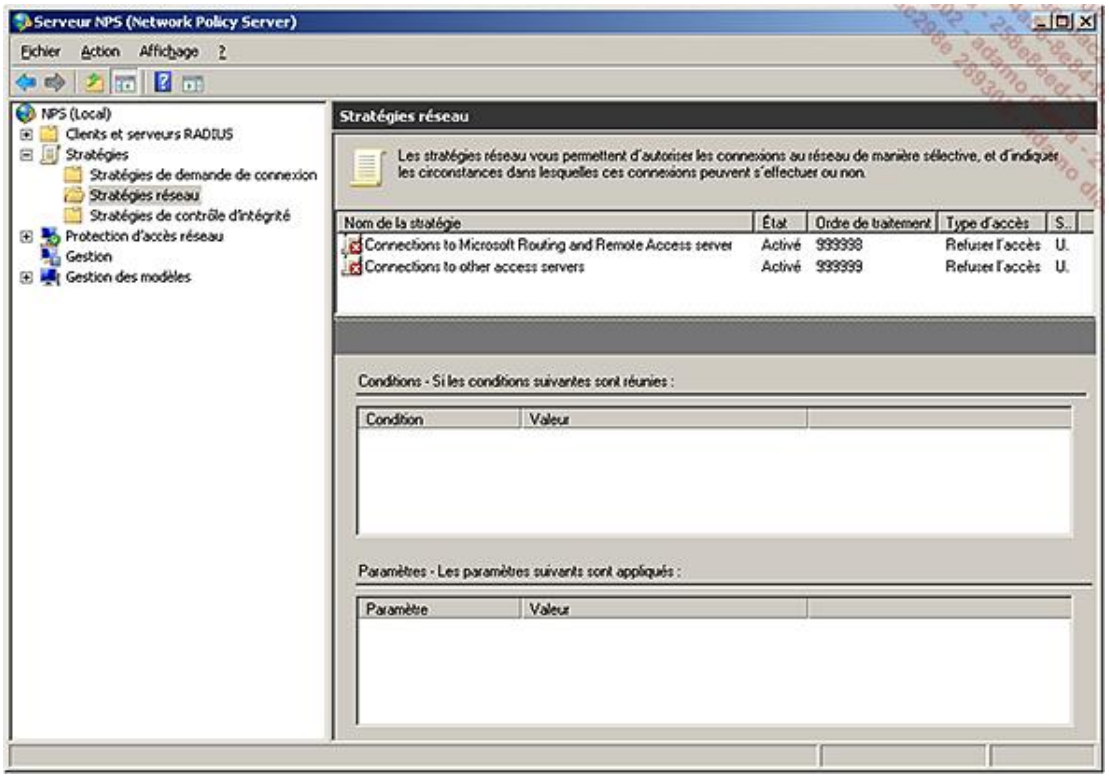
© ENI Editions - All rights reserved - adamo diarra

sans doute pouvoir contrôler la manière dont les utilisateurs se connectent. Comptes d'utilisateurs, plages horaires, groupes et bien d'autres paramètres encore sont configurables.

Dans les versions précédentes de Windows, ces paramètres étaient gérés via la console **Stratégies d'accès distant**. Désormais vous pourrez utiliser la console **Serveur NPS** (*Network Policy Server*).

Pour modifier une stratégie existante :

- Allez dans **Démarrer - Outils d'administration - Serveur NPS (Network Policy Server)**, puis cliquez sur le dossier **Stratégies réseau**.



La capture d'écran ci-dessus montre une des spécificités de Windows Server 2008 R2 : la gestion de modèles. En effet, vous pourrez faciliter la configuration de vos stratégies en important des modèles existants depuis un autre serveur ou encore en réutilisant des modèles du serveur local.

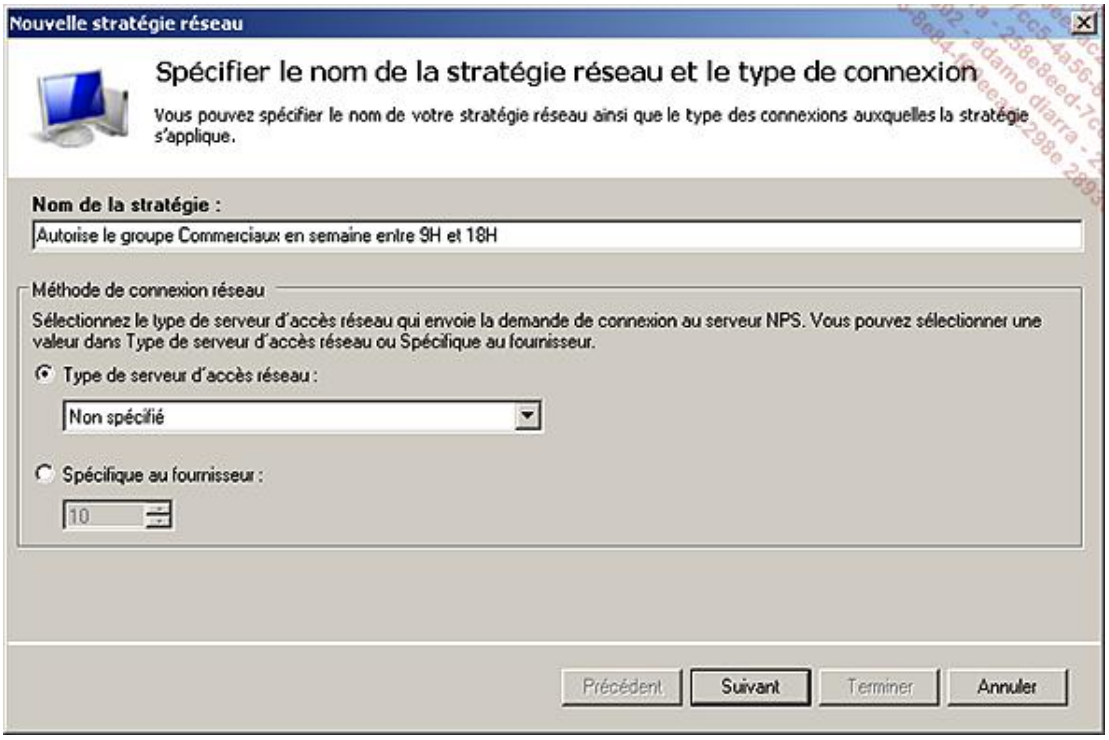
Vous y trouverez deux stratégies par défaut avec des valeurs maximales pour la colonne **Ordre de traitement**. Vous devez faire attention à cet ordre. En effet, les stratégies réseaux sont traitées dans l'ordre croissant. Le serveur va parcourir les stratégies en partant de la plus petite valeur. S'il en trouve une qui correspond aux critères de la demande de connexion, il autorise ou non le trafic. Aussi, si une stratégie est configurée pour refuser l'accès, lors de la vérification des stratégies l'accès sera automatiquement refusé même si une stratégie venant plus tard l'aurait autorisé.

Le mieux reste de créer vous-même vos stratégies d'accès réseau de façon à maîtriser leur contenu. Voici la marche à suivre pour créer une stratégie autorisant le groupe *Commerciaux* à se connecter en semaine de 9h à 18h :

- Dans la console **Serveur NPS**, allez dans **Stratégies réseaux**.

- Faites un clic droit sur le dossier **Stratégies réseaux** puis cliquez sur **Nouveau**. Spécifiez un nom pour votre stratégie. Attention à choisir des noms explicites, si vos stratégies doivent se multiplier vous gagnerez ainsi en lisibilité.

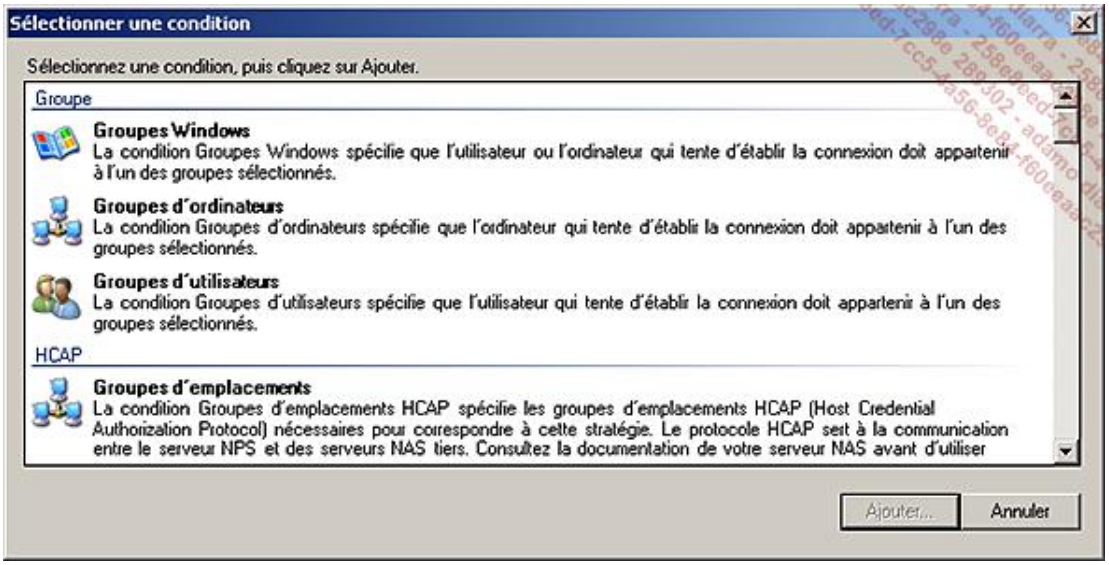
© ENI Editions - All rights reserved - adamo diarra



- La liste déroulante **Type de serveur d'accès réseau** se réfère à la technologie NAP (*Network Access Protection*) abordée précédemment dans le chapitre Mise en place des services réseaux d'entreprise. Ici seule la sécurité de ce serveur VPN sera gérée, vous laisserez donc le choix à **Non spécifié**.

- Cliquez sur **Suivant**.

- Vous arrivez ensuite à la page des conditions, cliquez sur **Ajouter**.



Vous avez alors la possibilité de choisir parmi une multitude de critères regroupés dans sept groupes distincts :

- Groupe (groupes d'ordinateurs, d'utilisateurs, etc.) ;
- HCAP (groupes correspondant à des serveurs d'accès réseaux tiers) ;
- Restrictions horaires (jours de la semaine, plage horaire, etc.) ;
- Protection d'accès (système d'exploitation, compatibilité NAP, etc.) ;

© ENI Editions - All rights reserved - adamo diarra

- Propriétés de la connexion (adresse IP du client, type d'authentification, etc.) ;
- Propriétés du client (nom du client RADIUS, IP du client RADIUS, etc.) ;
- Passerelle (numéro de téléphone du serveur Dial-Up, nom du périphérique réseau qui transmet la demande).

La présentation de toutes les conditions ne sera pas faite dans ce livre compte tenu de leur grand nombre. Vous pourrez cependant trouver plus de détails sur le TechNet de Microsoft à l'adresse : http://technet.microsoft.com/en-us/library/cc731220.aspx

---

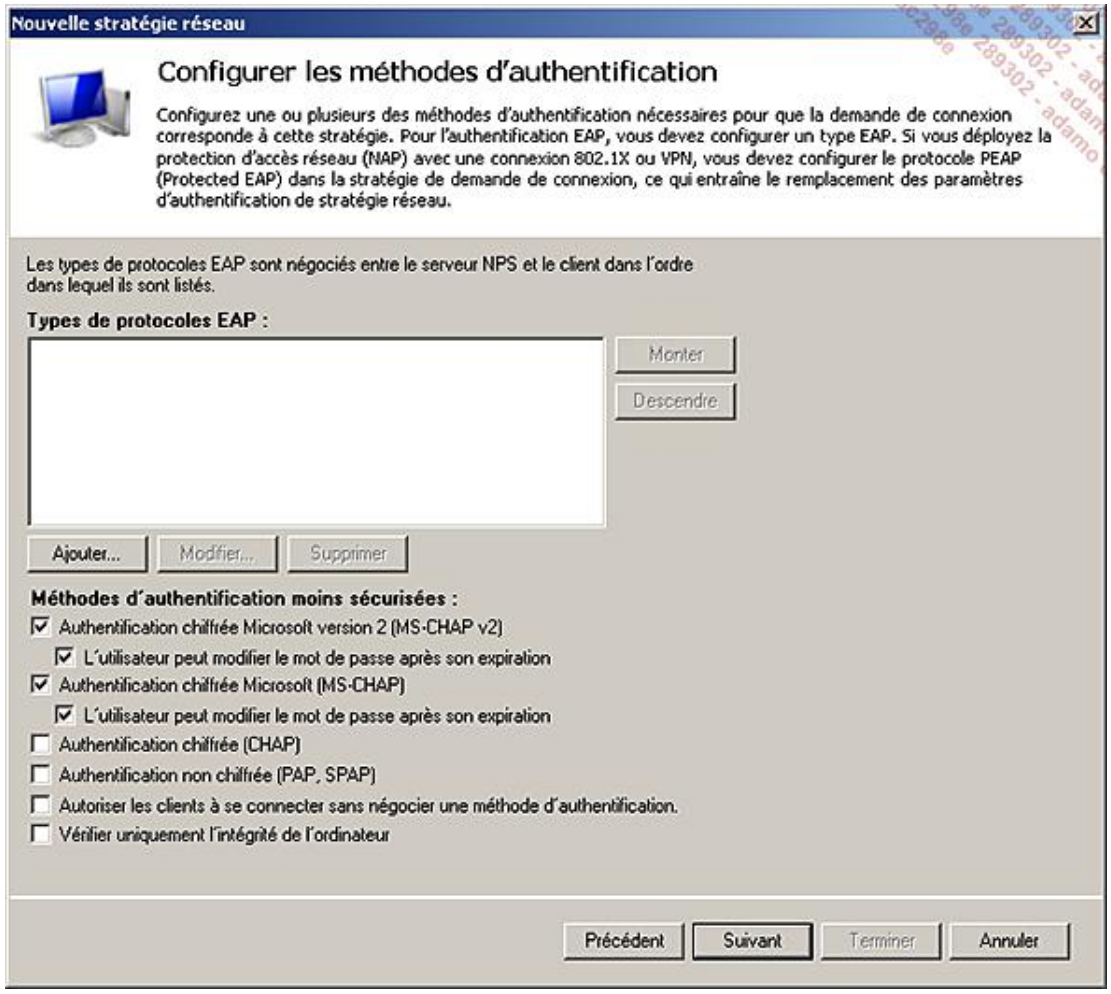
Les conditions sont cumulables, vous pouvez par exemple faire en sorte d'autoriser l'accès uniquement à un groupe d'utilisateurs et sur une plage horaire bien précise.

- Sélectionnez **Groupes d'utilisateurs** puis cliquez sur **Ajouter**.
- Dans la boîte de dialogue qui vient d'apparaître cliquez sur **Ajouter des groupes** puis saisissez le nom du groupe (Commerciaux dans notre exemple) puis validez par **OK**.

- Validez par **OK** puis cliquez sur **Suivant**.
- Une fois vos conditions ajoutées, vous avez le choix **D'accorder l'accès**, de **Refuser l'accès** ou encore de faire en sorte que ce soient les **propriétés de numérotation des utilisateurs qui déterminent l'accès** (dans ce cas ce sont les propriétés définies dans le compte de l'utilisateur qui sont prises en compte). Dans cet exemple, choisissez **D'accorder l'accès** puis cliquez sur **Suivant**.
- Vous avez ensuite le choix entre les différentes **Méthodes d'authentification**.

  Vous devez en choisir au moins une. Attention cependant, les cases non cochées dans l'image ci-dessous représentent des authentifications peu sécurisées et ne devraient pas être cochées dans la mesure du possible.

© ENI Editions - All rights reserved - adamo diarra



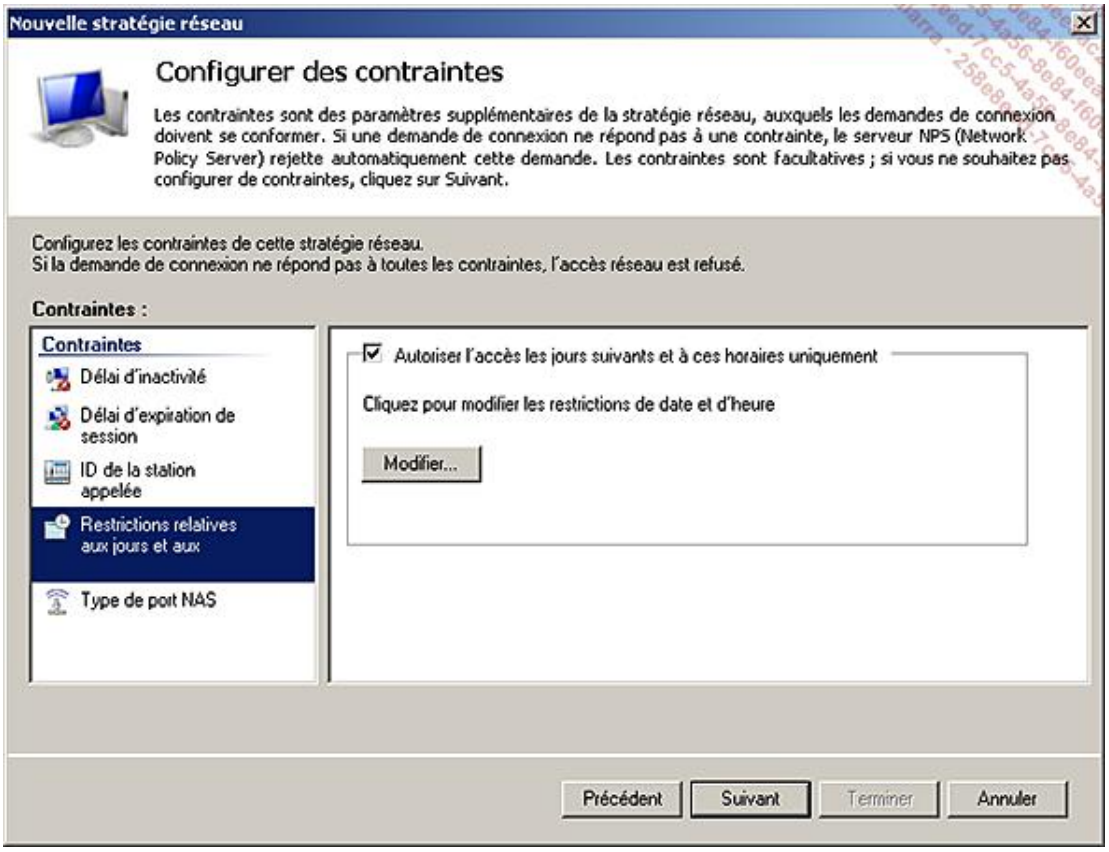
Ici laissez les cases cochées par défaut.

- Cliquez sur **Suivant**.

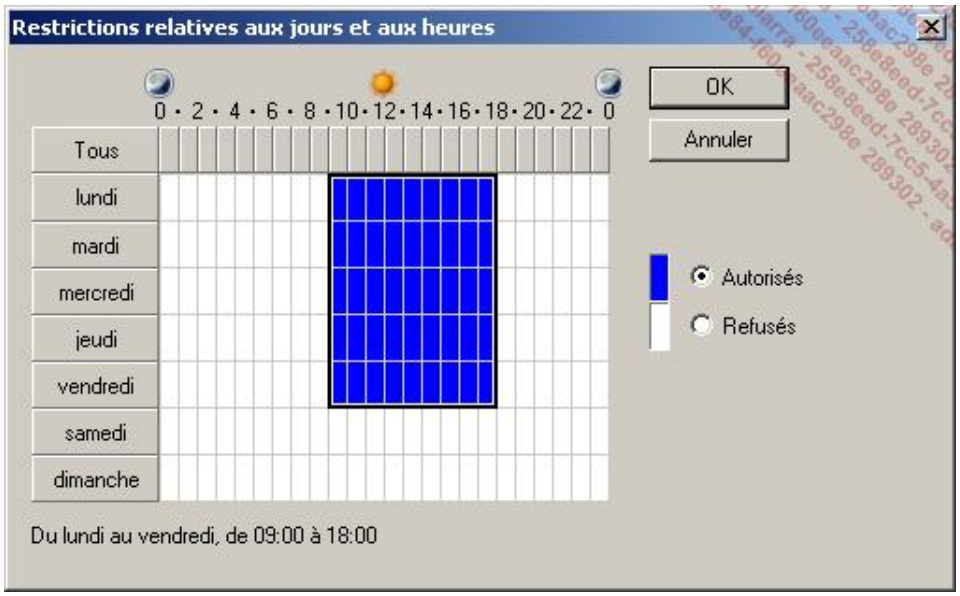
La page de contraintes permet d'appliquer des restrictions supplémentaires comme la plage horaire autorisée (cas de notre exemple).

- Cliquez sur **Restrictions relatives aux jours et aux** puis cochez la case **Autoriser l'accès les jours suivants et à ces horaires uniquement**.

© ENI Editions - All rights reserved - adamo diarra



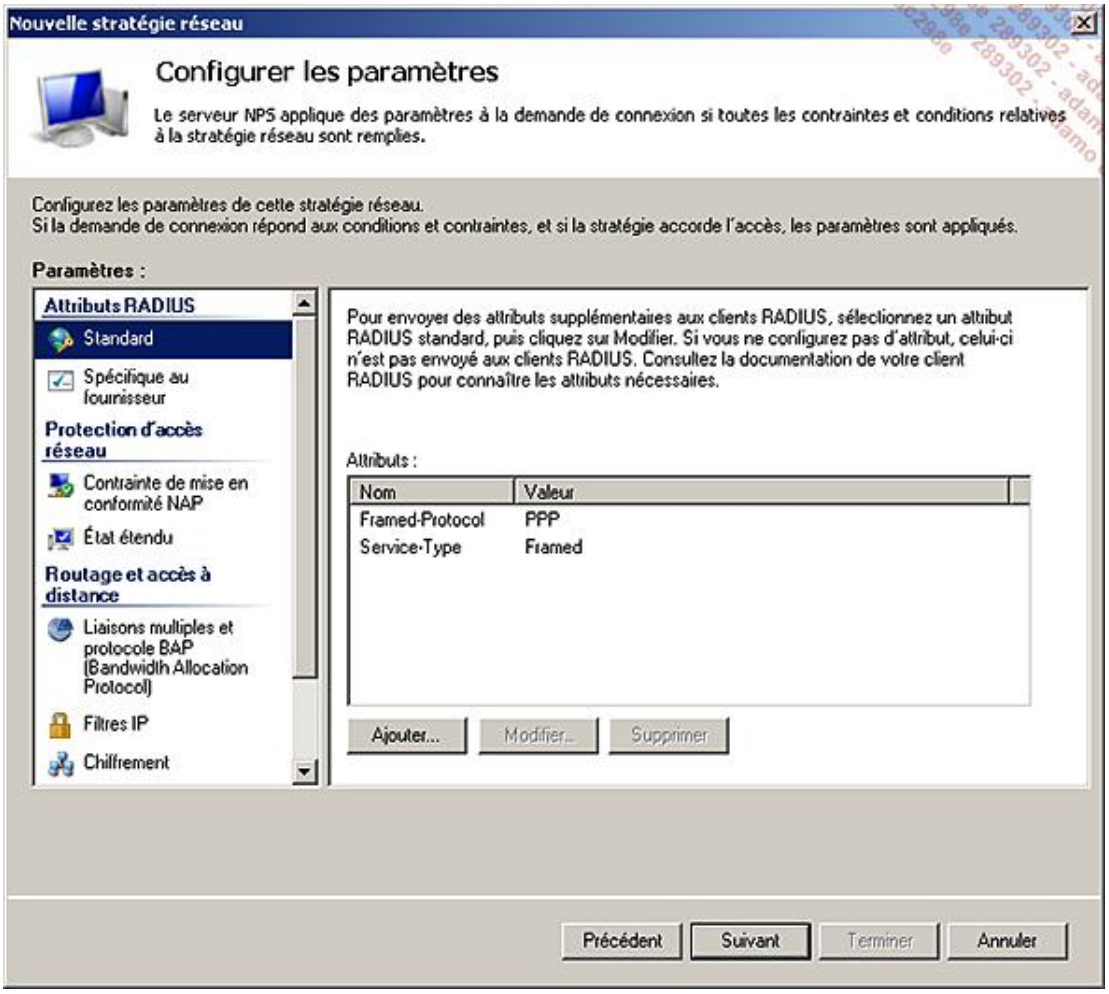
- Cliquez sur **Modifier** puis remplissez comme ci-après pour autoriser les jours de semaine entre 9h et 18h.



- Validez en cliquant sur **OK** puis cliquez sur **Suivant**.

- Dans cette fenêtre vous pouvez configurer des paramètres supplémentaires pour sécuriser la connexion. En effet, si la connexion répond aux critères précédents, à savoir conditions et contraintes, elle se voit appliquer des paramètres supplémentaires. Cela va de la mise en conformité via NAP à un chiffrement de la connexion ou encore à une restriction sur les protocoles utilisés pendant la connexion. Pour cet exemple, ne spécifiez pas de paramètres et cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- Sur la dernière page de l'assistant, vérifiez bien les informations saisies puis cliquez sur **Terminer**.

- Votre nouvelle stratégie apparaît avec un chiffre appliqué automatiquement pour l'ordre de traitement. Vous pouvez ensuite modifier à loisir cet ordre en faisant un clic droit sur la stratégie puis en choisissant l'une des options, **Monter** ou **Descendre**. Cela vous permet de définir sa priorité et donc l'ordre dans lequel elle est vérifiée lors d'une demande de connexion.

3. Gestion de l'authentification (IAS/RADIUS)

Dans la partie précédente vous avez vu comment configurer une stratégie de connexion pour l'accès via VPN grâce à la console NPS. Bien que techniquement faisable, cela devient rapidement ingérable lorsque vous disposez de plusieurs serveurs d'accès réseaux (serveurs VPN, bornes Wi-Fi, etc.).

Pour centraliser la gestion des règles d'accès et de l'authentification vous avez besoin du composant de service **NPS** (*Network Policy Server*). Ce rôle était connu dans les versions précédentes de Windows Server sous le nom d'IAS (*Internet Authentication Service*).

Pour centraliser l'authentification, utilisez le rôle de **serveur RADIUS**. L'intérêt de la technologie RADIUS est de pouvoir centraliser la gestion de la sécurité d'équipements informatiques autres que Microsoft. En effet, vous pouvez par exemple configurer un point d'accès Wi-Fi pour utiliser le serveur NPS Windows Server 2008 R2 pour gérer l'authentification.

Voici les fonctions que vous offre le rôle de Serveur NPS en matière de sécurisation :

- **Network Policy Server (NPS)** : authentification, autorisation, services pour serveurs d'accès distants, VPN, points d'accès Wi-Fi, passerelle TS.

- **NPS Accounting (ou journalisation)** : audit et enregistrement des authentifications et des requêtes de compte dans une base SQL ou un fichier local. Windows Server 2008 R2 intègre un nouvel assistant permettant de faciliter la configuration de cette journalisation en créant automatiquement les bases de données associées.

© ENI Editions - All rights reserved - adamo diarra

- **NPS RADIUS Proxy** : permet l'acheminement des messages entre les clients RADIUS (les serveurs d'accès et les serveurs RADIUS qui s'occupent de l'authentification).
- **NPS NAP** : reportez-vous au chapitre Mise en place des services réseaux d'entreprise - La mise en place de la quarantaine réseau.
- **NPS RADIUS serveur** : gère l'authentification, l'autorisation et l'enregistrement des demandes des clients RADIUS.
- **NPS RADIUS Client** : serveur d'accès distant utilisant un serveur RADIUS pour l'authentification.

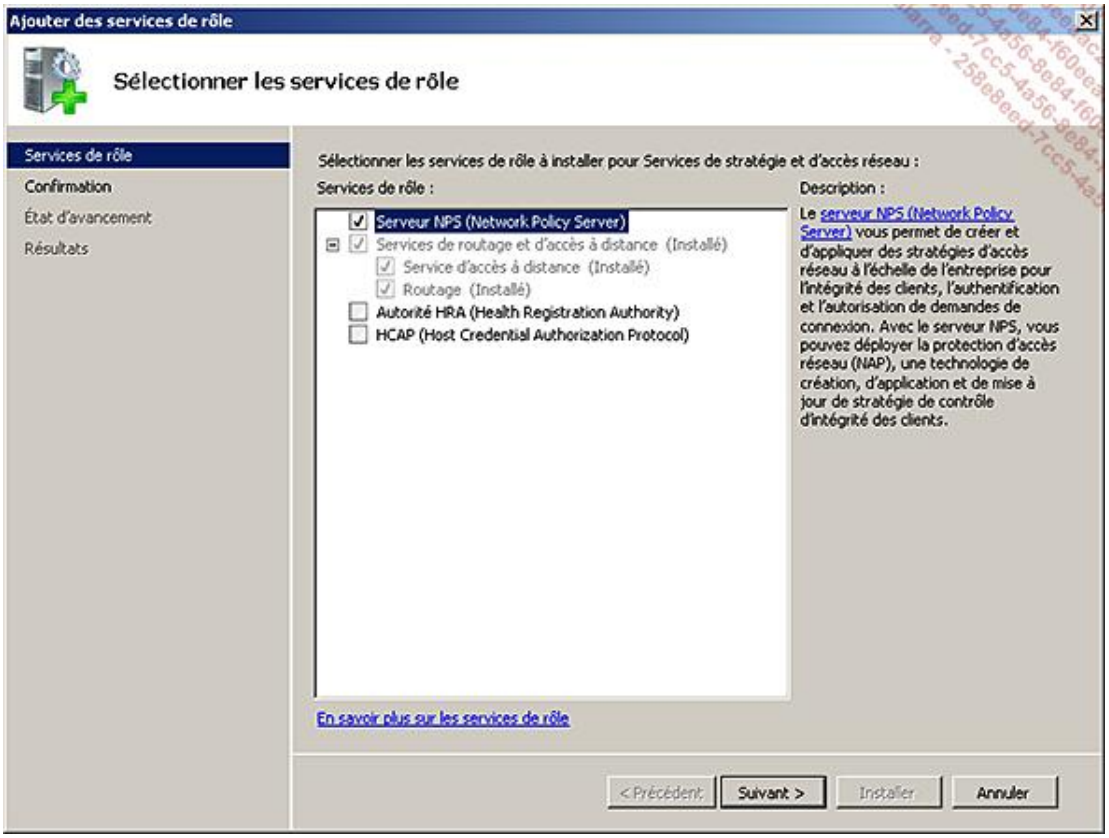
Les ordinateurs clients ne sont pas des clients RADIUS. Ce sont les équipements auxquels ils se connectent (serveur VPN, point d'accès Wi-Fi) qui le sont.

Dans les rubriques précédentes de ce chapitre vous avez vu comment ajouter le rôle de serveur d'accès distant. Pour pouvoir installer le composant NPS, procédez comme suit :

- Dans la console **Gestionnaire de serveur**, naviguez jusqu'à : **Rôles - Services de stratégies d'accès distant**.
- Dans la fenêtre de droite, cliquez sur **Ajouter des services de rôle**.

- Cochez la case **Serveur NPS (Network Policy Server)** comme figuré dans l'image ci-après puis cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- Cliquez ensuite sur **Installer**.

- Une fois l'installation terminée, cliquez sur **Fermer**.

Vous pouvez désormais gérer la sécurité des accès à votre réseau de manière centralisée et ce depuis votre console **Network Policy Server**.

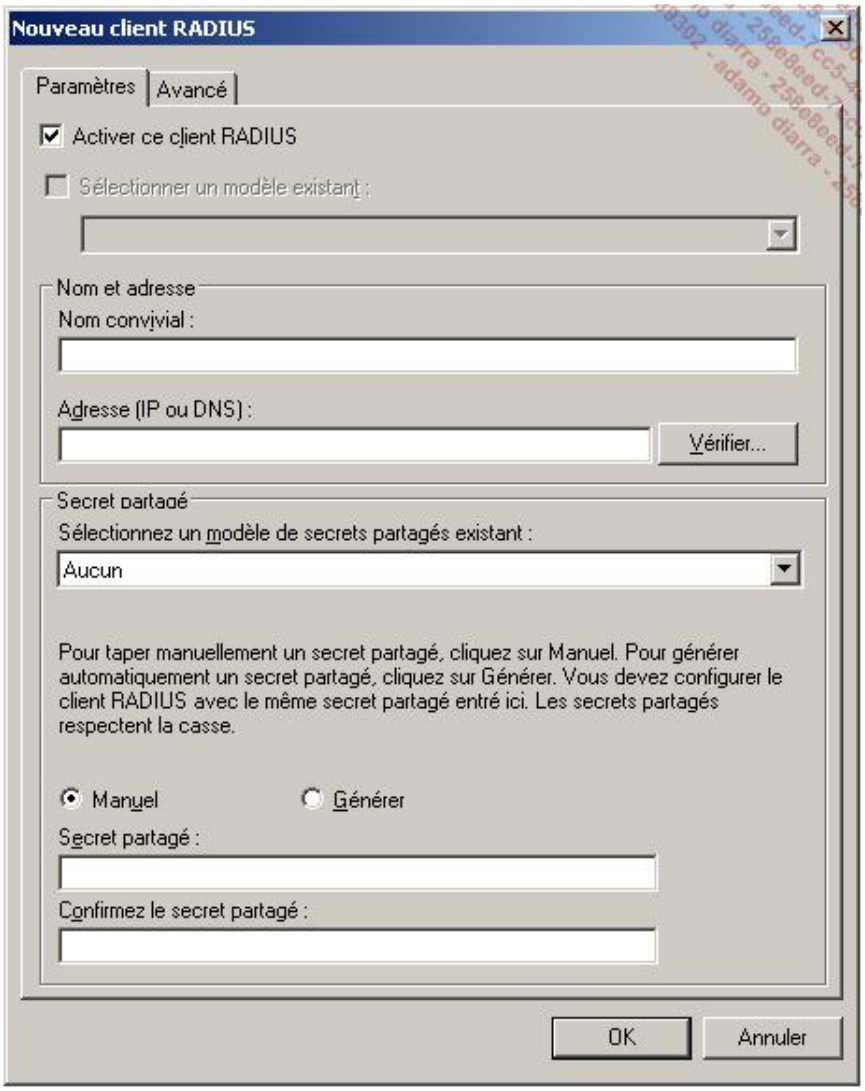
La configuration des stratégies d'accès (horaires, utilisateurs, etc.) se fait de la même façon que pour un serveur VPN (vu précédemment dans ce même chapitre). Vous pouvez cependant désormais configurer votre serveur NPS pour qu'il agisse en temps que serveur RADIUS ou encore en temps que Proxy RADIUS.

Pour permettre à un périphérique d'accès d'utiliser votre serveur en temps que serveur RADIUS il vous faut au préalable l'avoir autorisé. Pour cela voici comment procéder :

- Dans votre console NPS, naviguez jusqu'à **Clients et Serveurs RADIUS**.

- Faites un clic avec le bouton droit de la souris sur **Clients RADIUS** puis **Nouveau**.

© ENI Editions - All rights reserved - adamo diarra

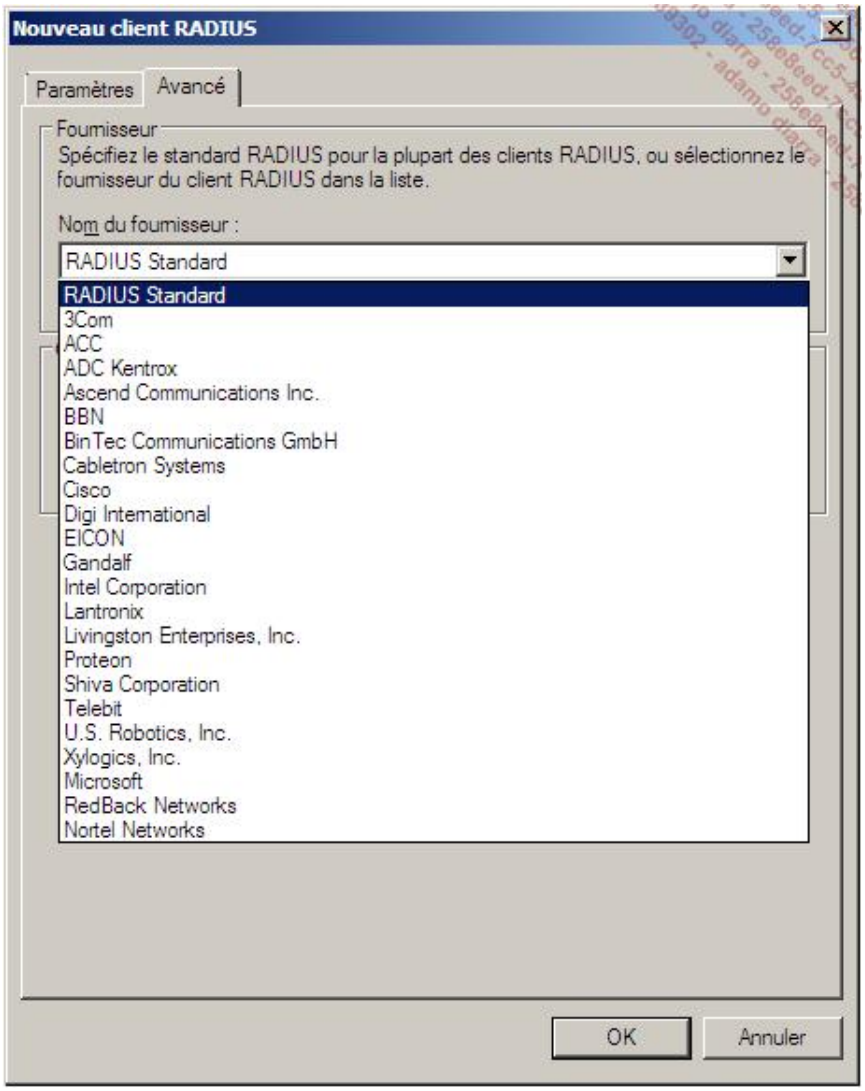


- Il vous suffit alors de déclarer le périphérique d'accès en lui donnant un **Nom convivial** et son **Adresse IP**.

  Si besoin, cliquez sur l'onglet **Avancé** et spécifiez :

  - Le **Nom du fournisseur** (la liste déroulante fournit de nombreux acteurs importants du monde informatique comme Cisco, etc.).

© ENI Editions - All rights reserved - adamo diarra



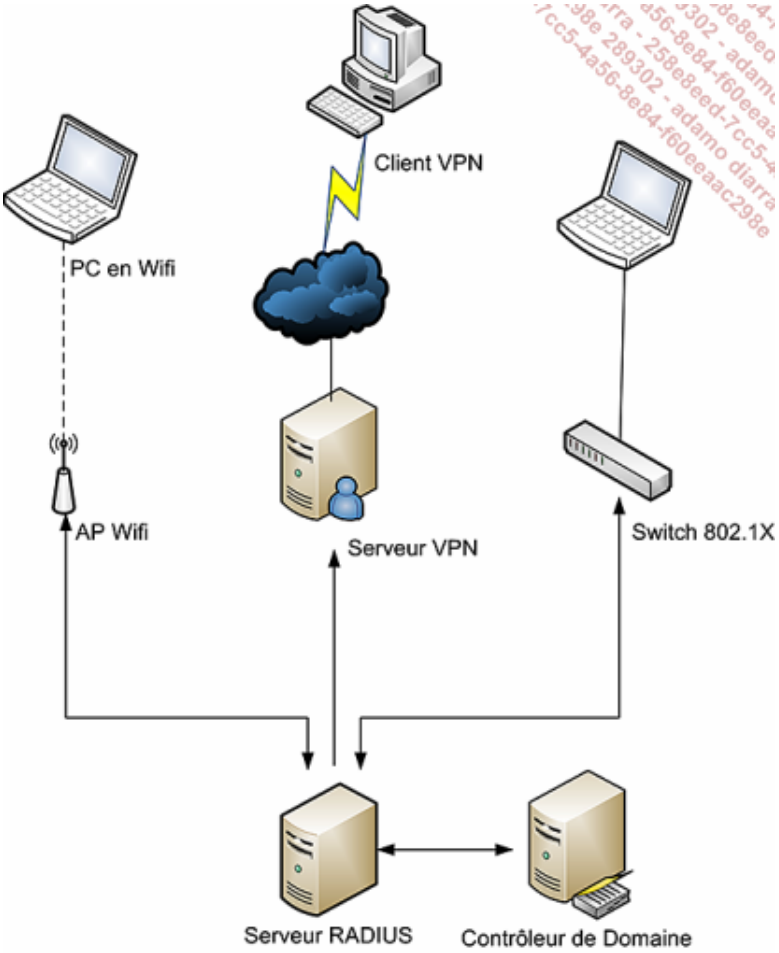
- Une clé de sécurité que vous configurerez aussi sur le périphérique d'accès.

Vous pourrez également choisir les protocoles d'authentification et spécifier si le client RADIUS est compatible NAP ou non.

Une fois un périphérique déclaré, vous pouvez l'activer ou le désactiver par un simple clic droit et une case à cocher. Pour cela il suffit, dans la rubrique **Clients RADIUS**, d'aller dans les propriétés du périphérique nouvellement créé. Il ne vous reste alors qu'à choisir entre **Activé** ou **Désactivé**.

Ci-dessous, un exemple d'utilisation de serveur RADIUS.

© ENI Editions - All rights reserved - adamo diarra



Il peut être intéressant d'utiliser un serveur Proxy RADIUS dans les cas suivants :

- Vous voulez fournir une authentification pour des comptes non membres du domaine dont le serveur NPS fait partie.
- Vous voulez fournir une authentification depuis une base de comptes autre que Windows.
- Vous voulez pouvoir traiter un grand nombre de requêtes de connexion. Le Proxy RADIUS agira comme un équilibreur de charge.
- Vous voulez sécuriser l'accès à votre base d'utilisateurs en plaçant un proxy RADIUS en DMZ.

Déclarer votre serveur en temps que Serveur proxy RADIUS est également très simple. Dans votre console NPS il vous suffit de :

- Naviguer jusqu'à **Clients et serveurs RADIUS**.
- Faire un clic droit sur **Groupes de serveurs RADIUS distants** puis **Nouveau**.
- Spécifier un nom de groupe puis cliquez sur **Ajouter**.
- Entrer le nom ou l'adresse IP d'un serveur RADIUS.
- Spécifier si le proxy RADIUS doit s'authentifier via une clé partagée auprès du serveur RADIUS, ou encore configurer l'équilibrage de charge.
- Ajouter plusieurs serveurs RADIUS dans un même groupe afin d'assurer une tolérance de pannes.

© ENI Editions - All rights reserved - adamo diarra

4. Implémentation de Direct Access

Les pré-requis à l'implémentation de Direct Access sont nombreux, aussi nous ne détaillerons pas leur installation dans ce chapitre. Voici la liste des pré-requis à respecter :

- Une infrastructure de clé publique (PKI) : elle servira à distribuer des certificats aux ordinateurs (elle peut également servir à fournir des certificats SSL pour les sites Web de votre plate-forme de tests).
- Un contrôleur de domaine exécutant Windows Server 2008 SP2 ou Windows Server 2008 R2.
- Un ordinateur client exécutant le système d'exploitation Windows 7.
- Des stratégies IPSec pour protéger le trafic entre les clients et le serveur.
- Deux interface réseaux sur le serveur Direct Access.

Pour plus de détails sur l'implémentation des pré-requis, reportez-vous au guide pas à pas que Microsoft a publié et qui est disponible (uniquement en anglais au moment de l'écriture de ce livre) à l'adresse : http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=8D47ED5F-D217-4D84-B698-F39360D82FAC&displaylang=en.

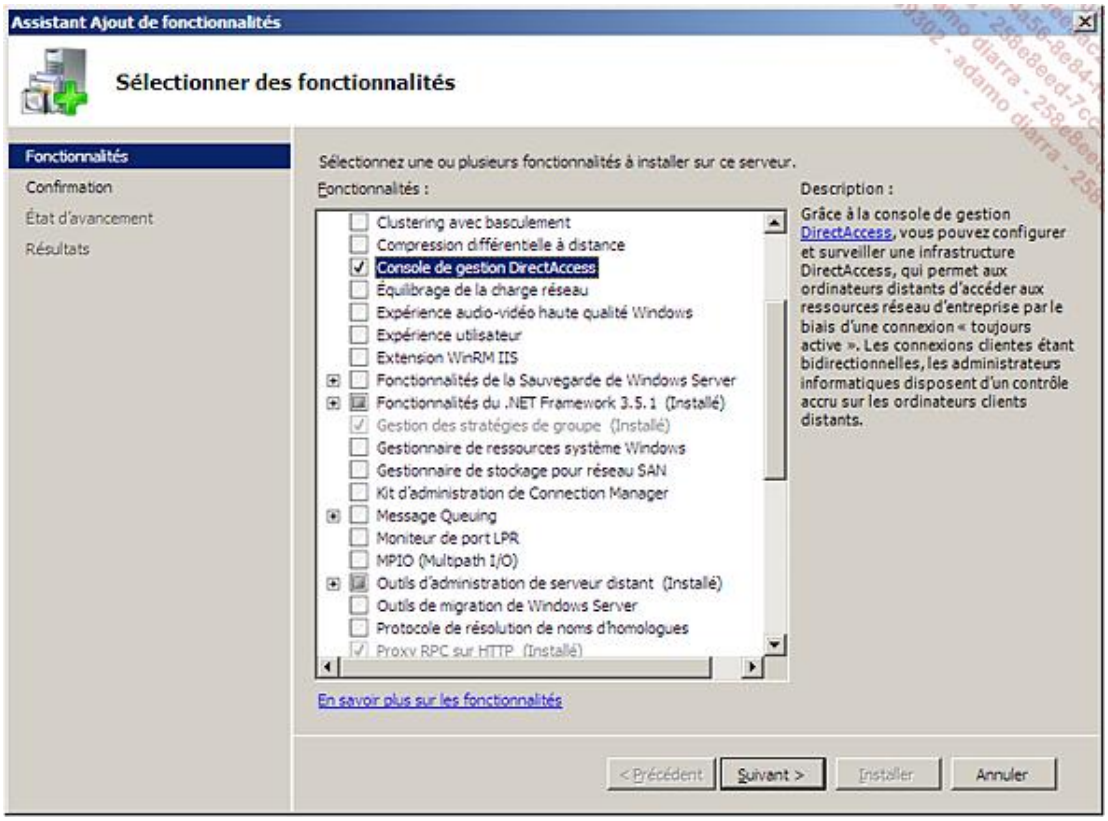
L'exemple présenté ci-après prend en compte les éléments suivants :

- Les pré-requis d'environnement sont présents.
- Le domaine interne se nomme masociete.lan et le serveur Direct Access (nommé DA1) est intégré au domaine.
- Le serveur Direct Access possède une interface publique possédant les adresses 131.107.0.2 et 131.107.0.3.
- Le serveur Direct Access possède une interface privée possédant l'adresse 192.168.0.2.
- Un certificat de type Web a été installé sur le serveur Direct Access avec un nom convivial : IP-HTTPS.
- Un groupe DA_Clients a été créé sur le domaine et la machine cliente Direct Access en est membre. Ce groupe servira à définir les machines autorisées à se connecter grâce à Direct Access.

Voici les étapes à suivre pour installer Direct Access :

- Dans la console **Gestionnaire de serveur**, sélectionnez **Rôles** puis dans le volet droit cliquez sur **Ajouter des rôles** et sur **Suivant**.
- Cochez la case **Serveur Web** (**IIS**) puis cliquez sur **Suivant** trois fois et enfin sur **Installer**.
- Une fois l'installation finalisée, cliquez sur **Fermer**.
- Toujours dans la console **Gestionnaire de serveur**, sélectionnez **Fonctionnalités** puis dans le volet droit cliquez sur **Ajouter des fonctionnalités**.
- Sélectionnez **Console de gestion DirectAccess** puis cliquez sur **Suivant**.

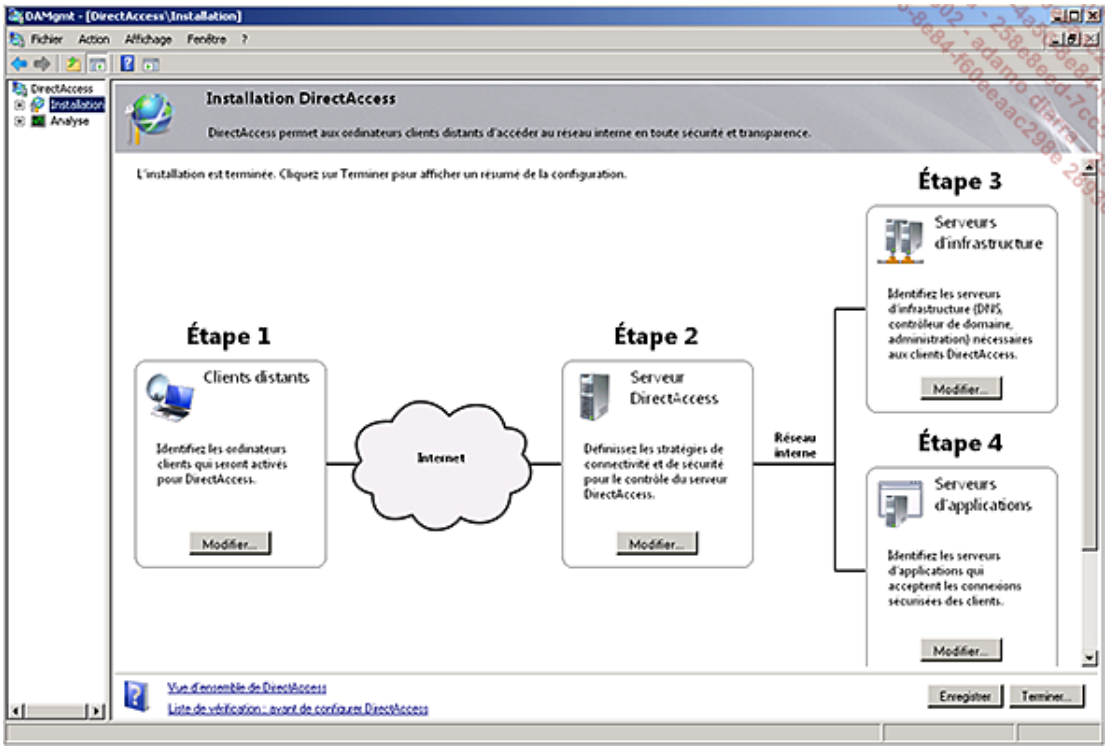
© ENI Editions - All rights reserved - adamo diarra



- Cliquez sur **Installer** et une fois l'installation finalisée, cliquez sur **Fermer**.

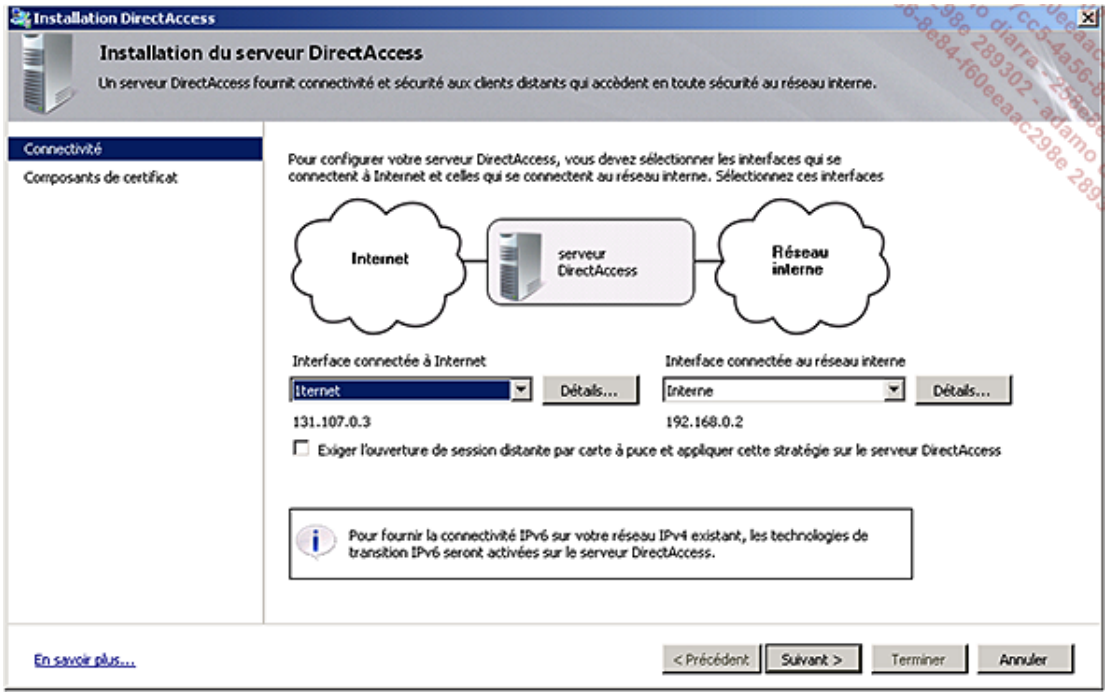
Il est maintenant temps de configurer la fonctionnalité Direct Access :

- Dans les **Outils d'administration**, cliquez sur **Gestion DirectAccess**.
- Sélectionnez le nœud **Installation** dans le volet gauche.



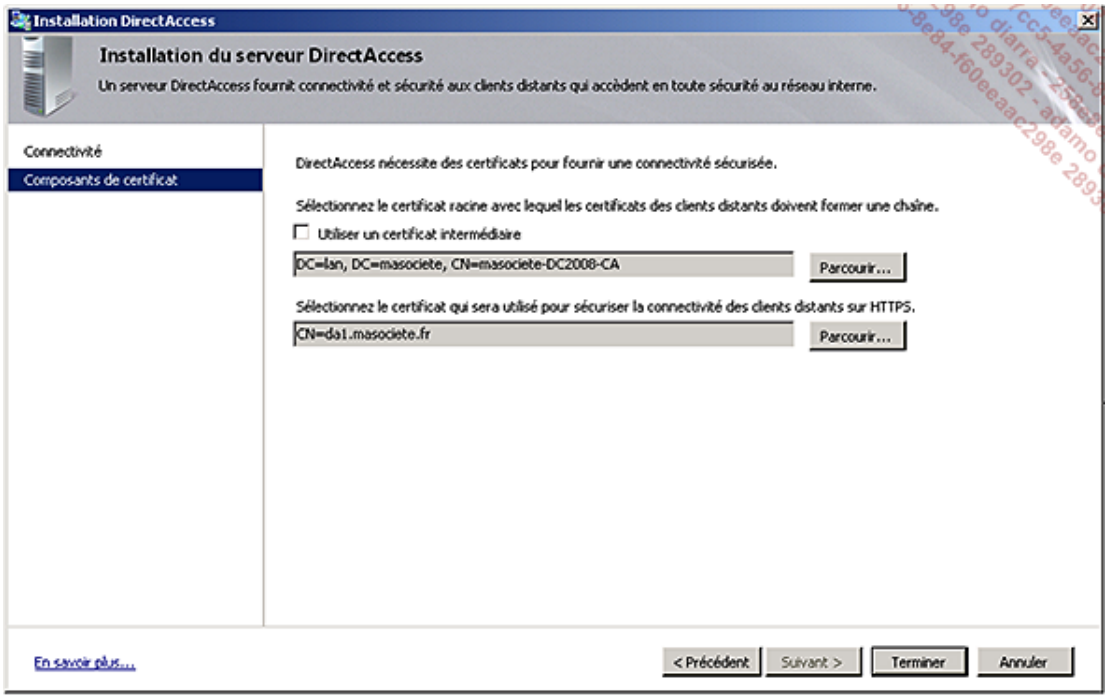
© ENI Editions - All rights reserved - adamo diarra

- Dans le volet central, cliquez sur le bouton **Modifier** de l'étape 1.
- Ajoutez le groupe *DA_Clients* puis cliquez sur **Terminer**.
- Dans le volet central, cliquez sur le bouton **Modifier** de l'étape 2.
- Sélectionnez les interfaces en fonction du réseau auquel elles sont connectées (Internet et Interne).



- Cliquez sur **Suivant**.
- Cliquez sur le premier bouton **Parcourir** pour sélectionner le certificat de l'autorité de certification Interne.
- Cliquez sur le second bouton **Parcourir** pour sélectionner le certificat utilisé pour sécuriser la connexion avec les clients distants (IP-HTTPS).

© ENI Editions - All rights reserved - adamo diarra

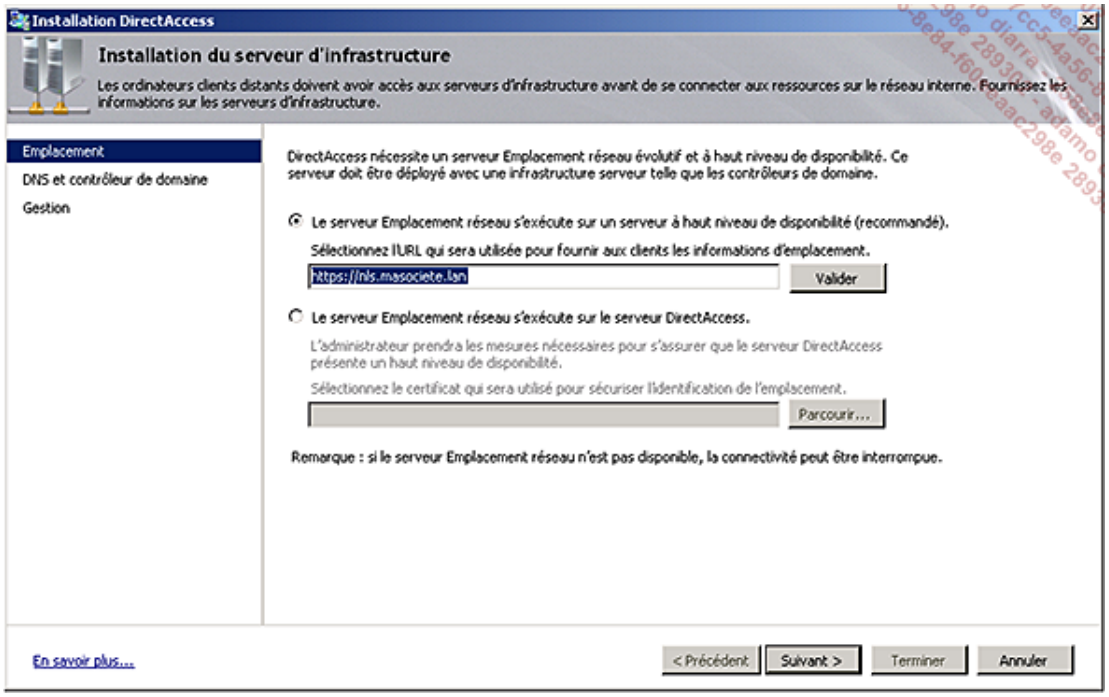


- Cliquez sur **Terminer**.

- Dans le volet central, cliquez sur le bouton **Modifier** de l'étape 3.

- Saisissez l'URL correspondant à un serveur Intranet (c'est cette URL qui permettra au client de déterminer s'il se trouve ou non au sein du réseau interne et s'il doit établir ou pas la connexion Direct Access).

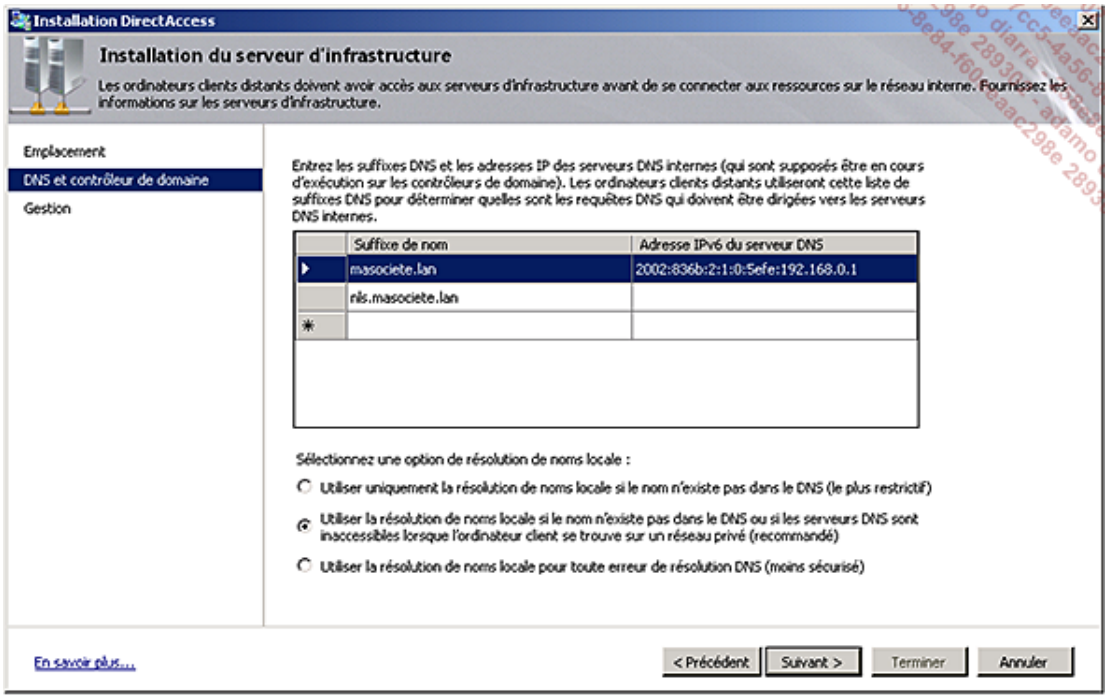
  Vous pouvez voir qu'il est également possible que le serveur Direct Access joue ce rôle.



- Cliquez sur **Suivant**.

- Choisissez le mode de résolution de noms en fonction de vos besoins, ici laissez le choix par défaut.

© ENI Editions - All rights reserved - adamo diarra



- Cliquez sur **Suivant**.

- Saisissez les adresses IP des serveurs pouvant gérer à distance le composant Direct Access puis cliquez sur **Terminer**.

- Dans le volet central, cliquez sur le bouton **Modifier** de l'étape 4.

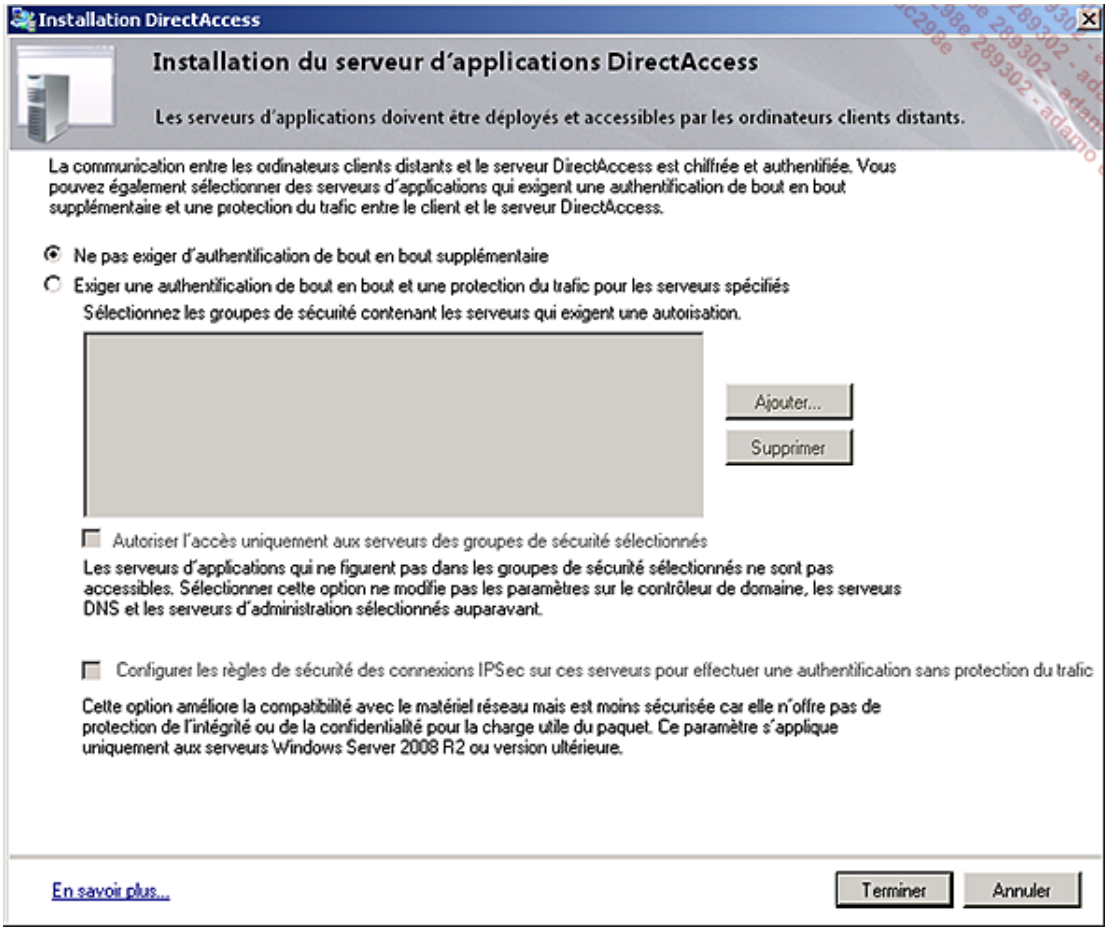
- Spécifiez les serveurs avec lesquels vous souhaitez que le chiffrement du trafic soit effectué de bout en bout (par défaut le chiffrement est effectué entre le client et le serveur Direct Access uniquement).

  Vous pouvez également restreindre les accès Direct Access uniquement aux serveurs spécifiés plutôt qu'à tous les serveurs internes.

  Pour plus de précisions, le chapitre Sécuriser votre architecture revient sur les différents types de tunnel IPsec.

- Cliquez sur **Terminer**.

© ENI Editions - All rights reserved - adamo diarra



- Cliquez ensuite sur **Enregistrer** puis sur **Terminer** en bas du volet central.

Il ne reste plus qu'à tester depuis un poste client en accédant à un serveur Web interne ou encore tout simplement au dossier SYSVOL du domaine (\\masociete.lan\sysvol).

Un guide de débogage est disponible (uniquement en anglais au moment de l'écriture de ce livre) sur le site de Microsoft à l'adresse : http://technet.microsoft.com/en-us/library/ee624056(WS.10).aspx.

Attention, si vous souhaitez réaliser cette maquette sur un serveur Hyper-V, il vous faudra positionner les cartes réseaux du serveur Direct Access en tant que carte héritée (ou Legacy) si vous rencontrez des problèmes de flux.

Vous venez de voir dans ce chapitre que pour fournir un accès à distance à vos utilisateurs, il vous faut configurer un serveur d'accès distant. Quand vos utilisateurs se trouvent en dehors de l'entreprise ils peuvent accéder aux ressources internes en utilisant soit une connexion de type Dial-up, soit une connexion VPN, soit Direct Access.

Windows Server 2008 R2 sait gérer les deux premières solutions. Il apporte également avec SSTP une mobilité accrue. Grâce à l'encapsulation du trafic VPN dans HTTPS vous évitez les contraintes de connexion liées à la sécurité sortante sur les pare-feu des réseaux dans lesquels vous vous situez.

Avec le couple Windows Server 2008 R2 Windows 7, vous fournirez à vos utilisateurs ce que nombre d'entre eux réclame : travailler hors du bureau comme au bureau.

Windows Server 2008 R2 vous permet également avec ses nouvelles stratégies d'accès de définir de façon très précise qui se connecte, quand et de quelle façon.

Si vous souhaitez centraliser la sécurité des connexions de vos équipements réseaux, Windows Server 2008 R2 assurera le rôle de concentrateur grâce à ses fonctions RADIUS.

© ENI Editions - All rights reserved - adamo diarra

Mettre en place un serveur Intranet/Internet

Dans ce chapitre vous apprendrez à installer et configurer un serveur Web grâce au rôle de serveur IIS (*Internet Information Services*).

1. Présentation d'IIS 7

a. Présentation générale

IIS 7.5 (*Internet Information Services*) est la dernière version du serveur Web de Microsoft. Inclus en version complète avec Windows Server 2008 R2, il fournit une plate-forme sécurisée et facile à administrer pour pouvoir héberger des services Web ainsi que des applications Web enrichies. Windows Server 2008 fournit IIS en version 7.

Dans cette septième version, IIS permet d'héberger et de gérer la plupart des langages utilisés sur le Web allant de l'ASP.NET au PHP. Sa rétrocompatibilité permet de migrer aisément vos sites Web hébergés sur les versions précédentes de IIS sans rencontrer de problème.

IIS 7 / 7.5 offrent des fonctionnalités différentes en fonction du système d'exploitation. Tout comme IIS 6, ils peuvent être installés sur le système d'exploitation client (Windows Vista/Windows 7) en version allégée. Windows Vista, Windows 7 et Windows Server 2008/2008 R2 partageant le même noyau, il est donc facile de développer des applications depuis son poste de travail pour ensuite les faire héberger par un serveur. Décliné en édition Web, Windows Web Server 2008 R2 propose lui aussi une plate-forme Web complète basée sur IIS 7.5. Moins cher que les autres éditions, Windows Web Server 2008 R2 supporte jusqu'à 32 Go de mémoire vive (sur un système non 32 bits, qui est limité à 4 Go) et jusqu'à 4 processeurs.

IIS 7 peut également être installé en mode Core mais il faut garder à l'esprit qu'aucun site développé en ASP.NET ne pourra être publié dans ce cas. En effet, le mode Core de Windows Server 2008 ne permet pas l'installation du .NET Framework pour des raisons de sécurité. Cependant, sachez qu'il est possible d'installer le .NET Framework 2.0 et 3.0 en mode Core sur un Windows Server 2008 R2 avec IIS 7.5. La version R2 permet également d'installer un FTP sécurisé et les fonctionnalités Webdav.

b. Nouvelle architecture

L'architecture d'IIS a été repensée afin de faciliter l'implémentation des fonctionnalités et donc l'extension des possibilités du serveur. Sous IIS 6, la structure était composée d'un seul bloc ce qui obligeait à tout installer pour utiliser le serveur Web. Avec IIS 7 / 7.5, les fonctionnalités ont été découpées de façon à pouvoir charger les modules en correspondance avec les besoins.

Ces modules sont découpés en cinq catégories pour la partie **Serveur Web**.

- Fonctionnalités HTTP communes (contenu statique, documents par défaut, etc.).
- Développement d'applications (prise en charge de : ASP.NET, ASP, CGI, etc.).
- Intégrité et diagnostics (journalisation, observateur de demandes, suivi, etc.).
- Sécurité (authentification de base, authentification Windows, autorisation Digest, etc.).
- Performances (compression de contenu statique ou dynamique).

Pour la partie **Outils de gestion**, on retrouve :

- la console de gestion de IIS ;
- les scripts et outils de gestion de IIS ;
- le service de gestion ;
- la gestion de la compatibilité avec IIS 6.

Le service FTP (*File Transfer Protocol*) est séparé de la partie serveur Web car il s'agit désormais d'un service de rôle à

© ENI Editions - All rights reserved - adamo diarra

part entière. Les modules Serveur FTP et Console de gestion FTP lui sont associés.

c. Nouvelle administration

IIS 7 / 7.5 diffèrent de leurs versions précédentes par la mise en place d'une nouvelle administration. La nouvelle console de gestion qui centralise l'administration de l'ensemble des modules du serveur n'est plus un simple composant enfichable. En effet, il s'agit d'une console à part entière qui se connecte sur le service d'administration.

La configuration a également changé. Sous IIS 6, elle était stockée dans une métabase au format XML. IIS 7 / 7.5 facilitent l'implémentation et surtout la maintenance des serveurs, en découpant cette configuration dans plusieurs fichiers XML :

- **applicationHost.config** : contient la configuration globale (liste des sites, pools d'applications, paramètres par défaut, etc.).
- **Redirection.config** : contient les informations de redirection (utilisé par exemple quand le contenu du site se trouve sur un autre serveur ou encore lorsqu'une partie du site ne doit pas être disponible en cas de maintenance, etc.).
- **Web.config** : contient la configuration globale ASP.NET du serveur (un fichier individuel peut être créé pour chaque site qui a besoin d'une configuration spécifique ; ceci est utile lorsque vous devez spécifier des paramètres différents de la configuration globale du serveur). Cela permet ainsi de gérer plus finement les paramétrages de sites Web.
- **Machine.config** : contient les propriétés requises pour les fonctionnalités Framework.

---

applicationHost.config et redirection.config sont stockés à l'emplacement : %windir%\system32\inetsrv\config. Le fichier web.config de premier niveau est lui situé à l'emplacement : C:\inetpub\wwwroot. Autrement, les fichiers web.config et machine.config se trouvent dans le dossier %windir%\Microsoft.NET\Framework\version_framework\CONFIG.

Il existe une hiérarchie avec ces différents fichiers de configuration une hiérarchie. Celle-ci définit un héritage des paramètres tout comme le feraient des droits de sécurité NTFS. Cette hiérarchie commence par le fichier **machine.config** puis suit l'ordre suivant : **web.config** (celui de premier niveau), **applicationHost.config** et enfin un fichier web.config optionnel situé à l'emplacement du site ou du répertoire virtuel. De cette façon, les propriétés sont héritées du fichier **machine.config** au dernier fichier **web.config** de l'arborescence.

Le stockage de la configuration des sites dans des fichiers XML distincts (aussi appelée configuration distribuée) permet ainsi de faciliter le déploiement ou la copie d'applications. Vous pouvez copier les applications entre des serveurs frontaux grâce à un simple *xcopy* en évitant toute erreur due à une réplication ou une quelconque synchronisation.

Les tâches administratives sont désormais automatisables grâce notamment à PowerShell, un nouveau fournisseur WMI, une nouvelle API.NET mais surtout grâce à l'outil AppCMD. AppCMD.exe permet de réaliser la majorité des tâches d'administration à l'aide d'une syntaxe simple.

L'administration peut également être déléguée. Vous pouvez spécifier quelles sont les fonctionnalités que les utilisateurs non administrateur sont en mesure de gérer. Il est ainsi possible par exemple de configurer les paramètres ASP.NET d'un site sans pour user de privilèges administrateur.

d. Nouveautés incluses avec IIS 7.5 dans Windows Server 2008 R2

Comme vu précédemment, Windows Server 2008 R2 propose IIS en version 7.5. Cette version apporte un certains nombre d'améliorations attendues par rapport à la version précédente, mais aussi quelques nouveautés.

Intégration d'extensions

- Webdav, désormais intégré en temps que fonctionnalité. Avant elle était disponible comme une extension à part.
- UrlScan (filtrage de requêtes) : fournit la possibilité de restreindre ou de carrément bloquer des requêtes HTTP.
- Packs d'administration des modules : administration des bases de données, *URL rewriting*, éditeur de configuration, etc.

© ENI Editions - All rights reserved - adamo diarra

Amélioration de la gestion

- Intégration dans l'interface de l'outil Best Practices Analyzer.
- Ajout de commandes PowerShell et de cmdlets.
- Configuration de la journalisation et du traçage.
- Outil de déploiement de sites Web (migration de sites, applications, serveurs entier).
- Nouveaux compteurs de performances.
- Webdav et FTP ont été améliorés. Il est désormais plus facile et plus sécurisé de publier du contenu.
- Les fonctionnalités d'authentification, d'audit et de journalisation sont également plus nombreuses.

Amélioration de l'intégration et de l'hébergement d'applications

- Support d'Asp.NET et du Framework en mode Core (leur absence était considérée comme une grosse lacune par les professionnels de l'informatique).
- Gestion des comptes de services (chaque pool d'applications dispose désormais d'une identité unique).
- Analyse et suivi des erreurs de requête FastCGI facilitant le débogage pour les développeurs.

Publication de sites via Visual Studio 10 en un seul clic

2. Installation du rôle Serveur Web (IIS) en mode console

Avant que vous vous lanciez dans l'installation, il est important que vous connaissiez la liste des modules non disponibles avec le mode Core de Windows Server 2008 R2 :

- IIS-ManagementConsole
- IIS-LegacySnapIn
- IIS-FTPManagement

Pour installer IIS en mode Core, il vous faut utiliser l'exécutable **pkgmgr.exe**.

a. Installation par défaut

Pour réaliser une installation par défaut sur un Windows Server 2008 R2 en mode Core, utilisez la commande ci-dessous :

```
start /w pkgmgr /l:log.etw /iu:IIS-WebServerRole;WAS-WindowsActivationService;
WAS-ProcessModel;WAS-NetFxEnvironment;WAS-ConfigurationAPI
```

b. Installation complète

Pour réaliser une installation complète d'IIS 7.5 (avec toutes les fonctionnalités) sur un serveur Core Windows Server 2008 R2, utilisez la commande suivante :

```
start /w pkgmgr /l:log.etw /iu:IIS-WebServerRole;IIS-WebServer;IIS-
CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-
DirectoryBrowsing;IIS-
HttpErrors;IIS-HttpRedirect;IIS-ApplicationDevelopment;
```

© ENI Editions - All rights reserved - adamo diarra

```
IIS-ASP;IIS-CGI;IIS-
ISAPIExtensions;IIS-ISAPIFilter;IIS-ServerSideIncludes;
IIS-HealthAndDiagnostics;
IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-
HttpTracing;IIS-
CustomLogging;IIS-ODBCLogging;IIS-Security;IIS-BasicAuthentication;IIS-
WindowsAuthentication;IIS-DigestAuthentication;IIS-
ClientCertificateMappingAuthentication;
IIS-IISCertificateMappingAuthentication;IIS-URLAuthorization;IIS-Request
Filtering;
IIS-IPSecurity;IIS-Performance;IIS-HttpCompressionStatic;IIS-
HttpCompressionDynamic;
IIS-WebServerManagementTools;IIS-ManagementScriptingTools;IIS-
IIS 6ManagementCompatibility;
IIS-Metabase;IIS-WMICompatibility;IIS-LegacyScripts;WAS-
WindowsActivationService;
WAS-ProcessModel;IIS-FTPServer;IIS-FTPSvc;IIS-FTPExtensibility;
IIS-WebDAV;IIS-ASPNET;IIS-NetFxExtensibility;WAS-NetFxEnvironment;
WAS-ConfigurationAPI;
IIS-ManagementService;MicrosoftWindowsPowerShell
```

Là encore, la différence entre les deux commandes est principalement due au support d'ASP.NET et du Framework en version R2.

Les fonctionnalités supplémentaires sont : IIS-FTPExtensibility, IIS-WebDAV, IIS-ASPNET, IIS-NetFxExtensibility, WAS-NetFxEnvironment, WAS-ConfigurationAPI, IIS-ManagementService, MicrosoftWindowsPowerShell.

On constate également l'intégration de Webdav en temps que fonctionnalité, ainsi que l'amélioration du service FTP et de la gestion d'IIS.

Vous pourrez vérifier que le rôle a bien été installé en utilisant la commande `oclist`. En la lançant vous verrez la liste des rôles de serveur disponibles. Pour chacun d'eux vous verrez mentionné *Installé* ou *Non Installé*. Pour les serveurs de rôle installés, un sous-arbre est représenté avec l'état d'installation de chaque service de rôle.

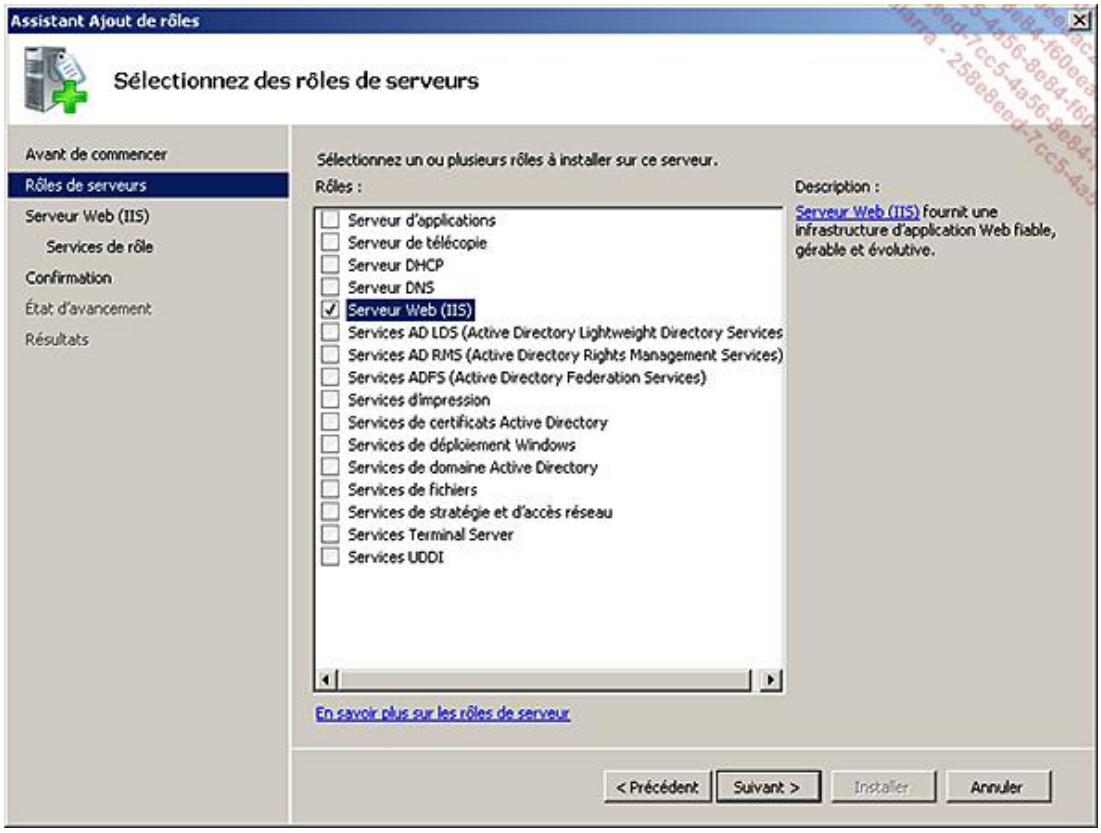
3. Installation du rôle Serveur Web (IIS) en mode graphique

L'installation du rôle se fait depuis la console **Gestionnaire de serveur**, dans le sous-dossier **Rôles**, en cliquant sur **Ajouter des rôles**.

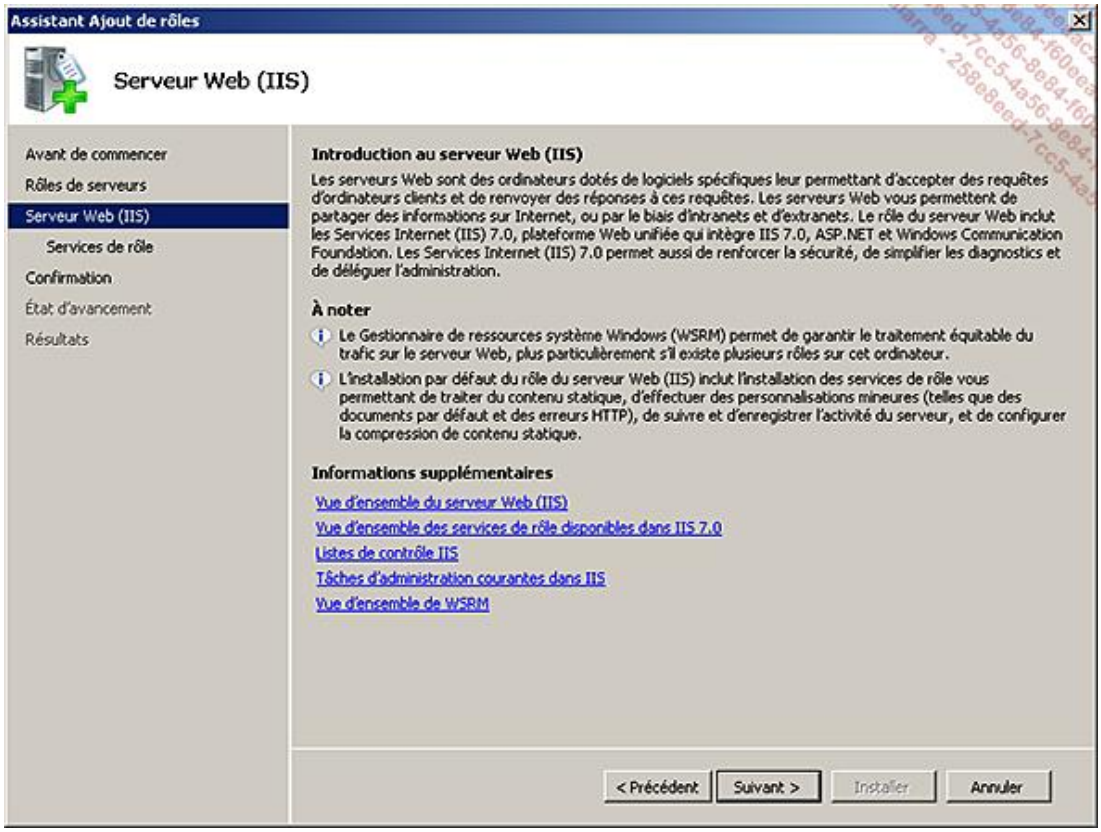
Voici les différentes étapes :

- Ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer - Outils d'administration** puis **Gestionnaire de serveur**.
- Au niveau de **Résumé des rôles**, cliquez sur **Ajouter des rôles**.
- Cliquez sur **Suivant**.
- Cochez la case **Serveur Web (IIS)** comme ci-dessous puis cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra

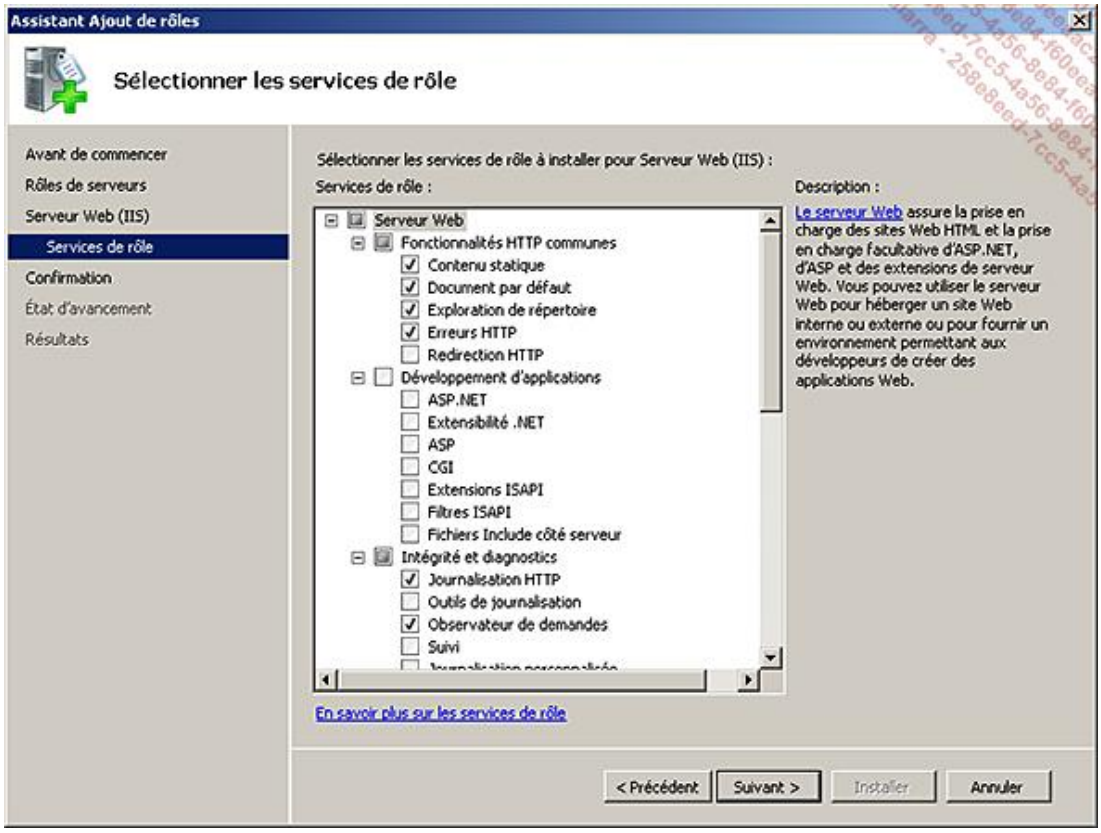


- Lisez la page d'introduction puis cliquez sur **Suivant**.

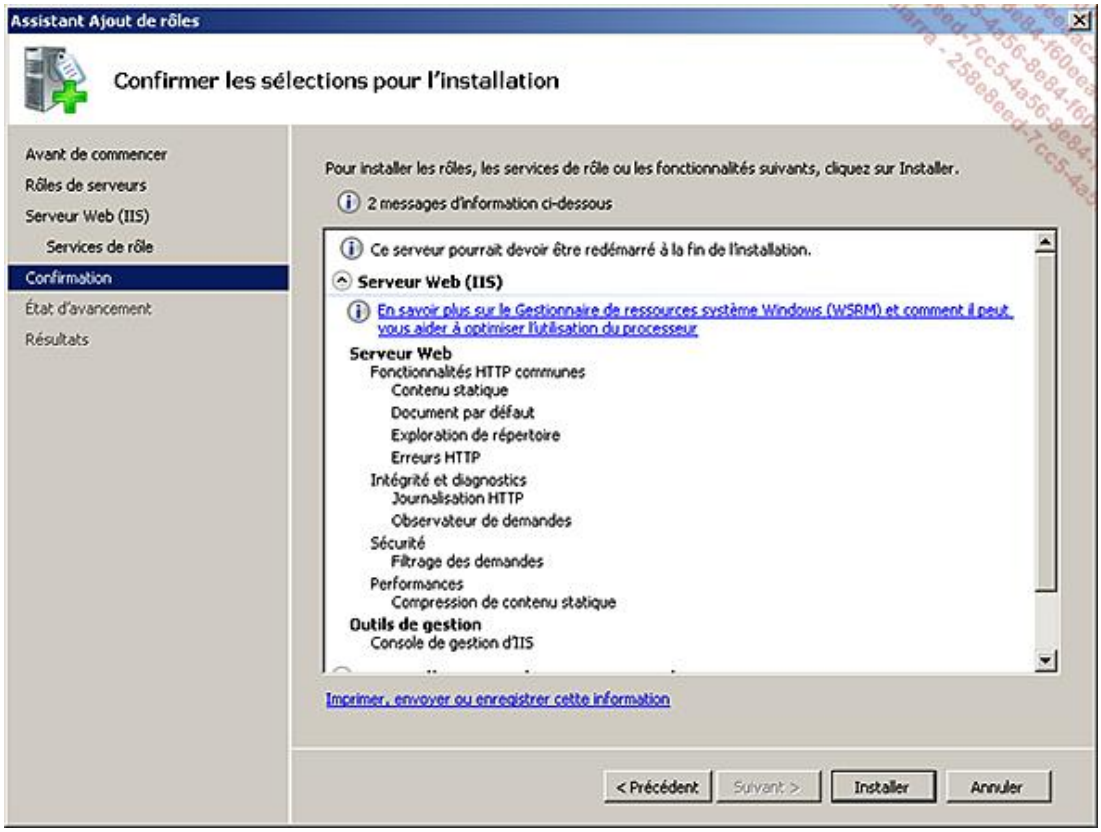


- Dans l'exemple en cours, vous n'utiliserez que les fonctions de base de IIS. Laissez les cases cochées par défaut puis cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra

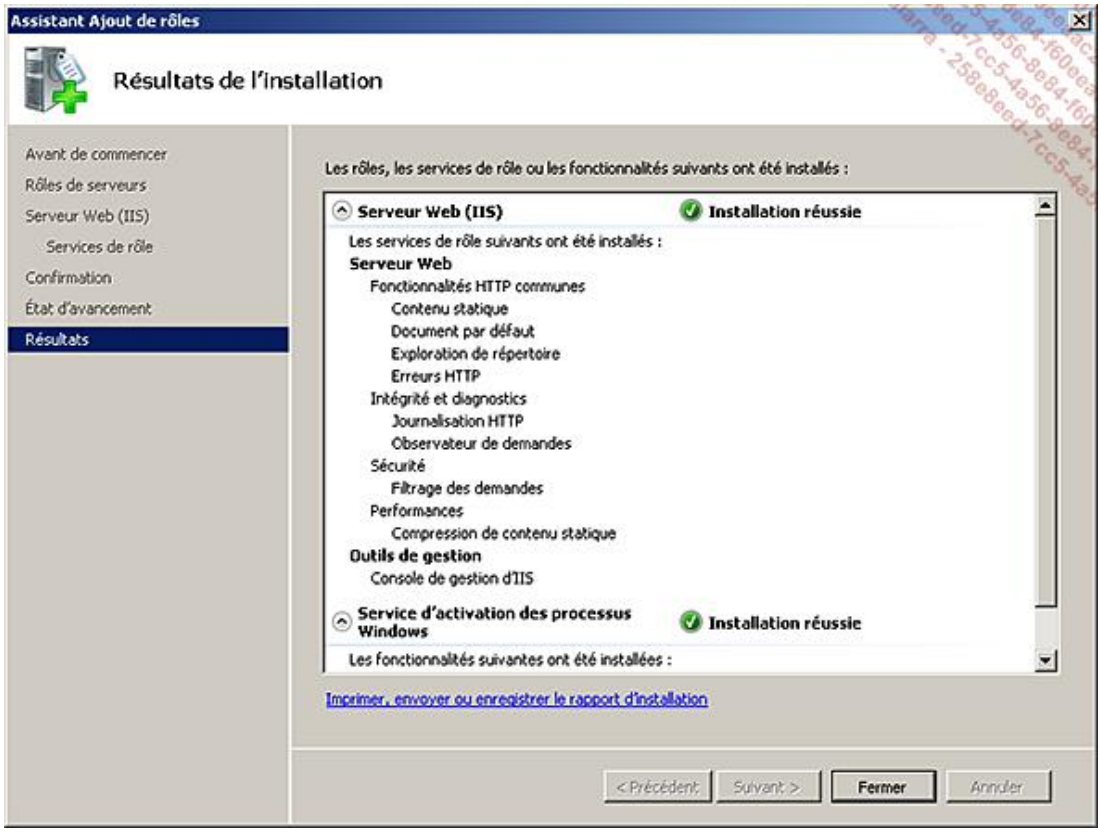


- Vérifiez les options choisies puis cliquez sur **Installer**.



- Vérifiez que l'installation s'est bien déroulée puis cliquez sur **Fermer**.

© ENI Editions - All rights reserved - adamo diarra



- Pour vérifier que IIS 7 / 7.5 est bien opérationnel, ouvrez Internet Explorer puis dans la barre d'adresse saisissez l'URL : http://localhost.

  Vous devriez voir apparaître la fenêtre suivante :

© ENI Editions - All rights reserved - adamo diarra

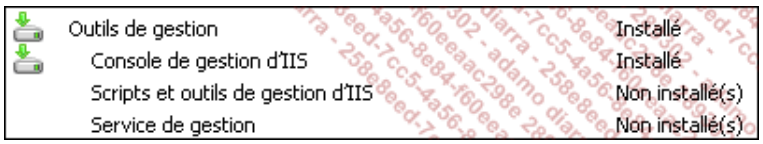
© ENI Editions - All rights reserved - adamo diarra

Monter un site Web

Maintenant que vous avez installé votre rôle de **Serveur Web (IIS)**, vous allez voir comment créer de nouveaux sites et les gérer facilement. Dans ce chapitre vous configurerez un site pour votre société (le contenu du site sera minimal, le but de ce livre n'étant pas de vous former aux langages de développement Web).

1. Création et configuration d'un site

Avec Windows Server 2008 R2, la gestion d'IIS est réalisée dans une console dédiée. Ainsi si vous regardez dans votre **Gestionnaire de serveur**, dans la section **Services de rôle de IIS** vous pouvez voir le service **Console de gestion d'IIS**.

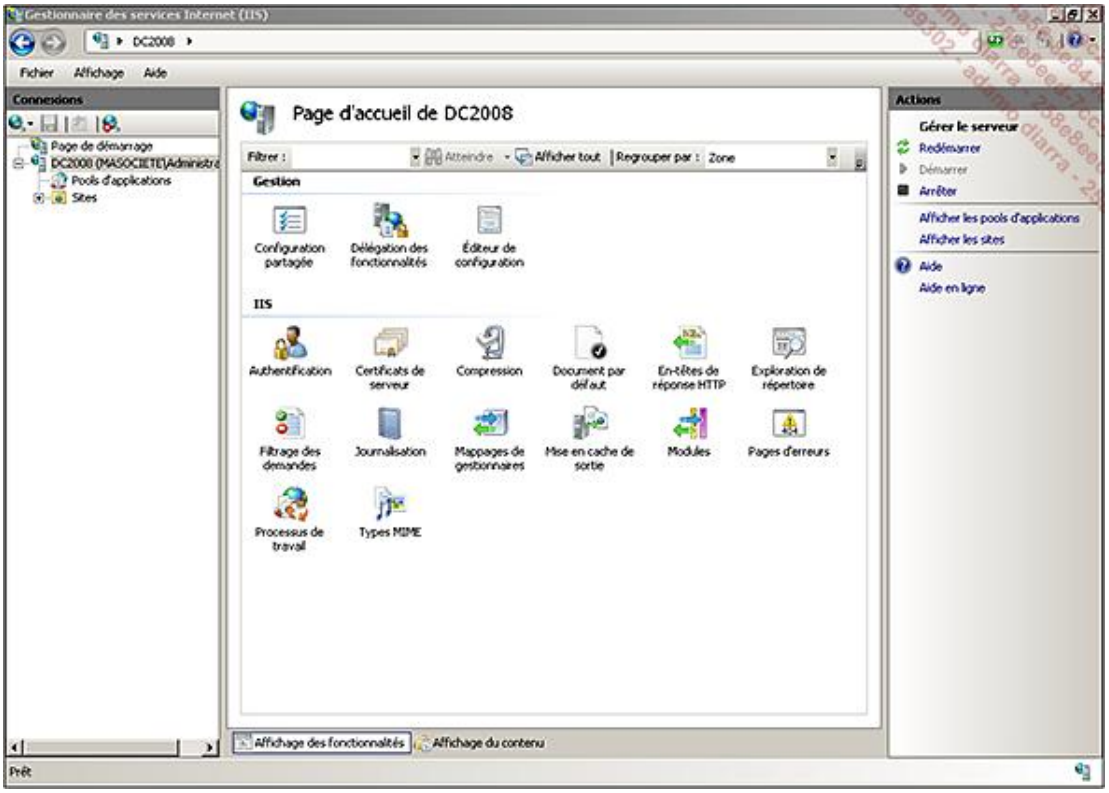


Pour atteindre cette console :

- Allez dans **Démarrer - Tous les programmes - Outils d'administration** et cliquez sur **Gestionnaire de services Internet (IIS)**.

  Par défaut la console de gestion d'IIS se connecte au serveur local. Cela vous permet de changer la configuration et les paramètres de ce serveur.

- Dans le volet de gauche, cliquez ensuite sur le nom de votre serveur (ici DC2008) pour faire apparaître la liste des fonctionnalités disponibles.



Par défaut, l'affichage regroupe les fonctionnalités par **Zone**. Vous pouvez changer cet affichage grâce à la liste déroulante située en haut du volet central. Il est ainsi possible de regrouper par **Zone** (par défaut), par **Catégorie** ou encore de ne pas utiliser de regroupement.

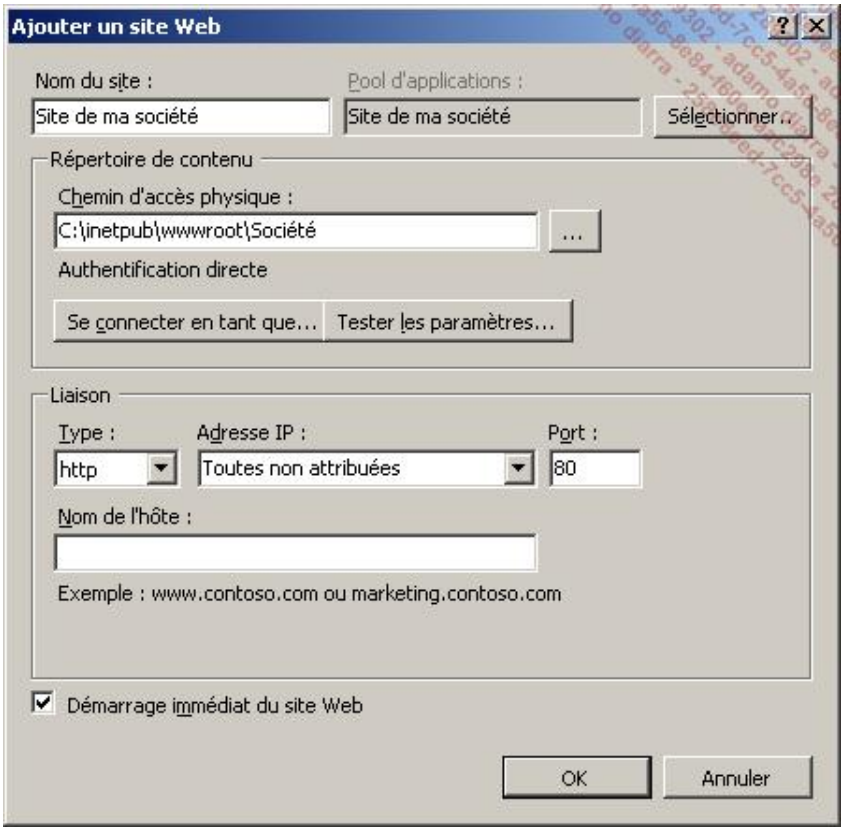
Voici les différentes étapes pour créer un nouveau site :

Pré-requis : vous devez créer un répertoire *Société* dans le dossier **C:\inetpub\wwwroot**.

© ENI Editions - All rights reserved - adamo diarra

- Toujours dans la console **Gestionnaire des services Internet (IIS)**, faites un clic avec le bouton droit de la souris sur le nom de votre serveur puis cliquez sur **Ajouter un site Web**. (La même opération peut être réalisée depuis plusieurs endroits. Par exemple directement depuis la sous-arborescence **Sites**).

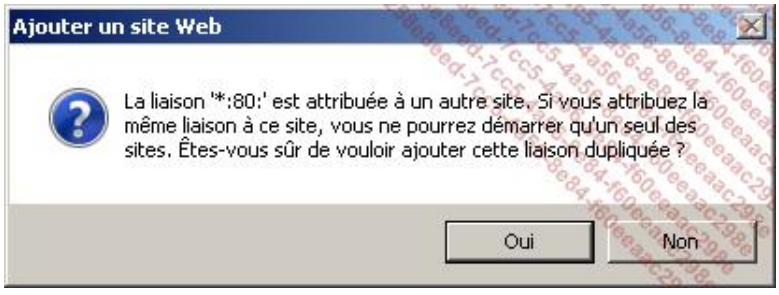
- Remplissez la fenêtre comme ci-dessous :



Le nom du site est purement informatif, les espaces ne poseront pas de problème à l'utilisation.

Dans cet exemple, ne remplissez pas le nom de l'hôte et laissez les paramètres de liaison par défaut. Ces paramètres de liaison servent à définir sur quel port et/ou avec quel nom vous accédez au site (vous trouverez plus de détails dans la sous-partie suivante de ce chapitre).

- Une fois les champs remplis, cliquez sur **OK**. Le message suivant apparaît :



La raison de ce message est qu'IIS héberge déjà un site utilisant le port 80 sur la même adresse IP. Il s'agit du site Web par défaut. Il n'est pas possible pour une seule adresse IP et un seul port d'avoir plusieurs sites Web (sauf en cas d'utilisation des en-têtes HTTP. Ce point est abordé dans la section suivante de ce chapitre).

Si vous essayez tout de même de démarrer le site Web vous serez confronté à un message d'erreur. Pour le constater, suivez la procédure ci-après :

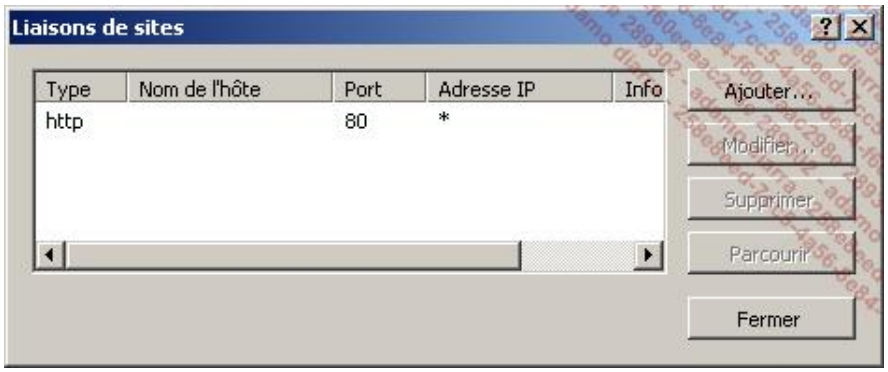
- Dans le volet central, sélectionnez votre site Web puis, dans le volet de droite, cliquez sur le bouton **Démarrer**. Vous obtenez le message ci-dessous.

© ENI Editions - All rights reserved - adamo diarra

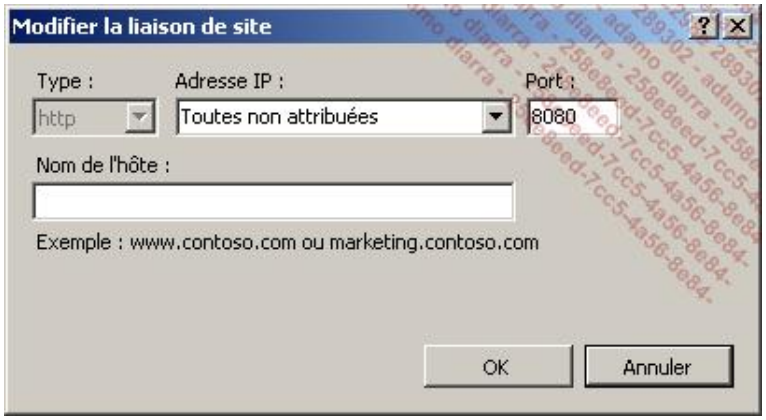
Pour les besoins de l'exemple, vous allez changer le port sur lequel ce site Web va écouter.

- Dans le volet de gauche, étendez l'arborescence **Sites** pour faire apparaître le site que vous venez de créer, puis sélectionnez-le.

- Dans le volet de droite, dans la rubrique **Actions**, cliquez sur **Liaisons**.



- Sélectionnez la liaison HTTP puis cliquez sur **Modifier**.



- Saisissez **8080** dans le champ **Port** puis cliquez sur **OK** pour valider puis sur **Fermer**.

- Dans le volet des actions, cliquez sur **Démarrer**.

- Il vous faut désormais un document à afficher dans votre site. Pour le créer, ouvrez l'éditeur Notepad puis saisissez le code suivant :

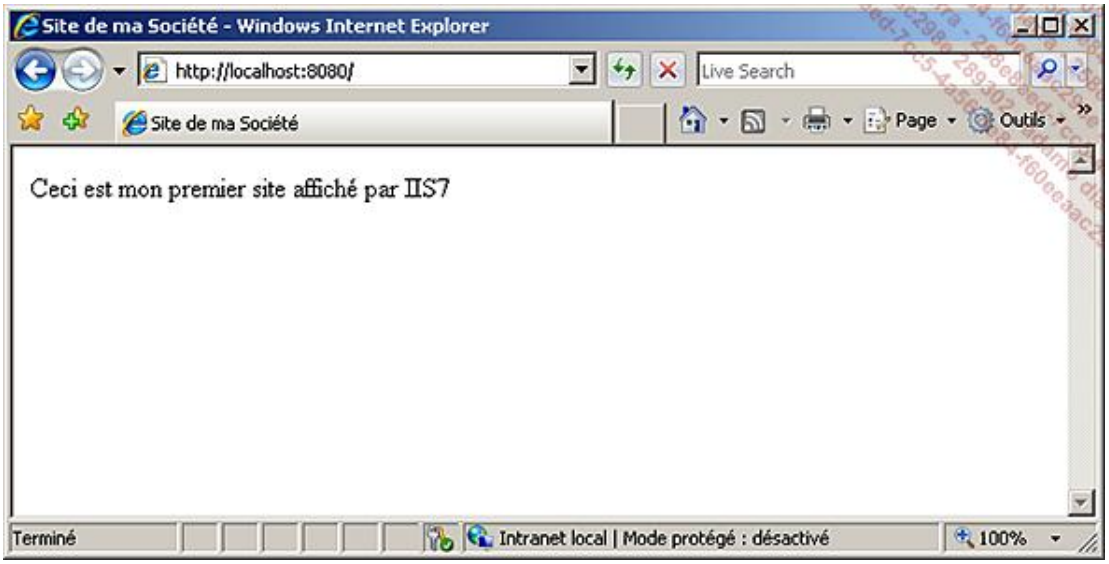
```
<HTML>
<head>
    <Title>Site de Ma société</Title>
</head>

<body>
    Ceci est mon premier site affiché par IIS7
```

© ENI Editions - All rights reserved - adamo diarra

```
</body>
</HTML>
```

- Enregistrez ensuite le fichier à l'emplacement : C:\inetpub\wwwroot\Société\default.htm

- Pour tester le fonctionnement, ouvrez Internet Explorer puis saisissez l'adresse http://localhost:8080.



2. Mise à jour du domaine DNS

Bien que l'on puisse utiliser des ports d'écoute différents pour chaque site, dans la pratique ce n'est pas une solution viable lorsque plusieurs sites sont hébergés sur un même serveur. Ce problème se pose tout particulièrement pour des sites Web publics. Les internautes ne savent pas sur quel port est configuré votre site Web et il n'est donc pas envisageable de leur demander d'indiquer un port particulier afin de pouvoir accéder au site Internet.

Une des solutions permettant de contourner ce problème de ports est de configurer plusieurs adresses IP sur votre serveur Web. Chaque IP est ensuite associée à un site unique. Si cette solution peut faire l'affaire pour une utilisation interne, elle se révèle très coûteuse pour une utilisation publique (les adresses IP fixes sur Internet représentent un investissement et sont fournies en quantité limitée).

Pour pouvoir gérer de façon efficace l'hébergement de nombreux sites Web, il vous faut faire appel aux **en-têtes d'hôte**. Ces en-têtes d'hôte permettent l'utilisation de plusieurs noms d'hôtes pour une seule adresse IP. IIS va écouter les demandes entrantes et regarder les informations envoyées par le navigateur. En fonction du nom d'hôte reçu, il redirige la requête du navigateur vers le site Web correspondant.

Vous allez, dans l'exemple qui suit, configurer le site créé à l'étape précédente pour écouter sur l'adresse www.masociete.fr.

Pré-requis : avoir un serveur DNS fonctionnel qui héberge la zone masociete.fr. Avoir dans cette zone un enregistrement de type A appelé **www** et qui pointe sur l'IP 192.168.0.1 (l'adresse IP de votre serveur Web).

Consultez le chapitre Mise en place des services réseaux d'entreprise - La mise en place des systèmes de résolutions de nom.

- Allez dans la console **Gestionnaire des services Internet (IIS)**.

- Développez l'arborescence **Sites** pour faire apparaître le site créé lors de la sous-partie précédente de ce chapitre (site de ma société).

- Sélectionnez votre site puis dans le volet de droite cliquez sur **Liaisons**.

- Dans la fenêtre **Liaisons de sites** cliquez sur **Ajouter**.

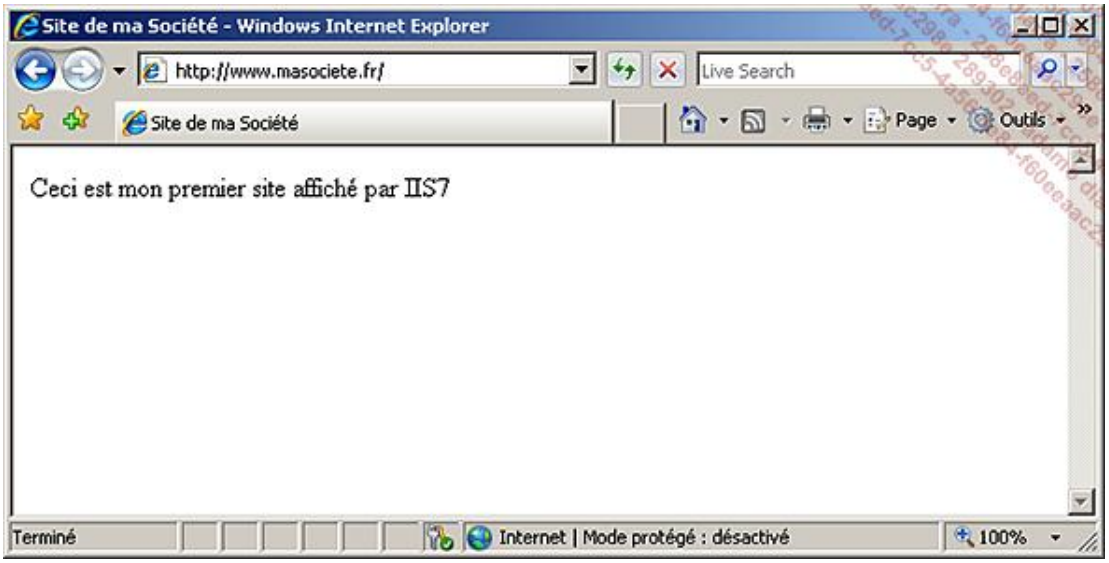
- Remplissez les champs comme ci-dessous :

© ENI Editions - All rights reserved - adamo diarra

- Validez en cliquant sur **OK** puis sur **Fermer**.

Vous pouvez tout aussi bien modifier la liaison existante pour spécifier ces paramètres. Cependant grâce à cet exemple vous constatez que l'on peut affecter des ports différents sur un même site et même des noms d'hôte différents.

- Testez ensuite la modification en ouvrant Internet Explorer et en saisissant l'adresse www.masociete.fr dans la barre d'adresse.



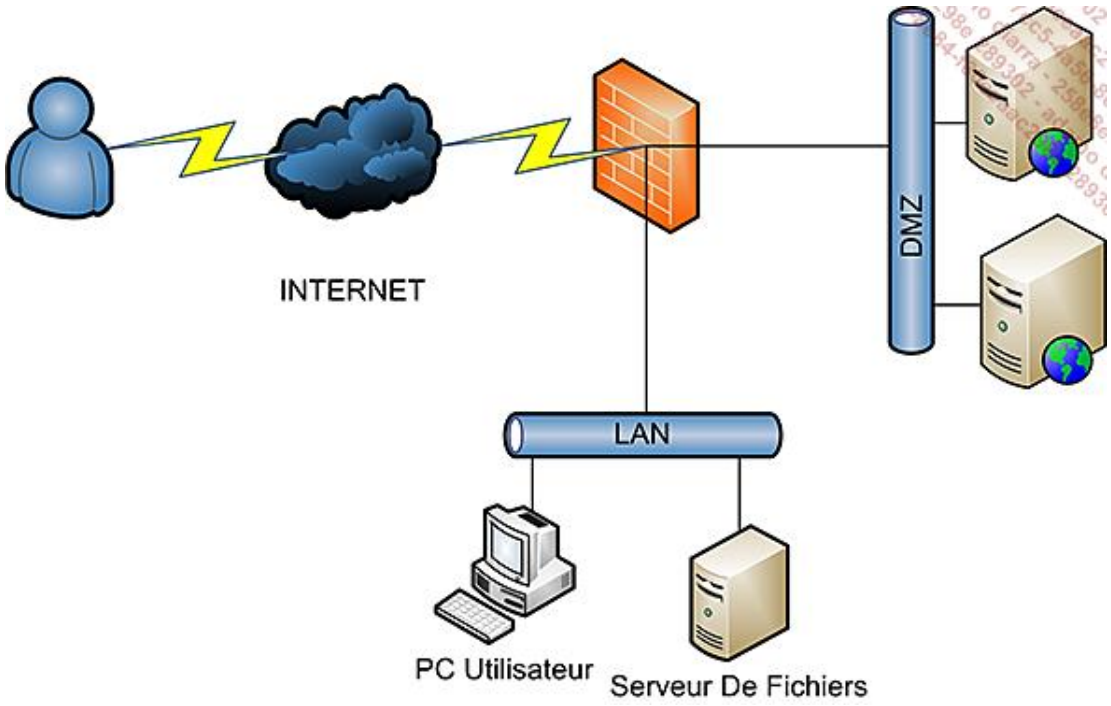
Chaque nom d'hôte que vous souhaitez utiliser pour IIS a besoin d'exister. Pour un site intranet, il vous suffit de rajouter des enregistrements dans votre zone DNS de domaine. Pour une utilisation publique, il vous faut le gérer sur la zone DNS publique. Soit vous avez accès à une interface d'administration qui vous le permet, soit vous devez demander au gestionnaire de votre zone DNS de créer les enregistrements en conséquence.

3. Mise en place d'une DMZ

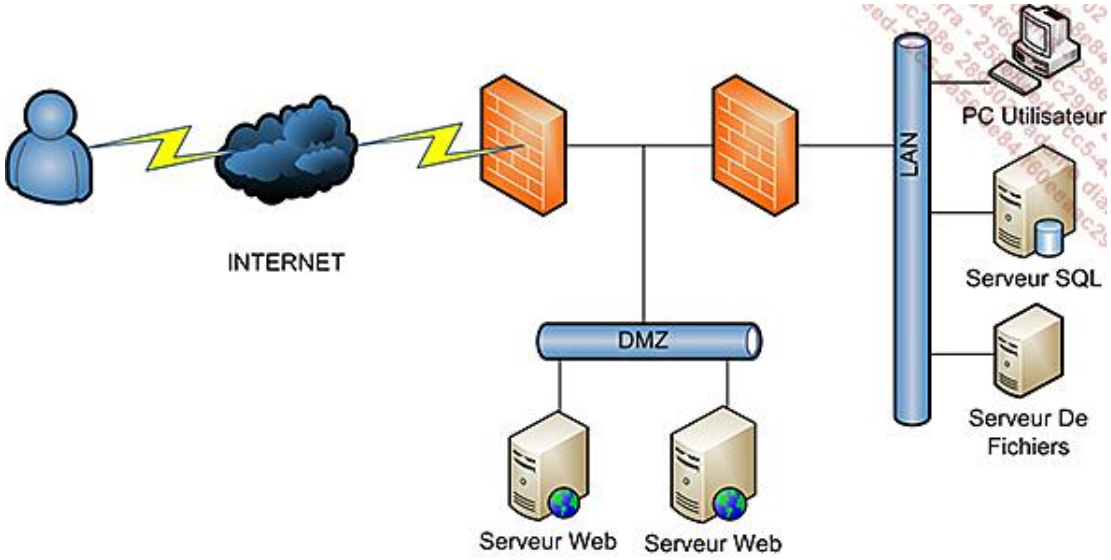
Une DMZ (*Demilitarized Zone*) ou Zone démilitarisée est un emplacement du réseau dans lequel les utilisateurs d'Internet peuvent accéder à vos serveurs sans mettre en péril la sécurité de votre réseau local. Le but de cette zone est de limiter la surface d'exposition de vos réseaux. En faisant en sorte que les serveurs qui hébergent des applicatifs publics soient dans ce réseau périmétrique, vous ne permettez pas d'accès à votre réseau local depuis Internet. Vous renforcez donc la sécurité de votre réseau local en empêchant la communication avec celui-ci.

Il existe deux implémentations typiques de DMZ. La première utilise un pare-feu à trois pattes ou plus (une patte correspond à une interface réseau).

© ENI Editions - All rights reserved - adamo diarra



La seconde quant à elle fait appel à deux pare-feu. Dans l'idéal et en vue de sécuriser un maximum, il est recommandé d'utiliser deux modèles de pare-feu différents. En effet, si une personne malintentionnée vient à trouver une faille sur le premier, le travail est déjà quasiment accompli pour arriver à percer le second s'il sont identiques.



Il ne vous reste ensuite plus qu'à gérer les flux entre Internet et la DMZ, et entre la DMZ et le LAN. En effet, si vos serveurs Web font appel à des ressources du réseau, ils auront besoin d'un accès à celui-ci. Il suffit donc d'autoriser les serveurs de la DMZ à communiquer avec le LAN pour les protocoles requis. Plus vous restreindrez les accès et mieux seront sécurisés à la fois votre DMZ et votre réseau local.

Côté serveur, Windows Server 2008 R2 configure automatiquement les exceptions de son Firewall. En ayant rajouté le rôle de serveur IIS, celui-ci a donc automatiquement autorisé les flux HTTP et HTTPS. Il ne vous reste alors plus qu'à gérer les ouvertures sur les équipements de pare-feu.

© ENI Editions - All rights reserved - adamo diarra

Monter un site FTP avec isolation des utilisateurs

Afin de fournir un espace de stockage Internet à vos utilisateurs, ou encore à des clients pour lesquels vous hébergez des sites Web, vous aurez sûrement besoin de leur fournir un accès FTP.

De façon à restreindre leur champ d'action et à vous assurer qu'ils ne verront pas les répertoires des autres personnes, vous allez devoir configurer l'isolation des utilisateurs.

Pré-requis : avoir installé IIS de façon basique ; avoir créé les comptes user1 et user2 dans Active Directory.

Avant d'attaquer l'installation et la configuration du service FTP, vous allez créer des données qui permettront de visualiser la bonne mise en place de l'isolation.

- Créez un répertoire **ftproot** dans le dossier C:\inetpub.
- Ouvrez une fenêtre ligne de commande et saisissez la commande suivante :

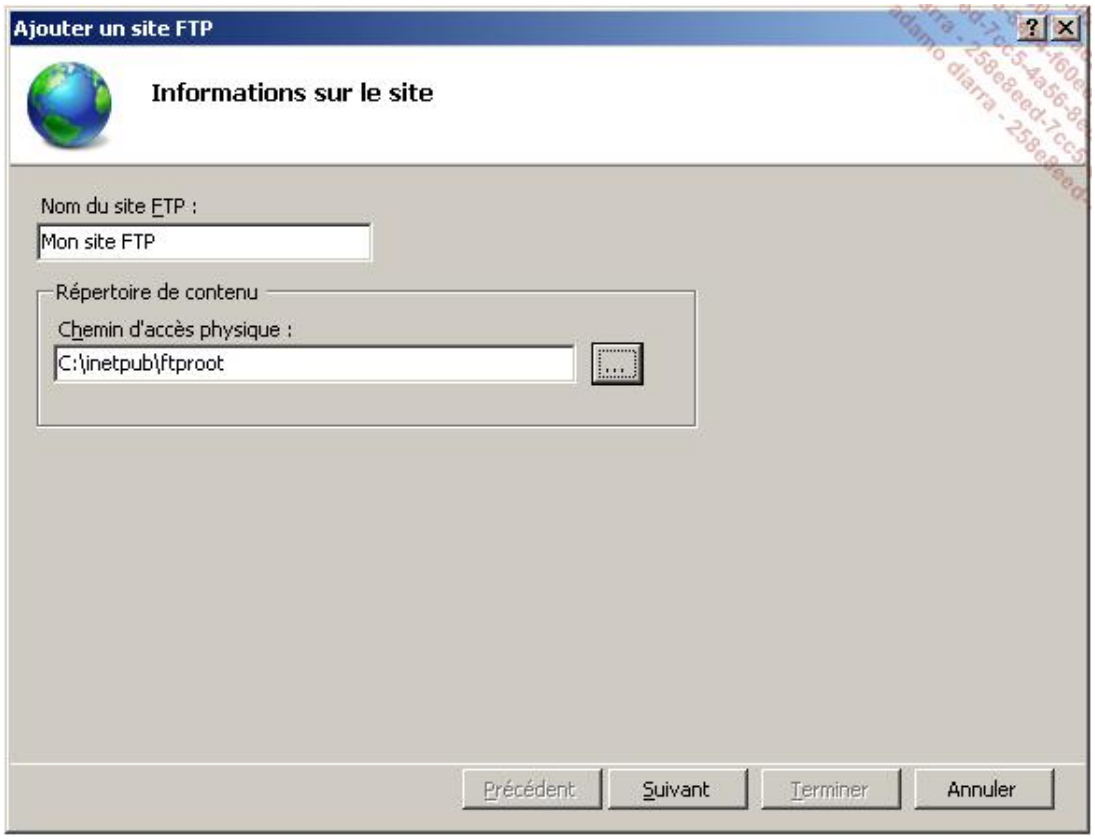
  CACLS "%SystemDrive%\inetpub\ftproot" /G IUSR:R /T /E

  Cette commande permet de donner le droit de lecture au compte anonyme de IIS sur le répertoire **ftproot**.
- Créez un répertoire **LocalUser** dans le répertoire **ftproot** et dans ce nouveau répertoire créez le répertoire **Public**. Ce répertoire servira pour le contenu fourni aux utilisateurs anonymes.
- Créez un fichier texte nommé **fichierpublic.txt** dans le répertoire **Public**.
- Créez un répertoire **Masociete** (nom netbios de votre domaine) dans le répertoire **ftproot**.

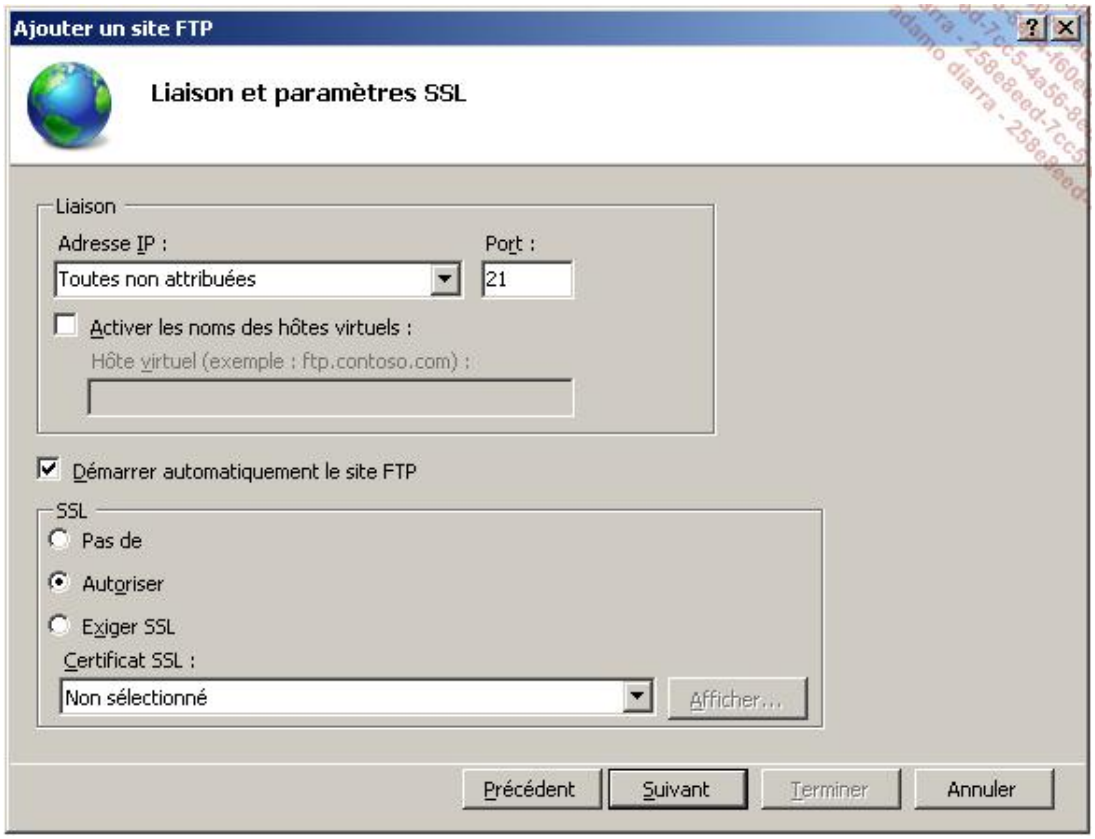
Attention, il est important que vous nommiez ce répertoire avec le nom de votre domaine. Si vous ne respectez pas cette contrainte, l'isolation des utilisateurs ne fonctionnera pas et ils seront incapables de joindre leur répertoire de base.

- Créez les répertoires **user1** et **user2** dans le répertoire **Masociete**.
- Créez un fichier texte nommé **fichieruser1.txt** dans le répertoire **user1** et faites de même avec un fichier nommé **fichieruser2.txt** dans le répertoire **user2**.
- Ouvrez la console **Gestionnaire de serveur**, puis développez **Rôles** et sélectionnez **Serveur Web (IIS)**.
- Dans le volet droit cliquez sur **Ajouter des services de rôle**.
- Cochez la case **Serveur FTP**, puis cliquez sur **Suivant**, puis sur **Installer**.
- Cliquez sur **Fermer** une fois l'installation terminée.
- Ouvrez la console **Gestionnaire de services Internet (IIS)**.
- Dans le volet **Connexions**, effectuez un clic droit sur le nom de votre serveur puis sélectionnez **Ajouter un site FTP...**

© ENI Editions - All rights reserved - adamo diarra



- Remplissez les champs comme ci-dessus puis cliquez sur **Suivant**.



- Sélectionnez **Autoriser** dans la rubrique SSL, puis cliquez sur **Suivant**.

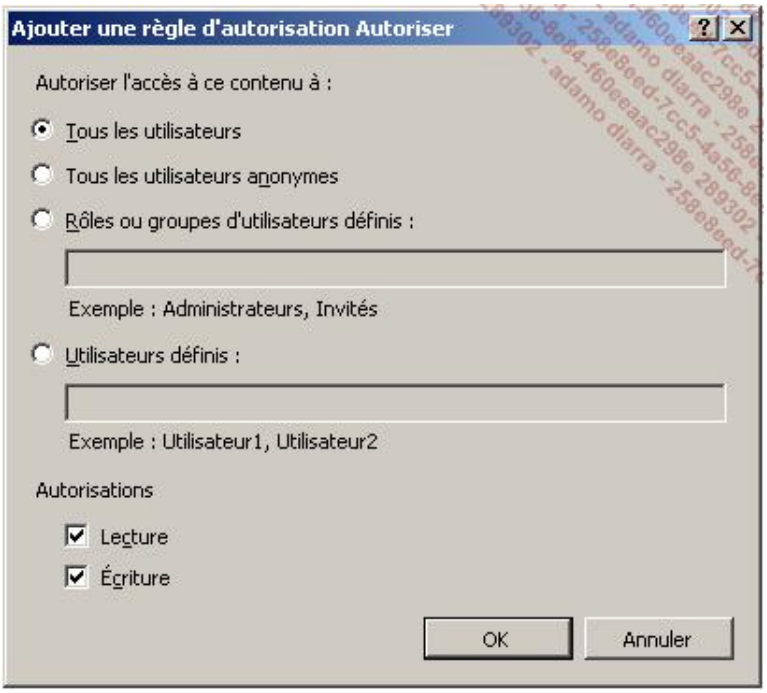
Dans cet exemple, vous configurez le serveur FTP pour ne pas exiger SSL. Dans la pratique, comme vous utilisez un

© ENI Editions - All rights reserved - adamo diarra

compte de domaine il conviendra de sécuriser l'authentification. Ainsi il vous faudra acquérir un certificat SSL (ou le délivrer via une autorité interne) et exiger SSL de façon à chiffrer les informations et éviter toute possibilité d'interception des identifiants.

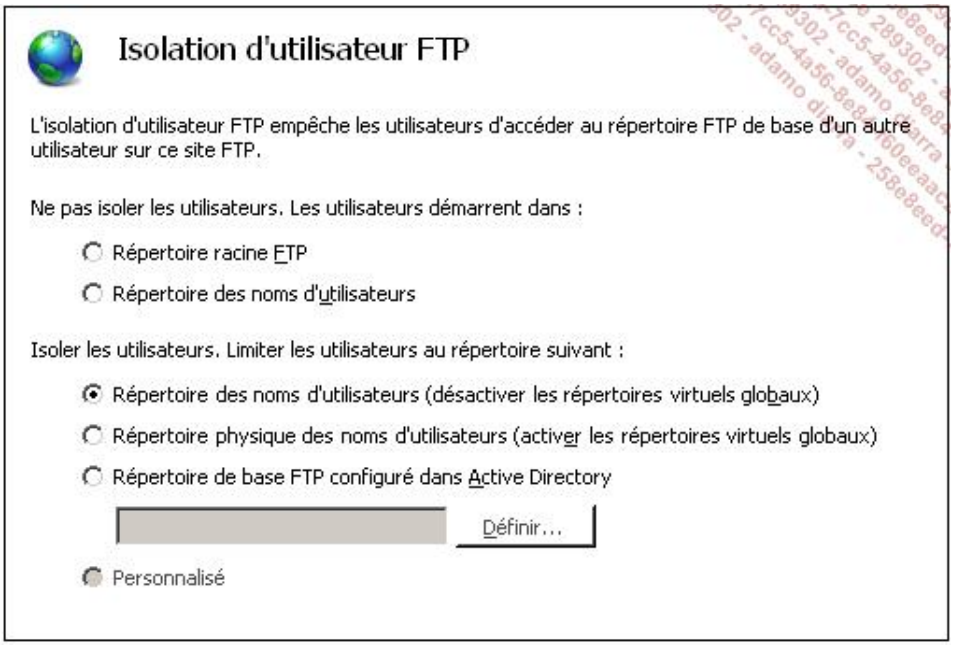
- Cochez la case **Anonyme**, dans la liste **Autorisation** sélectionnez **Utilisateurs anonymes** et cochez la case **Lecture**.
- Cliquez sur **Terminer**.
- Dans la console **Gestionnaire des services Internet (IIS)**, positionnez-vous sur votre site FTP.
- Dans le volet central, double cliquez sur **Authentification FTP**.
- Dans le volet central, effectuez un clic droit sur **Authentification de base** puis sélectionnez **Activer**.
- Repositionnez-vous sur votre site FTP puis double cliquez sur **Règles d'autorisation FTP** dans le volet central.
- Dans le volet **Actions**, cliquez sur **Ajouter une règle d'autorisation...**

Les règles d'autorisations permettent d'autoriser ou de refuser les accès à des utilisateurs. Il est possible d'y préciser si l'utilisateur a des droits en écriture ou simplement en lecture.



- Sélectionnez **Tous les utilisateurs** et cochez les cases **Lecture** et **Ecriture** puis validez par **OK**.
- Repositionnez-vous sur votre site FTP puis double cliquez sur **Isolation d'utilisateur FTP**.

© ENI Editions - All rights reserved - adamo diarra



- Sélectionnez **Répertoire des noms d'utilisateurs (désactiver les répertoires virtuels globaux)**.

  Cette option permet de restreindre l'accès des utilisateurs au répertoire physique ou virtuel du FTP qui porte le même nom que leur compte FTP. Ils ne peuvent pas remonter dans l'arborescence FTP. Les répertoires virtuels globaux racines sont ignorés (un répertoire virtuel global agit comme un raccourci vers un répertoire physique défini ; cela permet de donner accès à un répertoire sous un autre nom ou en simplifiant le chemin ; cela permet également de définir des autorisations d'accès différentes), les utilisateurs ne peuvent accéder qu'à ceux explicitement définis sous leur arborescence.

  Les autres choix possibles sont :

  Répertoire physique des noms d'utilisateurs (activer les répertoires virtuels globaux) : cette option isole les utilisateurs dans le répertoire physique qui porte le même nom que leur compte FTP. Les répertoires virtuels globaux sont accessibles dans la mesure où l'utilisateur bénéficie des autorisations associées.

  Répertoire de base FTP configuré dans Active Directory : les utilisateurs sont isolés dans un répertoire de base défini dans les propriétés de leur compte Active Directory.

- Dans le volet d'actions cliquez sur **Appliquer**.

Il est maintenant temps de vérifier l'isolation des utilisateurs.

- Ouvrez le navigateur Internet Explorer.

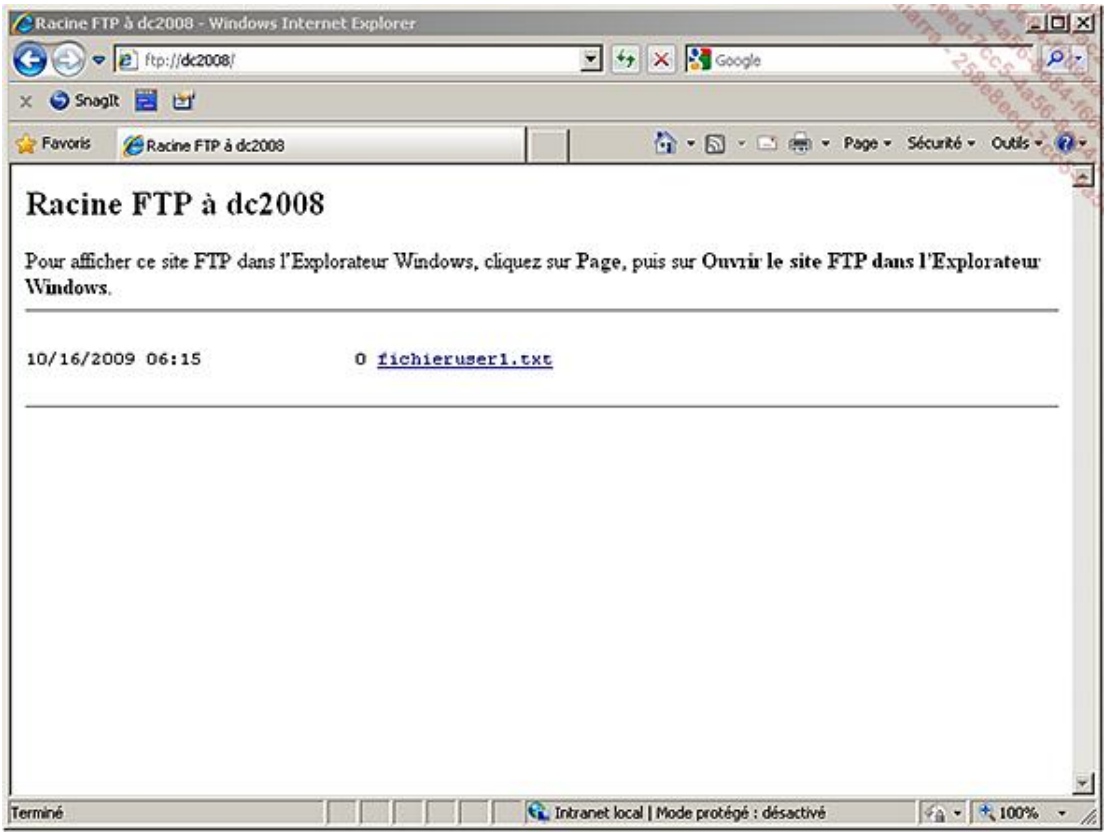
- Dans la barre d'adresse saisissez : **ftp://dc2008**.

- Entrez les informations d'identification sous la forme **Domaine\utilisateur**.

- Vérifiez que vous vous trouvez directement dans le répertoire de l'utilisateur et que vous ne pouvez pas voir les autres.

Vous devriez obtenir le résultat suivant :

© ENI Editions - All rights reserved - adamo diarra



- En vous connectant en tant qu'utilisateur anonyme, vous devriez uniquement voir le fichier fichierpublic.txt créé précédemment.

Dans cet exemple vous avez utilisé un domaine, et donc créé un répertoire correspondant au nom de domaine dans ftproot. Dans le cas de l'utilisation d'un serveur ftp autonome, utilisez le nom de dossier **LocalUser** pour créer les répertoires utilisateurs.

© ENI Editions - All rights reserved - adamo diarra

Monter un site Intranet

S'il n'est pas difficile de créer un site Web basique grâce à IIS, ceux d'entre vous qui ne sont pas initiés aux langages de développement Web auront du mal à satisfaire les besoins des utilisateurs pour le contenu.

Microsoft fournit gratuitement un CMS (*Content Management System*) pour répondre à ces besoins. Ce type de logiciel offre un environnement Web collaboratif dynamique qui facilite l'implémentation par des modèles préconfigurés. Il s'agit de Windows SharePoint Services. Actuellement disponible en version 3.0 avec Service Pack 2, il peut s'installer sur Windows 2003 ainsi que sur Windows Server 2008.

Pour télécharger Windows SharePoint Services 3.0 avec SP2 : http://www.microsoft.com/downloads/en/details.aspx?FamilyId=EF93E453-75F1-45DF-8C6F-4565E8549C2A&displaylang=en

---

WSS (*Windows SharePoint Services*) offre un espace de travail unique pour organiser les documents, programmer des réunions ou encore participer à des discussions.

Sa facilité de déploiement et de personnalisation permet aux utilisateurs une gestion des documents souple et rapide.

WSS contient de base plusieurs modèles de sites applicatifs qui vous aideront dans sa mise en place. On retrouve ainsi deux grandes catégories : les modèles de collaboration et ceux de réunions.

En collaboration, vous avez accès à :

- **Site d'équipe** : correspond au modèle de base. Il propose une bibliothèque de documents, des annonces, des éléments de calendrier, des tâches et des discussions.
- **Site vide** : seule la structure est présente à vous d'ajouter les composants voulus.
- **Espace de travail du document** : il s'agit d'une bibliothèque de documents permettant à plusieurs personnes de travailler sur un même fichier. Les fonctionnalités de gestion de version de SharePoint permettent un suivi des modifications. Une liste des tâches est associée de façon à répartir le travail entre plusieurs collaborateurs.
- **Site Wiki** : espace de partage d'idées, de définitions. Il peut être utilisé pour gérer une base de connaissances sur votre intranet.
- **Blog** : ni plus ni moins qu'un blog qui peut être alimenté en quelques clics par chaque utilisateur.

En réunions, vous avez accès à :

- **Réunion de base** : planification, organisation, compte rendu, gestion de l'ordre du jour et des participants.
- **Réunion vide** : possède uniquement la structure. La personnalisation est à réaliser en fonctions de vos besoins.
- **Réunion pour prise de décision** : suivi de l'état et de la prise de décision. Il propose une liste de création de tâches et de stockage de documents.
- **Réunion informelle** : planification d'événements informels, suivi des événements, des participants et des images liées.
- **Réunion multipage** : planification, organisation et collecte des résultats d'une réunion.

Des modèles d'applications sont disponibles gratuitement à l'adresse : http://technet.microsoft.com/fr-fr/windowsserver/sharepoint/bb407286(en-us).aspx

---

À l'heure où ce livre est écrit, il en existe une quarantaine disponibles en anglais et environ vingt en français. Ces modèles vont de la base de connaissance, à la gestion de demandes d'absence ou encore la gestion d'un stock.

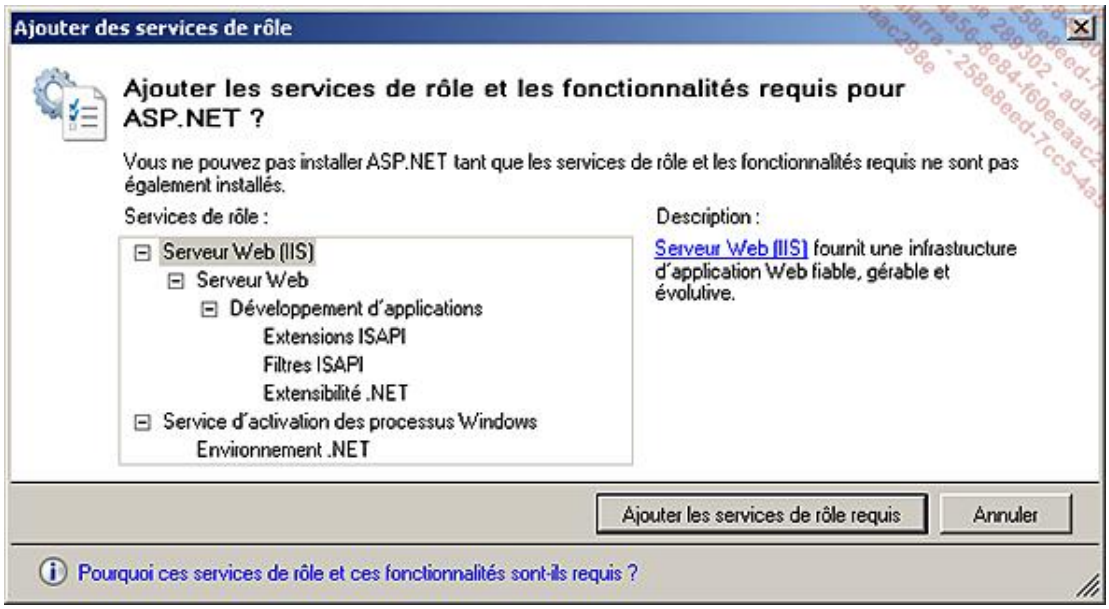
© ENI Editions - All rights reserved - adamo diarra

Vous allez maintenant procéder à l'installation de WSS sur votre serveur 2008 R2.

Pré-requis : avoir téléchargé WSS avec le lien mentionné plus haut dans cette page et avoir installé le rôle de serveur IIS par défaut.

Voici les étapes pour installer les derniers pré-requis ainsi que WSS :

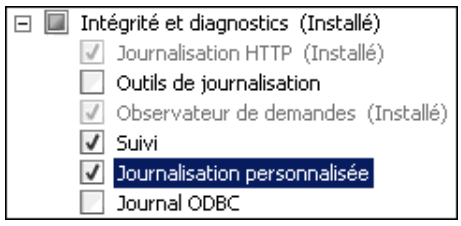
- Ouvrez votre console **Gestionnaire de serveur**.
- Dans **Rôles**, naviguez jusqu'à la section **Serveur Web (IIS)** et cliquez sur **Ajouter des services de rôle**.
- Dans la section **Développement d'applications**, cochez la case **ASP.NET** ; la fenêtre suivante apparaît :



- Cliquez sur **Ajouter les services de rôle requis**.

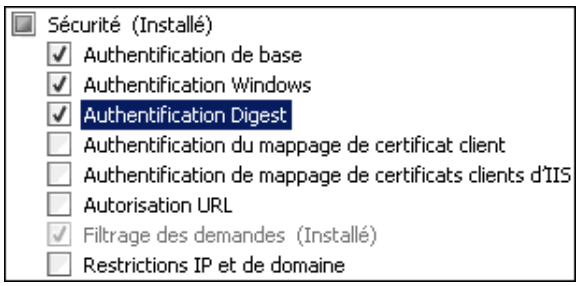
  Les cases **Extensibilité.NET**, **Extensions ISAPI** et **Filtres ISAPI** seront automatiquement cochées.

- Dans la section **Intégrité et diagnostics**, cochez les cases **Suivi** et **Journalisation personnalisée**.



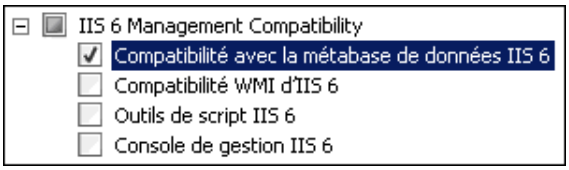
- Dans la section **Sécurité**, cochez les cases **Authentification de base**, **Authentification Windows**, **Authentification Digest**.

© ENI Editions - All rights reserved - adamo diarra



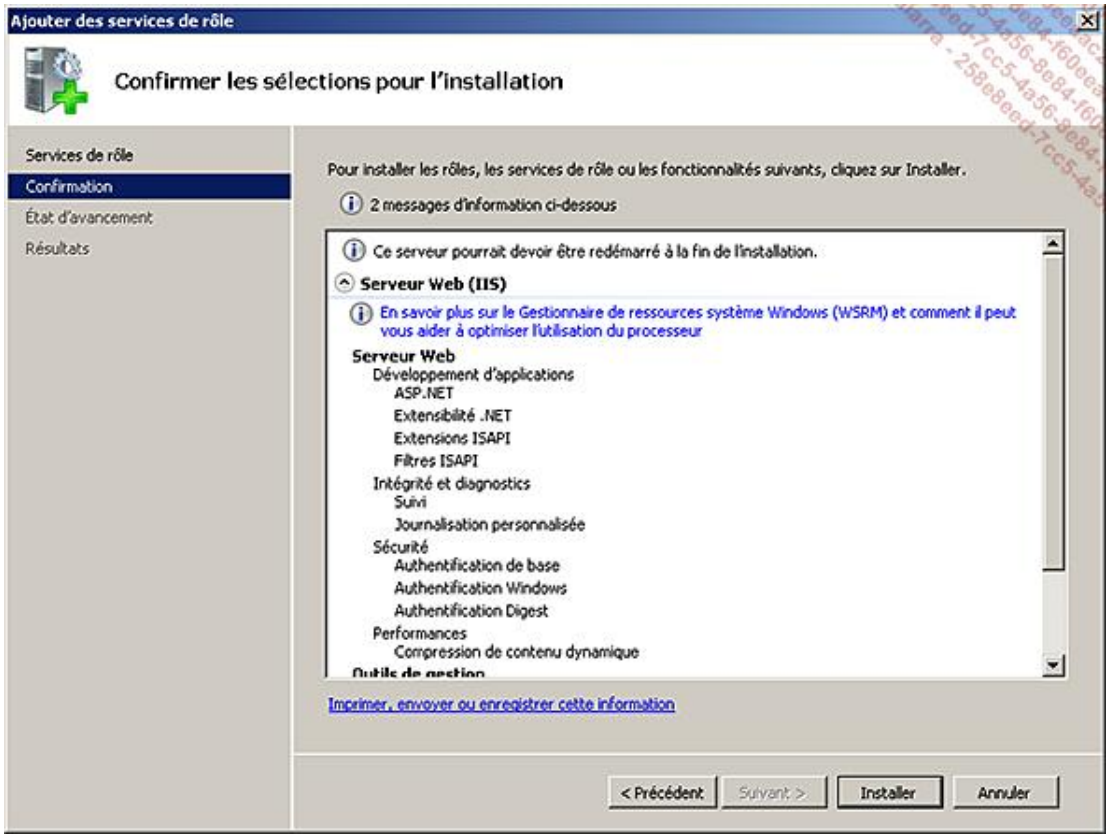
- Dans la section **Performances**, cochez la case **Compression de contenu dynamique**.

- Dans la section **IIS 6 Management Compatibility**, cochez la case **Compatibilité avec la métabase de données IIS 6**.



- Cliquez sur le bouton **Suivant**.

- Sur la page de confirmation vérifiez que vous avez sélectionné les bonnes fonctionnalités puis cliquez sur **Installer**.



- Sur la page de **Résultats**, vérifiez que l'installation s'est correctement déroulée puis cliquez sur **Fermer**.

© ENI Editions - All rights reserved - adamo diarra

- Retournez dans votre console **Gestionnaire de serveur** et cliquez sur **Ajouter des fonctionnalités**.
- Cochez la case **Fonctionnalités .NET Framework 3.5.1** puis cliquez sur **Suivant**.
- Cliquez ensuite sur **Installer**.
- Sur la page de **Résultats**, vérifiez que l'installation s'est correctement déroulée puis cliquez sur **Fermer**.
- Lancez l'exécutable d'installation **Sharepoint.exe** préalablement téléchargé.
- Sur la page de licence, cochez la case **J'accepte les termes de ce contrat** puis cliquez sur **Continuer**.
- Cliquez sur la case **De base**.

L'installation de base installe également une version allégée de SQL sur le serveur. Dans le cas où vous voudriez utiliser un serveur SQL distant, cliquez sur **Avancé**. La configuration des bases SQL aura lieu à la fin de l'installation de la partie Web grâce à l'assistant de configuration.

- Une fois l'installation terminée, cliquez sur **Fermer** pour lancer l'assistant de configuration.
- Cliquez sur **Suivant**, puis dans la fenêtre d'avertissement cliquez sur **Oui** (attention certains services dont IIS vont être redémarrés).
- Sur la page de résultats, cliquez sur **Fermer**.

La page d'accueil du site SharePoint se lance :

À partir de cette page, vous pouvez facilement personnaliser les éléments apparents comme le logo ou encore le titre de la page. La plupart des paramètres sont accessibles depuis le bouton **Actions du site** situé en haut à droite. Aucune intervention sur le code source de la page n'est nécessaire pour modifier celle-ci !

Pour accéder à la configuration du site, il vous faut passer par le menu **Démarrer - Outils d'administration - Administration centrale de SharePoint**. Un raccourci vers une page web s'ouvre et permet par exemple de spécifier un

© ENI Editions - All rights reserved - adamo diarra

serveur mail entrant et sortant pour les notifications, la configuration de la fonction de recherche, etc.

Pour vous aider dans la prise en main du produit voici un lien pointant vers le TechNet de Microsoft : http://technet.microsoft.com/en-us/windowsserver/sharepoint/default.aspx

WSS vous offre donc la possibilité de déployer facilement, et à moindre coût, un environnement collaboratif. La création et la personnalisation en sont simplifiées. Les accès peuvent être configurés de façon très précise de sorte à sécuriser les informations de votre Intranet. Vous disposez d'un suivi des documents et de leur modification et vous renforcez ainsi le travail en équipe.

Si certaines fonctionnalités venaient à manquer, sachez que Microsoft propose également une solution payante plus complète appelée MOSS (*Microsoft Office SharePoint Server 2007*). Les possibilités sont par contre plus étendues. À titre d'exemple, elle permet de créer des sites individuels pour chaque employé (appelé **My site**), la gestion de flux RSS, propose des modèles de site portail, etc. MOSS s'intègre également à la suite Office 2007. Il est du coup possible de lancer ou de participer à un *workflow* directement depuis les programmes de la suite Office 2007 (Word, Excel, etc.). Il offre également la possibilité de s'interfacer avec des produits tiers comme SAP ou encore Siebel et les modèles de site sont plus nombreux et répondent aux besoins des grandes organisations.

Vous pouvez trouver une comparaison entre les différentes versions de SharePoint à l'adresse suivante : http://office.microsoft.com/en-us/sharepointtechnology/FX101758691033.aspx

Vous venez de voir dans ce chapitre que pour gérer des sites Internet et/ou Intranet vous devez utiliser le rôle de Serveur Web (IIS).

Dans sa version 7 / 7.5, IIS offre de nombreux rôles de services liés à la sécurité, la performance, le diagnostic ou encore la rétrocompatibilité.

L'architecture de IIS 7 / 7.5 a été repensée pour renforcer la sécurité et apporter une modularité non présente dans les versions précédentes.

Les outils d'administration ont été étendus. Vous pouvez utiliser comme avant l'interface graphique mais aussi les outils en ligne de commande comme AppCMD et PowerShell pour automatiser vos tâches.

Windows SharePoint Services, avec son site Web par défaut, vous permet de publier facilement un site Web sur votre intranet. Ce site peut alors être personnalisé par les utilisateurs sans qu'ils aient la moindre compétence en termes de développement.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre est consacré à la sécurisation de Windows Server 2008 R2. La sécurité est au cœur de cet OS, pour laquelle la mise en œuvre la plus flagrante est l'installation dite « minimum », dont le nom anglais « Core » est utilisé pour la nommer. À travers ce chapitre, vous allez découvrir comment gérer cette version si particulière, et si utile en environnement hostile.

© ENI Editions - All rights reserved - adamo diarra

Principes du serveur Core

Cette section présente les principales caractéristiques du serveur Core, les domaines de prédilection pour lesquels il a été prévu, ainsi que ceux pour lesquels il n'est pas possible de l'utiliser.

1. Restrictions liées à une installation Core

L'intérêt d'une installation Core est de réduire la surface d'attaque ce qui a un impact sur les rôles pouvant être installés sur le serveur. Windows Server 2008 R2 apporte notamment le Framework .NET dans l'édition Core, ce qui ouvre de nouveaux usages (PowerShell, sites IIS...). Les rôles suivants peuvent être installés sur un Windows Server 2008 :

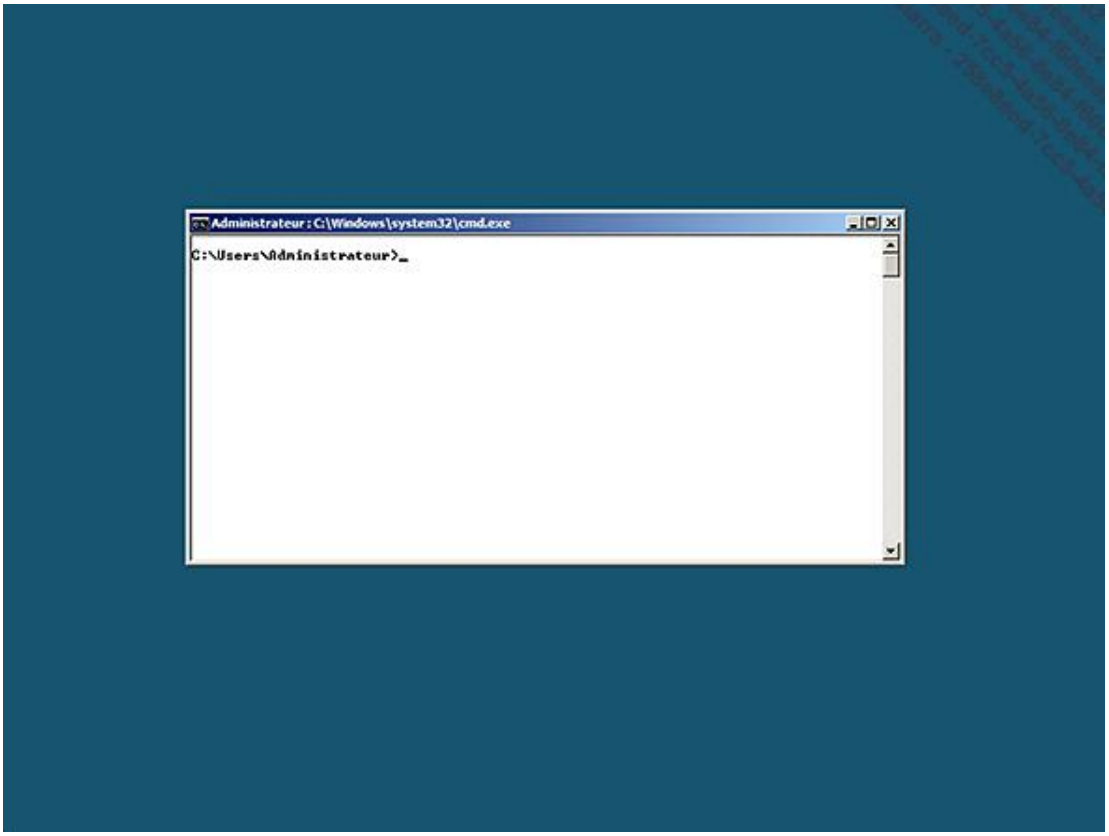
- Contrôleur de domaine (typiquement un RODC) ;
- Annuaire ADAM ;
- Serveur DHCP et DNS ;
- Serveur de fichiers ;
- Hyper-V (domaine de prédilection) ;
- Serveur d'impressions ;
- Serveur Web IIS (avec support de .NET). Sur un Windows Server 2008 R2, en complément :
    - BranchCache (relais)
    - Serveur de média
    - Serveur Web IIS avec .NET.

2. Installation minimale

L'installation Core est succincte, et cela se voit dès l'installation ! Seulement 6 minutes et 30 secondes environ sont nécessaires pour passer de l'insertion du DVD d'installation au prompt d'authentification, et ce même sans automatiser l'installation.

À ce stade, rien n'indique qu'il s'agit d'une installation minimale. Ce n'est qu'une fois authentifié que la différence est frappante :

© ENI Editions - All rights reserved - adamo diarra



Il ne s'agit pas d'une capture d'écran partielle, mais bien de l'écran entier. Explorer n'est pas dissimulé quelque part, le fichier binaire est bel et bien absent du disque dur ! L'objectif est de réduire au maximum les composants et ressources, ce qui est à la fois pertinent pour la sécurité et les machines virtuelles.

Du point de vue de la sécurité, moins d'éléments sont installés, exécutés ou accessibles, plus le niveau de sécurité augmente. Par exemple, puisqu'il n'y a pas *Explorer.exe*, toute faille de sécurité l'affectant n'aura aucun impact sur un serveur Core. Au delà du fait que la faille n'est pas exploitable, il n'est même pas nécessaire d'installer le hotfix qui la corrigera plus tard. Si une version Core de Windows Server 2000 avait existé, elle aurait réduit d'environ 60 % le nombre des mises à jour à installer, et d'environ 40 % sur Windows Server 2003. L'empreinte du système d'exploitation est également fortement réduite :

- Au démarrage, avec juste une session ouverte, 215 Mo de mémoire sont utilisés contre plus de 400 Mo sur une installation complète.

- 1,3 Go d'espace disque sont nécessaires, contre presque 11 Go pour une installation complète. Windows Server 2008 R2 rajoute systématiquement une partition cachée d'environ 100 Mo.

© ENI Editions - All rights reserved - adamo diarra

Configurer localement un Serveur Core

L'absence des consoles d'administration n'incite pas à administrer localement un serveur Core, ce qui est une partie de l'objectif. Une fois la configuration minimum effectuée, il suffit de s'y connecter depuis un hôte distant qui lui possède les consoles d'administration permettant de s'affranchir de ces contraintes. Cette section couvre la configuration initiale pour autoriser une administration décentralisée.

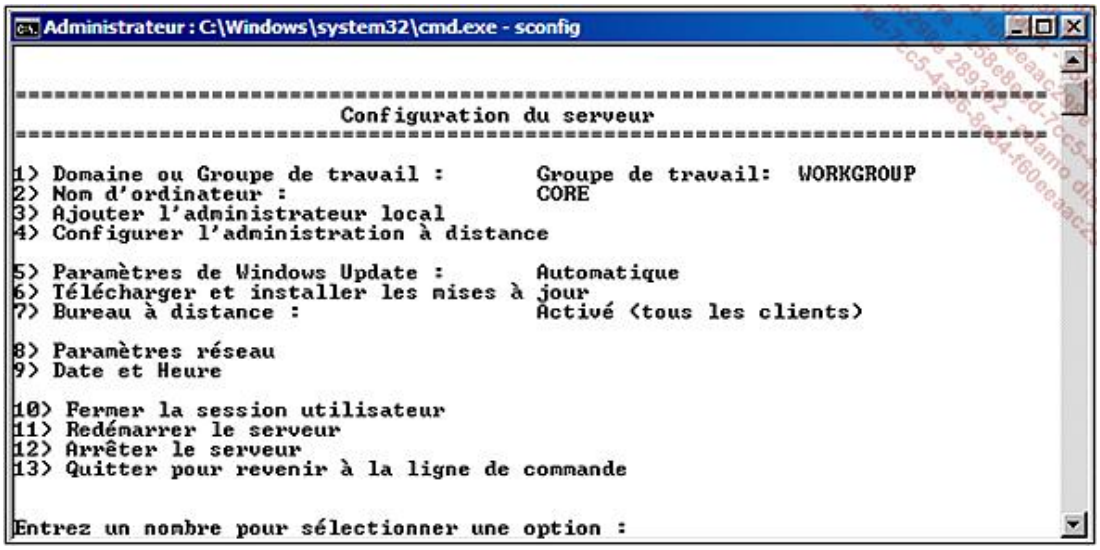
Avec Windows Server 2008 R2, il est même possible d'utiliser la console **Gestionnaire de serveur** pour gérer un Serveur Core (en activant winrm sur le serveur Core au préalable).

1. Sconfig

Afin de simplifier la configuration initiale d'un Serveur Core, Windows Server 2008 R2 introduit un nouvel outil : **sconfig**. Il permet de configurer les éléments suivants à travers un menu interactif :

- Joindre un domaine ou un groupe de travail.
- Changer le nom de l'ordinateur.
- Ajouter un administrateur local.
- Configurer l'administration à distance.
- Se connecter à Windows Update.
- Définir des Paramètres réseau.
- Configurer la date et l'heure.

Appeler cet outil est aussi simple que taper son nom dans l'invite de commande : **sconfig**.



Vous l'aurez compris, si vous avez la chance de posséder Windows Server 2008 R2, il ne vous sera pas nécessaire d'effectuer la plupart des configurations qui suivent. Néanmoins, il est toujours intéressant de connaître les différentes méthodes qui peuvent s'offrir à vous.

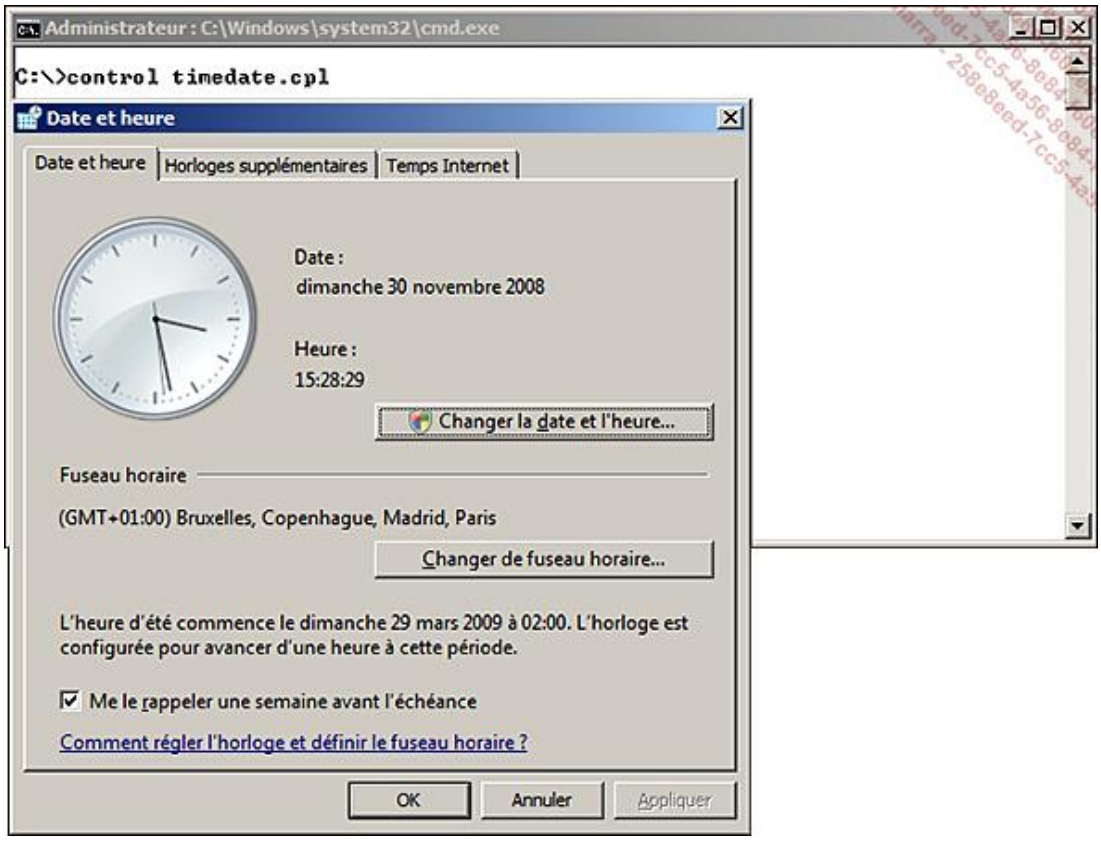
2. Configurer le temps

Certaines actions évidentes sur un serveur classique peuvent paraître déroutantes dans cette installation épurée. Une des premières à effectuer sur un serveur est de configurer la date et l'heure. Même si celui-ci va rejoindre un domaine, il doit avoir par défaut moins de 5 minutes de décalage avec l'heure du domaine pour que Kerberos puisse fonctionner et ainsi permettre la jonction du domaine.

© ENI Editions - All rights reserved - adamo diarra

Plusieurs solutions existent (les commandes `time` et `date` sont toujours présentes), mais voici comment obtenir une interface graphique sous un serveur Core :

- Depuis la ligne de commande, exécutez `control timedate.cpl` :



3. Paramètres régionaux

Si vous souhaitez modifier les paramètres régionaux, vous pouvez utiliser la commande `control intl.cpl`.

4. Résolution de l'écran

La seule solution pour changer la résolution de l'écran est de passer par la base de registre. Pour cela, appelez l'éditeur `regedit` depuis la ligne de commande ouverte à l'écran.

Naviguez dans l'arborescence jusqu'à cette racine :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Video.

Un identifiant aléatoire a été affecté à votre carte graphique. Vous pouvez déterminer lequel y correspond en regardant la sous-clé **Device Description** à l'intérieur.

Quatre clés permettent de gérer la résolution, le nombre de couleurs et le taux de rafraîchissement :

- **DefaultSettings.XResolution** : nombre de pixels sur l'axe horizontal.
- **DefaultSettings.YResolution** : nombre de pixels sur l'axe vertical.
- **DefaultSettings.BitsPerPel** : nombre de couleurs (32 bits par défaut).
- **DefaultSettings.VRefresh** : taux de rafraîchissement de l'écran.

© ENI Editions - All rights reserved - adamo diarra

5. Économiseur d'écran

L'économiseur d'écran peut aussi être modifié aussi en ligne de commande. Pour cela, appelez l'éditeur `regedit` depuis la ligne de commande ouverte à l'écran.

Naviguez dans l'arborescence jusqu'à cette racine : **HKEY_CURRENT_USER\Control Panel\Desktop**.

Trois clés permettent de gérer le nom de l'économiseur d'écran, le verrouillage de la session suite au lancement de l'économiseur d'écran et le temps d'attente avant son lancement :

- **ScreenSaveActive** : permet d'activer ou de désactiver l'économiseur d'écran de façon globale. Il peut prendre les valeurs **1** (actif) ou **0** (inactif).
- **SCRNSAVE.EXE** : spécifie l'économiseur d'écran à exécuter. Le paramètre par défaut est **C:\Windows\system32\logon.scr**. L'économiseur d'écran **scrsave.scr** est disponible sur le serveur, ce qui évite une consommation processeur inutile, notamment en environnement virtuel.
- **ScreenSaverIsSecure** : permet d'activer ou non le verrouillage de la session à l'exécution de l'économiseur d'écran. La valeur par défaut est **1**, ce qui rend active cette protection.
- **ScreenSaveTimeOut** : nombre de secondes avant le déclenchement de l'économiseur d'écran. Par défaut, la valeur est 600 secondes.

Dans le cadre d'un domaine Active Directory, ces paramètres peuvent être gérés par des stratégies de groupe de façon centralisée.

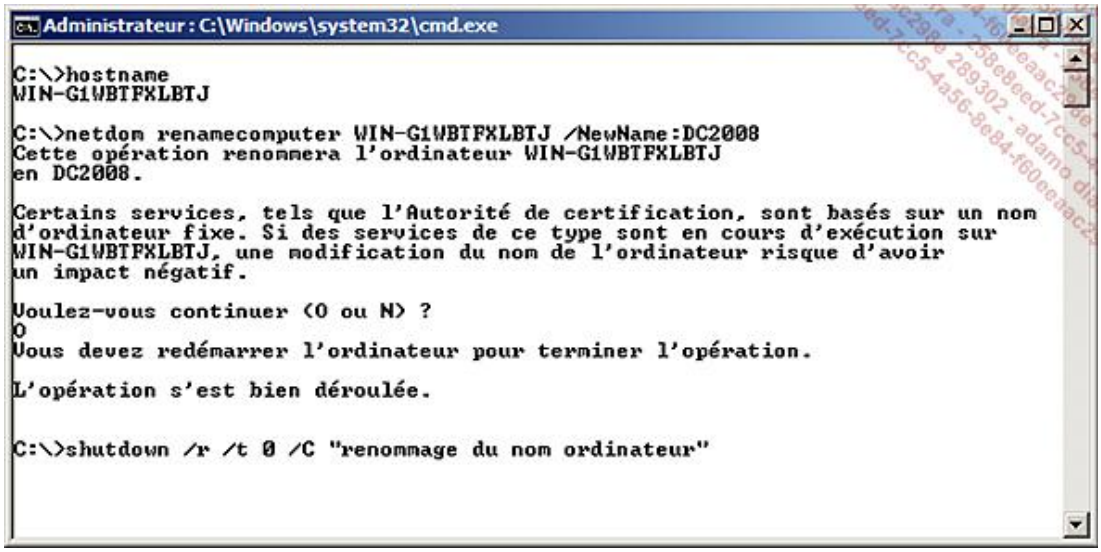
---

6. Nom du serveur

Par défaut, un nom de machine aléatoire est donné au serveur, toujours préfixé par **WIN-**.

- Pour connaître le nom actuel, exécutez la commande suivante depuis la ligne de commandes : `hostname`
- Pour changer le nom du serveur, exécutez la commande suivante depuis la ligne de commandes : `netdom renamecomputer <nomdevotreserveur> /NewName:DC2008`
- Il faut redémarrer pour prendre en compte ce changement :

```
shutdown /r /t 0 /C “renommage du nom ordinateur”
```



© ENI Editions - All rights reserved - adamo diarra

7. Gestion des pilotes

La gestion des pilotes est possible via la ligne de commande avec l'outil **pnputil**.

Vous pouvez lister les pilotes tiers installés en exécutant cette commande : `Pnputil -e`

Pour ajouter et installer des pilotes supplémentaires, il faut utiliser les paramètres `-a` et `-i` et préciser le dossier où les trouver : **Pnputil -a -i c:\mespilotes*.inf**

Pour obtenir la liste des pilotes actifs utilisez la commande suivante (ne pas oublier l'espace après le signe égal) : `sc query type= driver`

8. Configuration réseau

Le serveur utilise par défaut un adressage DHCP sur toutes les interfaces. Pour passer à un adressage IP statique, vous allez utiliser la commande `netsh`. Elle existe depuis Windows 2000, mais son usage n'est pas très répandu chez les administrateurs système. Chaque carte réseau a un numéro attribué qui est utilisé par `netsh` pour déterminer la carte réseau à laquelle appliquer les changements. Pour lister les cartes réseaux et voir les identifiants attribués par Windows, exécutez depuis la ligne de commande :

```
netsh interface ipv4 show interfaces
```

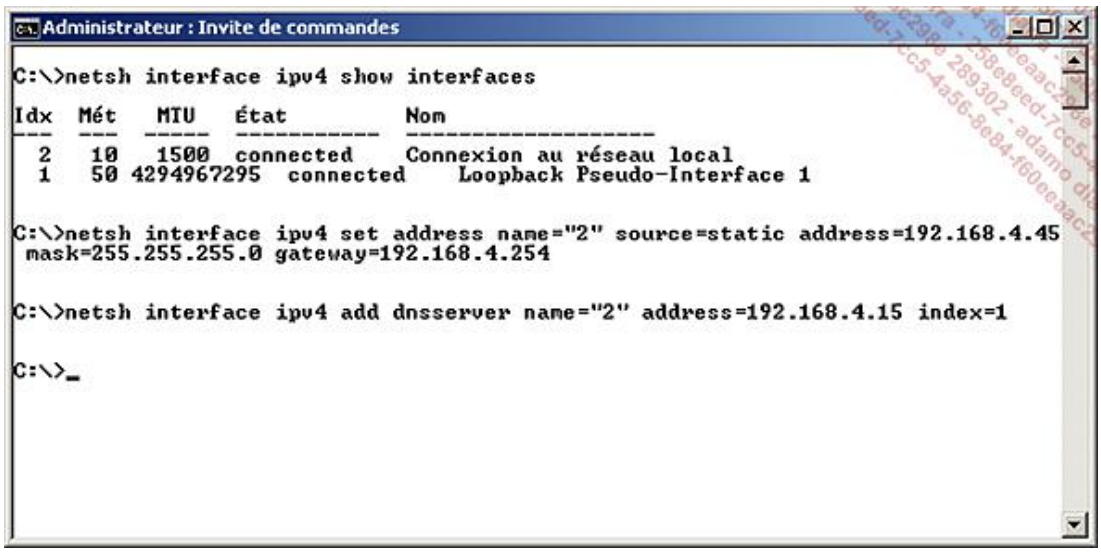
Par exemple, si vous souhaitez configurer la carte réseau ayant l'identifiant 2 en adressage IP statique, exécutez :

```
netsh interface ipv4 set address name="2" source=static address=192.168.4.45 mask=255.255.255.0 gateway=192.168.4.254
```

Pour configurer l'adresse 192.168.4.15 en tant que serveur DNS primaire, exécutez la commande :

```
netsh interface ipv4 add dnsserver name="2" address=192.168.4.15 index=1
```

Vous devriez obtenir un résultat équivalent à celui-ci :



La commande `netsh` accepte l'argument `store`, qui permet d'indiquer si la configuration doit persister après le prochain redémarrage du serveur, ce qui est le cas si le paramètre est omis. Si vous ne souhaitez pas conserver le paramétrage effectué après le redémarrage, vous pouvez ajouter l'argument `store=active`. Si vous souhaitez expliciter le fait que le paramétrage doit être persistant, vous pouvez utiliser l'argument `store=persistent`.

Pour configurer le suffixe DNS par défaut, il faut modifier la base de registre. Pour cela, exécutez depuis la ligne de commande :

```
reg add HKLM\SYSTEM\ CurrentControlSet\
Services\Tcpip\Parameters /v "NV Domain" /d "masociete.local" /f
```

9. Activation de Windows

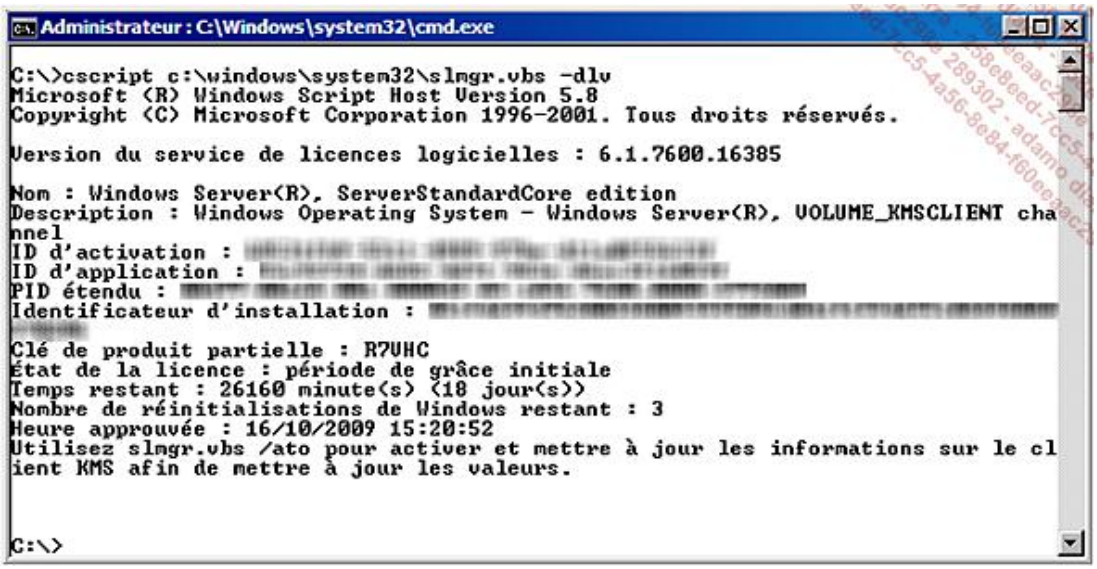
La gestion de l'activation de la licence Windows est gérable en ligne de commande. Le script VB `slmgr.vbs` est installé

© ENI Editions - All rights reserved - adamo diarra

avec Windows dans %systemroot%\System32 à cet effet. Pour rappel, contrairement aux versions précédentes de Windows l'activation est obligatoire, même avec une licence en volume. Ce script fonctionne aussi avec KMS (*Key Management Service*).

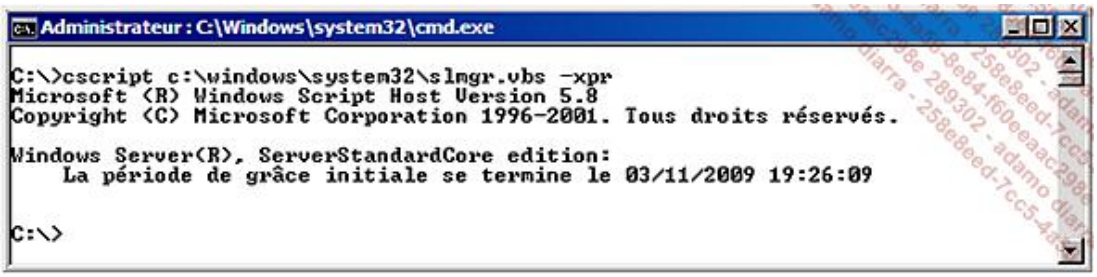
Pour vérifier l'état d'activation actuel, exécutez la commande :

```
cscript %systemroot%\System32\slmgr.vbs /dlv
```



Dans cet exemple, la licence expire dans 18 jours.

Si vous souhaitez juste connaître la date à laquelle la licence expire, exécutez le script avec le paramètre `/xpr`.



Par défaut, le service KMS est automatiquement trouvé sur votre domaine Active Directory avec la requête DNS suivante : `_vlmcs._tcp.masociete.local`.

Si cette entrée DNS existe, le serveur essayera de s'y connecter sur le port TCP 1688. Vous pouvez aussi indiquer manuellement le nom du serveur KMS avec le paramètre `-skms`.

Pour déclencher manuellement l'activation de Windows, exécutez la commande :

```
cscript %systemroot%\System32\slmgr.vbs /ato
```

10. Gestion du rapport d'erreurs

Le service de rapport d'erreurs peut être configuré depuis la ligne de commande.

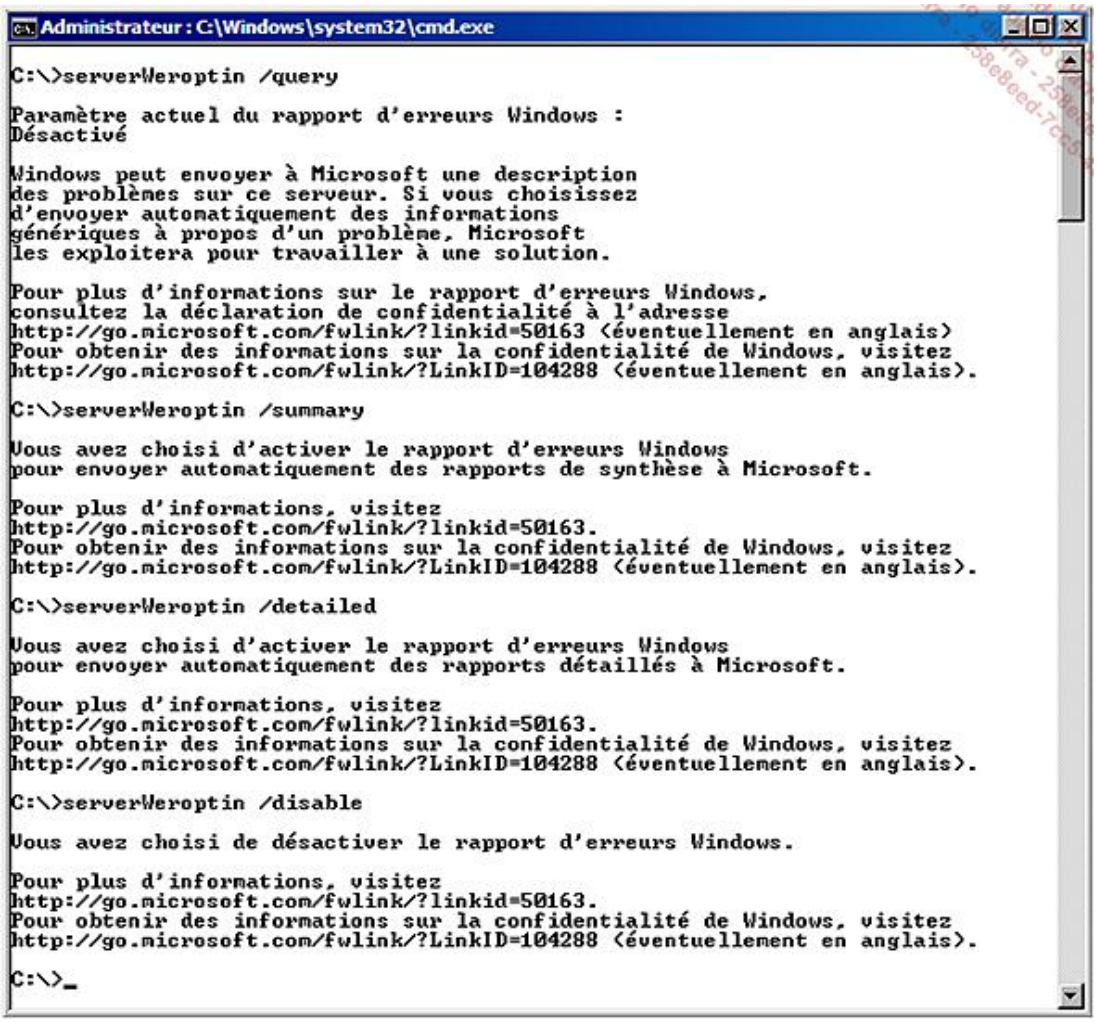
Pour vérifier la configuration actuelle, exécutez la commande `serverWerOptin /query`.

Pour activer le rapport d'erreurs détaillé : `serverWerOptin /detailed`.

Pour activer le rapport d'erreurs simple : `serverWerOptin /summary`.

Pour désactiver le rapport d'erreurs : `serverWerOptin /disable`.

© ENI Editions - All rights reserved - adamo diarra



11. Configurer le PageFile

Le fichier de pagination (PageFile) est géré automatiquement par défaut. Pour voir la configuration actuelle, vous pouvez utiliser la commande : `wmic pagefile list /format:list`

Avant de configurer manuellement le PageFile, il faut en désactiver la gestion automatique :

```
wmic computersystem where name="%computername%" set AutomaticManagedPagefile=
False
```

Pour forcer la taille du PageFile à 2 Go :

```
wmic pagefileset where name="C:\\pagefile.sys" set InitialSize=2048,
MaximumSize=2048
```

Il faut redémarrer pour que le changement soit pris en compte.

12. Joindre un domaine

La commande `netdom` permet aussi de joindre un domaine Active Directory existant. Depuis la ligne de commande, exécutez :

```
netdom join <nomdemonserveur> /domain:<monDomainAD>
/userd:<CompteADayantLesDroits> /passwordd:*
```


© ENI Editions - All rights reserved - adamo diarra

Le symbole * indique que le mot de passe doit être demandé ensuite, évitant qu'il ne soit écrit en clair dans la console.

La même commande permet de quitter un domaine Active Directory : `netdom remove`.

Avec Windows Server 2008 R2 il est possible de joindre le domaine sans être sur le réseau du domaine à ce moment là. Le chapitre Déploiement des serveurs et postes de travail couvre en détail cette manipulation (section Joindre le domaine sans réseau).

13. Gérer les journaux d'évènements

Bien que la console **Observateurs d'évènements** permette de visualiser les journaux d'un serveur distant, vous pouvez être amené à les gérer localement depuis le serveur Core. La liste des journaux peut être affichée sur la console avec la commande : `wevtutil el`.

La fenêtre Invite de commandes n'étant pas l'idéal pour un affichage massif, ni très rapide, vous pouvez restreindre la sortie en spécifiant le nombre d'évènements à afficher. Par exemple, pour n'afficher que les cinq derniers évènements : `wevtutil qe System /c:5 /f:Text`.

Il est même possible d'avoir uniquement les cinq dernières erreurs en ajoutant le paramètre `"/q:*[System[(Level=1 or Level=2)]]"`.

- Le niveau 1 correspond aux évènements « critiques ».
- Le niveau 2 correspond aux évènements « erreurs ».
- Le niveau 3 correspond aux évènements « avertissements ».
- Le niveau 4 correspond aux évènements « informations ».

Vous pouvez archiver le journal ouvert dans un fichier d'archive et ainsi commencer un nouveau journal avec la commande :

```
wevtutil cl system /bu:c:\MesArchives\syslog.evtx
```

© ENI Editions - All rights reserved - adamo diarra

Gestion à distance

1. Activation du bureau à distance

Comme tout Windows Server 2008 R2, l'accès à distance n'est pas activé par défaut. Vous pouvez vérifier l'état de l'activation avec la commande suivante :

```
cscript.exe c:\windows\system32\scregedit.wsf /AR /v
```

Comme expliqué au chapitre Bureau à distance (Terminal Services), la clé **fDenyTSConnections** désactive la prise de main à distance lorsqu'elle est positionnée à **1**, comme c'est le cas. Le même script permet de passer la clé à zéro afin d'autoriser les connexions :

```
cscript.exe c:\windows\system32\scregedit.wsf /AR 0
```

À ce stade, seuls les clients exécutant au moins Windows Vista ou Windows Server 2008 pourront se connecter. Pour autoriser les clients antérieurs à s'y connecter :

```
cscript.exe c:\windows\system32\scregedit.wsf /cs 0
```

2. Activation de WinRM

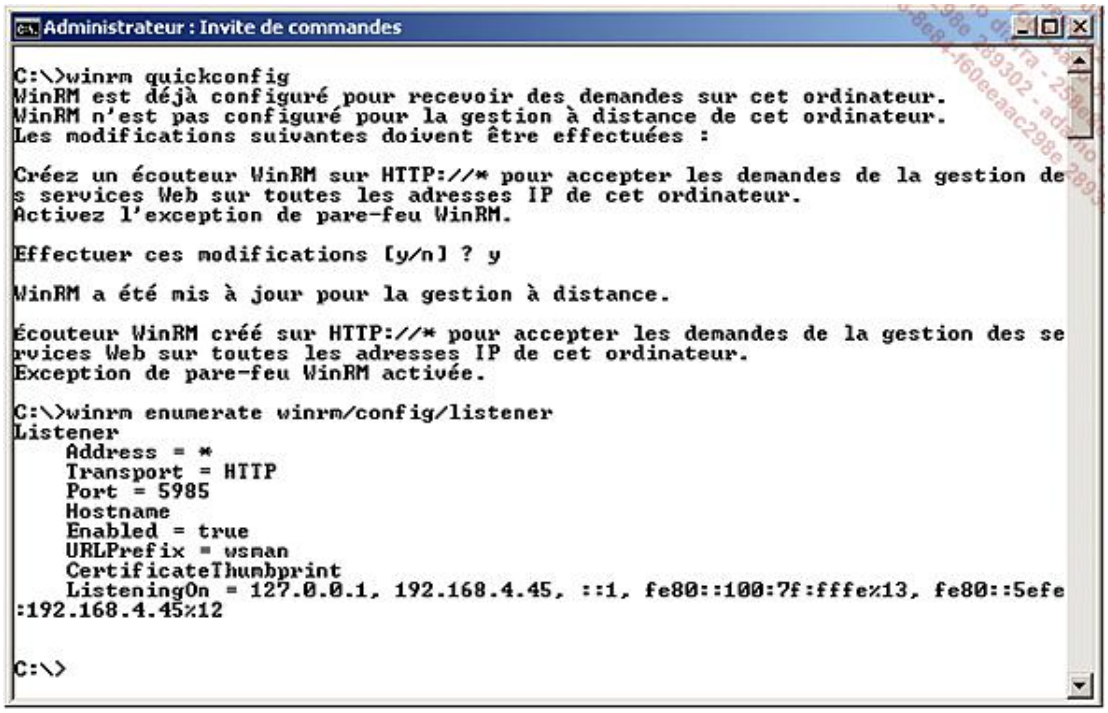
WinRM est l'implémentation par Microsoft du protocole WS-Management. L'objectif est de pouvoir communiquer entre deux systèmes à travers le système d'information, en pouvant correctement traverser les firewalls. Pour installer WinRM, exécutez cette commande depuis l'invite de commande : `WinRM quickconfig`.

Vous pouvez vérifier que WinRM écoute en utilisant la commande :

```
winrm enumerate winrm/config/listener
```


Quickconfig se charge d'ajouter l'exception sur le firewall afin que le service soit accessible via le réseau.

© ENI Editions - All rights reserved - adamo diarra



Par défaut, WinRM utilise le protocole HTTP. Il est possible d'utiliser HTTPS, à condition d'avoir déjà installé un certificat valide (non expiré, non auto-signé). Pour cela, il suffit de spécifier le transport HTTPS : `WinRM quickconfig -transport:https`. Si vous souhaitez utiliser WinRM pour accéder à un serveur qui n'est pas dans votre domaine Active Directory, vous devez soit utiliser un certificat SSL, soit utiliser la liste des ordinateurs approuvés. Cette liste étant située côté client, vous pourrez potentiellement la gérer par une stratégie de groupe, facilitant ainsi les ajouts et les suppressions de serveurs de cette liste.

Si vous souhaitez gérer directement localement cette liste, vous pouvez utiliser la commande suivante pour ajouter des serveurs :

```
winrm set winrm/config/client @{TrustedHosts="<maliste>"}
```

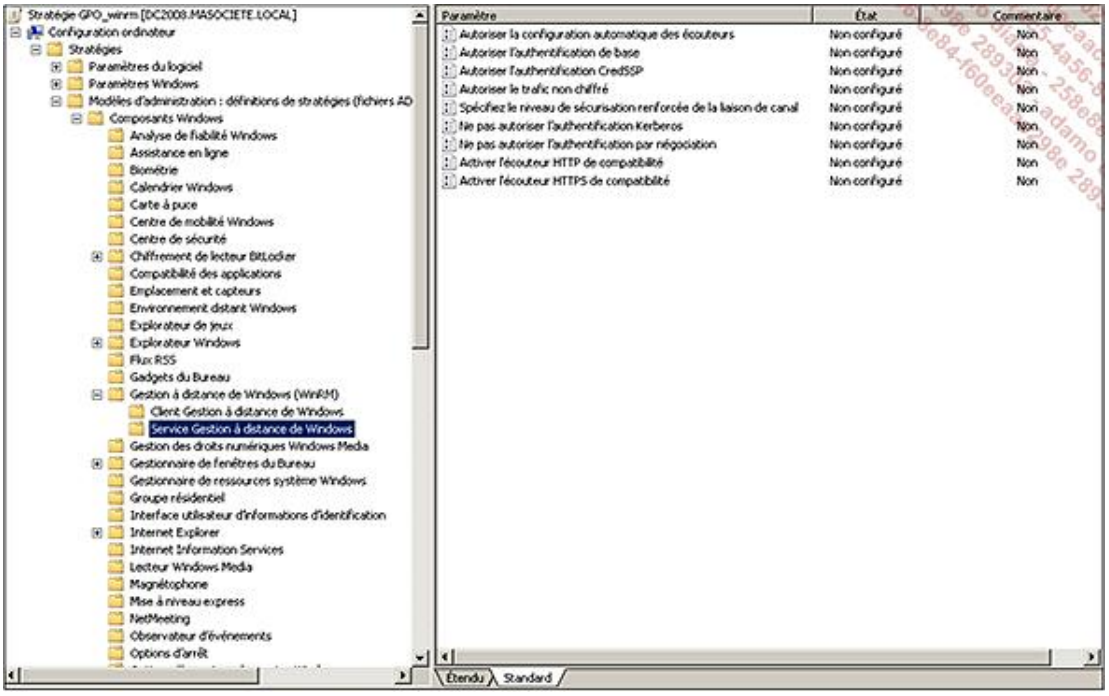
Il faudra remplacer *maliste* par un ou plusieurs éléments séparés par des virgules. Les adresses IP et noms DNS peuvent être utilisés.

Pour obtenir la liste actuelle des hôtes approuvés :

```
winrm get winrm/config/client
```

Si vos serveurs sont dans un domaine Active Directory, vous pouvez gérer WinRM depuis les stratégies de groupe :

© ENI Editions - All rights reserved - adamo diarra



Il serait tout à fait regrettable d'évoquer ce protocole sans démontrer par l'exemple ses capacités. Voici donc quelques possibilités offertes par WinRM.

- Afficher le résultat de la commande `ipconfig /all` d'un hôte distant :

```
winrs -r:NomDuServeur ipconfig /all
```

- Spécifier un compte utilisateur et un mot de passe (le mot de passe est demandé ensuite) :

```
winrs -r:NomDuServeur -u monautrecompte ipconfig /all
```

- Exécuter une requête WMI :

```
winrm get wmicimv2/win32_service?name=W32Time -r :NomDuServeur
```

WinRM est aussi disponible pour les versions antérieures de Windows (XP, 2003) comme composant supplémentaire. Il est en téléchargement à cette adresse :

http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=845289ca-16cc-4c73-8934-dd46b5ed1d33

© ENI Editions - All rights reserved - adamo diarra

Sécuriser le Serveur Core

1. Gestion du pare-feu

Comme chez sa grande sœur, le firewall Windows est actif par défaut dans l'édition minimale. Cela est très visible car le serveur ne répond pas au fameux ping, alors que l'adresse MAC correspondant à l'IP est visible depuis la commande `arp -a`. La gestion des règles du firewall peut s'avérer complexe, aussi est-il plus aisé de les gérer à distance. Cela peut se faire via les stratégies de groupes, mais aussi en utilisant la console adéquate de manière déportée. Avant cela, il faut autoriser la gestion des règles du firewall à distance sur le serveur, en exécutant la commande suivante :

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

La console **Pare-feu Windows avec fonctions avancées de sécurité** ne permet pas directement de choisir un ordinateur distant. Pour cela, il faut d'abord lancer le gestionnaire de console **mmc**, puis y ajouter la console **Pare-feu Windows avec fonctions avancées de sécurité**, et à ce moment là vous aurez la possibilité de choisir l'ordinateur cible. Vous trouverez davantage d'informations sur la configuration du pare-feu en mode graphique dans le chapitre Sécuriser votre architecture.

Les autres consoles mmc peuvent être autorisées sur le pare-feu afin de pouvoir être utilisées à distance. Voici une liste d'éléments enfichables avec les noms correspondants dans les règles :

- Services : Gestion à distance des services
- Planificateur de tâches : Gestion à distance des tâches planifiées
- Observateur d'événements : Gestion à distance des journaux des événements
- Moniteur de fiabilité et de performances : Journaux et alertes de performance
- Gestion du partage et du stockage : Partage de fichiers et d'imprimantes

```
Netsh advfirewall firewall set rule group= " nom_des_regles"
new enable=yes
```

Pour gérer à distance IPSec, il faut tout d'abord activer sa gestion à distance :

```
cscript \windows\System32\scregedit.wsf /im 1
```

Pour que la gestion des volumes à distance fonctionne, il faut démarrer au préalable le service disque virtuel : `net start vds`.

2. Gestion automatique des mises à jour

L'activation ou la désactivation des mises à jour automatiques peut être gérée en local. Si le serveur joint un domaine Active Directory, vous devriez vraiment gérer le paramétrage via les stratégies de groupes.

- Pour savoir si les mises à jour sont activées :

```
cscript C:\Windows\System32\Scregedit.wsf /au /v
```

- Pour activer les mises à jour :

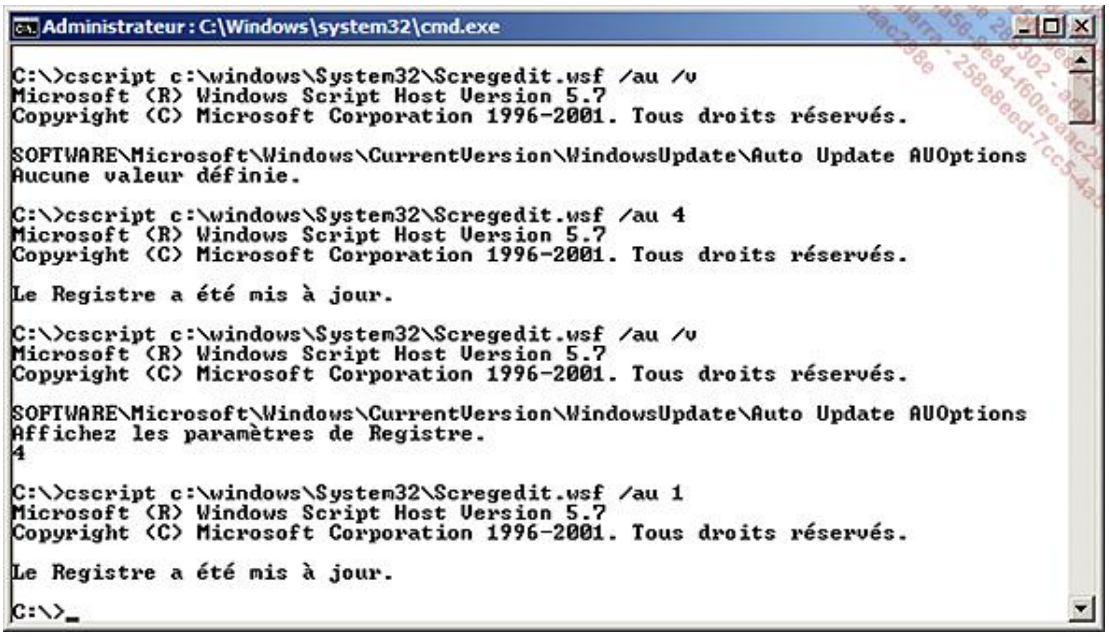
```
cscript C:\Windows\System32\Scregedit.wsf /au 4
```

© ENI Editions - All rights reserved - adamo diarra

Si vous obtenez le message d'erreur suivant : Scregedit.wsf(777, 3) (null): 0x80240037, supprimez la clé suivante : HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate.

- Pour désactiver les mises à jour :

```
cscript C:\Windows\System32\Scregedit.wsf /au 1
```



Vous pouvez forcer la vérification immédiate des mises à jour en exécutant : `wuauclt /detectnow`.

Vous pouvez forcer l'installation immédiate des mises à jour en exécutant : `wuauclt /install`.

Malgré ces commandes, le service de mises à jour stocke la date et l'heure de la dernière vérification. Aussi, après la demande initiale, un temps d'attente est imposé. Pour accélérer le processus, vous pouvez supprimer la clé de registre contenant la date et l'heure de la dernière et de la prochaine vérification :

```
Anet stop wuauserv
Breg delete
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\
Auto Update" /f
Cnet start wuauserv
Dwuauclt /detectnow
```

Un délai de quelques minutes reste toutefois imposé.

Pour consulter la liste des mises à jour installées, utilisez la commande `wmic qfe list` ou `wmic qfe.systeminfo`.

3. Sauvegarder le serveur

L'installation Core étant souvent utilisée en environnement hostile, il est parfois utile de pouvoir faire au moins des sauvegardes locales du système. La gestion des sauvegardes se fait en installant la fonctionnalité WindowsServerBackup : `start /wait ocsetup WindowsServerBackup`.

Pour déclencher manuellement une sauvegarde, il faut utiliser la commande `wbadmin`. Dans notre exemple, nous allons effectuer une sauvegarde du lecteur C:\ sur le partage \\autreserveur\partages\sauvegardes :

```
wbadmin start backup -
backuptarget :\\autreserveur\partages\sauvegardes -
include:c: -allcritical -vssfull -quiet
```


© ENI Editions - All rights reserved - adamo diarra

Les chemins UNC peuvent être directement utilisés comme destination de la sauvegarde. Un dossier nommé « WindowsImageBackup » sera créé. Ensuite un sous-dossier portant le nom du serveur sera automatiquement créé. Toute sauvegarde précédente sera automatiquement écrasée. La restauration complète peut être faite en utilisant le DVD d'installation (option restauration).

4. Sécurisation du stockage avec BitLocker

La plupart du temps, les serveurs sont dans un datacenter, souvent surnommé « bunker » afin de mettre en avant la sécurité physique qui est mise en œuvre (caméras, contrôles d'accès...). Ce niveau de sécurité n'est pas toujours possible, surtout dans le cadre des sites distants, comptant parfois seulement quelques utilisateurs. Bien que le nombre d'utilisateurs reste souvent assez faible, il apparaît indispensable de déployer sur place un serveur afin de fournir certains services localement, notamment un contrôleur de domaine ou un service DHCP. Dans le premier cas, le serveur dispose par défaut d'une copie du domaine et donc des mots de passe de tous les utilisateurs. Comme vu dans le second chapitre de cet ouvrage, la mise en place d'un RODC permet de pallier ce problème. Mais comment faire s'il s'agit d'un serveur de fichiers ou de bases de données ?

La fonctionnalité BitLocker permet de chiffrer les partitions du serveur nativement depuis Windows. Cela constitue une amélioration très notable pour la sécurité physique du serveur. Le vol du serveur ou de son stockage ne constitue plus un point de sécurité critique. Pour mettre en place BitLocker, le serveur doit posséder une puce TPM (*Trusted Platform Management*) sur la carte mère. Il faut tout d'abord installer la fonctionnalité avec cette commande :

```
start /wait ocsetup BitLocker
```

À la fin de l'installation, un redémarrage est nécessaire.

```
cscript %systemroot%\System32\manage-bde.wsf -tpm -turnOn
```

Vous devez ensuite fournir un mot de passe en exécutant :

```
cscript %systemroot%\System32\manage-bde.wsf -tpm -o password
```

Vous pouvez ensuite procéder au chiffrement de la partition avec la commande :

```
cscript %systemroot%\System32\manage-bde.wsf -on c: -rp
```

Windows 7 et Windows Server 2008 R2 introduisent BitLocker To Go. Il s'agit d'une extension de BitLocker pour chiffrer les clés USB et autres périphériques de stockage amovibles. Les systèmes d'exploitation antérieurs peuvent également lire les volumes protégés par cette extension, à condition d'installer un composant complémentaire, BitLocker Reader To go, téléchargeable ici : http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=64851943-78c9-4cd4-8e8d-f551f06f6b3d

Ils introduisent également une partition de 100 Mo en plus de la partition système, qui facilite la mise en œuvre de BitLocker et contient WinRE en cas de problème.

© ENI Editions - All rights reserved - adamo diarra

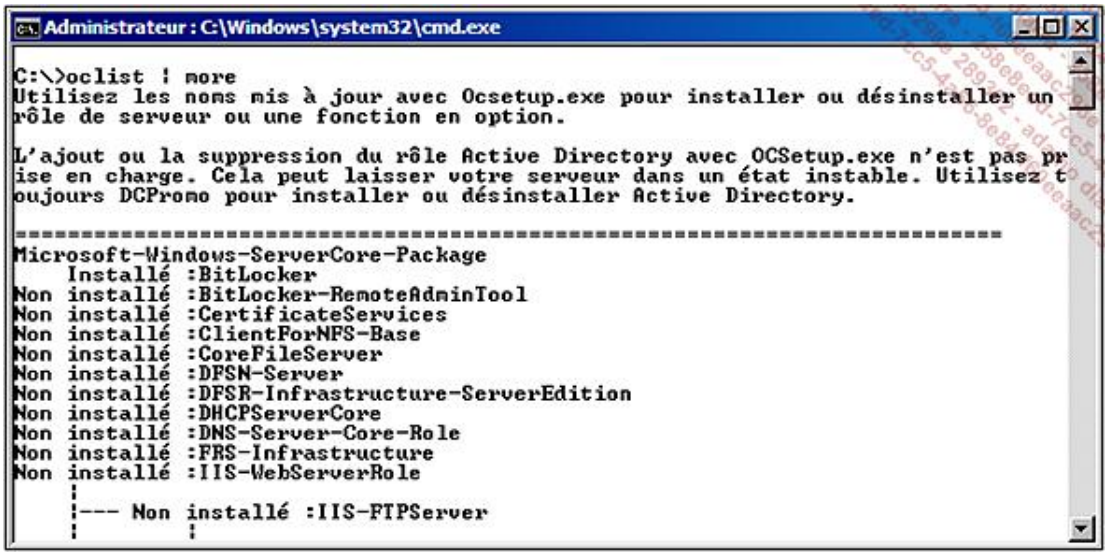
Mise en place d'un serveur Core et des applications associées

1. Installation des rôles et des fonctionnalités

Contrairement à la version complète, l'utilitaire d'installation en ligne de commande `servermanagercmd` n'est pas disponible. À la place, il faut utiliser `oclist` et `ocsetup`. Le premier établit un listing des rôles installés ou non, et le second permet de les installer et de les supprimer.

Attention, ocsetup est sensible à la casse. Ainsi, la commande ocsetup BitLocker échouera, alors que ocsetup BitLocker fonctionnera.

Exemple de sortie écran avec `oclist` :



a. Les rôles réseaux

L'installation des rôles réseaux se limite à une simple commande. Il est recommandé de les démarrer avec `start /w` afin de ne pas avoir un retour au prompt avant que l'installation ne soit effectivement terminée. Voici les commandes permettant l'installation des différents rôles réseaux disponibles. Ces rôles sont peu consommateurs en ressources systèmes mais sont nécessaires en permanence. Utiliser une installation minimale permet de les sécuriser, et limiter les coupures de services grâce à la réduction du nombre de mises à jour de sécurités à installer.

Installer le rôle DHCP Server

```
start /w ocsetup DHCPServerCore
sc config dhcpserver start=auto
net start dhcpserver
```

Pour autoriser le serveur DHCP, exécutez :

```
netsh dhcp add server dc2008.masociete.local 192.168.4.15
```

Si le serveur devient contrôleur de domaine par la suite, il faudra l'autoriser à nouveau.

Pour créer un scope sur le serveur DHCP :

```
netsh dhcp server add scope 192.168.4.0 255.255.255.0
"Scope de Ma Societe"
```

Pour définir une plage d'adresses IP :

© ENI Editions - All rights reserved - adamo diarra

```
netsh dhcp server scope 192.168.4.0 add iprange
192.168.4.100 192.168.4.250
```

Pour définir une plage d'exclusions :

```
netsh dhcp server scope 192.168.4.0 add excluderange
192.168.4.1 192.168.4.99
```

Pour fournir l'adresse IP de la passerelle par défaut et les serveurs DNS dans les baux DHCP :

```
netsh dhcp server scope 192.168.1.0 set optionvalue 003
ipaddress 192.168.4.254
netsh dhcp server scope 192.168.4.0 set optionvalue 006
ipaddress 192.168.4.15 192.168.4.16
```

Pour fournir le suffixe DNS dans le bail DHCP :

```
netsh dhcp server scope 192.168.4.0 set optionvalue 015
String masociete.local
```

Pour activer le scope :

```
netsh dhcp server scope 192.168.4.0 set state 1
```

Installer le rôle DNS server

Tout comme le rôle précédent, l'installation se résume à une simple commande :

```
start /w ocsetup DNS-Server-Core-Role
```

Pour ajouter une zone DNS primaire sur le serveur :

```
dnscmd /zoneadd masociete.local /primary
```

L'ajout manuel d'entrées est très simple. Par exemple, pour déclarer un second serveur DNS pour la zone :

```
dnscmd /recordadd madociete.local @ NS
dc02.masociete.local
```

La zone n'accepte pas par défaut les mises à jour dynamiques. Pour les autoriser, il faut utiliser la commande :

```
dnscmd /config masociete.local /allowupdate 1
```

Vous pouvez voir toutes les entrées d'une zone en ligne de commande :

```
dnscmd /zoneprint masociete.local
```

Pour lister toutes les zones déclarées sur le serveur :

```
dnscmd /enumzones
```

Windows Server 2008 R2 inclut la sécurisation du DNS (DNSSEC), permettant de vérifier que la source est digne de confiance pour la résolution et le transfert de zones. Une infrastructure de type PKI permettra de protéger les entrées DNS.

Installer le rôle IIS server

Depuis IIS 7.0, presque toutes les fonctionnalités sont vues comme des modules, l'objectif étant d'installer le strict nécessaire, tant pour la sécurité que pour les performances. L'implémentation du rôle IIS est un peu particulière dans l'installation. Le rôle est installé en exécutant la commande :

```
start /w ocsetup IIS-WebServerRole
```

Cependant, seuls quelques composants sont installés par défaut :

© ENI Editions - All rights reserved - adamo diarra

- IIS-WebServer
- IIS-ApplicationDevelopment
- IIS-CommonHttpFeatures
- IIS-HealthAndDiagnostics
- IIS-Performance
- IIS-Security
- IIS-WebServerManagementTools
- IIS-ASPNET
- IIS-NetFxExtensibility
- IIS-ManagementService
- WAS-NetFxEnvironment
- WAS-ConfigurationAPI

Contrairement à l'installation complète, les composants suivants ne sont pas disponibles :

- IIS-ManagementConsole
- IIS-LegacySnapIn
- IIS-FTPManagement

Par exemple, pour installer le module PHP sur un serveur Core :

- Téléchargez l'archive zip PHP sur un partage depuis une machine disposant d'un navigateur Internet : http://www.php.net/downloads.php
- Décompressez le contenu et déplacez-le dans %SystemDrive%\PHP.
- Renommez le fichier **php.ini-recommended** en **php.ini** dans ce répertoire.
- Installez les composants suivants :
    - IIS-WebServer
    - IIS-CommonHttpFeatures
    - IIS-StaticContent
    - IIS-DefaultDocument
    - IIS-DirectoryBrowsing
    - IIS-HttpErrors
    - IIS-HttpLogging

© ENI Editions - All rights reserved - adamo diarra

- IIS-LoggingLibraries
- IIS-RequestMonitor
- IIS-RequestFiltering
- IIS-HttpCompressionStatic
- IIS-CGI
- IIS-WebServerManagementTools
- WAS-WindowsActivationService
- WAS-ProcessModel

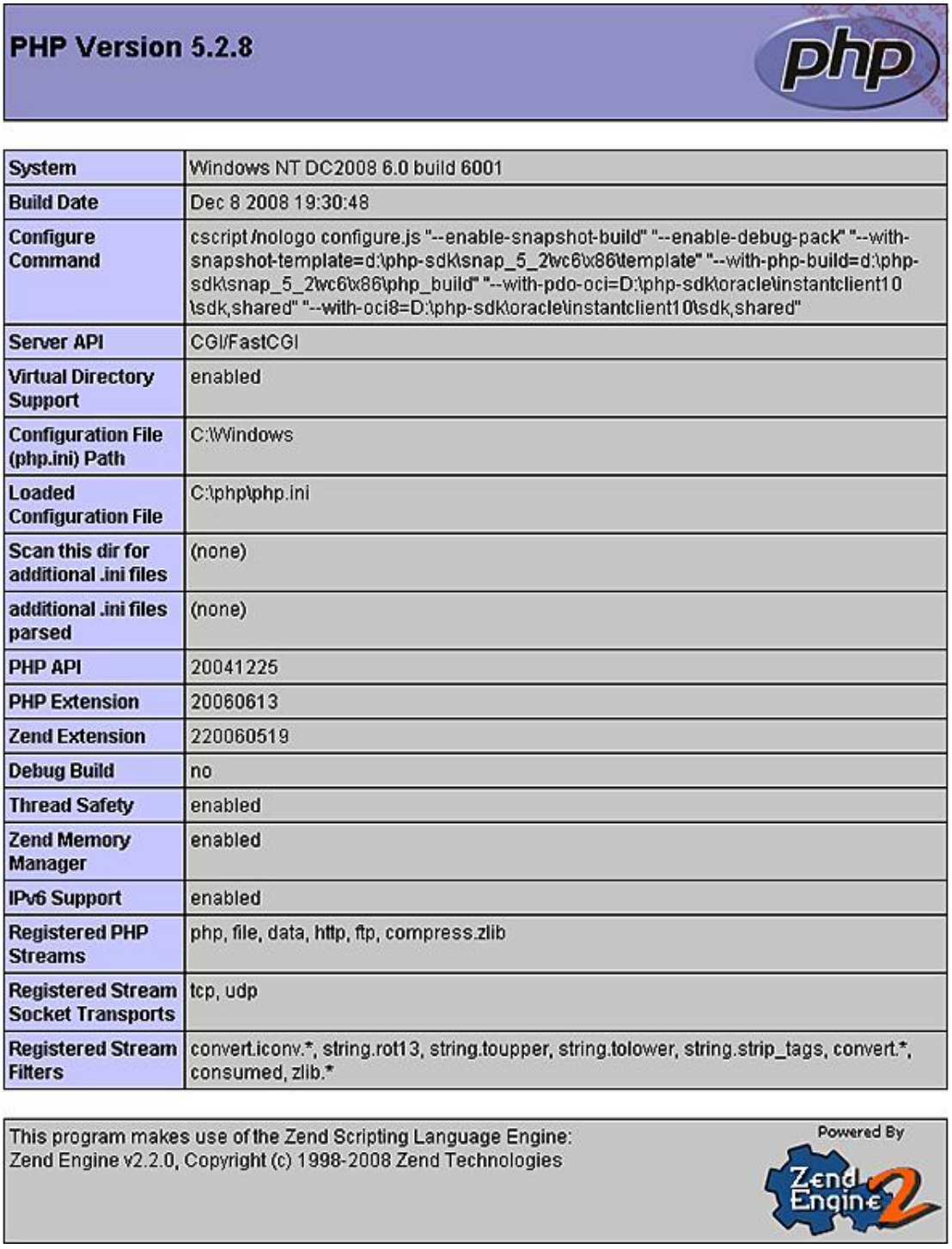
- Activez PHP dans IIS en ajustant la lettre de lecteur en fonction de votre environnement :

```
%WinDir%\System32\InetSrv\AppCmd set config
/section:system.webServer/fastCGI /+[fullPath='c:\php\php-
cgi.exe']

%WinDir%\System32\InetSrv\AppCmd set config
/section:system.webServer/handlers /+[name='PHP-
FastCGI',path='*.php',verb='*',modules='FastCgiModule',script
Processor='c:\php\php-cgi.exe',resourceType='Either']
```

Vous pouvez ensuite créer une page test.php avec à l'intérieur le code suivant, par exemple dans **%systemdrive%\inetpub\www\test.php** : `<?php phpinfo();?>`.

Une page semblable à celle-ci doit s'afficher :

© ENI Editions - All rights reserved - adamo diarra



PHP Version 5.2.8

System	Windows NT DC2008 6.0 build 6001
Build Date	Dec 8 2008 19:30:48
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared"
Server API	CGI/FastCGI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\php\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib
Registered Stream Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2008 Zend Technologies

Powered By Zend Engine 2

b. Le rôle serveur de fichiers

Contrairement aux rôles réseaux, plusieurs services de rôles sont proposés en fonction de vos besoins. Vous pouvez donc choisir d'installer ou non FRS, RFRS, DFS, SIS et même NFS. Le chapitre Architecture distribuée d'accès aux ressources de ce livre couvre en détail la gestion distribuée de ressources via DFS, nous allons donc ici nous intéresser aux spécificités liées à l'installation Core. Ce type d'installation est pertinent pour ce rôle dont la disponibilité est vitale pour la plupart des utilisateurs. Davantage de mémoire peut être utilisée pour le cache de fichiers grâce à l'empreinte plus faible du système, et la réduction du nombre de mises à jour réduit les interruptions de services.

- Installation du service minimum de partage de fichiers :

```
start /w ocsetup CoreFileServer
```

© ENI Editions - All rights reserved - adamo diarra

- Installation du service FRS :

```
start /w ocsetup FRS-Infrastructure
```

- Installation du service RFRS :

```
start /w ocsetup DFSR-Infrastructure-ServerEdition
```

- Installation du service DFS :

```
start /w ocsetup DFSN-Server
```

- Installation du service NFS :

```
start /w ocsetup ServerForNFS-Base
```

```
start /w ocsetup ClientForNFS-Base
```

Windows Server 2008 R2 introduit le service FSRM (*File Server Resource Manager*) sur l'édition Core. Cela permet de gérer le stockage bureautique (gestion de quota, blocage des fichiers par extension et rapports sur la consommation de l'espace disque).

Pour installer FSRM :

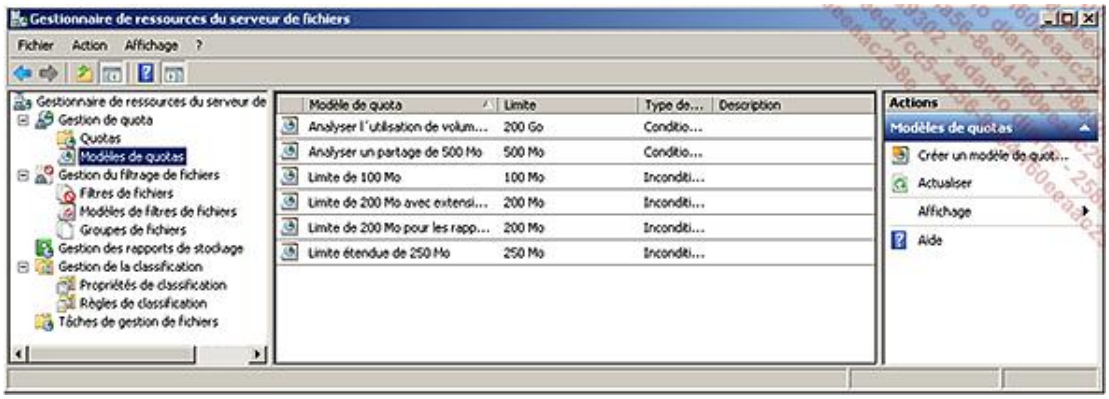
```
start /w ocsetup FSRM-Infrastructure-Core
```

La console **Gestionnaire de ressources du serveur de fichiers** doit être installée sur la machine utilisée pour gérer FSRM :

```
Import-module servermanager
Add-WindowsFeature RSAT-FSRM-Mgmt
```

Il suffit ensuite d'ajouter les exceptions sur le pare-feu pour gérer à distance les partages (sur le serveur Core en entrée et sur la machine exécutant le gestionnaire de serveur) :

```
netsh advfirewall firewall set rule group= "Gestion de ressources du serveur
de fichiers à distance" new enable="yes"
netsh advfirewall firewall set rule group= "Gestion des volumes à distance"
new enable="yes"
```



c. Le rôle serveur d'impression

Le rôle de serveur d'impression s'installe en une ligne de commande :

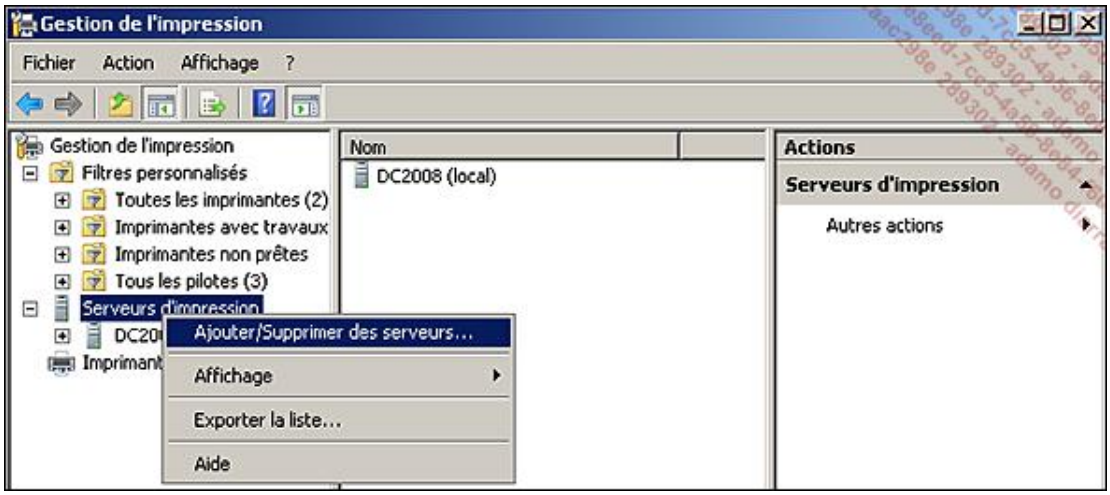
```
start /w ocsetup Printing-ServerCore-Role
```

Ajouter une imprimante sur le serveur :

© ENI Editions - All rights reserved - adamo diarra

Depuis un ordinateur Windows Vista/7 ou un autre Windows Server 2008/2008 R2 non Core, lancez la console de **gestion des imprimantes**. Si elle n'est pas présente sur un Windows Server 2008/2008 R2, vous pouvez l'ajouter indépendamment avec la commande :

```
servermanagercmd -i RSAT-Print-Services
```



Il suffit ensuite de gérer le rôle comme sur l'édition complète.

2. Service d'annuaire (AD)

Contrairement aux autres rôles, il n'est pas possible de le configurer après son installation. Il faut lui fournir certaines informations au moment de l'installation alors qu'il n'y a pas d'interface graphique. La solution consiste à passer par un fichier texte de réponses, qui doit être placé sur le serveur au préalable. Une fois le fichier de réponses prêt, il suffit d'exécuter la commande :

```
dcpromo /unattend:c:\monfichierunattend.txt
```

Voici quelques fichiers d'exemples afin de vous faciliter la création du fichier de réponses. Pour créer ces fichiers de réponses, vous pouvez utiliser notepad, qui est présent sur une installation Core (pratique, non ?).

Afin d'obtenir un contrôleur de domaine en lecture seule (RODC), il faut positionner `ReplicaOrNewDomain` à `ReadOnlyReplica`.

Fichier de réponses du premier serveur d'une nouvelle forêt :

```
[DCINSTALL]
ReplicaOrNewDomain=Domain
NewDomain=forest
InstallDNS=yes
NewDomainDNSName= masociete.local
DomainNetbiosName=masociete
ForestLevel=3
DomainLevel=3
SiteName=Default-First-Site-Name
DatabasePath=%systemroot%\ntds
LogPath=%systemroot%\ntds
SYSVOLPath=%systemroot%\sysvol
SafeModeAdminPassword=Passw0rd
RebootOnCompletion=Yes
```

Fichier de réponses du premier serveur d'une nouvelle arborescence dans une forêt existante :

```
[DCINSTALL]
UserName=administrateur
UserDomain=masociete
Password=Passw0rd
NewDomain=tree
NewDomainDNSName=masociete2.local
SiteName=Default-First-Site-Name
```

© ENI Editions - All rights reserved - adamo diarra

```
DomainNetBiosName= masociete2.local
ReplicaOrNewDomain=Domain
DomainLevel=3
DatabasePath=”%systemroot%\NTDS”
LogPath=”%systemroot%\NTDS”
SYSVOLPath=”%systemroot%\SYSVOL”
InstallDNS=yes
CreateDNSDelegation=yes
DNSDelegationUserName=administrateur
DNSDelegationPassword= Passw0rd
SafeModeAdminPassword=Passw0rd
RebootOnCompletion=yes
```

Fichier de réponses du premier serveur d’un nouveau domaine enfant dans une forêt existante :

```
[DCINSTALL]
ParentDomainDNSName=masociete.local
UserName=administrateur
UserDomain=masociete
Password=Passw0rd
NewDomain=childChild
Name=masociete2
SiteName=Default-First-Site-Name
DomainNetBiosName=masociete2
ReplicaOrNewDomain=domain
DomainLevel=3
DatabasePath=”%systemroot%\NTDS”
LogPath=”%systemroot%\NTDS”
SYSVOLPath=”%systemroot%\SYSVOL”
InstallDNS=yes
CreateDNSDelegation=yes
DNSDelegationUserName=administrateur
DNSDelegationPassword= Passw0rd
SafeModeAdminPassword=Passw0rd
RebootOnCompletion=yes
```

Fichier de réponses du second serveur d’un domaine :

```
[DCINSTALL]
UserName=administrateur
UserDomain=masociete
Password=Passw0rd
SiteName=Default-First-Site-Name
ReplicaOrNewDomain=replica
DatabasePath=”%systemroot%\NTDS”
LogPath=”%systemroot%\NTDS”
SYSVOLPath=”%systemroot%\SYSVOL”
InstallDNS=yes
ConfirmGC=yes
SafeModeAdminPassword=Passw0rd
RebootOnCompletion=yes
```

Sachez également que ce fichier de configuration pourra être créé à l’issu de l’installation d’un contrôleur de domaine par l’assistant en mode graphique.

3. Exécuter des applications 32 bits

Windows Server 2008 R2 est un système d’exploitation uniquement 64 bits. Cependant, les applications 32 bits peuvent encore fonctionner par une émulation (Wow64 pour Windows On Windows). L’objectif étant de réduire la surface d’attaque, notamment en rendant les virus ou vers 32 bits inopérants, il est donc conseillé de désactiver l’émulation Wow64 si vous n’avez pas d’applications la nécessitant. Pour cela, il suffit de supprimer le package ServerCore-WOW64 :

```
Start /w ocsetup ServerCore-WOW64 /uninstall
```

Vous disposez maintenant d’un serveur Core complètement fonctionnel dans votre environnement. Certains usages ont été présentés, d’autres comme Hyper-V sont décrits dans le chapitre Consolider vos serveurs. Les avantages de

© ENI Editions - All rights reserved - adamo diarra

cette installation minimum sont réels, la difficulté principale étant d'appréhender son administration au quotidien. Server Core signe-t-il la fin du clivage entre interface Windows et shell Unix ?

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre est dédié à la solution de virtualisation Microsoft, Hyper-V. Contrairement aux produits précédents de Microsoft sur le sujet, comme Virtual Server, la virtualisation a été pensée dès la conception du système d'exploitation. Ce véritable hyperviseur est même disponible gratuitement (sans achat de licence Windows Server 2008 R2) chez Microsoft. Dans ce chapitre, vous découvrirez comment rentabiliser davantage votre infrastructure existante et la rendre plus souple face aux changements.

© ENI Editions - All rights reserved - adamo diarra

Pourquoi consolider ?

La virtualisation est de plus en plus répandue dans les entreprises. Elle ne doit pas pour autant être systématique. Avant de lancer un projet de virtualisation, vous devez en mesurer toutes les conséquences ainsi que tous les avantages potentiels. Comme pour beaucoup de choses, il est recommandé de penser grand mais de commencer petit.

1. Virtuel versus Physique

En première approche, virtualiser permet de s'affranchir des contraintes matérielles tout en permettant un meilleur rendement. L'approche par des serveurs physiques est la plus simple au départ, mais elle se complique avec le nombre. En plus de la maintenance des systèmes d'exploitation et des applications, il faut gérer le cycle de vie du matériel :

- pannes matérielles,
- mises à jour des Bios, firmwares, pilotes,
- cycles d'amortissement.

Bien sûr, les solutions à ces problèmes sont bien connues et peuvent tout à fait être gérées dans les règles de l'art. Mais il y a toujours le risque d'un nouveau modèle de serveur qui vient en remplacement du précédent, pour lequel votre image d'installation de Windows ne contient pas le bon pilote. La virtualisation vous propose de masquer cette gestion afin de vous consacrer à des tâches présentant plus de valeur ajoutée.

a. Optimisation des coûts

Un des objectifs de la virtualisation est la réduction des coûts d'infrastructure. Pour y parvenir, un des grands axes est l'optimisation des ressources disponibles. Les capacités des serveurs continuent d'évoluer de façon importante, mais les besoins applicatifs ne suivent pas toujours la même progression. Même le serveur le moins cher proposé chez les constructeurs a au moins un processeur double ou quadruple cœurs, quelques gigaoctets de mémoire vive et du stockage SAS conséquent. Si un serveur héberge une ou même plusieurs applications, il n'utilisera sûrement qu'un modeste pourcentage de ces ressources. La plupart des éditeurs continuent par ailleurs à demander un serveur dédié pour assurer le support de leurs logiciels. Il en résulte des salles machines contenant beaucoup de serveurs, mais chacun d'eux étant utilisé à moins de 10 % de sa capacité. La virtualisation permet de maintenir un cloisonnement logique, dans un système d'exploitation dédié, tout en mutualisant l'infrastructure matérielle. Cette mutualisation physique a déjà un impact fort sur les coûts :

- Réduction de l'ensemble des coûts liés à la salle machine : électrique, climatique, câblages, encombrement au sol...
- Réduction des coûts de maintenance, proportionnellement aux nombres de serveurs physiques économisés.

La virtualisation réduit aussi les coûts liés à l'ajout d'un nœud dans l'infrastructure. La génération d'une machine virtuelle n'entraîne pas de coûts de câblage informatique, de mise en rack... Cette économie prend tout son sens dans un environnement où le nombre de demandes est important, comme dans les environnements de développement et de recette. La solution SCVMM (*System Center Virtual Machine Manager*) permet même l'implémentation d'un portail libre service pour la création de machines virtuelles à la demande.

Un usage un peu moins conventionnel est d'utiliser la virtualisation pour maintenir en fonctionnement des systèmes vieillissants, dont le matériel n'est plus maintenu ou maintenable. La plupart des systèmes d'informations possèdent quelques systèmes obsolètes, avec des applications pour lesquelles ils n'existe plus de documentation ni de sources. Les migrer sur des machines virtuelles permet de les maintenir dans le système d'information tout en évitant les problèmes matériels.

b. Les limites de la virtualisation

Tout n'est pas forcément un bon candidat à la virtualisation. La solution Hyper-V ne supporte pas l'ensemble des systèmes d'exploitation Microsoft par exemple. L'article 954958 de la base de connaissances recense les versions serveurs et clientes supportées par Hyper-V. Au moment de l'écriture de cet ouvrage, les versions suivantes sont supportées :

Côté serveur :

© ENI Editions - All rights reserved - adamo diarra

- Windows 2003 SP2, 2008, 2008 R2 en 32 et 64 bits ;
- Windows 2000 Server Service pack 4 ;
- SUSE Linux Enterprise Server 10 Service pack 1 et 2, en 32 et 64 bits.

Côté client :

- Windows XP SP2 et SP3, Vista SP1 et 7 en 32 et 64 bits.

Certains éditeurs ne supportent pas encore leur progiciel en environnement virtuel. Microsoft tient pour sa part à jour la liste de leurs logiciels supportés en environnement virtuel avec Hyper-V : http://support.microsoft.com/kb/957006.

Ainsi que ceux qui ne le sont pas (à ce jour, les autres solutions de virtualisation Microsoft dans des VM ainsi que le rôle serveur de fax Microsoft) : http://support.microsoft.com/kb/958664.

Certains éléments d'architecture ne doivent pas cohabiter sur la même infrastructure à des fins de disponibilité. Par exemple, deux serveurs DNS ou DHCP ne devraient pas être sur le même serveur Hyper-V. Dans le cas contraire, en cas de défaillance de celui-ci, ces services deviennent indisponibles en même temps alors qu'ils sont présents deux fois sur le réseau afin d'être très disponibles. Des services différents qui ont une forte activité en même temps devraient être sur des serveurs Hyper-V différents, afin de ne pas charger négativement l'infrastructure virtuelle. Des règles d'affinité et d'anti-affinité devraient être définies. Enfin, les solutions nécessitant des cartes matérielles (cartes numéris, accès primaire...) ou les solutions utilisant des dongles sont très difficiles à migrer vers un environnement virtuel. Les ports COM du serveur physique ne sont pas accessibles depuis les machines virtuelles, tout comme le lecteur de disquettes.

2. De nouvelles problématiques

Il serait illusoire de penser que la virtualisation n'amène que des avantages et aucun inconvénient. Comme toute solution technique, l'important est de la maîtriser afin d'en tirer parti. Deux sujets au moins nécessitent une attention particulière : les impacts de la mutualisation et la sauvegarde.

a. Environnement mutualisé

La mutualisation est un axe classique de rentabilisation, mais il devient beaucoup plus sensible avec la virtualisation, car poussé à l'extrême. Elle part du postulat que la plupart des systèmes ne consomment pas les ressources matérielles qui sont disponibles et les mutualisent donc pour les rentabiliser. Mais nous pouvons rarement prévoir la charge que vont générer les utilisateurs sur l'ensemble des systèmes virtuels à un instant T. Il se peut donc que plusieurs VM veuillent soudainement consommer le maximum disponible, perturbant ainsi les autres VM. La performance peut rapidement devenir un frein à la virtualisation si elle n'est pas gérée correctement. Le phénomène classique est que les utilisateurs constatent des lenteurs, qu'ils associent immédiatement au fait qu'il s'agit d'une machine virtuelle. Ils deviennent ainsi réfractaires à leur utilisation, pensant que c'est la cause unique de ces lenteurs. D'autant que ce type de problème peut apparaître de façon insidieuse avec le temps. Cette lenteur à l'utilisation apparaît aussi quand, au contraire, les performances sont là et que le succès de la solution incite à mettre en service plus de machines virtuelles que le dimensionnement de l'infrastructure ne le prévoyait. Tout projet de virtualisation devrait avoir un plan de capacité, maintenu à jour en permanence. Si le système à virtualiser est déjà en cours d'utilisation, journalisez au maximum l'utilisation des ressources au préalable. Cela permettra de prédire son impact sur l'infrastructure Hyper-V ainsi que les ressources à y allouer. Hyper-V permet de limiter la consommation de chaque machine virtuelle, ainsi que de garantir une certaine quantité de ressources à tout instant. La réservation de ressources a l'inconvénient de les bloquer, même si la machine virtuelle ne l'utilise pas. La limite permet de restreindre une machine virtuelle qui est soit non critique, comme une machine de test, soit qui consomme toutes les ressources disponibles, comme un serveur de traitements massifs. Vous pouvez aussi attribuer un poids à chaque machine virtuelle, permettant ainsi de prioriser l'accès aux ressources disponibles qui ne sont pas réservées. Si deux machines virtuelles demandent plus de ressource processeur en même temps par exemple, celle qui a le plus de poids sera prioritaire. Vous pouvez allouer de 1 à 4 processeurs virtuels à chaque machine virtuelle, du moment que vous disposez du nombre de cœurs physiques correspondants. Sur un serveur physique ayant quatre cœurs, chaque VM peut donc avoir quatre processeurs logiques. Les serveurs actuels ont généralement au moins deux voir quatre cœurs, ce qui est le plus rentable pour la virtualisation. Si vous assignez à chaque VM deux processeurs logiques, cela permet de maintenir un temps de réponse correct sur une VM, même si un processeur logique est consommé en entier par un programme ou un traitement. Si vous n'allouez qu'un seul processeur logique et qu'un thread consomme tous les cycles en boucle, il vous sera peut être même difficile d'accéder au système pour stopper ce processus. Ce phénomène est aussi vrai sur une machine physique avec un seul cœur, mais il est amplifié par la virtualisation et n'est plus présent dans l'esprit des utilisateurs qui ont généralement au moins deux cœurs sur leur station (Hyper Threading ou dual core).

La perte d'un serveur physique Hyper-V a des conséquences beaucoup plus graves qu'un serveur sans virtualisation. En effet, ce type de serveur héberge potentiellement plusieurs VM (une dizaine ?), qui vont toutes être indisponibles

© ENI Editions - All rights reserved - adamo diarra

en même temps. Il faut donc être préparé à ce scénario, afin de prendre de bonnes décisions, comme l'ordre dans lequel remettre en service ces VM. Il est recommandé de déployer au moins deux serveurs Hyper-V, afin d'avoir un plan de reprise rapide en cas de défaillance grave d'un des deux serveurs.

b. Sauvegarde

La sauvegarde d'une infrastructure virtuelle est un sujet d'attention particulier. Plusieurs implémentations sont possibles, vous devrez trouver celle qui vous apporte le plus de souplesse, tout en limitant les contraintes et les coûts associés. Votre objectif doit être de répondre à vos besoins de la manière la plus adaptée dans votre contexte, en respectant vos engagements de services auprès de vos clients.

Trois grands axes de sauvegarde sont possibles :

- Traiter les machines virtuelles comme s'il s'agissait de serveurs standards, en installant l'agent de sauvegarde traditionnel sur chaque machine virtuelle.
- Implémenter une sauvegarde en utilisant les possibilités offertes par l'infrastructure virtuelle.
- Sauvegarder les disques virtuels des machines virtuelles à froid, c'est-à-dire VM arrêtées.

La première solution a l'avantage d'être très classique, mais elle est aussi sûrement la plus coûteuse, car elle n'apporte pas d'économie liée à la virtualisation. Certains éditeurs de solution de sauvegarde proposent cependant un prix par agent inférieur quand il s'agit de machines virtuelles.

Nous allons nous attacher aux solutions de sauvegardes qui prennent en compte les fonctionnalités offertes par la virtualisation. Une machine virtuelle peut avoir plusieurs états :

- Allumée ou Éteinte ;
- En pause ;
- Avec une ou plusieurs images instantanées (ou aucune).

Les images instantanées permettent de prendre une « photo » de la VM à un instant T. Pour cela, Hyper-V va créer un nouveau disque virtuel (*.avhd) qui contiendra toutes les différences générées après cette image. Cela ne constitue pas pour autant un mécanisme de sauvegarde à lui tout seul. Le fichier maître est indispensable pour son fonctionnement, et ne peut donc pas être hors de la VM. Cette fonctionnalité n'est pas disponible pour les disques physiques attachés directement à la VM (pass-through). Pour certains rôles, comme le contrôleur de domaine, cette fonctionnalité n'est même pas supportée par Microsoft. En revanche, cette fonctionnalité est vraiment un « must » par ailleurs. Le nombre maximum d'images instantanées est de 50 par machine virtuelle.

Les sauvegardes à froid sont la solution la plus simple, mais impliquent une période d'arrêt qui n'est pas toujours possible. Un redémarrage du système d'exploitation peut générer des pertes de performances si un cache en mémoire est utilisé (SQL Server...).

Votre solution de sauvegarde peut proposer un agent de sauvegarde pour Hyper-V. Ce mécanisme utilise la technologie VSS (*Volume Shadowcopy Service*). Vous obtiendrez ainsi des copies autonomes des machines virtuelles, que vous pouvez déplacer ou conserver sur bande, sans temps d'arrêt. La solution de sauvegarde Microsoft DPM (*Data Protection Manager*) ainsi que la solution de sauvegarde native Windows Server 2008 R2 sont compatibles avec ce type de sauvegarde. Pour que ce type de solution fonctionne, certains pré-requis doivent être remplis :

- Les outils Services d'invité virtuel doivent être installés et le service Backup integration doit être actif.
- Tous les volumes utilisés par la VM doivent être en mode basique et formatés en NTFS.
- Le service Windows VSS doit être actif sur tous les volumes et chaque volume doit avoir son stockage VSS sur lui-même.

Si une sauvegarde en ligne ne peut pas être effectuée, alors une sauvegarde à froid de la machine sera effectuée. Pour cela, son état sera sauvegardé et, une fois la sauvegarde terminée, la VM sera mise de nouveau dans l'état antérieur à la sauvegarde. Ce type de sauvegarde permet de restaurer entièrement une machine virtuelle, mais pas une partie de celle-ci (comme un fichier du disque C:\ dans cette machine). Il ne faut pas lancer de sauvegarde ou de restauration à la fois sur une machine virtuelle et sur la partition racine. Vous pourriez générer des conflits si chaque instance essaye de verrouiller l'enregistreur VSS.

Voici une commande pour sauvegarder l'intégralité d'un serveur Hyper-V ainsi que l'ensemble des machines virtuelles à chaud :

© ENI Editions - All rights reserved - adamo diarra

```
wbadmin start backup -backuptarget:\\
autreserveur\partages\sauvegardes -include:c:,d: -
allcritical -vssfull -quiet
```

3. Préparer son déploiement

a. Pré-requis

Pour pouvoir porter le rôle Hyper-V, un serveur physique doit avoir des fonctionnalités de virtualisation (Intel-VT ou AMD-V) et de sécurité (Intel XD ou AMD NX). Cela est bien sûr en supplément des instructions 64 bits indispensables pour Windows Server 2008 R2 et pour Hyper-V de manière générale. Hyper-V supporte jusqu'à 32 processeurs sur le serveur physique (et non plus 16 comme c'était le cas sous Windows Server 2008), qu'ils proviennent de cœurs physiques ou logiques via Hyper Threading.

Windows Server 2008 R2 est capable de tirer également parti des fonctionnalités d'arrêt de cœur (Core Parking) et d'un deuxième niveau de translation, Extended Page Tables (EPT) chez Intel, Nested Page Tables (NPT) chez AMD. Le premier permet de réduire la consommation électrique en arrêtant les cœurs non utilisés. Le deuxième permet d'économiser environ 2% de temps processeur et 1 Mo par machine virtuelle.

Une installation minimale (Core) est fortement recommandée. Le chapitre Limiter les possibilités d'attaque avec Server Core de cet ouvrage couvre ce type d'installation.

La mémoire maximum est déterminée par le système d'exploitation. Windows Server 2008 R2 édition standard autorise 32 gigaoctets pour la partition racine et jusqu'à 31 gigaoctets par machine virtuelle.

Windows Server 2008 R2 versions Entreprise et Datacenter permettent un maximum de 2 téra-octets pour la partition racine et jusqu'à 64 gigaoctets par machine virtuelle.

Il est recommandé d'avoir au moins deux cartes réseaux physiques (voir plus loin Respect des meilleures pratiques). Chaque machine virtuelle peut avoir jusqu'à 12 cartes réseaux virtuelles (8 synthétiques + 4 émulées), chacune avec une adresse MAC statique ou dynamique. Les cartes réseaux synthétiques sont disponibles une fois les services d'invité virtuel, et donc les pilotes adéquats, installés. Les cartes réseaux émulées sont moins performantes. Elles utilisent un pilote standard qui ne nécessite pas les pilotes Hyper-V. Cela souligne l'importance de n'installer que des systèmes d'exploitation supportés par Hyper-V afin d'avoir un réseau virtuel performant. La technologie VLAN est supportée sur les cartes réseaux virtuelles. Un réseau virtuel ne peut pas être connecté à une carte réseau sans fil. Les machines virtuelles ne peuvent donc pas avoir de réseau sans fil.

Windows Server 2008 R2 supporte maintenant les technologies réseau suivantes :

- La technologie Jumbo Frames pour les machines virtuelles. Elle permet d'augmenter la MTU (*Maximum Transmission Unit*) de 1500 (Ethernet) à 9014. La même quantité de données peut donc être transmise avec six fois moins de paquets. Cela implique toutefois que les équipements réseaux supportent les Jumbo Frames.

- La technologie VMQ (*Virtual Machine Queue*) permet à la carte réseau d'envoyer directement les paquets réseau dans l'espace tampon en mémoire de la VM, sans passer par la partition racine. Cela évite aussi de vérifier le routage dans les switches virtuels via les VMQ Queue ID. L'objectif est un gain de performances en réduisant le nombre d'opérations à mettre en œuvre pour les communications réseaux. Le TCP Offload permet de décharger la gestion du trafic TCP/IP des machines virtuelles sur une carte physique du serveur. Ce déchargement augmente les performances et réduit la consommation processeur du serveur physique. La migration à chaud de VM peut tirer parti de cette fonctionnalité.

Un lecteur de DVD virtuel peut utiliser des images ISO ou le lecteur physique du serveur. En revanche, une seule machine virtuelle peut accéder au lecteur physique en même temps. Il est donc recommandé de convertir les CD et DVD nécessaires en images ISO.

La configuration de plusieurs cartes réseaux en équipe (teaming) n'est actuellement pas supportée avec Hyper-V par Microsoft. L'article 968703 couvre ce sujet : http://support.microsoft.com/kb/968703.

b. Méthodologie

La méthodologie est très importante dans un projet de virtualisation. Certains sujets comme la sauvegarde doivent vraiment être traités avant le passage en production. Les phases classiques d'un projet d'infrastructure s'appliquent, avec quelques spécificités :

- Déterminer le périmètre (environnements, systèmes d'exploitation...).

© ENI Editions - All rights reserved - adamo diarra

- Commencer la chasse aux candidats à la virtualisation en implémentant des outils de mesures (voir la section suivante).

- Déterminer le niveau de service à fournir sur le périmètre (SLA).

- Monter une maquette/POC (*Proof Of Concept*).

    - Utiliser l'infrastructure de stockage pressentie (interne, SAN, ISCSI, partages de fichiers...).

    - Mesurer l'intégration dans l'architecture réseau existante (VLAN, filtrage par adresse MAC, protection sur les commutateurs).

    - Implémenter au moins un exemplaire de chaque type de VM dans le périmètre (une VM de chaque OS et chaque application).

    - S'assurer de la capacité à sauvegarder et à restaurer chacune de ces VM.

    - Générer la même charge qu'en production avec les mêmes contraintes (traitements, fenêtre de sauvegarde...).

    - Implémenter la solution de supervision en prenant en compte la virtualisation (mesurer l'utilisation des processeurs disponibles dans Hyper-V ainsi que la consommation par VM...).

    - Évaluer l'intérêt de SCVMM dans votre contexte.

    - Mesurer l'impact sur la gestion des mises à jour Windows (utilisation du Offline Virtual Machine Servicing Tool au paragraphe Configuration du stockage).

    - Mesurer l'impact sur les procédures d'exploitation (procédure d'arrêt/démarrage...).

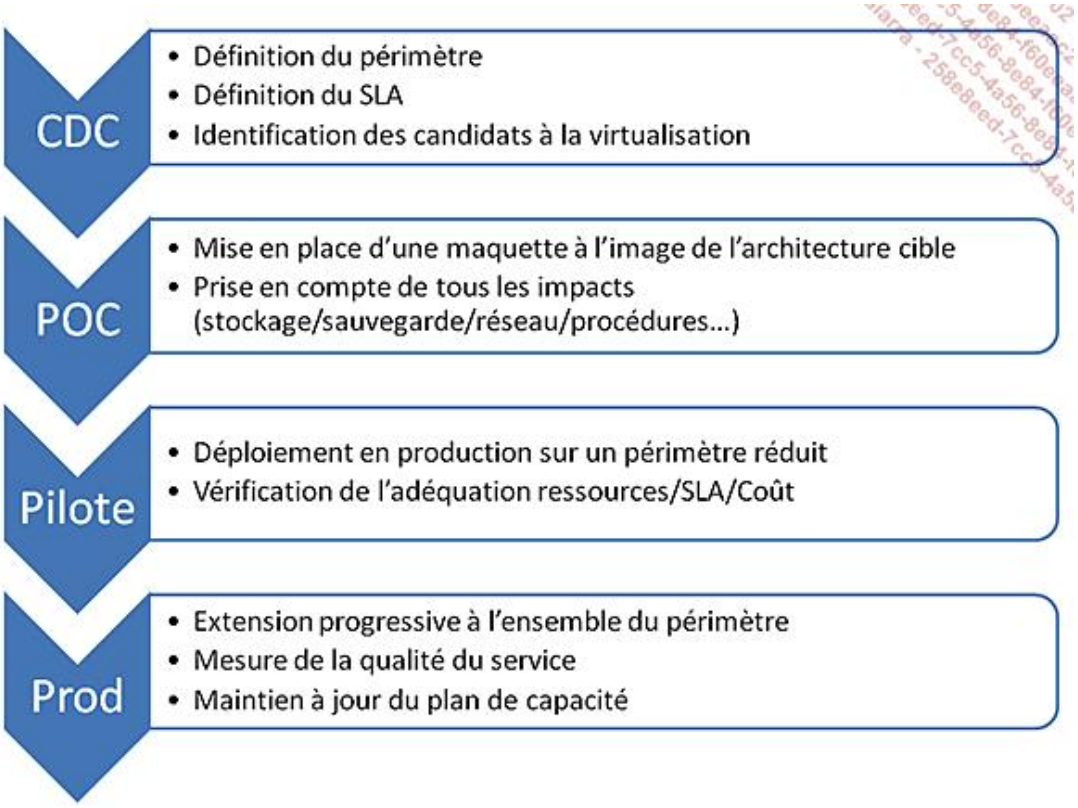
    - Évaluer l'impact sur les coûts.

- Mettre en place un pilote, qui sera la mise en production d'un échantillon du périmètre, afin de vérifier les hypothèses.

- Étendre le pilote à l'ensemble du périmètre de façon progressive.

La maquette est décisive, car elle permet de mettre en avant de nouvelles fonctionnalités, parfois importantes, de cette version et de vérifier que l'architecture pressentie tiendra la charge. Sous-évaluer cette phase risque de mener à l'échec une fois en production. La durée de cette phase doit permettre d'évaluer les impacts de la virtualisation, ainsi que les optimisations à réaliser, que ce soit sur Hyper-V, dans les machines virtuelles ou les autres briques du système d'information. Avec la maquette, tous les intervenants doivent avoir une vision claire des avantages et des inconvénients de la virtualisation afin de pouvoir faire un bilan pertinent. Le pilote doit confirmer sans réserve ce bilan avant de généraliser le déploiement.

© ENI Editions - All rights reserved - adamo diarra



c. Déterminer les serveurs et les applications propices à la virtualisation

Microsoft propose gratuitement un outil afin de préparer et accélérer votre projet de virtualisation : Microsoft Assessment and Planning Toolkit. Il est téléchargeable à cette adresse :

http://www.microsoft.com/downloads/details.aspx?familyid=67240B76-3148-4E49-943D-4D9EA7F77730&displaylang=en

Vous pouvez ainsi très facilement :

- faire un inventaire des serveurs ;
- collecter les consommations de ressources sur ces serveurs ;
- générer des rapports Office sur les données collectées avec des recommandations.

Il est à installer de préférence sur un poste de travail, car il nécessite notamment Microsoft Office (2003 ou 2007), et une instance SQL Express. L'installation de ce dernier peut être évitée s'il est déjà présent, en créant au préalable une instance nommée « MAPS ».

Une fois le logiciel installé, vous devrez :

- Créer une base pour le projet en cliquant sur **Select a database**.
- Créer manuellement un fichier texte contenant la liste des serveurs que vous souhaitez examiner pour votre projet de virtualisation (candidats potentiels). Par exemple, le script PowerShell suivant extrait le nom DNS de tous les serveurs de l'Active Directory dans le fichier **mondump.txt** :

```
$chercher = New-Object
DirectoryServices.DirectorySearcher("[ADSI]")
$chercher.SizeLimit = 10000
$chercher.PropertiesToLoad.Add("dNSHostName")
$chercher.Filter =
"(&(objectClass=Computer)(operatingSystem=*Serve*r*))"
$chercher.FindAll() | foreach-object
{$objet=$_.GetDirectoryEntry();$objet.dNSHostName;} >>
```


© ENI Editions - All rights reserved - adamo diarra

```
mondump.txt
```

- Cliquez sur **Capture performance metrics for server consolidation**.
- Indiquez le fichier texte créé précédemment.
- Spécifiez un ou plusieurs comptes ayant les droits administrateurs locaux sur les serveurs cibles.
- Spécifiez une date de fin pour la collecte des métriques. La station effectuant la collecte doit rester opérationnelle tout le temps de la collecte.
- Vous pouvez ensuite générer les rapports.

d. Respect des meilleures pratiques

Voici quelques règles considérées comme des meilleures pratiques à respecter par défaut, sauf cas particulier.

De façon générale, sur Hyper-V :

- Prévoyez au moins deux cartes réseaux physiques sur le serveur :
  - une pour la gestion de l'hyperviseur,
  - une ou plusieurs dédiées aux machines virtuelles,
  - une ou plusieurs pour le ISCSI si vous l'implémentez,
  - une pour les migrations rapides (live migration) si vous les implémentez.
- Connectez la carte réseau dédiée au management de l'hyperviseur sur votre réseau d'administration.
- N'exposez que les machines virtuelles au réseau Internet.
- Mettez une exclusion sur l'antivirus pour les fichiers *.vhd et *.avhd.
- Le lecteur DVD ne peut pas être partagé par plusieurs machines virtuelles. Privilégiez les images ISO à la place.

De façon générale, sur les machines virtuelles :

- Installez dès que possible les outils Services d'invité virtuel.
- Désactivez l'économiseur d'écran.
- Défragmentez toujours le disque physique avant de créer un disque dur virtuel.
- Si vous migrez des machines virtuelles depuis d'autres solutions de virtualisation, comme Virtual PC, Virtual Server, VMware, désinstallez les VMadditions ou les VMware Tools. Compactez le disque dur virtuel avant de le déplacer sur Hyper-V.
- Assurez-vous que l'affichage est optimisé pour les performances, afin que l'accélération matérielle soit effective.
- Créez des disques virtuels de taille fixe. Les performances sont supérieures, le système de fichiers sera moins fragmenté, et la gestion de l'espace sera plus simple.
- Si vous créez une VM Windows Server 2003, attribuez-lui deux processeurs virtuels afin d'avoir un HAL multiprocesseur.

© ENI Editions - All rights reserved - adamo diarra

- Utilisez autant que possible les pilotes synthétiques une fois les services d'invité virtuel installés, afin d'augmenter les performances.

Vous pouvez avoir un contrôleur de domaine Active Directory à l'intérieur d'une machine virtuelle Hyper-V. Cependant les règles suivantes s'appliquent :

- N'utilisez jamais la sauvegarde d'état. Cela peut engendrer des erreurs de synchronisation si vous restaurez un état antérieur aux autres contrôleurs de domaine.

- Ne mettez pas en pause un contrôleur de domaine pour une longue période, cela peut impacter la réplication. Arrêtez plutôt la machine virtuelle si nécessaire.

- Ne faites pas d'images instantanées. Cette fonctionnalité n'est pas supportée par Microsoft dans le cas d'un contrôleur de domaine.

- Choisissez comment synchroniser le temps. Il est crucial que l'ensemble du domaine soit à la même heure. Par défaut, Kerberos ne supporte qu'un écart maximum de 5 minutes. Vous pouvez soit synchroniser sur l'horloge matérielle du serveur à travers les services d'invité virtuel, soit synchroniser via le réseau du domaine.

- Si votre seul contrôleur de domaine est une machine virtuelle dans Hyper-V, la partition racine (l'hyperviseur) ne doit pas être jointe à ce domaine. Lorsque vous redémarrez le serveur, la partition racine cherchera un contrôleur de domaine qu'elle ne pourra pas trouver car la machine virtuelle ne sera pas encore démarrée.

Vous pouvez implémenter SQL Server dans une machine virtuelle. Dans ce cas, veuillez noter les remarques suivantes :

- Une machine virtuelle ne peut pas avoir plus de quatre processeurs virtuels. Votre charge SQL ne doit donc pas demander plus de quatre processeurs.

- Le stockage est un élément critique pour la base de données, et la virtualisation n'y change rien. Le stockage sur lequel résideront les données et les journaux doit fournir les performances nécessaires. Afin de ne pas diminuer ces performances avec la virtualisation, vous devriez utiliser uniquement des disques virtuels à taille fixe, en utilisant le pilote SCSI virtuel. L'autre alternative est l'utilisation de volumes directement en pass-through.

Vous pouvez implémenter Exchange Server 2007 dans une machine virtuelle. Dans ce cas, veuillez noter les remarques suivantes :

- Afin que la configuration soit supportée par Microsoft, installez le Service Pack 1 pour Exchange 2007.

- L'utilisation de disques virtuels de taille dynamique n'est pas supportée.

- L'utilisation des fonctions d'images instantanées et différencielles sur les disques virtuels n'est pas supportée.

En ce qui concerne la sécurité, vous ne devriez jamais donner de droits sur la partition racine aux administrateurs de machines virtuelles. Afin de respecter le célèbre principe du moindre privilège, vous ne devez leur accorder que le strict minimum nécessaire. Gérer cette sécurité peut devenir une tâche complexe, aussi vous pouvez utiliser la notion de rôles afin de classifier les accès.

© ENI Editions - All rights reserved - adamo diarra

Déployer Hyper-V

1. Installation

L'installation est aussi simple que l'ajout du rôle sur le serveur. Si vous avez choisi une installation Core, exécutez la commande `start /wait ocsetup Microsoft-Hyper-V`, sinon exécutez les commandes PowerShell suivante :

```
import-module servermanager
Add-WindowsFeature Hyper-V
```

Un redémarrage sera nécessaire pour prendre en compte le rôle.

Sur une installation Core, si des mises à jour sont disponibles pour le rôle Hyper-V, voici la méthode d'installation à utiliser :

```
wusa.exe nom_du_fichier.msu /quiet
```

L'état d'installation des mises à jour Windows, qu'elles soient réalisées par l'installation manuelle ou le client Windows Update, peut être vérifié en consultant les journaux d'évènements. Pour la version Core, la commande suivante les affiche sur la console :

```
wevtutil qe System /q:"*[System[Provider[@Name='Microsoft-
Windows-WindowsUpdateClient']]]" /f:Text
```

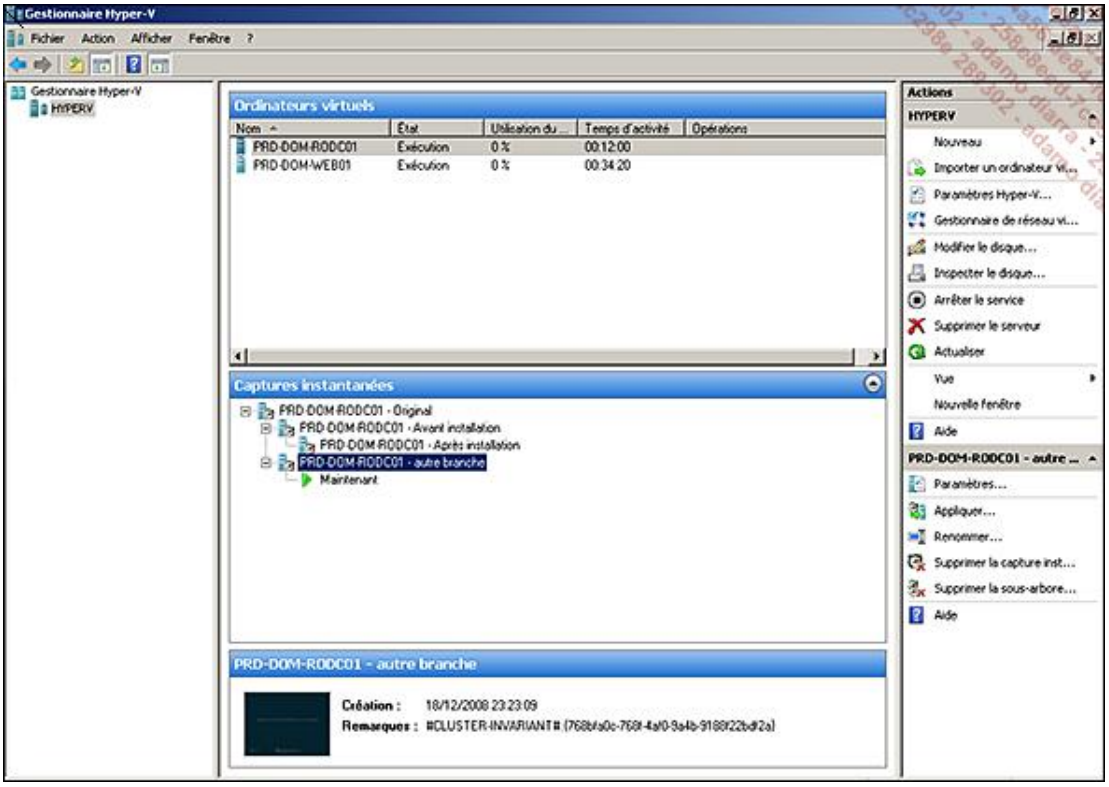
2. Configuration du rôle

La configuration du rôle couvre différents aspects :

- création et configuration des réseaux virtuels ;
- mise à disposition d'images ISO pour les différentes installations.

La console permet de gérer les serveurs Hyper-V ainsi que les machines virtuelles qu'ils hébergent. Ouvrez la console **Gestionnaire Hyper-V** en cliquant sur le bouton **Démarrer - Outils d'administration** puis **Gestionnaire Hyper-V**.

© ENI Editions - All rights reserved - adamo diarra



3. Configuration du stockage

Avec la virtualisation le stockage est le nerf de la guerre. Cela est d'autant plus vrai si les services offerts dans les machines virtuelles sont eux aussi consommateurs en entrées/sorties disques. Afin de réduire les coûts, il est intéressant d'utiliser du stockage « low cost », mais le risque est de souffrir de lenteurs certaines dans les machines virtuelles. Il vous faut donc trouver le juste équilibre, entre une solution SAN et un partage réseau ! Hyper-V supporte un large panel de solutions pour le stockage des machines virtuelles :

- Stockage local au serveur (IDE/SATA/ESATA/USB/Firewire/SAS/SCSI) ;
- Stockage sur un SAN (dont le stockage en cluster avec le mode Cluster Shared Volumes) ;
- Stockage via ISCSI ;
- Stockage sur un partage de fichiers ;
- Stockage en pass-through.

Vous pouvez même stocker les VM sur une clé USB, à condition qu'elle soit formatée en NTFS. Par défaut, vous devriez utiliser des disques virtuels. Il y a cependant certains cas où vous devrez utiliser un stockage en pass-through. Cette méthode donne un accès direct à une zone de stockage à la VM, comme si elle était une machine physique. Un des avantages est une meilleure performance, liée à l'absence de la couche de virtualisation. Voici quelques considérations à propos du mode pass-through :

- Les disques virtuels ont une limite de 2 tera-octets. L'accès en pass-through permet de lever cette limite jusqu'au maximum supporté par le système d'exploitation.
- Les volumes en pass-through ne sont pas sauvegardés par les mécanismes Hyper-V. Il vous faudra les sauvegarder par un autre moyen.
- Les mécanismes d'images instantanées ne sont pas disponibles sur ce type de volume.

Si vous choisissez de stocker les VM sur un partage de fichiers, il est recommandé de rendre ce partage hautement disponible. Le stockage via ISCSI peut se faire de deux manières, depuis la partition racine, ou depuis la machine

© ENI Editions - All rights reserved - adamo diarra

virtuelle. Ce choix a plusieurs conséquences :

- Si le stockage ISCSI est accédé depuis la partition racine, les performances sont meilleures que depuis la VM, et la sauvegarde via l'enregistreur VSS est supportée.

- Les machines virtuelles ne peuvent pas être démarrées depuis un stockage ISCSI (géré depuis les VM au lieu de la partition racine). Le stockage ISCSI accédé depuis la VM ne peut pas être sauvegardé via le VSS Hyper-V.

Un autre choix à faire porte sur la nature des contrôleurs virtuels pour les machines virtuelles. Ils peuvent être IDE ou SCSI. L'aspect performance ne joue pas du moment que les services d'invité virtuel sont installés. Les différences portent sur la volumétrie et le nombre de disques virtuels attachés à la VM. Le contrôleur SCSI ne permet pas de démarrer la VM, mais permet jusqu'à 256 périphériques de stockage (4 contrôleurs * 64 périphériques). Les volumes rattachés au contrôleur IDE sont au nombre maximum de 4 (en comptant le lecteur CD/DVD virtuel), et ont une taille maximum de 128 gigaoctets.

Le stockage sur une infrastructure SAN est généralement la solution la plus performante, et aussi la plus coûteuse. La technologie NPIV est disponible sur les cartes HBA, ce qui permet de respecter les meilleures pratiques pour le stockage SAN (zoning...). Vous devez pour cela activer les WWN (*World Wide Names*) virtuels pour les machines virtuelles. Voici quelques considérations pour le stockage sur un SAN :

- Un pilote MPIO (multiport) est nécessaire, même avec une seule HBA.

- Désactivez le montage automatique des volumes.

- Laissez les disques en basique et non en dynamique.

- Tous les fichiers de VM doivent être sur un seul volume.

- Ajoutez les LUN en tant que ressources disques au cluster avant de créer les VM. Windows Server 2008 R2 introduit les Cluster Shared Volumes, qui permettent d'avoir plusieurs VM par LUN, tout en ayant ces VM sur des hôtes différents.

Si les VM sont stockées en pass-through sur le SAN, deux LUN sont requises, une pour le disque de démarrage et une pour la configuration.

4. Configuration de la gestion de la mémoire dynamique

Le Service Pack 1 de Windows Server 2008 R2 permet de définir de façon dynamique l'allocation de la mémoire vive allouée à une machine virtuelle.

Ainsi, si une machine virtuelle lance un traitement spécifique qui utilise davantage de mémoire que ce qui lui avait été initialement alloué, Hyper-V sera en mesure d'augmenter momentanément la quantité de mémoire vive allouée à cette machine virtuelle soit directement à partir de la mémoire libre du serveur Hyper-V, soit à partir de celle inutilisée des autres machines virtuelles présentes sur le même serveur.

Une fois le traitement coûteux en mémoire terminé, la mémoire sera libérée si une autre machine en fait la demande.

La mémoire est ainsi considérée comme une ressource partagée entre les machines virtuelles. Son allocation ne nécessite plus l'arrêt de la machine virtuelle pour que la nouvelle capacité mémoire soit prise en compte.

Les pré-requis à l'utilisation de la mémoire dynamique sur Hyper-V sont les suivants :

- Le serveur hébergeant HyperV doit être sous Windows Server 2008 R2 avec le Service Pack 1 installé.

- Toutes les machines virtuelles ne supportent pas la gestion de la mémoire dynamique. Seuls les systèmes d'exploitation suivants sont compatibles avec cette fonctionnalité :

    - Windows Server 2008 R2 Standard ou Windows Server 2008 R2 Edition Web avec le SP1.

    - Windows Server 2008 R2 Enterprise ou Windows Server 2008 R2 Datacenter avec le SP1 ou les services d'intégration en SP1.

    - Windows 7 en version Entreprise ou Ultimate (32 et 64 bits) avec le SP1 ou les services d'intégration

© ENI Editions - All rights reserved - adamo diarra

en SP1.

- Windows Server 2008 SP2 Standard ou Edition Web (32 et 64 bits) avec les services d'intégration SP1 et le patch de la KB2230887 (http://go.microsoft.com/fwlink/?LinkId=206472).
- Windows Server 2008 SP Entreprise ou Datacenter (32 et 64 bits) avec les services d'intégration en SP1.
- Windows Vista SP1 en version Entreprise ou Ultimate (32 et 64 bits) avec les services d'intégration en SP1.
- Windows Server 2003 R2 SP2 Standard, Web, Entreprise ou Datacenter (32 et 64 bits) avec les services d'intégration en SP1.
- Windows Server 2003 SP2 Standard, Web, Entreprise ou Datacenter (32 et 64 bits) avec les services d'intégration en SP1.

Pour des informations plus détaillées sur sa mise en place, vous trouverez le guide de configuration de la mémoire dynamique à l'adresse suivante : http://technet.microsoft.com/en-us/library/ff817651(WS.10).aspx.

Sachez qu'il est également possible de configurer la mémoire dynamique à l'aide de PowerShell à l'adresse : http://social.technet.microsoft.com/wiki/contents/articles/hyper-v-how-to-set-dynamic-memory-using-powershell.aspx.

5. SCVMM 2008 R2

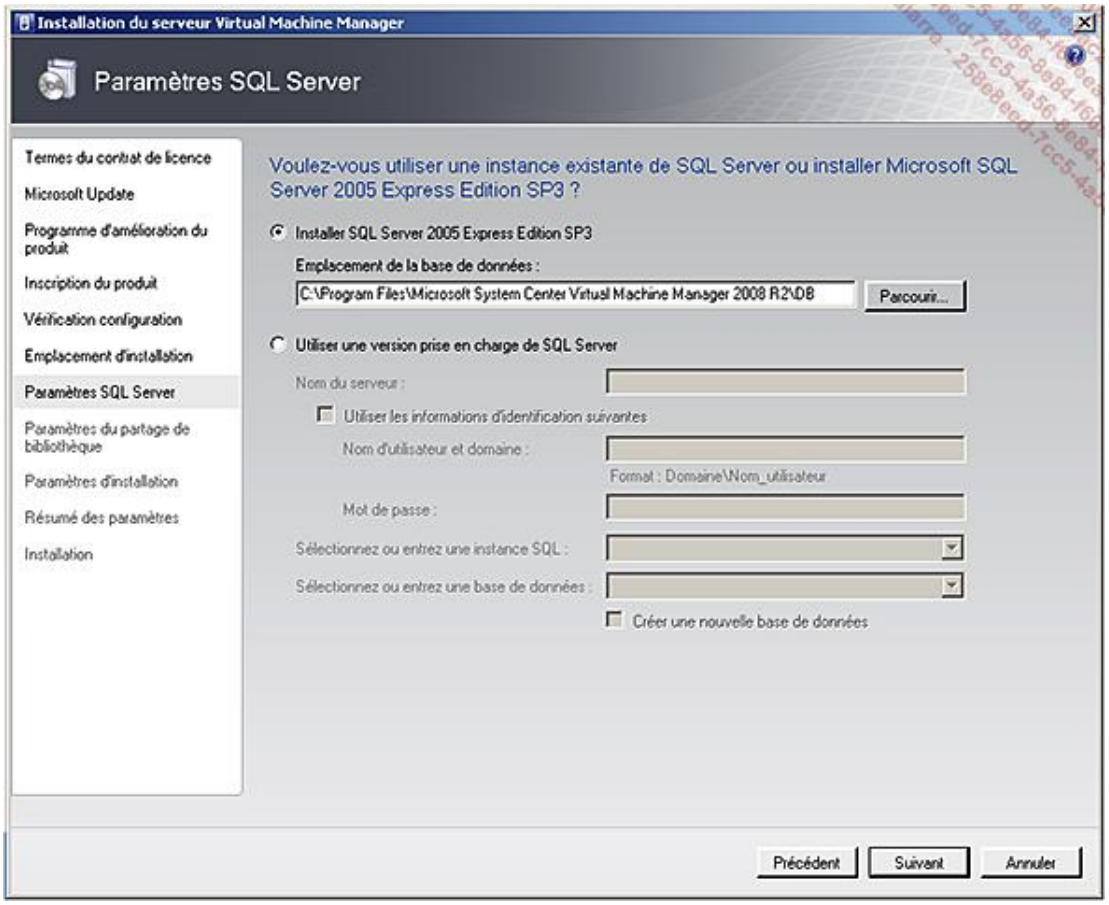
La version R2 est nécessaire pour gérer des serveurs Hyper-V sous Windows Server 2008 R2. L'installation du module complémentaire SCVMM (*System Center Virtual Machine Manager*) 2008 R2 est simple et rapide. Il ne faut pas pour autant sous-estimer son apport fonctionnel dans la gestion de l'infrastructure. Les fonctionnalités principales sont :

- Centralisation du déploiement et de la gestion des machines virtuelles pour Hyper-V, Virtual Server et VMware ESX.
- Conversion P2P et P2V rapide et fiable, sans outil supplémentaire.
- Intégration avec SCOM pour la supervision.
- Optimisation des ressources et de la performance en proposant des déplacements et des placements de machines virtuelles avec prise en compte des fonctions réseaux TCP Chimney Offload et VMQ dans les propositions de placement.
- Gestion centrale d'une bibliothèque de composants pour les machines virtuelles.
- Délégation de certaines tâches d'administration.
- Portail libre service pour la génération de machines virtuelles.
- Intégration avec les clusters.
- Entièrement scriptable avec PowerShell 2.0.
- Gestion de plusieurs solutions de virtualisation Microsoft (Virtual Server, Hyper-V 1.0) et non Microsoft (Vmware ESX, Virtual Center).
- Génération de rapports sur l'état de l'infrastructure virtuelle.
- Support des migrations de VM situés hors d'un cluster vers un cluster et vice-versa. Support des migrations à chaud (*live migration*).

© ENI Editions - All rights reserved - adamo diarra

- Support d'ajout de stockage dans les VM à chaud.
- Support des réseaux virtuels VMware ESX et des groupes de ports virtuels.
- Support du mode maintenance. La mise en mode maintenance d'un hôte met automatiquement les VM qu'il héberge en pause, empêche la création de VM sur cet hôte, ou le déplacement de VM vers celui-ci.

Il n'est cependant pas possible de l'installer sur une édition Core. Le seul choix réel à faire pendant l'installation concerne la base de données de SCVMM 2008 R2. Vous pouvez soit utiliser un moteur SQL Express 2005, soit lui indiquer un serveur SQL 2005 existant :



Après l'installation de SCVMM 2008 R2, il faut démarrer manuellement le service Windows correspondant si vous ne souhaitez pas redémarrer le serveur. Vous avez deux possibilités pour gérer votre environnement virtuel avec SCVMM :

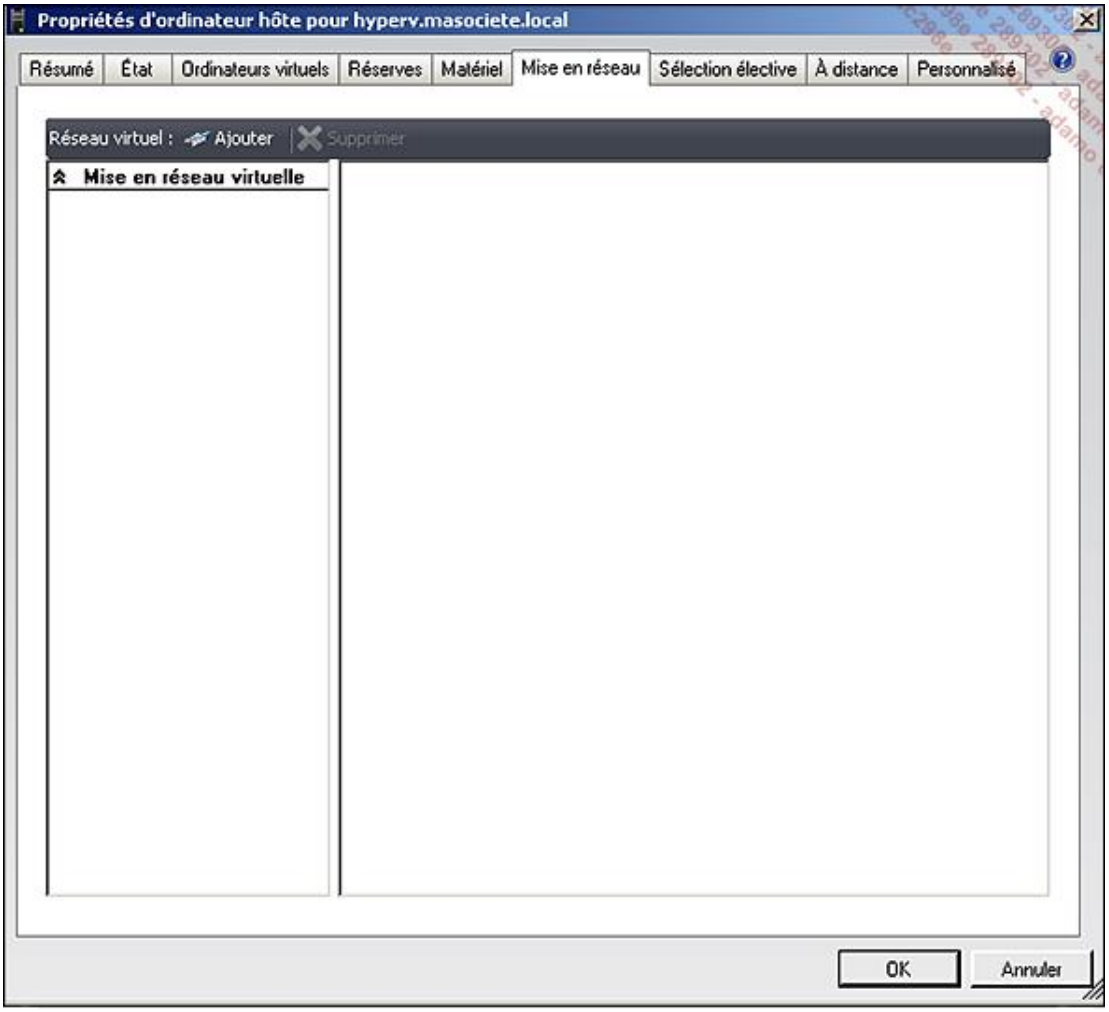
- via son interface graphique ;
- via l'extension PowerShell.

Avant de provisionner les machines virtuelles, vous devriez :

- Déclarer les serveurs Hyper-V à gérer (au moins un).
- Déclarer les réseaux virtuels.
- Créer des modèles de profils pour les machines virtuelles.
- Ajouter les images ISO à la bibliothèque.
- Créer des modèles de disques virtuels.

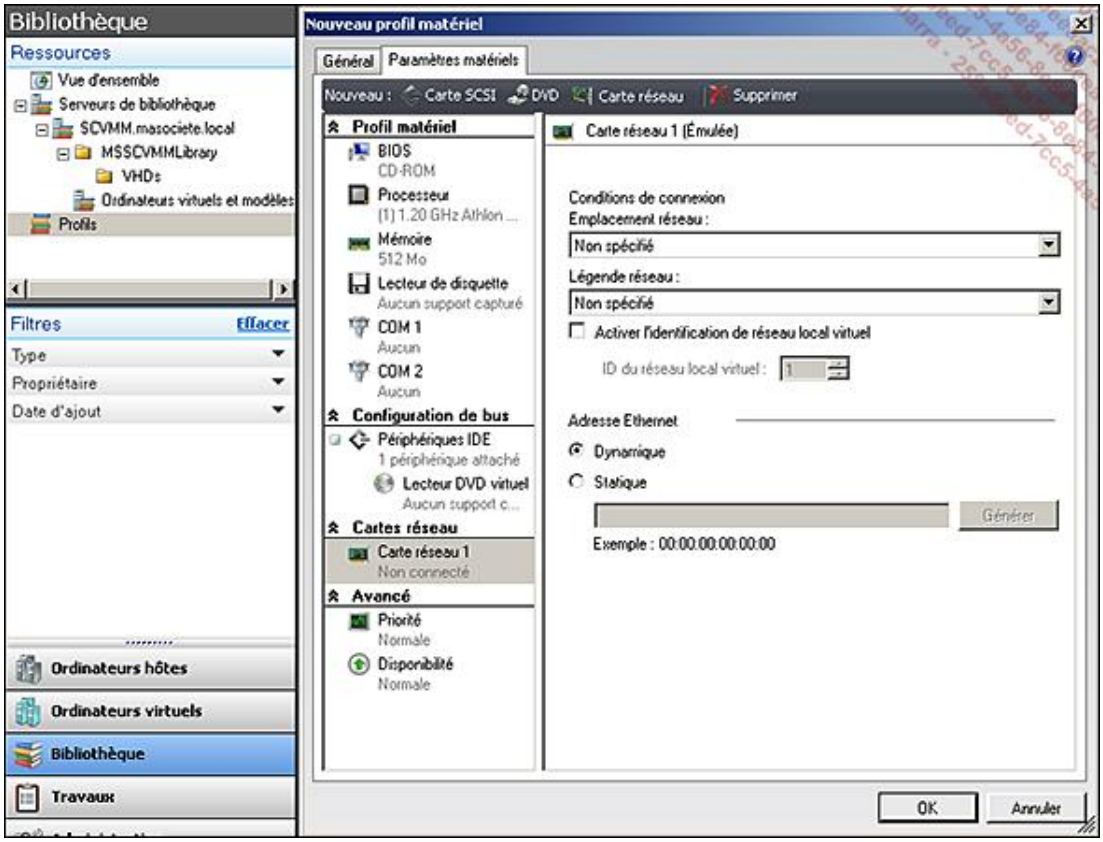
© ENI Editions - All rights reserved - adamo diarra

La déclaration de réseaux virtuels se fait depuis les propriétés du serveur virtuel :



Les profils matériels permettent d'utiliser des modèles de configuration plutôt que de configurer manuellement les ressources à chaque ajout de VM. Au-delà du gain en efficacité lors la création de VM, cela permet d'avoir une consistance de configuration entre deux machines virtuelles, gage de qualité. Pour gérer les profils matériels, allez dans **Bibliothèque**, puis **Profils**. Un profil comprend les paramètres suivants :

© ENI Editions - All rights reserved - adamo diarra



L'ajout d'images ISO consiste simplement à copier les fichiers ISO dans le partage de la bibliothèque SCVMM.

Lors d'une actualisation de la bibliothèque, Virtual Machine Manager indexe les fichiers enregistrés sur les partages de bibliothèque, puis met à jour la vue **Bibliothèque** et la liste de ressources. Tous les fichiers ne sont pas indexés et tous les fichiers indexés n'apparaissent pas dans la vue Bibliothèque. Le contenu de la bibliothèque est automatiquement rafraîchi toutes les heures par défaut. Le type de contenu suivant est indexé :

- les disques durs virtuels : .vhd (Hyper-V, Virtual Server), .vmdk (VMware) ;
- les disquettes virtuelles : .vfd (Virtual Server), .flp (VMware) ;
- les images ISO : .ISO ;
- les fichiers de réponses : .ps1 (Windows PowerShell) ; .inf ou .xml ;
- les modèles VMware : .vmtx.

Les types de fichiers de configuration suivants sont indexés, mais ils ne sont pas ajoutés à la bibliothèque en tant que ressources :

- Hyper-V : .exp (format d'exportation), .vsv (état enregistré), .bin ;
- Virtual Server : .vmc (configuration de l'ordinateur virtuel), .vsv (état enregistré) ;
- VMware : .vmtx (configuration de l'ordinateur virtuel), .vmx (format d'exportation) ;
- Les disques durs virtuels, images ISO et disquettes virtuelles attachés à un ordinateur virtuel.

La gestion des machines virtuelles peut se faire avec PowerShell, ce qui ouvre les portes nécessaires aux planifications, automatisations et traitements de masse.

Voici quelques exemples de commandes PowerShell :

Récupération du compte d'accès :

© ENI Editions - All rights reserved - adamo diarra

```
$Credential = get-credential
```

Récupération de l'identifiant du groupe "Tous les ordinateurs hôtes" :

```
$VMHostGroup = Get-VMHostGroup -VMMServer localhost | where
{$_.Path -eq "Tous les ordinateurs hôtes"}
```

Ajout de la ressource Hyper-V :

```
Add-VMHost -VMMServer localhost -ComputerName
"hyperv.masociete.local" -Description "" -Credential
$Credential -RemoteConnectEnabled $true -VmPaths " E:\VMDATA"
-Reassociate $false -RunAsynchronously -RemoteConnectPort
2179 -VMHostGroup $VMHostGroup
```

Déclaration d'un nouvel adaptateur réseau virtuel :

```
New-VirtualNetworkAdapter -VMMServer localhost -JobGroup
e4c2dfd1-0091-4a2a-992f-3406cfe833eb -PhysicalAddressType
Dynamic -VirtualNetwork "Net_LAN" -VLanEnabled $false
```

Déclaration d'un nouveau lecteur DVD Virtuel :

```
New-VirtualDVDDrive -VMMServer localhost -JobGroup e4c2dfd1-
0091-4a2a-992f-3406cfe833eb -Bus 1 -LUN 0
```

Utilisation d'un type de processeur déjà existant :

```
$CPUType = Get-CPUType -VMMServer localhost | where {$_.Name
-eq "3.07 GHz Xeon"}
```

Déclaration d'un nouveau profil matériel pour les VM :

```
New-HardwareProfile -VMMServer localhost -Owner
"MASOCIETE\mchateau" -CPUType $CPUType -Name
"Profil11d45f28-11b9-414b-aca0-ce8fbf6b9081" -
Description "Configuration matérielle utilisée pour
créer un ordinateur virtuel/modèle" -CPUCount 2 -
MemoryMB 512 -RelativeWeight 100 -HighlyAvailable $false -
NumLock $false -BootOrder "CD", "IdeHardDrive",
"PxeBoot", "Floppy" -LimitCPUFunctionality $false -
JobGroup e4c2dfd1-0091-4a2a-992f-3406cfe833eb
```

Récupération d'un profil matériel existant :

```
$HardwareProfile = Get-HardwareProfile -VMMServer
localhost | where {$_.Name -eq "Profil11d45f28-11b9-
414b-aca0-ce8fbf6b9081"}
```

Déclaration d'un nouveau disque virtuel :

```
New-VirtualDiskDrive -VMMServer localhost -IDE -Bus 0 -
LUN 0 -JobGroup e4c2dfd1-0091-4a2a-992f-3406cfe833eb -
Size 40960 -Dynamic -Filename "PRD-DOM-WEB01_disque_1"
```

Récupération d'un système d'exploitation existant :

```
$OperatingSystem = Get-OperatingSystem -VMMServer
localhost | where {$_.Name -eq "64-bit edition of
Windows Server 2008 Standard"}
```

Récupération d'un serveur Hyper-V :

```
$VMHost = Get-VMHost -VMMServer localhost | where
{$_.Name -eq "hyperv.masociete.local"}
```

Déclaration d'une nouvelle machine virtuelle :

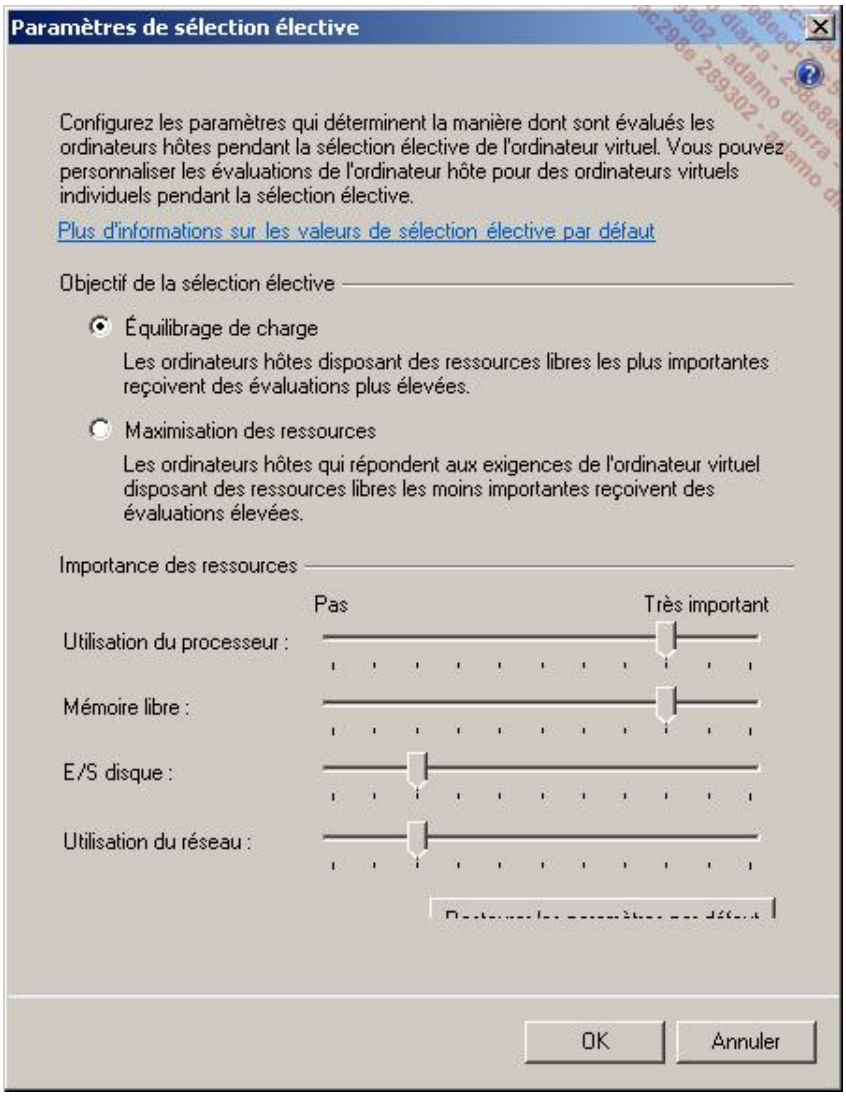
© ENI Editions - All rights reserved - adamo diarra

```
New-VM -VMMServer localhost -Name "PRD-DOM-WEB01" -
Description "Serveur WEB IIS sur le domaine" -Owner
"MASOCIETE\mchateau" -VMHost $VMHost -Path "E:\VMDATA" -
HardwareProfile $HardwareProfile -JobGroup e4c2dfd1-
0091-4a2a-992f-3406cfe833eb -RunAsynchronously -
OperatingSystem $OperatingSystem -RunAsSystem -
StartAction TurnOnVMIfRunningWhenVSStopped -DelayStart 0
-StopAction ShutdownGuestOS
```

Si vous souhaitez gérer des clusters Hyper-V depuis SCVMM, voici quelques considérations :

- Si vous ajoutez du stockage sur un cluster et souhaitez immédiatement ajouter des machines virtuelles sur ce stockage, assurez-vous au préalable que le cluster a été rafraîchi dans SCVMM pour prendre en compte ce nouveau stockage.
- La création/suppression des clusters ne peut pas être faite dans SCVMM.
- Les clusters qui ne sont pas dans un domaine de confiance ne peuvent pas être gérés par SCVMM.

L'optimisation des ressources peut être gérée en fonction des paramètres suivants :



Cet ensemble de critères est ensuite utilisé pour suggérer les placements et les déplacements des machines virtuelles à travers une notation étoilée.

SCVMM permet également de gérer l'attribution des adresses MAC aux machines virtuelles. Par défaut, une plage est positionnée, mais elle peut être changée en cas de problèmes :

© ENI Editions - All rights reserved - adamo diarra

6. Mises à jour Windows

Afin de faciliter l'installation des mises à jour Windows, Microsoft propose un outil complémentaire à SCVMM, « Offline Virtual Machine Servicing Tool 2.1 ». L'objectif de cet outil est de démarrer les machines virtuelles sur un réseau isolé (de préférence), de déclencher les mises à jour Windows, et d'éteindre la machine virtuelle, en la mettant de nouveau dans la bibliothèque. Il nécessite d'une part SCVMM, et d'autre part un serveur WSUS local (gratuit) ou SCCM. Il peut être téléchargé à cette adresse : http://www.microsoft.com/downloads/details.aspx?FamilyId=8408ECF5-7AFE-47EC-A697-EB433027DF73& displaylang=en.

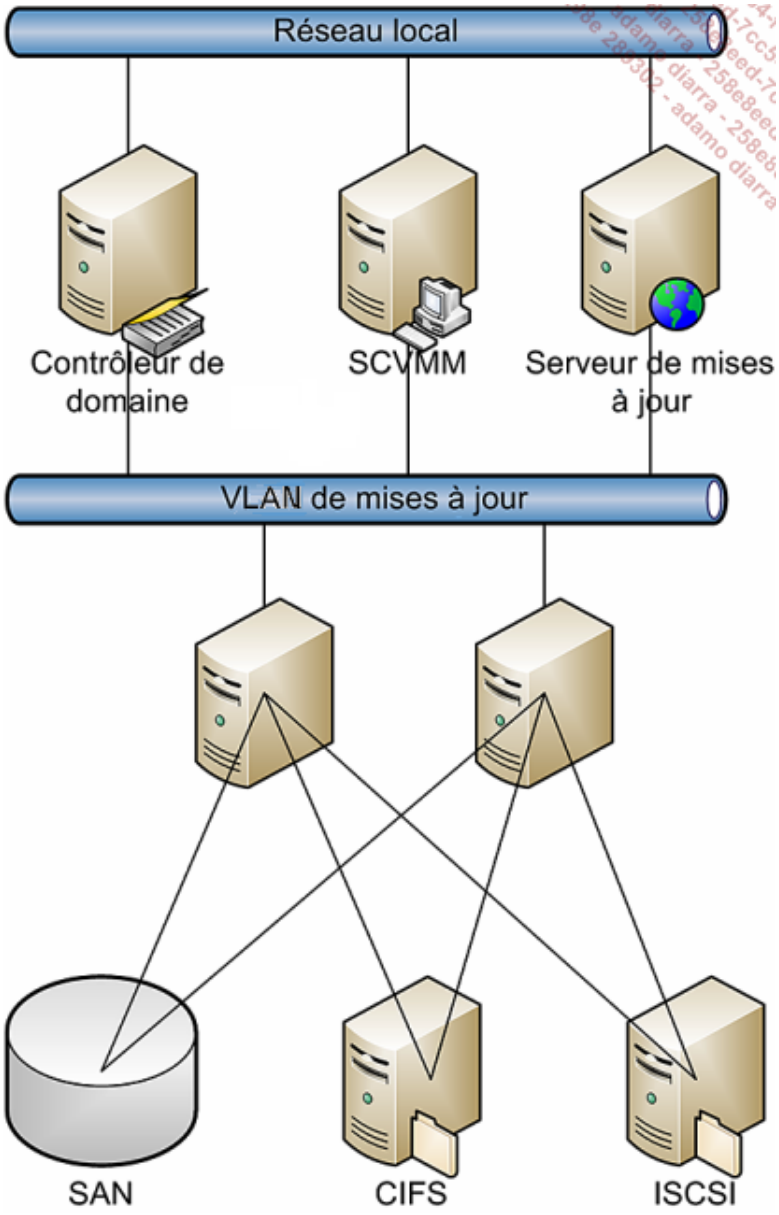
Cet outil est proposé à la fois en 32 et en 64 bits.

Il est recommandé, pour les infrastructures virtuelles conséquentes ayant un nombre important de machines virtuelles arrêtées, ou pour des environnements où la sécurité est un facteur important. Avant de décider d'utiliser cet outil ou non, voici quelques points à considérer :

- Les VM doivent être configurées pour utiliser le serveur WSUS via GPO ou autre (non pris en charge par l'outil), ou avoir le client SCCM installé et configuré.
- WSUS ou SCCM doivent être configurés au préalable afin que les mises à jour soient déjà approuvées pour le déploiement sur ces VM.
- Les VM doivent être en DHCP, ou avoir une configuration réseau fonctionnelle dans le réseau de mises à jour.
- Si plus de 20 machines virtuelles sont à maintenir à jour avec l'outil, il est recommandé que l'infrastructure autour soit physique et non virtuelle (serveurs WSUS, SCVMM...).
- Il fonctionne à la fois sur une infrastructure Hyper-V et Virtual Server 2005.
- Tous les serveurs physiques et les machines virtuelles doivent faire partie du domaine Active Directory, avec le service DNS en place et configuré.

Voici un exemple d'architecture :

© ENI Editions - All rights reserved - adamo diarra



7. Live migration

La migration à chaud (*live migration*) permet de déplacer une machine virtuelle d'un serveur à l'autre sans perte de service (perte de connexion réseau). Pour cela, plusieurs étapes sont nécessaires :

- Création de la VM sur la cible.
- Copie des pages mémoires depuis la source vers la destination. Les pages modifiées pendant le transfert sont envoyées de nouveau (marquées « dirty »), jusqu'à 10 fois.
- La machine virtuelle est mise en pause sur la source.
- L'accès au stockage (le disque virtuel de la VM) est donné au serveur cible.
- La machine virtuelle est remise en fonctionnement.

Le Clustered Shared Volume (expliqué dans le chapitre Haute disponibilité) permet à plusieurs serveurs d'accéder aux fichiers à l'intérieur d'une LUN. Un nœud est propriétaire de l'espace de noms et reste un passage obligé pour la création/suppression de meta données (répertoires...). Cependant, différents nœuds peuvent accéder simultanément à différents fichiers sur cette LUN, notamment les fichiers VHD. Cela permet donc de stocker tous les fichiers VHD sur

© ENI Editions - All rights reserved - adamo diarra

une seule LUN. Tous les nœuds pouvant accéder à l'ensemble des fichiers, il n'est plus nécessaire de changer le propriétaire de la LUN.

Les LUN peuvent aussi changer de propriétaire sans interruption, car les descripteurs sont persistants.

Les serveurs source et destination doivent utiliser des processeurs du même fabricant. Si les modèles de processeurs ne sont pas strictement identiques, Hyper-V peut masquer les fonctions qui ne sont pas communes à l'ensemble de la plate-forme. L'option **Migrer vers un ordinateur physique ayant une autre version de processeur** permet cela. Cette option est à positionner dans la configuration du processeur de la machine virtuelle à migrer.

En conclusion, vous connaissez maintenant ce que peut vous apporter la virtualisation, à condition de prendre en compte ses spécificités. Si, comme de plus en plus d'administrateurs, vous voyez un net avantage à virtualiser, vous devez construire une maquette afin de valider vos hypothèses. Suivant votre contexte, la complexité de ce type de projet peut fortement varier et il doit donc être préparé en conséquence. Comme indiqué en introduction, pensez grand mais commencez petit afin d'avoir une montée en charge maîtrisée.

© ENI Editions - All rights reserved - adamo diarra

Introduction

Ce chapitre a pour but de vous permettre d'aborder la sécurité de votre architecture de la meilleure des façons. En effet, il n'est pas rare d'entendre les professionnels de l'informatique s'exprimer avec des idées assez arrêtées en terme de sécurité. Ce domaine évoluant très régulièrement et très vite, il ne serait pas raisonnable de penser que l'architecture informatique et les solutions en termes de sécurité sont à jour. Il convient de se tenir régulièrement informé et de respecter un ensemble de bonnes pratiques.

Ce chapitre a donc pour intérêt de lister ces différentes bonnes pratiques et de vous présenter les nouvelles fonctionnalités vous permettant de les mettre en œuvre.

© ENI Editions - All rights reserved - adamo diarra

Principe de moindre privilège

Le principe de moindre privilège est, comme son nom l'indique, un principe qui consiste à lancer chaque tâche avec un compte utilisateur qui a exactement les permissions nécessaires à l'accomplissement de cette tâche.

Dans la pratique cela n'est bien sûr pas toujours réalisable mais il convient de toujours faire au mieux afin d'être le plus proche du besoin tout en laissant exposée une surface d'attaque la plus réduite possible. Si un utilisateur n'a pas besoin de droits spécifiques pourquoi les lui fournir ? Et comment s'assurer que l'utilisateur n'a pas plus de droits qu'il ne lui en faut ?

Différentes notions techniques sont à connaître afin de pouvoir faire les meilleurs choix.

1. Les différents types de compte

Sous Windows, il existe différents types de comptes utilisateur. Chacun d'eux définit un ensemble de droits tel que l'accès aux fichiers, les modifications que vous êtes autorisées à effectuer sur le système d'exploitation, etc. D'une façon générale, suivant le type de compte choisi, l'utilisateur aura un niveau d'accès plus ou moins important sur le système d'exploitation.

Il existe trois principaux types de comptes :

- Invité
- Standard
- Administrateur

Compte utilisateur invité

Un compte utilisateur ayant des droits de type Invité autorise l'accès aux ressources d'un ordinateur sans authentification de ce dernier. Ce type de compte n'est que très rarement utilisé en entreprise car il présente des risques non négligeables en termes de sécurité. Par défaut ce type de compte est désactivé.

Compte utilisateur standard

Un compte utilisateur standard permet d'utiliser la plupart des fonctionnalités du système d'exploitation tant que celles-ci ne touchent pas à la sécurité de l'ordinateur ou à des paramètres communs à tous les utilisateurs.

La principale différence entre un compte utilisateur standard et un compte administrateur est le niveau d'accès de l'utilisateur aux endroits définis comme protégés par le système d'exploitation.

Compte administrateur

Un compte utilisateur ayant les droits Administrateurs (et donc faisant partie d'une façon indirecte ou non du groupe Builtin\Administrateurs de l'ordinateur) est autorisé à agir sur la totalité du système d'exploitation et ainsi de pouvoir définir des paramètres communs à tous les utilisateurs (installation de logiciels, définition de la sécurité de l'ordinateur, etc.).

Dans la mesure où les droits de ce compte sont très étendus, il est fortement déconseillé d'utiliser celui-ci pour vos tâches courantes. Vous verrez un peu plus loin dans ce chapitre comment Microsoft a répondu au besoin de sécurisation de ces accès Administrateurs grâce à l'UAC (*User Account Control*).

Par exemple, un utilisateur standard ne peut pas, par défaut, écrire au niveau du dossier système (C:\windows) ou dans la plupart de la base de registre, tandis qu'un administrateur peut le faire. Un administrateur peut également activer/désactiver le pare-feu, configurer les politiques de sécurité, installer un service ou un pilote pour tous les utilisateurs, etc.

Dans Windows Vista, Windows 7 et Windows 2008/2008 R2, les comptes utilisateur standard peuvent effectuer des tâches qui nécessitaient autrefois les privilèges administrateur comme :

- Afficher l'horloge système, le calendrier et modifier le fuseau horaire.
- Modifier les paramètres d'affichage et les polices installées.
- Modifier les options d'alimentation.
- Ajouter des imprimantes et autres périphériques.

© ENI Editions - All rights reserved - adamo diarra

- Ajouter et configurer des connexions VPN.
- Définir une clé WEP/WPA à un réseau sans fil.

Des tâches planifiées supplémentaires permettent désormais de définir une tâche de défragmentation ou de sauvegarde automatique. Auparavant, ces fonctionnalités ne pouvaient pas être réalisées aisément et nécessitaient la plupart du temps des privilèges administrateur.

Voici une liste non exhaustive des différents droits pour un utilisateur standard et un administrateur. Celle-ci vous permettra de vous rendre un peu mieux compte des autorisations de chacun.

Utilisateurs standard	Administrateurs
Établir une connexion réseau.	Installer/désinstaller des applications.
Établir une connexion réseau sans fil.	Installer le pilote d'un périphérique.
Modifier les paramètres d'affichages.	Installer les mises à jour Windows.
Défragmenter le disque dur (par l'intermédiaire d'un service).	Configurer le contrôle parental.
Lire un CD/DVD.	Installer un contrôle ActiveX.
Graver un CD/DVD.	Configurer le pare-feu.
Modifier le fond d'écran.	Modifier le type de compte d'un utilisateur.
Accéder à la date et à l'horloge système et modifier le fuseau horaire.	Modifier les paramètres UAC.
Utiliser le bureau à distance pour se connecter à des ordinateurs distants.	Configurer l'accès au bureau à distance.
Configurer les options d'alimentation de la batterie.	Créer ou supprimer un compte utilisateur.
Configurer les options d'accessibilités.	Copier ou déplacer des fichiers dans les dossiers Program Files ou Windows.
Restaurer les fichiers sauvegardés de l'utilisateur.	Définir des tâches planifiées.
Définir une synchronisation entre un périphérique mobile et l'ordinateur (Smartphone, ordinateur portable, Personal Digital Assistant (PDA)).	Restaurer la sauvegarde de fichiers systèmes.
Connecter et configurer un périphérique Bluetooth.	Configurer le service de mise à jour automatique.

Un quatrième type de compte était souvent utilisé sous des environnements comme Windows 2000/XP. Il s'agissait des comptes étant membre du groupe Utilisateurs avec pouvoir. Ce groupe était à mi-chemin entre Utilisateur standard et Administrateur. Il permettait en effet d'effectuer certaines tâches comme la possibilité d'écrire à certains endroits de la base de registre et du système de fichiers, sans nécessairement avoir des droits d'administrateurs. Ce type de groupe ne permettant pas de répondre à tous les besoins des applications, il a été supprimé par défaut sous Windows Vista et Windows 7. Il faut tout de même savoir que ce groupe reste utilisable afin de permettre une compatibilité descendante pour les applications le nécessitant. Pour cela, il faut charger un modèle de sécurité particulier (compatws.inf) dans Windows Vista et Windows 7 afin de modifier les droits sur certains fichiers et certaines clés de la base de registre pour permettre au groupe **Utilisateurs avec pouvoir** d'y avoir accès.

2. Le contrôle d'accès utilisateur

© ENI Editions - All rights reserved - adamo diarra

Le contrôle d'accès utilisateur ou *User Account Control* (UAC) est une des principales avancées de la nouvelle gamme de systèmes d'exploitation Microsoft Windows Vista, Windows 7 et Windows Server 2008/2008 R2.

Cette nouvelle fonctionnalité (activée par défaut sous Windows Server 2008/2008 R2) permet de vous informer de toute action nécessitant des privilèges systèmes. Un jeton d'accès complet est alors créé avec les droits les plus importants de l'utilisateur puis est passé à l'application. Cela s'appelle une élévation des privilèges. L'UAC se caractérise par une élévation des privilèges automatisée, un message d'avertissement affiché lors de cette élévation, ainsi qu'un bureau sécurisé dédié à ce message d'avertissement.

Il sera ainsi beaucoup plus compliqué à un logiciel espion de s'installer sur le système ou de venir se greffer à un processus sans que vous en soyez informé.

Il est désormais plus simple d'identifier les tâches qui nécessiteront des droits plus importants. L'icône en forme de bouclier accolé à certaines applications et assistants de configuration indique que ces tâches vont se lancer avec des permissions d'administrateur de l'ordinateur.

Pour les autres applications, un message d'élévation de privilèges apparaîtra si besoin.

Notez que l'affichage de la fenêtre d'élévation de privilèges apparaît moins souvent sous Windows 7/2008 R2, notamment lors de tâches "sûres" comme l'installation de mises à jour ou de drivers téléchargés depuis Windows Update, l'affichage des paramètres Windows ou bien encore des outils de diagnostic de la carte réseau.

Avant que l'élévation des privilèges ne soit effectuée, Windows Server 2008 R2 bascule par défaut la fenêtre de confirmation demandant cette élévation de droits vers un bureau virtuel isolé (appelé aussi "Bureau estompé" depuis Windows 7 / 2008 R2) et sécurisé tandis que le reste des applications continue de s'exécuter au niveau du bureau interactif de l'utilisateur. Cela permet ainsi d'empêcher à un processus utilisateur (comme un logiciel espion) d'interagir avec la demande d'élévation de privilèges et ainsi d'accepter automatiquement l'élévation.

La fenêtre de demande d'élévation pour le processus en question se trouve donc dans un environnement hermétique. Ainsi, si un attaquant choisissait de créer un exécutable permettant de reproduire avec exactitude la fenêtre d'élévation de privilège, vous n'irez pas exécuter celle-ci car son affichage ne se ferait pas dans le bureau virtuel. De même, le bureau sécurisé empêche les attaques qui consistent à truquer l'affichage du pointeur de la souris. L'attaquant peut en effet modifier l'affichage de la souris de sorte que lorsque l'utilisateur choisit de cliquer sur **Annuler**, l'action du clic de souris est effectuée sur le bouton **Continuer** permettant ainsi d'exécuter l'application dangereuse. Le bureau virtuel permet de bloquer ce type d'attaque.

Par ailleurs, sous Windows Server 2008 R2 un mode particulier nommé **Mode d'approbation d'administrateur** est activé pour tous les membres du groupe Administrateurs (hormis le compte Administrateur intégré). Ce mode montre l'élévation de privilèges lorsqu'une application nécessitant des droits d'administrateurs est lancée.

Sous Windows Server 2008 R2, une granularité plus fine de l'UAC est possible afin de limiter les demandes de mot de passe. Cela est détaillé ci-après.

Il est possible de configurer ces différents paramètres via le Panneau de configuration ou via une stratégie de groupe (aussi bien locale que de domaine). Pour cela, ouvrez votre éditeur de stratégie, puis rendez-vous au niveau de **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Options de sécurité**.

Les stratégies relatives à la gestion de l'UAC sont les suivantes :

Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré

Description : permet de définir si le compte Administrateur intégré est soumis au Mode d'approbation administrateur ou pas.

Valeur par défaut : Désactivé

Contrôle de compte d'utilisateur : passer au bureau sécurisé lors d'une demande d'élévation

Description : indique si la demande d'élévation doit se faire sur le bureau des utilisateurs interactifs ou sur le bureau virtuel sécurisé.

Valeur par défaut : Activé

Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans utiliser le bureau sécurisé

Description : les programmes UIAccess comme l'assistance à distance peuvent demander l'utilisation de cette option.

Valeur par défaut : Désactivé

Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur

Description : définit si un utilisateur connecté avec un compte administrateur obtient une invite d'élévation de

© ENI Editions - All rights reserved - adamo diarra

privilèges lors de l'exécution d'applications nécessitant des privilèges administrateur.

Trois choix sont possibles sous Windows Server 2008 R2 :

- **Elever les privilèges sans invite utilisateur** : l'élévation se produit automatiquement et en silence (Inutile de vous préciser que cette option n'est pas recommandée).
- **Demande de consentement** : requiert une intervention de l'utilisateur pour Continuer ou Annuler l'opération d'élévation des privilèges.
- **Demande d'information d'identification** : un nom d'utilisateur et mot de passe est demandé lors de la demande d'élévation des privilèges.

Valeur par défaut : Demande de consentement.

Windows Server 2008 R2 possède également les paramètres suivants :

- **Demande de consentement sur le bureau sécurisé** : requiert une intervention de l'utilisateur sur le bureau sécurisé pour Continuer ou Annuler l'opération d'élévation des privilèges.
- **Demande d'information d'identification sur le bureau sécurisé** : un nom d'utilisateur et un mot de passe sont demandés sur le bureau sécurisé lors de la demande d'élévation des privilèges.
- **Demande de consentement pour les binaires non Windows** : requiert une intervention de l'utilisateur pour Continuer ou Annuler l'opération d'élévation des privilèges pour une application non signée par un certificat Microsoft.

Valeur par défaut : Demande de consentement pour les binaires non Windows.

Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard

Description : définit si un utilisateur connecté avec un compte standard obtient une invite d'élévation de privilèges lors de l'exécution d'applications nécessitant des privilèges administrateur.

Par défaut, un utilisateur standard aura la possibilité d'indiquer le mot de passe d'un compte administrateur. Il est également possible de désactiver cette option bien que cela n'empêche pas l'utilisateur de faire un clic avec le bouton droit de la souris sur un exécutable et de choisir **Exécuter en tant qu'administrateur**.

Valeur par défaut : Demande d'informations d'identification.

Demande d'informations d'identification sur le bureau sécurisé.

Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation

Description : lorsque ce paramètre est activé, l'utilisateur doit fournir son consentement lorsque Windows détecte un programme d'installation. Il n'est pas conseillé d'appliquer ce paramètre en environnement d'entreprise si l'utilisateur n'a pas les droits d'administrateur ou si un logiciel de télédistribution est déjà en place.

Valeur par défaut : Activé.

Contrôle de compte d'utilisateur : élever uniquement les applications UIAccess installées à des emplacements sécurisés

Description : indique que seules les applications nécessitant un niveau d'intégrité UIAccess (c'est-à-dire spécifiant `UIAccess=true` dans leur manifeste d'application) doivent se trouver à un emplacement sécurisé sur le système de fichiers. Les emplacements sécurisés sont :

- \Program Files\ (et sous-répertoires)
- \Program Files (x86)\ (et sous-répertoires)
- \Windows\System32

Valeur par défaut : Activé.

Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés

Description : seuls les exécutables signés et validés à l'aide d'un certificat auront l'autorisation d'élever leurs privilèges. La liste des applications d'administration peut donc être contrôlée par ce moyen.

Valeur par défaut : Désactivé.

© ENI Editions - All rights reserved - adamo diarra

Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur

Description : permet d'activer ou de désactiver le contrôle utilisateur pour les utilisateurs qui seront Administrateurs.

Valeur par défaut : Activé

Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre dans des emplacements définis par utilisateur

Description : cette option assure une compatibilité avec les anciennes applications qui s'exécutaient en tant qu'administrateur et écrivaient des données d'exécution de l'application dans %Program Files%, %Windir%, %Windir%\System32 ou HKLM\Software.

Valeur par défaut : Activé

Si vous utilisez une authentification biométrique, sachez que Windows Server 2008 R2 permet de simplifier l'élévation de privilèges demandée par l'UAC rendant ainsi l'expérience utilisateur meilleure.

Votre périphérique biométrique est d'ailleurs mieux géré sous Windows Server 2008 R2 que dans les versions précédentes et vous pourrez utiliser ce moyen d'authentification sans nécessairement avoir un logiciel tiers installé à partir du moment où le driver récupéré via Windows Update aura été installé.

Très souvent controversé car il modifie nos (mauvaises ?) habitudes, l'UAC permet néanmoins d'assurer un niveau de sécurité bien supérieur comparé aux versions précédentes de Windows. Ses améliorations notables sous Windows 7 et Windows Server 2008 R2 devraient néanmoins vous décider à très vite l'adopter.

3. Gérer vos groupes à l'aide des groupes restreints

Les groupes restreints vous permettent des gérer les membres de groupes de sécurité afin de vous assurer du contenu de ces groupes.

Les groupes restreints sont uniquement paramétrables au niveau des stratégies de domaine. Vous ne trouverez donc pas ce paramètre au niveau d'une stratégie locale. Il se trouve au niveau de **Configuration Ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Groupes restreints**.

L'avantage principal, vous l'aurez compris, est de figer les membres définis au niveau de **Membre** et **Membres de...** du groupe défini comme groupe restreint. Ainsi, si par exemple l'utilisateur se voit retirer manuellement d'un groupe défini en tant que groupe restreint, il sera automatiquement ajouté à celui-ci lors de l'application de la stratégie de groupe (soit toutes les 90 minutes environ).

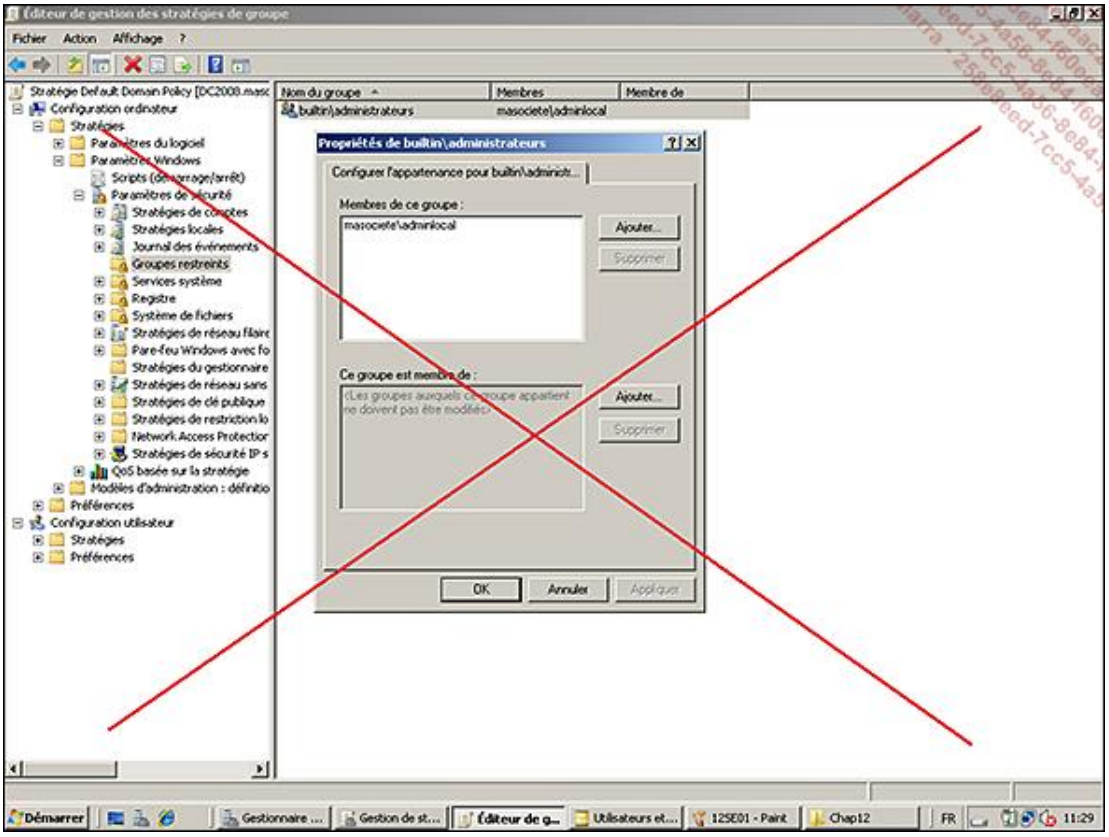
Avant de se lancer dans la configuration d'un groupe restreint, il convient de bien comprendre la différence entre le paramètre **Membres de ce groupe** et **Ce groupe est membre de**.

En configurant par exemple, depuis la stratégie de groupe, un groupe restreint comme le groupe local des ordinateurs nommé **BUILTIN\Administrateurs** (via un clic droit depuis la stratégie de groupes restreints puis **Ajouter un groupe - Builtin\Administrators**) et en lui indiquant un groupe de domaine nommé par exemple **MaSociete\AdminLocal** au niveau de **Membres de ce groupe**, alors tous les utilisateurs du groupe **MaSociete\AdminLocal** seront Administrateurs des ordinateurs se trouvant dans le conteneur lié à la stratégie de groupe définie.

Parfait ! Me direz-vous ? Et bien pas tant que cela...

Imaginez que ce groupe restreint soit défini au niveau des ordinateurs de votre Active Directory et qu'un utilisateur ait besoin d'être membre du groupe Administrateurs de son ordinateur (il n'est pas rare que les utilisateurs d'ordinateurs portables aient ce genre de besoin). En le rajoutant au groupe **MaSociete\AdminLocal**, l'utilisateur sera en effet membre du groupe BUILTIN\Administrateurs de son ordinateur mais également administrateur de tous les autres ordinateurs !

© ENI Editions - All rights reserved - adamo diarra



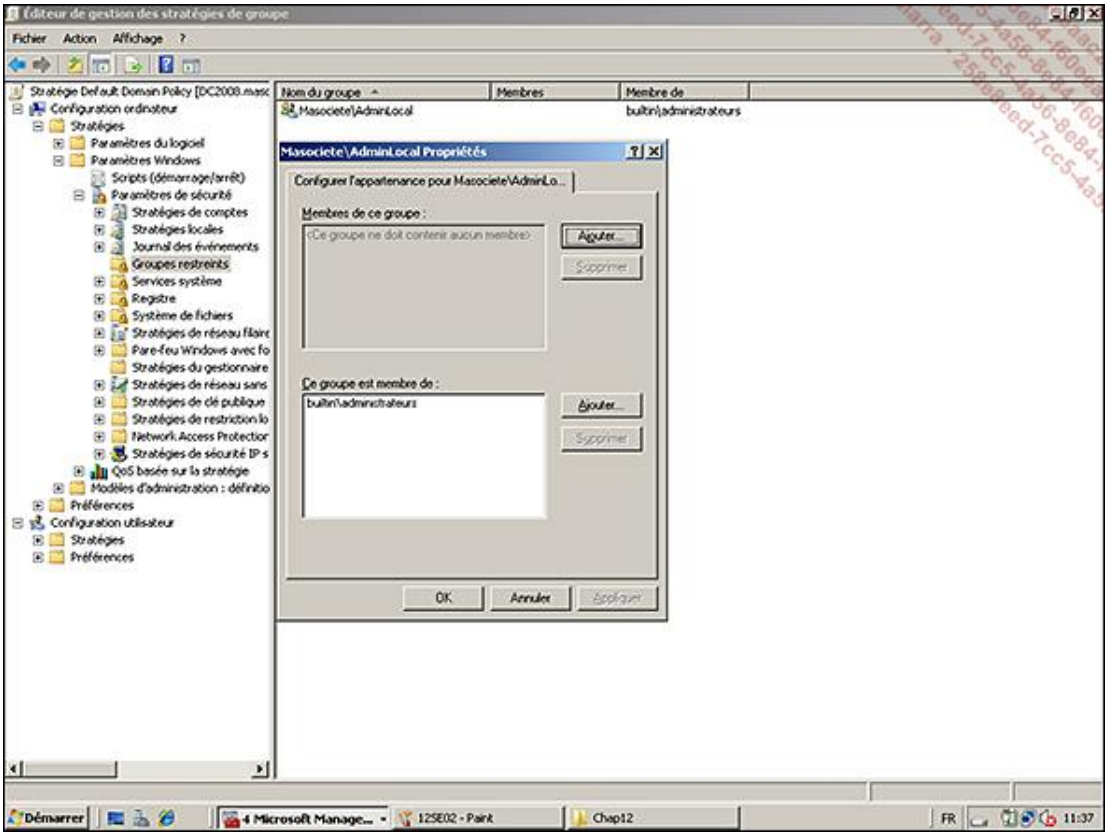
De même, si vous tentez de rajouter ce même utilisateur localement au groupe BUILTIN\Administrateurs de son ordinateur, l'application de la stratégie de groupe aura pour effet de nettoyer les membres des groupes locaux et par conséquent l'utilisateur se verra retirer à ce moment là les droits administrateurs.

Vous l'aurez compris, ce type de configuration n'est que peu adapté à la définition des membres des groupes au niveau des postes de travail mais il peut être très intéressant pour contrôler les membres des groupes des serveurs et contrôleurs de domaine afin de figer ces derniers.

Pour en revenir à notre utilisateur souhaitant être administrateur de son ordinateur en utilisant les groupes restreints, et sans que cela n'impacte la sécurité des autres ordinateurs, il convient de définir les groupes restreints de façon un peu différente.

Il faut en effet définir un groupe restreint à partir du groupe de domaine choisi (dans notre exemple le groupe **MaSociete\AdminLocal**) et définir le paramètre **Ce groupe est membre de :** afin d'y rajouter le groupe **BUILTIN\Administrateurs** (ou **BUILTIN\Administrators** selon que cette stratégie de groupe est définie depuis un ordinateur français ou anglais).

© ENI Editions - All rights reserved - adamo diarra



Ainsi, le groupe **MaSociete\AdminLocal** a son attribut ***IsMemberOf*** figé et les utilisateurs faisant partie de ce groupe sont effectivement membres du groupe Administrateurs de tous les ordinateurs mais sans que cela n'empêche un utilisateur lambda d'être administrateur de son ordinateur.

La gestion des groupes représentant toujours un véritable défi pour nos systèmes d'information et la sécurité qui en découle, les groupes restreints répondent fortement à cette attente de sécurisation du poste.

4. Applocker ou le contrôle de l'application

Applocker est une fonctionnalité qui a fait son apparition sous Windows 7 (en version Enterprise et Ultimate) et Windows Server 2008 R2 afin de remplacer les stratégies de restriction logicielle des versions précédentes de Windows.

Tout comme les stratégies de restriction logicielle, Applocker permet de définir les applications autorisées à être exécutées par vos utilisateurs standard au sein de votre domaine en déployant vos paramètres via des stratégies de groupe.

L'intérêt principal est donc de limiter l'installation de malwares sur les postes de travail mais également d'empêcher l'installation de logiciels non-normés ou nécessitant une licence que vous ne possédez pas, etc.

Cette fonctionnalité concerne donc principalement les postes clients sous Windows 7 mais il peut également être intéressant d'auditer et de limiter les exécutables lancés sur Windows Server 2008 R2.

Applocker présente plusieurs avantages comparés aux stratégies de restriction logicielle :

- La définition de règles plus fines basées sur l'éditeur (via la signature numérique du fichier et de ses attributs étendus tels que l'éditeur, le nom du produit et/ou le nom du fichier). Il est ainsi possible par exemple de n'autoriser qu'un logiciel provenant d'un éditeur spécifique et qu'à partir d'une version spécifique (comme n'autoriser que l'utilisation d'Office 2003 (Version 11.0.0.0) ou version suivante).
- La possibilité de définir des règles pour des utilisateurs ou des groupes spécifiques.
- La possibilité d'importer et d'exporter des règles.
- La possibilité d'identifier les effets de bord d'une règle en activant le mode d'audit.

Sachez également que si une stratégie de groupe possède à la fois une stratégie de restriction logicielle et une

© ENI Editions - All rights reserved - adamo diarra

stratégie de contrôle de l'application (Applocker), seule la stratégie Applocker sera appliquée sur le poste Windows 7 / 2008 R2.

Tâchons de configurer ensemble Applocker.

Avant de commencer il faut savoir qu'il existe trois types de règles possibles pour juger si une application est autorisée à être exécutée ou pas.

- **Chemin d'accès** : cette règle permet d'identifier un exécutable en se basant sur un chemin. Vous pouvez par exemple définir une règle afin d'autoriser l'exécutable C:\Windows\calc.exe. Cependant cette solution n'est pas la plus efficace car si un utilisateur renomme un exécutable interdit en calc.exe dans le dossier C:\Windows, il sera alors capable d'exécuter le fichier.

- **Hachage du fichier** : cette règle permet d'identifier un exécutable en se basant sur une valeur de hachage calculée. Chaque fichier possédant une valeur de hachage unique, Windows calcule la valeur de hachage d'un fichier et la compare aux valeurs définies dans les règles Applocker afin de savoir si la règle doit s'appliquer ou pas. L'inconvénient de cette solution est que la règle doit être mise à jour à chaque nouvelle version de fichier à autoriser.

- **Editeur** : cette règle permet d'identifier un exécutable en fonction de l'éditeur (tout comme c'était le cas avec les règles de certificat des anciennes restrictions logicielles) mais en y ajoutant également des conditions plus fines comme la version du produit, etc.

Avant de créer vos propres règles personnalisées, il faudra commencer par créer les règles par défaut. En effet, Applocker fonctionne un peu comme un pare-feu et tout ce qui n'est pas explicitement autorisé est alors refusé.

Voici donc les principales étapes à suivre afin de mettre en place Applocker au sein de votre entreprise.

- Générer les règles par défaut : afin d'éviter des effets de bord considérables, il vous faut donc générer les règles par défaut en autorisant tout le monde à lancer tous les exécutables se trouvant dans le dossier Program Files ou Windows.

- Générer les règles automatiques : vous n'aurez alors plus qu'à définir des règles pour bloquer ce que vous souhaitez. Cette façon de procéder vous évitera de vous "auto-bloquer" dans certaines situations à cause de règles mal définies.

- Auditer les règles Applocker avant le déploiement massif en production.

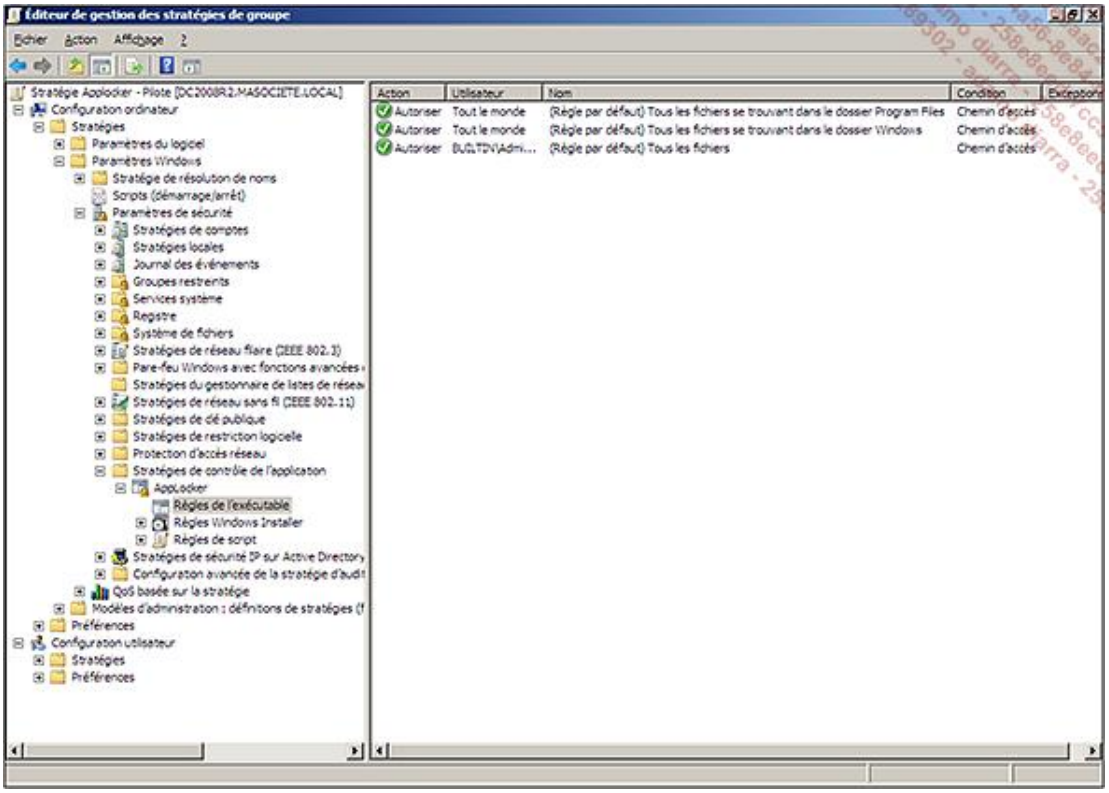
Générer les règles par défaut

- Afin de définir vos règles pour la première fois, utilisez un poste témoin (donc sous Windows 7 ou 2008 R2) qui sera le seul poste présent dans l'unité d'organisation attaché à la stratégie de groupe que vous allez configurer. Installez les applications normées ou celles que vous souhaitez autoriser. Installez également les outils RSAT afin de créer la stratégie et les règles Applocker directement depuis ce poste (vous verrez par la suite pour quelle raison).

- Toujours depuis ce poste témoin, rendez-vous alors au niveau du paramètre **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies de contrôle de l'application - Applocker**. Remarquez alors qu'il y a trois sous-catégories : **Règles de l'exécutable**, **Règles Windows Installer** et **Règles de script**. Faites un clic droit sur chacune de ces sous-catégories pour créer la règle par défaut en choisissant **Créer des règles par défaut**.

Ceci aura pour effet de créer des règles par défaut autorisant "Tout le monde" à exécuter les programmes se trouvant dans le dossier **%PROGRAMFILES%** et **%WINDIR%**. Il faudra garder cela à l'esprit au moment où vous réaliserez vos premiers essais en production. L'interdiction l'emportant sur l'autorisation, vous pourrez alors Refuser l'accès à un programme spécifique se trouvant dans l'un de ces dossiers.

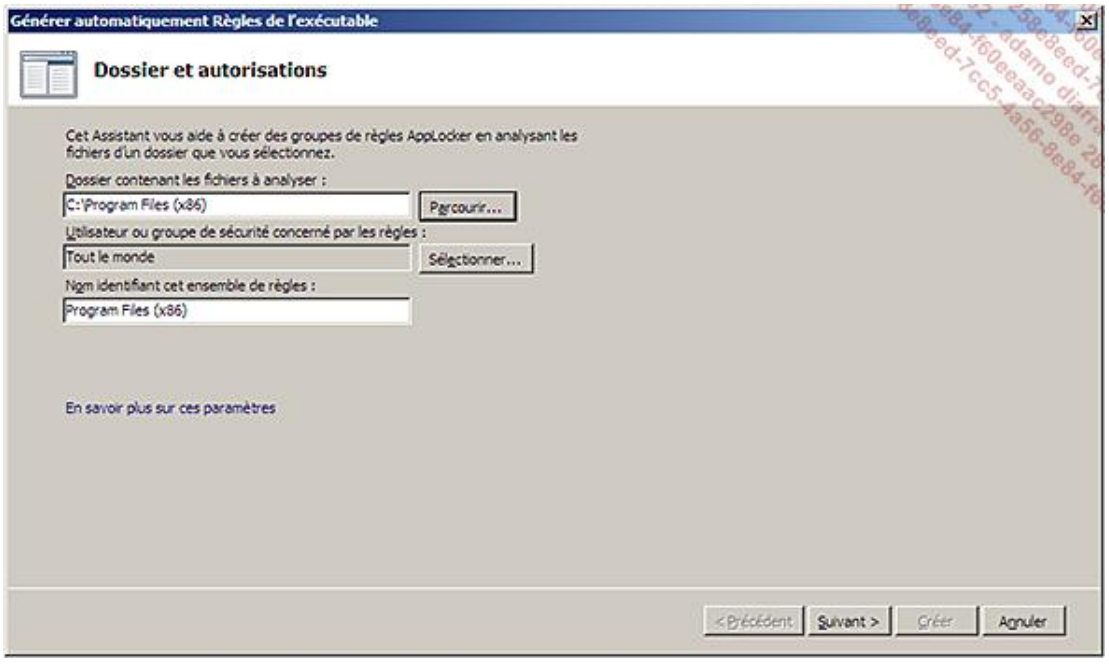
© ENI Editions - All rights reserved - adamo diarra



Générer les règles automatiques

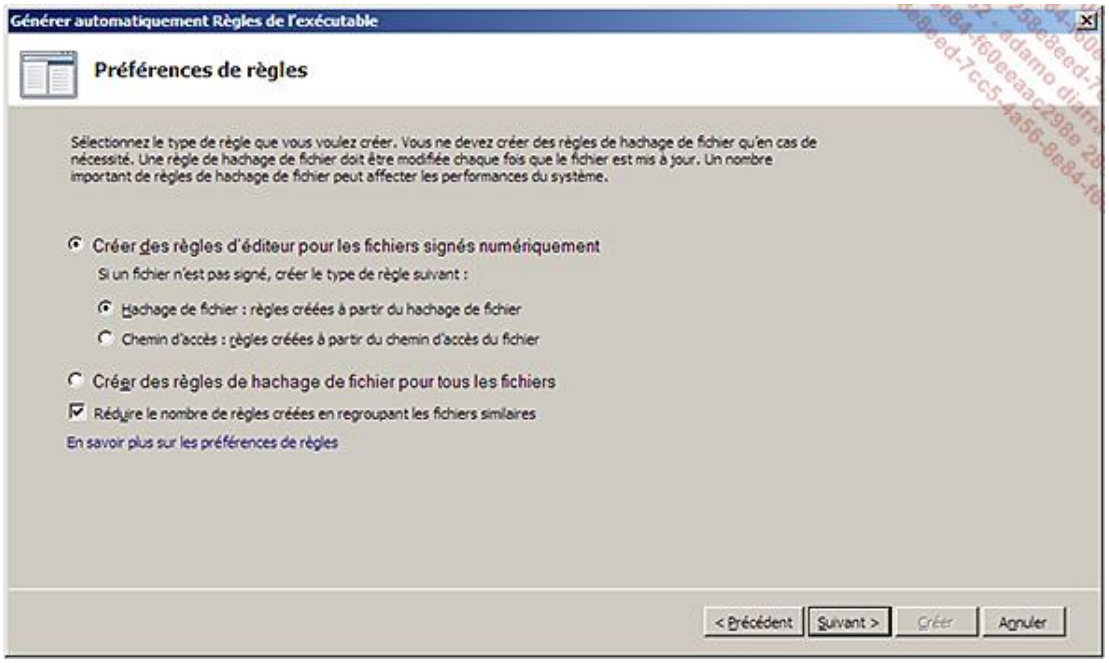
- La façon la plus simple de définir des règles pour des applications existantes est d'utiliser l'assistant. Il permet de générer les règles selon les spécificités de chaque binaire se trouvant dans le dossier que vous lui indiquez. Pour cela, faite un clic droit sur la catégorie **Règles de l'exécutable** et choisissez **Générer automatiquement les règles...**.

  Un assistant s'ouvre alors afin que vous lui indiquiez le répertoire à scanner, les utilisateurs concernés par cette règle, ainsi que le nom de la règle.

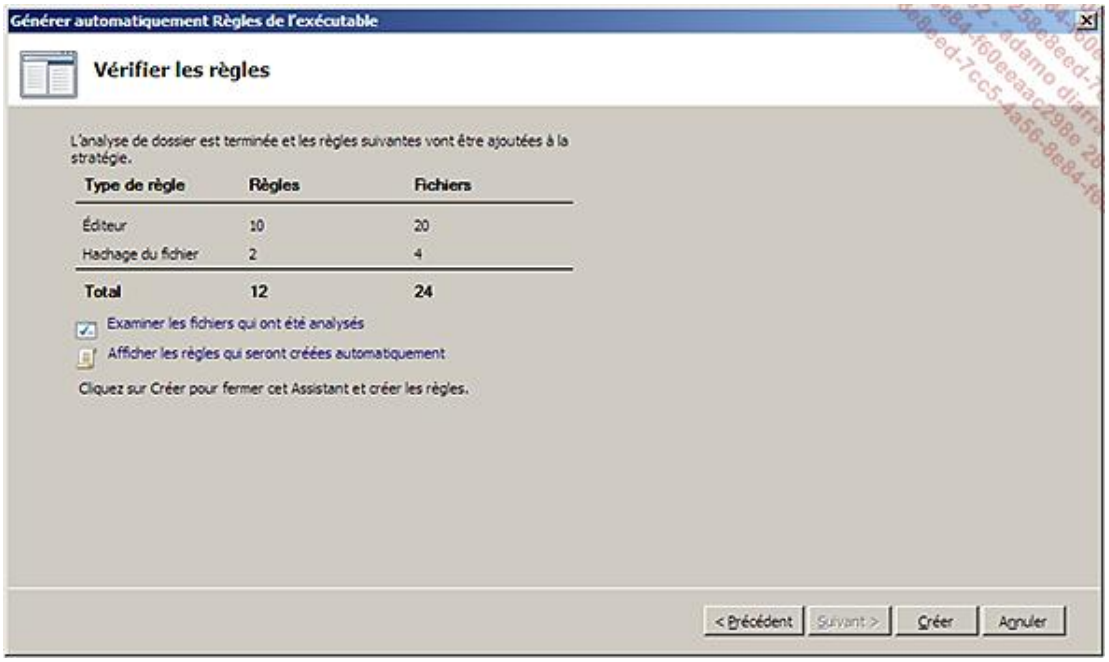


- L'étape suivant permet de définir les **Préférences de règles**. Les règles d'éditeur sont à préférer aux règles de hachage lors d'une première mise en place. Vous pouvez donc passer à l'étape suivante.

© ENI Editions - All rights reserved - adamo diarra

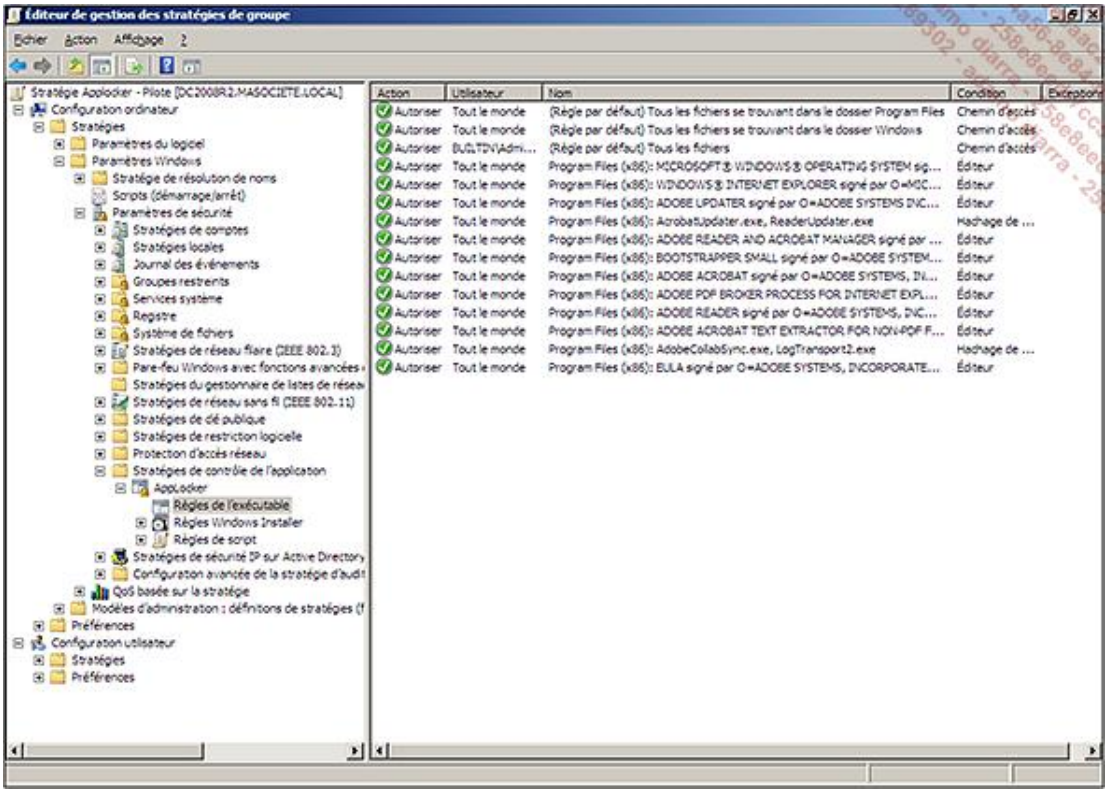


- Le scan débute alors et affiche le nombre de règles identifiées ainsi que le type de règle associé. Vous aurez la possibilité d'examiner les fichiers analysés afin de supprimer tout ou partie des règles proposées.



- Cliquez sur **Créer** pour créer les règles choisies. Celles-ci sont alors immédiatement ajoutées à la règle de l'exécutable.

© ENI Editions - All rights reserved - adamo diarra



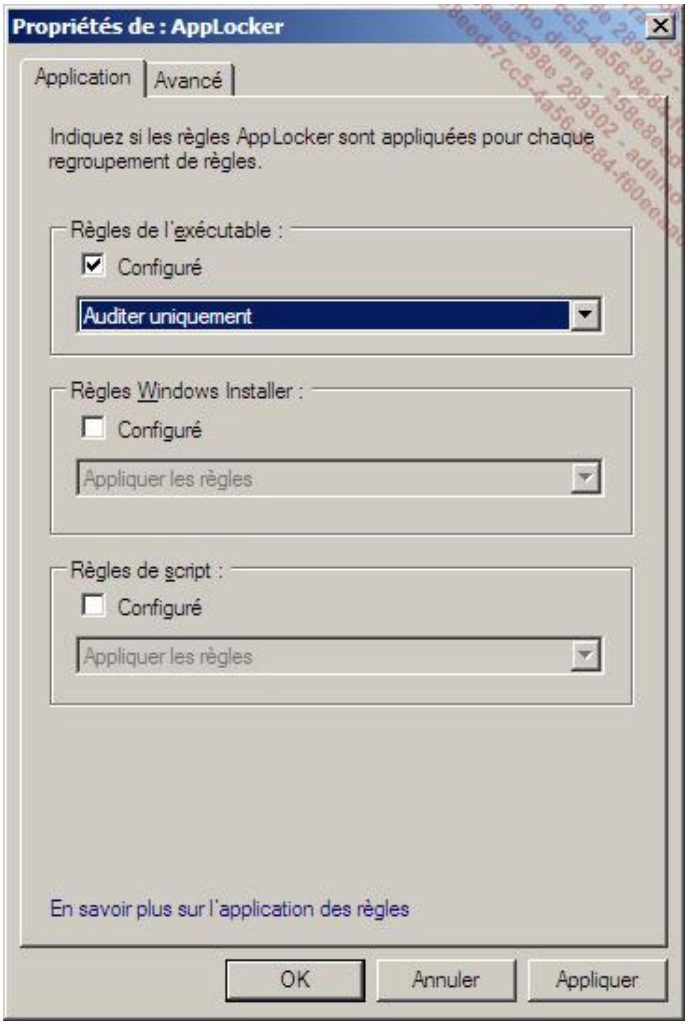
Auditer les règles Applocker sur les postes de production

Le but de cette étape est de faire "comme si" les règles que vous présentez étaient mises en place sur vos postes en production, à la différence que les règles établies ne bloqueront pas les applications. Il s'agit donc d'une phase d'apprentissage essentielle afin d'identifier des effets de bord majeurs.

- Afin de simuler le déploiement des règles Applocker sans que ces dernières soient réellement effectives, faites un clic droit sur **Applocker** (au niveau de **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies de contrôle de l'application - Applocker**) puis **Propriétés**.

  Cochez alors la case **Configuré** au niveau de la catégorie de règle de votre choix (dans notre exemple **Règle de l'exécutable**) et choisissez **Auditer uniquement** dans la liste déroulante correspondante.

© ENI Editions - All rights reserved - adamo diarra

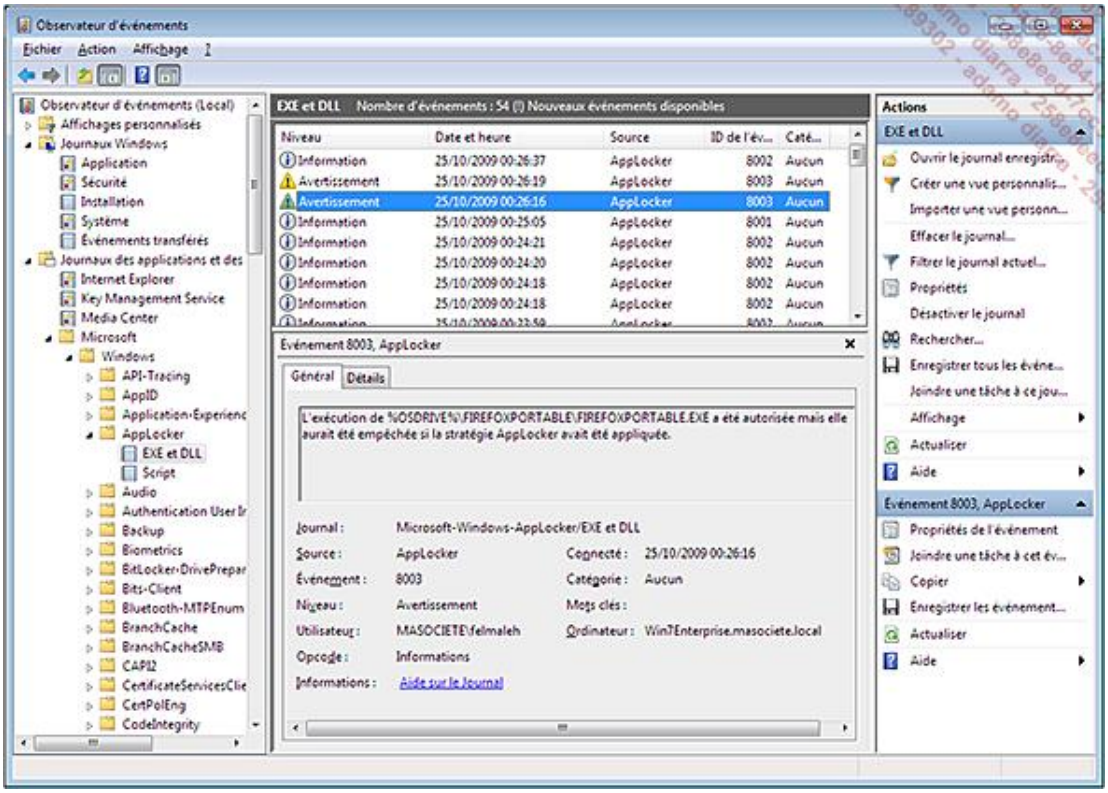


Validez en cliquant sur **OK**.

- Afin que ces paramètres puissent être appliqués sur vos postes cibles, il faut modifier le type de démarrage du service **Identité de l'application**. Celui-ci est en effet défini par défaut en démarrage Manuel et non Automatique. Vous pouvez donc configurer celui-ci directement depuis le poste client ou via cette même stratégie de groupe au niveau de **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Services système**. Sélectionnez alors le service **Identité de l'application** et définissez-le pour un démarrage automatique.

- Redémarrez votre poste client ou forcez l'actualisation de la stratégie via la commande **gpupdate /force** pour pouvoir tester immédiatement cette fonctionnalité. Vous pouvez alors identifier si les règles Applocker définies bloquent des applications normalement autorisées. À cette étape, l'application ne sera néanmoins pas bloquée. Afin de vérifier la liste des applications qui auraient été bloquées, lancez le journal des évènements puis rendez-vous sur le journal se trouvant dans **Journaux des applications et des services - Microsoft - Windows - Applocker**. Recherchez alors les évènements ayant l'ID 8002 (indiquant l'exécution autorisée d'une DLL ou d'un exécutable) ou 8003 (indiquant que le fichier exécuté aurait normalement été bloqué si le mode audit n'avait pas été activé).

© ENI Editions - All rights reserved - adamo diarra

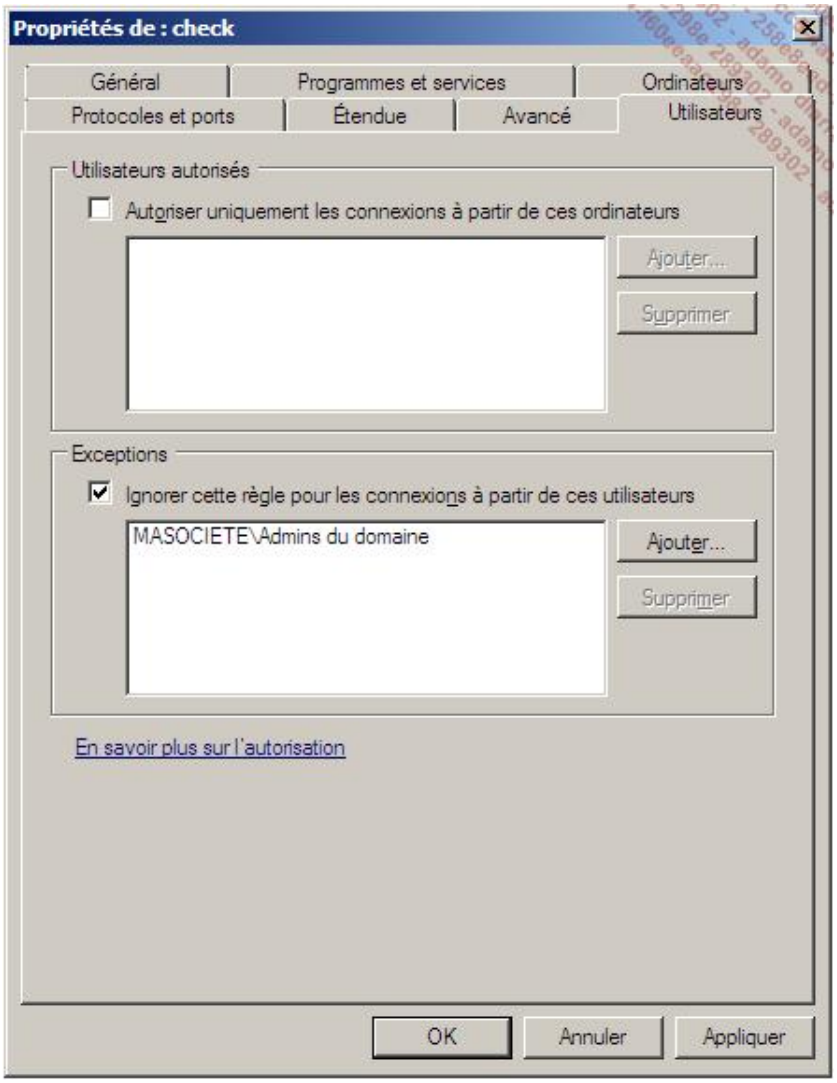


Appliquer les règles Applocker sur les postes de production

- Une fois vos règles correctement définies, vous pourrez les appliquer en éditant votre stratégie de groupe créée précédemment en vous rendant au niveau de **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies de contrôle de l'application - Applocker** puis **Propriétés**. Dans la liste déroulante correspondant au groupement de règles que vous souhaitez réellement appliquer, choisissez **Appliquer les règles**. Validez en cliquant sur **OK**.

- Si vous le souhaitez, vous pourrez optionnellement ajouter l'adresse vers un site web de votre choix lorsqu'une application sera bloquée pour vos utilisateurs. Vous pourrez ainsi les diriger vers une page spécifique de votre site Intranet afin de les informer sur ce blocage. Pour cela, éditez la stratégie **Configuration ordinateur - Stratégies - Modèles d'administration - Composants Windows - Explorateur Windows - Définir le lien d'une page web de support**.

© ENI Editions - All rights reserved - adamo diarra



Il est possible d'administrer la solution Applocker avec PowerShell. Vous trouverez les commandes PowerShell de référence à cette adresse : http://technet.microsoft.com/en-us/library/ee424349(WS.10).aspx

Vous venez donc de découvrir comment mettre en place une stratégie Applocker. La solution technique n'est pas particulièrement compliquée mais il faudra surtout bien réfléchir aux différents processus à mettre en place pour que cette solution évolue en même temps que les applications de votre entreprise et sans que cela ne pénalise les utilisateurs.

© ENI Editions - All rights reserved - adamo diarra

Délégation d'administration

L'un des principaux avantages d'un domaine Active Directory est de pouvoir fournir un annuaire commun à plusieurs entités au sein d'une même société. Cet annuaire partagé aide ainsi à réduire les coûts de gestion associés au maintien de l'infrastructure.

1. Approche de la délégation d'administration

Les politiques de sécurité étant généralement différentes au sein des divisions et les équipes IT n'étant pas les mêmes, il convient de trouver une solution afin de déléguer les tâches nécessaires au travail de chacun sans pour autant compromettre la sécurité de tout le domaine Active Directory.

La structure d'un domaine Active Directory est organisée par défaut de façon hiérarchique. Il est en effet possible de déléguer des tâches au niveau d'une forêt, d'un site, d'un domaine ou bien même d'une unité d'organisation. De plus, chaque objet possédant des attributs avec des DACL (*Discretionary Access Control List*) associées à ces derniers, il est également possible de déléguer des options de façon assez fine (réinitialiser le mot d'un utilisateur, autoriser la désactivation d'un compte utilisateur, etc.). Nous passerons à la pratique un peu plus loin dans ce chapitre.

Avant de vous lancer dans la configuration de la délégation de votre Active Directory, il convient de bien étudier les besoins auxquels vous devez répondre.

Une lecture (en anglais) vous permettra d'y voir un peu plus clair sur la délégation de l'administration d'un Active Directory. Elle est disponible à cette adresse http://www.microsoft.com/downloads/details.aspx?familyid=631747a3-79e1-48fa-9730-dae7c0a1d6d3&displaylang=en.

2. Délégation de comptes utilisateur

Passons maintenant à la pratique en déléguant deux actions particulièrement utiles à la hotline et au support informatique d'une entreprise. Ces services n'ayant pas pour vocation d'effectuer des tâches administratives lourdes sur l'Active Directory, il serait démesuré d'ajouter ces derniers au groupe « Administrateurs du domaine » par exemple.

Parmi les besoins les plus exprimés par ces services afin de répondre aux demandes des utilisateurs, vous trouverez notamment le droit de joindre un poste à un domaine Active Directory et le droit de réinitialiser les mots de passe des utilisateurs.

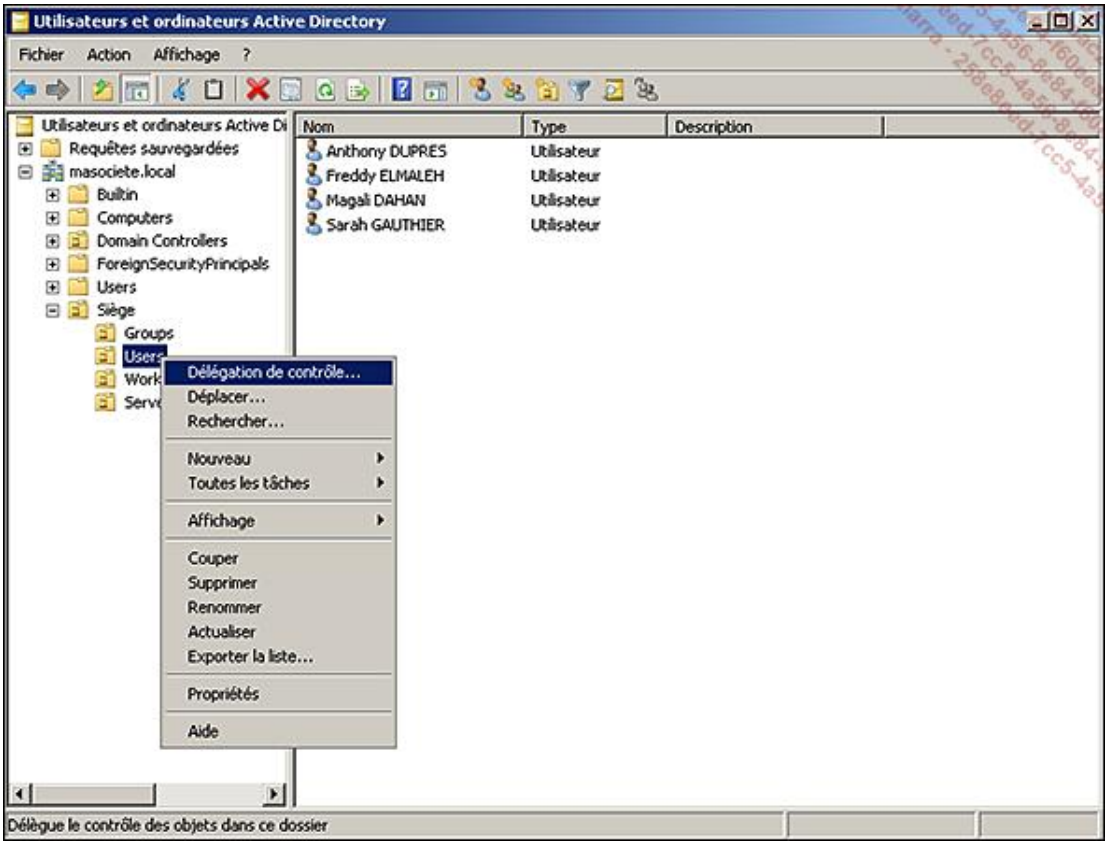
Les délégations s'effectuent généralement sur tout ou partie des objets d'une unité d'organisation (ou OU pour *Organizational Unit*) ou d'un domaine. Cela a pour but de simplifier l'administration et la gestion des droits de votre Active Directory. Inutile de vous rappeler qu'il est d'ailleurs impératif de garder une trace des délégations effectuées afin de faciliter l'administration quotidienne et les opérations de dépannage en cas de problème.

Prenons l'exemple du service de hotline qui souhaite pouvoir **réinitialiser les mots de passe des utilisateurs et déverrouiller leur compte**. Tous les utilisateurs de la hotline font partie du même groupe nommé **HotlineUsers**.

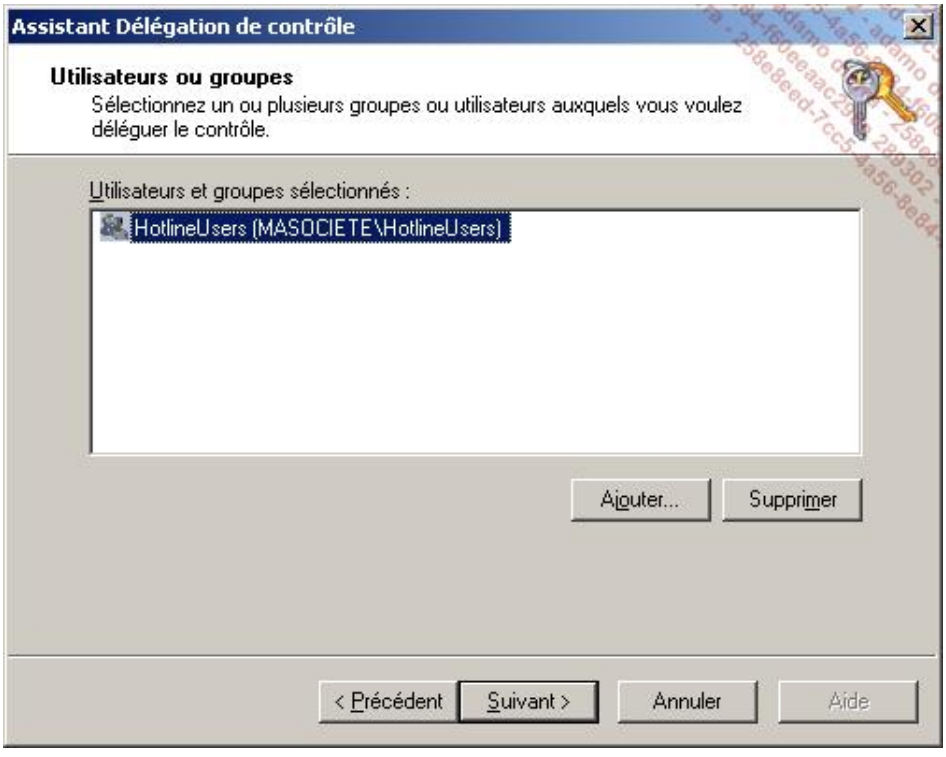
Afin de déléguer ces droits, Microsoft met à disposition un assistant délégation.

- Pour cela, placez-vous au niveau de l'objet ou du conteneur parent depuis lequel vous souhaitez effectuer une délégation de droits. Dans la plupart des cas, cette délégation s'effectue au niveau d'une unité d'organisation. Faites alors un clic avec le bouton droit de la souris sur l'objet et choisissez **Délégation de contrôle**.

© ENI Editions - All rights reserved - adamo diarra



- Cliquez sur **Suivant** dans l'écran de bienvenue. L'assistant vous demande alors de sélectionner les utilisateurs ou groupes pour lesquels les droits délégués seront attribués. Cliquez sur **Ajouter** puis tapez le nom de votre groupe et cliquez sur **Vérifier les noms**, puis **OK**.

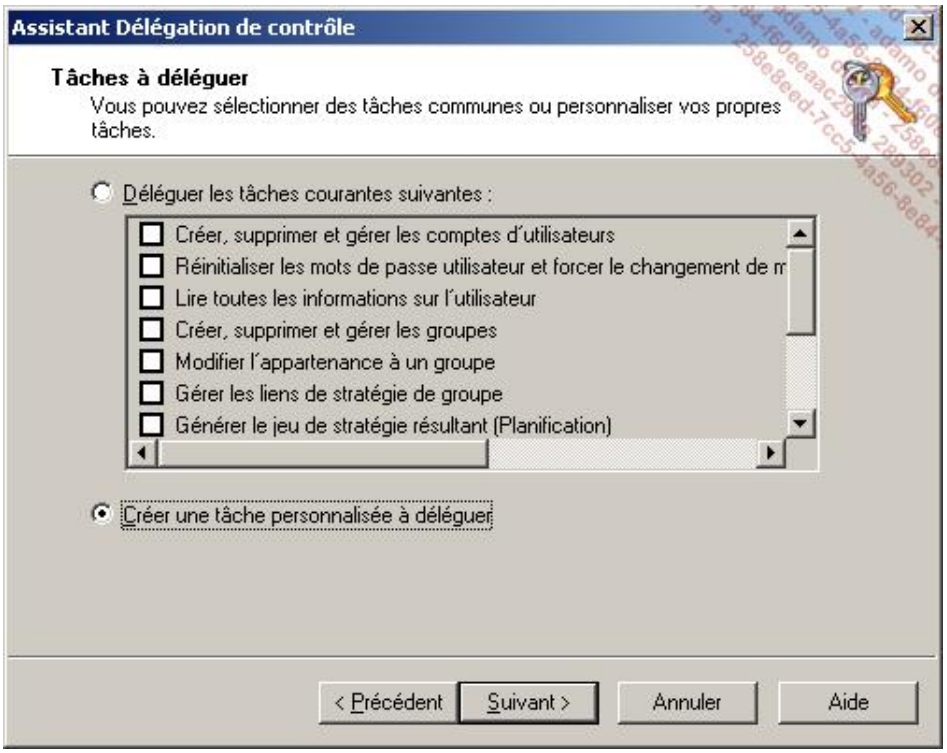


Une fois le ou les groupes ajoutés, cliquez sur **Suivant**.

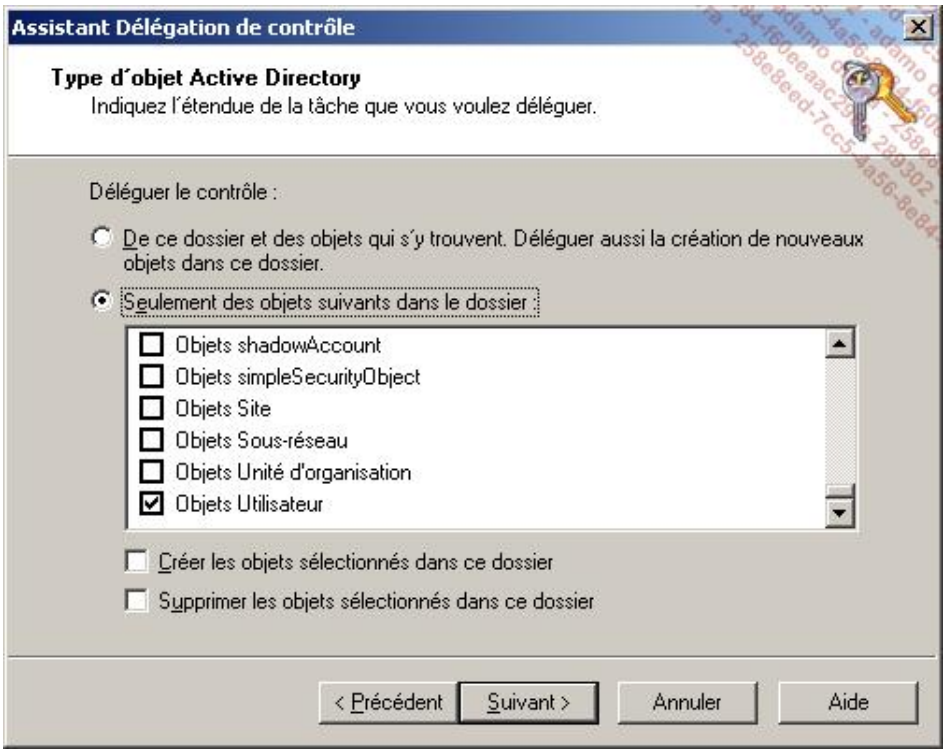
- Vous pouvez maintenant choisir le niveau de permissions qui sera appliqué à l'objet délégué. Vous avez le choix entre choisir des délégations prédéfinies pour des tâches courantes ou bien de définir une **tâche personnalisée à déléguer**.

© ENI Editions - All rights reserved - adamo diarra

- Dans notre exemple, nous pourrions choisir les tâches prédéfinies mais celles-ci offriraient trop de droits comparé à ce que nous souhaitons autoriser. Choisissez donc de **Créer une tâche personnalisée à déléguer** afin de pouvoir effectuer une délégation très granulaire, puis cliquez sur **Suivant**.



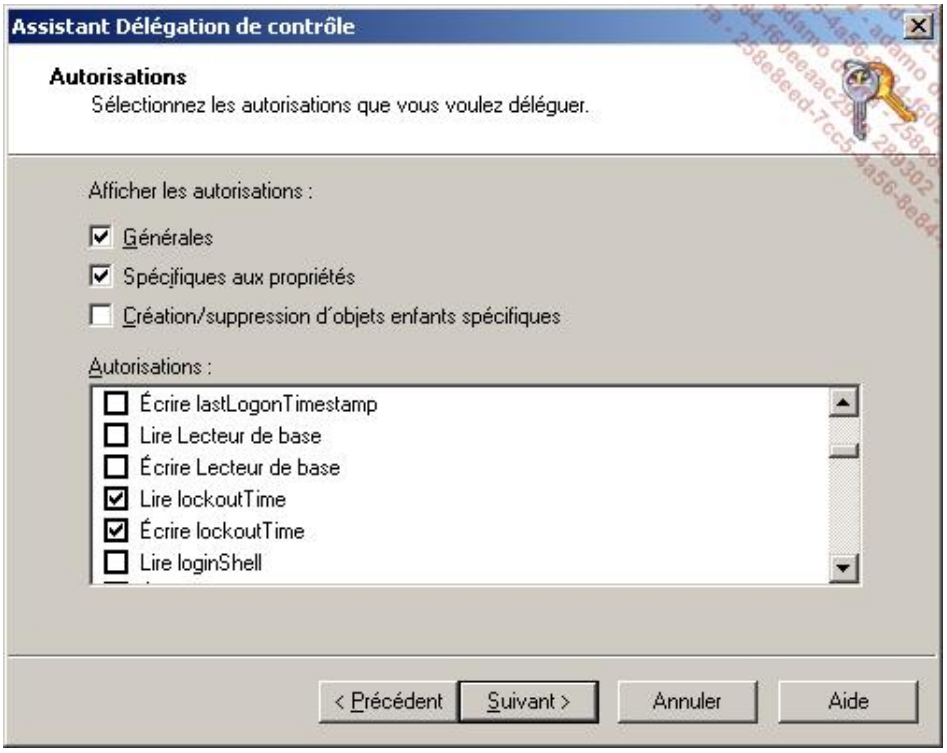
- Choisissez de déléguer le contrôle **Seulement des objets suivants dans le dossier**, cochez **Objets Utilisateur** puis cliquez sur **Suivant**.



- Sélectionnez alors le ou les types d'autorisations que vous souhaitez déléguer aux utilisateurs. Dans notre exemple l'attribut **Modifier le mot de passe** (ou *Change Password* en anglais) est utilisé pour la réinitialisation du mot de passe et les attributs **Lire lockoutTime** (ou *Read lockout Time*) et **Écrire lockoutTime** (ou *Write lockout Time*)

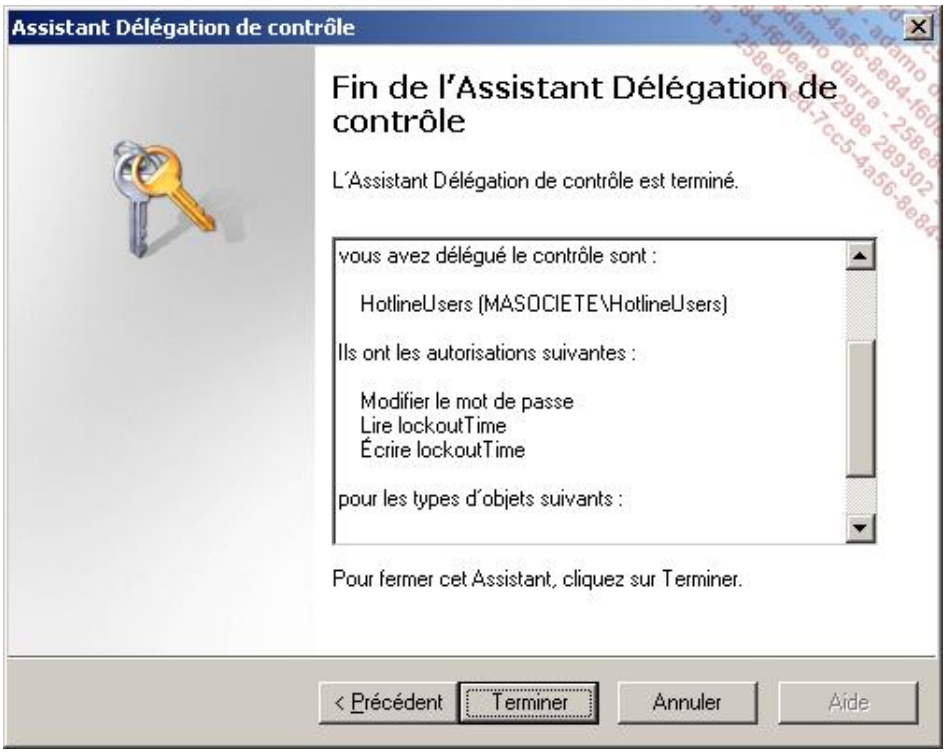
© ENI Editions - All rights reserved - adamo diarra

sont utilisés pour déverrouiller un compte utilisateur. Les deux derniers attributs ne sont visibles qu'en cochant la case **Spécifiques aux propriétés** car, comme son nom l'indique, ils sont spécifiques à l'objet Utilisateur.



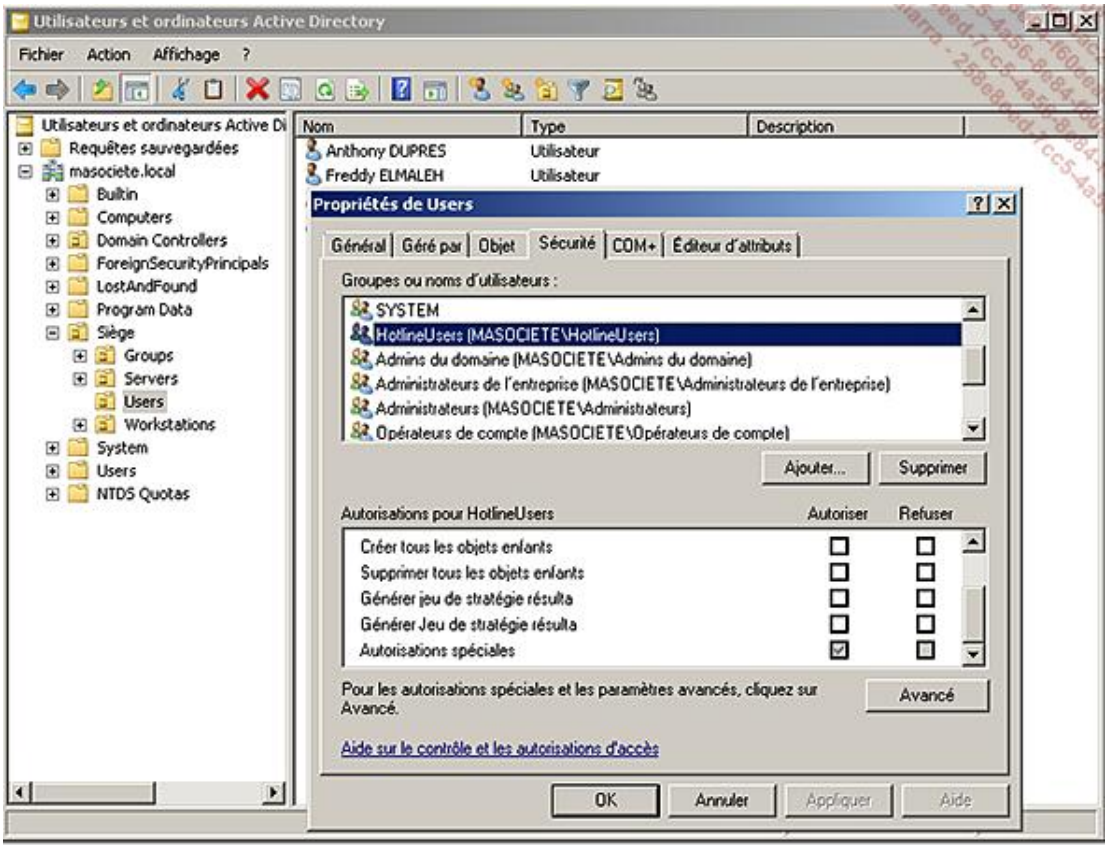
Une fois les trois cases cochées, cliquez sur **Suivant**.

- Une fenêtre récapitulative indique les différents choix effectués au cours de l'assistant délégation. En cliquant sur **Terminer**, les ACL seront modifiés sur le conteneur choisi.



Vous pouvez lister et définir une autorisation directement depuis la console Utilisateurs et Ordinateurs Active Directory. Il faut pour cela activer les **Fonctionnalités avancées** au niveau du menu **Affichage** de la console. Ensuite, en affichant les **Propriétés** du conteneur ou de l'objet délégué, un onglet **Sécurité** est disponible et vous permet d'afficher et de modifier la sécurité directement depuis cet endroit.

© ENI Editions - All rights reserved - adamo diarra



Une fois la délégation effectuée, il est courant qu'une console MMC personnalisée soit distribuée aux personnes concernées.

L'avantage d'une console MMC personnalisée est que ses utilisateurs n'ont accès qu'à une vue limitée de l'Active Directory. Il est également possible de définir de façon exhaustive les actions disponibles (dans notre exemple, ce serait les options de **réinitialiser les mots de passe des utilisateurs** et de **déverrouiller leur compte**). Vous trouverez plus d'informations sur la façon de créer une MMC personnalisée à cette adresse http://technet.microsoft.com/en-us/library/bb742441.aspx#XSLTsection126121120120 (en anglais).

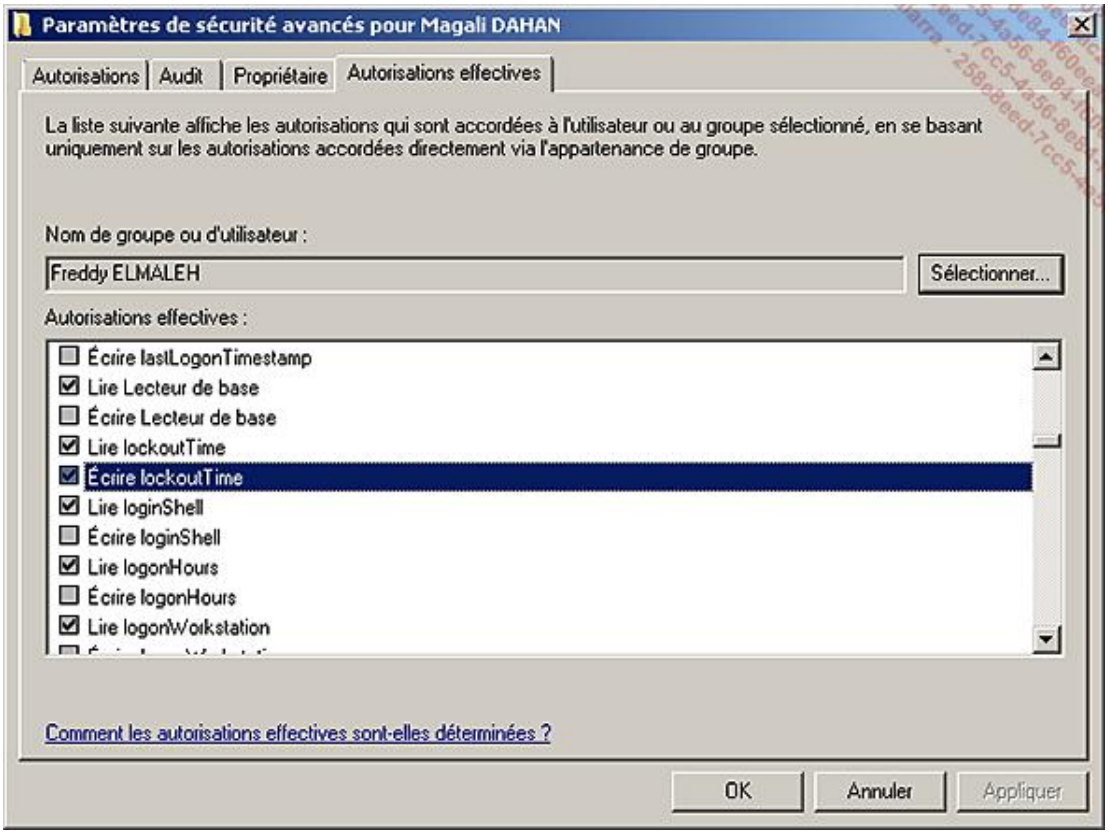
Bien qu'en ayant référencé toutes vos délégations, vous vous rendrez vite compte qu'il n'est pas toujours simple de retrouver le bon document pour savoir « qui a le droit de faire quoi ». Microsoft a inclus pour cela un onglet vous permettant de lister les **autorisations effectives** d'un compte ou d'un groupe utilisateur sur l'objet de votre choix (option disponible aussi bien au niveau des droits NTFS qu'au niveau de l'annuaire). Cette option peut donc être très pratique afin d'y voir plus clair dans la délégation mise en œuvre mais aussi afin de pallier les problèmes de droits souvent hérités d'objets parents difficilement identifiables. Grâce à cet outil, vous pourrez plus facilement identifier les problèmes.

- Ouvrez les **Propriétés** d'un compte utilisateur présent dans le conteneur de votre choix (par exemple l'unité d'organisation sur laquelle vous avez défini votre délégation lors du précédent exercice) puis cliquez sur l'onglet **Sécurité - Avancé - Autorisations effectives** (pour rappel, si l'onglet **Sécurité** n'est pas présent, il faut choisir d'afficher les **Fonctionnalités avancées** au niveau des options d'affichage).

- Cliquez sur **Sélectionner** et indiquez le compte d'un utilisateur (dans notre exemple, il s'agit d'un compte utilisateur membre du groupe HotlineUsers).

Tous les droits que possède le compte utilisateur sur l'objet sélectionné sont alors listés. Dans l'impression écran ci-après, nous voyons bien que la permission **Écrire lockoutTime** est activée.

© ENI Editions - All rights reserved - adamo diarra



La délégation des tâches administratives est donc un élément important à intégrer dans vos processus d'administration afin de délimiter au mieux le rôle de chacun.

© ENI Editions - All rights reserved - adamo diarra

Sécurisation du réseau

La sécurisation du réseau d'entreprise est également une étape primordiale de la sécurisation générale de votre infrastructure. Cette partie a pour but de présenter les fonctionnalités intéressantes de Windows Server 2008 R2 afin de l'implémenter au mieux dans votre infrastructure réseau existante.

1. Network Access Protection

Windows Server 2008 R2 apporte une surcouche réseau nommée NAP (pour *Network Access Protection*). Un contrôle de conformité est effectué sur tous les serveurs et postes de travail (supportant cette fonctionnalité) avant toute connexion au réseau de production.

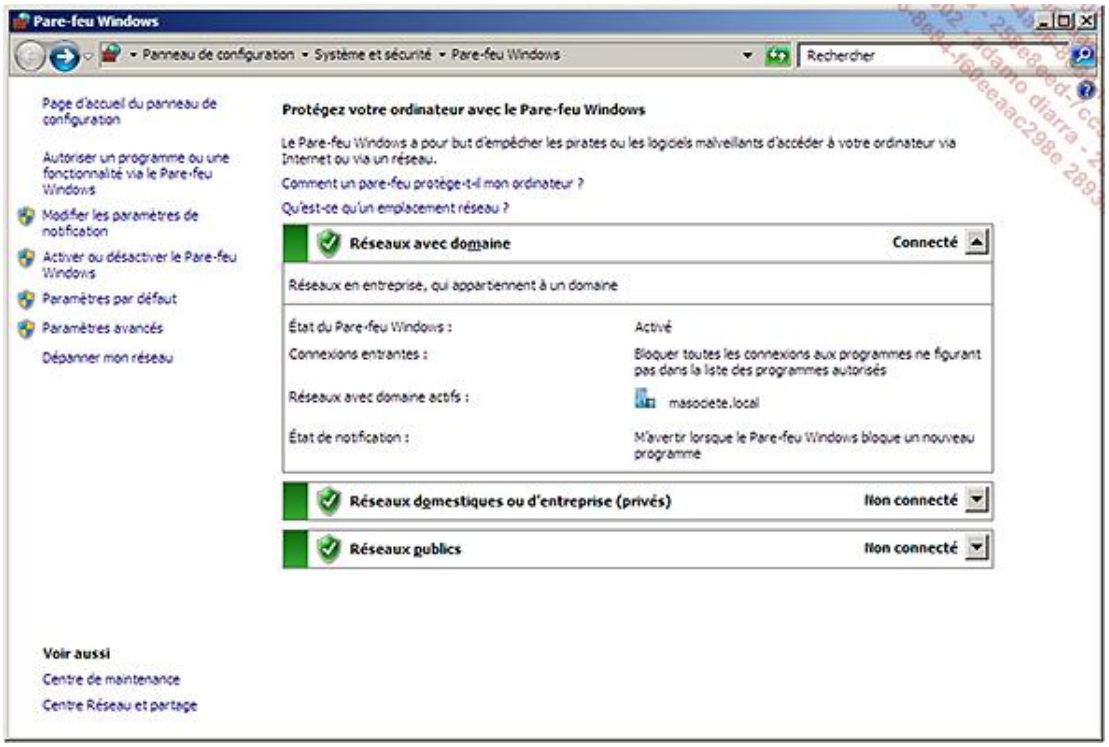
Vous devez ainsi définir au préalable un ensemble de pré-requis de sécurité (antivirus à jour, pare-feu activé, etc). Vous serez alors capable de garantir que les ordinateurs se connectant à votre réseau d'entreprise possèdent un niveau de sécurité minimal. Si ce n'est pas le cas, ces ordinateurs sont placés en quarantaine dans un réseau dédié et non routé le temps de pouvoir répondre aux pré-requis demandés. Vous pourrez obtenir davantage d'informations sur NAP en vous référant au chapitre Mise en place des services réseaux d'entreprise.

2. Le pare-feu Windows

Windows Server 2008 R2 met à disposition un pare-feu capable d'analyser à la fois le trafic entrant et le trafic sortant grâce à son nouveau module pare-feu à sécurité avancée accessible via la console MMC du même nom.

Ce module de pare-feu n'est pas à confondre avec le pare-feu « basique » bien connu des environnements XP et accessible via la commande `firewall.cpl` puis **Modifier les paramètres**. Le pare-feu basique ne permet pas de définir des règles pour le trafic sortant mais uniquement des exceptions pour le trafic entrant.

Sous Windows Server 2008 R2, l'interface du pare-feu basique a évolué (comparé à celle présente sous Windows 2008) et permet notamment l'activation simultanée de plusieurs profils de pare-feu. Chaque interface pourra ainsi avoir un profil actif différent (et donc les règles de pare-feu associées).



Sous Windows Server 2008 R2, il est désormais possible de configurer les règles de pare-feu depuis la console MMC **Pare-feu avec fonctions avancées de sécurité** (accessible depuis les Outils d'administration ou le raccourci **wf.msc**). Le pare-feu est également configurable en ligne de commande via l'argument **advfirewall** de la commande `netsh`.

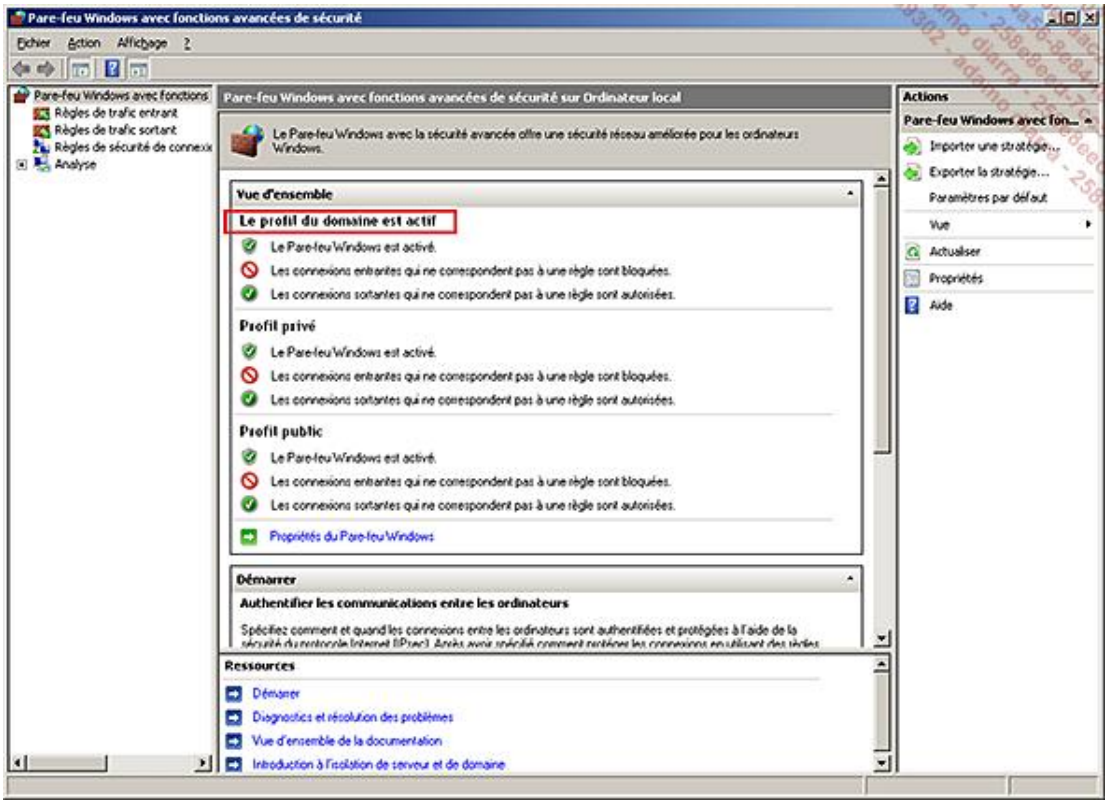
La console MMC permet de définir de façon simple une configuration très précise et granulaire. Cela permet de coller au mieux avec la réalité des besoins de production.

Il est possible de définir une configuration de pare-feu différente pour chacun des trois profils de réseau existants

© ENI Editions - All rights reserved - adamo diarra

sous Windows Server 2008 R2. Le choix du type de profil se fait lors de la première connexion de la carte réseau et peut donc se retrouver au niveau de la console **Centre Réseau et partage**.

Vous pouvez également connaître le profil actif (et donc pour lequel les règles de pare-feu associées s'appliqueront) directement depuis la console MMC de configuration du pare-feu avancé.



Pour rappel, les trois profils existants sont les suivants :

- Un **Profil de domaine** : il est automatiquement activé lorsque votre ordinateur est connecté à un domaine Active Directory.
- Un **Profil privé** : il est activé lorsque votre ordinateur est connecté à un réseau sans domaine Active Directory (aucun contrôleur de domaine disponible).
- Un **Profil public** : il est activé lorsque vous vous connectez à des réseaux que vous avez jugé peu sûrs comme les cybercafés, les aéroports, ou les autres lieux dans lesquels la sécurité réseau n'est pas ou peu assurée.

Afin de centraliser le paramétrage des règles de pare-feu sur vos serveurs membres du domaine, il vous est possible (et même conseillé !) d'utiliser les stratégies de groupe. À noter, que ces stratégies de groupe sont également disponibles pour le pare-feu de Windows Vista qui est identique à celui-ci. Pour cela, saisissez **gpedit.msc** depuis le menu **Démarrer - Exécuter** puis rendez-vous dans le conteneur **Configuration ordinateur - Stratégies - Modèles d'administration - Réseau - Connexion réseau - Pare-feu Windows**.

Vous allez maintenant configurer une règle de pare-feu afin de mieux vous rendre compte de toute l'étendue des possibilités proposées. Vous allez par exemple autoriser la connexion depuis Internet vers le port 80/TCP de votre serveur hébergeant pour l'heure un serveur Web Apache (nous avons délibérément choisi un serveur Web tiers afin de faciliter la compréhension des exceptions de pare-feu sur un exécutable).

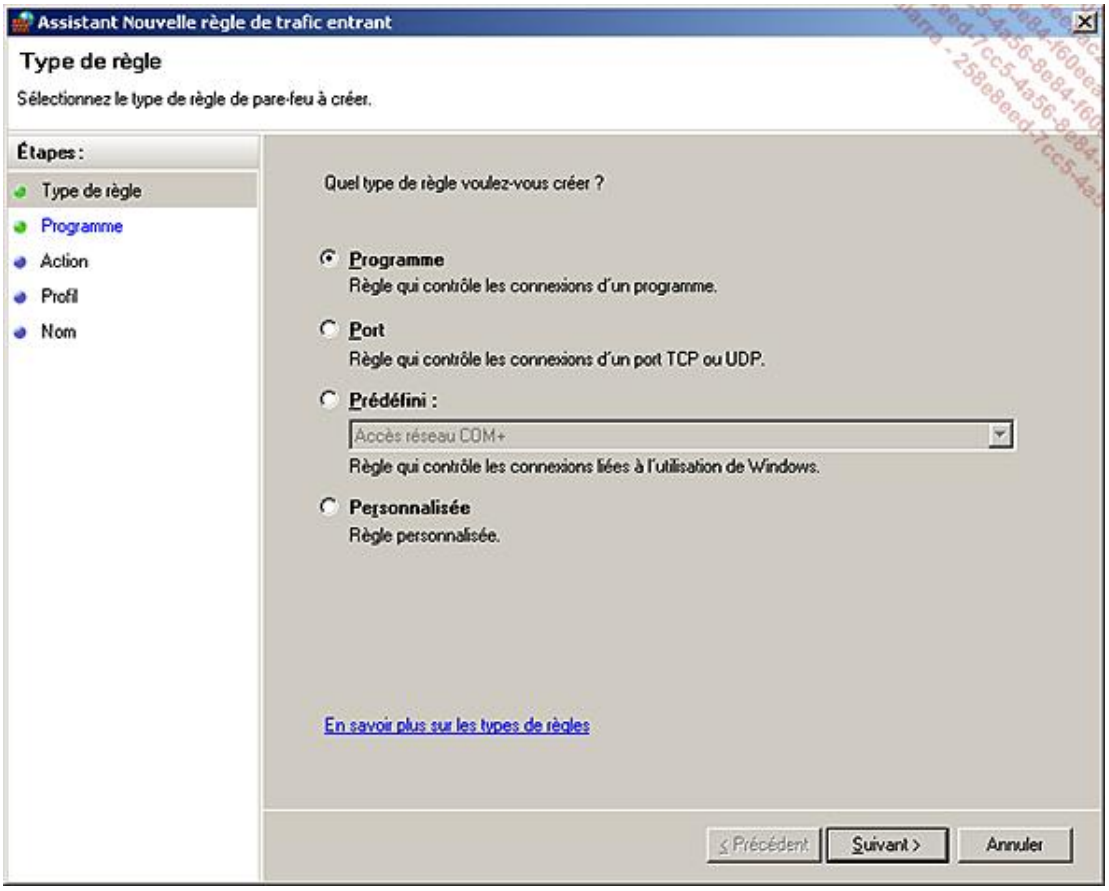
- Pour cela, ouvrez la console **Pare-feu Windows avec fonctions avancées de sécuritée** (**wf.msc** depuis le menu **Démarrer - Exécuter**), et faites un clic avec le bouton droit de la souris sur **Règles de trafic entrant**, puis **Nouvelle règle**.

L'assistant se lance alors afin de choisir le type de règle de pare-feu à créer. Quatre choix s'offrent alors à vous :

- **Programme** : cette option vous permet de définir l'exécutable pour lequel l'action définie à l'étape suivante s'appliquera.

© ENI Editions - All rights reserved - adamo diarra

- **Port** : permet de spécifier un port ou une liste de ports TCP ou UDP locaux de votre ordinateur.
- **Prédéfini** : règle correspondant à un service Windows (utile pour des ports ouverts dynamiquement et aléatoirement, ne nous obligeant pas à ouvrir toute une rangée de port).
- **Personnalisée** : permet de personnaliser sa règle afin de limiter l'autorisation uniquement à un programme précis sur un port défini par exemple.

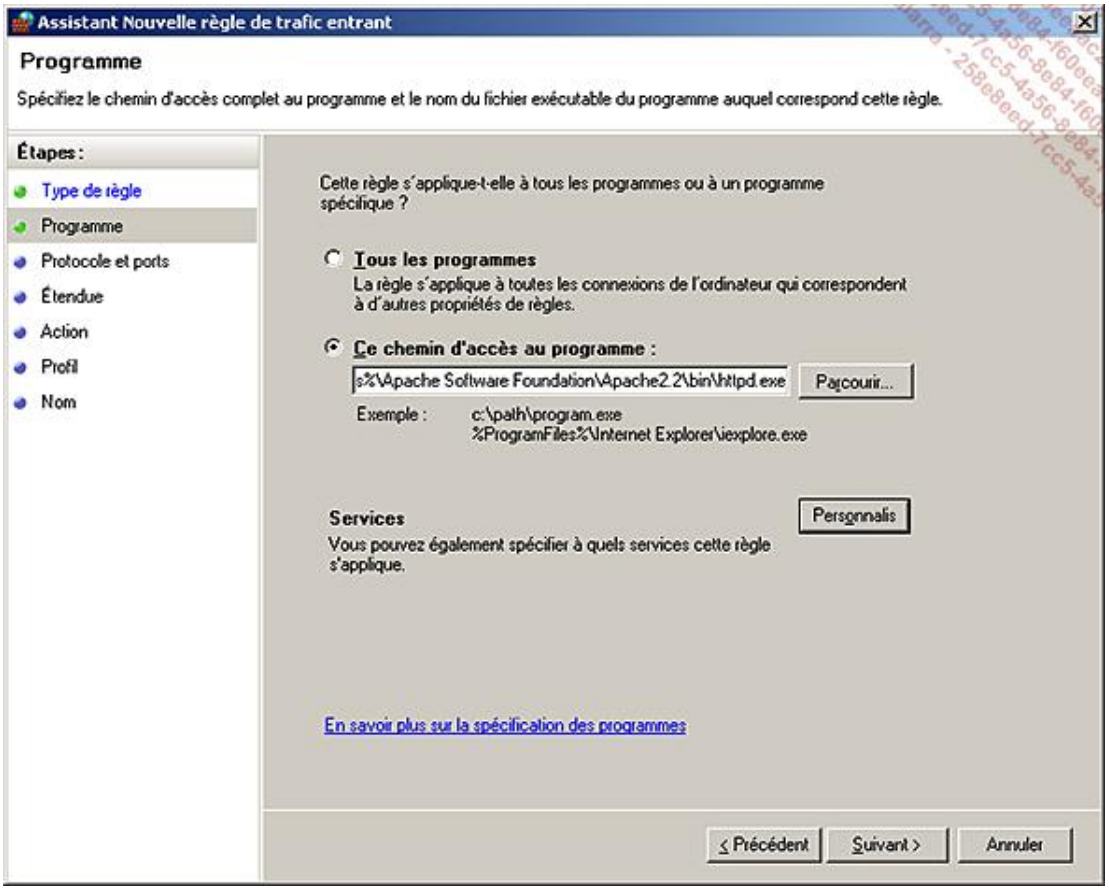


- Dans cet exemple, choisissez de créer une **règle personnalisée** puis cliquez sur **Suivant**.

Ainsi, si vous définissez une règle personnalisée associée au service **Agent de stratégie IPSec**, ce service démarrera une fois la règle activée. L'intérêt est ainsi de réduire le temps de démarrage de votre système d'exploitation. Vous connaîtrez les évènements spécifiques entraînant le démarrage d'un service à l'aide de la commande `sc qtriggerinfo <nom du service>` (dans cet exemple sc qtriggerinfo PolicyAgent).

- Spécifiez alors, si vous le souhaitez, l'exécutable ou le service de votre choix puis cliquez sur **Suivant**. Dans cet exemple, indiquez le chemin complet de l'exécutable du serveur Web Apache (**C:\Program Files\Apache Software Foundation\Apache2.2\bin\httpd.exe**). Il aurait également été possible de définir le service Apache au cours de cette même étape de l'assistant.

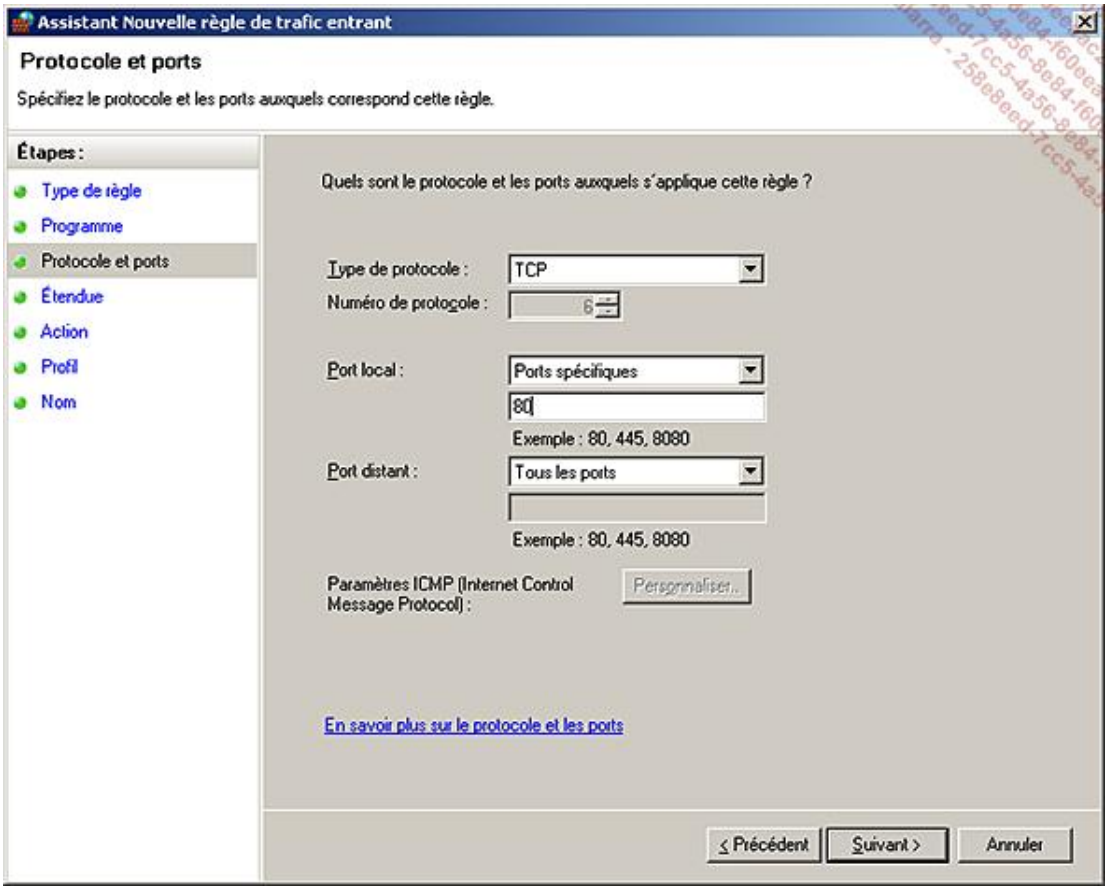
© ENI Editions - All rights reserved - adamo diarra



- Il vous reste maintenant à définir le ou les ports à autoriser (ou interdire) pour répondre à vos besoins. Le port local correspond au port de l'ordinateur sur lequel est appliqué le profil de pare-feu. Le port distant est le port situé sur l'ordinateur qui essaie de communiquer avec celui sur lequel est appliqué le profil de pare-feu. Dans cet exemple, il vous faut autoriser le port **80/TCP** local de votre serveur pour autoriser une connexion HTTP classique.

Notez qu'il est également possible de définir une plage de ports à ouvrir.

© ENI Editions - All rights reserved - adamo diarra



- L'étendue de la règle peut alors être paramétrée en indiquant les adresses IP sources et de destinations pour lesquelles cette règle s'applique. Vous pouvez laisser un accès à **Toute adresse IP** dans cet exemple. Cliquez alors sur **Suivant**.

  Trois actions s'offrent à vous. Votre choix s'applique au trafic défini à l'étape précédente :

  - **Autoriser la connexion** : en d'autres termes cela permet, dans notre exemple, le trafic entrant vers le serveur Web Apache.

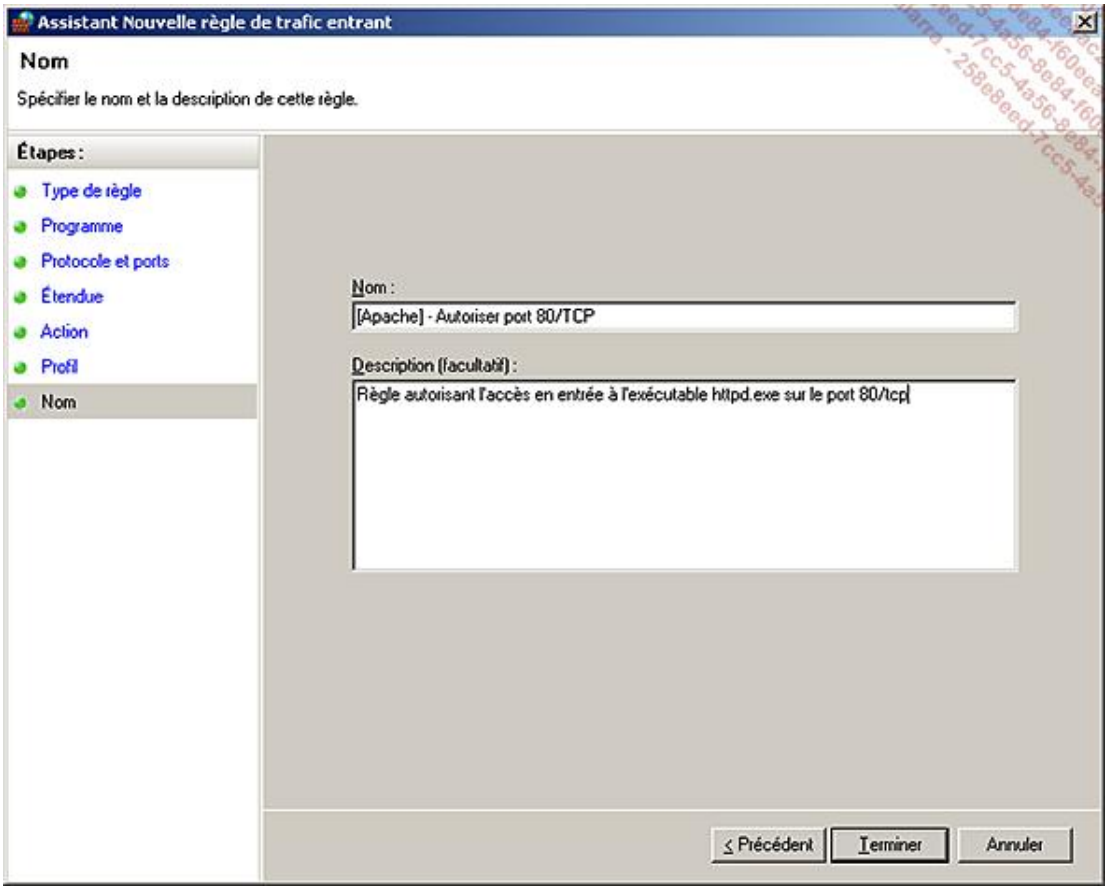
  - **Autoriser la connexion si elle est sécurisée** : permet de contrôler l'intégrité et l'authentification de chaque paquet envoyé depuis votre ordinateur en se basant sur le protocole IPSec. Nous verrons ce point un peu plus tard dans ce chapitre au paragraphe Le chiffrement IPSec. L'option **Exiger le chiffrement des connexions** permet d'activer l'IPSec afin de chiffrer les paquets lors de leur transmission. Le destinataire de ces paquets doit lui aussi être configuré afin de pouvoir envoyer et recevoir ce type de trafic, sans quoi le dialogue entre les deux correspondants est impossible.

  - **Bloquer la connexion** : bloque la condition définie précédemment dans l'assistant.

  Pour notre exemple, choisissez **Permettre toutes les connexions**, puis cliquez sur **Suivant**.

- Indiquez alors les profils de connexion pour lesquels cette règle s'appliquera puis cliquez sur **Suivant** pour donner un **Nom** à cette règle de pare-feu.

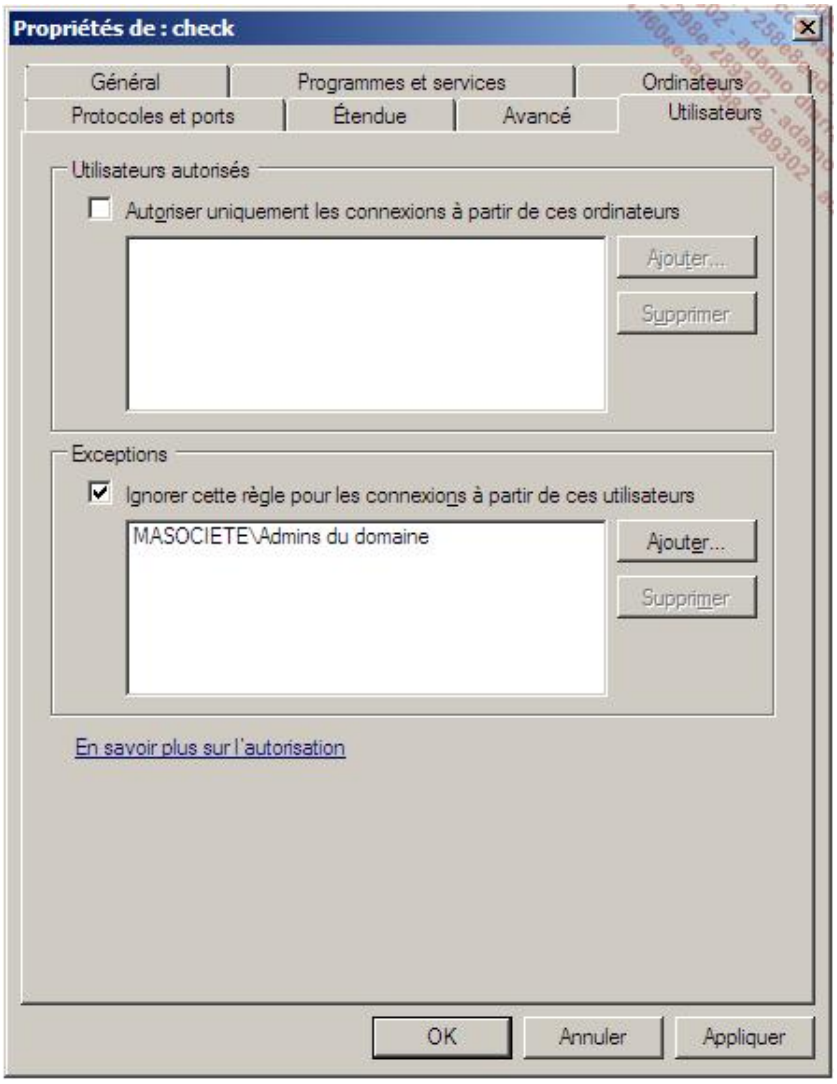
© ENI Editions - All rights reserved - adamo diarra



Votre règle de pare-feu est maintenant créée et effective ! Elle apparaît en haut de la liste de votre console MMC.

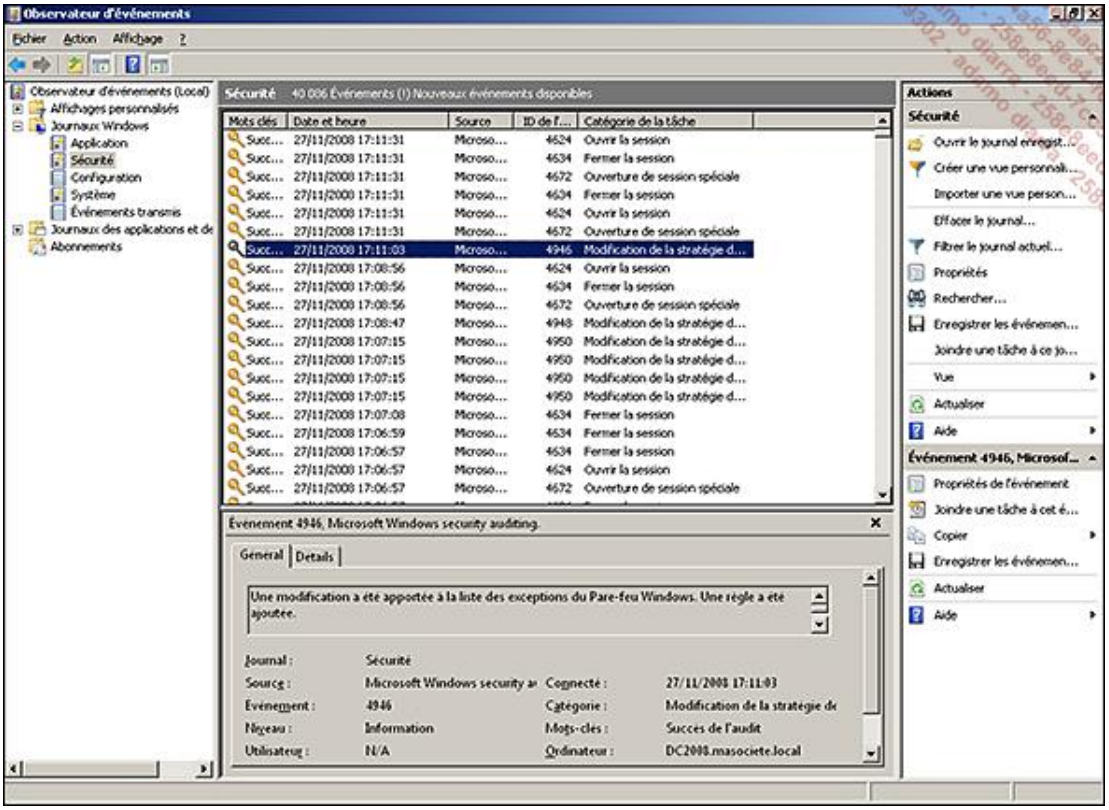
Sous Windows Server 2008 R2, si vous avez choisi de **N'autoriser que les connexions sécurisées** pour une règle spécifique, il est alors possible d'éditer cette règle afin de définir des utilisateurs ou des ordinateurs pour lesquels cette règle ne s'appliquera pas.

© ENI Editions - All rights reserved - adamo diarra



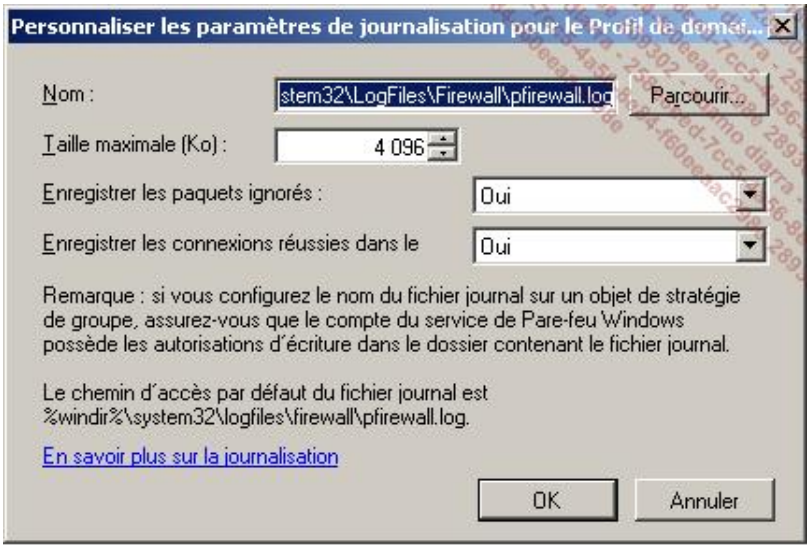
À noter que si l'audit des modifications des stratégies est activé (via la stratégie de groupe au niveau de **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Stratégie d'audit**), un évènement portant le numéro 4946 est généré dans le journal de sécurité afin d'indiquer qu'une règle de pare-feu vient d'être créée.

© ENI Editions - All rights reserved - adamo diarra



Il faut également savoir qu'aucun fichier de journalisation n'est créé par défaut. Il peut être utile de configurer celui-ci afin de faciliter la détection d'attaque sur votre serveur (scan des ports ouverts), ou le débogage permettant de trouver les ports à autoriser pour une application précise (Il suffira ainsi de tenter une connexion et de regarder dans le fichier de journalisation les paquets qui n'ont pas été autorisés).

Afin de configurer le fichier de journalisation, faites un clic avec le bouton droit de la souris sur **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local - Propriétés**. Cliquez sur **Personnaliser** au niveau d'**Enregistrement**. Vous pouvez alors définir un chemin et un nom pour le fichier journal, une taille maximale et le type d'évènements à journaliser (paquets ignorés et/ou connexions réussies).



3. Le chiffrement IPSec

L'IPSec est un standard de sécurité qui fournit l'**authentification** et le **chiffrement des connexions**. Ces deux notions de sécurité ne sont pas indissociables et IPSec peut fournir l'authentification sans le chiffrement et inversement. IPSec agissant sur la couche réseau du modèle OSI, il est ainsi capable de protéger n'importe quelle application réseau.

Le chiffrement des connexions via IPSec permet de rendre les attaques systèmes orientées réseau beaucoup plus

© ENI Editions - All rights reserved - adamo diarra

difficiles. Si un attaquant venait, par exemple, à écouter (sniffer) le réseau lors d'un transfert de fichiers entre deux ordinateurs configurés pour utiliser le chiffrement IPSec, il sera dans l'impossibilité de déchiffrer les fichiers échangés !

Le second avantage du protocole IPSec est également de fournir une authentification des participants et de garantir l'intégrité des données lors d'échange réseau. IPSec peut ainsi authentifier un client réseau (via une authentification Kerberos ou un certificat par exemple) avant de permettre l'initialisation de la connexion réseau. L'attaque de type « Man in the middle » consiste à ce qu'un attaquant se fasse passer pour le serveur aux yeux du client et inversement pour le client aux yeux du serveur. Il peut ainsi écouter tout le trafic réseau entre ces deux partenaires (puis le réémettre immédiatement au vrai destinataire) et alors récupérer le mot de passe de l'utilisateur lors d'une phase d'authentification sur le domaine Active Directory par exemple.

L'authentification IPSec permet d'empêcher ce type d'attaque en authentifiant les participants et en s'assurant que les données n'ont pas été modifiées durant leur transport.

Cette authentification peut également être très utile pour définir une réplication entre des contrôleurs de domaine se trouvant sur des sites différents et ainsi garantir l'intégrité de la transaction.

Il faut également savoir que le protocole IPSec fonctionne dans deux modes possibles. Le **mode transport** ou le **mode tunnel**.

Le mode transport d'IPSec permet de protéger des communications entre deux hôtes d'un même réseau privé ou entre deux hôtes n'étant pas séparés par une translation d'adresses réseau (NAT). Dans ce dernier cas, vous pourrez mettre en œuvre de l'IPSec Nat Traversal (NAT-T) à condition que le serveur NAT et les hôtes supportent le NAT-T (cf RFC 3947).

Le mode tunnel d'IPSec protège les communications entre un hôte et un réseau, ou de réseau à réseau. Ce mode est plus souple que le mode transport.

Windows Server 2008 R2 permet donc de définir des règles d'isolation (car une authentification est nécessaire) ou de chiffrement à l'aide du protocole IPSec.

Cette configuration peut être mise en place de façon assez fine via l'emplacement habituel et connu des anciennes versions de Windows Server, c'est-à-dire au niveau de la stratégie de groupe **Configuration ordinateur - Stratégies - Paramètres Windows Paramètres de sécurité - Stratégies de sécurité IP**. L'avantage de cette console est que vous pouvez définir le type de trafic IP que vous souhaitez autoriser. Si vos besoins se limitent cependant à définir des règles pour des connexions point-à-point (sans besoin de filtrage de ports entre les deux), les **règles de sécurité de connexion** sont bien mieux adaptées car elles sont beaucoup plus faciles à mettre en œuvre.

Vous pouvez configurer vos règles de sécurité de connexion depuis la même console MMC que le pare-feu Windows avancé. Cela facilite grandement sa mise en œuvre.

Avant de vous lancer dans la configuration de stratégies IPSec, assurez-vous d'avoir bien compris et paramétré vos stratégies IPSec sans quoi vous risquez de bloquer totalement l'accès réseau à ce serveur. Il convient donc de tester ces règles avant de les appliquer.

Vous allez maintenant tenter d'appliquer ce qui a été expliqué à l'aide d'un exemple. Dans cet exemple, vous allez chiffrer le trafic entre deux ordinateurs. Pour cela, suivez les étapes suivantes :

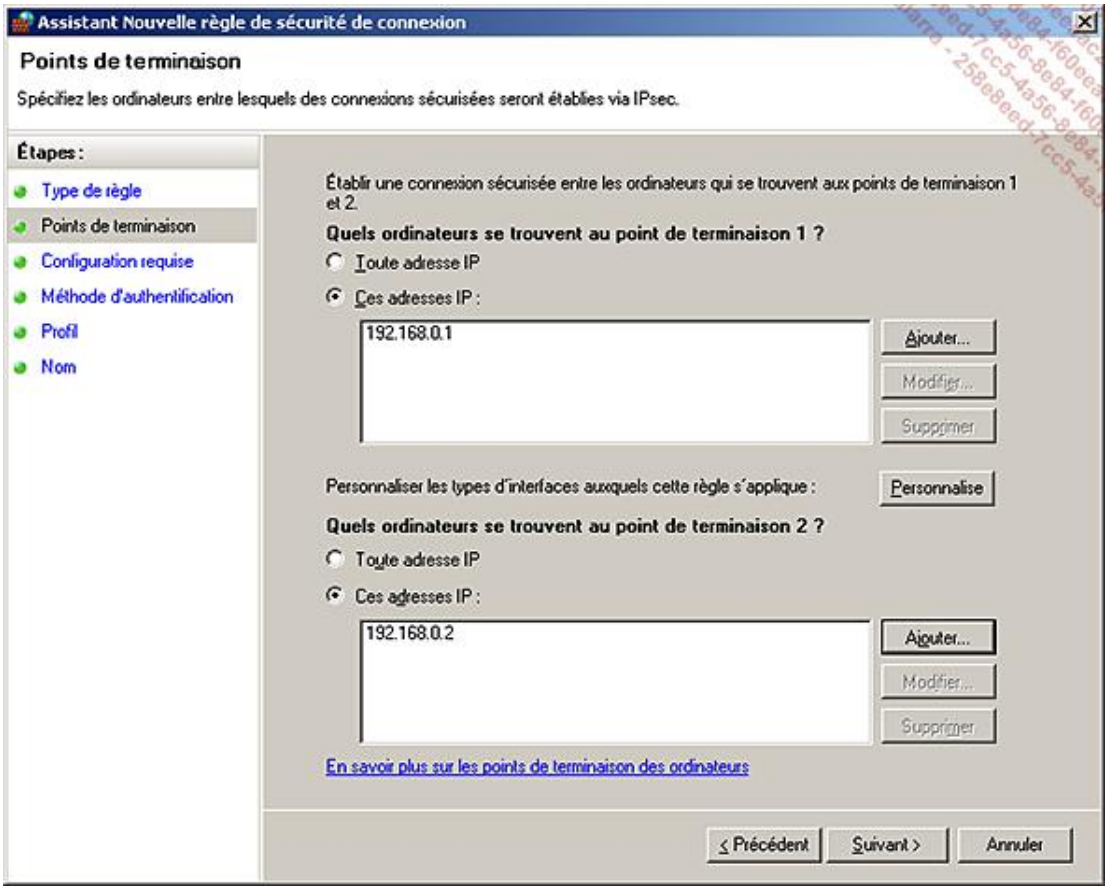
- Lancez la console **wf.msc** puis placez-vous au niveau de **Règles de sécurité de connexion - Action - Nouvelle règle**.

- Plusieurs types de règle de sécurité s'offrent à vous. Afin d'avoir une vision complète des possibilités choisissez **Personnalisée**, puis **Suivant**.

- Définissez alors un point de Terminaison 1 et point de Terminaison 2 correspondant à l'adresse IP de chacun des serveurs. Dans notre exemple, le point de Terminaison 1 est l'adresse IP de notre serveur local (192.168.0.1) et le point de Terminaison 2 est le serveur distant (192.168.0.2). Cliquez alors sur **Suivant**.

Depuis Windows Server 2008 R2 et Windows 7, la gestion des points de terminaison dynamique est possible. Cette fonctionnalité est notamment utilisée par Direct Access pour les utilisateurs nomades possédant une adresse IP dynamique. Vous obtiendrez davantage de renseignements sur Direct Access dans le chapitre Accès distant.

© ENI Editions - All rights reserved - adamo diarra



- Choisissez alors les conditions d'authentification requises. Dans notre exemple, choisissez d'**Imposer l'authentification des connexions entrantes et sortantes** puis cliquez sur **Suivant**.

  La méthode d'authentification utilisée se base sur la méthode définie au niveau des paramètres par défaut de l'IPSec. Ces paramètres sont configurables au niveau des **Propriétés** du **Pare-feu Windows avec fonctions avancées de sécurité -** onglet **Paramètres IPSec - Personnaliser**.

Tant que vous êtes à cet endroit, profitez-en pour définir l'obligation de chiffrement des données en cliquant sur **Personnaliser** au niveau de **Protection des données** (mode rapide) et en cochant la case **Demander le chiffrement de toutes les règles de sécurité de connexion pour protéger le trafic réseau**. Cliquez sur **OK** à trois reprises afin de revenir à l'assistant.

Dans cet exemple, au niveau de l'étape **Méthode d'authentification**, cliquez sur **Personnaliser** au niveau de **Avancé**. Cliquez alors sur **Ajouter** au niveau de la première authentification et choisissez **Clé pré-partagée** (ce paramètre n'est pas conseillé sur un réseau de production mais est acceptable dans le cadre de tests de mise en œuvre).

Il est également possible de définir depuis la console le **Protocole et ports** pour lesquels cette règle s'appliquera, ce qui permet de définir encore plus finement le tunnel IPsec créé. Cette opération est également possible via la commande netsh.

En environnement de production, si les ordinateurs sont sur un même domaine Active Directory, l'authentification Kerberos est recommandée car elle ne nécessite pas de configuration particulière des ordinateurs concernés. Pour des ordinateurs ne faisant pas partie du même domaine, une authentification par certificat devra être utilisée. Indiquez alors la valeur **TestAuthentification** à cette clé pré-partagée. Cliquez sur **OK** à deux reprises puis **Suivant**.

- Spécifiez les profils auxquels s'applique cette règle. Les trois profils peuvent rester cochés.

- Donnez alors un nom à cette règle et cliquez sur **Terminer**.

Comme nous avons imposé l'authentification des connexions entrantes et sortantes, à partir du moment où vous cliquerez sur **Terminer**, la connexion n'est plus possible entre les deux serveurs. Il convient donc de recréer cette même règle sur le second serveur.

Comme vous avez pu le constater, Windows Server 2008 R2 propose de nombreuses fonctionnalités de sécurité avancées. Ces dernières ne riment cependant pas nécessairement avec une perte de productivité. En effet, beaucoup de ces paramètres de sécurité sont facilement accessibles et peuvent être administrés de façon centralisée.

© ENI Editions - All rights reserved - adamo diarra

© ENI Editions - All rights reserved - adamo diarra

Introduction

Dans ce chapitre vous apprendrez à implémenter des solutions pour garantir la santé de votre réseau une fois celui-ci en place.

© ENI Editions - All rights reserved - adamo diarra

Gestion des sauvegardes

Penser qu'un système mis en place récemment ou qui tourne depuis longtemps ne nécessite aucune attention est illusoire. En effet, nul ne peut éviter les événements inattendus pour son système d'information. Crash de serveurs, pertes de fichiers, erreur de manipulation humaine, incendie, etc. Tous ces éléments peuvent rendre instable votre système informatique et même aller jusqu'à le rendre complètement indisponible.

Plusieurs solutions proactives sont à votre disposition pour vous prémunir face à « l'incident ». L'une d'entre elles est la sauvegarde. Le choix d'une stratégie de sauvegarde adaptée aux besoins de l'entreprise est la meilleure assurance contre une perte de données.

Différents mécanismes de sauvegarde existent :

- **Complète** : cette méthode transfère sur le support de sauvegarde une copie de toutes les données concernées par la sauvegarde, indépendamment de la modification des données depuis l'exécution de la précédente sauvegarde.
- **Différentielle** : sauvegarde toutes les données qui ont été modifiées depuis la dernière sauvegarde complète.
- **Incrémentielle** : sauvegarde toutes les données qui ont été modifiées depuis la dernière sauvegarde, que ce soit une complète ou une incrémentielle.

Si apparemment les sauvegardes incrémentielles et différentielles sont très proches, dans les faits elles ont chacune leurs avantages et inconvénients.

Une sauvegarde différentielle nécessite moins de médias pour effectuer une restauration. En effet, seule la dernière sauvegarde complète ainsi que la dernière sauvegarde différentielle sont nécessaires.

Avantage : la restauration est rapide.

Inconvénient : le volume de données sauvegardé est plus important et les sauvegardes sont donc plus longues à être réalisées.

La sauvegarde incrémentielle prend moins de temps. Celle-ci ne sauvegarde que les éléments ayant été modifiés depuis la dernière sauvegarde (complète ou incrémentielle). Le volume à sauvegarder est donc moins important.

Avantage : les sauvegardes sont plus rapides et nécessitent moins de capacité sur les médias.

Inconvénient : la restauration est plus lente car il vous faudra utiliser plus de médias. La restauration requiert la dernière sauvegarde complète, ainsi que toutes les incrémentielles qui suivent jusqu'à celle que vous avez besoin de restaurer.

Dans tous les cas, il faut que vous fassiez très attention à vos sauvegardes complètes. Ce sont elles qui vont déterminer le comportement des sauvegardes suivantes.

1. Windows Server Backup

Windows intègre, depuis sa version 3.1, un outil de sauvegarde appelé NTBACKUP. Avec l'arrivée de Windows Server 2008, celui-ci a été remplacé. Le nom de son successeur est : WSB (*Windows Server Backup*).

Ne saisissez donc plus `ntbackup` dans le menu **Exécuter**, autrement vous recevrez une erreur spécifiant que l'outil n'existe pas.

Windows Server Backup fournit une solution pour répondre aux besoins de sauvegarde et de restauration. Vous pouvez l'utiliser pour sauvegarder de façon complète un serveur, ou encore pour sauvegarder certains volumes, certaines applications ou bien uniquement l'état du système.

Il peut effectuer des sauvegardes locales ou distantes en fonction de votre organisation. Les sauvegardes sont planifiables afin de fonctionner de façon automatisées (le mécanisme reprend les tâches planifiées de Windows tout comme le faisait NTBACKUP). Il est également possible d'effectuer des sauvegardes ponctuelles.

Cette nouvelle version d'outil de sauvegarde intégrée à Windows Server 2008 change de façon significative les habitudes. Elle présente cependant quelques inconvénients dont :

- Impossibilité de sauvegarder un serveur Exchange Server (hormis la version Exchange Server 2007 SP2 qui inclut un plug-in rendant ces sauvegardes possibles).
- Impossibilité de sauvegarder sur des lecteurs de bandes.

© ENI Editions - All rights reserved - adamo diarra

- Impossibilité d'écrire la sauvegarde sur un volume distant pour les sauvegardes planifiées.
- Le plus petit point de sauvegarde est le volume (pas de possibilité de sauvegarder uniquement un répertoire par exemple).
- Seuls les volumes locaux en NTFS peuvent être sauvegardés.

La version de Windows Server 2008 R2 apporte des changements importants et bénéfiques à l'outil Windows Server Backup :

- Possibilité de sauvegarder/exclure des fichiers ou types de fichier individuellement.
- Amélioration de l'utilisation des sauvegardes incrémentielles (les anciens fichiers sont automatiquement supprimés).
- Nouvelles options d'emplacements de stockage (lecteur réseau, volume non dédié aux sauvegardes, disques durs virtuels). Attention, l'utilisation d'un lecteur réseau ne conservera qu'une version de la sauvegarde.
- La planification permet désormais de sauvegarder sur un volume distant.
- L'outil WBadmin reflète les changements apportés à la console (sauvegarde planifiée sur volume distant, sauvegarde de fichiers individuels, etc.).

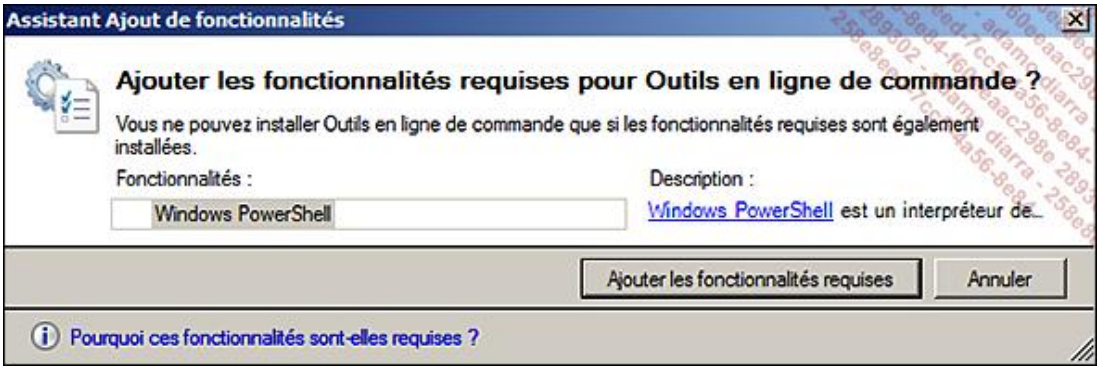
WSB ne permet pas de restaurer à partir de sauvegardes réalisées avec NTBackup. Il existe cependant une version téléchargeable de l'outil compatible avec Windows Server 2008 R2 et dédiée aux restaurations : http://support.microsoft.com/kb/974674.

---

a. Installation de Windows Server Backup

Voici les étapes requises pour procéder à l'installation de Windows Backup Server :

- Allez dans la console **Gestionnaire de serveur**.
- Développez l'arborescence **Fonctionnalités**, puis cliquez sur **Ajouter des fonctionnalités**.
- Cochez la case **Fonctionnalités** de la **Sauvegarde de Windows Server**.
- Cochez également la sous-case **Outils en ligne de commande**, le message suivant apparaît et vous devez cliquer sur **Ajouter les fonctionnalités requises**.



- Cliquez sur **Suivant**.
- Sur la page de confirmation, vérifiez que les fonctionnalités voulues ont bien été choisies puis cliquez sur **Installer**.

© ENI Editions - All rights reserved - adamo diarra

Pour installer l'outil de sauvegarde vous pouvez aussi utiliser la commande suivante : `START /W OCSETUP WindowsServerBackup`.

- Sur la page **Résultats de l'installation**, assurez-vous que celle-ci s'est bien déroulée puis cliquez sur **Fermer**.

Pour commencer à utiliser l'outil de sauvegarde :

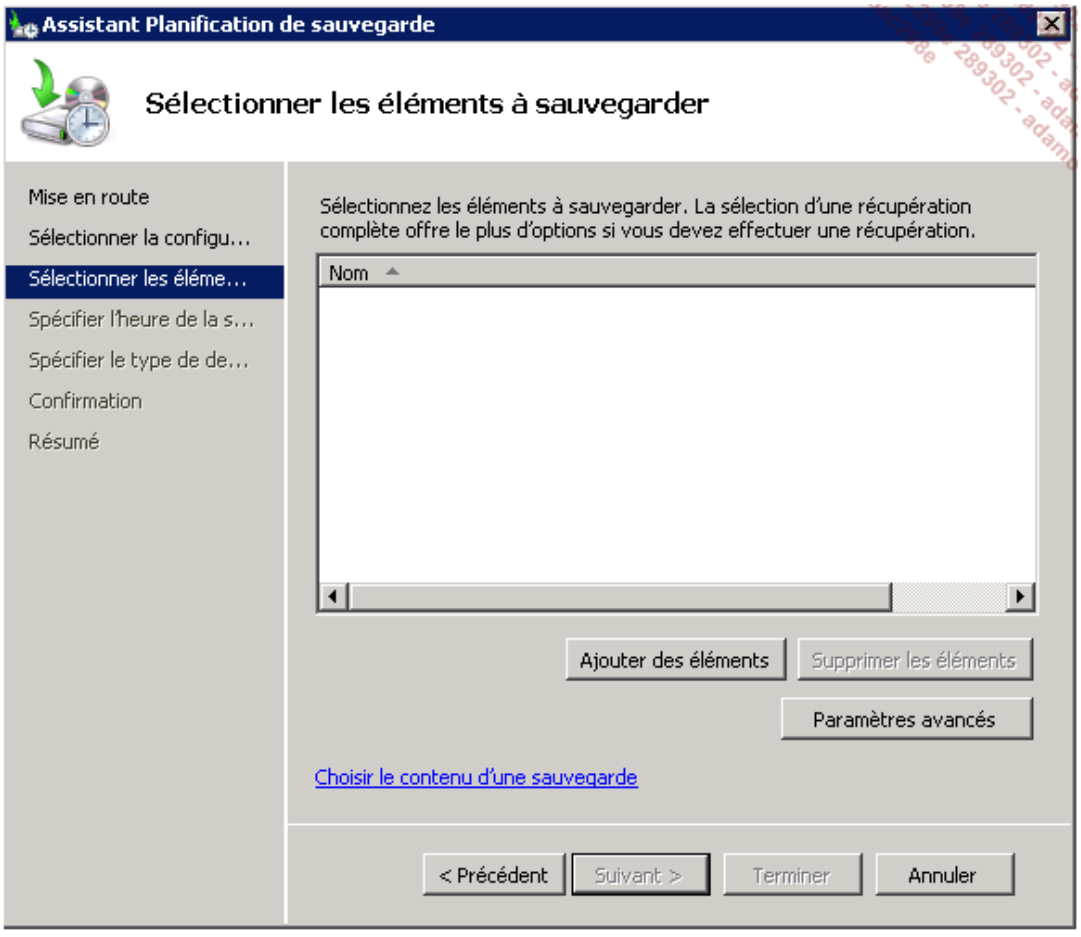
- Ouvrez le menu **Démarrer** puis développez les **Outils d'administration** et enfin cliquez sur **Sauvegarde de Windows Server**.

b. Création de la sauvegarde planifiée d'un dossier

Dans cet exemple, vous allez utiliser une des spécificités de Windows Server Backup sous Windows Server 2008 R2, à savoir la sauvegarde d'un dossier individuel.

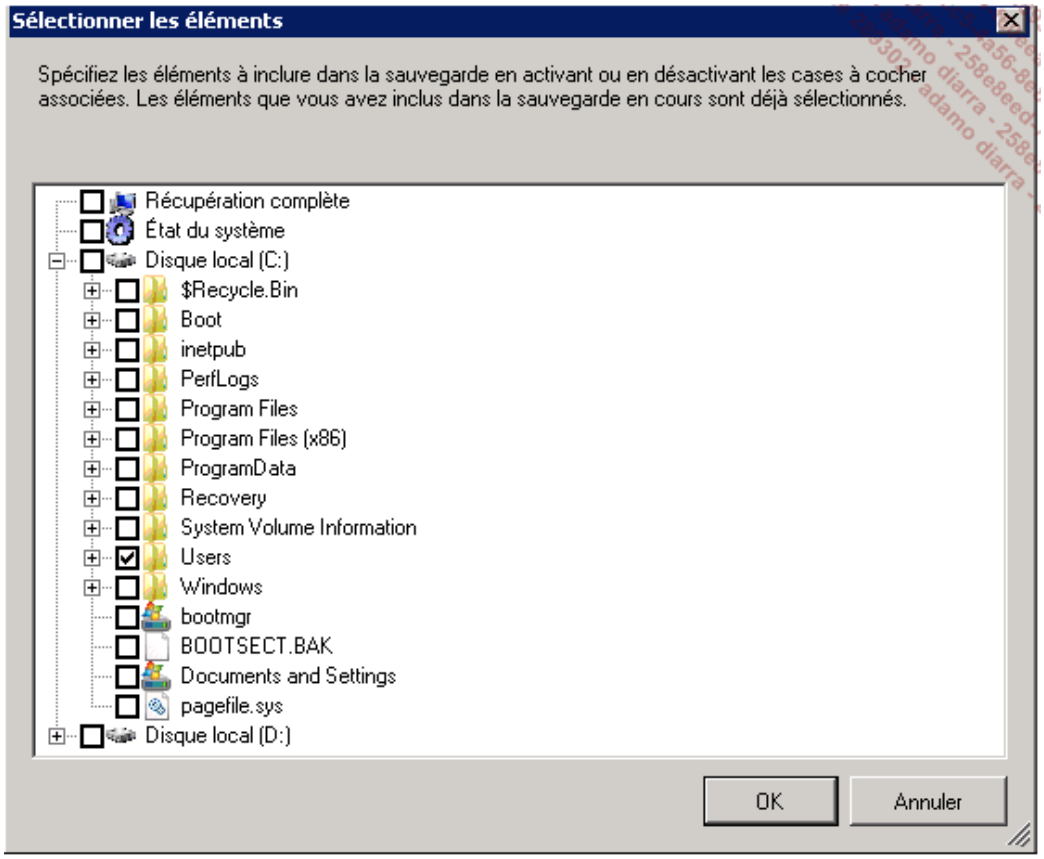
- Dans la console **Sauvegarde de Windows Server** (**Local**), dans le volet de droite cliquez sur **Planification de sauvegarde** puis cliquez sur **Suivant**.

- Sur la page de sélection, cliquez sur le bouton radio **Personnalisé** puis cliquez sur **Suivant**.



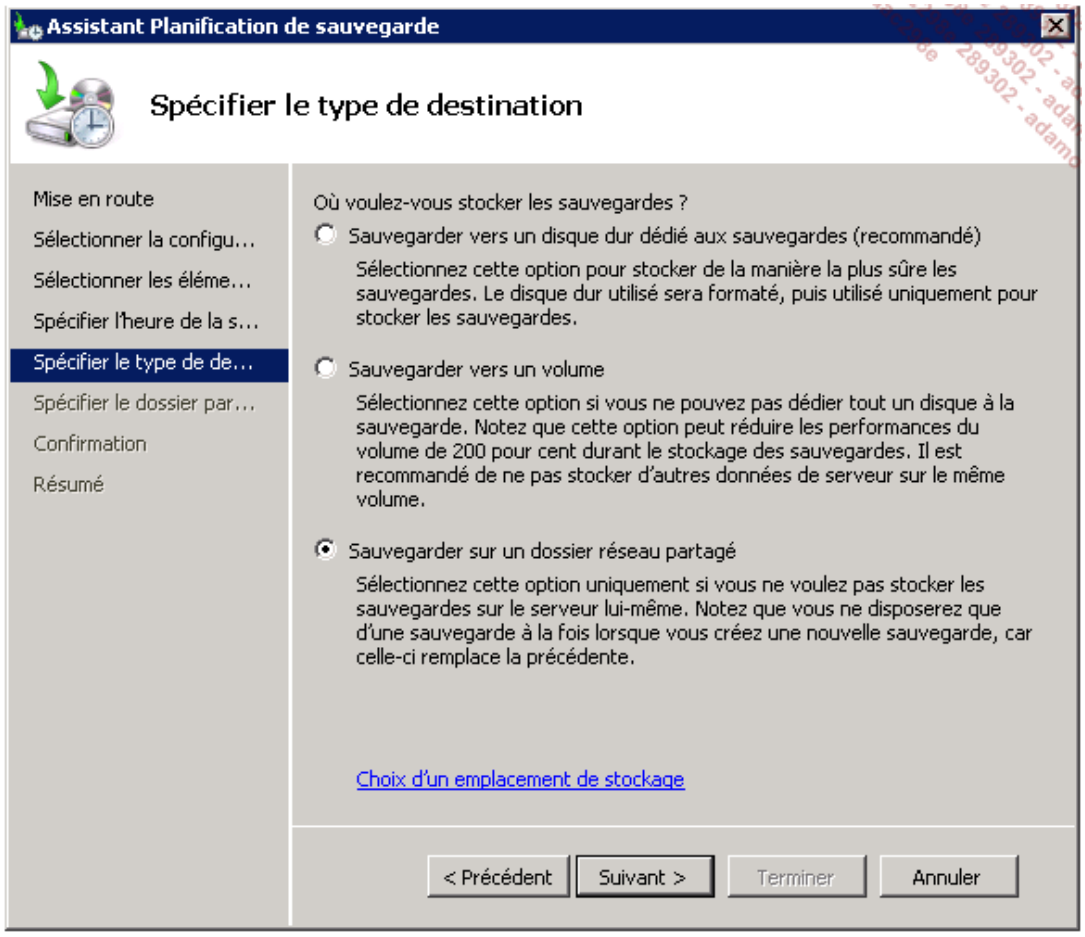
- Cliquez sur **Ajouter des éléments**.

© ENI Editions - All rights reserved - adamo diarra

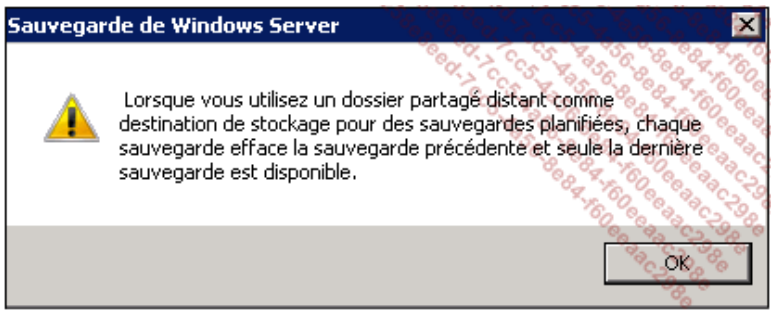


- Dans la fenêtre de sélection, cochez la case du répertoire **Users** puis cliquez sur **OK**.
- Cliquez ensuite sur **Suivant**.
- Laissez la planification par défaut (**Tous les jours à 21h**) puis cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- Sélectionnez **Sauvegarder sur un dossier réseau partagé** puis cliquez sur **Suivant**.



- Cliquez sur **OK** après avoir lu l'avertissement (celui-ci rappelle qu'une sauvegarde planifiée dont le stockage s'effectue sur un emplacement réseau efface systématiquement le fichier de sauvegarde précédent).
- Spécifiez le dossier partagé puis cliquez sur **Suivant**.
- Saisissez les identifiants qui serviront à exécuter la tâche planifiée puis validez par **OK**.
- Cliquez sur **Terminer** pour valider la création de la sauvegarde planifiée puis sur **Fermer** une fois l'opération achevée.

c. Outils associés à WSB et sauvegardes uniques

WSB offre également la possibilité d'effectuer des sauvegardes non planifiées. Cela peut être intéressant avant toute opération pouvant nécessiter de revenir en arrière (installation d'un nouveau produit, suppression d'un rôle, etc.). Ces sauvegardes uniques permettent également de ne pas inclure obligatoirement l'état du système dans la sauvegarde.

© ENI Editions - All rights reserved - adamo diarra

En suivant l'assistant **Sauvegarde unique** situé dans la console de **Sauvegarde de Windows Server**, vous pourrez :

- choisir un emplacement réseau pour effectuer la sauvegarde ;
- choisir entre une sauvegarde par Copie VSS (*Volume Shadow Copy*) ou sauvegarde complète VSS.

La copie VSS est utile si vous utilisez un autre système de sauvegarde. En effet, celle-ci laisse les attributs des fichiers intacts. De cette façon les sauvegardes qui se déroulent avec votre logiciel tiers ne sont pas affectées dans leur rotation. VSS permet également de sauvegarder des fichiers ouverts.

La sauvegarde complète VSS est utile lorsque vous n'utilisez que Windows Server Backup pour effectuer vos sauvegardes. Celle-ci, une fois son exécution terminée, met à jour l'historique de sauvegarde des fichiers.

L'outil en ligne de commande **wbadmin** est disponible avec les versions Core et Standard de Windows Server 2008 R2. Il permet de réaliser tout ce qui est paramétrable via l'interface graphique de l'assistant de sauvegarde et plus encore.

Quelques commandes utiles avec **wbadmin.exe** :

- `wbadmin enable backup` : permet de créer et de gérer les sauvegardes planifiées.
- `wbadmin start systemstatebackup` : permet de réaliser une sauvegarde de l'état du système.
- `wbadmin start backup` : permet de lancer une sauvegarde unique.
- `wbadmin get versions` : permet de voir les détails d'une sauvegarde qui a déjà été réalisée.
- `wbadmin get items` : permet de voir quels sont les éléments contenus dans un fichier de sauvegarde.

Wbadmin a l'avantage de permettre d'implémenter les commandes dans des batch. Ces batch peuvent être eux-mêmes lancés via des tâches planifiées. Vous avez également la possibilité de lancer rapidement une sauvegarde sur un stockage réseau. Par exemple la ligne suivante permet de sauvegarder le volume E sur un partage d'une autre machine :

```
Wbadmin start backup -backuptarget:\\AUTRESERVEUR\Partage -include:E: -
User:backupadmin@masociete.local -Password:P@ssw0rd
```

Pour plus d'informations sur la syntaxe de wbadmin, rendez-vous à l'adresse http://technet.microsoft.com/en-us/library/cc754015.aspx.

Bien que vous ne puissiez pas sauvegarder de ressources réseaux avec WSB, vous avez la possibilité de gérer les sauvegardes à distance :

- Depuis la console de Sauvegarde de Windows Server, cliquez sur **Se connecter à un autre...**
- Spécifiez le nom du serveur pour lequel vous voulez gérer la sauvegarde puis cliquez sur **Terminer**.

© ENI Editions - All rights reserved - adamo diarra

Microsoft a significativement restreint les capacités de l'outil de sauvegarde intégré au profit de son produit System Center Data Protection Manager (DPM) 2007.Ce produit à part entière et payant offre beaucoup plus de fonctionnalités que WSB. Pour plus d'informations sur DPM : http://technet.microsoft.com/en-us/library/bb795549.aspx.

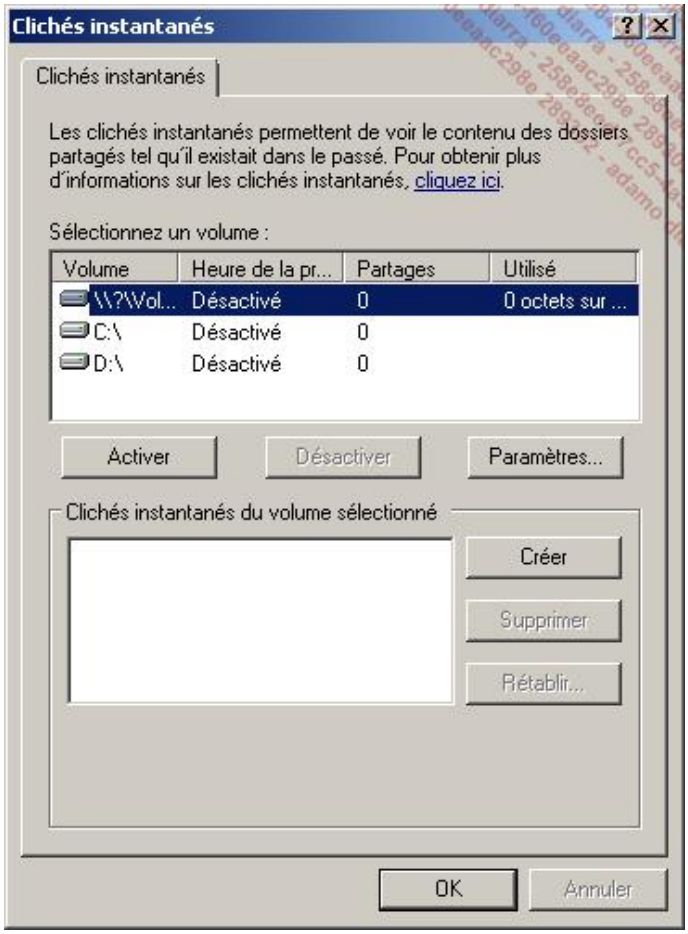
En complément des sauvegardes, vous pouvez utiliser les clichés instantanés (couramment appelés *Volume Shadow Copy*). Les clichés permettent une restauration des fichiers se trouvant sur les partages réseaux. Cette restauration s'effectue de façon très simple et très rapide.

Le principe de ce procédé est le suivant : le serveur va initier une capture de l'état des fichiers à un moment donné puis une autre capture plus tard dans le temps. Le système va alors comparer les différences entre les états. Si un fichier a été supprimé, modifié ou autre, alors le système en gardera une copie. Plusieurs planifications peuvent être positionnées pour un même volume dans une même journée. La contrainte est que le système ne conserve que 64 versions d'un fichier.

Les clichés instantanés sont activés au niveau des volumes. Pour les mettre en place :

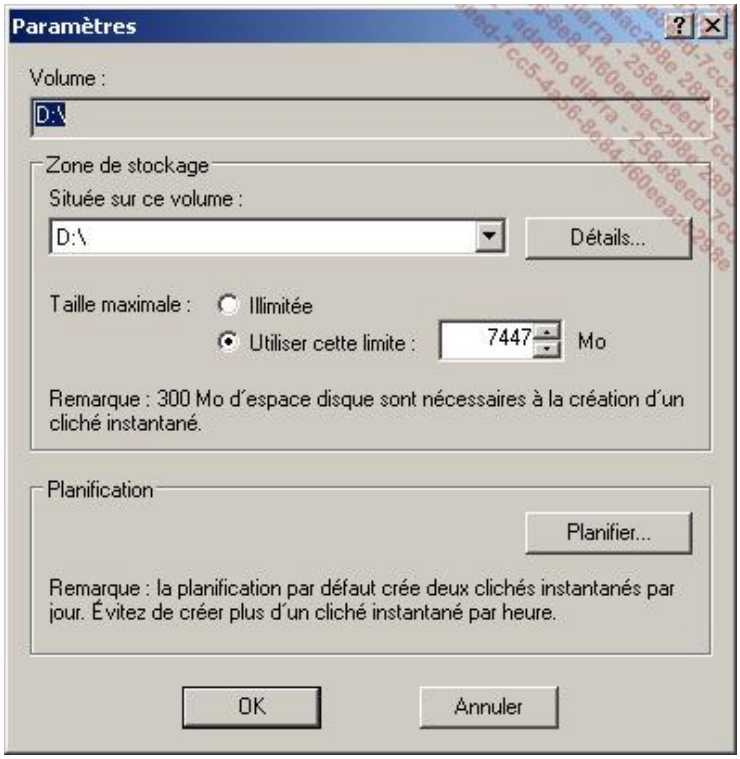
- Ouvrez votre console **Gestionnaire de serveur**.
- Développez l'arborescence **Stockage**, puis effectuez un clic avec le bouton droit de la souris sur **Gestion des disques**, puis sélectionnez **Toutes les tâches - Configurer les clichés instantanés**.

© ENI Editions - All rights reserved - adamo diarra



Depuis cette fenêtre vous pouvez activer ou désactiver les clichés. Vous pouvez également créer un cliché manuellement en appuyant simplement sur le bouton **Créer**.

Les paramètres avancés sont gérables en cliquant sur **Paramètres...** et après avoir sélectionné un volume. De là vous pouvez spécifier les planifications de ces clichés, leur emplacement de stockage ainsi que leur taille maximale.



© ENI Editions - All rights reserved - adamo diarra

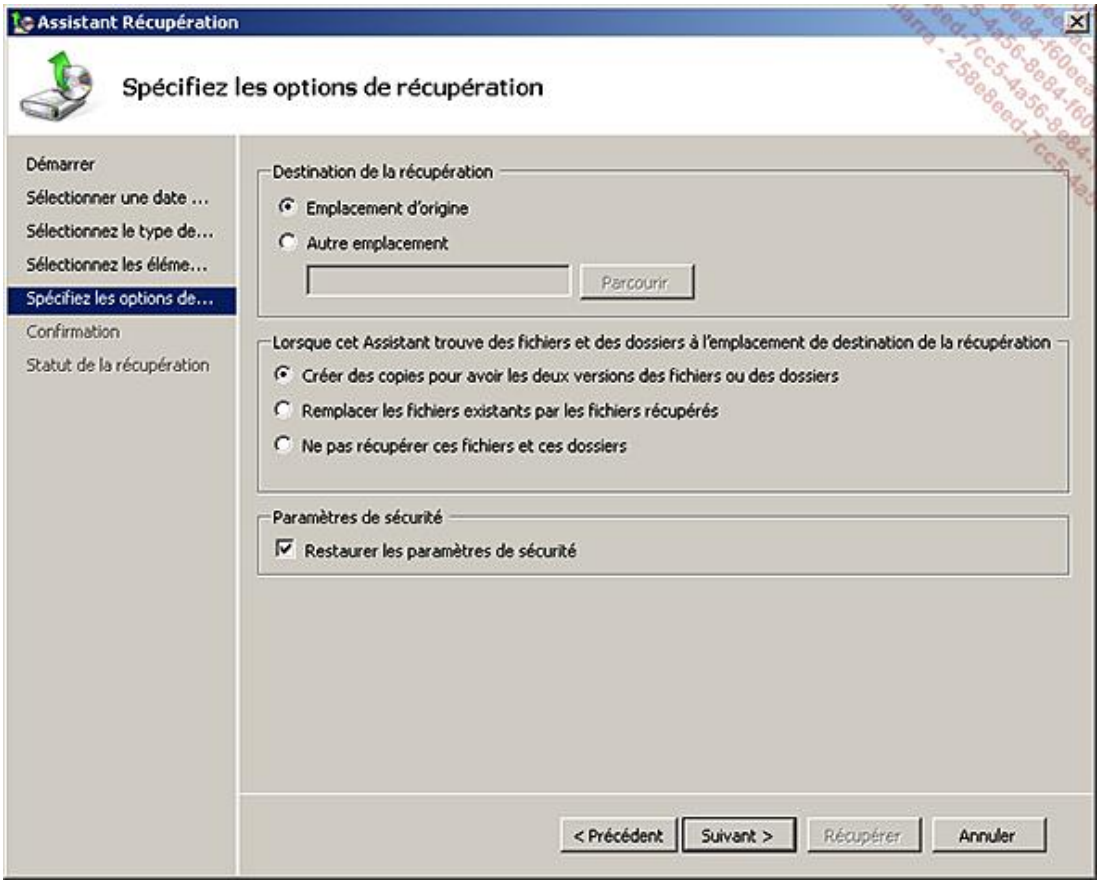
2. Restauration de données

Maintenant que vous savez comment sauvegarder vos données, vous allez voir comment les restaurer. Pour effectuer une restauration en utilisant WSB, vous devez être membre du groupe Opérateurs de sauvegarde ou du groupe Administrateurs de la machine.

a. Restauration des fichiers et/ou de dossiers

Pour effectuer la restauration d'un dossier :

- Allez dans la console **Sauvegarde de Windows Server**.
- Dans le volet de droite, cliquez sur **Récupérer**.
- Spécifiez le serveur pour lequel vous voulez récupérer les données, puis cliquez sur **Suivant**.
- Choisissez ensuite via le calendrier la sauvegarde que vous voulez restaurer puis cliquez sur **Suivant**.
- Choisissez le type de données que vous voulez récupérer (**fichiers et dossiers** ou **volumes**), puis cliquez sur **Suivant**.
- Choisissez l'élément (fichier et/ou dossier) à restaurer, puis cliquez sur **Suivant**.
- Spécifiez ensuite l'endroit où doit se faire la restauration, si vous voulez écraser les fichiers de destination ou bien effectuer une copie, ou ne pas récupérer les fichiers s'ils existent déjà à l'emplacement de destination. Spécifiez également si les droits NTFS doivent être récupérés.



- À la page de confirmation vérifiez les éléments choisis, puis cliquez sur **Récupérer**.

b. Restauration de l'état du système

© ENI Editions - All rights reserved - adamo diarra

En cas de défaillance majeure du système, vous devrez restaurer celui-ci. Cette opération s'apparente à une restauration complète, mais la différence est que vous ne restaurez pas les volumes contenant les données. Seuls les volumes critiques sont récupérés.

Cette opération peut s'effectuer sur la même machine ou, dans le cas d'un remplacement de matériel, sur une machine différente. Attention, la machine de remplacement doit cependant posséder des caractéristiques matérielles similaires.

La restauration du système est la manière la plus pratique de réparer des rôles de serveurs corrompus ou encore de restaurer Active Directory. Attention, il n'est pas possible d'effectuer une restauration partielle de l'état du système.

La restauration de l'état du système sur un contrôleur de domaine effectue une restauration non autoritaire de l'Active Directory.

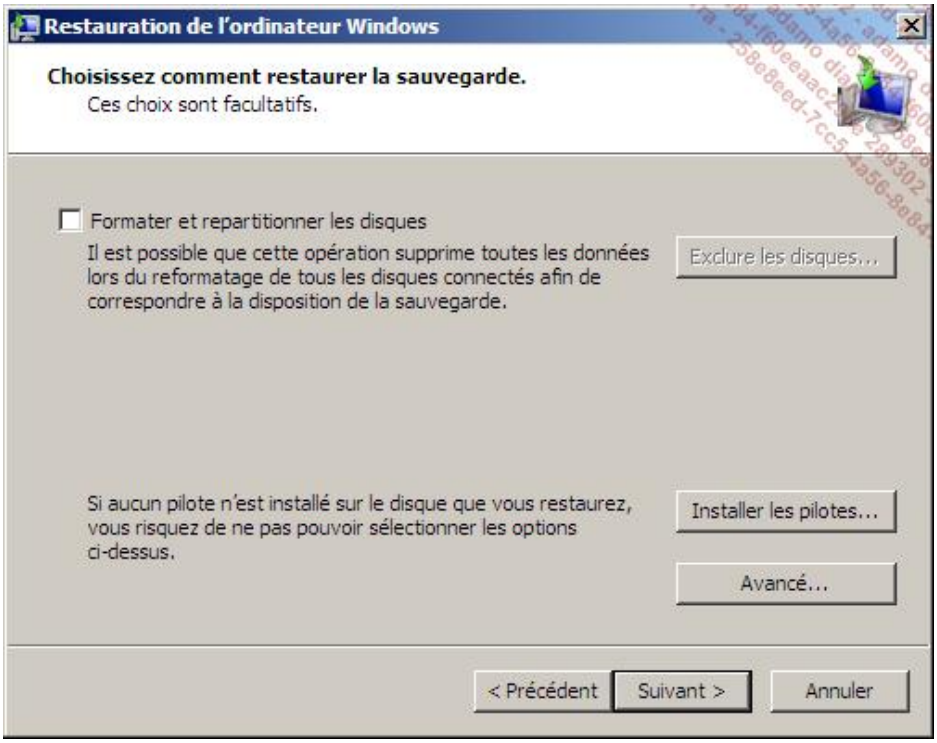
Voici les étapes à suivre pour procéder à la restauration de votre système :

- Démarrez votre serveur à partir du CD d'installation de Windows Server 2008 R2.
- Choisissez les paramètres de langues voulus puis cliquez sur **Suivant**.
- Cliquez sur **Réparer l'ordinateur**.
- Dans la fenêtre **Options de récupération système**, sélectionnez votre OS s'il est présent. Par contre, s'il s'agit d'un nouveau matériel, cliquez directement sur **Suivant**.
- Dans la fenêtre qui apparaît, cliquez sur **Restauration de l'ordinateur Windows**.

Notez qu'un outil de diagnostic de la mémoire a été directement intégré aux outils de réparation de Windows Server 2008 R2.

- Choisissez la sauvegarde à restaurer. Puis cliquez sur **Suivant**.
- Choisissez ensuite les options facultatives (formatage et repartitionnement des disques, installation de pilotes, etc.) puis cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- Cliquez sur **Terminer**, puis cochez la case de confirmation et enfin cliquez sur **OK**.
- Attendez que le système redémarre automatiquement pour que la restauration soit complètement terminée.

3. Grappe RAID

Une méthode alternative de fiabilisation des données existe. Très répandue dans les environnements serveurs et en expansion auprès des particuliers, cette technologie s'appelle RAID (*Redundant Array of Independent Disks*).

D'un point de vue simplifié, cette technologie permet de stocker les informations sur des disques durs multiples afin d'améliorer, en fonction du type de RAID choisi, la tolérance aux pannes et/ou les performances de l'ensemble.

Seuls les trois niveaux de RAID standard seront décrits dans ce chapitre à savoir : les RAID 0, RAID1 et RAID5. En fonction du niveau de RAID choisi, vous obtenez :

- soit un système de répartition qui améliore ses performances (RAID0) ;
- soit un système de redondance qui donne au stockage des données une certaine tolérance aux pannes matérielles (RAID1) ;
- soit les deux à la fois (RAID5).

Le système RAID est donc capable de gérer la répartition et la cohérence des données. Ce système de contrôle peut-être purement logiciel, ou utiliser un matériel dédié.

En RAID logiciel, le contrôle du RAID est intégralement assuré par une couche logicielle du système d'exploitation. Cette couche s'intercale entre la couche d'abstraction matérielle (pilote) et la couche du système de fichiers.

Dans le cas du RAID matériel, une carte ou un composant est dédié à la gestion des opérations. Du point de vue du système d'exploitation, le contrôleur RAID matériel offre une virtualisation complète du système de stockage. Le système d'exploitation considère chaque volume RAID comme un disque et n'a pas connaissance de ses constituants physiques.

Caractéristiques des niveaux de RAID :

- Le RAID0, ou agrégat par bandes, est le plus performant ; il est par contre le moins fiable. Il offre un cumul des disques. Par exemple trois disques de 500 Go en RAID0 vous fournissent un volume de 1,5 To. Inconvénient majeur de cette technologie, si un des disques vient à tomber en panne, les données situées sur les autres sont également perdues.

© ENI Editions - All rights reserved - adamo diarra

- LE RAID1, ou miroir, fournit de bonnes performances en écriture tout en assurant une tolérance de pannes. Dans le cas de deux disques en RAID1, les informations sont écrites de façon identique sur les deux disques. Deux disques de 500 Go en RAID1 fournissent un espace de stockage de 500 Go. Le second disque servant de « réplica » au premier. Les performances globales restent néanmoins inférieures à un RAID0.

- Le RAID5, ou agrégat par bandes avec parité est le plus performant en termes de lecture. Les informations sont réparties sur les différents disques de sorte à ne pas perdre de données en cas de panne d'un des disques. Ce niveau de RAID requiert un minimum de trois disques. Trois disques de 500 Go configurés en RAID5 offrent un espace de stockage de 1 To.

Sous Windows Server 2008 R2, les opérations de configuration des volumes en RAID se font depuis la console **Gestionnaire de serveur**. Ensuite il faut naviguer dans l'arborescence de stockage. Les options proposées vous permettront d'ajouter facilement un volume miroir ou de créer un agrégat.

Pour pouvoir configurer des volumes en RAID sous Windows Server 2008 R2, il faut avoir converti les disques en dynamique au préalable.

Windows Server 2008 R2 comme ses prédécesseurs ne permet pas de configurer le volume système en RAID5.

© ENI Editions - All rights reserved - adamo diarra

Gestion des mises à jour

1. Présentation de WSUS

Un autre moyen de vous prémunir contre d'éventuels problèmes est de vous assurer que vos machines clientes et serveurs sont bien mises à jour. Sur de petits parcs, configurer sur chaque poste les mises à jour en mode automatique est bien souvent suffisant. Sur de grands parcs informatiques, dans lesquels les configurations des machines sont strictes, il est parfois nécessaire de tester un patch avant de le déployer de façon centralisée sur tous les postes.

Microsoft met gratuitement à disposition l'outil WSUS (*Windows Server Update Services*) en version 3.0 avec SP2 (WSUS existe comme un rôle à part entière dans Windows Server 2008 R2 et est donc directement installable depuis la console **Gestionnaire de serveur** sans devoir télécharger quoi que ce soit). Cet outil permet le déploiement des dernières mises à jour pour les produits Microsoft. En l'utilisant, vous pouvez gérer intégralement la distribution des mises à jour (heure de déploiement, quels sont les patchs à déployer, etc.).

Vous disposez grâce à WSUS d'un outil de centralisation et de suivi de la gestion des mises à jour. Il vous est possible en un seul coup d'œil de voir quel poste n'a pas reçu les dernières mises à jour nécessaires et de les lui pousser.

Suivant votre infrastructure, WSUS peut se mettre à jour avec le site Microsoft Update ou encore avec un autre serveur WSUS. Les clients compatibles avec WSUS apparaissent à partir de Windows 2000 SP4. Outre les systèmes d'exploitation, WSUS permet la mise à jour des applicatifs Microsoft les plus courants (SQL Server, Exchange Server, Office, etc.).

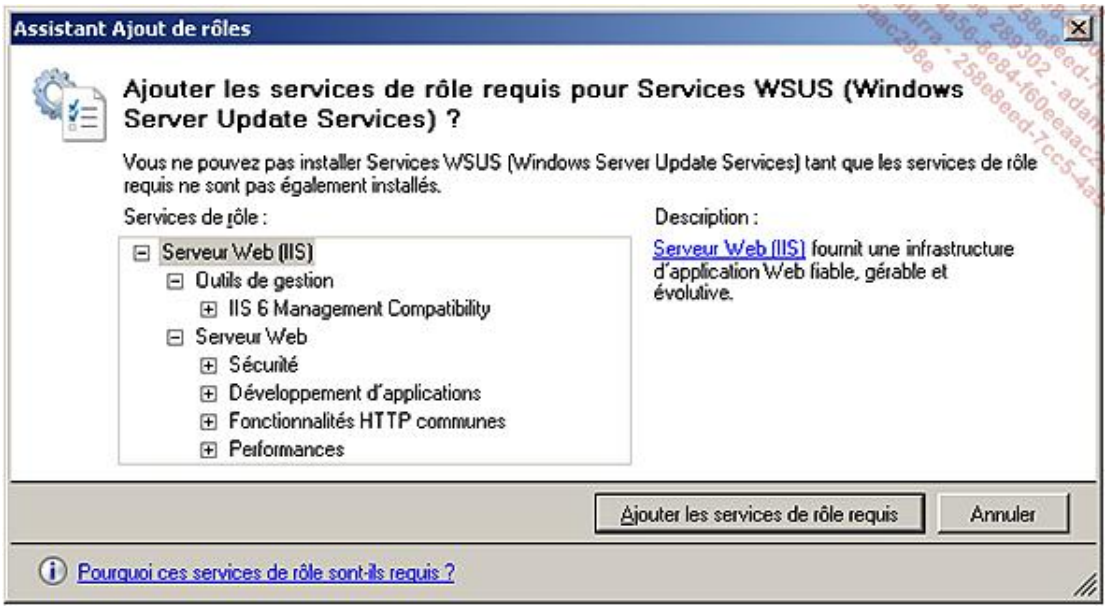
2. Installation de WSUS

a. Installation sur Windows Server 2008 R2

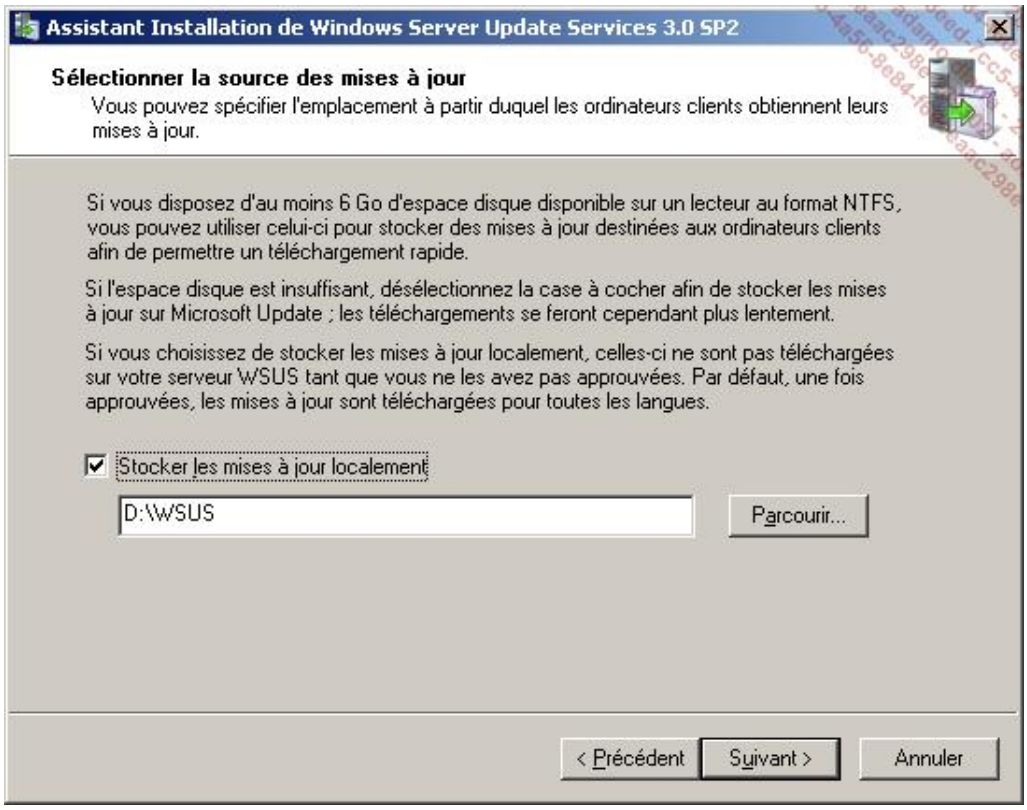
L'installation de WSUS sur la version R2 de Windows Server 2008 est largement facilitée par la sélection automatique des pré-requis lors de l'installation du rôle.

- Ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer** - **Outils d'administration**, puis **Gestionnaire de serveur**.
- Dans le volet gauche, sélectionnez **Rôles**, puis dans le volet droit cliquez sur **Ajouter des rôles**.
- Cliquez sur **Suivant**.
- Cochez la case **Services WSUS (Windows Server Update Services)**. La fenêtre suivante apparaît.

© ENI Editions - All rights reserved - adamo diarra

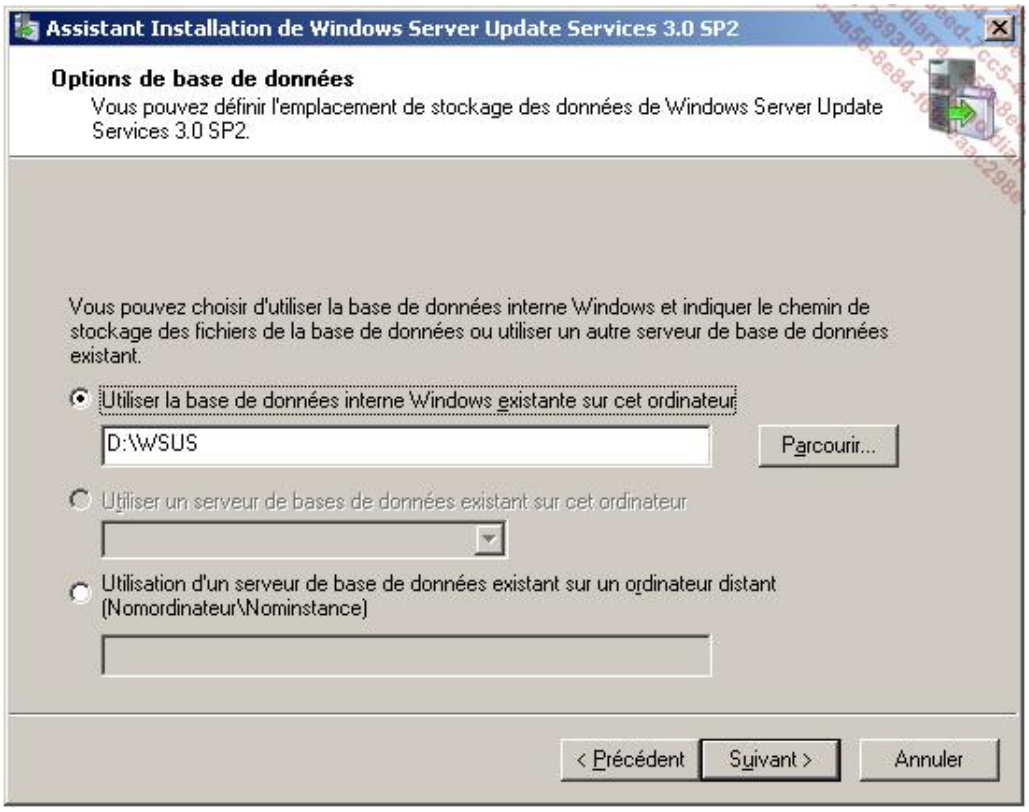


- Cliquez sur **Ajouter les services de rôle requis**.
- Cliquez sur **Suivant** trois fois, puis cliquez sur **Installer**.
- Une nouvelle boîte de dialogue s'ouvre, sélectionnez le bouton radio **J'accepte les termes du contrat de licence**.
- Cliquez sur **Suivant** deux fois.

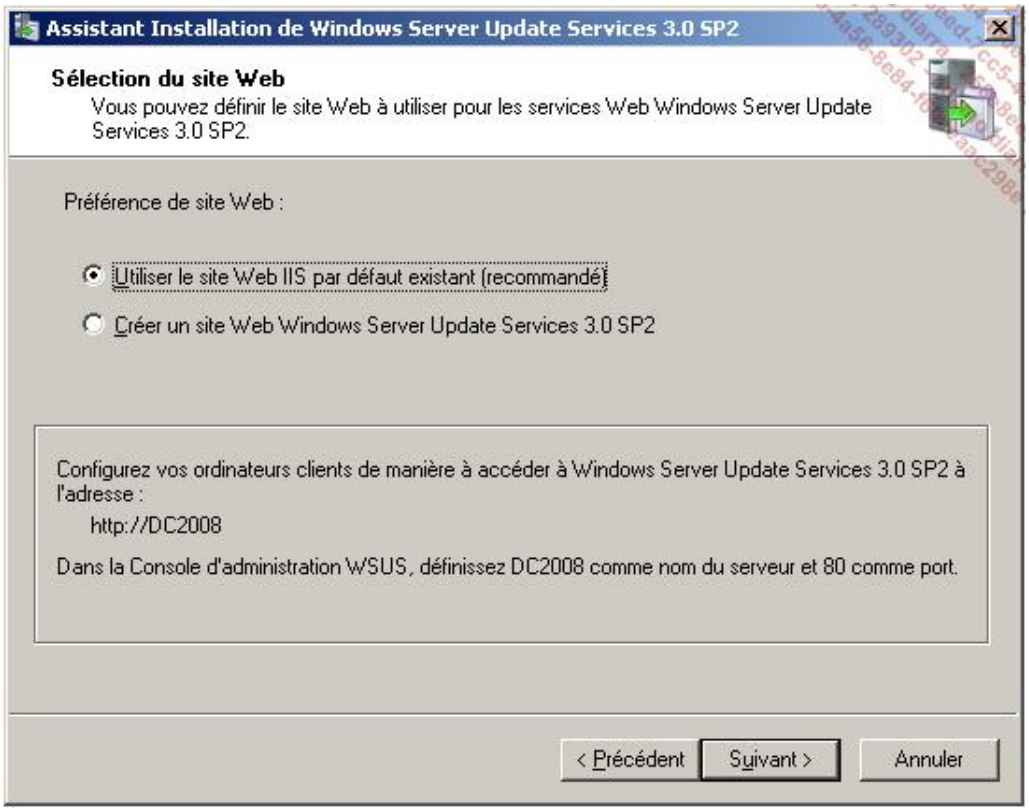


- Spécifiez l'emplacement de stockage des mises à jour puis cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra



- Choisissez l'emplacement de la base de données WSUS puis cliquez sur **Suivant**.

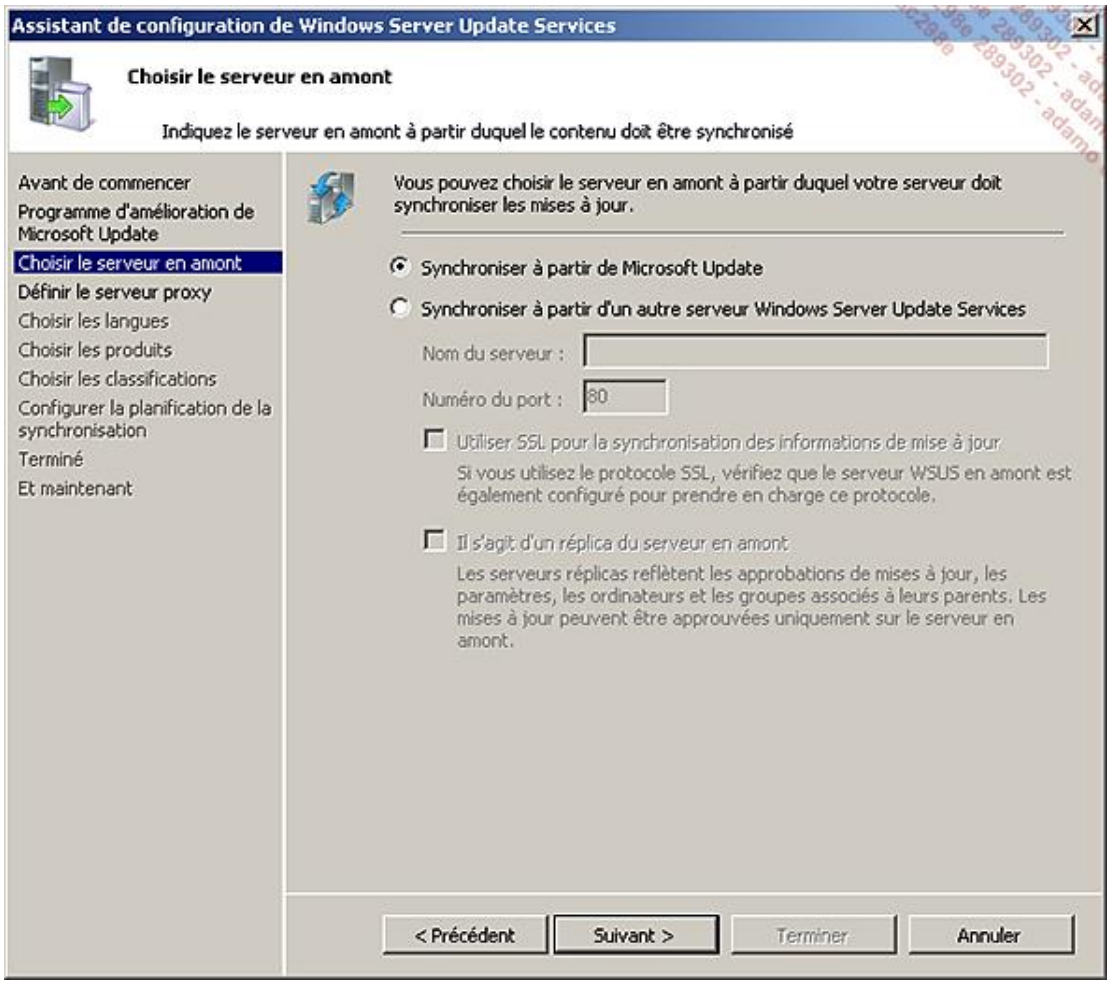


- Choisissez le site sur lequel vous voulez que WSUS soit installé puis cliquez sur **Suivant**.
- Sur la page récapitulative cliquez sur **Suivant**.
- Une fois l'installation finalisée, cliquez sur **Terminer**. L'assistant de configuration de WSUS se lance.

© ENI Editions - All rights reserved - adamo diarra

- À la page de présentation de la configuration, cliquez sur **Suivant**.
- Laissez cochée la case permettant de participer au programme d'amélioration puis cliquez sur **Suivant**.
- Laissez cochée la case **Synchroniser à partir de Microsoft Update** puis cliquez sur **Suivant**.
- Si vous n'utilisez pas de proxy, n'indiquez rien au niveau de la page proxy puis cliquez sur **Suivant**.

  Si vous utilisez un proxy, cette page permet de spécifier sa configuration.



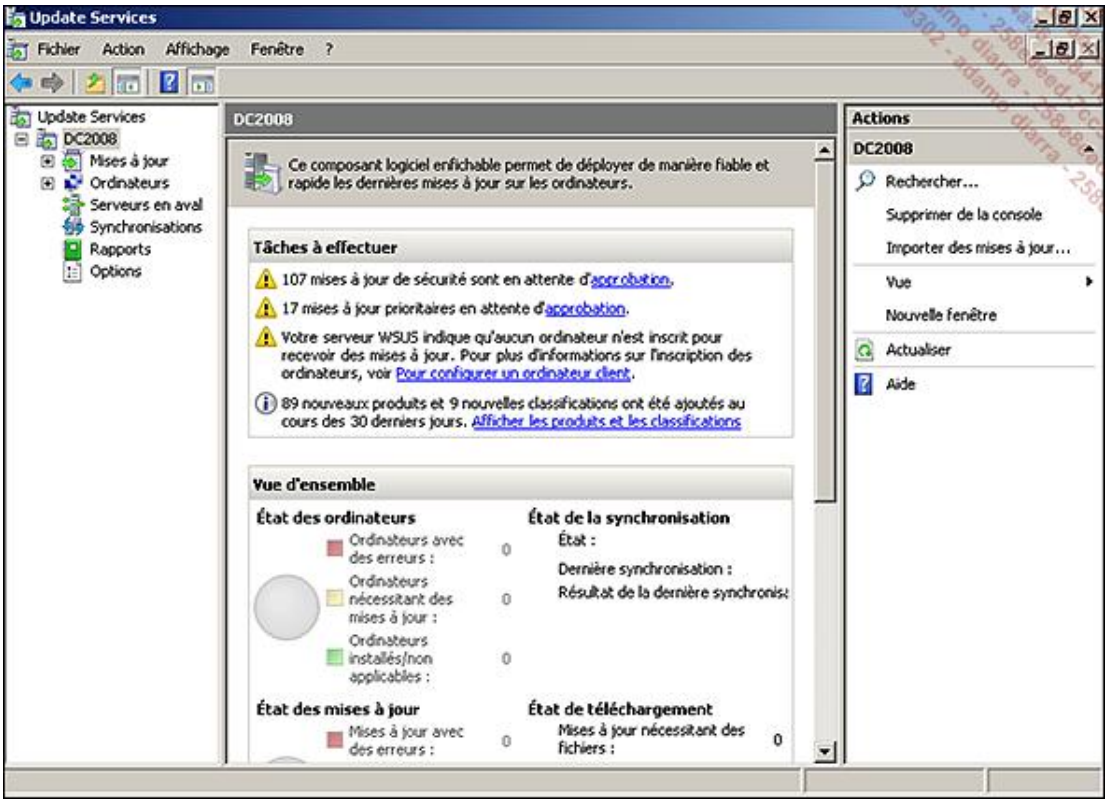
- Suivant l'architecture en place, sélectionnez **Synchroniser à partir de Microsoft Update** ou spécifiez un serveur WSUS comme source des mises à jour, puis cliquez sur **Suivant**.
- Cliquez sur **Démarrer la connexion** afin que WSUS récupère les informations disponibles au téléchargement. Une fois la connexion terminée, cliquez sur **Suivant**.
- Sélectionnez les langues utilisées par vos différents systèmes d'exploitation (dans notre exemple le français) si ce n'est pas déjà fait automatiquement puis cliquez sur **Suivant**. WSUS téléchargera alors tous les patchs dans les langues demandées. Prévoyez donc un espace disque conséquent si vous choisissez plusieurs langues.
- Dans la liste de sélection des produits, sélectionnez les produits que vous souhaitez mettre à jour, puis cliquez sur **Suivant**.
- Sélectionnez les classifications de mises à jour voulues, puis cliquez sur **Suivant**.
- Choisissez votre mode de synchronisation (manuelle ou automatique), puis cliquez sur **Suivant**.

© ENI Editions - All rights reserved - adamo diarra

- Cliquez sur **Suivant**, puis sur **Terminer**, et enfin sur **Fermer**.

3. Utilisation de WSUS

Une fois l'outil installé, sa console MMC d'administration s'ouvre automatiquement. Vous pouvez y contrôler rapidement l'état de mise à jour de votre parc ainsi que les mises à jour en attente d'approbation.



Cette console est accessible depuis les **Outils d'administration** dans le menu **Démarrer** sous le nom de **Microsoft Windows Server Update Services**.

Avant tout, il faut configurer les clients pour utiliser le serveur WSUS nouvellement installé.

Si vous disposez d'un domaine Active Directory, créez une nouvelle stratégie de groupe GPO au niveau du domaine ou d'une OU. Si votre PC n'est pas dans un domaine, utilisez la commande `gpedit.msc`.

- Dans l'**éditeur d'objets de stratégie de groupe**, développez **Configuration ordinateur - Modèles d'administration - Composants Windows - Windows Update**.
- Dans le volet de droite, éditez le paramètre **Spécifier l'emplacement Intranet du service de Mise à jour Microsoft**.
- Cochez la case **Activé**, puis saisissez l'URL d'accès à votre serveur WSUS dans les deux champs.

  Exemple : http://dc2008.masociete.local
- Cliquez ensuite sur **Appliquer**, puis **OK**.
- Éditez ensuite le paramètre **Configuration du service Mises à jour automatiques**.

  Cochez la case **Activé**, puis spécifiez la configuration des mises à jour automatiques (**notifier pour télécharger et installer**, **télécharger et planifier l'installation**, etc.).

  Choisissez ensuite les jours et les heures des installations des mises à jour.

© ENI Editions - All rights reserved - adamo diarra

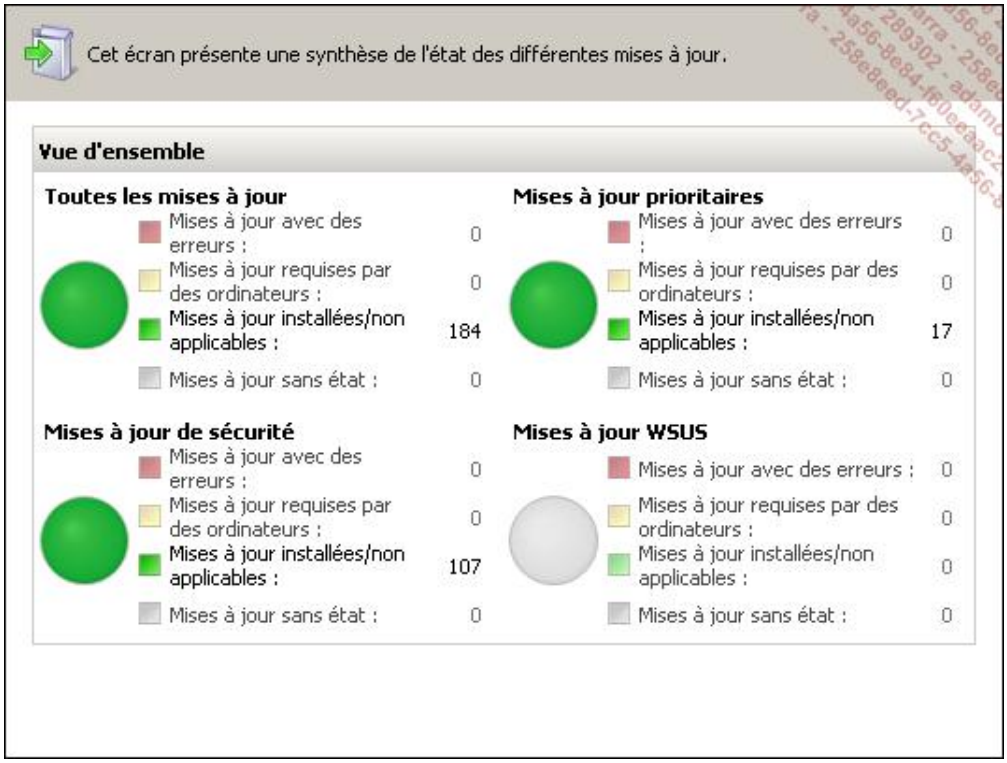
- Validez en cliquant sur **Appliquer**, puis **OK**.
- Fermez ensuite votre éditeur de stratégie de groupes.

Vous pouvez forcer le rafraîchissement de la stratégie de groupe sur le poste client via la commande `gpupdate`.

Pour forcer la détection par WSUS d'une machine cliente, lancez depuis le poste la commande `wuauclt /detectnow`.

Depuis la console **Microsoft Windows Server Update Services**, vous pouvez ensuite afficher l'état de déploiement des mises à jour.

- Développez l'arborescence et cliquez sur **Mises à jour**.



Des vues préconfigurées sont disponibles. Elles répondent aux besoins de la majorité des administrateurs. Vous pouvez cependant créer des vues personnalisées si vous avez besoin d'informations particulières. Les critères sont nombreux : par produit, par classification, par groupes, etc.

Il est également possible d'obtenir des rapports détaillés sur les mises à jour. Il suffit pour cela d'aller dans la rubrique associée et de choisir le rapport à visualiser.

© ENI Editions - All rights reserved - adamo diarra

Des rapports préconfigurés sont mis à votre disposition. Vous n'avez pas la possibilité d'en créer de nouveaux. Les modèles préexistants sont générés à la demande de façon à avoir les informations les plus à jour possibles.

La rubrique **Options** vous permet de configurer les options déjà spécifiées à l'installation (langues, classifications, produits, etc.) ainsi que d'autres paramètres :

- **Approbations automatiques** : permet de définir la façon dont sont appliquées les types de mises à jour (sécurité, critiques) pour des ordinateurs définis.
- **Notifications électroniques** : permet d'envoyer des notifications de rapports sur les mises à jour par mail.
- **Assistant de nettoyage du serveur** : permet de nettoyer les anciens ordinateurs, les anciennes mises à jour et les anciens fichiers de mise à jour.
- **Ordinateurs** : permet de spécifier si les groupes d'ordinateurs pour la mise à jour sont gérés depuis WSUS ou via une stratégie de groupe.
- **Personnalisation** : permet, dans le cas de l'utilisation de serveurs WSUS « enfants », d'avoir un état des ordinateurs qui lui sont associés.
- **Cumul des rapports** : permet dans le cas d'une architecture avec un WSUS frontal d'avoir une centralisation de tous les WSUS « enfants ».

Vous avez vu grâce à ce chapitre des éléments essentiels à la sécurisation de votre parc. En matière de système informatique il vaut mieux ne pas se contenter d'agir après coup. Soyez proactif, et vous gagnerez en rapidité pour remettre votre infrastructure en état de marche en cas de problème majeur.

Pensez votre schéma de sauvegarde en fonction de vos besoins (volume, plage horaire, etc.). Les clichés instantanés

© ENI Editions - All rights reserved - adamo diarra

sont un très bon complément à l'outil de sauvegarde Windows Server Backup. N'hésitez pas également à vous tourner vers des produits tiers comme celui de Microsoft (System Center Data Protection Manager). Ils vous offriront une granularité supplémentaire ainsi que des possibilités étendues de sauvegarde de vos applications (Exchange, SQL, SharePoint, etc.).

Vous prémunir face aux menaces comme les virus, les exploitations de failles et autres désagréments est également indispensable. Conserver vos applications toujours à jour permet de corriger les défauts de celles-ci. WSUS est gratuit, profitez-en, il vous facilitera grandement la difficile tâche de la gestion des patches de sécurité Microsoft. Plus besoin de passer individuellement sur chaque PC pour contrôler l'état de mise à jour, ni même pour forcer les mises à jour. Tout est désormais gérable à distance, de façon centralisée et simplifiée.

© ENI Editions - All rights reserved - adamo diarra

Après Windows Server 2008 R2 et Windows 7

La prochaine version de Windows Server devrait utiliser un nouveau noyau dont le nom de code est **Windows 8**. Bien entendu, ce nouveau noyau sera commun avec la future évolution de Windows 7. Il y a encore très peu d'informations diffusées par Microsoft sur ce futur système, seulement des indiscrétions.

Le prochain noyau ne serait prévu qu'en version 64 bits et peut-être 128 bits, basé sur le **Processeur Intel® Core™ i7**. L'utilisation du code 64 bits est l'occasion pour Microsoft de supprimer de nombreuses parties de code 32 bits conservées pour des questions de compatibilité.

L'environnement MIDORI, une interface Web et modulaire (issue de l'approche Singularity) pouvant se mettre à jour en ligne et qui avait un moment été prévue pour Windows 7, serait adaptée à Windows 8. Midori se présente sous la forme de deux noyaux : un micro-noyau pour gérer le matériel, l'environnement en code non managé (c'est-à-dire non géré) et un noyau de services en code managé qui fournirait la base du système d'exploitation. Le code non managé correspond à des programmes et exécutables directement interprétés par le processeur, sans contrôle automatique de la bonne exécution. Le code managé est exécuté dans un environnement de contrôle (type CLR ou machine virtuelle Java) vérifiant la bonne initialisation des variables, les permissions, ainsi que le nettoyage des éléments devenus inutiles.

Il y aura probablement une solution de virtualisation pour exécuter les anciennes applications 32 bits, comme cela est réalisé dans Windows 7 pour les applications XP.

Une nouvelle version du rôle **File Server** (*partage de fichier*) avec une convergence des fonctions de réplication de DFS et du BranchCache pour de nouvelles fonctionnalités révolutionnaires serait à l'étude.

La prochaine version de Windows administrera les serveurs par **grappes** et utilisera de nouveaux systèmes de réplication.

Microsoft travaillerait aussi sur une nouvelle interface graphique (un nouveau Framework) visant à remplacer l'interface vieillissante GDI et la WPF (*Windows Presentation Foundation*) qui est encore assez peu utilisée. L'intégration de Direct2D dans Windows 7 est une première approche.

Bien entendu, ces informations sont données avec toutes les réserves d'usage et des revirements sont toujours possibles lorsqu'il s'agit de nouveaux développements et d'adéquation avec le marché.

© ENI Editions - All rights reserved - adamo diarra

Le calendrier attendu

Windows 7 et Windows 2008 R2 SP1 sont maintenant sortis officiellement.

Pour Windows 8 et la version serveur correspondante, tout laisse à penser qu'il sont prévus pour la fin de l'année 2012.

En effet, Microsoft souhaite raccourcir le délai nécessaire entre la sortie d'une version majeure ou mineure de Windows : 2 ans entre une version majeure (2003) et une version mineure (2003 R2, sortie en 2005) puis environ 3 ans avant la version majeure suivante (2008) puis à nouveau environ 2 ans.

Si cette cadence est maintenue, elle permettrait d'éviter les versions intermédiaires, et d'éviter aux utilisateurs de s'habituer à une version précise comme ce fût le cas avec Windows XP, mais aussi de répondre à certains systèmes concurrents comme Apple dont les nouvelles versions sortent régulièrement.

© ENI Editions - All rights reserved - adamo diarra